UNIVERSIDADE ESTADUAL PAULISTA
"JÚLIO DE MESQUITA FILHO"
Campus de São José do Rio Preto

Cohomologia de Grupos e Invariantes Algébricos

Anderson Paião dos Santos

Orientadora: Profª Drª Ermínia de Lourdes Campello Fanti

Dissertação apresentada ao Instituto de Biociências, Letras e Ciências Exatas da Universidade Estadual Paulista, Câmpus de São José do Rio Preto, como parte dos requisitos para obtenção do título de Mestre em Matemática.

São José do Rio Preto, SP

2006

COMISSÃO JULGADORA

Titulares

Ermínia de Lourdes Campello Fanti

Professora Doutora - IBILCE - UNESP

Orientadora

Oziride Manzoli Neto

Professor Doutor - ICMC - USP

1º Examinador

Maria Gorete Carreira Andrade

Professora Doutora - IBILCE - UNESP

2º Examinador

Suplentes

Dirceu Penteado

Professor Doutor - UFSCar

1º Suplente

Denise de Mattos

Professora Doutora - IBILCE - UNESP

2º Suplente

À minha mãe
Albertina,
dedico.

Agradecimentos

Agradeço a Deus, por me conceder a graça de concluir mais esta jornada, por ter me fortalecido nos momentos que mais precisei e pelas pessoas que colocou em meu caminho e que com certeza foram fundamentais para esta conquista. Em especial quero deixar aqui meus sinceros agradecimentos:

À minha mãe Albertina, pela educação que me deu, por ter me apoiado em todas as decisões que tomei e pelas orações.

À Profª Drª Ermínia de Lourdes Campello Fanti, por ter aceito me orientar, pela amizade, pelos conselhos, pelas disponibilidade e paciência que teve em todos os momentos que precisei de sua ajuda.

À Profª Drª Maria Gorete Carreira Andrade, pela amizade, pelos conhecimentos que me foram transmitidos durante a disciplina de "Introdução à Topologia Algébrica" e pela sua alegria sempre presente.

À Profª Drª Denise de Mattos, pelas sugestões durante o Exame Geral de Qualificação.

Aos professores do IBILCE/UNESP - São José do Rio Preto, de modo especial agradeço à Profª Drª Aparecida Francisco da Silva, pela amizade e acolhimento, e ao Prof. Dr. Adalberto Spezamiglio, pelas correções finais do abstract.

Aos professores da FCT/UNESP - Presidente Prudente, pela minha formação. Em especial agradeço aos professores Dr. Ivam Resina e Olga pelo apoio.

À direção, professores, funcionários e alunos do Colégio Cooperativo, pelo apoio e torcida.

Aos amigos Fábio, Leandro (Uru), Mariene e Taciana, pelos momentos agradáveis que passamos em Rio Preto.

Aos amigos de pós-graduação: Aline, Cátia, Cibele, Durval, Elen, Évelin, Fernanda, Francielle, Giovana, Júlio, Marcus, Marina, Michele, Miriam, Rubens e Tatiane, pelos momentos inesquecíveis que passamos durante esses anos.

À minha irmã Nyejda, pelo apoio e pelas diversas vezes que me levou até a rodoviária.

À Maria Odete Pimentel Staut, pelas correções no abstract.

Que Deus os abençoe.

"Por vezes sentimos que aquilo que fazemos não é senão uma gota de água no mar. Mas o mar seria menor se lhe faltasse uma gota."

(Madre Teresa de Calcutá)

Sumário

Resumo

Para todo grupo G infinito, finitamente gerado, pode-se obter para o invariante algébrico "end", mais precisamente o número de ends $e(G)$, uma fórmula cohomológica 1-dimensional. O principal objetivo deste trabalho é apresentar, sob certas hipóteses, uma fórmula cohomológica 1-dimensional para o invariante algébrico $e(G, H)$, definido por Scott e Houghton, onde H é um subgrupo de G (Teorema de Swarup). Para tanto, o conceito de subconjunto H-quase invariante de G e resultados como a interpretação do grupo de cohomologia $H^1(G, M)$ em termos de derivações (à direita), onde M é um $\mathbb{Z}G$-módulo, e o Lema de Shapiro, são resultados imprescindíveis. Algumas relações desses invariantes com ends de espaços são também apresentadas.

Palavras chave: Cohomologia de Grupos, Lema de Shapiro, Ends de Grupos e Pares de Grupos, Ends de Espaços.

Abstract

For all infinite group G, finitely generated, one can obtain for the algebric invariant "end", more precisely the number of ends $e(G)$, a cohomological 1-dimensional formula. The main objective of this work is to present, under certain hypotheses, a cohomological 1-dimensional formula for the algebric invariant $e(G, H)$, defined by Scott and Houghton, where H is a subgroup of G (Swarup's Theorem). In order to do so, the concept of subset H-almost invariant of G and results like the interpretation of the cohomological group $H^1(G, M)$ in terms of derivations (to the right), where M is a $\mathbb{Z}G$-module, and the Shapiro's Lemma, are fundamental results. Some relations of these invariants with space ends are also presented.

Key words: Cohomology of Groups, Shapiro's Lemma, Ends of Groups and Pairs of Groups, Ends of Spaces.

Introdução

O objetivo principal deste trabalho é apresentar, sob certas condições, uma fórmula cohomológica 1-dimensional para o *número de ends* $e(G, H)$, de um par grupo (G, H), onde G indica um grupo finitamente gerado e H um subgrupo de G de índice infinito. Tal número é um invariante algébrico, isto é, se (G, H) e (G', H') são pares de grupos isomorfos, ou seja, existe um isomorfismo $\mu : G \longrightarrow G'$, com $\mu(H) = H'$, então $e(G, H) = e(G', H')$.

A teoria de *ends de grupos*, e portanto de *número de ends*, $e(G)$, de um grupo G, teve sua origem na teoria de *ends de espaços*, por Hopf ([11]) e Freudenthal ([8]). Hopf e Freudenthal mostraram que se um grupo *finitamente gerado* atua de uma forma "boa" sobre um espaço, a estrutura dos ends do espaço depende somente do grupo, de modo que pode-se definir o número de ends do grupo. Mais tarde, Specker ([26]), usando um tratamento algébrico, estendeu a definição do número de ends de modo a abranger *grupos arbitrários*, não apenas os finitamente gerados. Importantes resultados sobre ends de grupos têm sido obtidos. Por exemplo, pode-se provar que a função $e(G)$ assume somente os valores $0, 1, 2$ ou ∞.

Posteriormente o número de ends $e(G, H)$, para o par grupo (G, H), onde H é um subgrupo de G, foi definido por Houghton ([12]) e Scott ([22]) (de modo independente), e é uma extensão natural do conceito de número de ends de um grupo, visto que $e(G, \{1\}) = e(G)$. Desde então, generalizações (do conceito de número de ends de um grupo) para ends de pares (G, H) e pares $(G, \mathfrak{F})$, onde $\mathfrak{F}$ é uma família de subgrupos de G, têm sido objeto de estudos e

pesquisas ([1], [2], [15], [22] e [28]), com diversas aplicações.

Há uma forte relação entre ends de grupos (e pares) e cohomologia de grupos. Quando G é um grupo infinito, finitamente gerado, é válida a seguinte fórmula cohomológica 1-dimensional para $e(G)$:

$$e(G) = 1 + rank_{\mathbb{Z}} H^1(G, \mathbb{Z}G). \tag{1}$$

Como uma extensão (parcial) desse resultado, Swarup em [28] mostrou que para certos tipos especiais de pares de grupos, é válida uma fórmula envolvendo grupos de cohomologia 1-dimensional para o end do par grupo $e(G, H)$, ou seja:

Se um par (G, H) é tal que G é finitamente gerado, H é um subgrupo de índice infinito em G, e $e(G, N) = 1$, para todo subgrupo N normal de H, com $H/N \simeq \mathbb{Z}$, então

$$e(G, H) = 1 + rank_{\mathbb{Z}} H^1\big(G, \mathbb{Z}(G/H)\big). \tag{2}$$

Para a prova, Swarup ([28]) usou argumentos geométricos (ver também [9], Proposição 4.5.19). Posteriormente, uma demonstração algébrica desse resultado foi apresentada por Kropholler e Roller em [15]. O principal objetivo deste trabalho, como mencionamos anteriormente, é apresentar, de uma forma bastante detalhada, a prova (algébrica) de (2).

Nosso trabalho está dividido em três capítulos e um apêndice.

No *Apêndice*, são apresentados alguns pré-requisitos, conceitos e resultados de Álgebra Homológica, em especial da Teoria de Módulos, com destaque para *Resoluções Livres e Projetivas* (mais especificamente, *Padrão* e *Bar* de $R = \mathbb{Z}$ ou $\mathbb{Z}_2$ sobre RG, onde RG indica o anel grupo de G) e *Posto* ou *Rank de Módulos Livres*. Esses pré-requisitos são úteis para definirmos *Cohomologia de Grupos* e para melhor compreensão do texto, porém são dispensáveis para quem tem familiaridade com tais tópicos.

Em geral (no apêndice), R indica um anel com unidade, no entanto, em todo o nosso trabalho, sempre que nos referimos a RG-módulos, R se restringe a $\mathbb{Z}$ ou $\mathbb{Z}_2$.

No *Capítulo* 1, apresentamos um estudo de Cohomologia de Grupos. Inicialmente definimos os Grupos de Cohomologia n-dimensionais de um grupo G com coeficientes em um RG-módulo M (à esquerda), $H^n(G, M)$ e apresentamos alguns exemplos. Destacamos, dentre outros, os seguintes resultados que são úteis na prova de (2): a interpretação de $H^1(G, M)$ em termos do Grupo das Derivações (Proposição 1.2.2), e o Lema de Shapiro (Proposição 1.6.1) que relaciona o grupo de cohomologia de um grupo G com a de seus subgrupos, ou seja:

Sejam G um grupo, H um subgrupo de G e M um RH-módulo (à esquerda) ($R = \mathbb{Z}$ ou $\mathbb{Z}_2$). Considerando a inclusão $i : H \longrightarrow G$ e $\pi : Coind_H^G M \longrightarrow M$ dada por $\pi(\phi) = \phi(1)$, para todo $\phi \in Coind_H^G M$. Então, a aplicação induzida $(i, \pi)^* : H^*(G, Coind_H^G M) \longrightarrow H^*(H, M)$ é um isomorfismo.

Observamos que a Cohomologia de Grupos pode ser definida com coeficientes em um RG-módulo à *esquerda* ou um RG-módulo à *direita*. Não há nenhum problema em considerar uma outra situação, pois todo RG-módulo à esquerda M admite também uma estrutura natural (induzida) de RG-módulo à direita (e vice-versa, Proposição A.7.2), e os grupos de cohomologia obtidos de um modo ou de outro serão isomorfos. Em [4], o autor define grupos de cohomologia por considerar RG-módulos à esquerda. Já em [15], os autores trabalham com módulos à direita. Algumas pequenas diferenças podem ser observadas em tratar uma ou outra situação. Nesse sentido, apresentamos (no apêndice) as resoluções Padrão/Bar tanto para RG-módulos à esquerda como para RG-módulos à direita, e nesse capítulo, a interpretação de $H^1(G, M)$ em termos do Grupo das Derivações são tratadas por considerar M um RG-módulo à esquerda ou à direita.

No *Capítulo* 2, inicialmente (Seções 2.1 e 2.2) definimos o *número de ends*, $e(G)$, de um grupo G ([7], [23]) e apresentamos alguns resultados, com destaque para a Proposição 2.2.1, que fornece a fórmula cohomológica 1-dimensional (1) para $e(G)$, quando G é infinito e finitamente gerado, e, na Seção 2.3, definimos o *número de ends de um par* (G, H), $e(G, H)$, onde H é um subgrupo

de G ([12], [22]). Isto é feito usando um tratamento puramente algébrico. Encerrando esse capítulo, na Seção 2.4, definimos o *número de ends de um espaço topológico* Hausdorff, com base enumerável, localmente compacto, conexo e localmente conexo, e relacionamos ends de grupos finitamente gerados G e de pares de grupos (G, H), com ends de espaços, mais especificamente com espaços especiais, o Grafo de Cayley de G (Proposições 2.4.1 e 2.4.2). Também ilustramos, baseado num resultado de Scott ([22]), como obter $e(G, H)$, quando G é o grupo fundamental de uma superfície fechada S e H é o grupo fundamental de uma sub-superfície Y de S, *compacta* e *incompressível* (em S). Não é nosso objetivo demonstrar os resultados apresentados na seção, mas apenas ilustrar uma bela conexão entre a teoria de ends de grupos e ends de espaços topológicos.

Por último, no *Capítulo* 3, nos dedicamos essencialmente à prova de (2). Inicialmente vários resultados auxiliares são provados, dentre eles destacamos:

(1º) *Os ends de um par grupo (G, H) correspondem aos subconjuntos H-quase invariantes E de G, que satisfazem $E = HE$ e que não são H-finitos.* (Proposição 3.1.1)

(2º) *Sejam G um grupo finitamente gerado, H um subgrupo de índice infinito de G, E um subconjunto H-quase invariante de G e $N = \{h \in H \mid hE = E\}$. Se N é um subgrupo normal de H, $hE \cap E = \varnothing$, para todo $h \in H - N$, e $HE = G$, então $e(G, N) \geqslant [H : N]$.* (Proposição 3.1.2)

(3º) Se $\delta \in Der(G, I(A))$ e $N = Ker\left(\delta^*\big|_H\right)$, onde $\delta^* : G \longrightarrow A$ é definida por $\delta^*(g) = \delta(g)(1)$, então $e(G, N) \geqslant [H : N]$. (Lema 3.2.5)

(4º) *Se G é finitamente gerado e H é um subgrupo de índice infinito, então*

$$e(G, H) = 1 + rank_{\mathbb{Z}} Ker\ \rho,$$

onde

$$\begin{array}{rl} \rho : & H^1(G, \mathbb{Z}(G/H)) = \dfrac{Der(G, \mathbb{Z}(G/H))}{P(G, \mathbb{Z}(G/H))} \longrightarrow Hom(H, \mathbb{Z}) \\ & [\delta] = \delta + P(G, \mathbb{Z}(G/H)) \longmapsto \delta^*\big|_H \end{array} \quad \text{(Proposição 3.3.2)}$$

Daí, utilizando esses resultados e outros anteriormente apresentados, como a interpretação de $H^1(G, M)$ em termos do grupo das derivações (à direita) e o Lema de Shapiro, a prova do Teorema de Swarup (2) é concluída.

Um caso particular interessante desse teorema é:

Seja G um grupo finitamente gerado. Se $e(G) = 1$ e G tem um subgrupo H cíclico infinito, então $e(G, H) = 1 + rank_{\mathbb{Z}} H^1(G, \mathbb{Z}(G/H))$. (Corolário 3.3.3)

Finalizando o capítulo apresentamos alguns exemplos (Exemplo 3.3.1) e fazemos algumas considerações sobre o invariante end "$E(G, H)$" definido por Andrade e Fanti ([1]).

Capítulo 1

Cohomologia de Grupos

Neste capítulo, apresentamos um estudo de cohomologia de grupos. Em especial apresentamos, utilizando a resolução bar, uma interpretação do grupo de cohomologia 1-dimensional em termos de derivações, e o Lema de Shapiro.

Por todo este capítulo, R indica o anel $\mathbb{Z}$ dos inteiros ou o corpo $\mathbb{Z}_2$.

1.1 Grupos de Cohomologia

Definição 1.1.1. Sejam $\cdots \longrightarrow F_3 \xrightarrow{\partial_3} F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} R \longrightarrow 0$, ou simplesmente, $\varepsilon : F \longrightarrow R$ uma resolução projetiva de R sobre RG (com R visto como um RG-módulo trivial) e M um RG-módulo (à esquerda). Consideremos o complexo de cocadeias (à esquerda)

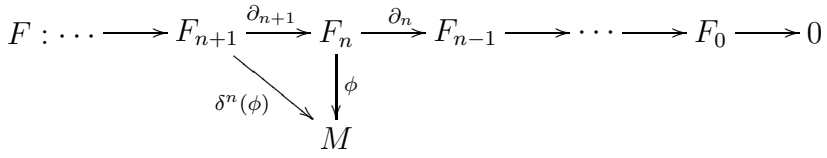
$$Hom_{RG}(F, M) : 0 \longrightarrow Hom_{RG}(F_0, M) \xrightarrow{\delta^0} Hom_{RG}(F_1, M) \xrightarrow{\delta^1} \cdots$$

com o operador cobordo dado por

$$\delta^n(\phi) := \phi \circ \partial_{n+1} \ ,$$

para todo $\phi \in Hom_{RG}(F_n, M)$.

Para compreendermos melhor a definição do operador cobordo, vejamos o diagrama seguinte



O ***n*-ésimo grupo de cohomologia** de G (sobre R) ***com coeficientes no módulo (à esquerda) M*** é, para todo $n \in \mathbb{Z}$, definido por

$$H^n(G, M) := H^n[Hom_{RG}(F, M)] = \frac{Ker(\delta^n)}{Im(\delta^{n-1})} \, .$$

A coleção $\{H^n(G, M)\}_{n\in\mathbb{Z}}$ é denominada ***cohomologia*** do grupo G com coeficientes em M.

Observação 1.1.1.

(1) Sejam $\varepsilon : F \longrightarrow R$ e $\varepsilon' : F' \longrightarrow R$ duas resoluções projetivas de R sobre RG. Uma vez que $Hom_{RG}(\_\_, M)$ é um funtor aditivo contravariante, temos, pela Proposição A.8.3, que $Hom_{RG}(F, M)$ e $Hom_{RG}(F', M)$ são homotopicamente equivalentes. Conseqüentemente, da Proposição A.2.4, obtemos que para todo $n \geqslant 0$,

$$H^n[Hom_{RG}(F, M)] \simeq H^n[Hom_{RG}(F', M)] \, ,$$

ou seja, os grupos de cohomologia independem da resolução escolhida.

(2) $H^n(G, M) = 0$, para todo $n < 0$.

(3) Similarmente, pode-se definir os ***grupos de cohomologia de G com coeficientes em um RG-módulo à direita M***, também denotado por $H^n(G, M) := H^n\left[Hom_{RG}(F, M)\right]$, com F agora uma resolução projetiva (de RG-módulos ***à direita***) de R sobre RG (e M um RG-módulo *à direita*). A menos de isomorfismos os mesmos *grupos* são obtidos. A base para isso é o fato (observado também no apêndice) de que todo RG-módulo à direita M pode ser considerado como um RG-módulo à esquerda M' por meio da regra $m.g := g^{-1}.m$ ($m \in M$ e $g \in G$), e conseqüentemente temos que $H^n\big(Hom_{RG}(F, M)\big) \simeq H^n\big(Hom_{RG}(F', M')\big)$,

onde F' é a resolução projetiva (à esquerda) obtida considerando-se os módulos (à esquerda) F'_n, obtidos a partir dos módulos (à direita) F_n, via a regra anterior.

Queremos agora, caracterizar os grupos de cohomologia no nível $n = 0$. Para isto, vejamos alguns conceitos importantes.

Na definição a seguir, G denota um grupo e M um RG-módulo (à esquerda).

Definição 1.1.2.

(a) O ***grupo de invariantes*** de M, denotado por $\boldsymbol{M^G}$, é definido por

$$M^G = \{m \in M \mid g.m = m, \ \forall \ g \in G\}.$$

(b) O ***grupo de coinvariantes*** de M, denotado por $\boldsymbol{M_G}$, é dado pelo quociente de M pelo subgrupo aditivo gerado pelos elementos da forma $g.m - m$ ($g \in G, \ \ m \in M$), isto é,

$$M_G = \frac{M}{\langle g.m - m \mid g \in G, \ \ m \in M \rangle}$$

Observação 1.1.2.

(1) Se a G-ação (à esquerda) sobre M for trivial, isto é, $g.m = m$ para todo $m \in M$ e para todo $g \in G$, temos que $M^G = M_G = M$.

(2) A G-ação (à esquerda) sobre M induz a G-ação trivial sobre M^G e assim, M^G é um RG-módulo trivial. Temos que M^G é o maior submódulo de M no qual G atua trivialmente.

Definição 1.1.3. (***G*-ação diagonal**) Sejam M e N dois RG-módulos (à esquerda). Temos que a G-ação (à esquerda) sobre M e N induz uma G-ação (à esquerda) sobre $Hom_R(M, N)$ dada por

$$\begin{aligned} v : G \times Hom_R(M,N) &\longrightarrow Hom_R(M,N) \\ (g, \phi) &\longmapsto g.\phi; \ \ (g.\phi)(m) = g.\phi(g^{-1}m), \end{aligned}$$

para todo $m \in M$, onde $g.\phi(g^{-1}m)$ indica g atuando no elemento $\phi(g^{-1}m) \in N$.

Temos também que a G-ação (à esquerda) sobre M e N induz uma G-ação (à esquerda) sobre $M \otimes_R N$, dada da seguinte maneira:

$$\begin{aligned} \upsilon' : G \times (M \otimes_R N) &\longrightarrow M \otimes_R N \\ (g, m \otimes n) &\longmapsto g.(m \otimes n) := g.m \otimes g.n \ . \end{aligned}$$

Denominamos a G-ação υ de ***ação diagonal***, bem como a G-ação υ'. Desta maneira, temos que $Hom_R(M, N)$ e $M \otimes_R N$ tornam-se ***RG-módulos à esquerda***.

Proposição 1.1.1. $\big[Hom_R(M, N)\big]^G = Hom_{RG}(M, N)$.

Demonstração.

Sejam $g \in G$ e $\phi \in Hom_R(M, N)$. Temos que,

$$\begin{aligned} g.\phi = \phi &\Leftrightarrow (g.\phi)(m) = \phi(m), \ \forall \, m \in M \\ &\Leftrightarrow g.\phi(g^{-1}.m) = \phi(m), \ \forall \, m \in M \\ &\Leftrightarrow g.\phi(m') = \phi(g.m'), \ \forall \, m' \in M \ (\text{tome } m' = g^{-1}m). \end{aligned}$$

Logo,

$$\begin{aligned} \big[Hom_R(M, N)\big]^G &= \big\{\phi \in Hom_R(M, N) \mid g.\phi(m) = \phi(g.m)\big\} \\ &= Hom_{RG}(M, N). \end{aligned}$$

■

Corolário 1.1.1. Se R é visto como RG-módulo trivial, então

$$Hom_{RG}(R, M) \simeq M^G$$

como grupos (e como RG-módulos triviais).

Proposição 1.1.2. Seja M um RG-módulo (à esquerda). Então,

$$H^0(G, M) \simeq M^G.$$

Demonstração.

Consideremos

$$\cdots \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \xrightarrow{\varepsilon} R \longrightarrow 0,$$

uma resolução projetiva de R sobre RG.

Assim, do Teorema A.6.2, temos que

$$0 \longrightarrow Hom_{RG}(R, M) \xrightarrow{\varepsilon^*} Hom_{RG}(F_0, M) \xrightarrow{\delta^0} Hom_{RG}(F_1, M) \longrightarrow \cdots$$
$$\uparrow{\scriptstyle \delta^{-1}}$$
$$0$$

é exata à esquerda, e daí temos que ε^* é monomorfismo e $Im(\varepsilon^*) = Ker(\delta^0)$.

Logo,

$$H^0(G, M) = \frac{Ker(\delta^0)}{Im(\delta^{-1})} \simeq Ker(\delta^0) = Im(\varepsilon^*). \tag{1.1}$$

Pelos Teorema do Isomorfismo e corolário anterior, temos

$$Im(\varepsilon^*) \simeq \frac{Hom_{RG}(R, M)}{Ker(\varepsilon^*)} \simeq Hom_{RG}(R, M) \simeq M^G. \tag{1.2}$$

Portanto, de (1.1) e (1.2), obtemos

$$H^0(G, M) \simeq M^G.$$

■

Corolário 1.1.2. Se M é um RG-módulo trivial, então $H^0(G, M) \simeq M$.

Exemplo 1.1.1.

(1) Sejam $G = \{1\}$ e M um RG-módulo (à esquerda). Então,

$$H^n\big(\{1\}, M\big) \simeq \begin{cases} M, & \text{se } n = 0; \\ 0, & \text{se } n \geqslant 1. \end{cases}$$

De fato, notemos que $RG = R$, $\varepsilon = id_R$ e $0 \longrightarrow R \xrightarrow{\varepsilon} R \longrightarrow 0$ é uma resolução projetiva de R sobre RG.

Desta maneira, obtemos o seguinte complexo

$$0 \longrightarrow Hom_R(R, M) \longrightarrow 0\,. \tag{1.3}$$

Mas, pela Proposição A.6.1, vem que $Hom_R(R, M) \simeq M$ e assim, o complexo (1.3) se reduz a

$$0 \longrightarrow M \longrightarrow 0 \ .$$

Portanto, $H^n\big(\{1\}, M\big) \simeq \begin{cases} M^{\{1\}} \simeq M, & \text{se } n = 0; \\ 0, & \text{se } n > 0. \end{cases}$

(2) Se $G = \langle t \rangle \simeq \mathbb{Z}$ e M é um RG-módulo (à esquerda), então

$$H^n(G, M) \simeq \begin{cases} M^G, & \text{se } n = 0; \\ M_G, & \text{se } n = 1; \\ 0, & \text{se } n \geqslant 2. \end{cases}$$

De fato, temos do Exemplo A.8.2 *(1)*, que a seqüência

$$0 \longrightarrow RG \xrightarrow{\partial} RG \xrightarrow{\varepsilon} R \longrightarrow 0,$$

com ε a aplicação aumentação dada por $\varepsilon\left(\sum_i \alpha_i.t^i\right) = \sum_i \alpha_i$ e ∂ a multiplicação por $(t-1)$ é uma resolução livre (portanto, projetiva) de R sobre RG.

Aplicando o funtor $Hom_{RG}(\_\_, M)$, obtemos

$$0 \longrightarrow Hom_{RG}(RG, M) \xrightarrow{\delta^0} Hom_{RG}(RG, M) \longrightarrow 0, \qquad (1.4)$$

onde δ^0 é a multiplicação por $(t-1)$, pois

$$\delta^0(\phi)(g) = (\phi \circ \partial)(g) = \phi[(t-1)(g)] = (t-1)\phi(g),$$

para todo $\phi \in Hom_{RG}(RG, M)$ e todo $g \in RG$.

Como $Hom_{RG}(RG, M) \simeq M$, a seqüência (1.4) equivale a

$$0 \longrightarrow M \xrightarrow{\delta^0} M \longrightarrow 0.$$

Assim, $H^1(G, M) = \dfrac{Ker(\delta^1)}{Im(\delta^0)} = \dfrac{M}{(t-1)M} \simeq M_G$ e $H^n(G, M) = 0$, para $n \geqslant 2$.

Portanto, $H^n(G,M) \simeq \begin{cases} M^G, & \text{se } n=0; \\ M_G, & \text{se } n=1; \\ 0, & \text{se } n \geqslant 2. \end{cases}$

Considerando ainda $G = \langle t \rangle \simeq \mathbb{Z}$, calculemos os grupos de cohomologia de G para módulos particulares:

(2a) M é um RG-módulo trivial.

Neste caso, temos por *(2)* e Observação 1.1.2 *(1)* que

$$H^n(G,M) = \begin{cases} M, & \text{se } n=0,1; \\ 0, & \text{se } n \geqslant 2. \end{cases}$$

(2b) $M = \mathbb{Z}G$ visto como $\mathbb{Z}G$-módulo (à esquerda) com a G-ação natural (à esquerda): $t^i.(\alpha t^{i'}) := \alpha t^{i+i'}$, para todos $t^i, t^{i'} \in G$ e $\alpha \in \mathbb{Z}$.

Como G é cíclico infinito gerado por t, temos que $t^i.t^{i'} \neq t^{i'}$ se $t^i \neq 1$ e assim, $H^0(G,\mathbb{Z}G) \simeq (\mathbb{Z}G)^G = 0$.

Agora, determinemos $H^1(G,\mathbb{Z}G) \simeq (\mathbb{Z}G)_G$.

Seja $I = \langle t^i.u - u \mid t^i \in G,\ u \in \mathbb{Z}G \rangle$ e denotemos $\overline{x} = x + I \in \dfrac{\mathbb{Z}G}{I} = (\mathbb{Z}G)_G$.

Consideremos $y = t^i \in \mathbb{Z}G$, com $i > 0$. Como

$$t^i - 1 = (t-1)(t^{i-1} + \cdots + t + 1) \in I,$$

segue que $\overline{t^i - 1} = \overline{0}$ e assim, $\overline{y} = \overline{t^i} = \overline{1}$ em $(\mathbb{Z}G)_G$.

Agora, se $y = t^{-i} \in \mathbb{Z}G$, com $i > 0$, também $\overline{y} = \overline{t^{-i}} = \overline{1}$, pois $t^{-i} = (1 - t^i).t^{-i} + 1$ e $\overline{1 - t^{-i}} = \overline{1 + (t^i - 1).t^{-i} - 1} = \overline{(t^i - 1).t^{-i}} = \overline{0}$.

Assim, para um elemento qualquer $x \in \mathbb{Z}G$, $x = \alpha_0 t^i + \alpha_1 t^{i+1} + \cdots + \alpha_m t^{i+m}$, com $i \in \mathbb{Z}$, $m \geqslant 0$ e $\alpha_j \in \mathbb{Z}$, temos que $\overline{x} = \overline{\alpha_0 + \alpha_1 + \cdots + \alpha_m}$ $= \alpha.\overline{1}$, com $\alpha = \alpha_0 + \alpha_1 + \cdots + \alpha_m \in \mathbb{Z}$. Logo, $H^1(G,\mathbb{Z}G) := \{\alpha.\overline{1},\ \ \alpha \in \mathbb{Z}\} = \langle \overline{1} = 1 + I \rangle = \mathbb{Z}.\overline{1} \simeq \mathbb{Z}$ e portanto

$$H^n(G,\mathbb{Z}G) \simeq \begin{cases} 0, & \text{se } n=0; \\ \mathbb{Z}, & \text{se } n=1; \\ 0, & \text{se } n \geqslant 2. \end{cases}$$

(2c) $M = \mathbb{Z}_2G$ visto como $\mathbb{Z}_2G$-módulo (à esquerda) com a G-ação (à esquerda): $t^i.(1.t^{i'}) := 1.t^{i+i'}$, com $1 \in \mathbb{Z}_2$ e $t^i, t^{i'} \in G = \langle t \rangle \simeq \mathbb{Z}$.

Como no caso anterior, verifica-se que

$$H^0(G,\mathbb{Z}G) = 0 \text{ e } H^1(G,\mathbb{Z}_2G) \simeq \langle 1+I \rangle.$$

Mas, neste caso, temos que $\langle 1+I \rangle = \{0+I, 1+I\} \simeq \mathbb{Z}_2$.

Portanto, $H^n(G,\mathbb{Z}_2G) \simeq \begin{cases} (\mathbb{Z}_2G)^G \simeq 0, & \text{se } n=0; \\ \mathbb{Z}_2, & \text{se } n=1; \\ 0, & \text{se } n \geqslant 2. \end{cases}$

(3) Sejam $G = \langle t \rangle \simeq \mathbb{Z}_n$, $n \geqslant 2$ e M um RG-módulo (à esquerda).

Consideremos a seqüência

$$\cdots \longrightarrow RG \xrightarrow{(t-1)} RG \xrightarrow{N} RG \xrightarrow{(t-1)} RG \xrightarrow{\varepsilon} R \longrightarrow 0$$

dada no Exemplo A.8.2 *(2)*.

Aplicando o funtor $Hom_{RG}(\_\_, M)$, temos que

$$0 \longrightarrow Hom_{RG}(RG, M) \xrightarrow{\delta^0} Hom_{RG}(RG, M) \xrightarrow{\delta^1} \cdots \qquad (1.5)$$

sendo que, $\delta^k(\phi)(x) := (\phi \circ \partial_{k+1})(x)$ com $\partial_{k+1} = t-1$ se k é par e $\partial_{k+1} = N$ se k é ímpar, para todo $x \in RG$.

Usando o fato de que $Hom_{RG}(RG, M) \simeq M$,

$$(\delta^{2n})(\phi)(x) = (\phi \circ \partial_{2n})(x) = \phi\big((t-1)x\big) = (t-1)\phi(x),$$

para todo $x \in RG$, isto é, $\delta^{2n}(\phi) = (t-1)\phi$ e também $\delta^{2n+1}(\phi) = N.\phi$, a seqüência (1.5) fica da seguinte forma:

$$0 \longrightarrow M \xrightarrow{t-1} M \xrightarrow{N} M \xrightarrow{t-1} \cdots .$$

$$\text{Portanto, } H^k(G,M) \simeq \begin{cases} M^G, & \text{se } k=0; \\ \dfrac{Ker(N)}{Im(t-1)} = \dfrac{Ker(N)}{(t-1)M}, & \text{se } k \text{ é ímpar}; \\ \dfrac{Ker(t-1)}{Im(N)} = \dfrac{M^G}{N.M}, & \text{se } k \text{ é par}. \end{cases}$$

Agora, calculemos os grupos de cohomologia de $G \simeq \mathbb{Z}_n$, para alguns casos particulares de M:

(3a) M é um RG-módulo trivial.

Neste caso,

$$(t-1).m = t.m - 1.m = m - m = 0 \text{ e } (1 + t + \cdots + t^{n-1}).m = n.m,$$

para todo $m \in M$, ou seja, $(t-1)$ é o homomorfismo nulo e N é a multiplicação por n.

Portanto,

$$H^k(G,M) \simeq \begin{cases} M, & \text{se } k=0; \\ Ker(N), & \text{se } k \text{ é ímpar}; \\ \dfrac{Ker(t-1)}{Im(N)} = \dfrac{M^G}{n.M}, & \text{se } k \text{ é par}. \end{cases}$$

Em particular, para $M = \mathbb{Z}$ (visto como $\mathbb{Z}G$-módulo trivial) obtemos

$$H^k(G,M) = H^k(\mathbb{Z}_n, \mathbb{Z}) \simeq \begin{cases} \mathbb{Z}, & \text{se } k=0; \\ 0, & \text{se } k \text{ é ímpar}; \\ \dfrac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}_n, & \text{se } k \text{ é par}. \end{cases}$$

(3b) $G = \{1, t\} \simeq \mathbb{Z}_2$ e $M = \mathbb{Z}$ visto como $\mathbb{Z}G$-módulo (à esquerda) com a G-ação (à esquerda): $1.\alpha := \alpha$ e $t.\alpha = -\alpha$, para todo $\alpha \in \mathbb{Z}$.

Temos que, $(t-1).\alpha = -2\alpha$ e $N.\alpha = (1+t)\alpha = 0$, para todo $\alpha \in \mathbb{Z}$.

Daí, $Ker(N) = \mathbb{Z}$, $Im(N) = 0$ e $Im(t-1) = 2\mathbb{Z}$.

$$\text{Logo, } H^k(\mathbb{Z}_2, \mathbb{Z}) \simeq \begin{cases} \mathbb{Z}^{\mathbb{Z}_2} = 0, & \text{se } k=0; \\ \dfrac{\mathbb{Z}}{2\mathbb{Z}} \simeq \mathbb{Z}_2, & \text{se } k \text{ é ímpar}; \\ 0, & \text{se } k \text{ é par}. \end{cases}$$

1.2 Interpretação de $H^1(G, M)$ em Termos de Derivações

Nesta seção, apresentamos uma interpretação para $H^1(G, M)$, em termos de derivações.

Definição 1.2.1.

(a) Sejam G um grupo e M um ***RG-módulo à esquerda***. Uma ***derivação*** de G em M é uma aplicação $d : G \longrightarrow M$ tal que

$$d(g.g') = d(g) + g.d(g') \ ,$$

para todos $g, g' \in G$.

O conjunto de todas as derivações de G em M, denotado por $\boldsymbol{Der(G, M)}$, é denominado ***grupo das derivações*** de G em M, isto é,

$$Der(G, M) = \{d : G \longrightarrow M \mid d(g.g') = d(g) + g.d(g'),\ \forall\ g, g' \in G\}$$

e o ***subgrupo das derivações principais*** é denotado por $\boldsymbol{P(G, M)}$ e definido por

$$P(G, M) := \{d_m \in Der(G, M),\ m \in M \mid d_m(g) = g.m - m,\ \forall\ g \in G\}.$$

(b) Similarmente, se M é um ***RG-módulo à direita***, uma ***derivação*** de G em M é uma aplicação $\delta : G \longrightarrow M$ tal que $\delta(g.g') = \delta(g)g' + \delta(g')$, para todos $g, g' \in G$ ([19], p. 304) e definimos

$$Der(G, M) := \left\{\delta : G \longrightarrow M \mid \delta(g.g') = \delta(g).g' + \delta(g'),\ \forall\ g, g' \in G\right\} \text{ e}$$

$$P(G, M) := \left\{\delta_m \in Der(G, M),\ m \in M \mid \delta_m(g) = m.g - m,\ \forall\ g \in G\right\}.$$

Proposição 1.2.1. Seja M um RG-módulo (à esquerda). Se consideramos $M' = M$, visto como RG-módulo (à direita) por definir $m.g := g^{-1}.m$, então os grupos $Der(G, M)$ e $Der(G, M')$ são isomorfos e ainda, a imagem de $P(G, M)$ por tal isomorfismo é $P(G, M')$.

Demonstração.

O isomorfismo é dado por

$$\begin{aligned}\psi:\ Der(G,M) &\longrightarrow Der(G,M')\\ d &\longmapsto \psi(d) \overset{not.}{=} \delta;\ \delta(g) := d(g^{-1})\ .\end{aligned}$$

Notemos que $\delta = \psi(d) \in Der(G,M')$, pois dados $g, g' \in G$,

$$\begin{aligned}\delta(gg') &= d\big((gg')^{-1}\big) = d\big((g')^{-1}g^{-1}\big) \overset{d\in Der(G,M)}{=} d\big((g')^{-1}\big) + (g')^{-1}d(g^{-1})\\ &= \delta(g') + d(g^{-1})g' = \delta(g)g' + \delta(g').\end{aligned}$$

Ainda, $\psi\big(P(G,M)\big) = P(G,M')$, pois

$$\psi(d_m)(g) = d_m(g^{-1}) = g^{-1}m - m = m.g - m.$$ ■

Propriedade 1.2.1.

(1) Se M é um RG-módulo e $d \in Der(G,M)$, então

$$d(1) = d(1.1) = d(1) + 1.d(1) = d(1) + d(1).$$

Daí, temos que $d(1) = 0$.

(2) Se M é um RG-módulo trivial, então $Der(G,M) = Hom(G,M)$ e $P(G,M) = 0$.

Antes de apresentarmos a interpretação para $H^1(G,M)$, fazemos algumas considerações.

Seja G um grupo e consideremos a Resolução Bar (à esquerda) de R sobre RG

$$F: \cdots \longrightarrow F_n \xrightarrow{\partial_n} \cdots \longrightarrow F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} R \longrightarrow 0$$

dada no Exemplo A.8.1 *(2)*.

Temos que, cada F_n é o RG-módulo livre gerado pelos símbolos $[g_1|\cdots|g_n]$ e

$$\begin{aligned}\partial_n\big([g_1|\cdots|g_n]\big) = g_1[g_2|\cdots|g_n] + \sum_{i=1}^{n-1}\big((-1)^i[g_1|\cdots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\cdots|g_n]\big) +\\ +(-1)^n[g_1|\cdots|g_{n-1}].\end{aligned}$$

Vamos denotar $\boldsymbol{C^n(G,M)} := Hom_{RG}(F_n, M)$ e $\boldsymbol{C^*(G,M)}$ o complexo associado.

Assim, $\phi \in C^n(G,M)$ é um homomorfismo

$$\begin{aligned} \phi : \quad F_n \quad &\longrightarrow M \\ [g_1|\cdots|g_n] &\longmapsto \phi\big([g_1|\cdots|g_n]\big) . \end{aligned}$$

Se identificamos $[g_1|\cdots|g_n]$ com $(g_1,\ldots,g_n)$, podemos ver ϕ como uma aplicação de n-variáveis, $\phi : G^n = G\times\cdots\times G \longrightarrow M$. Por convenção, G^0 é um conjunto com um elemento (denotado por $[\ \ ]$) de modo que $C^0(G,M) = Hom_{RG}(F_0,M) \simeq Hom_{RG}(RG,M) \simeq M$.

Assim, o operador cobordo $\delta^{n-1} : C^{n-1}(G,M) \longrightarrow C^n(G,M)$ é dado por

$$\begin{aligned} \big[\delta^{n-1}(\phi)\big](g_1,\ldots,g_n) &:= \phi\big[\partial_n(g_1,\ldots,g_n)\big] \\ &= g_1\phi(g_2,\ldots,g_n) + \sum_{i=1}^{n-1}\big[(-1)^i.\phi(g_1,\ldots,g_ig_{i+1},\ldots g_n)\big] \\ &\quad +(-1)^n\phi(g_1,\ldots,g_{n-1}). \end{aligned}$$

- no caso $n=1$

$$\delta^0(\phi)(g_1) = \phi\big[\partial_1(g_1)\big] = g_1\phi\big([\ \ ]\big) - \phi\big([\ \ ]\big).$$

- no caso $n=2$

$$\delta^1(\phi)(g_1,g_2) = g_1\phi(g_2) - \phi(g_1g_2) + \phi(g_1).$$

Proposição 1.2.2. Se G é um grupo e M um RG-módulo (à esquerda ou à direita), então $H^1(G,M) \simeq \dfrac{Der(G,M)}{P(G,M)}$.

Demonstração.

Faremos apenas a prova para o caso em que M é um RG-módulo à esquerda. O caso à direita é provado de modo similar, considerando a resolução bar à direita (Exemplo A.8.1 *(3)*) ou usando a proposição anterior.

Consideremos o complexo

$$C^*(G,M) : 0 \longrightarrow C^0(G,M) \xrightarrow{\delta^0} C^1(G,M) \xrightarrow{\delta^1} C^2(G,M) \longrightarrow \cdots$$

definido anteriormente.

Por definição, temos que $H^1(G,M) = \dfrac{Ker(\delta^1)}{Im(\delta^0)}$.

Desta forma, para mostrarmos a proposição, basta verificarmos que $Ker(\delta^1) = Der(G,M)$ e $Im(\delta^0) = P(G,M)$.

Vejamos inicialmente que $Ker(\delta^1) = Der(G,M)$.

Seja $\phi \in C^1(G,M)$. Então, $\phi : G^1 \longrightarrow M$ e $\delta^1(\phi) : G^2 \longrightarrow M$ tal que $\delta^1(\phi)(g,g') = g\phi(g') - \phi(gg') + \phi(g)$.

Assim,

$$\begin{aligned}\phi \in Ker(\delta^1) &\Leftrightarrow \delta^1(\phi) = 0 \Leftrightarrow \delta^1(\phi)(g,g') = 0,\ \forall\ g,g' \in G \\ &\Leftrightarrow \phi(gg') = \phi(g) + g\phi(g'),\ \forall\ g,g' \in G \Leftrightarrow \phi \in Der(G,M).\end{aligned}$$

Então, $Ker(\delta^1) = Der(G,M)$.

Agora, vejamos que $Im(\delta^0) = P(G,M)$.

Seja $d \in Im(\delta^0)$, então existe $\phi : G^0 \longrightarrow M$ tal que $\delta^0(\phi) = d$. Assim, para todo $g \in G$, $d(g) = \delta^0(\phi)(g) = g\phi([\ ]) - \phi([\ ])$. Mas $\phi([\ ]) = m$, para algum $m \in M$. Então, $d(g) = g.m - m$, ou seja, $d \in P(G,M)$. Logo, $Im(\delta^0) \subseteq P(G,M)$.

Reciprocamente, se $d \in P(G,M)$, então $d(g) = g.m - m$, para algum $m \in M$. Seja $\phi : G^0 \longrightarrow M$ tal que $\phi([\ ]) = m$. Desta maneira, $\delta^0(\phi)(g) = g.\phi([\ ]) - \phi([\ ]) = g.m - m = d(g)$ e assim, $d = \delta^0(\phi) \in Im(\delta^0)$. Logo, $P(G,M) \subseteq Im(\delta^0)$.

Então, temos que $Im(\delta^0) = P(G,M)$.

Portanto, $H^1(G,M) \simeq \dfrac{Der(G,M)}{P(G,M)}$. ■

Corolário 1.2.1. Se G é um grupo e M é um RG-módulo trivial, então

$$H^1(G,M) \simeq Hom(G,M).$$

Exemplo 1.2.1. Sejam $G = \langle t \rangle \simeq \mathbb{Z}$ e $M = RG$ ($R = \mathbb{Z}$ ou $R = \mathbb{Z}_2$), visto como RG-módulo (à esquerda) com a G-ação natural (à esquerda): $t^i(\alpha t^{i'}) := \alpha t^{i+i'}$, para todos $t^i, t^{i'} \in G$ e $\alpha \in R$.

Usando derivações, mostremos que $H^1(G, RG) \simeq R$. De fato,

(a) Suponhamos $M = \mathbb{Z}G$. Se $d \in Der(G, \mathbb{Z}G)$, então temos para $i > 0$ que:

- $d(t^i) = \sum_{j=0}^{i-1} t^j d(t)$.

  Para verificarmos esta igualdade usamos o princípio de indução finita sobre $i \in \mathbb{Z}$.

  Se $i = 1$, então $d(t) = t^0 d(t)$.

  Agora, suponhamos que $d(t^n) = \sum_{j=0}^{n-1} t^j d(t)$. Assim,

$$\begin{aligned} d(t^{n+1}) = d(tt^n) = td(t^n) + d(t) &= t\left(\sum_{j=0}^{n-1} t^j d(t)\right) + d(t) \\ &= \sum_{j=0}^{n-1} t^{j+1} d(t) + d(t) = \sum_{j=1}^{n} t^j d(t) + t^0 d(t) = \sum_{j=0}^{n} t^j d(t). \end{aligned}$$

- $d(t^{-i}) = \sum_{j=1}^{i} (-t^{-j}) d(t)$.

  Novamente usamos o princípio de indução finita sobre $i \in \mathbb{Z}$.

  Para $i = 1$, $d(t^{-1}) = (-t^{-1})d(t)$, pois $0 = d(t^{-1}t) = t^{-1}d(t) + d(t^{-1})$.

  Agora, suponhamos que $d(t^{-n}) = \sum_{j=1}^{n} (-t^{-j}) d(t)$. Logo,

$$\begin{aligned} d(t^{-n-1}) = d(t^{-n}.t^{-1}) = t^{-n}d(t^{-1}) + d(t^{-n}) &= t^{-n}(-t^{-1})d(t) + d(t^{-n}) \\ &= (-t^{-n-1})d(t) + \sum_{j=1}^{n} (-t^{-j})d(t) = \sum_{j=1}^{n+1} (-t^{-j})d(t). \end{aligned}$$

  Desta maneira, d fica bem determinada e depende somente de $d(t)$. Assim, todo elemento $x \in \mathbb{Z}G$ dá origem à uma derivação

$$d \in Der(G, \mathbb{Z}G).$$

  Portanto, $Der(G, \mathbb{Z}G) \simeq \mathbb{Z}G$ (como $\mathbb{Z}$-módulo).

Em particular, para cada $r \in \mathbb{Z}$, $d^r(t) := r.1$ dá origem à uma derivação e temos que $\{d^r \mid r \in \mathbb{Z}\} = \langle d^1 \rangle \simeq \mathbb{Z}$ e $\langle d^1 \rangle \subseteq Der(G, \mathbb{Z}G)$.

Notemos que d^r $(r \neq 0)$ não é uma derivação principal, pois se existisse um elemento $m = n_0.1 + n_1.t + \cdots + n_i t^i \in \mathbb{Z}G$ tal que $d_m = d^r$, então $d^r = t.m - m$ e assim,

$$t.(n_0.1 + n_1.t + \cdots + n_i t^i) - (n_0.1 + n_1.t + \cdots + n_i t^i) = r.1.$$

Logo, $(-r - n_0).1 + (n_0 - n_1).t + \cdots + (n_{i-1} - n_i)t^i + n_i t^{i+1} = 0$, o que implicaria em

$$r = n_0,\ n_0 = n_1, \ldots,\ n_{i-1} = n_i,\ n_i = 0 \text{ e conseqüentemente } r = 0.$$

Desta forma, $d^r = d^0 = t.0 - 0 = 0$.

É suficiente mostrarmos que para todo elemento $d \in Der(G, \mathbb{Z}G)$, existem $d_m \in P(G, \mathbb{Z}G)$ e $r \in \mathbb{Z}$ tais que $d - d_m = d^r$, pois isto implica que $d + P(G, \mathbb{Z}G) = d^r + P(G, \mathbb{Z}G)$ e assim, concluímos que

$$\frac{Der(G, \mathbb{Z}G)}{P(G, \mathbb{Z}G)} \simeq \{d^r + P(G, \mathbb{Z}G) \mid r \in \mathbb{Z}\} \simeq \mathbb{Z}.$$

Para isto, vejamos a seguinte afirmação: "Se $d(t) = t^i - 1$ ou $d(t) = t^{-i} - 1$, com $i > 0$, então $d \in P(G, \mathbb{Z}G)$".

De fato,

- $d(t) = t^i - 1 = (t-1)(t^{i-1} + \cdots + t + 1) = (t-1)\widetilde{m} = d_{\widetilde{m}}(t) \in P(G, \mathbb{Z}G)$.
- Para $d(t) = t^{-i} - 1$, temos

$$\begin{aligned} t^{-i} - t^i &= (t-1)(-t^{-i} - t^{-i+1} - \cdots - t^2 - t - \cdots - t^{i-1}) \\ &= (t-1)\widehat{m} = d_{\widehat{m}} \in P(G, \mathbb{Z}G). \end{aligned}$$

Por outro lado,

$$t^{-i} - t^i = (t^{-i} - 1) - (t^i - 1) = (t^{-i} - 1) - d_{\widetilde{m}}(t) = d(t) - d_{\widetilde{m}}(t).$$

Logo, $d_{\widehat{m}} = d(t) - d_{\widetilde{m}}(t)$ o que implica $d(t) = d_{\widehat{m}} + d_{\widetilde{m}} \in P(G, \mathbb{Z}G)$.

Agora, para todo $d \in Der(G, \mathbb{Z}G)$, temos

$$\begin{aligned} d(t) = x &= r_0 t^i + r_1 t^{i+1} + \cdots + r_n t^{i+n} \\ &= r_0(t^i - 1) + r_1(t^{i+1} - 1) + \cdots + r_n(t^{i+n} - 1) + r_0 + r_1 + \cdots + r_n \\ &= d_m(t) + d^r(t), \text{ onde } r = r_0 + \cdots + r_n, \end{aligned}$$

isto é, existe $m \in M = \mathbb{Z}G$ tal que $d - d_m = d^r$.

Portanto, $H^1(G, \mathbb{Z}G) \simeq \dfrac{Der(G, \mathbb{Z}G)}{P(G, \mathbb{Z}G)} \simeq \mathbb{Z}$.

(b) Consideremos agora $M = \mathbb{Z}_2G$ e $d \in Der(G, \mathbb{Z}_2G)$.

De modo análogo ao item *(a)*, temos que:

- d depende somente de $d(t)$,
- $s \in \mathbb{Z}_2G$ dá origem à uma derivação d em $Der(G, \mathbb{Z}_2G)$ e daí,

$$Der(G, \mathbb{Z}_2G) \simeq \mathbb{Z}_2G.$$

- se $d(t) = t^i - 1$ ou $d(t) = t^{-i} - 1$, com $i > 0$, então $d \in P(G, \mathbb{Z}_2G)$.

  Seja $d \in Der(G, \mathbb{Z}_2G)$. Temos que $d(t) = t^{i_1} + t^{i_2} + \cdots + t^{i_n} \in \mathbb{Z}_2G$.

  ★ Se n é par, então

  $$d(t) = (t^{i_1} - 1) + (t^{i_2} - 1) + \cdots + (t^{i_n} - 1) \in P(G, \mathbb{Z}_2G),$$

  implica em $d + P(G, \mathbb{Z}_2G) = 0 + P(G, \mathbb{Z}_2G)$.

  ★ Se n é ímpar, então

  $$d(t) = (t^{i_1} - 1) + (t^{i_2} - 1) + \cdots + (t^{i_n} - 1) + 1,$$

  implica em $d + P(G, \mathbb{Z}_2G) = 1 + P(G, \mathbb{Z}_2G)$.

Assim,

$$\begin{aligned} H^1(G, \mathbb{Z}_2G) &\simeq \frac{Der(G, \mathbb{Z}_2G)}{P(G, \mathbb{Z}_2G)} = \{0 + P(G, \mathbb{Z}_2G), 1 + P(G, \mathbb{Z}_2G)\} \\ &\simeq \mathbb{Z}_2. \end{aligned}$$

1.3 Restrição e (Co)extensão de Escalares

Definição 1.3.1. Sejam R_1, R_2 anéis e $h : R_1 \longrightarrow R_2$ um homomorfismo de anéis. Temos as seguintes situações:

(a) Se M é um R_2-módulo (à esquerda), sempre podemos ver M como um R_1-módulo (à esquerda), considerando a seguinte lei de composição externa

$$\begin{aligned} \mu : \ R_1 \times M \ &\longrightarrow \ M \\ (\alpha, m) \ &\longmapsto \ \mu(\alpha, m) \overset{not.}{=} \alpha.m := h(\alpha).m. \end{aligned}$$

Neste caso, M é chamado um ***R_1-módulo por restrição de escalares*** (via h).

(b) Se M é um R_1-módulo (à esquerda), podemos obter dois R_2-módulos (à esquerda), bastante relacionados com M, da seguinte maneira:

- O R_2-módulo (à esquerda) $Hom_{R_1}(R_2, M)$.

  Para isso consideramos R_2 como um R_1-módulo (à esquerda), como em *(a)*, ou seja, por restrição de escalares (via h), fazendo sentido então considerar $Hom_{R_1}(R_2, M)$.

  Agora, seja

$$\begin{aligned} \mu : \ R_2 \times Hom_{R_1}(R_2, M) \ &\longrightarrow \ Hom_{R_1}(R_2, M) \\ (\beta, \phi) \ &\longmapsto \ \beta.\phi \ ; \ (\beta.\phi)(\beta') := \phi(\beta'.\beta) \end{aligned}$$

  com $\beta, \beta' \in R_2$ e $\phi \in Hom_{R_1}(R_2, M)$.

  Podemos verificar que μ está bem definida e é uma R_2-multiplicação (à esquerda).

  Desta forma, $Hom_{R_1}(R_2, M)$ é um R_2-módulo (à esquerda), denominado ***R_2-módulo obtido de M por coextensão de escalares*** de R_1 para R_2 (via h).

- O R_2-módulo (à esquerda) $R_2 \otimes_{R_1} M$.

Primeiramente, para obter o produto tensorial, consideramos R_2 como um R_1-módulo à direita por definir $\beta.\alpha := \beta.h(\alpha)$.

Uma vez que a ação natural à esquerda de R_2 sobre si mesmo comuta com a ação à direita de R_1 sobre R_2, isto é,

$$\beta.(\beta'.\alpha) = \beta.\beta'.h(\alpha) = (\beta.\beta').h(\alpha) = (\beta.\beta').\alpha,$$

segue que

$$\beta.\beta' \otimes \alpha.m = (\beta.\beta').\alpha \otimes m = \beta(\beta'.\alpha) \otimes m.$$

Assim, considerando a aplicação

$$\begin{aligned} \mu' : R_2 \times (R_2 \otimes_{R_1} M) &\longrightarrow R_2 \otimes_{R_1} M \\ (\beta, \beta' \otimes m) &\longmapsto \beta.(\beta' \otimes m) := (\beta.\beta') \otimes m \end{aligned}$$

temos que, μ' está bem definida $\big($visto que, $\beta(\beta' \otimes \alpha.m) = \beta(\beta'.\alpha \otimes m)\big)$ e é uma R_2-multiplicação (à esquerda). Assim, $R_2 \otimes_{R_1} M$ é um R_2-módulo (à esquerda), denominado ***R_2-módulo obtido de M por extensão de escalares*** de R_1 para R_2 (via h).

Lema 1.3.1. Sejam M um R_1-módulo (à esquerda) e $h : R_1 \longrightarrow R_2$ um homomorfismo de anéis. Então, existem aplicações naturais de R_1-módulos (à esquerda):

(a) $\pi : Hom_{R_1}(R_2, M) \longrightarrow M$ dada por $\pi(\phi) := \phi(1_{R_2})$, para todo $\phi \in Hom_{R_1}(R_2, M)$, onde $Hom_{R_1}(R_2, M)$ é visto inicialmente como um R_2-módulo (à esquerda) por coextensão de escalares e depois como um R_1-módulo (à esquerda) por restrição de escalares.

(b) $i : M \longrightarrow R_2 \otimes_{R_1} M$ dada por $i(m) = 1_{R_2} \otimes m$, para todo $m \in M$, onde $R_2 \otimes_{R_1} M$ é visto inicialmente como R_2-módulo (à esquerda) por extensão de escalares e depois como R_1-módulo (à esquerda) por restrição de escalares.

Demonstração.

Vejamos apenas que são aplicações de R_1-módulos (à esquerda).

(a) Seja $\pi : Hom_{R_1}(R_2, M) \longrightarrow M$ tal que $\pi(\phi) := \phi(1_{R_2})$.

Para todo $\alpha \in R_1$, temos que,

$$\pi(\alpha.\phi) = \pi[h(\alpha).\phi] = [h(\alpha).\phi](1_{R_2}) = \phi[1_{R_2}.h(\alpha)] = \phi[h(\alpha)]$$
$$= \phi[h(\alpha).1_{R_2}] = \phi(\alpha.1_{R_2}) = \alpha.\phi(1_{R_2}) = \alpha.\pi(\phi).$$

Portanto, π é uma aplicação de R_1-módulos (à esquerda).

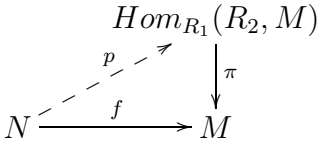
(b) Similarmente, dado $\alpha \in R_1$,

$$\alpha i(m) = h(\alpha)(1 \otimes m) = h(\alpha) \otimes m = 1.\alpha \otimes m = 1 \otimes \alpha.m = i(\alpha.m). \blacksquare$$

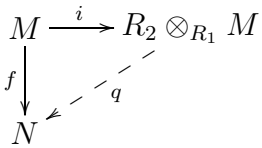
Os dois resultados seguintes podem ser encontrados em [4] III, §3.

Lema 1.3.2. Sejam $h : R_1 \longrightarrow R_2$ um homomorfismo de anéis, N um R_2-módulo (à esquerda) e M um R_1-módulo (à esquerda).

(a) Se $f : N \longrightarrow M$ é uma aplicação de R_1-módulos (à esquerda), então existe uma única aplicação de R_2-módulos (à esquerda) $p : N \longrightarrow Hom_{R_1}(R_2, M)$ tal que $\pi \circ p = f$, onde π é a aplicação dada no lema anterior.



(b) Se $f : M \longrightarrow N$ é uma aplicação de R_1-módulos (à esquerda), então existe uma única aplicação de R_2-módulos (à esquerda) $q : R_2 \otimes_{R_1} M \to N$ tal que $q \circ i = f$, onde i é a aplicação dada no lema anterior.



Proposição 1.3.1. Se $h : R_1 \longrightarrow R_2$ é um homomorfismo de anéis, N é um R_2-módulo (à esquerda) e M é um R_1-módulo (à esquerda), então

(a) $Hom_{R_1}(N, M) \simeq Hom_{R_2}\big(N, Hom_{R_1}(R_2, M)\big)$, como grupos.

(b) $Hom_{R_1}(M, N) \simeq Hom_{R_2}(R_2 \otimes_{R_1} M, N)$, como grupos.

1.4 Módulos (Co)induzidos

Sejam G um grupo e H um subgrupo de G. Agora, aplicamos a construção feita na seção anterior, para o homomorfismo $\widetilde{i} : RH \longrightarrow RG$ induzido da inclusão $i : H \longrightarrow G$.

(a) Sendo M um RG-módulo (à esquerda), podemos vê-lo como um RH-módulo (à esquerda) por restrição de escalares (via $\widetilde{i}$). Denotamos tal RH-módulo por $\boldsymbol{Res^G_H M}$.

(b) Se M é um RH-módulo (à esquerda), podemos associar os seguintes RG-módulos (à esquerda):

- O RG-módulo obtido de M por coextensão de escalares, que chamamos neste caso de ***coindução*** e denotamos por $\boldsymbol{Coind^G_H M}$, isto é,

$$Coind^G_H M = Hom_{RH}(RG, M).$$

Temos que a G-ação (à esquerda) no $Coind^G_H M$ é dada por

$$\begin{aligned} G \times Coind^G_H M &\longrightarrow Coind^G_H M \\ (g, \phi) &\longmapsto g.\phi \,;\; (g.\phi)(g') = \phi(g'.g). \end{aligned}$$

- O RG-módulo obtido de M por extensão de escalares, que neste caso denominamos ***indução*** e denotamos por $\boldsymbol{Ind^G_H M}$, isto é,

$$Ind^G_H M = RG \otimes_{RH} M,$$

e a G-ação (à esquerda) neste caso é dada por

$$\begin{aligned} G \times Ind^G_H M &\longrightarrow Ind^G_H M \\ (g, g' \otimes m) &\longmapsto g.(g' \otimes m) = gg' \otimes m. \end{aligned}$$

Definição 1.4.1. Quando $H = \{1\}$, denominamos

$$Coind_{\{1\}}^{G} M = Hom_R(RG, M) \text{ e } Ind_{\{1\}}^{G} = RG \otimes_R M$$

por ***módulo coinduzido*** e ***módulo induzido***, respectivamente.

Observação 1.4.1. Se consideramos $M = N$ e $f = id_M$, segue do lema anterior, que as aplicações π e i definidas no Lema 1.3.1 são epimorfismo e monomorfismo de RH-módulos (à esquerda), respectivamente.

Proposição 1.4.1. Sejam G um grupo, H um subgrupo de G e E um conjunto de representantes para as classes laterais à esquerda de H em G. Se M é um RH-módulo, então:

(a) $Coind_H^G M \simeq \prod_{g \in E} gM$.

(b) $Ind_H^G M \simeq \bigoplus_{g \in E} gM$,

onde gM indica o transformado de M sob a ação de g.

Demonstração. [4] III, §5. ■

Proposição 1.4.2. Seja M um RH-módulo. Então,

(a) $\vartheta : Ind_H^G M \longrightarrow Coind_H^G M$, dada por

$$\vartheta(g' \otimes m)(g) := \begin{cases} (gg').m, & \text{se } gg' \in H; \\ 0, & \text{c. c.} \end{cases}$$

é um RG-monomorfismo.

(b) Ainda, se $[G : H] < \infty$, então ϑ é um isomorfismo, isto é, $Ind_H^G M \simeq Coind_H^G M$.

Demonstração. [4] III, Proposição 5.9 ou [25], Proposição 1.4.4. ■

Proposição 1.4.3. Se H é um subgrupo de G com $[G : H] = \infty$, então para todo RH-módulo M

$$\left(Ind_H^G M\right)^G = 0.$$

Demonstração. [4], p. 71. ■

Vamos denotar por $\boldsymbol{R(G/H)}$ o R-módulo livre gerado pelas classes laterais à esquerda gH, $g \in G$. Existe uma G-ação natural de G em $R(G/H)$ induzida pela multiplicação à esquerda $\big(g.(g_0H) = (gg_0)H\big)$ e assim $R(G/H)$ é um RG-módulo à esquerda $\big($e também um RG-módulo à direita, por considerar $(g_0H).g = g^{-1}g_0H\big)$.

Similarmente, se denotamos por $\boldsymbol{R(H\backslash G)}$ o R-módulo livre gerado pelas classes laterais à direita Hg, $g \in G$, então $R(H\backslash G)$ torna-se um RG-módulo à direita considerando a G-ação natural $\big((Hg_0)g = H(g_0g)\big)$. Temos que:

Lema 1.4.1. O RG-módulo à direita $R(H\backslash G)$ é RG-isomorfo ao RG-módulo $R(G/H)$ visto como RG-módulo à direita.

Demonstração.

A aplicação

$$\begin{aligned} \mu :\ R(H\backslash G) &\longrightarrow R(G/H) \\ Hg &\longmapsto g^{-1}H \end{aligned}$$

é um RG-isomorfismo. ■

Se M é um RG-módulo (à esquerda), podemos dar a $Hom_R\big(R(G/H), M\big)$ e $R(G/H) \otimes_R M$ estruturas de RG-módulos com a G-ação diagonal (Definição 1.1.3). Considerando os RG-módulos $Coind_H^G Res_H^G M$ e $Ind_H^G Res_H^G M$ obtidos por coindução e indução de escalares, respectivamente, obtemos:

Proposição 1.4.4. Seja M um RG-módulo (à esquerda). Então, existem RG-isomorfismos naturais:

(a) $Coind_H^G Res_H^G M \overset{\xi}{\simeq} Hom_R(R(G/H), M)$. $\big(f \longmapsto \xi(f)\ ;\ \xi(f)(gH) = gf(g^{-1})\big)$.

(b) $Ind_H^G Res_H^G M \overset{\phi}{\simeq} R(G/H) \otimes_R M$. $\big(g \otimes m \longmapsto \phi(g \otimes m) := gH \otimes gm\big)$.

onde os módulos da direita são vistos como RG-módulos com a ação diagonal dada na Definição 1.1.3.

Demonstração. [4], Proposição III.5.6 ou [25], Proposição 1.4.10. ■

Corolário 1.4.1. $Ind_H^G R \simeq R(G/H)$.

Observação 1.4.2. Podemos definir $Coind_H^G M := Hom_{RH}(RG, M)$ e $Ind_H^G M := M \otimes_{RH} RG$, considerando M um RG-módulo à direita ([14], §2), e resultados similares aos apresentados anteriormente, são válidos.

Em particular, obtemos (como no corolário anterior) que

$$Ind_H^G R \simeq R(H\backslash G),$$

onde $R(H\backslash G)$ é o RG-módulo livre à direita dado pelas classes laterais Hg, $g \in G$, com a G-ação natural à direita.

1.5 Seqüência Exata Longa em Cohomologia

Definição 1.5.1. Consideremos os pares (G, M) e (G', M'), onde G, G' são grupos, M é um RG-módulo (à esquerda) e M' é um RG'-módulo (à esquerda). Uma ***aplicação*** de (G, M) em (G', M') é um par de aplicações (φ, ξ) que satisfaz as seguintes condições:

(a) $\varphi : G \longrightarrow G'$ é um homomorfismo de grupos e

(b) $\xi : M' \longrightarrow M$ é um homomorfismo de grupos abelianos tal que

$$\xi[\varphi(g).m'] = g.\xi(m'), \quad \text{para todos} \quad g \in G \quad \text{e} \quad m' \in M'.$$

Dizemos que os pares (G, M) e (G', M') são ***isomorfos***, se φ e ξ forem isomorfismos.

Notação 1.5.1. $(G, M) \simeq (G', M')$.

Seja $(\varphi, \xi) : (G, M) \longrightarrow (G', M')$ uma aplicação, como definida acima, e consideremos $\varepsilon : F \longrightarrow R$ e $\varepsilon' : F' \longrightarrow R$ resoluções projetivas de R sobre RG e RG', respectivamente.

Observemos que, $\varepsilon' : F' \longrightarrow R$ também é uma resolução projetiva de R sobre RG (via φ). De fato, basta considerarmos a G-ação (à esquerda) sobre cada F'_n da seguinte maneira:

$$\begin{aligned} G \times F'_n &\longrightarrow F'_n \\ (g, y) &\longmapsto g * y := \varphi(g).y \ . \end{aligned}$$

Assim, pela Proposição A.8.2, temos que existe uma única aplicação $f : F \longrightarrow F'$, a menos de homotopia preservando aumentação. Notemos que $f(g.x) = g.f(x)$, para todos $g \in G$ e $x \in F$ $\big($pois, f é uma aplicação de RG-módulos (à esquerda)$\big)$.

Logo, podemos considerar a seguinte aplicação

$$\begin{aligned} Hom(f, \xi) : \ Hom_{RG'}(F', M') &\longrightarrow Hom_{RG}(F, M) \\ \phi &\longmapsto \xi \circ \phi \circ f \end{aligned}$$

a qual é uma aplicação de cocadeias e induz uma aplicação bem definida

$$\begin{aligned} \boldsymbol{(\varphi, \xi)^*} : \ H^*(G', M') &\longrightarrow H^*(G, M) \\ [\phi] &\longmapsto [\xi \circ \phi \circ f] \ . \end{aligned}$$

Definição 1.5.2. Dada uma aplicação (φ, ξ) de (G, M) em (G', M'), a aplicação $(\varphi, \xi)^*$ construída anteriormente é denominada ***aplicação induzida em cohomologia*** por (φ, ξ). Em particular, se consideramos $\varphi = id_G : G \longrightarrow G$ e $\xi : M' \longrightarrow M$ obtemos

$$\begin{aligned} (id_G, \xi)^* : \ H^*(G, M') &\longrightarrow H^*(G, M) \\ [\phi] &\longmapsto [\xi \circ \phi] \ . \end{aligned}$$

Notação 1.5.2. (**Casos Particulares**)

(1) $(\varphi, id_M)^* = \varphi^*$, se $\varphi : G \longrightarrow G'$.

(2) $(id_G, \xi)^* = H^*(G, \xi)$, se $\xi : M' \longrightarrow M$.

Propriedade 1.5.1.

(1) se $\varphi = id_G : G \longrightarrow G$ e $\xi = id_M : M \longrightarrow M$, então $(\varphi, \xi)^* = id_{H^*(G,M)}$.

(2) $(\varphi, \xi)^* \circ (\varphi', \xi')^* = (\varphi' \circ \varphi, \xi \circ \xi')^* \overset{not.}{=} \big((\varphi', \xi') \circ (\varphi, \xi)\big)^*$, para todas as aplicações $(\varphi, \xi) : (G, M) \longrightarrow (G', M')$ e $(\varphi', \xi') : (G', M') \longrightarrow (G'', M'')$

Proposição 1.5.1. Se $(\varphi, \xi) : (G, M) \longrightarrow (G', M')$ é um isomorfismo de pares, então

$$(\varphi, \xi)^* : H^*(G, M) \longrightarrow H^*(G', M'),$$

é um isomorfismo e $\big((\varphi, \xi)^*\big)^{-1} = (\varphi^{-1}, \xi^{-1})^*$.

Demonstração.

Da hipótese, temos que existem isomorfismos $\varphi : G \longrightarrow G'$ e $\xi : M' \longrightarrow M$ e conseqüentemente, consideremos $\varphi^{-1} : G' \longrightarrow G$ e $\xi^{-1} : M \longrightarrow M'$ as inversas de φ e ξ, respectivamente.

Seja $(\varphi, \xi)^* : H^*(G', M') \longrightarrow H^*(G, M)$. Temos das propriedades vistas anteriormente que

$$(\varphi, \xi)^* \circ (\varphi^{-1} \circ \xi^{-1})^* = (\varphi^{-1} \circ \varphi, \xi \circ \xi^{-1})^* = (id_G, id_M)^* = id_{H^*(G,M)} \quad \text{e}$$

$$(\varphi^{-1}, \xi^{-1})^* \circ (\varphi \circ \xi)^* = (\varphi \circ \varphi^{-1}, \xi^{-1} \circ \xi)^* = (id_{G'}, id_{M'})^* = id_{H^*(G',M')}$$

Daí, temos que $(\varphi^{-1}, \xi^{-1})^*$ é uma inversa de $(\varphi, \xi)^*$ e portanto

$$H^*(G, M) \simeq H^*(G', M'). \qquad \blacksquare$$

Corolário 1.5.1. Se M é isomorfo a N, como RG-módulos, então $H^*(G, M) \simeq H^*(G, N)$.

Proposição 1.5.2. Seja $0 \longrightarrow M' \xrightarrow{\phi'} M \xrightarrow{\phi''} M'' \longrightarrow 0$ uma seqüência exata curta de RG-módulos (à esquerda). Então, para todo $n \in \mathbb{Z}$, existe uma aplicação natural $\Delta^n : H^n(G, M'') \longrightarrow H^{n+1}(G, M')$ tal que a seqüência

$$0 \longrightarrow H^0(G, M') \xrightarrow{(\phi')^0} H^0(G, M) \xrightarrow{(\phi'')^0} H^0(G, M'') \xrightarrow{\Delta^0} H^1(G, M') \xrightarrow{(\phi')^1} \cdots$$

é exata, onde as aplicações $(\phi')^n$ e $(\phi'')^n$ são as induzidas em cohomologia, ou seja, $(\phi')^n = H^n(G, \phi')$ e $(\phi'')^n = H^n(G, \phi'')$.

1.6 Lema de Shapiro

Dados G um grupo e H um subgrupo de G, apresentamos nesta seção uma relação entre a cohomologia de G e a de H. Tal resultado, dado a seguir, é conhecido como *Lema de Shapiro* e é utilizado na demonstração do principal resultado deste trabalho (Teorema 3.3.1).

Proposição 1.6.1. Sejam G um grupo, H um subgrupo de G e M um RH-módulo (à esquerda) ($R = \mathbb{Z}$ ou $\mathbb{Z}_2$). Consideremos a inclusão $i : H \longrightarrow G$ e $\pi : Coind_H^G M \longrightarrow M$ dada por $\pi(\phi) = \phi(1)$, para todo $\phi \in Coind_H^G M$. Então, a aplicação induzida $(i,\pi)^* : H^*\big(G, Coind_H^G M\big) \longrightarrow H^*(H,M)$ é um isomorfismo.

Demonstração.

Consideremos $\varepsilon : \cdots \longrightarrow F_1 \xrightarrow{\partial_1} F_0 \longrightarrow R$ e $\varepsilon' : \cdots \longrightarrow F_1' \xrightarrow{\partial_1'} F_0' \longrightarrow R$, ou simplesmente, $\varepsilon : F \longrightarrow R$ e $\varepsilon' : F' \longrightarrow R$, resoluções projetivas de R sobre RH e RG, respectivamente.

Notemos que pelo Lema A.8.1, $\varepsilon' : F' \longrightarrow R$ também é uma resolução projetiva de R sobre RH e como os grupos de cohomologia independem da resolução, podemos considerar $F = F'$ e, a aplicação de cadeias $f : F \longrightarrow F'$ como sendo a identidade de F, isto é, $f = id_F$.

Temos então que

$$\begin{aligned}(i,\pi)^* : H^*\left(G, Coind_H^G M\right) &\longrightarrow H^*(H,M)\\ [\varphi] &\longmapsto [\pi\circ\varphi\circ id_F] = [\pi\circ\varphi],\end{aligned}$$

onde $\varphi \in Hom_{RG}(F, Coind_H^G M)$ e $\pi\circ\varphi \in Hom_{RH}(F,M)$.

Agora, para cada $n \geqslant 0$, consideremos

$$\begin{aligned}\phi_n : Hom_{RG}\left(F_n, Coind_H^G M\right) &\longrightarrow Hom_{RH}(F_n, M)\\ \varphi &\longmapsto \phi_n(\varphi) = \pi\circ\varphi\ .\end{aligned}$$

Observemos que, $(\pi\circ\varphi)(hx) = h(\pi\circ\varphi)(x)$, para todos $h \in H$ e $x \in F_n$. De fato, pela definição de π, temos que $(\pi\circ\varphi)(hx) = \varphi(hx)(1)$.

Como $\varphi \in Hom_{RG}\big(F_n, Coind_H^G M\big)$ e $h \in H \subseteq G$, segue que

$$\varphi(hx)(1) = [h.\varphi(x)](1).$$

Daí, pela G-ação (à esquerda) no $Coind_H^G M$, vem que

$$[h.\varphi(x)](1) = \varphi(x)(1.h) = \varphi(x)(h) = \varphi(x)(h.1)$$

e usando o fato de que $\varphi(x) \in Coind_H^G M$, temos que

$$\varphi(x)(h.1) = h[\varphi(x)(1)] = h.(\pi \circ \varphi)(x).$$

Logo, $\phi_n(\varphi) = \pi \circ \varphi \in Hom_{RH}(F_n, M)$.

Ainda, temos que ϕ_n é um isomorfismo. Para vermos este fato, basta considerarmos

$$\begin{aligned} \psi_n : \ Hom_{RH}(F_n, M) &\longrightarrow Hom_{RG}(F_n, Coind_H^G M) \\ \rho &\longmapsto \psi_n(\rho) \ ; \ \psi_n(\rho)(x)(g) := \rho(g.x), \end{aligned}$$

para todos $x \in F_n$ e $g \in G$. Assim, temos que

- ψ_n está bem definida,
- $\psi_n \circ \phi_n = id_{Hom_{RG}(F_n, Coind_H^G M)}$ e
- $\phi_n \circ \psi_n = id_{Hom_{RH}(F_n, M)}$.

Agora, consideremos os complexos de cocadeias

$$C = \big\{C^n := Hom_{RG}(F_n, Coind_H^G M)\big\}_{n\in\mathbb{Z}} \text{ e } D = \big\{D^n := Hom_{RH}(F_n, M)\big\}_{n\in\mathbb{Z}}.$$

Seja $\phi = \{\phi_n\}_{n\in\mathbb{Z}}$ a família das aplicações $\phi_n : C^n \longrightarrow D^n$, que indicamos no diagrama abaixo

$$\begin{array}{ccc} \vdots & & \vdots \\ \downarrow & & \downarrow \\ C^n & \xrightarrow{\phi_n} & D^n \\ \downarrow{\scriptstyle \widetilde{\delta}^n} & & \downarrow{\scriptstyle \delta^n} \\ C^{n+1} & \xrightarrow[\phi_{n+1}]{} & D^{n+1} \\ \downarrow & & \downarrow \\ \vdots & & \vdots \end{array}$$

É fácil ver que ϕ é uma aplicação de cocadeias, isto é, $\delta^n \circ \phi_n = \phi_{n+1} \circ \widetilde{\delta}^n$.

Conseqüentemente, $\phi : Hom_{RG}(F, Coind_H^G M) \longrightarrow Hom_{RH}(F, M)$ induz um isomorfismo

$$\begin{aligned} \phi^* : H^*(C) &\longrightarrow H^*(D) \\ [\varphi] &\longmapsto \phi^*\big([\varphi]\big) = [\pi \circ \varphi] = (i, \pi)^*\big([\varphi]\big). \end{aligned}$$

Mas, $H^*(C) = H^*(G, Coind_H^G M)$ e $H^*(D) = H^*(H, M)$, e portanto temos que

$$H^*(G, Coind_H^G M) \simeq H^*(H, M). \qquad \blacksquare$$

Corolário 1.6.1. Sejam G um grupo e H um subgrupo de G tal que $[G : H] < \infty$. Então, $H^*(H, RH) \simeq H^*(G, RG)$.

Dado G um grupo, queremos determinar, como uma aplicação do resultado de Shapiro, os grupos de cohomologia $H^n\big(G, \mathcal{P}(G)\big)$ de G com coeficientes no $\mathbb{Z}_2G$-módulo (à esquerda) $\mathcal{P}(G)$, onde $\mathcal{P}(G)$ é o conjunto das partes de G (Exemplo A.7.2 *(2)*). Para isso, necessitamos inicialmente do seguinte lema:

Lema 1.6.1. Dados G um grupo e $\mathcal{P}(G)$ o conjunto das partes de G. Então, $\overline{\mathbb{Z}_2G} := Coind_{\{1\}}^G \mathbb{Z}_2 = Hom_{\mathbb{Z}_2}(\mathbb{Z}_2G, \mathbb{Z}_2) \simeq \mathcal{P}(G)$ como $\mathbb{Z}_2G$-módulos (à esquerda).

Demonstração.

Seja

$$\begin{aligned} \rho : \overline{\mathbb{Z}_2G} &\longrightarrow \mathcal{P}(G) \\ \phi &\longmapsto \rho(\phi) := A_\phi \,, \end{aligned}$$

tal que $A_\phi = \{g \in G \mid \phi(g^{-1}) = 1\}$.

Podemos verificar que ρ está bem definida e é uma aplicação de $\mathbb{Z}_2G$-módulos, pois é um homomorfismo de grupos e satisfaz $\rho(g'\phi) = g'\rho(\phi)$, para todo $g' \in G$.

Agora, consideremos

$$\begin{aligned} \psi : \mathcal{P}(G) &\longrightarrow \overline{\mathbb{Z}_2 G} = Hom_{\mathbb{Z}_2}(\mathbb{Z}_2 G, \mathbb{Z}_2) \\ A &\longmapsto \psi(A) := \phi_A \ , \end{aligned}$$

tal que $\phi_A(g) := \begin{cases} 1, & \text{se } \ g^{-1} \in A; \\ 0, & \text{se } \ g^{-1} \notin A. \end{cases}$

Temos também que ψ está bem definida e além disso

$$\rho \circ \psi = id_{\mathcal{P}(G)} \ \text{ e } \ \psi \circ \rho = id_{\overline{\mathbb{Z}_2 G}} \ .$$

Portanto, $\overline{\mathbb{Z}_2 G} = Hom_{\mathbb{Z}_2}(\mathbb{Z}_2 G, \mathbb{Z}_2) \simeq \mathcal{P}(G)$. ■

Proposição 1.6.2. Sejam G um grupo e $\mathcal{P}(G)$ o conjunto das partes de G. Então,

$$H^n\big(G, \mathcal{P}(G)\big) = \begin{cases} \mathbb{Z}_2, & \text{se } \ n = 0; \\ 0, & \text{se } \ n \geqslant 1. \end{cases}$$

Demonstração.

Usando o Lema de Shapiro e o resultado anterior, obtemos

$$H^n\big(G, \mathcal{P}(G)\big) \simeq H^n\left(G, Coind_{\{1\}}^G \mathbb{Z}_2\right) \simeq H^n(\{1\}, \mathbb{Z}_2) \simeq \begin{cases} \mathbb{Z}_2, & \text{se } \ n = 0; \\ 0, & \text{se } \ n \geqslant 1. \end{cases}$$ ■

Capítulo 2

Ends

Neste capítulo inicialmente (Seções 2.1 e 2.2) definimos o número de ends, $e(G)$, de um grupo G ([7] e [23]) e apresentamos alguns resultados, com destaque para a Proposição 2.2.1, que nos fornece uma fórmula cohomológica 1-dimensional para $e(G)$, quando G é infinito (finitamente gerado), e na Seção 2.3, definimos o número de ends de um par grupo (G, H), $e(G, H)$, onde H é um subgrupo de G ([12] e [22]). Isto é feito usando um tratamento puramente algébrico. Finalmente, na Seção 2.4, relacionamos ends de grupos finitamente gerados e de pares de grupos, com ends de espaços, mais especificamente com ends de Grafos de Cayley ([22]).

Vemos ainda, como conseqüência de um resultado de Scott (Proposição 2.4.4), que $e(G, H)$ pode assumir valores distintos de $0, 1, 2$ ou ∞, o que não ocorre para $e(G)$.

2.1 Subconjuntos Quase Invariantes e Ends de Grupos

Sejam G um grupo e $\mathcal{P}(G) = \{A \mid A \subseteq G\}$ o conjunto das partes de G. Vimos no Exemplo A.7.2 *(2)*, que $\mathcal{P}(G)$ tem uma estrutura de $\mathbb{Z}_2G$-módulo (à

esquerda), onde a operação de adição é a diferença simétrica, isto é,

$$A + B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A) = (A \cap B^c) \cup (A^c \cap B),$$

com A^c indicando o complementar de A em G e $A-B$ a diferença de conjuntos.

Agora, consideremos o subconjunto de $\mathcal{P}(G)$ dado por:

$$\mathcal{F}(G) := \{A \in \mathcal{P}(G) \mid A \text{ é finito } \}.$$

Definição 2.1.1. Dizemos que uma propriedade ocorre para ***quase todos os elementos*** de um conjunto, se ela ocorre para quase todos, exceto um número finito de elementos do conjunto.

Em particular, B é ***quase contido*** em um conjunto C, e denotamos por $B \overset{a}{\subseteq} C$, se quase todo elemento de B pertence a C.

Dizemos que B é ***quase igual*** a C, e denotamos por $B \overset{a}{=} C$, se $B \overset{a}{\subseteq} C$ e $C \overset{a}{\subseteq} B$.

Ainda, um subconjunto A de um grupo G é ***quase invariante (à esquerda)*** se $A \overset{a}{=} gA$, para todo $g \in G$, onde $gA := \{g.a \mid a \in A\}$.

Observação 2.1.1.

(1) A relação de *quase igualdade* é uma relação de equivalência.

(2) $B \overset{a}{=} C$ se, e somente se, $B + C$ é um conjunto finito, onde " $+$ " indica a operação diferença simétrica.

(3) A é quase invariante (à esquerda) em G se, e somente se, $A+gA \in \mathcal{F}(G)$, para todo $g \in G$.

(4) Dado A um subconjunto de G, $G_A := \{g \in G \mid A + gA \in \mathcal{F}(G)\} = \{g \in G \mid A \overset{a}{=} gA\}$ é um subgrupo de G $\big($pois dados $g, h \in G_A$, $gh^{-1} \in G_A$, visto que $(A+gh^{-1}A) = (A+gA)+gh^{-1}(A+hA) \in \mathcal{F}(G)\big)$, e A é quase invariante em G, quando $G_A = G$. Assim, A é quase invariante em G se, e somente se, $A + xA \in \mathcal{F}(G)$, para todo x variando num conjunto de geradores de G.

Seja $\mathcal{Q}(G) = \{A \in \mathcal{P}(G) \mid \forall\ g \in G,\ A + gA \in \mathcal{F}(G)\}$, o conjunto dos elementos quase invariantes em G. Observemos que $\mathcal{F}(G) \subseteq \mathcal{Q}(G)$, ainda $\mathcal{F}(G)$ e $\mathcal{Q}(G)$ são $\mathbb{Z}_2G$-submódulos (à esquerda) de $\mathcal{P}(G)$ e temos os $\mathbb{Z}_2G$-módulos quocientes $\dfrac{\mathcal{P}(G)}{\mathcal{F}(G)}$ e $\dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$. Denotamos um elemento de $\dfrac{\mathcal{P}(G)}{\mathcal{F}(G)}$ ou de $\dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$ por $\overline{A} := A + \mathcal{F}(G)$. Em particular, $\overline{\varnothing} = \varnothing + \mathcal{F}(G)$.

Propriedade 2.1.1.

(1) $G \in \mathcal{Q}(G)$, pois $G + gG = G + G = \varnothing$.

(2) Dados $A, B \in \mathcal{Q}(G)$, temos:

$$\begin{aligned} \overline{A} = \overline{B} \text{ em } \frac{\mathcal{Q}(G)}{\mathcal{F}(G)} &\Leftrightarrow A + \mathcal{F}(G) = B + \mathcal{F}(G) \\ &\Leftrightarrow A + B = A + (-B) \in \mathcal{F}(G) \\ &\Leftrightarrow A \overset{a}{=} B. \end{aligned}$$

(3) Se A é um elemento de $\mathcal{Q}(G)$, então A^c também pertence a $\mathcal{Q}(G)$, pois

$$\begin{aligned} A^c + gA^c &= \left[A^c \cap (gA^c)^c\right] \cup \left[A \cap (gA^c)\right] \\ &= \left[A^c \cap gA\right] \cup \left[A \cap (gA)^c\right] \\ &= A + gA \in \mathcal{F}(G). \end{aligned}$$

(4) Se $A \in \mathcal{Q}(G)$ e G é infinito, então $\overline{A}$ e $\overline{A^c}$ são elementos de $\dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$ distintos, pois $A + A^c = G \notin \mathcal{F}(G)$.

(5) Se $A, B, C \in \mathcal{P}(G)$ (ou $\mathcal{Q}(G)$), são infinitos, dois a dois disjuntos, então $\overline{A}, \overline{B}$ e $\overline{C}$ são elementos distintos em $\dfrac{\mathcal{P}(G)}{\mathcal{F}(G)}$ $\left(\text{ou } \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}\right)$ e ainda, $\overline{A}+\overline{B} = \overline{A \cup B}$ é diferente de $\overline{A}, \overline{B}$ e $\overline{C}$.

Definição 2.1.2. Seja G um grupo. O ***número de ends de G***, que denotamos por $\boldsymbol{e(G)}$, é definido por

$$e(G) := dim_{\mathbb{Z}_2}\left(\frac{\mathcal{Q}(G)}{\mathcal{F}(G)}\right).$$

Observação 2.1.2.

(1) Poderíamos ter considerado $\mathcal{P}(G)$ como um $\mathbb{Z}_2G$-módulo *à direita*, o subconjunto de $\mathcal{P}(G)$ dos elementos quase invariantes *à direita*,

$$\mathcal{Q}(G) = \{A \in \mathcal{P}(G) \mid \forall\, g \in G, A + Ag \in \mathcal{F}(G)\},$$

e de modo similar, definir

$$e(G) := dim_{\mathbb{Z}_2}\left(\frac{\mathcal{Q}(G)}{\mathcal{F}(G)}\right).$$

(2) Temos que as duas definições apresentadas para $e(G)$ coincidem $\big($pois, A é quase invariante *à esquerda* $\Leftrightarrow A + gA \in \mathcal{F}(G),\ \forall\ g \in G \Leftrightarrow A^{-1} + A^{-1}g^{-1} \in \mathcal{F}(G),\ \forall\ g \in G \Leftrightarrow A^{-1}$ é invariante *à direita*, onde $A^{-1} := \{a^{-1} \mid a \in A\}\big)$, e resultados similares aos que apresentamos usando a G-ação e elementos quase invariantes à esquerda são válidos também quando trabalhamos à direita.

(3) Segue da Propriedade 2.1.1 *(2)*, que $e(G)$ mede quantos subconjuntos quase invariantes G contém (e que *não* são quase iguais).

(4) Podemos facilmente verificar (proposição seguinte) que $\dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$ consiste precisamente dos elementos de $\dfrac{\mathcal{P}(G)}{\mathcal{F}(G)}$ que são invariantes pela G-ação.

Proposição 2.1.1. $\left(\dfrac{\mathcal{P}(G)}{\mathcal{F}(G)}\right)^G = \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$.

Demonstração. De fato,

$$\begin{aligned}
\left(\frac{\mathcal{P}(G)}{\mathcal{F}(G)}\right)^G &= \left\{\overline{A} \in \frac{\mathcal{P}(G)}{\mathcal{F}(G)} \mid g.\overline{A} = \overline{A},\ \forall\ g \in G\right\} \\
&= \left\{\overline{A} \in \frac{\mathcal{P}(G)}{\mathcal{F}(G)} \mid \overline{gA} = \overline{A},\ \forall\ g \in G\right\} \\
&= \left\{\overline{A} \in \frac{\mathcal{P}(G)}{\mathcal{F}(G)} \mid g.A + \mathcal{F}(G) = A + \mathcal{F}(G),\ \forall\ g \in G\right\} \\
&= \left\{\overline{A} \in \frac{\mathcal{P}(G)}{\mathcal{F}(G)} \mid g.A + A \in \mathcal{F}(G),\ \forall\ g \in G\right\} \\
&= \frac{\mathcal{Q}(G)}{\mathcal{F}(G)}\,.
\end{aligned}$$

■

Proposição 2.1.2. Seja G um grupo.

(a) Se G é infinito, então $\overline{\varnothing}$ e $\overline{G}$ são elementos distintos em $\dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$ e portanto $e(G) \geqslant 1$.

(b) G é finito se, e somente se, $e(G) = 0$.

(c) $e(G) \geqslant 2$ se, e somente se, existe $\overline{A} \in \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$ tal que $\overline{A} \neq \overline{\varnothing}$ e $\overline{A} \neq \overline{G}$. Neste caso, $\overline{\varnothing}$, $\overline{A}$, $\overline{A^c}$ e $\overline{G}$ são elementos distintos em $\dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$.

(d) $e(G) = 2$ se, e somente se, existe $\overline{A}$ como em *(c)* tal que para qualquer $\overline{B} \in \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$, com $\overline{B} \neq \overline{\varnothing}$ e $\overline{B} \neq \overline{G}$, tem-se que $\overline{B} = \overline{A}$ ou $\overline{B} = \overline{A^c}$.

Demonstração.

(a) Como já observamos, $G \in \mathcal{Q}(G)$.

Agora, como G é infinito, temos que $G \notin \mathcal{F}(G)$. Logo, $G + \mathcal{F}(G) \neq \varnothing + \mathcal{F}(G)$ e assim $\overline{G} \neq \overline{\varnothing}$.

Portanto, $e(G) = dim_{\mathbb{Z}_2}\left(\dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}\right) \geqslant 1$.

(b) Observemos que $\mathcal{P}(G) = \mathcal{F}(G) = \mathcal{Q}(G)$, pois G é finito.

Assim, $e(G) = dim_{\mathbb{Z}_2}\left(\dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}\right) = dim_{\mathbb{Z}_2}(\{\overline{\varnothing}\}) = 0$.

Reciprocamente, suponhamos por absurdo que G seja infinito. Então, por *(a)*, segue que $e(G) \geqslant 1$, contradizendo o fato de $e(G) = 0$.

Portanto, G é finito.

(c) Claramente, $e(G) \geqslant 2$ se, e somente se, existe $\overline{A} \in \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$ tal que $\overline{A} \neq \overline{\varnothing}$ e $\overline{A} \neq \overline{G}$. Neste caso, considerando um tal $A \in \mathcal{Q}(G)$, temos também que $A^c \in \mathcal{Q}(G)$ (Propriedade 2.1.1 *(3)*). Logo, $\overline{A^c} \in \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$.

- $\overline{A^c} \neq \overline{A}$. De fato,
  se $\overline{A^c} = \overline{A}$, então $A^c + A = (A^c \cap A^c) \cup (A \cap A) = A^c \cup A = G \in \mathcal{F}(G)$, o que é uma contradição, pois G é infinito $\big($pelo fato de $e(G) \geqslant 2$ e pelo item *(b)*$\big)$.

- $\overline{A^c} \neq \overline{\varnothing}$, pois como $\overline{A} \neq \overline{G}$ segue que

$$A^c = (A \cap G^c) \cup (A^c \cap G) = A + G \notin \mathcal{F}(G).$$

$\overline{A^c} \neq \overline{G}$, pois se $\overline{A^c} = \overline{G}$, então

$$A^c + G = (A^c \cap G^c) \cup (A \cap G) = A \in \mathcal{F}(G),$$

o que é um absurdo, uma vez que A é infinito $\big($pois $\overline{A} \neq \overline{\varnothing} \Leftrightarrow A + \varnothing \notin \mathcal{F}(G) \Leftrightarrow A \notin \mathcal{F}(G)\big)$.

Logo, $\big\{\overline{\varnothing}, \overline{A}, \overline{A^c}, \overline{G}\big\} \subseteq \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$ e como $\big\{\overline{\varnothing}, \overline{A}, \overline{A^c}, \overline{G}\big\} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$, segue que $e(G) \geqslant 2$.

(d) Segue diretamente de *(c)*. ■

Exemplo 2.1.1. Como $\mathbb{Z}_n$, S_3 e $\mathbb{Z}_2 \times \mathbb{Z}_3$ são grupos finitos, temos que

$$e(\mathbb{Z}_n) = e(S_3) = e(\mathbb{Z}_2 \times \mathbb{Z}_3) = 0.$$

Proposição 2.1.3. Se G e G' são grupos isomorfos, então $e(G) = e(G')$, isto é, $e(G)$ é um invariante algébrico.

Demonstração.

Basta observarmos que, se $G \simeq G'$, então $\dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)} \simeq \dfrac{\mathcal{Q}(G')}{\mathcal{F}(G')}$ como $\mathbb{Z}_2$-espaços vetoriais. ■

Teorema 2.1.1. Se G é um grupo cíclico infinito, isto é, $G = \langle t \rangle \simeq \mathbb{Z}$, então $e(G) = 2$.

Demonstração.

Pela Proposição 2.1.2, é suficiente mostrar que existe $\overline{A} \in \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$ tal que $\overline{A} \neq \overline{\varnothing}$ e $\overline{A} \neq \overline{G}$, e para qualquer $\overline{B} \in \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$, com $\overline{B} \neq \overline{\varnothing}$ e $\overline{B} \neq \overline{G}$, tenhamos $\overline{B} = \overline{A}$ ou $\overline{B} = \overline{A^c}$.

Sendo assim, consideremos $A = \{t^n \mid n > 0\}$. Logo,

- $\overline{A} \in \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$, pois para todo $g = t^k \in G$, $gA = \{t^{k+n} \mid n > 0\}$ e

$$A + gA = \big(A \cap (gA)^c\big) \cup (A^c \cap gA) = (A \cap gA^c) \cup (A^c \cap gA) \in \mathcal{F}(G).$$

$\big($Por exemplo, se $k > 0$, $A \cap gA^c = \{t, \ldots, t^k\}$ e $A^c \cap gA = \varnothing.\big)$

- $\overline{A} \neq \overline{\varnothing}$, pois $A \notin \mathcal{F}(G)$ e $\overline{A} \neq \overline{G}$, pois, se $\overline{A} = \overline{G}$, então

$$A^c = (A \cap G^c) \cup (A^c \cap G) = A + G \in \mathcal{F}(G),$$

o que é um absurdo, pois $A^c = \{t^n \mid n \leqslant 0\}$ é infinito.

Agora, provemos a seguinte afirmação:

Afirmação. Se $\overline{B} \in \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$, então para quase todo $n \in \mathbb{Z}$ (ou seja, exceto para um número finito, isto é, $n \neq n_1, \ldots, n_k$), $t^n \in B$ implica que $t^{n+1} \in B$ e $t^{n-1} \in B$.

De fato, seja $\overline{B} \in \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$, com $B \in \mathcal{Q}(G)$. Assim, para todo $g \in G$, $B + gB \in \mathcal{F}(G)$, isto é, $\overline{B} = \overline{gB}$. Particularmente, temos que $\overline{B} = \overline{tB}$.

Suponhamos que existam infinitos valores inteiros n tais que:

(a) $t^n \in B$ e $t^{n+1} \notin B$, ou

(b) $t^n \in B$ e $t^{n-1} \notin B$ (equivalentemente, $t^n \notin tB$).

Desta forma, existiriam infinitos valores de n tais que:

(a) $t^{n+1} = t.t^n \in tB$ (pois, $t^n \in B$) e $t^{n+1} \notin B$, logo $t^{n+1} \in tB \cap B^c$, ou

(b) $t^n = t.t^{n-1} \notin tB$ (pois, $t^{n-1} \notin B$) e $t^n \in B$, logo, $t^{n+1} \in (tB)^c \cap B$.

Então, $tB + B = (tB \cap B^c) \cup [(tB)^c \cap B]$ seria infinito, isto é, $B \notin \mathcal{Q}(G)$ e assim $\overline{B} \notin \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$, o que é uma contradição.

Logo, a afirmação acima é verdadeira e nos diz que pode existir apenas um número finito de elementos de B tal que $t^n \in B$ mas $t^{n+1} \notin B$ ou $t^{n-1} \notin B$. O caso de maior interesse é quando B é infinito, pois no caso de B ser finito já

temos que isto acontece e também é válido para $B = A = \{t^n \mid n > 0\}$, pois apenas para $n = 1$ tem-se que $t^n \in B$ mas $t^{n-1} \notin B$. Para $n \geqslant 2$, $t^n \in B$ e temos $t^{n+1} \in B$ e $t^{n-1} \in B$.

Agora, sejam $\overline{B} \in \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$ e A como acima. Vejamos as possibilidades para $B \cap A$ e $B \cap A^c$:

- $B \cap A$ finito e $B \cap A^c$ finito.

  Assim, temos que $B = B \cap (A \cup A^c) = (B \cap A) \cup (B \cap A^c) \in \mathcal{F}(G)$.

  Portanto, $\overline{B} = \overline{\varnothing}$.

- $B \cap A$ infinito e $B \cap A^c$ infinito.

  Como $B \cap A$ é infinito, temos que B também o é, e da afirmação segue que existe um inteiro positivo m_1 tal que $t^n \in B \cap A$, para todo $n > m_1$. De fato, tomemos $m_0 = max\ \{n_1, \ldots, n_k\}$ onde $n_1, \ldots, n_k$ são os inteiros dados na afirmação. Como $B \cap A$ é infinito, existe $m_1 > m_0,\ m_1 > 0$ tal que $t^{m_1} \in B \cap A$ e como $m_1 \neq n_i,\ i = 1, \ldots, k$, então $t^{m_1+1}, t^{m_1+2}, \ldots \in B \cap A$, isto é, $t^m \in B \cap A$, para todo $m > m_1$. Conseqüentemente, $A \cap B^c \subseteq \{t^r \mid 0 \leqslant r \leqslant m_1\}$ e portanto é finito.

  Analogamente, usando que $B \cap A^c$ é infinito e a afirmação, temos que existe um inteiro m_2 tal que $t^n \in B \cap A^c$, para todo $n > m_2$. Tome $m_0 = min\ \{n_1, \ldots, n_k\}$. Como $B \cap A^c$ é infinito, existe $m_2 < m_0$, $m_2 < 0$ tal que $t^{m_2} \in B \cap A^c$ e $t^m \in B \cap A^c$, para todo $m < m_2$. Daí, $A^c \cap B^c \subseteq \{t^r \mid m_2 \leqslant r \leqslant 0\}$ e portanto é finito.

  Desta forma, $B^c = B^c \cap (A \cup A^c) = (B^c \cap A) \cup (B^c \cap A^c)$ é finito.

  Portanto, $\overline{B^c} = \overline{\varnothing}$, ou equivalentemente, $\overline{B} = \overline{G}$.

- $B \cap A$ finito e $B \cap A^c$ infinito.

  Vimos anteriormente que, $B \cap A^c$ infinito implica em $A^c \cap B^c$ ser finito.

  Logo, $B + A^c = (B \cap A) \cup (B^c \cap A^c)$ é finito e portanto, $\overline{B} = \overline{A^c}$.

- $B \cap A$ infinito e $B \cap A^c$ finito.

  Já sabemos que $B \cap A$ infinito, implica em $A \cap B^c$ finito.

  Logo, $B + A = (B \cap A^c) \cup (B^c \cap A)$ é finito e portanto, $\overline{B} = \overline{A}$.

Então, dado qualquer $\overline{B} \in \dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)}$, com $\overline{B} \neq \overline{\varnothing}$ e $\overline{B} \neq \overline{G}$ temos que $\overline{B} = \overline{A}$ ou $\overline{B} = \overline{A^c}$.

Portanto, segue que $\dfrac{\mathcal{Q}(G)}{\mathcal{F}(G)} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$ e assim $e(G) = 2$. ■

Teorema 2.1.2. Sejam G um grupo e H um subgrupo normal e finito de G. Então, $e(G) = e(G/H)$, onde G/H indica o grupo quociente de G por H.

Demonstração.

Como H é um subgrupo normal de G, temos que $gH = Hg$, para todo $g \in G$, e os conjuntos $G/H = \{gH \mid g \in G\}$ e $H\backslash G = \{Hg \mid g \in G\}$ coincidem.

Consideremos $G/H = \{Hg \mid g \in G\}$ o grupo quociente de G por H e $\pi : G \longrightarrow G/H$ o homomorfismo quociente tal que, para cada $g \in G$ associa o elemento $\pi(g) = Hg \in G/H$.

Notemos que,

(1) como π é sobrejetor, temos que $\pi\left[\pi^{-1}(B)\right] = B$, para todo $B \subseteq G/H$.

(2) $\pi^{-1}[\pi(A)] = HA$, para todo $A \subseteq G$. De fato,

$$\begin{aligned}
\pi^{-1}[\pi(A)] &= \{g \in G \mid \pi(g) \in \pi(A)\} = \{g \in G \mid Hg \in \pi(A)\} \\
&= \{g \in G \mid Hg = Ha, \text{ para algum } a \in A\} \\
&= \{g \in G \mid ga^{-1} \in H,\ a \in A\} \\
&= \{g \in G \mid ga^{-1} = h,\ h \in H \text{ e } a \in A\} \\
&= \{g \in G \mid g = ha,\ h \in H \text{ e } a \in A\} = HA.
\end{aligned}$$

(3) $\pi^{-1}(B + B') = \pi^{-1}(B) + \pi^{-1}(B')$, para todos $B, B' \subseteq G/H$, onde $+$ denota a operação diferença simétrica. De fato,

$$\begin{aligned}\pi^{-1}(B + B') &= \pi^{-1}[(B \cap (B')^c) \cup (B^c \cap B')] \\ &= \pi^{-1}[B \cap (B')^c] \cup \pi^{-1}(B^c \cap B') \\ &= [\pi^{-1}(B) \cap \pi^{-1}((B')^c)] \cup [\pi^{-1}(B^c) \cap \pi^{-1}(B')] \\ &= [\pi^{-1}(B) \cap (\pi^{-1}(B'))^c] \cup [(\pi^{-1}(B))^c \cap \pi^{-1}(B')] \\ &= \pi^{-1}(B) + \pi^{-1}(B').\end{aligned}$$

(4) $\pi^{-1}[\pi(g)B] = g\pi^{-1}(B)$, para todos $g \in G$ e $B \subseteq G/H$.

Observemos que,

$$x \in \pi^{-1}[\pi(g)B] \Rightarrow \pi(x) \in \pi(g)B \Rightarrow \pi(x) = \pi(g).b, \quad \text{para algum} \quad b \in B.$$

Como π é sobrejetor, temos que existe $g' \in G$ tal que $b = \pi(g')$. Assim,

$$\begin{aligned}\pi(x) = \pi(g).\pi(g') = \pi(gg') \Rightarrow Hx = Hgg' \Rightarrow (gg')x^{-1} \in H \\ \Rightarrow gg'x^{-1} = h, \quad \text{para algum} \quad h \in H.\end{aligned}$$

Logo, $gg' = hx \in Hx = xH$. Desta forma, existe $h' \in H$ tal que

$$gg' = xh' \Rightarrow x = gg'(h')^{-1}.$$

Pelo fato de,

$$\begin{aligned}\pi[g'(h')^{-1}] &= \pi(g')\pi[(h')^{-1}] = (Hg')[H(h')^{-1}] \\ &= (Hg')(He) = Hg' = \pi(g') = b \in B,\end{aligned}$$

segue que $x = gg'(h')^{-1} \in g\pi^{-1}(B)$.

Assim, temos que $\pi^{-1}[\pi(g)B] \subseteq g\pi^{-1}(B)$.

Agora, seja $u \in g\pi^{-1}(B)$. Temos que, $u = gy$, com $y \in \pi^{-1}(B)$. Daí, $\pi(y) \in B$ e $\pi(u) = \pi(gy) = \pi(g)\pi(y) \in \pi(g)B$.

Logo, $u \in \pi^{-1}[\pi(g)B]$ e portanto $g\pi^{-1}(B) \subseteq \pi^{-1}[\pi(g)B]$.

(5) $\pi^{-1}[B+\pi(g)B] = \pi^{-1}(B)+\pi^{-1}[\pi(g)B] = \pi^{-1}(B)+g\pi^{-1}(B)$, para todo $B \subseteq G/H$.

(6) $B \in \mathcal{Q}(G/H)$ se, e somente se, $\pi^{-1}(B) \in \mathcal{Q}(G)$.

De fato, se $B \in \mathcal{Q}(G/H)$, então $B+\overline{g}B \in \mathcal{F}(G/H)$, para todo $\overline{g} = \pi(g) \in G/H$. Logo, $B+\pi(g)B \in \mathcal{F}(G/H)$, para todo $g \in G$, isto é, $B+\pi(g)B = \{Hg_1, \ldots, Hg_k\}$. Então,

$$\begin{aligned}\pi^{-1}(B)+g\pi^{-1}(B) &= \pi^{-1}[B+\pi(g)B] = \pi^{-1}\big(\{Hg_1,\ldots,Hg_k\}\big)\\ &= Hg_1 \cup \ldots \cup Hg_k \in \mathcal{F}(G),\end{aligned}$$

pois H é finito.

Reciprocamente, se $\pi^{-1}(B) \in \mathcal{Q}(G)$, então $\pi^{-1}(B)+g\pi^{-1}(B) \in \mathcal{F}(G)$, para todo $g \in G$. Assim,

$$\pi^{-1}[B+\pi(g)B] \in \mathcal{F}(G) \Rightarrow \pi[\pi^{-1}(B+\pi(g)B)] \in \mathcal{F}(G/H).$$

Daí, $B+\pi(g)B \in \mathcal{F}(G/H)$, para todo $g \in G$, pois π é sobrejetor.

Portanto, $B \in \mathcal{Q}(G/H)$.

(7) Para todo $A \in \mathcal{Q}(G)$, temos que $\pi^{-1}[\pi(A)]+\mathcal{F}(G) = A+\mathcal{F}(G)$ e $\pi^{-1}[\pi(A)] \in \mathcal{Q}(G)$.

De fato, seja $A \in \mathcal{Q}(G)$. Suponhamos que $H = \{h_1, \ldots, h_n\}$. Daí,

$$\begin{aligned}A+\pi^{-1}[\pi(A)] = A+HA &= A+(h_1A \cup \ldots \cup h_nA)\\ &\subseteq (A+h_1A)\cup\ldots\cup(A+h_nA) \in \mathcal{F}(G),\end{aligned}$$

pois $A \in \mathcal{Q}(G)$.

Mas, $A+\pi^{-1}[\pi(A)] \in \mathcal{F}(G)$ se, e somente se,

$$A+\mathcal{F}(G) = \pi^{-1}[\pi(A)]+\mathcal{F}(G).$$

Além disso, $A+\pi^{-1}[\pi(A)] = X \in \mathcal{F}(G)$ e assim, $\pi^{-1}[\pi(A)] = A+X \in \mathcal{Q}(G)$, uma vez que $A \in \mathcal{Q}(G)$ e $X \in \mathcal{F}(G) \subseteq \mathcal{Q}(G)$.

(8) Se $A \in \mathcal{Q}(G)$, então $\pi^{-1}[\pi(A)] \in \mathcal{Q}(G/H)$.

Como vimos anteriormente, se $A \in \mathcal{Q}(G)$, então $\pi^{-1}[\pi(A)] \in \mathcal{Q}(G)$. Por outro lado, se $\pi^{-1}[\pi(A)] \in \mathcal{Q}(G)$, então $B = \pi(A) \in \mathcal{Q}(G/H)$.

Desta maneira, temos bem definida uma aplicação induzida

$$\begin{aligned} \widetilde{\pi}: \quad \frac{\mathcal{Q}(G)}{\mathcal{F}(G)} &\longrightarrow \frac{\mathcal{Q}(G/H)}{\mathcal{F}(G/H)} \\ A + \mathcal{F}(G) &\longmapsto \pi(A) + \mathcal{F}(G/H). \end{aligned}$$

Observemos que $\widetilde{\pi}$ é um homomorfismo bijetor.

Portanto,

$$e(G) = dim_{\mathbb{Z}_2}\left(\frac{\mathcal{Q}(G)}{\mathcal{F}(G)}\right) = dim_{\mathbb{Z}_2}\left(\frac{\mathcal{Q}(G/H)}{\mathcal{F}(G/H)}\right) = e(G/H). \qquad \blacksquare$$

Exemplo 2.1.2. Para qualquer grupo finito G, temos que

$$e(\mathbb{Z} \oplus G) = 2.$$

2.2 Uma Fórmula Cohomológica para $e(G)$

Nosso objetivo nesta seção, é relacionar a teoria de *ends* com a de *cohomologia* de grupos. Tal relação, está explicita nos resultados abaixo.

Lema 2.2.1. Seja G um grupo. Então, $e(G) = dim_{\mathbb{Z}_2} H^0\left(G, \frac{\mathcal{P}(G)}{\mathcal{F}(G)}\right)$.

Demonstração.

É conseqüência imediata das Proposições 2.1.1 e 1.1.2, mais precisamente

$$e(G) = dim_{\mathbb{Z}_2}\left(\frac{\mathcal{Q}(G)}{\mathcal{F}(G)}\right) = dim_{\mathbb{Z}_2}\left[\left(\frac{\mathcal{P}(G)}{\mathcal{F}(G)}\right)^G\right] = dim_{\mathbb{Z}_2} H^0\left(G, \frac{\mathcal{P}(G)}{\mathcal{F}(G)}\right). \qquad \blacksquare$$

Lema 2.2.2. O isomorfismo $\rho : \overline{\mathbb{Z}_2 G} \longrightarrow \mathcal{P}(G)$, dado no Lema 1.6.1, leva o $\mathbb{Z}_2G$-módulo (à esquerda) $\mathbb{Z}_2G$, que pode ser visto como um $\mathbb{Z}_2G$-submódulo de $\overline{\mathbb{Z}_2 G}$, no $\mathbb{Z}_2G$-submódulo $\mathcal{F}(G)$ de $\mathcal{P}(G)$.

Demonstração.

Definamos

$$\begin{aligned} \xi : \mathbb{Z}_2G &\longrightarrow \overline{\mathbb{Z}_2G} \\ g' &\longmapsto \xi(g') , \end{aligned}$$

tal que $\xi(g')(g) = \begin{cases} 1, & \text{se } g = (g')^{-1}; \\ 0, & \text{c. c.} \end{cases}$

Temos que

- ξ é uma aplicação de $\mathbb{Z}_2G$-módulos, isto é, $\xi(g_0g') = g_0\xi(g')$, para todo $g_0, g' \in G$, pois

$$\xi(g_0g')(g) = \begin{cases} 1, & \text{se } g = (g_0g')^{-1} \Rightarrow g' = g_0^{-1}.g^{-1}; \\ 0, & \text{c. c.} \end{cases} \quad \text{e}$$

$$\big(g_0.\xi(g')\big)(g) = \xi(g')(gg_0) = \begin{cases} 1, & \text{se } gg_0 = (g')^{-1} \Rightarrow g' = g_0^{-1}.g^{-1}; \\ 0, & \text{c. c.} \end{cases}$$

- ξ é um monomorfismo. Desta forma, $\mathbb{Z}_2G \simeq \xi(\mathbb{Z}_2G)$.

Agora, precisamos mostrar que $\rho[\xi(\mathbb{Z}_2G)] = \mathcal{F}(G)$.

Para isto, seja $A \in \rho[\xi(\mathbb{Z}_2G)]$. Então, $A = \rho[\xi(x)]$, $x \in \mathbb{Z}_2G$. Logo,

$$x = 1.g_1 + \cdots + 1.g_s, \quad \text{onde } \ 1 \in \mathbb{Z}_2, \quad g_i \in G, \quad g_i \neq g_j, \quad i, j = 1, \ldots, s.$$

Desta maneira,

$$\xi(x) = 1\xi(g_1) + \cdots + \xi(g_s), \ \text{ onde } \xi(g_i)(g) = \begin{cases} 1, & \text{se } g = g_i^{-1}; \\ 0, & \text{c. c.} \end{cases}, \ i = 1, \ldots, s.$$

Assim, $A = \rho[\xi(x)] = \{g \in G \mid \xi(x)(g^{-1}) = 1\} = \{g_1, \ldots, g_s\}$, isto é, $A \in \mathcal{F}(G)$.

Reciprocamente, seja $A = \{g_1, \ldots, g_s\} \in \mathcal{F}(G)$. Consideremos

$$x = 1g_1 + \cdots + 1g_s \in \mathbb{Z}_2G.$$

Daí, $\xi(x) \in \xi(\mathbb{Z}_2G)$.

Como $\rho[\xi(x)] = \{g \in G \mid \xi(x)(g^{-1}) = 1\} = \{g_1, \ldots, g_s\} = A$ e assim temos que $A \in \rho[\xi(\mathbb{Z}_2G)]$.

Portanto, $\mathbb{Z}_2G \simeq \xi(\mathbb{Z}_2G)$ e $\rho[\xi(\mathbb{Z}_2G)] = \mathcal{F}(G)$. ■

Lema 2.2.3. Seja G um grupo. Temos um $\mathbb{Z}_2G$-isomorfismo entre $\dfrac{\mathcal{P}(G)}{\mathcal{F}(G)}$ e $\dfrac{\overline{\mathbb{Z}_2G}}{\mathbb{Z}_2G}$, onde $\overline{\mathbb{Z}_2G} = Hom_{\mathbb{Z}_2}(\mathbb{Z}_2G, \mathbb{Z}_2) = Coind_{\{1\}}^{G}\mathbb{Z}_2$ e daí,

$$e(G) = dim_{\mathbb{Z}_2} H^0\left(G, \frac{\overline{\mathbb{Z}_2G}}{\mathbb{Z}_2G}\right).$$

Demonstração.

Conforme o Lema 1.6.1

$$\begin{aligned} \rho:\ Hom_{\mathbb{Z}_2}(\mathbb{Z}_2G, \mathbb{Z}_2) &\longrightarrow \mathcal{P}(G) \\ \phi &\longmapsto \rho(\phi) := A_\phi\ , \end{aligned}$$

tal que $A_\phi = \{g \in G \mid \phi(g^{-1}) = 1\}$, é um $\mathbb{Z}_2G$-isomorfismo.

Assim ρ induz um $\mathbb{Z}_2G$-isomorfismo $\overline{\rho}: \dfrac{\overline{\mathbb{Z}_2G}}{\rho^{-1}(\mathcal{F}(G))} \longrightarrow \dfrac{\mathcal{P}(G)}{\mathcal{F}(G)}$.

Pelo Lema 2.2.2, podemos identificar $\rho^{-1}(\mathcal{F}(G))$ com $\mathbb{Z}_2G$ e daí, $\mathbb{Z}_2G$ pode ser considerado um $\mathbb{Z}_2G$-submódulo de $\overline{\mathbb{Z}_2G}$.

Logo, temos o $\mathbb{Z}_2G$-isomorfismo

$$\sigma: \frac{\mathcal{P}(G)}{\mathcal{F}(G)} \longrightarrow \frac{\overline{\mathbb{Z}_2G}}{\mathbb{Z}_2G}.$$

Portanto, $H^0\left(G, \dfrac{\mathcal{P}(G)}{\mathcal{F}(G)}\right) \simeq H^0\left(G, \dfrac{\overline{\mathbb{Z}_2G}}{\mathbb{Z}_2G}\right)$ e conseqüentemente,

$$e(G) = dim_{\mathbb{Z}_2} H^0\left(G, \frac{\overline{\mathbb{Z}_2G}}{\mathbb{Z}_2G}\right).$$ ■

Observação 2.2.1. Podemos mostrar que se G é finitamente gerado $H^0\left(G, \dfrac{\overline{\mathbb{Z}G}}{\mathbb{Z}G}\right)$ é um grupo abeliano livre, onde $\overline{\mathbb{Z}G} := Hom_{\mathbb{Z}}(\mathbb{Z}G, \mathbb{Z})$ ([27], Lema 3.6) e que $e(G) := rank_{\mathbb{Z}} H^0\left(G, \dfrac{\overline{\mathbb{Z}G}}{\mathbb{Z}G}\right)$, ou mais geralmente

$$e(G) := rank_R H^0\left(G, \frac{\overline{RG}}{RG}\right), \tag{2.1}$$

onde R é qualquer domínio de ideais principais e "$rank_R$" indica o *posto* ou *rank* como R-módulo ([28], p. 93). Assim, podemos usar (2.1) como a definição de $e(G)$.

Vamos considerar aqui apenas $R = \mathbb{Z}$ ou $\mathbb{Z}_2$.

Proposição 2.2.1. Seja G um grupo infinito, então

(a) $e(G) = 1 + dim_{\mathbb{Z}_2} H^1(G, \mathbb{Z}_2 G) = 1 + dim_{\mathbb{Z}_2} \left(\dfrac{Der(G, \mathbb{Z}_2 G)}{P(G, \mathbb{Z}_2 G)} \right)$.

(b) $e(G) = 1 + rank_{\mathbb{Z}} H^1(G, \mathbb{Z}G) = 1 + rank_{\mathbb{Z}} \left(\dfrac{Der(G, \mathbb{Z}G)}{P(G, \mathbb{Z}G)} \right)$, se G é também finitamente gerado.

Demonstração.

Seja

$$0 \longrightarrow RG \xrightarrow{\sigma} \overline{RG} \xrightarrow{\varphi} \frac{\overline{RG}}{RG} \longrightarrow 0 \tag{2.2}$$

uma seqüência exata curta de RG-módulos (à esquerda).

A partir da seqüência (2.2), temos induzida a seguinte seqüência exata longa em cohomologia:

$$0 \to H^0(G, RG) \to H^0(G, \overline{RG}) \to H^0\left(G, \frac{\overline{RG}}{RG}\right) \to H^1(G, RG) \to \cdots \tag{2.3}$$

Temos por Shapiro, que $H^0\big(G, \overline{RG}\big) = H^0\big(G, Coind_{\{1\}}^G R\big) \simeq H^0(\{1\}, R) \simeq R$ e $H^1\big(G, \overline{RG}\big) \simeq H^1\big(\{1\}, R\big) = 0$.

Além disso, $H^0(G, RG) \simeq [RG]^G = 0$ (Exemplo 1.1.1 *(2b)* e *(2c)*).

Desta maneira, temos que a seqüência (2.3), se reduz a

$$0 \longrightarrow R \longrightarrow H^0\left(G, \frac{\overline{RG}}{RG}\right) \longrightarrow H^1(G, RG) \longrightarrow 0 \longrightarrow \cdots$$

Quando $R = \mathbb{Z}_2$, temos uma seqüência exata de espaços vetoriais e portanto

$$e(G) = dim_{\mathbb{Z}_2} H^0\left(G, \frac{\overline{\mathbb{Z}_2 G}}{\mathbb{Z}_2 G}\right) = 1 + dim_{\mathbb{Z}_2} H^1(G, \mathbb{Z}_2 G).$$

Agora, considerando $R = \mathbb{Z}$ e G finitamente gerado, temos que $H^0\left(G, \dfrac{\overline{\mathbb{Z}G}}{\mathbb{Z}G}\right)$ e $H^1(G, \mathbb{Z}G)$ são grupos abelianos livres (ou $\mathbb{Z}$-módulos livres) ([27], Lema 3.6 e Corolário 3.7). Assim, a seqüência exata curta inicial cinde ([16], I.Teorema 6.3 ou Proposição A.4.3) e daí

$$\begin{aligned} e(G) &= rank_{\mathbb{Z}} H^0\left(G, \frac{\overline{\mathbb{Z}G}}{\mathbb{Z}G}\right) = 1 + rank_{\mathbb{Z}} H^1(G, \mathbb{Z}G) \\ &= 1 + rank_{\mathbb{Z}}\left(\frac{Der(G, \mathbb{Z}G)}{P(G, \mathbb{Z}G)}\right). \end{aligned}$$

■

Corolário 2.2.1. Seja G um grupo infinito (finitamente gerado). Então, $e(G) = 1$ se, e somente se, $H^1(G, RG)$ é trivial ($R = \mathbb{Z}$ ou $\mathbb{Z}_2$).

Observação 2.2.2.

(1) Pode-se provar mais geralmente que: se G é um grupo infinito, finitamente gerado, e R um domínio de ideais principais, então $H^1(G, RG)$ é um R-módulo livre e $e(G) = 1 + rank_R H^1(G, RG)$, onde " $rank_R$" indica o *rank* como um R-módulo livre ([9], Proposições 4.5.1 e 4.5.3).

(2) $H^1(G, \mathbb{Z}G)$ pode não ser livre ($\mathbb{Z}$-módulo livre) se G não é finitamente gerado ([9], Exercício após Teorema 4.5.20, p. 289).

A Proposição 2.2.1 nos fornece uma outra maneira de obter que $e(G) = 2$ quando $G \simeq \mathbb{Z}$.

Corolário 2.2.2. Se $G = \langle t \rangle \simeq \mathbb{Z}$, então $e(G) = 2$.

Demonstração.

Sendo G um grupo infinito, temos pela Proposição 2.2.1 que

$$e(G) = 1 + dim_{\mathbb{Z}_2}\left(\frac{Der(G, \mathbb{Z}_2G)}{P(G, \mathbb{Z}_2G)}\right).$$

Vimos, no Exemplo 1.2.1, que $\dfrac{Der(G, \mathbb{Z}_2G)}{P(G, \mathbb{Z}_2G)} \simeq \mathbb{Z}_2$.

Assim, $dim_{\mathbb{Z}_2}\left(\dfrac{Der(G, \mathbb{Z}_2G)}{P(G, \mathbb{Z}_2G)}\right) = 1$.

Portanto, $e(G) = 1 + 1 = 2$. ■

Proposição 2.2.2. Seja H um subgrupo de G, com $[G : H] < \infty$. Então, $e(G) = e(H)$.

Demonstração.

Se G for um grupo finito, então H também é finito. Logo, pela Proposição 2.1.2 *(b)*, temos que $e(G) = e(H) = 0$.

Agora, provemos que $e(G) = e(H)$ no caso em que G é um grupo infinito.

Temos pela proposição anterior que $e(G) = 1 + dim_{\mathbb{Z}_2} H^1(G, \mathbb{Z}_2 G)$. Como $[G : H] < \infty$ e G é infinito, segue que H é infinito. Assim, $e(H) = 1 + dim_{\mathbb{Z}_2} H^1(H, \mathbb{Z}_2 H)$.

Pelo Corolário 1.6.1, temos que $H^*(H, \mathbb{Z}_2 H) \simeq H^*(G, \mathbb{Z}_2 G)$.

Portanto,

$$e(G) = 1 + dim_{\mathbb{Z}_2} H^1(G, \mathbb{Z}_2 G) = 1 + dim_{\mathbb{Z}_2} H^1(H, \mathbb{Z}_2 H) = e(H). \qquad \blacksquare$$

Corolário 2.2.3. Dado um grupo infinito G, se existe H subgrupo de G tal que $H \simeq \mathbb{Z}$ e $[G : H] < \infty$, então $e(G) = 2$.

Demonstração. Segue da proposição anterior e do Corolário 2.2.2. $\blacksquare$

Observação 2.2.3.

(1) O corolário anterior nos dá uma condição suficiente para que $e(G)$ seja igual a dois. De fato esta condição, quando G é finitamente gerado, é também necessária. Grupos finitamente gerados com dois ends são completamente caracterizados ([23], Teorema 5.12).

(2) Para todo grupo G, pode-se provar que $e(G) = 0, 1, 2$ ou ∞.

Para o caso G finitamente gerado ver, por exemplo [23] (Corolário 5.9), [9] (Teorema 4.5.6) ou [5] (Proposição 3.4.20) (ainda, quando G é finitamente gerado e $e(G)$ é infinito, tem-se $e(G) = \aleph_0$ ([6], Proposição 2.16 (iii))). O caso geral, isto é, quando G é um grupo qualquer (não finito), decorre dos seguintes fatos:

(2a) Se G não é localmente finito*, então $e(G) = 1, 2$ ou ∞ ([6], Teorema 2.11).

(2b) Se G é localmente finito e enumerável, então $e(G) = \infty$ $\big($[6], Exemplo 3$\big)$.

(2c) Se G é não enumerável, então $e(G) = 1$ ou ∞ $\big($[10] ou [5], Proposição 3.1.5$\big)$.

(* Um grupo G é ***localmente finito*** se todo subgrupo finitamente gerado de G é finito $\big($[19], 14.2$\big)$. Necessariamente um grupo infinito e localmente finito não é finitamente gerado).

2.3 Ends de Pares de Grupos

Denominamos ***par grupo***, a um par do tipo $\boldsymbol{(G, H)}$, onde G denota um grupo e H um subgrupo de G. Embora, em geral o conjunto quociente $G/H = \{gH \mid g \in G\}$ não seja um grupo podemos considerar, como feito na seção anterior (para um grupo G), os seguintes $\mathbb{Z}_2G$-módulos (à esquerda):

- $\mathcal{P}(G/H) = \{A \mid A \subseteq G/H\}$,
- $\mathcal{F}(G/H) = \{A \in \mathcal{P}(G/H) \mid A \text{ é finito}\}$,
- $\mathcal{Q}(G/H) = \{A \in \mathcal{P}(G/H) \mid \forall\, g \in G,\ A + gA \in \mathcal{F}(G/H)\}$ e
- o $\mathbb{Z}_2G$-módulo quociente $\dfrac{\mathcal{Q}(G/H)}{\mathcal{F}(G/H)}$.

Propriedade 2.3.1.

(1) $G/H \in \mathcal{Q}(G/H)$, pois $G/H + g(G/H) = \varnothing$.

(2) Dados $A, B \in \mathcal{Q}(G/H)$, temos:

$$\begin{aligned} \overline{A} = \overline{B} \text{ em } \frac{\mathcal{Q}(G/H)}{\mathcal{F}(G/H)} &\Leftrightarrow A + \mathcal{F}(G/H) = B + \mathcal{F}(G/H) \\ &\Leftrightarrow A + B = A + (-B) \in \mathcal{F}(G/H) \\ &\Leftrightarrow A \overset{a}{=} B. \end{aligned}$$

(3) Se A é um elemento de $\mathcal{Q}(G/H)$, então A^c também pertence a $\mathcal{Q}(G/H)$, pois

$$A^c + gA^c = A + gA \in \mathcal{F}(G/H).$$

(4) Se $A \in \mathcal{Q}(G/H)$ e $[G : H]$ é infinito, então $\overline{A}$ e $\overline{A^c}$ são elementos de $\dfrac{\mathcal{Q}(G/H)}{\mathcal{F}(G/H)}$ distintos, pois $A + A^c = G/H \notin \mathcal{F}(G/H)$.

Definição 2.3.1.

(a) O ***número de ends de um par grupo*** (G, H), denotado por $\boldsymbol{e(G, H)}$ é definido por

$$e(G, H) := dim_{\mathbb{Z}_2}\left(\frac{\mathcal{Q}(G/H)}{\mathcal{F}(G/H)}\right).$$

(b) Considerando $H\backslash G = \{Hg \mid g \in G\}$, o conjunto de classes laterais *à direita* de H em G, e os $\mathbb{Z}_2G$-módulos *à direita* $\mathcal{P}(H\backslash G)$, $\mathcal{F}(H\backslash G)$ e $\mathcal{Q}(H\backslash G) := \{B \in \mathcal{P}(H\backslash G) \mid \forall\ g \in G,\ B + Bg \in \mathcal{F}(H\backslash G)\}$, podemos definir de modo similar, o ***número de ends do par grupo*** (G, H) por

$$e(G, H) := dim_{\mathbb{Z}_2}\left(\frac{\mathcal{Q}(H\backslash G)}{\mathcal{F}(H\backslash G)}\right).$$

Claramente essas duas definições coincidem, pois

$$B = \{g_\lambda H \mid \lambda \in J\} \in \mathcal{Q}(G/H) \Leftrightarrow B^{-1} := \{Hg_\lambda^{-1} \mid \lambda \in J\} \in \mathcal{Q}(H\backslash G).$$

Por comodidade trabalhamos com a primeira definição (dada pelas classes à esquerda). Enfatizamos, entretanto, que resultados similares aos apresentados a seguir, são válidos se consideramos classes laterais à direita. A Definição 2.3.1 *(b)* será usada no próximo capítulo, pois como já observamos, Kropholler-Roller em [15] trabalham com classes à direita.

Exemplo 2.3.1. Temos que $e(G, \{1\}) = e(G)$ para qualquer grupo G.

Como para $e(G)$ (Lema 2.2.1), temos também uma fórmula cohomológica 0-dimensional para o end de um par grupo (G, H).

Lema 2.3.1. Seja (G, H) um par grupo. Então,

$$e(G,H) = dim_{\mathbb{Z}_2} H^0\left(G, \frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)}\right).$$

Demonstração.

Notemos que $\left(\frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)}\right)^G = \left(\frac{\mathcal{Q}(G/H)}{\mathcal{F}(G/H)}\right)$.

De fato,

$$\begin{aligned}
\left(\frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)}\right)^G &= \left\{\overline{A} \in \frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)} \mid g.\overline{A} = \overline{A},\ \forall\, g \in G\right\} \\
&= \left\{\overline{A} \in \frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)} \mid \overline{g.A} = \overline{A},\ \forall\, g \in G\right\} \\
&= \left\{\overline{A} \in \frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)} \mid g.A + \mathcal{F}(G/H) = A + \mathcal{F}(G/H),\ \forall\, g \in G\right\} \\
&= \left\{\overline{A} \in \frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)} \mid A + g.A \in \mathcal{F}(G/H),\ \forall\, g \in G\right\} \\
&= \frac{\mathcal{Q}(G/H)}{\mathcal{F}(G/H)}.
\end{aligned}$$

Logo,

$$\begin{aligned}
e(G,H) &= dim_{\mathbb{Z}_2}\left(\frac{\mathcal{Q}(G/H)}{\mathcal{F}(G/H)}\right) = dim_{\mathbb{Z}_2}\left(\frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)}\right)^G \\
&= dim_{\mathbb{Z}_2} H^0\left(G, \frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)}\right).
\end{aligned}$$

■

Proposição 2.3.1. Se (G, H) e (G', H') são pares isomorfos, isto é, existe $\mu : G \longrightarrow G'$ isomorfismo, com $\mu(H) = H'$, então $e(G, H) = e(G', H')$, ou seja, $e(G, H)$ é um invariante algébrico.

Proposição 2.3.2. Sejam G um grupo e H um subgrupo normal de G, isto é, $H \lhd G$, então $e(G, H) = e(G/H)$.

Demonstração.

Sendo H um subgrupo normal de G, temos que G/H $(= H\backslash G)$ é um grupo. Assim, faz sentido calcular o grupo de invariantes de $\frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)}$ sobre G/H.

Logo,

$$\begin{aligned}\left(\frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)}\right)^{G/H} &= \left\{\overline{A} \in \frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)} \mid gH.\overline{A} = \overline{A},\ \forall\, gH \in G/H\right\} \\ &= \left\{\overline{A} \in \frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)} \mid \overline{gHA} = \overline{A},\ \forall\, gH \in G/H\right\} \\ &= \left\{\overline{A} \in \frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)} \mid \overline{gA} = \overline{A},\ \forall\, g \in G\right\} \\ &= \left(\frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)}\right)^{G}.\end{aligned}$$

Daí, pelo Lema 2.3.1 temos

$$e(G,H) = dim_{\mathbb{Z}_2}\left[\left(\frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)}\right)^{G}\right] = dim_{\mathbb{Z}_2}\left[\left(\frac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)}\right)^{G/H}\right] = e(G/H). \blacksquare$$

Corolário 2.3.1. Sejam G um grupo e H um subgrupo normal e finito de G. Então, $e(G,H) = e(G)$.

Demonstração.

Notemos que, pelo Teorema 2.1.2 temos que $e(G) = e(G/H)$. Assim, usando a proposição anterior, segue que $e(G,H) = e(G/H) = e(G)$. $\blacksquare$

Exemplo 2.3.2.

(1) $e(\mathbb{Z} \oplus \mathbb{Z}, \mathbb{Z}) = e(\mathbb{Z}) = 2$.

(2) $e(\mathbb{Z} \oplus \mathbb{Z}_2, \mathbb{Z}_2) = e(\mathbb{Z}) = 2$.

(3) $e(\mathbb{Z}_2 \oplus \mathbb{Z}_2, \mathbb{Z}_2) = 0$.

Podemos mostrar que os $\mathbb{Z}_2G$-módulos

$$\mathcal{P}(G/H) \ \text{ e } \ \overline{\mathbb{Z}_2(G/H)} := Hom_{\mathbb{Z}_2H}\big(\mathbb{Z}_2G, \mathbb{Z}_2\big) \simeq Hom_{\mathbb{Z}_2}\big(\mathbb{Z}_2(G/H), \mathbb{Z}_2\big)$$

são $\mathbb{Z}_2G$-isomorfos e ainda que $\mathbb{Z}_2(G/H)$, o $\mathbb{Z}_2$-módulo livre com base G/H, visto como um $\mathbb{Z}_2G$-submódulo de $\overline{\mathbb{Z}_2(G/H)}$, é isomorfo a $\mathcal{F}(G/H)$. Assim temos o seguinte resultado:

Lema 2.3.2. Sejam (G, H) um par grupo e $\overline{\mathbb{Z}_2(G/H)} = Hom_{\mathbb{Z}_2 H}(\mathbb{Z}_2 G, \mathbb{Z}_2) = Coind_H^G \mathbb{Z}_2$. Então, $\dfrac{\mathcal{P}(G/H)}{\mathcal{F}(G/H)}$ e $\dfrac{\overline{\mathbb{Z}_2(G/H)}}{\mathbb{Z}_2(G/H)}$ são $\mathbb{Z}_2 G$-isomorfos e assim

$$e(G, H) = dim_{\mathbb{Z}_2} H^0 \left(G, \frac{\overline{\mathbb{Z}_2(G/H)}}{\mathbb{Z}_2(G/H)} \right).$$

Demonstração. Similar à demonstração do Lema 2.2.3. ■

Lema 2.3.3. Sejam G um grupo e H um subgrupo de G. Temos:

(a) $e(G, H) = 0$ se, e somente se, H tem índice finito em G, isto é, $[G : H] < \infty$.

(b) Se H' é um subgrupo de índice finito em G que contém H, então $e(H', H) = e(G, H)$.

(c) Se H' é subgrupo normal em G com quociente G', isto é, $\dfrac{G}{H'} = G'$ tal que $[H' : H' \cap H] < \infty$, então $e(G, H) = e(G', \pi(H))$, onde $\pi : G \longrightarrow G'$ é a projeção natural.

Demonstração. [22], Lemas 1.3, 1.4 e 1.5. ■

Observação 2.3.1. Quando G é finitamente gerado, como no caso de $e(G)$, para $e(G, H)$ tem-se que $H^0 \left(G, \dfrac{\overline{\mathbb{Z}(G/H)}}{\mathbb{Z}(G/H)} \right)$ é um *grupo abeliano livre*, onde $\overline{\mathbb{Z}(G/H)} = Hom_{\mathbb{Z}}(\mathbb{Z}(G/H), \mathbb{Z}) \simeq Hom_{\mathbb{Z}H}(\mathbb{Z}G, \mathbb{Z}) = Coind_H^G \mathbb{Z}$ e podemos tomar

$$e(G, H) = rank_{\mathbb{Z}} H^0 \left(G, \frac{\overline{\mathbb{Z}(G/H)}}{\mathbb{Z}(G/H)} \right),$$

como definição de $e(G, H)$. De fato, como mencionado em [28], p. 93, pode-se tomar

$$e(G, H) = rank_R H^0 \left(G, \frac{\overline{R(G/H)}}{R(G/H)} \right)$$

para R domínio de ideais principais. Consideramos aqui $R = \mathbb{Z}$ ou $\mathbb{Z}_2$.

2.4 Interpretação Topológica

Nesta seção, definimos ends de espaços topológicos ou mais precisamente, número de ends de um espaço topológico, e apresentamos algumas das relações existentes entre ends de espaços e ends de grupos (finitamente gerados) e pares de grupos, definidos nas seções anteriores. Não é nosso objetivo nesta seção demonstrar os resultados apresentados, mas sim ilustrar tais relações.

Definição 2.4.1. Seja $\mathcal{X}$ um espaço topológico Hausdorff, com base enumerável, localmente compacto, conexo e localmente conexo. Definimos o ***número de ends de*** $\boldsymbol{\mathcal{X}}$, denotado por $\boldsymbol{e(\mathcal{X})}$, da seguinte maneira

$$e(\mathcal{X}) = sup\ \{n(K) \mid K \text{ é compacto, } K \subseteq \mathcal{X}\},$$

onde $\boldsymbol{n(K)}$ denota o número de componentes conexas de $\mathcal{X} - K$ cujo ***fecho*** é não compacto.

Observação 2.4.1.

(1) Intuitivamente, o número de ends de um espaço topológico $\mathcal{X}$ indica de quantas maneiras $\mathcal{X}$ pode "ir para o infinito".

(2) Uma referência interessante para número de ends de complexos simpliciais (localmente finitos) é [7]. Sugerimos também [5] e [21].

(3) Pode-se provar que:

(3a) Se $\mathcal{X}$ é um espaço topológico Hausdorff, localmente compacto, com base enumerável, conexo, localmente conexo e K um subconjunto compacto de $\mathcal{X}$, então $\mathcal{X} - K$ tem um número finito de componentes conexas (isto é afirmado em [18], §2. O caso em que $\mathcal{X}$ é um CW-complexo é apresentado em [9], Proposição 4.4.3).

(3b) A definição acima é equivalente a seguinte definição (dada em [24], Lema 1.8): Seja $\mathcal{X}$ um espaço topológico Hausdorff, com base enumerável,

localmente compacto, conexo e localmente conexo. O número de ends de $\mathcal{X}$ é definido por

$$e(\mathcal{X}) = sup\ \{n(U) \mid U \subseteq \mathcal{X},\ U \text{ aberto e } \overline{U} \text{ é compacto}\},$$

onde $n(U)$ denota o número de componentes conexas não compactas de $\mathcal{X} - U$ ([21], p. 66).

(3c) O número de ends de um espaço topológico é um invariante topológico, ou seja, se $\mathcal{X}$ e $\mathcal{Y}$ são espaços topológicos homeomorfos, então $e(\mathcal{X}) = e(\mathcal{Y})$.

(4) Pode-se definir "end" de um espaço $\mathcal{X}$ (Hausdorff) ([24], Definição 1.2 ou [18], §2) e assim falar em *conjunto de ends* de $\mathcal{X}$. Quando $\mathcal{X}$ é um espaço Hausdorff, localmente compacto, com base enumerável, conexo e localmente conexo, o *número de elementos desse conjunto* coincide com o *número de ends* $e(\mathcal{X})$ definido anteriormente ([24], Definição 1.2).

Exemplo 2.4.1.

(1) Se $\mathcal{X} = \mathbb{R}$, então $e(\mathbb{R}) = sup\{n(K) \mid K \text{ é compacto, } K \subseteq \mathbb{R}\} = 2$.

Visualizando por exemplo o caso em que o compacto é $K = [0,1] \cup [3,5]$ e analisando $\mathbb{R} - K$ obtemos $n(K) = 2$, visto que o número de componentes conexas de $\mathbb{R} - K$, cujo fecho não é compacto, é 2.

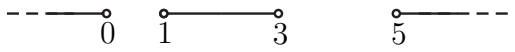


Figura 2.1: $\mathbb{R} - K$.

(2) Se $\mathcal{X} = S^1 = \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$, então $e(S^1) = 0$.

Ilustrando uma situação particular:

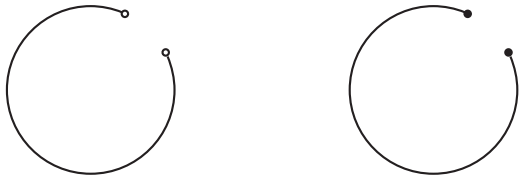


Figura 2.2: $S^1 - K$ e $\overline{S^1 - K}$, respectivamente.

(3) Se $\mathcal{X} = S^2 = \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$, então $e(S^2) = 0$. Observemos a figura abaixo, onde K é um círculo ($K \equiv S^1$):

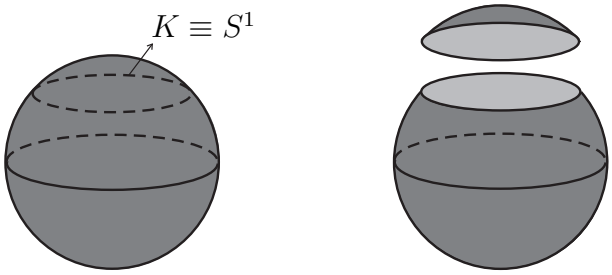


Figura 2.3: $S^2 - K$ e o fecho das duas componentes conexas de $S^2 - K$, respectivamente.

(4) Se $\mathcal{X} = T^2 \simeq S^1 \times S^1$ (Toro), então $e(T^2) = 0$.

Figura 2.4: $T^2 - K$ e $\overline{T^2 - K}$, respectivamente.

Para obter a relação entre (número) de ends de grupos e espaços, precisamos do conceito de Grafo de Cayley.

Definição 2.4.2. Sejam G um grupo e V um conjunto de geradores de G. O ***grafo de Cayley de G*** (associado a V) é um grafo (ou seja, um CW-complexo 1-dimensional) com conjunto de vértices G e 1-células (arestas) orientadas (u, vu) ligando u a vu, com $u \in G$ e $v \in V$ (multiplicação à direita por elementos do conjunto de geradores V de G).

Notação 2.4.1. $\boldsymbol{\Gamma(G,V)}$, $\boldsymbol{\Gamma_V}$ ou simplesmente $\boldsymbol{\Gamma}$.

Proposição 2.4.1. Se G é um grupo finitamente gerado, com conjunto finito V de geradores, então $e(G) = e(\Gamma_V)$.

Demonstração. [22], Lema 1.1 (i) ou [5], Proposição 3.4.17. ■

Exemplo 2.4.2.

(1) $G = \langle a \rangle \simeq \mathbb{Z}$ e $V = \{a\}$. Notemos que as arestas de Γ_V são da seguinte forma: (a^k, a^{k+1}), com $k \in \mathbb{Z}$.

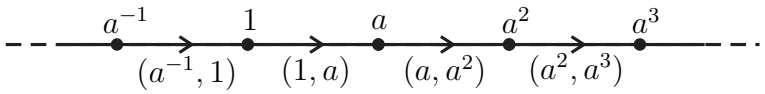


Figura 2.5: representação do grafo de Cayley Γ_V.

Observemos que Γ_V é homeomorfo à $\mathbb{R}$. Logo, pelo teorema anterior, temos que

$$e(G) = e(\Gamma_V) = e(\mathbb{R}) = 2.$$

(2) $G = \langle a \mid a^2 = 1 \rangle \simeq \mathbb{Z}_2$ e $V = \{a\}$.

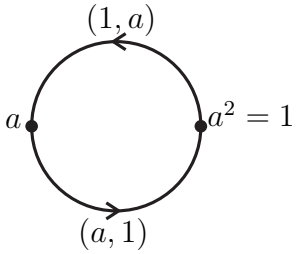


Figura 2.6: representação do grafo de Cayley Γ_V.

Assim,

$$e(G) = e(\Gamma_V) = e(S^1) = 0.$$

(3) $G = \langle a, b \mid ab = ba \rangle \simeq \mathbb{Z} \oplus \mathbb{Z}$ e $V = \{a, b\}$. As arestas de Γ_V são dadas por (u, au) e (u, bu), com $u \in G$.

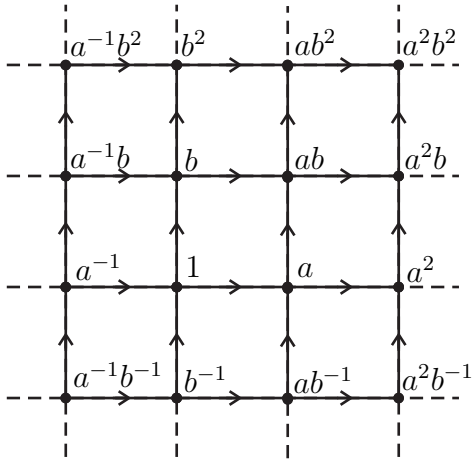


Figura 2.7: representação do grafo de Cayley Γ_V.

Temos que $e(\Gamma_V) = 1$ e portanto, pelo teorema anterior, $e(G) = 1$.

(4) $G = \langle a, b \mid a^2 = b^2 = 1\rangle = \{\ldots, aba, ba, a, 1, b, ab, bab, \ldots\} \simeq \mathbb{Z}_2 * \mathbb{Z}_2$ (produto livre) e $V = \{a, b\}$. As arestas de Γ_V são da forma (u, au) e (u, bu) com $u \in G$. Por exemplo, para $u = ba$, temos as seguintes arestas: (ba, aba) e (ba, a).

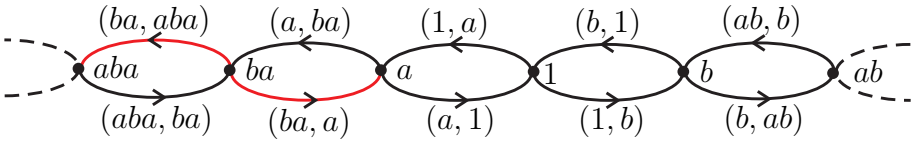


Figura 2.8: representação do grafo de Cayley Γ_V.

Logo, de maneira intuitiva, temos que $e(\Gamma_V) = 2$ e portanto, $e(G) = 2$.

(5) $G = \langle a, b \mid ab = ba,\ b^2 = 1\rangle = \{1, b, a^m, ba^n \mid m, n \in \mathbb{Z}\} \simeq \mathbb{Z} \oplus \mathbb{Z}_2$ e $V = \{a, b\}$.

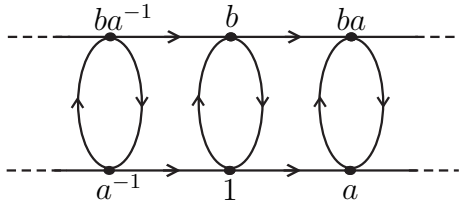


Figura 2.9: representação do grafo de Cayley Γ_V.

Logo, $e(G) = e(\Gamma_V) = 2$.

(6) $G = \langle a \rangle * \langle b \rangle = \{a^{n_1}b^{m_1} \dots a^{n_k}b^{m_k} \mid n_1, m_1, \dots, n_k, m_k \in \mathbb{Z}\} \simeq \mathbb{Z} * \mathbb{Z}$ (produto livre) e $V = \{a, b\}$.

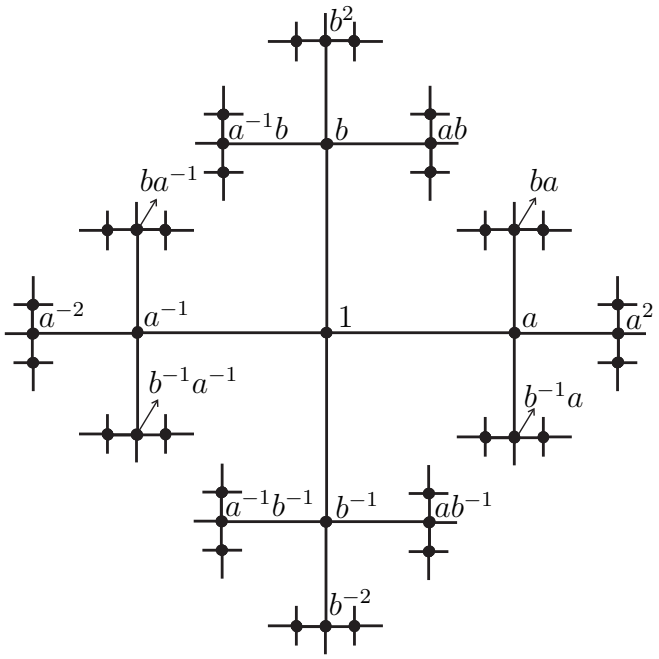


Figura 2.10: representação do grafo de Cayley Γ_V.

Então, $e(G) = e(\Gamma_V) = \infty$.

Vejamos agora, uma relação entre o número de ends de um par grupo (G, H) com o número de ends de um espaço topológico. Para isto:

Proposição 2.4.2. Sejam G um grupo finitamente gerado, H um subgrupo de G e Γ_V o grafo de Cayley associado a V, com V um conjunto finito de geradores de G. Se Γ/H denota o quociente de Γ_V pela ação (à direita) de H induzida da ação de H em G, então $e(G, H) = e(\Gamma/H)$.

Demonstração. [22], Lema 1.1 (ii) ou [5], Proposição 4.1.1.5. ■

Exemplo 2.4.3.

(1) $G = \langle a, b \mid a^2 = b^2 = 1\rangle \simeq \mathbb{Z}_2 * \mathbb{Z}_2$, $H = \langle a \rangle = \{1, a\}$ e $V = \{a, b\}$. Vejamos inicialmente a representação de Γ_V, já apresentada anteriormente

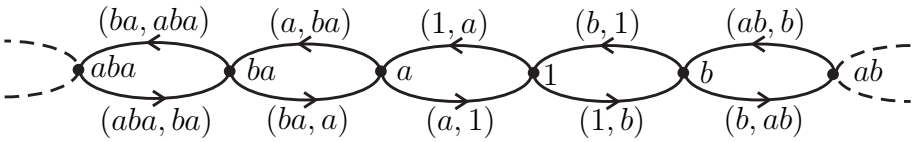


Figura 2.11: representação do grafo de Cayley Γ_V.

Temos as seguintes H-órbitas em Γ_V:

$H(a) = \{ah \mid h \in H\} = \{a, 1\}$,

$H(b) = \{bh \mid h \in H\} = \{b, ba\}$,

$H(ab) = \{(ab)h \mid h \in H\} = \{ab, aba\}$,

$\vdots$

$H((1, a)) = \{(1, a)h \mid h \in H\} = \{(1, a), (a, 1)\}$,

$H((b, 1)) = \{(b, 1)h \mid h \in H\} = \{(b, 1), (ba, a)\}$,

$H((1, b)) = \{(1, b)h \mid h \in H\} = \{(1, b), (a, ba)\}$,

$\vdots$

Considerando as órbitas dos vértices e das arestas, temos a seguinte representação para Γ/H:

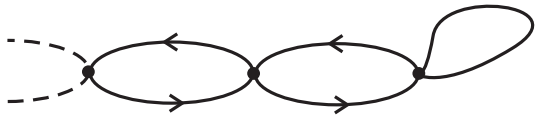


Figura 2.12: representação do quociente Γ/H.

Portanto, pelo teorema anterior, vem que

$$e(G, H) = e(\Gamma/H) = 1.$$

(2) $G = \langle a, b \mid ab = ba \rangle$, $H = \langle a \rangle$ e $V = \{a, b\}$.

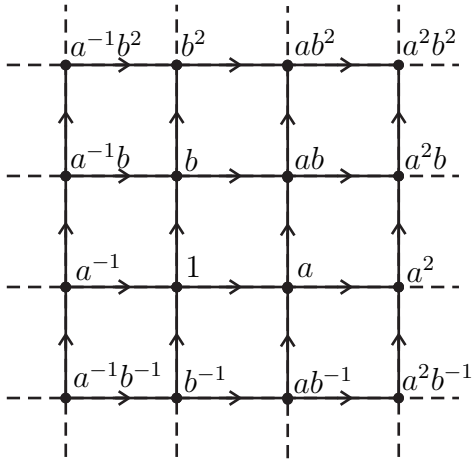


Figura 2.13: representação do grafo de Cayley Γ_V.

Vejamos as H-órbitas de Γ_V:

$$
\begin{aligned}
H(b^n) &= \{b^n h \mid h \in H\} = \{b^n a^m \mid n, m \in \mathbb{Z}\} = \{a^m b^n \mid m, n \in \mathbb{Z}\},\\
H((b^n, b^{n+1})) &= \{(b^n, b^{n+1}).h \mid h \in H,\ n \in \mathbb{Z}\}\\
&= \{(a^m b^n, a^m b^{n+1}) \mid n, m \in \mathbb{Z}\},\\
H((a^n, a^{n+1})) &= \{(a^n, a^{n+1}).h \mid h \in H,\ n \in \mathbb{Z}\}\\
&= \{(a^{(n+m)} b^{(n+m)+1}, a^m b^{n+1}) \mid n, m \in \mathbb{Z}\},\\
H((b, ab)) &= \{(b, ab).h \mid h \in H\} = \{(a^n b, a^{n+1} b) \mid n \in \mathbb{Z}\},\\
&\vdots
\end{aligned}
$$

Assim, temos a seguinte representação para o quociente Γ/H:

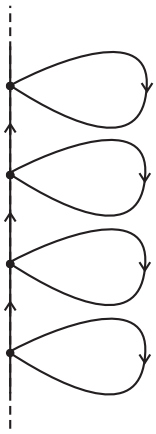


Figura 2.14: quociente Γ/H.

Portanto, $e(G, H) = e(\Gamma/H) = 2$.

Os resultados apresentados nas Proposições 2.4.1 e 2.4.2, podem ser estendidos como segue:

Proposição 2.4.3. Seja X um CW-complexo finito com um espaço de recobrimento $\widetilde{X}$, cujo grupo das transformações de recobrimento é G. Então,

(a) $e(\widetilde{X}) = e(G)$.

(b) $e(\widetilde{X}/H) = e(G, H)$, onde H é um subgrupo de G e $\widetilde{X}/H$ denota o quociente de $\widetilde{X}$ pela ação de H.

Demonstração. [22], Lema 1.2. ■

Podemos ainda dar a $e(G, H)$, uma interpretação topológica no caso em que G é o grupo fundamental de uma superfície fechada.

Como conseqüência, obtemos exemplos de pares (G, H), com G finitamente gerado e $e(G, H) \neq 0, 1, 2$ ou ∞ (Exemplo 2.4.4 *(2)*, a seguir).

Definição 2.4.3.

(a) Sejam S uma superfície e C uma circunferência mergulhada em S. Dizemos que ***C é incompressível em S*** se a aplicação natural $\Pi_1(C) \longrightarrow \Pi_1(S)$ é injetora (onde Π_1 indica o grupo fundamental).

(b) Seja Y uma sub-superfície compacta de S. Dizemos que Y é ***incompressível em*** S, se toda componente de bordo de Y é incompressível em S.

Proposição 2.4.4. Sejam G o grupo fundamental de uma superfície fechada S e H o grupo fundamental de uma sub-superfície Y de S, compacta e incompressível (em S). Então, $e(G, H)$ é igual ao número de componentes de bordo de Y.

Demonstração. [22], Lema 2.2. ■

Exemplo 2.4.4.

(1) Sejam $S = T^2$ (toro) e Y uma sub-superfície compacta como na figura:

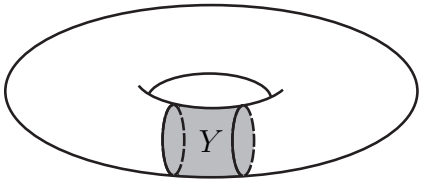


Figura 2.15: toro T^2 e a sub-superfície Y.

Então, Y é incompressível, $\Pi_1(T^2) = \mathbb{Z} \oplus \mathbb{Z}$ e $\Pi_1(Y) = \mathbb{Z}$.

Portanto, $e(\mathbb{Z} \oplus \mathbb{Z}, \mathbb{Z}) = 2$.

(2) Consideremos $S = T^2 \# T^2 \# T^2$ (soma conexa de três toros), G o grupo fundamental de S e H o grupo fundamental da sub-superfície incompressível Y de S como na figura:

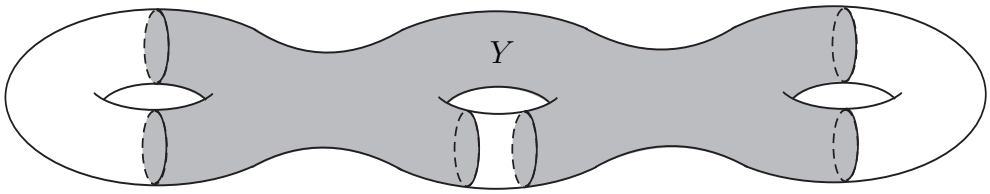


Figura 2.16: $T^2 \# T^2 \# T^2$ e a sub-superfície incompressível Y.

Então, $e(G, H) = 6$.

Capítulo 3

Uma Fórmula Cohomológica 1-dimensional para $e(G, H)$: Teorema de Swarup

Para ends de grupos mostramos (Proposição 2.2.1) que, quando G é infinito, finitamente gerado ($R = \mathbb{Z}$ ou $\mathbb{Z}_2$), uma fórmula cohomológica 1-dimensional é válida:

$$e(G) = 1 + rank_R H^1(G, RG).$$

Se H é um subgrupo de um grupo finitamente gerado G de índice infinito, Swarup em [28], mostrou que para o end do par $e(G, H)$, uma fórmula cohomológica similar ocorre para certos tipos especiais de pares de grupos (G, H). Para a prova Swarup usou argumentos geométricos. Posteriormente, uma demonstração algébrica desse resultado foi apresentada por Kropholler e Roller [15].

Nosso principal objetivo neste capítulo é apresentar, de forma detalhada, a prova (algébrica) do Teorema de Swarup (Teorema 3.3.1).

Por todo este capítulo, G denota um grupo finitamente gerado e H um subgrupo de índice infinito em G, e portanto $e(G, H) \geqslant 1$.

É interessante observar que Swarup ([28]) trabalhou com o $\mathbb{Z}G$-módulo

à esquerda $\mathbb{Z}(G/H)$, onde $\mathbb{Z}(G/H)$ é o $\mathbb{Z}$-módulo livre gerado pelas classes laterais gH, $g \in G$ e a G-ação natural é dada por $g_0.(gH) = g_0gH$. Kropholler e Roller em [15] usaram o $\mathbb{Z}G$-módulo (natural) à direita $\mathbb{Z}(H\backslash G)$ dado pelas classes laterais à direita $\{Hg \mid g \in G\}$. No entanto, isto não causa nenhuma contradição (ver Lema 1.4.1).

3.1 Subconjuntos H-Quase Invariantes

Definição 3.1.1. Um subconjunto E de G é denominado ***H-finito*** (à direita), se E está contido em uma união finita de classes laterais à direita de H em G, isto é, existem $g_1, \ldots, g_k \in G$ tais que $E \subseteq Hg_1 \cup \ldots \cup Hg_k = H.\{g_1, \ldots, g_k\}$, ou ainda, $E \subseteq H.F$, para algum subconjunto finito $F \subseteq G$.

Definição 3.1.2. Dizemos que $E \subseteq G$ é ***H-quase invariante*** (à direita) se, e somente se, $E + Ex$ é H-finito, para todo $x \in G$ (isto é, $E + Ex \subseteq HF_x$, com F_x um subconjunto finito de G), onde $E + Ex$ indica a operação diferença simétrica entre os conjuntos E e Ex.

Observação 3.1.1.

(1) Se $E \subseteq G$ é quase invariante (à direita), então E é H-quase invariante, pois $E + Ex = F_x$ (finito) implica $E + Ex \subseteq H.F_x$.

(2) Se $B \in \mathcal{F}(H\backslash G)$, isto é, $B = \{Hg_1, \ldots, Hg_n\}$, então $E_B := Hg_1 \cup \ldots \cup Hg_n$ é claramente H-finito.

Proposição 3.1.1. Os ends do par (G, H) correspondem aos subconjuntos H-quase invariantes E de G que satisfazem $E = HE$ e que não são H-finitos, mais precisamente existe uma correspondência biunívoca entre $\left(\frac{\mathcal{Q}(H\backslash G)}{\mathcal{F}(H\backslash G)}\right)^* = \frac{\mathcal{Q}(H\backslash G)}{\mathcal{F}(H\backslash G)} - \{\overline{\varnothing}\}$ e $\mathcal{H} = \{E \subseteq G \mid E$ é H-quase invariante, $E = HE$ e E não é H-finito$\}$.

Demonstração.

Sabemos (Definição 2.3.1 *(b)*) que $e(G,H)$ pode ser definido por $e(G,H) = dim_{\mathbb{Z}_2}\left(\dfrac{\mathcal{Q}(H\backslash G)}{\mathcal{F}(H\backslash G)}\right)$, onde $\mathcal{Q}(H\backslash G) = \{B \in \mathcal{P}(H\backslash G) \mid B+Bg \in \mathcal{F}(H\backslash G),\ \forall g \in G\}$.

(1) A cada $\overline{B} = B + \mathcal{F}(H\backslash G) \in \left(\dfrac{\mathcal{Q}(H\backslash G)}{\mathcal{F}(H\backslash G)}\right)^*$, com $B = \{Hg_\mu \mid \mu \in J\}$, façamos corresponder o elemento $\alpha(\overline{B}) = E_B := \bigcup_{\mu\in J} Hg_\mu$, que vamos denotar simplesmente por E.

Afirmamos que $\alpha(\overline{B}) = E \in \mathcal{H}$, isto é,

(1a) $H.E = E$.

- $E \subseteq H.E$, pois o elemento neutro $1 \in H$.
- $HE \subseteq E$, pois $y \in HE$ implica que $y = h(h_1g_\mu) = (hh_1)g_\mu \in Hg_\mu$. Daí, $y = h_0g_\mu \in E$.

(1b) Dado $x \in G$, mostremos que $E = \bigcup_{\mu\in J} Hg_\mu$ é H-quase invariante. Temos que $B + Bx = \{Hg_\mu \mid \mu \in J\} + \{Hg_\mu x \mid \mu \in J\}$ e $B + Bx \in \mathcal{F}(H\backslash G)$ $\big($pois, $B \in \mathcal{Q}(H\backslash G)\big)$, ou seja $(B \cup Bx) - (B \cap Bx) = \{Hg_{\mu_1}, \ldots, Hg_{\mu_k}\}$.

Agora, $Ex = \bigcup_{\mu\in J} Hg_\mu x$ e visto que $Hg_\mu x \cap Hg_{\mu'} \neq \varnothing$ se, e somente se, $Hg_\mu x = Hg_{\mu'}$, obtemos que

$$E + Ex = \left[\left(\bigcup_{\mu\in J} Hg_\mu x\right) \bigcup \left(\bigcup_{\mu\in J} Hg_\mu\right)\right] - \left[\left(\bigcup_{\mu\in J} Hg_\mu x\right) \bigcap \left(\bigcup_{\mu\in J} Hg_\mu\right)\right]$$
$$\subseteq Hg_{\mu_1} \cup \ldots \cup Hg_{\mu_k} = H.F_x\ ,$$

$\big($onde $F_x = \{g_{\mu_1}, \ldots, g_{\mu_k}\}\big)$, isto é, $E + Ex \subseteq H.F_x$, para todo $x \in G$. Assim, $E + Ex$ é H-finito e portanto E é H-quase invariante.

(1c) E não é H-finito.

De fato, suponhamos que $E = \bigcup_{\mu\in J} Hg_\mu$ fosse H-finito, então existiria $F = \{g_1, \ldots, g_k\}$ tal que $E \subseteq H.F = Hg_0 \cup \ldots \cup Hg_k$. Assim, para todo $v \in Hg_{\mu_r}$, com $\mu_r \in J$, temos que $v \in Hg_j$, para algum $j = 0, \ldots, k$.

Logo, $v = h_1 g_{\mu_r} = h_2 g_j$, o que implicaria em $g_j g_{\mu_r}^{-1} = h_2^{-1} h_1$ e daí, $Hg_j = Hg_{\mu_r}$. Desta forma, $B = \{Hg_\mu \mid \mu \in J\} \subseteq \{Hg_0, \ldots, Hg_k\} \in \mathcal{F}(H\backslash G)$, o que é uma contradição, pois $B \notin \mathcal{F}(H\backslash G)$.

Portanto, E não é H-finito.

(2) Agora, dado um elemento qualquer $E \in \mathcal{H}$, considere $\beta(E) = B + \mathcal{F}(H\backslash G)$, onde $B := \{Hv \mid v \in E\}$. Podemos mostrar que $\beta(E) = \overline{B} \in \left(\dfrac{\mathcal{Q}(H\backslash G)}{\mathcal{F}(H\backslash G)}\right)^*$, isto é, $B \in \mathcal{Q}(H\backslash G)$ e $B \notin \mathcal{F}(H\backslash G)$.
Com efeito,

(2a) Temos que $B \notin \mathcal{F}(H\backslash G)$, pois se $B = \{Hv_1, \ldots, Hv_k\} \in \mathcal{F}(H\backslash G)$ teríamos que:

$$\begin{aligned} v \in E &\Rightarrow \exists\, h_0 \in H \text{ e } v_0 \in E \text{ tais que } v = h_0 v_0 \\ &\overset{def.\ B}{\Rightarrow} v \in Hv_0 \in B = \{Hv_1, \ldots, Hv_k\} \\ &\Rightarrow v \in Hv_j, \text{ para algum } j = 1, \ldots, k \\ &\Rightarrow v \in H.\{v_1, \ldots, v_k\} \\ &\Rightarrow E \subseteq H.F, \end{aligned}$$

ou seja, E seria H-finito, o que é um absurdo.

(2b) Provemos que $B \in \mathcal{Q}(H\backslash G)$, isto é, $B + Bx \in \mathcal{F}(H\backslash G)$, para todo $x \in G$.

Seja $x \in G$. Por hipótese $E + Ex \subseteq H.F_x = H.\{g_1, \ldots, g_r\}$ (pois E é H-quase invariante).

Afirmamos que,

$$B + Bx \subseteq \{Hg_1, \ldots, Hg_r\}.$$

Com efeito, para todo $W \in B + Bx$, temos que $W \in (B \cup Bx) - (B \cap Bx)$.

Suponhamos que $W \in B$, então $W = Hv_1$, $v_1 \in E$. Afirmamos que $v_1 \notin Ex$, pois caso contrário, $v_1 = v_2 x$ para algum $v_2 \in E$ e portanto $Hv_1 = Hv_2 x \in B \cap Bx$, o que é um absurdo. Assim, $v_1 \in E$ e $v_1 \notin E \cap Ex$. Logo, $v_1 \in E + Ex \subseteq H.\{g_1, \ldots, g_r\}$ e então existe g_s, $1 \leqslant s \leqslant r$ tal que

$v_1 \in Hg_s$, donde $v_1 = hg_s$, para algum $h \in H$. Daí, $W = Hv_1 = Hhg_s = Hg_s$ e portanto $W \in \{Hg_1, \ldots, Hg_r\}$.

Similarmente, se $W \in B + Bx$ e $W \in Bx$, verifica-se que $W \in \{Hg_1, \ldots, Hg_r\}$.

Assim, $B + Bx \subseteq H.\{g_1, \ldots, g_r\} = H.F$.

Logo, $B + \mathcal{F}(H\backslash G) \in \left(\dfrac{\mathcal{Q}(H\backslash G)}{\mathcal{F}(H\backslash G)}\right)^*$, como desejado.

Além disso, podemos ver que $\alpha \circ \beta = id$ e $\beta \circ \alpha = id$.

Portanto, o resultado segue. ■

Pela suposição inicial do capítulo, G e H são tais que $[G : H] = \infty$. Assim, se N é um subgrupo de H, então também $[G : N] = \infty$ e portanto $e(G, N) \geqslant 1$. O resultado seguinte nos dá uma condição em que esta cota pode ser melhorada (sempre que $[H : N] \geqslant 2$).

Proposição 3.1.2. Sejam E um subconjunto H-quase invariante de G e $N = \{h \in H \mid hE = E\}$. Suponhamos que as seguintes condições sejam válidas:

(a) N é um subgrupo normal de H, isto é, $N \lhd H$,

(b) $hE \cap E = \varnothing$, para todo $h \in H - N = \{h \in H \mid h \notin N\}$ (notemos que, $h \in N \Rightarrow hE \cap E = E = hE$),

(c) $HE = G$.

Então, $e(G, N) \geqslant [H : N]$.

Demonstração.

A demonstração será feita em vários passos.

(1) Mostremos que para todos $x, y \in G$, $Ex \cap Hy$ está contido em uma classe lateral de N, isto é, dados $x, y \in G$, existe $g_{xy} \in G$ (que depende de x e y) tal que $Ex \cap Hy \subseteq Ng_{xy}$. Para isso, inicialmente verifiquemos que para todos $z, z' \in Ex \cap Hy$, tem-se $z'z^{-1} \in H$ e $(z'z^{-1})E \cap E \neq \varnothing$. De

fato, suponhamos dados $z, z' \in Ex \cap Hy$. Então, temos que $z'z^{-1} \in H$, pois $z, z' \in Hy$ implica que existem $h, h' \in H$ tais que $z = hy$ e $z' = h'y$ e desta forma,

$$z'z^{-1} = (h'y)(hy)^{-1} = (h'y)(y^{-1}h^{-1}) = h'(yy^{-1})h^{-1} = h'h^{-1} \in H.$$

Observemos também que $z'x^{-1} \in (z'z^{-1})E \cap E$, pois como $z, z' \in Ex$, existem $u, v \in E$ tais que $z = ux$ e $z' = vx$. Daí,

(1.1) $z = ux \Rightarrow z^{-1} = (ux)^{-1} \Rightarrow z^{-1} = x^{-1}u^{-1} \Rightarrow z'z^{-1} = z'x^{-1}u^{-1}$ $\Rightarrow (z'z^{-1})u = z'x^{-1}u^{-1}u \Rightarrow (z'z^{-1})u = z'x^{-1} \Rightarrow z'x^{-1} = (z'z^{-1})u \in (z'z^{-1})E$.

(1.2) $z' = vx \Rightarrow z'x^{-1} = v \Rightarrow z'x^{-1} \in E$.

Logo, de *(1.1)* e *(1.2)* temos que $z'x^{-1} \in (z'z^{-1})E \cap E$ e assim $(z'z^{-1})E \cap E \neq \varnothing$.

Conseqüentemente, $z'z^{-1} \in N$, pois caso contrário teríamos $z'z^{-1} \in H - N$ e pela hipótese *(b)*, $(z'z^{-1})E \cap E = \varnothing$, o que é um absurdo.

Daí, tomando $z_0 \in Ex \cap Hy$ (z_0 fixo) temos que, para todo $z \in Ex \cap Hy$, $zz_0^{-1} \in N$. Mas, $zz_0^{-1} \in N$ implica que $N(zz_0^{-1}) = N$ e assim $Nz = Nz_0$.

Logo, para todo $z \in Ex \cap Hy$, $z \in Nz = Nz_0$, onde Nz_0 é uma classe lateral fixa. Portanto, $Ex \cap Hy \subseteq Nz_0$, ou seja, $Ex \cap Hy \subseteq Ng_{xy}$ se denotamos z_0 por g_{xy}.

(2) Para todo $x \in G$, $E + Ex$ é N-finito. Por hipótese, para todo $x \in G$, $E + Ex$ é H-finito, pois E é H-quase invariante. Assim, dado $x \in G$, existe $F = \{g_1, \ldots, g_k\} \subseteq G$ tal que

$$E + Ex \subseteq H.F = H.\{g_1, \ldots, g_k\} = Hg_1 \cup \ldots \cup Hg_k.$$

Então,

$$\begin{aligned} E + Ex &= (E + Ex) \cap (Hg_1 \cup \ldots \cup Hg_k) \subseteq (E \cup Ex) \cap (Hg_1 \cup \ldots \cup Hg_k) \\ &= (E \cap Hg_1) \cup \ldots \cup (E \cap Hg_k) \cup (Ex \cap Hg_1) \cup \ldots \cup (Ex \cap Hg_k). \end{aligned}$$

De acordo com o que foi provado anteriormente, temos que $E \cap Hg_i = E.1 \cap Hg_i \subseteq Ng_{1i}$ e $Ex \cap Hg_i \subseteq Ng_{xi}$, onde $g_{1i}, g_{xi} \in G$, $i = 1, \ldots, k$. Logo, $E + Ex \subseteq \left(\bigcup_{i=1}^{k} Ng_{1i}\right) \bigcup \left(\bigcup_{i=1}^{k} Ng_{xi}\right) = Ng_{11} \cup \ldots \cup Ng_{1k} \cup Ng_{x1} \cup \ldots \cup Ng_{xk}$, ou seja, $E + Ex$ é N-finito, para todo $x \in G$, e portanto, E é N-quase invariante.

(3) E não é N-finito. De fato, suponhamos que E seja N-finito, isto é, $E \subseteq Ng_1 \cup \ldots \cup Ng_n$, onde $g_i \in G$, $i = 1, \ldots, n$. Usando o fato de que N é um subgrupo (normal) de H e a hipótese de que $G = HE$, temos

$$G = HE \subseteq H(Ng_1 \cup \ldots \cup Ng_n) \subseteq Hg_1 \cup \ldots \cup Hg_n,$$

de onde concluímos que G é H-finito e conseqüentemente $[G : H] < \infty$. Mas isto contradiz o fato de $[G : H] = \infty$. Portanto, E não é N-finito.

(4) Cada subconjunto $E_h := hE$, com $h \in H$, corresponde a um end do par (G, N).

Para isso mostramos que, para cada h, $E_h = hE$ satisfaz as condições da proposição anterior, isto é, E_h é um subconjunto N-quase invariante de G, que satisfaz $E_h = NE_h$ e que não é N-finito (Proposição 3.1.1).

(4.1) hE é subconjunto N-quase invariante de G, isto é, $(hE) + (hE)x$ é N-finito, para todo $x \in G$. Para isso observemos inicialmente que, $(hE) + (hE)x = h(E + Ex)$. De fato, seja $w \in [(hE) + (hE)x] = [(hE) - (hE)x] \cup [(hE)x - (hE)]$ (note que "$-$" indica a diferença entre conjuntos).

- Se $w \in [(hE) - (hE)x]$, então $w \in hE$ e $w \notin (hE)x$. Assim, $w = hu$, com $u \in E$ e $u \notin Ex$, isto é, $u \in E - Ex$. Logo, $w = hu \in h(E - Ex) \subseteq h(E + Ex)$.
- Se $w \in [(hE)x - (hE)]$, então $w \in (hE)x$ e $w \notin hE$, isto é, $w = (hu)x$, com $u \in E$ e $ux \notin E$. Logo, $w = hux \in h(Ex - E) \subseteq h(E + Ex)$.

Assim, $(hE) + (hE)x \subseteq h(E + Ex)$. Similarmente, verifica-se que $h(E + Ex) \subseteq (hE) + (hE)x$.

Agora, por *(2)*, $E + Ex \subseteq Ng_1 \cup \ldots \cup Ng_j$. Daí, $(hE) + (hE)x = h(E + Ex) \subseteq h(Ng_1 \cup \ldots \cup Ng_j)$.

Como N é normal em H,

$$(hE) + (hE)x \subseteq hNg_1 \cup \ldots \cup hNg_j = Nhg_1 \cup \ldots \cup Nhg_j,$$

onde $hg_i \in G$, $i = 1, \ldots, j$, ou seja, $(hE) + (hE)x$ é N-finito, para todo $x \in G$ e assim, temos que hE é N-quase invariante.

(4.2) $hE = N(hE)$. Claramente $hE \subseteq N(hE)$, pois $1 \in N$. Agora, tomando $y \in N(hE)$ temos, pela normalidade de N em H, que $y \in hNE$. Logo, $y = hnu$, com $n \in N$ e $u \in E$. Mas, $N = \{h \in H \mid hE = E\}$ e como $n \in N$ temos que $nu = v$, com $v \in E$. Então, $y = h(nu) = hv \in hE$ e portanto, $N(hE) \subseteq hE$. Assim, $N(hE) = hE$ como desejado.

(4.3) Falta mostrarmos que hE não é N-finito. Suponhamos que hE é N-finito, isto é, $hE \subseteq Ng_1 \cup \ldots \cup Ng_m$, $g_i \in G$, $i = 1, \ldots, m$. Assim, $E \subseteq h^{-1}(Ng_1 \cup \ldots \cup Ng_m) = h^{-1}Ng_1 \cup \ldots \cup h^{-1}Ng_m$. Novamente, usando a normalidade de N em H vem que

$$E \subseteq N(h^{-1}g_1) \cup \ldots \cup N(h^{-1}g_m), \text{ onde } h^{-1}g_i \in G, i = 1, \ldots, m.$$

De onde concluímos que E é N-finito, o que é uma contradição, pois já provamos em *(3)* que E não é N-finito.

Desta forma, temos que hE, $h \in H$, corresponde a um elemento end do par (G, N).

(5) Para finalizarmos a demonstração da proposição, vejamos que existe uma correspondência bijetiva entre $H/N = \{hN \mid h \in H\}$ $(= N\backslash H$, pois $N \lhd H)$ e $\{hE \mid h \in H\}$, pois dados $h_1, h_2 \in H$,

$$h_1E = h_2E \Leftrightarrow h_2^{-1}h_1E = E \overset{def.\ N}{\Leftrightarrow} h_2^{-1}h_1 \in N \Leftrightarrow h_1N = h_2N.$$

Logo, $\big|\{hE \mid h \in H\}\big| = \big|(H/N)\big| = [H : N]$. Notemos ainda que, se $h_1N \neq h_2N$, então $h_1E \cap h_2E = \varnothing$, pois:

$$h_1e_1 = h_2e_2 \Rightarrow h_2^{-1}h_1e_1 = e_2 \in h_2^{-1}h_1E \cap E \overset{item\,(b)}{\Rightarrow} h_2^{-1}h_1 \in N.$$

Sabemos que cada elemento de $\{hE \mid h \in H\}$ corresponde a um end do par (G, N), mais precisamente (ver demonstração da proposição anterior) aos elementos $\overline{B_h} = B_h + \mathcal{P}(N\backslash G)$, onde $B_h = \{Nhv \mid v \in E\}$ é um subconjunto infinito (isto é, $B_h \notin \mathcal{F}(N\backslash G)$) e $B_h \in \mathcal{Q}(N\backslash G)$.

Ainda, se $\{h_\lambda \mid \lambda \in J\}$ é um conjunto de representantes das classes laterais de N em H, então B_{h_λ}, com $\lambda \in J$, são subconjuntos disjuntos e portanto, considerando o subgrupo gerado por $\overline{B_{h_\lambda}}$, $\lambda \in J$, obtemos (Propriedade 2.1.1 *(5)* e [22], Lema 1.6) que

$$e(G, N) \geqslant [H : N].$$

■

Observação 3.1.2.

(1) Temos que $E = G$ satisfaz as condições da proposição anterior, mas este caso não é interessante, visto que teríamos $H = N$ e portanto $[H : N] = 1$.

(2) Na demonstração da proposição anterior, parte *(1)*, estamos interessados nos casos em que $Ex \cap Hy \neq \varnothing$, pois se $Ex \cap Hy = \varnothing$, então $Ex \cap Hy \subseteq Ng$, para todo $g \in G$.

(3) Podemos afirmar apenas que a desigualdade é válida, pois mostramos que hE dá origem a um elemento end do par (G, N), porém não mostramos que todo elemento end do par (G, N) corresponde a um elemento da forma hE.

3.2 De Derivações para Conjuntos Quase Invariantes

Definição 3.2.1. Dado um grupo A denotamos por $\boldsymbol{C(A)}$ *o conjunto das aplicações de G em A que são constantes sobre as classes laterais à esquerda gH de H em G*, isto é, $C(A) = \{f : G \to A \ ; \ f\big|_{gH} : gH \to A$ é constante, $\forall\, g \in G\}$, e denotamos por $\boldsymbol{I(A)}$ *o subconjunto de $C(A)$, das aplicações que são suportadas sobre um número finito de classes laterais à esquerda*, isto é, $I(A) = \{f \in C(A) \ ; \ f\big|_{gH} = 1,$ exceto em um nº finito de classes laterais $g_iH,\ i = 1, \ldots, n\}$ (onde 1 indica o elemento neutro de A).

Assim, dado $f \in C(A)$ temos que $f \in I(A)$ se, e somente se, $f(g)$ é trivial, exceto para $g \in g_1H \cup \ldots \cup g_nH$.

Nosso objetivo agora é dar **uma estrutura de $\mathbf{Z}G$-módulo (à direita) para $\boldsymbol{C(A)}$ e $\boldsymbol{I(A)}$**.

(1) Como A é um grupo, podemos dar a $C(A)$ uma estrutura de grupo com a multiplicação ponto a ponto, isto é, para todos $f_1, f_2 \in C(A)$, $f_1.f_2 \in C(A)$ é definida por

$$(f_1.f_2)(g) := f_1(g).f_2(g), \quad \text{para todo} \quad g \in G,$$

onde "." indica a operação de A.

Se A for abeliano, então $C(A)$ também será abeliano.

(2) Se $f_1, f_2 \in I(A)$, então $f_1.f_2 \in I(A)$ e podemos verificar que $I(A)$ é um subgrupo de $C(A)$.

(3) $C(A)$ admite uma G-ação (à direita) dada por

$$\begin{aligned} C(A) \times G &\longrightarrow C(A) \\ (f, g) &\longmapsto f * g \overset{not.}{=} f^g \ , \end{aligned}$$

tal que

$$\begin{aligned} f^g : G &\longrightarrow A \\ g_0 &\longmapsto (f*g)(g_0) = f^g(g_0) := f(gg_0)\ , \end{aligned}$$

para todos $f \in C(A)$ e $g, g_0 \in G$.

De fato,

(a) $(f*1)(g_0) = (f^1)(g_0) = f(1g_0) = f(g_0)$.
Como g_0 é um elemento arbitrário de G, temos que $f*1 = f$, para todo $f \in C(A)$.

(b) $[f*(g_1g_2)](g_0) = (f^{g_1g_2})(g_0) = f[(g_1g_2)g_0] = f[g_1(g_2g_0)] = (f^{g_1})(g_2g_0)$
$= (f*g_1)(g_2g_0) = (f*g_1)^{g_2}(g_0) = [(f*g_1)*g_2](g_0)$.
Sendo $g_0 \in G$ arbitrário, temos que $f*(g_1g_2) = (f*g_1)*g_2$, para todos $g_1, g_2 \in G$ e $f \in C(A)$.

Conseqüentemente, temos que $I(A)$ também admite uma G-ação (à direita).

(4) Se A é abeliano, segue de *(1)* e *(3)* que $C(A)$ e $I(A)$ são $\mathbb{Z}G$-módulos (à direita). É no caso em que A é abeliano que estamos interessados. De fato, no Teorema 3.3.1 da seção seguinte, nos restringimos a $A = \mathbb{Z}$.

Recordemos que, considerando A um grupo (abeliano) multiplicativo, uma ***derivação*** de G em $I(A)$ é uma aplicação

$$\begin{aligned} \delta : G &\longrightarrow I(A) \\ g &\longmapsto \delta(g) \overset{not.}{=} \delta g : G \longrightarrow A \end{aligned}$$

satisfazendo $\delta(gg') = \big(\delta(g).g'\big).\big(\delta(g')\big) \overset{not.}{=} (\delta g)^{g'}.(\delta g')$, para todos $g, g' \in G$. Assim, dado $g_0 \in G$,

$$\delta(gg')(g_0) = [(\delta g)^{g'}.(\delta g')](g_0) = (\delta g)^{g'}(g_0).(\delta g')(g_0) = (\delta g)(g'g_0).(\delta g')(g_0),$$

isto é,

$$\delta(gg')(g_0) = (\delta g)(g'g_0).(\delta g')(g_0), \tag{3.1}$$

e usando para A a notação aditiva (ver Definição 1.2.1 *(b)*)

$$\delta(gg')(g_0) = (\delta g)(g'g_0) + (\delta g')(g_0). \tag{3.2}$$

Para uma derivação $\delta : G \longrightarrow I(A)$, vamos associar a aplicação de G em A, denotada por $\boldsymbol{\delta^*}$ e definida por

$$\begin{aligned} \delta^* : G &\longrightarrow A \\ g &\longmapsto \delta^*(g) := (\delta g)(1) \, . \end{aligned}$$

Notemos que em geral, $\delta^* : G \longrightarrow A$ não é um homomorfismo de grupos, pois

$$\delta^*(gg') = \delta(gg')(1) = (\delta g)(g').(\delta g')(1) = (\delta g)^{g'}(1).\delta^*(g').$$

Consideremos $\delta : G \longrightarrow I(A)$ uma derivação (fixada) e δ^* a aplicação associada a δ, como antes. Vamos provar uma série de lemas que serão úteis posteriormente.

Lema 3.2.1. Sejam $g \in G$ e $h \in H$. Então, $\delta^*(gh) = \delta^*(g).\delta^*(h)$, em particular $\delta^*(h_1h_2) = \delta^*(h_1).\delta^*(h_2)$, para todos $h_1, h_2 \in H$, isto é, $\delta^*\big|_H : H \longrightarrow A$ é um homomorfismo.

Demonstração.

Temos,

$$\begin{aligned} \delta^*(gh) = [\delta(gh)](1) &= [(\delta g)^h.(\delta h)](1) = (\delta g)^h(1).(\delta h)(1) \\ &= (\delta g)(h.1).(\delta h)(1) = (\delta g)(h).(\delta h)(1) \end{aligned} \tag{3.3}$$

Como 1 e h são elementos de $1.H$ e $\delta g \in I(A)$ é constante em $1.H$, segue que $(\delta g)(h) = (\delta g)(1)$. Daí, de (3.3) temos

$$\delta^*(gh) = (\delta g)(1).(\delta h)(1) = \delta^*(g).\delta^*(h). \qquad \blacksquare$$

Definição 3.2.2. Dados $\delta^* : G \longrightarrow A$ e Y um subconjunto de A, definimos $\boldsymbol{E_Y}$ como o subconjunto de G dado por

$$E_Y := \{g \in G \mid \delta^*(g^{-1}) \in Y\}.$$

Lema 3.2.2. Para todo $Y \subseteq A$, E_Y é H-quase invariante.

Demonstração.

Fixemos $Y \subseteq A$. Por conveniência, vamos denotar E_Y apenas por E. Precisamos mostrar que para todo $x \in G$, o conjunto dado pela diferença simétrica $E+Ex$ é H-finito, isto é, $E+Ex \subseteq H.F$, onde F é algum subconjunto finito de G.

Para $g \in G$, temos que $g \in E + Ex$ se, e somente se, exatamente um dos elementos g ou gx^{-1} pertence a E, ou equivalentemente

$$g \in E+Ex \Leftrightarrow \text{exatamente um dos elementos} \begin{cases} \delta^*(g^{-1}) \\ \text{ou} \\ \delta^*(xg^{-1}) \end{cases} \text{pertence a } Y. \quad (3.4)$$

De fato,

$g \in (E+Ex) \Leftrightarrow g \in (E-Ex) \cup (Ex-E) \Leftrightarrow g \in (E-Ex)$ ou $g \in (Ex-E)$.

- se $g \in (E - Ex)$ temos que

$$\begin{aligned} g \in E \ \text{ e } \ g \notin Ex &\Leftrightarrow g \in E \ \text{ e } \ g \neq \theta x, \ \forall\, \theta \in E \\ &\Leftrightarrow g \in E \ \text{ e } \ gx^{-1} \neq \theta, \ \forall\, \theta \in E \\ &\Leftrightarrow g \in E \ \text{ e } \ gx^{-1} \notin E \\ &\Leftrightarrow \delta^*(g^{-1}) \in Y \ \text{ e } \ \delta^*(xg^{-1}) \notin Y. \end{aligned}$$

- se $g \in (Ex - E)$, então

$$\begin{aligned} g \in Ex \ \text{ e } \ g \notin E &\Leftrightarrow g = \theta x, \ \text{ para algum } \ \theta \in E \ \text{ e } \ g \notin E \\ &\Leftrightarrow gx^{-1} = \theta \ \text{ para algum } \ \theta \in E \ \text{ e } \ g \notin E \\ &\Leftrightarrow gx^{-1} \in E \ \text{ e } \ g \notin E \\ &\Leftrightarrow \delta^*(xg^{-1}) \in Y \ \text{ e } \ \delta^*(g^{-1}) \notin Y. \end{aligned}$$

Observemos que

$$\delta^*(xg^{-1}) = \delta x(g^{-1}).\delta^*(g^{-1}), \quad (3.5)$$

pois

$$\begin{aligned}\delta^*(xg^{-1}) &= [\delta(xg^{-1})](1) = [(\delta x)^{g^{-1}}.(\delta g^{-1})](1) = (\delta x)^{g^{-1}}(1).(\delta g^{-1})(1)\\ &= (\delta x)(g^{-1}1).(\delta g^{-1})(1) = \delta x(g^{-1}).\delta^*(g^{-1}).\end{aligned}$$

De onde segue que $\delta x(g^{-1}) \in A$ não é trivial, para todo $g \in E + Ex$, pois se existisse $g_0 \in E + Ex$ tal que $\delta x(g_0^{-1}) = 1$ teríamos

$$\delta x(g_0^{-1}) = 1 \overset{(3.5)}{\Rightarrow} \delta^*(xg_0^{-1}) = \delta^*(g_0^{-1}).$$

Assim, $\delta^*(xg_0^{-1}) \in Y$ se, e somente se, $\delta^*(g_0^{-1}) \in Y$, o que contradiz (3.4).

Agora,

$$\delta x(g^{-1}) \neq 1 \Leftrightarrow g^{-1} \in \{\widetilde{g} \in G \mid \delta x(\widetilde{g}) \neq 1\} := supp(\delta x) \Leftrightarrow g \in \big(supp(\delta x)\big)^{-1}.$$

Desta forma,

$$g \in E + Ex \Rightarrow \delta x(g^{-1}) \neq 1 \Rightarrow g \in \big(supp(\delta x)\big)^{-1}$$

e portanto, $E + Ex \subseteq \big(supp(\delta x)\big)^{-1}$.

Logo, para concluírmos que $E + Ex$ é H-finito, basta mostrarmos que $\big(supp(\delta x)\big)^{-1}$ é H-finito.

Como $\delta : G \longrightarrow I(A)$ e $x \in G$, então $\delta x \in I(A) = \{f : G \to A \ ; \ f\big|_{gH} = 1,$ exceto para um número finito de classes laterais à esquerda$\}$. Sejam $g_1H, \ldots, g_kH$ as classes laterais em que $\delta x(g_iH) \neq 1$, $i = 1, \ldots, k$, então

$$\begin{aligned}g \in \big(supp(\delta x)\big)^{-1} &\Leftrightarrow (\delta x)(g^{-1}) \neq 1\\ &\Leftrightarrow g^{-1} \in g_1H \cup \ldots \cup g_kH\\ &\Leftrightarrow g^{-1} \in \{g_1, \ldots, g_k\}.H\\ &\Leftrightarrow g \in H.\{g_1^{-1}, \ldots, g_k^{-1}\} = H.F, \ F = \{g_1^{-1}, \ldots, g_k^{-1}\} \text{ finito.}\end{aligned}$$

Então, concluímos que $\big(supp(\delta x)\big)^{-1}$ é H-finito. Conseqüentemente, $E + Ex \subseteq \big(supp(\delta x)\big)^{-1}$ é H-finito e portanto, $E := E_Y$ é H-quase invariante. ■

Lema 3.2.3. Sejam $h \in H$ e $Y \subseteq A$. Então, $hE_Y = E_{Y.[\delta^*(h)]^{-1}}$.

Demonstração.

Consideremos novamente $E = E_Y = \{g \in G \mid \delta^*(g^{-1}) \in Y\}$ e seja $g \in G$. Então, $g \in hE$ se, e somente se, $\delta^*(g^{-1}h) \in Y$. De fato,

$$\begin{aligned} g \in hE &\Leftrightarrow g = h\theta, \text{ para algum } \theta \in E \Leftrightarrow h^{-1}g = \theta, \text{ para algum } \theta \in E \\ &\Leftrightarrow h^{-1}g \in E. \end{aligned}$$

Assim, pela definição de E, temos que $g \in hE$ se, e somente se, $\delta^*(g^{-1}h) \in Y$.

Pelo Lema 3.2.1,

$$\delta^*(g^{-1}h) = \delta^*(g^{-1}).\delta^*(h).$$

Daí, segue que $\delta^*(g^{-1}) = \delta^*(g^{-1}h).[\delta^*(h)]^{-1}$.

Logo,

$$\begin{aligned} g \in hE &\Rightarrow \delta^*(g^{-1}h) \in Y \Rightarrow \delta^*(g^{-1}) \in Y.[\delta^*(h)]^{-1} \\ &\Rightarrow g \in E_{Y.[\delta^*(h)]^{-1}} = \{a \in G \mid \delta^*(a^{-1}) \in \widetilde{Y} := Y.[\delta^*(h)]^{-1}\}. \end{aligned}$$

Assim, $hE \subseteq E_{Y.[\delta^*(h)]^{-1}}$.

Agora,

$$\begin{aligned} g \in E_{Y.[\delta^*(h)]^{-1}} &\Rightarrow \delta^*(g^{-1}) \in Y.[\delta^*(h)]^{-1} \\ &\Rightarrow \delta^*(g^{-1}) = y.\delta^*(h)^{-1}, \text{ para algum } y \in Y \\ &\Rightarrow \delta^*(g^{-1}).\delta^*(h) = y, \text{ para algum } y \in Y \\ &\Rightarrow \delta^*(g^{-1}h) = y, \text{ para algum } y \in Y \text{ (pelo Lema 3.2.1)} \\ &\Rightarrow \delta^*(g^{-1}h) \in Y \\ &\Rightarrow (g^{-1}h)^{-1} \in E \\ &\Rightarrow h^{-1}g \in E \\ &\Rightarrow g \in hE\ . \end{aligned}$$

Desta forma, $E_{Y[\delta^*(h)]^{-1}} \subseteq hE$ e portanto,

$$hE = \{g \in E \mid \delta^*(g^{-1}) \in Y[\delta^*(h)]^{-1}\} = E_{Y[\delta^*(h)]^{-1}}. \qquad \blacksquare$$

Lema 3.2.4. Sejam Y e Y' subconjuntos de A. Então, $E_Y \cap E_{Y'} = E_{Y \cap Y'}$.

Demonstração.

$$\begin{aligned} g \in E_Y \cap E_{Y'} &\Leftrightarrow g \in E_Y \text{ e } g \in E_{Y'} \\ &\Leftrightarrow \delta^*(g^{-1}) \in Y \text{ e } \delta^*(g^{-1}) \in Y' \\ &\Leftrightarrow \delta^*(g^{-1}) \in Y \cap Y' \\ &\Leftrightarrow g \in E_{Y \cap Y'}. \end{aligned}$$

■

Sejam $\delta : G \longrightarrow I(A)$ uma derivação e $\delta^* : G \longrightarrow A$ a aplicação definida anteriormente. Vimos no Lema 3.2.1 que $\delta^*\big|_H : H \longrightarrow A$ é um homomorfismo de grupos.

Lema 3.2.5. Se $N = Ker\left(\delta^*\big|_H\right)$, então $e(G, N) \geqslant [H : N]$.

Demonstração.

Tomemos o subgrupo de A dado por $B := Im\left(\delta^*\big|_H\right)$ e seja $Y \subseteq A$ um conjunto de representantes para as classes laterais de B em A. Podemos supor que (o elemento neutro de A) $1 \in Y$. Assim, $A/B = \{yB \mid y \in Y\}$ e $A = \dot{\bigcup_{y \in Y}} yB$.

Consideremos para Y o subconjunto $E_Y = \{g \in G \mid \delta^*(g^{-1}) \in Y\}$, como na Definição 3.2.2.

Notemos que $E_Y \neq \varnothing$, pois $1 \in Y$ (o representante da classe $1.B$) e $\delta^*(1^{-1}) = \delta^*(1) = 1 \in Y$ e assim $1 \in E_Y$.

A demonstração do lema consiste essencialmente em provarmos que E_Y, G, H (com $[G : H] = \infty$) e N satisfazem as condições da Proposição 3.1.2.

Notemos inicialmente que, pelo Lema 3.2.2, E_Y é ***H-quase invariante***.

(a) Claramente, $N = Ker\left(\delta^*\big|_H\right)$ é normal a H.

(b) Vejamos que $hE_Y \cap E_Y = \varnothing$, para todo $h \in H - N$. Para isso, seja $h \in H - N = H - Ker\left(\delta^*\big|_H\right)$. Então, $h \in H \subseteq G$ e $b := \delta^*(h) \in B \subseteq A$, com $\delta^*(h)$ não trivial.

Afirmamos que:

$$b = \delta^*(h) \text{ não trivial, implica em } \quad Y \cap Yb^{-1} = \varnothing, \tag{3.6}$$

pois caso contrário existiria um elemento $z \in Y \cap Yb^{-1}$, o que levaria em $z \in Y$ e $z = yb^{-1}$, para algum $y \in Y$. Daí,

$$zB = (yb^{-1})B = yB \overset{def.\ Y}{\Rightarrow} z = y \Rightarrow yb^{-1} = y \Rightarrow b \text{ trivial},$$

o que é uma contradição.

Conseqüentemente, para $b = \delta^*(h) \neq 1$ obtemos

$$E_Y \cap E_{Yb^{-1}} \overset{Lema\ 3.2.4}{=} E_{Y \cap Yb^{-1}} = E_{\varnothing} = \{g \in G \mid \delta^*(g^{-1}) \in \varnothing\} = \varnothing.$$

Agora, pelo Lema 3.2.3, $E_{Yb^{-1}} = E_{Y[\delta^*(h)]^{-1}} = hE_Y$. Logo, para todo $h \in H - N$, temos $hE_Y \cap E_Y = E_{Yb^{-1}} \cap E_Y = \varnothing$, como afirmado.

Da afirmação (3.6) segue também que *os conjuntos*

$$N = Ker\left(\delta^*\big|_H\right) \text{ e } \{h \in H \mid hE_Y = E_Y\}$$

coincidem, isto é, $N = \{h \in H \mid hE_Y = E_Y\}$. De fato,

$$\begin{aligned} h \in N = Ker\left(\delta^*\big|_H\right) \quad &\Rightarrow \quad h \in H \text{ e } \delta^*(h) = 1 \\ &\overset{Lema\ 3.2.3}{\Rightarrow} \quad h \in H \text{ e } hE_Y = E_{Y[\delta^*(h)]^{-1}} = E_Y \ . \end{aligned}$$

Assim, $N \subseteq \{h \in H \mid hE_Y = E_Y\}$.

Por outro lado, se $h \in H$ e $hE_Y = E_Y$, tome $b := \delta^*(h)$. Então, $E_{Yb^{-1}} = E_{Y[\delta^*(h)]^{-1}} \overset{Lema\ 3.2.3}{=} hE_Y = E_Y$ e assim $E_Y \cap E_{Yb^{-1}} = E_Y \neq \varnothing$.

Mas a afirmação (3.6) é equivalente a: $E_Y \cap E_{Yb^{-1}} \neq \varnothing$ implica $b = \delta^*(h)$ trivial.

Assim, $h \in H$ e $hE_Y = E_Y$ implica que $h \in H$ e $\delta^*(h)$ é trivial, isto é $h \in Ker\left(\delta^*\big|_H\right)$.

Logo, $\{h \in H \mid hE_Y = E_Y\} \subseteq N$ e portanto $N = \{h \in H \mid hE_Y = E_Y\}$.

(c) $H.E_Y = G$. Obviamente $HE_Y \subseteq G$, pois $E_Y = \{g \in G \mid \delta^*(g^{-1}) \in Y\}$ e H é subgrupo de G. Agora, se $g \in G$, então $\delta^*(g^{-1}) \in A = \dot{\bigcup\limits_{y \in Y}} yB$.

Assim, existem $y \in Y$ e $h \in H$ tais que $\delta^*(g^{-1}) = y.\delta^*(h)$ e conseqüentemente

$$\delta^*(g^{-1}h^{-1}) \overset{Lema\ 3.2.1}{=} \delta^*(g^{-1}).\delta^*(h^{-1}) = \delta^*(g^{-1}).[\delta^*(h)]^{-1} = y \in Y.$$

Daí, $hg = (g^{-1}h^{-1})^{-1} \in E_Y$ e portanto, $g \in h^{-1}E_Y \subseteq HE_Y$ de onde concluímos que $HE_Y = G$.

Finalmente, tendo verificado que $E = E_Y$, G, H e N satisfazem todas as condições da Proposição 3.1.2, concluímos então que $e(G, N) \geqslant [H : N]$. ■

3.3 Teorema de Swarup

Por toda esta seção, consideramos G um grupo finitamente gerado e denotamos por A um grupo abeliano aditivo, com a estrutura de $\mathbb{Z}G$-módulo trivial.

Vejamos inicialmente, mais alguns resultados.

Proposição 3.3.1. Sejam G e A grupos. Então, $C(A)$ e $I(A)$ são isomorfos aos módulos $Coind_H^G A$ e $Ind_H^G A$, respectivamente. Em particular, se $A = \mathbb{Z}$, $C(\mathbb{Z}) \simeq Hom_{\mathbb{Z}}\big(\mathbb{Z}(G/H), \mathbb{Z}\big) \overset{not.}{=} \overline{\mathbb{Z}(G/H)}$ e $I(\mathbb{Z}) \simeq \mathbb{Z}(G/H) \simeq \mathbb{Z}(H\backslash G)$.

Demonstração.

Como A é um grupo abeliano, podemos vê-lo como um $\mathbb{Z}$-módulo e como um $\mathbb{Z}G$-módulo com a G-ação trivial. Por conveniência, como $Coind_H^G A$ e $Ind_H^G A$ foram estudados considerando módulos à esquerda, vamos aqui considerar $C(A)$ e $I(A)$ como $\mathbb{Z}G$-módulos à esquerda, bastando para isso tomar a G-ação à esquerda: $g.f := f.g^{-1}$.

(1) $C(A) \simeq Coind_H^G A$. Temos,

$$C(A) = \Big\{ f : G \to A \ ;\ f\big|_{gH} \text{ é constante, } \forall\ gH \in G/H \Big\}$$

e pela Proposição 1.4.4, temos um $\mathbb{Z}G$-isomorfismo

$$Coind_H^G A = Hom_{\mathbb{Z}H}(\mathbb{Z}G, A) \simeq Hom_{\mathbb{Z}}\big(\mathbb{Z}(G/H), A\big).$$

Seja $E = \{g_\alpha \mid \alpha \in J\}$ um conjunto de representantes para as classes laterais à esquerda de H em G, isto é, $G = \bigcup\limits_{\alpha\in J}^{\cdot} g_\alpha H$.

Consideremos $f \in C(A)$, então $f\big|_{g_\alpha H}$ é constante, isto é, $f(g_\alpha) = c_\alpha$ (c_α constante).

Desta forma, definamos

$$\begin{aligned} \varphi :\ C(A) &\longrightarrow Hom_{\mathbb{Z}}(\mathbb{Z}(G/H), A) \\ f &\longmapsto \varphi(f) : \mathbb{Z}(G/H) \longrightarrow A \end{aligned}$$

de modo que nos elementos básicos $g_\alpha H$ de $\mathbb{Z}(G/H)$, $\big[\varphi(f)\big](g_\alpha H) := f(g_\alpha) = c_\alpha \in A$ e estendemos por linearidade:

$$\big[\varphi(f)\big]\left(\sum_{\alpha\in J} n_\alpha(g_\alpha H)\right) = \sum_{\alpha\in J} n_\alpha f(g_\alpha).$$

Observemos que essa soma é finita, pois cada elemento $\sum\limits_{\alpha\in J} n_\alpha(g_\alpha H) \in \mathbb{Z}(G/H)$ é tal que $n_\alpha = 0$ para quase todo $\alpha \in J$ e $\varphi(f)(gH) = f(g)$, para todo $g \in G$, pois $gH = g_\alpha H \overset{def.\ f}{\Rightarrow} f(g) = f(g_\alpha) = \varphi(f)(g_\alpha H) = \varphi(f)(gH)$.

Temos que $\varphi(f) \in Hom_{\mathbb{Z}}\big(\mathbb{Z}(G/H), A\big)$, isto é, $\varphi(f)$ é um homomorfismo de grupos abelianos, pois se $x = \sum\limits_{\alpha\in J} n_\alpha(g_\alpha H)$ e $y = \sum\limits_{\alpha\in J} m_\alpha(g_\alpha H) \in \mathbb{Z}(G/H)$, então

$$\begin{aligned} \varphi(f)(x+y) &= \varphi(f)\left[\sum_{\alpha\in J} n_\alpha(g_\alpha H) + \sum_{\alpha\in J} m_\alpha(g_\alpha H)\right] \\ &= \varphi(f)\left[\sum_{\alpha\in J} (n_\alpha + m_\alpha)(g_\alpha H)\right] \\ &= \sum_{\alpha\in J} (n_\alpha + m_\alpha) f(g_\alpha) \\ &= \sum_{\alpha\in J} n_\alpha f(g_\alpha) + \sum_{\alpha\in J} m_\alpha f(g_\alpha) \end{aligned}$$

$$= \varphi(f)\left[\sum_{\alpha\in J} n_\alpha(g_\alpha H)\right] + \varphi(f)\left[\sum_{\alpha\in J} m_\alpha(g_\alpha H)\right]$$
$$= \varphi(f)(x) + \varphi(f)(y).$$

Também temos que φ é um homomorfismo de $\mathbb{Z}G$-módulos (à esquerda):

(a) $\varphi(f.f') = \varphi(f) + \varphi(f')$ visto que, nos geradores,

$$\begin{aligned}\varphi(f.f')(g_\alpha H) &= (f.f')(g_\alpha) = f(g_\alpha) + f'(g_\alpha)\\ &= \varphi(f)(g_\alpha H) + \varphi(f')(g_\alpha H)\\ &= [\varphi(f) + \varphi(f')]\,(g_\alpha H).\end{aligned}$$

(b) $\varphi(g.f) = g.\varphi(f)$, para todo $g \in G$, pois

- $\varphi(g.f)(g_\alpha H) = \varphi(f.g^{-1})(g_\alpha H) \overset{def.\,\varphi}{=} (f.g^{-1})(g_\alpha) = f(g^{-1}g_\alpha)$ e
- $\big(g.\varphi(f)\big)(g_\alpha H) = g.\varphi(f)(g^{-1}g_\alpha H) = \varphi(f)(g^{-1}g_\alpha H) = f(g^{-1}g_\alpha)$.

Consideremos agora

$$\begin{aligned}\psi :\ Hom_{\mathbb{Z}}(\mathbb{Z}(G/H), A) &\longrightarrow C(A)\\ \phi &\longmapsto \psi(\phi)\end{aligned}$$

onde $\psi(\phi)$ é definida por

$$\begin{aligned}\psi(\phi) :\quad G &\longrightarrow A\\ g = g_\alpha h &\longmapsto \psi(\phi)(g) = \phi(g_\alpha H) = \phi(gH).\end{aligned}$$

Ainda, temos que ψ é um homomorfismo e é o inverso de φ. De fato,

- ψ é um homomorfismo,
- $\psi \circ \varphi = id_{C(A)}$

$$(\psi\circ\varphi)(f)(g) = \psi[\varphi(f)(g)] \overset{def.\,\psi}{=} \varphi(f)(gH) \overset{def.\,\varphi}{=} f(g),$$

- $\varphi \circ \psi = id_{Hom_{\mathbb{Z}}(\mathbb{Z}(G/H),A)}$

$$(\varphi\circ\psi)(\phi)(gH) \overset{def.\,\varphi}{=} \psi(\phi)(g) = \phi(gH).$$

Logo, $C(A) \simeq Hom_{\mathbb{Z}}\big(\mathbb{Z}(G/H), A\big)$ (como $\mathbb{Z}G$-módulos) e portanto, da Proposição 1.4.4, temos que $C(A) \simeq Coind_H^G A$.

(2) $I(A) \simeq Ind_H^G A$.

Para isso consideramos a composição das três aplicações seguintes (já adaptadas ao fato que A é $\mathbb{Z}G$-módulo trivial):

(1ª) O $\mathbb{Z}G$-monomorfismo

$$\begin{aligned} \vartheta : Ind_H^G A &\longrightarrow Coind_H^G A \\ g_0 \otimes a &\longmapsto \vartheta(g_0 \otimes a), \end{aligned}$$

tal que $\vartheta(g_0 \otimes a)(g) = \begin{cases} a, & \text{se } gg_0 \in H; \\ 0, & \text{c. c.} \end{cases}$ $\big($dado na Proposição 1.4.2 *(a)*$\big)$.

(2ª) O $\mathbb{Z}G$-isomorfismo

$$\begin{aligned} \xi : Coind_H^G A &\longrightarrow Hom_{\mathbb{Z}}(\mathbb{Z}(G/H), A) \\ f &\longmapsto \xi(f), \end{aligned}$$

tal que $\xi(f)(gH) = f(g^{-1})$ (dado na Proposição 1.4.4 *(a)*).

(3ª) O $\mathbb{Z}G$-isomorfismo $\psi : Hom_{\mathbb{Z}}\big(\mathbb{Z}(G/H), A\big) \longrightarrow C(A)$ dado anteriormente.

Deste modo, obtemos um $\mathbb{Z}G$-monomorfismo

$$\eta = \psi \circ \xi \circ \vartheta : Ind_H^G A \longrightarrow C(A).$$

Agora, $Im(\eta) = I(A)$, pois num elemento básico $g_0 \otimes a \in Ind_H^G A = \mathbb{Z}G \otimes_{\mathbb{Z}H} A$, temos:

$$\begin{aligned} \big(\eta(g_0 \otimes a)\big)(g) &= \big((\psi \circ \xi \circ \vartheta)(g_0 \otimes a)\big)(g) = \psi\big(\xi(\vartheta(g_0 \otimes a))\big)(g) \\ &\overset{def.\ \psi}{=} \xi\big(\vartheta(g_0 \otimes a)\big)(gH) \overset{def.\ \xi}{=} \vartheta(g_0 \otimes a)(g^{-1}) \\ &\overset{def.\ \vartheta}{=} \begin{cases} a, & \text{se } g^{-1}g_0 \in H; \\ 0, & \text{c. c.} \end{cases} \end{aligned}$$

isto é, $\big(\eta(g_0 \otimes a)\big)(g) = \begin{cases} a, & \text{se } g \in g_0H; \\ 0, & \text{c. c.} \end{cases}$

Assim, $f_{g_0,a} := \eta(g_0 \otimes a)$ é um elemento de $I(A)$ constante nos elementos de classe g_0H e nulo nos demais elementos.

Claramente, as funções da forma $f_{g_0,a}$, com $g_0 \in G$ e $a \in A$, geram $I(A)$. Logo,

$$Ind_H^G A \simeq Im(\eta) = I(A),$$

como queríamos mostrar.

(3) Finalmente, se $A = \mathbb{Z}$, temos:

$$C(\mathbb{Z}) \simeq Coind_H^G \mathbb{Z} = Hom_{\mathbb{Z}H}(\mathbb{Z}G, \mathbb{Z}) \simeq Hom_{\mathbb{Z}}(\mathbb{Z}(G/H), \mathbb{Z}) \overset{not.}{=} \overline{\mathbb{Z}(G/H)} \text{ e}$$

$$I(\mathbb{Z}) \simeq Ind_H^G \mathbb{Z} = \mathbb{Z}G \otimes_{\mathbb{Z}H} \mathbb{Z} \simeq \mathbb{Z}(G/H) \overset{Lema\ 1.4.1}{\simeq} \mathbb{Z}(H\backslash G). \qquad \blacksquare$$

Corolário 3.3.1. Seja A um grupo abeliano, visto como $\mathbb{Z}G$-módulo trivial. Então,

(a) $H^1(G, C(A)) \simeq Hom(H, A)$.

(b) Identificando $H^1(G, C(A))$ com $Hom(H, A)$, podemos ver o homomorfismo induzido em cohomologia $(id_G, \alpha)^* : H^1(G, I(A)) \longrightarrow H^1(G, C(A))$ da inclusão $\alpha : I(A) \longrightarrow C(A)$ como a aplicação

$$\begin{aligned} \rho : \ H^1(G, I(A)) &\longrightarrow H^1(G, C(A)) \equiv Hom(H, A) \\ [\delta] &\longmapsto \delta^*\big|_H \ , \end{aligned}$$

onde $\delta : G \longrightarrow I(A)$ é uma derivação representando uma classe de cohomologia $[\delta] \in H^1(G, I(A))$.

Demonstração.

(a) Da proposição anterior (ver demonstração, parte *(2)*) e Proposição 1.5.1, segue que $H^1(G, C(A)) \simeq H^1(G, Coind_H^G A)$.

Agora, usando o Lema de Shapiro (Proposição 1.6.1), a Proposição 1.2.2 e o Corolário 1.2.1 (visto que A é um $\mathbb{Z}G$-módulo trivial), obtemos

$$H^1(G, Coind_H^G A) \overset{(i,\pi)^*}{\simeq} H^1(H, A) = \frac{Der(H, A)}{P(H, A)} = Hom(H, A),$$

onde $i : H \longrightarrow G$ é a inclusão.

(b) Seja $[\delta] \in H^1(G, I(A)) = \dfrac{Der(G, I(A))}{P(G, I(A))}$. Como $I(A) \subseteq C(A)$, podemos ver $[\delta]$ como um elemento de $H^1(G, C(A))$ $\big([\delta] \equiv [\alpha \circ \delta]\big)$. Ainda, identificando $H^1(G, C(A))$ com $H^1(G, Coind_H^G A)$, podemos considerar $[\delta] \in H^1(G, Coind_H^G A)$. Analisando $(i, \pi)^*$ temos que $(i, \pi)^*([\delta]) = [\pi \circ \delta \circ \tau]$, onde $\tau : F \longrightarrow F'$ é uma aplicação de cadeias entre as resoluções projetivas de $\mathbb{Z}$ sobre $\mathbb{Z}H$ e $\mathbb{Z}G$, respectivamente. Mas podemos tomar F e F' como sendo as resoluções bar e τ como a inclusão. Daí, $(i, \pi)^*([\delta]) = [\pi \circ \delta \circ \tau] = [\pi \circ \delta] \overset{P(H,A)=0}{=} \pi \circ \delta$.

Agora, $(\pi \circ \delta)(h) = \delta(h)(1) = \delta^*(h) = \delta^*\big|_H(h)$. ■

Proposição 3.3.2. Sejam G um grupo finitamente gerado e H um subgrupo de G de índice infinito. Então,

$$e(G, H) = 1 + rank_{\mathbb{Z}}(Ker\ \rho),$$

onde

$$\begin{aligned} \rho = (id, \alpha)^* : H^1(G, I(\mathbb{Z})) &\longrightarrow H^1(G, C(\mathbb{Z})) \\ [\delta] &\longmapsto \delta^*\big|_H \end{aligned}$$

é a aplicação do corolário anterior.

Demonstração.

Do $\mathbb{Z}G$-monomorfismo natural $I(\mathbb{Z}) \longrightarrow C(\mathbb{Z})$, obtemos a seqüência exata curta

$$0 \longrightarrow I(\mathbb{Z}) \longrightarrow C(\mathbb{Z}) \longrightarrow \frac{C(\mathbb{Z})}{I(\mathbb{Z})} \longrightarrow 0. \tag{3.7}$$

Esta seqüência, induz uma seqüência exata longa em cohomologia

$$\begin{aligned} 0 \longrightarrow\ & H^0\big(G, I(\mathbb{Z})\big) \longrightarrow H^0\big(G, C(\mathbb{Z})\big) \longrightarrow H^0\left(G, \frac{C(\mathbb{Z})}{I(\mathbb{Z})}\right) \\ \longrightarrow\ & H^1\big(G, I(\mathbb{Z})\big) \xrightarrow{\ \rho\ } H^1\big(G, C(\mathbb{Z})\big) \longrightarrow \cdots \end{aligned} \tag{3.8}$$

Agora,

- $H^0\big(G, I(\mathbb{Z})\big) \simeq H^0\big(G, Ind_H^G\mathbb{Z}\big) = 0$, visto que $[G : H] = \infty$ (Proposição 1.4.3).
- $H^0\big(G, C(\mathbb{Z})\big) \simeq H^0\big(G, Coind_H^G\mathbb{Z}\big) \overset{Shapiro}{\simeq} H^0(H, \mathbb{Z}) \simeq \mathbb{Z}$.
- $\dfrac{C(\mathbb{Z})}{I(\mathbb{Z})} \simeq \dfrac{Coind_H^G\mathbb{Z}}{Ind_H^G\mathbb{Z}} \simeq \dfrac{\overline{\mathbb{Z}(G/H)}}{\mathbb{Z}(G/H)}$, onde $\overline{\mathbb{Z}(G/H)} = Hom_{\mathbb{Z}}(\mathbb{Z}(G/H), \mathbb{Z})$.

Assim, obtemos de (3.8) a seguinte seqüência exata curta

$$0 \longrightarrow \mathbb{Z} \longrightarrow H^0\left(G, \frac{\overline{\mathbb{Z}(G/H)}}{\mathbb{Z}(G/H)}\right) \longrightarrow Ker\ \rho \longrightarrow 0$$

Agora, $Im(\rho)$ é um $\mathbb{Z}$-módulo livre, pois é um $\mathbb{Z}$-submódulo de $H^1(G, \mathbb{Z}(G/H))$ que é livre ([9], Proposição 4.5.16) e $\mathbb{Z}$ é domínio de ideais principais (Proposição A.4.4) e daí obtemos (vide Observação 2.3.1 e Proposição A.4.3) que

$$e(G, H) = rank_{\mathbb{Z}} H^0\left(G, \frac{\overline{\mathbb{Z}(G/H)}}{\mathbb{Z}(G/H)}\right) = 1 + rank_{\mathbb{Z}}(Ker\ \rho). \qquad \blacksquare$$

Corolário 3.3.2. Seja H um subgrupo de índice infinito num grupo finitamente gerado G. Então,

$$e(G, H) \leqslant 1 + rank_{\mathbb{Z}} H^1(G, \mathbb{Z}(G/H)).$$

Observação 3.3.1. A proposição anterior e corolário são válidos por considerar mais geralmente A um corpo primo ou um subanel de $\mathbb{Q}$, ao invés de $\mathbb{Z}$ ([15], 3.1) (ou ainda um Domínio de Ideais Principais ([9], 4.5.17)). O caso $A = \mathbb{Z}_2$ foi provado por Andrade-Fanti em [1], Lema 3.2 e a idéia aqui apresentada é essencialmente a mesma.

Finalmente, o Teorema de Swarup segue por combinar os resultados desta seção com o Lema 3.2.5.

Teorema 3.3.1. Sejam G um grupo finitamente gerado e H um subgrupo de índice infinito em G. Se $e(G,N)=1$, para todo $N \lhd H$, com $\dfrac{H}{N} \simeq \mathbb{Z}$, então

$$e(G,H) = 1 + rank_{\mathbb{Z}} H^1\big(G, I(\mathbb{Z})\big) = 1 + rank_{\mathbb{Z}} H^1\big(G, \mathbb{Z}(G/H)\big).$$

Demonstração.

Em vista do Corolário 3.3.1 *(b)*, é suficiente mostrar que

$$\rho : H^1\big(G, I(\mathbb{Z})\big) \longrightarrow Hom(H, \mathbb{Z})$$

é o homomorfismo trivial, daí

$$Ker\rho = H^1\big(G, I(\mathbb{Z})\big) \text{ e } e(G,H) = 1 + rank_{\mathbb{Z}}(Ker\rho) = 1 + rank_{\mathbb{Z}} H^1\big(G, I(\mathbb{Z})\big).$$

Se $\rho = 0$, então não há nada a demonstrar. Caso contrário, existiria $\mu \in H^1\big(G, I(\mathbb{Z})\big) = \dfrac{Der\big(G, I(\mathbb{Z})\big)}{P\big(G, I(\mathbb{Z})\big)}$ tal que $\rho(\mu) \neq 0$, logo $\mu \neq 0$. Mas, $\mu = \delta + P\big(G, I(\mathbb{Z})\big)$, onde $\delta : G \longrightarrow I(\mathbb{Z})$ é uma derivação.

Seja então $\delta : G \longrightarrow I(\mathbb{Z})$ uma derivação. Pelo Lema 3.2.5, temos que

$$e(G,N) \geqslant [H:N], \quad \text{onde} \quad N = Ker\left(\delta^*\big|_H\right).$$

Se $\delta^*\big|_H : H \longrightarrow \mathbb{Z}$ é não trivial, isto é, $Im\left(\delta^*\big|_H\right) \neq \{0\}$, então pelo Teorema do Isomorfismo $\dfrac{H}{N} = \dfrac{H}{N = Ker\left(\delta^*\big|_H\right)} \simeq Im\left(\delta^*\big|_H\right)$ que é um subgrupo não trivial de $\mathbb{Z}$, o que implica que $\dfrac{H}{N} \simeq k\mathbb{Z} \simeq \mathbb{Z}$ $(k \in \mathbb{N}^*)$, de onde concluímos que $[H:N] = |H/N| = \infty$.

Logo, como $e(G,N) \geqslant [H:N]$, obtemos que $e(G,N) = \infty$, o que contradiz a hipótese inicial.

Assim, $\rho([\delta]) = \delta^*\big|_H$ é trivial para todo δ.

Portanto, pela Proposição 3.3.2 temos que

$$e(G,H) = 1 + rank_{\mathbb{Z}}(Ker\ \rho) = 1 + rank_{\mathbb{Z}} H^1\big(G, I(\mathbb{Z})\big).$$

Agora, a última igualdade segue da Proposição 3.3.1. ■

Corolário 3.3.3. Seja G um grupo finitamente gerado. Se $e(G) = 1$ e G tem um subgrupo H cíclico infinito, então

$$e(G, H) = 1 + rank_{\mathbb{Z}} H^1(G, \mathbb{Z}(G/H)).$$

Demonstração.

Seja $N \lhd H$, com $\dfrac{H}{N} \simeq \mathbb{Z}$. Como por hipótese $H \simeq \mathbb{Z}$, devemos ter necessariamente $N = \{1\}$. Daí, $e(G, N) = e(G, \{1\}) = e(G) = 1$ e o resultado segue do teorema anterior. ■

Exemplo 3.3.1.

(1) Consideremos $G = \mathbb{Z} \oplus \mathbb{Z}$ e $H = \mathbb{Z}$. Temos que, $e(\mathbb{Z} \oplus \mathbb{Z}) = 1$. Então, pelo corolário anterior,

$$e(G, H) = 1 + rank_{\mathbb{Z}} H^1\big(G, \mathbb{Z}(G/H)\big),$$

isto é, $e(\mathbb{Z} \oplus \mathbb{Z}, \mathbb{Z}) = 1 + rank_{\mathbb{Z}} H^1\big(\mathbb{Z} \oplus \mathbb{Z}, \mathbb{Z}\big)$ que já sabemos ser igual a 2 (Exemplo 2.3.2 *(1)*) e assim $rank_{\mathbb{Z}} H^1\big(\mathbb{Z} \oplus \mathbb{Z}, \mathbb{Z}\big) = 1$.

(2) Mais geralmente, se $G = \mathbb{Z} \oplus \mathbb{Z} \oplus K$, onde K é um grupo finito e $H = \mathbb{Z}$, então

$$e(G, H) = 1 + rank_{\mathbb{Z}} H^1\big(G, \mathbb{Z}(G/H)\big),$$

pois, $e(G) \overset{\text{Teorema 2.1.2}}{=} e(\mathbb{Z} \oplus \mathbb{Z}) = 1$.

Observação 3.3.2.

(1) Como conseqüência do teorema anterior, Swarup em [28] apresentou algumas aplicações para grupos de dualidade de Poincaré.

(2) É interessante observar que quando $[G : H] = \infty$, Andrade e Fanti em [1] definiram um invariante end "$E(G, H)$", provaram que $E(G, H) \leqslant e(G, H)$ e analisaram algumas situações em que $E(G, H)$ e $e(G, H)$ coincidem. O invariante end $E(G, H)$ é dado através de uma fórmula cohomológica 1-dimensional (envolvendo *cohomologia relativa* de grupos):

$$E(G, H) = 1 + dim_{\mathbb{Z}_2} \left(\frac{H^1\big(G, H, \mathbb{Z}_2(G/H)\big)}{P\big(G, H, \mathbb{Z}_2(G/H)\big)} \right),$$

onde $P\big(G,H,\mathbb{Z}_2(G/H)\big)=\big\{\delta\in P\big(G,\mathbb{Z}_2(G/H)\big)\ ;\ \delta\big|_H=0\big\}$.

Assim, nos casos em que $E(G,H)$ e $e(G,H)$ coincidem (como no Teorema 3.1 e Corolário 3.6 de [1]), obtemos também para $e(G,H)$ uma fórmula cohomológica (relativa) 1-dimensional.

Referências Bibliográficas

[1] ANDRADE, M. G. C.; FANTI, E. L. C. A Relative Cohomological Invariant for Group Pairs. *Manuscripta Math.*, 83 p. 1-18, 1994.

[2] ANDRADE, M. G. C.; FANTI, E. L. C.; DACCACH, J. A. On Certain Relative Cohomological Invariants. *International Journal of Pure and Applied Mathematics*, 21 p. 335-351, 2005.

[3] AZEVEDO, A. de *Módulos sobre Domínios Principais*. IMPA, Rio de Janeiro, 1971.

[4] BROWN, K. S. *Cohomology of Groups*. G. T. M. 87, New York, Springer Verlag, 1982.

[5] CIOCA, D. M. *Cohomologia e Ends de Grupos*. Dissertação (Mestrado em Matemática) - IBILCE-UNESP, São José do Rio Preto, 1997.

[6] COHEN, D. E. *Groups of Cohomological Dimension One*. Lectures Notes in Mathematics 245, Springer-Verlag, Berlin, 1972.

[7] EPSTEIN, D. B. A. Ends, in Topology of 3-Manifolds and related topics. Ed. M. K. Fort, Prentice-Hall, p. 110-117, 1962.

[8] FREUDENTHAL, H. Über die Enden diskreter Raüme und Gruppen. *Comment. Math. Helv.* 17, p. 1-38, 1944.

[9] GEOGHEGAN, R. *Topological Methods in Groups Theory*. (to appear)

[10] GOALBY, A. J. *Ends*. M. Sc. dissertation, Departament of Pure Mathematics, University of Liverpool, 1975.

[11] HOPF, H. Enden offener raüme and unendlicher diskontinuierliche gruppen. *Comm. Math. Helv.* 16, p. 81-100, 1943.

[12] HOUGHTON, C. H. Ends of locally compact groups and their quotient spaces. *J. Aust. Math. Soc.* 17, p. 274-284, 1974.

[13] HU, S. T. *Introduction to Homological Algebra*. Holden-Day Series in Mathematics, Holden-Day Inc. São Francisco, 1968.

[14] KROPHOLLER, P. H.; ROLLER, M. A. Relative Ends and Duality Groups. *Journal of Pure and Applied Algebra* 61, p. 197-210, 1989.

[15] KROPHOLLER, P. H.; ROLLER, M. A. Remarks on the theorem of Swarup on ends of pairs of groups. *Journal of Pure and Applied Algebra* 109, p. 107-110, 1996.

[16] MACLANE, S. *Homology*. Springer-Verlag, Berlin, 1967.

[17] MILIES, F. C. P. *Anéis e Módulos*. ed. São Paulo: IME-USP, 1972.

[18] RAYMOND, F.; LEE, R. Manifolds Covered by Euclidean Space. *Topology* Vol. 14, Pergamon Press, p. 49-57, 1975.

[19] ROBINSON, D. J. S. *A Course in the Theory of Groups*. Graduate Texts in Mathematics, v. 80, New York, Springer Verlag, 1982.

[20] ROTMAN, J. J. *An Introduction to Homological Algebra*. Academic Press, Inc., 1979.

[21] SAITO, S. *Alguns Aspectos da Teoria de Ends*. Dissertação (Mestrado em Matemática) - IBILCE-UNESP, São José do Rio Preto, 2004.

[22] SCOTT, G. P. Ends of pairs of groups. *Journal of Pure and Applied Algebra* 11 p. 179-198, 1977.

[23] SCOTT, G. P.; WALL, C. T. C. Topological methods in group theory. Homological Groups Theory. *London Math. Soc. Lecture Notes Series* 36, Cambridge p. 137-203, 1979.

[24] SIEBENMANN, L. C. *The obstruction to finding a boundary for an open manifold of dimension greater than five*. PhD. Thesis, Princiton Univ. Press, 1965.

[25] SILVEIRA, F. S. M. *Um Invariante Cohomológico para Pares de Grupos*. Dissertação (Mestrado em Matemática) - IBILCE-UNESP, São José do Rio Preto, 2003.

[26] SPECKER, E. Endenverbände von Raüme und Gruppen. *Math. Annalen* 122, p. 167-174, 1950.

[27] SWAN, R. G. Groups of Cohomological Dimension One. *Journal of Algebra* 12, p. 585-601, 1969.

[28] SWARUP, G. A. On the ends of pairs of groups. *Journal of Pure and Applied Algebra* 87 p. 93-96, 1993.

Apêndice A

Tópicos de Álgebra Homológica

Em geral, no que segue, R indica um anel com unidade, no entanto, sempre que nos referimos a RG-módulos, R se restringe a $\mathbb{Z}$ ou $\mathbb{Z}_2$.

Fazemos aqui uma revisão de conceitos e resultados importantes de Álgebra Homológica, relativos à teoria de Módulos, necessários para o desenvolvimento do trabalho. Destacamos as resoluções Padrão e Bar (de R sobre RG-módulos, tanto à esquerda como à direita), bem como um estudo de posto/rank de módulos livres sobre anéis comutativos (com unidade). A maioria dos resultados são apenas enunciados.

Um livro texto inicialmente utilizado (com algumas adaptações) foi [13], no entanto, para tópicos como, por exemplo, *produto tensorial* este texto não é bom e assim utilizamos mais de perto [20]. Isto deve-se ao fato que em [13] o autor trabalhe com R-módulos, sendo R anel comutativo com unidade, e não é nosso interesse considerar apenas tais anéis comutativos, pois na definição de cohomologia de grupos (Capítulo 1), os módulos considerados são módulos sobre *anéis grupos* ($\mathbb{Z}G$ e $\mathbb{Z}_2G$) que não são comutativos quando G não é comutativo.

Outras referências usadas são [16], [20], [3], [17], [4] e [19].

A.1 Módulos e Homomorfismos

Definição A.1.1. Seja R um anel com unidade. Dizemos que um conjunto não vazio M é um ***R-módulo à esquerda***, se M é um grupo abeliano aditivo, junto com uma aplicação

$$\mu : R \times M \longrightarrow M$$

tal que para cada $\alpha \in R$ e cada $m \in M$, associa o elemento $\mu(\alpha, m) := \alpha m \in M$ satisfazendo as seguintes condições:

(a) $\alpha(\beta m) = (\alpha\beta)m$,

(b) $\alpha(m + m') = \alpha m + \alpha m'$,

(c) $(\alpha + \beta)m = \alpha m + \beta m$,

(d) $1m = m$,

para todos $\alpha, \beta \in R$ e $m, m' \in M$.

Observação A.1.1.

(1) De maneira análoga, podemos definir R-módulo *à direita*, para isto basta considerarmos uma multiplicação à direita por elementos do anel R.

(2) Em geral definições, exemplos e resultados, são apresentados com maior ênfase para R-módulos à esquerda, uma vez que a teoria de cohomologia de grupos (Capítulo 1) é introduzida seguindo [4], que trabalha com módulos à esquerda. No entanto, resultados similares continuam válidos se consideramos R-módulos à direita. Assim, em muitas situações diremos simplesmente R-módulo, sem especificar se é à direita ou à esquerda.

(3) Se R é um anel comutativo, todo R-módulo à esquerda M, admite uma estrutura natural de R-módulo à direita, por definir $m * \alpha := \alpha.m$, para todos $\alpha \in R$ e $m \in M$ (e reciprocamente).

Exemplo A.1.1.

(1) Todo anel com unidade R, admite uma estrutura de R-módulo à esquerda (à direita) considerando a multiplicação por escalar como sendo a multiplicação usual do anel. Às vezes denota-se ${}_RR$ (R_R) para indicar R com a estrutura de R-módulo à esquerda (à direita). Por exemplo, o anel $\mathbb{R}$ (dos reais) é um $\mathbb{R}$-módulo (à esquerda e à direita), $\mathbb{Z}_n$ (visto como um anel) é um $\mathbb{Z}_n$-módulo (à esquerda e à direita) etc. Ainda, se $\mathcal{I}$ é um ideal à esquerda (à direita) de um anel R, considerando em $\mathcal{I}$ a soma induzida da soma de R e a multiplicação à esquerda (à direita) por escalar definida pela multiplicação de R, podemos ver $\mathcal{I}$ como um R-módulo à esquerda (à direita).

(2) Sejam G um grupo abeliano (que denotamos aditivamente) e $R = \mathbb{Z}$ o anel dos inteiros. Definindo

$$\begin{aligned} \mu : \mathbb{Z} \times G &\longrightarrow G \\ (n, g) &\longmapsto \mu(n, g) := n.g, \end{aligned}$$

para todos $n \in \mathbb{Z}$ e $g \in G$, com $1.g = g$, $(n+1).g = n.g + g$ e $-n.g = -(n.g)$, para $n \in \mathbb{N}^*$, temos que G é um $\mathbb{Z}$-módulo (à esquerda). Em particular, $\mathbb{Z}_n$ o grupo das classes de restos módulo n é um $\mathbb{Z}$-módulo (à esquerda), $\mathbb{R}$ é um $\mathbb{Z}$-módulo (à esquerda) etc.

(3) Sejam G um grupo e $\mathcal{P}(G) = \{A \mid A \subseteq G\}$ o conjunto das partes de G.

Consideremos em $\mathcal{P}(G)$ a operação diferença simétrica, que denotamos por $+$, isto é, $A+B = (A-B)\cup(B-A) = (A\cap B^c)\cup(A^c\cap B)$, ou ainda, $A+B = (A\cup B)-(A\cap B) = (A\cup B)\cap(A\cap B)^c$, para todos $A, B \in \mathcal{P}(G)$. Observemos que tal operação faz de $\mathcal{P}(G)$ um grupo abeliano e portanto um $\mathbb{Z}$-módulo (à esquerda).

Agora, considerando a multiplicação (à esquerda) por escalar

$$\mu : \mathbb{Z}_2 \times \mathcal{P}(G) \longrightarrow \mathcal{P}(G)$$

tal que, $\overline{0}.A := \varnothing$ e $\overline{1}.A := A$, para todo $A \in \mathcal{P}(G)$, obtemos para $\mathcal{P}(G)$ uma estrutura de $\mathbb{Z}_2$-módulo (à esquerda). Notemos que todo elemento de $\mathcal{P}(G)$ tem ordem 2 e assim "$-B = B$". Observemos ainda que em geral a notação $A - B$ *não* indica $A + (-B)$ $(= A + B)$, mas sim a diferença entre os conjuntos.

Definição A.1.2. Um subconjunto N de um R-módulo (à esquerda) M, diz-se um ***R*-submódulo** de M, ou simplesmente um ***submódulo*** de M, se

(a) N é um subgrupo de M,

(b) N é fechado com relação à multiplicação (à esquerda) por escalares, isto é, para todos $\alpha \in R$ e $n \in N$ tem-se $\alpha n \in N$.

Lema A.1.1. Sejam M um R-módulo (à esquerda) e $\mathfrak{F} = \{N_i \mid i \in I\}$ uma família de submódulos de M. Então, $\bigcap_{i \in I} N_i$ é um submódulo de M.

Seja S um subconjunto arbitrário de um R-módulo (à esquerda) M. Temos que S está contido em pelo menos um submódulo de M, a saber, o próprio M. Pelo lema anterior, temos que a intersecção de todos os submódulos de M contendo S é um submódulo de M. Denotamos tal submódulo por N, isto é, $N = \bigcap_{i \in I} N_i$, onde N_i é um submódulo de M tal que $S \subseteq N_i$, para todo $i \in I$. Este submódulo N é chamado o ***submódulo de M gerado por S***. No caso em que $N = M$, dizemos que S é um ***conjunto de geradores de M*** e que M é ***gerado*** por S.

Definição A.1.3. Seja S um subconjunto de um R-módulo (à esquerda) M. Um elemento m do R-módulo (à esquerda) M é uma ***combinação linear de elementos de S*** se, e somente se, existe um número finito de elementos $m_1, \ldots, m_k \in S$ tais que

$$m = \sum_{i=1}^{k} \alpha_i m_i, \text{ com } \alpha_i \in R,\ i = 1, \ldots, k.$$

Definição A.1.4. Consideremos M e N dois R-módulos à esquerda (à direita) arbitrários. Uma aplicação $f : M \longrightarrow N$ diz-se um ***homomorfismo de R-módulos***, se

(a) $f(m+m') = f(m) + f(m')$ e

(b) $f(\alpha m) = \alpha f(m) \quad \big(f(m\alpha) = f(m)\alpha\big)$,

para todos $\alpha \in R$ e $m, m' \in M$.

Exemplo A.1.2. A aplicação de R-módulos $f : M \longrightarrow N$, dada por $f(m) = 0$, para todo $m \in M$ é um homomorfismo de R-módulos, chamado ***homomorfismo nulo*** ou ***trivial***.

Definição A.1.5. Um homomorfismo de R-módulos $f : M \longrightarrow N$ diz-se um ***monomorfismo*** (***epimorfismo***) se f for injetor (sobrejetor). Se f for bijetivo, então dizemos que f é um ***isomorfismo*** e que os R-módulos M e N são ***isomorfos*** ($M \simeq N$).

Proposição A.1.1. Sejam $f : M \longrightarrow M'$ e $g : M' \longrightarrow M''$ homomorfismos de R-módulos. Então, $h = g \circ f : M \longrightarrow M''$ é um homomorfismo de R-módulos e,

(a) se h é um monomorfismo, então f também o é,

(b) se h é um epimorfismo, então g também o é.

Definição A.1.6. Consideremos a seqüência (finita ou infinita) de R-módulos e homomorfismos

$$\cdots \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow \cdots \tag{A.1}$$

Esta seqüência é denominada ***semi-exata*** $\big($***exata***$\big)$ ***em*** $\boldsymbol{Y}$ se

$$Im(f) \subseteq Ker(g) \quad \big(Im(f) = Ker(g)\big).$$

Se a seqüência (A.1) é semi-exata (exata) em todo módulo, exceto nos módulos extremos (caso existam), dizemos que a seqüência (A.1) é uma ***seqüência semi-exata (exata)*** .

Definição A.1.7. Uma seqüência exata de homomorfismos de R-módulos, da forma

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$$

é denominada ***seqüência exata curta***.

Exemplo A.1.3. Sejam N um submódulo de um R-módulo M e $\dfrac{M}{N}$ o R-módulo quociente. Consideremos a inclusão $i : N \longrightarrow M$ e a projeção $p : M \longrightarrow \dfrac{M}{N}$ tal que $p(m) = \overline{m} = m + N$. Temos que, $Im(i) = N = Ker(p)$. Assim, obtemos a seguinte seqüência exata curta

$$0 \longrightarrow N \xrightarrow{i} M \xrightarrow{p} \frac{M}{N} \longrightarrow 0 \quad .$$

A.2 Complexos de (Co)cadeias

Definição A.2.1. Uma seqüência semi-exata de R-módulos e homomorfismos da forma (decrescente)

$$C : \cdots \longrightarrow C_{n+1} \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \longrightarrow \cdots \ ,$$

com $n \in \mathbb{Z}$, é chamada ***complexo de cadeias***. Os homomorfismos $\partial_n : C_n \longrightarrow C_{n-1}$ são denominados ***operadores bordos***. Tal complexo é usualmente denotado por $\boldsymbol{C = (C_n, \partial_n)_{n\in\mathbf{Z}}}$ ou simplesmente $\boldsymbol{C = (C_n)_{n\in\mathbf{Z}}}$. O quociente $H_n(C) := \dfrac{Ker(\partial_n)}{Im(\partial_{n+1})}$ é chamado ***módulo de homologia n-dimensional de C*** e a coleção $H_*(C) = \{H_n(C)\}_{n\in\mathbb{Z}}$ é denominada ***homologia*** de C.

Exemplo A.2.1. Consideremos o seguinte complexo de cadeias

$$C : \cdots \longrightarrow C_3 = \mathbb{Z} \xrightarrow{\partial_3} C_2 = \mathbb{Z} \xrightarrow{\partial_2} C_1 = \mathbb{Z} \xrightarrow{\partial_1} C_0 = \mathbb{Z} \longrightarrow \cdots \ ,$$

onde

$$\partial_n(x) = \begin{cases} 0, & \text{se } n \text{ é par;} \\ kx, & \text{se } n \text{ é ímpar,} \end{cases}$$

para todos $x \in \mathbb{Z}$ e $k \in \mathbb{Z}$, $k > 1$ (fixo). Assim,

- se n é ímpar, então $Ker(\partial_n) = \{0\}$ e $Im(\partial_{n+1}) = \{0\}$ e daí,

$$H_n(C) = \{0\};$$

- se n é par, então $Ker(\partial_n) = \mathbb{Z}$ e $Im(\partial_{n+1}) = k\mathbb{Z}$. Portanto,

$$H_n(C) = \frac{\mathbb{Z}}{k\mathbb{Z}} \simeq \mathbb{Z}_k.$$

Definição A.2.2. Uma seqüência semi-exata de R-módulos e homomorfismos da forma (crescente)

$$D : \cdots \longrightarrow D^{n-1} \xrightarrow{\delta^{n-1}} D^n \xrightarrow{\delta^n} D^{n+1} \longrightarrow \cdots$$

é chamada ***complexo de cocadeias***. Neste caso, os homomorfismos $\delta^n : D^n \longrightarrow D^{n+1}$ são denominados ***operadores cobordos***. Notação: $\boldsymbol{D = (D^n, \delta^n)_{n\in\mathbf{Z}}}$ ou simplesmente $\boldsymbol{D = (D^n)_{n\in\mathbf{Z}}}$. O quociente $H^n(D) := \dfrac{Ker(\delta^n)}{Im(\delta^{n-1})}$ é chamado ***módulo de cohomologia n-dimensional de D*** e a coleção $H^*(D) = \{H^n(D)\}_{n\in\mathbb{Z}}$ é chamada ***cohomologia*** de D.

Observação A.2.1.

(1) Observemos que a única diferença entre os complexos de cadeias e cocadeias, é a indexação por inteiros, ou seja, um complexo de cadeias é indexado por inteiros na ordem decrescente enquanto que um complexo de cocadeias é indexado por inteiros na ordem crescente.

(2) Um complexo de cadeias pode ser visto como um complexo de cocadeias e reciprocamente. Mais precisamente, dados um complexo de cadeias $C = (C_n)_{n\in\mathbb{Z}}$ e um complexo de cocadeias $D = (D^n)_{n\in\mathbb{Z}}$. Então, $\boldsymbol{C}$=$(\boldsymbol{C^n}{:=} C_{-n})_{n\in\mathbb{Z}}$ e $\boldsymbol{D}$=$(\boldsymbol{D_n}{:=} D^{-n})_{n\in\mathbb{Z}}$ serão complexos de cocadeias e cadeias, respectivamente.

(3) Como a cohomologia de um grupo é a cohomologia de um complexo de cocadeias especial, nos dedicaremos mais ao estudo de resultados para complexos de cocadeias. Resultados similares aos apresentados, também são válidos para complexos de cadeias.

(4) Dado um complexo de cocadeias C, denotamos $Ker\,(\delta^n)$ por $\boldsymbol{Z^n(C)}$ e $Im\,(\delta^{n-1})$ por $\boldsymbol{B^n(C)}$.

Definição A.2.3. Sejam

$$C : \cdots \longrightarrow C^{n-1} \xrightarrow{\delta^{n-1}} C^n \xrightarrow{\delta^n} C^{n+1} \longrightarrow \cdots \quad \text{e}$$
$$D : \cdots \longrightarrow D^{n-1} \xrightarrow{\widetilde{\delta}^{n-1}} D^n \xrightarrow{\widetilde{\delta}^n} D^{n+1} \longrightarrow \cdots \quad ,$$

complexos de cocadeias. Um ***homomorfismo de grau* 0** ou ***aplicação de cocadeias*** $f : C \longrightarrow D$ é uma família de homomorfismos de R-módulos $f = \{f^n : C^n \longrightarrow D^n, n \in \mathbb{Z}\}$, tais que $\widetilde{\delta}^n \circ f^n = f^{n+1} \circ \delta^n$, para todo $n \in \mathbb{Z}$.

Exemplo A.2.2.

(1) Se C é um complexo de cocadeias, a aplicação $id : C \longrightarrow C$, dada pela família

$$id = \{id^n : C^n \longrightarrow C^n, n \in \mathbb{Z}\},$$

de homomorfismos identidade id^n dos módulos C^n, isto é, $id^n(x) = x$, para todo $x \in C^n$ é uma aplicação de cocadeias, denominada ***homomorfismo identidade*** e denotada por $id : C \longrightarrow C$.

(2) Dados C e D complexos de cocadeias, a aplicação $f : C \longrightarrow D$, tal que $f^n : C^n \longrightarrow D^n$ é o homomorfismo trivial para todo $n \in \mathbb{Z}$, é uma aplicação de cocadeias, denominada ***homomorfismo trivial*** do complexo C no complexo D. Denotamos tal homomorfismo por $\boldsymbol{f = 0}$.

Proposição A.2.1. Seja $f : C \longrightarrow D$ uma aplicação de cocadeias. Então, $f^n\,[Z^n(C)] \subseteq Z^n(D)$ e $f^n\,[B^n(C)] \subseteq B^n(D)$.

Definição A.2.4. Dada uma aplicação de cocadeias $f = (f^n) : C \longrightarrow D$, temos induzido, para cada $n \in \mathbb{Z}$, um homomorfismo

$$H^n(f) : H^n(C) \longrightarrow H^n(D),$$

tal que a cada $\overline{x} = x + B^n(C) \in H^n(C)$ associa $H^n(f)(\overline{x}) := f^n(x) + B^n(D)$. Tal homomorfismo é denominado ***homomorfismo induzido n-dimensional de f***.

Proposição A.2.2.

(a) Consideremos $id : C \longrightarrow C$ o homomorfismo identidade. Então, para cada $n \in \mathbb{Z}$, o homomorfismo induzido $H^n(id)$ é o homomorfismo identidade do módulo $H^n(C)$, isto é, $H^n(id) = id_{H^n(C)}$.

(b) Sejam C e D complexos de cocadeias. Se $f : C \longrightarrow D$ é o homomorfismo trivial, então $H^n(f) : H^n(C) \longrightarrow H^n(D)$ é também um homomorfismo trivial (de grupos), para todo $n \in \mathbb{Z}$.

(c) Se $f : C \longrightarrow D$ e $g : D \longrightarrow E$ são homomorfismos de complexos de cocadeias, então $H^n(g \circ f) = H^n(g) \circ H^n(f)$, para todo $n \in \mathbb{Z}$.

Definição A.2.5. Sejam $C = \left(C^n, \delta^n\right)_{n\in\mathbb{Z}}$ e $D = \left(D^n, \widetilde{\delta}^n\right)_{n\in\mathbb{Z}}$ complexos de cocadeias e $f, g : C \longrightarrow D$ aplicações de cocadeias. Dizemos que f e g são ***homotópicas*** se, e somente se, existe uma família de homomorfismo (de grau -1) $h = \{h^n : C^n \longrightarrow D^{n-1}, n \in \mathbb{Z}\}$ tal que

$$\widetilde{\delta}^{n-1} \circ h^n + h^{n+1} \circ \delta^n = f^n - g^n,$$

para todo $n \in \mathbb{Z}$.

Para uma melhor compreensão da definição anterior, vejamos o diagrama seguinte:

$$\begin{array}{ccccccccccc}
\cdots & \longrightarrow & C^{n-1} & \xrightarrow{\delta^{n-1}} & C^n & \xrightarrow{\delta^n} & C^{n+1} & \xrightarrow{\delta^{n+1}} & C^{n+2} & \longrightarrow & \cdots \\
 & & & \swarrow^{h^n} & \downarrow^{f^n} & & \downarrow^{g^n} & \swarrow^{h^{n+1}} & & & \\
\cdots & \longrightarrow & D^{n-1} & \xrightarrow[\widetilde{\delta}^{n-1}]{} & D^n & \xrightarrow[\widetilde{\delta}^n]{} & D^{n+1} & \xrightarrow[\widetilde{\delta}^{n+1}]{} & D^{n+2} & \longrightarrow & \cdots
\end{array}$$

A família h é chamada ***homotopia*** (ou ***homotopia de cocadeias***), entre as aplicações de cocadeias f e g e denotamos por $\boldsymbol{f \sim g}$.

Proposição A.2.3. Sejam $f, g : C \longrightarrow D$ aplicações de cocadeias. Se f é homotópica a g, então $H^n(f) = H^n(g)$, para todo $n \in \mathbb{Z}$.

Definição A.2.6. Dizemos que um complexo de cocadeias C é ***contrátil*** se existe uma homotopia de cocadeias entre id_C e a aplicação nula. Tal homotopia é denominada ***homotopia contrátil***.

Definição A.2.7. Uma aplicação de cocadeias $f : C \longrightarrow D$ é denominada uma ***equivalência de homotopia*** se existe uma aplicação de cocadeias $g : D \longrightarrow C$ tal que $g \circ f \sim id_C$ e $f \circ g \sim id_D$. Neste caso, dizemos que C e D são ***homotopicamente equivalentes***.

Proposição A.2.4. Se C e D são complexos de cocadeias homotopicamente equivalentes, então

$$H^n(C) \simeq H^n(D),$$

para todo $n \in \mathbb{Z}$.

Demonstração.

Se $f : C \longrightarrow D$ é uma equivalência de homotopia e $g : D \longrightarrow C$ é tal que $g \circ f \sim id_C$ e $f \circ g \sim id_D$, então pela Proposição A.2.2 *(a)* e *(c)*, obtemos que

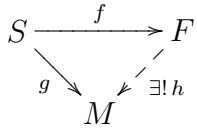
$$H^n(g) \circ H^n(f) = H^n(g \circ f) = H^n(id_C) = id_{H^n(C)} \text{ e}$$

$$H^n(f) \circ H^n(g) = H^n(f \circ g) = H^n(id_D) = id_{H^n(D)}.$$

Portanto, $H^n(f)$ é um isomorfismo, para todo $n \in \mathbb{Z}$ e $\left[H^n(f)\right]^{-1} = H^n(g)$. ■

A.3 Módulos Livres e Projetivos

Definição A.3.1. Seja S um conjunto qualquer. Um par $\boldsymbol{(F, f)}$, onde F é um R-módulo e f é uma aplicação do conjunto S no R-módulo F, é chamado ***R-módulo livre sobre S*** se para toda aplicação $g : S \longrightarrow M$, onde M é um R-módulo, existir um único homomorfismo $h : F \longrightarrow M$ tal que a relação de comutatividade $h \circ f = g$ é válida no seguinte triângulo:



Exemplo A.3.1.

(1) Considerando S um conjunto unitário, temos que R é um R-módulo livre sobre S.

De fato, sejam $S = \{s\}$ e $f : S \longrightarrow R$ dada por $f(s) = 1$. Qualquer que seja

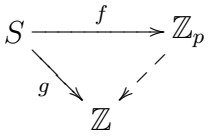
$$\begin{aligned} g : S = \{s\} &\longrightarrow M \\ s &\longmapsto g(s) = x_0 \quad (x_0 \text{ fixo}), \end{aligned}$$

basta definir $h : R \longrightarrow M$ tal que $h(1) = x_0$ e $h(\alpha) := \alpha.h(1) = \alpha x_0$, com $\alpha \in R$. Daí, $(h \circ f)(s) = h[f(s)] = h(1) = x_0 = g(s)$, ou seja, $h \circ f = g$, e tal h é único.

(2) $\mathbb{Z}_p$, $p \in \mathbb{Z}$, $p \geqslant 2$ é um $\mathbb{Z}_p$-módulo livre, no entanto não é $\mathbb{Z}$-módulo livre.

O fato de $\mathbb{Z}_p$ ser um $\mathbb{Z}_p$-módulo livre (sobre um conjunto unitário S) segue diretamente do exemplo anterior.

Agora, temos que $\mathbb{Z}_p$ não é um $\mathbb{Z}$-módulo livre, pois caso contrário, existiria S e f satisfazendo a Definição A.3.1, para $F = \mathbb{Z}_p$. Tomemos $M = \mathbb{Z}$ e consideremos o diagrama



Se $f(s) = \overline{0}$, para todo $s \in S$, basta considerarmos $g : S \longrightarrow \mathbb{Z}$, com $g(s) \neq 0$ para algum $s \in S$. Desta forma, não existe $h : \mathbb{Z}_p \longrightarrow \mathbb{Z}$ tal que $h \circ f = g$.

Agora, se $f(s) = \overline{a} \neq \overline{0}$, para algum $s \in S$, basta tomarmos a aplicação constante $g : S \longrightarrow \mathbb{Z}$, com $g(s) = n_0 \neq 0$ (n_0 fixo), para todo $s \in S$. Também não existe $h : \mathbb{Z}_p \longrightarrow \mathbb{Z}$ tal que $h \circ f = g$, pois se existisse tal h, teríamos

$$0 = h(\overline{0}) = h(p.\overline{a}) = p.h(\overline{a}) = p.h[f(s)] = p.g(s) = p.n_0 \neq 0,$$

o que é uma contradição.

Portanto, temos que $\mathbb{Z}_p$ não é $\mathbb{Z}$-módulo livre.

Teorema A.3.1. Se o par (F, f) é um R-módulo livre sobre um conjunto S, então f é injetiva e a imagem $f(S)$ gera o módulo F.

Teorema A.3.2. (**Unicidade**) Se (F, f) e (F', f') são R-módulos livres sobre um mesmo conjunto S, então existe um único isomorfismo $\kappa : F \longrightarrow F'$ tal que $\kappa \circ f = f'$.

Teorema A.3.3. (**Existência**) Dado um conjunto S, sempre existe um R-módulo livre sobre S.

Segue dos resultados anteriores, que todo conjunto S determina essencialmente um único R-módulo livre (F, f). Como a aplicação $f : S \longrightarrow F$ é injetiva, podemos identificar S com sua imagem $f(S)$. Daí, S torna-se um subconjunto de F que *gera* o R-módulo F e podemos considerar $f = i : S \longrightarrow F$ como a aplicação inclusão. Assim, se F é livre sobre S, toda aplicação $g : S \longrightarrow M$, onde M é um R-módulo arbitrário, se estende a um único homomorfismo $h : F \longrightarrow M$. Este módulo F sobre R será referido como o ***módulo livre sobre R gerado por S***.

Definição A.3.2. Um R-módulo M é denominado ***livre*** se M é isomorfo a um módulo livre sobre S, para algum S.

Proposição A.3.1. Se F é R-módulo livre sobre S, então F é isomorfo a uma soma direta da família $\mathfrak{F} = \{X_s \mid s \in S\}$, onde X_s é o anel R considerado como um módulo sobre si mesmo, isto é, $F \simeq \sum_{s \in S} X_s$.

Demonstração. [13], Corolário 4.4. ■

Teorema A.3.4. Todo R-módulo (à esquerda) é isomorfo a um quociente de um R-módulo livre.

Demonstração.

Seja M um R-módulo (à esquerda) arbitrário. Tomemos S um subconjunto de M que gera M e consideremos o R-módulo livre F gerado por S. Daí, a aplicação inclusão $i : S \longrightarrow M$ se estende a um homomorfismo $h : F \longrightarrow M$.

Como $S = i(S) = h(S) \subseteq h(F) \subseteq M$ e S gera M, temos que $h(F) = M$. Logo, h é um epimorfismo.

Portanto, pelo Teorema do Isomorfismo, temos que $M \simeq \dfrac{F}{Ker(h)}$. ■

Definição A.3.3. Dizemos que um R-módulo (à esquerda) P é ***projetivo*** se, para todo homomorfismo $f : P \longrightarrow Y$ e todo epimorfismo $g : X \longrightarrow Y$ de R-módulos (à esquerda), existir um homomorfismo $h : P \longrightarrow X$ tal que $g \circ h = f$, no seguinte diagrama

$$\begin{array}{ccccc} & & P & & \\ & \overset{h}{\swarrow} & \downarrow{\scriptstyle f} & & \\ X & \xrightarrow[g]{} & Y & \longrightarrow & 0 \ . \end{array}$$

Proposição A.3.2. Todo R-módulo livre é projetivo.

Demonstração.

Seja F um R-módulo livre arbitrário, gerado por um conjunto $S \subseteq F$. Consideremos um homomorfismo $f : F \longrightarrow Y$ e um epimorfismo $g : X \longrightarrow Y$ de R-módulos (à esquerda), como no diagrama:

$$\begin{array}{ccccc} & & F & & \\ & & \downarrow{\scriptstyle f} & & \\ X & \xrightarrow[g]{} & Y & \longrightarrow & 0 \end{array}$$

Como g é um epimorfismo e $f(s) \in Y$, para todo $s \in S$, temos que existe $x_s \in X$ tal que $g(x_s) = f(s)$. Então, definamos $k : S \longrightarrow X$ tal que $k(s) = x_s$.

Logo, $g[k(s)] = f(s)$. Como F é um R-módulo livre sobre $S \subseteq F$, temos que k se estende a um único homomorfismo $h : F \longrightarrow X$.

$$\begin{array}{ccccc} S & \xrightarrow{i} & F & & \\ {\scriptstyle k}\downarrow & \overset{h}{\swarrow} & \downarrow{\scriptstyle f} & & \\ X & \xrightarrow[g]{} & Y & \longrightarrow & 0 \end{array}$$

Agora, seja $u \in F$. Assim, temos que $u = \sum_{j=1}^{r} \alpha_j s_j$, com $\alpha_j \in R$ e $s_j \in S$, $j = 1, \ldots, r$. Então,

$$g[h(u)] = \sum_{j=1}^{r} \alpha_j g[h(s_j)] = \sum_{j=1}^{r} \alpha_j g[k(s_j)] = \sum_{j=1}^{r} \alpha_j f(s_j) = f\left(\sum_{j=1}^{r} \alpha_j s_j\right) = f(u),$$

para todo $u \in F$. Logo, $g \circ h = f$ e assim temos que F é projetivo. ■

Observação A.3.1. A recíproca da proposição anterior, nem sempre é verdadeira. Por exemplo, $\mathbb{Z}$ é $\mathbb{Z} \oplus \mathbb{Z}$ projetivo, mas não é $\mathbb{Z} \oplus \mathbb{Z}$ livre.

A.4 Posto (Rank) de Módulos Livres

Sabemos que se M é um módulo gerado por S, então todo elemento de M é uma combinação linear (não necessariamente única) de elementos de S. Veremos que, quando M é módulo livre sobre S, a *unicidade* ocorre.

Definição A.4.1. Consideremos $\mathfrak{F} = \{m_1, m_2, \ldots, m_t\}$ uma família finita de elementos de um R-módulo M (à esquerda).

(a) Dizemos que $\mathfrak{F}$ é ***linearmente dependente (l.d.)***, quando existem escalares $\alpha_1, \alpha_2, \ldots, \alpha_t$ em R, não todos nulos, tais que

$$\alpha_1 m_1 + \alpha_2 m_2 + \cdots + \alpha_t m_t = 0 \ .$$

(b) Dizemos que $\mathfrak{F}$ é ***linearmente independente (l.i.)***, quando os únicos escalares $\alpha_1, \alpha_2, \ldots, \alpha_t$, que satisfazem

$$\alpha_1 m_1 + \alpha_2 m_2 + \cdots + \alpha_t m_t = 0 \ ,$$

são todos nulos, isto é, $\alpha_1 = \alpha_2 = \cdots = \alpha_t = 0$.

Definição A.4.2. Seja $(m_i)_{i \in I}$ uma família arbitrária de elementos de um R-módulo M.

(a) $(m_i)_{i \in I}$ é ***linearmente dependente*** quando existir uma subfamília finita linearmente dependente.

(b) $(m_i)_{i\in I}$ é ***linearmente independente*** quando existir uma subfamília finita linearmente independente.

Proposição A.4.1. Um R-módulo M é livre sobre um conjunto $S = \{m_i \in I\} \subseteq M$ se, e somente se,

(a) a família $(m_i)_{i\in I}$ é linearmente independente.

(b) todo elemento $m \in M$ é combinação linear da família $(m_i)_{i\in I}$.

Qualquer família $(m_i)_{i\in I}$ de elementos de M que satisfaz as condições *(a)* e *(b)* anteriores é chamada de ***base*** (livre) do R-módulo livre M. Ou equivalentemente,

(c) todo elemento de M pode ser representado unicamente como uma soma $\sum \alpha_{ij} m_{ij}$, com $\alpha_{ij} \in R$ quase todos nulos, ou seja, exceto um número finito.

Demonstração. [16], Capítulo I, Proposição 5.2. ■

Observação A.4.1. Uma base de um R-módulo livre M pode ser infinita.

Exemplo A.4.1.

(1) Se V é um espaço vetorial (sobre um corpo $\mathbb{K}$) e $\mathcal{B}$ é uma base de V, então V é um $\mathbb{K}$-módulo livre e $\mathcal{B}$ é uma base (livre) de V.

(2) Se R é um anel e n é um inteiro, $n \geqslant 1$, o produto cartesiano R^n é um R-módulo livre. Uma base para R^n é dada por

$$S = \{e_1 = (1, 0, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots, 0), \ldots, e_n = (0, 0, 0, \ldots, 1)\}.$$

(3) Mais geralmente, se R é um anel e I é um conjunto qualquer, consideremos o submódulo $R^{(I)}$ de R^I de todas as aplicações $f : I \longrightarrow R$ tais que

o conjunto $\{i \in I \mid f(i) \neq 0\}$ é finito. Temos que $R^{(I)}$ é um R-módulo livre, tendo por base S, a família $(e_i)_{i\in I}$ definida por

$$e_i(j) = \begin{cases} 1, & \text{se } i = j; \\ 0, & \text{se } i \neq j. \end{cases}$$

Notemos que, S é infinito se I é um conjunto infinito.

(4) O corpo $\mathbb{Q}$ dos números racionais, considerado como um $\mathbb{Z}$-módulo, não é livre. Observemos que se $r = \frac{a}{b}$ e $s = \frac{c}{d}$ são elementos de $\mathbb{Q}$, então eles são linearmente dependentes. Se $r = 0$, então $1.r + 0.s = 0$. Se $r \neq 0$, então $(bc)r - (ad)s = 0$, com $ad \neq 0$. Segue que se $\mathbb{Q}$ é um $\mathbb{Z}$-módulo livre, uma base livre de $\mathbb{Q}$ tem um único elemento.

Teorema A.4.1. Seja M um R-módulo livre. Se R é anel comutativo com unidade, então todas as bases livres de M tem a mesma cardinalidade.

Demonstração. [20], Teorema 3.4 ou [3], Teorema 2, Capítulo 2. ■

Observação A.4.2.

(1) No enunciado do teorema anterior, as bases não precisam ser necessariamente finitas.

(2) Se R não é comutativo, o resultado anterior pode não ser verdadeiro ([3], p. 25).

(3) Em [17], é apresentada a prova do Teorema A.4.1 apenas para o caso em que R é anel de integridade e M finitamente gerado (Teorema III.2.1).

Definição A.4.3. Seja M um R-módulo livre, com R anel comutativo com unidade. Chamamos de ***posto*** (***rank***) de M e denotamos $rank_R M$ (ou, *posto* M), ao cardinal de uma base livre de M. Se M é o módulo trivial, dizemos que M tem posto 0.

Observação A.4.3.

(1) Se V é um espaço vetorial sobre $\mathbb{K}$, então $rank_{\mathbb{K}}V = dim_{\mathbb{K}}V$.

(2) Pode-se definir posto de um R-módulo livre sempre que o anel R tem "*Número de Base Invariante*" (IBN), ou seja, se para todo R-módulo livre M, duas bases quaisquer de M têm o mesmo cardinal ([20], p. 58).

Proposição A.4.2. Se M é um R-módulo (R anel comutativo) gerado por t elementos, então M é isomorfo a um quociente de um módulo livre de posto t.

Demonstração. [3], Capítulo 2, Proposição 2. ■

Proposição A.4.3. Se numa seqüência exata $0 \longrightarrow N \xrightarrow{f} M \xrightarrow{g} L \longrightarrow 0$ o módulo L é livre, então $M \simeq N \oplus L$. Em particular, se R é um anel comutativo com unidade e $0 \longrightarrow R \longrightarrow M \longrightarrow L \longrightarrow 0$ é uma seqüência exata de R-módulos, com L livre, então $rank_R M = 1 + rank_R L$.

Demonstração. [17], Proposição II.5.5 e Corolário I, p. 65 ou [3], Capítulo 2, Proposição 3. ■

Recordemos que um anel comutativo com unidade R é denominado ***domínio de ideais principais*** se:

(a) R é um domínio, isto é, $R \neq 0$ e se r e s são elementos não nulos de R, então $rs \neq 0$,

(b) todo ideal $\mathcal{I}$ de R é principal, isto é, existe $s \in R$ tal que

$$\mathcal{I} = Rs = \{rs \mid r \in R\} = \{sr \mid r \in R\} = sR.$$

Como exemplos de domínios de ideais principais, temos:

(1) O anel $\mathbb{Z}$ dos inteiros é um domínio de ideais principais.

(2) Todo corpo $\mathbb{K}$ é um domínio de ideais principais.

(3) $\mathbb{K}[x]$ o anel dos polinômios a uma variável com coeficientes em um corpo $\mathbb{K}$ também é um domínio de ideais principais.

Proposição A.4.4. Sejam R um domínio de ideais principais e L um R-módulo livre. Se N é um submódulo de L, então N é livre e $rank_R N \leqslant rank_R L$.

Demonstração. [20], Corolário 4.19. ■

Observação A.4.4. A prova da proposição anterior, no caso em que $rank_R L = n < \infty$ é mais simples e pode ser encontrada em [17], Proposição III.3.1.

A.5 Produto Tensorial

A referência principal para esta seção é [20].

Definição A.5.1. Um ***produto tensorial*** de um R-módulo à direita M e um R-módulo à esquerda N, é um par $\boldsymbol{(T, f)}$, onde T é um grupo abeliano aditivo e f é uma aplicação R-*biaditiva* de $M \times N$ em T, isto é,

(a) $f(m + m', n) = f(m, n) + f(m', n)$,

(b) $f(m, n + n') = f(m, n) + f(m, n')$,

(c) $f(m\alpha, n) = f(m, \alpha n)$,

para todos $m, m' \in M$, $n, n' \in N$ e $\alpha \in R$, e que satisfaz o seguinte problema de diagrama universal: para todo grupo U e para toda aplicação R-biaditiva

$$g : M \times N \longrightarrow U$$

existe um único homomorfismo $h : T \longrightarrow U$ que satisfaz a relação de comutatividade $h \circ f = g$ no seguinte triângulo

$$\begin{array}{ccc} M \times N & \xrightarrow{\ f\ } & T \\ & \searrow^{g} \quad \swarrow_{\exists!\, h} & \\ & U & \end{array}$$

Teorema A.5.1. (**Unicidade**) Se (T, f) e (T', f') são produtos tensoriais dos mesmos R-módulos M e N, então existe um único isomorfismo $\kappa : T \longrightarrow T'$ tal que $\kappa \circ f = f'$.

Demonstração. [20], Teorema 1.3. ■

Teorema A.5.2. (**Existência**) Sejam dois R-módulos arbitrários M e N. Então, existe um produto tensorial de M e N.

Demonstração.

Consiste essencialmente em mostrar que o grupo abeliano $T := \dfrac{F}{L}$, onde F é o grupo livre ($\mathbb{Z}$-módulo livre) que tem por base o conjunto $M \times N$ e L é o subgrupo gerado pelos elementos dos três tipos:

$$(m+m', n)-(m, n)-(m', n);\ (m, n+n')-(m, n)-(m, n');\ (m\alpha, n)-(m, \alpha n),$$

juntamente com a aplicação

$$\begin{aligned} f :\ M \times N &\longrightarrow \frac{F}{L} \\ (m, n) &\longmapsto m \otimes n := (m, n) + L \end{aligned}$$

satisfaz as condições da definição de produto tensorial ([20], Teorema 1.4). ■

Segue dos dois últimos resultados, que todo par de R-módulos M (à direita) e N (à esquerda) determina essencialmente um único produto tensorial (T, f). O R-módulo T é usualmente denotado por

$$\boldsymbol{M \otimes_R N}$$

e é chamado ***produto tensorial dos R-módulos*** M e N.

A aplicação $f : M \times N \longrightarrow M \otimes_R N$ é denominada ***aplicação tensorial***.

Dados $m \in M$ e $n \in N$, o elemento $m \otimes n := f(m, n) \in M \otimes_R N$ é denominado ***produto tensorial sobre R dos elementos m e n***. Como $f(M \times N)$ gera o grupo abeliano $M \otimes_R N$, temos que todo elemento t de $M \otimes_R N$ pode ser escrito na forma

$$t = \sum_{j=1}^{k} m_j \otimes n_j\ ,$$

onde $m_j \in M$ e $n_j \in N$, $j = 1, \ldots, k$.

Obviamente estas expressões dos elementos de $M \otimes_R N$ não são únicas, pois (da biaditividade da f) segue que

$$(m + m') \otimes n = (m \otimes n) + (m' \otimes n);\ m \otimes (n + n') = (m \otimes n) + (m \otimes n') \text{ e}$$

$$(m\alpha \otimes n) = m \otimes \alpha n,$$

para todos $m, m' \in M$, $n, n' \in N$ e $\alpha \in R$.

Em particular, tomando $\alpha = 0$ ou $\alpha = -1$, obtemos que

$$0 \otimes n = 0 = m \otimes 0 \ \text{ e } \ (-m) \otimes n = -(m \otimes n) = m \otimes (-n).$$

Observação A.5.1. ***(Produto tensorial sobre anéis comutativos)***

Quando o anel R é comutativo, sabemos (Observação A.1.1 *(3)*) que todo R-módulo à esquerda M tem uma estrutura natural de R-módulo à direita (e reciprocamente). Logo, neste caso o produto tensorial $M \otimes_R N$ pode ser definido considerando M e N como R-módulos à esquerda.

Ainda, $f : M \times N \longrightarrow T = M \otimes_R N$ será uma aplicação bilinear e, $T = M \otimes_R N$ será um R-módulo com $\alpha(m \otimes n) = \alpha m \otimes n = m \otimes \alpha n$, para todos $m \in M$, $n \in N$ e $\alpha \in R$ ([13], Capítulo I, Seção 7).

Proposição A.5.1. Seja R um anel (com unidade) com as estruturas naturais de R-módulos à esquerda e à direita (Exemplo A.1.1 *(1)*). Se M é um R-módulo à esquerda e N um R-módulo à direita, então

$$N \otimes_R R \simeq N \ \text{ e } \ R \otimes_R M \simeq M.$$

Demonstração. [20], Teorema 1.12. Notemos que em $R \otimes_R M$, $\alpha \otimes m = 1\alpha \otimes m = 1 \otimes \alpha m$ e o isomorfismo $R \otimes_R M \longrightarrow M$ será dado por $1 \otimes m' \longrightarrow m'$. Similarmente para N. ■

Teorema A.5.3. Sejam $f_1 : M \longrightarrow M'$ um homomorfismo de R-módulos à direita e $f_2 : N \longrightarrow N'$ um homomorfismo de R-módulos à esquerda. Existe um único homomorfismo (de grupos) $M \otimes_R N \longrightarrow M' \otimes_R N'$, com $m \otimes n \longmapsto f_1(m) \otimes f_2(n)$.

Demonstração. [20], Teorema 1.5. ■

Definição A.5.2. A aplicação $M \otimes_R N \longrightarrow M' \otimes_R N'$ que associa $m \otimes n$ a $f_1(m) \otimes f_2(n)$ é denotada por $\boldsymbol{f_1 \otimes f_2}$ e é chamada ***produto tensorial dos homomorfismos*** $\boldsymbol{f_1}$ ***e*** $\boldsymbol{f_2}$.

Proposição A.5.2.

(a) Se $id_M : M \longrightarrow M$ e $id_N : N \longrightarrow N$ são os homomorfismos idênticos de R-módulos, então $id_M \otimes id_N = id_{M \otimes_R N} : M \otimes_R N \longrightarrow M \otimes_R N$.

(b) Se $M \xrightarrow{f_1} M' \xrightarrow{g_1} M''$ são homomorfismos de R-módulos à direita e $N \xrightarrow{f_2} N' \xrightarrow{g_2} N''$ são homomorfismos de R-módulos à esquerda, então

$$(g_1 \circ f_1) \otimes (g_2 \circ f_2) = (g_1 \otimes g_2) \circ (f_1 \otimes f_2).$$

Teorema A.5.4. Sejam M um R-módulo à direita e $\{N_\nu \mid \nu \in J\}$ uma família de R-módulos à esquerda. Então, a aplicação

$$\begin{aligned} \theta : \ M \otimes_R \sum_{\nu \in J} N_\nu \ &\longrightarrow \ \sum_{\nu \in J} (M \otimes_R N_\nu) \\ m \otimes (n_\nu) \ &\longmapsto \ (m \otimes n_\nu) \end{aligned}$$

é um isomorfismo. Existe um isomorfismo similar se a soma direta é na primeira variável.

Demonstração. [20], Teorema 2.8. ■

Teorema A.5.5. Se N é um R-módulo à esquerda e

$$X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$$

é uma seqüência exata de R-módulos à direita, então a seqüência (de grupos abelianos)

$$X \otimes_R N \xrightarrow{f \otimes id_N} Y \otimes_R N \xrightarrow{g \otimes id_N} Z \otimes_R N \longrightarrow 0$$

também é exata (ou seja, o "funtor" $\_\_ \otimes_R N$ é exato à direita. Similarmente $M \otimes_R \_\_$ é exato à direita).

Demonstração. [20], Teorema 2.10. ■

A.6 O Grupo de Homomorfismos de R-módulos

Sejam M e N dois R-módulos (à esquerda) arbitrários e o seguinte conjunto

$$Hom_R(M, N)$$

de todos os homomorfismos do R-módulo M no R-módulo N.

Consideremos em $Hom_R(M, N)$ a operação de adição $(+)$, tal que para todos $\phi, \psi \in Hom_R(M, N)$ é associado o homomorfismo

$$\phi + \psi : M \longrightarrow N$$

definido por $(\phi + \psi)(m) = \phi(m) + \psi(m)$, para todo $m \in M$. Com esta operação, $Hom_R(M, N)$ torna-se um grupo abeliano e assim podemos vê-lo como um $\mathbb{Z}$-módulo (à esquerda).

Agora, para todos $\alpha \in R$ e $\phi \in Hom_R(M, N)$, consideremos a aplicação

$$\alpha\phi : M \longrightarrow N$$

dada por $(\alpha\phi)(m) = \alpha[\phi(m)]$, para todo $m \in M$. Se R for um ***anel comutativo***, então podemos verificar que $\alpha\phi$ é um homomorfismo e assim definimos

$$\begin{aligned} \mu : \ R \times Hom_R(M, N) &\longrightarrow \ Hom_R(M, N) \\ (\alpha, \phi) &\longmapsto \ \alpha\phi \end{aligned}$$

de maneira que $Hom_R(M, N)$ seja visto como um R-módulo (à esquerda).

Definição A.6.1. O grupo abeliano $Hom_R(M, N)$ é chamado ***grupo dos homomorfismos de R-módulos*** e se R é um anel comutativo com unidade, o R-módulo (à esquerda) $Hom_R(M, N)$ é denominado ***módulo de homomorfismos*** do módulo M no módulo N.

Observação A.6.1. Caso R não seja comutativo, podemos garantir apenas que $Hom_R(M, N)$ é um grupo abeliano ($\mathbb{Z}$-módulo).

A prova dos resultados seguintes podem ser vistos em [13], lembrando que em nosso contexto, $Hom_R(M, N)$ pode ser apenas grupo abeliano, ou em [20] e [16].

Proposição A.6.1. Se M é um R-módulo (à esquerda) qualquer, então a aplicação

$$\begin{aligned} \rho : \ Hom_R(R, M) &\longrightarrow M \\ \phi &\longmapsto \phi(1) \end{aligned}$$

é um isomorfismo.

Agora, sejam $f : M' \longrightarrow M$ e $g : N \longrightarrow N'$ homomorfismos de R-módulos (à esquerda) dados arbitrariamente, e consideremos (os grupos abelianos) $Hom_R(M, N)$ e $Hom_R(M', N')$. Definamos a aplicação

$$\begin{aligned} h : \ Hom_R(M, N) &\longrightarrow Hom_R(M', N') \\ \phi &\longmapsto h(\phi) = g \circ \phi \circ f \ , \end{aligned}$$

para todo $\phi \in Hom_R(M, N)$.

O diagrama abaixo nos ajuda a compreender melhor a definição de h:

$$\begin{array}{ccc} M & \xrightarrow{\phi} & N \\ {\scriptstyle f}\uparrow & & \downarrow{\scriptstyle g} \\ M' & \xrightarrow[h(\phi)]{} & N' \end{array}$$

É fácil ver que h é um homomorfismo. Tal homomorfismo será denotado por $\boldsymbol{Hom(f, g)}$.

Em particular, considerando os homomorfismos identidade $id_M : M \longrightarrow M$ e $id_N : N \longrightarrow N$, temos que
$Hom(f, id_N) : Hom_R(M, N) \longrightarrow Hom_R(M', N)$ é tal que

$$Hom(f, id_N)(\phi) = \phi \circ f$$

e
$Hom(id_M, g) : Hom_R(M, N) \longrightarrow Hom_R(M, N')$ é tal que

$$Hom(id_M, g)(\phi) = g \circ \phi.$$

É usual ainda denotar $\boldsymbol{f^*} := Hom(f, id_N)$ e $\boldsymbol{g_*} := Hom(id_M, g)$.

Proposição A.6.2.

(a) Se $id_M : M \longrightarrow M$ e $id_N : N \longrightarrow N$ são os homomorfismos idênticos, então

$$Hom(id_M, id_N) : Hom_R(M,N) \longrightarrow Hom_R(M,N)$$

é o homomorfismo idêntico de $Hom_R(M,N)$.

(b) Se $M'' \xrightarrow{f'} M' \xrightarrow{f} M$ e $N \xrightarrow{g} N' \xrightarrow{g'} N''$ são homomorfismos de R-módulos (à esquerda), então

$$Hom(f \circ f', g' \circ g) = Hom(f', g') \circ Hom(f, g).$$

Corolário A.6.1. Se $f : M' \longrightarrow M$ e $g : N \longrightarrow N'$ são isomorfismos de R-módulos (à esquerda), então

$$Hom(f,g) : Hom_R(M,N) \longrightarrow Hom_R(M',N')$$

também é um isomorfismo.

Teorema A.6.1. Se $M = \sum_{\mu \in I} M_\mu$ e $N = \prod_{\nu \in J} N_\nu$, então

$$Hom_R(M,N) \simeq \prod_{(\mu,\nu)} Hom_R(M_\mu, N_\nu).$$

Teorema A.6.2. Sejam M um R-módulo (à esquerda) arbitrário e $X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$ uma seqüência exata de R-módulos (à esquerda), então a seqüência (de grupos abelianos)

$$0 \longrightarrow Hom_R(Z,M) \xrightarrow{g^*} Hom_R(Y,M) \xrightarrow{f^*} Hom_R(X,M)$$

é também exata, ou seja, o "funtor" (contravariante) $Hom_R(\_\_, M)$ é exato à esquerda.

Demonstração. [20], Teorema 2.9 ou [13], Teorema 8.7. ■

A.7 RG-módulos

Embora, em geral, R esteja indicando um anel com unidade, sempre que nos referimos a RG-módulos, R indica $\mathbb{Z}$ ou $\mathbb{Z}_2$.

Definição A.7.1. Consideremos G um grupo multiplicativo, com elemento neutro 1. Seja RG o R-módulo livre gerado pelos elementos de G ($R = \mathbb{Z}$ ou $\mathbb{Z}_2$). Desta maneira, um elemento de RG é expresso unicamente na forma $\sum_{g\in G} \alpha_g.g$, com $\alpha_g \in R$ e $\alpha_g = 0$ para quase todo $g \in G$, ou seja, $\alpha_g = 0$ exceto para um número finito de elementos $g \in G$.

Assim, podemos definir em RG as operações de adição e multiplicação, respectivamente, da seguinte forma

$$\left(\sum_{g\in G} \alpha_g.g\right) + \left(\sum_{g\in G} \beta_g.g\right) = \sum_{g\in G} (\alpha_g + \beta_g).g$$

$$\left(\sum_{g\in G} \alpha_g.g\right) . \left(\sum_{g'\in G} \beta_{g'}.g'\right) = \sum_{g,g'\in G} (\alpha_g.\beta_{g'}).(gg')$$

Desta forma, RG ganha uma estrutura de anel com unidade, e o denominamos ***anel grupo***.

Notação A.7.1.

(1) $1_{RG} = 1_R.1$ (unidade do anel grupo RG).

(2) $1_R.g := g \in RG$.

Exemplo A.7.1. Se $G = \langle t \rangle \simeq \mathbb{Z}_n$, temos que

$$RG = \{\alpha_0 + \alpha_1 t + \cdots + \alpha_{n-1}t^{n-1} \mid \alpha_i \in R, \quad i = 1, \ldots, n-1\}.$$

Observação A.7.1. Dado um grupo G, podemos definir o homomorfismo

$$\begin{aligned} \varepsilon : \ RG &\longrightarrow R \\ g &\longmapsto \varepsilon(g) = 1, \end{aligned}$$

para todo $g \in G$ e estender por linearidade. Temos que, ε é sobrejetor e é denominado ***aplicação aumentação***.

Definição A.7.2. Consideremos G um grupo multiplicativo e M um conjunto não vazio. Uma ***G-ação à esquerda sobre M*** é uma aplicação

$$\begin{aligned} \upsilon : G \times M &\longrightarrow M \\ (g, m) &\longmapsto \upsilon(g, m) := g.m \end{aligned}$$

satisfazendo

(a) $1.m = m$, para todo $m \in M$,

(b) $(gg')m = g(g'm)$, para todos $g, g' \in G$ e $m \in M$.

Se M tiver estrutura de grupo aditivo, para que a G-ação (à esquerda) sobre M preserve tal estrutura, além das condições *(a)* e *(b)* deve ser satisfeita a seguinte condição:

(c) $g(m + m') = gm + gm'$, para todos $g \in G$ e $m, m' \in M$.

Observação A.7.2.

(1) Equivalentemente, uma G-ação (à esquerda) sobre M é um homomorfismo

$$\begin{aligned} \upsilon : G &\longrightarrow B_{ij}(M) \\ g &\longmapsto \upsilon(g) \overset{not.}{=} \upsilon_g \ , \end{aligned}$$

tal que $\upsilon_g(m) := g.m$, onde $B_{ij}(M)$ é o grupo das bijeções de M em M. Neste caso, dizemos que M é um ***G-conjunto***.

(2) Analogamente, podemos definir uma G-ação à direita sobre um conjunto não vazio M, isto é, uma ***G-ação à direita sobre M*** é uma aplicação

$$\begin{aligned} \upsilon : M \times G &\longrightarrow M \\ (m, g) &\longmapsto \upsilon(m, g) := m.g \end{aligned}$$

satisfazendo

(a) $m.1 = m$, para todo $m \in M$,

(b) $m(gg') = (m.g)g'$, para todos $g, g' \in G$ e $m \in M$.

(3) Dada uma G-ação à esquerda sobre um conjunto não vazio M, sempre podemos definir, a partir dessa G-ação, uma G-ação à direita sobre M, para isto, basta considerarmos $m.g := g^{-1}.m$.

Definição A.7.3. Uma G-ação (à esquerda) sobre M é denominada ***livre***, se a seguinte condição é verdadeira:

$$g.m = m, \text{ para algum } m \in M \text{ se, e somente se, } g = 1.$$

Neste caso M é chamado um ***G-conjunto livre***.

Definição A.7.4. Dada uma G-ação (à esquerda) sobre M, dizemos que ela é ***trivial***, se para todo $m \in M$ e todo $g \in G$, tivermos $g.m = m$.

Proposição A.7.1. Sejam G um grupo e M um conjunto não vazio. Então, M é um RG-módulo (à esquerda) se, e somente se, M é um R-módulo (à esquerda) munido de uma G-ação (à esquerda) sobre M. Vale também um resultado similar para RG-módulos à direita.

Demonstração.

Seja M um RG-módulo (à esquerda). Temos que M é um R-módulo (à esquerda), considerando $\alpha.m = (\alpha.1)m$, com $\alpha \in R$ e $m \in M$ e podemos definir uma G-ação (à esquerda) sobre M da seguinte forma

$$g.m = (1_R.g)m.$$

Agora, se M é um R-módulo (à esquerda) e existe uma G-ação (à esquerda) sobre M, então podemos ver M como um RG-módulo (à esquerda) da seguinte maneira:

$$\left(\sum_{g\in G}\alpha_g.g\right).m := \sum_{g\in G}\alpha_g(g.m), \text{ onde } \alpha_g \in R \text{ e } m \in M. \qquad \blacksquare$$

Corolário A.7.1.

(a) M é um $\mathbb{Z}G$-módulo (à esquerda) se, e somente se, M é um grupo abeliano munido de uma G-ação (à esquerda).

(b) M é um $\mathbb{Z}_2G$-módulo (à esquerda) se, e somente se, M é um $\mathbb{Z}_2$-módulo (à esquerda) munido de uma G-ação (à esquerda).

Observação A.7.3. Segue dos corolários anteriores que todo $\mathbb{Z}_2G$-módulo (à esquerda) é um $\mathbb{Z}G$-módulo (à esquerda), mas a recíproca obviamente não é verdadeira.

Exemplo A.7.2.

(1) Todo R-módulo (à esquerda) M tem pelo menos uma estrutura de RG-módulo (à esquerda). Para isto, basta considerarmos a G-ação trivial. Neste caso, dizemos que M é um ***RG-módulo trivial***. Em particular, todo grupo abeliano ($\mathbb{Z}$-módulo) tem uma estrutura de $\mathbb{Z}G$-módulo trivial.

(2) Sejam G um grupo e $\mathcal{P}(G)$ o conjunto das partes de G. Vimos no Exemplo A.1.1 *(3)*, que $\mathcal{P}(G)$ é um $\mathbb{Z}_2$-módulo (à esquerda). Agora, considerando a multiplicação (à esquerda) por escalar

$$\begin{aligned} \upsilon :\ G \times \mathcal{P}(G) &\longrightarrow \mathcal{P}(G) \\ (g, A) &\longmapsto g.A = \{g.a \mid a \in A\} \end{aligned}$$

temos que υ é uma G-ação (à esquerda) sobre $\mathcal{P}(G)$ e portanto segue do corolário anterior, que $\mathcal{P}(G)$ é um $\mathbb{Z}_2G$-módulo (à esquerda).

Proposição A.7.2. Todo RG-módulo à esquerda M tem também uma estrutura de RG-módulo à direita (induzida da estrutura anterior), e reciprocamente.

Demonstração. Basta considerarmos em M a G-ação à direita $m.g := g^{-1}.m$ (ver Observação A.7.2 *(3)*). ■

Observação A.7.4. ([4], p. 55) Recordemos que o produto tensorial $M \otimes_{\mathcal{R}} N$ foi definido quando M é um $\mathcal{R}$-módulo à direita e N é um $\mathcal{R}$-módulo à esquerda ($\mathcal{R}$ anel com unidade). No caso em que $\mathcal{R}$ é um anel grupo RG ($R = \mathbb{Z}$ ou

$\mathbb{Z}_2$), segue da proposição anterior que faz sentido (mesmo que RG não seja comutativo) considerar o produto tensorial $M \otimes_{RG} N$ de dois RG-módulos à esquerda (a relação fica $gm \otimes n = m \otimes g^{-1}n$, ou ainda, $gm \otimes gn' = m \otimes n'$ se tomarmos $n' = g^{-1}n$).

Definição A.7.5. Seja $m \in M$, onde M é um G-conjunto.

(a) A ***G-órbita de m***, denotada por $\boldsymbol{G(m)}$, é o seguinte subconjunto de M:

$$G(m) = \{g.m \mid g \in G\}.$$

(b) O ***estabilizador de m***, denotado por $\boldsymbol{G_m}$, é o seguinte subgrupo de G:

$$G_m = \{g \in G \mid g.m = m\}.$$

Proposição A.7.3. Consideremos X um G-conjunto livre e E um conjunto de representantes para as G-órbitas em X. Então, RX, o R-módulo livre gerado por X, é um RG-módulo livre com base E.

Demonstração.

Seja $E = \{x_\lambda \mid \lambda \in \Lambda\}$ um conjunto de representantes para as G-órbitas em X. Assim,

$$RX = R\left(\dot{\bigcup_{x_\lambda \in E}} G(x_\lambda)\right) = \bigoplus_{x_\lambda \in E} R\big(G(x_\lambda)\big).$$

Como a G-ação é livre, para cada x_λ temos que a aplicação

$$\begin{aligned} \varphi_\lambda : G &\longrightarrow G(x_\lambda) \\ g &\longmapsto \varphi_\lambda(g) = g.x_\lambda \end{aligned}$$

é uma bijeção. Assim, G é equipotente à $G(x_\lambda)$.

Portanto, $R\big(G(x_\lambda)\big) \simeq RG$. ■

Corolário A.7.2. Seja H um subgrupo de G. Consideremos G como um H-conjunto livre, onde a H-ação é dada pela multiplicação dos elementos de

H por elementos de G. Então, RG é um RH-módulo livre com base num conjunto E de representantes para as classes laterais à direita Hg (órbita de $g \in G$), isto é,

$$RG = \bigoplus_{g \in E} (RH)_g.$$

Demonstração. [25], Corolário 1.1.14. ■

A.8 Resoluções Padrão e Bar para RG-módulos (à esquerda e à direita)

Definição A.8.1. Sejam $\mathcal{R}$ um anel com unidade e M um $\mathcal{R}$-módulo (à esquerda) arbitrário. Uma ***resolução de M sobre o anel $\mathcal{R}$***, ou uma ***$\mathcal{R}$-resolução de M*** é uma seqüência exata de $\mathcal{R}$-módulos (à esquerda)

$$F : \cdots \longrightarrow F_{n+1} \xrightarrow{\partial_{n+1}} F_n \xrightarrow{\partial_n} F_{n-1} \longrightarrow \cdots$$

a qual satisfaz as seguintes condições:

(a) $F_{-1} = M$,

(b) $F_n = 0$, para todo $n < -1$.

De acordo com a definição dada acima, temos que uma $\mathcal{R}$-resolução de M é uma seqüência exata de $\mathcal{R}$-módulos (à esquerda) da seguinte forma:

$$F : \cdots \longrightarrow F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} M \longrightarrow 0.$$

Definição A.8.2. A aplicação $\varepsilon : F_0 \longrightarrow M$ é chamada de ***aplicação aumentação***. Se cada F_i é livre, dizemos que a resolução é ***livre***. Se cada F_i é projetivo, dizemos que a resolução é ***projetiva***.

Notação A.8.1. $\varepsilon : F \longrightarrow M$ denota uma $\mathcal{R}$-resolução de M.

Observação A.8.1.

(1) Toda resolução livre é projetiva.

(2) Se existir um inteiro n tal que $F_i = 0$, para $i > n$, dizemos que a resolução tem ***comprimento no máximo n***. Neste caso, escrevemos simplesmente

$$0 \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_0 \longrightarrow M \longrightarrow 0 \longrightarrow \cdots .$$

Proposição A.8.1. Todo $\mathcal{R}$-módulo (à esquerda) M possui uma resolução livre (e portanto, também projetiva pela Proposição A.3.2).

Demonstração. [13], Proposição 1.1, p. 124. ■

Nosso maior interesse são nas resoluções projetivas e livres de $M = R$ ($R = \mathbb{Z}$ ou $\mathbb{Z}_2$) sobre o anel RG, que são as utilizadas para definir cohomologia de grupos. Apresentamos a seguir exemplos de resoluções livres (logo projetivas) de R sobre RG (Padrão e Bar). As resoluções Padrão e Bar são essenciais para nosso trabalho.

Exemplo A.8.1.

(1) **Resolução Padrão**.

Sejam G um grupo e F_n o R-módulo livre ($R = \mathbb{Z}$ ou $\mathbb{Z}_2$) gerado por X_n, onde X_n é o conjunto das $(n+1)$-uplas $(g_0, g_1, \ldots, g_n)$ de elementos de G.

Consideremos o complexo

$$\cdots \longrightarrow F_n \xrightarrow{\partial_n} F_{n-1} \longrightarrow \cdots \longrightarrow F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} R \longrightarrow 0 \quad \text{(A.2)}$$

onde $\partial_n : F_n \longrightarrow F_{n-1}$ é definida por

$$\begin{aligned}\partial_n(g_0, g_1, \ldots, g_n) &:= \sum_{i=0}^{n} (-1)^i (g_0, \ldots, g_{i-1}, g_{i+1}, \ldots, g_n) \\ &\overset{not.}{=} \sum_{i=0}^{n} (-1)^i (g_0, \ldots, \widehat{g_i}, \ldots, g_n)\end{aligned}$$

e $\varepsilon : F_0 \longrightarrow R$ é definida por $\varepsilon(g_0) = 1_R$, definidas nos geradores e estendidas por linearidade.

Temos que a G-ação livre sobre F_n é obtida da G-ação livre sobre X_n, que é dada pela ***translação à esquerda***, isto é, $g.(g_0, \ldots, g_n) := (g.g_0, \ldots, g.g_n)$. Assim, pela Proposição A.7.3, temos que $F_n = RX_n$ é um RG-módulo livre com base em um conjunto de representantes para as G-órbitas em X_n.

Vejamos agora, que o complexo (A.2) é exato.

Consideremos $F = F_i$, com $F_{-1} = R$ e $h_n : F_n \longrightarrow F_{n+1}$ definida por:

$$\begin{cases} h_n(g_0, \ldots, g_n) = (1, g_0, \ldots, g_n), & \text{se } n \geqslant 0; \\ h_n(1_R) = (1), & \text{se } n = -1. \end{cases}$$

Neste caso, (A.2) será considerado como um complexo de R-módulos (à esquerda), pois h_n não é aplicação de RG-módulos (à esquerda).

Observemos que,

$$\begin{aligned} &\varepsilon \circ h_{-1} = id_{F_{-1}} \\ &h_{-1} \circ \varepsilon + \partial_1 \circ h_0 = id_{F_0} \\ &h_{n-1} \circ \partial_n + \partial_{n+1} \circ h_n = id_{F_n},\ n \geqslant 1, \end{aligned}$$

ou seja, h é uma homotopia entre id_F e a aplicação nula.

Logo, ver Proposição A.2.3 e Observação A.2.1, as aplicações induzidas na homologia coincidem, isto é, $id_{H_n(F)} = H_n(id_F) = H_n(0) = 0$. Daí, para todo n, $H_n(F) = 0$ e assim $Ker(\partial_n) = Im(\partial_{n+1})$. Portanto, o complexo (A.2) é exato.

Desta forma, (A.2) é uma resolução livre de ***RG-módulos à esquerda*** de R sobre RG, denominada ***Resolução Padrão***.

(2) **Resolução Bar**.

Consideremos na resolução anterior, como representante para a G-órbita de $(g_0, \ldots, g_n)$ o elemento

$$g_0^{-1}.(g_0, \ldots, g_n) = (1, g_0^{-1}.g_1, \ldots, g_0^{-1}.g_n) = (1, g'_1, g'_1g'_2, \ldots, g'_1g'_2 \ldots g'_n),$$

onde $g'_j := g_{j-1}^{-1}g_j$, $j = 1, \ldots, n$.

Denotemos um elemento $(1, g_1, g_1g_2, \ldots, g_1g_2 \ldots g_n)$ de F_n por

$$[g_1|g_2|\ldots|g_n].$$

Tal notação será denominada ***notação bar***.

Desta maneira, F_n é o ***RG-módulo livre à esquerda*** gerado pelos elementos $[g_1|g_2|\ldots|g_n]$, e $\partial_n\big([g_1|g_2|\ldots|g_n]\big) = \sum_{i=0}^{n}(-1)^i d_i\big([g_1|g_2|\ldots|g_n]\big)$, com

$$d_i\big([g_1|g_2|\ldots|g_n]\big) = \begin{cases} g_1[g_2|\ldots|g_n], & \text{se } \ i = 0; \\ [g_1|\ldots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\ldots|g_n], & \text{se } \ 0 < i < n; \\ [g_1|\ldots|g_{n-1}], & \text{se } \ i = n. \end{cases}$$

Sendo F_0 gerado por (1) temos, na notação bar, que F_0 é o RG-módulo livre gerado pelo símbolo [ ] e assim $F_0 \simeq RG$.

Por exemplo,

$$\begin{aligned} \partial_3\big([g_1|g_2|g_3]\big) &= d_0\big([g_1|g_2|g_3]\big) - d_1\big([g_1|g_2|g_3]\big) + d_2\big([g_1|g_2|g_3]\big) - \\ &\quad -d_3\big([g_1|g_2|g_3]\big) \\ &= g_1[g_2|g_3] - [g_1g_2|g_3] + [g_1|g_2g_3] - [g_1|g_2]\ , \\ \partial_2\big([g_1|g_2]\big) &= g_1[g_2] - [g_1g_2] + [g_1] \ \text{ e} \\ \partial_1\big([g_1]\big) &= g_1[\ ] - [\ ]. \end{aligned}$$

Quando a notação bar é usada, denominamos a Resolução Padrão por ***Resolução Bar***.

(3) **Resoluções Padrão e Bar para RG-módulos à direita** ([19], 11.3.6).

Podemos de forma similar, definir/construir resoluções Padrão/Bar considerando RG-módulos à direita. A resolução Bar à direita será útil no Capítulo 3 para a prova do Teorema 3.3.1.

- A ***Resolução Padrão*** é similar à dada em *(1)*: F_n e ∂_n sã definidos de modo análogo, no entanto, a G-ação agora é dada pela ***translação à direita***, isto é, $(g_0, \ldots, g_n)g := (g_0.g, \ldots, g_n.g)$.

- Para obter a ***Resolução Bar***, consideremos como representante para a G-órbita de $(g_0, \ldots, g_n)$ o elemento

$$\begin{aligned}(g_0, \ldots, g_n).g_n^{-1} &= (g_0.g_n^{-1}, \ldots, g_{n-1}g_n^{-1}, 1)\\ &= (g_1' \ldots g_{n-1}'g_n', \ldots, g_{n-1}'g_n', g_n', 1),\end{aligned}$$

onde $g_j' := g_{j-1}.g_j^{-1}$, $j = 1, \ldots, n$.

A ***notação bar*** $[g_1|\ldots|g_{n-1}|g_n]$ indicará o elemento

$$(g_1 \ldots g_{n-1}g_n, \ldots, g_{n-1}g_n, g_n, 1) \text{ de } F_n\ .$$

Deste modo F_n será um RG-módulo livre à direita, gerado pelos elementos $[g_1|\ldots|g_{n-1}|g_n]$ e os operadores bordos ∂_n são definidos da seguinte maneira:

$$\begin{aligned}\partial_n\big([g_1|g_2|\ldots|g_n]\big) &= \sum_{i=0}^{n}(-1)^i d_i\big([g_1|g_2|\ldots|g_n]\big)\\ &= [g_2|\ldots|g_n] + \sum_{i=1}^{n-1}(-1)^i[g_1|\ldots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\ldots|g_n] +\\ &\quad +(-1)^n[g_1|\ldots|g_{n-1}]g_n\ .\end{aligned}$$

Assim,

- $\partial_1\big([g]\big) = [\ ] - [\ ]g$,

- $\partial_2\big([g_1|g_2]\big) = [g_2] - [g_1g_2] + [g_1]g_2$,

- $\partial_3\big([g_1|g_2|g_3]\big) = [g_2|g_3] - [g_1g_2|g_3] + [g_1|g_2g_3] - [g_1|g_2]g_3$.

  Verifiquemos para ∂_2:

$$\begin{aligned}\partial_2\big([g_1|g_2]\big) = \partial_2\big((g_1g_2, g_2, 1)\big) &= (g_2, 1) - (g_1g_2, 1) + (g_1g_2, g_2)\\ &= [g_2] - [g_1g_2] + [g_1]g_2.\end{aligned}$$

Exemplo A.8.2.

(1) Seja $G = \langle t\rangle \simeq \mathbb{Z}$. Consideremos a seguinte seqüência

$$0 \longrightarrow RG \xrightarrow{\partial} RG \xrightarrow{\varepsilon} R \longrightarrow 0 \tag{A.3}$$

onde ∂ é a multiplicação por $(t-1)$ e ε é a aplicação aumentação, isto é,
$\partial\left(\sum_i \alpha_i t^i\right) = (t-1)\left(\sum_i \alpha_i t^i\right) = \sum_i (\alpha_i t^{i+1} - \alpha_i t^i) = \sum_i (\alpha_{i-1} - \alpha_i)t^i$
e $\varepsilon\left(\sum_i \alpha_i t^i\right) = \sum_i \alpha_i$.
Então, (A.3) é uma resolução livre de R sobre RG ([4] ou [25], 1.5.3 (2)).

(2) Seja $G = \langle t\rangle \simeq \mathbb{Z}_n$. Consideremos a seqüência

$$\cdots \longrightarrow RG \xrightarrow{t-1} RG \xrightarrow{N} \cdots \xrightarrow{N} RG \xrightarrow{t-1} RG \xrightarrow{\varepsilon} R \longrightarrow 0 \tag{A.4}$$

onde ε é a aplicação aumentação, $(t-1)$ e N denotam, respectivamente, a multiplicação por $t-1$ e $1+t+\cdots+t^{n-1}$. Podemos verificar que (A.4) é uma resolução livre de R sobre RG $\big($[4] ou [25], 1.5.3 (3)$\big)$.

Lema A.8.1. Sejam G um grupo e H um subgrupo de G. Se $\varepsilon : F \longrightarrow R$ é uma resolução projetiva de R sobre RG, então $\varepsilon : F \longrightarrow R$ também é uma resolução projetiva de R sobre RH se consideramos cada F_n como um RH-módulo com a H-ação induzida da G-ação (por "restrição de escalares").

Proposição A.8.2. (Unicidade de resoluções a menos de equivalência de homotopia) Sejam $\varepsilon : F \longrightarrow R$ e $\varepsilon' : F' \longrightarrow R$ resoluções projetivas de R sobre RG. Então, existe uma aplicação de cadeias $f : F \longrightarrow F'$ tal que $\varepsilon' \circ f = \varepsilon$, única a menos de homotopia, e f é uma equivalência de homotopia.

Demonstração.

Dadas $\varepsilon : F \longrightarrow R$ e $\varepsilon' : F' \longrightarrow R$ resoluções projetivas de R sobre RG, consideremos no diagrama abaixo, $f_{-1} = id_R$.

$$\begin{array}{ccccccccccccc} F : \cdots & \longrightarrow & F_1 & \xrightarrow{\partial_1} & F_0 & \xrightarrow{\varepsilon} & R & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \cdots \\ & & & & & & \downarrow{\scriptstyle id_R} & & & & & & \\ F' : \cdots & \longrightarrow & F'_1 & \xrightarrow{\partial'_1} & F'_0 & \xrightarrow{\varepsilon'} & R & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & \cdots \end{array}$$

Observemos que para $n \leqslant -1$ temos que $\partial'_n \circ f_n = f_{n-1} \circ \partial_n$, pois $\partial'_n = \partial_n = 0$.

Como F' é exata, temos que $H_n(F') = 0$, para todo $n \geqslant -1$. Além disso, F_n é projetivo para todo $n > -1$. Logo, por [4], Lema 7.4, temos que a família f se estende a uma aplicação de cadeias $f : F \longrightarrow F'$, única a menos de homotopia e que preserva aumentação, isto é, $\varepsilon' \circ f_0 = id_R \circ \varepsilon = \varepsilon$.

Agora, mostremos que f é uma equivalência de homotopia.

Por raciocínio análogo ao feito anteriormente, temos que existe $f' : F' \longrightarrow F$, aplicação de cadeias tal que $\varepsilon \circ f' = \varepsilon'$.

Daí, $f' \circ f : F \longrightarrow F$ e $id_F : F \longrightarrow F$ são aplicações de cadeias que estendem id_R.

Logo, pela unicidade em [4], Lema 7.4, segue que $f' \circ f \sim id_F$.

De maneira análoga, conclui-se que $f \circ f' \sim id_{F'}$.

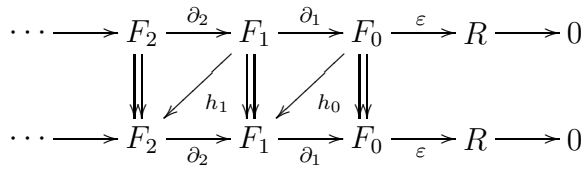
Portanto, f é uma equivalência de homotopia. ■

Proposição A.8.3. Sejam $\varepsilon : F \longrightarrow R$ e $\varepsilon' : F' \longrightarrow R$ resoluções projetivas de R sobre RG e T um funtor covariante (contravariante) aditivo. Então, os complexos $T(F)$ e $T(F')$ são homotópicos.

Demonstração.

Na demonstração da proposição anterior vimos que existem e são únicas, aplicações de cadeias $f : F \longrightarrow F'$ e $f' : F' \longrightarrow F$, preservando aumentação. E mais, existem homotopias de cadeias h e h' tais que $f' \circ f \overset{h}{\sim} id_F$ e $f \circ f' \overset{h'}{\sim} id_{F'}$.

Consideremos o seguinte diagrama



Temos que, $h \circ \partial + \partial \circ h = (f' \circ f) - id_F$. Assim,

$$T(h \circ \partial) + T(\partial \circ h) = T(f' \circ f) - T(id_F).$$

Se T é covariante, então $T(h) \circ T(\partial) + T(\partial) \circ T(h) = T(f') \circ T(f) - id_{T(F)}$, ou seja, $T(h)$ é uma homotopia de cadeia entre $T(f') \circ T(f)$ e $id_{T(F)}$. De maneira análoga, temos que $T(h')$ é uma homotopia de cadeia entre $T(f) \circ T(f')$ e $id_{T(F')}$.

Portanto, $T(f)$ é uma equivalência de homotopia entre $T(F)$ e $T(F')$.

Analogamente, se T é contravariante também obtemos que $T(f)$ é uma equivalência de homotopia entre $T(F)$ e $T(F')$. ■

Índice Remissivo