IDEAIS EM ANÉIS DE GRUPO: UMA INTRODUÇÃO

César Polcino Milies
Sônia Pitta Coelho

INTRODUÇÃO

Os anéis de grupo fizeram sua aparição muito cedo na história moderna da álgebra abstrata. Eles foram definidos pela primeira vez em 1854 no mesmo artigo de A. Cayley que é hoje considerado a origem da teoria abstrata de grupos. Até então, somente grupos de permutações tinham sido estudados.

Após estudos de T. Molien e dos trabalhos de G.Frobenius sobre números hipercomplexos, o assunto ganha uma nova dimensão quando no período 1927-1929 R. Brauer e sobretudo E. Noether estabeleceram a íntima conexão existente entre a teoria de representações de grupos e a estrutura de álgebras usando decisivamente, para tanto, o conceito de anel de grupo (a este respeito, veja por exemplo [11]).

Finalmente, a partir dos anos 40 o assunto adquire relevância em si mesmo, quando as propriedades algébricas destas estruturas começam a ser cuidadosamente investigadas.

O leitor encontrará mais detalhes sobre o desenvolvimento histórico da teoria em [6], [15] e [16].

Talvez valha a pena observar que a estrutura algébrica dos anéis de grupo é particularamente rica. Para explorá-la é necessário recorrer a técnicas da teoria dos números algébricos, de representações de grupos e álgebras, de teoria de anéis ou teoria de grupos e até, de álgebra homológica.

Esta foi uma das razões que nos levaram a oferecer o presente curso numa Escola de Álgebra; acreditamos que o jovem que começa a estudar a matéria, iniciando-se na pós graduação, muito se beneficiará de abordar um assunto que mostra a interligação entre as distintas diciplinas algébricas, em vez de vê-las como compartimentos estanques.

Nestas notas damos especial atenção ao estudo de ideais em anéis de grupo e, consequentemente, a teoria de anéis terá um peso maior na nossa abordagem; porém, o peso da teoria dos grupos não deixa de ser aparente.

Existem em língua inglesa quatro textos que abordam aspectos gerais dos anéis de grupo, devidos a G. Karpilovsky [9] - I.B.S., Passi [12], D.S. Passman [13] e S.K. Seghal [18]. A leitura de qualquer um deles abrirá, ao leitor interessado, as portas que o levarão até problemas de pesquisa ainda em aberto e, em particular, o texto de D.S. Passman, pelo seu caráter quase enciclopédico, mostrará as conexões do assunto com um vastíssimo universo algébrico.

Agradecemos à comissão organizadora da VIII Escola de Álgebra pelo convite para ministrar este curso e à Srta. Antonia Soares pela cuidadosa datilografia das notas.

oOo

ANÉIS DE GRUPO

§1. Breve introdução histórica

Em 1843, Sir William Rowan Hamilton publicou seu primeiro artigo sobre Quatérnios; como se sabe este viria a ser um dos fatores determinantes do nascimento da Álgebra Abstrata.

Hamilton tentava extender algumas de suas idéias anteriores sobre números complexos para desenvolver um "cálculo com vetores de três dimensões". Estas tentativas o levaram gradualmente a introduzir o conceito de "quatérnio". i.e. a trabalhar com o conjunto dos elementos da forma:

$$a + bi + cj + dk$$

onde a,b,c,d são números reais e os símbolos i,j,k deviam desempenhar um papel semelhante àquele do i entre os números complexos.

Era natural somar elementos desta forma somando coeficientes, isto é, de acordo com a seguinte regra:

$$(a+bi+cj+dk)+(a'+b'i+c'j+d'k)=(a+a')+(b+b')i+(c+c')j+(d+d')k.$$

Hamilton assumiu implicitamente que deveria valer a propriedade distributiva e, para definir o produto de dois destes elementos, precisaria apenas decidir como multiplicar os símbolos i,j,k entre si. As regras que achou parecem-nos hoje muito razoáveis, já que lembram as regras do produto vetorial:

$$i^2 = j^2 = k^2 = -1 \qquad jk = i = -ki$$

$$ij = k = -ji \qquad ki = j = -ik\ .$$

Seguindo os passos de Hamilton, muitos matemáticos começaram a procurar outros "sistemas hipercomplexos" ou, como diríamos na terminologia atual, álgebras de dimensão finita sobre o corpo real ou complexo.

Definia-se um sistema hipercomplexo como o conjunto de todos os elementos da forma:

$$x_1e_1 + x_2e_2 + \ldots + x_ne_n$$

onde $x_1, x_2, \ldots, x_n$ são números reais (ou complexos) e $e_1, e_2, \ldots, e_n$ são símbolos, chamados as unidades básicas do sistema. Por analogia com os quatérnios, a soma de duas expressões desta forma se definia somando coeficientes:

$$\left(\sum_{i=1}^{n} x_ie_i\right) + \left(\sum_{i=1}^{n} y_ie_i\right) = \sum_{i=1}^{n} (x_i+y_i)e_i \ .$$

Da mesma forma, para definir o produto de dois destes elementos, bastaria definir todos os produtos e_ie_j, $1 \leq i,j \leq n$ e extender, distributivamente. Como o produto e_ie_j deve ser ainda um elemento deste conjunto, ele deve poder se escrever na forma:

$$e_ie_j = \sum_{k=1}^{n} \gamma_k(i,j)e_k$$

Assim, o produto estaria determinado ao definir os valores dos coeficientes $\gamma_k(i,j)$, que por causa disso eram chamados as *constantes estruturais* do sistema.

Em pouco tempo foram descobertos muitos "sistemas hipercomplexos" novos e gradualmente se começou a sentir a necessidade de achar uma "classificação". Num artigo de 1870, publicado em litografia em 1871 (e, em forma final, em 1881 no primeiro número do American Journal of Mathematics), cujo título era precisamente

"*Álgebras Lineares Associativas*", Benjamin Peirce tentou uma tal classificação e achou, a menos de isomorfismo, 162 álgebras de dimensão menor ou igual a 6. Nesta primeira exposição organizada de um esboço de teoria, Peirce introduziu algumas das noções que tornariam fundamentais, como o conceito de elemento idempotente e de elemento nilpotente.

No período de 1889-1898 E. Study e G. Scheffers introduziram algumas noções básicas da teoria de estruturade álgebras, inspirando-se no trabalho de classificação de S. Lie e W. Killing para as álgebras de Lie.

Seguindo esta linha de idéias, T. Molien e E. Cartan obtiveram independentemente resultados importantes sobre a estrutura de álgebras de dimensão finita sobre o corpo real ou complexo. Em particular, introduziram as noções de álgebras simples e semisimples e as caracterizaram em termos de álgebras de matrizes.

Pode-se dizer que todo este trabalho culminou com os clássicos teoremas de J.H.M. Wedderburn de 1908 que descrevem a estrutura de álgebras de dimensão finita sobre corpos arbitrários, utilizando técnicas relacionadas com o conceito de elemento idempotente , tal como sugerido no trabalho de Peirce.

É neste contexto, do desenvolvimento da teoria de álgebras, que os anéis de grupo foram definidos e suas primeiras propriedades estudadas.

A primeira definição explícita é de A. Cayley [1], num artigo de 1854 onde aparece também, pela primeira vez, uma definição abstrata do conceito de grupo. Ali, a definiçao de anel de

grupo é dada no parágrafo final e Cayley destaca justamente a analogia com o sistema dos quatérnios.

Porém, a própria teoria de estrutura de álgebras não existia ainda e o conceito passou desapercebido na época.

Em 1892, Molien apresentou sua tese de doutoramento à Universidade de Yurev, na Estonia. Lá ele começou a desenvolver sua teoria de estrutura de álgebras e deu, em particular, um critério para decidir se uma dada álgebra é ou não, semisimples em função das constantes estruturais.

Para poder aplicar este critério, precisava de álgebras cujas constantes estruturais fossem razoavelmente simples e lhe ocorreu então estudar o caso em que as unidades básicas $e_1, e_2, \ldots, e_n$ formam um grupo em relação à multiplicação. Neste caso, o produto $e_i e_j$ seria uma outra unidade básica e_t, consequentemente, dados i,j fixos ter-se-á que $\gamma_t(i,j) = 1$ e $\gamma_k(i,j) = 0$ se $k \neq j$.

Estava considerando então álgebras de grupo (daremos a definição precisa na próxima seção) e, em dois trabalhos subsequentes, de 1897 e 1898 desenvolveu estas idéias aplicando-as à teoria de representações, chegando inclusive a descobrir as chamadas relações de ortogonalidade de caracteres.

Estes resultados, contudo, não tiveram maior impacto na coletividade matemática e muitos deles foram redescobertos posteriormente, a partir de um outro enfoque, por Dedekind, Burnside e Frobenius.

Finalmente, no período de 1927 a 1929, E. Noether e R. Brauer reconheceram a interligação profunda existente entre a teo-

ria de estrutura de álgebras e a teoria de representações de grupos e mostraram que ela pode ser explicitada, precisamente, a partir do conceito de álgebra de grupo.

A partir dessa data eles têm se tornado objeto de estudo tanto pelo seu interesse como estrutura algébrica muito rica como pelas conexões com outras áreas da álgebra.

oOo

§2. Definição e primeiros resultados

A definição de anel de grupo será feita, essencialmente seguindo o modelo dos sistemas hipercomplexos. Apenas deixaremos de lado a idéia de "dimensão finita" e tomaremos coeficientes em famílias mais gerais de anéis.

Sejam G um grupo (não necessariamente finito) e R um anel com unidade. Indicaremos por RG o conjunto de todas as combinações lineares formais do tipo:

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

onde $a(g) \in R$ e apenas um número finito de coeficientes é diferente de zero, i.e. a família $(a(g))_{g \in G}$ é quase nula.

Dado um elemento $\alpha = \sum_{g \in G} a(g)g \in RG$, chama-se *suporte* de α ao conjunto:

$$\text{(2.1)} \qquad \sup(\alpha) = \{ g \in G \mid a(g) \neq 0 \}.$$

Obviamente, $\sup(\alpha)$ é um subconjunto finito de G.

Note que, como estamos trabalhando com expressões formais tem-se que $\sum_{g \in G} a(g)g = \sum_{g \in G} b(g)g$ se e somente se $a(g) = b(g)$, $\forall g \in G$.

Definimos a soma de duas expressões desta forma por:

$$\text{(2.2.)} \qquad \sum_{g \in G} a(g)g + \sum_{g \in G} b(g)g = \sum_{g \in G} (a(g) + b(g))g$$

Também, dados dois elementos $\alpha = \sum_{g \in G} a(g)g$, $\beta = \sum_{g \in G} g(g)g$ definimos seu produto, distributivamente, como a soma de todos os

produtos possíveis de termos da forma a(g)g por termos da forma b(g)g, i.e.:

$$(2.3.) \qquad \alpha\beta = \sum_{g,h \in G} a(g).b(h)g.h$$

Note que, na verdade, temos procedido exatamente como na definição de produto nos sistemas hipercomplexos, utilizando o produto em G para definir a multiplicação das unidades básicas que, neste caso, são os próprios elementos de G.

Pode-se reordenar a expressão (2.3) e escrever o produto $\alpha\beta$ na forma

$$\alpha\beta = \sum_{x \in G} \gamma(x)x$$

onde:

$$(2.4.) \qquad \gamma(x) = \sum_{g.h=x} a(g)b(h).$$

Verifica-se facilmente que, com as operações acima, RG é um anel, chamado de anel de grupo de G sobre R. Este anel tem unidade; se indicamos por 1_G o elemento neutro do grupo G, a unidade de RG é o elemento $1 = \sum_{g \in G} a(g)g$ onde $a(1_G) = 1$ e $a(g) = 0$ se $g \neq 1_G$.

Podemos também definir o produto de elementos $\alpha \in RG$ por escalares $\lambda \in R$ por:

$$(2.5.) \qquad \lambda(\sum_{g} a(g)g) = \sum_{g} \lambda a(g).g.$$

Novamente, é muito fácil verificar que com a soma e o produto por escalares definidos acima, RG é um R-módulo. Ainda, se R é comutativo, segue que RG é uma álgebra sobre R e, neste ca-

so, fala-se frequentemente da álgebra de grupo de G sobre R.

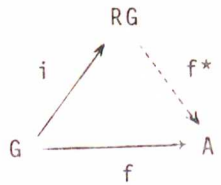
Pode-se definir uma imersão $i: G \longrightarrow RG$ associando a cada elemento $x \in G$ o elemento $i(x) = \sum_g a(g)g$ onde $a(x) = 1$ e $a(g)=0$ se $g \neq x$. Nós identificaremos G com sua imagem em RG; com esta identificação segue imediatamente que G é uma base de RG sobre R. Em particular, se G é finito e R comutativo, tem-se que $\dim_R RG = |G|$.

Da mesma forma, pode-se definir uma imersão $\nu: R \longrightarrow RG$ por : $\nu(r) = \sum_g a(g)g$ onde $a(1_G) = r$ e $a(g) = 0$ se $g \neq 1$.

Com ambas as identificações acima, da definição do produto em RG segue que $gr = rg$, $\forall r \in R$, $g \in G$. Consequentemente, se R é comutativo, temos que $R \subset Z(RG)$, o centro de RG.

Enunciamos a seguir uma propriedade simples, porém importante, dos anéis de grupo.

(2.5) Proposição - Sejam G um grupo e R um anel com unidade. Para todo anel A que contém R e toda função $f: G \longrightarrow A$ tal que $f(gh) = f(g).f(h)$ $\forall g,h \in G$, existe um único homomorfismo de anéis $f^*: RG \longrightarrow A$ tal que $f^* \circ i = f$ (onde $i: G \longrightarrow RG$ é a imersão dada acima) i.e. tal que o seguinte diagrama é comutativo:



Ainda mais, se R é central em A então f^* é um homomorfismo de R-álgebras.

Demonstração - Dada $f: G \longrightarrow A$ nas condições do enunciado, definimos $f^*: RG \longrightarrow A$ por:

$$\sum_g a(g)g \xrightarrow{f^*} \sum_g a(g)f(g).$$

A demonstração de que f^* é, efetivamente, um homomorfismo segue de um cálculo direto. □

Na verdade, esta propriedade pode ser usada para dar uma outra definição de anéis de grupo (veja o exercício 2 desta seção).

O corolário que damos a seguir é apenas um caso particular da proposição acima. Vamos enunciá-lo separadamente apenas pela sua especial utilidade.

(2.6.) Corolário - Seja $f: G \longrightarrow H$ um homomorfismo de grupo. Então, existe um único homomorfismo de anéis $f^*: RG \longrightarrow RH$ tal que $f^*(g) = f(g)$, $\forall g \in G$; se R é comutativo, então f^* é um homomorfismo de R-álgebras.

Ainda, pode-se mostrar facilmente que se f é um epimorfismo ou um monomorfismo, então f^* também o é.

Damos um resultado semelhante no exercício 1.

Vale a pena observar que se $H = \{1\}$ então o corolário (2.6) mostra que a função trivial $G \longrightarrow \{1\}$ induz um homomorfismo de anéis $\varepsilon: RG \longrightarrow R$ tal que $\varepsilon(\sum_g a(g)f) = \sum_g a(g)$. Este homomorfismo chama-se função de aumento de RG e irá desempenhar um papel fundamental na teoria.

Concluimos esta seção observando que os anéis de grupos são anéis com involução:

(2.7) Proposição - A função $*: RG \longrightarrow RG$ definida por

$$(\sum_g a(g)g)^* = \sum_g a(g^{-1})g$$

verifica

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

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

(iii) $(\alpha^*)^* = \alpha$.

A demonstração é trivial.

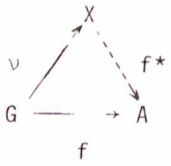
EXERCÍCIOS

1. Seja $\phi: R \longrightarrow S$ um homomorfismo de anéis com unidade e seja G um grupo. Provar que a função $\phi^*: RG \longrightarrow SG$ definida por:

$$\sum_g a(g)g \xrightarrow{g^*} \sum_g \phi(a(g))g$$

é um homomorfismo de anéis. Provar que se ϕ é um epimorfismo ou um monomorfismo então ϕ^* também o é.

2. Sejam G um grupo e R um anel com unidade. Seja X um anel que contém R e $\nu: G \longrightarrow X$ uma função tal que $\nu(gh) = \nu(g).\nu(h)$, $\forall g,h \in G$ e tal que, para todo anel $A \supset R$ e toda função $f: G \longrightarrow A$ que verifica $f(gh) = f(g)f(h)$, $\forall g,h \in G$ existe $f^*: X \longrightarrow A$ tal que o seguinte diagrama é comutativo:



Provar que $X \cong RG$ como anéis com unidade (ou como R-álgebras, de R é comutativo).

3. Sejam $\{R_i\}_{i \in I}$ uma família de anéis e $R = \bigoplus_{i \in I} R_i$. Dado um grupo G arbitrário, provar que:

$$RG \cong \bigoplus_{i \in I} R_i G$$

4. Sejam J um ideal de um anel com unidade R e G um grupo. Provar que $JG = \{\sum_g a(g)g \in RG \mid a(g) \in J, \forall g \in G\}$ é um ideal de RG e que $RG/JG \cong (R/J).G$.

5. Sejam R um anel comutativo com unidade e G,H grupos; denotamos por $G \times H$ o produto direto de G e H. Provar que $R(G \times H) \cong (RG)H$, o anel de grupo de H sobre o anel RG. Prove também que:

$$R(G \times H) \cong RG \otimes_R RH.$$

6. Sejam $R \subset S$ anéis comutativos com a mesma unidade e G um grupo. Provar que:

$$SG \cong S \otimes_R RG.$$

§3. Ideais de aumento

Na seção anterior introduzimos o conceito de anel de grupo; desejamos agora desenvolver técnicas para explorar a estrutura algébrica destes anéis. Um dos métodos mais frequentes, na álgebra, consiste em tentar decompor uma certa estrutura como soma direta de duas subestruturas.

Para desenvolver a teoria nesta direção vamos começar estudando a relação existente entre subgrupos de um dado grupo G e certos ideais do seu anel de grupo RG sobre um anel R. Esta relação tem interesse em si mesma e é útil para estudar diversas propriedades dos anéis de grupo. Apareceu pela primeira vez num artigo de A. Jennings [7] e, na forma aqui apresentada, num trabalho de W. A. Deskins [5]. A idéia de aplicá-la ao estudo de decomponibilidade é de I. G. Connell [3].

3.1. Definição - Sejam H um subgrupo de um grupo G e R um anel com unidade. Denotaremos por $\Delta_R(G:H)$ o ideal à esquerda de RG gerado pelo conjunto $\{h-1 \mid h \in H\}$ i.e.

$$\Delta_R(G:H) = \{ \sum_{h \in H} \alpha_h (h-1) \mid \alpha_h \in RG,\ (\alpha_h)_{h \in H} \text{ quase nula} \}$$

Quando for claro, do contexto, qual é o anel de coeficientes R com o qual estamos trabalhando, indicaremos este ideal apenas por $\Delta(G:H)$. Em particular, o ideal $\Delta(G:G)$ desempenhará um papel fundamental na teoria e será denotado apenas pelo símbolo $\Delta(G)$. Este ideal chama-se o ideal de aumento de RG .

Seja $Q = \{q_i\}_{i \in I}$ um conjunto completo de representantes de classes laterais à esquerda de H em G, que chamaremos brevemente de um transversal de H em G. No que segue, assumiremos sempre que como representante da classe H escolhemos o elemento neutro de G.

Obviamente, todo elemento $g \in G$ admite uma decomposição única na forma $g = q_i h_j$, $q_i \in Q$, $h_j \in H$.

(3.2.) Proposição - O conjunto $B = \{q(h-1) \mid q \in Q, h \in H, h \neq 1\}$ é uma base de $\Delta(G:H)$ considerado como módulo sobre R.

Demonstração - Mostraremos inicialmente que B é linearmente independente. Suponhamos que temos uma combinação linear:

$$\sum_{i,j} r_{ij} q_i (h_j - 1) = 0 \qquad , r_{ij} \in R$$

Reordenando temos:

$$\sum_{i,j} r_{ij} q_i h_j - \sum_i (\sum_j r_{ij}) q_i = 0$$

donde

$$\sum_{i,j} r_{ij} q_i h_j = \sum_i (\sum_j r_{ij}) q_i$$

Como $h_j \neq 1$, $\forall\, j$, segue facilmente que ambos os membros da igualdade acima tem suportes disjuntos; consequentemente ambos devem ser iguais a 0, separadamente.

Ainda, como $q_i h_j \neq q_r h_s$ quando $(i,j) \neq (r,s)$, de $\sum_{i,j} r_{ij} q_i h_j = 0$ segue imediatamente que $r_{ij} = 0$ para todo par (i,j).

Para provar que B também é um conjunto gerador de $\Delta(G:H)$, da própria definição vem que bastará provar que todo elemento da forma $g(h-1)$ com $g \in G$, $h \in H$ é combinação linear de elementos de B.

Agora, dado $g \in G$, sabemos que $g = q_h.h_j$ para algum $q_i \in Q$ e algum $h_j \in H$. Logo:

$$g(h-1) = q_i h_j(h-1) = q_i(h_j h-1) + q_i(h_j-1) \quad \square$$

(3.3.) Corolário - $\Delta(G) = \{\sum_g a(g)(g-1) \mid a(g) \in R\}$.

Demonstração - Conforme a proposição acima, o conjunto

$$\{g-1 \mid g \in G \ , \ g \neq 1\}$$

é uma base de $\Delta(G)$ sobre R, donde segue a afirmação. $\square$

No caso particular em que H é um subgrupo normal de G é possível dar uma interpretação especial ao ideal $\Delta(G:H)$. Com efeito, se $H \triangleleft G$, consideramos o homomorfismo canônico $\omega: G \longrightarrow G/H$ que a cada elemento $g \in G$ associa a sua classe $\bar{g} = gH \in G/H$. Conforme o Corolário (2.6) ele pode ser extendido a um epimorfismo de anéis $\omega^*: RG \longrightarrow R(G/H)$ tal que:

$$\omega^*(\sum_g a(g)g) = \sum_g a(g)\bar{g} \ .$$

(3.4.) Proposição - Com a notação acima, tem-se que $\Delta(G:H) = Ker(\omega^*)$.

Demonstração - Seja novamente Q um transversal de H em G.

Um elemento $\alpha \in RG$ pode então ser escrito como uma soma finita do tipo $\alpha = \sum_{i,j} r_{ij} q_i h_j$, $r_{ij} \in R$, $q_i \in Q$, $h_j \in H$.

Temos então que:

$$\omega^*(\alpha) = \sum_{i,j} r_{ij} \bar{q}_i \bar{h}_j = \sum_i (\sum_j r_{ij}) \bar{q}_i$$

Consequentemente, $\alpha \in Ker(\omega^*)$ se e somente se $\sum_j r_{ij} = 0$, para todo i.

Se $\alpha \in Ker(\omega^*)$ podemos então escrever (somando "zero" onde for conveniente):

$$\alpha = \sum_{i,j} r_{ij} q_i h_j = \sum_{i,j} r_{ij} q_i h_j - \sum_i (\sum_j r_{ij}) q_i = \sum_{i,j} r_{ij} q_i (h_j - 1) \in \Delta(G:H).$$

Portanto, temos que $Ker(\omega^*) \subset \Delta(G:H)$. A demonstração de que vale também a inclusão de sentido contrário é trivial. □

(3.5.) Corolário - Se $H \trianglelefteq G$ então $\Delta(G:H)$ é um ideal bilateral de RG e vale:

$$\frac{RG}{\Delta(G:H)} \cong R(G/H)$$

Segue também da proposição acima que o ideal de aumento $\Delta(G)$ de RG é, precisamente, o núcleo da função de aumento $\varepsilon: RG \to R$.

EXERCÍCIOS

1. Sejam $R \subset S$ anéis com a mesma unidade e seja G um grupo. Para todo subgrupo H de G, provar que $\Delta_S(G:H) = S.\ \Delta_R(G:H)$.

2. Seja S um conjunto de geradores de um subgrupo H de um grupo G. Provar que o conjunto $\{s-1 \mid s \in S\}$ é um conjunto de geradores de $\Delta(G:H)$ como ideal à esquerda de RG.

3. Sejam R um anel com unidade e H um subgrupo de um grupo G. Pode mos considerar RH como sub anel de RG e, consequentemente, também

$\Delta(H)$ como sbconjunto de RG. Com esta convenção, provar que:

(i) $\Delta(G:H) = RG.\Delta(H)$

(ii) $\Delta(G:H) = \Delta(H) + \Delta(G)\Delta(G:H)$ (sugestão: provar primeiro que $RG = R \oplus \Delta(G)$ como R-módulos).

4. (Karpilovsky [8]) Sejam H e N subgrupos de um grupo G e considere $\Delta(H)$, $\Delta(N)$ e $\Delta(H \cap N)$ incluidos em RG. Provar que:

(i) $\Delta(H)\Delta(N) \cap \Delta(N) = \Delta(H \cap N)\Delta(N)$.

(ii) $\Delta(G)\Delta(N) \cap \Delta(N) = \Delta(N)^2$.

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

(sugestão: Para provar (i) considere um transversal Q de H em N e demonstre primeiro que $\Delta(H)\Delta(N) = \Delta(H \cap N)\Delta(N) + \sum_{q \in Q} (q-1)\Delta(N))$.

5. Seja H um subgrupo de um grupo G e seja $\{H_i\}_{i \in I}$ a família de todos os conjugados de H em G. Provar que os ideais $U(H) = \sum_{i \in I} \Delta(G:H_i)$ e $V(H) = \bigcap_{i \in I} \Delta(G:H_i)$ são ideais bilaterais de RG.

6. Seja Q um transversal de um subgrupo H num grupo G. Dado um anel com unidade R, mostrar que o anel de grupo RG admite estrutura de RH-módulo, com as operações induzidas pelas operações de RG. Mostrar que este módulo é livre, com base Q.

7. (Coleman [2]) - Seja I um ideal de RG. Provar que o anel quociente RG/I é comutativo se e somente se $I \supset \Delta(G:G')$, onde G' indica o subgrupo comutador de G.

§4. Anéis de grupo completamente redutíveis

Lembramos que um anel diz-se *completamente redutível* se todo ideal à esquerda é somando direto ou, equivalentemente se pode ser escrito como soma direta de ideais à esquerda minimais.

Para anéis com unidade, isto é equivalente a dizer que o anel dado é semisimples, artiniano (Veja [4, (25.8)]).

A estrutura dos anéis completamente redutíveis é bem conhecida, uma vez que ela é descrita pelo famoso Teorema de Artin-Wedderburn, que enunciamos a seguir:

(4.1.) Teorema - Seja R um anel com unidade, completamente redutível. Então:

(i) R pode-se escrever como soma direta de ideais bilaterais:

$$R \cong B_1 \oplus \ldots \oplus B_m$$

onde cada B_i, $1 \leq i \leq n$, é um anel simples. (Estes ideais são chamados as *componentes simples* de R).

(ii) Cada anel simples B_i é isomorfo a um anel de matrizes $M_{n_i}(D_i)$ onde D_i é um anel com divisão.

(iii) As componentes simples estão univocamente determinadas e todo ideal bilateral de R é soma direta de componentes simples. Ainda, se $M_{n_i}(D_i) \cong M_{n_j}(D_j)$ então $n_i = n_j$ e $D_i \cong D_j$.

Para uma demonstração deste teorema veja ([4, (25.15) e (26.8)] ou [14, Teorema VI.6.2.].

Em vista disso resultará interessante - e útil - determinar condições sobre R e G para que o anel de grupo RG seja completamente redutível.

Começamos nosso trabalho nessa direção lembrando o seguinte:

(4.2) Definição - Seja $X \subset RG$. Chama-se anulador à direita de X ao conjunto:

$$\rho(X) = \{\alpha \in RG \mid x\alpha = 0, \forall\, x \in X\}$$

De forma análoga define-se o anulador à esquerda de X como o conjunto

$$\lambda(X) = \{\alpha \in RG \mid \alpha x = 0\ , \forall\, x \in X\}$$

(4.3) Lema - Sejam H um subgrupo de um grupo G e R um anel com unidade. Então $\rho(\Delta(G:H)) \neq 0$ se e somente se H é finito.

Demonstração

Seja $0 \neq \alpha = \sum_g a(g)g \in \rho(\Delta(G:H))$.

Para cada elemento $h \in H$ temos que $(h-1)\alpha = 0$ donde $h\alpha = \alpha$ i.e.

$$\sum_g a(g)hg = \sum_g a(g)g\ .$$

Seja g_0 um elemento do suporte de α. Da igualdade acima segue que deve existir um elemento $g_1 \in \sup(\alpha)$ tal que $hg_1 = g_0$, donde $h = g_0 g_1^{-1}$. Como isto é válido para todo elemento $h \in H$ segue que $H \in \{xy^{-1} \mid x,y \in \sup(\alpha)\}$. Ainda, como $\sup(\alpha)$ é um conjunto finito, segue imediatamente que H também o é.

Reciprocamente, seja $H = \{h_1, \ldots, h_n\}$ um subgrupo finito de G. Consideramos então o elemento $h = \sum_{i=1}^{n} h_i$. Obviamente $h \neq 0$ e temos:

$$h\hat{h} = \sum_{i=1}^{n} hh_i = \hat{h}$$

donde

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

Portanto

$$\hat{h} \in \rho(\Delta(G:H)).$$

(4.4) Lema - Sejam G um grupo finito e $\hat{g} \in RG$ a soma de todos os elementos de G. Então:

(i) $\hat{g}$ é central em RG e $\rho(\Delta(G)) = \lambda(\Delta(G)) = R.\hat{g}$

(ii) $\rho(\Delta(G)) \cap \Delta(G) = \{a\hat{g} \mid a \in R \ , \ a\,|G| = 0\}$

Demonstração - Notamos inicialmente que, dado $x \in G$ temos que:

$$x\hat{g}x^{-1} = \sum_{g \in G} xgx^{-1} = \sum_{g \in G} g = \hat{g} \ .$$

Logo, $x\hat{g} = \hat{g}x$, $\forall\, x \in G$ donde $\hat{g}$ é central em RG.

Ainda, a demonstração do lema acima mostra que, dado a arbitrário em R tem-se que:

$a\hat{g} \in \rho(\Delta(G))$ donde $R\hat{g} \subset \Delta(G)$.

Para provar a inclusão contrária consideramos um elemento $\alpha = \sum_g a(g)g \in \rho(\Delta(G))$ e seja g_0 arbitrário em G. Temos então que:

$$(g_0^{-1}-1)\alpha = 0 \quad \text{donde} \quad g_0^{-1}\alpha = \alpha$$

ou seja

$$\sum_g a(g)g_0^{-1}g = \sum_g a(g)g \ .$$

O coeficiente de $1 \in G$ na expressão no primeiro membro é $\alpha(g_0)$ enquanto que, na expressão no segundo membro é $\alpha(1)$. Logo, deve ser $a(g_0) = a(1)$. Como isto vale para todo $g_0 \in G$ segue que

$$\alpha = \sum_g \alpha(g)g = \alpha(1)\sum_g g = \alpha(1)\bar{g} \in R\bar{g} \quad \square$$

(4.5) Lema - Seja J um ideal à esquerda de RG tal que

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

então $J = \rho(\Delta(G))$ é, consequentemente, é um ideal bilateral de RG.

Demonstração - Sejam $\alpha \in J$ e $\rho \in \Delta(G)$ arbitrários. Como J é ideal à esquerda temos que $\beta\alpha \in J$. Ainda, como $\Delta(G)$ é bilateral, também temos que $\beta\alpha \in \Delta(G)$ i.e. $\beta\alpha \in J \cap \Delta(G) = 0$, $\forall \alpha \in J$, $\forall\ \beta \in \Delta(G)$. Isto prova que $J \subset \rho(\Delta(G))$.

Reciprocamente, seja $x \in \rho(\Delta(G))$. Podemos escrever

$1 = e_1+e_2$ com $e_1 \in J$, $e_2 \in \Delta(G)$ e temos que $x = xe_1+xe_2$.

Como $x \in \rho(\Delta(G))$ segue que $xe_2 = 0$; portanto $x = xe_1 \in J$. $\square$

(4.6) Lema - Se o ideal de aumento, $\Delta(G)$, é somando direto de RG então G é finito e $|G|$ é inversível em R.

Demonstração - Dos lemas anteriores, segue imediatamente que $\rho(\Delta(G)) \neq 0$ e, consequentemente, que G é finito.

Como no lema acima, escrevemos $RG = \rho(\Delta(G)) \oplus \Delta(G)$ e $1 = e_1+e_2$, com $e_1 \in \rho(\Delta(G))$ e $e_2 \in \Delta(G)$. Então temos:

$$1 = \varepsilon(1) = \varepsilon(e_1) + \varepsilon(e_2) = \varepsilon(e_1)\ .$$

Como $e_1 = a\bar{g}$ para algum $a \in R$, segue que $\varepsilon(e_1)=a\ \varepsilon(\bar{g})=a|a|=1$. Logo, $|G|$ é inversível em R. □

Estamos agora em condições de demonstrar o resultado principal desta seção. Ele foi obtido em 1898-1899, para grupos finitos, por Heinrich Maschke (1853-1908), um estudante de F. Klein que emigrou aos Estados Unidos e se juntou a O. Bolza e E.H. Moore para criar o departamento de matemática da Universidade de Chicago.

Na verdade, existem antecedentes deste resultado nos trabalhos de T. Molien; a respeito, veja Hawkins [6 , p. 271].

A demonstração geral que damos a seguir segue essencialmente as idéias de I. G. Connell [3].

(4.7) Teorema de Maschke - Um anel de grupo RG é completamente redutível se e somente se as seguintes condições estão verificadas:

(i) G é finito

(ii) $|G|$ é inversível em R

(iii) R é completamente redutível

Demonstração - Suponhamos que RG é completamente redutível. Então, em particular $\Delta(G)$ é somando direto e, do lema anterior, seguem imediatamente (i) e (ii).

Por outro lado, temos que $R \cong RG/\Delta(G)$. Como quocientes de anéis completamente redutíveis também o são, (iii) resulta diretamente.

Para a recíproca, suponhamos que valem as condições (i), (ii) e (iii) e seja M um ideal à esquerda de RG, arbitrário. Mostra

remos que M é somando direto de RG.

Como R é completamente redutível, todo R-módulo é completamente redutível (veja, por exemplo [4 , (25.8)] ou [14, Teorema VI.6.1]. Logo, existe um R-submódulo N de RG (que não é, necessariamente um RG-submódulo) tal que

$$RG = M \oplus N .$$

Seja agora π: RG $\longrightarrow$ M a projeção natural associada à decomposição em soma direta. Definimos ainda:

$$\pi^*: RG \longrightarrow M$$

por

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

Se demonstrarmos que π^* é um RG-homomorfismo que verifica $\pi^{*2} = \pi^*$ e $Im(\pi^*) = M$ então, chamando $M_1 = Ker(\pi^*)$ ter-se-á que M_1 é um RG-submódulo de RG e $RG = M \oplus M_1$, com o que a nossa afirmação estará demonstrada.

Agora, como π^* é um R-homomorfismo, para demonstrar que também é um RG-homomorfismo, bastará provar que

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

Mas:

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

Quando g percorre todos os elementos de G também ga percorre todos os elementos de G. Temos assim que

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

Como π é uma projeção sobre M, temos que $\pi(m) = m$, $\forall m \in M$.

Ainda, se $m \in M$, como M é RG-módulo, temos que $gm \in M$, $\forall g \in G$; logo:

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

Desta observação decorre facilmente que $M \subset Im(\pi^*)$.

Dado um elemento arbitrário $x \in RG$, temos que $\pi(gx) \in M$, $\forall g \in G$; consequentemente, $\pi^*(x) \in M$ donde $Im(\pi^*) \subset M$ e segue a igualdade.

Finalmente, se $\pi^*(x) \in M$, $\forall \ x \in RG$, da observação anterior segue que $\pi^*(\pi^*(x)) = \pi^*(x)$ $\forall x \in RG$, i.e. $\pi^{*2} = \pi$. □

Tanto por razões históricas como pela sua aplicação na teoria de representações de grupos, resulta particularmente importante o caso em que $R = K$, um corpo.

Neste caso, K é sempre completamente redutível e $|G|$ é inversível em K se e somente se $|G| \neq 0$ em K, ou equivalentemente, se e só se $car(K) \nmid |G|$. Em presença destas observações, podemos enunciar como consequência direta do teorema acima a versão mais clássica do Teorema de Maschke:

(4.8) Corolário - Sejam G um grupo finito e K um corpo. Então, KG é completamente redutível se e somente se $car(K) \nmid |G|$.

Temos caracterizado aqui completamente os anéis de grupo RG que são completamente redutíveis, isto é, que são simultaneamente artinianos e semisimples. No próximo capítulo estudaremos estas condições separadamente.

EXERCÍCIOS

1. Sejam G um grupo finito e K um corpo tal que car(K) $\mid |G|$. Demonstrar que KG não é completamente redutível mostrando que o ideal gerado por $\hat{g} = \sum_{g \in G} g$ nao é somando direto.

2. Seja S_3 o grupo das permutações de três elementos. Determinar a decomposição de $\mathbb{C}S_3$ em soma direta de álgebras de matrizes.

3. Sejam G um grupo comutativo finito e K um corpo tal que car(K) $\nmid |G|$. Provar que KG é isomorfo a uma soma direta de corpos.

4. Utilizar o exercício anterior para mostrar que existem grupos G,H não isomorfos, tais que $\mathbb{C}G \cong \mathbb{C}H$.

5. Provar que vale a recíproca do lema (4.5) i.e. que se G é um grupo finito e |G| é inversível em R então $\Delta(G)$ é um somando direto de RG.

6. (D.A.R. Wallace [19]) Seja I um ideal de um anel de grupo RG tal que $ab = ba$, $\forall\ a,b \in I$. Provar que $I \subset \lambda(\Delta(G:G'))$ e demonstrar que G' é finito.

7. Seja H um subgrupo finito de um grupo G e seja $\hat{h} = \sum_{h \in H} h$. Provar que $\rho(\Delta(G:H)) = \hat{h}RG$. Provar que se $H \lhd G$ então $\hat{h}$ é central em RG e $\rho(\Delta(G:H)) = \lambda(\Delta(G:H))$.

§5. Anéis de grupos decomponíveis

Na seção anterior estudamos anéis de grupo que são completamente redutíveis. Nessa mesma direção, pretendemos determinar agora em que condições é possível decompor RG ao menos como soma direta de ideais.

Para isso precisaremos determinar inicialmente em que condições o ideal de aumento, $\Delta(G)$, é nilpotente. Esta questão foi estudada por S. A. Jennings [7], e I.G. Connell [3].

(5.1.) Lema - Sejam $G = \langle a \mid a^p = 1 \rangle$ um grupo cíclico de ordem p e R um anel com unidade. Então $\Delta(G)$ coincide com o ideal à esquerda gerado pelo elemento (a-1).

Demonstração - Sabemos, do corolário (3.3), que o conjunto $\{a^i - 1 \mid 1 \leq i \leq p-1\}$ é uma base de $\Delta(G)$ sobre R.

Como $a^i - 1 = a^{i-1}(a-1) + a^{i-2}(a-1) + \ldots + (a-1)$, a afirmação segue imediatamente. □

(5.2.) Teorema - Sejam G um grupo e R um anel com unidade. Então, o ideal de aumento $\Delta(G)$ é nilpotente se e somente se G é um p-grupo finito, para algum inteiro primo p e R tem característica p^m, para algum $m \geq 1$.

Demonstração - Seja n tal que $\Delta(G)^n = 0$ e $\Delta(G)^{n-1} \neq 0$. Então, como $\rho(\Delta(G)) \supset \Delta(G)^{n-1}$, segue que G é finito. Para provar que G deve ser um p-grupo, para algum primo p, suponhamos que $|G|$ admite dois

divisores primos diferentes p,q.

Tomando elementos $x,y \in G$ tais que $o(x) = p$, $o(y) = q$, podemos escrever:

$$1 = x^p = [1 + (x-1)]^p = 1 + p(x-1) + \binom{p}{2}(x-1)^2 + \ldots + (x-1)^p$$

$$1 = y^q = [1 + (y-1)]^q = 1 + q(y-1) + \binom{q}{2}(y-1)^2 + \ldots + (y-1)^q.$$

Sejam r,s inteiros tais que $rp + sq = 1$. Multiplicando a primeira equação à esquerda por $r(y-1)$ e a segunda à direita por $s(x-1)$ e somando, temos:

$$-(x-1)(y-1) = [\binom{p}{2}(x-1)+\ldots+(x-1)^{p-1}](x-1)(y-1)+(x-1)(y-1)[\binom{q}{2}(y-1)+\ldots+(y-1)^{q-1})]$$

donde

$$(x-1)(y-1) \in \Delta(G)(x-1)(y-1) + (x-1)(y-1)\Delta(G) \subset \Delta(G)^3 .$$

Mas, se $(x-1)(y-1) \in \Delta(G)^3$ a mesma equação acima implica que também $(x-1)(y-1) \in \Delta(G)^4$ e, indutivamente, $(x-1)(y-1) \in \Delta(G)^m$, para todo inteiro positivo m.

Como $\Delta(G)^n = 0$ segue que $(x-1)(y-1) = 0$. Desenvolvendo, $xy - x - y + 1 = 0$.

Como todos os elementos do suporte do primeiro membro são diferentes dois a dois, pois $x \neq y$; isto é uma contradição.

Queremos provar agora que car(R) é uma potência de p.

Consideremos primeiro o caso em que $car(R) = m \neq 0$ e suponhamos que um outro primo $q \neq p$ divida m. Então $\mathbb{Z}_m$ contém uma cópia de $\mathbb{Z}_q$ e temos:

$$\mathbb{Z}_q G \subset \mathbb{Z}_m G \subset RG \quad \text{donde} \quad \Delta_{\mathbb{Z}_q}(G) \subset \Delta_R(G) ;$$

portanto $\Delta_{\mathbb{Z}_q}(G)^n = 0$.

Mas, de acordo com o Teorema (4.7), $\mathbb{Z}_q(G)$ é completamente redutível e estes anéis não contêm ideais nilpotentes; uma contradição.

Ainda, se car(R) = 0 e q é um primo arbitrário, diferente de p consideramos o homomorfismo canônico $\omega: \mathbb{Z} \longrightarrow \mathbb{Z}_q$, que estendemos a um homomorfismo de anéis de grupos $\omega^*: \mathbb{Z}G \longrightarrow \mathbb{Z}_q G$.

Como $\mathbb{Z}G \subset RG$ segue que $\Delta_{\mathbb{Z}}(G)^n = 0$ logo $\omega^*(\Delta_{\mathbb{Z}}(G)) = \Delta_{\mathbb{Z}_q}(G)$ é nilpotente; uma contradição.

Reciprocamente, suponhamos que $car(R) = p^m$, $m \geq 1$ e que G é um p-grupo de ordem p^n, $n \geq 1$. Faremos a demonstração da nilpotência de $\Delta(G)$ por indução em n.

Se n=1 então G é cíclico de ordem p e, se a é um gerador de G, do lema (5.1) temos que $\Delta(G) = (1-a)RG = RG(1-a)$.

Escolhendo p elementos arbitrários $\alpha_1,\ldots,\alpha_p$ em $\Delta(G)$, podemos escrever o produto na forma $\alpha_1 \ldots \alpha_p = \beta_1 \ldots \beta_p (1-a)^p$.

Mas $(1-a)^p = 1 + \binom{p}{1}a+\ldots+\binom{p}{p-1}a^{p-1}-a^p = \binom{p}{1}a-\binom{p}{2}a^2+\ldots+\binom{p}{p-1}a^{p-1}$.

Como todos estes coeficientes são múltiplos de p, vemos que o produto $\alpha_1 \ldots \alpha_p$ pode ser escrito na forma:

$$\alpha_1 \ldots \alpha_p = p.\beta \quad \text{com} \quad \beta \in RG.$$

De forma análoga, se tomamos $\alpha_1,\ldots,\alpha_{mp}$ arbitrários em $\Delta(G)$ teremos

$$\alpha_1 \ldots \alpha_{mp} = p^m\gamma \text{, com } \gamma \in RG \text{, i.e. } \alpha_1 \ldots \alpha_{mp} = 0.$$

Consequentemente, $\Delta(G)^{mp} = 0$ donde $\Delta(G)$ é nilpotente.

Suponhamos agora que o resultado vale para grupos de ordem p^{n-1} e que $|G| = p^n$.

Como G é um p-grupo, existe um elemento a de ordem p no centro de G. Então, o subgrupo gerado por a, que denotamos $\langle a \rangle$ é normal em G e temos:

$$\frac{RG}{\Delta(G:\langle a \rangle)} \cong RG/\langle a \rangle$$

Como $|G/\langle a \rangle| = p^{n-1}$, sabemos que o ideal de aumento de $RG/\langle a \rangle$ é nilpotente. Isto significa que existe um inteiro m_o tal que $\Delta(G)^{m_o} = 0$ no quociente $RG/\Delta(G:\langle a \rangle)$ i.e. tal que

$$\Delta(G)^{m_o} \subset \Delta(G:\langle a \rangle). \tag{5.3}$$

Ainda, $\Delta(G:\langle a \rangle) = \Delta(\langle a \rangle)RG = RG(1-a)$

(A primeira igualdade segue do exercício 3 parte (i) da seção §3 e a segunda, do lema (5.1)).

Por outro lado, como a é central em G temos que

$$[RG(1-a)]^{mp} = RG(1-a)^{mp} = 0 \tag{5.4}$$

De (5.3) e (5.4) segue que $\Delta(G)^{m_o mp} = 0$. □

Podemos extender agora este resultado, sem maiores dificuldades, a ideais de aumento de subgrupos normais de G.

(5.5) Corolário - Sejam H um subgrupo normal de um grupo G e R um anel com unidade. Então $\Delta_R(G:H)$ é nilpotente se e somente se H é um p-subgrupo finito de G, para algum primo p, e $car(R) = p^m$, com $m \geq 1$.

Demonstração - Suponhamos primeiro que $\Delta(G:H)$ é nilpotente. Como $\Delta(H) \subset \Delta(G:H)$ temos que também $\Delta(H)$ é nilpotente e a tese segue diretamente do teorema acima.

Reciprocamente, se H é um p-subgrupo normal, finito de G e $car(R) = p^m$, $m \geq 1$ sabemos que $\Delta(H)^t = 0$ para algum inteiro $t > 1$.

Tomando novamente um transversal Q de H em G temos que todo elemento $\alpha \in \Delta(G:H)$ pode-se escrever na forma:

$$\alpha = \sum_{i,j} r_{ij} q_i (h_j - 1) \ , \ r_{ij} \in R \ , \ q_i \in Q \ , \ h_j \in H \ .$$

Para calcular o produto de dois destes elementos, aplicando a propriedade distributiva, devemos calcular produtos da forma

$$r_{ij} r_{st} q_i (h_j - 1) q_s (h_t - 1)$$

Como $H \lhd G$, temos que $q_s^{-1} h_j q_s$ é um outro elemento de H, que indicaremos por h_j'. Então $h_j q_s = h_j' q_s$ e temos:

$$r_{ij} r_{st} q_i (h_j - 1) q_s (h_t - 1) = r_{ij} r_{st} q_i q_s (h_j' - 1)(h_t - 1) \in RG\Delta(H)^2 .$$

Indutivamente:

$$\Delta(G:H)^t \subset RG\Delta(H)^t = 0 \ . \ \square$$

CAPÍTULO II

CONDIÇÕES DE FINITUDE

Este capítulo é dedicado ao estudo das condições de finitude em anéis de grupos. Observamos que, em virtude da existência da involução * (Proposição I.2.7), um anel de grupo com coeficientes num anel comutativo R é artiniano ou noetheriano à esquerda se e somente se é artiniano ou noetheriano à direita respectivamente. Assim, neste capítulo, ocupar-nos-emos apenas de condições à esquerda. No que segue, R denotará um anel com unidade e K um corpo.

§1. Resultados preliminares

Para estudar os anéis de grupo artinianos, precisaremos dar inicialmente uma caracterização dos anéis de grupo que são primos.

(1.1) Definição - Um anel R diz-se primo se para quaisquer dois ideais A,B de R tais que AB = 0, tem-se que A = 0 ou B = 0.

Seja agora H um subgrupo de G. Existe uma projeção natural π_H: KG → KH, dada por:

$$\pi_H\Big(\sum_{g\in G}\alpha(g)g\Big) = \sum_{g\in H}\alpha(g)g.$$

Em outras palavras, se $\alpha \in KG$, então $\pi_H(\alpha)$ se obtém anulando todos aqueles coeficientes que não correspondem a elementos de H.

Enunciamos abaixo algumas propriedades básicas da função π_H.

(1.2) Proposição - Dados $\alpha,\beta \in RG$, $\gamma \in RH$, $r,s \in R$, tem-se que:

(i) $\pi_H^2 = \pi_H$.

(ii) $\pi_H(r\alpha+s\beta) = r\pi_H(\alpha) + s\pi_H(\beta)$.

(iii) $\pi_H(\gamma\alpha) = \gamma.\pi_H(\alpha)$, $\pi_H(\alpha\gamma) = \pi_H(\alpha)\gamma$.

(iv) Se $H \lhd G$, então $\forall\, x \in G$, tem-se: $\pi_H(x^{-1}\alpha x) = x^{-1}\pi_H(\alpha)x$.

Prova: A título de ilustração, demonstraremos (iii). Escrevendo $\alpha = \pi_H(\alpha) + \alpha'$, com $\sup(\alpha') \cap H = \phi$, vem que $\gamma\alpha = \gamma\pi_H(\alpha) + \gamma\alpha'$, onde $\sup(\gamma\pi_H(\alpha)) \subset H$, $\sup(\gamma\alpha') \cap H = \phi$. Logo, $\pi_H(\gamma\alpha) = \gamma\pi_H(\alpha)$, como queríamos demonstrar. A demonstração de que $\pi_H(\alpha\gamma) = \pi_H(\alpha)\gamma$ é análoga. □

(1.3) Lema - Seja I um ideal de KG. Então,

$$I \subset \pi_H(I).KG$$

Prova - Seja $Q = \{q_i\}_{i\in I}$ um transversal à direita de H em G, com $q_1 = 1$. Dado $\alpha \in I$, escrevemos: $\alpha = \sum_g \alpha(g)g = \sum_i \beta(q_i)q_i$, com $\beta(q_i) \in RH$. Notamos ainda que $\pi_H(\alpha) = \beta(q_1)$, e em geral $\pi_H(\alpha q_i^{-1}) = \beta(q_i)$. Assim, $\alpha = \sum_i \pi_H(\alpha q_i^{-1})q_i$. Como I é um ideal, $\alpha q_i^{-1} \in I$. Logo, $\alpha \in \pi_H(I)KG$. □

Precisaremos ainda do Lema abaixo sobre grupos:

(1.4) Lema - Sejam G um grupo, $H_1, H_2, \ldots, H_n$ subgrupos de G, distintos dois a dois. Suponhamos que existe uma coleção finita de elementos $x_{ij} \in G$ tais que $G = \bigcup_{i,j} H_i x_{ij}$. Então, para algum i, $[G:H_i] < \infty$.

Prova - Vamos proceder por indução em n.

Se n=1, o resultado é imediato.

Se um conjunto completo de coclasses de H_n comparece na união, é claro que $[G: H_n] < \infty$. Suponhamos então que a coclasse $H_n x$ não comparece, para algum $x \in G$. Então, $H_n x \subset G \subset \bigcup_{i,j} H_i x_{ij}$. Mas $H_n x \cap H_n x_{nj} = \phi$, para todo j, logo $H_n x \subset \bigcup_{\substack{i \neq n \\ j}} H_i x_{ij}$.

Daí é fácil ver que, para todo elemento x_{nr}, tem-se que $H_n x_{nr} \subset \bigcup_{\substack{i \neq n \\ j}} H_i x_{ij} x^{-1} x_{nr}$, e G pode ser coberto por uma união finita de coclasses $H_1, H_2, \ldots, H_{n-1}$. Pela hipótese de indução, temos que $[G: H_i] < \infty$, para algum $i \leq n-1$. □

Dado um grupo G, consideramos o conjunto

$\phi(G) = \{g \in G \mid$ a classe de conjugação de G tem ordem finita $\}$

Note que a classe de conjugação de um elemento g G tem ordem finita se e somente $[G: C(g)] < \infty$, onde C(g) denota o centralizador de g em G.

Pode-se demonstrar que $\phi(G)$ é um subgrupo normal de G [ver 17, p. 441], que é conhecido como o FC-subgrupo de G (FC por finite class).

Em particular, um grupo G diz-se FC se $G = \phi(G)$. Neste

caso, pode-se provar que todo elemento de G', o subgrupo comutador de G, é de ordem finita [ver 17, p. 442]. Consequentemente um grupo FC, sem torção, é necessariamente abeliano.

No que segue, consideraremos a função $\pi_{\phi(G)}$, que denotaremos simplesmente por π.

(1.5) Lema - Sejam $\alpha,\beta \in KG$. Se $\alpha x \beta = 0$, $\forall x \in G$, então $\pi(\alpha)\beta = 0$.

Prova - Suponhamos por absurdo, que $\gamma = \pi(\alpha)\beta \neq 0$, e seja $\sup(\alpha) = \{u_1, u_2, \ldots, u_n\}$. Se $C(u_i)$ denota o centralizador de u_i em G, consideremos o subgrupo $\Omega = \bigcap_i C(u_i)$. Como $[G: C(u_i)] < \infty$, tem-se que $[G: W] < \infty$.

Ainda, note que todo elemento $x \in \Omega$ comuta com $\pi(\alpha)$.

Ora, $\alpha = \pi(\alpha) + \alpha'$, com $\sup(\alpha')$ disjunto de $\phi(G)$. Escrevemos: $\alpha' = \sum_j \alpha_j y_j$, $y_j \in G$, $y_j \notin \phi(G)$,

$$\beta' = \sum_k b_k z_k \ , \ z_k \in G \ .$$

Seja agora $v \in \sup(\gamma)$. Se algum y_j é conjugado de algum vz_k^{-1}, escolhemos $h_{jk} \in G$ tal que $h_{jk}^{-1} y_j h_{jk} = vz_k^{-1}$.

Seja $x \in \Omega$. Por hipótese, $\alpha x \beta = 0$. Multiplicando esta igualdade à esquerda por x^{-1}, vem que $x^{-1} \alpha x \beta = 0$, ou:

$$x^{-1}(\pi(\alpha)+\alpha')x\beta = 0 \ , \ x^{-1}\pi(\alpha)x\beta + x^{-1}\alpha' x\beta = 0 \ , \text{ logo:}$$

$$\pi(\alpha)\beta + x^{-1}\alpha' x\beta = 0.$$

Portanto, $-\gamma = x^{-1}\alpha' x\beta$.

Como $v \in \sup(\gamma)$, v ocorre também no suporte do lado direito. Ou seja, existem y_j, z_k tais que $v = x^{-1}y_j x z_k$, ou $x^{-1}y_j x = vz_k^{-1} = h_{jk}^{-1}\, y_j\, h_{jk}$.

Assim, $xh_{jk}^{-1} \in C(y_j)$ e $x \in C(y_j)h_{jk}$. Acabamos de provar que $\Omega \subset \bigcup_{j,k} C(y_j)h_{jk}$.

Como $[G: W] < \infty$, segue facilmente que G está nas condições do Lema (1.4). Como nenhum dos $C(y_j)$ tem índice finito, temos uma contradição. □

(1.6) Lema - Sejam A_1, A_2 ideais de KG tais que $A_1, A_2 = 0$. Então, $\pi(A_1)\pi(A_2) = 0$.

Prova - Mostraremos primeiro que $\pi(A_1)A_2 = 0$. Para cada $x \in G$, $\alpha_1 \in A_1$, $\alpha_2 \in A_2$, tem-se que $\alpha_1 x \alpha_2 = 0$. Pelo Lema (1.5), vem que $\pi(\alpha_1)\alpha_2 = 0$.

Sejam agora $\alpha_1 \in A_1$, $\alpha_2 \in A_2$, $x \in G$. Como $\alpha_2 x \in A_2$, vem que $\pi(\alpha_1)\alpha_2 x = \pi(\alpha_1)\alpha_2 x.1 = 0$.

Pelo Lema (1.5), vem que $\pi(\pi(\alpha_1)\alpha_2)1 = 0$ e, do Lema (1.2), tem-se: $\pi(\alpha_1)\pi(\alpha_2) = 0$, como queríamos demonstrar. □

(1.7) Lema - Sejam G um grupo ordenado e R um anel sem divisores de zero. Então, RG não contém divisores de zero.

Prova - Sejam $\alpha, \beta \in RG$, diferentes de zero. Mostraremos que $\alpha\beta \neq 0$.

Com efeito, como $\sup(\alpha)$ é finito, podemos determinar um elemento $g_0 \in \sup(\alpha)$ que seja mínimo, i.é. tal que $g_0 < g$, $\forall\, g \in \sup(\alpha)$, $g \neq g_0$, e seja $a \neq 0$ o seu coeficiente na expressão de α.

Escrevemos então $\alpha = ag_0 + \sum_{g \neq g_0} a(g)g$.

De modo análogo, podemos escrever β na forma

$\beta = bh_0 + \sum_{h \neq h_0} b(h)h$, onde $h_0 < h$, $\forall h \in \sup(\beta)$, e $b \neq 0$.

Agora, $\alpha\beta = abg_0h_0 + \sum_{(g,h) \neq (g_0,h_0)} a(g)b(h)gh$, onde o elemento g_0h_0 certamente não comparece na segunda parcela da soma, já que $g_0h_0 \neq gh$ quando $(g,h) \neq (g_0,h_0)$.

Como R não contém divisores de zero, temos que $ab \neq 0$, donde $\alpha\beta \neq 0$. □

(1.8) Lema - Seja G um grupo abeliano sem torção. Então, se R é um anel sem divisores de zero, RG não contém divisores de zero.

Prova - Sejam $\alpha, \beta \in RG$ tais que $\alpha\beta = 0$. Considerando o subgrupo de G gerado por $\sup(\alpha) \cup \sup(\beta)$, podemos supor que G é finitamente gerado.

O resultado segue agora do lema acima e do fato de que todo grupo abeliano finitamente gerado sem torção é ordenado.

(1.9) Teorema - O anel de grupo KG é primo se e somente se G não contém subgrupos normais finitos não triviais.

Prova ($\Longrightarrow$) - Seja H um subgrupo normal finito de G, e consideremos o elemento $\hat{H} = \sum_{h \in H} h$. Como $H \lhd G$, é fácil ver que $\hat{H} \in Z(KG)$, o centro de KG. Calculando, vem diretamente que $\hat{H}^2 = |H|\hat{H}$. Portanto, $\hat{H}(\hat{H} - |H|.1) = 0$.

Ora, como KG é primo, Z(KG) não contém divisores de zero. Logo, $\hat{H} = |H|.1$ e $H = \{1\}$.

($\Longleftarrow$) - Sejam A_1, A_2 ideais de KG tais que $A_1 A_2 = 0$. Pelo Lema (1.6), $\pi(A_1)\pi(A_2) = 0$. Mas estes são ideais de $K\phi(G)$. Da hipótese, $\phi(G)$ é sem torção, logo abeliano. Pelo Lema (1.8), $K\phi(G)$ não contêm divisores de zero.

Suponhamos então que $\pi(A_1) \neq 0$, e seja $\alpha \neq 0$ em $\pi(A_1)$.

Tem-se que $\alpha\beta = 0$, para todo $\beta \in \pi(A_2)$. Logo, $\beta = 0$ e $\pi(A_2) = 0$.

Acabamos de provar que $\pi(A_1) = 0$ ou $\pi(A_2) = 0$. Do Lema (1.3), vem então que $A_1 = 0$ ou $A_2 = 0$. □

§2. Anéis artinianos

Neste seção caracterizaremos os anéis de grupo que são artinianos. Começaremos estudando o caso em que o anel de coeficientes é um corpo.

(2.1) Teorema - O anel KG é artiniano se e somente se G é finito.

Prova ($\Longleftarrow$) - Se G é finito, de ordem n, KG é um espaço vetorial de dimensão n sobre K. Como todo ideal à esquerda de KG é, em particular, um subespaço vetorial, segue facilmente que uma cadeia descendente de ideais tem, no máximo, comprimento igual a n.

($\Longrightarrow$) Como KG é artiniano, J(KG), o radical de Jacobson de KG, é nilpotente. Suponhamos primeiro que KG é primo. Neste caso, J(KG) = 0. Pelo teorema de Wedderburn, KG deve ser uma soma direta de anéis simples. Como estamos supondo que KG é primo, deve ser ele próprio um anel simples. Mas $\Delta(G)$ é um ideal bilateral próprio de KG; logo, deve ser trivial. Assim, devemos ter $G = \{1\}$.

Seja agora n o comprimento de uma sequência de composição para KG. Procederemos por indução em n. Se n=1, o ideal $\{0\}$ é o único ideal próprio de KG, logo $\Delta(G) = \{0\}$ e portanto $G = \{1\}$.

Suponhamos o teorema demonstrado para todo anel de grupo que admita uma sequência de composição de comprimento menor ou igual a n-1.

Se KG é primo, pela observação acima, o teorema está demonstrado. Se KG não é primo, pelo Teorema (1.9), G contém um sub-grupo normal finito $H \neq \{1\}$. Seja $\omega^*: KG \longrightarrow KG/H$ o homomorfismo canônico definido no §3 do Capítulo I. Então, KG/H é artiniano e tem uma sequência de composição de comprimento menor que n, já que $\ker \omega^* \neq \{0\}$. Pela hipótese de indução, vem que $|G/H| < \infty$. Como $|H| < \infty$, segue que $|G| < \infty$. □

Trataremos agora de obter a caracterização para o caso em que o anel de coeficientes não é necessariamente um corpo.

(2.2) Lema - Seja $R = M_n(D)$, em que D é um anel com divisão de centro K. Se RG é artiniano, então KG é artiniano.

Prova - De fato, seja $I \supset I_2 \supset \ldots \supset I_n \supset \ldots$ uma cadeia de ideais à esquerda de KG. Então, $RI_1 \supset \ldots \supset RI_n \supset \ldots$ é uma cadeia de ideais de RG.

Da hipótese, existe $n \in N$, tal que $RI_n = RI_{nn} = \ldots$ Observamos agora que, pra todo ideal à esquerda I de KG, tem-se que $RI \cap KG = I$.

Daí segue facilmente que $I_n = I_{n+1} = \ldots$ □

(2.3) Teorema - Seja R um anel com unidade. Então, RG é artiniano se e somente se R é artiniano e G é finito.

Prova ($\Longrightarrow$) - Considerando o epimorfismo $\varepsilon: RG \longrightarrow R$, definido no §2 do Capítulo I, vem imediatamente que R é artiniano.

Pelo teorema de Wedderkurn, $\frac{R}{J(R)} = \bigoplus_i M_{n_i}(D_i)$ em que os D_i são anéis com divisão.

Sejam $f: R \longrightarrow M_{n_1}(D_1)$ o epimorfismo natural e $f^*: RG \longrightarrow M_{n_1}(D_1)G$ o epimorfismo de anéis definido no exercício 1, §2, Capítulo I.

Como RG é artiniano, $M_{n_1}(D_1)G$ é artiniano. Se K denota o centro de D_1, do Lema (2.2) vem que KG é artiniano e do Teorema (2.1) segue que G é finito.

($\Longleftarrow$) A recíproca é imediata, pois o R-módulo RG é finitamente gerado, logo artiniano. Como os ideais à esquerda de RG são em particular R-submódulos, a tese segue imediatamente. □

§3. Anéis noetherianos

Analogamente, pode-se fazer um estudo semelhante dos anéis de grupo noetherianos.

No entanto, ainda não foi obtida a caracterização dos grupos G para os quais KG é noetheriano.

A família de grupos definidos abaixo aparece naturalmente neste estudo.

(3.1) Definição - Um grupo G diz-se noetheriano se para toda cadeia $H_1 \subset H_2 \subset \ldots \subset H_n \subset \ldots$ de subgrupos de G, existe $r \in N$ tal que $H_r = H_{r+h}$, para todo inteiro positivo h.

(3.2) Proposição - Se RG é um anel noetheriano, então R e G são noetherianos.

Prova - Considerando novamente o epimorfismo $\varepsilon: RG \longrightarrow R$, definido no §2 do Capítulo I, vem imediatamente que R é noetheriano.

Seja agora $H_1 \subset H_2 \subset \ldots \subset H_n \subset \ldots$ uma cadeia de subgrupos de G. Então,

$\Delta(G: H_1) \subset \Delta(G: H_2) \subset \ldots \subset \Delta(G: H_n) \subset \ldots$ é uma cadeia de ideais à esquerda de RG. Da hipótese, existe r N tal que $\Delta(G: H_r) = \Delta(G: H_{r+1}) = \ldots$

Daí pode-se concluir que $H_r = H_{r+1} = \ldots$. De fato, seja $h \in H_j$, $j > r$. Então, $h-1 \in \Delta(G: H_j) = \Delta(G: H_1)$ e suponhamos por absurdo, que $h \notin H_r$.

Agora, seja $Q = \{q_i\}_{i\in I}$ um transversal à esquerda de H_r em G, com $q_1 = 1$. Então, h se escreve na forma: $h = q'h'$, com $q' \in Q$, $q' \neq 1$, $h' \in H_r$. Logo,

$$h - 1 = q'h'-1 = q'(h'-1) + (q'-1).$$

Como $q'(h'-1) \in \Delta(G:H_r)$, vem que $q'-1 \in \Delta(G,H_r)$.

Pela proposição (3.2) do Capítulo I, $q'-1$ pode ser escrito na forma:

$$q'-1 = \sum_{i,j} r_{ij}q_i(h_j-1) = \sum_{i,j} r_{ij}q_ih_j - \sum_i (\sum_j r_{ij})q_i ,$$

$h_j \in H_r$, $r_{ij} \in R$, $h_j \neq 1$

Como os elementos do suporte do segundo membro são dois a dois distintos, vem que

$$\sum_{i,j} r_{ij}q_ih_j = 0 \quad , \quad \sum_i(\sum_j r_{ij})q_i = q'-1 .$$

Da primeira equação decorre que todos os r_{ij} são nulos; a segunda equação leva então a uma contradição. □

Até hoje não foi possível decidir se a recíproca desta proposição é verdadeira.

Apresentamos a seguir uma família de grupos que são os únicos exemplos conhecidos de grupos noetherianos.

(3.3) Definição - Um grupo G diz-se policíclico-por-finito se existem subgrupos $\{1\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$ tais que $G_i \lhd G_{i+1}$, $0 \leq i \leq n-1$, e os quocientes $\frac{G_{i+1}}{G_i}$ são finitos ou cíclicos infinitos.

(3.4) Lema - Seja G um grupo que admite um subgrupo normal H tal que H e G/H são noetherianos. Então, G é noetheriano.

Prova - Seja $G_0 \subset G_1 \subset \ldots \subset G_n \subset \ldots$ uma cadeia ascendente de subgrupos de G.

Então, $G_0 \cap H \subset G_1 \cap H \subset \ldots \subset G_n \cap H \subset \ldots$ é uma cadeia ascendente de subgrupos de H, logo existe n_0 tal que

$G_{n_0} \cap H = G_{n_0+h} \cap H$, $h \geq 1$.

Por outro lado, $\frac{G_0H}{H} \subset \frac{G_1H}{H} \subset \ldots \subset \frac{G_nH}{H} \subset \ldots$ é uma cadeia de subgrupos de $\frac{G}{H}$, logo existe n_1 tal que

$$\frac{G_{n_1}H}{H} = \frac{G_{n_1+h}H}{H} \quad , \quad h \geq 1 .$$

Chamando t ao maior dos inteiros n_0, n_1 , vem imediatamente que $G_tH = G_iH$, $G_t \cap H = G_i \cap H$, $\forall i \geq t$.

Seja agora $g \in G_i$, com $i \geq t$. Como $gH = kH$, para algum $k \in G_t$, vem que $k^{-1}g \in H \cap G_i = H \cap G_t$. Logo, $k^{-1}g \in H \cap G_t$ e, como $k \in G_t$, vem que $g \in G_t$.

Isto mostra que $G_i = G_t$, $\forall i \geq t$.

(3.5) Proposição - Se G é um grupo policíclico-por-finito, então G é noetheriano.

Prova - Observamos primeiro que os grupos cíclicos infinitos são noetherianos. De fato, seja $H = \langle g \rangle$ um grupo cíclico infinito, e seja

$$H_0 \subset H_1 \subset \ldots \subset H_n \subset \ldots$$

uma cadeia ascendente de subgrupos de H, com $H_i = \langle g^{n_i} \rangle$, $n_i \in N$.

Como $H_i \subset H_{i+1}$, $g^{n_i} = (g^{n_{i+1}})^{\ell}$, e $n_{i+1} | n_i$, $\forall i$. Em particular, $n_i | n_0$, $\forall i$, e daí é fácil concluir que a cadeia é estacionária.

Agora, seja $\{1\} = G_0 \subset G_1 \subset \ldots \subset G_n \subset \ldots$ uma cadeia de subgrupos de G como na definição (3.3).

Faremos a demonstração por indução em n. Se n = 1, $G = G_1$ é finito ou cíclico infinito, logo noetheriano.

Suponhamos agora n > 1 e que a proposição seja verdadeira para todo grupo que admite uma cadeia de subgrupos como a da definição (3.3), de comprimento menor ou igual a n-1.

Ora, G_n/G_{n_1} é finito ou cíclico infinito, logo noetheriano, e G_{n-1} é noetheriano pela hipótese de indução. Logo, $G = G_n$ é noetheriano, pela proposição (3.4). □

(3.6) Lema - Seja $H \lhd G$, tal que G/H é finito ou cíclico infinito. Sejam M um RG-módulo, N um RH-submódulo de N, com M = RG.N. Se o RH-módulo N é noetheriano, então o RG-módulo M também é noetheriano.

Prova - Suponhamos primeiro que $\left|\frac{G}{H}\right| = n$. Então, existem $s_1, s_2, \ldots, s_n \in G$ tais que $G = \bigcup_i s_i H$.

Temos então que $M = s_1 N + \ldots + s_n N$. Vamos demonstrar que cada sN é um RH-módulo noetheriano. Primeiro observamos que cada sN é, de fato, um RH-módulo. Para isso, basta verificar que sN

é fechado em relação à multiplicação por elementos de H. Mas, se $h \in H$ e $n \in N$ então $hsn = sh'n$, para algum $h' \in H$, pois $H \lhd G$.

Seja agora T um submódulo de N, e seja

$$T' = \{n \in N \mid sn \in T\}.$$

Verifica-se facilmente que T' é um submódulo de N, e que $T = sT'$.

Assim, dada uma cadeia $sT'_1 \subset sT'_2 \subset \ldots \subset sT'_n \subset \ldots$ de submódulos de sN, em que os T'_i são definidos como acima, a cadeia $T'_1 \subset T'_2 \subset \ldots \subset T'_n \subset \ldots$ de submódulos de N é estacionária, logo sN é um RH-módulo noetheriano.

Portanto, obtém-se que M é um RH-módulo noetheriano. Como todo RG-submódulo de M é também um RH-submódulo, vem imediatamente que M é um RG-módulo noetheriano.

Suponhamos agora que $\frac{G}{H} = \langle \bar{x} \rangle$, com $\bar{x}$ de ordem infinita. Então, $G = \bigcup_{i \in Z} x^i H$. Como $M = RGN$, vem que todo elemento $\alpha \in M$ se escreve na forma:

$$= \sum_{i \in Z} x^i n_i \ , \text{ com } n_i \in N \ .$$

Seja agora $M_0 \neq \{0\}$ um submódulo arbitrário de M. Vamos mostrar que M_0 é finitamente gerado, donde seguirá que M é noetheriano.

Dado um elemento $\alpha = \sum_{i \in Z} x^i n_i$, não nulo, chamaremos coeficiente dominante de α ao elemento n_t correspondente à maior potência de x que efetivamente comparece na expressão de α, isto é, n_t é o coeficiente dominante de α se $n_t \neq 0$ mas $n_i = 0$, para todo $i > t$.

Seja então N_0 o subconjunto de N formado pelo elemento 0 e por todos os coeficientes dominantes de elementos de M_0 .

Verifica-se trivialmente que N_0 é um RH-submódulo de N. Logo, é finitamente gerado. Seja então $\{a_1,a_2,\ldots,a_\ell\}$ um conjunto de geradores de N_0.

Tomemos elementos $m_1,m_2,\ldots,m_\ell$ de M cujos coeficientes dominantes são respectivamente $a_1,a_2,\ldots,a_\ell$. Podemos escolhê-los com a propriedade de que o termo de maior grau é da forma $a_i x^k$, em que o inteiro k não depende de i, e tais que não apresentam potências negativas de x. (referir-nos-emos a esta última propriedade como a propriedade (*)). De fato, sejam $a_1x^{r_1},\ldots,a_\ell x^{r_\ell}$ os termos correspondentes aos coeficientes dominantes dos m_i , e seja $r = \max\{r_i\}$. Então, os elementos $x^{r-r_i}m_i$ têm têrmo de maior grau da forma $a_i x^r$, e são elementos de M_0 .

Agora, para que satisfaçam a propriedade (*), basta multiplicar por uma potência suficientemente grande de x.

Seja agora $u_1 \in M_0$, e seja $u = x^n u_1 \in M_0$, tal que u tem a propriedade (*), e o termo de maior grau tem a forma: ax^q , com $q \geq k$.

Então, $a \in N_0$, logo a é uma soma: $a = \sum_i y_i a_i$, $y_i \in RH$.

Tomemos então a soma: $\sum_i y_i m_i$. Este é um elemento de M_0 , com a propriedade (*). Multiplicando-o por x^{q-k} , vem que o elemento $n = x^{q-k}\sum y_i m_i$ ainda pertence a M_0 , tem a propriedade (*), e o termo de maior grau é ax^q .

Podemos escrever n na forma: $n = ax^q + n'$, em que n' tem a propriedade (*), e tal que na sua expressão só aparecem as potências $1,x,x^2,\ldots,x^{q-1}$.

Analogamente, temos que $u = ax^q + u'$, em que u' tem as mesmas propriedades que n'.

Logo, $u = n-n' + u'$. Chamando $n_1 = u'-n'$, vem que n_1 pertence a M_0 (pois $u,n \in M_0$), tem a propriedade * e em n_1 só aparecem as potências $1,x,\ldots,x^{q-1}$.

Repetindo o argumento empregado para u, podemos escrever n_1 na forma: $n_1 = n_2+n_3$, com n_2 no submódulo de M_0 gerado por $m_1,\ldots,m_\ell$, e $n_3 \in M_0$, com a propriedade (*), e tal que na sua expressão só aparecem as potências $1,x,\ldots,x^{q-2}$.

Aplicando este processo um número suficiente de vezes, podemos escrever u na forma: $u=m+m'$, em que $m \in [m_1,\ldots,m_\ell] \subset M_0$, $m'_0 \in M_0$ tem a propriedade (*) e na expressão de m' só aparecem as potências $1,x,\ldots,x^{p-1}$.

Ora, m' pertence então a $L = N+xN+\ldots+x^{p-1}N$, que é um RH-módulo noetheriano (para ver isto, basta repetir o argumento empregado para mostrar que M é noetheriano, quando $|G/H| < \infty$). Assim, o RH-submódulo $L \cap M_0$ é finitamente gerado. Seja $\{m_{\ell+1},\ldots,m_t\}$ um conjunto de geradores de $L \cap M_0$.

Então, $u = \sum_{i=1}^{\ell} \alpha_i m_i + \sum_{i=\ell+1}^{k} \beta_i m_i$, $\alpha_i \in RG$, $\beta_i \in RH$, e $u_1 = x^{-n}u$ é uma combinação linear dos m_i , com coeficientes em RG; logo, M_0 é gerado pelo conjunto $\{m_i\}_{1\le i\le k}$. □

(3.7) Teorema - Sejam G um grupo policíclico-por-finito e R um anel noetheriano. Então, RG é noetheriano.

Prova - Seja $\{1\} = G_0 \subset G_1 \subset \ldots \subset G_n = G$ uma cadeia como na definição (3.3). Procederemos por indução em n. Se n=1, tomando, no

Lema (3.6), H = {1} , M = RG , N=R , vem que RG é noetheriano.

Suponhamos agora o teorema demonstrado para todo grupo que admite uma cadeia como a da definição (3.3), de comprimento menor ou igual a n-1 ($n \geq 1$). Então, pela hipótese de indução, RG_{n-1} é noetheriano.

Tomando $H = G_{n-1}$, $M = RG$, $N = RG_{n-1}$, o Lema (3.6) mostra imediatamente que RG é noetheriano.

Conjectura-se que todos os grupos noetherianos sejam policíclicos-por-finitos. A verificação desta conjectura provaria a recíproca do Teorema (3.7).

§4. O Radical de Jacobson

Apresentamos aqui alguns resultados e conjecturas sobre o radical de Jacobson de KG.

Primeiramente, observamos que, no caso de grupos finitos é fácil decidir em que condições RG é semi-simples, isto é, J(KG)=0.

De fato, temos a seguinte

(4.1) Proposição - Seja G um grupo finito. Então, J(KG) = 0 se e somente se car K $\nmid$ |G|.

Prova - Suponhamos primeiro que J(KG) = 0. Como G é finito, KG é artiniano, pelo Teorema (2.1). Logo, KG é completamente redutível, e pelo corolário 4.7 do capítulo I, temos que car K x |G|.

Reciprocamente, temos que, se car $K \nmid |G|$, pelo corolário mencionado acima, KG é completamente redutível, logo $J(KG) = 0$.

Talvez o provlema mais difícil envolvendo anêis de grupo de grupos infinitos seja o de determinar condições necessárias e suficientes para que $J(KG) = 0$, ou , mais geralmente, determinar a estrutura de $J(KG)$.

Possivelmente, se car $K = 0$, $J(KG)$ é sempre trivial, mesmo que G seja infinito. Na direção desta conjectura, temos os seguintes teoremas:

(4.2) Teorema (Villamayor, 59): Se car $K = 0$ e G é solúvel, então $J(KG) = 0$.

(4.3) Teorema (Amitsur, 59): Se car $K = 0$ e K é uma extensão transcendente de seu corpo primo, então $J(KG) = 0$.

Observamos ainda que, graças aos trabalhos de Amitsur, sabe-se que para demonstrar que $J(KG) = 0$ no caso em que car $K = 0$, K é uma extensão algébrica de seu corpo primo Q, é suficiente demonstrar que $J(QG) = 0$.

Agora, conforme a Proposição (4.1), se car $K = p$ e G é finito, com elementos de ordem p, então $J(KG) \neq \{0\}$. No entanto, como o radical de Jacobson de um anel artiniano é nilpotente [ver 10, p. 67], podemos ao menos afirmar que, nestas condições, $J(KG)$ é nilpotente.

Assim, se G é um grupo arbitrário e car $(K) = p$, a conjectura clássica é que $J(KG)$ é um ideal nil. (Um ideal I de um anel R diz-se nil se $\forall x \in I$, $\exists n \in N$ tal que $x^n = 0$).

Nesta direção, os resultados mais importantes são os seguintes:

(4.4) Teorema (Villamayor, 59): Se car K = p e G é solúvel, sem elementos de ordem p, então J(KG) = 0 .

(4.5) Teorema (Passman, 62): Se car K = p , K é uma extensão transcendente de seu corpo primo e G não tem elementos de ordem p, então J(KG) = 0 .

A condição "G não tem elementos de ordem p" não é, no entanto, necessária: existem exemplos de grupos G, com p-elementos, tais que J(KG) = 0, para todo corpo de característica p. Para referências adicionais, ver [13, p. 295].

O problema se torna bastante mais difícil se se procura determinar a estrutura de J(KG). Para se ter uma idéia do grau de dificuldade desta questão, observamos que os trabalhos recentes nesta direção estão restritos ao caso em que car K = p e G é finito. Os resultados, por outro lado, não dão informações sobre a estrutura de J(KG) mas sim sobre o seu índice de nilpotência ou sua dimensão.

Para referências mais detalhadas, recomendamos os trabalhos de D.A.R. Wallace (por exemplo: Proc. Edinb. Math. Soc., II, Ser 16 (1968), 127-134).

BIBLIOGRAFIA

[1] A. Cayley - On the theory of groups as depending on the symbolic equation $\Theta^n = 1$, *Philos. Mag.* 7 (1854), 40-47.

[2] D.B. Coleman - Finite groups with isomorphic group algebras, *Trans. Amer. Math. Soc.* 105 (1962), 1-8.

[3] I. G. Connell - On the group ring, *Can. J. of Math.* 15 (1963), 650-685.

[4] C.W. Curtis e I. Reiner - *Representation theory of Finite Groups and Associative Algebras*, Interscience, New York, 1962.

[5] W.A. Deskins - Finite abelian groups with isomorphic group algebras, *Duke Math. J.* 23 (1956), 35-40.

[6] T. Hawkins - Hypercomplex Numbers, Lie Groups and the creation of Group Representation Theory, *Arch. History Exact Sc.* 8 (1972), 243-287.

[7] S.A. Jennings - On the structure of the group ring of a p-group over a modular field, *Trans. Amer. Math. Soc.* 50 (1941), 175-185.

[8] G. Karpilovsky - On group rings of finite metabelian groups, *J. Austral. Math. Soc.* 28 (1979), 378-384.