ELEMENTOS ALGÉBRICOS E IDEAIS
IDEMPOTENTES EM ANÉIS DE GRUPOS

Jairo Zacarias Gonçalves

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

ORIENTADOR: Prof. Dr. FRANCISCO CESAR POLCINO MILIES

Durante a realização deste trabalho, o autor teve apoio financeiro do CNPq.

Fevereiro de 1977.

Aos meus pais pelo

apoio e por me

ensinarem a perseverar

PREFÁCIO

Os anéis de grupo vêm sendo há já algum tempo, objeto de extensa pesquisa. Representam um tema interessante e acessível para um aluno com algum conhecimento básico de álgebra e portanto, uma escolha mais ou menos natural para uma dissertação de mestrado. Porém, não se pode dizer que seja um assunto fácil pois, se por um lado as questões sobre anéis de grupos não requerem conhecimento muito especializado para serem entendidas, o mesmo não pode ser dito sobre as respostas, quando estas são conhecidas.

A atração que o tema exerceu sobre nós veio principalmente da sua ligação com a teoria dos grupos finitos. O objetivo inicial foi o estudo das propriedades de um grupo finito G que podem ser refletidas pelas propriedades do anel de grupo $\mathbb{Z}G$; algumas respostas podem ser encontradas nos capítulos II e III onde são dadas, entre outras, caracterizações dos grupos finitos perfeitos, nilpotentes e solúveis. Depois, pela relação com a existência de ideais idempotentes, fomos naturalmente levados a pesquisar a existência de elementos idempotentes de RG , onde R é um anel comutativo com unidade.

Chegou-nos então, às mãos, um "pre-print" de um artigo de S.K. Sehgal e H. Zassenhauss, o qual tornou-se parte substancial do capítulo I.

Finalmente, não nos restringimos apenas aos grupos finitos, procurando mostrar algumas das dificuldades que aprecem quando se permite um tal grau de generalidade.

Embora o trabalho seja essencialmente expositivo, aqui e ali é possível encontrar uma contribuição nossa, como a simplificação da demonstração do Lema I.4.3, as provas do teorema II.3.4 e da proposição I.4.4 e o exemplo II.3.1.

Seria impossível agradecer a todas as pessoas que de uma forma ou de outra colaboraram em minha formação, durante meus estudos no IME da USP, sem cometer injustas omissões. Porém, não posso deixar de citar os seguintes professores:

Galdino C. Rocha Filho, que muito me incentivou e ensinou durante meus primeiros estudos;

Francisco Cesar P. Milies, que sugeriu o tema desta dissertação e com apoio e paciência infinita contribuiu, de modo decisivo, para a sua execução.

São Paulo, fevereiro de 1977

J. Z. Gonçalves

Í N D I C E

pg

CAPÍTULO 0

CAPÍTULO I

I.1	Introdução	3
I.2	O teorema de Zalesskii-Kaplansky	4
I.3	A conjectura de Bovdi-Mihovski para grupos finitos.	8
I.4	Alguns resultados relativos a conjectura de Bovdi-Mihovski para grupos infinitos	15

CAPÍTULO II

II.1	Introdução	23
II.2	Teoremas e proposições auxiliares.	23
II.3	Algumas caracterizações.	27

CAPÍTULO III

III.1	Introdução	41
III.2	Alguns resultados sobre "potências" transfinitas de $\Delta_R(G)$	42
III.3	Ideais idempotentes em RG	50
III.4	Ideais idempotentes em $\mathbb{Z}G$	54
	Bibliografia.	70

CAPÍTULO 0

Vamos apresentar aqui, de modo breve, os elementos que aparecerão no texto que segue. O leitor poderá encontrar uma exposição clara e didática em [31].

Seja R um anel com unidade e G um grupo multiplicativo, não necessariamente finito. O anel de grupo RG é um R -módulo livre com base G e com uma multiplicação definida distributivamente usando a multiplicação dada de G . Em outras palavras, com a multiplicação

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

onde $\gamma_u = \sum_{gh=u} \alpha_g \beta_h$.

As afirmações abaixo são de fácil verificação.

Sejam R e R' anéis comutativos com unidade, G um grupo e $\phi: R \rightarrow R'$ um homomorfismo de anéis com unidade. A função $\phi^*: RG \rightarrow R'G$ definida por

$$\phi^*\left(\sum \alpha_g g\right) = \sum \phi(\alpha_g) g$$

é um homomorfismo de álgebras. Ainda, se ϕ é um epimorfis-

mo ou monomorfismo ϕ^* também o é.

Se H é um subgrupo normal de um grupo G notaremos por $\bar{g}$ a classe do elemento g no quociente G/H . O homomorfismo canônico $\psi: G \rightarrow G/H$ se estende a um homomorfismo $\psi^*: RG \rightarrow R(G/H)$ definido por

$$\psi^*(\sum \alpha_g g) = \sum \alpha_g \bar{g} .$$

Notaremos $\text{Ker } \psi^* = \{x \in RG / \psi^*(x) = 0\}$ por $\Delta_R(G, H)$.

Uma situação especial merece destaque. Tomando $G=H$, concluímos que o morfismo trivial $G \rightarrow \{1\}$ se estende à função $\epsilon: RG \rightarrow R$ definida por

$$\epsilon(\sum \alpha_g g) = \sum \alpha_g ,$$

chamada *função índice*.

Notaremos ainda $\text{Ker } \epsilon = \{x \in RG / \epsilon(x) = 0\}$ por $\Delta_R(G)$.

É fácil ver que $\Delta_R(G, H) = \Delta_R(H)RG$.

Finalmente se R é um anel e M um R -módulo, indicaremos por $J(M)$ o radical de Jacobson de M .

CAPÍTULO I

1.1. Introdução

O problema de determinar se um anel de grupo RG é ou não indecomponível é equivalente a estudar a existência de elementos idempotentes não triviais, (i.e., diferentes de 0 e 1) em RG .

Em 1960, R. Swan [1] demonstrou que se G é um grupo finito e R um domínio de Dedekind, então RG é indecomponível. Posteriormente, em 1966, apareceu uma primeira extensão deste resultado.

Teorema (Coleman) [2] - Sejam R um anel de integridade e G um grupo finito de ordem n . Então, RG contém um idempotente não trivial se e só se algum divisor primo de n é inversível em R .

Entretanto, a condição de R ser um anel de integridade parecia muito restritiva e num artigo de 1970, Bovdi e Mihovski [3] sugeriram a seguinte extensão

Conjetura - Sejam R um anel comutativo, com unidade, indecomponível e G um grupo tal que nenhum elemento não unitário

rio de G tem ordem inversível em R . Então RG não possui idempotentes não triviais.

No caso em que G é de ordem finita, Sehgal e Zassenhauss [4] responderam afirmativamente à questão. Para grupos G de ordem infinita conhecemos apenas respostas parciais: a conjectura é válida, por exemplo, quando G é um grupo supersolúvel. Este é um resultado dos trabalhos de Parmenter e Sehgal e Sehgal em [5] e [25] respectivamente.

O objetivo deste capítulo é dar uma exposição detalhada destes resultados.

1.2 O Teorema de Zaleskii-Kaplansky

Os anéis, com os quais iremos trabalhar, a menos de menção explícita em contrário, serão sempre anéis com unidade 1. Ainda, dado um grupo G notado multiplicativamente, indicaremos o elemento neutro de G também por 1, sempre que não houver perigo de confusão.

A aplicação $\text{tr}: RG \rightarrow R$

$$\text{tr}(\sum \alpha_g g) = \alpha_1$$

é chamada *função traço*.

Observamos que é fácil verificar que a função traço é um morfismo de R -módulos.

Proposição 1.2.1 Sejam $\alpha, \beta \in RG$. Então $\text{tr} \alpha \beta = \text{tr} \beta \alpha$.

Prova: Se $\alpha = \sum_{g \in G} \alpha_g g$ e $\beta = \sum_{h \in G} \beta_h h$,

$$\text{tr } \alpha \beta = (\alpha \beta)_1 = \sum_{gh=1} \alpha_g \beta_h .$$

Como num grupo $gh=1$ se e só se $hg=1$ e $\text{tr } \beta \alpha = \sum_{hg=1} \beta_h \alpha_g$, vem imediatamente que $\text{tr } \alpha \beta = \text{tr } \beta \alpha$. $\square$

Definição 1.2.1 Seja A uma álgebra sobre o corpo K . Chamamos *subespaço comutador* de A , que notaremos por $[A, A]$, ao subespaço da álgebra A gerado pelos produtos $[a, b] = ab - ba$, com $a, b \in A$.

Proposição 1.2.2 Seja A uma álgebra sobre um corpo K de característica $p > 0$. Se $a_1, \dots, a_m \in A$ e se $n > 0$ for um inteiro dado, então existe um elemento $b \in [A, A]$ com

$$(a_1 + \dots + a_m)^{p^n} = a_1^{p^n} + \dots + a_m^{p^n} + b .$$

Prova: Observe que

$$(a_1 + a_2 + \dots + a_m)^{p^n} = a_1^{p^n} + \dots + a_m^{p^n} + b$$

onde b é a soma de todas as palavras $a_{i_1} a_{i_2} \dots a_{i_{p^n}}$ com pelo menos dois índices distintos. Se as palavras ω_1 e ω_2 são permutações cíclicas uma da outra, isto é, se

$$\omega_1 = a_{i_1} a_{i_2} \dots a_{i_{p^n}} , \quad \omega_2 = a_{i_j} a_{i_{j+1}} \dots a_{i_{p^n}} a_{i_1} \dots a_{i_{j-1}}$$

então $\omega_1 - \omega_2 = \gamma \delta - \delta \gamma \in [A, A]$ onde

$$\gamma = a_{i_1} a_{i_2} \dots a_{i_{j-1}} \quad \text{e} \quad \delta = a_{i_j} a_{i_{j+1}} \dots a_{i_{p^n}} .$$

Portanto, módulo $[A, A]$, todas as permutações cíclicas de uma palavra são iguais. Façamos agora o grupo $\mathbb{Z}_{p^n}$ agir sobre o conjunto dessas palavras através de deslocamentos cíclicos. Então, o número de permutações formalmente distintas de uma palavra w ocorrendo em b é o tamanho de uma órbita não trivial de $\mathbb{Z}_{p^n}$ e portanto é divisível por p . Como K tem característica p o resultado segue. $\square$

Definição 1.2.2 Seja $\alpha = \sum_{g \in G} \alpha_g g$ um elemento de RG .

Chamaremos suporte de α , notando $\text{supp } \alpha$, ao conjunto

$$\text{supp } \alpha = \{g \in G / \alpha_g \neq 0\}.$$

Na demonstração do próximo teorema, precisaremos do seguinte resultado, enunciado por Passman em [26]. O leitor interessado poderá procurar a demonstração em [7], afirmações IV, V e VI.

Lema 1.2.3 Seja $A = \mathbb{Z}[a_1, \dots, a_r]$ um anel de integridade de característica zero, que é finitamente gerado, como anel, sobre os inteiros.

Seja $b \in A \setminus \mathbb{Q}$. Nestas condições, existe um ideal maximal M de A tal que $F = A / M$ é um corpo de característica prima $p > 0$ e tal que a imagem de b em F não pertence ao corpo primo de F .

Teorema 1.2.4 (Zaleskii - Kaplansky). Seja $e \in KG$ um idempotente. Então $\text{tr}(e)$ pertence ao subcorpo primo de K .

Prova:

Caso 1: K tem característica $p > 0$.

Seja $e = \sum e_g g = e^2$ e $S = \{g \in \text{Supp}(e) / \exists n \in \mathbb{N} \text{ o}(g) = p^n\}$ onde $\text{o}(g)$ indica a ordem do elemento $g \in G$.

Como o conjunto S é finito, existe um inteiro positivo s tal que $g^{p^s} = 1$ para todo $g \in S$.

Seja, agora, n um inteiro tal que $n \geq s$. Como e é um idempotente temos que

$$e^{p^n} = e = (\sum e_g g)^{p^n},$$

e da proposição I.2.2 vem que existe um elemento $\gamma \in [KG, KG]$ tal que

$$e = e^{p^n} = \sum_{g \in G} (e_g)^{p^n} g^{p^n} + \gamma,$$

$$\text{logo, } \text{tr}(e) = \text{tr} \left(\sum_{g \in G} (e_g)^{p^n} g^{p^n} \right) + \text{tr}(\gamma).$$

Da proposição I.2.1 vem imediatamente que para todo elemento da forma $x = \alpha\beta - \beta\alpha$ tem-se que:

$$\text{tr}(x) = 0;$$

consequentemente, temos que $\text{tr}(\gamma) = 0$.

Ainda, desde que $n \geq s$, segue que, para cada $g \in \text{supp}(e)$ temos $g^{p^n} = 1$ se e só se $g \in S$. Assim

$$\text{tr}(e) = \sum_{g \in S} (e_g)^{p^n} = \left(\sum_{g \in S} e_g \right)^{p^n}.$$

A igualdade acima vale para todos os inteiros $n \geq s$; tomando $n = s$ e $n = s + 1$ obtemos

$$(\text{tr}(e))^p = \left[\left(\sum_{g \in S} e_g \right)^{p^s} \right]^p = \left(\sum_{g \in S} e_g \right)^{p^{s+1}} = \text{tr}(e).$$

Portanto, $\text{tr}(e) \in K$ é um elemento que satisfaz a equação $x^p = x$ cujas raízes pertencem todas ao corpo primo de K .

Caso 2: K é um corpo de característica 0.

Seja $e = \sum e_g g = e^2$ e $A = \mathbb{Z}[\{e_g / g \in \text{supp}(e)\}]$.

Então, A é um anel de integridade de característica zero, que é finitamente gerado como anel sobre os inteiros. Ainda, o elemento e é um idempotente de AG .

Suponhamos que $b = \text{tr}(e) \notin \mathbb{Q}$. Pelo Lema I.2.3, existe um ideal maximal M de A tal que $F = A / M$ é um corpo de característica $p > 0$ e tal que a imagem de b em F não pertence ao corpo primo. Por outro lado, considerando o morfismo canônico

$$\phi: AG \longrightarrow (A / M)G = FG$$

temos que $\phi(e)$ é um idempotente. Da primeira parte do teorema segue que a imagem de b está no corpo primo, um absurdo. $\square$

I.3 A conjectura de Bovdi-Mihovski para grupos finitos

Estamos, agora, em condições de provar a veracidade

da conjectura de Bovdi-Mihovski para grupos finitos. Porém, vamos enunciar antes, alguns resultados dos quais depende a demonstração.

Lema 1.3.1 (Herstein-Small) [8] Seja A uma álgebra sobre um anel comutativo R , que é finitamente gerada como R -módulo. Se A tem um conjunto finito de geradores, cada um dos quais é um elemento nilpotente, então A é nilpotente.

Teorema 1.3.2 (Goldie) [9] Seja A um anel com unidade tal que

- (i) A não contém ideais nilpotentes não nulos
- (ii) O conjunto dos anuladores à direita de elementos de A verifica a condição maximal
- (iii) Não existe uma família infinita de ideais à direita, não nulos, cuja soma é direta.

Seja $S = \{x \in A / x \text{ não é divisor do zero}\}$.

Então, o anel de frações A_S é um anel semi-simples.

Os lemas seguintes serão necessários na prova do teorema.

Lema 1.3.3 Seja G um grupo e R um anel comutativo, indecomponível, tal que $U(R) \cap \{o(g) / g \in G\} = \{1\}$. Seja ainda, N o conjunto dos elementos nilpotentes de R . Então, se RG contém idempotentes não triviais $(R/N)G$ também

contêm idempotentes não triviais e $U(R/N) \cap \{o(g) / g \in G\} = \{1\}$.

Prova: Seja $\phi^*: RG \longrightarrow (R/N)G$ o morfismo induzido pelo morfismo canônico $\phi: R \longrightarrow R/N$ e $e = \sum e_g g = e^2 \in RG$ um elemento idempotente não trivial. Sem perda de generalidade, considerando $1-e$ se necessário, podemos admitir que $e \in \Delta_R(G)$.

Assim, se $I = [\{e_g\}]$, como e é idempotente vem que $I^2 = I$ e que $\phi^*(e)$ é um elemento idempotente de $(R/N)G$.

Se $\phi^*(e)$ fosse trivial, teríamos necessariamente $\phi^*(e) = 0$. Logo $e_g \in N$, $\forall g \in \text{supp}(e)$, e portanto $I \subseteq N$, um absurdo. Agora, seja $g \in G$ tal que $o(g) \in U(R/N)$. Então, existe $\bar{m} \in R/N$ tal que $\bar{m} \overline{o(g)} = \bar{1}$, e $1 - m o(g)$ é um elemento nilpotente; logo $m o(g) = 1 - (1 - m o(g)) \in U(R)$ e consequentemente $o(g) \in U(R)$. $\square$

Lema 1.3.4 ([27], pg 279) - Sejam R um anel e $a \in R$ um elemento não nilpotente tal que $a^2 - a$ seja nilpotente. Então, existe um polinômio $f \in \mathbb{Z}[X]$ tal que

- (i) $f(1) = 1$
- (ii) $f(0) = 0$
- (iii) $f^2(a) = f(a)$ e $f(a) \neq 0$.

O polinômio f é definido do seguinte modo: seja $m \in \mathbb{N}^*$ tal que $(a^2 - a)^m = 0$. Então, se $(X - X^2)^m = X^m - X^{m+1}g(X)$, $f(X) = X^m g(X)$.

Lema 1.3.5 Seja R um anel comutativo, indecomponível. Se N indica o conjunto dos elementos nilpotentes de R , então R/N não tem elementos idempotentes não triviais.

Prova: Seja $\bar{x} = \overline{x^2} \in R/N$ com $\bar{x} \neq \bar{0}$.

Então, x não é nilpotente mas $x^2 - x$ é. Do lema 1.3.4, $f(x)$ é um elemento idempotente não nulo de R . Logo $f(x)=1$. Mas, $1 = f(x) = x^m g(x)^m = x(x^{m-1}g(x)^m)$. Logo $x \in U(R)$ e portanto $x^{-1}(x^2 - x) \in N$ e $x-1 \in N$. Portanto $\bar{x} = \bar{1}$. $\square$

Lema 1.3.6 Seja R um anel comutativo, indecomponível, sem elementos nilpotentes e G um grupo finito tal que $U(R) \cap \{o(g) / g \in G\} = \{1\}$. Então, ou $\text{car } R = 0$ ou RG não tem idempotentes não triviais.

Prova: Suponhamos que a característica de R seja $m > 0$. Discutiremos vários casos:

(i) m não é potência de um primo. Então, podemos escrever:

$$m = m_1 m_2 \text{ com } (m_1, m_2) = 1 \text{ e } m_1, m_2 > 1.$$

Neste caso:

$$\mathbb{Z}_m = (m_1) \oplus (m_2) \subseteq R$$

contém um idempotente não trivial.

(ii) $m = p^\alpha$, com $\alpha > 1$ e p primo. Então, $\mathbb{Z}_{p^\alpha} \subseteq R$ contém o elemento $x = p + (p^\alpha)$, que é um elemento nilpotente não trivial.

(iii) $m = p$, primo. Seja $e = \sum e_g g = e^2 \in RG$. Como $\epsilon(e)$ é um elemento idempotente de R e este anel não contém idempotentes não triviais, temos que $\epsilon(e) = 0$ ou $\epsilon(e) = 1$. Assim, sem perda de generalidade, podemos assumir que $e \in \Delta_R(G)$.

Porém, para todo $n \in \mathbb{N}^*$ tal que $(n, p) = 1$ tem-se que $n \in U(R)$ e da hipótese segue que G deve ser um p -grupo finito. Do lema I.3.1 vem que $\Delta_R(G)$ é nilpotente e consequentemente $e = 0$. $\square$

Teorema I.3.7 Seja R um anel comutativo, indecomponível e G um grupo finito tal que $U(R) \cap \{o(g) / g \in G\} = \{1\}$. Então RG não possui elementos idempotentes não triviais.

Prova: Em vista dos Lemas I.3.3, I.3.5 e I.3.6 podemos assumir que R é um anel de característica zero, sem elementos nilpotentes.

Podemos assumir, também, que R é noetheriano. De fato, se $e = \sum e_g g$ é um elemento idempotente não nulo de RG , então o anel $S = \mathbb{Z}[\{e_g / g \in \text{supp}(e)\}]$ é noetheriano pois é imagem epimórfica do anel noetheriano $\mathbb{Z}[X_1, \dots, X_n]$ onde $n = |\text{supp}(e)|$ e $e \in SG$.

Pelo teorema I.3.2, o anel de quocientes de R é uma soma direta de corpos e temos que:

$$R \subseteq Q(R) = F_1 \oplus \dots \oplus F_k \oplus \dots \oplus F_r,$$

onde os F_i são corpos de característica zero para, $1 \leq i \leq k$, e os F_{k+j} , $1 \leq j \leq r-k$, são corpos de característica fini

ta.

Seja $T: Q(R)G \longrightarrow M_n(Q(R))$ a representação regular de $Q(R)G$ na base formada pelos elementos de G e $T(e)$ a matriz associada a e .

Seja $\pi_i: F_1 \oplus \dots \oplus F_k \oplus \dots \oplus F_r \longrightarrow F_i$ a projeção canônica sobre F_i e representemos por $\chi(X)$ e $\chi_i(X)$ os polinômios característicos de $T(e)$ e $T(\pi_i(e)) = T_i(e)$, respectivamente.

Temos:

$$\chi(X) = \det [XI - T(e)] = X^n - a_1 X^{n-1} + \dots + (-1)^n a_n,$$

$$a_i \in R, \quad 1 \leq i \leq r, \quad e$$

$$\chi_i(X) = \det [XI - T_i(e)] = X^n - \pi_i(a_1) X^{n-1} + \dots + (-1)^n \pi_i(a_n).$$

Por outro lado, sabemos que

$$\chi_i(X) = X^{n-j} (X-1)^j$$

onde j é o posto da matriz idempotente $T_i(e) \in M_n(F_i)$.

Seja $m = \max \{j / 1 \leq i \leq r\}$. Se $T_i(e)$ é uma matriz de posto precisamente m segue que

$$\chi_i(X) = X^{n-m} (X-1)^m = X^n - mX^{n-1} + \dots + (-1)^m X^{n-m}.$$

Portanto, $(-1)^m a_{n-m}$ é um idempotente com tantas componentes não nulas e iguais a 1 quantas forem as soluções da equação $j=m$. Mas, como R é indecomponível temos que:

$$a_{n-m} = (-1)^m (1, 1, \dots, 1).$$

Assim, como todas as $T_i(e)$ tem posto m , vem que:

$$\text{tr } T(e) = ne_1 = (m, m, \dots, m) .$$

Escrevendo $n=ds$ e $m=dt$ com $(s,t)=1$ temos que:

$$e_1 = (t/s, \dots, t/s, \alpha_1, \dots, \alpha_{r-k})$$

onde t/s aparece k vezes e os coeficientes α_i pertencem a um corpo finito. Se conseguirmos mostrar que $s \in U(R)$, então $s=1$, $m=n=|G|$ e portanto, $e=1$.

De fato, se $s \in U(R)$, necessariamente $s=1$, pois caso contrário se p é um primo que divide s temos $p \in U(R)$ e seria $U(R) \cap \{o(g) / g \in G\} \neq \{1\}$. Logo $m=n=|G|$ e $\chi_i(X) = (X-1)^n$ para todo i , o que implica que $T_i(e) = I_n$.

Desde que $(t,s)=1$, existem inteiros a e b tal que $at + bs = 1$. Então:

$$\beta = ae_1 + bl_R = (1/s, \dots, 1/s, a\alpha_1 + b, a\alpha_2 + b, \dots) \in R .$$

Podemos supor que $a\alpha_i + b \neq 0$ para todo i , pois em caso contrário, uma potência conveniente de $s\beta$ seria um idempotente não trivial de R . Mas:

$$s\beta - 1 = (0, \dots, 0, s(a\alpha_1 + b) - 1, s(a\alpha_2 + b) - 1, \dots) \in R .$$

Novamente, $s(a\alpha_i + b) - 1 = 0$ para todo i e portanto:

$$s\beta - 1 = 0 \quad \text{ou} \quad s\beta = 1 .$$

Logo, $s \in U(R)$ com $s^{-1} = \beta = (1/s, \dots, 1/s) . \quad \square$

1.4 Alguns resultados relativos a conjectura de Bovdi-Mihovski para grupos infinitos.

A tentativa de responder afirmativamente a conjectura de Bovdi-Mihovski segue um caminho diferente no caso dos grupos infinitos. Vamos apresentar aqui os resultados conseguidos por M.M. Parmenter e S.K. Sehgal em [5] e por S.K. Sehgal em [25].

Os seguintes resultados serão necessários na demonstração do principal teorema desta secção.

Teorema 1.4.1 [10, pg 50]: Seja R um anel comutativo, I um ideal de R , A um R -módulo gerado por n elementos e x um elemento de R tal que $xA \subseteq IA$. Então $(x^n + y)A = 0$ para algum $y \in I$.

Fazendo $x = 1$ e tomando $A = I$, ideal idempotente, finitamente gerado de R , obtemos o corolário abaixo, o qual será utilizado na prova do lema que se segue.

Corolário 1.4.2 Seja R um anel comutativo e I um ideal idempotente de R que é finitamente gerado como R -módulo. Então, existe $y \in I$ tal que $(1 - y)I = 0$.

Lema 1.4.3 Seja R um anel comutativo, indecomponível e p um primo que não é inversível em R . Seja, ainda, N um p -subgrupo normal, finito de G tal que $R(G/N)$ não possui idempotentes não triviais. Então, RG não possui idempoten-

tes não triviais.

Prova: Seja $e = e^2 = \sum e_g g \in RG$. Considerando 1-e se necessário, podemos assumir que $e \in \Delta_R(G)$. Seja $\phi^*: RG \rightarrow R(G/N)$ o morfismo induzido pelo morfismo canônico $\phi: G \rightarrow G/N$. Então, $\ker \phi^* = \Delta_R(G, N)$ e para todo $m \in \mathbb{N}^*$ temos que:

$$e \in \bigcap_{n=1}^m \Delta_R^n(G, N) = \bigcap_{n=1}^m [\Delta_R(N)RG]^n = [\Delta_R(N)RG]^m = \Delta_R^m(N)RG.$$

Observemos que a última igualdade é consequência do fato que $N \trianglelefteq G$, i.e., para todo $n \in N$ e para todo $g \in G$ existe $n' \in N$ tal que $gn = n'g$, o que implica $\Delta_R(N)RG = RG\Delta_R(N)$.

Como $p \notin U(R)$, $\bar{R} = R/pR$ é um anel, não nulo, de característica p e do lema I.3.1 vem que $\Delta_{\bar{R}}(N)$ é uma subálgebra nilpotente de $\bar{R}N$. Concluimos, assim, que $\bar{e} = 0$ em $\bar{R}G$.

Seja $I = [\{e_g / g \in \text{supp}(e)\}]$. Então, $I^2 = I$ e $I \subseteq pR$. Do corolário I.4.2 existe $i \in I$ tal que $(1-i)I = 0$. Portanto, $i^2 = i$, logo $i = 0$. Concluimos, assim, que $I = 0$ e portanto, também $e = 0$. $\square$

Definição I.4.1 Um grupo G diz-se supersolúvel se possui uma série normal finita $G = G_n \supseteq G_{n-1} \supseteq \dots \supseteq G_0 = \{1\}$, na qual cada grupo quociente G_i/G_{i-1} , $1 \leq i \leq n$, é cíclico.

Proposição I.4.4 Seja G um grupo e N um subgrupo de G . Então

$$\bigcap_{n=1}^{\infty} [\Delta_R^n(N) RG] = [\bigcap_{n=1}^{\infty} \Delta_R^n(N)] RG.$$

Prova: (i) $\bigcap_{n=1}^{\infty} [\Delta_R^n(N) RG] \supseteq [\bigcap_{n=1}^{\infty} \Delta_R^n(N)] RG.$

Seja $n \in \mathbb{N}^*$. Se $x \in [\bigcap_{n=1}^{\infty} \Delta_R^n(N)] RG$, então $x = \sum_{j=1}^s u_j w_j$, com

$$u_j \in \bigcap_{n=1}^{\infty} \Delta_R^n(N) \text{ e } w_j \in RG.$$

Desse modo $x = \sum_{j=1}^s u_j w_j$ com $u_j \in \Delta_R^n(N)$ e $w_j \in RG$ para todo

$n \in \mathbb{N}^*$, logo $x \in \bigcap_{n=1}^{\infty} [\Delta_R^n(N) RG].$

$$(ii) \bigcap_{n=1}^{\infty} [\Delta_R^n(N) RG] \subseteq [\bigcap_{n=1}^{\infty} \Delta_R^n(N)] RG.$$

Seja $\{x_v\}_{v \in I}$ um conjunto completo de representantes de classes laterais à direita de N em G .

Assim,

$$RG = \sum_{v \in I} RN x_v \text{ e } \Delta_R^n(N) RG = \sum_{v \in I} \Delta_R^n(N) RN x_v.$$

Mas $\Delta_R^n(N)$ é um ideal de RN e

$$\Delta_R^n(N) RG = \sum_{v \in I} \Delta_R^n(N) x_v = \Delta_R^n(N) \{x_v\}_{v \in I}.$$

Seja agora, $x \in \bigcap_{n=1}^{\infty} \Delta_R^n(N) \{x_v\}_{v \in I}$. Então, para todo $n \in \mathbb{N}^*$

$x = \sum_k u_k(n) x_{v_k}(n)$, com $u_k(n) \in \Delta_R^n(N)$ e onde os elementos $x_{v_k}(n)$ e $u_k(n)$ em princípio dependem do n fixado. Porém, a expressão de $x \in RG$ na forma $\sum_{v \in I} R N x_v$ é única, o que mostra que os $u_k(n)$ e os $x_{v_k}(n)$ na realidade, não dependem de n . Desse modo $x = \sum_k u_k x_{v_k}$ onde $u_k \in \Delta_R^n(N)$ para todo $n \in \mathbb{N}^*$ e portanto $x \in [\prod_{n=1}^{\infty} \Delta_R^n(N)] RG$. $\square$

Lema 1.4.5 (Jennings) [11] Seja G um grupo nilpotente, finitamente gerado, sem torção. Então, para qualquer anel R , o ideal de aumento $\Delta_R(G)$ de RG satisfaz

$$\Delta_R^\omega(G) = \prod_{n=1}^{\infty} \Delta_R^n(G) = 0.$$

Pode-se ver uma demonstração do lema acima em [11].

Lema 1.4.6 [12] Seja G um grupo supersolúvel. Então G possui uma série característica $\{1\} \subseteq L \subseteq M \subseteq G$ onde L é um subgrupo finito de ordem ímpar, M/L um grupo nilpotente, finitamente gerado, sem torção e G/M um 2-grupo finito.

Proposição 1.4.7 Seja N um grupo finito solúvel. Então, existe um subgrupo característico T de N tal que N/T é um p -grupo para algum primo p .

Prova: Indução sobre a ordem de N . $\square$

Estamos, agora, em condições de responder parcialmente à conjectura de Bovdi-Mihovski para grupos supersolúveis.

Teorema I.4.8 Suponhamos que G seja um grupo supersolúvel e R um anel comutativo, indecomponível, tal que $2 \nmid U(R)$ e $U(R) \cap \{o(g) / g \in G\} = \{1\}$. Então, RG não possui idempotentes não triviais.

Prova: Como G é supersolúvel, pelo lema I.4.6, G possui uma série característica $\{1\} \subseteq L \subseteq M \subseteq G$ tal que L é um subgrupo finito de ordem ímpar, M/L um grupo nilpotente, finitamente gerado, sem torção e G/M um 2-grupo finito. Provemos, em primeiro lugar, que RG não possui idempotentes não triviais se $L = \{1\}$.

Suponhamos, então, que $e = e^2 \in \Delta_R(G)$ e $\{1\} \subseteq M \subseteq G$ com M e G/M nas condições acima.

Como no Lema I.4.3, temos:

$$e \in \bigcap_{n=1}^{\infty} \Delta_R^n(G, M) = \bigcap_{n=1}^{\infty} \Delta_R^n(M) RG = \left[\bigcap_{n=1}^{\infty} \Delta_R^n(M) \right] RG,$$

sendo a última igualdade uma consequência da proposição I.4.4.

Mas, do lema I.4.5 vem que:

$$\bigcap_{n=1}^{\infty} \Delta_R^n(M) = 0, \quad \text{portanto } e = 0.$$

Podemos, assim, admitir que $R(G/L)$ não possui idempotentes não triviais.

Suponhamos agora $L \neq \{1\}$ e seja $N \neq \{1\}$ um subgrupo normal de L , minimal com relação à propriedade de $R(G/N)$ não ter idempotentes não triviais. Como N é solúvel, por ser subgrupo de um grupo supersolúvel, da proposição I.4.7 vem que existe um subgrupo característico T de N tal que N/T é um p -grupo. Assim, $T \triangleleft G$ e $G/T/N/T \cong G/N$. Do lema I.4.3 segue que $R(G/T)$ não possui idempotentes não triviais. Isto contradiz a minimalidade de N ; portanto N é trivial e RG não possui idempotentes não triviais. $\square$

Observação: No que segue mostraremos que se pode prescindir da hipótese $2 \nmid U(R)$. Deve-se notar, entretanto, que ela foi utilizada na demonstração acima para garantir que $e \in \Delta_R(G/M)$.

De fato, se $\phi^*: RG \longrightarrow R(G/M)$ é o morfismo induzido pelo morfismo canônico $\phi: G \longrightarrow G/M$, $\phi^*(e) \in \Delta_R(G/M)$ é um idempotente de $R(G/M)$. Pelo teorema I.3.7, $R(G/M)$ não possui idempotentes não triviais; logo $\phi^*(e) = 0$.

Teorema I.4.9 (Formanek) [28] Seja KG o anel de grupo de um grupo supersolúvel, sem torção, sobre um corpo. Então, KG não tem divisores do zero.

Lema I.4.10 Seja R um anel comutativo, indecomponível e G um grupo supersolúvel, sem torção. Então RG não possui

idempotentes não triviais.

Prova: Seja $e = \sum e_g g = e^2 \in RG$. Podemos assumir, como na prova do teorema I.3.7, que R é noetheriano e que $e \in \Delta_R(G)$. Seja N o conjunto dos elementos nilpotentes de R e $\phi^*: RG \rightarrow (R/N)G$ o morfismo induzido pelo morfismo canônico $\phi: R \rightarrow R/N$. Pelo teorema I.3.2, R/N está contido numa soma direta de corpos:

$$R/N \subseteq F_1 \oplus \dots \oplus F_k.$$

Agora, $\bar{e} = \phi^*(e)$ é um idempotente de $(R/N)G$, que está contido em

$$(F_1 \oplus \dots \oplus F_k)G \cong F_1G \oplus \dots \oplus F_kG$$

onde o isomorfismo acima, que notaremos por σ , é o isomorfismo natural dado por

$$\sigma\left(\sum_1 (a_{i_1}, \dots, a_{i_k}) g_i\right) = \left(\sum_1 a_{i_1} g_i, \dots, \sum_1 a_{i_k} g_i\right).$$

Como $\sigma(\bar{e})$ é um elemento idempotente, cada componente de $\sigma(\bar{e})$ será um idempotente. Pelo teorema I.4.9, cada componente de $\sigma(\bar{e})$ é 0 pois $\epsilon(\sigma(\bar{e})) = (0, \dots, 0)$.

Segue então, que $\bar{e} = 0$. Logo, para todo $g \in \text{supp}(e)$ tem-se que $e_g \in N$. Portanto, se $I = [\{e_g / g \in \text{supp}(e)\}]$ vem que $I^2 = I \subseteq N$, o que implica que $I = 0$, donde $e = 0$. $\square$

Teorema I.4.11 Seja R um anel comutativo, indecomponível e G um grupo supersolúvel tal que para todo elemento $g \in G - \{1\}$ de ordem finita, tem-se que $o(g) \nmid U(R)$. Então

RG não possui idempotentes não triviais.

Prova: Sabemos que G tem uma série característica $G \supseteq M \supseteq L \supseteq \{1\}$ tal que L é finito de ordem ímpar, M/L é nilpotente, finitamente gerado, sem torção e G/M é um 2-grupo finito. Vamos considerar dois casos:

(i) G/L é sem torção. Então, pelo Lema I.4.10, $R(G/L)$ não possui idempotentes não triviais. Assim, de modo análogo à demonstração do teorema I.4.8, concluímos que RG não possui idempotentes não triviais

(ii) G/L tem um elemento de torção. Então, existe um elemento de ordem 2 em G e o resultado segue do teorema I.4.8. $\square$

CAPÍTULO II

11.1 Introdução

Porque estudar os anéis de grupos? Esta é uma pergunta que se coloca para quem, pela primeira vez, toma conta com a sua noção. Por que, dado um grupo G e um anel com unidade R , construir um novo conjunto RG , que possui dentro de si uma cópia de G , uma cópia de R , uma estrutura de anel e uma estrutura de R -módulo?

Sem pretender, com a nossa justificativa, dar uma resposta completa a esta questão, podemos dizer que, afora o interesse matemático pela rica estrutura de RG , quando o anel R é bem escolhido, o anel de grupo RG reflete muitas propriedades do grupo G . Em particular, se tomarmos $R = \mathbb{Z}$ e G finito, $\mathbb{Z}G$ torna-se uma $\mathbb{Z}$ -álgebra de dimensão finita. É nestas condições que mostraremos que certas propriedades do grupo G são equivalentes à algumas de RG .

11.2 Teoremas e Proposições auxiliares

Teorema 11.2.1 [20] Seja $e = \sum e_g$ um idempotente cen-

tral em RG , onde R é um anel comutativo. Então, o grupo suporte de e , isto é, o subgrupo de G gerado pelo conjunto $\{g \in G / e_g \neq 0\}$ é finito.

Teorema II.2.2 Seja I o anel dos inteiros algébricos e $\gamma = \sum \gamma_g g \in IG$, satisfazendo:

- (1) $\gamma^2 = m\gamma$ para $m \in \mathbb{N}^*$
- (2) $\sum \gamma_g \neq 0$
- (3) $\gamma_1 = 1$
- (4) γ é central

Então $\gamma = \sum_{g \in N} g$ onde N é um subgrupo normal, finito, de G .

Prova: Como γ/m é um idempotente central de $Q(I)G$, onde $Q(I)$ é o corpo de frações de I , podemos supor, de acordo com o teorema II.2.1 que G é finito. Seja T a representação regular de IG ; para um elemento $\alpha \in IG$ indicaremos por $\text{tr} T(\alpha)$ o traço da matriz $T(\alpha)$.

Como $T(\gamma)$ é raiz do polinômio $x^2 - mx$, $T(\gamma)$ é semelhante a uma matriz diagonal da forma

$$A = \begin{bmatrix} m & & & & & \\ & m & & & & \\ & & \ddots & & & \\ & & & m & & \\ & & & & 0 & \\ & & & & & \ddots \\ & & & & & & 0 \\ & & & & & & & 0 \end{bmatrix}$$

e temos

$$(1.1) \quad \text{tr} T(\gamma) = |G| \gamma_1 = |G| 1 = m\ell$$

onde ℓ é o número de elementos não nulos na diagonal de A .

Seja agora $g \in G$. Observando que γg^{-1} satisfaz a equação

$$(1.2) \quad x^{n+1} = m^n x$$

onde $n = o(g^{-1})$, concluímos que o polinômio minimal de $T(\gamma g^{-1})$ divide $x^{n+1} - m^n x$ e portanto $T(\gamma g^{-1})$ é semelhante a uma matriz da forma

$$B = \begin{bmatrix} m\xi_1 & & & & \\ & m\xi_2 & & & \\ & & \ddots & & \\ & & & m\xi_\ell & \\ & & & & 0 \\ & & & & & 0 \\ & & & & & & \ddots \\ & & & & & & & 0 \end{bmatrix}$$

onde ξ_1 é uma raiz n -ésima da unidade em I .

Assim,

$$\text{tr} T(\gamma g^{-1}) = |G| \gamma_g = \sum_{i=1}^{\ell} m\xi_i \quad \text{e} \quad \ell \gamma_g = \sum_{i=1}^{\ell} \xi_i \quad \text{ou}$$

$$(1.3) \quad \ell \gamma_g \xi_1^{-1} = \sum_{i=2}^{\ell} \xi_i \xi_1^{-1} + 1.$$

Seja $F = \mathbb{Q}(\zeta)$ onde ζ é uma raiz primitiva n -ésima

ma da unidade. Tomando Norma $F/\mathbb{Q}$ de ambos os lados de (1.3) vem que:

$$(1.4) \quad \ell^s a = 1 + \sum_{i=2}^{\ell} \xi_i \xi_1^{-1} + \sum_{i=\ell+1}^{\ell^s} x_i$$

onde $a = \text{Norma}_{F/\mathbb{Q}} (\gamma_g \xi_1^{-1}) \in \mathbb{Z}$, $s = [F:\mathbb{Q}]$ e $x_1^n = 1$.

Portanto, se $\gamma_g \neq 0$, tomando valor absoluto em (1.4) obtemos

$$\left| 1 + \sum_{i=2}^{\ell} \xi_i \xi_1^{-1} + \sum_{i=\ell+1}^{\ell^s} x_i \right| = |\ell^s a| = \ell^s.$$

Logo $1 = \xi_2 \xi_1^{-1} = \dots = \xi_{\ell} \xi_1^{-1}$ ou $\xi_1 = \xi_2 = \dots = \xi_{\ell}$.

Assim, temos que $\gamma_g = \xi_g$ onde $\xi_g^n = 1$.

Vamos escrever agora $\gamma^* = \sum \bar{\xi}_1 g_1^{-1}$ onde $\bar{\xi}_1$ representa o complexo conjugado de ξ_1 . Então, $(\gamma \gamma^*)^2 = m^2 (\gamma \gamma^*)$ e tomando o traço da representação regular obtemos:

$$\text{tr} T(\gamma \gamma^*) = |G| \sum \xi_1 \bar{\xi}_1 \leq m^2 \ell = m^2 \frac{|G|}{m} = m |G|$$

e

$$(1.5) \quad \sum \xi_1 \bar{\xi}_1 \leq m.$$

Portanto, o número de termos não nulos em γ é no máximo m . Mas, $\gamma^2 = m\gamma$ implica que $\epsilon(\gamma) = m$. Logo $\sum_{i=1}^m \xi_i = m$. Tomando o módulo de ambos os lados da igualdade anterior concluímos que $\xi_1 = \xi_2 = \dots = \xi_m$ e que $m\xi_1 = m$. Portanto $\xi_1 = \xi_2 = \dots = \xi_m = 1$ e $\gamma = \sum_{g \in N} g$.

Devemos mostrar, ainda, que N é um subgrupo normal de G .

Mas,

$$\gamma^2 = \sum_{g, h \in N} gh = m\gamma = m \sum_{g \in N} g$$

e daqui vem imediatamente que todos os produtos gh , $g, h \in N$ pertencem a N ; consequentemente este é um subgrupo.

Ainda, do fato de γ ser central vem que:

$$\gamma = g\gamma g^{-1} \text{ para todo } g \in G \text{ e } \sum_{h \in N} h = \sum_{h \in N} ghg^{-1}$$

o que implica que os elementos da forma ghg^{-1} pertencem a N para todo $h \in N$ e para todo $g \in G$; logo, $N \triangleleft G$. $\square$

Definição 11.2.1 Seja G um grupo finito. Um elemento $\alpha \in \mathbb{Z}G$ é chamado de *quase idempotente* se as seguintes condições estiverem verificadas:

- (i) $\alpha_1 = 1$
- (ii) $\varepsilon(\alpha) \neq 0$
- (iii) existe $m \in \mathbb{N}^*$, $1 < m < |G|$ tal que $\alpha^2 = m\alpha$
- (iv) α é central

11.3 Algumas Caracterizações

Escolhendo convenientemente o anel R , mostraremos como certas propriedades algébricas do anel de grupo RG se refletem em propriedades do grupo G . Temos, por exemplo, que o anel $\mathbb{Z}G$ é comutativo se e só se o grupo G for abe-

liano. Isto ilustra o tipo de proposição que procuramos.

Teorema II.3.1 Seja G um grupo finito. Então G é simples se e só se $\mathbb{Z}G$ não possui elementos quase idempotentes.

Prova: Segue imediatamente do teorema II.2.2. $\square$

Teorema II.3.2 Seja G um grupo finito e $|G| = p_1^{r_1} \dots p_k^{r_k}$ a decomposição da ordem de G em produto de fatores primos distintos. Então G é nilpotente se e só se existem quase idempotentes $\alpha_1, \dots, \alpha_k \in \mathbb{Z}G$ com $\alpha_i^2 = p_1^{r_1} \alpha_i$ $1 \leq i \leq k$.

Prova: (a) Seja G nilpotente. Se $S_1(G)$ é o p_1 subgrupo de Sylow de G , temos que $G = S_1(G) \times \dots \times S_k(G)$. Definamos $\alpha_i = \sum_{g \in S_1(G)} g$, $1 \leq i \leq k$. É imediata a verificação de que α_i é um quase idempotente de $\mathbb{Z}G$ com $\alpha_i^2 = |S_1(G)| \alpha_i = p_1^{r_1} \alpha_i$, $1 \leq i \leq k$.

(b) Sejam $\alpha_1, \dots, \alpha_k \in \mathbb{Z}G$ quase idempotentes com $\alpha_i^2 = p_1^{r_1} \alpha_i$, $1 \leq i \leq k$. Do teorema II.2.2 existem subgrupos normais H_i de G , $1 \leq i \leq k$, tais que $\alpha_i = \sum_{g \in H_i} g$ e $|H_i| = p_1^{r_1}$. Como cada H_i é um p_1 -subgrupo de Sylow que é normal em G , a afirmação segue imediatamente. $\square$

Definição II.3.1 Um grupo G diz-se perfeito, se coincide com seu subgrupo comutador G' .

Utilizaremos em sequência, o resultado abaixo, devido a Krull. Entretanto, não consegui encontrá-lo na forma em

que está apresentado, o que me obrigou a demonstrá-lo. O leitor poderá consultar [32, pg 216] e [10, pg 49].

Teorema 11.3.3 (Krull) - Seja R um anel comutativo, noetheriano e I um ideal de R . Então existe $x \in I$ tal que

$$I^{\omega}(1-x) = 0 \quad \text{onde} \quad I^{\omega} = \bigcap_{n=1}^{\infty} I^n.$$

O teorema seguinte pode ser obtido a partir do lema 12.12 de [31, pg 98]. Contudo, estou apresentando aqui uma demonstração feita quando ainda não conhecia este resultado. Isto porque ela reflete, de um certo modo, a linha de raciocínio seguida neste trabalho.

Teorema 11.3.4 Seja G um grupo finito. Então G é perfeito se e só se o ideal de aumento $\Delta_{\mathbb{Z}}(G)$ é um ideal idempotente.

Prova: (a) Seja G perfeito. Então $G = G'$, isto é, $G = [\{xyx^{-1}y^{-1} / x, y \in G\}]$ e será suficiente mostrar que $\Delta_{\mathbb{Z}}(G) \subseteq \Delta_{\mathbb{Z}}^2(G)$ já que a recíproca vale para todo ideal de $\mathbb{Z}G$. Como o conjunto $\{g-1 / g \in G\}$ é um conjunto de geradores de $\Delta_{\mathbb{Z}}(G)$ sobre $\mathbb{Z}$, bastará mostrar que $g-1 \in \Delta_{\mathbb{Z}}^2(G)$ para todo $g \in G$.

Agora, um argumento de indução sobre r , onde $r = \min \{k / g = u_1 \dots u_k, u_j \in G'\}$, e as igualdades abaixo, provam a afirmação.

$$g-1 = u_1 w_1 u_1^{-1} w_1^{-1} - 1 = [(u_1-1)(w_1-1) - (w_1-1)(u_1-1)]u_1^{-1} w_1^{-1}$$

$$x-1 = g u_1 w_1 u_1^{-1} w_1^{-1} - 1 = g(u_1 w_1 u_1^{-1} w_1^{-1} - 1) + (g-1) .$$

(b) Seja G finito tal que $\Delta_{\mathbb{Z}}^2(G) = \Delta_{\mathbb{Z}}(G)$ e seja $\phi: \mathbb{Z}G \rightarrow \mathbb{Z}(G/G')$ o morfismo canônico. Notaremos $A = \phi(\Delta_{\mathbb{Z}}(G))$. Temos assim que A é um ideal idempotente de $\mathbb{Z}(G/G')$, que é um anel comutativo.

Como G/G' é finito e $\mathbb{Z}$ é noetheriano, $\mathbb{Z}(G/G')$ é noetheriano [21, teorema 2]. Pelo teorema II.3.3 existe $x \in A$ tal que $A(1-x) = 0$, isto é, existe $x \in \mathbb{Z}(G/G')$ tal que $x^2 = x$. Porém, pelo teorema de Coleman $\mathbb{Z}(G/G')$ só possui idempotentes triviais. Logo $A = 0$ ou $A = \mathbb{Z}(G/G')$.

Mas $A \subseteq \ker \varepsilon \subseteq \mathbb{Z}(G/G')$, onde $\varepsilon: \mathbb{Z}(G/G') \rightarrow \mathbb{Z}$. Portanto $A = 0$ e assim, qualquer que seja $g \in G$ $g \equiv 1 \pmod{G'}$ e consequentemente $g \in G'$. $\square$

Vamos mostrar, a seguir, que se G é um grupo finito, a álgebra $\mathbb{Z}G$ não possui elementos nilpotentes se e só se G for abeliano ou Hamiltoniano de ordem $2^m t$, onde a ordem multiplicativa de 2 módulo t é ímpar.

Proposição II.3.5 Seja R um anel sem elementos nilpotentes. Então, todo elemento idempotente de R é central.

Prova: Para todo $x \in R$ tem-se que $[ex(1-e)]^2 = [(1-e)xe]^2 = 0$, logo $ex = exe = xe$. Consequentemente e é central. $\square$

Proposição II.3.6 Seja R um anel comutativo de característica $n > 0$ tal que RG não possui elementos nilpotentes. Então n é livre de quadrados, (i.e., $n = p_1 p_2 \dots p_k$,

um produto de primos distintos). Podemos, ainda, escrever $R \cong \bigoplus_{i=1}^k R_i$, onde R_i tem característica p_i , $1 \leq i \leq k$. Assim, RG não possui elementos nilpotentes se e só se cada $R_i G$ não possui elementos nilpotentes.

Prova: (i) Seja $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Se para algum i , com $1 \leq i \leq k$ tem-se que $\alpha_i > 1$, então o elemento

$x = p_1^{\alpha_1} \dots p_i \dots p_k^{\alpha_k}$ é não nulo em R e

$$x^{\alpha_i} = (p_1^{\alpha_1} \dots p_i \dots p_k^{\alpha_k})^{\alpha_i} = \begin{bmatrix} p_1^{\alpha_1(\alpha_i-1)} & \dots & p_{i-1}^{\alpha_{i-1}(\alpha_i-1)} & \dots \\ \dots & p_{i+1}^{\alpha_{i+1}(\alpha_i-1)} & \dots & p_k^{\alpha_k(\alpha_i-1)} \end{bmatrix} p_1^{\alpha_1} \dots p_i^{\alpha_i} \dots p_k^{\alpha_k} = 0,$$

em contradição com o fato de R não possuir elementos nilpotentes.

(ii) $R \cong \bigoplus_{j=1}^k R_j$ onde os R_j são anéis de característica p_j .

Seja $n = p_1 \dots p_k$ e $\phi: R \longrightarrow \bigoplus_{j=1}^k R/p_j R$ definido por $\phi(r) = (r + p_1 R, \dots, r + p_k R)$.

É claro que $R/p_j R$, $1 \leq j \leq k$, é um anel de característica p_j e que ϕ é um homomorfismo. Provemos que ϕ é um isomorfismo.

Se $\phi(r) = (0, \dots, 0)$ temos que $(r + p_1 R, \dots, r + p_k R) = (0, \dots, 0)$ ou $r \in p_1 R \cap \dots \cap p_k R$. Logo $n = p_1 \dots p_k$ divide r e portanto $r = 0$. Consequentemente ϕ é injetora.

Seja $(r_1 + p_1 R, \dots, r_k + p_k R) \in \bigoplus_{j=1}^k R/p_j R$ e $n_i = p_1 \dots \hat{p}_1 \dots p_k$, onde o chapéu sobre o primo p_i indica que o mesmo não aparece no produto em questão. Então, $(p_i, n_i) = 1$, $1 \leq i \leq k$, e existe $a_i \in \mathbb{Z}$ tal que $a_i n_i \equiv 1$. Logo, se $r = \sum_{j=1}^k r_j a_j n_j$, então $\phi(r) = (r_1 + p_1 R, \dots, r_k + p_k R)$. De fato, se $j \neq i$, p_i divide n_j e $r_j a_j n_j \equiv 0 \pmod{p_i R}$ e $r_i a_i n_i \equiv r_i \pmod{p_i R}$. Portanto ϕ é sobrejetora. $\square$

Definição 11.3.2 Seja R um anel comutativo. O conjunto dos elementos nilpotentes de R forma um ideal, chamado *nilradical* de R .

Teorema 11.3.7 ([10], pg 16) (Krull) O nilradical de um anel comutativo R é a intersecção de todos os ideais primos de R .

Proposição 11.3.8 Sejam G um grupo finito e R um anel comutativo. Seja ainda $\gamma = \sum \gamma_g g$ um elemento nilpotente de RG . Então, $|G|\gamma_1$ é um elemento nilpotente de R .

Prova: Seja P um ideal primo de R e $\phi^*: RG \rightarrow (R/P)G$ o morfismo induzido pelo morfismo canônico $\phi: R \rightarrow R/P$. Representemos por $Q(R/P)$ o corpo de frações de R/P .

Considerando a matriz da representação regular de $\phi^*(\gamma) = \bar{\gamma}$ e tomando o traço, obtemos

$$|G|\gamma_1 \equiv 0 \pmod{P}.$$

De fato, se $|G| = n$ e $T: (R/P)G \longrightarrow M_n(Q(R/P))$ é a representação regular de $(R/P)G$, a matriz $T(\bar{\gamma})$ tem como polinômio característico $f(X) = X^n$. Logo $\text{tr}(T(\bar{\gamma})) = \overline{|G|\gamma_1} \equiv 0 \pmod{P}$.

Assim $|G|\gamma_1 \in \bigcap_{P\text{-primo}} P$ que é o nilradical de R , pelo teorema II.3.7. $\square$

Teorema II.3.9 Seja K um corpo. Se KG não possui elementos nilpotentes, então, todo subgrupo finito de G é normal em G e, portanto, os elementos de torção de G , $T(G)$, formam um subgrupo de G .

Prova: É suficiente considerar o caso em que $\text{car} K = p$ primo. Neste caso, G não possui elementos de ordem p pois $(g-1)^p = 0$. Seja H um subgrupo finito de G ; então $p \nmid |H|$ e

$$e^2 = \left(\frac{1}{|H|} \sum_{h \in H} h \right)^2 = \frac{1}{|H|} \sum_{h \in H} h = e$$

é um idempotente central de KG , conforme a proposição II.3.5. Logo $H \triangleleft G$.

Para mostrar que $T(G)$ é um subgrupo de G basta provar que $T(G)$ é fechado em relação ao produto. Sejam $x, y \in T(G)$. Como $[x] \triangleleft G$ vem que

$$y x y^{-1} = x^r \quad \text{com} \quad 0 \leq r < |[x]|.$$

Assim $yx = x^r y$ e $(xy)^m = x^{1+r+\dots+r^{m-1}} y^m$ para todo inteiro positivo m , donde concluímos que $xy \in T(G)$. $\square$

Corolário 11.3.10 Seja K um corpo e G um grupo finito. Se KG não possui elementos nilpotentes, então G é abeliano ou Hamiltoniano.

Proposição 11.3.11 Seja G um grupo finito e F_p o corpo com p -elementos. Então, $F_p G$ não contém elementos nilpotentes se e só se for abeliano e $p \nmid |G|$.

Prova: Suponhamos que $F_p G$ não possui elementos nilpotentes. Se $g^p = 1$ para algum elemento $g \in G$, ter-se-ia que $(g-1)^p = 0$ em $F_p G$; conseqüentemente G não possui elementos de ordem p . Assim, temos que $p \nmid |G|$ e pelo teorema de Wedderburn:

$$F_p G \cong \oplus M_{n_i}(D_i),$$

uma soma direta de anéis de matrizes sobre anéis com divisão. Para cada i , temos que D_i é uma álgebra de dimensão finita sobre F_p , logo D_i é finito e portanto comutativo. Também, deve ser $n_i = 1$ para todo i , pois caso contrário, $M_{n_i}(D_i)$ possuiria elementos nilpotentes. Portanto $F_p G$ é comutativo e G é abeliano.

A recíproca também segue do teorema de Wedderburn. De fato, como $p \nmid |G|$, pelo teorema de Wedderburn

$$F_p G \cong \oplus M_{n_i}(D_i).$$

Mas G abeliano implica que $F_p G$ é comutativa. Logo, para todo i , $n_i = 1$ e os D_i são comutativos, o que acarreta que $F_p G$ não possui elementos nilpotentes. $\square$

Proposição II.3.12 Seja G um grupo finito e R um anel comutativo de característica $n > 0$. Então, RG não possui elementos nilpotentes se e só se R não possui elementos nilpotentes, $|G|$ não é um divisor do zero em R e G é abeliano.

Prova: Provaremos primeiro a necessidade das condições.

Como $R \subseteq RG$, R não possui elementos nilpotentes.

Suponhamos que $|G|r = 0$ para algum $r \in R$. Então

$\alpha = r \sum_{g \in G} g$ é um elemento nilpotente, pois:

$$\left(r \sum_{g \in G} g \right)^2 = r(r|G|) \sum_{g \in G} g = 0 ;$$

consequentemente $r = 0$. Obviamente, como $R \supseteq F_n$, da proposição II.3.6 segue que $n = p_1 \dots p_k$ e portanto $F_n G \cong \bigoplus_{j=1}^k F_{p_j} G$ não possui elementos nilpotentes.

Da proposição II.3.11 segue que G é abeliano.

Para provar a recíproca, suponhamos as condições válidas e suponhamos também que $0 \neq \gamma = \sum \gamma_g g$ seja um elemento nilpotente. Como G é abeliano, considerando γg^{-1} se necessário, podemos supor que $\gamma_1 \neq 0$. Segue então, da proposição II.3.8, que $|G|\gamma_1$ é nilpotente e, como R não contém elementos nilpotentes, vem que $|G|\gamma_1 = 0$; logo $\gamma_1 = 0$, o que é uma contradição. $\square$

Observação: Notemos que se R é um anel comutativo de característica zero, sem elementos nilpotentes e G é um grupo abeliano finito tal que $|G|$ não é um divisor do zero em

R, então RG não possui elementos nilpotentes.

A demonstração é igual à dada na proposição II.3.12 .

Seja $K_8 = [a, b / a^4 = 1, a^2 = b^2, b^{-1}ab = a^{-1}]$ o grupo quaternio de ordem 8. Estamos interessados em saber em que condições o anel RK_8 possui elementos nilpotentes. Esta questão será respondida pela proposição abaixo.

Proposição II.3.13 Seja R um anel comutativo sem elementos nilpotentes tal que 2 não é um divisor do zero em R . Então RK_8 não possui elementos nilpotentes se e só se a equação

$$x^2 + y^2 + z^2 = 0 \quad x, y, z \in R$$

não possui solução não nula em R .

Prova: Vamos observar, inicialmente, que um anel R possui elementos nilpotentes se e só se existe $\gamma \in R$, $\gamma \neq 0$ tal que $\gamma^2 = 0$.

Assim, seja $\gamma = \sum \alpha_g g \in RK_8$ tal que $\gamma^2 = 0$ e $\phi^*: RK_8 \rightarrow R(K_8/[a^2])$ o morfismo induzido pelo morfismo canônico $\phi: K_8 \rightarrow K_8/[a^2]$. Como $R(K_8/[a^2])$ está nas condições da proposição II.3.12 ou da sua observação, $R(K_8/[a^2])$ não possui elementos nilpotentes. Logo $\phi^*(\gamma) = 0$ ou $\gamma \in \Delta_R(K_8, [a^2])$. Da proposição II.3.8 concluímos que $\gamma_1 = 0$ pois $8\gamma_1 = 0$ e 2 não é um divisor do zero em R . Assim, γ é da forma

$$\gamma = (xa + yb + zab)(1 - a^2) \quad e$$
$$\gamma^2 = (xa + yb + zab)^2(1 - a^2)^2.$$

Mas,

$$(xa + yb + zab)^2 =$$
$$= (x^2 + y^2 + z^2)a^2 + xyab + xza^2b + yxa^3b + yza + zxb + zya^3.$$

Também

$$(xa + yb + zab)^2(a^2 - 1) = (x^2 + y^2 + z^2)(1 - a^2).$$

Assim,

$$\gamma^2 = (xa + yb + zab)^2(a^2 - 1)^2 =$$
$$= (x^2 + y^2 + z^2)(1 - a^2)(a^2 - 1) = 2(x^2 + y^2 + z^2)(a^2 - 1).$$

Portanto $\gamma^2 = 0$ se e só se $x^2 + y^2 + z^2 = 0$, provando a afirmação. $\square$

O próximo teorema depende do seguinte resultado de Claude Moser:

Teorema II.3.14 [22] - Seja $\mathbb{Q}_m = \mathbb{Q}(\xi_m)$ um corpo ciclotômico onde ξ_m é uma raiz primitiva m -ésima da unidade, m ímpar e $m \geq 3$. Então, a equação $-1 = x^2 + y^2$ tem uma solução em $\mathbb{Q}_m$ se e só se a ordem multiplicativa de 2 módulo m for par.

Teorema II.3.15 Seja G um grupo finito. Então, $\mathbb{Q}G$ não possui elementos nilpotentes se e só se uma das seguintes condições estiver satisfeita:

- (1) G é abeliano
- (ii) G é Hamiltoniano de ordem $2^m t$, t ímpar, tal que a ordem multiplicativa de 2 módulo t é ímpar.

Prova: Suponhamos que G seja um grupo não abeliano tal que $\mathcal{Q}G$ não possui elementos nilpotentes. Então, pelo corolário II.3.10 G é Hamiltoniano.

Logo, $G = E \rtimes A \rtimes K_8$ onde E é um 2-grupo abeliano elementar, A é um grupo abeliano de ordem ímpar e K_8 é o grupo quaternário de ordem 8.

Assim,

$$\mathcal{Q}G \cong (\mathcal{Q}E) (A \rtimes K_8) \cong (\mathcal{Q} \mathcal{Q}) (A \rtimes K_8) \cong \mathcal{Q} \mathcal{Q} (A \rtimes K_8) \cong \mathcal{Q} (\mathcal{Q}A) K_8$$

e será suficiente considerarmos $(\mathcal{Q}A) K_8$.

Porém, de [23] vem que

$$\mathcal{Q}A \cong \bigoplus_{d|a} n_d \mathcal{Q}_d$$

onde $n_d \mathcal{Q}_d$ representa n_d cópias de $\mathcal{Q}(\xi_d)$ e a é o expoente de A .

Logo

$$(\mathcal{Q}A) K_8 \cong \bigoplus_{d|a} n_d \mathcal{Q}_d(K_8)$$

e pela proposição II.3.13, para todo divisor d de a , a equação $x^2 + y^2 + z^2 = 0$ não tem solução em $\mathcal{Q}_d$.

Do teorema II.3.14 concluímos que isto acontece se e somente se para todo $d \in \mathbb{N}^*$, $d|a$, a ordem multiplicativa de 2 módulo d for ímpar.

Sejam $t = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ e $a = p_1^{\beta_1} \dots p_k^{\beta_k}$, respectivamente, as decomposições de $t = |A|$ e a em fatores primos distintos e suponhamos que s_1 , a ordem multiplicativa de 2 módulo $p_1^{\beta_1}$ seja um número ímpar. Vamos provar que v_1 , a ordem multiplicativa de 2 módulo $p_1^{\alpha_1}$ também é ímpar.

Sabemos [24, pg 121] que se p for um primo ímpar, Γ_{p^Y} , o grupo dos elementos inversíveis do anel $\mathbb{Z}_{p^Y}$, é cíclico e $|\Gamma_{p^Y}| = (p-1)p^{Y-1}$. Portanto, se $a \in \Gamma_{p_1^{\alpha_1}}$ com $o(a) = p_1^{\alpha_1 - \beta_1}$, então $\Gamma_{p_1^{\alpha_1}} / [a] \cong \Gamma_{p_1^{\beta_1}}$ e existe $r \in \mathbb{N}$ tal que $2^{s_1} \equiv a^r \pmod{p_1^{\alpha_1}}$ donde

$$2^{s_1 p_1^{\alpha_1 - \beta_1}} \equiv 1 \pmod{p_1^{\alpha_1}}.$$

Logo v_1 é ímpar.

Finalmente, é imediato que a ordem multiplicativa de 2 mod t é ímpar.

O mesmo argumento, junto com a proposição II.3.13 e o teorema II.3.14 provam a recíproca. $\square$

Corolário II.3.16 Seja G um grupo finito. Então, $\mathbb{Z}G$ não possui elementos nilpotentes se e só se uma das seguintes condições estiver satisfeita:

- (i) G é abeliano
- (ii) G é Hamiltoniano de ordem $2^m t$, t ímpar, tal que a ordem multiplicativa de 2 módulo t é ímpar.

Prova: Basta observar que $\mathbb{Z}G$ possui elementos nilpotentes se e só se $\mathbb{Q}G$ possui. $\square$

Exemplo 11.3.1 Seja $[c]$ o grupo cíclico de ordem 3 e $G = [c] \rtimes K_8$.

Então, se $x = c^2 - c$, $y = 1 - c$, $z = 1 - c^2$, o elemento $\gamma = (xa + yb + zab)(1 - a^2) \in \mathbb{Z}([c] \rtimes K_8)$ é um elemento nilpotente.

De fato,

$$(c^2 - c)^2 = c - 2 + c^2 = x^2$$

$$(1 - c)^2 = -2c + 1 + c^2 = y^2$$

$$(1 - c^2)^2 = c + 1 - 2c^2 = z^2$$

e portanto $x^2 + y^2 + z^2 = 0$.

$$\text{Logo, } \gamma^2 = 2(x^2 + y^2 + z^2)(a^2 - 1) = 0.$$

CAPÍTULO III

III.1 Introdução

Neste capítulo consideraremos um grupo finito G e estudaremos condições que são necessárias e suficientes, sobre o anel do grupo $\mathbb{Z}G$, para que o grupo G seja solúvel.

Em 1971, estudando este problema, T. Akasaki [14] provou que se G é um grupo finito nilpotente, então $\mathbb{Z}G$ não possui ideais (bilaterais) idempotentes, não triviais e mostrou que se G é finito, não solúvel, então $\mathbb{Z}G$ possui um ideal idempotente não trivial. Conjeturou ainda que $\mathbb{Z}G$ não possui ideais idempotentes não triviais se e somente se G é solúvel.

Uma resposta parcial a esta questão foi conseguida pelo próprio T. Akasaki em [15] e por M. M. Parmenter e S. K. Sehgal [5], que provaram que o ideal de aumento $\Delta_{\mathbb{Z}}(G)$ de $\mathbb{Z}G$ não contém ideais (de $\mathbb{Z}G$), idempotentes, se e só se G é solúvel.

Restaria, ainda, a possibilidade de existirem ideais idempotentes não contidos em $\Delta_{\mathbb{Z}}(G)$; porém, K. W. Roggenkamp [16] demonstrou que isto não pode acontecer.

Vamos expor inicialmente a demonstração de Parmenter e Sehgal, a qual utiliza técnicas e resultados já vistos nos capítulos anteriores.

III.2 Alguns resultados sobre "potências" transfinitas de $\Delta_R(G)$

Sejam R um anel comutativo e G um grupo. Definiremos certas "potências" transfinitas de $\Delta_R(G)$, que não são, na verdade, potências no sentido usual mas certos operadores. Entretanto, isto não deverá causar nenhuma confusão no texto que segue.

Escreveremos:

$$\Delta_R^\omega(G) = \bigcap_{n=1}^{\infty} \Delta_R^n(G)$$

e por indução, para cada $m \in \mathbb{N}^*$ definimos

$$\Delta_R^{\omega^m}(G) = \bigcap_{n=1}^{\infty} [\Delta_R^{\omega^{m-1}}(G)]^n$$

Ainda, chamaremos

$$\Delta_R^\lambda(G) = \Delta_R^{\omega^\omega}(G) = \bigcap_{m=1}^{\infty} \Delta_R^{\omega^m}(G) .$$

Finalmente, vamos definir por indução, para $m \in \mathbb{N}^*$

$$\Delta_R^{\lambda^m}(G) = [\Delta_R^{\lambda^{m-1}}(G)]^\lambda .$$

Definição III.2.1 Seja G um grupo que contém uma série finita de subgrupos normais

$$\{1\} = G_{n+1} \subseteq G_n \subseteq \dots \subseteq G_1 = G.$$

Dizemos que esta é uma *série central forte* se as seguintes condições estiverem verificadas:

- (i) $[G_i, G_j] = [xyx^{-1}y^{-1} \mid x \in G_i, y \in G_j] \subseteq G_{i+j}$ quaisquer que sejam i e j .
- (ii) cada um dos grupos abelianos G_i/G_{i+1} é o produto direto (não necessariamente finito) de grupos cíclicos que são ou infinitos ou de ordem p^k , onde p é um primo fixo e k é limitado por algum inteiro r dependente apenas de G .

O teorema seguinte, devido a B. Hartley [17], será usado repetidamente.

Teorema III.2.1 Seja G um grupo que admite uma série central forte, onde cada fator é produto direto de um grupo abeliano livre e de um grupo de expoente p^n , onde p é um primo fixo e n um inteiro fixo. Seja, ainda, R um anel comutativo tal que:

$$\bigcap_{m=1}^{\infty} p^m R = 0.$$

Então $\Delta_R^\omega(G) = 0$.

Lema III.2.2 Seja G um grupo que contém uma sequência $\{N_i\}_{i \in \mathbb{N}}$ de subgrupos normais $N_0 \supseteq N_1 \supseteq \dots \supseteq N_1 \supseteq \dots$

tal que $\bigcap_{i \in \mathbb{N}} N_i = \{1\}$.

Então $\bigcap_{i \in \mathbb{N}} \Delta_R(G, N_i) = 0$.

Prova: Seja $x = \sum_{k=1}^m x_k g_k \in \bigcap_{i \in \mathbb{N}} \Delta_R(G, N_i) = A$.

Como A é um ideal de RG

$$y = g_1^{-1} x = x_1 1 + \sum_{k=2}^m x_k g_1^{-1} g_k \in A.$$

Mas $\bigcap_{i \in \mathbb{N}} N_i = \{1\}$; logo existe $s \in \mathbb{N}$ tal que $g_1^{-1} g_2, \dots,$

$g_1^{-1} g_m$ não pertencem a N_s . Portanto, se $\phi: RG \rightarrow R(G/N_s)$ é o morfismo induzido pelo morfismo canônico $\phi^*: G \rightarrow G/N_s$ temos que

$$\phi(y) = x_1 \phi(1) + \sum_{k=2}^m x_k \phi(g_1^{-1} g_k) = x_1 \bar{1} + \sum_{k=2}^m x_k \overline{g_1^{-1} g_k} = 0,$$

onde o coeficiente de $\bar{1}$ é precisamente x_1 . Como $\phi(y) = 0$ vem que, em particular, $x_1 = 0$.

Com raciocínio análogo

$$x_2 = \dots = x_m = 0 \quad \text{e} \quad A = 0.$$

□

Lema III.2.3 Seja P um p -grupo abeliano de expoente finito e R um anel comutativo tal que:

$$\bigcap_{n \in \mathbb{N}} p^n R = 0.$$

Então

$$\Delta_R^\omega(P) = 0.$$

Prova: Seja $H = [a]$ um grupo cíclico de ordem infinita e consideremos $G = [a] \times P$. O grupo G é abeliano e está nas condições do teorema III.2.1, logo:

$$\Delta_R^\omega(G) = \Delta_R^\omega([a] \times P) = 0.$$

Levando em conta que

$$\Delta_R([1] \times P) \subseteq \Delta_R([a] \times P)$$

concluimos que

$$\Delta_R^\omega(P) = 0.$$

□

A proposição seguinte é clássica. Veja, por exemplo [30], pg 91.

Proposição III.2.4 Seja P o conjunto dos inteiros primos, G um grupo abeliano e T seu subgrupo de torção. Então $T = \prod_{p \in P} G_p$ onde $G_p = \{x \in G / o(x) = p^n \text{ para algum } n\}$.

Lema III.2.5 Sejam G um grupo abeliano com torção e R um anel comutativo. Vamos supor, ainda, que para qualquer $p \in P$ tal que o p -subgrupo de Sylow $S_p(G)$ é não trivial, tem-se que:

$$\bigcap_{n \in \mathbb{N}} p^n R = 0.$$

e $S_p(G)$ tem expoente finito

Então $\Delta_R^\lambda(G) = 0$.

Prova: Pela proposição III.2.4 podemos encontrar uma sequência de subgrupos de G , não necessariamente finita

$$[1.1] \quad G = G_1 \supseteq G_2 \supseteq \dots \supseteq G_i \supseteq \dots$$

tal que G_i/G_{i+1} é um p_i -grupo, onde $p_i \neq p_j$ para $i \neq j$.

Provemos, por indução, que para todo $n \in \mathbb{N}^*$ tem-se que:

$$\Delta_R^{\omega^n}(G) \subseteq \Delta_R(G, G_{n+1}).$$

$$(i) \quad \underline{\Delta_R^{\omega}(G) \subseteq \Delta_R(G, G_2)}$$

Seja $\phi^*: RG \rightarrow R(G/G_2)$ o morfismo induzido pelo morfismo canônico $\phi: G \rightarrow G/G_2$ e $x \in \Delta_R^{\omega}(G)$. Então,

como $x \in \Delta_R^m(G)$ para todo $m \in \mathbb{N}^*$, vem que $\phi^*(x) \in \Delta_R^m(G/G_2)$,

logo $\phi^*(x) \in \bigcap_{m=1}^{\infty} \Delta_R^m(G/G_2)$. Mas, do Lema III.2.3 tem-se que

$\bigcap_{m=1}^{\infty} \Delta_R^m(G/G_2) = 0$. Portanto $\phi^*(x) = 0$ e $x \in \Delta_R(G, G_2)$.

$$(ii) \quad \underline{\text{Supondo que } \Delta_R^{\omega^n}(G) \subseteq \Delta_R(G, G_{n+1}), \text{ vamos provar que}}$$

$$\underline{\Delta_R^{\omega^{n+1}}(G) \subseteq \Delta_R(G, G_{n+2})}$$

Sejam $x \in \Delta_R^{\omega^{n+1}}(G)$ e $\phi^*: RG \rightarrow R(G/G_{n+2})$ o

morfismo induzido pelo morfismo canônico $\phi: G \rightarrow G/G_{n+2}$.

Então, para todo $m \in \mathbb{N}^*$ temos que $(\Delta_R^{\omega^n}(G))^m$ e da hipótese

de indução $x \in \Delta_R^m(G, G_{n+1})$. Mas $\Delta_R(G, G_{n+1}) = \Delta_R(G_{n+1})RG$.

Portanto:

$$\phi^*(x) \in \phi^*(\Delta_R^m(G_{n+1})) R(G/G_{n+2}) = \Delta_R^m(G_{n+1}/G_{n+2}) R(G/G_{n+2}) .$$

Logo:

$$\begin{aligned} \phi^*(x) &\in \bigcap_{m=1}^{\infty} [\Delta_R^m(G_{n+1}/G_{n+2}) R(G/G_{n+2})] = \\ &= [\bigcap_{m=1}^{\infty} \Delta_R^m(G_{n+1}/G_{n+2})] R(G/G_{n+2}) , \end{aligned}$$

onde a última igualdade vem da proposição I.4.4. Finalmente, do Lema III.2.3, temos que

$$[\bigcap_{m=1}^{\infty} \Delta_R^m(G_{n+1}/G_{n+2})] R(G/G_{n+2}) = 0 .$$

Logo $\phi^*(x) = 0$ e $x \in \Delta_R(G, G_{n+2})$.

Como $\bigcap_{n=1}^{\infty} G_n = \{1\}$, do Lema III.2.2 vem que $\bigcap_{n=1}^{\infty} \Delta_R(G, G_{n+1}) = 0$.

Mas,

$$[1.2] \quad \bigcap_{n=1}^{\infty} \Delta_R^{\omega^n}(G) \subseteq \bigcap_{n=1}^{\infty} \Delta_R(G, G_{n+1}) ,$$

donde concluímos que $\Delta_R^1(G) = \bigcap_{n=1}^{\infty} \Delta_R^{\omega^n}(G) = 0$. $\square$

Lema III.2.6 Seja G um grupo abeliano finitamente gerado e R um anel comutativo tal que $\bigcap_{n \in \mathbb{N}} p^n R = 0$ para todos os primos p tais que $S_p(G) \neq \{1\}$. Então existe algum inteiro positivo k tal que:

$$\Delta_R^{\omega^k}(G) = 0 .$$

Prova: Se G é sem torção, pelo Lema I.4.5 temos que:

$$\Delta_R^\omega(G) = 0 \quad \text{e o lema vale.}$$

Seja agora $G = S \times T$, onde S é a parte livre de G e T é a parte de torção. Então, $G/T \cong S$ e, pelo Lema I.4.5 temos que:

$$\Delta_R^\omega(G/T) \cong \Delta_R^\omega(S) = 0.$$

Isto significa que

$$\Delta_R^\omega(G) \subseteq \Delta_R(G, T) = \Delta_R(T)RG.$$

Como T é finitamente gerado, pode-se obter uma sequência finita

$$T = T_1 \supseteq T_2 \supseteq \dots \supseteq T_\ell \supseteq T_{\ell+1} = 1$$

nas condições da sequência [1.1] da demonstração do Lema III.2.5.

Portanto, a fórmula [1.2] reduz-se a

$$\Delta_R^{\omega_\ell}(T) = \bigcap_{n=1}^{\ell} \Delta_R^{\omega_n}(T) \subseteq \bigcap_{n=1}^{\ell} \Delta_R(T, T_{n+1}) = 0.$$

Logo:

$$\Delta_R^{\omega_\ell}(G) \subseteq \Delta_R^{\omega_\ell}(T)RG = 0.$$

□

Lema III.2.7 Seja G um grupo solúvel, tal que cada fator na série derivada é finitamente gerado e seja R um anel comutativo tal que, para cada primo p que ocorre nos grupos fatores da série derivada de G , tem-se que:

$$\bigcap_{n \in \mathbb{N}} p^n R = 0.$$

Então $\Delta_R^{\lambda^c}(G) = 0$, onde c é o comprimento da série derivada de G .

Prova: Seja $G = G_0 \supseteq G_1 \supseteq \dots \supseteq G_c = \{1\}$ a série derivada de G . Se $c = 1$ o resultado segue do Lema III.2.6. Usando indução, temos que:

$$\Delta_R^{\lambda^{c-1}}(G/G_{c-1}) = 0, \text{ isto é, } \Delta_R^{\lambda^{c-1}}(G) \subseteq \Delta_R(G, G_{c-1}) = \Delta_R(G_{c-1})RG.$$

Porém, como na demonstração da proposição I.4.4,

$$[\Delta_R(G_{c-1})RG]^\lambda = \Delta_R^\lambda(G_{c-1})RG$$

e portanto

$$\Delta_R^{\lambda^c}(G) \subseteq [\Delta_R(G_{c-1})RG]^\lambda = \Delta_R^\lambda(G_{c-1})RG = 0. \quad \square$$

Teorema III.2.3 Seja G um grupo finito e R um anel comutativo tal que para todo primo p que divide $|G|$ tem-se que:

$$\bigcap_{n \in \mathbb{N}} p^n R = 0.$$

Então existe um inteiro positivo c tal que $\Delta_R^{\lambda^c}(G) = 0$, se e só se G é solúvel.

Prova: Se G é solúvel, do Lema III.2.7 vem diretamente que:

$$\Delta_R^{\lambda^c}(G) = 0.$$

Se G não é solúvel, G contém um subgrupo nor-

mal, perfeito, não trivial N . Procedendo como na demonstração do Teorema II.3.4 concluímos que

$$\Delta_R^2(N) = \Delta_R(N) \subseteq \Delta_R(G)$$

e portanto

$$0 \neq \Delta_R(N) \subseteq \Delta_R^{\lambda^c}(G)$$

para todo $c \in \mathbb{N}^*$. □

III.3 Ideais idempotentes em RG

Definição III.3.1 Um conjunto de geradores $\{x_1, \dots, x_n\}$ de um ideal de um anel R chama-se um conjunto centralizante de geradores se:

- (i) $x_1 \in C(R)$, o centro de R e
- (ii) $x_i + (x_1, \dots, x_{i-1}) \in C(R / (x_1, \dots, x_{i-1}))$ para $2 \leq i \leq n$, onde $(x_1, \dots, x_{i-1})$ indica o ideal bilateral de R gerado pelo conjunto $\{x_1, \dots, x_{i-1}\}$.

J. E. Roseblade provou em [18] que se G é um grupo nilpotente finitamente gerado e $I \subseteq \mathbb{Z}G$ é um ideal bilateral, então I possui um conjunto centralizante de geradores.

O próximo lema será utilizado para dar uma generalização do resultado obtido por T. Akasaki em [14].

Lema III.3.1 Seja G um grupo nilpotente finitamente gerado. Sejam A e M ideais de $\mathbb{Z}G$ tais que $A \subseteq AM$. Então,

existe um elemento $m \in M$ tal que $(1-m)A = 0$.

Prova: Seja $\{x_1, \dots, x_n\}$ um conjunto centralizante de geradores de A , escritos na ordem contrária, i.e., $x_n \in C(R)$

$x_{n-1} + (x_{n-i+1}, \dots, x_n) \in C(R / (x_{n-i+1}, \dots, x_n)) \quad 1 \leq i \leq n-1$.

Notaremos $A_i = (x_i, \dots, x_n)$, $1 \leq i \leq n$, o ideal de R gerado por $\{x_i, \dots, x_n\}$.

Exibiremos, por indução, elementos $m_i \in M$ tais que

$$(1-m_i)A \subseteq A_i, \quad 1 \leq i \leq m.$$

Para $i = 1$ tomamos $m_1 = 0$.

Suponhamos já ter encontrado $m_1, \dots, m_i$ com a propriedade requerida. Então $A \subseteq AM$ e $(1-m_i)A \subseteq A_i$ nos dá

$$(1-m_i)A \subseteq (1-m_i)AM \subseteq A_i M \subseteq M A_{i+1} \quad (\text{mod } A_{i+1})$$

(Basta notar que $A_i = (x_i, \dots, x_n)$, $A_{i+1} = (x_{i+1}, \dots, x_n)$, $x_i + (x_{i+1}, \dots, x_n) \in C(R / (x_{i+1}, \dots, x_n))$, $A_i = [x_i, A_{i+1}]$).

Assim,

$$(1-m_i)x_i = \sum_{j=1}^n m_{ij} x_j \quad \text{com } m_{ij} \in M.$$

Portanto

$$(1-m_i-m_{ii})x_i \in A_{i+1}$$

e podemos tomar

$$(1-m_{i+1}) = (1-m_i-m_{ii})(1-m_i).$$

Então:

$$(1 - m_{i+1})A = (1 - m_i - m_{ii})(1 - m_i)A \subseteq (1 - m_i - m_{ii})A_i \subseteq A_{i+1}.$$

Finalmente, notamos que tomando $A_{n+1} = 0$ e refazendo o argumento acima resulta, de forma análoga que, tomando $(1 - m_{n+1}) = (1 - m_n - m_{nn})(1 - m_n)$ vem que:

$$(1 - m_{n+1})A = 0.$$

□

Precisamos, ainda, dos teoremas abaixo:

Teorema III.3.2 (Baer) [29] Seja G um grupo nilpotente tal que o quociente de G pelo subgrupo comutador é finitamente gerado. Então, todos os fatores da série central descendente de G são finitamente gerados e G satisfaz a condição maximal para subgrupos. (Veja também [38], pg 232).

Teorema III.3.3 ([30], pg 155) Um grupo nilpotente G é supersolúvel se e só se satisfaz a condição maximal para subgrupos.

Finalmente, podemos generalizar [14].

Teorema III.3.4 Seja G um grupo nilpotente finitamente gerado. Então ZG não contém ideais idempotentes não triviais.

Prova: Seja I um ideal idempotente de ZG . Tomando $A = M = I$, pelo Lema III.3.1 existe $i \in I$ tal que $(1-i)I=0$, logo $i^2 = i$ e, como G é supersolúvel, do teorema I.4.11

vem que $i=0$ ou $i=1$; consequentemente $I=0$ ou $I = \mathbb{Z}G$. $\square$

Observação É natural se perguntar se o resultado acima pode se estender a grupos nilpotentes quaisquer. A resposta a esta questão é negativa.

De fato, em [19], demonstra-se que se G é um grupo abeliano divisível, com torção, então

$$\Delta_{\mathbb{Z}}^2(G) = \Delta_{\mathbb{Z}}^4(G) \neq 0.$$

Vamos provar, agora, o resultado central desta seção.

Teorema III.3.5 Seja G um grupo finito e R um anel comutativo tal que para todo primo p que divide $|G|$ tem-se que

$$\bigcap_{n \in \mathbb{N}} p^n R = 0.$$

Então, $\Delta_R(G)$ não contém um ideal idempotente não nulo se e só se G é solúvel.

Prova: Seja G finito solúvel e $I^2 = I \subseteq \Delta_R(G)$ um ideal de RG . Pelo teorema III.2.8 existe $c \in \mathbb{N}^*$ tal que $\Delta_R^{\lambda^c}(G) = 0$, logo deve ser $I = 0$.

Reciprocamente, se G não for solúvel, existe um subgrupo normal $N \neq \{1\}$, perfeito, de G . Então $\Delta_R(G, N) \subseteq \Delta_R(G)$ e do teorema II.3.4 vem que:

$$\Delta_R(N) = \Delta_R^2(N) \neq 0$$

e conseqüentemente

$$\Delta_R^2(G, N) = [\Delta_R(N)RG]^2 = \Delta_R^2(N)RG = \Delta_R(N)RG = \Delta_R(G, N) . \quad \square$$

Corolário III.3.6 Seja G um grupo finito. Então $\Delta_{\mathbb{Z}}(G)$ não contém um ideal idempotente não trivial se e só se G é solúvel.

III.4 Ideais idempotentes de $\mathbb{Z}G$

Definição III.4.1 Um grupo finito G é chamado *p-solúvel* se possui uma série normal $\{1\} = G_0 \leq G_1 \leq \dots \leq G_n = G$ na qual cada fator G_{i+1}/G_i ou é um p -grupo ou tem ordem prima com p .

O teorema abaixo pode ser encontrado em [33], pg 139.

Teorema III.4.1 Seja G um grupo finito solúvel. Então G é p -solúvel para todo primo p .

Lema III.4.2 Seja R um domínio de Dedekind cujo corpo quociente K é um corpo de números algébricos e seja G um grupo finito. Se e é um idempotente de RG tal que o ideal RGe é bilateral, então e é um elemento central.

Prova: Seja $I = RGe$ bilateral tal que $e^2 = e$. Então $I^K = K \otimes_R I = K \otimes_R RGe$ é um ideal bilateral de KG . Como KG é semi-simples, existe $e_1 \in KG$, idempotente central, tal que

$$KGe = KGe_1.$$

Suponhamos que $e \neq e_1$. Se isto acontece, $e_1 - e \neq 0$ é um idempotente de KG .

De fato,

$$(e_1 - e)^2 = e_1^2 - 2e_1e + e^2 = e_1 - e$$

pois $e_1e = e$, como consequência de e_1 ser unidade de KGe_1 .

Temos também, que $e_1(e - e_1) = 0$, pois e é unidade de KG e $e_1 \in KGe$.

Portanto:

$$KGe_1 = KGe = KGe_1 \otimes KG(e - e_1),$$

onde $KG(e - e_1) \neq 0$, um absurdo. Logo $e_1 = e$. $\square$

Para o próximo teorema precisaremos do seguinte resultado:

Teorema III.4.3 (Fong e Swan) ([37], teorema 5) Seja R um domínio de Dedekind de característica zero com corpo de quocientes K . Seja G p -solúvel para todo primo racional $p \nmid U(R)$. Então um KG -módulo L é da forma $K \otimes_R P$ onde P é um RG -módulo projetivo se e só se o caracter χ de L verifica $\chi(x) = 0$ para todo $x \in G$ tal que $o(x) \nmid U(R)$.

Teorema III.4.4 Seja R um domínio de Dedekind local cujo corpo de quocientes K é um corpo de números algébricos e G um grupo finito que é p -solúvel para todo primo $p \nmid U(R)$.

Suponhamos ainda que K é um corpo de decomposição para G . Então, se I é um ideal bilateral idempotente de RG tal que existe um RG -módulo projetivo P , finitamente gerado, verificando $KI \cong KP$, então existe um idempotente central $e \in RG$ tal que $I = RGe$.

Prova: Seja R local com ideal maximal P . Então $P \cap \mathbb{Z} = p\mathbb{Z}$ para algum primo $p \in \mathbb{Z}$ e, em particular, o grupo G é p -solúvel. Se $J(RG)$ é o radical de Jacobson de RG , a imagem de I em $RG/J(RG)$, $\bar{I}$, é um ideal bilateral, idempotente, não nulo de $RG/J(RG)$.

De fato, se fosse $I \subseteq J(RG)$, como existe um inteiro positivo m tal que $[J(RG)]^m \subseteq J(R)RG$ ([37], pg 2.5), ter-se-ia que:

$$I \subseteq J(R)RG.$$

Logo, para todo inteiro positivo n

$$I = I^n \subseteq J(R)^n RG \quad e$$

$$I = \bigcap_{n \in \mathbb{N}^*} I^n \subseteq \bigcap_{n \in \mathbb{N}^*} J(R)^n RG = \left[\bigcap_{n \in \mathbb{N}^*} J(R)^n \right] RG.$$

Mas R é um anel comutativo noetheriano, portanto:

$$\bigcap_{n=1}^{\infty} J(R)^n = 0 \quad ([27], \text{pg } 270),$$

logo $I = 0$, um absurdo.

Seja $\hat{R}$ o completado de R segundo a topologia de

finida a partir do ideal $J(R)$.

Temos então que

$$RG / J(RG) \cong \hat{R}G / J(\hat{R}G) .$$

Como $\hat{R}G / J(\hat{R}G)$ é artiniano ([35], pg 187) também $RG / J(RG)$ é um anel artiniano e consequentemente semi-simples. Logo

$$\bar{I} = (RG / J(RG)) \bar{e}$$

onde $\bar{e}$ é um idempotente central de $RG / J(RG)$.

Agora, $\bar{e}$ pode ser levantado a um idempotente e em RG ([35], pg 189) e então temos:

$$(1.1) \quad I + J(RG) = RGe + J(RG) .$$

Multiplicando a igualdade (1.1) por e , à direita, obtemos:

$$Ie + J(RG)e = RGe + J(RG)e = RGe .$$

Mas $J(RG)e = J(RGe)$ ([39], pg 196).

Assim, como RGe é um RG -módulo finitamente gerado, pelo Lema de Nakayama temos que:

$$Ie = RGe .$$

Ainda, como

$$I = Ie \oplus I(1-e) ,$$

vem que:

$$(1.2) \quad I = RGe \oplus I(1-e) .$$

Observamos que $I(1-e) \subseteq J(RG)$ pois, se $\alpha \in I(1-e)$, de (1.2) vem que $\alpha = x - y$ com $x \in I$ e $y \in RGe$. De (1.1) $x - y \in J(RG)$.

Provaremos agora que $I(1-e) = 0$. Se tal não acontece, como I é idempotente, temos:

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

com

$$\begin{aligned} RGe RGe + I(1-e)RGe &\subseteq RGe \quad e \\ RGe I(1-e) + I(1-e) I(1-e) &\subseteq I(1-e) . \end{aligned}$$

Logo:

$$(1.3) \quad RGe RGe + I(1-e)RGe = RGe$$

$$(1.4) \quad RGe I(1-e) + I(1-e) I(1-e) = I(1-e) .$$

Observamos, agora, que:

- (i) $I(1-e)RGe \subseteq J(RG)RGe \subseteq J(RG)e = J(RGe)$
- (ii) $I(1-e) I(1-e) \subseteq J(RG) I(1-e) \subseteq J(I(1-e))$ onde $I(1-e)$ é um RG -módulo finitamente gerado por ser um submódulo do RG -módulo noetheriano $RG(1-e)$.

Assim, aplicando o Lema de Nakayama em (1.3) e

(1.4) obtemos:

$$RGe RGe = RGe \quad e$$

$$(1.5) \quad RGe I(1-e) = I(1-e) .$$

Seja $\{y_1, \dots, y_s\}$ um conjunto finito de geradores de $I(1-e)$ como RG -módulo. Pela relação (1.5), cada y_i , $1 \leq i \leq s$, pode ser escrito na forma:

$$y_i = \sum_{j=1}^{m(i)} x_j u_{ij} \quad \text{onde } x_j \in RGe \text{ e } u_{ij} \in I(1-e).$$

Assim, chamando $t = \sum_{i=1}^s m(i)$, temos que a aplicação:

$$\phi: \bigoplus_{i=1}^t RGe \longrightarrow I(1-e)$$

definida por:

$$(\alpha_{11}, \dots, \alpha_{1m(1)}, \dots, \alpha_{s1}, \dots, \alpha_{sm(s)}) \longmapsto \sum_{k=1}^s \sum_{i=1}^{m(k)} \alpha_{ki} u_{ki}$$

é um epimorfismo de RG -módulos.

Como $I = Ie \oplus I(1-e)$, multiplicando a igualdade tensorialmente por K , vem que:

$$K I e \oplus K I (1-e) = K I \cong K P$$

onde $K P$ é um KG -módulo projetivo.

Assim, como $L = K I (1-e)$ é somando direto de $K P$, também é KG -projetivo e considerando a sequência

$$(K G e)^{(t)} \xrightarrow{1 \otimes \phi} K I (1-e) \longrightarrow 0$$

concluimos que existe um KG -módulo L_1 tal que:

$$(1.6) \quad (K G e)^{(t)} = L \oplus L_1.$$

Representaremos por χ , χ_L e χ_{L_1} os respectivos caracteres associados à decomposição acima.

Da igualdade

$$I = Ie \oplus I(1-e)$$

concluimos que

$$KI \cong K Ie \oplus KI(1-e) ,$$

e notando por χ_I e χ' os caracteres associados aos KG-módulos KI e $K Ie$ temos que:

$$\chi_I = \chi' + \chi_L .$$

Observemos agora que:

(iii) $Ie = RGe$ e $K Ie = K \otimes_R RGe$, onde RGe é um RG-módulo projetivo

(iv) $KI \cong KP$, onde P é um RG-módulo projetivo.

Portanto, pelo teorema de Fong e Swan, para todo $x \in G$ com $o(x) \nmid U(R)$ temos

$$0 = \chi_I(x) = \chi'(x) + \chi_L(x) = 0 + \chi_L(x) ,$$

logo $\chi_L(x) = 0$.

Ainda, pelo teorema de Fong e Swan, existe um RG-módulo projetivo Q tal que:

$$(1.7) \quad KI(1-e) = K \otimes_R Q .$$

Notemos que:

$$(KGe)^{(t)} \cong K \otimes_R (RGe)^{(t)} .$$

Consequentemente, para todo $x \in G$ com $o(x) \notin U(R)$ temos que $\chi(x) = 0$. Assim, se $x \in G$ com $o(x) \notin U(R)$

$$0 = \chi(x) = \chi_L(x) + \chi_{L_1}(x) = 0 + \chi_{L_1}(x) \quad e$$

$$\chi_{L_1}(x) = 0.$$

Novamente, pelo teorema de Fong e Swan, existe um RG-módulo projetivo Q_1 tal que:

$$(1.8) \quad L_1 = K \otimes_R Q_1.$$

Substituindo (1.7) e (1.8) em (1.6) conseguimos:

$$K \otimes_R (RGe)^{(t)} \cong K \otimes_R (Q \oplus Q_1).$$

Conforme o teorema 76.17 ([34]),

$$(RGe)^{(t)} \cong Q \oplus Q_1$$

e, como vale o teorema de Krull-Schmidt para RG-módulos ([34], pg 541), todo somando direto de Q é somando direto de RGe .

Do fato de K ser R -plano, temos também que:

$$K \otimes_R Q = L = KI(1-e) = K \otimes_R I(1-e) \subseteq K \otimes_R RG(1-e) = KG(1-e)$$

e como KG é semi-simples, $K \otimes_R Q$ é somando direto de $KG(1-e)$. Desse modo, se M é somando direto de Q , $K \otimes_R M$ é somando direto de $KG(1-e)$.

Assim, temos que:

$$KG(1-e) = (K \otimes_R M) \otimes \bar{N}$$

com $\bar{N} = K \otimes_R N$, onde N é um RG -módulo ([37], pg 3.13).

Então,

$$KG(1-e) \cong K \otimes_R (M \otimes N)$$

e pelo teorema 76.17 de [34] vem que:

$$RG(1-e) \cong M \otimes N.$$

Portanto, todo somando direto X de Q é somando direto de $RG(1-e)$ e conseqüentemente, um somando direto comum a RGe e $RG(1-e)$. Assim

$$Xe \subseteq RG(1-e)e = 0$$

$$X(1-e) \subseteq RGe(1-e) = 0$$

logo $X \cdot 1 = 0$; o que implica $Q = 0$, um absurdo.

Desse modo $I(1-e) = 0$, $I = RGe$ e pelo Lema III.4.2, e é central. □

Teorema III.4.5 O teorema III.4.4 vale também quando R não é local.

Prova: Seja R um domínio de Dedekind com corpo quociente K , que é um corpo de números algébricos e um corpo de decomposição para G . Seja G p -solúvel para todo primo racional $p \notin U(R)$ e I um ideal bilateral, idempotente, tal que $K \otimes_R I \cong K \otimes_R P$ para um RG -módulo projetivo P .

Se P é um ideal maximal de R , denotaremos por R_P a localização em P . Assim, $pZ = P \cap Z$ e G é p -solúvel pois $P \nsubseteq R$. Podem ocorrer, então, as duas seguintes situações:

$$(i) \quad p \mid |G|$$

Neste caso $P \mid |G|R$ e conforme o teorema III.4.4 $R_P \otimes_R I = R_P G e_P$, onde e_P é um idempotente central de $R_P G$.

$$(ii) \quad p \nmid |G|$$

Neste caso $P \nmid |G|R$ e conforme o teorema 4.8 de [35], $R_P G$ é uma ordem separável e $R_P \otimes_R I = R_P G e_P$, para um idempotente central e_P .

Portanto, como no Lema III.4.2

$$K \otimes_R (R_P \otimes_R I) = K \otimes_R (R_P G e_P) = K G e_P = K G e$$

e $e = e_P$, onde e é um idempotente central de KG . Assim, conforme [35], pg 51

$$I = \bigcap_{P \in \max R} R_P \otimes_R I = \bigcap_{P \in \max R} R_P G e = \bigcap_{P \in \max R} R_P \otimes_R R G e = R G e.$$

Isto prova o teorema III.4.5. □

Teorema III.4.6 O teorema III.4.5 vale também quando K não é um corpo de decomposição de G .

Prova: Seja K_0 , uma extensão finita de K , um corpo de decomposição para G e R_0 o fecho inteiro de R em K_0 .

Então, qualquer que seja o primo racional p , $p \in U(R)$ se e só se $p \in U(R_0)$.

De fato, se $p \in U(R_0)$ existe $f \in R[X]$, irreduzível, unitário, tal que $f(1/p) = 0$. Seja $f = X^n + a_j X^{n-j} + \dots + a_{n-1} X + a_n$ onde j é o menor inteiro positivo tal

que $a_j \neq 0$.

Assim,

$$f(1/p) = 1/p^n + a_j/p^{n-j} + \dots + a_{n-1}/p + a_n = 0$$

$$1 + a_j p^j + a_{j+1} p^{j+1} + \dots + a_{n-1} p^{n-1} + a_n p^n = 0$$

$$p(-a_j p^{j-1} - a_{j+1} p^j - \dots - a_{n-1} p^{n-2} - a_n p^{n-1}) = 1$$

e $p \in U(R)$. Consequentemente G e R_0 estão nas condições do teorema III.4.5.

Seja I um ideal bilateral idempotente de RG . Então $I^{R_0} = R_0 \otimes_R I$ é um ideal ibilateral, idempotente, de $R_0 G$. Do teorema III.4.5 vem que $I^{R_0} = R_0 G e$ é um idempotente central de $R_0 G$.

Temos também que I^K é um ideal bilateral de KG e, como KG é semi-simples, $I^K = K G e_1$, onde e_1 é um idempotente central de KG . Assim, por um lado

$$I^{K_0} = (I^K)^{K_0} = K_0 G e_1$$

e por outro

$$I^{K_0} = (I^{R_0})^{K_0} = (R_0 G e)^{K_0} = K_0 G e. \quad (2.1)$$

Agora, de modo análogo à prova do Lema III.4.2, concluímos que $e = e_1 \in KG$.

Portanto $e \in KG \cap R_0 G = RG$.

Provemos agora que $I = I^{R_0} \cap RG$.

Levando em conta que RG é um R -módulo finitamente gerado e que R é um domínio de Dedekind, concluímos que I também é um R -módulo finitamente gerado. Ainda, como RG é R -livre de torção, I também é R -livre de torção. Assim, por [34], pg 147

$$I \cong \bigoplus_{i=1}^k I_i^*$$

onde $I_i^* = \alpha_i^* \alpha_i^*$ com $\alpha_i^* \in K$ e α_i^* ideal inteiro de R , $1 \leq i \leq k$. Portanto,

$$I = \bigoplus_{i=1}^k I_i$$

onde $I_i = \alpha_i \alpha_i$ com $\alpha_i \in RG$ e α_i ideal de R , $1 \leq i \leq k$.

Observemos que, como $RG \subseteq KG$, $I^{R_0} \cap RG = (I^{R_0} \cap KG) \cap RG$. Também, do fato que:

- (i) K e K_0 são R -planos
- (ii) I é R -projetivo, pois R é hereditário e

$$I = \bigoplus_{i=1}^k I_i$$

concluímos que são válidas as inclusões abaixo:

$$R \otimes_R I \hookrightarrow K \otimes_R I \hookrightarrow K \otimes_R RG \hookrightarrow K_0 \otimes_R RG = K_0 G.$$

Agora,

$$R_0 \otimes_R I = R_0 \otimes_R \left(\bigoplus_{i=1}^k \lambda_i \alpha_i \right) \cong \bigoplus_{i=1}^k R_0 \lambda_i \alpha_i .$$

Seja $\alpha \in (I^{R_0} \cap KG) \cap RG$. Então $\alpha \in I^{R_0} \cap KG$ e $\alpha = \sum_{i=1}^k a_i \alpha_i$

com $a_i \in (R_0 \lambda_i) \cap K$, $1 \leq i \leq k$. Mas, conforme [34], pg 130

$R_0 \lambda_i \cap K = \lambda_i$ e portanto

$$(I^{R_0} \cap KG) \cap RG \subseteq \left(\bigoplus_{i=1}^k \lambda_i \alpha_i \right) \cap RG = I .$$

Sendo a inclusão contrária imediata, concluímos que:

$$I = I^{R_0} \cap RG . \quad (2.2)$$

Finalmente, de (2.1) e (2.2)

$$I = I^{R_0} \cap RG = (R_0 G e) \cap RG = R_0 G e \cap R G e = R G e ,$$

a última igualdade sendo consequência de que $RG \subseteq R_0 G$. $\square$

Teorema III.4.7 Seja G um grupo solúvel finito e R um domínio de Dedekind com corpo quociente K , um corpo de números algébricos, tal que nenhum divisor primo de $|G|$ seja inversível em R . Então, RG não possui ideais bilaterais, idempotentes, próprios.

Prova: Seja I um ideal bilateral, idempotente. Faremos a demonstração por indução sobre a ordem de G .

Demonstraremos primeiro que $K \otimes_R I = KG$.

Seja N um p -subgrupo normal de G . Então, se $N = \Delta_R(N)RG$, temos uma sequência exata de RG -módulos

$$E_1 : 0 \longrightarrow N \xrightarrow{1} RG \xrightarrow{\phi} R\bar{G} \longrightarrow 0$$

onde $\bar{G} = G/N$. Esta sequência induz uma sequência exata

$$E_2 : 0 \longrightarrow J \xrightarrow{1} I \xrightarrow{\phi|_I} I_1 \longrightarrow 0$$

onde $J = \text{Ker}(\phi|_I)$ e I_1 é um ideal bilateral, idempotente, de $R\bar{G}$.

Por indução $I_1 = 0$ ou $I_1 = R\bar{G}$.

Seja agora P um ideal maximal de R que contém pR e localizemos R em P . Então, mostraremos que $\Delta_{R_P}(N)$ está contido em $J(R_P N)$.

De fato, sabemos que:

- (i) $PR_P N \subseteq J(R_P N)$ ([37], pg 2.5)
- (ii) Seja S um anel e I um ideal bilateral de S . Se $I \subseteq J(S)$ e $\bar{a} \in J(S/I)$ então $a \in J(S)$, como se pode facilmente verificar.

Assim,

$$R_P N / PR_P N \cong (R_P / PR_P)N \cong F_P N$$

e para todo $n \in N$ $1-n \in J(F_P N)$. Utilizando (i) e (ii) vem que $1-n \in J(R_P N)$ e portanto $\Delta_{R_P}(N) \subseteq J(R_P N)$.

Localizemos as sequências exatas E_1 e E_2 em P .

Se $R_P \otimes_R I_1 = 0$, então:

$$0 \longrightarrow R_p \otimes_R J \longrightarrow R_p \otimes_R I \longrightarrow 0 \longrightarrow 0 \quad e$$

$$R_p \otimes_R I \cong R_p \otimes_R J .$$

Porém, existe um inteiro positivo m tal que $[J(R_p N)]^m \subseteq PR_p N$ ([37], pg 2.5) e assim temos que $[\Delta_{R_p}(N)]^m \subseteq PR_p N$.

Também, como $N \trianglelefteq G$, para todo $k \in \mathbb{N}^*$ temos que $[\Delta_{R_p}(N) R_p G]^k = \Delta_{R_p}^k(N) R_p G$; logo existe $r \in \mathbb{N}^*$ tal que $[\Delta_{R_p}(N) R_p G]^r \subseteq PR_p G$.

Mas, então, de

$$J \subseteq N = \Delta_R(G, N)$$

concluimos que $R_p \otimes_R J \subseteq N_p = \Delta_{R_p}(N) R_p G$ e que $R_p \otimes_R I$ é nilpotente módulo P , o que é absurdo pois $R_p \otimes_R I$ é idempotente e $P \not\subseteq P^2 \not\subseteq P^3 \subseteq \dots$. Logo isto não pode acontecer e $R_p \otimes_R I_1 = R_p \bar{G}$.

Desse modo, a partir das sequências exatas

$$\begin{array}{ccccccc} E_3 : & 0 & \longrightarrow & N_p & \longrightarrow & R_p G & \longrightarrow & R_p \bar{G} & \longrightarrow & 0 & e \\ & & & & & & & \text{III} & & & \\ E_4 : & 0 & \longrightarrow & R_p \otimes_R J & \longrightarrow & R_p \otimes_R I & \longrightarrow & R_p \otimes_R I_1 & \longrightarrow & 0 \end{array}$$

concluimos que:

$$R_p \otimes_R I + \Delta_{R_p}(N) R_p G = R_p G .$$

De fato, se $\alpha \in R_p G$ existe $m \in R_p \otimes_R I$ tal que $\bar{\alpha} = \bar{m}$, onde $\bar{m} \in R_p \bar{G}$. Logo $\bar{\alpha} - \bar{m} = \bar{0}$ ou $\alpha - m \in N_p$, ficando provada a afirmação.

Mas $R_p G$ é um $R_p G$ -módulo finitamente gerado e $\Delta_{R_p}(N) R_p G \subseteq J(R_p G)$. Logo, pelo lema de Nakayama vem que $R_p \otimes_R I = R_p G$. Portanto $KI = KG$. Isto prova a afirmação inicial.

Aplicando agora o teorema III.4.6, vem que $I = RGe$ para um idempotente central $e \in RG$. Mas então $e = 1$ pois, pelo teorema I.3.7 ou pelo teorema de Coleman RG é indecomponível. $\square$

BIBLIOGRAFIA

- [1] - R.G. SWAN, Induced representations and projective modules. Ann. of Math. 71, 552-578, 1960.
- [2] - D.B. COLEMAN, Idempotents in group rings. Proc. Amer. Math. Soc. 17, 962, 1966.
- [3] - A.A. BOVDI and S.V. MIHOVSKI, Idempotents in crossed products. Dokl. Akad. Nauk. S.S.S.R 195, Soviet. Math. Dok. 11, 1439-1442, 1970.
- [4] - S.K. SEHGAL and H. ZASSENHAUSS, Group rings without nontrivial idempotents. (to appear).
- [5] - M.M. PARMENTER and S.K. SEHGAL, Idempotents elements and ideals in group rings and the intersection theorem. Arch. Math. 24, 586-600, 1973.
- [6] - D.S. PASSMAN, Infinite group rings. Marcel Dekker, New York, 1971.
- [7] - A.E. ZALESSKII, On a problem of Kaplansky. Soviet. Math. 13, 449-452, 1972.
- [8] - I. HERSTEIN and L. SMALL, Nil rings satisfying certain chain conditions: an addendum. Can J. of Math. 18, 300-302, 1966.
- [9] - G. RENAULT, Algèbre non Commutative. Gauthier-Villars Éditeur, 1975.

- [10] - IRVING KAPLANSKY, Commutative rings. Allyn and Bacon, Inc., Boston, 1970.
- [11] - E. FORMANEK, A short proof of a theorem of Jennings. Proc. Amer. Math. Soc. 26, 405-407, 1970.
- [12] - D.J.S. ROBINSON, Finiteness conditions and generalized soluble groups. Berlin, 1972.
- [13] - S.D. BERMAN, On the equation $x^m = 1$ in a integral group ring. Ukranian Math. Z 7, 253-261, 1955.
- [14] - T. AKASAKI, Idempotent ideals in integral group rings. J. Algebra 23, 343-346, 1972.
- [15] - T. AKASAKI, Idempotent ideals in integral group rings II. Arch. Math., 24, 126-128, 1973.
- [16] - K.W. ROGGENKAMP, Integral group rings of solvable finite groups have no idempotent ideals. Arch. Math. 25, 125-128, 1974.
- [17] - B. HARTLEY, The residual nilpotence of wreath products. Proc. London Math. Soc. 3, 20, 365-392, 1970.
- [18] - J.E. ROSEBLADE, The integral group rings of hypercentral groups. Bull. London Math. Soc. 3, 351-355, 1971.
- [19] - K.W. GRUENBERG, Cohomological topics in group theory. Lec. Notes in Math., 143, Berlin, 1970.
- [20] - R.G. BURNS, Central idempotents in group rings. Can. Math. Bull. 13, 527-528, 1970.
- [21] - I.G. CONNELL, On the group ring. Can. J. of Math. 15, 650-685, 1963.

- [22] - C. MOSER, Representation de -1 comme somme de carrés dans un corps cyclotomique quelconque. J. Number Theory 5, 139-141, 1973.
- [23] - R.G. AYOUB, C. AYOUB, On the group ring of a finite abelian group. Bull. Austral. Math. Soc. 1, 245-265, 1969.
- [24] - L.H. JACY MONTEIRO, Teoria de Galois. Instituto de Pesquisas Matemáticas, USP, 1969.
- [25] - S.K. SEHGAL, Certain algebraic elements in group rings. Arch. Math. 26, 139-143, 1975.
- [26] - D.S. PASSMAN, What is a group ring? Amer. Math. Monthly 83, 3, 173-185, 1976.
- [27] - L. DORNHOFF, Group representation theory. Part B. Marcel Dekker, Inc., New York, 1972.
- [28] - E. FORMANEK, The zero divisor question for supersolvable groups. Bull. Austral. Math. Soc. 9, 69-71, 1973.
- [29] - R. BAER, Representations of groups as quotient groups. Trans. Amer. Math. Soc. 58, 295-419, 1945.
- [30] - W.R. SCOTT, Group theory. Prentice Hall, Inc., Englewood Cliffs, New Jersey, 1964.
- [31] - FRANCISCO CESAR P. MILIES, Anéis de Grupos. IV Escola de Álgebra, USP, 1976.
- [32] - OSCAR ZARISKI and PIERRE SAMUEL, Commutative Algebra. Vol. I. Van Nostrand Company, Princeton, 1958.
- [33] - M. HALL, The theory of groups. Mc Millan, New York, 1959.

- [34] - I. REINER and C.W. CURTIS, Representation theory of finite groups and associative algebras. John Wiley & Sons, Inc., 1962.
- [35] - K.W. ROGGENKAMP and VERENA HUBER-DYSON, Lattices over orders I. Springer-Verlag, 115.
- [36] - R.G. SWAN, The Grothendieck ring of a finite group. Topology 2, 85-110, 1963.
- [37] - I. REINER, Topics in integral representation theory. Notas publicadas pela IV Escola de Álgebra, USP, 1976.
- [38] - A. KUROSH, The theory of groups. Vol. II, Chelsea Publishing Co., New York, 1955.
- [39] - KENT R. FULLER and FRANK W. ANDERSON, Rings and Categories of modules. Springer-Verlag Inc., New York, 1973.