UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

VAGNER PEREIRA COSTA

CONJECTURAS EM ANÉIS DE GRUPO

VITÓRIA
2018

VAGNER PEREIRA COSTA

CONJECTURAS EM ANÉIS DE GRUPO

Dissertação de mestrado apresentada ao PPGMAT como parte dos requisitos exigidos para a obtenção do título de Mestre em Matemática

Orientador: Prof. Dr. Renato Fehlberg Júnior

VITÓRIA
2018

Dados Internacionais de Catalogação-na-publicação (CIP)
(Biblioteca Central da Universidade Federal do Espírito Santo, ES, Brasil)
Bibliotecária: Michele Rodrigues da Silva – CRB-6 ES-000630/O

Costa, Vagner Pereira, 1989-
C837c Conjecturas em anéis de grupo / Vagner Pereira Costa. – 2018.
97 f.

Orientador: Renato Fehlberg Júnior.
Dissertação (Mestrado em Matemática) – Universidade Federal do Espírito Santo, Centro de Ciências Exatas.

1. Anéis (Álgebra). 2. Isomorfismos (Matemática). 3. Unidades de medida. I. Fehlberg Júnior, Renato. II. Universidade Federal do Espírito Santo. Centro de Ciências Exatas. III. Título.

CDU: 51

UNIVERSIDADE FEDERAL DO ESPÍRITO SANTO
Centro de Ciências Exatas
Programa de Pós-Graduação em Matemática

"Conjecturas em Anéis de Grupo"

Vagner Pereira Costa

Dissertação submetida ao Programa de Pós-Graduação em Matemática da Universidade Federal do Espírito Santo como requisito parcial para a obtenção do título de Mestre em Matemática.

Aprovada em 07/03/2018 por:

Renato Fehlberg Junior – UFES

Thiago Filipe da Silva - UFES

Javier Sánchez Serdà - IME/USP

Dedicatória

À minha esposa e ao meu filho Miguel.

Agradecimentos

Agradeço primeiramente a Deus, poderoso e soberano, digno de toda honra e adoração, por ter me sustentado até aqui.

Agradeço à minha esposa, a quem dedico essa dissertação, por todo companheirismo, compreensão e oração.

Agradeço à minha família por todo apoio, sempre preocupados com os meus resultados.

Agradeço ao meu orientador, professor Renato Felhberg Júnior, por toda assistência a mim fornecida. Sou imensamente grato por ter aceito orientar este trabalho. Sua orientação foi primordial para a conclusão do mesmo.

Agradeço aos professores Thiago Filipe da Silva e Javier Sanchéz Serdà pela leitura criteriosa da versão preliminar e pelas dicas e correções que contribuiram para esta versão final.

Agradeço a todos os professores do Departamento de Matemática que tive o privilégio de ser aluno na licenciatura, em especial, agradeço aos professores do PPGMAT.

Agradeço aos meus colegas discentes do PPGMAT, com os quais convivi nesses últimos anos, pelas valiosas trocas de informação.

Agradeço à CAPES pelo apoio financeiro.

Resumo

Os anéis de grupo possuem uma estrutura algébrica muito rica, uma vez que para explorá-la precisamos recorrer a outras técnicas além da teoria de grupos e da teoria de anéis; precisamos recorrer também à teoria dos números algébricos, a representação de grupos e álgebras e outras teorias algébricas. Dentre os assuntos de interesse em anéis de grupo, destacamos algumas conjecturas que serão os objetos de estudo da presente dissertação: o problema do isomorfismo, o problema do normalizador e as conjecturas de Zassenhaus. Sobre o problema do isomorfismo e o problema do normalizador, demonstraremos sua validade em alguns casos particulares e apresentaremos os contraexemplos conhecidos. Sobre as conjecturas de Zassenhaus, enunciaremos e apresentaremos para quais classes de grupo elas foram demonstradas. Mostraremos como essas conjecturas estão relacionadas ao problema do isomorfismo.

Palavras-chaves: Anéis de grupo. O problema do isomorfismo. O problema do normalizador. As conjecturas de Zassenhaus. Aplicação de aumento. Isomorfismo normalizado. Unidades.

Abstract

Group rings have a very rich algebraic structure, since to explore it we must resort to techniques other than group theory and ring theory; we must also resort to the theory of algebraic numbers, the representation of groups and algebras and other algebraic theories. Among the subjects of interest in group rings, we highlight some conjectures that will be the objects of study of the present dissertation: the isomorphism problem, the normalizer problem and the Zassenhaus conjectures. On the isomorphism problem and the normalizer problem, we will prove its validity in some particular cases and it will be presented the known counterexamples. On the Zassenhaus conjectures, we will enunciate and present for which group classes they were proved. We will show how these conjectures relate to the isomorphism problem.

Key-Words: Group rings. The isomorphism problem. The normalizer problem. The Zassenhaus conjectures. Augmentation mapping. Normalized isomorphism. Units.

Sumário

[1] Definida por Hyman Bass em [30]

Introdução

Na teoria dos Anéis de Grupo, um dos problemas de grande destaque é o chamado **Problema do Isomorfismo**. Tal problema possui diferentes versões, mas que em sua essência questiona se a existência de um isomorfismo de R-álgebras entre os anéis de grupo RG e RH implica na existência de um isomorfismo entre G e H. Veremos, a partir da definição de anel de grupo, que é sempre verdade que grupos isomorfos induzem anéis de grupo isomorfos sobre o mesmo anel, qualquer que seja o anel. Então, a questão mais relevante é: para um determinado anel R e para grupos G e H, seria verdade que $RG \simeq RH \Rightarrow G \simeq H$?

O primeiro trabalho relacionado ao problema do isomorfismo foi publicado por G. Higman em 1940 [7], onde ele diz: *"Se é possível que dois grupos não isomorfos tenham anéis de grupo integral isomorfos, não sei; mas os resultados da Seção 5 sugerem que é improvável "*. Desde então, diversos autores contribuiram para o avanço dessa questão.

De modo geral o problema do isomorfismo tem resposta negativa. Reservaremos uma seção no capítulo 3 para mostrar tal fato, onde exibiremos dois grupos, G e H, abelianos de mesma ordem, tais que $G \ncong H$, mas $\mathbb{C}G \simeq \mathbb{C}H$, onde $\mathbb{C}$ é o corpo dos complexos.

O problema do isomorfismo foi posto pela primeira vez na Conferência de Álgebra em Michigan em 1947 por T. M. Thrall com a seguinte formulação: *"Dados um grupo G e um corpo K, determine todos os grupos H tais que $KG \simeq KH$"*. Em 1950, S. Perlis e G. Walker [8] provaram que grupos abelianos finitos são determinados por seus anéis de grupo sobre o corpo dos racionais, ou seja, se G é um grupo abeliano finito e H é outro grupo tal que $\mathbb{Q}G \simeq \mathbb{Q}H$, então $G \simeq H$. W. E. Deskins [9] mostrou que p-grupos abelianos são determinados por seus anéis de grupo sobre qualquer corpo de característica p. Isso parecia sugerir que, para famílias específicas de grupos, poder-se-ia determinar um corpo adequado para o qual o problema do isomorfismo tivesse resposta positiva. Porém, E. Dade em [29] publicou um exemplo de dois grupos metacíclicos não isomorfos, porém com anéis de grupo isomorfos sobre qualquer corpo K.

Isso levou a concentrar o problema do isomorfismo a anéis de grupo sobre o anel dos inteiros $\mathbb{Z}$. Uma razão é o fato de que se tivermos $\mathbb{Z}G \simeq \mathbb{Z}H$, então $RG \simeq RH$ (como R-álgebras), para qualquer anel comutativo R. Isso será justificado no capítulo 3. Assim, sobre os anéis dos inteiros foi formulada a seguinte conjectura, a qual é conhecida por (ISO):

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

Recentemente, Martin Hertweck em [6] apresentou um contraexemplo para

ISO, exibindo dois grupos de mesma ordem, a saber, $2^{21}.97^{28}$, não isomorfos, porém com anéis de grupo isomorfos sobre os inteiros.

A existência de um contraexemplo não torna o assunto menos importante, apenas mudam-se os rumos das pesquisas, que agora passam a ser a de classificar para quais classes de grupos ISO tem resposta positiva.

A conjectura ISO foi demonstrada em uma série de casos particulares, por exemplo, para grupos abelianos e 2-grupos Hamiltonianos (*Higman* em [7]), grupos metabelianos (*Whitcomb* em [10]), grupos nilpotentes (*Roggenkamp e Scott* em [2]), grupos simétricos e alternados, grupos finitos que são grupos de unidades de algum anel, grupos circulares (*R. Sandling* em [25]).

Destaca-se também na teoria dos anéis de grupo as questões relacionadas ao grupo das unidades. Uma das questões é determinar o normalizador do grupo G dentro do grupo das unidades de $\mathbb{Z}G$. O próprio grupo G e $Z(U(\mathbb{Z}G))$, o centro do grupo das unidades de $\mathbb{Z}G$, normalizam G em $U(\mathbb{Z}G)$ e são chamados de normalizadores triviais. A conjectura do normalizador afirma que os normalizadores triviais determinam todo o normalizador de G em $U(\mathbb{Z}G)$, isto é,

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

Martin Kertweck em [6] na construção do contraexemplo para a conjectura ISO, obteve também um contraexemplo para a conjectura do normalizador. Ainda sobre o grupo das unidades do anel de grupo $\mathbb{Z}G$, no início da década de setenta, H.J Zassenhaus formulou uma série de conjecturas, as quais dizem respeito à conjugação de subgrupos do grupo das unidades de $\mathbb{Z}G$ por unidades de $\mathbb{Q}G$.

A presente dissertação está dividida em quatro capítulos. No capítulo 1 desenvolveremos os conceitos preliminares, falaremos da teoria dos módulos e uma breve abordagem sobre produto tensorial. No capítulo 2 definiremos anéis de grupo e estudaremos os principais resultados. No capítulo 3 mostraremos que grupos abelianos finitos não estão determinados por seus anéis de grupo sobre o corpo dos complexos, em seguida apresentaremos os resultados centrais desta dissertação, onde demonstraremos a validade da conjectura ISO para algumas classes de grupos finitos. As classes a serem abordadas serão: grupos abelianos, 2-grupos Hamiltonianos, grupos Metabelianos e grupos Nilpotentes. No capítulo 4 apresentaremos as conjecturas de Zassenhaus sobre o grupo das unidades do anel de grupo integral, as classes de grupo para os quais tais conjecturas foram provadas e como essas conjecturas estão relacionadas com o problema do isomorfismo. Falaremos sobre o problema do normalizador e demonstraremos alguns casos para os quais valem a conjectura. Finalizaremos apresentando os contraexemplos das referidas conjecturas.

Lista de Notações

Ao longo dessa dissertação adotaremos as seguintes notações:

R - Anel.

G - Grupo finito.

$Z(G)$ - Centro do grupo G.

G' - subgrupo dos comutadores de G.

(H, K) - subgrupo de G gerado por $xyx^{-1}y^{-1}$, $x \in H,\ y \in K$ com H e K subgrupos de G.

$N_G(H)$ - O normalizador em G do subgrupo H.

$C_G(H)$ - O centralizador em G do subgrupo H.

$\mathbb{Z}$ - Anel dos inteiros.

RG - Anel de grupo de G por R.

$supp(\alpha)$ - suporte de α.

$U(\mathbb{Z})$ - Unidades do anel de grupo $\mathbb{Z}G$.

$U_1(\mathbb{Z})$ - Unidades normalizadas do anel de grupo $\mathbb{Z}G$.

ϵ - Aplicação de aumento.

$\Delta(G)$ - Ideal de aumento, o kernel da aplicação de aumento.

$\Delta(G, H)$ - Ideal de RG gerado por $(h-1)$ com $h \in H$.

$M_n(K)$ - Matriz $n \times n$ com coeficientes em K.

$Inn(G)$ - Grupo dos automorfismos internos de G.

S_n - Grupo das permutações de ordem n.

D_n - O grupo Dihedral.

Capítulo 1

Preliminares

Para os fins desta dissertação, um anel R é um conjunto não-vazio juntamente com duas operações binárias, $+$ e $\cdot$, denominadas soma e produto, respectivamente, tais que :

i) (R, +) é um grupo abeliano

ii) O produto é associativo

iii) Vale a distributividade do produto com relação à soma.

Se além disso o produto for comutativo, então $(R, +, \cdot)$ é dito comutativo. Se o produto tem um elemento neutro então $(R, +, \cdot)$ é dito anel com unidade. Denotaremos a unidade de um anel por "1".

1.1 Módulos e Álgebras

No presente capítulo apresentaremos os conceitos preliminares. Começamos com a definição e alguns resultados básicos sobre módulos. Daremos uma condição para que um módulo seja semissimples e finalizamos o capítulo com o conceito de produto tensorial.

Definição 1.1.1. *Seja R um anel com unidade. Um grupo abeliano aditivo M é chamado um R-módulo (à esquerda) se existe uma função*

$$\cdot : R \times M \to M,$$

definida por

$$(r, m) \mapsto r.m$$

tal que $\forall\, a, b \in R$ e $m, m_1, m_2 \in M$, valem:

(i) $(a + b)m = am + bm$.

(ii) $a(m_1 + m_2) = am_1 + am_2$.

(iii) $a(bm) = (ab)m$.

(iv) $1m = m$.

De modo similar, dado um anel R definimos um R-módulo à direita.

Observação 1.1.2. Segue da definição que se K é um corpo, então o conceito de *K-módulo* coincide com a noção de espaço vetorial sobre o corpo K.

Definição 1.1.3. *Seja R um anel comutativo. Um R-módulo A é chamado uma R-álgebra se existe uma multiplicação, definida em A, tal que, com a adição dada em A e esta multiplicação, A é um anel satisfazendo*

$$r(ab) = (ra)b = a(rb)$$

$\forall\, r \in R$ *e* $\forall\, a, b \in A$.

Exemplo 1.1.4. Seja I um ideal à esquerda de um anel R e seja R/I o grupo quociente sob adição. Então R/I possui uma estrutura de R-módulo com o produto

$$r(a + I) = ra + I, \forall\, r,\ a \in R.$$

Exemplo 1.1.5. Seja L um ideal à esquerda de um anel R. Como o produto de elementos de R por elementos de L permanecem em L, segue que L pode ser considerado com um R-módulo à esquerda. Analogamente um ideal à direita pode ser considerado um R-módulo à direita, em particular, um anel R é sempre um módulo sobre si mesmo.

Definição 1.1.6. *Seja M um módulo sobre um anel R. Um subconjunto não vazio $N \subset M$ é chamado um R-submódulo de M se as seguintes condições são satisfeitas:*

$(i)\, \forall\, x, y \in N$, *temos que* $x + y \in N$.

$(ii)\, \forall\, r \in R$ *e* $\forall\, n \in N$, *temos que* $rn \in N$.

Observação 1.1.7. Segue da definição acima que se V é um espaço vetorial sobre um corpo K, então os K-submódulos de V são exatamente os seus subespaços vetoriais. Similarmente os $\mathbb{Z}$-submódulos de um grupo abeliano A são os seus subgrupos.

Exemplo 1.1.8. Seja V um espaço vetorial sobre um corpo K e seja $T : V \to V$ uma aplicação linear. Considere V como $K[X]$-módulo com a estrutura de módulo definida por $f(X)v = f(T)(v)$ para $v \in V$, $f(X) \in K[X]$. Então os $K[X]$-submódulos de V são os subespaços de V que são invariantes por T, isto é, os subespaços S tais que $T(S) \subset S$. Pela observação acima, basta notar que se S é um $K[X]$-submódulo de V e $s \in S$, então para $f(x) = x \in K[x]$ temos que $f(x)s \in S$, mas

$$f(x)s = f(T)(s) = T(s).$$

O que mostra que $T(s) \in S$, logo $T(S) \subset S$. Portanto, os $K[X]$-submódulos são invariantes por T.

Agora, dados um subespaço S de V invariante por T, $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$ e $s \in S$, temos que

$$f(T)(s) = a_0 + a_1T(s) + \cdots + a_nT^n(s) \in S,$$

pois como S é subespaço invariante por T, temos que $T^n(s) \in S$, $\forall\ n \geq 1$ e combinações lineares de vetores em S continuam em S. A condição (i) segue do fato de S ser subespaço vetorial. Portanto, S é um $K[X]$-submódulo de V.

Cada módulo $M \neq (0)$ contém pelo menos dois submódulos; a saber, M e (0), chamados *submódulos triviais*. Todo módulo $M \neq (0)$ contém (0) como submódulo próprio.

Definição 1.1.9. *Um módulo M é simples se possui apenas submódulos triviais.*

Exemplo 1.1.10. Sejam K um corpo e $i \in \{1, \ldots, n\}$. O ideal à esquerda

$$L_i = \left\{ \begin{pmatrix} 0 & \cdots & 0 & a_{1i} & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & a_{ni} & 0 & \cdots & 0 \end{pmatrix}, a_{ji} \in K,\ \forall\ j = 1, \ldots, n \right\}$$

é um $M_n(K)$ - módulo simples com a operação usual.

1.2 Módulos Livres, Soma Direta e Semissimplicidade

Se S é um subconjunto de um *R-módulo M*, denotaremos por RS o conjunto de todas as somas da forma $\sum_{i=1}^{n} x_is_i$, onde n é um inteiro positivo, $x_i \in R$ e $s_i \in M$, para $1 \leq i \leq n$.

Definição 1.2.1. *Seja $S = \{s_i\}_{i \in I}$ um subconjunto de elementos de um R-módulo M.*

*a) $S = \{s_i\}_{i \in I}$ é chamado de **conjunto de geradores** de M se $M = RS$; isto é, se cada elemento de M pode ser escrito como uma combinação linear finita de elementos de S com coeficientes em R.*

*b) $S = \{s_i\}_{i \in I}$ é chamado **linearmente independente** se para qualquer combinação linear finita de elementos de S com coeficientes em R,*

$$r_1s_1 + \cdots + r_ts_t = 0$$

temos que $r_1 = \cdots = r_t = 0$.

*c) $S = \{s_i\}_{i \in I}$ é chamado de **base** de M sobre R se S é linearmente independente e um conjunto de geradores de M.*

Exemplo 1.2.2. Não são todos os módulos que possuem uma base. No conjunto $\mathbb{Z}_6$ como um $\mathbb{Z}$-módulo, para cada elemento $\overline{a} \in \mathbb{Z}_6$ temos que $6\overline{a} = \overline{0}$ e $6 \neq 0$ em $\mathbb{Z}$, o que mostra que nenhum subconjunto de $\mathbb{Z}_6$ é linearmente independente sobre $\mathbb{Z}$.

Definição 1.2.3. *Um R-módulo M é chamado livre se possui uma base.*

Teorema 1.2.4. (Ver [1] Teorema 2.4.4, pág. 84.) *Seja M um módulo sobre um anel comutativo R. Se $B_1 = \{v_1, \cdots, v_m\}$ e $B_2 = \{w_1, \cdots, w_n\}$ são duas R-bases para M, então $m = n$.*

Exemplo 1.2.5. $\mathbb{Q}$ como $\mathbb{Z}$-módulo não é livre. Para verificar essa afirmação, mostraremos que nenhum subconjunto finito de pelo menos dois elementos de $\mathbb{Q}$ é linearmente independente sobre $\mathbb{Z}$. Com efeito, dados $\alpha = p_1/q_1$ e $\beta = p_2/q_2$ não nulos em $\mathbb{Q}$, tome como coeficiente de α o inteiro $m_1 = p_2q_1$ e como coeficiente de β o inteiro $m_2 = -p_1q_2$, assim

$$m_1\alpha + m_2\beta = (p_2q_1)\left(\frac{p_1}{q_1}\right) - (p_1q_2)\left(\frac{p_2}{q_2}\right) = 0.$$

é uma combinação linear nula sem que todos os coeficientes sejam iguais a zero. Agora, dado um subconjunto finito $\{\xi_1, \cdots, \xi_n\}$ em $\mathbb{Q}$, se n é par, agrupe as frações duas a duas e aplique o argumente anterior em cada par de frações. Se n for impar, some duas das frações, o que resultará em uma quantidade par de frações e aplique o argumento anterior.

Definição 1.2.6. *Seja $\{M_i\}_{i\in I}$ uma família de submódulos de um R-módulo. Dizemos que M é soma direta dos submódulos dessa família, e escrevemos $M = \oplus_{i\in I} M_i$, se*

$$M_i \cap \left(\sum_{j\neq i} M_j\right) = (0)$$

e cada elemento $m \in M$ pode ser escrito de forma única como

$$m = m_{i_1} + m_{i_2} + \cdots + m_{i_t}$$

com $m_{i_j} \in M_{i_j}$, $1 \leq j \leq t$.

Definição 1.2.7. *Um submódulo N de um R-módulo M é chamado **somando direto** se existe outro submódulo N' tal que $M = N \oplus N'$. Um módulo que não contém somando direto não trivial é chamado **indecomposto.***

O teorema a seguir caracteriza quando um submódulo N é somando direto.

Teorema 1.2.8. *Seja N um submódulo de um R-módulo M. Então N é somando direto se, e somente se, existe um endomorfismo de R-módulos $f : M \to M$ tal que $f \circ f = f$ e $Im(f) = N$.*

Demonstração. ($\Rightarrow$) Admitindo que N é somando direto, seja N' tal que $M = N \oplus N'$. Seja $f : M \to M$ dada por $f(n + n') = n$. Assim definida, f é um homomorfismo de R-módulos. Assim,

$$(f \circ f)(n + n') = f(f(n + n')) = f(n) = n = f(n + n'),$$

o que mostra que

$$f \circ f = f.$$

Por definição da f temos que

$$Im(f) \subset N,$$

e dado $n \in N$, temos que $f(n + N') = n$ o que mostra que $N \subset Im(f)$ e, portanto, $Im(f) = N$.

Reciprocamente, admitindo a existência de tal endomorfismo, considere $N' := \{m - f(m); m \in M\}$. Afirmamos que $M = N \oplus N'$. Com efeito, primeiramente verificamos que N' é um R-submódulo.

Sejam x, $y \in N'$, então

$$x = m_1 - f(m_1)$$

e

$$y = m_2 - f(m_2)$$

com m_1 e m_2 em M. Assim,

$$\begin{aligned} x + y &= (m_1 - f(m_1)) + (m_2 - f(m_2)) \\ &= [m_1 + m_2] - [f(m_1) + f(m_2)] \\ &= [m_1 + m_2] - [f(m_1 + m_2)] \in N'. \end{aligned}$$

E se $r \in R$, temos que

$$rx = r(m_1 - f(m_1)) = rm - rf(m_1) = rm - f(rm) \in N',$$

pois $rm \in M$. Portanto N' é um R-submódulo.

Para mostrar que $N \cap N' = (0)$, notamos primeiramente que f deixa os elementos de N fixos. De fato, dado $n \in N$, como $Im(f) = N$, $\exists\, x \in M$ tal que $f(x) = n$ e como $f \circ f = f$,

$$n = f(x) = f(f(x)) = f(n).$$

Agora, seja $a \in N \cap N'$, note que $N' \subseteq \mathrm{Ker}(f)$, pois

$$f(m - f(m)) = f(m) - f(f(m)) = f(m) - f(m) = 0.$$

Portando, como $a \in N', f(a) = 0$ e como $a \in N, f(a) = a$, portanto $a = 0$. Finalmente, para mostrar que M se escreve como soma de elementos de N e N', dado $m \in M$, temos que $m = f(m) + [m - f(m)]$.

□

Definição 1.2.9. *Um R-módulo M é chamado **semissimples** se cada submódulo de M é um somando direto de M.*

Proposição 1.2.10. (Ver [1] Proposição 2.5.2 pág. 91.) *Seja $N \neq (0)$ um submódulo de um módulo semissimples M. Então N é semissimples e contém um submódulo simples.*

Teorema 1.2.11. (Ver [1] Teorema 2.5.3 pág. 92.) *Seja M um R-módulo. Então as seguintes condições são equivalentes:*

(i) M é semissimples.
(ii) M é soma direta de submódulos simples.
(iii) M é soma (não necessariamente direta) de submódulos simples.

Definição 1.2.12. *Um anel R é chamado* ***semissimples*** *se o módulo ${}_RR$ é semissimples. Em que a notaçao ${}_RR$ refere-se ao anel R visto como um R-módulo à esquerda.*

Teorema 1.2.13. *Seja R um anel com unidade. Então R é semissimples se, e somente se, cada ideal à esquerda L de R é da forma $L = Re$, onde $e \in R$ é idempotente.*

Demonstração. Assumindo que R é semissimples, seja L um ideal à esquerda de R. Então L é um somando direto, assim existe um ideal à esquerda L' tal que $R = L \oplus L'$. Assim, podemos escrever $1 = x + y$ com $x \in L$ e $y \in L'$.

Então

$$x = x \cdot 1 = x^2 + xy,$$

consequentemente,

$$xy = x - x^2 \in L,$$

e, como L' é ideal à esquerda, temos que

$$xy \in L'.$$

Como $L \cap L' = (0)$, segue que $xy = 0$, assim $x = x^2$ e, portanto, x é idempotente.

Claramente $Rx \subset L$. Agora, dado um elemento $a \in L$ temos que $a = a.1 = ax + ay$, assim $a - ax = ay \in L \cap L' = (0)$ e, portanto, $a = ax$, provando a inclusão contrária.

Reciprocamente, seja L um ideal à esquerda de R, devemos mostrar que L é somando direto. Por hipótese, temos que $L = Re$, onde e é idempotente. Afirmamos primeiramente que se e é idempotente então, $1 - e$ também é. De fato,

$$\begin{aligned}(1-e)^2 &= 1 - 2e + e^2 \\ &= 1 - 2e + e \\ &= 1 - e.\end{aligned}$$

O que mostra que $(1 - e)$ é idempotente.

Seja $L' = R(1 - e)$. L' é um ideal à esquerda de R. Dado um elemento $x \in R$, temos que

$$x = xe + x(1 - e),$$

o que mostra que

$$R = Re + R(1 - e).$$

Finalmente, se $x \in Re \cap R(1 - e)$, temos que

$$x = re = s(1 - e),$$

com $r, s \in R$. Portanto,

$$xe = re.e = re^2 = re = x.$$

Por outro lado,

$$\begin{aligned} xe &= s(1-e)e \\ &= s(e-e^2) \\ &= s(e-e) \\ &= 0. \end{aligned}$$

Assim, $x = 0$, o que mostra que $Re \cap R(1-e) = (0)$ e, portanto, $R = Re \oplus R(1-e)$. □

Exemplo 1.2.14. Se K é um corpo, então K é um anel semissimples, pois para todo ideal I de K, tem-se que $I = K$, o ideal gerado por 1 que é idempotente, ou I é o ideal nulo que também é gerado por um idempotente (0).

O anel $\mathbb{Z}$ dos inteiros não é semissimples, de fato, qualquer ideal próprio de $\mathbb{Z}$ é gerado por um elemento não idempotente.

1.3 Produto Tensorial

O produto tensorial de módulos é usualmente definido via propriedade universal.

Definição 1.3.1. *Sejam R um anel, M um R-módulo à direita, N um R-módulo à esquerda e A um grupo abeliano aditivo. Uma aplicação $f : M \times N \to A$ é dita* ***balanceada*** *se satisfaz:*

(i) $f(m_1 + m_2, n) = f(m_1, n) + f(m_2, n)$.

(ii) $f(m, n_1 + n_2) = f(m, n_1) + f(m, n_2)$.

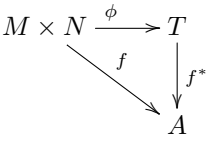
(iii) $f(m, rn) = f(mr, n)$.

$\forall\, m, m_1, m_2 \in M, n, n_1, n_2 \in N, r \in R$.

Definição 1.3.2. *Sejam M e N R-módulos, à direita e à esquerda, respectivamente. Um grupo abeliano T, juntamente com uma aplicação balanceada $\phi : M \times N \to T$ é chamado um* ***produto tensorial*** *de M por N e denotado por $M \otimes N$, se as seguintes condições são satisfeitas:*

(i) Os elementos da forma $\phi(m, n)$, $m \in M$, $n \in N$ geram T (como um grupo aditivo)

(ii) Para qualquer grupo abeliano aditivo A e qualquer aplicação balanceada $f : M \times N \to A$, existe um homomorfismo de grupos abelianos $f^* : T \to A$ tal que $f = f^* \circ \phi$; isto é, tal que o seguinte diagrama é comutativo:



Para $m \in M$ e $n \in N$ denotamos $\phi(m,n) = m \otimes n$, assim cada elemento em $M \otimes N$ é uma soma finita da forma $\sum_i m_i \otimes n_i$.

No caso em que o anel R é comutativo, obtemos um homomorfismo de R-módulos.

Teorema 1.3.3. (Ver [1], pag 118 e 119) *Sejam M e N R-módulos è direita e à esquerda, respectivamente. Então, o produto tensorial de M e N existe e é único, a menos de isomorfismo de grupos abelianos.*

Propriedades: Sejam m, $m' \in M$, n, $n' \in N$, então:

i) $(m + m') \otimes n = m \otimes n + m' \otimes n$

ii) $m \otimes (n + n') = m \otimes n + m \otimes n'$

Observação 1.3.4. Em $M \otimes_R N, m \otimes 0 = 0$ e $0 \otimes n = 0$. A justificativa é análoga à usada para demonstrar que a.0 = 0 em um anel. Fixados m e n,

$$m \otimes 0 = m \otimes (0 + 0) = m \otimes 0 + m \otimes 0.$$

Subtraindo $m \otimes 0$ em ambos os lados, temos $m \otimes 0 = 0$. Para $0 \otimes n$ segue analogamente.

Exemplo 1.3.5. Se A é um grupo abeliano finito, então $\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$. Com efeito, para $a \in A$, existe um inteiro não-nulo n tal que $na = 0$, assim para $r \otimes a \in \mathbb{Q} \otimes_{\mathbb{Z}} A$ temos que

$$\begin{aligned} r \otimes a &= n(r/n) \otimes a \\ &= r/n \otimes na \\ &= r/n \otimes 0 \\ &= 0. \end{aligned}$$

Como os elementos desta forma geram $\mathbb{Q} \otimes_{\mathbb{Z}} A$, segue o resultado.

Exemplo 1.3.6. Seja M um R-módulo à esquerda para um certo anel R. Então, $R \otimes_R M \simeq M$.

Para provar essa afirmação, considere a aplicação: $f : R \times M \to M$ dada por $f(r,m) = rm$. Como f é uma aplicação balanceada, existe um único homomorfismo de grupos abelianos $f^* : R \otimes_R M \to M$ tal que $f = f^* \circ \phi$ (ver propriedade universal). Agora, considere a aplicação $\psi : M \to R \otimes_R M$ dada por $\psi(m) = 1 \otimes m$. Então, ψ é um homomorfismo de grupos abelianos e

$$\begin{aligned}
\psi \circ f^*(r \otimes m) &= \psi \circ f^* \circ \phi(r, m). \\
&= \psi \circ f((r, m)). \\
&= \psi(rm). \\
&= 1 \otimes rm. \\
&= r \otimes m.
\end{aligned}$$

Como os elementos desta forma geram $R \otimes_R M$, temos que $\psi \circ f^* = I$. Analogamente, mostra-se que $f^* \circ \psi = I$. Assim, ψ é uma bijeção, logo, um isomorfismo e segue o resultado.

Capítulo 2

Anéis de Grupo

No presente capítulo faremos um estudo geral dos anéis de grupo para grupos finitos. Na primeira seção apresentamos a definição de anel de grupo bem como a definição de algumas aplicações que serão utilizadas no decorrer desta dissertação. Na segunda seção definiremos um tipo especial de ideal, chamado ideal de aumento, demonstraremos alguns resultados importantes acerca desse ideal e daremos condições necessárias e suficientes para que um anel de grupo seja semissimples. Na terceira seção falaremos de representação de grupo; conceito esse que será utilizado na demonstração de alguns resultados na última seção. Finalizamos o capítulo com o estudo das unidades do anel de grupo integral. O objetivo central da seção sobre unidades é caracterizar os grupos finitos tais que seus anéis de grupo integral contém apenas unidades triviais.

2.1 Conceitos Básicos

Sejam G um grupo (não necessariamente finito) e R um anel com unidade. Desejamos construir um R-módulo, tendo os elementos de G como base e então usar as operações em G e R para definir uma estrutura de anel nele. Para isso denotamos por RG o conjunto de todas as combinações lineares formais da forma

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

ou,

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

onde $a_g \in R$ e $a_g \neq 0$ apenas para uma quantidade finita de elementos $g \in G$.

Definição 2.1.1. *Dado um elemento $\alpha = \sum_{g \in G} a_g g \in RG$, definimos o suporte de α como sendo o conjunto*

$$supp(\alpha) = \{g \in G; a_g \neq 0\} \tag{2.1}$$

Dois elementos, $\alpha = \sum_{g\in G} a_g g$ e $\beta = \sum_{g\in G} b_g g$, são iguais se, e somente se, $a_g = b_g$, $\forall g \in G$

Definimos a soma de dois elementos em RG componente a componente

$$\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}(a_g + b_g)g \tag{2.2}$$

e o produto por

$$\alpha\beta = \sum_{g,h\in G} a_g b_h gh. \tag{2.3}$$

De forma equivalente, podemos escrever o produto $\alpha\beta$ como

$$\alpha\beta = \sum_{u\in G} c_u u,$$

onde

$$c_u = \sum_{gh=u} a_g b_h.$$

Com as operações definidas acima, verifica-se que RG é um anel com unidade $1 = \sum_{g\in G} u_g g$, onde o coeficiente correspondente ao elemento neutro do grupo é 1 e $u_g = 0$ para os demais elementos $g \in G$.

Podemos também definir um produto de elementos em RG por elementos $\lambda \in R$ como segue:

$$\lambda\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G}(\lambda a_g)g. \tag{2.4}$$

Com isso, RG é um *R-módulo.*

Definição 2.1.2. *O conjunto RG, com as operações definidas acima, é chamado o* ***Anel de Grupo de*** *G* ***sobre*** *R. No caso em que R é comutativo, RG é também chamado de* ***Álgebra de Grupo de*** *G* ***sobre*** *R. No caso em que $R = \mathbb{Z}$, o anel de grupo $\mathbb{Z}G$ é chamado* ***anel de grupo integral****.*

Observação 2.1.3. Note que da definição de produto no anel de grupo, segue que se R é comutativo e G é abeliano, então RG é comutativo.

As duas aplicações a seguir mostram como R e G podem ser visto no anel de grupo RG.

Definição 2.1.4. *A aplicação $i : G \to RG$ definida por*

$$i(x) = \sum_{g\in G} a_g g,$$

onde $a_x = 1$ e $a_g = 0$ se $g \neq x$, é chamada ***incorporação*** *de G em RG. Assim, podemos considerar o grupo G como um subconjunto de RG.*

Também definimos a aplicação $v : R \to RG$ dada por

$$v(r) = \sum_{g \in G} a_g g,$$

onde $a_e = r$ e $a_g = 0$ se $g \neq e$. A aplicação v é um monomorfismo de anel e, portanto, podemos também considerar R como um subanel de RG.

Anéis de grupo também podem ser definidos via propriedade universal.

Teorema 2.1.5. ("Propriedade Universal" para Anéis de Grupo). *Sejam G um grupo, R e A anéis comutativos com unidade,*

$$f : G \to A^*,$$

um homomorfismo de grupos, em que A^* denota o grupo multiplicativo de A e

$$\phi : R \to A$$

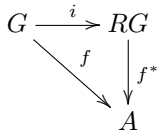
um homomorfismo de anéis tal que

$$f(g)\phi(r) = \phi(r)f(g),$$

$\forall\, g \in G$, $\forall\, r \in R$. Então, existe um único homomorfismo de anéis

$$f^* : RG \to A$$

que estende f e ϕ e tal que o seguinte diagrama é comutativo



Demonstração. Dada $f : G \to A$, considere $f^* : RG \to A$ definida por:

$$\sum_{g \in G} a_g g \mapsto \sum_{g \in G} \phi(a_g) f(g).$$

Verificaremos que f^* é um homomorfismo de anéis.
Dados $\alpha = \sum\limits_{g \in G} a_g g$, $\beta = \sum\limits_{g \in G} b_g g$ e $r \in R$ em RG, temos que

$$\begin{aligned}
f^*(\alpha + \beta) &= f^*\left(\sum_{g \in G} (a_g + b_g) g\right) \\
&= \sum_{g \in G} \phi(a_g + b_g) f(g) \\
&= \sum_{g \in G} \phi(a_g) f(g) + \sum_{g \in G} \phi(b_g) f(g) \\
&= \sum_{g \in G} \phi(a_g) f(g) + \sum_{g \in G} \phi(b_g) f(g) \\
&= f^*(\alpha) + f^*(\beta)
\end{aligned}$$

Além disso,

$$\begin{aligned} f^*(\alpha\beta) &= f^*\left(\sum_{g,h\in G} a_g b_h gh\right) \\ &= \sum_{g,h\in G} \phi(a_g b_h) f(gh) \\ &= \sum_{g,h\in G} \phi(a_g)\phi(b_h) f(g) f(h) \\ &= \sum_{g,h\in G} \phi(a_g) f(g) \phi(b_h) f(h) \\ &= \sum_{g\in G} \phi(a_g) f(g) \sum_{h\in G} \phi(b_h) f(h) \\ &= f^*(\alpha) f^*(\beta). \end{aligned}$$

Portanto, f^* é um homomorfismo de anéis.

Para a unicidade, suponha que exista outra função π, nas condições do teorema, tal que

$$\pi \circ i = f.$$

Para um elemento arbitrário $\alpha = \sum_{g\in G} a_g g \in RG$, temos que

$$\begin{aligned} \pi\left(\sum_{g\in G} a_g g\right) &= \sum_{g\in G} \pi(a_g)\pi(g) \\ &= \sum_{g\in G} \phi(a_g)\pi(i(g)) \\ &= \sum_{g\in G} \phi(a_g) f(g) \\ &= f^*\left(\sum_{g\in G} a_g g\right) \end{aligned}$$

□

Observação 2.1.6. No Teorema 2.1.5, se A for uma R-álgebra, então o homomorfismo f^* é de R-álgebras. Com efeito, sendo A uma R-álgebra, tome

$$\phi : R \to A$$

definida por

$$r \mapsto r \cdot 1_A.$$

Assim, se $r \in R$ então,

$$
\begin{aligned}
f^*\left(\sum_{g\in G} ra_g g\right) &= \sum_{g\in G} \phi(ra_g) f(g) \\
&= \sum_{g\in G} (ra_g)\cdot 1_A f(g) \\
&= \sum_{g\in G} r(a_g\cdot 1_A) f(g) \\
&= r\sum_{g\in G} (a_g\cdot 1_A) f(g) \\
&= r\sum_{g\in G} \phi(a_g) f(g) \\
&= rf^*\left(\sum_{g\in G} a_g g\right).
\end{aligned}
$$

A proposição a seguir mostra que é sempre verdade que grupos isomorfos induzem anéis de grupos isomorfos. O estudo do problema do isomorfismo, que é um dos objetivos desta dissertação, é analisar a recíproca dessa proposição.

Proposição 2.1.7. *Seja $\pi : G \to H$ um isomorfismo entre os grupos G e H. Então existe um isomorfismo entre RG e RH, para qualquer anel R.*

Demonstração. Considere $\pi^* : RG \to RH$ definida por

$$
\pi^*\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \pi(g).
$$

Verificaremos que π^* é um homomorfismo de anéis. Sejam $\alpha = \sum_{g\in G} a_g g$ e $\beta = \sum_{g\in G} b_g g$, elementos arbitrários de RG.

$$
\begin{aligned}
\pi^*(\alpha+\beta) &= \pi^*\left(\sum_{g\in G} (a_g+b_g) g\right). \\
&= \sum_{g\in G} (a_g+b_g)\pi(g). \\
&= \sum_{g\in G} a_g\pi(g) + \sum_{g\in G} b_g\pi(g). \\
&= \pi^*(\alpha)+\pi^*(\beta).
\end{aligned}
$$

Além disso,

$$\begin{aligned}
\pi^*(\alpha\beta) &= \pi^*\left(\sum_{g,h\in G} a_g b_h gh\right). \\
&= \sum_{g,h\in G} a_g b_h \pi(gh). \\
&= \sum_{g,h\in G} a_g b_h \pi(g)\pi(h). \\
&= \left(\sum_{g\in G} a_g \pi(g)\right)\left(\sum_{g\in G} b_g \pi(g)\right). \\
&= \pi^*(\alpha)\pi^*(\beta).
\end{aligned}$$

Assim, π^* é um homomorfismo de anéis.

Para verificar a injetividade, note que se $\sum_{g\in G} a_g g \in \mathrm{Ker}(\pi^*)$, então

$$\sum_{g\in G} a_g \pi(g) = 0,$$

ou seja, $a_g = 0$ para todo $g \in G$, o que mostra que $\sum_{g\in G} a_g g = 0$.

Para a sobrejetividade, dado $\sum_{h\in H} a_h h \in RH$, tome $\sum_{h\in H} a_h \pi^{-1}(h) \in RG$, daí

$$\pi^*\left(\sum_{h\in H} a_h \pi^{-1}(h)\right) = \sum_{h\in H} a_h(\pi\circ\pi^{-1})(h) = \sum_{h\in H} a_h h.$$

□

Para analisar a recíproca da Proposição 2.1.7, poderemos considerar os isomorfismos envolvidos como sendo isomorfismos normalizados. Para definir tais isomorfismos precisaremos do conceito de aplicação de aumento que é definido a seguir. A aplicação de aumento aparecerá com frequência nas demonstrações dos teoremas desta dissertação.

Proposição 2.1.8. *A aplicação $\epsilon : RG \to R$ dado por*

$$\sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g$$

é um homomorfismo de anéis.

Demonstração. Sejam $\alpha = \sum_{g\in G} a(g)g$ e $\beta = \sum_{g\in G} b(g)g$ elementos arbitrários em RG. Assim,

$$\begin{aligned}\epsilon(\alpha+\beta) &= \epsilon\left(\sum_{g\in G}(a(g)+b(g))g\right)\\ &= \sum_{g\in G}a(g)+b(g)\\ &= \sum_{g\in G}(a(g))+\sum_{g\in G}(b(g))\\ &= \epsilon(\alpha)+\epsilon(\beta).\end{aligned}$$

Além disso,

$$\begin{aligned}\epsilon(\alpha\beta) &= \epsilon\left(\sum_{g,h\in G}a(g)b(h)gh\right)\\ &= \sum_{g,h\in G}a(g)b(h)\\ &= \left(\sum_{g\in G}a(g)\right)\left(\sum_{h\in G}b(h)\right)\\ &= \epsilon(\alpha)\epsilon(\beta).\end{aligned}$$

□

Definição 2.1.9. *O homomorfismo de anéis $\epsilon : RG \to R$ definido acima é chamado **aplicação de aumento** de RG e seu kernel, denotado por $\Delta(G)$, é chamado de **ideal de aumento** de RG.*

Proposição 2.1.10. *O conjunto $\{g-1;\, g\in G,\, g\neq e\}$ é uma base de $\Delta(G)$ sobre R.*

Demonstração. Note que se $\alpha \in \mathrm{Ker}(\epsilon)$ então $\sum\limits_{g\in G} a_g = 0$. Assim, 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 todo elemento da forma $g-1$ pertence a $\Delta(G)$, isso mostra que $\{g-1;\, g\in G,\, g\neq e\}$ é um conjunto de geradores de $\Delta(G)$. A independência linear desse conjunto segue por argumentos usuais.

□

Definição 2.1.11. *Sejam G e H grupos finitos. Um isomorfismo $\phi : \mathbb{Z}G \to \mathbb{Z}H$ é chamado **isomorfismo normalizado** se preserva a aplicação de aumento, ou seja, se para cada elemento $\alpha \in \mathbb{Z}G$ temos que $\epsilon_G(\alpha) = \epsilon_H(\phi(\alpha))$* (ou, equivalentemente, se para cada elemento $g \in G$, temos que $\epsilon(\phi(g)) = 1$)

Observação 2.1.12. Vamos verificar que de fato a condição $\epsilon(\phi(\alpha)) = \epsilon(\alpha)$ é equivalente a $\epsilon(\phi(g)) = 1$, para cada $g \in G$.

Com efeito, se para cada $\alpha \in \mathbb{Z}G$ temos que $\epsilon(\phi(\alpha)) = \epsilon(\alpha)$, então, em particular, temos que

$$1 = \epsilon(g) = \epsilon(\phi(g)).$$

Reciprocamente, se $\epsilon(\phi(g)) = 1$ para cada $g \in G$, então para cada $\alpha = \sum_{g\in G} a_g g \in \mathbb{Z}G$, temos que

$$\phi(\alpha) = \phi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \phi(g).$$

Aplicando ϵ obtemos,

$$\epsilon(\phi(\alpha)) = \sum_{g\in G} a_g \epsilon(\phi(g)).$$

Como $\epsilon(\phi(g)) = 1$ para cada $g \in G$, segue que

$$\begin{aligned} \epsilon(\phi(\alpha)) &= \sum_{g\in G} a_g \epsilon(\phi(g)) \\ &= \sum_{g\in G} a_g \\ &= \epsilon(\alpha). \end{aligned}$$

Observação 2.1.13. A existência de um isomorfismo entre $\mathbb{Z}G$ e $\mathbb{Z}H$ implica na existência de um isomorfismo normalizado. De fato, dado um isomorfismo

$$\phi : \mathbb{Z}G \to \mathbb{Z}H,$$

defina

$$\psi : \mathbb{Z}G \to \mathbb{Z}H$$

da seguinte forma: para cada elemento $\alpha = \sum_{i=1}^{n} r_i g_i$ associamos

$$\psi(\alpha) = \sum_{i=1}^{n} \epsilon((\phi(g_i))^{-1} r_i \phi(\alpha).$$

(Note que como g é invertível em $\mathbb{Z}G$, então $\phi(g)$ é invertível em $\mathbb{Z}H$. Daí segue

$$1 = \epsilon(1) = \epsilon(\phi(g)\phi^{-1}(g)) = \epsilon(\phi(g))\epsilon(\phi(g)^{-1}),$$

ou seja, $\epsilon(\phi(g))$ é invertível em $\mathbb{Z}$.)

Para verificarmos que de fato ψ é um isomorfismo normalizado, calculamos $\epsilon(\psi(g))$ para um elemento $g \in G$ arbitrário. Note que

$$\psi(g) = \epsilon(\phi(g))^{-1}.1.\phi(g),$$

portanto

$$\epsilon(\psi(g)) = \epsilon(\phi(g))^{-1}.1.\epsilon(\phi(g)) = 1.$$

Finalizamos essa seção com duas propriedades dos anéis de grupo. Precisaremos do seguinte lema:

Lema 2.1.14. (Ver [36] pág. 144) *Sejam R um anel comutativo com unidade, A, B e T R-álgebras, $A \xrightarrow{f} T$ e $B \xrightarrow{g} T$ homomorfismos de R-álgebras tais que*

$$f(a)g(b) = g(b)f(a), \forall\, a \in A, \forall\, b \in B.$$

Então, existe um único homomorfismo de R-álgebras

$$\psi : A \otimes_R B \to T$$

tal que

$$(a \otimes b) \mapsto f(a)g(b),$$

$\forall\, a \in A, \forall\, b \in B$.

Lema 2.1.15. *Sejam S, R um anéis comutativos com unidade, com S uma R-álgebra. Então,*

$$SG \simeq S \otimes_R RG.$$

Demonstração. Considere $i : G \to SG$ a inclusão de G em SG e $l : R \to S$ definida por $r \mapsto r \cdot 1_s$. Pelo Teorema 2.1.5, existe um único homomorfismo de R-álgebras $\psi : RG \to SG$ que estende i e l. Considere também

$$f : S \to SG$$

definida por

$$s \mapsto s \cdot e.$$

Note que

$$f(s)\psi(\alpha) = \psi(\alpha)f(s),$$

$\forall\, s \in S, \forall\, \alpha \in RG$. Assim, pelo Lema 2.1.14, existe um único homomorfismo de R-álgebras

$$\psi_1 : S \otimes_R RG \to SG,$$

tal que

$$(s \otimes \alpha) \mapsto f(s)\psi(\alpha),$$

$\forall\, s \in S, \forall\, \alpha \in RG$.

Por outro lado, defina $h : SG \to S \otimes_R RG$ por

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

Assim definida, h é um homomorfismo de R-álgebras. Para mostrar que h é bijeção, verificaremos que ψ_1 é sua inversa. Com efeito,

$$\begin{aligned}
\psi_1 \circ h \left(\sum_{g \in G} a(g)g \right) &= \psi_1 \left(\sum_{g \in G} a(g) \otimes g \right). \\
&= \sum_{g \in G} f(a(g))\psi(g). \\
&= \sum_{g \in G} (a(g) \cdot e)(g \cdot 1_s). \\
&= \sum_{g \in G} a(g)g.
\end{aligned}$$

Além disso,

$$\begin{aligned} h \circ \psi_1 \left(s \otimes \sum_{g \in G} a(g)g \right) &= h \left(f(s)\psi \left(\sum_{g \in G} a(g)g \right) \right). \\ &= h \left((s \cdot e) \sum_{g \in G} l(a(g))i(g) \right). \\ &= h \left(\sum_{g \in G} sa(g)g \right). \\ &= \sum_{g \in G} (sa(g) \otimes g). \\ &= \sum_{g \in G} (s \otimes a(g)g). \\ &= s \otimes \sum_{g \in G} a(g)g. \end{aligned}$$

Portanto, $h \circ \psi_1 = \psi_1 \circ h = id$ e segue o resultado.

□

Teorema 2.1.16. *Seja R um anel comutativo com unidade, e sejam G e H grupos. Então,*

$$R(G \times H) \simeq (RG)H.$$

Demonstração. Considere a aplicação $f : R(G \times H) \to (RG)H$, dada por

$$\sum_{g \in G,\, h \in H} a_{gh}(g, h) \mapsto \sum_{h \in H} \left(\sum_{g \in G} a_{gh} g \right) h.$$

Para verificar que f é um homomorfismo de R-álgebras, note que se $\alpha = \sum_{g \in G,\, h \in H} a_{gh}(g, h)$, $\beta = \sum_{g' \in G,\, h' \in H} b_{g'h'}(g', h')$ e $r \in R$, então

$$\begin{aligned}
f(\alpha\beta) &= f\left(\sum_{g,g'\in G,\, h,h'\in H} a_{gh}b_{g'h'}(gg', hh')\right)\\
&= \sum_{h,h'\in H}\left(\sum_{g,g'\in G} a_{gh}b_{g'h'}gg'\right)hh'\\
&= \sum_{h,h'\in H}\left(\left(\sum_{g\in G} a_{gh}g\right)\left(\sum_{g'\in G} b_{g'h'}\right)hh'\right)\\
&= \left[\sum_{h\in H}\left(\sum_{g\in G} a_{gh}g\right)h\right]\left[\sum_{h'\in H}\left(\sum_{g'\in G} a_{g'h'}g'\right)h'\right]\\
&= f\left(\sum_{g\in G,\, h\in H} a_{gh}(g,h)\right) f\left(\sum_{g'\in G,\, h'\in H} b_{g'h'}(g',h')\right)\\
&= f(\alpha)f(\beta).
\end{aligned}$$

Além disso,

$$\begin{aligned}
f(r\alpha+\beta) &= f\left(\sum_{g\in G,\, h\in H}(ra_{gh}+b_{gh})(g,h)\right)\\
&= \sum_{h\in H}\left(\sum_{g\in G}(ra_{gh}+b_{gh})g\right)h\\
&= \sum_{h\in H}\left(\sum_{g\in G} ra_{gh}g + \sum_{g\in G} b_{gh}g\right)h\\
&= \sum_{h\in H}\left(\sum_{g\in G} ra_{gh}g\right)h + \sum_{h\in H}\left(\sum_{g\in G} b_{gh}g\right)h\\
&= \sum_{h\in H}\left(r\sum_{g\in G} a_{gh}g\right)h + \sum_{h\in H}\left(\sum_{g\in G} b_{gh}g\right)h\\
&= r\sum_{h\in H}\left(\sum_{g\in G} a_{gh}g\right)h + \sum_{h\in H}\left(\sum_{g\in G} b_{gh}g\right)h\\
&= rf(\alpha)+f(\beta).
\end{aligned}$$

Definindo $g : (RG)H \to R(G\times H)$, por

$$\sum_{h\in H}\left(\sum_{g\in G} a_{gh}g\right)h \mapsto \sum_{g\in G,\, h\in H} a_{gh}(g,h),$$

uma conta semelhante a anterior mostra que g é um homomorfismo de $R-$álgebras e é a inversa de f. □

2.2 Ideais de Aumento e Semissimplicidade

Dado um grupo finito G, denotaremos por $S(G)$ o conjunto de todos os subgrupos de G.

Definição 2.2.1. *Para um subgrupo $H \in S(G)$ e um anel R com unidade, denotamos por $\Delta_R(G,H)$ o ideal à esquerda de RG gerado pelo conjunto $\{h-1;\, h \in H\}$, isto é,*

$$\Delta_R(G,H) = \{\sum_{h\in H} a_h(h-1); a_h \in RG\}.$$

Lema 2.2.2. *Seja H um subgrupo de um grupo G e seja S um conjunto de geradores de H. Então, o conjunto $\{s-1; s \in S\}$ é um conjunto de geradores de $\Delta_R(G,H)$.*

Daremos uma melhor descrição de $\Delta_R(G,H)$, em especial, quando $H \triangleleft G$.

Seja $\Upsilon = \{q_i\}_{i\in I}$ um conjunto completo de representantes das classes laterais à esquerda de H em G. Então, cada elemento $g \in G$ pode ser escrito de forma unívoca como $g = q_i h_j$, onde $q_i \in \Upsilon$ e $h_j \in H$

Proposição 2.2.3. (Ver [1] proposição 3.3.3, pág. 135) *O conjunto $B_H = \{q(h-1); q \in \Upsilon,\, h \in H,\, h \neq e\}$ é uma base de $\Delta_R(G,H)$ sobre R.*

Caracterizaremos o ideal $\Delta_R(G,H)$ no caso em que H é subgrupo normal de G. Omitiremos o subíndice R sempre que estiver subentendido o anel a ser considerado e escreveremos simplesmente $\Delta(G,H)$.

Observação 2.2.4. No caso em que $H \triangleleft G$, o homomorfismo canônico $\omega : G \to G/H$ pode ser estendido para um epimorfismo $\omega^* : RG \to R(G/H)$ tal que

$$\omega^*\left(\sum_{g\in G} a(g)g\right) = \sum_{g\in G} a(g)\omega(g).$$

Proposição 2.2.5. *Se $H \triangleleft G$, então* $\mathrm{Ker}(\omega^*) = \Delta(G,H)$.

Demonstração. Cada elemento $\alpha \in RG$ pode ser escrito como uma soma finita $\alpha = \sum_{i,j} r_{ij} q_i h_j$ onde $r_{ij} \in R$, $q_i \in \Upsilon$ *e* $h_j \in H$.

Se denotarmos por $\overline{q_i}$ a imagem de q_i no grupo quociente G/H então temos que

$$\omega^*(\alpha) = \sum_i \left(\sum_j r_{ij}\right)\overline{q_i}.$$

Consequentemente, $\alpha \in \mathrm{Ker}(\omega^*)$ se, e somente se, $\sum_j r_{ij} = 0$ para cada valor de i. Assim, se $\alpha \in \mathrm{Ker}(\omega^*)$, podemos escrever, adicionando somas de zeros:

$$\begin{aligned}\alpha &= \sum_{i,j} r_{ij} q_i h_j \\ &= \sum_{i,j} r_{ij} q_i h_j - \sum_i \left(\sum_j r_{ij} \right) q_i \\ &= \sum_{i,j} r_{ij} q_i (h_j - 1) \in \Delta(G, H).\end{aligned}$$

Portanto, $\mathrm{Ker}(\omega^*) \subset \Delta(G, H)$. A outra inclusão segue do fato que $w^*(h - 1) = w(h) - w(1) = H - H = 0$, para todo $h \in H$.

□

Segue da proposição anterior e do Teorema do Isomorfismo o seguinte corolário:

Corolário 2.2.6. *Seja H um subgrupo normal de G. Então, $\Delta(G, H)$ é um ideal bilateral de RG e*

$$\frac{RG}{\Delta(G, H)} \simeq R(G/H).$$

Esse corolário será bastante utilizado nos resultados do capítulo 3.

Definição 2.2.7. *Seja X um subconjunto de um anel de grupo RG. O anulador à esquerda de X é o conjunto*

$$Ann_l(X) = \{\alpha \in RG; \alpha x = 0, \forall x \in X\}.$$

Similarmente, define-se o anulador à direita, denotado por $Ann_r(X)$.

Definição 2.2.8. *Dado um anel de grupo RG e um subconjunto finito X do grupo G, denotaremos por $\widehat{X}$ o seguinte elemento de RG:*

$$\widehat{X} = \sum_{x \in X} x.$$

Lema 2.2.9. *Sejam H um subgrupo de um grupo G e R um anel. Então o $Ann_r(\Delta(G, H)) \neq 0$ se, e somente se, H é finito. Neste caso, temos*

$$Ann_r(\Delta(G, H)) = \widehat{H}.RG.$$

Além disso, se $H \triangleleft G$, então o elemento $\widehat{H}$ é central em RG e

$$Ann_r(\Delta(G, H)) = Ann_l(\Delta(G, H)) = RG.\widehat{H}.$$

Demonstração. Assumindo que $Ann_r(\Delta(G, H)) \neq 0$ e tomando $\alpha = \sum_{g \in G} a(g)g \neq 0$ no $Ann_r(\Delta(G, H))$, temos que para cada elemento $h \in H$, $(h - 1)\alpha = 0$, consequentemente $h\alpha = \alpha$; isto é,

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

Isso mostra que para cada $g_0 \in supp(\alpha)$, temos que $hg_0 \in supp(\alpha)$, $\forall\, h \in H$. Como $supp(\alpha)$ é finito, segue que H é finito.

Note que o argumento acima mostra que sempre que $g_0 \in supp(\alpha)$, então o coeficiente de cada elemento da forma hg_0 é igual ao coeficiente de g_0. Assim, podemos escrever α na forma:

$$\alpha = a_{g_0}\widehat{H}g_0 + \cdots + a_{g_t}\widehat{H}g_t = \widehat{H}\beta,\ \beta \in RG$$

Isto mostra que, se H é finito, então

$$Ann_r(\Delta(G,H)) \subset \widehat{H}.RG.$$

Para a outra inclusão, basta notar que $h\widehat{H} = \widehat{H}$, portanto

$$(h-1)\widehat{H} = 0,\ \forall\, h \in H.$$

Finalmente, se $H \triangleleft G$, para qualquer $g \in G$ temos que $g^{-1}Hg = H$; consequentemente,

$$g^{-1}\widehat{H}g = \sum_{x\in H} g^{-1}xg = \sum_{y\in H} y = \widehat{H}.$$

Portanto, $\widehat{H}g = g\widehat{H}$, para todo $g \in G$, o que mostra que $\widehat{H}$ é central. Consequentemente,

$$RG.\widehat{H} = \widehat{H}.RG.$$

□

Como uma consequência dos resultados precedentes desta seção, obtemos condições necessárias e suficientes para que um anel de grupo seja semissimples. Para isso precisaremos dos dois lemas que seguem:

Lema 2.2.10. *Seja I um ideal bilateral de um anel R. Suponha que exista um ideal à esquerda J, tal que $R = I \oplus J$ (como R-módulo à esquerda). Então, $J \subset Ann_r(I)$.*

Demonstração. Sejam, $x \in J$ e $y \in I$ arbitrários. Como J é um ideal à esquerda e I é um ideal bilateral, temos que $yx \in J \cap I = (0)$. Consequentemente, $yx = 0$ e $x \in Ann_r(I)$.

□

Lema 2.2.11. *Se o Ideal de aumento $\Delta(G)$ é um somando direto de RG como um RG-módulo, então G é finito e $|G|$ é invertível em R.*

Demonstração. Assumindo que $\Delta(G)$ é um somando direto de RG, existe um submódulo N de RG tal que

$$RG = \Delta(G) \oplus N.$$

Assim, temos pelo Lema 2.2.10 que $N \subset Ann_r(\Delta(G))$, portanto $Ann_r(\Delta(G)) \neq 0$ e segue do Lema 2.2.9 que G é finito e que

$$Ann_r(\Delta(G)) = \widehat{G}(RG) = \widehat{G}R. \tag{2.5}$$

Escrevemos

$$RG = \Delta(G) \oplus J$$

e

$$1 = e_1 + e_2$$

com $e_1 \in \Delta(G)$ e $e_2 \in J$. Então,

$$1 = \epsilon(1) = \epsilon(e_1) + \epsilon(e_2),$$

Como

$$e_1 \in \Delta(G) = \mathrm{Ker}(\epsilon),$$

segue que $\epsilon(e_1) = 0$.

Como $J \subset Ann_r(\Delta(G))$, e_2 se escreve como $e_2 = a\widehat{G}$ por 2.5, para algum $a \in R$. Assim, $1 = a\epsilon(\widehat{G})$, mas $\epsilon(\widehat{G}) = |G|$, portanto, $a|G| = 1$, o que mostra que ordem de G é invertível em R.

□

Teorema 2.2.12. *(**Maschke**). Seja G um grupo, então o anel de grupo RG é semissimples se, e somente se:*

(i) R é um anel semissimples.
(ii) G é finito.
(iii) $|G|$ é invertível em R.

Demonstração. Assumimos que RG é semissimples. Segue do Corolário 2.2.6 que $R \simeq \dfrac{RG}{\Delta(G)}$. Como o quociente de um anel semissimples por um ideal é também semissimples, segue imediatamente que R também é. A semissimplicidade de RG garante que todo ideal de RG é somando direto, em particular, $\Delta(G)$ é um somando direto. Do Lema 2.2.11 segue as condições (ii) e (iii).

Reciprocamente, assumindo as condições (i), (ii) e (iii) considere M um *RG-submódulo* de RG. Como R é semissimples, RG é semissimples como *R-módulo*, logo existe um *R-submódulo* N de RG tal que

$$RG = M \oplus N.$$

Seja $\pi : RG \to M$ a projeção canônica associada a soma, (ver Teorema 1.2.8). Definimos

$$\pi^*(x) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gx),$$

para todo $x \in RG$.

Afirmamos que π^* cumpre $(\pi^*)^2 = \pi^*$ e $Im(\pi^*) = M$. Com efeito, como π^* é um *R-homomorfismo*, para mostrar que também é um *RG-homomorfismo* é suficiente mostrar que

$$\pi^*(ax) = a\pi^*(x), \forall\, a \in G.$$

Note que,

$$\pi^*(ax) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\pi(gax) = \frac{a}{|G|} \sum_{g \in G} (ga)^{-1}\pi((ga)x).$$

Mas, quando g varia por todos os elementos de G, o produto ga também varia por todos os elementos de G, portanto

$$\pi^*(ax) = a\frac{1}{|G|}\sum_{t\in G} t^{-1}\pi(tx) = a\pi^*(x).$$

Como π é projeção em M, segue que $\pi(m) = m, \forall\, m \in M$. Também, como M é um RG-módulo, temos que $gm \in M$ para todo $g \in G$. Portanto

$$\pi^*(m) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gm) = \frac{1}{|G|}\sum_{g\in G} g^{-1}gm.$$

Mas, $\sum\limits_{g\in G} g^{-1}g = \sum\limits_{g\in G} 1 = |G|$, consequentemente

$$\pi^*(m) = \frac{1}{|G|}\sum_{g\in G} g^{-1}\pi(gm) = \frac{1}{|G|}\sum_{g\in G} g^{-1}gm = \frac{1}{|G|}|G|m = m.$$

Dado arbitrariamente $x \in RG$, temos pela definição da π que $\pi(gx) \in M$, assim $\pi^*(x) \in M$, pois M é um RG-submódulo, e segue que $Im(\pi^*) \subset M$, com isso

$$\pi^*(\pi^*(x)) = \pi^*(x),$$

para todo $x \in RG$.

Finalmente, o fato de que $\pi^*(m) = m$, para todo $m \in M$, mostra que $M \subset Im(\pi^*)$. Segue do Teorema 1.2.8 que o *RG-submódulo* M é um somando direto e, portanto, RG é semissimples.

□

Como uma consequência do teorema acima temos:

Corolário 2.2.13. *Seja G um grupo finito e seja K um corpo. Então, KG é semissimples se, e somente se,* $\mathrm{Car}(K) \nmid |G|$.

Demonstração. No caso em que $R = K$, um corpo, temos que K é sempre semissimples e $|G|$ é invertível em K se, e somente se, $|G| \neq 0$ em K, isto é, se, e somente se, $\mathrm{Car}(K) \nmid |G|$.

□

Finalizamos essa seção apresentando o enunciado da versão generalizada do importante Teorema de Wedderburn-Artin, com destaque ao item iii) que diz que uma álgebra de grupo, sob certas condições, é isomorfa à uma soma direta de matrizes complexas. No entanto, para o enfoque da presente dissertação, não faremos uso do mesmo.

Teorema 2.2.14. *(**Wedderburn-Artin Generalizado**) Seja G um grupo finito e seja K um corpo tal que $char(K) \nmid |G|$. Então:*

(i) KG é uma soma direta de um número finito de ideais bilaterais $\{B_i\}_{1\leq i\leq r}$, as componentes simples de KG

(ii) Qualquer ideal bilateral de KG é soma direta de membros da família $\{B_i\}_{1\leq i\leq r}$.

(iii) Cada componente simples B_i é isomorfa ao anel de matrizes completas da forma $M_{n_i}(D_i)$, onde D_i é um anel de divisão contendo uma cópia de K no seu centro, e isomorfismo

$$KG \overset{\phi}{\simeq} \oplus_{i=1}^{r} M_{n_i}(D_i)$$

é um isomorfismo de K-álgebras.

2.3 Representação de Grupos

Nessa seção trataremos brevemente o conceito de representação de grupos. Faremos uso desse conceito mais adiante para demonstrar resultados importantes acerca das unidades do anel de grupo integral $\mathbb{Z}G$ para G finito.

Definição 2.3.1. *Sejam G um grupo finito, R um anel comutativo e V um R-módulo livre de posto finito. Uma **representação** de G sobre R, com espaço de representação V, é um homomorfismo de grupos $T : G \to GL(V)$, onde $GL(V)$ denota o grupo dos R-automorfimos de V. O posto de V é chamado **grau** da representação T e é denotado por $grau(T)$.*

Definição 2.3.2. *Sejam G um grupo e R um anel comutativo. Uma representação matricial de G sobre R de grau n é um homomorfismo de grupos $T : G \to GL(n, R)$.*

Exemplo 2.3.3. Dados um grupo G e um anel comutativo R, a aplicação $T : G \to GL(n, R)$ que associa para cada elemento de G a matriz identidade em $GL(n, R)$ é chamada de *representação trivial* de G sobre R de grau n.

Exemplo 2.3.4. Sejam S_n o grupo simétrico, R um anel comutativo e V um R-módulo livre de posto finito com base $v_1, ..., v_n$. A aplicação

$$T : S_n \to GL(V)$$

que para cada $\sigma \in S_n$ associa $T_\sigma \in GL(V)$, tal que $T_\sigma(v_i) = v_{\sigma(i)}$ é chamada **Representação de Permutação**. Denotando por $A(\sigma)$ a matriz associada à T_σ na dada base, então a j-ésima coluna de $A(\sigma)$ é obtida escrevendo $T_\sigma(v_j)$ como combinação linear dos elementos da base.

Como T_σ leva um elemento da base em outro elemento da base, temos que os coeficiente nessa coluna são todos iguais a zero, exceto para a entrada $(\sigma(j), j)$, que é igual a 1. Consequentemente, a matriz $A(\sigma)$ tem exatamente uma entrada igual a 1 em cada linha e em cada coluna e zero em todas as outras entradas.

Exemplo 2.3.5. ***A Representação Regular.***

Sejam G um grupo finito de ordem n e R um anel comutativo. Desejamos definir uma representação de G sobre R, tomando como espaço de representação, RG, o anel de grupo de G sobre R. Para isso, definimos a aplicação $T : G \to GL(RG)$ que para cada $g \in G$ associa a aplicação linear T_g que atua na base por multiplicação à esquerda, isto é, $T_g(g_i) = gg_i$. Para verficar que T é um homomorfismo de grupos, note que

$$T_{gh}(y) = (gh)y = g(hy) = T_g T_h(y),$$

o que mostra que de fato T é uma representação de G. Por argumento análogo ao usado no exemplo anterior, vê-se que a matriz de representação correspondente, com respeito à base G de RG, de cada elemento $g \in G$ é uma matriz de permutação.

Observação 2.3.6. Note que $T_g(g_i) = gg_i \neq g_i$, para todo g diferente do elemento neutro do grupo G, de modo que a única entrada 1 de cada linha e cada coluna não ocorre na diagonal principal da matriz de representação para um elemento g diferente do elemento neutro do grupo.

Exemplo 2.3.7. Como ilustração podemos calcular essa representação para um exemplo concreto. Considere $G = \{e, a, a^2\}$, um grupo cíclico de ordem 3, enumerando seus elementos como

$$g_1 = e,\ g_2 = a,\ g_3 = a^2,$$

temos que

$$T_a(g_1) = g_2,\ T_a(g_2) = g_3,\ T_a(g_3) = g_1,$$

Consequentemente, a matriz associada a T_a na base dada é

$$\rho(a) = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

2.4 Unidades do Anel de Grupo Integral

2.4.1 Unidades Triviais

Definição 2.4.1.1. *Seja G um grupo. O grupo $U(\mathbb{Z}G) = \{\alpha \in \mathbb{Z}G;\ \alpha$ é invertível $\}$ é chamado o* ***grupo das unidades*** *de $\mathbb{Z}G$ e*

$$U_1(\mathbb{Z}G) = \{\alpha \in U(\mathbb{Z}G);\ \epsilon(\alpha) = 1\}$$

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

Proposição 2.4.1.2. $U(\mathbb{Z}G) = U_1(\mathbb{Z}G) \cup (-U_1(\mathbb{Z}G))$.

Demonstração. De fato, se α é uma unidade do anel $\mathbb{Z}G$, então

$$1 = \epsilon(1) = \epsilon(\alpha\alpha^{-1}) = \epsilon(\alpha)\epsilon(\alpha^{-1})$$

O que mostra que $\epsilon(\alpha)$ é invertível em $\mathbb{Z}$, ou seja, $\epsilon(\alpha) = \pm 1$.

□

Todo elemento $g \in G$ é uma unidade de $\mathbb{Z}G$ com inverso $g^{-1} \in G$. Os elementos da forma $\pm g$ com $g \in G$ são chamados de ***unidades triviais*** de $\mathbb{Z}G$.

Lema 2.4.1.3. *Sejam G um grupo finito, K um corpo, ρ uma representação regular de KG e $\gamma = \sum_{g\in G} \gamma(g)g \in KG$. Então, o traço de $\rho(\gamma)$ é dado por*

$$tr\rho(\gamma) = |G|\gamma(e).$$

Demonstração. Sabemos que o $tr\rho(\gamma)$ independe da base escolhida, assim escolhemos o conjunto $G = \{g_1, g_2, ..., g_n\}$ como uma K-base de KG e assumindo que $g_1 = e$. Então

$$\rho(\gamma) = \rho\left(\sum_{g\in G} \gamma(g)g\right) = \sum_{g\in G} \gamma(g)\rho(g).$$

Segue da Observação 2.3.6 que as entradas na diagonal da matriz $\rho(\gamma)$ são todas iguais a zero, portanto $tr\rho(\gamma) = 0$ para todo $g \neq e$. Como $\rho(e)$ é a matriz identidade, $tr\rho(e) = |G|$, temos, portanto,

$$tr\rho(\gamma) = tr\left(\sum_{g\in G} \gamma(g)\rho(g)\right) = \sum_{g\in G} \gamma(g)tr\rho(g) = \gamma(e)tr\rho(e) = \gamma(e)|G|.$$

□

Lema 2.4.1.4. *Seja $\gamma = \sum_{g\in G} \gamma(g)g$ uma unidade de ordem finita do anel integral $\mathbb{Z}G$ de um grupo finito G e assuma que $\gamma(e) \neq 0$. Então, $\gamma = \gamma(e) = \pm 1$.*

Demonstração. Seja $|G| = n$. Como γ é de ordem finita, existe um inteiro m tal que $\gamma^m = 1$.

Consideraremos a representação regular ρ da álgebra do grupo $\mathbb{C}G$ e consideraremos $\mathbb{Z}G$ como um subanel de $\mathbb{C}G$. Então,

$$tr\rho(\gamma) = n\gamma(e)$$

pelo lema anterior. Como $\gamma^m = 1$, temos que

$$(\rho(\gamma))^m = \rho(\gamma^m) = I.$$

Segue que $\rho(\gamma)$ é uma raíz do polinômio $X^m - 1$, o qual tem todas as raízes distintas, assim $\rho(\gamma)$ é diagonalizável. Isto implica que existe uma base de $\mathbb{C}G$ onde a matriz de $\rho(\gamma)$ é diagonal, da forma

$$A = \begin{pmatrix} \xi_1 & & \\ & \ddots & \\ & & \xi_n \end{pmatrix}$$

onde os elementos da diagonal principal são raízes m-ésimas da unidades, $\xi_i^m = 1$. Assim, $tr\rho(\gamma) = \sum_{i=1}^{n} \xi_i$. Portanto,

$$n\gamma(e) = \sum_{i=1}^{n} \xi_i.$$

Tomando o valor absoluto, temos

$$|n\gamma(e)| = |\sum_{i=1}^{n} \xi_i| \leq \sum_{i=1}^{n} |\xi_i| = n.$$

Como $|n\gamma(e)| = n|\gamma(e)| \leq n$, temos que $|\gamma(e)| \leq 1$ e do fato que $\gamma(e) \in \mathbb{Z}$ e $\gamma(e) \neq 0$, temos que $|\gamma(e)| = 1$ e também $|\sum_{i=1}^{n} \xi_i| = \sum_{i=1}^{n} |\xi_i|$. Isso ocorre se, e somente se, $\xi_1 = \xi_2 = \cdots = \xi_n$.[1]

Portanto, $n\gamma(e) = n\xi_1$ e consequentemente $\gamma(e) = \xi_1 = \pm 1$, concluimos assim, que $\rho(\gamma) = \pm I$, logo, $\gamma = \pm 1$.

□

Corolário 2.4.1.5. *Suponha que $\gamma = \sum_{g \in G} \gamma(g)g$ é uma unidade central de ordem finita do anel de grupo integral $\mathbb{Z}G$ de um grupo finito G. Então γ é da forma $\gamma = \pm g$, com $g \in Z(G)$.*

Demonstração. Seja $\gamma = \sum_{g \in G} \gamma(g)g$ de ordem finita m. Seja $g_0 \in G$ tal que $\gamma(g_0) \neq 0$. Então γg_0^{-1} também é de ordem finita, pois $\gamma \in Z(\mathbb{Z}G)$ e $(\gamma g_0^{-1})^\alpha = 1$, onde $\alpha = o(\gamma)o(G)$.

Mais ainda, note que o elemento e na expressão γg_0^{-1} é obtido na parcela $\gamma(g_0)g_0g_0^{-1}$, de modo que o coeficiente do elemento e em γg_0^{-1} é $\gamma(g_0) \neq 0$. Segue do Lema anterior que $\gamma g_0^{-1} = \pm 1$, portanto $\gamma = \pm g_0$.

□

[1] Lembre que $|\xi_1 + \xi_2| = |\xi_1| + |\xi_2|$ implica que existe $\alpha \geq 0 \in \mathbb{R}$ tal que $\xi_1 = \alpha\xi_2$. Como $|\xi_1| = |\xi_2| = 1$, segue que $\alpha = 1$. O caso geral sai por indução.

Outra consequência é o famoso teorema de Graham Higman.

Teorema 2.4.1.6. *Seja A um grupo abeliano finito. Então o grupo das unidades de torção de $\mathbb{Z}A$ é $\pm A$. Em outras palavras, $TU(\mathbb{Z}A)$ é igual a $\pm A$.*

Demonstração. Como A é abeliano, segue que o anel de grupo $\mathbb{Z}A$ é comutativo, em particular, cada unidade de ordem finita é central. Assim, se $\gamma = \sum_{g \in G} \gamma(g)g$ é uma unidade de torção, então, pelo corolário anterior, $\gamma = \pm g$, onde $g \in Z(A) = A$.

□

2.4.2 Unidades Bicíclicas

O objetivo agora é definir um tipo especial de unidade afim de obtermos as classes de grupos G para os quais as unidades de $\mathbb{Z}G$ sejam triviais.

Seja R um anel com divisores de zero. Considere $x, y \in R$, ambos diferentes de zero, tais que $xy = 0$. Então, para qualquer $t \in R$ o elemento $\eta = ytx$ satisfaz $\eta^2 = 0$. De fato,

$$\eta^2 = (ytx)(ytx) = (yt)(xy)(tx) = (yt)0(tx) = 0.$$

Assim, $1 + \eta$ é uma unidade, pois

$$(1 + \eta)(1 - \eta) = 1 - \eta^2 = 1.$$

No caso especial em que $R = \mathbb{Z}G$, um caminho simples para obtermos divisores de zero é considerar um elemente $a \in G$ de ordem finita $n > 1$. Então $a - 1$ é um divisor de zero, pois

$$(a - 1)(1 + a + \cdots + a^{n-1}) = a^n - 1 = 0.$$

Portanto, para qualquer outro elemento $b \in G$, nós podemos construir a unidade

$$\mu_{a,b} = 1 + (a - 1)b\widehat{a},$$

onde $\widehat{a} = 1 + a + \cdots + a^{n-1}$, onde $\eta := (a - 1)b\widehat{a}$.

Definicão 2.4.2.1. *Seja a um elemento de ordem finita no grupo G e seja b outro elemento qualquer de G. A unidade $\mu_{a,b}$ construída acima é chamada uma* ***Unidade Bicíclica*** *do anel de grupo $\mathbb{Z}G$.*

Se a e b comutam, então $\mu_{a,b} = 1$. Desejamos agora decidir quando as unidades bicíclicas são triviais.

Proposição 2.4.2.2. *Sejam g, h elementos de um grupo G com $|g| = n < \infty$. Então, a unidade $\mu_{g,h}$ é trivial se, e somente se, h normaliza $\langle g \rangle$ e, neste caso, $\mu_{g,h} = 1$*

Demonstração. Assumamos que h normaliza $\langle g \rangle$, ou seja

$$h^{-1}gh = g^j$$

para algum inteiro j. Então, $gh = hg^j$ e como $g^j\widehat{g} = \widehat{g}$, temos que $gh\widehat{g} = h\widehat{g}$. Assim,

$$\mu_{g,h} = 1 + (g-1)h\widehat{g} = 1 + gh\widehat{g} - h\widehat{g} = 1 + gh\widehat{g} - gh\widehat{g} = 1.$$

Reciprocamente, Como $\epsilon(\mu_{g.h}) = 1$, existe um elemento $x \in G$ tal que $\mu_{g,h} = x$. Assim, temos que

$$1 + (g-1)h\widehat{g} = x.$$

Com isso,

$$1 + h(1 + g + \cdots + g^{n-1}) = x + gh(1 + g + \cdots + g^{n-1}). \tag{2.6}$$

Se $x = 1$, então

$$h + hg + \cdots + hg^{n-1} = gh + ghg + \cdots + ghg^{n-1}. \tag{2.7}$$

Como h aparece no lado esquerdo da igualdade 2.7, deve também aparecer no lado direito. Assim, $h = ghg^i$ para algum inteiro i. Portanto,

$$h^{-1}gh = g^{-i},$$

o que mostra que h normaliza $\langle g \rangle$.

Agora, suponha por contradição que $\mu_{g,h} = x \neq 1$. Segue que $h \notin \langle g \rangle$. De fato, se tivéssemos $h \in \langle g \rangle$, então $h\widehat{g} = \widehat{g}$ o que implicaria, diretamente da definição, que $\mu_{g,h} = 1$.

Como 1 aparece no lado esquerda da igualdade 2.6, ele deve também aparecer no lado direito, isto implica que deve existir um inteiro positivo i tal que $1 = ghg^i$, o que implica que

$$h = g^{-(i+1)}$$

e segue que

$$h^{-1}gh = g^{i+1}gg^{-(i+1)} = g,$$

ou seja, g e h comutam, o que dá $gh\widehat{g} = h\widehat{g}$, o que implica, como já visto, que $x = \mu_{g,h} = 1$ e esta contradição conclui a demonstração

□

2.4.3 Unidades Cíclicas de Bass [2]

Para introduzir essa outra unidade, $\phi(n)$ denotará a função ϕ de Euler. Lembramos também, que para calcular ϕ em um inteiro positivo n, basta decompor n como produto de fatores primos:

$$n = p_1^{n_1} \cdots p_t^{n_t}.$$

Assim, temos que

$$\phi(n) = p_1^{n_1-1}(p_1 - 1) \cdots p_t^{n_t-1}(p_t - 1).$$

[2] Definida por Hyman Bass em [30]

Esta fórmula é frequentemente escrita como

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

cuja dedução segue do fato da função ϕ de Euler ser multiplicativa para termos primos entre si e $\phi(p^k) = p^k - p^{k-1}$.

Uma importante propriedade dessa função é dada pelo Teorema de Euler:

Teorema 2.4.3.1. *Se i e n são relativamente primos então, $i^{\phi(n)} \equiv 1 \ (mod\, n)$.*

Definicão 2.4.3.2. *Seja g um elemento de ordem n em um grupo G. Uma **Unidade Cíclica de Bass** é um elemento do anel de grupo $\mathbb{Z}G$ da forma:*

$$\mu_i = (1 + g + \cdots + g^{i-1})^{\phi(n)} + \frac{1 - i^{\phi(n)}}{n}\widehat{g},$$

onde i é um inteiro tal que $1 < i < n - 1$ e $(i, n) = 1$.

O elemento μ_i é de fato uma unidade cujo inverso é da forma:

$$\mu = (1 + g + \cdots + g^{i(k-1)})^{\phi(n)} + \frac{1 - k^{\phi(n)}}{n}\widehat{g},$$

onde k é um inteiro tal que $1 < k < n$ e $n \mid (1 - ik)$. Para uma demonstração o leitor pode consultar [5] página 22, ou [1] página 239. Ambas as demonstrações utilizam o conceito de $\mathbb{Z}$-ordem.

A proposição seguinte dá condições para que uma unidade cíclida de Bass seja **não** trivial. A demonstração usa alguns argumentos aritméticos.

Proposição 2.4.3.3. *Seja g um elemento de ordem n em um grupo finito G e seja i um inteiro tal que $1 < i < n$ e $(i, n) = 1$. Se $i \not\equiv \pm 1 \ (mod\, n)$, então a unidade cíclica de Bass*

$$\mu = (1 + g + \cdots + g^{i-1})^{\phi(n)} - \frac{1 - i^{\phi(n)}}{n}\widehat{g}$$

não é trivial.

Demonstração. Suponha, por absurdo, que μ é trivial. Como o suporte de μ só contém potências de g, se μ é trivial deve existir um inteiro positivo j tal que $\mu = g^j$. Seja $m = \phi(n)$. Assim,

$$(1 + g + \cdots + g^{i-1})^m - \frac{1 - i^m}{n}\widehat{g} = g^j. \tag{2.8}$$

Multiplicando ambos os lados em 2.8 por $(1 - g)^m$, obtemos

$$(1 - g^i)^m - \frac{(1 - g)^m(1 - i^m)}{n}\widehat{g} = (1 - g)^m g^j, \tag{2.9}$$

pois

$$\begin{aligned}(1 - g)^m(1 + g + \cdots + g^{i-1})^m &= [(1 - g)(1 + g + \cdots + g^{i-1})]^m \\ &= (1 - g^i)^m.\end{aligned}$$

Além disso, note que $g\widehat{g} = \widehat{g}$, ou seja, $(1-g)\widehat{g} = 0$. Em particular,

$$(1-g)^m \widehat{g} = 0.$$

Com isso, de 2.9 obtemos que

$$(1-g^i)^m = (1-g)^m g^j. \tag{2.10}$$

Assim, aplicando o binômio de Newton em ambos os lados de 2.10 segue a igualdade

$$1 - mg^i + \binom{m}{2} g^{2i} + \cdots + (-1)^m g^{im} = g^j - mg^{j+1} + \binom{m}{2} g^{j+2} + \cdots + (-1)^m g^{j+m}. \tag{2.11}$$

Como $1 < i < n$, segue que $n > 2$, logo $m = \phi(n)$ é par. Da hipótese de $i \not\equiv \pm 1 \ (mod\, n)$ segue $n > 4$ e, portanto, $m > 2$.

Como as potências de g no primeiro membro da igualdade 2.11 são todas diferentes, resulta que o elemento neutro do grupo G aparece efetivamente nesse membro, com coeficiente igual a 1. Logo, deve aparecer também no segundo membro e também com coeficiente igual a 1. Temos, portanto, duas possibilidades: $g^j = e$ ou $g^{j+m} = e$.

Consideremos o caso em que $g^j = e$.

Comparando os elementos de ambos os membros em 2.11 que têm coeficiente igual a m segue que

$$g^i = g^{j+1}, \text{ ou } g^i = g^{j+m-1},$$

(referente ao termo que acompanha $\binom{m}{1}$ e $\binom{m}{m-1}$). Como estamos assumindo que $g^j = e$, temos que

$$g^i = g \text{ ou } g^i = g^{m-1} \tag{2.12}$$

No entanto, nossa hipótese sobre i implica que a primeira possibilidade em 2.12 não pode ocorrer, uma vez que $g^{i-1} = e$ implicaria $i \equiv 1 (mod\, n)$. Logo deve ocorrer

$$g^i = g^{m-1}.$$

Isso implica que

$$g^{2i} = g^{2m-2}.$$

Comparando os elementos com coeficientes $\binom{m}{2}$ devemos ter

$$g^{2i} = g^{2m-2} = g^{j+2} = g^2,$$

ou

$$g^{2i} = g^{2m-2} = g^{j+m-2} = g^{m-2},$$

uma vez que $\binom{m}{m-2} = \binom{m}{2}$. Mas, a segunda opção não ocorre, pois se tivéssemos

$$g^{2m-2} = g^{m-2} \tag{2.13}$$

deveríamos ter, multiplicando ambos os lados de 2.13 por $g^{-(m-2)}$,

$$g^m = g^{2m-2} g^{-(m-2)} = g^{m-2} g^{-(m-2)} = e.$$

Com isso, teríamos

$$g^m = e,$$

o que implicaria que $n \mid m$, o que é uma contradição.

Portanto,

$$g^{2m-2} = g^2,$$

e segue desta igualdade que

$$g^{2m-4} = e,$$

logo, $n \mid 2m-4$.

Afirmamos que $n = 2m-4$. Com efeito, como $2 < m < n$, temos que $2m-4 > 0$, assim, como $n \mid 2m-4$, $\exists\, k \in \mathbb{N}$ tal que $2m-4 = kn$. Suponha por absurdo que $k > 1$. Como $m = \phi(n)$, podemos escrever

$$2n \prod_{p|n} \left(1 - \frac{1}{p}\right) - 4 = kn. \tag{2.14}$$

Chamando de $\pi := \prod_{p|n} \left(1 - \frac{1}{p}\right)$, temos que $\pi < 1$ e como $k > 1$, então $2n \leq kn$. Portanto, segue de 2.14 que

$$2n \leq kn = 2n\pi - 4 \leq 2n - 4,$$

o que é um absurdo, logo devemos ter $k = 1$, portanto

$$n = 2m - 4.$$

Assim, n é par e tem-se que $m = \phi(n) \leq \frac{n}{2}$. Como $m = \frac{n+4}{2} > \frac{n}{2}$ temos uma contradição.

No caso em que $g^{j+m} = 1$, comparando novamente termos com coeficiente igual a m em ambos os membros da igualdade, temos

$$g^i = g^{j+1} = g^{j+m+1-m} = g^{1-m}$$

ou

$$g^i = g^{j+m-1} = g^{-1}.$$

Como nossa hipótese sobre i implica que o segundo caso não ocorre, devemos ter

$$g^i = g^{1-m},$$

o que implica que

$$g^{2i} = g^{2-2m} \neq g^{2-m},$$

pelo argumento em 2.13. Logo, comparando os termos que têm coeficientes igual a $\binom{m}{2}$ segue que $g^{2i} = g^{-2}$. Assim,

$$g^{2-2m} = g^{-2}.$$

Com isso, $g^{4-2m} = (g^{-1})^{2m-4} = e$, ou seja, $n \mid 2m-4$. O que gera uma contradição, como visto anteriormente.

□

2.4.4 Anéis de Grupo Contendo Somente Unidades Triviais

Usaremos os resultados obtidos sobre unidades bicíclicas e unidades cíclicas de Bass para caracterizar os grupos para os quais seu anel de grupo integral contém somente unidades triviais.

Lembramos que uma unidade trivial de $\mathbb{Z}G$ é um elemento da forma $\pm g$ com $g \in G$, em outras palavras, se G é um grupo tal que todas as unidades de $\mathbb{Z}G$ são triviais, então $U(\mathbb{Z}G) = G \cup (-G)$. Esta condição pode ser reformulada em termos das unidades normalizadas como $U_1(\mathbb{Z}G) = G$.

A proposição seguinte mostrará, em particular, que se G é um grupo finito tal que $\mathbb{Z}G$ contém apenas unidades triviais, então todos os subgrupos de G são normais.

Proposição 2.4.4.1. *Seja G um grupo de torção tal que $U_1(\mathbb{Z}G) = G$. Então, cada subgrupo de G é normal.*

Demonstração. Note que é suficiente provar que todo subgrupo cíclico de G é normal em G. Com efeito, sejam N um subgrupo de G, $n \in N$ e $g \in G$. Supondo que $\langle n \rangle \triangleleft G$, temos que $gng^{-1} = n^j \in N$, pois N é subgrupo. Logo, pela arbitrariedade do elemento n, segue $gNg^{-1} = N$, $\forall g \in G$, ou seja $N \triangleleft G$.

Dito isto, suponha por contradição que exista um subgrupo cíclico $\langle g \rangle$ que não seja normal. Então, existe $h \in G$ tal que $h^{-1}gh \notin \langle g \rangle$, em particular, h não normaliza $\langle g \rangle$, segue da proposição 2.4.2.2 que a unidade bicíclica $u = 1 + (1-g)h\widehat{g}$ não é trivial. Contradição.

□

É bem conhecido que se um grupo G é abeliano, então todos os seus subgrupos são normais. A recíproca é falsa, e os grupos de torção não abelianos tais que todos os seus subgrupos são normais são chamados **Grupos Hamiltonianos**. Eles são da forma:

$$G = K_8 \times E \times A, \tag{2.15}$$

(ver Teorema 1.8.5 em [1]) onde E é um 2-grupo abeliano elementar, isto é, cada elemento $a \neq e$ tem ordem 2, A é um grupo abeliano cujos elementos têm ordem impar e K_8 é o grupo quatérnio de ordem 8:

$$K_8 = \langle a,\, b; a^4 = 1,\, a^2 = b^2,\, bab^{-1} = a^{-1} \rangle.$$

Mostraremos que a classe dos grupos Hamiltonianos para os quais as unidades do seu anel de grupo integral são trivias, são os 2-grupos Hamiltonianos.

Observação 2.4.4.2. Um grupo Hamiltoniano finito é um 2-grupo se, e somente se, $A = \{e\}$.

Lema 2.4.4.3. *Sejam G um grupo tal que as unidades de $\mathbb{Z}G$ são triviais e C_2 um grupo cíclico de ordem 2. Então, as unidades de $\mathbb{Z}(G \times C_2)$ também são triviais.*

Demonstração. Seja $C_2 = \{e, a\}$. Pelo Teorema 2.1.16, temos que

$$\mathbb{Z}(G \times C_2) \simeq (\mathbb{Z}G)C_2.$$

Assim, um elemento em $\mathbb{Z}(G \times C_2)$ pode ser escrito da forma $u = \alpha + \beta a$ com $\alpha, \beta \in \mathbb{Z}G$. Supondo que u é uma unidade, existe $u^{-1} = \gamma + \delta a$ tal que

$$(\alpha + \beta a)(\gamma + \delta a) = (\alpha\gamma + \beta\delta) + (\alpha\delta + \beta\gamma)a = 1.$$

Então,

$$(\alpha\delta + \beta\gamma) = 0$$
$$(\alpha\gamma + \beta\delta) = 1.$$

Portanto, temos que

$$(\alpha + \beta)(\gamma + \delta) = (\alpha\delta + \beta\gamma) + (\alpha\gamma + \beta\delta) = 1$$

e também

$$(\alpha - \beta)(\gamma - \delta) = (\alpha\gamma + \beta\delta) - (\alpha\delta + \beta\gamma) = 1.$$

Com isso, temos que $\alpha + \beta$ e $\alpha - \beta$ são unidades em $\mathbb{Z}G$, as quais por hipótese são triviais. Assim, existem $g_1, g_2 \in G$ tais que

$$\alpha + \beta = \pm g_1, \;\; \alpha - \beta = \pm g_2.$$

Consequentemente,

$$2\alpha = (\alpha + \beta) + (\alpha - \beta) = \pm g_1 \pm g_2,$$

logo

$$\alpha = \frac{1}{2}(\pm g_1 \pm g_2).$$

Como os coeficientes de α são números inteiros, segue que $g_1 = \pm g_2$. Assim, umas das duas opções se verifica:

$$\alpha + \beta = \alpha - \beta = \pm g_1$$

ou

$$\alpha + \beta = -(\alpha - \beta) = \pm g_1.$$

No primeiro caso, temos que $\alpha = \pm g_1$ e $\beta = 0$ e no segundo caso, temos que $\beta = \pm g_1$ e $\alpha = 0$. Em ambos os casos temos que u é trivial.

□

Lema 2.4.4.4. *As unidades do anel $\mathbb{Z}K_8$ são triviais.*

Demonstração. Lembramos que $K_8 = \{1, a, b, ab, a^2, a^3, a^2b, ab^3\}$, portanto cada elemento $\alpha \in \mathbb{Z}K_8$ é da forma

$$\alpha = x_0 + x_1a + x_2b + x_3ab + y_0a^2 + y_1a^2b + y_2a^2b + y_3ab^3,$$

$x_i, y_i \in \mathbb{Z}, 0 \leq i \leq 3$.

Agora, consideramos o anel de quatérnios integral; isto é, o anel

$$H = \{m_0 + m_1i + m_2j + m_3k;\, m_t, \in \mathbb{Z},\, 0 \leq t \leq 3\}.$$

Temos que as unidades de H são ± 1, $\pm i$, $\pm j$, $\pm k$(ver Exemplo 2.1.8 em [1]).

Considere o epimorfismo $\phi : \mathbb{Z}K_8 \to H$, dado por

$$\alpha \mapsto (x_0 - y_0) + (x_1 - y_1)i + (x_2 - y_2)j + (x_3 - y_3)k.$$

Se α é uma unidade em $\mathbb{Z}K_8$, então $\phi(\alpha)$ é uma unidade em H. Assim, para algum $0 \leq r \leq 3$,

$$x_r - y_r = \pm 1$$

$$x_s - y_s = 0 \ se \ s \neq r.$$

Segue das operações do grupo que $a^2 \in Z(K_8)$. Do fato de K_8 não ser abeliano, tem-se que

$$|Z(K_8)| \neq 8$$

e também

$$|Z(K_8)| \neq 4,$$

pois o centro de um grupo não tem índice primo (ver [4] Proposição V.4.8; pág. 140).

Como as possíveis ordens para o centro de K_8 são 8, 4, 2 ou 1 pelo Teorema de Lagrange, e como

$$a^2 \in Z(K_8),$$

segue que

$$Z(K_8) = \langle a^2 \rangle,$$

cuja ordem é 2, ou seja,

$$\left| \frac{K_8}{Z(K_8)} \right| = 4.$$

Como K_8 não é abeliano,

$$\frac{K_8}{Z(K_8)}$$

não é cíclico (ver [4] Proposição V.4.8; pág. 140), o que implica que

$$\frac{K_8}{Z(K_8)} \ncong C_4$$

portanto,

$$\frac{K_8}{Z(K_8)} \simeq C_2 \times C_2,$$

onde C_2 é um grupo cíclico de ordem 2. Logo,

$$\frac{K_8}{\langle a^2 \rangle} \simeq C_2 \times C_2.$$

Sejam $\overline{g}$ a imagem de $g \in K_8$ pelo homomorfismo canônico de K_8 em $\dfrac{K_8}{\langle a^2 \rangle}$ e

$$\psi : \mathbb{Z}K_8 \to \mathbb{Z}\left(\frac{K_8}{\langle a^2 \rangle}\right)$$

a extensão do homomorfismo canônico para $\mathbb{Z}K_8$ (ver Observação 2.2.4).

Temos, portanto,

$$\psi(\alpha) = (x_0 + y_0) + (x_1 + y_1)\overline{a} + (x_2 + y_2)\overline{b} + (x_3 + y_3)\overline{ab}.$$

Segue do Lema 2.4.4.3 que as unidades de $\mathbb{Z}(C_2 \times C_2)$, logo de $\mathbb{Z}\left(\frac{K_8}{\langle a^2\rangle}\right)$, são triviais. Portanto, para algum índice j, $0 \leq j \leq 3$, devemos ter

$$x_j + y_j = \pm 1$$

$$x_k + y_k = 0 \text{ se } k \neq j.$$

Como os coeficientes são inteiros temos que $r = j$ e

$$x_r = \pm 1,\ y_r = 0,\ x_s = y_s = 0 \text{ se } s \neq r,$$

ou

$$x_r = 0,\ y_r = \pm 1,\ x_s = y_s = 0 \text{ se } s \neq r.$$

Em ambos os casos temos que α é uma unidade trivial de $\mathbb{Z}K_8$.

□

Segue dos dois lemas precedentes o seguinte teorema:

Teorema 2.4.4.5. *Seja G um 2-grupo Hamiltoniano. Então, as unidades de $\mathbb{Z}G$ são triviais.*

Demonstração. Como G é um 2-grupo Hamiltoniano, então G é da forma $G = K_8 \times E$ por 2.15. Pelo teorema fundamental dos grupos abelianos finitos, E pode ser escrito como produto direto de subgrupos cíclicos de ordem 2. Pelo Lema 2.4.4.4, as unidades de $\mathbb{Z}K_8$ são triviais, assim aplicando sucessivamente o Lema 2.4.4.3 uma quantidade finita de vezes, obtemos que as unidades de $\mathbb{Z}G$ são triviais.

□

No Teorema 2.4.4.1 vimos que se um grupo de torção é tal que as unidades de seu anel de grupo integral são triviais, então esse grupo é abeliano ou Hamiltoniano. O teorema a seguir é um refinamento do Teorema 2.4.4.1.

Teorema 2.4.4.6. *Seja G um grupo de torção tal que $U_1(\mathbb{Z}G) = G$. Então, G ou é um grupo abeliano de expoente[3] igual a 1, 2, 3, 4 ou 6 ou um 2-grupo Hamiltoniano.*

Demonstração. Suponha que G é abeliano. Supondo por contradição que o expoente de G é diferente de 1, 2, 3, 4 ou 6, então, G contém um elemento de ordem n tal que $n = 5$ ou $n > 6$. Em ambos os casos temos que $\phi(n) > 2$, em que ϕ denota a função de Euler. Assim, a demonstração da Proposição 2.4.3.3 mostra que G contém uma unidade cíclica de Bass não trivial. O que é uma contradição.

No caso em que G é Hamiltoniano, lembrando que $G = K_8 \times E \times A$, supondo por contradição que G não é um 2-grupo, então G contém um elemento $x \in A$ de ordem $p > 2$. Então, o elemento $g = ax$ tem ordem $n = 4p$, onde a é um dos geradores de K_8 de ordem 4, e, novamente, temos que $\phi(n) > 2$, assim também neste caso G contém uma unidade cíclica de Bass não trivial.

□

[3]Menor inteiro positivo n tal que $g^n = e$, $\forall\, g \in G$.

Observação 2.4.4.7. Vale a recíproca do Teorema 2.4.4.6 (Ver [1] Teorema 8.2.6 pág.245.)

Capítulo 3

O Problema do Isomorfismo

No presente capítulo estudaremos o problema do isomorfismo com ênfase em anéis de grupo integral. Todos os isomorfismos entre anéis de grupo integral que aparecerão serão de $\mathbb{Z}$-álgebras. Tal problema questiona se grupos não isomorfos poderiam determinar anéis de grupo isomorfos. A resposta desse questionamente está intimamente ligada ao anel em que se está trabalhando. O ambiente mais simples para se exibir grupos não isomorfos, com álgebras de grupo isomorfas, é quando trabalhamos com o corpo dos complexos. Veremos na Seção 3.1 que grupos abelianos finitos não são determinados por suas álgebras de grupo sobre o corpo dos complexos. No entanto, S. Perlis e G. Walker [8] provaram que grupos abelianos finitos são determinados por seus anéis de grupo sobre o corpo dos racionais.

Para anéis de grupo integral foi formulada a seguinte conjectura, atualmente conhecida como (ISO): *Se G e H são dois grupos tais que*

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

então $G \simeq H$.

Higman [7] demonstrou que grupos abelianos finitos e 2-grupos Hamiltonianos finitos são determinados por seus anéis de grupo integral. Outros autores dedicaram-se a essa questão demonstrando a veracidade dessa conjectura em alguns outros casos particulares, como dito na introdução desta dissertação.

Este capítulo está dividido da seguinte forma: na primeira seção, mostraremos que grupos abelianos finitos não são determinados por suas álgebras de grupo sobre o corpo dos complexos, isto é, exibiremos dois grupos, G e H, abelianos de mesma ordem, não isomorfos, porém com $\mathbb{C}G \simeq \mathbb{C}H$. Este resultado mostra que o problema do isomorfismo, em sua generalidade, tem resposta negativa. No entanto, dada a dificuldade para apresentar um contraexemplo no caso em que o anel dos coeficientes é o anel dos inteiros, acreditava-se que a conjectura ISO fosse verdadeira. A conjectura foi demonstrada em alguns casos particulares e ficou em aberto até 2001, quando foi apresentado um contraexemplo, devido a Martin Hertweck [6]. Esse contraexemplo será apresentado no Capítulo 4.

A partir da Seção 3.2 demonstraremos a conjectura ISO em alguns casos particulares. Para os resultados deste capítulo estamos seguindo principalmente:

na Seção 3.1 o artigo [5], nas Seções 3.2, 3.3 e 3.4, o livro [1], e na Seção 3.5 os artigos [3] e [2].

3.1 Álgebras de Grupo Abeliano

Consideremos primeiro o caso em que $G = \langle a \mid a^n = 1\rangle$ é um grupo cíclico de ordem n e seja K um corpo tal que $\text{car}(K) \nmid n$. Considere a função $\psi : K[X] \to KG$ dada por:

$$\psi(f(x)) \mapsto f(a).$$

ψ é um homomorfismo sobrejetor de anéis, logo,

$$KG \simeq \frac{K[X]}{\text{Ker}(\psi)}.$$

Como $K[X]$ é um domínio de ideais principais, $\text{Ker}(\psi)$ é o ideal gerado pelo polinômio mônico f_0, de grau mínimo, que tem a como raiz. Neste isomorfismo o elemento a corresponde com a classe $X + (f_0)$.

Como $a^n = 1$, segue que $X^n - 1 \in \text{Ker}(\psi)$. Note também que se $f(x) = \sum_{i=1}^{r} \alpha_i X^i$ é um polinômio de grau $r < n$ temos que $f(a) \neq 0$, porque os elementos $\{1, a, \cdots, a^r\}$ são linearmente independentes sobre K, (lembre-se que da definição de anel de grupo o grupo G é uma base para KG). Com isso, qualquer elemento no $\text{Ker}(\psi)$ é múltiplo de $X^n - 1$. Assim,

$$\text{Ker}(\psi) = (X^n - 1).$$

Seja

$$X^n - 1 = f_1 f_2 \cdots f_t$$

a decomposição de $F(X) = X^n - 1$ como produto de polinômios irredutíveis em $K[X]$.

Como estamos na hipótese de $\text{Car}(K) \nmid n$, este polinômio é separável em $K[X]$, pois como $n \neq 0$ em K, $F'(X) = nX^{n-1} = 0$ se, e somente se, $X = 0$. Assim, todas as raízes de $F(X)$ são simples, portanto $f_i \neq f_j$, se $i \neq j$.

Como os polinômio $f_1, f_2, \cdots, f_t$, são irredutíveis em $K[X]$, segue que estes são dois a dois primos entre si, portanto coprimos. Pelo Teorema Chinês do Resto, podemos escrever:

$$KG \simeq \frac{K[X]}{(f_1)} \oplus \cdots \oplus \frac{K[X]}{(f_t)}.$$

Seja ζ_i uma raíz de f_i em alguma extensão de K, $1 \leq i \leq t$. Então, temos que $\dfrac{K[X]}{(f_i)} \simeq K[\zeta_i]$. Consequentemente:

$$KG \simeq K(\zeta_1) \oplus \cdots \oplus K(\zeta_t).$$

Como todos os elementos ζ_i, $1 \leq i \leq t$, são raízes de $X^n - 1$, isso mostra que KG é isomorfo a uma soma direta de extensões de K por raízes da unidade. Neste isomorfismo, o elemento a corresponde ao elemento $(\zeta_1, \zeta_2, \cdots, \zeta_t)$.

Se $K = \mathbb{C}$, o corpo dos números complexos, então todo polinômio irredutível de $\mathbb{C}[X]$ é de primeiro grau e todos os quocientes da forma $\frac{\mathbb{C}[X]}{(f_i)}$ são isomorfos a $\mathbb{C}$, de modo que, se G é cíclico de ordem n, então:

$$\mathbb{C}G \simeq \underbrace{\mathbb{C} \oplus \cdots \oplus \mathbb{C}}_{n\ vezes}.$$

Desejamos estender o resultado acima para grupos abelianos em geral. Lembramos que se G é um grupo que pode ser escrito como produto direto de dois subgrupos, $G = H \times N$, e K é um corpo qualquer, então do Teorema 2.1.16 temos que

$$K(H \times N) \simeq (KH)N.$$

Observamos também que se R é um anel que é soma direta de uma família finita de anéis, $R = \oplus_{i \in I} R_i$, tem-se que:

$$RG \simeq \oplus_{i \in I}(R_i G).$$

Proposição 3.1.1. *Seja G um grupo abeliano de ordem finita n. Então:*

$$\mathbb{C}G \simeq \underbrace{\mathbb{C} \oplus \cdots \oplus \mathbb{C}}_{n\ vezes},$$

como $\mathbb{C}$-álgebras.

Demonstração. Como G é abeliano, podemos escrever $G = G_1 \times \cdots \times G_t$, onde cada G_i é um grupo cíclico, $1 \leq i \leq t$. Demonstraremos por indução em t.

Se $t = 1$, então G é cíclico e neste caso o resultado já foi obtido anteriormente.

Suponha que o resultado seja válido para um grupo que seja produto direto de $t-1$ grupos cíclicos.

Escrevendo $G = (G_1 \times \cdots \times G_{t-1}) \times G_t$ temos que:

$$\begin{aligned} \mathbb{C}G &= \mathbb{C}((G_1 \times \cdots \times G_{t-1}) \times G_t). \\ &\simeq (\mathbb{C}(G_1 \times \cdots \times G_{t-1}))G_t. \\ &\simeq (\mathbb{C} \oplus \cdots \oplus \mathbb{C})G_t. \\ &\simeq \mathbb{C}G_t \oplus \cdots \oplus \mathbb{C}G_t. \end{aligned}$$

Como G_t é cíclico, $\mathbb{C}G_t$ é soma direta de cópias de $\mathbb{C}$, isto mostra que $\mathbb{C}G$ é soma direta de cópias de $\mathbb{C}$. Como a dimensão de $\mathbb{C}G$ como $\mathbb{C}$-espaço vetorial é precisamente $n = |G|$, segue que o número de somandos diretos é igual a n. □

O corolário a seguir vale mais geralmente para qualquer corpo K contendo uma raiz primitiva da unidade de ordem n, tal que $\mathrm{Car}(K) \nmid n$, (ver [1] Seção 3.5.)

Corolário 3.1.2. *Sejam G e H dois grupos abelianos de mesma ordem n, então*

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

Demonstração. Basta observar que

$$\mathbb{C}G \simeq \underbrace{\mathbb{C} \oplus \cdots \oplus \mathbb{C}}_{n\ vezes} \simeq \mathbb{C}H.$$

□

Como não é difícil exibir grupos abelianos de mesma ordem que não são isomorfos, por exemplo, $\mathbb{Z}_4$ e $\mathbb{Z}_2 \times \mathbb{Z}_2$, o corolário acima mostra que

$$\mathbb{C}\mathbb{Z}_4 \simeq \mathbb{C}(\mathbb{Z}_2 \times \mathbb{Z}_2).$$

Assim, o problema do isomorfismo tem resposta negativa sobre o corpo dos complexos.

O restante desde capítulo é dedicado a apresentar algumas das classes para os quais a conjectura (ISO) tem resposta positiva.

3.2 Grupos Abelianos e 2-grupos Hamiltonianos

Voltaremos nossa atenção para o caso que o anel dos coeficientes é o anel dos inteiros.

O motivo para concentrarmos nessa questão segue da seguinte:

Proposição 3.2.1. *Sejam G e H dois grupos tais que $\mathbb{Z}G \simeq \mathbb{Z}H$. Então, $RG \simeq RH$ para qualquer anel R comutativo com unidade (como R-álgebras).*

Demonstração. Assuma que G e H são grupos tais que $\mathbb{Z}G \xrightarrow{\theta} \mathbb{Z}H$ é um isomorfismo. Sendo R um anel comutativo com unidade, R pode ser visto como $\mathbb{Z}$-módulo com a estrutura dada por $nr = \underbrace{r + \cdots + r}_{n \text{ vezes}}$.

Considere

$$i : G \to RG$$

a inclusão de G em RG e considere

$$z : \mathbb{Z} \to RG$$

definida por

$$n \mapsto n \cdot 1_r.$$

Como $rg = gr$ em RG, $\forall\, r \in R\ \forall\, g \in G$, temos que

$$i(g)z(n) = z(n)i(g),$$

$\forall\, n \in \mathbb{Z}\ \forall\, g \in G$. Assim, pelo Teorema 2.1.5, existe um único homomorfismo de $\mathbb{Z}$-álgebras

$$\psi : \mathbb{Z}G \to RG$$

que estende i e z.

Considere também

$$v : R \to RG$$

a inclusão de R em RG. Note que,

$$v(r)\psi(\alpha) = \psi(\alpha)v(r),$$

$\forall\ r \in R\ \forall\ \alpha \in \mathbb{Z}G$. Segue do Lema 2.1.14 que existe um único homomorfismo de $\mathbb{Z}$-álgebras

$$f : R \otimes_{\mathbb{Z}} \mathbb{Z}G \to RG$$

tal que

$$(r \otimes \alpha) \mapsto v(r)\psi(\alpha),$$

$\forall\ r \in R\ \forall\ \alpha \in \mathbb{Z}G$.

A identificação natural de G e R em $R \otimes_{\mathbb{Z}} \mathbb{Z}G$, nos permite, via propriedade universal (Teorema 2.1.5), definir um homomorfismo de $\mathbb{Z}$-álgebras

$$h : RG \to R \otimes_{\mathbb{Z}} \mathbb{Z}G$$

tal que

$$\sum_{a_g \in G} a_g g \mapsto \sum_{a_g \in G} (a_g \otimes g).$$

Afirmamos que h e f são inversas uma da outra. De fato,

$$\begin{aligned} h \circ f \left(r \otimes \sum_{b_g \in G} b_g g \right) &= h \left(r \cdot e \sum_{b_g \in G} (b_g \cdot 1_r) g \right) \\ &= h \left(\sum_{b_g \in G} r(b_g \cdot 1_r) g \right) \\ &= \sum_{b_g \in G} (r(b_g \cdot 1_r) \otimes g) \\ &= \sum_{b_g \in G} (r \otimes b_g g) \\ &= r \otimes \sum_{b_g \in G} b_g g \end{aligned}$$

Além disso,

$$\begin{aligned} f \circ h \left(\sum_{a_g \in G} a_g g \right) &= f \left(\sum_{a_g \in G} (a_g \otimes g) \right) \\ &= \sum_{a_g \in G} (v(a_g)\psi(g)) \\ &= \sum_{a_g \in G} (a_g \cdot e)(g \cdot 1_r) \\ &= \sum_{a_g \in G} a_g g. \end{aligned}$$

Portanto, temos que

$$R \otimes_{\mathbb{Z}} \mathbb{Z}G \simeq RG. \tag{3.1}$$

Analogamente, mostra-se que

$$R \otimes_{\mathbb{Z}} \mathbb{Z}H \simeq RH. \tag{3.2}$$

Denotemos por $\widehat{h}$ o isomorfismo 3.2.

Para mostrar que $R \otimes_{\mathbb{Z}} \mathbb{Z}G \simeq R \otimes_{\mathbb{Z}} \mathbb{Z}H$, considere

$$l_1 : \mathbb{Z}G \to R \otimes_{\mathbb{Z}} \mathbb{Z}H,$$

definida por

$$\alpha \mapsto (1 \otimes \theta(\alpha))$$

e considere

$$l_2 : R \to R \otimes_{\mathbb{Z}} \mathbb{Z}H$$

definida por

$$r \mapsto (r \otimes 1).$$

Com essas definições, l_1 e l_2 são homomorfismos de $\mathbb{Z}$-álgebras. Note também que

$$(1 \otimes \theta(\alpha))(r \otimes 1) = (r \otimes \theta(\alpha)) = (r \otimes 1)(1 \otimes \theta(\alpha)).$$

Assim, pelo Lema 2.1.14 existe um único homomorfismo de $\mathbb{Z}$-álgebras

$$L_1 : R \otimes_{\mathbb{Z}} \mathbb{Z}G \to R \otimes_{\mathbb{Z}} \mathbb{Z}H$$

tal que

$$(r \otimes \alpha) \mapsto l_1(\alpha) l_2(r),$$

$\forall\ \alpha \in \mathbb{Z}G$, $\forall\ r \in R$.

Por uma construção análoga, existe um único homomorfismo de $\mathbb{Z}$-álgebras

$$L_2 : R \otimes_{\mathbb{Z}} \mathbb{Z}H \to R \otimes_{\mathbb{Z}} \mathbb{Z}G$$

tal que

$$(r \otimes \beta) \mapsto (r \otimes \theta^{-1}(\beta)).$$

Assim construídas, L_1 e L_2 são inversas uma da outra. Portanto,

$$R \otimes_{\mathbb{Z}} \mathbb{Z}G \simeq R \otimes_{\mathbb{Z}} \mathbb{Z}H. \tag{3.3}$$

Segue de 3.1, 3.2 e 3.3 que

$$RG \overset{h}{\simeq} R \otimes_{\mathbb{Z}} \mathbb{Z}G \overset{L_1}{\simeq} R \otimes_{\mathbb{Z}} \mathbb{Z}H \overset{\widehat{h}}{\simeq} RH,$$

como $\mathbb{Z}$-álgebras. Para verificar que tal isomorfismo é R-álgebras basta notar que a composta

$$(\widehat{h} \circ L_1 \circ h) : RG \to RH$$

é dada por

$$\sum_{g \in G} a_g g \mapsto \sum_{g \in G} a_g \theta(g)$$

a qual, para $s \in R$ e $\alpha \in RG$, satisfaz

$$(\widehat{h} \circ L_1 \circ h)(s\alpha) = s(\widehat{h} \circ L_1 \circ h)(\alpha).$$

□

No que segue, sempre que nos referirmos a álgebras de grupo isomorfas, suporemos, sem perda de generalidade, pela Definição 2.1.11, que existe um isomorfismo normalizado.

Observação 3.2.2. Suponha que G e H são grupos finitos e seja $\phi : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado. Se $\phi(g) \in H$ para cada elemento $g \in G$ então a restrição $\phi|_G$ fornece um isomorfismo entre G e H. Foi exatamente essa técnica empregada por Higman em [7] para mostrar que grupos abelianos finitos e 2-grupos Hamiltonianos são determinados por seus anéis de grupo integral. A principal dificuldade é que, em geral, não parecem ter motivos para que isso aconteça. No entanto, alguns fatos são conhecidos, por exemplo, se a ordem $|G| = n$, então $g^n = 1$ em $\mathbb{Z}G$, para todo $g \in G$, e segue que, $\phi(g)^n = 1$. Isto mostra que $\phi(g)$, $g \in G$, é sempre um elemento invertível de ordem finita em $\mathbb{Z}H$.

Teorema 3.2.3. *Sejam G grupo finito, H outro grupo e θ um isomorfismo de $\mathbb{Z}$-álgebras entre $\mathbb{Z}G$ e $\mathbb{Z}H$. Então, $\theta(G)$ é uma base para $\mathbb{Z}H$ sobre $\mathbb{Z}$.*

Demonstração. Podemos escrever o grupo G como $G = \{g_1, g_2, \ldots, g_n\}$. Para verificar que o conjunto $\{\theta(g_i) \mid i = 1, \ldots, n\}$ é LI sobre $\mathbb{Z}$, considere a combinação linear

$$c_1\theta(g_1) + \cdots + c_n\theta(g_n) = 0,$$

$c_i \in \mathbb{Z}$. Como θ é um isomorfismo de anéis temos que

$$c_1\theta(g_1) + \cdots + c_n\theta(g_n) = \theta(c_1g_1 + \cdots + c_ng_n) = 0,$$

assim

$$c_1g_1 + \cdots + c_ng_n = 0.$$

Como o grupo G, por definição, é base para $\mathbb{Z}G$, segue que os elementos de G formam um conjunto LI sobre $\mathbb{Z}$, portanto

$$c_1 = \cdots = c_n = 0.$$

Note que para mostrar que $\theta(G)$ gera $\mathbb{Z}H$ é suficiente mostrar que os elementos de H podem ser escritos como combinação linear de elementos de $\theta(G)$ com coeficientes em $\mathbb{Z}$, pois cada elemento em $\mathbb{Z}H$ é uma combinação linear do elementos de H com coeficientes em $\mathbb{Z}$. Assim, dado $h \in H$, existe $\alpha \in \mathbb{Z}G$ tal que $\theta(\alpha) = h$.

Escrevendo $\alpha = \sum_{g \in G} a(g)g$ temos que

$$\theta(\alpha) = \theta\left(\sum_{g \in G} a(g)g\right) = \sum_{g \in G} a(g)\theta(g),$$

que é uma combinação linear de elementos de $\theta(G)$ com coeficientes em $\mathbb{Z}$.

□

Corolário 3.2.4. *Seja G um grupo finito e H outro grupo tal que $\mathbb{Z}G \xrightarrow{\phi} \mathbb{Z}H$ é um isomorfismo de $\mathbb{Z}$-álgebras. Então, $|G| = |H|$.*

Demonstração. Com efeito, pelo Teorema 3.2.3, $\phi(G)$ é uma base para $\mathbb{Z}H$ sobre $\mathbb{Z}$ e por definição, H também é uma base para $\mathbb{Z}H$ sobre Z. Portanto, segue do Teorema 1.2.4 que

$$|H| = |\phi(G)| = |G|.$$

□

Teorema 3.2.5. *Seja G um grupo abeliano finito e seja H outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$. Então $G \simeq H$.*

Demonstração. Se $\mathbb{Z}G \simeq \mathbb{Z}H$, podemos assumir que existe um isomorfismo normalizado $\phi : \mathbb{Z}G \to \mathbb{Z}H$.

Como G é abeliano, segue da definição do produto em anel de grupo que $\mathbb{Z}G$ é comutativo. Assim, $\mathbb{Z}H$ é comutativo, em particular, $h_1h_2 = h_2h_1, \forall\, h_1,\, h_2 \in H$, ou seja, H é abeliano. Pelo Teorema 3.2.4, temos que

$$|H| = |G|.$$

Para cada elemento $g \in G$, o elemento $\phi(g)$ é uma unidade de ordem finita em $\mathbb{Z}H$, como visto na Observação 3.2.2. Segue do Teorema 2.4.1.6 que $\phi(g) = \pm h$, para algum $h \in H$, e como ϕ é normalizado, $\epsilon(\phi(g)) = \epsilon(g) = 1$, o que mostra que $\phi(g) = h \in H$. Isto mostra que $\phi(G) \subseteq H$ e, como $|G| = |H|$ e ϕ é uma bijeção, temos que $\phi(G) = H$. Em outras palavras, a restrição $\phi|_G$ é um isomorfismo de grupos entre G e H.

□

Note que os argumentos acima permitem provar que o centro de um grupo finito é invariante sob isomorfismos de anéis de grupo, como mostra a proposição seguinte:

Proposição 3.2.6. *Seja G um grupo finito e seja H outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$. Então, $Z(G) \simeq Z(H)$.*

Demonstração. Seja $g \in Z(G)$. Vamos mostrar primeiramente que se $\phi : \mathbb{Z}G \to \mathbb{Z}H$ é um isomorfismo normalizado então $\phi(g)$ é uma unidade central de ordem finita em $\mathbb{Z}H$.

A parte que $\phi(g)$ é uma unidade de ordem finita já foi visto na Observação 3.2.2. Verificaremos que ela é central.

Seja $\beta \in \mathbb{Z}H$, devemos mostrar que $\beta\phi(g) = \phi(g)\beta$. De fato, seja $\rho \in \mathbb{Z}G$ tal que $\phi(\rho) = \beta$. Assim,

$$\begin{aligned} \beta\phi(g) &= \phi(\rho)\phi(g). \\ &= \phi(\rho g). \\ &= \phi(g\rho). \\ &= \phi(g)\phi(\rho). \\ &= \phi(g)\beta, \end{aligned}$$

onde a terceira igualdade se justifica pelo fato de $g \in Z(G)$, o que implica $g \in Z(\mathbb{Z}G)$.

Assim, pelo Corolário 2.4.1.5,

$$\phi(g) = \pm h,\ h \in Z(H).$$

Como ϕ é normalizado, $\epsilon(\phi(g)) = \epsilon(g) = 1$, assim

$$\phi(g) \in Z(H).$$

Portanto,

$$\phi(Z(G)) \subseteq Z(H)$$

e analogamente

$$\phi^{-1}(Z(H)) \subseteq Z(G),$$

ou seja,

$$Z(H) \subseteq \phi(Z(G)).$$

□

Teorema 3.2.7. *Seja G um 2-grupo hamiltoniano finito e seja H outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$. Então $G \simeq H$.*

Demonstração. Como G é um 2-grupo hamiltoniano então, pelo Teorema 2.4.4.5, todas as unidades do anel de grupo integral $\mathbb{Z}G$ são triviais. Portanto, o número de unidades de $\mathbb{Z}G$ é $2|G|$, pois as unidades trivias são da forma $\pm g$ com $g \in G$. Consequentemente, o número de unidades de $\mathbb{Z}H$ é $2|G|$. Pelo Teorema 3.2.4, temos que $|G| = |H|$. Com isso, segue que o número de unidades de $\mathbb{Z}H$ é $2|G|$ $= 2|H|$, portanto todas as unidades de $\mathbb{Z}H$ são triviais.

Como H não é abeliano, pois do contrário, o Teorema 3.2.5, forneceria que G é abeliano, segue por 2.4.4.6 que H é também um 2-grupo hamiltoniano finito. Supondo o isomorfismo entre $\mathbb{Z}G$ e $\mathbb{Z}H$ normalizado, segue dos mesmos argumentos do Teorema 3.2.5 que $\phi(G) = H$, assim a restrição $\phi|_G$ é um isomorfismo entre G e H.

□

3.3 A Correspondência Entre Subgrupos Normais

Para a validade da conjectura ISO nos demais casos, o isomorfismo entre os grupos envolvidos não necessariamente será a restrição do isomorfismo original ao grupo G. Assim, precisaremos dar uma abordagem diferente à dada nos dois casos precedentes. A correspondência definida a seguir é uma importante ferramenta e será utilizada na demonstração da conjectura ISO no caso nilpotente.

O leitor pode consultar [25] para outras aplicações.

Definição 3.3.1. *Sejam G um grupo finito, R um anel comutativo e $\{C_i\}_{i\in I}$ o conjunto das classes de conjugação de G. Para cada $i \in I$ seja*

$$\gamma_i = \widehat{C_i} = \sum_{x \in C_i} x \in RG.$$

*Esses elementos são chamados **somas de classes** de G sobre R.*

Teorema 3.3.2. *Sejam G e H grupos finitos e seja $\phi : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado. Denote por $\{\gamma_i\}_{i\in I}$ e por $\{\delta_j\}_{j\in I}$ as somas de classes de G e H, respectivamente. Então, para cada γ_i existe um unico δ_j tal que $\phi(\gamma_i) = \delta_j$. Isto é, existe um correspondência biunívoca entre as somas de classes de G e H, respectivamente.*

A demonstração desse teorema será omitida pelo fato dela ser baseada no conceito de caracteres, que não é abordado nesta dissertação. O leitor pode encontrá-la em [25], Teorema 3.1.

Lembramos que para um dado subconjunto N de um grupo G, denotamos $\widehat{N} = \sum_{x\in N} x$.

Teorema 3.3.3. *Sejam G e H grupos finitos tais que $\mathbb{Z}G \simeq \mathbb{Z}H$ e N um subgrupo normal de G. Seja $\phi : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado. Então, existe $M \lhd H$ tal que $\phi(\widehat{N}) = \widehat{M}$ e $|N| = |M|$. A correspondência $N \mapsto M$ preserva inclusão e, portanto, também interseções e produtos.*

Demonstração. Como $N \lhd G$, N é uma união disjunta e finita de classes de conjugação de G, ou seja, $N = C_1 \cup \cdots \cup C_t$. Considere $\widehat{C_i}$ a correspondente soma de classe, logo, $\widehat{N} = \sum_{i=1}^{t} \widehat{C_i}$. Pelo Teorema 3.3.2, segue $\phi(\widehat{C_i})$ é uma soma de classe em H, digamos $\widehat{D_i}$.

Note que $\widehat{N}\widehat{N} = |N|\widehat{N}$, pois

$$\widehat{N}\widehat{N} = \widehat{N}\sum_{n\in N} n = \sum_{n\in N} \widehat{N}n = \sum_{n\in N} \widehat{N} = |N|\widehat{N}.$$

Além disso,

$$\phi(\widehat{N}) = \phi\left(\sum_{i=1}^{t} \widehat{C_i}\right) = \sum_{i=1}^{t} \phi(\widehat{C_i}) = \sum_{i=1}^{t} \widehat{D_i} = \widehat{M},$$

para algum subconjunto M de H. Verificaremos que M é um subgrupo de H.

Aplicando ϕ nos dois membros da igualdade $\widehat{N}\widehat{N} = |N|\widehat{N}$, vemos que

$$\widehat{M}\widehat{M} = \phi(\widehat{N}\widehat{N}) = \phi(|N|\widehat{N}) = |N|\phi(\widehat{N}) = |N|\widehat{M}. \tag{3.4}$$

Como o suporte de $\widehat{M}\widehat{M}$ é da forma

$$supp(\widehat{M}\widehat{M}) = \{m_i \cdot m_j \mid m_i, m_j \in M\}$$

e

$$supp(|N|\widehat{M}) = M,$$

a igualdade entre esses elementos, dada por 3.4, mostra que M é fechado para multiplicação.

Para verificar que o inverso de cada elemento de M está em M, seja $k := |M|$. Como N é finito,

$$\phi(\widehat{N}) = \phi(e + n_1 + \cdots + n_l) = \phi(e) + \phi(n_1) + \cdots + \phi(n_l),$$ [1]

[1] Vale ressaltar que para um certo $n_i \in N$ não há, *a priori*, motivos para que $\phi(n_i) \in M$, como observado em 3.2.2. O que os argumentos anteriores nos permitem garantir é que $\phi(e) + \phi(n_1) + \cdots + \phi(n_l)$ resultará no elemento $\widehat{M}$.

para algum índice l. Como $\phi(e) = e$, segue que $e \in M$.

Agora para cada índice i, $1 \leq i \leq k$, considere o seguinte conjunto:

$$M_i = \{m_i m_1, \cdots, m_i^2, \cdots, m_i m_k\}.$$

Como em M_i temos k elementos distintos de M, segue $M_i = M$. Assim, para algum índice t, $1 \leq t \leq k$, temos que

$$m_i m_t = e,$$

logo $m_i^{-1} = m_t \in M$.

Como M é uma união de classes de conjugação pelo Teorema 3.3.2, segue que $M \lhd H$. Assim, $\widehat{M}\widehat{M} = |M|\widehat{M}$ e já vimos que $\widehat{M}\widehat{M} = |N|\widehat{M}$, portanto $|M|\widehat{M} = |N|\widehat{M}$, consequentemente $|N| = |M|$.

A correspondência $N \mapsto M$ preserva inclusões devido ao fato que se $N' \subset N$ é normal em G, então N' se escreve com união de alguns dos C_i, $1 \leq i \leq t$. Isso implica que o subgrupo normal M' correspondente será uma união de algumas das classes D_i, $1 \leq i \leq t$, ou seja, $M' \subset M$.

□

Observação 3.3.4. Resulta do Teorema 3.3.3 que se G é um grupo simples finito e H é outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$, então H também é um grupo simples. Os grupos simples finitos estão determinados por sua ordem a menos de duas exceções (ver [31]) que são tratadas separadamente. Assim, como o isomorfismo entre $\mathbb{Z}G$ e $\mathbb{Z}H$ implica que $|G| = |H|$, temos a validade da conjectura ISO no caso em que G é um grupo simples finito. Para mais detalhes, o leitor por consultar [31] ou [25].

Observação 3.3.5. Em 2.2.7 definimos o anulador de um subconjunto de um anel de grupo RG. O lema a seguir diz qual é o anulador do elemento $\widehat{N} = \sum_{n \in N} n \in \mathbb{Z}G$ quando $N \lhd G$. A partir desse lema demonstraremos uma importante propriedade da correspondência entre subgrupos normais.

Lema 3.3.6. *Sejam G um grupo finito e $N \lhd G$. Então,*

$$Ann(\widehat{N}) = \{x \in \mathbb{Z}G \mid x\widehat{N} = 0\} = \Delta(G, N).$$

Demonstração. Note que $(n-1)\widehat{N} = n\widehat{N} - \widehat{N} = \widehat{N} - \widehat{N} = 0$ para todo $n \in N$. Assim, $\Delta(G, N) \subset Ann(\widehat{N})$.

Para mostrar a outra inclusão vamos olhar para a expressão da imagem de $\alpha\widehat{N}$ pela extensão canônica ω^* definida em 2.2.4.

$$\omega^*(\alpha\widehat{N}) = \omega^*(\alpha)\omega^*(\widehat{N}).$$

Mas, $\omega^*(\widehat{N}) = \sum_{n \in N} 1\overline{n}$. Como $\overline{n}$ é a identidade em G/N para cada $n \in N$, temos que

$$\omega^*(\widehat{N}) = |N|\overline{e}.$$

Com isso,

$$\omega^*(\alpha\widehat{N}) = \omega^*(\alpha)|N|\overline{e} = |N|\omega^*(\alpha)\overline{e} = |N|\omega^*(\alpha).$$

Assim, se $\alpha \in Ann(\widehat{N})$, então

$$0 = \omega^*(\alpha\widehat{N}) = |N|\omega^*(\alpha),$$

o que mostra que $\omega^*(\alpha) = 0$, ou seja, $\alpha \in \mathrm{Ker}(\omega^*) = \Delta(G, N)$ pela Proposição 2.2.5. Isso mostra que $Ann(\widehat{N}) \subset \Delta(G, N)$, portanto temos a igualdade

$$\Delta(G, N) = Ann(\widehat{N}).$$

□

Proposição 3.3.7. *Sejam G e H grupos finitos, $\theta : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado, $N \lhd G$ e $M \lhd H$ o correspondente de N dado pelo Teorema 3.3.3. Então, $\theta(\Delta(G, N)) = \Delta(H, M)$.*

Demonstração. Pelo Lema 3.3.6, temos que $\Delta(G, N)\widehat{N} = 0$. Assim,

$$0 = \theta(\Delta(G, N))\theta(\widehat{N}) = \theta(\Delta(G, N))\widehat{M}.$$

Com isso, $\theta(\Delta(G, N)) \subset Ann(\widehat{M}) = \Delta(H, M)$. Analogamente, mostra-se que $\Delta(H, M) \subset \theta(\Delta(G, N))$.

□

3.4 Grupos Metabelianos

O teorema central desta seção é o Teorema de Whitcomb, do qual, como corolário, resulta a validade da conjectura ISO para grupos metabelianos finitos.

Definição 3.4.1. *Um grupo G é chamado um **grupo metabeliano** se contém um subgrupo normal A, tal que, ambos, A e $\dfrac{G}{A}$, são abelianos.*

Exemplo 3.4.2. O grupo D_4 é metabeliano, pois tomando $A = (D_4)'$, o subgrupo dos comutadores de D_4, temos que A é abeliano uma vez que $|A| = 2$, além disso, como $\left|\dfrac{D_4}{(D_4)'}\right| = 4$, segue que $\dfrac{D_4}{(D_4)'}$ também é abeliano. Outro exemplo de grupo metabeliano é o S_3, pois tomando $A = \langle a; |a| = 3\rangle$, temos que A é abeliano, e $\dfrac{S_3}{A}$ também é abeliano, pois $\left|\dfrac{S_3}{A}\right| = 2$.

Mostraremos que esse tipo de grupo é determinado por seu anel de grupo integral. Para isso precisaremos de alguns resultados técnicos. Primeiramente, diremos que $x \in \Delta^2(G)$ se $x = \alpha\beta$, com $\alpha, \beta \in \Delta(G)$. Note que se $g, h \in G$ então temos a seguinte identidade:

$$gh - 1 = (g - 1) + (h - 1) + (g - 1)(h - 1). \tag{3.5}$$

Além disso, como

$$(g - 1)(h - 1) \in \Delta^2(G), \tag{3.6}$$

de 3.5 obtemos

$$gh - 1 \equiv (g - 1) + (h - 1) \mod \Delta^2(G). \tag{3.7}$$

Fazendo $h = g^{-1}$, temos que

$$g^{-1} - 1 \equiv -(g-1) \mod \Delta^2(G). \tag{3.8}$$

Portanto, para qualquer inteiro a

$$g^a - 1 \equiv a(g-1) \mod \Delta^2(G). \tag{3.9}$$

Para verificar a congruência 3.9 usaremos indução em a. Consideraremos primeiramente o caso em que $a > 0$. Se $a = 1$, então o resultado é verdadeiro, pois $a = 1 \Rightarrow (g^a - 1) = a(g-1) = (g-1)$. Suponha por hipótese de indução o resultado verdadeiro para $a-1$, $a > 1$. Escreva $g^a - 1 = g^{a-1}g - 1$ e segue por 3.7 que

$$g^a - 1 \equiv (g^{a-1} - 1) + (g-1) \mod \Delta^2(G).$$

Usando a hipótese de indução, temos que

$$g^a - 1 \equiv (a-1)(g-1) + (g-1) \mod \Delta^2(G),$$

o que mostra que

$$g^a - 1 \equiv a(g-1) \mod \Delta^2(G).$$

Assim temos que o resultado é verdadeiro para todo $a \in \mathbb{N}$.

Se $a < 0$, então $-a > 0$, assim por 3.8 temos que

$$(g^a - 1) = (g^{-a})^{-1} - 1 \equiv -(g^{-a} - 1) \mod \Delta^2(G).$$

Como

$$(g^{-a} - 1) \equiv -a(g-1) \mod \Delta^2(G),$$

segue que

$$(g^a - 1) \equiv a(g-1) \mod \Delta^2(G).$$

Como o caso $a = 0$ é imediato, concluimos nossa verificação.

Consequentemente, a aplicação

$$\phi : G \to \Delta(G)/\Delta^2(G) \tag{3.10}$$

dada por $\phi(g) = (g-1) + \Delta^2(G)$ é um homomorfismo de grupos. De fato,

$$\begin{aligned}
\phi(gh) &= (gh-1) + \Delta^2(G) \\
&= (g-1) + (h-1) + (g-1)(h-1) + \Delta^2(G) \text{ (por 3.5)} \\
&= (g-1) + (h-1) + \Delta^2(G) \\
&= [(g-1) + \Delta^2(G)] + [(h-1) + \Delta^2(G)] \\
&= \phi(g) + \phi(h)
\end{aligned}$$

Observação 3.4.3. Para os próximos resultados, faremos uso do conhecido resultado da Teoria de Grupos:

(i) $G' \triangleleft G$. Em que G' denota o subgrupo dos comutadores de G.

(ii) $\dfrac{G}{G'}$ é abeliano.

(iii) Se N é outro subgrupo normal de G tal que $\dfrac{G}{N}$ é abeliano, então, $G' \subset N$.

Lema 3.4.4. *Seja G um grupo finito. Então,*

$$\frac{G}{G'} \simeq \frac{\Delta(G)}{\Delta^2(G)}.$$

Demonstração. Dado G, defina $\phi : G \to \Delta(G)/\Delta^2(G)$ como acima. Temos que

$$\frac{G}{\mathrm{Ker}(\phi)} \simeq Im(\phi),$$

que é abeliano, pois $\Delta(G)/\Delta^2(G)$ é um grupo aditivo. Como $\mathrm{Ker}(\phi) \triangleleft G$, temos que $G' \subset \mathrm{Ker}(\phi)$, por (iii) da Observação 3.4.3. Consequentemente, ϕ induz uma aplicação

$$\phi^* : \frac{G}{G'} \to \frac{\Delta(G)}{\Delta^2(G)}$$

que associa

$$gG' \mapsto (g-1) + \Delta^2(G).$$

Para mostrarmos que ϕ^* é um isomorfismo, exibiremos sua inversa. Na Proposição 2.1.10, vimos que o conjunto $\{g-1;\ g \in G\}$ é uma base de $\Delta(G)$ sobre $\mathbb{Z}$. Podemos definir uma aplicação $\psi : \Delta(G) \to G/G'$ definindo a imagem dos elementos desta base:

$$\psi(g-1) = gG' \ \ \forall\ g \in G.$$

Note que se $\alpha = -(a-1)(b-1) \in \Delta^2(G)$, então $\alpha = (a-1)+(b-1)-(ab-1)$, além disso, sendo ψ um homomorfismo de grupos, devemos ter

$$\begin{aligned} \psi(0) &= \psi(-(ab-1)+(ab-1)) \\ &= \psi(-(ab-1))\psi(ab-1)) \\ &= eG' \\ &= \overline{e} \end{aligned}$$

Segue que $\psi(-(ab-1)) = (ab)^{-1}G'$.
Assim, temos que:

$$\psi(\alpha) = aG'.bG'.(ab)^{-1}G' = abb^{-1}a^{-1}G' = G'.$$

Portanto, $\alpha \in \mathrm{Ker}(\psi)$. Isto mostra que $\Delta^2(G) \subset \mathrm{Ker}(\psi)$. Assim, ψ induz um homomorfismo de grupos $\psi^* : \dfrac{\Delta(G)}{\Delta^2(G)} \to \dfrac{G}{G'}$, associando $(g-1)+\Delta^2(G) \mapsto gG'$. Com isso, ϕ^* e ψ^* são inversas uma da outra. Com efeito,

$$(\phi^* \circ \psi^*)[(g-1)+\Delta^2(G)] = \phi(gG') = (g-1)+\Delta^2(G),$$

e também,

$$(\psi^* \circ \phi^*)(gG') = \psi([(g-1) + \Delta^2(G)]) = gG',$$

concluímos que

$$\phi^* \circ \psi^* = \psi^* \circ \phi^* = Id.$$

□

Temos os seguintes corolários:

Corolário 3.4.5. *Sejam G um grupo e G' seu subgrupo dos comutadores. Então,*

$$G \cap (1 + \Delta^2(G)) = G'.$$

Demonstração. Os argumentos da prova anterior mostram, em particular, que $\text{Ker}(\phi) = G'$. Mas, $\text{Ker}(\phi) = \{g \in G;\ g - 1 \in \Delta^2(G)\} = G \cap (1 + \Delta^2(G))$.

□

Corolário 3.4.6. *Sejam G e H grupos tais que $\mathbb{Z}G \simeq \mathbb{Z}H$. Então,*

$$\frac{G}{G'} \simeq \frac{H}{H'}.$$

Demonstração. Seja $\theta : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado. Sendo $\Delta(G)$ e $\Delta(H)$ os kernels das respectivas aplicações de aumento, temos que $\theta(\Delta(G)) = \Delta(H)$. Com efeito, seja $\alpha \in \Delta(G)$. Como θ é um isomorfismo normalizado, temos que,

$$0 = \epsilon(\alpha) = \epsilon(\theta(\alpha)).$$

Isso mostra que $\theta(\alpha) \in \Delta(H)$, portanto, $\theta(\Delta(G)) \subset \Delta(H)$. Analogamente, com a ressalva que se θ é um isomorfismo normalizado, então θ^{-1} também é um isomorfismo normalizado, mostra-se que $\Delta(H) \subset \theta(\Delta(G))$. Consequentemente, $\theta(\Delta(G)) = \Delta(H)$ e também, $\theta(\Delta^2(G)) = \Delta^2(H)$.

Agora considere o homomorfismo de grupos $\omega : \Delta(G) \to \dfrac{\Delta(H)}{\Delta^2(H)}$ dado por:

$$g - 1 \mapsto \theta(g-1) + \Delta^2(G), \text{(nos elementos da base)}$$

cujo kernel é exatamente $\Delta^2(G)$, pois $\theta(\Delta^2(G)) = \Delta^2(H)$. Portanto, pelo Teorema do Isomorfismo,

$$\frac{\Delta(G)}{\Delta^2(G)} \simeq \frac{\Delta(H)}{\Delta^2(H)}.$$

Finalmente, pelo Lema 3.4.4, obtemos:

$$\frac{G}{G'} \simeq \frac{\Delta(G)}{\Delta^2(G)} \simeq \frac{\Delta(H)}{\Delta^2(H)} \simeq \frac{H}{H'}.$$

□

Antes de enunciar e demonstrar o Teorema de Whitcomb, precisamos ainda dos três lemas seguintes:

Lema 3.4.7. *Seja I um ideal de $\mathbb{Z}G$. Então, o anel quociente $\mathbb{Z}G/I$ é comutativo se, e somente se, $\Delta(G, G') \subset I$.*

Demonstração. Seja I um ideal de $\mathbb{Z}G$ tal que o quociente $\mathbb{Z}G/I$ é comutativo. Assim,

$$\overline{gh} = \overline{hg} \ \ \forall\ g,\ h \in G,$$

ou seja,

$$gh - hg \equiv 0 \mod I,$$

e, portanto, para todo $g,\ h \in G$ temos que $gh - hg \in I$, assim,

$$hg(g^{-1}h^{-1}gh - 1) \in I.$$

Como hg é invertível em $\mathbb{Z}G$, temos que $g^{-1}h^{-1}gh - 1 = (g,h) - 1 \in I$, e segue que $\Delta(G, G') \subset I$.

Reciprocamente, note que $gh - hg = hg((g,h) - 1) \in \Delta(G, G'),\ \forall\ g, h \in G$.

Se $\Delta(G, G') \subset I$, temos que $gh \equiv hg \mod I$, para todos $g,\ h \in G$, logo

$$\overline{gh} = \overline{hg}$$

em $\mathbb{Z}G/I,\ \forall\ g, h \in G$. Portanto, $\mathbb{Z}G/I$ é comutativo.

□

Lema 3.4.8. (Ver [1] pág. 294.) *Seja $N \triangleleft G$. Se um elemento $g \in G$ é tal que $g - 1 \in \Delta(G)\Delta(G, N)$, então $g \in N'$.*

Corolário 3.4.9. *Seja G um grupo. Denotando por $G'' := (G')'$, temos que*

$$G'' = 1 + \Delta(G)\Delta(G, G')$$

Demonstração. O Lema 3.4.8 mostra que

$$1 + \Delta(G)\Delta(G, G') \subseteq G''.$$

Por outro lado,

$$G'' = G' \cap 1 + \Delta^2(G')$$

pelo Corolário 3.4.5. Como $\Delta^2(G') \subseteq \Delta(G)\Delta(G, G')$, temos que

$$G'' = G' \cap 1 + \Delta^2(G') \subseteq 1 + \Delta(G)\Delta(G, G').$$

Poranto, temos a igualdade. □

Lema 3.4.10. *Sejam G e H grupos finitos tais que $\mathbb{Z}G \simeq \mathbb{Z}H$ e seja θ um isomorfismo normalizado entre $\mathbb{Z}G$ e $\mathbb{Z}H$. Então,*

$$\theta(\Delta(G, G')) = \Delta(H, H').$$

Demonstração. Considere o homomorfismo sobrejetor de anéis $\theta^* : \mathbb{Z}G \to \dfrac{\mathbb{Z}H}{\Delta(H, H')}$, dado por

$$\alpha \mapsto \overline{\theta(\alpha)}.$$

Do Lema 3.4.7, temos que $\dfrac{\mathbb{Z}H}{\Delta(H, H')}$ é comutativo. Como

$$\frac{\mathbb{Z}G}{\mathrm{Ker}(\theta^*)} \simeq \frac{\mathbb{Z}H}{\Delta(H, H')},$$

segue que $\dfrac{\mathbb{Z}G}{\mathrm{Ker}(\theta^*)}$ é comutativo, o que implica que $\Delta(G,G') \subset \mathrm{Ker}(\theta^*)$, pelo Lema 3.4.7. Assim,

$$\theta^*(\Delta(G,G')) = 0,$$

logo,

$$\theta(\Delta(G,G')) \subset \Delta(H,H').$$

Analogamente, definimos um homormorfismo sobrejetor $\Psi : \mathbb{Z}H \to \dfrac{\mathbb{Z}G}{\Delta(G,G')}$ por:

$$\beta \mapsto \overline{\theta^{-1}(\beta)}.$$

Assim, aplicando novamente o lema 3.4.7, temos que $\dfrac{\mathbb{Z}H}{\mathrm{Ker}(\Psi)}$ é comutativo e $\Delta(H,H') \subset \mathrm{Ker}(\Psi)$, assim $\Psi(\Delta(H,H')) = 0$, o que mostra que

$$\theta^{-1}(\Delta(H,H')) \subset \Delta(G,G').$$

Aplicando θ nesta última inclusão temos que

$$\Delta(H,H') \subset \theta(\Delta(G,G')).$$

Consequentemente,

$$\theta(\Delta(G,G')) = \Delta(H,H').$$

□

Teorema 3.4.11. *(Whitcomb) Seja G um grupo finito. Se H é outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$, então*

$$\frac{G}{G''} \simeq \frac{H}{H''}.$$

Demonstração. Seja $\theta : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado.

Dado um elemento $g \in G$, como G é finito, $\gamma = \theta(g)$ é uma unidade de ordem finita em $\mathbb{Z}H$. Se denotarmos por $\overline{\gamma}$ a imagem de γ no anel quociente

$$\frac{\mathbb{Z}H}{\Delta(H,H')} \simeq \mathbb{Z}\left(\frac{H}{H'}\right), \tag{3.11}$$

(Corolário 2.2.6), então $\overline{\gamma}$ também será uma unidade de ordem finita em $\dfrac{\mathbb{Z}H}{\Delta(H,H')}$.

Como $\dfrac{H}{H'}$ é um grupo abeliano e de torção, segue que as unidades de $\mathbb{Z}\left(\dfrac{H}{H'}\right)$ são triviais pelo Teorema 2.4.1.6, logo pelo isomorfismo 3.11 temos que as unidades em $\dfrac{\mathbb{Z}H}{\Delta(H,H')}$ são triviais. Mas, uma unidade trivial em $\dfrac{\mathbb{Z}H}{\Delta(H,H')}$ é a classe de uma unidade trivial em $\mathbb{Z}H$.

Logo, existe um elemento $h_0 \in H$ tal que $\overline{\gamma} = \overline{h_0}$ em $\dfrac{\mathbb{Z}H}{\Delta(H,H')}$, ou, equivalentemente, tal que

$$\gamma \equiv h_0 \mod \Delta(H,H').$$

Isso mostra que $\gamma = h_0 + \delta$ para algum $\delta \in \Delta(H,H')$ da forma $\delta = \sum_{h \in H'} \alpha_h(h-1)$, com $\alpha_h \in \mathbb{Z}H$.

Seja $b_h := \epsilon(\alpha_h)$. Assim, podemos escrever

$$\gamma = h_0 + \sum_{h \in H'} [b_h(h-1) + (\alpha_h - b_h)(h-1)].$$

Escrevendo $\alpha_h = \sum_{h \in H} a(h)h$, temos que,

$$\alpha_h - b_h = \sum_{h \in H} a(h)h - \sum_{h \in H} a(h) = \sum_{h \in H} a(h)(h-1) \in \Delta(H),$$

portanto

$$\gamma \equiv h_0 + \sum_{h \in H'} b_h(h-1) \mod \Delta(H)\Delta(H, H').$$

Assim,

$$\gamma - 1 \equiv h_0 - 1 + \sum_{h \in H'} b_h(h-1) \mod \Delta(H)\Delta(H, H'). \tag{3.12}$$

Podemos reescrever esta equação como

$$\gamma - 1 \equiv h_0 \prod_{h \in H'} h^{b_h} - 1 \mod \Delta(H)\Delta(H, H').$$

Com efeito, aplicando a equação 3.9 a cada um dos termos do somatório, a equação 3.12 pode ser escrita como

$$\gamma - 1 \equiv h_0 - 1 + \sum_{h \in H'} (h^{b_h} - 1) \mod \Delta(H)\Delta(H, H')). \tag{3.13}$$

Assim, aplicando 3.7 em $h_0 - 1$ e em cada termo do somatório, podemos escrever 3.13 como

$$\gamma - 1 \equiv \left(h_0 \prod_{h \in H'} h^{b_h} \right) - 1 \mod \Delta(H)\Delta(H, H').$$

Portanto, $h_g := h_0 \prod_{h \in H'} h^{b_h}$ é um elemento em H tal que $\gamma \equiv h_g \mod \Delta(H)\Delta(H, H')$.

Definimos então a seguinte aplicação: $\phi : G \to \dfrac{H}{H''}$ por

$$\phi(g) = \overline{h_g}.$$

Afirmamos que ϕ está bem definida e é um homomorfismo de grupos. De fato, se h_1, $h_2 \in H$ são tais que

$$h_1 \equiv h_2 \mod \Delta(H)\Delta(H, H'),$$

então,

$$h_1 h_2^{-1} \equiv 1 \mod \Delta(H)\Delta(H, H'),$$

assim,

$$h_1 h_2^{-1} - 1 \in \Delta(H)\Delta(H, H').$$

Pelo Lema 3.4.8, $h_1 h_2^{-1} \in H''$. Consequentemente, $\overline{h_1} = \overline{h_2}$ em $\dfrac{H}{H''}$.

Para verificar que ϕ é homomorfismo de grupos note que para g e y elementos arbitrários de G temos que

$$\theta(gy) \equiv h_{gy} \mod \Delta(H)\Delta(H, H')). \tag{3.14}$$

Por outro lado,

$$\theta(g) \equiv h_g \mod \Delta(H)\Delta(H, H')$$

e também

$$\theta(y) \equiv h_y \mod \Delta(H)\Delta(H, H').$$

Com isso,

$$\theta(gy) = \theta(g)\theta(y) \equiv h_g h_y \mod \Delta(H)\Delta(H, H'). \tag{3.15}$$

Assim, pelas equações 3.14 e 3.15, temos que

$$h_{gy} \equiv h_g h_y \mod \Delta(H)\Delta(H, H').$$

Com isso,

$$\phi(gy) = \overline{h_{gy}} = \overline{h_g h_y} = \overline{h_g}\,\overline{h_y},$$

ou seja, ϕ é um homomorfismo de grupos.

Agora, seja $g \in \mathrm{Ker}(\phi)$. Então,

$$\overline{h_g} \in H'' = 1 + \Delta(H)\Delta(G, H'),$$

pelo Corolário 3.4.9. Com isso, $\overline{h_g} \equiv 1 \mod \Delta(H)\Delta(H, H')$ e como $\theta(g) \equiv \overline{h_g} \mod \Delta(H)\Delta(H, H')$, segue que

$$\theta(g) \equiv 1 \mod \Delta(H)\Delta(H, H').$$

Aplicando θ^{-1} temos que $g \equiv 1 \mod \Delta(G)\Delta(G, G')$, assim pelo Lema 3.4.8, obtemos que $g \in G''$. Portanto, ϕ induz um homomorfismo injetivo de grupos $\phi^* : \dfrac{G}{G''} \to \dfrac{H}{H''}$.

Para mostrar que ϕ^* é também sobrejetiva, dado um elemento $h \in H$, existe $g_0 \in G$, construído a partir de θ^{-1} seguindo os mesmos passos da construção do elemento h_g, tal que

$$\theta^{-1}(h) \equiv g_0 \mod \Delta(G)\Delta(G, G').$$

Como $\theta(\Delta(G)) = \Delta(H)$ (ver demonstração do Corolário 3.4.6) e $\theta(\Delta(G, G')) = \Delta(H, H')$ pelo Lema 3.4.10, aplicando θ obtemos

$$h \equiv \theta(g_0) \mod \Delta(H)\Delta(H, H').$$

Portanto, $\phi(g_0) = \overline{h}$. Isto mostra que ϕ^* é também sobrejetiva e, portanto,

$$\frac{G}{G''} \simeq \frac{H}{H''}.$$

□

O Teorema de Whitcomb nos permite mostrar que grupos metabelianos finitos são determinados por seu anel de grupo integral.

Corolário 3.4.12. *Seja G um grupo metabeliano finito e seja H outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$. Então, $G \simeq H$.*

Demonstração. Primeiramente, note que se G é metabeliano, então G' é abeliano. De fato, como G é metabeliano, G contém um subgrupo normal A tal que, ambos, A e $\dfrac{G}{A}$ são abelianos, donde segue que $G' \subset A$, portanto G' é abeliano. Em particular, $G'' = \{e\}$.

A existência de um isomorfismo entre $\mathbb{Z}G$ e $\mathbb{Z}H$ implica pelo Teorema 3.2.4 que $|G| = |H|$. Como $G'' = \{id\}$, segue do Teorema de Whitcomb que

$$G \simeq \frac{H}{H''}$$

e como $|H| = |G|$, segue que $H'' = \{id\}$. Portanto,

$$G \simeq H.$$

□

3.5 Grupos Nilpotentes Finitos

3.5.1 Propriedades de Grupos Nilpotentes

Começaremos definindo grupos nilpotentes e destacaremos suas principais propriedades. Tal abordagem é encontrada nos livros clássicos de Grupos, mas tomamos como referência [3].

Definicão 3.5.1.1. *Um grupo G diz-se **nilpotente** se ele contém uma série de subgrupos*

$$\{e\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

*tal que cada G_{i-1} é normal em G e cada quociente $\dfrac{G_i}{G_{i-1}}$ está contido no centro de $\dfrac{G}{G_{i-1}}$, $1 \leq i \leq n$. Uma tal série de subgrupos, chama-se uma **série central** de G.*

Uma vez que as condições na definição de nilpotência são mais restritas que as condições que aparecem na definição de solubilidade, resulta que todo grupo nilpotente é, em particular, solúvel.

Note que da definição temos que G_1 está contido no centro de G. Se $G_1 = \{e\}$ então G_2 está contido no centro de G, e assim sucessivamente. Como a série central é finita, resulta que o centro de um grupo nilpotente é não trivial.

Exemplo 3.5.1.2. Se G é um grupo abeliano, então $Z(G) = G$, assim a cadeia trivial

$$\{e\} = G_0 \subset G$$

satisfaz as condições de nilpotência, logo, todo grupo abeliano é nilpotente.

Exemplo 3.5.1.3. O grupo simétrico S_3 não é nilpotente, pois seu centro é trivial, uma vez que $Z(S_3) \neq S_3$ já que S_3 não é abeliano e também $|Z(S_3)| \notin \{2, 3\}$, pois do contrário $Z(S_3)$ teria índice primo, o que não ocorre (ver [4] Proposição V.4.8; pág. 140). Este é um exemplo de um grupo solúvel mas que não é nilpotente.

Assim a classe dos grupos nilpontes, de certa forma, "está entre"a classe dos grupos abelianos e a classe dos grupos solúveis.

Daremos duas caracterizações alternativas da nilpotência. Para isso, definimos uma nova série de subgrupos, indutivamente:

$$\gamma_1(G) = G,\ \gamma_2(G) = G'$$

e

$$\gamma_i(G) = (\gamma_{i-1}(G), G).$$

A outra série é também definida indutivamente, porém agora, apoiada no conceito de *centro* de um grupo.

Denotamos $\zeta_0(G) = \{e\}$, $\zeta_1(G) = Z(G)$ e definimos indutivamente $\zeta_i(G)$ como sendo o único subgrupo de G tal que $\dfrac{\zeta_i(G)}{\zeta_{i-1}(G)} = Z(G/\zeta_{i-1}(G))$.

O subgrupo $\zeta_i(G)$ chama-se o **i-ésimo centro** de G.

Observação 3.5.1.4. O i-ésimo centro de G está bem definido. Para verificar esta afirmação, considere o homomorfismo canônico $\pi : G \to \dfrac{G}{\zeta_{i-1}(G)}$ e tome $\zeta_i(G) := \pi^{-1}\left(Z\left(\dfrac{G}{\zeta_{i-1}(G)}\right)\right)$. É imediata a verificação que $\zeta_{i-1}(G)$ é um subgrupo de $\zeta_i(G)$. Para verificar que $\zeta_{i-1}(G) \lhd \zeta_1(G)$, note que se $x \in \zeta_i(G)$ e $\delta \in \zeta_{i-1}(G)$, então temos que

$$\pi(x\delta x^{-1}) = \pi(x)\pi(\delta)\pi(x)^{-1} = id,$$

pois $\pi(\delta) = id$. Portanto, $x\delta x^{-1} \in \zeta_{i-1}(G)$. Além disso,

$$\frac{\zeta_i(G)}{\zeta_{i-1}(G)} = \pi(\zeta_i(G)) = Z\left(\frac{G}{\zeta_{i-1}(G)}\right).$$

Para unicidade, note que se $N \lhd G$ é tal que $\dfrac{N}{\zeta_{i-1}(G)} = \left(Z\left(\dfrac{G}{\zeta_{i-1}(G)}\right)\right)$, então temos que

$$\begin{aligned} n \in N &\Leftrightarrow \pi(n) \in \frac{N}{\zeta_{i-1}(G)} = \left(Z\left(\frac{G}{\zeta_{i-1}(G)}\right)\right) \\ &\Leftrightarrow n \in \pi^{-1}\left(Z\left(\frac{G}{\zeta_{i-1}(G)}\right)\right). \end{aligned}$$

Portanto,

$$N = \pi^{-1}\left(Z\left(\frac{G}{\zeta_{i-1}(G)}\right)\right).$$

Definicão 3.5.1.5. *As sequências de subgrupos*

$$\{e\} = \zeta_0(G) \subset \zeta_1(G) \subset \cdots \subset \zeta_n(G) \cdots$$

e

$$G = \gamma_1(G) \supset \gamma_2(G) \supset \cdots \supset \gamma_n(G) \cdots$$

chamam-se a ***série central superior*** *e a* ***série central inferior*** *de G, respectivamente.*

Podemos destacar duas relações entre essas séries definidas:

Lema 3.5.1.6. *Seja $\{e\} = A_0 \subset A_1 \subset \cdots \subset A_n \cdots$ uma série central de G. Então, $A_i \subset \zeta_i(G)$ para todo i.*

Demonstração. Provaremos por indução em i.

Se $i = 1$ o resultado é verdadeiro, pois $A_1 \subset Z(G) = \zeta_1(G)$.

Assumimos então, por hipótese de indução, que $A_i \subset \zeta_i(G)$, $i \geq 1$. Dados $x \in A_{i+1}$ e $g \in G$, como $A_{i+1}/A_i \subset Z(G/A_i)$ temos que $\overline{x}$ comuta com $\overline{g}$, assim

$$\overline{xg} = \overline{gx},$$

logo,

$$x^{-1}g^{-1}xg \in A_i \subset \zeta_i(G),$$

por hipótese de indução. Temos então que $\overline{x} \in Z\left(\frac{G}{\zeta_i(G)}\right) = \frac{\zeta_{i+1}(G)}{\zeta_i(G)}$, o que mostra que $x \in \zeta_{i+1}(G)$, logo $A_{i+1} \subset \zeta_{i+1}$.

□

Lema 3.5.1.7. *Seja $\{e\} = A_0 \subset A_1 \subset \cdots \subset A_n = G$ uma série central de G. Então, $\gamma_i(G) \subset A_{n-i+1}$, para todo i.*

Demonstração. Também demonstraremos por indução em i. Se $i = 1$, então $A_{n-i+1} = A_n = G = \gamma_1(G)$. Suponha por indução que $\gamma_i(G) \subset A_{n-i+1}$, para $i \geq 1$. Como $A_{n-i+1}/A_{n-i} \subset Z(G/A_{n-i})$, dados arbitrariamente $x \in A_{n-i+1}$ e $g \in G$, temos que $\overline{x}$ comuta com $\overline{g}$, assim

$$\overline{xg} = \overline{gx},$$

com isso, $xgx^{-1}g^{-1} \in A_{n-i}$, o que mostra que

$$(A_{n-i+1}, G) \subset A_{n-i}.$$

Assim,

$$\gamma_{i+1}(G) = (\gamma_i(G), G) \subset (A_{n-i+1}, G) \subset A_{n-i}.$$

□

Destes resultados segue a seguinte caracterização dos grupos nilpotentes.

Teorema 3.5.1.8. *Seja G um grupo. São equivalentes:*

(i) G é nilpotente.

(ii) Existe um inteiro positivo m tal que $\zeta_m(G) = G$.

(iii) Existe um inteiro positivo n tal que $\gamma_n(G) = \{e\}$.

Demonstração. $(i) \Rightarrow (ii)$. Seja $\{e\} = A_0 \subset A_1 \subset \cdots \subset A_n = G$ uma série central de G. Pelo Lema 3.5.1.6, $G = A_n \subset \zeta_n(G)$, logo $\zeta_n(G) = G$.

$(i) \Rightarrow (iii)$. Pelo Lema 3.5.1.7, $\gamma_{n+1}(G) \subset A_{n-(n+1)+1} = A_0 = \{e\}$.

$(ii) \Rightarrow (i)$. A série

$$\{e\} = \zeta_0(G) \subset \zeta_1(G) \subset \cdots \subset \zeta_m(G) = G$$

satisfaz as hipóteses de nilpotência. Com efeito, para verificar que $\zeta_i(G) \triangleleft G$ sejam $x \in \zeta_i(G)$, $g \in G$ e $h \in G$, arbitrários. Uma vez que $\overline{x} \in \dfrac{\zeta_i(G)}{\zeta_{i-1}(G)} = Z(G/\zeta_{i-1}(G))$, segue que $\overline{xg} = \overline{gx}$ em $G/\zeta_{i-1}(G)$, para todo $g \in G$, o que implica que

$$\overline{gxg^{-1}}.\overline{h} = \overline{h}.\overline{gxg^{-1}}.$$

Portanto, $\overline{gxg^{-1}} \in Z(G/\zeta_{i-1}(G))$, logo $gxg^{-1} \in \zeta_i(G)$.

Note também que $\dfrac{\zeta_{i+1}(G)}{\zeta_i(G)} = Z(G/\zeta_i(G)),\ \forall\, i = 1, \cdots, m-1$. Portanto, G é nilpotente.

Finalmente, para $(iii) \Rightarrow (i)$ considere a sequência de subgrupos

$$G = \gamma_1(G) \supset \cdots \supset \gamma_{n+1}(G) = \{e\}$$

Para verificar que $\gamma_i(G)/\gamma_{i+1}(G) \subset Z(G/\gamma_{i+1}(G))$, note que dados $h \in \gamma_i(G)$ e $g \in G$, então

$$hgh^{-1}g^{-1} \in (\gamma_i(G), G) = \gamma_{i+1}(G).$$

Portanto,

$$\overline{hg} = \overline{gh}.$$

Além disso, $\gamma_2(G) = G' \triangleleft G$. Assim, para verificar que $\gamma_3(G) \triangleleft G$, sejam $xyx^{-1}y^{-1} \in (G', G)$ e $g \in G$. Segue que

$$g(xyx^{-1}y^{-1})g^{-1} = (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1})gg^{-1} \in (G', G),$$

pois $G' \triangleleft G$. Esse argumento mostra que $\gamma_3(G) \triangleleft G$. Indutivamente, temos que cada termos da série central inferior é normal em G. Portanto, G é nilpotente. □

Observação 3.5.1.9. Como a série central superior e a série central inferior são definidas com índices a partir do zero e do um, respectivamente, segue da demonstração do teorema acima que se G é nilpotente, então as sequências de subgrupos

$$\{e\} = \zeta_0(G) \subset \zeta_1(G) \subset \cdots \subset \zeta_n(G)$$

e

$$G = \gamma_1(G) \supset \gamma_2(G) \supset \cdots \supset \gamma_{n+1}(G),$$

têm o mesmo comprimento.

Esse número chama-se a **classe de nilpotência** de G.

Proposição 3.5.1.10. *Todo p-subgrupo de um grupo finito G é nilpotente.*

Demonstração. É conhecido da teoria dos grupos que o centro de um p-grupo é não trivial. Como todos os quocientes de G são também p-grupos, segue que $\zeta_{i-1}(G) \subsetneq \zeta_i(G)$ para todo inteiro positivo i. Como G é finito, existe um inteiro n tal que $\zeta_n(G) = G$, portanto G é nilpotente.

□

Proposição 3.5.1.11. (Ver [35] pag 101) *Produtos diretos finitos de grupos nilpotentes são também nilpotentes.*

Proposição 3.5.1.12. *Seja $H \neq \{e\}$ um subgrupo normal de um grupo nilpotente G. Então $H \cap Z(G) \neq \{e\}$.*

Demonstração. Como $G = \zeta_n(G)$ para algum n, existe um índice i que é o menor inteiro tal que $H \cap \zeta_i(G) \neq \{e\}$.

Afirmamos que

$$(H \cap \zeta_i(G), G) \subset H \cap \zeta_{i-1}(G) = \{e\}.$$

Com efeito, se $h \in H \cap \zeta_i(G)$ e $g \in G$, então $hgh^{-1}g^{-1} \in H$, pois $H \triangleleft G$, e como

$$\frac{\zeta_i(G)}{\zeta_{i-1}(G)} = Z\left(\frac{G}{\zeta_{i-1}(G)}\right),$$

temos que $\overline{hg} = \overline{gh}$, o que mostra que

$$hgh^{-1}g^{-1} \in \zeta_{i-1}(G).$$

Como $H \cap \zeta_{i-1}(G) = \{e\}$, segue que $hgh^{-1}g^{-1} = e$, ou seja, $hg = gh$, para todo $g \in G$. Portanto, $H \cap Z(G) \supset H \cap \zeta_i(G) \neq \{e\}$.

□

Definicão 3.5.1.13. *Diz-se que um grupo G tem a **propriedade do normalizador** se todo subgrupo próprio de G está estritamente contido no seu normalizador.*

Proposição 3.5.1.14. *Todo grupo nilpotente tem a propriedade do normalizador.*

Demonstração. Seja H um subgrupo próprio de um grupo nilpotente. Como

$$\{e\} = \zeta_0(G) \subset H \subset \zeta_n(G) = G,$$

existe um inteiro i tal que $\zeta_i(G) \subset H$ e $\zeta_{i+1}(G) \not\subset H$. Escolhemos um elemento $x \in \zeta_{i+1}(G) \setminus H$ e um elemento arbitrário $h \in H$. Afirmamos que $x \in N_G(H)$. De fato, da definição de $\zeta_{i+1}(G)$ temos que $\zeta_{i+1}(G)$ é o único subgrupo de G tal que $\zeta_{i+1}(G)/\zeta_i(G) = Z(G/\zeta_i(G))$. Assim, $\overline{x}$ comuta com $\overline{g}$, para todo $g \in G$, o que fornece $x^{-1}g^{-1}xg \in \zeta_i(G)$, logo $(\zeta_{i+1}(G), G) \subset \zeta_i(G)$.

Tome $y := xhx^{-1}h^{-1}$. Então, $y \in (\zeta_{i+1}(G), G) \subseteq \zeta_i(G) \subseteq H$, consequentemente,

$$xhx^{-1} = yh.$$

Logo, $xHx^{-1} = H$, o que mostra $x \in N_G(H)$. Portanto, $H \subsetneq N_G(H)$.

□

Definicão 3.5.1.15. *Sejam G um grupo finito, p um número primo e p^m a maior potência de p que divide $|G|$. Os subgrupos de G que têm ordem p^m, cuja existência é garantida pelo Teorema de Sylow, são chamados de p-subgrupos de Sylow de G.*

Para demonstrar o teorema seguinte, faremos uso do seguinte resultado acerca do normalizador de um p-subgrupo de Sylow:

Lema 3.5.1.16. (Ver [3] Corolário 2.11) *Seja P um p-subgrupo de Sylow de um grupo G. Então, $N_G(N_G(P)) = N_G(P)$.*

Teorema 3.5.1.17. *Seja G um grupo finito. Então, as seguintes condições são equivalentes.*

(i) G é nilpotente;

(ii) G tem a propriedade do normalizador;

(iii) Todo p-subgrupo de Sylow de G é normal em G;

(iv) G é o produto direto dos seus subgrupos de Sylow;

Demonstração. O fato que $(i) \Rightarrow (ii)$ foi provado na proposição 3.5.1.14.

$(ii) \Rightarrow (iii)$. Seja P um p-subgrupo de Sylow de G. Suponha por contradição que $N_G(P) \neq G$ (ou seja, P não é normal em G). Assim, $N_G(P)$ é um subgrupo próprio de G e segue por (ii) que $N_G(P) \subsetneq N_G(N_G(P))$. O que contradiz o Lema 3.5.1.17. Com isso,

$$N_G(P) = G.$$

$(iii) \Rightarrow (iv)$. Como G é finito, então

$$|G| = p_1^{n_1} \cdots p_k^{n_k},$$

com p_i primo e $n_i \geq 0$, $1 \leq i \leq k$.

Sejam $H_1, \ldots, H_k$ os respectivos p_i-subgrupos de Sylow, os quais são normais em G por (iii).

Como $|H_i| = p_i^{n_i}$, segue que

$$H_i \cap H_j = \{e\},$$

para $i \neq j$, pois $p_i \neq p_j$.

Como cada subgrupo de Sylow de G é normal em G, temos que $\overline{H} := H_1 \cdots H_{i-1} H_{i+1} \cdots H_k \lhd G$. Segue do Teorema de Lagrange que cada elemento em $\overline{H}$ tem ordem um divisor de $p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k}$, o que implica que

$$H_i \cap \overline{H} = \{e\}.$$

Assim

$$H_1 \cdots H_k = H_1 \times \cdots \times H_k.$$

Como

$$|G| = p_1^{n_1} \cdots p_k^{n_k} = |H_1 \times \cdots \times H_k| = |H_1 \cdots H_k|.$$

Segue que G é produto direto de seus subgrupos de Sylow.

$(iv) \Rightarrow (i)$. Segue do fato que todo p-grupo é nilpotente (proposição 3.5.1.10) e que produto direto de nilpotente é também nilpotente (proposiçao 3.5.1.11). □

3.5.2 O Caso p-grupo

A conjectura ISO tem resposta positiva no caso em que G é um p-grupo finito. Esse será o principal argumento para demonstrá-la no caso em que G é um grupo nilpotente finito, uma vez que grupos nilpotentes finitos podem ser escritos como produto direto de seus p-subgrupos de Sylow (Teorema 3.5.1.17).

Os autores Klaus Roggenkamp e Leonard Scott em [2] demonstraram a referida conjectura em ambos os casos. A abordagem adotada por esses autores para o caso p-grupo é muito técnica, longa e faz uso de conceitos que fogem o escopo desta dissertação. Iremos enunciar e discutir os resultados de [2].

O teorema central do artigo [2] tem o seguinte enunciado:

Teorema 3.5.2.1. *Seja G um p-grupo finito para algum primo p e S um domínio local ou semilocal de Dedekind de característica zero com um único ideal maximal contendo p. Se H é um subgrupo das unidades normalizadas de SG com $|H| = |G|$, então H é conjugado a G por um automorfismo interno de SG.*

No apêndice de [2], é demonstrado que qualquer domínio integral Noetheriano de característica zero em que p não é invertível está contido em um domínio local satistazendo as hipóteses do Teorema 3.5.2.1. Consequentemente, o Teorema 3.5.2.1 implica em uma resposta positiva para o problema do isomorfismo para p-grupos sobre o domínio original, em particular para $\mathbb{Z}$.

Assim a demonstração da conjectura ISO no caso p-grupo se reduz à demonstração do Teorema 3.5.2.1. Deste teorema são obtidos alguns corolários; destacamos aqui o Corolário 1 ([2], pág. 617) que, na verdade, como demonstrados pelos autores, é um resultado equivalente ao Teorema 3.5.2.1. Com essa equivalência, a demonstração do Teorema 3.5.2.1 se reduz à demonstração do Corolário 3.5.2.2, a qual é baseada em uma série de reduções.

Corolário 3.5.2.2. *Seja G um p-grupo finito para algum primo p e S um domínio local ou semilocal de Dedeking de característica zero com um único ideal maximal contendo p. Se α é um automorfismo normalizado de SG, então α é uma composição de um automorfismo de SG induzido por automorfismo de G seguido de um automorfismo interno de SG.*

3.5.3 A Conjectura ISO Para Grupos Nilpotentes Finitos

Uma vez postos os resultados principais sobre grupos nilpotentes e a discussão sobre o caso p-grupo, podemos enunciar e demonstrar a conjectura (ISO) no caso em que o grupo G é nilpotente finito.

Teorema 3.5.3.1. *Seja G um grupo nilpotente finito. Se H é outro grupo tal que $\mathbb{Z}G \simeq \mathbb{Z}H$, então $G \simeq H$.*

Demonstração. Antes de considerarmos o isomorfismo entre $\mathbb{Z}G$ e $\mathbb{Z}H$, faremos algumas considerações que resultam do fato do grupo G ser nilpotente.

Como G é nilpotente, segue do Teorema 3.5.1.17 que G é um produto direto de seus p-subgrupos de Sylow e que cada um desses p-subgrupos de Sylow é normal em G e segue do Teorema de Sylow que para cada primo p existe um único p-subgrupo de Sylow de G, pois se X e K são dois p-subgrupos de Sylow de G então X e K são conjugados, assim

$$X = gKg^{-1}$$

para algum $g \in G$, mas como K é normal em G temos que

$$gKg^{-1} = K,$$

consequentemente,

$$X = K.$$

Agora, para um primo p arbitrário divisor da ordem de G, escreva

$$G = G_p \times G_{p'},$$

onde G_p é o único p-subgrupo de Sylow de G e $G_{p'}$ é o produto direto dos demais subgrupos de Sylow de G.

Seja $\theta : \mathbb{Z}G \to \mathbb{Z}H$ um isomorfismo normalizado. Sabemos do Teorema 3.2.4 que $|H| = |G|$. Assim, como G_p é normal em G, a correspondência entre subgrupos normais, vista no Teorema 3.3.3, fornece a existência de um subgrupo normal M de H tal que

$$\theta(\widehat{G_p}) = \widehat{M},$$

e

$$|G_p| = |M|,$$

em que $\widehat{G_p}$ é a soma formal dos elementos de G_p. Isso mostra que M é um p-subgrupo de Sylow (normal) de H, uma vez que G_p é um subgrupo de Sylow de G, $|G_p| = |M|$ e $|G| = |H|$. Mas essa correspondência é biunívoca, ou seja, cada subgrupo de Sylow de H é normal em H. Portanto, pelo Teorema 3.5.1.17, H é um grupo nilpotente. Denotaremos o subgrupo M por H_p. Assim, o grupo H admite uma fatoração $H = H_p \times H_{p'}$ análoga à fatoração do grupo G.

Como $G_{p'}$ é um produto direto de subgrupos normais de G, segue que $G_{p'} \triangleleft G$. Note que

$$G_p \simeq \frac{G}{G_{p'}} \tag{3.16}$$

Como θ é normalizado, temos também, pela Proposição 3.3.7, que

$$\theta(\Delta(G, G_{p'})) = \Delta(H, H_{p'}) \tag{3.17}$$

Com isso, podemos considerar a aplicação:

$$\theta^* : \mathbb{Z}G \to \frac{\mathbb{Z}H}{\Delta(H, H_{p'})},$$

definida por

$$\left(\sum_{g\in G} a(g)g\right) \mapsto \theta\left(\sum_{g\in G} a(g)g\right) + \Delta(H, H_{p'}).$$

em outras palavras, se $\alpha \in \mathbb{Z}G$ então,

$$\theta^*(\alpha) = \overline{\theta(\alpha)}.$$

Com essa definição, θ^* é um homomorfismo sobrejetor de anéis e seu kernel é o conjunto $\mathrm{Ker}(\theta^*) = \{\alpha \in \mathbb{Z}G;\ \theta(\alpha) \in \Delta(H, H_{p'})\}$. Assim, a igualdade 3.17 mais o fato de θ ser um isomorfismo, implicam que $\mathrm{Ker}(\theta^*) = \Delta(G, G_{p'})$. Segue do Teorema do Isomorfismo que

$$\mathbb{Z}G/\Delta(G, G_{p'}) \simeq \mathbb{Z}H/\Delta(H, H_{p'}). \tag{3.18}$$

Pelo Corolário 2.2.6 segue que

$$\mathbb{Z}(G/G_{p'}) \simeq \mathbb{Z}G/\Delta(G, G_{p'}) \text{ e } \mathbb{Z}H/\Delta(H, H_{p'}) \simeq \mathbb{Z}(H/H_{p'}) \tag{3.19}$$

Além disso,

$$\mathbb{Z}G_p \simeq \mathbb{Z}(G/G_{p'}) \text{ e } \mathbb{Z}(H/H_{p'}) \simeq \mathbb{Z}H_p \tag{3.20}$$

como visto na Proposição 2.1.7, uma vez que vale o isomorfismo 3.16 e um isomorfismo análogo para H_p.

Portanto, segue de 3.18, 3.19 e 3.20 que

$$\mathbb{Z}G_p \simeq \mathbb{Z}(G/G_{p'}) \simeq \mathbb{Z}G/\Delta(G, G_{p'}) \simeq \mathbb{Z}H/\Delta(H, H_{p'}) \simeq \mathbb{Z}(H/H_{p'}) \simeq \mathbb{Z}H_p. \tag{3.21}$$

Assim, por 3.21 temos que

$$\mathbb{Z}G_p \simeq \mathbb{Z}H_p,$$

para cada primo p divisor da ordem de G.

Como ISO tem resposta positiva para p-grupos, temos que $G_p \simeq H_p$, para cada primo p divisor da ordem de G. Consequentemente,

$$G = \prod_p G_p \simeq \prod_p H_p = H.$$

□

Capítulo 4

Outras Conjecturas e os Contraexemplos

Neste capítulo apresentaremos na primeira seção as conjecturas formuladas no início da década de setenta por Hans Julius Zassenhaus sobre as unidades de $\mathbb{Z}G$, listaremos os resultados conhecidos e as relações dessas conjecturas com o problema do isomorfismo. Na segunda seção apresentaremos a conjectura do normalizador, demonstraremos o Teorema de Coleman, do qual resulta a validade da conjectura do normalizador para grupos nilpotentes finitos. Demonstraremos o Teorema de Krempa, como consequência obteremos a validade da conjectura do normalizador para grupos de ordem ímpar. O Teorema de Krempa também será útil na demonstração do Teorema 4.2.14, que fornece uma condição sobre os 2-subgrupos de Sylow de um grupo finito G para que o problema do normalizador tenha resposta positiva para G. Enunciaremos dois resultados que mostram como o problema do normalizador se relaciona com o problema do isomorfismo para grupos infinitos. Finalizaremos o capítulo, e a presente dissertação, apresentando os contraexemplos conhecidos sobre tais conjecturas.

4.1 As Conjecturas de Zassenhaus

(Aut) *Seja $\theta : \mathbb{Z}G \to \mathbb{Z}G$ um automorfismo normalizado. Então, existem uma unidade $\alpha \in \mathbb{Q}G$ e um automorfismo $\sigma \in Aut(G)$ tais que $\theta(g) = \alpha^{-1}\sigma(g)\alpha$ para todo $g \in G$.*

(ZC1) *Seja $u \in U(\mathbb{Z}G)$ um elemento de ordem finita. Então, existe uma unidade $\alpha \in \mathbb{Q}G$ tal que $\alpha^{-1}u\alpha \in G$.*

(ZC2) *Seja H um subgrupo finito de $U_1(\mathbb{Z}G)$ tal que $|H| = |G|$. Então, existe uma unidade $\alpha \in \mathbb{Q}G$ tal que $\alpha^{-1}H\alpha = G$.*

(ZC3) *Seja H um subgrupo finito de $U_1(\mathbb{Z}G)$. Então, existe uma unidade $\alpha \in \mathbb{Q}G$ tal que $\alpha^{-1}H\alpha \subset G$.*

Note que $(ZC2)$ é um caso particular de $(ZC3)$, pois $|\alpha^{-1}H\alpha| = |H| = |G|$, assim, por $ZC3$,

$$\alpha^{-1}H\alpha = G.$$

Além disso, $(ZC1)$ é um caso particular de $(ZC3)$ no caso dos grupos cíclicos. Assim como a conjectura (ISO), essas conjecturas não são verdadeiras no caso geral, logo o problema passa a ser de classificação. Os contraexemplos para essas conjecturas serão apresentadas na seção 4.3.

Listaremos a seguir algumas classes de grupos e exemplos para os quais valem essas conjecturas:

(ZC1) foi estabelecido para as seguintes classes:

- S_3 (I. Hughes e K.R. Pearson [12]).

- D_4 (C. Polcino Milies [13]).

- Grupos metacíclicos da forma $G = \langle x\rangle \ltimes \langle y\rangle$, onde $o(x) = p$ e $o(y) = q$, com p e q primos diferentes (A.K, Bhandari e I.S. Luthar [14]).

- Grupos metacíclicos da forma $G = \langle x\rangle \ltimes \langle y\rangle$, onde $mdc(o(x), o(y)) = 1$ (C. Polcino Milies, J. Ritter e S.K. Sehgal [15]).

- S_4 (N.A. Fernandes [16]).

- A_5 (I.S. Luthar e I.B.S. Passi [17]).

- S_5 (I.S. Luthar e P. Trama [18]).

(ZC3) foi estabelecido para as seguintes classes:

- Grupos nilpotentes (A. Weiss [19]).

- Grupos metacíclicos da forma $G = \langle x\rangle \ltimes \langle y\rangle$, onde $mdc(o(x), o(y)) = 1$ (A. Valenti [20]).

- S_4 e o grupo conhecido como *binary octahedral* (M. Dokuchaev e S.O. Juriaans [21]).

- S_5, A_5 e $SL(2, 5)$ (M. Dokuchaev, S.O. Juriaans e C. Polcino Milies [22].

Para relacionar as conjecturas de Zassenhaus com o problema do isomorfismo, enunciaremos o seguinte lema provado por G. Higman (ver Corolário 1.1.3 em [2] pág. 602).

Lema 4.1.1. *Se H é subgrupo finito de $U_1(\mathbb{Z}G)$ então os elementos de H são linearmente independentes sobre $\mathbb{Z}$. Além disso, $|H|$ é um divisor da $|G|$, valendo a igualdade $|H| = |G|$ se, e somente se, $\mathbb{Z}G = \mathbb{Z}H$.*

Proposição 4.1.2. $(ZC2) \Rightarrow (ISO)$.

Demonstração. Seja H um grupo finito tal que $\mathbb{Z}H \simeq \mathbb{Z}G$ e seja $\theta : \mathbb{Z}H \to \mathbb{Z}G$ um isomorfismo normalizado. Temos que $\theta(H)$ é um subgrupo finito de $U_1(\mathbb{Z}G)$ com a mesma ordem G, logo, pelo Lema 4.1.1 temos $\mathbb{Z}G = \mathbb{Z}\theta(H)$. Por $(ZC2)$, $\theta(H) = \alpha^{-1}G\alpha$, para alguma unidade $\alpha \in \mathbb{Q}G$. Consequentemente,

$$H \simeq \theta(H) = \alpha^{-1}G\alpha \simeq G.$$

□

Proposição 4.1.3. $(ZC2) \Rightarrow (Aut)$

Demonstração. Suponha $(ZC2)$ e seja $\theta \in Aut(\mathbb{Z}G)$. Temos pelo Lema 4.1.1 que

$$\mathbb{Z}G = \mathbb{Z}\theta(G).$$

Assim, $(ZC2)$ assegura que

$$\theta(G) = \alpha^{-1}G\alpha,$$

para alguma unidade $\alpha \in \mathbb{Q}G$. Com isso, para cada $g \in G$, existe $g_1 \in G$, tal que

$$\theta(g) = \alpha^{-1}g_1\alpha.$$

Como a aplicação

$$g \mapsto g_1$$

determina um automorfismo de G, segue a conjectura (Aut).

□

Proposição 4.1.4. $(ISO) + (Aut) \Rightarrow (ZC2)$

Demonstração. Seja $H \in U_1(\mathbb{Z}G)$ tal que $|H| = |G|$. Pelo Lema 4.1.1 temos que $\mathbb{Z}G = \mathbb{Z}H$. A conjectura (ISO) garante a existência de um isomorfismo θ entre G e H, enquanto que a conjectura (Aut) garante a existência de uma unidade $\alpha \in \mathbb{Q}G$ e um automorfismo $\sigma \in Aut(G)$ tais que

$$\theta(g) = \alpha^{-1}\sigma(g)\alpha, \ \ \forall\, g \in G.$$

Com isso, temos que

$$H = \alpha^{-1}G\alpha,$$

como desejado.

□

Finalizamos essa seção com a seguinte observação acerca de grupos nilpotentes finitos:

Observação 4.1.5. Como $(ZC3) \Longrightarrow (ZC2) \Longrightarrow (ISO)$ e uma vez que $(ZC3)$ tem resposta positiva para grupos nilpotentes, essa seria uma outra forma de demonstrar que grupos nilpotentes são determinados por seu anel de grupo integral.

4.2 O Problema do Normalizador

Outro problema de grande relevância sobre as unidades do anel de grupo integral $\mathbb{Z}G$ é o chamado **Problema do Normalizador**, que questiona como se localiza o grupo G dentro de $U(\mathbb{Z}G)$, mais precisamente, o problema do normalizador questiona quem é o normalizador de G em $U(\mathbb{Z}G)$. O centro do grupo das unidades de $\mathbb{Z}G$, denotado por $Z(U(\mathbb{Z}G))$, normaliza G em $U(\mathbb{Z}G)$, pois se $u \in Z(U(\mathbb{Z}G))$ e $g \in G$, então,

$$ugu^{-1} = g$$

pois u comuta com g. Naturalmente, o próprio grupo G também normaliza G em $U(\mathbb{Z}G)$. Esses são chamados os normalizadores triviais de G em $U(\mathbb{Z}G)$.

A **Conjectura do Normalizador** afirma que eles determinam todo o normalizador, em outras palavras,

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

Assim como a conjectura (ISO) e as conjecturas de Zassenhaus, a conjectura do normalizador foi demonstrada em alguns casos particulares. Entretanto, um contraexemplo foi dado por M. Hertweck em [6] e será citado na seção seguinte, Teorema 4.3.1.2.

Por simplicidade escreveremos $N_U(G)$ ao invés de $N_{U(\mathbb{Z}G)}(G)$.

Qualquer unidade $u \in N_U(G)$ determina um automorfismo $\rho = \rho(u) : G \to G$, tal que

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

Assim, a associação $u \mapsto \rho(u)$ determina uma aplicação

$$\psi : N_U(G) \to Aut(G). \tag{4.1}$$

Denotaremos por $Aut_U(G)$ a imagem de ψ.

Daremos uma forma equivalente do problema do normalizador em termos de $Aut_U(G)$.

Proposição 4.2.1. *$N_U(G) = G.Z(U(\mathbb{Z}G))$ se, e somente se, $Aut_U(G) = Inn(G)$, onde $Inn(G)$ denota o grupo dos automorfismos internos de G.*

Demonstração. Suponha que $N_U(G) = G.Z(U(\mathbb{Z}G))$. Seja $u \in N_U(G)$, então u se escreve como $u = gw$, com $g \in G$ e $w \in Z(U(\mathbb{Z}G))$. Assim, para $x \in G$, temos que

$$\rho(u)(x) = \rho(gw)(x) = (gw)x(gw^{-1}) = gwxw^{-1}g^{-1},$$

como w comuta com x segue que

$$gwxw^{-1}g^{-1} = gxg^{-1}.$$

O que mostra que $\rho(u)$ é um automorfismo interno de G. Logo $Aut_U(G) \subset Inn(G)$, e como $Inn(G) = \psi(G) \subset Aut_U(G)$, temos a igualdade.

Reciprocamente, admitindo que $Aut_U(G) = Inn(G)$, seja $u \in N_U(G)$ arbitrário. Assim, para $g \in G$, arbitrário, temos que

$$ugu^{-1} = y^{-1}gy,$$

para algum $y \in G$, logo

$$(yu)g(yu)^{-1} = g,$$

o que mostra que yu e g comutam. Como g é arbitrário, yu comuta com todos os elementos do grupo G, logo yu comuta com todos os elementos de $\mathbb{Z}G$, portanto $yu \in Z(\mathbb{Z}G)$, em particular, $yu \in Z(U(\mathbb{Z}G))$, consequentemente,

$$u = y^{-1}(yu) \in G.Z(U(\mathbb{Z}G)).$$

□

Usaremos essa equivalência para demonstrar que o problema do normalizador tem resposta positiva em alguns casos particulares. Precisamos também dos seguintes lemas:

Lema 4.2.2. *(**Coleman**) Seja P um p-grupo contido em um grupo arbitrário G. Suponha que $u \in N_U(G)$. Então, existe $y \in G$ tal que $u^{-1}gu = y^{-1}gy$, para todo $g \in P$.*

Demonstração. Para $g \in G$ defina $\phi(g) = u^{-1}gu$. Como u normaliza G, temos que $\phi(g) \in G$, $\forall\, g \in G$. Como elemento de $\mathbb{Z}G$, escrevemos

$$u = \sum_{x \in G} u(x)x.$$

Como $u = g^{-1}u\phi(g)$, temos que

$$u = g^{-1}\left(\sum_{x \in G} u(x)x\right)\phi(g) = \sum_{x \in G} u(x)g^{-1}x\phi(g). \tag{4.2}$$

Portanto, o grupo G age no conjunto G por

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

O elemento u pode ser visto como uma função $u : G \to \mathbb{Z}$ dada por

$$x \mapsto u(x).$$

Segue da igualdade 4.2 que a função u é constante nas órbitas dessa ação. A órbita do elemento $x \in G$ é o conjunto

$$\mathcal{O}(x) := \{\sigma_g(x) \mid g \in G\}.$$

Restrigindo a ação acima a P, temos que as órbitas dessa ação são conjuntos com cardinalidade potência de p. Como $u \in U(\mathbb{Z}G)$, a aplicação de aumento ϵ fornece que

$$1 = \epsilon(1) = \epsilon(uu^{-1}) = \epsilon(u)\epsilon(u)^{-1},$$

assim $\epsilon(u)$ é invertível em $\mathbb{Z}$. Com isso,

$$\pm 1 = \epsilon(u) = \sum_{x \in G} u(x) = \sum u(\xi) p_g^k, \tag{4.3}$$

onde p_g^k indica que o comprimento da órbita de g é p^k e ξ é um representante de classe de g.

Assim, a igualdade 4.3 é uma combinação linear de potências de p, com coeficientes em $\mathbb{Z}$, dando $\pm$ 1, mas isso implica que uma das potências de p é igual a 1, pois do contrário, poderíamos por p em evidência e ficaríamos com uma expressão da forma

$$pm = \pm 1,$$

com $p,\ m \in \mathbb{Z},\ m := (1/p) \sum u(\xi) p_g^k$ e $p \neq \pm 1$, o que é um absurdo.

Logo, existe uma órbita de comprimento 1, o que quer dizer que existe um $y \in G$ tal que $\sigma_g(y) = y$, e, portanto, $\phi(g) = y^{-1}gy$, para todo $g \in P$.

□

Lema 4.2.3. *Seja G um grupo nilpotente finito. Então, os subgrupos de Sylow de G comutam.*

Demonstração. Com efeito, do Teorema 3.5.1.17 os subgrupos de Sylow de G são normais e para cada primo p divisor da ordem de G existe um único p-subgrupo de Sylow. Assim, se x_i e x_j pertencem à P_i e P_j, respectivamente, $i \neq j$, então

$$x_i x_j x_i^{-1} x_j^{-1} \in P_i,$$

pois como $P_i \triangleleft G$ temos que $x_j x_i^{-1} x_j^{-1} \in P_i$. Por outro lado,

$$x_i x_j x_i^{-1} x_j^{-1} \in P_j,$$

pois como $P_j \triangleleft G$ temos que

$$x_i x_j x_i^{-1} \in P_j.$$

Com isso,

$$x_i x_j x_i^{-1} x_j^{-1} \in P_i \cap P_j = \{e\}.$$

Portanto,

$$x_i x_j = x_j x_i.$$

□

Teorema 4.2.4. *Seja G um grupo nilpotente finito. Então, $N_{U(\mathbb{Z}G)}(G) = G.Z(U(\mathbb{Z}G))$.*

Demonstração. Escreva G como produto dos seus p_i-subgrupos de Sylow, assim $G = \prod P_i$.

Sejam $u \in N_{U(\mathbb{Z}G)}(G)$ e $g = g_1 \dots g_t \in G$ com $g_i \in P_i,\ i = 1, \dots, t$. Assim,

$$\begin{aligned} u^{-1}gu &= u^{-1}(g_1 \dots g_t)u \\ &= u^{-1}g_1uu^{-1}g_2u \dots u^{-1}g_{t-1}uu^{-1}g_tu \\ &= (u^{-1}g_1u)(u^{-1}g_2u) \dots (u^{-1}g_{t-1}u)(u^{-1}g_tu), \end{aligned}$$

Aplicando o lema 4.2.2 em cada um dos parênteses, temos que existem $x_1, \ldots, x_t$, com $x_i \in G,\ i = 1, \ldots, t.$ tais que

$$u^{-1}gu = (x_1^{-1}g_1x_1)\ldots(x_t^{-1}g_tx_t), \tag{4.4}$$

Note que pelo fato dos subgrupos de Sylow de G comutarem, podemos supor, sem perda de generalidade, que $x_i \in P_i$, pois do contrário, ao escrever

$$x_i = a_1 \ldots a_t$$

como produto de elementos dos subgrupos de Sylow de G, as parcelas que não estão em P_i se cancelam em

$$x_i^{-1}g_ix_i.$$

Portanto, comutando de forma conveniente os elementos no lado direito da igualdade 4.4, podemos escrever

$$u^{-1}gu = (x_1 \cdots x_t)^{-1}g(x_1 \ldots x_t).$$

Concluimos que

$$u^{-1}gu = x^{-1}gx,$$

para todo $g \in G$ com $x = \prod x_i$, e $i = 1, \ldots, t$. O resultado segue da proposição 4.2.1.

□

A proposição a seguir diz que anéis de grupo sobre anéis comutativos são anéis com involução. Essa propriedade será utilizada nos próximos resultados desta seção.

Proposição 4.2.5. *Seja R um anel comutativo com unidade e G um grupo. A aplicação $^* : RG \to RG$ dada por:*

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

satisfaz as seguintes propriedades (e portanto, definite uma involução):

(i) $(a+b)^* = a^* + b^*$.

(ii) $(ab)^* = b^*a^*$.

(iii) $a^{**} = a$.

Observação 4.2.6. Note que se $\alpha \in \mathbb{Z}G$ e $\alpha\alpha^* = 1$, então $\alpha = \pm g$ para algum $g \in G$. Com efeito, se $\alpha \in \mathbb{Z}G$, então podemos escrever

$$\alpha = (a_1g_1 + \cdots + a_ng_n),$$

com $a_i \in \mathbb{Z}, 1 \leq i \leq n$. Assim,

$$\begin{aligned} \alpha\alpha^* &= (a_1g_1 + \cdots + a_ng_n)(a_1g_1^{-1} + \cdots + a_ng_n^{-1}) \\ &= (a_1^2 + \cdots + a_n^2) + \sum_{i\neq j} a_ia_jg_ig_j^{-1}. \end{aligned}$$

Portanto, se $\alpha\alpha^* = 1$, devemos ter que $a_i = \pm 1$, para algum $1 \leq i \leq n$ e $a_j = 0, j \neq i$. Com isso, temos que $\alpha = \pm g$, para algum $g \in G$.

Proposição 4.2.7. *Seja $u \in U(\mathbb{Z}G)$. Então, $u \in N_U(G)$ se, e somente se, $u^*u \in Z(\mathbb{Z}G)$.*

Demonstração. Seja $u \in N_U(G)$ e seja ρ a imagem de u pela aplicação dada em 4.1. Para qualquer $x \in G$, temos que

$$uxu^{-1} = \rho(u)(x).$$

Aplicando a involução * em ambos os lados e substituindo x por x^{-1} temos que

$$(u^*)^{-1}xu^* = \rho(x),$$

portanto

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

Assim, u^*u comuta com todos elementos de G, o que mostra que $u^*u \in Z(\mathbb{Z}G)$.

Reciprocamente, suponha que $u^*u \in Z(\mathbb{Z}G)$. Note que,

$$(uxu^{-1}).(uxu^{-1})^* = ux(u^*u)^{-1}x^{-1}u^* = uu^*(u^*u)^{-1} = u(u^*u)^{-1}u^* = 1.$$

Portanto, segue da Observação 4.2.6 que $uxu^{-1} = \pm g$, para algum $g \in G$, mas

$$\epsilon(uxu^{-1}) = \epsilon(x) = 1,$$

o que mostra que $uxu^{-1} \in G$, logo $u \in N_U(G)$.

□

Teorema 4.2.8. *(Krempa) Seja G um grupo finito. Então,*

$$Aut_U(G)/Inn(G)$$

é um 2-grupo abeliano elementar.

Demonstração. Sejam $u \in N_U(G)$ e $\phi = \rho(u)$ o automorfismo de G dado pela aplicação dada em 4.1, ou seja, $\phi(x) = uxu^{-1}$. Seja $v = u^*u^{-1}$, assim

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

Pela Observação 4.2.6, segue que $v = \pm g$ para algum $g \in G$. Como u é uma unidade, $\epsilon(u^{-1}) = \pm 1$ e como $\epsilon(u^*) = \epsilon(u^{-1})$, temos também que

$$\epsilon(v) = \epsilon(u^*)\epsilon(u^{-1}) = 1.$$

Assim, $v = g$ para algum $g \in G$. Consequentemente,

$$u^* = gu,$$

além disso

$$gu^2 = u^*u = c \in Z(\mathbb{Z}G),$$

pela Proposição 4.2.7.

Assim,

$$\phi^2(x) = (\phi \circ \phi)(x) = u^2 x u^{-2} = g^{-1} c x c^{-1} g = g^{-1} x g,$$

para todo $x \in G$, isto é, $\phi^2 \in Inn(G)$. Um grupo em que todo elemento diferente da identidade tem ordem 2 é abeliano e, consequentemente, abeliano elementar. □

Definição 4.2.9. *$Aut_c(G)$ denotará o grupo dos automorfismos de G que preservam classes de conjugação.*

Lema 4.2.10. (Ver [23], proposição 2.3 pág. 243.) *Seja G um grupo finito, então $Aut_U(G) \subset Aut_c(G)$.*

Lema 4.2.11. *A ordem de $Aut_c(G)$ (e portanto de $Aut_U(G)$) é divisível somente pelos primos que dividem a ordem de G.*

Demonstração. Seja $\varphi \in Aut_c(G)$ tal que $\varphi^q = id$ para algum primo q tal que $q \nmid |G|$. Provaremos que $\varphi = id$.

Considere o subgrupo H de G dos pontos fixados por φ, ou seja,

$$H = \{g \in G; \varphi(g) = g\}.$$

Afirmamos que para cada classe de conjugação C de G, temos que $H \cap C \neq \emptyset$. Com efeito, suponha por contradição que exista uma classe C de G tal que $\varphi(g) \neq g$, $\forall\, g \in C$.

Para $g \in C$, considere $A_g := \{g, \varphi(g), \ldots, \varphi^{q-1}(g)\}$. Note que:

(1) $\#A_g = q$, pois como $|\varphi| = q$, os elementos em A_q são distintos.

(2) $A_g \cap A_h = \emptyset$, para $g \neq h$ em C.

Com isso, temos que $C = \dot{\bigcup}_{g \in C} A_g$. Isso implica que $q \,|\, |C|$, consequentemente, $q \,|\, |G|$, o que é uma contradição. Portanto, $H \cap C \neq \emptyset$ para cada classe C. Assim, os conjugados de H percorrem todo o grupo G. Com isso, podemos escrever

$$G = \bigcup_{y \in G} yHy^{-1}.$$

É conhecido da teoria de grupos que o número de conjugados de H é dado por $[G : N_G(H)]$. Como $H \subseteq N_G(H)$, segue que $[G : N_G(H)] \leq [G : H]$. Assim,

$$|G| = 1 + (|H| - 1)[G : N_G(H)] \leq 1 + (|H| - 1)[G : H],$$

ou seja,

$$|G| \leq 1 + |G| - [G : H],$$

o que implica $[G : H] \leq 1$, logo $[G : H] = 1$, o que fornece $H = G$. Portanto, $\varphi = id$.

□

A demonstração do teorema seguinte segue as ideias da demonstração encontrada em [24]. Para uma outra demonstração o leitor pode consultar [23], Teorema 3.4.

Teorema 4.2.12. *O problema do normalizador tem resposta positiva para qualquer grupo de ordem ímpar.*

Demonstração. Sejam G um grupo de ordem impar, $u \in N_U(G)$ e $\phi(x) = uxu^{-1}$. Pelo Teorema 4.2.8, $\phi^2 \in Inn(G)$, ou seja, existe $g \in$ para todo $x \in G$ temos que $\phi^2(x) = gxg^{-1}$.

Pelo Lema 4.2.11, $\phi^s = id$, para algum s impar. Pelo Teorema de Bézout, existem l, t tais que $2l + st = 1$, logo,

$$\phi = \phi^{2l+st} = (\phi^2)^l \circ (\phi^s)^t = (\phi^2)^l.$$

Como $\phi^2 \in Inn(G)$ temos que

$$\phi(x) = ((\phi^2)^l(x) = g^l x g^{-l}.$$

□

O lema a seguir traz uma propriedade de grupos que será utilizada no próximo teorema.

Lema 4.2.13. *Sejam P um p-subgrupo de Sylow de G e $g \in G$ com $o(g) = p^k$, $k \in \mathbb{N}$, tal que $g \in N_G(P)$. Então, $g \in P$.*

Demonstração. Como $P \triangleleft N_G(P)$, P é o único p-subgrupo de Sylow de $N_G(P)$. Como $g \in N_G(P)$ tem ordem potência de p, existe um p-subgrupo de Sylow de $N_G(P)$ contendo $\langle g \rangle$, mas como P é o único p-subgrupo de Sylow de $N_G(P)$, segue que $g \in P$.

□

Para o próximo teorema, usaremos a seguinte notação: fixado um 2-subgrupo de Sylow P de um grupo G, I_P denota o conjunto de todas as involuções de $Aut_U(G)$ que fixam P, ou seja,

$$I_P = \{\phi \in Aut_U(G) \mid \phi^2 = id \text{ e } \phi \mid_p = id\}.$$

Teorema 4.2.14. *Se $I_P \subset Inn(G)$ para um 2-subgrupo de Sylow $P \subseteq G$, para um grupo finito G, então $Aut_U(G) = Inn(G)$.*

Demonstração. Suponha que $I_p \subset Inn(P)$ para algum 2-subgrupo de Sylow $P \subseteq G$ e sejam $u \in N_U(G)$ e $\phi \in Aut_U(G)$ o automorfismo dado por u (ver 4.1). Pelo Teorema 4.2.2, podemos supor que $\phi(x) = x$ para todo $x \in P$.[1] Pelo Teorema 4.2.8, existe $z \in G$ tal que

$$\phi^2(x) = z^{-1}xz, \tag{4.5}$$

para todo $x \in G$. Note que existem elementos $g, h \in \langle z \rangle$ tais que

$$z = gh^2, \tag{4.6}$$

com $o(g)$ uma potência de 2 e $o(h)$ impar. Seja $\alpha \in Inn(G)$ dado por

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

[1] Se ϕ não fixa os elementos de P, então definindo $\gamma \in Inn(G)$ por $\gamma(x) = y^{-1}xy$, em que y é dado pelo Lema 4.2.2, temos que $(\gamma \circ \phi)|_P = id$.

Note que da demonstração do Teorema 4.2.8 temos que

$$u^* = zu, \tag{4.7}$$

onde * é a involução dada em 4.2.5.

Aplicando a involução * nessa igualdade, obtemos

$$u = (zu)^* = u^* z^{-1} = zuz^{-1},$$

ou seja, u e z comutam, e como $h \in \langle z \rangle$, h e u comutam e segue que

$$\alpha \circ \phi = \phi \circ \alpha.$$

Mais ainda, como estamos supondo que ϕ fixa P, temos que ϕ^2 também fixa P e segue por 4.5 que

$$z^{-1}xz = x$$

para todo $x \in P$, ou seja, $z \in C_G(P)$, o centralizador de P em G. Assim, α também deixa fixos os elementos de P, pois $h \in \langle z \rangle \subset C_G(P)$.

Podemos supor, sem perda de generalidade, que $o(z)$ é uma potência de 2, pois caso não seja, conseguimos construir uma $\Psi \in Aut_U(G)$ tal que $\Psi(x) = x$ para todo $x \in P$ e $\Psi^2(x) = g^{-1}xg$, com $o(g)$ uma potência de 2. A saber,

$$\Psi = \alpha \circ \phi$$

cumpre tais condições (ou seja, podemos trocar z pelo g na fatoração 4.6). Assim, $\phi^2|_P = id_P$, $o(z)$ é uma potência de 2 e $z \in C_G(P) \subset N_G(P)$. Pelo Lema 4.2.13, $z \in P$, mas como $z \in C_G(P)$, temos que $z \in Z(P)$, o centro de P. Mostraremos que existe um elemento em $Z(P)$ cujo quadrado é z.

Temos que, para todo $x \in P$, $\phi(x) = uxu^{-1}$, logo $x^{-1}u\phi(x) = u$, mas como $\phi(x) = x$, segue que

$$x^{-1}ux = u. \tag{4.8}$$

Escreva $u = \sum_{g \in G} u(g)g$.

Pelos mesmos argumentos da demonstração do Teorema 4.2.2, segue que a função $u : G \to \mathbb{Z}$, dada por

$$g \mapsto u(g)$$

é constante nas órbitas da seguinte ação de grupo quando restrita à P:

$$G \to Aut(G),$$

que leva

$$g \mapsto \sigma_g,$$

onde

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

Como $2 \nmid \epsilon(u)$, existe um $g_0 \in supp(u)$ que é fixado por essa ação por conjugação (mesmos argumentos em 4.3 da demonstração do Lema 4.2.2). Note que $g_0 \in C_G(P)$.

Seja v a restrição de u a $\mathbb{Z}(C_G(P)) \subseteq \mathbb{Z}G$, isto é,

$$v = \sum_{g \in C_G(P)} u(g)g.$$

Como $g_0 \in supp(u) \cap C_G(P)$, segue que $v \neq 0$. Seja $\overline{v} \in \mathbb{Z}_2(C_G(P))$ a redução de v módulo 2, ou seja,

$$\overline{v} = \sum_{g \in C_G(P)} \overline{u(g)}g,$$

$\overline{u(g)} \in \mathbb{Z}_2$. Com isso, se $g \in supp(\overline{v})$ então $\overline{u(g)} = \overline{1}$.

Vamos verificar que $supp(\overline{v})$ consiste de um número impar de elementos $g \in C_G(P)$. De $\overline{u(g)} = \overline{1}$, segue que $u(g)$ é impar. Escrevendo $\epsilon(u)$ em termos da cardinalidade das órbitas da ação por conjugação, como em 4.3 no Teorema 4.2.2, e notando que se $g \in C_G(P)$, então $\mathcal{O}(g) = \{g\}$, podemos escrever

$$\pm 1 = \epsilon(u) = \epsilon(v) + \sum_{g \in G-(C_G(P))} u(\xi)p_g^k,$$

o que implica que $\epsilon(v)$ é impar, uma vez que o valor do somatório é par. Assim, como $\epsilon(v) = \sum_{g \in C_G(G)} u(g)$, necessariamente, existe uma quantidade impar de elementos $g \in C_G(P)$ com $u(g)$ impar, logo com $\overline{u(g)} = \overline{1}$. Isto mostra que $\text{card}(supp(\overline{v}))$ é impar, como desejado.

Como o elemento $z \in G$ satisfaz a identidade

$$u^* = zu,$$

segue que $\overline{v}^* = z\overline{v}$, pois $z \in C_G(P)$.

Escolha um $x_1 \in supp(\overline{v})$. Assim, existe $x_2 \in supp(\overline{v})$ tal que

$$zx_1 = x_2^{-1}.$$

Temos também que

$$zx_2 = z(x_1^{-1}z^{-1}) = x_1^{-1},$$

pois $x_1 \in C_G(P)$ e $z \in P$. Portanto, podemos escrever $supp(\overline{v})$ como união disjunta de subconjuntos $\{x_1, x_2\}$ com $zx_1 = x_2^{-1}$.

Como $\text{card}(supp)(\overline{v})$ é impar, para algum desses subconjuntos teremos $x_1 = x_2$, o que implicará $zx_1 = x_1^{-1}$, consequentemente

$$x_1^{-2} = z. \tag{4.9}$$

Isso mostra que $o(x_1)$ é uma potência de 2, e como $x_1 \in C_G(P)$, segue que $x_1 \in Z(P)$. Com isso, $x_1^{-1} \in Z(P)$ é tal que o quadrado dá z, como desejado. Agora, considere o automorfismo $\beta \in Inn(G)$ dado por

$$\beta(x) = x_1 x x_1^{-1}.$$

Pela igualdade 4.8, segue que x_1 e u comutam, logo

$$\beta \circ \phi = \phi \circ \beta.$$

Com isso,

$$\begin{aligned}(\beta\circ\phi)^2(x) &= (\phi^2\circ\beta^2)(x)\\ &= \phi^2(x_1^2 x x_1^{-2})\\ &= \phi^2(z^{-1}xz)\\ &= z(z^{-1}xz)z^{-1}\\ &= x,\end{aligned}$$

para todo $x \in G$ e, por construção, $(\beta\circ\phi)|_P = id$. Portanto, $\beta\circ\phi \in I_P \subseteq Inn(G)$. Com isso,

$$(\beta\circ\phi)(x) = g_1 x g_1^{-1}, \forall\, x \in G,$$

para algum $g_1 \in G$, e segue que

$$\phi(x) = (x_1^{-1}g_1)x(x_1^{-1}g_1)^{-1} \in Inn(G).$$

□

Observação 4.2.15. Pode-se mostrar que se G tem um 2-subgrupo de Sylow normal P, então $I_P \subset Inn(G)$. Logo, pelo teorema anterior $Aut_U(G) = Inn(G)$. Ver [23] Teorema 3.6, pág. 246.

Finalizamos esta seção enunciando dois resultados que mostram como o problema do normalizador se relaciona com o problema do isomorfismo para grupos infinitos. As demonstrações podem ser encontradas em [32]. Um estudo sobre o problema do isomorfismo para grupo infinitos, devido à Marcin Mazur, pode ser encontrado em [33].

Teorema 4.2.16. *Seja $G = N \times A$ o produto direto de um grupo finito N por um grupo abeliano A infinito e finitamente gerado. Suponha que o problema do isomorfismo tem resposta positiva para N. Então, o problema do normalizador tem resposta positiva para N se, e somente se, o problema do isomorfismo tem resposta positiva para G*

Corolário 4.2.17. *Seja $G = N \times A$ o produto direto de um grupo finito N por um grupo abeliano A não trivial finitamente gerado. Então, o problema do isomorfismo tem resposta positiva para G se, e somente se, ambos, o problema do normalizador e o problema do isomorfismo, tem resposta positiva para N.*

4.3 Os Contraexemplos das Conjecturas

4.3.1 Contraexemplos da Conjectura ISO e da Conjectura do Normalizador

Recentemente, mais precisamente em 2001, Martin Hertweck apresentou um contraexemplo para (ISO). O contraexemplo é absolutamente não trivial; não é o objetivo dessa dissertação detalhá-lo, o leitor interessado pode encontrá-lo em [6]. Na construção de tal contraexemplo M. Hertweck obteve também um contraexemplo para a conjectura do normalizador.

Definição 4.3.1.1. *Seja G um grupo finito e seja $\mathbb{Z}G$ seu anel de grupo integral. Um* ***grupo base*** *de $\mathbb{Z}G$ é um subgrupo H do grupo das unidades normalizadas de $\mathbb{Z}G$ tal que $|G| = |H|$ e $\mathbb{Z}G = \mathbb{Z}H$.*

No trabalho de M. Hartweck é dado um exemplo de um grupo X tal que, $\mathbb{Z}X$ tem um grupo base que não é isomorfo a X. O principal argumento é a existência de um subgrupo G de X possuindo um automorfismo não interno que se torna interno no anel de grupo integral $\mathbb{Z}G$.

Teorema 4.3.1.2. *(M. Hertweck) Existe um grupo finito G com um automorfismo não interno τ, e $t \in U_1(\mathbb{Z}G)$, tal que*

$$g \overset{\tau}{\mapsto} t^{-1}gt,$$

para todo $g \in G$. O grupo G tem ordem $2^{21}.97^{28}$, um 97-subgrupo de Sylow normal, e é metabeliano.

Note que o Teorema 4.3.1.2 é um contraexemplo para a conjectura do normalizador, uma vez que pela definição do automorfismo τ temos que $t \in N_U(G)$, no entanto o automorfismo $\tau \in Aut(G)$ não é interno. Portanto, pela pela Proposição 4.2.1 $N_U(G) \neq G.Z(U(\mathbb{Z}G))$.

Teorema 4.3.1.3. *(M. Hertweck) Existe um grupo finito solúvel X, que é um produto semi-direto de um subgrupo normal G e um subgrupo cíclico $\langle c \rangle$, tal que:*

a) Existe um automorfismo τ não interno de G, e $t \in U_1(\mathbb{Z}G)$, tal que

$$g \overset{\tau}{\mapsto} t^{-1}gt,$$

para todo $g \in G$.

b) $(tc)^2 = c^2$; isto é, o elemento c inverte o elemento t em $\mathbb{Z}X$.

c) O grupo $Y = \langle G, tc \rangle$ é um grupo base de $\mathbb{Z}X$ que não é isomorfo a X.

d) O grupo X tem ordem $2^{21}.97^{28}$, um 97-subgrupo de Sylow normal, e derivada de comprimento 4.

O item c) deste teorema é o único contraexemplo conhecido para a conjectura ISO até a presente data.

4.3.2 Contraexemplos Para as Conjecturas de Zassenhaus

Definição 4.3.2.1. *Diz-se que um automorfismo normalizado α de $\mathbb{Z}G$ tem a fatoração de Zassenhaus se α é composição de automorfismo de $\mathbb{Z}G$, induzido por um automorfismo de G, seguido de um automorfismo central de $\mathbb{Z}G$.*

Roggenkamp e Scoot em [28] produziram um grupo metabeliano de ordem 2880, tal que existe um automorfismo normalizado α que não tem a fatoração de Zassenhaus, de modo que G e sua imagem $\alpha(G)$ são grupos bases de $\mathbb{Z}G$ que não são racionalmente conjugados. O contraexemplo desses autores foi simplificado por Klinger em [26].

Outro contraexemplo foi dado por M. Hertweck em [27] seguindo as ideias de Roggenkamp e Scoot, o qual enunciaremos a seguir:

Teorema 4.3.2.2. *Existe um grupo metabeliano de ordem* $1440 = 2^5.3^2.5$ *e um automorfismo* α *de* $\mathbb{Z}G$ *que não tem a fatoração de Zassenhaus.*

O grupo G é um produto semidireto $G = (M \times N \times Q) \ltimes W$, em que

i) $W = \langle w : w^8 \rangle \ltimes (\langle b : b^2 \rangle \times \langle c : c^2 \rangle)$ com $w^b = w^{-1}$ e $w^c = w^5$.

ii) $M = \langle m : m^5 \rangle$, $N = \langle n : n^3 \rangle$ e $Q = \langle q : q^3 \rangle$.

iii) $C_w(m) = \langle wc, b \rangle$, $C_w(n) = \langle w^2, b, c \rangle$ e $C_w(q) = \langle w, b \rangle$ são subgrupos de índice 2 em W.

Referências Bibliográficas

[1] F. C. P. Milies and S. K. Sehgal,*An Introduction to Group Rings*; Kluwer Academic Publishers, Dordrecht(2002).

[2] K. W. Roggenkamp and L. L. Scott, *Isomorphisms for p-adic Group Rings*, Ann. Math. 126 (1987), 593-647.

[3] F. C. P. Milies. *Grupos Nilpotentes: Uma Introdução*; Matemática Universitária nº34 - junho 2003 - pp.55-100

[4] A. Garcia e Y. Lequain, *Elementos de Álgebra*; 5.ed. Rio de Janeiro: IMPA, 2010

[5] F. C. P. Milies, *Unidades em Anéis de Grupos*; Rio de Janeiro: IMPA, 1998

[6] M. Hertweck, *A Counterexample to the Isomorphism Problem For Integral Group Rings*, Ann. Math. 154 (2001), 1-26.

[7] G. Higman. *Units of Group Rings, D.Phil. Thesis*, University of Oxford, Oxford, 1940.

[8] S. Perlis and G. Walker, *AbelJan Group Algebras of Finite Order*, Trans. Amer. Math. Soc. 68 (1950), 420-426.

[9] W. E. Deskins, *Finite Abelian Groups With Isomorphic Group algebras*, Duke Math. J. 23 (1956), 35-40.

[10] A. Whitcomb, *The Group Ring Problem, Ph.D. Thesis*, University of Chicago, 1968.

[11] R. Sandling, *Group Rings of Circle and Unit Groups*, Math. Z. , 140 (1974), 195-202.

[12] I. Hughes and K. R. Pearson, *The Group of Units of the Integral Group Ring* $\mathbb{Z}S_3$ Canad. Math, Bull., 15 (1972), 529-534.

[13] F. C. P. Milies *The Group of Units of the Integral Group Ring* ZD_4 , Bol. Soc. Brasileira de Mat., 4, 2, (1973) 85 - 92.

[14] A. K. Bhandari e I. S. Luthar, *Torsion Units of Integral Group Rings of Metacyclic Groups*, J. Number Theory, 17 (1983), 170-183.

[15] F. C. P. Milies, J. Ritter e S. K. Sehgal, *A Conjecture of Zassenhaus on Torsion Units of Integral Group Rings II*, Proc. A.M.S., 97 , 3 (1986) 201 - 206.

[16] N. Fernandes, *Torsion Units in the Integral Group Ring of* S_4 , Bol. Soc. Bras. Mat., 18, 1(1987), 1-10.

[17] I. S. Luthar and I. B. S. Passi, *Zassenhaus Conjecture For* A_5 , Proc. Indian Acad. 1989), 1-5.

[18] I. S. Luthar and P. Trama, *Zassenhaus Conjecture For* S_5. Communications in Algebra, 2353-2362 (1991).

[19] A. Weiss, *Rigidity of p-adic Torsion*, Ann. Math.127 (1988), 317-332.

[20] A. Valenti, *Torsion Units in Integral Group Rings*, Proc. Amer. Math. Soc. 120 (1) (1994), 1-4.

[21] M. A. Dokuchaev and S. O. Juriaans, *Finite Subgroups in Integral Group Rings*, Canad. J. Math., 48, (6) (1996), 1170-1179.

[22] M. A. Dokuchaev, S. O. Juriaans and F. C. P. Milies *Integral Group Rings of Frobenius Groups and the Conjectures of H. J. Zassenhaus*, Comm. in Algebra, 25, 7 (1997), 2311-2325.

[23] S. Jackowski, and Z. Marciniak, *Group Automorphisms Inducing the Identity Map On Cohomology;* Communicated by E.M. Friedlander and S. Priddy Received 4 September 1985

[24] G. Janssens. *The Isomorphism Problem for Integral Group Rings of Finite Groups*; Vrije Universiteit Brussel, Faculty of Science and Bio-Engineering science, Departement Mathematics

[25] R. Sandling *The Isomorphism Problem For Group Rings: A Survey*; Maths. Dept., The University, Manchester M13 9PL

[26] L. Klinger, *Constrution of a Counterexample to a Conjecture of Zassenhaus*, Commun. Algebra 19 (1993), 2303-2330.

[27] M. Hertweck *Another Counterexample to a Conjecture of Zassenhaus*, Beitrage zur Algebra und Geometrie Contributions to Algebra and Geometry Volume 43 (2002), No. 2, 513-520.

[28] K. W. Roggenkamp and L. L. Scott, *On a conjecture of Zassenhaus for finite group rings.* Manuscript, November 1988, 1–60.

[29] E. C. Dade, *Deux Groups finis ayant la même algebre of group sur tout corps*, Math. Z, 119 (1971), 345 - 348

[30] *H. Bass. the Dirichlet Unit Theorem, Induced Characters, and Whitehead Groups Of Finite Groups.* Topoly 4, (1966), 391, 410.

[31] W. Kimmerle, R. Lyons, R. Sandling, and D. N. Teague *Composition Factors From The Group Ring and Artin's Theorem On Orders Of Simple Groups.* Received 10 December 1987 - Revised 7 March 1989.

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

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

[34] E. Jespers, S. O. Juriaans, J. M. de Miranda e J. R. Rogério. *On the Normalizer Problem*. Journal of Algebra 247, 24-26 (2002).

[35] W. H. Thomas *Algebra* . Graduate Texts in Mathematics 73 Editorial Board S. Axler F. W. Gehring K. A. Ribet.

[36] N. Jacobson. *Basic Algebra II* W. H Freeman and Company, New York.