UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS FÍSICAS E MATEMÁTICAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA PURA E APLICADA

Luiza Augusta Moreira Sorice

Grupos finitos com cohomologia periódica

Florianópolis
2020

Luiza Augusta Moreira Sorice

Grupos Finitos com Cohomologia Periódica

Dissertação submetida ao Programa de Pós-Graduação em Matemática Pura e Aplicada para a obtenção do título de mestre em Matemática Pura e Aplicada. Orientador: Sérgio Tadao Martins, Dr.

Universidade Federal de Santa Catarina – UFSC
Centro de Ciências Físicas e Matemáticas
Departamento de Matemática

Orientador: Prof. Dr. Sérgio Tadao Martins

Florianópolis
2020

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Sorice, Luiza
Grupos Finitos com Cohomologia Periódica / Luiza Sorice ; orientador, Sérgio Tadao Martins, 2020.
89 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências Físicas e Matemáticas, Programa de Pós-Graduação em Matemática Pura e Aplicada, Florianópolis, 2020.

Inclui referências.

1. Matemática Pura e Aplicada. 2. Cohomologia de Grupos Periódicos. 3. Grupos Finitos. 4. Homologia. 5. Cohomologia. I. Martins, Sérgio Tadao . II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Matemática Pura e Aplicada. III. Título.

Luiza Augusta Moreira Sorice

Grupos Finitos com Cohomologia Periódica

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. Abdelmoubine Amar Henni, Dr.
Universidade Federal de Santa Catarina

Prof. Giuliano Boava, Dr.
Universidade Federal de Santa Catarina

Prof. Daciberg Lima Gonçalves, Dr.
Universidade de São Paulo

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de mestrado.

Documento assinado digitalmente
Daniel Goncalves
Data: 11/03/2020 17:07:12-0300
CPF: 017.022.459-77

Prof. Daniel Gonçalves, Dr.
Coordenador do Programa

Documento assinado digitalmente
Sergio Tadao Martins
Data: 11/03/2020 12:22:38-0300
CPF: 313.598.118-50

Prof. Sérgio Tadao Martins, Dr.
Orientador

Florianópolis, 2020.

Aos meus pais, à minha irmã
Gabriele e ao Paulinho.

AGRADECIMENTOS

Agradeço aos meus pais e minha irmã que estiveram sempre ao meu lado e me apoiaram de forma incondicional. Ao Paulinho pela compreensão, paciência e amor durante todo o tempo que precisei. Aos meus amigos, que mesmo de longe, me apoiaram e ouviram quando precisei.

A todos os professores que me ensinaram o que sei hoje, em especial ao meu orientador que me ensinou e apoiou durantes esses anos e também ao professor Giuliano Boava por inúmeros atendimentos e pelo apoio em diversos momentos.

Ao departamento de matemática da UFSC e ao CNPq pelo apoio financeiro.

RESUMO

O objetivo principal deste trabalho é dar uma caracterização de grupos finitos com cohomologia periódica e mostrar vários exemplos utilizando o teorema que caracteriza tais grupos. Para isso, foi necessário o estudo de resoluções de $\mathbb{Z}$ sobre $\mathbb{Z}G$, módulos induzidos e coinduzidos, mudança de dimensão, morfismo transfer, extensão de grupo, produto cup e cap. Além disso, estudamos a cohomologia de Tate e suas propriedades para então estudar os grupos finitos com cohomologia periódica. Apresentamos, no final deste trabalho, o Teorema de Suzuki-Zassenhaus, que classifica os grupos finitos que têm cohomologia periódica.

Palavras-chave: Cohomologia de Grupos Finitos. Grupos com Cohomologia Periódica. Morfismo Transfer. Extensões de Grupo. Cohomologia de Tate.

ABSTRACT

The main purpose of this work is to caracterize finite groups with periodic cohomology and show some examples using the theorem that caracterizes such groups. For that, we study resolutions of $\mathbb{Z}$ over $\mathbb{Z}G$, induced and co-induced modules, dimension shifting, transfer morphism, group extensions, cup and cap product. More over, we study Tate cohomology and its properties to then study finite groups with periodic cohomology. We present in the end of this work the Suzuki-Zassenhaus Theorem, which classifies all finite groups that have periodic cohomology.

Keywords: Cohomology of Finite Groups. Group with Periodic Cohomology. Transfer Morphism. Group extensions. Tate Cohomology.

SUMÁRIO

1 INTRODUÇÃO

A teoria de cohomologia de grupos se desenvolve na fronteira entre a Topologia e a Álgebra. Especificamente, dado um grupo (discreto) G, a cohomologia de G nada mais é que a cohomologia de um espaço $K(G, 1)$, isto é, um espaço que possui G como seu grupo fundamental e cujo recobrimento universal é contrátil. Neste texto, entretanto, desenvolveremos a teoria do ponto de vista puramente algébrico, com o objetivo de estudar grupos finitos cuja cohomologia é periódica.

Destacamos, entretanto, que o interesse por grupos de cohomologia periódica, apesar de ser um problema algébrico interessante por si mesmo, está também intimamente ligado à Topologia. Por exemplo, pode-se mostrar que um grupo finito que age livremente na esfera S^{2n-1} possui cohomologia de período $2n$. Swan estudou, em [1], a recíproca desta afirmação e, desde então, muitos trabalhos se desenvolveram para tentar estender os resultados obtidos por Swan para grupos infinitos. Entre tais estudos, destacamos [2], [3], [4]. Neste trabalho, entretanto, nos limitamos a discutir a periodicidade da cohomologia de grupos finitos.

No segundo capítulo foram dadas algumas ferramentas fundamentais para o estudo, em que podemos destacar, principalmente, os funtores de restrição por escalares e extensão por escalares, módulos induzidos e coinduzidos juntamente com algumas propriedades importantes desses módulos e o morfismo transfer, que é um morfismo de restrição (e correstrição) de escalares, com quatro pontos de vista diferentes.

No terceiro capítulo tratamos de extensões de grupos e algumas de suas propriedades. Também abordamos dois importantes teoremas que mostram como os grupos H^2 e H^3 classificam extensões de grupos. Além disso, classificamos p-grupos que possuem um subgrupo cíclico de índice p que serão de grande importância para o capítulo cinco.

No quarto capítulo definimos a cohomologia de Tate, damos algumas de suas propriedades e demonstramos que o produto cup $\hat{H}^i(G;\mathbb{Z})\otimes\hat{H}^{-i}(G;\mathbb{Z}) \to \hat{H}^0(G;\mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$ é um pareamento dual, no sentido da definição 4.28.

No quinto capítulo, demonstramos alguns teoremas que nos dizem quando um grupo possui cohomologia periódica e, no final deste trabalho, apresentamos alguns exemplos de grupos que possuem cohomologia periódica e apresentamos a tabela de Suzuki-Zassenhaus.

Ao final do trabalho, encontra-se um apêndice que foi usado para o leitor rever algumas definições, proposições e teoremas de álgebra homológica. Além disso, é importante que o leitor tenha conhecimento de assuntos como teoria de módulos e grupos de Sylow.

2 (CO)HOMOLOGIA DE GRUPOS

Este capítulo tem por objetivo de introduzir algumas das ferramentas necessárias para entender os grupos finitos com cohomologia periódica.

2.1 Preliminares

O produto tensorial $M \otimes_R N$ é definido sempre que M é um R-módulo à direita e N um R-módulo à esquerda. Sabemos que o produto tensorial é um quociente de $M \otimes_{\mathbb{Z}} N$ $(M \otimes N)$ em que vale a seguinte relação: $mr \otimes n = m \otimes rn$ $(m \in M,\ r \in R, n \in N)$.

Quando R é um anel de grupo $\mathbb{Z}G$, podemos evitar ter que considerar tanto módulos à esquerda quanto à direta usando o antiautomorfismo $g \mapsto g^{-1}$ de G. Deste modo, podemos considerar qualquer G-módulo à esquerda M como um G-módulo à direta, em que $mg = g^{-1}m$ $(m \in M,\ g \in G)$ e assim faz sentido considerarmos o produto tensorial $M \otimes_{\mathbb{Z}G} N$, denotado também por $M \otimes_G N$, de dois G-módulos à esquerda [1].

Observamos ainda que, munindo $M \otimes N$ com a ação "diagonal" $g \cdot (m \otimes n) = gm \otimes gn$, temos que $(M \otimes N)_G$ [2] é obtido de $M \otimes N$ ao introduzirmos a relação $m \otimes n = gm \otimes gn$. Assim, temos que $mg \otimes n = g^{-1}m \otimes n = g^{-1}m \otimes g^{-1}gn = m \otimes gn$, que nos permite concluir que $(M \otimes N)_G = M \otimes_G N$. Segue também que $- \otimes_G -$ é comutativo: $M \otimes_G N \cong N \otimes_G M$.

A G-ação diagonal usada anteriormente é mais geral e pode ser usada sempre que um funtor de um ou vários grupos abelianos são aplicados a G-módulos. Consideramos, por exemplo, o funtor $\mathrm{Hom}(\ ,\ ) = \mathrm{Hom}_{\mathbb{Z}}(\ ,\ )$. Se M e N são G-módulos, então a ação de G em M e N induz, pela funtorialidade, uma ação "diagonal" de G em $\mathrm{Hom}(M, N)$, dada por $(g \cdot u)(m) = g \cdot u(g^{-1} \cdot m)$, para $g \in G$, $u \in \mathrm{Hom}(M, N)$ e $m \in M$, em que é necessário usar g^{-1} para compensar o funtor contravariante Hom convertendo M para um módulo à direta.

Note que, pela igualdade $(g \cdot u)(m) = g \cdot u(g^{-1} \cdot m)$, temos $gu = u$ se, e somente se, $g \cdot u(g^{-1} \cdot m) = u(m)$, para todo $m \in M$. Em outras palavras $gu = u$ se, e somente se, u comuta com a ação de g. Logo, $\mathrm{Hom}_G(M, N) = \mathrm{Hom}(M, N)^G$ [3].

2.2 Definições de $H_*(G; M)$ e $H^*(G; M)$

Nesta seção introduziremos conceitos chaves para continuação do trabalho como um todo. Aqui veremos homologia e cohomologia com coeficientes. Nesta parte o texto se baseia principalmente em [5].

Definição 2.1. *Sejam F uma resolução projetiva de $\mathbb{Z}$ sobre $\mathbb{Z}G$ e M um G-módulo. Definimos a* homologia de G com coeficientes em M *por*

$$H_*(G; M) = H_*(F \otimes_G M). \tag{2.1}$$

Quando considerarmos os coeficientes em $\mathbb{Z}$, isto é, $H_*(G; \mathbb{Z})$, escreveremos $H_*(G)$.

O complexo $F \otimes_G M$ também pode ser pensado como o produto tensorial de complexos de cadeia, em que M é visto como um complexo de cadeia concentrado na dimensão 0. E, pensando assim, existe uma certa assimetria em (2.1). Uma forma mais simétrica da definição é obtida quando escolhemos resoluções projetivas $\varepsilon : F \to \mathbb{Z}$ e $\eta : P \to M$ tanto para $\mathbb{Z}$ quanto para M e então definimos

$$H_*(G; M) = H_*(F \otimes_G P) \tag{2.2}$$

[1] Ao longo do texto, usaremos G-módulo significando $\mathbb{Z}G$-módulo.
[2] Será definido na próxima seção.
[3] Também será definido na próxima seção.

que é consistente com a definição de (2.1), pois η induz uma equivalência fraca $F\otimes\eta : F\otimes_G P \to F\otimes_G M$, pelo teorema A.13. E temos ainda que A.13 também nos dá uma equivalência fraca $\varepsilon\otimes P : F\otimes_G P \to \mathbb{Z}\otimes_G P$. Logo, $H_*(G;M) = H_*(G)$.

Exemplo 2.2. O *grupo de coinvariantes* de M, denotado por M_G, é definido como o quociente de M pelo subgrupo aditivo gerado por elementos da forma $gm - m$ para $g\in G$ e $m\in M$.

Além disso, podemos apresentar uma outra descrição de M_G dada por

$$M_G \cong \mathbb{Z}\otimes_{\mathbb{Z}G} M, \tag{2.3}$$

em que $\mathbb{Z}$ é um $\mathbb{Z}G$-módulo à direita com a G-ação trivial. De fato, consideremos

$$\begin{aligned}\varphi : &M_G \to \mathbb{Z}\otimes_{\mathbb{Z}G} M\\ &\overline{m}\mapsto 1\otimes m\end{aligned}$$

em que $\overline{m}$ é a imagem em M_G de um elemento $m\in M$. Para provar a boa definição de φ, consideremos m, $n\in M$ tais que $\overline{m}=\overline{n}$. Assim $m-n\in Q$, em que Q é o subgrupo aditivo de M gerado pelos elementos da forma $gp-p$, para $g\in G$, $p\in M$. Por linearidade, podemos assumir, sem perda de generalidade, que

$$m-n = gp-p$$

em que $g\in G$, $p\in M$. Portanto,

$$1\otimes m - 1\otimes n = 1\otimes(m-n) = 1\otimes(gp-p) = 1\otimes gp - 1\otimes p = 1\cdot g\otimes p - 1\otimes p = 1\otimes p - 1\otimes p = 0.$$

Logo $\varphi(\overline{m}) = \varphi(\overline{n})$, concluindo a boa definição.

Observe ainda que, pela propriedade universal do produto tensorial, existe um único morfismo de grupos $\psi : \mathbb{Z}\otimes_{\mathbb{Z}G} M \to M_G$ tal que $\psi(z\otimes m) = z\overline{m}$, com $z\in\mathbb{Z}$, $m\in M$. Logo,

$$(\varphi\circ\psi)(z\otimes m) = \varphi(z\overline{m}) = 1\otimes zm = z\otimes m$$

para todo $z\in\mathbb{Z}$ e $m\in M$. Além disso

$$(\psi\circ\varphi)(\overline{m}) = \psi(1\otimes m) = \overline{m}$$

para todo $m\in M$. Assim, $\psi^{-1} = \varphi$, seguindo o isomorfismo.

Mostraremos agora que $H_0(G;M)\cong M_G$. Seja F uma resolução projetiva de $\mathbb{Z}$ sobre $\mathbb{Z}G$. Aplicando $-\otimes_G M$ em $F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} \mathbb{Z}\to 0$, obtemos $F_1\otimes_G M \xrightarrow{d_1^*} F_0\otimes_G M \xrightarrow{d_0^*} \mathbb{Z}\otimes_G M \to 0$. Note que a partir da sequência exata $0\to \ker(d_0) \xhookrightarrow{\partial_1} F_0 \xrightarrow{d_0} \mathbb{Z}\to 0$, temos: $\ker(d_0)\otimes_G M \xhookrightarrow{\partial_1^*} F_0\otimes_G M \xrightarrow{d_0^*} \mathbb{Z}\otimes_G M \to 0$, que é exata. Assim, $H_0(G;M) = \dfrac{F_0\otimes_G M}{\operatorname{im}(d_1^*)} = \dfrac{F_0\otimes_G M}{\operatorname{im}(\partial_1^*)} = \dfrac{F_0\otimes_G M}{\ker(d_0^*)} \overset{\star}{\cong} \mathbb{Z}\otimes_G M \cong M_G$, em $\star$ foi usado o Primeiro Teorema do Isomorfismo.

Note que M_G é obtido de M "dividindo" pela G-ação.

Além do grupo de coinvariantes, temos o *grupo de invariantes de* M, denotado por M^G e que é definido por $M^G = \{m\in M \mid gm = m \text{ para todo } g\in G\}$. Note que $M^G\cong \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z}, M)$. De fato, defina

$$\begin{aligned}\varphi : \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z},M) &\to M^G & \qquad \psi : M^G &\to \operatorname{Hom}_{\mathbb{Z}G}(\mathbb{Z},M)\\ f&\mapsto f(1) & m&\mapsto h_m\end{aligned}$$

tal que $h_m(z) = zm$. Note que ψ está bem definido, pois para $m\in M^G$, temos que

$$\psi(gm-m)(z) = \psi(gm)(z) - \psi(m)(z) = h_{gm}(z) - h_m(z) = zgm - zm = zm - zm = 0$$

para todo $z \in \mathbb{Z}$.

Além disso,

$$(\varphi \circ \psi)(m) = \varphi(h_m) = h_m(1) = 1m = m$$
$$(\psi \circ \varphi)(f)(z) = \psi(f(1))(z) = h_{f(1)}(z) = zf(1) = f(z)$$

para todo $z \in \mathbb{Z}$. Portanto, $(\psi \circ \varphi)(f) = f$, seguindo o isomorfismo.

Observe ainda que, o nome coinvariante vem do fato de que M_G é o maior quociente de M em que G age trivialmente, enquanto M^G, o grupo dos invariantes, é o maior submódulo de M em que G age trivialmente.

Agora iremos tratar de cohomologia com coeficientes, a qual é definida com $\mathscr{H}om$ ao invés de $\otimes$.

Definição 2.3. *Seja R um anel e sejam (C,d) e (C',d') complexos de cadeia. Definimos $\mathscr{H}om_R(C,C')$ como o complexo de cadeia tal que na posição de grau n temos o conjunto $\mathscr{H}om_R(C,C')_n$ de todos os morfismos de módulos graduados de grau n e o operador de bordo $D_n : \mathscr{H}om_R(C,C')_n \to \mathscr{H}om_R(C,C')_{n-1}$ é definido por $D_n(f) = d'f - (-1)^n fd$.*

Note que, em particular, $\mathscr{H}om_R(C,C')_0$ é o conjunto de todos os morfismos de cadeia de C para C'.

Considere uma resolução projetiva $F \to \mathbb{Z}$ sobre $\mathbb{Z}G$ e o complexo $\mathscr{H}om_G(F,M)$, em que M é visto como um complexo de cadeia concentrado na dimensão 0. Note que, pela definição de $\mathscr{H}om$, temos que $\mathscr{H}om_G(F,M)_n = \mathrm{Hom}_G(F_{-n},M)$, portanto é interessante ver $\mathscr{H}om_G(F,M)$ como um complexo de cocadeia com indexação usual, isto é, com

$$\mathscr{H}om_G(F,M)^n := \mathscr{H}om_G(F,M)_{-n} := \mathrm{Hom}_G(F_n,M).$$

Dados $u \in \mathscr{H}om(C,C')_p$ e $x \in C_q$, utilizaremos $\langle u,x\rangle$, para denotar $u(x) \in C'_{p+q}$. Assim temos um complexo de cocadeia não negativo com o operador de cobordo δ tal que $\langle \delta u, x\rangle + (-1)^{\deg u}\langle u, \partial x\rangle = 0$, para $u \in \mathscr{H}om_G(F,M)^n$ e $x \in F_{n+1}$.

Definição 2.4. *Definimos a* cohomologia de G com coeficientes em M *por*

$$H^*(G;M) = H^*(\mathscr{H}om_G(F,M)).$$

Exemplo 2.5. Como mostramos anteriormente, temos $\mathrm{Hom}_G(\mathbb{Z},M) \cong M^G$. Assim, dada a sequência exata $F_1 \to F_0 \to \mathbb{Z} \to 0$ conseguimos a sequência exata $0 \to \mathrm{Hom}_G(\mathbb{Z},M) \to \mathrm{Hom}_G(F_0,M) \to \mathrm{Hom}_G(F_1,M)$ e portanto temos que

$$H^0(G;M) = M^G.$$

Exemplo 2.6. Seja G um grupo cíclico infinito com gerador t, considere

$$0 \to \mathbb{Z}G \xrightarrow{t-1} \mathbb{Z}G \xrightarrow{\varepsilon} \mathbb{Z} \to 0,$$

que é uma resolução livre. De fato, primeiro notemos que

$$(t-1)\left(\sum_{i\in\mathbb{Z}} a_i t^i\right) = \sum_{i\in\mathbb{Z}} a_i t^{i+1} - \sum_{i\in\mathbb{Z}} a_i t^i = \sum_{i\in\mathbb{Z}} (a_i - a_{i+1}) t^{i+1}. \tag{2.4}$$

Agora provaremos que $(t-1)$ é injetiva. Seja $\sum_{i\in\mathbb{Z}} a_i t^i \in \ker(t-1)$. Logo, por (2.4) $a_i = a_j$ para todo $i,j \in \mathbb{Z}$. Como $a_i = 0$ para todo índice, exceto possivelmente para uma quantidade finita de índices, temos $a_i = 0$ para todo i. Logo $t-1$ é injetiva. A sobrejetividade de ε é clara.

Observe que por (2.4) $\mathrm{im}(t-1) \subseteq \ker(\varepsilon)$. Falta provar então que $\ker(\varepsilon) \subseteq \mathrm{im}(t-1)$. Seja $x = \sum_{i\in\mathbb{Z}} a_i t^i \in \ker(\varepsilon)$. Então, $\sum_{i\in\mathbb{Z}} a_i = 0$. Definimos para cada k, $b_k = -\sum_{i\geq k} a_i$. Como

$\sum_{i\in\mathbb{Z}} a_i = 0$, $b_k = 0$ para todo índice, exceto possivelmente para uma quantidade finita de índices. Além disso, $b_k - b_{k+1} = a_{k+1}$ e, portanto,

$$(t-1)\left(\sum_k b_k t^k\right) \overset{(2.4)}{=} \sum_k (b_k - b_{k+1})t^{k+1} = \sum_k a_{k+1}t^{k+1}.$$

Logo, $x \in \operatorname{im}(t-1)$, concluindo que é uma resolução.

Assim, $H_*(G;M)$ é a homologia de

$$\cdots \to 0 \to M \overset{t-1}{\to} M$$

e $H^*(G;M)$ é a cohomologia

$$M \overset{t-1}{\to} M \to 0 \to \ldots.$$

Assim $H^1(G;M) = H_0(G;M) = M_G$, $H_1(G;M) = H^0(G;M) = M^G$ e $H_i(G;M) = H^i(G;M) = 0$ para $i > 1$.

Exemplo 2.7. Seja G um grupo cíclico finito de ordem n com gerador t, temos então a resolução

$$\ldots \overset{N}{\to} \mathbb{Z}G \overset{t-1}{\to} \mathbb{Z}G \overset{N}{\to} \mathbb{Z}G \overset{t-1}{\to} \mathbb{Z}G \to \mathbb{Z} \to 0, \tag{2.5}$$

em que $N = \sum_{i=0}^{n-1} t^i$. Observamos que de fato (2.5) é uma resolução livre. Consideremos $\sum_{i=0}^{n-1} a_i t^i \in \ker(t-1)$, ou seja,

$$(t-1)\left(\sum_{i=0}^{n-1} a_i t^i\right) = (a_{n-1} - a_0) + t(a_0 - a_1) + \cdots + t^{n-1}(a_{n-2} - a_{n-1}) = 0.$$

Logo $a_0 = a_1 = \cdots = a_{n-1}$ e, portanto, $\sum_{i=0}^{n-1} at^i = aN$, isto é, $\ker(t-1) \subseteq im(N)$. Além disso, considere $\sum_{i=0}^{n-1} a_i t^i \in \ker(N)$, ou seja,

$$\begin{aligned} N\left(\sum_{i=0}^{n-1} a_i t^i\right) &= (1 + \cdots + t^{n-1})(a_0 + \cdots + a_{n-1}t^{n-1}) \\ &= (a_0 + \cdots + a_{n-1}) + (a_0 + \cdots + a_{n-1})t + \cdots + (a_0 + \cdots + a_{n-1})t^{n-1} = 0, \end{aligned}$$

assim $a_0 + \cdots + a_{n-1} = 0$. Considerando $a_0 = -a_1 - \cdots - a_{n-1}$, temos que

$$\begin{aligned} N\left(\sum_{i=0}^{n-1} a_i t^i\right) &= -a_1 - \cdots - a_{n-1} + a_1 t + a_2 t^2 + \cdots + a_{n-1}t^{n-1} \\ &= a_1(t-1) + a_2(1+t)(t-1) + \cdots + a_{n-1}(1 + t + \cdots + t^{n-2})(t-1) \\ &= (a_1 + a_2(1+t) + \cdots + a_{n-1}(1 + t + \cdots + t^{n-2}))(t-1), \end{aligned}$$

portanto $\ker(N) \subseteq \operatorname{im}(t-1)$.

Note ainda que $N(t-1)(\sum_{i=0}^{n-1} a_i t^i) = 0$ e que $(t-1)N(\sum_{i=0}^{n-1} a_i t^i) = 0$, concluímos então que a sequência é exata e, consequentemente, é uma resolução projetiva.

Assim, $H_*(G;M)$ é a homologia de

$$\ldots \overset{N}{\to} M \overset{t-1}{\to} M \overset{N}{\to} M \overset{t-1}{\to} M$$

e $H^*(G;M)$ é a cohomologia de

$$M \overset{t-1}{\to} M \overset{N}{\to} M \overset{t-1}{\to} M \overset{N}{\to} \ldots$$

Note que, para todo $g \in G$ existe $0 \le x \le n-1$ tal que $g = t^x$. Logo $Ng = t^x + t^{x+1} + \cdots + t^{n-1} + \cdots + t^{n+x-1} = t^x + \cdots + t^{n-1} + 1 + t + \cdots + t^{x-1} = N$, assim $Ngm = Nm$ para todo $m \in M$ e portanto $\operatorname{im}(N) = NM \subseteq M^G$.

Note que, pela propriedade universal do quociente, N induz um morfismo $\overline{N} : M_G \to M^G$ tal que $\overline{N}(\overline{m}) = N(m) \in M_G$, chamado de *morfismo norma* (estes fatos valem para qualquer grupo G finito, em que $N = \sum_{g\in G} g$). Pelo que fizemos até agora neste exemplo, conseguimos concluir que

(a) para i ímpar ($i \geq 1$)

$$H_i(G; M) = H^{i+1}(G; M) = \frac{\ker(t-1)}{\mathrm{im}(N)} = \frac{M^G}{NM} = \mathrm{coker}(\overline{N})$$

(b) para i par ($i \geq 2$)

$$H_i(G; M) = H^{i-1}(G; M) = \frac{\ker(N)}{\mathrm{im}(t-1)} = \ker(\overline{N}).$$

Se considerarmos agora a mesma resolução projetiva, mas utilizando coeficientes em $\mathbb{Z}$, temos que o complexo pode ser visto como

$$\cdots \xrightarrow{0} \mathbb{Z} \xrightarrow{N} \mathbb{Z} \xrightarrow{0} \mathbb{Z}.$$

Portanto,

$$H_0(G) = \mathbb{Z},$$
$$H_i(G) = \frac{\ker(0)}{\mathrm{im}(n)} = \mathbb{Z}_n \text{ se } i \text{ é ímpar e}$$
$$H_i(G) = \frac{ker(n)}{\mathrm{im}(0)} = 0 \text{ se } i \text{ é par não nulo.}$$

Exemplo 2.8. Seja $F_* = C_*(G)$ um complexo de cadeia ordenado de $\mathbb{Z}$ sobre $\mathbb{Z}G$, em que F_n é o $\mathbb{Z}$-módulo livre gerado por $(n+1)$-uplas $(g_0, \cdots, g_n)$ de elementos de G, e a G-ação é dada por $g \cdot (g_0, \cdots, g_n) = (gg_0, \cdots, gg_n)$ (esta é conhecida como descrição homogênea). Além disso, temos que o operador de bordo $\partial \colon F_n \to F_{n-1}$ é dado por $\partial = \sum_{i=0}^{n} (-1)^i d_i$, em que $d_i(g_0, \cdots, g_n) = (g_0, \cdots \hat{g}_i, \cdots, g_n)$ (repare que o operador ∂ define uma sequência exata) e o morfismo de aumento $\varepsilon \colon F_0 \to \mathbb{Z}$ é dado por $\varepsilon(g_0) = 1$.

Como uma base de um $\mathbb{Z}G$-módulo livre F_n, podemos considerar as $(n+1)$-uplas cujo primeiro elemento é o 1, assim temos $(1, g_1, g_1g_2, \cdots, g_1g_2\cdots g_n)$, que também pode ser escrita na *notação bar*:

$$[g_1|\ldots|g_n] = (1, g_1, g_1g_2, \cdots, g_1g_2\cdots g_n).$$

Podemos então, calcular $\partial \colon F_n \to F_{n-1}$ em termos dessa $\mathbb{Z}G$-base $[g_1|\cdots|g_n]$ e teremos que $\partial = \sum_{i=0}^{n} (-1)^i d_i$, em que d_i é um $\mathbb{Z}G$-morfismo dado por

$$d_i[g_1|\cdots|g_n] = \begin{cases} g_1[g_2|\cdots|g_n] & i = 0 \\ [g_1|\cdots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\cdots|g_n] & 0 < i < n \\ [g_1|\cdots|g_{n-1}] & i = n. \end{cases}$$

Chamamos a resolução F_* de *resolução standard* ou também conhecida como *resolução bar*. Em dimensões mais baixas, temos uma resolução da seguinte forma

$$F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} \mathbb{Z}G \xrightarrow{\varepsilon} Z \to 0,$$

em que $\partial_2([g_1|g_2]) = g_1[g_2] - [g_1g_2] + [g_1]$, $\partial_1([g_1]) = g_1 - 1$ e $\varepsilon(1) = 1$.

Para os casos $C_*(G, M)$ e $C^*(G, M)$, estamos considerando $F \otimes_G M = M \otimes_G F$ e $\mathscr{H}om_G(F, M)$, respectivamente. Um elemento de $C_n(G, M)$ pode ser escrito unicamente como soma de elementos da forma $m \otimes [g_1|\ldots|g_n]$, ou seja, como uma soma formal com coeficientes em M dos símbolos $[g_1|\ldots|g_n]$. O operador de bordo $\partial : C_n(G, M) \to C_{n-1}(G, M)$ é dado por

$$\partial(m \otimes [g_1|\ldots|g_n]) = mg_1 \otimes [g_2|\ldots|g_n] - m \otimes [g_1g_2|\ldots|g_n] + \cdots + (-1)^n m \otimes [g_1|\ldots|g_{n-1}].$$

Similarmente, um elemento de $C^n(G, M)$ pode ser visto como uma função $f\colon G^n \to M$. O operador de cobordo $\delta\colon C^{n-1}(G, M) \to C^n(G, M)$ é, a menos de sinal, dado por

$$(\delta f)(g_1, \ldots, g_n) = g_1 f(g_2, \ldots, g_n) - f(g_1 g_2, \ldots, g_n) + \cdots + (-1)^n f(g_1, \ldots, g_{n-1}).$$

Por convenção, se $n = 0$, então G^n é um conjunto de um elemento, assim, $C^0(G, M) \cong M$.

$$d_i(g_0, \cdots, g_n) = (g_0, \cdots, \hat{g}_i, \cdots, g_n)$$

O morfismo de aumento $\varepsilon : F_0 \to \mathbb{Z}$ é dado por $\varepsilon(g_0) = 1$.

2.3 Extensão e coextensão de escalares

Seja $\alpha\colon R \to S$ um morfismo de anéis. Então, qualquer S-módulo pode ser considerado como um R-módulo via α, isto é, se M é um S-módulo (à esquerda), M também pode ser visto como um R-módulo (à esquerda) com a ação dada por $r \cdot m := \alpha(r) \cdot m$.

No sentido contrário, queremos estudar as construções de R-módulos para S-módulos. Para qualquer R-módulo (à esquerda) M, consideramos o produto tensorial $S \otimes_R M$, em que S é visto como um R-módulo à direta com ação dada por $s \cdot r = s \cdot \alpha(r)$. Pela associatividade de S, essa ação à direita de R em S comuta com a ação natural à esquerda de S nele mesmo. Assim, podemos ver $S \otimes_R M$ um S-módulo (à esquerda) de forma que $s \cdot (s' \otimes m) = ss' \otimes m$.

Definição 2.9. *As duas construções acima definem funtores chamados de* restrição por escalares *e* extensão por escalares, *respectivamente.*

Existe um morfismo natural $i\colon M \to S \otimes_R M$ dado por $i(m) = 1 \otimes m$. Note que, para $r \in R$, temos $1 \otimes rm = \alpha(r) \otimes m = \alpha(r) \cdot (1 \otimes m)$. Assim $i(rm) = \alpha(r)i(m)$, ou seja, i é un morfismo de R-módulos, em que o S-módulo $S \otimes_R M$ é visto como um R-módulo pela restrição por escalares. Além disso, vale a seguinte propriedade universal:

Proposição 2.10. *(Propriedade universal) Dado um S-módulo N e um morfismo de R-módulos $f\colon M \to N$, existe um único morfismo de S-módulos $g\colon S \otimes_R M \to N$, dado por, $g(s \otimes m) = s \cdot f(m)$ tal que $gi = f$.*

$$\begin{tikzcd} M \arrow[r, "i"] \arrow[d, "f"'] & S \otimes_R M \arrow[dl, dashed, "g"] \\ N & \end{tikzcd}$$

□

Assim, temos que

$$\operatorname{Hom}_S(S \otimes_R M, N) \cong \operatorname{Hom}_R(M, N) \tag{2.6}$$

mostrando que a extensão de funtores escalares (R-mod) $\to$ (S-mod) é adjunta à esquerda para a restrição por escalares dos funtores (S-mod) $\to$ (R-mod). A propriedade universal, proposição 2.10, nos diz que $S \otimes_R M$ é o menor S-módulo que recebe um morfismo de R-módulos de M.

Note que, se $M = N$ na proposição 2.10, isto é, vendo como um R-módulo por restrição por escalares e $f = \mathrm{id}_N$, teremos para qualquer S-módulo N um morfismo de S-módulo canônico $S \otimes_R N \to N$ dado por $s \otimes n \mapsto sn$. Além disso, este morfismo é sobrejetivo e, visto como um morfismo de R-módulos é uma sobrejeção que cinde.

Dado um R-módulo (à esquerda) M, consideremos o grupo abeliano $\operatorname{Hom}_R(S, M)$, em que S é visto como um R-módulo à esquerda dado por $r \cdot s = \alpha(r)s$. Como a ação natural à direita de S nele mesmo comuta com a ação à esquerda de R em S, podemos ver $\operatorname{Hom}_R(S, M)$

como um S-módulo à esquerda de forma que $(sf)(s') = f(s's)$ para $f \in \mathrm{Hom}_R(S, M)$ (pela contravariância do funtor Hom a ação à direita de S nele mesmo induz uma ação à esquerda de S).

Definição 2.11. *O S-módulo $\mathrm{Hom}_R(S, M)$ acima é dito ser obtido de M por* coextensão de escalares *de R para S.*

Existe um morfismo natural $\pi\colon \mathrm{Hom}_R(S, M) \to M$ dado por $\pi(f) = f(1)$. Note que, para $r \in R$, temos $\pi(\alpha(r)f) = (\alpha(r)f)(1) = f(\alpha(r)1) = f(\alpha(r)) = r \cdot f(1) = r \cdot \pi(f)$, logo π é um morfismo de R-módulos se o S-módulo $\mathrm{Hom}_R(S, M)$ é visto como um R-módulo pela restrição por escalares. Além disso, vale a seguinte propriedade universal:

Proposição 2.12. *(Propriedade universal) Dado um S-módulo N e um morfismo de R-módulos $f\colon N \to M$, existe um único morfismo de S-módulos $g\colon N \to \mathrm{Hom}_R(S, M)$, dado por $g(n)(s) = f(sn)$, tal que $\pi g = f$.*

$$\begin{tikzcd} & \mathrm{Hom}_R(S, M) \arrow[d, "\pi"] \\ N \arrow[ur, dashed, "g"] \arrow[r, "f"'] & M \end{tikzcd}$$

□

Assim, temos que

$$\mathrm{Hom}_S(N, \mathrm{Hom}_R(S, M)) \cong \mathrm{Hom}_R(N, M), \tag{2.7}$$

mostrando que a coextensão de escalares é adjunta à direta para a restrição por escalares. A propriedade universal 2.12 nos diz que $\mathrm{Hom}_R(S, M)$ é o menor S-módulo que é mapeado em M por um morfismo de R-módulos.

Note que, se $M = N$ é visto como um R-módulo e $f = \mathrm{id}_N$, teremos pela proposição 2.12 um morfismo de S-módulos canônico

$$N \to \mathrm{Hom}_R(S, N) \tag{2.8}$$

dado por $n \mapsto (s \mapsto sn)$. Além disso, este morfismo é injetivo e, visto como um morfismo de R-módulos, é uma injeção que cinde.

Exemplo 2.13. Se α é o morfismo de aumento $\varepsilon : \mathbb{Z}G \to \mathbb{Z}$ então o funtor de "extensão de escalares" de $\mathbb{Z}G$-módulos para $\mathbb{Z}$-módulos é $M \mapsto M_G$ e o funtor de "coextensão de escalares" é $M \mapsto M^G$.

2.4 Módulos induzidos e coinduzidos

Definição 2.14. *Sejam H e G grupos tais que $H \subseteq G$ e considere o morfismo inclusão $\mathbb{Z}H \hookrightarrow \mathbb{Z}G$. Neste caso, a extensão de escalares (resp. coextensão) é chamada de* indução *(resp.* coindução*) de H para G. Escreveremos da seguinte forma*

$$\mathbb{Z}G \otimes_{\mathbb{Z}H} M = \mathrm{Ind}_H^G M$$

e

$$\mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M) = \mathrm{Coind}_H^G M$$

para um H-módulo M. Temos que $\mathrm{Ind}_{\{1\}}^G M$ é chamado de módulo induzido *e $\mathrm{Coind}_{\{1\}}^G M$ de* coinduzido.

Observe que $\mathbb{Z}G$ é um $\mathbb{Z}H$-módulo livre à direita, pois a ação de translação à direita de H em G é livre. Como base, podemos pegar qualquer conjunto E de representantes para as classes laterais à esquerda gH. Deste modo, temos que $\mathbb{Z}G \otimes_{\mathbb{Z}H} M$, como um grupo abeliano, admite uma decomposição

$$\mathbb{Z}G \otimes_{\mathbb{Z}H} M = \bigoplus_{g \in E} g \otimes M \tag{2.9}$$

em que $g \otimes M = \{g \otimes m : m \in M\}$ e $g \otimes M \cong M$ via $g \otimes m \leftrightarrow m$.

Proposição 2.15. *O G-módulo $\operatorname{Ind}_H^G M$ contém M como um H-submódulo e é a soma direta de cópias de gM, em que g varia sobre algum conjunto de representantes das classes laterais à esquerda de H em G.*

Demonstração. Seja 1 o representante da sua classe lateral, assim, o morfismo canônico $i\colon M \to \mathbb{Z}G \otimes_{\mathbb{Z}H} M$ de H, definido na seção anterior, mapeia M isomorficamente na sua imagem $1 \otimes M$. Então, basta usar i para ver M como um H-submódulo de $\operatorname{Ind}_H^G M$. Além disso, o somando direto $g \otimes M$ anterior (2.9) é apenas a transformação desse H-submódulo sobre a ação de g, pois $g \cdot (1 \otimes m) = g \otimes m$. □

A segunda parte da proposição anterior 2.15 nos diz que

$$\operatorname{Ind}_H^G M = \bigoplus_{g \in G/H} gM. \tag{2.10}$$

Note que o lado direito dessa igualdade faz sentido, pois M é mapeado nele mesmo pela ação de H, logo o subgrupo gM de $\operatorname{Ind}_H^G M$ depende apenas da classe de g em G/H.

Observe que (2.10) caracteriza completamente G-módulos da forma $\operatorname{Ind}_H^G M$. Mais precisamente:

Proposição 2.16. *Seja N um G-módulo cujo grupo abeliano subjacente é a soma direta $\oplus_{i\in I} M_i$ e suponha que exista uma ação de G em I transitiva tal que $gM_i = M_{gi}$ para todo $g \in G$ e $i \in I$. Seja M um dos somandos M_i e $H \subseteq G$ o grupo de isotropia de i. Então M é um H-módulo e $N \cong \operatorname{Ind}_H^G M$.*

Demonstração. Claro que M é um H-submódulo de N e pela propriedade universal 2.10, obtemos que a inclusão de M em N se estende para um morfismo de G-módulos $\operatorname{Ind}_H^G M$

$$\begin{tikzcd} M \arrow[r] \arrow[d, hook] & \operatorname{Ind}_H^G M \arrow[dl, dashed, "\varphi"] \\ N & \end{tikzcd}$$

Além disso, quando aplicamos φ no somando gM de $\operatorname{Ind}_H^G M$, φ mapeia isomorficamente no somando M_{gi}. Em outras palavras, todo somando direto de $\operatorname{Ind}_H^G M$ é isomorfo a um somando direto de N. Além disso, podemos ver G/H como a órbita de i e portanto somandos diretos diferentes de $\operatorname{Ind}_H^G M$ são mapeados em somandos diretos diferentes de N. Por fim, como a ação é transitiva, a órbita de i é todo I e portanto todo somando direto de N é isomorfo a um somando de $\operatorname{Ind}_H^G M$. Logo φ é um isomorfismo. □

Corolário 2.17. *Seja N um G-módulo cujo grupo abeliano subjacente é da forma $\bigoplus_{i\in I} M_i$. Assuma que a G-ação permuta os somandos de acordo com alguma ação de G em I. Seja G_i o grupo de isotropia de i e considere E o conjunto de representantes para $I \mod G$. Então M_i é um G_i-módulo e existe um G-isomorfismo $N \cong \bigoplus_{i\in E} \operatorname{Ind}_{G_i}^G M_i$.*

Demonstração. Temos que $I = \bigcup_{i\in E} Gi$, assim $N = \bigoplus_{i\in I} M_i = \bigoplus_{i\in E} \left(\bigoplus_{j\in Gi} M_j\right)$ e também M_i é um G_i-módulo, pois M_i é invariante pela ação de g_i. Utilizando o isomorfismo de 2.16 obtemos $\bigoplus_{j\in Gi} M_j \cong \operatorname{Ind}_{Gi}^G M_i$, assim $N \cong \bigoplus_{i\in E} \operatorname{Ind}_{Gi}^G M_i$. □

Exemplo 2.18. O módulo de permutação $\mathbb{Z}[G/H]$ é isomorfo a $\operatorname{Ind}_H^G \mathbb{Z}$, em que H age trivialmente em $\mathbb{Z}$, pois se escrevermos $\mathbb{Z}[G/H]$ como soma direta de somas de $\mathbb{Z}$, basta utilizar a proposição 2.16. Outra forma de ver é pela própria definição de $\operatorname{Ind}_H^G \mathbb{Z}$.

Observe ainda que o somando gM de $\operatorname{Ind}_H^G M$ é fechado sobre a ação de gHg^{-1}, portanto gM é um gHg^{-1}-módulo. Note também que a ação de g^{-1} nos dá uma bijeção $f : gM \xrightarrow{\cong} M$ tal que $f(kn) = g^{-1}kg \cdot f(n)$, para $k \in gHg^{-1}$ e para $n \in gM$. Portanto gM pode ser identificado com o gHg^{-1}-módulo obtido pelo H-módulo M pela "restrição por escalares" via o isomorfismo de conjugação $gHg^{-1} \xrightarrow{\cong} H$.

Para qualquer G-módulo N, denotamos por $\operatorname{Res}_H^G N$ o H-módulo obtido da restrição por escalares de G para H.

Proposição 2.19. *(a) Sejam N um G-módulo e H subgrupo de G. Então existe um isomorfismo de $\mathbb{Z}G$-módulos*

$$\operatorname{Ind}_H^G \operatorname{Res}_H^G N \cong \mathbb{Z}[G/H] \otimes N,$$

em que G age diagonalmente no produto tensorial.

(b) Sejam H e K subgrupos de G e considere E um conjunto de representantes das classes laterais duplas KgH. Para qualquer H-módulo M, existe um K-isomorfismo

$$\operatorname{Res}_H^G(\operatorname{Ind}_H^G M) \cong \bigoplus_{g\in E} \operatorname{Ind}_{K\cap gHg^{-1}}^K(\operatorname{Res}_{K\cap gHg^{-1}}^{gHg^{-1}} gM).$$

Em particular, se $H \lhd G$, então existe um H-isomorfismo

$$\operatorname{Res}_H^G(\operatorname{Ind}_H^G M) \cong \bigoplus_{g\in G/H} gM.$$

Demonstração. (a) Primeiro, note que $\mathbb{Z}G \otimes_{\mathbb{Z}H} N = \operatorname{Ind}_H^G \operatorname{Res}_H^G N$. Consideremos então os morfismos

$$\begin{aligned} \varphi\colon \mathbb{Z}G \otimes_{\mathbb{Z}H} N &\to \mathbb{Z}[G/H] \otimes N \\ g \otimes n &\mapsto gH \otimes g \cdot n \end{aligned}$$

e

$$\begin{aligned} \varphi'\colon \mathbb{Z}[G/H] \otimes N &\to \mathbb{Z}G \otimes_{\mathbb{Z}H} N \\ gH \otimes n &\mapsto g \otimes g^{-1} \cdot n. \end{aligned}$$

Pode-se verificar que φ está bem definida, e temos que φ' também está, pois dados g, $g_0 \in G$ tal que $gg_0^{-1} \in H$, temos

$$g \otimes g^{-1} \cdot n = g_0 g_0^{-1} g \otimes g^{-1} n = g_0 \otimes g_0^{-1} g g^{-1} n = g_0 \otimes g_0^{-1} \cdot n.$$

Além disso, temos que

$$\varphi(\varphi'(gH \otimes n)) = \varphi(g \otimes g^{-1} \cdot n) = gH \otimes g \cdot g^{-1} n = gH \otimes n$$

$$\varphi'(\varphi(g \otimes n)) = \varphi'(gH \otimes g \cdot n) = g \otimes g^{-1} gn = g \otimes n$$

e, portanto provamos que existe o isomorfismo desejado.

(b) Sabemos que os somandos do $\operatorname{Ind}_H^G M = \bigoplus_{g\in G/H} gM$ são permutados pela ação de K de acordo com a ação de translação à esquerda de K em G/H. Como as órbitas de K em G/H são as classes laterais duplas KgH e o grupo de isotropia de K na classe lateral gH é $K \cap gHg^{-1}$, pelo corolário 2.17, segue a primeira parte de (b). Para $H \lhd G$, o resultado é claro. □

Se $H = \{1\}$, obtemos:

Corolário 2.20. *Seja M um G-módulo e seja M_0 seu grupo abeliano subjacente. Assim $\mathbb{Z}G \otimes M$ (com a G-ação diagonal) é canonicamente isomorfo ao módulo induzido $\mathbb{Z}G \otimes M_0$. Em particular, $\mathbb{Z}G \otimes M$ é um $\mathbb{Z}G$-módulo livre se M é livre como um $\mathbb{Z}$-módulo.*

Podemos estender a proposição 2.19(a) para um caso ainda mais geral:

Proposição 2.21. *Para quaisquer H-módulo M e G-módulo N, existe o isomorfismo de $\mathbb{Z}G$-módulos*

$$N \otimes \operatorname{Ind}_H^G M \cong \operatorname{Ind}_H^G(\operatorname{Res}_H^G N \otimes M),$$

em que o produto tensorial da esquerda tem a G-ação diagonal e o da direita tem a H-ação diagonal.

Demonstração. Pela proposição 2.15, temos

$$\begin{aligned} N \otimes \operatorname{Ind}_H^G M &\cong N \otimes \left(\bigoplus_{g\in G/H} gM \right) \\ &\cong \bigoplus_{g\in G/H} (N \otimes gM), \end{aligned} \tag{2.11}$$

que possui $N \otimes M$ como somando direto do grupo abeliano subjacente. Vendo (2.11) como o H-módulo $\operatorname{Res}_H^G N \otimes M$ com a ação diagonal, de forma que H é seu grupo de isotropia (a ação de h em gH é trivial), temos pela proposição 2.16 o isomorfismo desejado. □

A coindução possui propriedades análogas àquelas de indução dadas anteriormente, mas a soma direta será substituída pelo produto direto. Porém, para reformular as afirmações, precisaremos de algumas notações: se $\pi_1 \colon N \twoheadrightarrow M_1$ e $\pi_2 \colon N \twoheadrightarrow M_2$ são sobrejeções de grupos abelianos, então escrevemos $\pi_1 \sim \pi_2$ se existe um isomorfismo $h : M_1 \xrightarrow{\cong} M_2$ tal que $h\pi_1 = \pi_2$, ou equivalentemente, se $\ker(\pi_1) = \ker(\pi_2)$. Se $\pi \colon N \twoheadrightarrow M$ é uma sobrejeção e N possui uma estrutura de G-módulo, então denotamos por πg, para $g \in G$, a sobrejeção de N para M definida por $(\pi g)(x) = \pi(gx)$.

Definição 2.22. *Uma* decomposição em produto direto *de N é uma família de sobrejeções $(\pi_i : N \twoheadrightarrow M_i)_{i\in I}$ tal que o morfismo correspondente $N \to \prod_{i\in I} M_i$ é um isomorfismo.*

Agora, podemos fazer os análogos das proposições 2.15, 2.16, 2.17 e 2.19, faremos aqui apenas o análogo de 2.16 é:

Proposição 2.23. *Seja N um G-módulo do qual seu grupo abeliano admite uma decomposição em produto direto $(\pi_i \colon N \twoheadrightarrow M_i)_{i\in I}$. Assuma que existe uma ação transitiva à direta de G em I tal que $\pi_i g \sim \pi_{ig}$ para todo $i \in I$ e $g \in G$. Seja $\pi \colon N \to M$ um dos π_i e $H \subseteq G$ o grupo de isotropia de i. Assim M herda de N uma estrutura de H-módulo, e $N \cong \operatorname{Coind}_H^G M$.*

Logo, como o produto direto indexado por um conjunto finito pode ser visto como uma soma direta, obtemos

Proposição 2.24. *Se $(G : H) < \infty$ então $\operatorname{Ind}_M^G \cong \operatorname{Coind}_G^M$.*

Demonstração. Seja $\varphi_0 \colon M \to \mathrm{Hom}_H(\mathbb{Z}G, M)$ o H-morfismo tal que

$$\varphi_0(m)(g) = \begin{cases} gm, & g \in H \\ 0, & g \notin H. \end{cases}$$

Pela propriedade universal, propriedade 2.10, conseguimos estender φ_0 para o morfismo $\varphi : \mathbb{Z}G \otimes_{\mathbb{Z}H} M \to \mathrm{Hom}_H(\mathbb{Z}G, M)$ tal que $\varphi(g \otimes m) = g \cdot \varphi_0(m)$.

Podemos então definir o morfismo

$$\begin{aligned} \psi \colon \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M) &\to \mathbb{Z}G \otimes_{\mathbb{Z}H} M \\ f &\mapsto \sum_{g \in G/H} g \otimes f(g^{-1}). \end{aligned}$$

Note que

$$\begin{aligned} (\varphi \circ \psi)(f)(g') &= \varphi\left(\sum_{g \in G/H} g \otimes f(g^{-1}) \right)(g') \\ &= \sum_{g \in G/H} \varphi(g \otimes f(g^{-1}))(g') \\ &= \sum_{g \in G/H} (g \cdot \varphi_0(f(g^{-1})))(g') \\ &= \sum_{g \in G/H} \varphi_0(f(g^{-1}))(g'g) \end{aligned}$$

e temos que

$$\varphi_0(f(g^{-1}))(g'g) = \begin{cases} g'gf(g^{-1}), & g'g \in H \\ 0, & g'g \notin H \end{cases} = \begin{cases} f(g'), & g'g \in H \\ 0, & g'g \notin H. \end{cases}$$

Assim, temos que $\sum_{g \in G/H} \varphi_0(f(g^{-1}))(g'g)$ possui apenas um dos somandos não nulo, já que se $g'g \notin H$, então $\varphi_0(f(g^{-1}))(g'g) = 0$, portanto $(\varphi \circ \psi)(f)(g') = f(g')$.

Além disso,

$$\begin{aligned} (\psi \circ \varphi)(g' \otimes m) &= \psi(g' \cdot \varphi_0(m)) \\ &= \sum_{g \in G/H} g \otimes g'\varphi_0(m)(g^{-1}) \\ &= \sum_{g \in G/H} g \otimes \varphi_0(m)(g^{-1}g') \end{aligned}$$

para $g^{-1}g' \in H$, temos portanto $(\psi \circ \varphi)(g' \otimes m) = g' \otimes m$.

Concluímos então que ψ é inversa da φ e portanto $\mathrm{Ind}_M^G \cong \mathrm{Coind}_G^M$.

□

Proposição 2.25. *(Lema de Shapiro) Se $H \subseteq G$ e M é um H-módulo, então*

$$H_*(H; M) \cong H_*(G; \mathrm{Ind}_H^G M)$$

e

$$H^*(H; M) \cong H^*(G; \mathrm{Coind}_H^G M).$$

Demonstração. Seja F uma resolução projetiva de $\mathbb{Z}$ sobre $\mathbb{Z}G$. Então F é uma resolução projetiva de $\mathbb{Z}$ sobre $\mathbb{Z}H$, assim

$$H_*(H, M) \cong H_*(F \otimes_{\mathbb{Z}H} M).$$

Mas sabemos que $F \otimes_{\mathbb{Z}H} M \cong F \otimes_{\mathbb{Z}G} (\mathbb{Z}G \otimes_{\mathbb{Z}H} M) \cong F \otimes_G (\mathrm{Ind}_H^G M)$, portanto segue o primeiro isomorfismo.

O segundo isomorfismo segue da propriedade universal de coindução, que implica a equação (2.7), ou seja $\mathscr{H}om_H(F, M) \cong \mathscr{H}om_G(F, \mathrm{Coind}_H^G M)$. □

2.5 H_* e H^* como funtores de módulos coeficientes

Sabemos que os funtores $F \otimes_G -$ e $\mathrm{Hom}_G(F; -)$ são funtores covariantes, da mesma forma teremos então que $H_*(G; -)$ e $H^*(G; -)$ são funtores covariantes de módulos coeficientes. Algumas propriedades desses funtores são dadas na proposição abaixo.

Proposição 2.26. *(i) Existe um isomorfismo natural $H_0(G; M) \cong M_G$.*

(i') Existe um isomorfismo natural $H^0(G; M) \cong M^G$.

(ii) Para qualquer sequência exata $0 \to M' \xrightarrow{i} M \xrightarrow{j} M'' \to 0$ de G-módulos e qualquer inteiro $n \geq 1$, existe um morfismo natural $\partial\colon H_n(G; M'') \to H_{n-1}(G; M')$ tal que a sequência

$$\cdots \to H_1(G; M) \to H_1(G, M'') \xrightarrow{\partial} H_0(G; M') \to H_0(G; M) \to H_0(G; M'') \to 0$$

é exata (em que os morfismos sem nome são os induzidos por i e j).

(ii') Para qualquer sequência exata $0 \to M' \xrightarrow{i} M \xrightarrow{j} M'' \to 0$ de G-módulos e qualquer inteiro $n \geq 1$, existe um morfismo natural $\delta\colon H^n(G; M'') \to H^{n+1}(G; M')$ tal que a sequência

$$0 \to H^0(G; M') \to H^0(G; M) \to H^0(G; M'') \xrightarrow{\delta} H^1(G; M') \to H^1(G; M) \to \dots$$

é exata.

(iii) Se P é um $\mathbb{Z}G$-módulo projetivo, então $H_n(G; P) = 0$ para $n > 0$.

(iii') Se Q é um $\mathbb{Z}G$-módulo injetivo, então $H^n(G; Q) = 0$ para $n > 0$.

Demonstração. Os isomorfismos de (i) e (i') foram provados nos exemplos 2.2 e 2.5, respectivamente. Sejam M e N $\mathbb{Z}G$-módulos e $f\colon M \to N$ um morfismo, o diagrama abaixo é comutativo,

$$\begin{array}{ccc} H_0(G; M) & \xrightarrow{H_0(G;f)} & H_0(G; N) \\ \downarrow{\scriptstyle \varphi_M} & & \downarrow{\scriptstyle \varphi_N} \\ \mathbb{Z} \otimes_{\mathbb{Z}G} M & \xrightarrow{\mathrm{id} \otimes f} & \mathbb{Z} \otimes_{\mathbb{Z}G} N \end{array}$$

pois $((\mathrm{id} \otimes f) \circ \varphi_M)(\overline{m}) = (\mathrm{id} \otimes f)(1 \otimes m) = 1 \otimes f(m) = \varphi_N(\overline{f(m)}) = (\varphi_N \circ H_0(G, f))(\overline{m})$, seguindo a naturalidade de (i). A naturalidade de (i') segue de forma similar.

(ii) Considere a sequência exata dada e uma resolução projetiva F de $\mathbb{Z}$ sobre $\mathbb{Z}G$. Teremos então a seguinte sequência de complexos de cadeia:

$$0 \to M' \otimes_G F \to M \otimes_G F \to M'' \otimes_G F \to 0,$$

que é exata pela planaridade de F e, portanto, vale a sequência exata longa de homologia. (ii') De forma similar ao anterior, consideramos uma resolução projetiva F de $\mathbb{Z}$ sobre $\mathbb{Z}G$ e obtemos a seguinte sequência exata de complexos de cocadeia:

$$0 \to \mathscr{H}om_G(F, M') \to \mathscr{H}om_G(F, M) \to \mathscr{H}om_G(F, M'') \to 0$$

que é exata pela definição de projetivo e, portanto, vale a sequência exata longa de cohomologia. (iii) e (iii') Seguem da definição de H_* e H^* e pelo fato de $- \otimes_G P$ e $\mathrm{Hom}_G(-, Q)$ serem exatos. $\square$

Note que, em (ii) da proposição 2.26, a naturalidade significa que para qualquer diagrama comutativo

$$\begin{tikzcd} 0 \arrow[r] & M' \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & M'' \arrow[r] \arrow[d] & 0 \\ 0 \arrow[r] & N' \arrow[r] & N \arrow[r] & N'' \arrow[r] & 0 \end{tikzcd}$$

com linhas exatas, o quadrado

$$\begin{tikzcd} H_n(G, M'') \arrow[r, "\partial"] \arrow[d] & H_{n-1}(G, M') \arrow[d] \\ H_n(G, N'') \arrow[r, "\partial"] & H_{n-1}(G, N') \end{tikzcd}$$

é comutativo.

Exemplo 2.27. Se $M = \mathbb{Z}$, pelo Lema de Shapiro 2.25, temos

$$H_*(H) \cong H_*(G, \mathbb{Z}[G/H]). \tag{2.12}$$

Caso $(G : H) < \infty$, temos pela proposição 2.24, $\mathrm{Ind}_M^G \cong \mathrm{Coind}_G^M$, assim

$$H^*(H, \mathbb{Z}) \cong H^*(G, \mathbb{Z}[G/H]). \tag{2.13}$$

Similarmente, se assumimos $(G : H) < \infty$, conseguimos que

$$H^*(H, \mathbb{Z}H) \cong H^*(G, \mathbb{Z}G), \tag{2.14}$$

pois $\mathbb{Z}G \otimes_{\mathbb{Z}H} \mathbb{Z}H \cong \mathbb{Z}G$. Note que, $H_*(H, \mathbb{Z}H) \cong H_*(G, \mathbb{Z}G)$ também vale, mas, pela proposição 2.26(iii), sabemos que não é de nosso interesse.

Definição 2.28. *Dizemos que um módulo projetivo é* H_*-acíclico *quando a propriedade (iii), da proposição 2.26, é satisfeita e que um módulo injetivo é* H^*-acíclico *quando a propriedade (iii'), da proposição 2.26, é satisfeita.*

Definição 2.29. *Seja T um funtor de R-módulos para grupos abelianos. Dizemos que T é* effaceable *se todo módulo M é o quociente de um módulo $\overline{M}$ tal que $T(\overline{M}) = 0$. Similarmente, T é dito* coeffaceable *se todo módulo M pode ser injetado em um $\overline{\overline{M}}$ tal que $T(\overline{\overline{M}}) = 0$.*

Podemos notar que, se $T(P) = 0$ para todo módulo projetivo P, então T é effaceable. Além disso, se T é effaceable, então $T(P) = 0$ para todo projetivo P. De fato, suponha T effaceable e P um módulo projetivo. Por definição, existe um módulo $\overline{P}$ tal que $T(\overline{P}) = 0$ e um morfismo sobrejetor $\pi : \overline{P} \to P$. Como P é projetivo, π é uma sobrejeção que cinde. Portanto, aplicando o funtor T, obtemos a sobrejeção que cinde $T(\pi) : T(\overline{P}) \to T(P)$ e como $T(\overline{P}) = 0$, devemos ter $T(P) = 0$. Logo, pela proposição 2.26(iii) temos que $H_n(G, -)$ é effaceable para $n > 0$ e por (iii'), $H^n(G; -)$ é coeffaceable para $n > 0$, isto é, todo módulo M pode ser injetado em um $\overline{\overline{M}}$ tal que $H^n(G, \overline{\overline{M}}) = 0$.

Aplicando o Lema de Shapiro 2.25 para $H = \{1\}$, temos:

Corolário 2.30. *Módulos induzidos $\mathbb{Z}G \otimes A$ são H_*-acíclicos e módulos coinduzidos $\mathrm{Hom}(\mathbb{Z}G, A)$ são H^*-acíclicos.*

2.6 Mudança de dimensão

Como acabamos de ver na seção anterior, $H_n(G;-)$ é effaceable e $H^n(G;-)$ é coeffaceable para $n > 0$. Isto nos permite agora utilizar a técnica de *mudança de dimensão*: dado um G-módulo M, escolha um módulo H_*-acíclico $\overline{M}$ que mapeia sobrejetivamente sobre M (por exemplo, considere $\overline{M} = \mathbb{Z}G \otimes M$) e seja $K = \ker\{\overline{M} \to M\}$. Logo, pela proposição 2.26(ii), a sequência exata $0 \to K \to \overline{M} \to M \to 0$ fornece a sequência exata

$$\cdots \to H_n(G;\overline{M}) \to H_n(G,M) \xrightarrow{\partial} H_{n-1}(G;K) \to H_{n-1}(G;\overline{M}) \to \cdots .$$

Assim, para $n > 1$, ∂ é um isomorfismo e para $n = 1$, ∂ é um monomorfismo. Logo,

$$H_n(G;M) \cong \begin{cases} H_{n-1}(G;K), & n > 1 \\ \ker\{H_0(G;K) \to H_0(G;\overline{M})\}, & n = 1. \end{cases} \tag{2.15}$$

Podemos perceber que, a princípio, uma questão sobre H_n pode ser reduzida para uma questão de H_{n-1}, desde que estejamos dispostos a mudar o coeficiente.

De forma similar, mergulhando M em um módulo H^*-acíclico $\overline{\overline{M}}$ (por exemplo, $\overline{\overline{M}} = \operatorname{Hom}(\mathbb{Z}G, M)$) e considerando $C = \operatorname{coker}\{M \to \overline{\overline{M}}\}$, encontramos:

$$H^n(G;M) \cong \begin{cases} H^{n-1}(G;C), & n > 1 \\ \operatorname{coker}\{H^0(G;\overline{\overline{M}}) \to H^0(G;C)\}, & n = 1. \end{cases} \tag{2.16}$$

Observe que a partir destes argumentos, a "teoria de homologia" com propriedade análogas a (ii) e (iii) da proposição 2.26 é completamente determinada pelo funtor H_0. Similarmente, a "teoria de cohomologia" satisfazendo (ii') e (iii') da proposição 2.26 é determinada por H^0. O que faremos nesta seção será para formular melhor essas ideias e prová-las.

Sejam R um anel arbitrário e $T = (T_n)_{n\in\mathbb{Z}}$ uma família de funtores covariantes de R-módulos para grupos abelianos. Assumiremos que é dado um "morfismo de conexão" $\partial : T_n(M'') \to T_{n-1}(M')$ para toda sequência exata curta $0 \to M' \to M \to M'' \to 0$ de R-módulos. Além disso, é necessário que ∂ seja natural, no sentido do comentário após a proposição 2.26, e que todas as composições sejam zero na sequência

$$\cdots \to T_{n+1}(M'') \xrightarrow{\partial} T_n(M') \to T_n(M) \to T_n(M'') \xrightarrow{\partial} T_{n-1}(M') \to \cdots . \tag{2.17}$$

Definição 2.31. *Se T for da forma acima, diremos então que T (ou, mais precisamente (T, ∂)) é um ∂-*funtor*. Se T também satisfizer $T_n = 0$ para $n < 0$ e (2.17) for exata para toda sequência exata curta $0 \to M' \to M \to M'' \to 0$, diremos que T é um* funtor homológico*.*

Exemplo 2.32. Na proposição 2.26(ii), temos que $H_*(G;-)$ é um funtor homológico na categoria dos G-módulos.

Note que, se S e T são ∂-funtores, então um morfismo de S para T é uma família φ de transformações naturais $\varphi_n : S_n \to T_n$ tal que o quadrado

$$\begin{tikzcd} S_n(M'') \arrow[r, "\partial"] \arrow[d, "\varphi_n(M'')"'] & S_{n-1}(M') \arrow[d, "\varphi_{n-1}(M')"] \\ T_n(M'') \arrow[r, "\partial"] & T_{n-1}(M') \end{tikzcd}$$

comuta para toda sequência exata curta $0 \to M' \to M \to M'' \to 0$ e todo n.

Teorema 2.33. *Seja H um funtor homológico tal que H_n é effaceable para $n > 0$. Se T é um ∂-funtor arbitrário e $\varphi_0 \colon T_0 \to H_0$ é uma transformação natural, então φ_0 se estende unicamente para um morfismo $\varphi\colon T \to H$ de ∂-funtores. Esse morfismo φ é um isomorfismo se, e somente se, as seguintes condições valem:*

(i) φ_0 *é um isomorfismo.*

(ii) T *é homológico.*

(iii) T_n *é effaceable para* $n > 0$.

Demonstração. Iremos mostrar primeiro que φ_0 se estende unicamente para um morfismo $\varphi\colon T \to H$ de ∂-funtores. Queremos construir $\varphi_n\colon T_n \to H_n$ de forma que

$$\begin{tikzcd} T_n(M'') \arrow[r, "\partial"] \arrow[d, "\varphi_n(M'')"'] & T_{n-1}(M') \arrow[d, "\varphi_{n-1}(M')"] \\ H_n(M'') \arrow[r, "\partial"] & H_{n-1}(M') \end{tikzcd} \tag{2.18}$$

comuta para toda sequência exata curta $0 \to M' \to M \to M'' \to 0$. Para $n \leq 0$ não há o que fazer, todos os diagramas (2.18) comutam automaticamente. Assim, assumimos que $n > 0$ e que φ_{n-1} tenha sido definido. Para qualquer módulo M, escolha uma sequência exata curta $0 \to K \xrightarrow{\iota} P \to M \to 0$ com P projetivo, e considere o diagrama

$$\begin{tikzcd} & T_n(M) \arrow[r, "\partial"] \arrow[d, dashed, "\varphi_n(M)"] & T_{n-1}(K) \arrow[r, "\iota_\star"] \arrow[d, "\varphi_{n-1}(K)"] & T_{n-1}(P) \arrow[d, "\varphi_{n-1}(P)"] \\ 0 = H_n(P) \arrow[r] & H_n(M) \arrow[r, "\partial"] & H_{n-1}(K) \arrow[r, "\iota_*"] & H_{n-1}(P). \end{tikzcd} \tag{2.19}$$

Queremos definir $\varphi_n(M)\colon T_n(M) \to H_n(M)$. Note que, pela definição de ∂-funtor, a composição na primeira linha de (2.19) é zero e por ser uma sequência exata longa de homologia a linha de baixo é exata. Além disso, o quadrado da direita comuta pela naturalidade de φ_{n-1}. Consequentemente, existe um único morfismo $\varphi_n(M)$ que faz o diagrama (2.19) comutar. De fato, note que dado $a \in T_n(M)$, temos $(\varphi_{n-1}(P) \circ \iota_\star \circ \partial)(a) = 0$ e pela naturalidade de φ_{n-1} obtemos que $(\iota_* \circ \varphi_{n-1}(K) \circ \partial)(a) = 0$, isto é $(\varphi_{n-1}(K) \circ \partial)(a) \in \ker(\iota_*) = \operatorname{im}(\partial)$. Logo, como $H_n(P) = 0$, existe um único $b \in H_n(M)$ tal que $\partial(b) = (\varphi_{n-1}(K) \circ \partial)(a)$. Defina então $\varphi_n(M)(a) = b$ e teremos a comutatividade desejada. Resta mostrar que $\varphi_n(M)$ é um morfismo. De fato, dados $a, a' \in T_n(M)$ consideremos $b = \varphi_n(M)(a)$ e $b' = \varphi_n(M)(a')$, assim $\partial(b + b') = \partial(b) + \partial(b') = (\varphi_{n-1}(K) \circ \partial)(a) + (\varphi_{n-1}(K) \circ \partial)(a') = (\varphi(K) \circ \partial)(a + a')$, logo $b + b'$ é o único elemento de $H_n(M)$ tal que $(\varphi_{n-1}(K) \circ \partial)(a + a') = b + b'$. Por definição, $\varphi_n(M)(a + a') = b + b' = \varphi_n(M)(a) + \varphi_n(M)(a')$. Além disso, como a definição de $\varphi_n(M)$ foi forçada pelo diagrama (2.18), a unicidade de φ do teorema é clara.

Se φ é isomorfismo, é claro que (i) vale. Além disso, como H é homológico, $H_n = 0$ para $n > 0$ e como φ é isomorfismo, necessariamente, $T_n = 0$ para $n > 0$ e toda sequência da forma (2.17) é exata, pela naturalidade da φ, já que H é homológico. Assim, T é homológico. Temos também que, como H_n é effaceable para $n \geq 1$ e φ é isomorfismo, T_n é effaceable para $n > 0$.

Basta mostrar agora que φ_n existe, provando sua boa definição, naturalidade e que todos quadrados da forma (2.18) comutam. Para isso, usaremos o lema a seguir.

Lema 2.34. *Seja* $\varphi_n(M)$ *definido como anteriormente, seja* $0 \to K \to P \to M \to 0$ *uma sequência exata curta. Para qualquer diagrama*

$$\begin{tikzcd} & & & M \arrow[d, "f"] & \\ 0 \arrow[r] & N' \arrow[r] & N \arrow[r] & N'' \arrow[r] & 0 \end{tikzcd}$$

com linha exata, o diagrama

$$\begin{tikzcd}
T_n(M) \arrow[r, "T_n(f)"] \arrow[d, "\varphi_n(M)"'] & T_n(N'') \arrow[r, "\partial"] & T_{n-1}(N') \arrow[d, "\varphi_{n-1}(N')"] \\
H_n(M) \arrow[r, "H_n(f)"] & H_n(N'') \arrow[r, "\partial"] & H_{n-1}(N')
\end{tikzcd}$$

comuta.

Demonstração. Como P é projetivo, o diagrama dado no enunciado pode ser completado para um diagrama comutativo

$$\begin{tikzcd}
0 \arrow[r] & K \arrow[r] \arrow[d, "g"] & P \arrow[r] \arrow[d] & M \arrow[r] \arrow[d, "f"] & 0 \\
0 \arrow[r] & N' \arrow[r] & N \arrow[r] & N'' \arrow[r] & 0
\end{tikzcd}$$

Considere então o diagrama:

$$\begin{tikzcd}
T_n(M) \arrow[rrr, "\partial"] \arrow[dr, "\varphi_n(M)"] \arrow[ddd, "T_n(f)"] & {} \arrow[r, phantom, "1"] & {} & T_{n-1}(K) \arrow[dl, "\varphi_{n-1}(K)"] \arrow[ddd, "T_{n-1}(g)"] \\
& H_n(M) \arrow[r, "\partial"] \arrow[d, "H_n(f)"] \arrow[dr, phantom, "2"] & H_{n-1}(K) \arrow[d, "H_{n-1}(g)"] \arrow[dr, phantom, "3"] & \\
& H_n(N'') \arrow[r, "\partial"] & H_{n-1}(N') & {} \\
T_n(N'') \arrow[rrr, "\partial"] & & & T_{n-1}(N') \arrow[ul, "\varphi_{n-1}(N')"]
\end{tikzcd}$$

em que os morfismos ∂ em (1) são morfismos de conexão associados a $0 \to K \to P \to M \to 0$. Assim (1) comuta por (2.19), (2) comuta por H ser um ∂-funtor, e (3) comuta pela naturalidade de φ_{n-1}. Além disso, o quadrado de fora ($\square$) comuta por T_n ser um ∂-funtor. Portanto

$$\begin{aligned}
\varphi_{n-1}(N') \circ \partial \circ T_n(F) &\overset{\square}{=} \varphi_{n-1}(N') \circ T_{n-1}(g) \circ \partial \\
&\overset{(3)}{=} H_{n-1}(g) \circ \varphi_{n-1}(K) \circ \partial \\
&\overset{(1)}{=} H_{n-1}(g) \circ \partial\varphi_n(M) \\
&\overset{(2)}{=} \partial \circ H_n(f) \circ \varphi_n(M).
\end{aligned}$$

$\square$

Agora, voltando para terminar a prova do teorema 2.33:

Seja $f : M_1 \to M_2$ um morfismo arbitrário de R-módulos. Escolha sequências exatas $0 \to K_i \to P_i \to M_i \to 0$ com P_i projetivo ($i = 1, 2$), e defina $\varphi_n(M_i) : T_n(M_i) \to H_n(M_i)$ como em (2.19). Aplicando o lema 2.34 no diagrama

$$\begin{tikzcd}
& & & M_1 \arrow[d, "f"] & \\
0 \arrow[r] & K_2 \arrow[r] & P_2 \arrow[r] & M_2 \arrow[r] & 0
\end{tikzcd}$$

concluímos que o retângulo de fora é um diagrama comutativo

$$\begin{tikzcd}
T_n(M_1) \arrow[r, "T_n(f)"] \arrow[d, "\varphi_n(M_1)"'] & T_n(M_2) \arrow[r, "\partial"] \arrow[d, "\varphi_n(M_2)"] & T_{n-1}(K_2) \arrow[d, "\varphi_{n-1}(K_2)"] \\
H_n(M_1) \arrow[r, "H_n(f)"] & H_n(M_2) \arrow[r, "\partial"] & H_{n-1}(K_2)
\end{tikzcd}$$

e por (2.19), temos que o quadrado da direita comuta e $\partial : H_n(M_2) \to H_{n-1}(K_2)$ é injetivo. Assim, $\partial \circ \varphi_n(M_2) \circ T_n(f) = \varphi_{n-1}(K_2) \circ \partial \circ T_n(f) = \partial \circ H_n(f) \circ \varphi_n(M_1)$ e como ∂ é injetiva, segue a comutatividade do quadrado da esquerda. Concluindo que φ_n é natural. E também mostra que $\varphi_n(M)$ está bem definido independentemente da escolha da sequência exata $0 \to K \to P \to M \to 0$. Finalmente, se $0 \to M' \to M \to M'' \to 0$ é uma sequência exata qualquer, podemos aplicar o lema 2.34 ao diagrama

$$\begin{tikzcd}
 & & & M'' \arrow[d, "\mathrm{id}"] & \\
0 \arrow[r] & M' \arrow[r] & M \arrow[r] & M'' \arrow[r] & 0
\end{tikzcd}$$

para concluir que (2.18) comuta. Concluindo a ida do teorema.

Devemos provar agora que $\varphi_n \colon T_n \to H_n$ é isomorfismo. Observe que temos as sequências exatas longas de homologia

$$\cdots \to H_{n+1}(M) \xrightarrow{\cong} H_n(K) \to H_n(P) \to H_n(M) \xrightarrow{\cong} H_{n-1}(K) \to \cdots$$

e

$$\cdots \to T_{n+1}(M) \xrightarrow{\cong} T_n(K) \to T_n(P) \to T_n(M) \xrightarrow{\cong} T_{n-1}(K) \to \cdots .$$

Como H_n e T_n são effaceable, temos que $H_n(P) = 0 = T_n(P)$ e assim segue o isomorfismo $T_n(P) \to H_n(P)$. Suponha, por hipótese de indução, que $T_{n-1}(K) \to H_{n-1}(K)$ seja um isomorfismo e, pelas sequências exatas longas de homologia, $H_n(M) \to H_{n-1}(K)$ e $T_n(M) \to T_{n-1}(K)$ são isomorfismos. Logo, temos

$$\begin{tikzcd}
\cdots \arrow[r] & T_n(K) \arrow[r] \arrow[d] & T_n(P) \arrow[r, "0"] \arrow[d, "\cong"] & T_n(M) \arrow[r, "\cong"] \arrow[d] & T_{n-1}(K) \arrow[r] \arrow[d, "\cong"] & \cdots \\
\cdots \arrow[r] & H_n(K) \arrow[r] & H_n(P) \arrow[r, "0"] & H_n(M) \arrow[r, "\cong"] & H_{n-1}(K) \arrow[r] & \cdots
\end{tikzcd}$$

e, como os quadrados comutam, $T_n(M) \to H_n(M)$ é isomorfismo. Portanto, φ_n é um isomorfismo para todo n.

□

Similarmente, podemos definir um *δ-funtor* e um *funtor cohomológico*. E podemos provar:

Teorema 2.35. *Seja H um funtor cohomológico tal que H^n é coeffaceable para $n > 0$. Se T é um δ-funtor arbitrário e $\varphi^0 : H^0 \to T^0$ é uma transformação natural, então φ^0 se estende unicamente para um morfismo $\varphi : T \to H$ de δ-funtor. Esse morfismo φ é um isomorfismo se, e somente se, as seguintes condições valem:*

(i) φ^0 é um isomorfismo.

(ii) T é cohomológico.

(iii) T^n é coeffaceable para $n > 0$.

2.7 H_* e H^* como funtores de duas variáveis

Considere a seguinte categoria $\mathscr{C}$: um objeto é um par (G, M), em que G é um grupo e M é um G-módulo; um morfismo em $\mathscr{C}$ de (G, M) para (G', M') é um par (α, f) em que $\alpha : G \to G'$ é um morfismo de grupos e $f : M \to M'$ é um morfismo de grupos abelianos tal que $f(gm) = \alpha(g)f(m)$ para $g \in G$, $m \in M$. Em outras palavras, f é um morfismo de G-módulos se M' é visto como um G-módulo via α. Dado (α, f), seja F (resp. F') uma resolução projetiva de $\mathbb{Z}$ sobre $\mathbb{Z}G$ (resp. $\mathbb{Z}G'$), e seja $\tau : F \to F'$ um morfismo de cadeia compatível com α, ou seja, $\tau(gx) = \alpha(g)\tau(x)$ para $g \in G$ e $x \in F$. Logo, existe um morfismo de cadeia $\tau \otimes f : F \otimes_G M \to F' \otimes_{G'} M'$, e $\tau \otimes f$ induz um morfismo bem definido $(\alpha, f)_* : H_*(G; M) \to H_*(G'; M')$. Assim, H_* se torna um funtor covariante de $\mathscr{C}$ para a categoria dos grupos abelianos. No caso em que $M = M'$ e $f = \mathrm{id}_{M'}$ escrevemos α_* para $(\alpha, f)_* : H_*(G; M) \to H_*(G'; M')$. Note que o morfismo $(\alpha, f)_*$ pode sempre ser escrito como a composição

$$H_*(G; M) \overset{H_*(G,f)}{\to} H_*(G, M') \overset{\alpha_*}{\to} H_*(G'; M'),$$

em que $H_*(G, f)$ faz sentido por f ser um morfismo de G-módulos.

Exemplo 2.36. Neste exemplo consideramos morfismos induzidos por conjugação. Dados $H \subseteq G$, um G-módulo M, e um elemento $g \in G$, denotamos por $c(g) : (H, M) \to (gHg^{-1}, M)$ o isomorfismo em $\mathscr{C}$ dado por

$$(h \mapsto ghg^{-1},\ m \mapsto gm).$$

Para calcular $c(g)_* : H_*(H; M) \to H_*(gHg^{-1}; M)$, escolhemos uma resolução projetiva F de $\mathbb{Z}$ sobre $\mathbb{Z}G$ e usamos F para calcular a homologia de H e gHg^{-1}. Consideramos $\tau : F \to F$ definida por $\tau(x) = gx$. Assim, $\tau \otimes f : F \otimes_H M \to F \otimes_{gHg^{-1}} M$ dado por $x \otimes m \mapsto gx \otimes gm$ induz $c(g)_*$. Neste caso, podemos perceber que o morfismo obtido é a ação diagonal usual de g em $F \otimes M$ pela passagem para os quocientes.

Para $z \in H_*(H; M)$, definimos $gz = c(g)_* z \in H_*(gHg^{-1}, M)$. No ponto de vista da descrição de $c(g)_*$ a nível de cadeia, temos:

Proposição 2.37. *Se $h \in H$ então $hz = z$ para todo $z \in H_*(H; M)$.*

Demonstração. Note que $c(h) : F \otimes_H M \to F \otimes_H M$ é a identidade, pois $hx \otimes hm = xh^{-1} \otimes hm = x \otimes h^{-1}hm = x \otimes m$. Logo $c(h)_*$ é também a identidade. $\square$

Corolário 2.38. *Se $H \lhd G$ e M é um G-módulo, então a ação de conjugação de G em (H, M) induz uma ação de G/H em $H_*(H; M)$.*

Demonstração. Basta notar que se g, $g' \in G$ são tais que $gH = g'H$, então $g^{-1}g' \in H$ e pela proposição anterior, temos $g^{-1}gz = z$ para todo $z \in H_*(H; M)$, isto é, $g'z = gz$ para todo $z \in H_*(H; M)$. $\square$

Para cohomologia o que temos é similar. Consideremos $\mathscr{D}$ uma categoria com os mesmos objetos de $\mathscr{C}$, mas um morfismo $(G, M) \to (G', M')$ é um par

$$(\alpha : G \to G',\ f : M' \to M).$$

Como antes, é necessário que f seja um morfismo de G-módulos, ou seja, $f(\alpha(g)m') = gf(m')$ para $g \in G$ e $m' \in M'$. Se F e F' são resoluções sobre G e G' e $\tau : F \to F'$ é um morfismo de cadeia compatível com α, então existe um morfismo de cadeia

$$\mathscr{H}om(\tau, f) : \mathscr{H}om_{G'}(F', M') \to \mathscr{H}om_G(F, M),$$

que induz $(\alpha, f)^* : H^*(G'; M') \to H^*(G; M)$. Assim, H^* é um funtor contravariante de $\mathscr{D}$ na categoria dos grupos abelianos. No caso em que $M = M'$ e $f = \mathrm{id}_M$ escrevemos α^* para $(\alpha, f)^*$. Note que o morfismo $(\alpha, f)^*$ é a composição

$$H^*(G'; M') \xrightarrow{\alpha^*} H^*(G, M') \xrightarrow{H^*(G,f)} H^*(G; M).$$

Seja $\mathscr{C}_0$ a subcategoria de $\mathscr{C}$ que consiste de todos os objetos (G, M) e de morfismos (α, f) tal que f é bijetiva. Assim $\mathscr{C}_0$ é isomorfo a uma subcategoria de $\mathscr{D}$ por $(\alpha, f) \mapsto (\alpha, f^{-1})$, portanto H^* pode ser visto como um funtor contravariante em $\mathscr{C}_0$. Note que os morfismos de conjugação $c(g)$ anteriores estão em $\mathscr{C}_0$. Com isso, temos um isomorfismo $c(g)^* : H^*(gHg^{-1}; M) \to H^*(H, M)$ para quaisquer $g \in G$, $H \subseteq G$, e G-módulo M. Se $z \in H^*(H; M)$, definimos

$$gz = (c(g)^*)^{-1}(z) \in H^*(gHg^{-1}; M).$$

Em termos de uma resolução projetiva F de $\mathbb{Z}$ sobre $\mathbb{Z}G$, o morfismo $z \mapsto gz$ é induzido pelo morfismo de cadeia $\mathscr{H}om_H(F, M) \to \mathscr{H}om_{gHg^{-1}}(F, M)$ dado por

$$f \mapsto [x \mapsto gf(g^{-1}x)],$$

em que utilizamos a ação diagonal de g em $\mathscr{H}om(F, M)$ restrito ao sub-complexo $\mathscr{H}om_H(F, M)$. Caso $g \in H$, obtemos também:

Proposição 2.39. *Se $h \in H$ então $hz = z$ para todo $z \in H^*(H; M)$.*

Corolário 2.40. *Se $H \lhd G$ e M é um G-módulo, então a ação de conjugação de G em (H, M) induz uma ação de G/H em $H^*(H; M)$.*

2.8 O morfismo Transfer

Dado um G-módulo M e uma inclusão $\alpha\colon H \hookrightarrow G$, pelo que já vimos, existem os morfismos $\alpha_* : H_*(H; M) \to H_*(G; M)$ e $\alpha^* : H^*(G; M) \to H^*(H; M)$.

Definição 2.41. *Chamamos α^* de* morfismo de restrição, *denotado por res^G_H. Similarmente, chamamos α_* de* morfismo de corestrição, *denotado por* cor^G_H.

O que queremos nesta seção é mostrar que se $(G : H) < \infty$, então existem morfismos na outra direção, chamados de *transfer*. A existência desses morfismos é, de alguma forma, mais sutil do que a de α_* e α^*; em particular, eles não são induzidos por morfismos nas categorias $\mathscr{C}$ e $\mathscr{D}$ que acabamos de ver na seção anterior.

Definiremos o morfismo transfer sobre quatro pontos de vistas diferentes (obviamente equivalentes).

(A) Para qualquer G-módulo M e qualquer $H \subseteq G$ temos a sobrejeção canônica de G-módulos

$$\mathbb{Z}G \otimes_{\mathbb{Z}H} M \to M \tag{2.20}$$

e a injeção canônica

$$M \to \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M). \tag{2.21}$$

Aplicando $H_*(G; -)$ em (2.20) e usando o Lema de Shapiro, obtemos o morfismo $H_*(H; M) \to H_*(G; M)$ que coincide com α_*. Similarmente, se aplicarmos $H^*(G; -)$ em (2.21) e utilizando o Lema de Shapiro, obtemos $\alpha^* : H^*(G; M) \to H^*(H; M)$. E, assumindo que $(G : H) < \infty$, temos pela proposição 2.24 que $\mathbb{Z}G \otimes_{\mathbb{Z}H} M \cong \mathrm{Hom}_{\mathbb{Z}H}(\mathbb{Z}G, M)$. Consequentemente, podemos aplicar

$H^*(G;-)$ em (2.20) e $H_*(G;-)$ em (2.21), obtemos então os morfismos transfer que estão indo na outra direção. E são geralmente denotados por

$$\operatorname{cor}_H^G : H^*(H;M) \to H^*(G;M)$$

e

$$\operatorname{res}_H^G : H_*(G;M) \to H_*(H;M)$$

ou podemos chamá-los de tr_H^G se no contexto estiver claro se estamos nos referindo à H_* ou H^*.

(B) Para qualquer $H \subseteq G$, podemos ver $H_*(G;-)$ e $H_*(H;-)$ como funtores homológicos na categoria dos G-módulos e temos também que ambos funtores são effaceable em dimensão positiva, pela proposição 2.26 (iii) e (iii'). Assumimos agora que $(G:H) < \infty$, e definimos $\operatorname{tr} : M_G \to M_H$ por $\operatorname{tr}(\overline{m}) = \sum_{g\in H\backslash G} \overline{\overline{gm}}$, em que $\overline{m}$ (resp. $\overline{\overline{m}}$) denota a imagem de m em M_G (resp. M_H). Note que a soma faz sentido, pois $\overline{\overline{m}}$ depende apenas da classe de g em $H \setminus G$. Definimos agora $\operatorname{res} : H_*(G;-) \to H_*(H;-)$ como a única extensão de tr para um morfismo de funtores homológicos, como no teorema 2.33. Podemos notar ainda que o res é compatível com o funtor ∂, no sentido que o seguinte diagrama comuta

$$\begin{array}{ccc} H_n(G;M'') & \xrightarrow{\text{res}} & H_n(H;M'') \\ \downarrow{\scriptstyle\partial} & & \downarrow{\scriptstyle\partial} \\ H_{n-1}(G;M') & \xrightarrow{\text{res}} & H_{n-1}(H;M') \end{array}$$

para toda sequência exata $0 \to M' \to M \to M'' \to 0$. Além disso, pelo que já vimos, $H_0(G;M) \to H_0(H;M)$ é o mesmo que tr em dimensão zero. Portanto é claro que as definições coincidem com àquelas dadas em (A). Similarmente, $\operatorname{cor} : H^*(H;-) \to H^*(G;-)$ pode ser definido como o único morfismo de funtores cohomológicos do qual em dimensão zero é o morfismo $\operatorname{tr} : M^H \to M^G$, definido por $\operatorname{tr}(m) = \sum_{g\in G/H} gm$. Note ainda que um G-módulo coinduzido é também um H-módulo coinduzido.

(C) Seja F uma resolução projetiva de $\mathbb{Z}$ sobre $\mathbb{Z}G$. Então $F \otimes_H M = (F \otimes M)_H$ e $F \otimes_G M = (F \otimes M)_G$. Definimos $\operatorname{res} : H_*(G;M) \to H_*(H;M)$ como o morfismo induzido do morfismo de cadeia $\operatorname{tr} : (F\otimes M)_G \to (F\otimes M)_H$, em que tr é como em (B). Note que em dimensão zero tr define um morfismo de funtores homológicos, também como em (B). De forma similar, $\mathscr{H}om_G(F,M) = \mathscr{H}om(F,M)^G$ e $\mathscr{H}om_H(F,M) = \mathscr{H}om(F,M)^H$ em que G age diagonalmente no $\mathscr{H}om$. Portanto, existe um morfismo de cocadeia $\operatorname{tr} : \mathscr{H}om(F,M)^H \to \mathscr{H}om(F,M)^G$ que induz $\operatorname{cor} : H^*(H,M) \to H^*(G,M)$.

(D) Queremos utilizar o morfismo transfer do caso (C), utilizando uma resolução $F(G)$ para G e uma diferente $F(H)$ para H, deste modo, precisamos de um H-morfismo de cadeia que preserva aumento $\tau\colon F(G) \to F(H)$ ao invés de utilizar o morfismo canônico $H_*(F(G)\otimes_H M) \overset{\cong}{\to} H_*(F(H) \otimes_H M)$. O morfismo transfer então será induzido por

$$F(G) \otimes_G M \overset{\text{tr}}{\to} F(G) \otimes_H M \overset{\tau\otimes M}{\to} F(H) \otimes_H M \tag{2.22}$$

e

$$\mathscr{H}om_H(F(H),M) \overset{\mathscr{H}om(\tau,M)}{\to} \mathscr{H}om_H(F(G),M) \overset{\text{tr}}{\to} \mathscr{H}om_G(F(G),M), \tag{2.23}$$

Considerando $F(G)$ e $F(H)$ resoluções standard, por exemplo, podemos então escrever facilmente o morfismo τ como segue: escolha um conjunto de representantes para as classes laterais à direita Hg. Logo, existe um único morfismo $\rho\colon G \to H$ tal que $\rho(hg) = h\rho(g)$ para todo $g \in G$, $h \in H$ tal que ρ manda todo representante da classe lateral no 1; explicitamente, se $\bar{g}$ denota um representante de Hg, temos $\rho(g) = \rho(g\bar{g}^{-1}\bar{g}) = g\bar{g}^{-1}\rho(\bar{g}) = g\bar{g}^{-1}$. Usando a descrição homogênea das resoluções standard, podemos definir $\tau\colon F(G) \to F(H)$ por $\tau(g_0, \cdots, g_n) = (\rho(g_0), \cdots, \rho(g_n))$.

Iremos agora dar algumas propriedades do morfismo transfer. Denotaremos por $H(-;-)$ tanto H_* quanto H^*.

Proposição 2.42. *(i) Dados $K \subseteq H \subseteq G$ com $(G:H) < \infty$,*

$$\mathrm{cor}_K^G = \mathrm{cor}_H^G \circ \mathrm{cor}_K^H \quad e \quad res_K^G = res_K^H \circ res_H^G .$$

(ii) Dados $H \subseteq G$ com $(G:H) < \infty$ e $z \in H(G;M)$, $\mathrm{cor}_H^G\, res_H^G\, z = (G:H)z$.

(iii) Sejam H, $K \subseteq G$. Suponha que $(G:H) < \infty$ se $H(-;-) = H^*$ e que $(G:K) < \infty$ se $H(-;-) = H_*$. Nessas condições

$$res_K^G\, \mathrm{cor}_H^G\, z = \sum_{g \in E} \mathrm{cor}_{K\cap gHg^{-1}}^K\, res_{K\cap gHg^{-1}}^{gHg^{-1}}\, gz$$

para qualquer $z \in H(H;M)$, em que E é um conjunto de representantes das classes laterais duplas KgH. Em particular, se $H \lhd G$ e $(G:H) < \infty$, então $res_H^G\, \mathrm{cor}_H^G\, z = \sum_{g\in G/H} gz = Nz$, em que $N = \sum_{g \in G/H} g$ é o elemento norma de $\mathbb{Z}[G/H]$.

Demonstração. (i) Segue das definições de cor e res.
(ii) Provaremos o resultado para cohomologia. Considere o diagrama abaixo

$$\begin{tikzcd} H^n(G;M) \arrow[r, "\mathrm{res}_H^G"] \arrow[dr, dashed] & H^n(H;M) \arrow[d, "\mathrm{cor}_H^G"] \\ & H^n(G;M). \end{tikzcd}$$

Se $n = 0$, então para um elemento $z \in M^G$, temos que $\mathrm{res}_H^G(z) \in M^H$ é basicamente o mesmo elemento, pois $M^G \hookrightarrow M^H$. Assim,

$$\mathrm{cor}_H^G \circ \mathrm{res}_H^G(z) = \sum_{g\in G/H} gz = \sum_{g \in G/H} z = (G:H)z.$$

Indutivamente, se o resultado vale para n, utilizando a técnica de mudança de dimensão, temos o diagrama comutativo

$$\begin{tikzcd} H^{n+1}(G;M) \arrow[r, "\mathrm{cor}\circ\mathrm{res}"] \arrow[d, "\cong"] & H^{n+1}(G;M) \arrow[d, "\cong"] \\ H^n(G;C) \arrow[r, "\mathrm{cor}\circ\mathrm{res}"] & H^n(G;C) \end{tikzcd}$$

em que $C = \mathrm{coker}\, M \to \mathrm{Hom}(\mathbb{Z}G, M)$. Logo, para $z \in H^{n+1}(G;M)$ temos

$$\mathrm{cor}\circ\mathrm{res}(z) = (\delta^{-1} \circ \mathrm{cor} \circ \mathrm{res} \circ \delta)(z) = \delta^{-1}((G:H)\delta(z)) = (G:H)z$$

concluindo a demonstração de (ii).

(iii) Provaremos o resultado para cohomologia: Seja $u \in \mathscr{H}\!om(F,M)^H$ representante de z. Assim, $\mathrm{res}_K^G \circ \mathrm{cor}_H^G\, z$ é representado por $\sum_{g\in G/H} gu \in \mathscr{H}\!om(F,M)^G \subseteq \mathscr{H}\!om(F,M)^K$. Agrupando os termos gu que pertencem à mesma órbita de K em G/H, temos

$$\sum_{g\in G/H} gu = \sum_{g\in E} \sum_{k \in K/K_g} kgu,$$

em que $K_g = \{k \in K | kgH = gH\} = K \cap gHg^{-1}$. Mas note que o lado direito da igualdade representa exatamente $\mathrm{cor}_{K\cap gHg^{-1}}^K\, \mathrm{res}_{K\cap gHg^{-1}}^{gHg^{-1}}\, gz$. ∎

Iremos agora enunciar os próximos resultados apenas para cohomologia, mas resultados similares valem também para homologia.

Proposição 2.43. *Sejam M um G-módulo e $H \subseteq G$ um subgrupo de índice finito tal que $H^n(H; M) = 0$ para algum n. Assim, $H^n(G; M)$ é anulado por $(G : H)$. Em particular, se $(G : H)$ é inversível em M (isto é, se a multiplicação por $(G : H)$ é um isomorfismo), então $H^n(G; M) = 0$.*

Demonstração. A primeira parte da demonstração segue da proposição 2.42(ii). Já para a segunda parte, basta notar que se $(G : H)$ é inversível em M, então $(G : H)$ é inversível em $H^n(G; M)$ e usando a primeira parte, segue que $H^n(G; M) = 0$. □

Podemos reescrever a proposição anterior para $n > 0$ e $H = \{1\}$:

Corolário 2.44. *Se G é finito, então $H^n(G; M)$ é anulado pela ordem de G para todo $n > 0$. Se $|G|$ é inversível em M (por exemplo, se M é um $\mathbb{Q}G$-módulo), então $H^n(G; M) = 0$ para todo $n > 0$.*

Segue que $H^n(G; M)$ admite uma decomposição primária

$$H^n(G; M) = \bigoplus_p H^n(G; M)_{(p)},$$

em que p varia sobre todos os primos que dividem $|G|$ e $H^n(G; M)_{(p)}$ é a componente p-primária de $H^n(G; M)$. Agora, fixe p e considere H um p-subgrupo de Sylow de G. Como $(G : H)$ é relativamente primo com p, pela proposição 2.42(ii), temos que $\operatorname{cor}_H^G \operatorname{res}_H^G$ é um isomorfismo em $H^n(G; M)_{(p)}$. Em particular, o morfismo de restrição induz um monomorfismo $H^n(G; M)_{(p)} \hookrightarrow H^n(H; M)_{(p)}$.

Definição 2.45. *Sejam G um grupo, $H \subseteq G$ um subgrupo e M um G-módulo. Dizemos que um elemento $z \in H^*(H; M)$ é* G-invariante *se $res^H_{H\cap gHg^{-1}} z = res^{gHg^{-1}}_{H\cap gHg^{-1}} gz$ para todo $g \in G$. Se $H \lhd G$ dizemos apenas que $z \in H^*(H; M)^{G/H}$.*

Note que se $z = \operatorname{res}_H^G w$ para algum $w \in H^*(G; M)$, então z é G-invariante.

Teorema 2.46. *Sejam G um grupo finito e H um p-subgrupo de Sylow de G. Para qualquer G-módulo M e qualquer $n > 0$, res_H^G mapeia $H^n(G; M)_{(p)}$ isomorficamente no conjunto dos elementos G-invariantes de $H^n(H; M)$. Em particular, se $H \lhd G$, então*

$$H^n(G; M)_{(p)} \cong H^n(H; M)^{G/H}.$$

Demonstração. Note que anteriormente já dissemos que o morfismo de restrição mapeia $H^n(G; M)_{(p)}$ monomorficamente nos elementos G-invariantes, assim, basta provar que qualquer invariante z está na imagem. Considere o elemento $w = \operatorname{cor}_H^G z \in H^n(G; M)$. Como $H^n(H; M)$ é anulado pela ordem de H, temos que $w \in H^n(G; M)_{(p)}$. Assim

$$\begin{aligned}
\operatorname{res}_H^G w &= \sum_{g\in H\backslash G/H} \operatorname{cor}^H_{H\cap gHg^{-1}} \operatorname{res}^{gHg^{-1}}_{H\cap gHg^{-1}} gz \\
&= \sum_{g\in H\backslash G/H} \operatorname{cor}^H_{H\cap gHg^{-1}} \operatorname{res}^{H}_{H\cap gHg^{-1}} z \\
&= \sum_{g\in H\backslash G/H} (H : H \cap gHg^{-1}) z \\
&= (G : H) z
\end{aligned}$$

em que $H\backslash G/H$ representa classes laterais duplas. Para a última igualdade, note que podemos decompor G/H em H-órbitas e que $(H : H \cap gHg^{-1})$ possui a cardinalidade das H-órbitas de gH. Como a ordem de $(G : H)$ é relativamente prima a p, temos que $z = \operatorname{res}_H^G w'$, em que $w' = w/(G : H) \in H^n(G; M)_{(p)}$. □

2.9 Produtos

2.9.1 Produtos tensoriais de resoluções

Se G e G' são grupos, M é um G-módulo e M' é um G'-módulo, então $M \otimes M'$ é um $G \times G'$-módulo ao definirmos $(g, g')(m \otimes m') = gm \otimes g'm'$. Notemos que se M é projetivo sobre $\mathbb{Z}G$ e M' é projetivo sobre $\mathbb{Z}G'$, então $M \otimes M'$ é projetivo sobre $\mathbb{Z}[G \times G']$. De fato, é suficiente verificar o caso em que $M = \mathbb{Z}G$ e $M' = \mathbb{Z}G'$, mas neste caso vale o seguinte isomorfismo: $\mathbb{Z}G \otimes \mathbb{Z}G' \cong \mathbb{Z}[G \times G']$.

Sejam $\varepsilon : F \to \mathbb{Z}$ e $\varepsilon' : F' \to \mathbb{Z}$ resoluções projetivas de $\mathbb{Z}$ sobre $\mathbb{Z}G$ e $\mathbb{Z}G'$, respectivamente, e considere o complexo $F \otimes F'$. Esse é um complexo projetivo de $\mathbb{Z}[G \times G']$-módulos e é aumentado sobre $\mathbb{Z}$ por $\varepsilon \otimes \varepsilon' : F \otimes F' \to \mathbb{Z}$. Além disso, temos também que $\varepsilon \otimes \varepsilon'$ é uma equivalência fraca, pois, como F é livre, temos que ε é uma resolução livre de $\mathbb{Z}$ como $\mathbb{Z}$-módulo, portanto, pelo corolário A.24, se ignorarmos a G-ação, ε é uma equivalência homotópica; e, da mesma forma, temos que ε' é uma equivalência homotópica. Logo, ignorando a G-ação $\varepsilon \otimes \varepsilon'$ é também uma equivalência homotópica, pela proposição A.8. Assim, pela proposição A.14 concluímos que $\varepsilon \otimes \varepsilon'$ é una equivalência fraca. Assim:

Proposição 2.47. *Se $\varepsilon : F \to \mathbb{Z}$ e $\varepsilon' : F' \to \mathbb{Z}$ são resoluções projetivas de $\mathbb{Z}$ sobre $\mathbb{Z}G$ e $\mathbb{Z}G'$, respectivamente, então $\varepsilon \otimes \varepsilon' : F \otimes F' \to \mathbb{Z}$ é uma resolução projetiva de $\mathbb{Z}$ sobre $\mathbb{Z}[G \times G']$.*

Corolário 2.48. *Se $\varepsilon : F \to \mathbb{Z}$ e $\varepsilon' : F' \to \mathbb{Z}$ são resoluções projetivas de $\mathbb{Z}$ sobre $\mathbb{Z}G$, então $\varepsilon \otimes \varepsilon' : F \otimes F' \to \mathbb{Z}$ também é, em que G age diagonalmente em $F \otimes F'$.*

Demonstração. Segue de 2.47 pela restrição por escalares com respeito ao mergulho da "diagonal", isto é, $G \to G \times G$ em que $g \mapsto (g, g)$ □

Note que, se $F = F'$ no corolário 2.48, temos dois morfismos $F \otimes F \to \mathbb{Z}$ de resoluções: o morfismo $F \otimes \varepsilon : F \otimes F \to F \otimes \mathbb{Z} = F$ e o morfismo $\varepsilon \otimes F : F \otimes F \to \mathbb{Z} \otimes F = F$. Sabemos também, pelo teorema A.23 que existem G-morfismos de cadeias $\Delta : F \to F \otimes F$ que preservam aumento e que quaisquer dois são homotópicos.

Definição 2.49. *Qualquer morfismo $\Delta : F \to F \otimes F$ é chamado de* aproximação da diagonal.

Exemplo 2.50. No caso em que F é a resolução standard, é conhecida uma aproximação da diagonal, chamada de morfismo de Alexander-Whitney é dado por:

$$\Delta(g_0, \dots, g_n) = \sum_{p=0}^{n} (g_0, \dots, g_p) \otimes (g_p, \dots g_n).$$

Colocando o morfismo na notação bar, temos

$$\Delta[g_1| \dots |g_n] = \sum_{p=0}^{n} [g_1| \dots |g_p] \otimes g_1 \dots g_p [g_{p+1}| \dots |g_n].$$

2.9.2 Produto Cruzado

Consideremos G, G' grupos, F e F' resoluções projetivas de $\mathbb{Z}$ sobre $\mathbb{Z}G$ e $\mathbb{Z}G'$, respectivamente. Para quaisquer G-módulo M e G'-módulo M' existe o morfismo

$$\begin{aligned} (F \otimes_G M) \otimes (F' \otimes_{G'} M') &\to (F \otimes F') \otimes_{G \times G'} (M \otimes M') \\ (x \otimes m) \otimes (x' \otimes m') &\mapsto (x \otimes x') \otimes (m \otimes m'). \end{aligned} \tag{2.24}$$

Se $z \in F \otimes_G M$ e $z' \in F' \otimes_{G'} M'$, então denotaremos por $z \times z'$ a imagem de $z \otimes z'$ sobre este morfismo. Assim, temos $\partial(z \times z') = \partial z \times z' + (-1)^p z \times \partial z'$ se $\deg z = p$. Portanto, o produto de dois ciclos é um ciclo cuja classe de homologia depende apenas das classes dos ciclos dados. Assim, pelo teorema 2.47, obtemos um produto induzido:

$$H_p(G, M) \otimes H_q(G', M') \to H_{p+q}(G \times G', M \otimes M'). \tag{2.25}$$

Também denotamos por $z \otimes z' \mapsto z \times z'$ o produto (2.25), o qual está bem definido independentemente das escolhas das resoluções F e F'. De fato, sejam a, $a' \in Z_p(G, M)$, b, $b' \in Z_q(G', M')$. Queremos definir $[a] \times [b] \in H_{p+q}(G \times G'; M \otimes M')$, e esperamos que $[a \times b] = [a] \times [b]$. Como a e b são ciclos, temos que $\partial(a \times b) = \partial a \times b + (-1)^p a \times \partial b = 0$, ou seja, $a \times b$ é um ciclo. Precisamos mostrar ainda que a classe de homologia depende apenas da classe de homologia que começamos, isto é, que está bem definido. Consideremos a', b' dois ciclos na mesma classe de homologia, queremos que $[a \times b] = [a' \times b']$, isto é, que a diferença entre $a \times b$ e $a' \times b'$ seja um cobordo. Consideremos $a' = a + \partial\bar{a}$ e $b' = b + \partial\bar{b}$, assim $a' \times b' = (a + \partial\bar{a}) \times (b + \partial\bar{b}) = a \times b + a \times \partial\bar{b} + \partial\bar{a} \times b + \partial\bar{a} \times \partial\bar{b}$, mas $\partial(a \times \bar{b}) = \partial a \times \bar{b} + (-1)^p a \times \partial\bar{b} = (-1)^p a \times \partial\bar{b}$, pois $\partial a = 0$, de forma similar para $\partial(\bar{a} \times b) = \partial\bar{a} \times b$, e também temos que $\partial(\bar{a} \times \partial\bar{b}) = \partial\bar{a} \times \partial\bar{b} + (-1)^p \bar{a} \times \partial^2\bar{b} = \partial\bar{a} \times \partial\bar{b}$, pois $\partial^2 = 0$, logo $a' \times b' - a \times b = \partial((-1)^p(a \times \bar{b}) + (\bar{a} \times b) + (\bar{a} \times \partial\bar{b}))$, portanto o produto está bem definido.

Definição 2.51. *O produto induzido acima* (2.25)*, é chamado de* produto cruzado em homologia.

Similarmente, dadas cocadeias $u \in \mathscr{H}om_G(F; M)$ e $u' \in \mathscr{H}om_{G'}(F'; M')$, definimos $u \times u' \in \mathscr{H}om_{G \times G'}(F \otimes F', M \otimes M')$ como o produto tensorial dos morfismos u e u' como definimos em A.7; portanto $\langle u \times u', x \otimes x' \rangle = (-1)^{\deg u' \cdot \deg x} \langle u, x \rangle \otimes \langle u', x' \rangle$. E pela proposição A.8 podemos verificar que $\delta(u \times u') = \delta u \times u' + (-1)^p u \times \delta u'$ se $\deg u = p$.

Definição 2.52. *O produto induzido $H^p(G; M) \otimes H^q(G'; M') \to H^{p+q}(G \times G', M \otimes M')$ é chamado de* produto cruzado em cohomologia.

2.9.3 Produto Cup

Anteriormente, lidamos com produtos que envolviam três grupos: G, G', $G \times G'$. Nesta seção iremos tratar com homologia e cohomologia utilizando apenas um único grupo G. Escreveremos $C_*(G, M)$ para $F \otimes_G M$ e $C^*(G, M)$ para $\mathscr{H}om_G(F, M)$.

Definição 2.53. *Dados $u \in H^p(G, M)$ e $v \in H^q(G, N)$, definimos o* produto cup *de u e v, denotado por $u \smile v$, como o elemento $d^*(u \times v) \in H^{p+q}(G, M \otimes N)$, em que $d : G \to G \times G$ é o morfismo diagonal. Neste caso, $M \otimes N$ possui a G-ação diagonal.*

Note que o produto cup é induzido pelo seguinte produto em nível de cocadeia: sejam F e F' resoluções projetivas de $\mathbb{Z}$ sobre $\mathbb{Z}G$. Pelo corolário 2.48, temos que $F \otimes F'$ com a G-ação diagonal também é uma resolução projetiva de $\mathbb{Z}$ sobre $\mathbb{Z}G$. Dados $u \in \mathscr{H}om_G(F; M)$ e $v \in \mathscr{H}om_G(F'; N)$, defina $u \smile v$ como $u \times v$, como feito anteriormente, mas visto como sendo um elemento de $\mathscr{H}om_G(F \otimes F'; M \otimes N)$. Se quisermos usar apenas uma resolução projetiva F, então escolhemos uma aproximação da diagonal $\Delta : F \to F \otimes F$ e definimos $u \smile v = (u \times v) \circ \Delta \in \mathscr{H}om_G(F; M \otimes N)$ para $u \in \mathscr{H}om_G(F; M)$ e $v \in \mathscr{H}om_G(F; N)$.

Exemplo 2.54. Se F é a resolução bar e Δ é o morfismo Alexander-Whitney, definido no exemplo 2.50, então o produto de $u \in C^p(G, M)$ e $v \in C^q(G, N)$ é o elemento $u \smile v \in C^{p+q}(G, M \otimes N)$, dado por:

$$(u \smile v)(g_1, \ldots, g_{p+q}) = (-1)^{pq} u(g_1, \ldots, g_p) \otimes g_1 \ldots g_p v(g_{p+1}, \ldots, g_{p+q})$$

Iremos listar agora algumas propriedades do produto cup:

Propriedades 2.55.

(1) Dimensão zero: O produto cup $H^0(G;M) \otimes H^0(G;N) \to H^0(G;M \times N)$ é o morfismo $M^G \otimes N^G \to (M \otimes N)^G$ induzido pelas inclusões $M^G \hookrightarrow M$ e $N^G \hookrightarrow N$.

(2) Naturalidade com respeito ao morfismo com coeficientes: Dados morfismos de G-módulos $f : M \to M'$ e $g : N \to N'$ e elementos $u \in H^*(G,M)$ e $v \in H^*(G,N)$, temos $(f \otimes g)_*(u \smile v) = f_*u \smile g_*v$ em $H^*(G, M' \otimes N')$, em que $f_* = H^*(G,f)$ e $g_* = H^*(G,g)$.

(3) Compatibilidade com δ: Seja $0 \to M' \to M \to M'' \to 0$ uma sequência exata curta de G-módulos e seja N um G-módulo tal que a sequência $0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$ é exata. Temos $\delta(u \smile v) = \delta u \smile v$ para todos $u \in H^p(G;M'')$ e $v \in H^q(G;N)$, isto é, o quadrado abaixo comuta:

$$\begin{tikzcd}
H^p(G;M'') \arrow[r, "\delta"] \arrow[d, "-\smile v"'] & H^{p+1}(G;M') \arrow[d, "-\smile v"] \\
H^{p+q}(G;M'' \otimes N) \arrow[r, "\delta"] & H^{p+q+1}(G;M' \otimes N)
\end{tikzcd} \tag{2.26}$$

Para conseguirmos provar a compatibilidade com δ, consideraremos o diagrama comutativo abaixo:

$$\begin{tikzcd}
0 \arrow[r] & C^*(G;M') \arrow[r] \arrow[d] & C^*(G;M) \arrow[r] \arrow[d] & C^*(G;M'') \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & C^*(G;M' \otimes N) \arrow[r] & C^*(G;M \otimes N) \arrow[r] & C^*(G;M'' \otimes N) \arrow[r] & 0
\end{tikzcd}$$

em que os morfismos verticais são dados pelo produto cup à direita com um cociclo fixado em $C^q(G,N)$ representando v. Esses morfismos na vertical comutam com o operador de cobordo δ em $C^*(G,-)$, assim a fórmula $\delta(a \smile b) = \delta a \smile b + (-1)^{\deg a} a \smile \delta b$ se reduz a $\delta(a \smile b) = \delta a \smile b$, se b é um cociclo . Logo, o diagrama 2.26 comuta pela naturalidade dos morfismos de conexão com respeito aos morfismos de sequências exatas curtas.

(3') Se $0 \to N' \to N \to N'' \to 0$ é uma sequência exata curta tal que $0 \to M \otimes N' \to M \otimes N \to M \otimes N'' \to 0$ é exata, então $\delta(u \smile v) = (-1)^p u \smile \delta v$ em $H^{p+q+1}(G;M \otimes N')$ para quaisquer $u \in H^p(G;M \otimes N')$, $v \in H^q(G,N'')$. Podendo ser provado de maneira semelhante ao item (3) utilizando argumentos de mudança de dimensão.

(4) Existência do elemento neutro: O elemento $1 \in H^0(G;\mathbb{Z}) = \mathbb{Z}$ satisfaz $1 \smile u = u = u \smile 1$ para todo $u \in H^*(G;M)$. Isto segue diretamente da fórmula de Alexander-Whitney, dada no exemplo 2.54.

(5) Associatividade: Dados $u_i \in H^*(G;M_i)$, para $(i = 1,2,3)$, temos $(u_1 \smile u_2) \smile u_3 = u_1 \smile (u_2 \smile u_3)$ em $H^*(G;M_1 \otimes M_2 \otimes M_3)$. Note que, em nível de cocadeia, a associatividade vale como uma identidade em $\mathscr{H}om_G(F \otimes F \otimes F; M_1 \otimes M_2 \otimes M_3)$.

(6) Naturalidade com respeito a morfismos de grupos: Dado $\alpha : H \to G$, temos que $\alpha^*(u \smile v) = \alpha^* u \smile \alpha^* v$, para quaisquer $u \in H^*(G;M)$, $v \in H^*(G;N)$. Este fato segue diretamente pela definição.

(7) Fórmula do transfer: Suponha que $H \subseteq G$ seja um subgrupo de índice finito. Para quaisquer $u \in H^*(G;M)$ e $v \in H^*(H;N)$, temos que $\mathrm{cor}_H^G(\mathrm{res}_H^G(u) \smile v) = u \smile \mathrm{cor}_H^G v$. De fato, seja F uma resolução projetiva de $\mathbb{Z}$ sobre $\mathbb{Z}G$. Provaremos a fórmula em nível de cocadeia.

Dados $u \in \mathscr{H}om(F, M)^G$ e $v \in \mathscr{H}om(F, N)^H$, temos, em $\mathscr{H}om(F \otimes F; M \otimes N)^G$

$$\begin{aligned}
\operatorname{cor}_H^G(\operatorname{res}_H^G(u) \smile v) &= \sum_{g \in G/H} g \cdot (u \otimes v) \\
&= \sum_{g \in G/H} u \otimes gv \ \ (u \text{ é invariante}) \\
&= u \otimes \sum_{g \in G/H} gv \\
&= u \smile \operatorname{cor}_H^G v.
\end{aligned}$$

Em particular, note que, por essa fórmula, o morfismo transfer $H^*(H; k) \to H^*(G; k)$, em que k é um anel comutativo qualquer, é um morfismo de $H^*(G; k)$-módulos, em que $H^*(H; k)$ é visto como um $H^*(G; k)$-módulo pelo morfismo de restrição $H^*(G; k) \to H^*(H; k)$.

2.9.4 Produto Cap

Se F é uma resolução projetiva de $\mathbb{Z}$ sobre $\mathbb{Z}G$, então existe um morfismo de complexos de cadeia

$$\begin{aligned}
\gamma : \mathscr{H}om_G(F, M) \otimes ((F \otimes F) \otimes_G N) &\to F \otimes_G (M \otimes N) \\
u \otimes (x \otimes y \otimes n) &\mapsto (-1)^{\deg u \cdot \deg x} x \otimes u(y) \otimes n.
\end{aligned}$$

Definição 2.56. *Sejam $u \in \mathscr{H}om_G(F, M)^p = \mathscr{H}om_G(F, M)_{-p}$ e $z \in (F \otimes F)_q \otimes_G N$. Chamamos de* produto cap *de u e z o elemento $\gamma(u \otimes z)$ de $F_{q-p} \otimes_G (M \otimes N)$ o denotamos por $u \frown z$.*

Utilizamos a mesma notação e terminologia para o produto induzido

$$H^p(G, M) \otimes H_q(G, N) \to H_{q-p}(G, M \otimes N).$$

Como no produto cup, podemos utilizar a aproximação da diagonal $\Delta : F \to F \otimes F$ para calcular o produto cap em termos de apenas uma resolução F. Basta compor γ com o morfismo

$$\operatorname{id} \otimes (\Delta \otimes \operatorname{id}) : \mathscr{H}om_G(F, M) \otimes (F \otimes_G N) \to \mathscr{H}om_G((F \otimes F) \otimes_G N).$$

O produto cap pode ser motivado pelo fato que ele é *adjunto* ao produto cup, como explicaremos a seguir. Considere o morfismo de avaliação:

$$\begin{aligned}
\mathscr{H}om_G(F, M) \otimes (F \otimes_G N) &\to M \otimes_G N \\
u \otimes (x \otimes n) &\mapsto u(x) \otimes n.
\end{aligned}$$

Denotamos por $\langle u, z \rangle$ a imagem de $u \otimes z$ por esse morfismo. O morfismo de avaliação é um morfismo de cadeia, isto é, $\langle \delta u, z \rangle + (-1)^{\deg u} \langle u, \delta z \rangle = 0$. Conseguimos então o morfismo induzido

$$H^p(G; M) \otimes H_p(G; N) \to M \otimes_G N,$$

que ainda denotamos por $\langle \cdot, \cdot \rangle$ e que é independente da escolha da resolução F. Note que, para quaisquer $u \in H^p(G; M_1)$, $v \in H^q(G; M_2)$ e $z \in H_{p+q}(G; M_3)$, temos

$$\langle u \smile v, z \rangle = \langle u, v \frown z \rangle,$$

em que os dois lados da equação estão em $(M_1 \otimes M_2 \otimes M_3)_G$. Se $u = 1 \in H^0(G; \mathbb{Z})$, obtemos o seguinte para quaisquer $v \in H^q(G; M)$ e $z \in H_q(G; N)$, temos $v \frown z = \langle v, z \rangle$ em $H_0(G; M \otimes N) = M \otimes_G N$.

Além disso, o produto cap também possui propriedades análogas às da proposição 2.55 referentes ao produto cup.

3 COHOMOLOGIA E EXTENSÕES DE GRUPOS

Neste capítulo definimos extensão de grupo, mostramos como uma ação de um grupo G em um grupo abeliano A, transforma A em um G-módulo. Mostramos também dois importantes teoremas para nosso estudo, são eles o 3.6 e o 3.7, que mostram como os grupos H^2 e H^3 classificam extensões.

3.1 Preliminares

Definição 3.1. *Uma* extensão *de um grupo A por um grupo G (ou uma* extensão de A por G*) é uma sequência exata curta de grupos*

$$1 \to A \to E \to G \to 1. \tag{3.1}$$

Definição 3.2. *Uma segunda extensão $1 \to A \to E' \to G \to 1$ de A por G é dita* equivalente à (3.1) *se existe um morfismo $E \to E'$ fazendo o diagrama*

$$\begin{tikzcd}
 & & E \arrow[dd, "\alpha"] \arrow[dr, "\psi"] & & \\
1 \arrow[r] & A \arrow[ur, "\varphi"] \arrow[dr, "\varphi'"'] & & G \arrow[r] & 1 \\
 & & E' \arrow[ur, "\psi'"'] & &
\end{tikzcd}$$

comutar.

Note ainda que tal morfismo α é necessariamente um isomorfismo. De fato, seja $k \in \ker\alpha$, assim $\psi'(\alpha(k)) = \psi(k)$, assim $\psi(k) = \psi'(1) = 1$, portanto $k \in \ker(\psi) = \mathrm{im}(\varphi)$, deste modo, existe $n \in A$ tal que $\varphi(n) = k$, assim $\alpha(\varphi(n)) = \varphi'(n) = 1$, logo $n = 1$ o que nos dá $k = 1$, logo α é injetiva. Seja $e' \in E'$, assim $\psi'(e') \in G$, logo existe $e \in E$ tal que $\psi(e) = \psi'(e')$, então $\psi'(\alpha(e)) = \psi(e) = \psi'(e')$, logo $\alpha(e)^{-1}e' \in \ker(\psi') = \mathrm{im}(\varphi')$, assim existe $n \in A$ tal que $\varphi'(n) = \alpha(e)^{-1}e'$, portanto $(\alpha \circ \varphi)(n) = \varphi'(n) = \alpha(e)^{-1}e'$, assim $\alpha(e)\alpha(\varphi(n)) = e'$, ou seja, $\alpha(e\varphi(n)) = e'$ assim α é sobrejetiva.

Por enquanto consideraremos o caso em que o núcleo A é um grupo abeliano A'. Uma característica especial desse caso é que uma extensão

$$0 \to A' \xrightarrow{i} E \xrightarrow{\pi} G \to 1$$

dá origem a uma ação de G em A', tornando A' um G-módulo. De fato, dado $g \in G$, seja $\tilde{g} \in E$ tal que $\pi(\tilde{g}) = g$. Assim a ação de G em A' é caracterizada por

$$i(ga) = \tilde{g}i(a)\tilde{g}^{-1}. \tag{3.2}$$

Note que a igualdade acima não depende da escolha de $\tilde{g}$. De fato, se $g' \in E$ é tal que $\pi(g') = \pi(\tilde{g})$, então $\tilde{g}^{-1}g' \in \ker(\pi) = i(A')$. Logo, existe $b \in A'$, tal que $i(b) = \tilde{g}^{-1}g'$ e portanto $\tilde{g}i(b) = g'$. Assim,

$$g'i(a)g'^{-1} = \tilde{g}i(b)i(a)i(b)^{-1}\tilde{g}^{-1} = \tilde{g}i(bab^{-1})\tilde{g}^{-1} = \tilde{g}i(a)\tilde{g}^{-1}.$$

É frequentemente conveniente reescrever (3.2) como uma regra de comutatividade

$$\tilde{g}i(a) = i(ga)\tilde{g}. \tag{3.3}$$

Em particular, isto mostra que, $i(A')$ é central em E se, e somente se, a G-ação é trivial. Neste caso, a extensão é dita *extensão central*.

3.2 Extensões de grupo, H^2 e H^3

Nesta seção, além do livro [5], também foi utilizado o artigo [6] para referências.

Considere A e G grupos, com A não abeliano. Veremos nesta seção como os grupos de cohomologia $H^2(G; Z(A))$ e $H^3(G; Z(A))$ classificam extensões de A por G. Considere a extensão de A por G

$$1 \to A \to E \xrightarrow{\pi} G \to 1$$

em que $A = ker(\pi)$ e $A \subseteq E$, isto é, A é um subgrupo normal de E. Para $g \in G$, escolha $x_g \in E$ em que $\pi(x_g) = g$, e note que x_g é determinado a menos de multiplicação por um elemento de A. Como A é normal em E, a conjugação por x_g se restringe a um automorfismo de A, isto é, existe uma automorfismo ω_g de A dado por $\omega_g(a) = x_g a x_g^{-1}$. Note que a função $\omega : G \to \operatorname{Aut}(A)$ tal que $\omega(g) = \omega_g$ não precisa ser um morfismo de grupos, diferentemente de quando A é abeliano. Ademais, $\omega_g \omega_h \omega_{gh}^{-1}$ é a conjugação por $x_g x_h x_{gh}^{-1}$ que não precisa ser a identidade em A. Porém, considere $f(g, h) = x_g x_h x_{gh}^{-1}$, que pertence a A, pois $\pi(x_g x_h x_{gh}^{-1}) = 1$. Desse modo, temos uma função $\omega : G \to \operatorname{Aut}(A)$ e uma função $f : G \times G \to A$, tal que

$$\omega_g \omega_h = \operatorname{Inn}(f(g, h))\omega_{gh}, \tag{3.4}$$

em que $\operatorname{Inn}(a)$ é o automorfismo interno de conjugação por a. Assim, $\operatorname{Inn}(f(g, h))\omega_{gh}(a) = f(g, h)\omega_{gh}(a)f(g, h)^{-1}$. Além disso, a associatividade em E nos dá a *condição de cociclo generalizado*

$$f(g, h)f(gh, k) = \omega_g(f(h, k))f(g, hk). \tag{3.5}$$

Outro ponto de vista da função ω é considerar o grupo dos automorfismos externos, isto é: $\operatorname{Out}(A) = \operatorname{Aut}(A)/\operatorname{Inn}(A)$, em que $\operatorname{Inn}(A)$ é o grupo dos automorfismo internos. Note que a equação (3.4) dá origem a um morfismo $\bar{\omega} : G \to \operatorname{Out}(A)$ tal que $\bar{\omega} = q \circ \omega$, em que $q\colon \operatorname{Aut}(A) \to \operatorname{Out}(A)$ é a aplicação quociente. Logo, dada uma extensão de grupo, obtemos um par de funções (ω, f) que satisfazem as equações (3.4) e (3.5) anteriores, e que ω induz um morfismo de grupos $G \to \operatorname{Out}(A)$. Podemos assim definir uma relação de equivalência nesses pares em que mudamos o x_g para $y_g = a_g x_g$ com $a_g \in A$. Com esta nova mudança, se definirmos (ω', f') por $\omega'_g = \operatorname{Inn}(a_g x_g) = \operatorname{Inn}(a_g)\omega_g$ e $f'(g, h) = y_g y_h y_{gh}^{-1}$, teremos

$$\begin{aligned} f'(g, h) &= a_g x_g a_h x_h (a_{gh} x_{gh})^{-1} \\ &= a_g x_g a_h x_h x_{gh}^{-1} a_{gh}^{-1} \\ &= a_g x_g a_h x_g^{-1} x_g x_h x_{gh}^{-1} a_{gh}^{-1} \\ &= a_g (x_g a_h x_g^{-1})(x_g x_h x_{gh}^{-1}) a_{gh}^{-1} \\ &= a_g \omega_g(a_h) f(g, h) a_{gh}^{-1}. \end{aligned} \tag{3.6}$$

Desta forma, temos que dois pares (ω, f) e (ω', f') são ditos *equivalentes* se para cada $g \in G$, existe $a_g \in A$ com $\omega'_g = \operatorname{Inn}(a_g)\omega_g$ e $f'(g, h) = a_g \omega_g(a_h) f(g, h) a_{gh}^{-1}$. Essa relação é de fato uma relação de equivalência:

(i) Reflexividade: é claro que $(\omega, f) \sim (\omega, f)$.

(ii) Simetria: como $(\omega, f) \sim (\omega', f')$, temos $\omega'_g = \operatorname{Inn}(a_g)\omega_g$ e $f'(g, h) = a_g \omega_g(a_h) f(g, h) a_{gh}^{-1}$, portanto $\omega_g = \operatorname{Inn}(a_g)^{-1}\omega'_g$ e queremos que $f(g, h) = a_g^{-1}\omega'_g(a_h^{-1}) f'(g, h) a_{gh}$. Mas por (3.6):

$$\begin{aligned} \omega_g(a_h)^{-1} a_g^{-1} f'(g, h) a_{gh} &= f(g, h) \\ (a_g^{-1}\omega'_g(a_h) a_g)^{-1} a_g^{-1} f'(g, h) a_{gh} &= f(g, h) \\ a_g^{-1}\omega'_g(a_h^{-1}) a_g a_g^{-1} f'(g, h) a_{gh} &= f(g, h). \end{aligned}$$

Logo $f(g, h) = a_g^{-1}\omega'_g(a_h^{-1}) f'(g, h) a_{gh}$ e $(\omega', f') \sim (\omega, f)$.

(iii) Transitividade: suponha $(\omega, f) \sim (\omega', f')$ e $(\omega', f') \sim (\bar{\omega}, \bar{f})$. Assim temos $\omega'_g = \mathrm{Inn}(a_g)\omega_g$, $f'(g,h) = a_g\omega_g(a_h)f(g,h)a_{gh}^{-1}$, $\bar{\omega}_g = \mathrm{Inn}(b_g)^{-1}\omega'_g$ e $\bar{f}(g,h) = b_g\omega'_g(b_h)f'(g,h)b_{gh}^{-1}$. Portanto $\bar{\omega}_g = \mathrm{Inn}(b_g a_g)\omega_g$ e queremos mostrar que $\bar{f}(g,h) = b_g a_g \omega_g(b_h a_h) f(g,h)(b_{gh}a_{gh})^{-1}$. Temos

$$\begin{aligned}
\bar{f}(g,h) &= b_g\omega'_g(b_h)f'(g,h)b_{gh}^{-1} \\
&= b_g\omega'_g(b_h)(a_g\omega_g(a_h)f(g,h)a_{gh}^{-1})b_{gh}^{-1} \\
&= b_g((\mathrm{Inn}(a_g)\omega_g)(b_h))a_g\omega_g(a_h)f(g,h)(b_{gh}a_{gh})^{-1} \\
&= b_g(a_g\omega_g(b_h)a_g^{-1})a_g\omega_g(a_h)f(g,h)(b_{gh}a_{gh})^{-1} \\
&= b_g a_g\omega_g(b_h)\omega_g(a_h)f(g,h)(b_{gh}a_{gh})^{-1} \\
&= b_g a_g\omega_g(b_h a_h)f(g,h)(b_{gh}a_{gh})^{-1}.
\end{aligned}$$

Logo $(\omega, f) \sim (\bar{\omega}, \bar{f})$.

Definição 3.3. *O par (ω, f) que definimos anteriormente é chamado de* cociclo generalizado.

Agora, ao invés de começarmos com uma extensão de grupo, começaremos com A e G grupos e suponhamos que existe um morfismo de grupos $\bar{\omega} : G \to \mathrm{Out}(A)$. Veremos quando existe uma extensão de A por G induzindo $\bar{\omega}$; e, se existem extensões dessa forma, quando é possível classificá-las.

Para encontrar uma extensão de A por G induzindo $\bar{\omega}$, escolhemos para cada $g \in G$, um levantamento $\xi_g \in \mathrm{Aut}(A)$ de ω_g, ou seja, escolhemos um representante ξ_g para a classe lateral ω_g em $\mathrm{Out}(A)$.

$$\begin{tikzcd}
G \arrow[r, "\xi"] \arrow[dr, "\bar{\omega}"'] & \mathrm{Aut}(A) \arrow[d, "q"] \\
& \mathrm{Out}(A)
\end{tikzcd}$$

Note que podemos escolher $\xi_g = \mathrm{id}$ quando $g = 1$. Portanto $\xi_g\xi_h\xi_{gh}^{-1} \in \mathrm{Inn}(A)$ já que é um levantamento de $\bar{\omega_g}\bar{\omega_h}\bar{\omega_{gh}}^{-1} = 1 \in \mathrm{Out}(A)$. Escolhemos um elemento $f(g,h) \in A$ com $\xi_g\xi_h\xi_{gh}^{-1} = \mathrm{Inn}(f(g,h))$ e, note que podemos escolher $f(g,h) = 1$ se $g = 1$ ou $h = 1$ pois em ambos os casos $\xi_g\xi_h\xi_{gh}^{-1} = \mathrm{id}$. Se (ω, f) é um cociclo generalizado, podemos então produzir uma extensão E de A por G da seguinte forma: seja $E = A \times G$ e definimos uma operação em E por:

$$(a,g)(b,h) = (a\omega_g(b)f(g,h), gh). \tag{3.7}$$

Mostremos então que E é um grupo com tal operação:

(i) Elemento neutro: Note que

$$(a,g)(1,1) = (a\omega_g(1)f(g,1), 1) = (a,g)$$

e

$$(1,1)(a,g) = (1\omega_1(a)f(1,g), g) = (a,g),$$

logo $(1,1)$ é o elemento neutro.

(ii) Inverso: Note que

$$\begin{aligned}
(a,g)(\omega_{g^{-1}}(a^{-1}), g^{-1}) &= (a\omega_g(\omega_{g^{-1}}(a^{-1}))f(g,g^{-1}), gg^{-1}) \\
&= (1,1)
\end{aligned}$$

e

$$\begin{aligned}(\omega_{g^{-1}}(a^{-1}), g^{-1})(a,g) &= (\omega_{g^{-1}}(a^{-1})\omega_{g^{-1}}(a)f(g^{-1},g), g^{-1}g)\\ &= (\omega_{g^{-1}}(a^{-1}a), 1)\\ &= (1,1)\end{aligned}$$

assim temos que o inverso de (a,g) é $(\omega_{g^{-1}}(a^{-1}), g^{-1})$.

(iii) Associatividade: Sejam a, b, $c \in A$ e g, h, $k \in G$, temos:

$$\begin{aligned}((a,g)(b,h))(c,k) &= (a\omega_g(b)f(g,h), gh)(c,k)\\ &= (a\omega_g(b)f(g,h)\omega_{gh}(c)f(gh,k), ghk)\\ &= (a\omega_g(b)f(g,h)\omega_{gh}(c)f(g,h)^{-1}\omega_g(f(h,k))f(g,hk), ghk)\\ &= (a\omega_g(b)\operatorname{Inn}(f(g,h))\omega_{gh}(c)\omega_g(f(h,k))f(g,hk), ghk)\\ &= (a\omega_g(b)\omega_g(\omega_h(c))\omega_g(f(h,k))f(g,hk), ghk)\\ &= (a\omega_g(b\omega_h(c)f(h,k))f(g,hk), ghk)\\ &= (a,g)(b\omega_h(c)f(h,k), hk)\\ &= (a,g)((b,h)(c,k))\end{aligned}$$

Note ainda que as funções $a \mapsto (a,1)$ e $(a,g) \mapsto g$ são morfismos de grupo, e que $1 \to A \to E \to G \to 1$ é uma extensão de A por G; escolhemos $\xi_1 = \mathrm{id}$ e $f(g,h) = 1$ se $g = 1$ ou $h = 1$ para mostrar que o morfismo $A \to E$ é um morfismo de grupos. Entretanto, existe a possibilidade de f não satisfazer a condição de cociclo generalizado, mas podemos dizer que

$$\operatorname{Inn}(f(g,h)f(gh,k)) = \xi_g\xi_h\xi_{gh}^{-1}\xi_{gh}\xi_k\xi_{ghk}^{-1} = \xi_g\xi_h\xi_k\xi_{ghk}^{-1}. \tag{3.8}$$

E temos também que

$$\operatorname{Inn}(\omega_g(f(h,k))f(g,hk)) = \xi_g(\xi_h\xi_k\xi_{hk}^{-1}\xi_g^{-1})\xi_g\xi_{hk}\xi_{ghk}^{-1} = \xi_g\xi_h\xi_k\xi_{ghk}^{-1}.$$

Assim, podemos ver que $f(g,h)f(gh,k)$ e $\omega_g(f(h,k))f(g,k)$ conjugam A da mesma forma que em (3.8). Temos que $\operatorname{Inn}(a) = \operatorname{Inn}(b)$ se, e somente se, $a \equiv b \pmod{Z(A)}$, em que $Z(A)$ é o centro do grupo A. Logo existe $c(g,h,k) \in Z(A)$ que satisfaz

$$f(g,h)f(gh,k) = c(g,h,k)\omega_g(f(h,k))f(g,k). \tag{3.9}$$

Teorema 3.4. *O elemento $c = c(g,h,k)$ é um 3-cociclo.*

Demonstração. Considere a expressão:

$$J = \omega_g(\omega_h(f(k,l))f(h,kl))f(g,hkl).$$

Por um lado, note que, usando (3.9) três vezes e que $c(g,h,k) \in Z(A)$ para todo g, h, k, temos

$$\begin{aligned}J &= \omega_g((c(h,k,l)f(h,k)f(hk,l))f(g,hkl)\\ &= \omega_g(c(h,k,l)f(h,k))\omega_g(f(hk,l))f(g,hkl)\\ &= \omega_g(c(h,k,l)f(h,k))c(g,hk,l)f(g,hk)f(ghk,l)\\ &= \omega_g(c(h,k,l))c(g,hk,l)\omega_g(f(h,k))f(g,hk)f(ghk,l)\\ &= \omega_g(c(h,k,l))c(g,hk,l)\omega_g(f(h,k))f(g,hk)f(ghk,l)\\ &= \omega_g(c(h,k,l))c(g,hk,l)c(g,h,k)f(g,h)f(gh,k)f(ghk,l)\\ &= g(c(h,k,l))c(g,hk,l)c(g,h,k)f(g,h)f(gh,k)f(ghk,l).\end{aligned}$$

Por outro lado, se usarmos (3.4) teremos

$$\begin{aligned} J &= \mathrm{Inn}(f(g,h))\omega_{gh}(f(k,l))\omega_g(f(h,kl))f(g,hkl) \\ &= f(g,h)\omega_{gh}(f(k,l))f(g,h)^{-1}\omega_g(f(h,kl))f(g,hkl) \\ &= f(g,h)\omega_{gh}(f(k,l))f(g,h)^{-1}f(g,h)c(g,h,kl)f(gh,kl) \\ &= f(g,h)\omega_{gh}(f(k,l))c(g,h,kl)f(gh,kl) \\ &= c(g,h,kl)f(g,h)\omega_{gh}(f(k,l))f(gh,kl) \\ &= c(g,h,kl)c(gh,k,l)f(g,h)f(gh,k)f(ghk,l). \end{aligned}$$

Comparando as expressões acima, temos

$$g(c(h,k,l))c(g,hk,l)c(g,h,k) = c(g,h,kl)c(gh,k,l)$$

$$g(c(h,k,l))c(g,hk,l)c(g,h,k)c(gh,k,l)^{-1}c(g,h,kl)^{-1} = 1$$

que é compatível com o que sabemos da resolução bar. Assim, c é um 3-cociclo. □

Temos que c representa um elemento de $H^3(G; Z(A))$.

Lema 3.5. *Se mudarmos f em (3.4), temos que c será trocado por um cociclo na mesma classe de cohomologia.*

Demonstração. Notemos que qualquer outra escolha de $f(g,h)$ em (3.4) será da forma

$$f'(g,h) = \eta(g,h)f(g,h)$$

para $\eta(g,h) \in Z(A)$. Calculando c' em (3.5) utilizando a f' anterior, temos:

$$\begin{aligned} c'(g,h,k) &= \omega_g(f'(h,k))f'(g,hk)f'(gh,k)^{-1}f'(g,h)^{-1} \\ &= \omega_g(\eta(h,k)f(h,k))\eta(g,hk)f(g,hk) \\ &\qquad f(gh,k)^{-1}\eta(gh,k)^{-1}f(g,h)^{-1}\eta(g,h)^{-1} \\ &= g\,\eta(h,k)\omega_g(f(h,k))\eta(g,hk)f(g,hk) \\ &\qquad f(gh,k)^{-1}\eta(gh,k)^{-1}f(g,h)^{-1}\eta(g,h)^{-1} \\ &= g\,\eta(h,k)(c(g,h,k)f(g,h)f(gh,k)f(g,hk)^{-1}) \\ &\qquad f(g,h,k)f(gh,k)^{-1}f(g,h)^{-1} \\ &\qquad \eta(gh,k)^{-1}\eta(g,hk)^{-1}\eta(g,h)^{-1} \\ &= g\,c(g,h,k)\eta(h,k)\eta(gh,k)^{-1}\eta(g,hk)\eta(g,h)^{-1} \end{aligned}$$

e note que $g\,\eta(h,k)\eta(gh,k)^{-1}\eta(g,hk)\eta(g,h)^{-1}$ é o cobordo $\delta(\eta(g,h,k))$. Como o cobordo é arbitrário, provamos o que queríamos. □

Teorema 3.6. *Seja c um 3-cociclo. Existe uma extensão de grupo de A por G induzindo o morfismo $\bar{\omega} : G \to \mathrm{Out}(A)$ se, e somente se, a classe de c em $H^3(G; Z(A))$ é trivial.*

Demonstração. ($\Rightarrow$) Suponhamos que exista uma extensão de A por G que induz $\bar{\omega} : G \to \mathrm{Out}(A)$ e selecionamos para cada $g \in G$ um representante $\iota(g) \in E$ com $\pi(\iota(g)) = g$. Assim, para cada par g, $h \in G$ existe um elemento $n(g,h)$ em A com

$$\iota(g)\iota(h) = n(g,h)\iota(gh).$$

Temos que o automorfismo interno induzido por $\iota(g)$ em A está na classe de automorfismo de $\omega(g)$. Para a construção de $c \in A$, é possível escolher ω_g como o automorfismo interno induzido por $\iota(g)$ e $f(g,h)$ como $n(g,h)$. Assim

$$\begin{aligned} \omega_g(f(h,k))f(g,hk) &= \iota(g)n(h,k)\iota(g)^{-1}n(g,hk) \\ &= \iota(g)\iota(h)\iota(k)\iota(hk)^{-1}\iota(g)^{-1}\iota(g)\iota(hk)\iota(ghk)^{-1} \\ &= \iota(g)\iota(h)\iota(k)\iota(ghk)^{-1} \end{aligned} \tag{3.10}$$

e

$$\begin{aligned} f(g,h)f(gh,k) &= \iota(g)\iota(h)\iota(gh)^{-1}\iota(gh)\iota(k)\iota(ghk)^{-1} \\ &= \iota(g)\iota(h)\iota(k)\iota(ghk)^{-1}. \end{aligned} \tag{3.11}$$

Como (3.10) e (3.11) são iguais, temos que $c(g,h,k) = 1$ para essa escolha de ω e f.

($\Leftarrow$) Suponhamos agora que a classe de cohomologia $\bar{c}$ seja nula. Selecionamos algum ω_g com $\omega_1 = 1$. Pelo lema 3.5, podemos considerar $f(g,h)$ normalizado (isto é, $f(g,1) = 1$ e $f(1,h) = 1$), logo $c(g,h,k) = 1$ e note que, como fizemos em (3.7), temos então um grupo E produz uma extensão de A por G: $1 \to A \to E \to G \to 1$. □

Pelo teorema 3.6, dado $\bar{\omega} : G \to \mathrm{Out}(A)$, obtemos uma "obstrução" em $H^3(G; Z(A))$ que trivialmente determina quando existe uma extensão de grupo A por G induzindo $\bar{\omega}$.

Para a próxima proposição assumiremos que existe uma extensão de A por G induzindo um dado morfismo $\bar{\omega}\colon G \to \mathrm{Out}(A)$ e mostraremos que $H^2(G; Z(A))$ classifica estas extensões.

Teorema 3.7. *Seja $\bar{\omega} : G \to Out(A)$ um morfismo. Se existe uma extensão de grupo de A por G, então $H^2(G; Z(A))$ classifica as extensões de A por G que induzem $\bar{\omega}$.*

Demonstração. Primeiro, notemos que as classes de equivalência das extensões de grupos de A por G que induzem o morfismo $\bar{\omega}$ são cociclos generalizados (ω, f). Assim, como existe uma extensão de grupo de A por G, existe um cociclo (ω, f_0) correspondente. Definimos um morfismo φ de $H^2(G, Z(A))$ para o conjunto das classes de equivalência dos cociclos generalizados por $\bar{c} \mapsto (\omega, cf_0)$. É claro que (ω, cf_0) é um cociclo generalizado e também que φ está bem definida.

Sejam c e c' cociclos que representam a mesma classe em $H^2(G; Z(A))$, assim (ω, cf_0) e $(\omega, c'f_0)$ são equivalentes. Para mostrar a sobrejetividade de φ, consideremos (ω, f) um cociclo generalizado. Então,

$$\mathrm{Inn}(f(g,h)) = \omega_g\omega_h\omega_{gh}^{-1} = \mathrm{Inn}(f_0(g,h))$$

para qualquer par (g,f). Assim, como os elementos $f(g,h)$ e $f_0(g,h)$ induzem o mesmo automorfismo interno em A, existe $c(g,h) \in Z(A)$ tal que $f(g,h) = c(g,h)f_0(g,h)$ e, usando que tanto f quanto f_0 satisfazem a condição de cociclo generalizado e $c(g,h) \in Z(A)$, temos que c é um 2-cociclo. Logo, (ω, f_0) é equivalente a (ω, cf_0). Para provarmos a injetividade de φ, suponhamos que (ω, cf_0) e $(\omega, c'f_0)$ são equivalentes, isto é, para todo $g \in G$ existe $a_g \in A$ com

$$\omega_g = \mathrm{Inn}(a_g)\omega_g, \tag{3.12}$$

$$c(g,h)f_0(g,h) = a_g\omega_g(a_h)c'(g,h)f_0(g,h)a_{gh}^{-1}. \tag{3.13}$$

Note que (3.12) nos diz que $\mathrm{Inn}(a_g) = \mathrm{id}$, logo $a_g \in Z(A)$ para todo $g \in G$; já por (3.13) temos que $c(g,h) = a_g\omega_g(a_h)a_{gh}^{-1}c'(g,h)$, mostrando que c e c' são iguais em $H^2(G, Z(A))$. □

3.3 p-grupos com subgrupos cíclicos de índice p primo

Como aplicação da seção anterior, iremos classificar p-grupos, p primo, que possuem um subgrupo cíclico de índice p. Observe que tal subgrupo é necessariamente normal pelo Teorema de Sylow ([7], capítulo IV, página 44).

Começaremos listando alguns exemplos de p-grupos com um subgrupo cíclico de índice p:

(A) $\mathbb{Z}_q$, em que $q = p^n$, $n \geq 1$.
Considere $\mathbb{Z}_{p^{n-1}}$ como o subgrupo de $\mathbb{Z}_q$, assim, pelo Teorema de Lagrange, $[\mathbb{Z}_q : \mathbb{Z}_{p^{n-1}}] = p$.

(B) $\mathbb{Z}_q \times \mathbb{Z}_p$, em que $q = p^n$, $n \geq 1$.
Considere $\mathbb{Z}_{p^n} \times \{e\}$, pelo Teorema de Lagrange, $[\mathbb{Z}_q \times \mathbb{Z}_p : \mathbb{Z}_q \times \{e\}] = p$.

(C) $\mathbb{Z}_q \rtimes \mathbb{Z}_p$, em que $q = p^n$, $n \geq 2$ e o gerador canônico de $\mathbb{Z}_p$ age em $\mathbb{Z}_q$ multiplicando por $1 + p^{n-1}$, que está bem definido, pois $(1 + p^{n-1})^p \equiv 1 \pmod{p^n}$.
Note que a justificativa do item (B) anterior também vale para este item.

Se $p = 2$, damos três outros exemplos:

(D) 2-grupo diedral, em que para qualquer inteiro $m \geq 2$, o grupo diedral D_{2m} é definido por $\mathbb{Z}_m \rtimes \mathbb{Z}_2$, tal que o gerador de $\mathbb{Z}_2$ age em $\mathbb{Z}_m$ multiplicando por -1. Ainda, se m é uma potência de 2, é claro que D_{2m} é um 2-grupo. Note também que, D_4 é do tipo (B) anterior, já que $\mathrm{Aut}(\mathbb{Z}_2) = \mathrm{id}$ e $-1 \equiv 1 \pmod 2$; e que D_8 é do tipo (C) anterior, pois $3 \equiv -1 \pmod 4$. Agora, para $m > 4$, temos que D_{2m} não é isomorfo a nenhum dos exemplos anteriores, pois sabendo que uma presentação de D_{2m} pode ser dada por $\langle a, b | a^m = 1, b^2 = 1, bab^{-1} = a^{m-1}\rangle = \langle a\rangle \cup \langle a\rangle b$, temos que os elementos possuem ordem m, 2 ou no máximo $2m$, não coincidindo a ordem dos elementos de nenhum dos outros exemplos.
Como aqui também tratamos com o produto semidireto, recaímos novamente na justificativa do item (B).

(E) 2-grupo quatérnio generalizado: Seja $\mathbb{H}$ a álgebra dos quatérnios $\mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$. O grupo dos quatérnios generalizado $\mathcal{Q}_{4m}$, para $m \geq 2$, é definido como o subgrupo do grupo multiplicativo $\mathbb{H}^*$ gerado por $x = e^{\pi i/m}$ e $y = j$. Note que $x^{2m} = e^{2m\pi i/m} = e^{2\pi i} = 1$ e que $x^m = y^2 = j^2 = -1$, logo, a ordem de x é $o(x) = 2m$ e $o(y) = 4$, e claro que $yxy^{-1} = x^{-1}$ (basta usar que $e^{\pi i/m} = \cos(\frac{\pi}{m} + i\sin(\frac{\pi}{m})))$. Considere o subgrupo cíclico $C = \langle x\rangle$, logo C é normal em $\mathcal{Q}_{4m}$ pela relação anterior e, como $y^2 = x^m \in C$, temos que $y^2C = xC$, portanto existem apenas duas classes laterais distintas em $\mathcal{Q}_{4m}/C$, (xC e yC), logo C tem índice 2, assim, pelo Teorema de Lagrange $|\mathcal{Q}_{4m}| = 4m$. E, claro que, se m é uma potência de 2, $\mathcal{Q}_{4m}$ é um 2-grupo.

(F) $\mathbb{Z}_q \rtimes \mathbb{Z}_2$, em que $q = p^n$, $n \geq 3$ e o gerador de $\mathbb{Z}_2$ age em $\mathbb{Z}_q$ por multiplicação de $-1 + 2^{n-1}$.
Este grupo possui um subgrupo de índice p, também por (B).

Relembraremos aqui algumas propriedades de $\mathcal{Q}_{4m}$, em que C é o subgrupo dado em (E):

(a) Na extensão
$$0 \to C \xrightarrow{i} \mathcal{Q}_{4m} \to \mathbb{Z}_2 \to 0,$$
o gerador de $\mathbb{Z}_2$ age como -1 em C. De fato, note que y é mapeado em -1 e assim
$$i(-1x^k) = yi(x^k)y^{-1} = yx^ky^{-1} = (yxy^{-1})^k = x^{-k}.$$

(b) Todo elemento de $\mathcal{Q}_{4m} - C$ tem ordem 4. De fato, note que os elementos de $\mathcal{Q}_{4m} - C$ são da forma yx^k para $k = 1, \ldots, 2m$. Além disso, como $yxy^{-1} = x^{-1}$, temos que $yx = x^{-1}y$ e, mais geralmente, $yx^k = x^{-k}y$. Logo,
$$(yx^k)^2 = yx^kyx^k = yx^kx^{-k}y = y^2 = -1.$$
e portanto segue o resultado.

(c) $\mathcal{Q}_8$ possui os três seguintes subgrupos de índice 2: $\{\pm 1, \pm i\}$, $\{\pm 1, \pm j\}$, $\{\pm 1, \pm k\}$. E $\mathcal{Q}_{4m}$, $m > 2$, possui um único subgrupo cíclico de índice 2. Isto pode ser visto da seguinte maneira: considere A um subgrupo cíclico de $\mathcal{Q}_{4m}$ de índice 2 e seja $a \in A$ tal que $A = \langle a \rangle$. É claro que $|A| = o(a)$ e por Lagrange temos: $|\mathcal{Q}_{4m}| = |A| \cdot (\mathcal{Q}_{4m} \colon A)$, ou seja, $o(a) = 2m > 4$, pelo caso (b) anterior, todo elemento de $\mathcal{Q}_{4m} - C$ tem ordem 4, portanto $a \in C$, isto é, $A \leq C$. Note também que qualquer subgrupo próprio de C tem índice maior do que $(\mathcal{Q}_{4m} \colon C) = 2$. Como $(\mathcal{Q}_{4m} \colon A) = 2$, temos que $A = C$.

(d) $\mathcal{Q}_{4m}$ possui um único elemento de ordem 2. Pelo que fizemos anteriormente, sabemos que $\mathcal{Q}_{4m} \setminus A$ possui ordem 4. Assim, se um elemento possui ordem diferente de 4, este elemento deve pertencer a A. Como A é cíclico e possui ordem par, A tem um único elemento de ordem 2, concluindo que $\mathcal{Q}_{4m}$ tem um único elemento de ordem 2.

(e) A extensão
$$0 \to C \to \mathcal{Q}_{4m} \to \mathbb{Z}_2 \to 0,$$
não cinde, pois caso contrário, existiria um morfismo $q : \mathbb{Z}_2 \to \mathcal{Q}_{4m}$ tal que $\pi \circ q = \mathrm{id}_{\mathbb{Z}_2}$ e assim, $q(-1)$ seria um elemento de $\mathcal{Q}_{4m} - C$ de ordem 2, o que não pode acontecer.

Lema 3.8. *Seja $a \in \mathbb{Z}$ tal que $a^p \equiv 1 \pmod{p^n}$ para algum $n \geq 2$. Se p é ímpar, então $a \equiv 1 \pmod{p^{n-1}}$. Se $p = 2$, então $a \equiv \pm 1 \pmod{2^{n-1}}$.*

Demonstração. Para p ímpar faremos por indução em n. Base de indução $n = 2$: Suponha que $a^p \equiv 1 \pmod{p^2}$. Logo $a^p \equiv 1 \pmod{p}$ e pelo Pequeno Teorema de Fermat, temos que $a \equiv a^p \pmod{p}$, assim, $a \equiv 1 \pmod{p}$.

Suponhamos agora que o resultado seja válido para algum $n \geq 2$ e provaremos que vale para $n+1$. Suponhamos $a^p \equiv 1 \pmod{p^{n+1}}$. Assim, também temos que $a^p \equiv 1 \pmod{p^n}$ e, por hipótese de indução, $a \equiv 1 \pmod{p^{n-1}}$. Se $a \equiv 1 \pmod{p^{n+1}}$, teríamos $a \equiv 1 \pmod{p^n}$ e não haveria mais o que fazer. Vamos supor agora que $a \not\equiv 1 \pmod{p^{n+1}}$. Logo,
$$\begin{cases} a \equiv 1 & \pmod{p^{n-1}} \\ a \not\equiv 1 & \pmod{p^{n+1}} \end{cases}$$
Portanto, existem $m \in \mathbb{Z}$ e $k \in \{n-1, n\}$ tais que $p \nmid m$ e $a - 1 = p^k m$. Se $k = n$, $a \equiv 1 \pmod{p^n}$ e não temos nada para fazer. Se $k = n-1$, temos que $a = 1 + p^{n-1}m$, portanto
$$\begin{aligned} a^p &= (1 + p^{n-1}m)^p \\ &= \sum_{i=0}^{p} \binom{p}{i} (p^{n-1}m)^i \\ &= 1 + \sum_{i=1}^{p} \binom{p}{i} (p^{n-1}m)^i \\ &= 1 + p^n y, \end{aligned}$$
para algum y inteiro não divisível por p, que é um absurdo. Logo, o caso $k = n-1$ não ocorre e portanto $a \equiv 1 \pmod{p^n}$.

Para $p = 2$. Suponha que $a^2 \equiv 1 \pmod{2^n}$. Assim, existe $k \in \mathbb{Z}$ tal que
$$(a+1)(a-1) = 2^n k. \tag{3.14}$$
Como $a+1$ e $a-1$ diferem por 2, eles têm a mesma paridade, mas não podem ser simultaneamente divisíveis por 2^i para $i > 1$. Logo, por (3.14), temos
$$2^{n-1} | (a+1) \text{ ou } 2^{n-1} | (a-1).$$
Portanto $a \equiv \pm 1 \pmod{2^{n-1}}$. □

Teorema 3.9. *Se G é um p-grupo com um subgrupo cíclico de índice p, então G é isomorfo a um dos grupos da lista de (A)-(F) (que consta no início desta seção).*

Demonstração. Por hipótese, temos a extensão

$$0 \longrightarrow \mathbb{Z}_q \longrightarrow G \longrightarrow H \longrightarrow 0$$

em que $H = \mathbb{Z}_p$ e $q = p^n$ para $n \geq 0$. Denotamos $\mathbb{Z}_q = \langle s | s^q = 1\rangle$ e $H = \langle \bar{t} | \bar{t}^p = 1\rangle$.

Analisemos o caso em que H age trivialmente em $\mathbb{Z}_q$:

Temos que $\mathbb{Z}_q$ é um $\mathbb{Z}_p$-módulo em que a ação é a conjugação, isto é, $\bar{t} \cdot s = tst^{-1} = s$, como G é gerado por t e s, G é abeliano. Logo, pelo teorema de classificação de grupos abelianos finitamente gerados, segue que G é do tipo (A) ou (B) da lista.

Analisemos o caso em que H age não trivialmente em $\mathbb{Z}_q$:

Temos que $\bar{t} \cdot s = tst^{-1} = s^a$, para $a \in \mathbb{Z}$, portanto $t^z s t^{-z} = s^{a^z}$, para $z \geq 1$. Assim, como $t^p s t^{-p} = s^{a^p}$ e $t^p s t^{-p} = t^p \cdot s = 1 \cdot s = s$, temos que $a^p \equiv 1 \pmod{q}$, desse modo, estamos nas hipóteses do Lema 3.8.

Observe que $n \geq 2$, pois se $n = 1$, temos $q = p$, logo $a \equiv 1 \pmod{p = q}$ e novamente temos a ação trivial.

Se p é ímpar, considere o mergulho

$$\begin{aligned} \varphi\colon H &\hookrightarrow \mathbb{Z}_q^* \\ t &\mapsto a \end{aligned}$$

assim, $Im(\varphi) = \{1, a, \dots, a^{p-1}\} \subseteq \mathbb{Z}_q^*$. Logo, pelo Lema 3.8 , temos que $Im(\varphi)$ é gerada por $1 + p^{n-1}$. Em particular, H possui um gerador que age como $1 + p^{n-1}$ como em (C) da lista. Com essa ação de H em $\mathbb{Z}_q$, podemos calcular

$$\begin{aligned} \mathbb{Z}_q^H &= \{x \in \mathbb{Z}_q \,|\, \forall\, h \in H \; h \cdot x = x\} \\ &= \{s^x \in \mathbb{Z}_q \,|\, \bar{t} \cdot s^x = s^x\} \\ &= \{s^x \in \mathbb{Z}_q \,|\, ts^x t^{-1} = s^x\} \\ &= \{s^x \in \mathbb{Z}_q \,|\, (s^{1+p^{n-1}})^x = s^x\} \\ &= \{s^x \in \mathbb{Z}_q \,|\, p^{n-1}x \equiv 0 \,(mod\, q = p^n)\} = {}^{p\mathbb{Z}}\!\big/_{p^n\mathbb{Z}}. \end{aligned}$$

Utilizando o operador norma de $\mathbb{Z}_q$, temos

$$N = \left(\sum_{h \in H} h\right) s^i = \left(\sum_{k=1}^{p} 1 + kp^{n-1}\right) s^i = \left(p + p^{n-1}\frac{p(p+1)}{2}\right) s^i,$$

para $i \geq 1$, como p é ímpar, temos que $N \equiv p \pmod{p^n}$, assim,

$$\begin{aligned} N\colon \mathbb{Z}_q &\to \mathbb{Z}_q \\ s^x &\mapsto s^{p^x} \end{aligned}$$

logo, $\mathrm{im}(N) = p\mathbb{Z}/p^n\mathbb{Z}$. Portanto, pelo que fizemos no exemplo 2.7, $H^2(H; \mathbb{Z}_q) = 0$ assim, a sequência cinde, então G é o produto semidireto, isto é, (C) da lista.

Se $p = 2$ consideraremos novamente o mergulho $\varphi'\colon H \hookrightarrow \mathbb{Z}_q^*$. Pelo Lema 3.8, temos que $a \equiv \pm 1 \pmod{2^{n-1}}$ e, analogamente ao anterior, $Im(\varphi')$ é gerada por $\pm 1 + 2^{n-1}$. Portanto, existem três possibilidades para a imagem $a \in \mathbb{Z}_q^*$ do gerador de H:

(i) Caso em que $a = -1$:

$$\begin{aligned}
\mathbb{Z}_q^H &= \{x \in \mathbb{Z}_q \,|\, \forall\, h \in H\, h \cdot x = x\} \\
&= \{s^x \in \mathbb{Z}_q \,|\, \bar{t} \cdot s^x = s^x\} \\
&= \{s^x \in \mathbb{Z}_q \,|\, ts^x t^{-1} = s^x\} \\
&= \{s^x \in \mathbb{Z}_q \,|\, s^{(-1)x} = s^x\} \\
&= \{s^x \in \mathbb{Z}_q \,|\, (-1)x = x \pmod{q = 2^n}\} \\
&= \{s^x \in \mathbb{Z}_q \,|\, 2x \equiv 0 \pmod{q = 2^n}\} = {}^{2^{n-1}\mathbb{Z}}\!/\!_{2^n\mathbb{Z}}.
\end{aligned}$$

Sabemos que o operador norma é $N = 0$. Logo $H^2(H; \mathbb{Z}_q) \cong \mathbb{Z}_2$. Portanto, existem duas extensões de H em $\mathbb{Z}_q$ correspondendo a essa ação de H em $\mathbb{Z}_q$. Na extensão $0 \to \mathbb{Z}_m \to D_{2m} \to \mathbb{Z}_2 \to 0$ o gerador de $\mathbb{Z}_2$ age em $\mathbb{Z}_m$ pela multiplicação por -1, em que $D_{2m} = \langle \rho, \sigma \,|\, \rho^m = \sigma^2 = 1, \sigma\rho\sigma^{-1} = \sigma^{-1}\rangle$; e na extensão $0 \to C \to Q_{4m} \to \mathbb{Z}_2 \to 0$ em que a ação do gerador de $\mathbb{Z}_2$, $\bar{y}$, age como -1 em C, isto é, $\bar{y} \cdot x = yxy^{-1} = x^{-1}$, para x gerador de C. Logo, G é do tipo (D) ou (E) de 3.3.

(ii) Caso em que $a = 1 + 2^{n-1}$:

$$\begin{aligned}
\mathbb{Z}_q^H &= \{x \in \mathbb{Z}_q \,|\, \forall\, h \in H\, h \cdot x = x\} \\
&= \{s^x \in \mathbb{Z}_q \,|\, \bar{t} \cdot s^x = s^x\} \\
&= \{s^x \in \mathbb{Z}_q \,|\, ts^x t^{-1} = s^x\} \\
&= \{s^x \in \mathbb{Z}_q \,|\, (s^{1+2^{n-1}})^x = s^x\} \\
&= \{s^x \in \mathbb{Z}_q \,|\, 2^{n-1}x \equiv 0 \pmod{q = 2^n}\} = {}^{2\mathbb{Z}}\!/\!_{2^n\mathbb{Z}}.
\end{aligned}$$

Sabemos que o operador norma é $N = (2+2^{n-1})s^i$ para $i \geq 1$, temos então que $N \equiv 2+2^{n-1} \pmod{2^n}$, ou, $N \equiv 2(1 + 2^{n-2}) \pmod{2^n}$. Assumimos que $n \geq 3$, pois caso contrário estamos no caso em que $a = -1$. Portanto a imagem do operador norma é $2\mathbb{Z}/2^n\mathbb{Z}$, logo, $H^2(H; \mathbb{Z}_q) = 0$, assim, a extensão cinde e G é do tipo (C).

(iii) Caso em que $a = -1 + 2^{n-1}$:

$$\begin{aligned}
\mathbb{Z}_q^H &= \{x \in \mathbb{Z}_q \,|\, \forall\, h \in H\, h \cdot x = x\} \\
&= \{s^x \in \mathbb{Z}_q \,|\, \bar{t} \cdot s^x = s^x\} \\
&= \{s^x \in \mathbb{Z}_q \,|\, ts^x t^{-1} = s^x\} \\
&= \{s^x \in \mathbb{Z}_q \,|\, (s^{-1+2^{n-1}})^x = s^x\} \\
&= \{s^x \in \mathbb{Z}_q \,|\, 2x(-1 + 2^{n-2}) \equiv 0 \pmod{q = 2^{n-1}}\} = {}^{2^{n-1}\mathbb{Z}}\!/\!_{2^n\mathbb{Z}}.
\end{aligned}$$

E o operador norma é: $N = (2^{n-1})s^i$ para $i \geq 1$, temos então que $N \equiv 2^{n-1} \pmod{2^n}$, para $n \geq 3$. Portanto, a imagem do operador norma é $2^{n-1}\mathbb{Z}/2^n\mathbb{Z}$, logo, $H^2(H; \mathbb{Z}_q) = 0$ e assim, a extensão cinde e G é do tipo (F) de 3.3.

$\square$

Teorema 3.10. *Se G é um p-grupo que possui um único subgrupo de ordem p, então G é um grupo cíclico ou um quatérnio generalizado.*

Demonstração. Fazendo indução em $|G|$, assumiremos que todo subgrupo próprio de G é cíclico ou quatérnio generalizado. Escolha $H \triangleleft G$ de índice p (que sempre existe por [7]). Se H é cíclico, então pelo Teorema 3.9, H é um grupo da lista (A)-(F), verificaremos agora quais desses são os subgrupos que possuem um único subgrupo de ordem p:

(A) $\mathbb{Z}_q$. Como $p \mid q$ e $\mathbb{Z}_q$ é cíclico, temos que existe apenas um subgrupo de ordem p.

(B) $\mathbb{Z}_q \times \mathbb{Z}_p$. Note primeiro que existe $S \leq \mathbb{Z}_q$ em que $|S| = p$, $S = \{0, p^{k-1}, 2p^{k-1}, \ldots, (p-1)p^{k-1}\}$, e que $\{(a, 0) : \ a \in S\}$ é um subgrupo de $\mathbb{Z}_q \times \mathbb{Z}_p$ de ordem p. Mas $\{(0, b) : \ a \in \mathbb{Z}_p\}$ é também um subgrupo de $\mathbb{Z}_q \times \mathbb{Z}_p$, logo existe mais de um subgrupo de ordem p em $\mathbb{Z}_q \times \mathbb{Z}_p$.

(E) Quatérnio generalizado $\mathcal{Q}_{2^i}$. Pelo item (d) em (E), temos que $\mathcal{Q}_{2^i}$ possui um único subgrupo de ordem 2.

Note que os itens (C), (D) e (F) podem ser mostrados de maneira similar ao item (B) que têm mais de um subgrupo de ordem prima.

Portanto os grupos de (A) e (E) são aqueles possuem um único subgrupo de ordem p.

Suponha agora que H seja um quatérnio generalizado, logo $p = 2$. Afirmamos que H possui um único subgrupo cíclico N de índice 2 que é normal em G. De fato, se $\mathscr{S}$ é o conjunto dos subgrupos cíclicos de H de índice 2, temos que $card(\mathscr{S})$ é ímpar, já que, por (c) em (E) da lista, $\mathcal{Q}_8$ possui os três seguintes subgrupos de índice 2 e $\mathcal{Q}_{4m}$, $m > 2$, possui um único subgrupo cíclico de índice 2.

Note que a ação de conjugação do 2-grupo G em $\mathscr{S}$ deve fixar algum $N \in \mathscr{S}$, pois, se $\mathscr{S}$ contém apenas um subgrupo cíclico, claramente a ação G em $\mathscr{S}$ fixa; se $\mathscr{S}$ contém 3 subgrupos cíclicos, um subgrupo sempre será fixado, isto é, considere $\mathscr{S} = \{X, Y, Z\}$. Sejam $g \in G$ e $h \in H$. Se $X \mapsto g \cdot X = gXg^{-1} = Y$, então $Y \mapsto g \cdot Y = gYg^{-1} = g^2Xg^{-2} = X$, pois, como $(G \colon H) = 2$, temos que $G = H \cup gH$. Além disso, suponhamos sem perda de generalidade que $g \notin H$, mas $g^2 \in H$ (pois, se $g^2 \in gH$, temos $g^2 = gh$, para $h \in H$, logo $g = h$) e X é normal em H. Portanto temos então que $Z \mapsto Z$, fixando um dos subgrupos. Note também que Z é normal em G, pois $ghZh^{-1}g^{-1} = gZg^{-1} = Z$, já que Z é normal em H.

Considere agora a ação de G/N em N dada pela conjugação, isto é, dados $g \in G$, $n \in N$ temos

$$gN \cdot n := gng^{-1} \text{(está bem definida, pois } N \text{ é normal).}$$

Como N é cíclico, para cada $g \in G$ existe $a_g \in \{1, \cdots, q = |N| \geq 4\}$ tal que $gN \cdot n = n^{a_g}$, em que n é um gerador fixado de N. Como $q = 2^k$, para algum $k \geq 2$ e $4|q$, temos um morfismo bem definido

$$\begin{aligned} \mathbb{Z}_q^* &\to \mathbb{Z}_4^* = \{\pm 1\} \\ a_g \pmod q &\mapsto a_g \pmod 4. \end{aligned}$$

Assim, da composição, temos o morfismo

$$\begin{aligned} \varphi \colon {}^{G}\!/_{N} &\to \mathbb{Z}_4^* \\ gN &\mapsto a_g \pmod 4. \end{aligned}$$

Note que φ é sobrejetora, pois caso contrário a ação de conjugação seria trivial, mas já sabemos, pelas relações de (E) da lista, que $yxy^{-1} = x^{-1}$. Portanto, $\ker(\varphi)$ é um subgrupo K/N de G/N de ordem 2. Assim, a ação de K/N em N é trivial, isto é, K/N não age como -1 em N. Logo K não pode ser um quatérnio generalizado, sendo então cíclico, voltando ao caso anterior.

□

4 GRUPOS FINITOS E COHOMOLOGIA DE TATE

Nesse capítulo definimos a cohomologia de Tate e suas principais propriedades. Além disso, mostraremos que o produto cup $\hat{H}^i(G;\mathbb{Z}) \otimes \hat{H}^{-i}(G;\mathbb{Z}) \to \hat{H}^0(G;\mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$ é um pareamento dual.

4.1 Álgebra Homológica Relativa

Utilizaremos aqui um grupo finito G e H um subgrupo fixado.

Definição 4.1. *Uma* injeção $i : M' \to M$ *de G-módulos será chamada de* admissível *se é uma injeção que cinde quando vista como uma injeção de H-módulos, isto é, se existe um H-morfismo $\pi : M \to M'$ tal que $\pi i = id_{M'}$.*

Definição 4.2. *Uma* sequência exata $M' \xrightarrow{i} M \xrightarrow{j} M''$ *é dita* admissível *se a inclusão* $\mathrm{im}(j) \hookrightarrow M''$ *é admissível.*

Definição 4.3. *Um* complexo de cadeia acíclico C *de G-módulos é chamado de* admissível *se cada uma das sequências exatas $C_{i+1} \to C_i \to C_{i-1}$ é admissível.*

Se temos um complexo de cadeia C de G-módulos que é admissível, pelo ponto de vista da proposição A.17, C é contrátil quando visto como um complexo de H-módulos.

Definição 4.4. *Um G-módulo Q é* relativamente injetivo *se satisfaz uma das (e, portanto todas) seguintes condições equivalentes:*

(i) Dado um diagrama da forma

$$\begin{tikzcd} M' \arrow[r, "i"] \arrow[dr, "0"'] & M \arrow[r, "j"] \arrow[d, "r"] & M'' \arrow[dl, dashed, "\alpha"] \\ & Q & \end{tikzcd}$$

com linha exata admissível, conseguimos encontrar α.

(ii) Dado um diagrama da forma

$$\begin{tikzcd} M' \arrow[r, hook, "i"] \arrow[d] & M \arrow[dl, dashed, "\beta"] \\ Q & \end{tikzcd}$$

em que i é injetivo admissível, conseguimos encontrar β.

(iii) O funtor contravariante $\mathrm{Hom}_G(-, Q)$ leva injeções admissíveis de G-módulos em sobrejeções de grupos abelianos.

Em particular, todo módulo injetivo é relativamente injetivo. Mas existem vários módulos que são relativamente injetivos e não são injetivos:

Proposição 4.5. *Para qualquer H-módulo N, o G-módulo $\mathrm{Coind}_H^G N$ é relativamente injetivo.*

Demonstração. Pela propriedade universal de coindução, temos que

$$\mathrm{Hom}_G(-, \mathrm{Coind}_H^G N) \cong \mathrm{Hom}_H(\mathrm{Res}_H^G(-), N).$$

Mas sabemos que $\mathrm{Hom}_H(\mathrm{Res}_H^G(-), N)$ leva injeções admissíveis de G-módulos para sobrejeções de grupos abelianos, satisfazendo a propriedade (iii) da definição de injetividade relativa. $\square$

Corolário 4.6. *Para qualquer G-módulo M existe uma injeção admissível canônica $M \hookrightarrow \overline{M}$, em que $\overline{M}$ é relativamente injetivo. Se $(G : H) < \infty$, então esta construção têm as seguintes propriedades:*

(a) Se M é livre (resp. projetivo) como um $\mathbb{Z}H$-módulo, então $\overline{M}$ é livre (resp. projetivo) sobre $\mathbb{Z}G$.

(b) Se M é finitamente gerado como um G-módulo, então $\overline{M}$ também o é.

Demonstração. Consideremos $\operatorname{Coind}_H^G(\operatorname{Res}_H^G M) = \overline{M}$ e por 2.8, existe a injetividade canônica de $M \hookrightarrow \overline{M}$. Se $(G : H) < \infty$, temos que $\operatorname{Ind}_H^G(-) \cong \operatorname{Coind}_H^G(-)$. Consideremos que M é livre como $\mathbb{Z}H$-módulo. Sabemos que $\operatorname{Ind}_H^G(\operatorname{Res}_H^G M) = \overline{M} = \mathbb{Z}[G/H] \otimes M$ e que produto tensorial de módulos livres é livre, assim $\overline{M}$ é livre (analogamente para projetivo). Suponha agora M finitamente gerado. Como $(G : H) < \infty$, segue que $\mathbb{Z}[G/H]$ é finitamente gerado. Logo, pela igualdade $\operatorname{Ind}_H^G(\operatorname{Res}_H^G M) = \overline{M} = \mathbb{Z}[G/H] \otimes M$, temos que $\overline{M}$ é finitamente gerado. □

.

Corolário 4.7. *Suponha $(G : H) < \infty$. Então qualquer $\mathbb{Z}G$-módulo projetivo é relativamente injetivo.*

Demonstração. Note primeiro que um somando direto de um relativamente injetivo é relativamente injetivo. Assim, como todo módulo projetivo é somando direto de um módulo livre, podemos apenas provar o caso para módulos livres. Se F é um $\mathbb{Z}G$-módulo livre, então, para F' um $\mathbb{Z}H$-módulo livre de mesmo posto, temos que $F \cong \mathbb{Z}G \otimes_{\mathbb{Z}H} F' = \operatorname{Ind}_H^G F'$. Mas pela proposição 4.5, temos que $F \cong \operatorname{Ind}_H^G F' \cong \operatorname{Coind}_H^G F'$ é relativamente injetivo. □

Proposição 4.8. *Sejam C e C' complexos de cadeia de G-módulos e seja r um inteiro. Suponha que C_i' seja relativamente injetivo para $i < r$ e que $C_{i+1} \to C_i \to C_{i-1}$ seja exata e admissível para $i \leq r$.*

(a) Qualquer família $(f_i : C_i \to C_i')_{i \geq r}$ de morfismos comutando com seus operadores de bordo estende para um morfismo de cadeia $C \to C'$.

(b) Sejam $f, g : C \to C'$ morfismos de cadeia e seja $(h_i : C_i \to C_i')_{i \geq r-1}$ uma família de morfismos tal que $\partial_i' h_i + h_{i-1}\partial_i = f_i - g_i$ para $i \geq r$. Então $(h_i)_{i \geq r-1}$ estende para uma homotopia de f para g.

Demonstração. A prova é igual ao lema A.22 em que todas as setas são invertidas. □

Definição 4.9. *Uma* resolução relativamente injetiva *de G-módulos M é um complexo de cocadeia não negativo Q de relativamente injetivo juntamente com uma equivalência fraca $\eta : M \to Q$ tal que o complexo aumentado $0 \to M \to Q^0 \to Q^1 \to \ldots$ é admissível.*

Corolário 4.10. *Quaisquer duas resoluções relativamente injetivas M são canonicamente homotopicamente equivalentes.*

Demonstração. Segue de forma imediata da proposição 4.8. □

Proposição 4.11. *Suponha $(G : H) < \infty$. Se M é um $\mathbb{Z}G$-módulo projetivo (resp. finitamente gerado e projetivo) como $\mathbb{Z}H$-módulo, então M admite uma resolução relativa injetiva $\eta : M \to Q$ tal que cada Q^n é um $\mathbb{Z}G$-módulo projetivo (resp. finitamente gerado e projetivo).*

Demonstração. Note que resoluções relativas injetivas existem para qualquer M, pois podemos considerar $\eta : M \to Q^0$ uma injeção admissível canônica do corolário 4.6, assim, aplicando novamente 4.6 conseguimos uma injeção admissível $\operatorname{coker}(\eta) \hookrightarrow Q^1$, e da mesma forma para todo Q^n. Além disso, como η cinde como morfismo de H-módulos, temos que $\operatorname{coker}(\eta)$ é projetivo como $\mathbb{Z}H$-módulo, utilizando o corolário 4.6 conseguimos que Q^1 é projetivo sobre $\mathbb{Z}G$. De forma similar, conseguimos para todo Q^n. E de forma análoga, quando M é finitamente gerado, temos que Q^n também o é. □

4.2 Resoluções Completas

Como consequência da proposição 4.11, o G-módulo $\mathbb{Z}$ admite uma resolução "para trás" $0 \to \mathbb{Z} \to Q^0 \to Q^1 \to \dots$, em que cada Q^i é finitamente gerado e projetivo. Considerando $F_i = Q^{-i-1}$ temos então

$$0 \to \mathbb{Z} \xrightarrow{\eta} F_{-1} \to F_{-2} \to \dots . \tag{4.1}$$

Juntando 4.1 com uma resolução projetiva ordinária $\varepsilon : (F_n)_{n\geq 0} \to \mathbb{Z}$ obtemos um complexo acíclico

$$\begin{tikzcd} \dots \arrow[r] & F_2 \arrow[r] & F_1 \arrow[r] & F_0 \arrow[rr] \arrow[dr, "\varepsilon"'] & & F_{-1} \arrow[r] & F_{-2} \arrow[r] & \dots \\ & & & & \mathbb{Z} \arrow[ur, hook, "\eta"'] & & & \end{tikzcd} . \tag{4.2}$$

Definição 4.12. *Uma* resolução completa para G *é um complexo acíclico* $F = (F_i)_{i\in\mathbb{Z}}$ *de* $\mathbb{Z}G$*-módulos projetivos, juntamente com um morfismo* $\varepsilon : F_0 \to \mathbb{Z}$*, tal que* $\varepsilon : F_+ \to \mathbb{Z}$ *é uma resolução no sentido usual, em que* $F_+ = (F_i)_{i\geq 0}$*. O complexo acíclico dado em 4.2 é uma resolução completa para* G*.*

Note que, pela própria definição, $\partial : F_0 \to F_{-1}$ se fatora unicamente como $\partial = \eta\varepsilon$, em que $\eta : \mathbb{Z} \to F_{-1}$ é um monomorfismo. Além disso, o complexo 4.1 é uma resolução relativamente injetiva de $\mathbb{Z}$, pela proposição 4.11.

Lema 4.13. *Qualquer complexo de cadeia acíclico C de grupos abelianos livres é contrátil.*

Demonstração. O grupo abeliano Z_n dos n-ciclos é livre, já que é um subgrupo de um grupo abeliano livre, logo a sequência $0 \to Z_{n+1} \to C_{n+1} \to Z_n \to 0$ cinde. □

Observe que, como em resoluções ordinárias, podemos ver o morfismo ε em uma resolução completa como um morfismo de cadeia $F \to \mathbb{Z}$ (que não é uma equivalência fraca).

Definição 4.14. *Dadas resoluções completas* $\varepsilon : F \to \mathbb{Z}$ *e* $\varepsilon' : F' \to \mathbb{Z}$*, um morfismo de cadeia* $\tau : F \to F'$ preserva aumento *se* $\varepsilon'\tau = \varepsilon$*.*

Definição 4.15. *Dizemos que uma* resolução F *é* de tipo finito *se cada* F_i *é finitamente gerado.*

Proposição 4.16. *Se* $\varepsilon : F \to \mathbb{Z}$ *e* $\varepsilon' : F' \to \mathbb{Z}$ *são resoluções completas, então existe uma única classe de homotopia de morfismos que preservam aumento de* F *para* F'*. Esses morfismos são equivalências homotópicas.*

Demonstração. Note que temos os seguintes complexos:

$$\begin{tikzcd} \dots \arrow[r] & F_1 \arrow[r] \arrow[dd, dashed, "\tau_1"] & F_0 \arrow[rr] \arrow[dd, dashed, "\tau_0"] \arrow[dr] & & F_{-1} \\ & & & \mathbb{Z} \arrow[ur, hook] \arrow[dr, hook] & \\ \dots \arrow[r] & F'_1 \arrow[r] & F'_0 \arrow[rr] \arrow[ur] & & F'_{-1} \end{tikzcd}$$

em que τ_n para $n \geq 0$ existem pelo Lema Fundamental da Álgebra Homológica A.22 e são morfismos que preservam aumento nas dimensões positivas. Precisamos estender τ_n para o lado negativo dos complexos. O complexo da linha de cima é uma resolução completa, portanto é exata. Como G é finito e o complexo de baixo é projetivo, pelo corolário 4.7, o complexo é relativamente injetivo e, utilizando a proposição 4.8(a), temos que τ_n pode ser estendida para dimensões negativas. Consideremos agora dois morfismos que preservam aumento $\tau, \tau' \colon F \to F'$. Pelo Lema Fundamental da Álgebra Homológica A.22, temos que existe uma homotopia entre τ_n e τ'_n, mas que pela proposição 4.8(b) pode ser estendida para as dimensões negativas. Logo, existe uma única classe de homotopia de morfismos que preservam aumento de F para F'. Além disso, temos que id_F e $\tau' \circ \tau$ são morfismos de F para F, portanto são homotópicos, assim pela unicidade das classes de homotopia, concluímos que é uma equivalência homotópica.

□

Queremos mostrar agora que a parte negativa de uma resolução completa de tipo finito é o dual de uma resolução projetiva ordinária de $\mathbb{Z}$ sobre $\mathbb{Z}G$. Consideramos um G-módulo M cujo dual é $M^* = \mathrm{Hom}_G(M, \mathbb{Z}G)$ que é um módulo projetivo finitamente gerado, pela proposição A.29. Podemos notar ainda que M^* é um G-módulo à direta se M é um G-módulo à esquerda, mas como vimos em 2, é possível transformá-lo em um módulo à esquerda. Assim, $(gu)(m) = u(m)g^{-1}$ para $g \in G$, $u \in M^*$ e $m \in M$. Outro modo é considerar o dual $\mathrm{Hom}(M, \mathbb{Z})$ de M como um $\mathbb{Z}$-módulo, que é um G-módulo via a ação diagonal, em que G age trivialmente em $\mathbb{Z}$. Portanto, $(gu)(m) = u(g^{-1}m)$ para $g \in G$, $u \in \mathrm{Hom}(M, \mathbb{Z})$ e $m \in M$. Mas o que acontece é que $\mathrm{Hom}(M, \mathbb{Z})$ coincide com o dual M^*:

Proposição 4.17. *Para todo grupo finito G e qualquer G-módulo M (à esquerda), existe um isomorfismo de G-módulos:*

$$\psi \colon \mathrm{Hom}(M, \mathbb{Z}) \to M^* = \mathrm{Hom}_G(M, \mathbb{Z}G)$$

dado por $\psi(u)(m) = \sum_{g \in G} u(g^{-1}m)g$ para $u \in \mathrm{Hom}(M, \mathbb{Z})$, $m \in M$.

Demonstração. Seja $u \in \ker(\psi)$. Note que $\sum_{g \in G} u(g^{-1}m)g = \psi(u)(m) = 0$ para todo $m \in M$. Logo, $u(g^{-1}m) = 0$ para todo $m \in M$ e para todo $g \in G$ e, em particular, $u(m) = 0$ para todo $m \in M$. Portanto $u = 0$ e ψ é injetivo.

Seja $\varphi \in \mathrm{Hom}_G(M, \mathbb{Z}G)$. Para cada $g \in G$, denote por $\varphi_g(m)$ o coeficiente de $\varphi(m) \in \mathbb{Z}G$ relativo a g. Note que, para cada $g \in G$, o morfismo $\varphi_g \colon M \to \mathbb{Z}$ dado por $m \mapsto \varphi_g(m)$ é um morfismo de grupos, pois

$$\sum_{g \in G} \varphi_g(m+n)g = \varphi(m+n) = \varphi(m) + \varphi(n) = \sum_{g \in G} \varphi_g(m)g + \sum_{g \in G} \varphi_g(n)g = \sum_{g \in G} (\varphi_g(m) + \varphi_g(n))g$$

para todo $m, n \in M$, de onde segue $\varphi_g(m+n) = \varphi_g(m) + \varphi_g(n)$ para todo $g \in G$ e $m, n \in N$. Além disso, note que

$$\sum_{g \in G} \varphi_g(h^{-1}m)g = \varphi(h^{-1}m) = h^{-1}\varphi(m) = h^{-1}\left(\sum_{g \in G} \varphi_g(m)g\right) = \sum_{g \in G} \varphi_g(m)h^{-1}g = \sum_{g \in G} \varphi_{hg}(m)g$$

para todo $m \in M$ e $h \in G$. Portanto $\varphi_g(h^{-1}m) = \varphi_{hg}(m)$ para todo $g, h \in G$ e $m \in M$. Logo

$$\psi(\varphi_1)(m) = \sum_{g \in G} \varphi_1(g^{-1}m)g = \sum_{g \in G} \varphi_g(m)g = \varphi(m)$$

para todo $m \in M$, concluindo a sobrejetividade de ψ. Portanto ψ é um isomorfismo. □

Como uma aplicação deste resultado, daremos uma interpretação concreta de uma "resolução projetiva para trás" $\mathbb{Z} \to Q$ discutida no início da seção.

Definição 4.18. *O dual de um complexo de cadeia F (sobre anel R arbitrário) é o complexo $\bar{F} = \mathscr{H}om_R(F, R).$, isto é, $\bar{F}^n = \bar{F}_{-n} = \mathrm{Hom}_R(F_n, R) = (F_n)^*$.*

Proposição 4.19. *Se $\varepsilon : P \to \mathbb{Z}$ é uma resolução projetiva de tipo finito de $\mathbb{Z}$ sobre $\mathbb{Z}G$ (G finito), então $\varepsilon^* : \mathbb{Z}^* = \mathbb{Z} \to \bar{P}$ é uma resolução projetiva para trás. Ainda, a menos de isomorfismo, toda resolução projetiva para trás de tipo finito é obtida desse modo. Consequentemente, qualquer resolução completa de tipo finito é obtida a partir de resoluções projetivas ordinárias de tipo finito $P' \to \mathbb{Z}$ e $P \to \mathbb{Z}$ grudando P' e ΣP, em que ΣP é a suspensão de P.*

Demonstração. O complexo de cadeia aumentado associado a $\varepsilon : P \to \mathbb{Z}$ é contrátil como complexo de grupos abelianos, pelo lema 4.13. Note que ao aplicarmos a dualidade $(-)^* \cong \mathrm{Hom}(-, \mathbb{Z})$, o complexo permanece contrátil, logo $\varepsilon\colon \mathbb{Z}^* = \mathbb{Z} \to \bar{P}$ é uma resolução projetiva para trás, provando a primeira parte. Similarmente, dada qualquer resolução projetiva para trás de tipo finito $\mathbb{Z} \to Q$ o dual $\bar{Q} \to \mathbb{Z}$ é uma resolução projetiva ordinária e Q pode ser identificado com o dual de $\bar{Q}$ por A.29(d). ☐

4.3 Cohomologia de Tate

Desde o início podemos perceber que homologia e cohomologia possuem propriedades similares. O americano John Tate, descobriu uma forma de explorar as similaridades entre H_* e H^* para um grupo finito G, que é o que veremos a seguir.

Definição 4.20. *A* cohomologia de Tate *de um grupo finito G com coeficientes em um G-módulo M é definida por*

$$\hat{H}^i(G; M) = H^i(\mathscr{H}om_G(F, M))$$

para todo $i \in \mathbb{Z}$, em que F é uma resolução completa para G.

Note que H^i está bem definida (como vimos na proposição 4.16) a menos de um isomorfismo canônico. Sejam $F_+ = (F_i)_{i>0}$ e $F_- = (F_i)_{i<0}$ e seja C^+ (respectivamente C^-) o complexo $\mathscr{H}om_G(F_+, M)$ (respectivamente $\mathscr{H}om_G(F_-, M)$). Então temos

$$\hat{H}^i(G; M) = \begin{cases} H^i(C^+), & i > 0 \\ H^i(C^-), & i < -1 \end{cases}$$

e existe uma sequência exata

$$0 \to \hat{H}^{-1}(G; M) \to H^{-1}(C^-) \xrightarrow{\alpha} H^0(C^+) \to \hat{H}^0(G; M) \to 0$$

em que α é induzido pelo operador de cobordo $\delta : C^{-1} \to C^0$. Mais precisamente, α é determinada pelo diagrama:

$$\begin{tikzcd} C^{-1} \arrow[r, "\delta"] \arrow[d, two heads] & C^0 \\ H^{-1}(C^-) \arrow[r, "\alpha"] & H^0(C^+). \arrow[u, hook] \end{tikzcd} \tag{4.3}$$

Temos que $\varepsilon : F_+ \to \mathbb{Z}$ é uma resolução projetiva de $\mathbb{Z}$, logo $H^i(C^+) \cong H^i(G; M)$ para $i \in \mathbb{Z}$. E assumindo que F é de tipo finito, pela proposição 4.19 temos que $F_- = \overline{\Sigma P}$ para alguma resolução projetiva de tipo finito $P \to \mathbb{Z}$. O isomorfismo de dualidade dado pela proposição A.29:

$$C^- = \mathscr{H}om_G(F_-, M) = \mathscr{H}om_G(\overline{\Sigma P}, M) \cong \Sigma P \otimes_G M$$

assim, $H^i(C^-) \cong H_{-i}(\Sigma P \otimes_G M) = H_{-i-1}(P \otimes_G M) = H_{-i-1}(G; M)$. Logo temos

$$H^i(G; M) = \begin{cases} H^i(G; M), & i > 0 \\ H_{-i-1}(G; M), & i < -1 \end{cases}$$

e existe a sequência exata

$$0 \to \hat{H}^{-1}(G;M) \to H_0(G;M) \xrightarrow{\alpha} H^0(G;M) \to \hat{H}^0(G;M) \to 0$$

Afirmamos que α é o morfismo norma $\overline{N} : M_G \to M^G$. De fato, podemos assumir que as resoluções projetivas F_+ e P acima possuem $\mathbb{Z}G$ na dimensão 0 e que ambas resoluções começam com o morfismo canônico de aumento $\mathbb{Z}G \to \mathbb{Z}$, pois podemos considerar qualquer resolução projetiva de tipo finito. Então $\eta = \varepsilon^* : \mathbb{Z} \to \mathbb{Z}G$ é dado por $\eta(1) = \sum_{g \in G} g$. Como $\mathrm{Hom}_G(\mathbb{Z}G, M) = M$, o diagrama 4.3 fica:

$$\begin{tikzcd} M \arrow[r, "N"] \arrow[d, two heads] & M \\ H_0(G;M) \arrow[r, "\alpha"] & H^0(G;M) \arrow[u, hook] \end{tikzcd} \tag{4.4}$$

e sabemos que $H_0(G;M) = M_G$ e $H^0(G;M) = M^G$. Provando o que afirmamos.
Além disso, provamos que

$$\hat{H}^{-1}(G;M) = \ker \overline{N} \subseteq H_0(G;M)$$

e

$$\hat{H}^0(G;M) = \operatorname{coker} \overline{N} \twoheadleftarrow H^0(G;M).$$

Resumindo, temos:

$$\begin{tikzcd} & & & H^0 \arrow[d, two heads] & H^1 \arrow[d, equal] & H^2\cdots \arrow[d, equal] \\ & & & \hat{H}^0 & \hat{H}^1 & \hat{H}^2\cdots \\ \cdots\hat{H}^{-3} \arrow[d, equal] & \hat{H}^{-2} \arrow[d, equal] & \hat{H}^{-1} \arrow[d, hook] & & & \\ \cdots H_2 & H_1 & H_0 \arrow[uuur, "\overline{N}"] & & & \end{tikzcd}$$

Podemos também definir a *homologia de grupos de Tate* por $\hat{H}_*(G;M) = H_*(F \otimes_G M)$, em que F é uma resolução completa. Com argumentos análogos aos anteriores temos que

$$\hat{H}_i = \begin{cases} H_i & \text{i} > 0 \\ \ker \overline{N} & \text{i} = 0 \\ \operatorname{coker} \overline{N} & \text{i} = \text{-1} \\ H^{-i-1} & \text{i} < \text{-1} \end{cases}$$

Em outras palavras, $\hat{H}_i = \hat{H}^{-i-1}$.

4.4 Propriedades da Cohomologia de Tate

Como a cohomologia de Tate é definida em termos de resoluções, temos que algumas propriedades que valem para H^* também valem para $\hat{H}^*$. Veremos algumas delas a seguir:

(1) Como em 2.26(ii'), temos:
Uma sequência exata curta de G-módulos $0 \to M' \to M \to M'' \to 0$ dá origem a uma sequência exata longa

$$\ldots \xrightarrow{\delta} \hat{H}^i(G;M') \to \hat{H}^i(G;M) \to \hat{H}^i(G;M'') \xrightarrow{\delta} \hat{H}^{i+1}(G;M') \to \ldots$$

(2) Sabemos que uma resolução completa para G pode ser vista como uma resolução completa para qualquer $H \subseteq G$. Note ainda que o Lema de Shapiro também vale para a cohomologia de Tate e por G ser finito, a coindução é igual à indução. Logo, temos:
Se $H \subseteq G$ e M é um H-módulo, então $\hat{H}^*(H; M) \cong \hat{H}^*(G; \mathbb{Z}G \otimes_{\mathbb{Z}H} M)$.

(3) Se considerarmos $H = \{1\}$, temos que $\hat{H}^*(H, -) = 0$. Assim, pelo item (2) anterior, para qualquer grupo abeliano A, $\hat{H}^*(G; \mathbb{Z}G \otimes A) = 0$, consequentemente, cada $\hat{H}^i$ é effaceable e coeffaceable.

(4) Note que pelos itens (1) e (3) anteriores, podemos usar mudança de dimensão. Dado um G-módulo M podemos encontrar K e C (como 2.15 e 2.16) tais que: $\hat{H}^i(G; M) \cong \hat{H}^{i+1}(G; K)$ e $\hat{H}^i(G; M) \cong \hat{H}^{i-1}(G; C)$, para todo $i \in \mathbb{Z}$.

(5) Dados $H \subseteq G$, uma resolução completa F para G, e um G-módulo M, temos morfismos de cocadeias $\mathscr{H}om_G(F, M) \hookrightarrow \mathscr{H}om_H(F, M)$ e $\mathscr{H}om_H(F, M) \to \mathscr{H}om_G(F, M)$, em que o segundo morfismo é o transfer. Assim, temos o morfismo de restrição $\hat{H}^*(G; M) \to \hat{H}^*(G; M)$ e o morfismo de correstrição $\hat{H}^*(H; M) \to \hat{H}^*(G; M)$, em que esses morfismos possuem propriedades análogas àquelas dadas em 2.42. E segue que o análogo a 2.44 e 2.46 também vale para $\hat{H}^*$.

(6) Existe um produto cup $\hat{H}^p(G; M) \otimes \hat{H}^q(G; N) \to \hat{H}^{p+q}(G; M \otimes N)$ com propriedades análogas as 2.55, que mostraremos a seguir. Note que, para o análogo da naturalidade da propriedade (6) de 2.55, devemos assumir que $\alpha\colon H \to G$ é uma inclusão, pois é nesta propriedade em que temos o morfismo $\alpha^*\colon \hat{H}^*(G; M) \to \hat{H}^*(H; M)$.

Pelas quatro primeiras propriedades podemos notar que, heuristicamente, a teoria da cohomologia de Tate está completamente determinada por qualquer $\hat{H}^i$.

Mostraremos agora a construção do produto cup para a cohomologia de Tate. Lembremos que, quando falamos do produto cup na cohomologia ordinária, usamos que o produto tensorial de resoluções é uma resolução. Em nível de cocadeia, o produto cup é apenas o morfismo:

$$\mathscr{H}om_G(F, M) \otimes \mathscr{H}om_G(F, N) \to \mathscr{H}om_G(F \otimes F, M \otimes N) \tag{4.5}$$

dado pelo produto tensorial de morfismos graduados. Além disso, podemos também definir o produto cup em termos de um única resolução F escolhendo uma aproximação da diagonal $\Delta : F \to F \otimes F$ e compondo o produto anterior com

$$\mathscr{H}om_G(\Delta, M \otimes N) : \mathscr{H}om_G(F \otimes F, M \otimes N) \to \mathscr{H}om_G(F, M \otimes N).$$

Assim, o produto cup

$$\mathscr{H}om_G(F, M)^p \otimes \mathscr{H}om_G(F, N)^q \to \mathscr{H}om_G(F, M \otimes N)^{p+q}$$

depende apenas da componente (p, q): $\Delta_{pq} : F_{p+q} \to F_p \otimes F_q$.

Suponhamos agora que F seja uma resolução completa. Se quiséssemos tentar fazer o análogo do que foi feito anteriormente, deveríamos ter que $F \otimes F$ é uma resolução completa, mas, em particular, note que $(F \otimes F)_+$ não é o mesmo do que $F_+ \otimes F_+$, e consequentemente, não é nada óbvio que a definição da forma 4.5 induz $\hat{H}^p \otimes \hat{H}^q \to \hat{H}^{p+q}$. Além disso, podemos notar que $F \otimes F$ não é um bom candidato para a aproximação da diagonal, já que para qualquer $n \in \mathbb{Z}$ existem vários (p, q) tal que $p + q = n$ e pelo que já vimos na mudança de dimensão os correspondentes ao produto cup devem ser todos não triviais. Assim, Δ deve possuir uma componente não trivial Δ_{pq} para todo (p, q), logo o candidato de Δ deve ser um módulo graduado de forma que na dimensão n é $\prod_{p+q=n} F_p \otimes F_q$ e não da forma $\bigoplus_{p+q=n} F_p \otimes F_q$. O que nos motiva para as seguintes definições:

Definição 4.21. *Se C e C' são módulos graduados, o* produto tensorial completo $C\hat{\otimes}C'$ *é definido por*

$$(C\hat{\otimes}C')_n = \prod_{p+q=n} C_p \otimes C'_q$$

Definição 4.22. *Dados os módulos graduados C, C', D e D' e os morfismos $u : C \to D$ de grau r e $v : C' \to D'$ de grau s, existe um morfismo $u\hat{\otimes}v : C\hat{\otimes}C' \to D\hat{\otimes}D'$ de grau $r+s$ definido por*

$$(u\hat{\otimes}v)_n = \prod_{p+q=n} (-1)^{ps} u_p \otimes v_q : \prod_{p+q=n} C_p \otimes C'_q \to \prod_{p+q=n} D_{p+r} \otimes D'_{q+s}.$$

Consideraremos agora uma resolução completa $\varepsilon : F \to \mathbb{Z}$, e seja d o diferencial em F. Logo $F\hat{\otimes}F$ possui "diferenciais parciais" $d\hat{\otimes}\,\mathrm{id}_F$ e $\mathrm{id}_F\,\hat{\otimes}d$. Lembrando que a composição de morfismos graduados é dada por $(u\hat{\otimes}v) \circ (u'\hat{\otimes}v') = (-1)^{\deg v \cdot \deg u'}(u \circ u')\hat{\otimes}(v \circ v')$, temos que $(d\hat{\otimes}\,\mathrm{id}_F)^2 = 0$, $(\mathrm{id}_F\,\hat{\otimes}d)^2 = 0$ e que $(d\hat{\otimes}\,\mathrm{id}_F)(\mathrm{id}_F\,\hat{\otimes}d) = d\hat{\otimes}d$ e $(\mathrm{id}_F\,\hat{\otimes}d)(d\hat{\otimes}\,\mathrm{id}_F) = -d\hat{\otimes}d$, ou seja, é anticomutativo. Logo, a "diferencial total" $\partial = d\hat{\otimes}\,\mathrm{id}_F + \mathrm{id}_F\,\hat{\otimes}d$ tem o quadrado igual a zero, o que nos dá que $F\hat{\otimes}F$ é um complexo de cadeia. Ainda, temos o "morfismo de aumento" $\varepsilon\hat{\otimes}\varepsilon : F\hat{\otimes}F \to \mathbb{Z}\hat{\otimes}\mathbb{Z} = \mathbb{Z}$. Por *aproximação completa da diagonal* queremos dizer que um morfismo $\Delta : F \to F\hat{\otimes}F$ preserva aumento, mas não é claro que as aproximações completas da diagonal realmente existem. Aceitando a sua existência, podemos definir o produto cup em nível de cocadeia:

Definição 4.23. *O* produto cup de cocadeia *é dado por*

$$\mathscr{H}om_G(F; M) \otimes \mathscr{H}om_G(F; N) \xrightarrow{\smile} \mathscr{H}om_G(F; M \otimes N)$$

em que $u \smile v = (u\hat{\otimes}v) \circ \Delta$

Obtemos então a fórmula do cobordo

$$\delta(u \smile v) = \delta u \smile v + (-1)^p u \smile \delta v$$

e segue que existe um produto induzido $\hat{H}^p(G, M) \otimes \hat{H}^q(G, N) \to \hat{H}^{p+q}(G, M \otimes N)$. Como na propriedade 2.55 item (2), é imediato que esse produto é natural com respeito ao morfismos de coeficientes, e como nas propriedades 2.55 itens (3.3) e (3.3'), temos que o produto cup é compatível com o morfismo de conexão δ em uma sequência exata longa de cohomologia. Mais ainda, pelo fato de que Δ ser um morfismo de aumento, conseguimos calcular o produto cup $\hat{H}^0 \otimes \hat{H}^0 \to \hat{H}^0$ e, como no item (1) propriedade 2.55, temos que o produto cup é induzido do morfismo $M^G \otimes N^G \to (M \otimes N)^G$.

Agora, usando mudança dimensão provaremos que o produto cup é independente das escolhas de F e de Δ:

Lema 4.24. *Existe no máximo um produto cup em $\hat{H}^*(G, -)$ satisfazendo os análogos dos itens (1), (3) e (3') da propriedade 2.55.*

Demonstração. Dado um G-módulo M, seja $\overline{M}$ o módulo induzido $\mathbb{Z}G \otimes M$, seja $0 \to K \to \overline{M} \to M \to 0$ uma sequência exata que $\mathbb{Z}$ cinde como $\mathbb{Z}$-módulos. Para qualquer G-módulo N temos que a sequência $0 \to K \otimes N \to \overline{M} \otimes N \to M \otimes N \to 0$ é exata e o módulo $\overline{M} \otimes N$ é induzido pela proposição 2.21. Assim, temos os isomorfismos

$$\delta : \hat{H}^i(G; M) \xrightarrow{\cong} \hat{H}^{i+1}(G; K) \text{ e } \delta : \hat{H}^i(G; M \otimes N) \xrightarrow{\cong} \hat{H}^{i+1}(G; K \otimes N).$$

Além disso, qualquer produto cup que satisfaz o análogo do item (3), da propriedade 2.55, é compatível com esses isomorfismos, isto é, o diagrama abaixo comuta para qualquer $v \in \hat{H}^q(G;N)$.

$$\begin{tikzcd} \hat{H}^p(G;M) \arrow[r, "\cong"] \arrow[d, "-\smile v"'] & \hat{H}^{p+1}(G;K) \arrow[d, "-\smile v"] \\ \hat{H}^{p+q}(G;M\otimes N) \arrow[r, "\cong"] & \hat{H}^{p+q+1}(G;K\otimes N) \end{tikzcd} \tag{4.6}$$

Suponhamos agora que temos dois produtos cup $\hat{H}^p \otimes \hat{H}^q \to \hat{H}^{p+q}$ como no enunciado do lema. Pela hipótese, os produtos cup coincidem quando $p = q = 0$, assim, pelo diagrama anterior temos, por indução decrescente em p, que quando $p \leq 0$ e $q = 0$ o diagrama anterior também comuta. Agora, escreva N como o quociente de um módulo induzido, por indução decrescente em q podemos estender pra o caso $p \leq 0$, $q \leq 0$. Agora, mergulhamos M em um módulo induzido e indutivamente temos que o produto cup é o mesmo para um p arbitrário e $q \leq 0$ e depois, mergulhamos N em um módulo induzido para mostrar que para todo p e q temos o mesmo produto cup. $\square$

Para completar a construção do produto cup, provaremos que existe a aproximação completa da diagonal Δ. Para isso, usaremos os lemas que seguem

Lema 4.25. *$F\hat{\otimes}F$ é acíclico e em cada dimensão é relativamente injetivo.*

Demonstração. O fato de ser relativamente injetivo segue do fato que o produto arbitrário de relativamente injetivos é relativamente injetivo. Já para provar que $F\hat{\otimes}F$ é acíclico, consideremos $h : F \to F$ uma homotopia de contração, visto como um complexo de grupos abelianos, e seja $H = h\hat{\otimes}\,\mathrm{id}_F$. Notemos que H é uma homotopia de contração para $F\hat{\otimes}F$, pois pela definição do diferencial ∂ em $F\hat{\otimes}F$, temos:

$$\begin{aligned} \partial H + H\partial &= (d\hat{\otimes}\,\mathrm{id}_F + \mathrm{id}_F\,\hat{\otimes} d)\circ(h\hat{\otimes}\,\mathrm{id}_F) + (h\hat{\otimes}\,\mathrm{id}_F)\circ(d\hat{\otimes}\,\mathrm{id}_F + \mathrm{id}_F\,\hat{\otimes}) \\ &= dh\hat{\otimes}\,\mathrm{id}_F - h\hat{\otimes}d + hd\hat{\otimes}\,\mathrm{id}_F + h\hat{\otimes}d \\ &= (dh+hd)\hat{\otimes}\,\mathrm{id}_F \\ &= \mathrm{id}_F\,\hat{\otimes}\,\mathrm{id}_F \\ &= \mathrm{id}_{F\hat{\otimes}F}\,. \end{aligned}$$

$\square$

Lema 4.26. *Sejam (C,∂) e (C',∂') dois complexos acíclicos de $\mathbb{Z}G$-módulos. Assuma que cada C_i é projetivo e cada C'_i é relativamente injetivo. Se $\tau_0 : C_0 \to C'_0$ é um morfismo tal que $\partial'_0\tau_0\partial_1 = 0$, então τ_0 pode ser estendido para um morfismo de complexos de cadeia $\tau : C \to C'$.*

Demonstração. Note que, como C é projetivo e C' é acíclico, podemos construir $(\tau_i)_{i\geq 0}$ como na prova do Lema Fundamental da Álgebra Homológica A.22 de forma que $(\tau_i)_{i\geq 0}$ comute com os diferenciais. Ainda, podemos observar que $\partial'_0\tau_0\partial_1 = 0$ é exatamente o que é preciso para começar uma indução construtiva. Similarmente, como C é acíclico e admissível (pelo lema 4.13) e C' é relativamente injetivo, $(\tau_i)_{i\geq 0}$ pode ser estendido para dimensão negativa pela proposição 4.8. $\square$

Lema 4.27. *Seja C um complexo admissível de $\mathbb{Z}G$-módulos. Para qualquer $\mathbb{Z}G$-módulo projetivo P, o complexo $P \otimes C$ (com a G ação diagonal) é contrátil como um complexo de $\mathbb{Z}G$-módulos.*

Demonstração. Note que basta provar para $P = \mathbb{Z}G$, pois todo módulo projetivo é somando direto de um módulo livre e uma vez que vale a distributividade do produto tensorial em relação à soma direta, basta então mostrar para esse módulo livre P. Pelo corolário 2.20, temos que $\mathbb{Z}G \otimes C$ é isomorfo ao complexo induzido $\mathbb{Z}G \otimes C'$, em que C' é C visto como um complexo de grupos abelianos. Como C' é contrátil por hipótese, segue que $\mathbb{Z}G \otimes C$ é contrátil. $\square$

Do ponto de vista dos Lemas 4.25 e 4.26, a construção de $\Delta : F \to F\hat{\otimes}F$ se reduz a construção de um morfismo $\alpha = (\alpha_p) : F_0 \to \prod_{p\in\mathbb{Z}} F_p \otimes F_{-p}$ tal que

(i) $\partial\alpha|_{B_0} = 0$ e

(ii) $(\varepsilon \otimes \varepsilon)\alpha_0 = \varepsilon$

em que $B_0 \subset F_0$ é o módulo dos bordos. Consideremos $\partial'_{pq} = d_p \otimes F_q : F_p \otimes F_q \to F_{p-1} \otimes F_q$ e também $\partial''_{pq} = (-1)^p F_p \otimes d_q : F_p \otimes F_q \to F_p \otimes F_{q-1}$. Logo, temos que o morfismo $\partial\alpha : F_0 \to \prod_{p\in\mathbb{Z}} F_{p-1} \otimes F_{-p}$ possui componentes $\partial'_{p,-p}\alpha_p + \partial''_{p-1,1-p}\alpha_{p-1}$. Deste modo, provar (i) é o mesmo que provar (i') $(\partial'\alpha_p + \partial''\alpha_{p-1})|_{B_0} = 0$, em que omitimos os índices de ∂' e ∂''. Vamos então construir o morfismo α em que tomamos $\alpha_0 : F_0 \to F_0 \otimes F_0$ um morfismo qualquer que satisfaça (ii), note que isso é possível por F_0 ser projetivo. Considerando $p > 0$ e que α_{p-1} já tenha sido definido, queremos construir $\alpha_p : F_0 \to F_p \otimes F_{-p}$ de forma que o diagrama abaixo comute:

$$\begin{tikzcd} & & B_0 \arrow[dll, dashed, "\alpha_p|_{B_0}"'] \arrow[d, "\beta|_{B_0}"] & & \\ F_p \otimes F_{-p} \arrow[rr, "\partial'"] & & F_{p-1} \otimes F_{-p} \arrow[rr, "\partial'"] & & F_{p-2} \otimes F_{-p}, \end{tikzcd}$$

em que $\beta = -\partial''\alpha_{p-1}$. Note que, se $p > 1$ então podemos assumir indutivamente que $(\partial'\alpha_{p-1} + \partial''\alpha_{p-2})|_{B_0} = 0$, portanto em B_0 nós temos:

$$\begin{aligned} \partial'\beta &= -\partial'\partial''\alpha_{p-1} && \text{pela definição de } \beta \\ &= \partial''\partial'\alpha_{p-1} && \text{pois } \partial' \text{ e } \partial'' \text{ anticomutam} \\ &= -\partial''\partial''\alpha_{p-2} && \text{por hipótese de indução} \\ &= 0. \end{aligned}$$

Se $p = 1$, então em B_0 nós temos

$$\begin{aligned} \partial'\beta &= -\partial'\partial''\alpha_0 && \text{pela definição de } \beta \\ &= -(d_0 \otimes d_0)\alpha_0 && \text{pela definição de } \partial' \text{ e } \partial'' \\ &= -(\eta \otimes \eta)(\varepsilon \otimes \varepsilon)\alpha_o && \text{pois } d_0 = \eta\varepsilon \\ &= -(\eta \otimes \eta)\varepsilon && \text{por (ii), pois } \varepsilon|_{B_0} = 0. \end{aligned}$$

Logo, $\partial'\beta|_{B_0} = 0$. Além disso, pelo lema 4.27, o complexo $(F_* \otimes F_{-p}, \partial')$ é contrátil. Ainda, podemos escolher uma homotopia de contração h e definir $\alpha_p = h\beta$, o que completa o passo indutivo. De forma similar, é possível construir α_p para $p < 0$ utilizando a indução decrescente, dessa forma, provamos o item (6) dada no início da seção 4.4.

Temos que também existe o produto cap para a teoria de Tate. Sabemos que existe um morfismo

$$\mathcal{H}om_G(F, M) \to \mathcal{H}om((F\hat{\otimes}F) \otimes_G N, F \otimes_G (M \otimes N))$$

dado por $u \mapsto \mathrm{id}\,\hat{\otimes} u \otimes \mathrm{id}_N$, que corresponde (adjunção entre os funtores $\mathcal{H}om$ e $\otimes$) ao morfismo

$$\gamma : \mathcal{H}om_G(F, M) \otimes ((F\hat{\otimes}F) \otimes_G N) \to F \otimes_G (M \otimes N).$$

Assim, definimos o produto cap

$$\mathcal{H}om_G(F, M) \otimes (F \otimes_G N) \stackrel{\frown}{\to} F \otimes_G (M \otimes N)$$

como γ composto com

$$\mathrm{id} \otimes (\Delta \otimes \mathrm{id}) : \mathcal{H}om_G(F, M) \otimes (F \otimes_G N) \to \mathcal{H}om_G(F, M) \otimes ((F\hat{\otimes}F) \otimes_G N),$$

em que $\Delta : F \to F\hat{\otimes}F$ é qualquer aproximação completa da diagonal, induzindo então o produto cap

$$\hat{H}^* \otimes \hat{H}_* \stackrel{\frown}{\to} \hat{H}_*$$

com as propriedades usuais.

4.5 Teorema da Dualidade

Para qualquer grupo abeliano A, definimos $A' = \text{Hom}(A, \mathbb{Q}/\mathbb{Z})$ e usaremos a notação $F^* = \text{Hom}_R(F, R)$ em que R é um R-módulo à esquerda.

Definição 4.28. *Um morfismo $\rho\colon A \otimes B \to \mathbb{Q}/\mathbb{Z}$ dá origem ao morfismo $\overline{\rho}\colon A \to B'$ dado por $x \mapsto (f \mapsto f(x))$ e dizemos que ρ á um* pareamento dual *se $\overline{\rho}$ é um isomorfismo.*

Claro que ρ também dá origem ao morfismo $\overline{\overline{\rho}} : B \to A'$, que é igual a composição de $B \to B'' \xrightarrow{\overline{\rho}} A'$. Além disso, se A e B são finitos, ρ é um pareamento dual se, e somente se, $\overline{\overline{\rho}}$ é um isomorfismo. Assim, o par dual entre grupos abelianos finitos nos dá um isomorfismo de cada um deles no dual do outro.

Se G é um grupo e M é um G-módulo, então $M' = \text{Hom}(M, \mathbb{Q}/\mathbb{Z})$ herda uma G-ação da forma usual: $(gu)(m) = u(g^{-1}m)$ para $g \in G$, $u \in M'$ e $m \in M$. Existe um pareamento de avaliação $\rho\colon H^i(G; M') \otimes H_i(G; M) \to \mathbb{Q}/\mathbb{Z}$ obtido compondo o pareamento $\langle \cdot, \cdot \rangle$ do produto cap com o morfismo avaliação $M' \otimes_G M \to \mathbb{Q}/\mathbb{Z}$ tal que $\varphi \otimes m \mapsto \varphi(m)$. Similarmente, se G é finito, existe um pareamento $\hat{\rho}\colon \hat{H}^i(G; M') \otimes \hat{H}_i(G; M) \to \mathbb{Q}/\mathbb{Z}$.

Proposição 4.29. *Os pareamentos ρ e $\hat{\rho}$, como no parágrafo acima, são pareamentos duais. Logo $H^i(G; M') \cong H_i(G; M)'$ para quaisquer G e M, e $\hat{H}^i(G; M') \cong \hat{H}_i(G; M)'$ se G é finito.*

Demonstração. Seja F uma resolução projetiva de $\mathbb{Z}$ sobre $\mathbb{Z}G$. Assim $\mathscr{H}om_G(F, M') = \mathscr{H}om_G(F, \text{Hom}(M, \mathbb{Q}/\mathbb{Z})) \cong \mathscr{H}om_G(F \otimes M, \mathbb{Q}/\mathbb{Z}) = \mathscr{H}om(F \otimes_G M, \mathbb{Q}/\mathbb{Z}) = (F \otimes_G M)'$. Como $(\,)'$ é exato, podemos passar à homologia e obtemos $H^*(G; M') = H_*(G; M)'$. É fácil ver que esse isomorfismo corresponde ao pareamento ρ. E da mesma forma podemos fazer para $\hat{\rho}$. $\square$

Assumiremos agora que G é finito. E como já vimos, existe um isomorfismo $\hat{H}^i(G; M) \cong \hat{H}_{-1-i}(G; M)$.

Proposição 4.30. *Existe um elemento $z \in \hat{H}_{-1}(G, \mathbb{Z})$ tal que o morfismo do produto cap $- \frown z : \hat{H}^i(G; M) \to \hat{H}_{-1-i}(G; M)$ é um isomorfismo para qualquer G-módulo M.*

Demonstração. Seja (F, d) uma resolução completa de tipo finito, com $d_0 = \eta\varepsilon$, e seja $\overline{F} = \mathscr{H}om_G(F, \mathbb{Z}G)$. Então, $\overline{F}_i = (F_{-i})^*$. Pela proposição 4.19, $\overline{F}$ continua acíclico e projetivo. Temos que o operador de bordo $\overline{F}_1 \to \overline{F}_0$ é a composição $(F_{-1})^* \overset{\eta^*}{\twoheadrightarrow} \mathbb{Z} \overset{\varepsilon^*}{\hookrightarrow} (F_0^*)$. Se desconsiderarmos os índices, temos que $\overline{F}$ é uma resolução completa, mais precisamente, temos que $\overline{F}$ é uma suspensão ΣE de uma resolução completa E. Utilizando a proposição A.29(b), obtemos o isomorfismo $\mathscr{H}om_G(F, M) \cong \overline{F} \otimes_G M$, o que nos dá

$$\hat{H}^i(G; M) \cong H_{-i}(\overline{F} \otimes_G M) = H_{-i-1}(E \otimes_G M) = \hat{H}_{-i-1}(G; M).$$

Note que esse isomorfismo é dado, a menos de sinal, pelo produto cap com um elemento universal $z \in \hat{H}_{-1}(G; \mathbb{Z})$. De fato, chamaremos o isomorfismo $\hat{H}^i(G; M) \to \hat{H}_{-i-1}(G; M)$ de φ e temos que φ é natural e compatível com δ. Além disso, considerando $z = \varphi(1)$, temos que φ e $- \frown z$ são iguais em $1 \in \hat{H}^0(G; \mathbb{Z})$. Suponhamos que M e $u \in \hat{H}^0(G; M)$ sejam arbitrários, assim, existe um morfismo $\mathbb{Z} \to M$ de G-módulos tal que $1 \mapsto u$ dá origem ao morfismo induzido $\alpha : \hat{H}^0(G; \mathbb{Z}) \to \hat{H}^0(G; M)$ que é o mesmo que $\mathbb{Z}^G \to M^G$ pois $\hat{H}^0(G; \mathbb{Z}) = \mathbb{Z}^G$ e $\hat{H}^0(G; M) = M^G$. Como o produto cap é natural com respeito aos morfismo de coeficientes, temos o diagrama comutativo

$$\begin{array}{ccc}
\hat{H}^0(G; \mathbb{Z}) & \xrightarrow{-\frown z} & \hat{H}_{-1}(G; \mathbb{Z}) \\
\downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\
\hat{H}^0(G; M) & \xrightarrow{-\frown z} & \hat{H}_{-1}(G; M)
\end{array}$$

de forma que $\beta(z) = \beta(1 \frown z) = \alpha(1) \frown z = u \frown z$. Assim, pela naturalidade de φ, temos o diagrama comutativo

$$\begin{tikzcd} \hat{H}^0(G;\mathbb{Z}) \arrow[r, "\varphi"] \arrow[d, "\alpha"] & \hat{H}_{-1}(G;\mathbb{Z}) \arrow[d, "\beta"] \\ \hat{H}^0(G;M) \arrow[r, "\varphi"] & \hat{H}_{-1}(G;M) \end{tikzcd}$$

e portanto $\varphi(u) = \varphi\alpha(1) = \beta\varphi(1) = \beta(z) = u \frown z$. Podemos perceber que, em dimensão zero, φ e $- \frown \beta$ possuem o mesmo domínio e que φ é δ-compatível (pelo que fizemos anteriormente). Assim, usando mudança de dimensão, temos que φ e $- \frown z$ são iguais em todas as dimensões e temos o diagrama comutativo

$$\begin{tikzcd} \hat{H}^0(G;\mathbb{Z}) \arrow[r, "-\frown z"] \arrow[d, "\delta"] & \hat{H}_{-1}(G;\mathbb{Z}) \arrow[d, "\delta"] \\ \hat{H}^n(G;K) \arrow[r, "-\frown z"] & \hat{H}_{-1-n}(G;K) \end{tikzcd}$$

em que os morfismos verticais são dados pela propriedade (4) do início da seção 4.4. Assim, o isomorfismo nos dá uma ambiguidade no sinal e temos que $\varphi(u) = \pm u \frown z$ em qualquer dimensão, seguindo o isomorfismo. $\square$

Corolário 4.31. *Para qualquer G-módulo M, a composição*

$$\hat{H}(G;M) \otimes \hat{H}^{-1-i}(G;M) \xrightarrow{\smile} H^{-1}(G;M' \otimes M) \xrightarrow{\alpha_*} \hat{H}^{-1}(G;\mathbb{Q}/\mathbb{Z})$$

é um pareamento dual, em que α_* é induzido pelo pareamento canônico $\alpha : M' \otimes M \to \mathbb{Q}/\mathbb{Z}$.

Demonstração. Pelas proposições 4.29 e 4.30 temos que $\hat{H}^i(G;M') \xrightarrow{\cong} \hat{H}_i(G;M)' \xrightarrow{\cong} \hat{H}^{-1-i}(G;M)'$, em que esta composição nos dá explicitamente $u \mapsto (v \mapsto \overline{\alpha}\langle u, v \frown z\rangle)$, em que $\overline{\alpha} : M' \otimes_G M \to \mathbb{Q}/\mathbb{Z}$ é induzido de α. Temos também que

$$\overline{\alpha}\langle u, v \frown z\rangle = \overline{\alpha}\langle u \frown v, z\rangle = \langle \alpha_*(u \smile v), z\rangle$$

nos dando a composição

$$\hat{H}^i(G;M') \otimes \hat{H}^{-1-i}(G;M) \xrightarrow{\smile} \hat{H}^{-1}(G;M' \otimes M) \xrightarrow{\alpha_*} \hat{H}^{-1}(G;\mathbb{Q}/\mathbb{Z}) \xrightarrow{\langle -,z\rangle} \mathbb{Q}/\mathbb{Z}$$

que é um pareamento dual.

Note que $\langle -, z\rangle$ mapeia $\hat{H}^{-1}(G;\mathbb{Q}/\mathbb{Z})$ isomorficamente em $|G|^{-1}\mathbb{Z}/\mathbb{Z}$, pois $\langle -, z\rangle$ é a composição

$$\hat{H}^{-1}(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\cong} \hat{H}_{-1}(G;\mathbb{Z})' \to \mathbb{Q}/\mathbb{Z},$$

em que o primeiro morfismo é dado na proposição 4.29 e o segundo é a avaliação do gerador $z \in \hat{H}_{-1}(G;\mathbb{Z})$. E claro que, se A é finito, a avaliação de um gerador de A nos dá um isomorfismo $A' \xrightarrow{\cong} |A|^{-1}\mathbb{Z}/\mathbb{Z}$. $\square$

Teorema 4.32. *O produto cup $\hat{H}^i(G;\mathbb{Z}) \otimes \hat{H}^{-i}(G;\mathbb{Z}) \to \hat{H}^0(G;\mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$ é um pareamento dual.*

Demonstração. Sabemos que $\hat{H}^*(G;\mathbb{Q}) = 0$, assim a sequência exata $0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$ nos dá o isomorfismo $\delta : \hat{H}^j(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\cong} \hat{H}^{j+1}(G;\mathbb{Z})$ para todo j. Pela compatibilidade com δ temos o diagrama comutativo:

$$\begin{tikzcd} \hat{H}^{i-1}(G;\mathbb{Q}/\mathbb{Z}) \otimes \hat{H}^{-i}(G;\mathbb{Z}) \arrow[r, "\smile"] \arrow[d, "\delta\otimes\mathrm{id}"] & \hat{H}^{-1}(G,\mathbb{Q}/\mathbb{Z}) \arrow[d, "\delta"] \\ \hat{H}^i(G;\mathbb{Z}) \otimes \hat{H}^{-i}(G;\mathbb{Z}) \arrow[r, "\smile"] & \hat{H}^0(G;\mathbb{Z}). \end{tikzcd}$$

Como a linha de cima é um pareamento dual pelo corolário 4.31, em que $M = \mathbb{Z}$, então a linha de baixo também é. $\square$

5 GRUPOS FINITOS COM COHOMOLOGIA PERIÓDICA

Neste capítulo estudaremos a periodicidade da cohomologia de alguns grupos finitos. Os resultados dados pela seção 3.3 são de grande importância aqui.

Definição 5.1. *Dizemos que um grupo finito G tem* cohomologia periódica *se, para algum $d \neq 0$, existe um elemento $u \in \hat{H}^d(G;\mathbb{Z})$ que é inversível no anel $\hat{H}^*(G;\mathbb{Z})$.*

Fazendo o produto cup com u, obteremos então um isomorfismo periódico:

$$u \smile - : \hat{H}^n(G;M) \xrightarrow{\cong} \hat{H}^{n+d}(G;M)$$

para todo $n \in \mathbb{Z}$ e todo G-módulo M. Note que, para $n = 0$ e $M = \mathbb{Z}$, temos que $\hat{H}^0(G;\mathbb{Z}) \xrightarrow{\cong} \hat{H}^d(G;\mathbb{Z})$ e, pelo que ja vimos anteriormente, $\hat{H}^0(G;\mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}$, assim, para este caso temos $\hat{H}^d(G;\mathbb{Z}) \cong \mathbb{Z}/|G|\mathbb{Z}$ e u gera $\hat{H}^d(G;\mathbb{Z})$.

Sabemos que se um grupo G tem cohomologia periódica, então o trabalho de calcular $\hat{H}^*(G;\mathbb{Z})$ é simplificado. Deste modo, é interessante encontrar um critério que possa decidir se G possui ou não cohomologia periódica e é o que faremos nesta seção.

Teorema 5.2. *São equivalentes:*

(i) *G possui cohomologia periódica.*

(ii) *existem inteiros n e d, com $d \neq 0$, tal que $\hat{H}^n(G;M) \cong \hat{H}^{n+d}(G;M)$ para todo G-módulo M.*

(iii) *para algum $d \neq 0$, $\hat{H}^d(G;\mathbb{Z}) \cong \mathbb{Z}/|G|\mathbb{Z}$.*

(iv) *para algum $d \neq 0$, $\hat{H}^d(G;\mathbb{Z})$ contém um elemento u de ordem $|G|$.*

Demonstração. (i) $\Rightarrow$ (ii) Definição.
(ii) $\Rightarrow$ (iii) Fizemos anteriormente, logo após a definição.
(iii) $\Rightarrow$ (iv) Não há o que fazer.
(iv) $\Rightarrow$ (i) Pela proposição A.9, existe um morfismo $\hat{H}^d \to \mathbb{Q}/\mathbb{Z}$ tal que $u \mapsto 1/|G| \pmod{\mathbb{Z}}$. Pelo teorema 4.32, esse morfismo é dado por

$$\hat{H}^d(G,\mathbb{Z}) \xrightarrow{-\smile v} \hat{H}^0(G,\mathbb{Z}) \cong \mathbb{Z}/_{|G|\mathbb{Z}} \hookrightarrow \mathbb{Q}/_{\mathbb{Z}}$$

para algum $v \in \hat{H}^{-d}(G,\mathbb{Z})$. Assim, $uv = 1$ (ou seja, u é inversível) e segue (i). $\square$

Observação 5.3.

(1) Se G tem cohomologia periódica, então qualquer subgrupo H também tem, pois o morfismo de restrição $\hat{H}^*(G;\mathbb{Z}) \to \hat{H}^*(H,\mathbb{Z})$ é um morfismo de anel, portanto elementos inversíveis são levados em elementos inversíveis.

(2) Se G é abeliano e não cíclico, então G não possui cohomologia periódica. De fato, para este caso, G deve conter um subgrupo isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_p$, para algum primo p, mas utilizando a fórmula de Künneth dada em A.19, temos que $\hat{H}^n(\mathbb{Z}_p \times \mathbb{Z}_p;\mathbb{Z})$ sobre $\mathbb{Z}_p$ possui dimensão $n+1$, para $n \geq 0$, portanto pela dimensão ser maior que n, G não é periódico.

Definição 5.4. *Um p-*grupo abeliano elementar *de posto $r \geq 0$ é um grupo isomorfo a $\mathbb{Z}_p^r = \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$.*

Queremos encontrar um critério para um grupo possuir cohomologia periódica. No caso em que G é um p-grupo, existe um critério que é a proposição a seguir.

Proposição 5.5. *Se G é um p-grupo, para algum primo p, então são equivalentes:*

(i) G possui cohomologia periódica.

(ii) Todo subgrupo abeliano de G é cíclico.

(iii) Todo p-subgrupo abeliano elementar de G tem posto ≤ 1.

(iv) G possui um único subgrupo de ordem p.

(v) G é cíclico ou quatérnio generalizado.

Demonstração. (i) $\Rightarrow$ (ii) Nada a fazer (pela observação 5.3).
(ii) $\Rightarrow$ (iii) Trivial.
(iii) $\Rightarrow$ (iv) Como G é um p-grupo, sabemos que G contém um subgrupo central de ordem p. Se existisse outro subgrupo de ordem p, os dois gerariam um p-grupo abeliano elementar de posto 2, contrariando (iii).
(iv) $\Rightarrow$ (v) Teorema 3.10.
(v) $\Rightarrow$ (i) Nada a fazer para o caso cíclico, já para os quatérnios generalizados, consultar seção três do artigo [8]. $\square$

Para passar do caso do p-grupo para o caso geral, temos:

Proposição 5.6. *Um grupo finito G possui cohomologia periódica se, e somente se, todo subgrupo de Sylow de G possui cohomologia periódica.*

Demonstração. ($\Rightarrow$) Segue da observação 5.3 item (1).
($\Leftarrow$) Fixe um primo p e seja $H \subseteq G$ um p-subgrupo de Sylow. Por hipótese, $\hat{H}^*(H;\mathbb{Z})$ contém um elemento inversível u de grau $d \neq 0$.

Vamos mostrar que alguma potência de u é G-invariante, no sentido da definição 2.45.

Seja $e > 0$ um inteiro tal que $a^e = 1$ para todo $a \in (\mathbb{Z}/|H|\mathbb{Z})^*$ em que $(\mathbb{Z}/|H|\mathbb{Z})^*$ é o grupo das unidades em $(\mathbb{Z}/|H|\mathbb{Z})$. Note que e sempre existe, pois, no pior dos casos ele é $\phi(\mathbb{Z}/|H|\mathbb{Z})$ (número de elementos inversíveis). Ainda, note que para qualquer $g \in G$, os elementos $v = \operatorname{res}^H_{H\cap gHg^{-1}} u$ e $w = \operatorname{res}^{gHg^{-1}}_{H\cap gHg^{-1}} gu$ são inversíveis em $\hat{H}^*(H \cap gHg^{-1};\mathbb{Z})$. De fato, como $\operatorname{res}^H_{H\cap gHg^{-1}} : H^*(H;\mathbb{Z}) \to H^*(H \cap gHg^{-1};\mathbb{Z})$ é morfismo, temos que $\operatorname{res}^H_{H\cap gHg^{-1}}(x \smile y) = x \operatorname{res}^H_{H\cap gHg^{-1}} y = \operatorname{res}^H_{H\cap gHg^{-1}} x \smile \operatorname{res}^H_{H\cap gHg^{-1}} y$ para todo $x, y \in H^*(H \cap gHg^{-1};\mathbb{Z})$ e podemos considerar o seguinte diagrama comutativo:

$$\begin{tikzcd} H^*(H) \arrow[r, "\mathrm{res}"] \arrow[d, "u^{-1}\smile -"'] & H^*(H \cap gHg^{-1}) \arrow[d, "\mathrm{res}(u^{-1})\smile -"] \\ H^*(H) \arrow[r, "\mathrm{res}"] & H^*(H \cap gHg^{-1}). \end{tikzcd}$$

Temos então que

$$\operatorname{res}^H_{H\cap gHg^{-1}}(u^{-1} \smile u) = \operatorname{res}^H_{H\cap gHg^{-1}}(u^{-1}) \smile v,$$

assim

$$\operatorname{res}^H_{H\cap gHg^{-1}}(1) = \operatorname{res}^H_{H\cap gHg^{-1}}(u^{-1}) \smile v$$

e pela observação 5.3 item (1) sabemos que $\operatorname{res}^H_{H\cap gHg^{-1}} : H^*(H) \to H^*(H \cap gHg^{-1})$ é um morfismo de anéis, portanto $\operatorname{res}^H_{H\cap gHg^{-1}}(1) = 1$, logo $v^{-1} = \operatorname{res}^H_{H\cap gHg^{-1}}(u^{-1})$. De forma análoga, $w^{-1} =$

$\mathrm{res}^{gHg^{-1}}_{H\cap gHg^{-1}}(u^{-1}g^{-1})$. Como v e w são inversíveis, eles geram o grupo cíclico $\hat{H}^d(H\cap gHg^{-1},\mathbb{Z})$. Assim, $v^e = w^e$ e segue que $u^e \in \hat{H}^{de}(H,\mathbb{Z})$ é G-invariante e similarmente u^{-e} também é G-invariante, como queríamos mostrar.

Se analisarmos o teorema 2.46 na versão da cohomologia de Tate, provamos então que $\hat{H}^*(G;\mathbb{Z})_{(p)}$ possui um elemento inversível $u(p)$ de grau $d(p)$. Note que se elevarmos todos $u(p)$ a potências adequadas (basta utilizar o mínimo múltiplo comum de todos os graus $d(p)$) e considerarmos todos os primos que dividem a ordem de G, como $\hat{H}^*(G;\mathbb{Z}) = \bigoplus_p \hat{H}^*(G;\mathbb{Z})_p$, temos que $\hat{H}^*(G;\mathbb{Z})$ possui um elemento inversível de grau positivo.

□

Juntando as proposições anteriores 5.5 e 5.6, temos:

Teorema 5.7. *Para um grupo finito G, são equivalentes:*

(i) G possui cohomologia periódica.

(ii) Todo subgrupo abeliano de G é cíclico.

(iii) Todo p-subgrupo abeliano elementar de G tem posto ≤ 1.

(iv) Os subgrupos de Sylow de G são cíclicos ou quatérnios generalizados.

5.1 Exemplos de grupos periódicos

Estudaremos em um primeiro momento alguns grupos e logo após veremos que tais grupos possuem cohomologia periódica. Para esta parte foi utilizado tanto o livro [5], como o livro [9] e também utilizamos [10] para a descrição do grupo $\mathcal{O}_i^*$ e [11] para a descrição do grupo $TL_2(\mathbb{F}_p)$.

Note ainda que, os grupos cíclicos e os quatérnios generalizados, pelo que acabamos de ver no início do capítulo, possuem cohomologia periódica. No caso dos grupos cíclicos, basta analisar se em alguma dimensão existe um grupo cíclico com exatamente o número de elementos do grupo G, pelo teorema 5.2. Já no caso dos quatérnios, temos por [8], que a cohomologia desses possui período 4.

5.1.1 Os grupos T_i e $\mathcal{O}_i^*$

Considere $\mathbb{Z}_3 \circlearrowright \mathcal{Q}_8$ dada por

$$\begin{array}{rrcl} \alpha: & \mathbb{Z}_3 & \to & \mathrm{Aut}(\mathcal{Q}_8) \\ & 0 & \mapsto & \alpha_0 \\ & 1 & \mapsto & \alpha_1 \\ & -1 & \mapsto & \alpha_1^{-1} \end{array}$$

em que $\alpha_0 = id$, $\alpha_1(i) = k$, $\alpha_1(j) = i$ e $\alpha_1(k) = j$. Temos que o grupo binário tetraedral T é, por definição, $\mathcal{Q}_8 \rtimes_\alpha \mathbb{Z}_3$.

Notemos que, se $\omega \in \mathbb{R}\oplus\mathbb{R}i\oplus\mathbb{R}j\oplus\mathbb{R}k$ é tal que $\omega = \frac{1}{2}(-1+i+j+k)$, então $\langle\omega\rangle \cong \mathbb{Z}_3$, pois $\omega^3 = 1$:

$$\begin{aligned} \omega^2 &= \left(\frac{1}{2}(-1+i+j+k)\right)\cdot\left(\frac{1}{2}(-1+i+j+k)\right) \\ &= \frac{1}{4}\left(1-i-j-k-1-i-j+k-1+i-j-k-1-i+j-k\right) \\ &= \frac{1}{4}\left(-2-2i-2j-2k\right) \\ &= -\frac{1}{2}\left(1+i+j+k\right) \end{aligned}$$

e

$$\begin{aligned}\omega^2\cdot\omega &= \Big(-\frac{1}{2}(1+i+j+k)\Big)\cdot\Big(\frac{1}{2}(-1+i+j+k)\Big)\\ &= -\frac{1}{4}\left(-1+i+j+k-1-i-j+k-1+i-j-k-1-i+j-k\right)\\ &= 1.\end{aligned}$$

Provaremos agora que existe um isomorfismo $\varphi\colon T\to SL_2(\mathbb{F}_3)$. Primeiro, definimos φ em $\mathcal{Q}_8$ da seguinte forma:

$$i\mapsto\begin{pmatrix}-1 & -1\\ -1 & 1\end{pmatrix},\qquad j\mapsto\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$$

E estendemos para T:

$$\omega\mapsto\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}.$$

Note ainda que φ é um morfismo, por

$$\begin{aligned}\varphi(\omega\, i\,\omega^{-1}) &= \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}-1 & -1\\ -1 & 1\end{pmatrix}\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}\\ &= \begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix}\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}\\ &= \begin{pmatrix}1 & -1\\ -1 & -1\end{pmatrix}\\ &= \varphi(k)\end{aligned}$$

$$\begin{aligned}\varphi(\omega\, j\,\omega^{-1}) &= \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}\\ &= \begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix}\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}\\ &= \begin{pmatrix}-1 & -1\\ -1 & 1\end{pmatrix}\\ &= \varphi(i)\end{aligned}$$

$$\begin{aligned}\varphi(\omega\, k\,\omega^{-1}) &= \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & -1\\ -1 & -1\end{pmatrix}\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}\\ &= \begin{pmatrix}0 & 1\\ -1 & -1\end{pmatrix}\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix}\\ &= \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}\\ &= \varphi(j).\end{aligned}$$

Considerando $\gamma=-\varphi(\omega)$ e $y=\varphi(j)$, é bem sabido que uma presentação de $SL_2(\mathbb{F}_3)$ é dada por:

$$SL_2(\mathbb{F}_3)=\{\gamma,\, y|\gamma^3=y^2=(y\gamma)^3\}.$$

Deste modo, temos

$$\gamma^3 = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}^3 = -\,\mathrm{id}$$

$$y^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = -\,\mathrm{id}$$

$$y\,\gamma = \varphi(-j\,\omega) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$$

$$(y\,\gamma)^3 = \varphi(-j\,\omega)^3 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}^3 = -\,\mathrm{id}$$

concluímos assim que φ é sobrejetivo. Mas como $|T| = 24 = |SL_2(\mathbb{F}_3)|$, temos que $T \cong SL_2(\mathbb{F}_3)$.

Note que $Z(T) = \{(1,0), (-1,0)\}$, portanto, pelo teorema 3.7, para classificar as extensões de T por $\mathbb{Z}_2$, basta calcularmos $H^2(\mathbb{Z}_2; \mathbb{Z}_2)$. Pelo exemplo 2.7, temos a seguinte resolução

$$\cdots \xrightarrow{0} \mathbb{Z}_2 \xrightarrow{0} \mathbb{Z}_2 \xrightarrow{0} \mathbb{Z}_2 \to 0$$

e temos também que $H^2(\mathbb{Z}_2; \mathbb{Z}_2) = H_1(\mathbb{Z}_2; \mathbb{Z}_2) = \mathbb{Z}_2$. Logo existem duas extensões de T por $\mathbb{Z}_2$, são elas: o produto semidireto, $T \rtimes_\phi \mathbb{Z}_2$, e o binário octaedral, denotado por $\mathcal{O}^*$,

$$0 \to T \to \mathcal{O}^* \to \mathbb{Z}_2 \to 0,$$

temos ainda que uma presentação para $\mathcal{O}^*$ pode ser dada por

$$\langle t, p, q, r | t^3 = p^4 = 1, p^2 = q^2 = r^2, pqp^{-1} = q^{-1}, tpt^{-1} = q, tqt^{-1} = pq, rtr^{-1} = t^{-1},$$
$$rpr^{-1} = qp, rqr^{-1} = qp, rqr^{-1} = q^{-1} \rangle.$$

Existe também o caso mais geral que é grupo binário tetraedral generalizado, denotado por T_i, construído a partir da ação $\alpha_n : \mathbb{Z}_{3^i} \to \mathrm{Aut}(\mathcal{Q}_8)$ para $n \geq 1$ e definimos $T_i = \mathcal{Q}_8 \rtimes_{\alpha_n} \mathbb{Z}_{3^i}$. E, de forma similar ao feito anteriormente, cada T_i admite uma extensão T_i por $\mathbb{Z}_2$, que generaliza a extensão anterior

$$1 \to T_i \to \mathcal{O}_i^* \to \mathbb{Z}_2 \to 0.$$

em que $\mathcal{O}_i^*$ é o grupo binário octaedral generalizado, uma presentação para $\mathcal{O}_i^*$ pode ser dada por

$$\langle t, p, q, r | t^{3^i} = p^4 = 1, p^2 = q^2 = r^2, pqp^{-1} = q^{-1}, tpt^{-1} = q, tqt^{-1} = pq, rtr^{-1} = t^{-1},$$
$$rpr^{-1} = qp, rqr^{-1} = qp, rqr^{-1} = q^{-1} \rangle.$$

Devemos provar agora que T_i e $\mathcal{O}_i^*$ possuem cohomologia periódica.

Note que, como $T_i = \mathcal{Q}_8 \rtimes_{\alpha_n} \mathbb{Z}_{3^i}$, temos o 2-subgrupo de Sylow $(\mathcal{Q}_8, 0)$, isto é, um subgrupo dos quatérnios e o 3-subgrupo de Sylow cíclico $(0, \mathbb{Z}_{3^i})$, portanto pelo teorema 5.7, T_i possui cohomologia periódica.

Sabendo a presentação do $\mathcal{O}_i^*$, temos que

$$\mathcal{Q}_{16} \cong \langle pr, pq | (pr)^4 = (pq)^2, (pq)(pr)(pq)^{-1} = (pr)^{-1}, (pq)^4 = 1, (pr)^8 = 1 \rangle,$$

e como $|\mathcal{O}_i^*| = |T_i| \cdot |\mathbb{Z}_2| = 8 \cdot 3^i \cdot 2 = 16 \cdot 3^i$, temos que o 2-subgrupo de Sylow é o $\mathcal{Q}_{16}$ e o 3-subgrupo de Sylow cíclico é $\mathbb{Z}_{3^i}$. Logo, pelo teorema 5.7, $\mathcal{O}_i^*$ possui cohomologia periódica.

5.1.2 O grupo $\mathbf{SL}_2(\mathbb{F}_q)$

Primeiro, consideraremos M um subgrupo de $\mathrm{SL}_2(\mathbb{F}_q)$, para q uma potência de um primo ímpar, que consiste das matrizes

$$A = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \text{ e } B = \begin{pmatrix} 0 & -\lambda^{-1} \\ \lambda & 0 \end{pmatrix},$$

tal que $\lambda \in \mathbb{F}_q^*$. Note que $M \cong \mathcal{Q}_{2(q-1)}$ se $q \neq 3$. De fato, pelas relações que já conhecemos dos quatérnios $\mathcal{Q}_{4m}$ (conforme o item (E) da seção 3.3), temos que $m = \frac{1}{2}(q-1)$.

Seja λ de ordem $q-1$ e note que

$$\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}^{q-1} = \begin{pmatrix} \lambda^{q-1} & 0 \\ 0 & \lambda^{-(q-1)} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

e

$$\begin{pmatrix} 0 & -\lambda^{-1} \\ \lambda & 0 \end{pmatrix}^{4} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Deste modo, como sabemos que $o(x) = q-1$ e $o(y) = 4$, consideremos o morfismo $\psi : \mathcal{Q}_{2(q-1)} \to M$ definido por

$$x \mapsto \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$$

e

$$y \mapsto \begin{pmatrix} 0 & -\lambda^{-1} \\ \lambda & 0 \end{pmatrix}$$

que satisfaz as relações $\psi(yxy^{-1}) = \psi(x^{-1})$ e $\psi(y^2) = \psi(x^m)$, pois:

$$\begin{aligned} \psi(yxy^{-1}) &= \begin{pmatrix} 0 & -\lambda \\ \lambda & 0 \end{pmatrix} \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} 0 & \lambda^{-1} \\ -\lambda & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & -\lambda^{-2} \\ \lambda^2 & 0 \end{pmatrix} \begin{pmatrix} 0 & \lambda^{-1} \\ -\lambda & 0 \end{pmatrix} \\ &= \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix} \\ &= \psi(x^{-1}) \end{aligned}$$

e observemos que $\psi(y^2) = -\operatorname{id}$ e que $(\lambda^m)^2 = 1$, logo ou $\lambda^m = 1$ ou $\lambda^m = -1$, mas $o(\lambda) = 2m = q-1$, portanto $\lambda^m = -1$, assim $\psi(x^m) = -\operatorname{id} = \psi(y^2)$.

Observe agora que $\mathrm{Gal}(K/\mathbb{F}_q) = \mathbb{Z}_2$, para q uma potência de um primo ímpar e $K = \mathbb{F}_q[x]/\langle x^2 - \alpha \rangle$, em que α não é um quadrado perfeito em $\mathbb{F}_q$. De fato, considere o morfismo

$$\begin{aligned} \varphi : K &\to K \\ 1 &\mapsto 1 \\ \overline{x} &\mapsto \varphi(\overline{x}) = c\overline{x} + d \end{aligned}$$

para $c, d \in \mathbb{F}_q$ e sabemos que $\varphi(\overline{x})^2 = \varphi(\overline{x}^2) = \varphi(\alpha) = \alpha$, pois $\alpha \in \mathbb{F}_q$. Além disso, os elementos de K estão em bijeção com os elementos da forma $c\overline{x} + d$ e, note que se $c = 0$, teremos $d^2 = \alpha$, mas α não é um quadrado perfeito, logo $c \neq 0$ e, por outro lado também temos $2c\overline{x}d = 0$, logo $d = 0$. Então, $\varphi(\overline{x}) = c\overline{x}$ e $c^2 = 1$, portanto $c = \pm 1$ (temos que φ é injetor, por isso não temos o caso em que c e d são simultaneamente nulos).

Observemos que temos um morfismo $\mathbb{F}_{q^2}^* \hookrightarrow \mathrm{GL}(\mathbb{F}_q^2) = \mathrm{GL}_2(\mathbb{F}_q)$ tal que

$$c\overline{x} + d \mapsto \begin{pmatrix} d & c\alpha \\ c & d \end{pmatrix}$$

chamaremos a matriz acima de $\varphi_{c,d}$. Repare que o morfismo acima está bem definido, pois se o determinante da matriz $\varphi_{c,d}$ fosse nula, α seria um quadrado perfeito.

Verificaremos agora que $\mathrm{Gal}(K/\mathbb{F}_q)$ e $\mathbb{F}_{q^2}$ geram um subgrupo de $GL_2(\mathbb{F}_q)$ de ordem $2(q^2-1)$, ou seja, queremos saber qual é a ordem do subgrupo gerado por

$$\left\langle \zeta = \zeta^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \varphi_{c,d} = \begin{pmatrix} d & c\alpha \\ c & d \end{pmatrix} \text{ tal que } c\overline{x} + d \neq 0 \right\rangle \tag{5.1}$$

Um elemento subgrupo (5.1) é da forma

$$\zeta^{\alpha_1} \cdot \varphi_{c_1,d_1}^{\beta_1} \cdot \zeta^{\alpha_2} \cdot \varphi_{c_2,d_2}^{\beta_2} \cdot \zeta^{\alpha_3} \dots$$

Mas, note que

$$\varphi_{c,d} \cdot \zeta = \begin{pmatrix} d & c\alpha \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} d & -c\alpha \\ c & -d \end{pmatrix}$$

e

$$\zeta \cdot \varphi_{-c,d} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} d & -c\alpha \\ -c & d \end{pmatrix} = \begin{pmatrix} d & -c\alpha \\ c & -d \end{pmatrix}$$

ou seja, $\varphi_{c,d} \cdot \zeta = \zeta \cdot \varphi_{-c,d}$. E também o produto de duas matrizes da forma $\varphi_{c,d}$ tem a forma de $\varphi_{c',d'}$.

Assim, sem perda de generalidade, podemos supor que esse subgrupo é da forma

$$\{\zeta^{\epsilon} \cdot \varphi \,|\, \epsilon \in \{0,1\}, \varphi \in \mathbb{F}_{q^2}^*\},$$

portanto, sua ordem é realmente a ordem de $\mathrm{Gal}(K/\mathbb{F}_q) \cdot \mathbb{F}_{q^2}^*$, isto é, $2(q^2-1)$.

Provaremos agora que $J = \langle \mathrm{Gal}(K/\mathbb{F}_q) \bigcup \mathbb{F}_{q^2}^* \rangle \bigcap \mathrm{SL}(\mathbb{F}_{q^2}^*) \cong \mathcal{Q}_{2(q+1)}$. Observemos primeiro que em $GL_2(\mathbb{F}_q)$ existem $q-1$ valores possíveis para os determinantes das matrizes. Se todos os determinantes do subgrupo $\langle \mathrm{Gal}(K/\mathbb{F}_q) \bigcup \mathbb{F}_{q^2} \rangle$ aparecem com a mesma frequência, aqueles que possuem determinante igual a 1, isto é, todo o J, terá ordem $\dfrac{2(q^2-1)}{q-1} = 2(q+1)$. Deste modo, o que queremos provar é que todos os determinantes do subgrupo $\langle \mathrm{Gal}(K/\mathbb{F}_q) \bigcup \mathbb{F}_{q^2} \rangle$ aparecem com uma mesma frequência.

É claro que em J as matrizes terão a forma $\varphi_{c,d}$. Definimos a norma

$$\begin{aligned} N : \mathbb{F}_{q^2}^* &\to \mathbb{F}_q^* \\ c\overline{x} + d &\mapsto (d + c\overline{x})(d - c\overline{x}). \end{aligned}$$

Sabemos que $\ker(N) = \overline{N}$ é um subgrupo normal de $\mathbb{F}_{q^2}^*$, além disso, notemos que se pegarmos dois elementos com a mesma norma, ao multiplicarmos um pelo inverso do outro, temos um elemento do núcleo, ou seja, se $|z| = l$, então temos $\{\omega \in \mathbb{F}_{q^2} | |w| = l\} = \overline{N} \cdot z$. Logo, determinar a quantidade de elementos que possuem norma l, é equivalente a determinar a cardinalidade da classe lateral $\overline{N} \cdot z$. Mas é claro que $\overline{N} \cdot z$ possui a mesma cardinalidade de $\overline{N}$. Logo, para concluir que a norma aparece com a mesma frequência, resta mostrar que N é sobrejetor. De fato, pelo Teorema das Raízes da Unidade, $\mathbb{F}_{q^2}$ é cíclico, assim, consideremos um gerador θ de $\mathbb{F}_{q^2}^*$, que claramente tem ordem $q^2 - 1 = (q-1)(q+1)$, logo $N(\theta) \in \mathbb{F}_q^*$ tem ordem $q-1$, ou seja, N é sobrejetor. Logo, $|J| = 2(q+1)$.

Note que existe $\varphi_{c,d} = \xi \in J$ tal que $o(\xi) = q^2 - 1$, logo $o(\xi^{q-1}) = q+1$ e existe $\sigma = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in J$ tal que $o(\sigma) = 4$. Além disso, sabemos que o gerador padrão de $\mathcal{Q}_{2(q+1)}$ possui ordem $q+1$ e também temos que $o(y) = 4$ para $y \in \mathcal{Q}_{2(q+1)}$. Consideraremos portanto o morfismo:

$$\begin{aligned} \psi\colon \mathcal{Q}_{2(q+1)} &\to J \\ x &\mapsto \xi^{q-1} \\ y &\mapsto \sigma. \end{aligned}$$

Assim, basta provarmos que vale $\psi(y^2) = \psi(x^m)$ e $\psi(yxy^{-1}) = \psi(x^{-1})$.

Observemos que $\psi(y^2) = -\operatorname{id}$ e também que $\psi(x^m) = (\xi^{q-1})^{(q+1)/2} = \xi^{(q^2-1)/2}$, mas sabemos que

$$\xi^{q^2-1} = 1$$
$$\xi^{q^2-1} - 1 = 0$$
$$(\xi^{(q^2-1)/2} + 1)(\xi^{(q^2-1)/2} - 1) = 0,$$

porém se $\xi^{(q^2-1)/2} - 1 = 0$, teríamos $\xi^{(q^2-1)/2} = 1$, que é um absurdo, logo $\xi^{(q^2-1)/2} = -1$. Concluímos então que $\psi(y^2) = \psi(x^m)$.

Agora, $\psi((yxy^{-1})^m) = \psi(yx^m y^{-1}) = -\operatorname{id}$ e $\psi((x^{-1})^m) = \psi((x^m)^{-1}) = (-\operatorname{id})^{-1} = -\operatorname{id}$, portanto $\psi(yxy^{-1}) = \psi(x^{-1})$.

Logo, $J \cong \mathcal{Q}_{2(q+1)}$.

Provaremos que $\mathrm{SL}_2(\mathbb{F}_\mathrm{q})$ possui um 2-subgrupo de Sylow que é isomorfo a algum $\mathcal{Q}_{2^i}$ e um l-subgrupo de Sylow cíclico, para qualquer primo ímpar $l \neq \operatorname{char}(\mathbb{F}_q) = p$. Pelo que acabamos de fazer temos que $J \subseteq \mathrm{SL}_2(\mathbb{F}_\mathrm{q})$, $\mathcal{Q}_{2(q-1)} \subseteq \mathrm{SL}_2(\mathbb{F}_\mathrm{q})$ e $\mathcal{Q}_{2(q+1)} \subseteq \mathrm{SL}_2(\mathbb{F}_\mathrm{q})$. Suponhamos que 2^z é a maior potência de 2 que divide a ordem de $\mathrm{SL}_2(\mathbb{F}_\mathrm{q})$. Logo, $2^z || q(q^2-1)$ [1], como q é ímpar, temos $2^z || q^2 - 1$ ou $2^z || (q-1)(q+1)$, assim, podemos ter que ou $2 || q-1$ e $2^{z-1} || q+1$ ou $2^{z-1} || q-1$ e $2 || q+1$. E também vamos supor que l^w é outra maior potência que divide $|\,\mathrm{SL}_2(\mathbb{F}_\mathrm{q})\,|$, em que l é ímpar. Assim, $l^w || q(q^2-1)$, como l é ímpar, ou $l^w || q-1$ ou $l^w || q+1$.

Para provar que $\mathrm{SL}_2(\mathbb{F}_\mathrm{q})$ possui um 2-subgrupo de Sylow dos quatérnios, temos que se $2 || q-1$ e $2^{z-1} || q+1$, existe um subgrupo cíclico de ordem 2^{z-1} em $\mathcal{Q}_{2(q+1)}$, mas note que este subgrupo é exatamente $\langle \xi^k \rangle$ e temos que existe um subgrupo $I = \langle \sigma, \xi^{q-1} \rangle$ que é um quatérnio, assim se considerarmos um subgrupo de I sendo gerado por σ e alguma potência de ξ, conseguimos um subgrupo dos quatérnios que é um 2-Sylow. De forma similar, pode-se fazer quando $2 || q+1$ e $2^{z-1} || q-1$.

Além disso, sabemos que as matrizes da forma $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$ possuem ordem $q-1$ em $\mathcal{Q}_{2(q-1)}$, logo, se $l^w || q-1$, teremos que existe um subgrupo cíclico de ordem l^w em $\mathrm{SL}_2(\mathbb{F}_\mathrm{q})$. E, se $l^w || q+1$ e $o(\xi) = q+1$ em $\mathcal{Q}_{2(q+1)}$, então existe um subgrupo cíclico de ordem l^w em $\mathrm{SL}_2(\mathbb{F}_\mathrm{q})$ e provamos que $\mathrm{SL}_2(\mathbb{F}_\mathrm{q})$ possui um l-subgrupo de Sylow cíclico.

Agora precisamos analisar quando $\mathrm{SL}_2(\mathbb{F}_\mathrm{q})$ possui cohomologia periódica. Primeiro iremos analisar para $q = p$. Sabemos que $|\,\mathrm{SL}_2(\mathbb{F}_p)| = p(p^2-1)$, portanto temos um p-subgrupo de Sylow de ordem p que é cíclico, portanto possui cohomologia periódica, pelo teorema 5.7. Já para $q \neq p$, considere o subgrupo $\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{F}_q \right\}$ que é isomorfo ao grupo $(\mathbb{F}_q, +)$ é que abeliano, mas não é cíclico, portanto $\mathrm{SL}_2(\mathbb{F}_\mathrm{q})$ com $q \neq p$ não possui cohomologia periódica.

Ademais, o grupo $\mathrm{SL}_n(\mathbb{F}_q)$ com $n \geq 3$, não possui cohomologia periódica. De fato, consideremos $A = \langle \operatorname{diag}(a, a^{-1}, 1, 1, \cdots, 1) \rangle$ e $B = \langle \operatorname{diag}(1, 1, \cdots, 1, b, b^{-1},) \rangle$, temos que $A \cdot B = \operatorname{diag}(a, a^{-1}, 1, 1, \cdots, 1, b, b^{-1}) \subseteq \mathrm{SL}_n(\mathbb{F}_q)$ é um subgrupo abeliano, mas não é cíclico.

5.1.3 O grupo $\mathrm{TL}_2(\mathbb{F}_p)$

O grupo $\mathrm{TL}_2(\mathbb{F}_p)$ é definido por

$$\frac{\mathrm{SL}_2(\mathbb{F}_\mathrm{q}) * \langle \gamma \rangle}{\left\langle \gamma^2 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \gamma A \gamma^{-1} = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} A \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & 1 \end{pmatrix} \right\rangle}.$$

Agora, conseguimos provar

Proposição 5.8. $\mathrm{TL}_2(\mathbb{F}_p)$ *possui cohomologia periódica.*

[1] Usaremos a notação $p^e || n$ para significar que e é a maior potência de p que divide n.

Demonstração. (Caso 1) $p \equiv 1 \pmod 4$.

Pelo que fizemos anteriormente, sabemos que

$$\mathrm{SL}_2(\mathbb{F}_p) = \left\langle \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle$$

e $\mathrm{SL}_2(\mathbb{F}_p)_2 \cong \mathcal{Q}_{2^l}$.

Assim,

$$\begin{aligned} \gamma y \gamma^{-1} &= \gamma \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \gamma^{-1} \\ &= \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_\mathrm{q})_2 \end{aligned}$$

isto é $\gamma y \gamma^{-1} = \gamma^2 y$, portanto $y \gamma y^{-1} = \gamma^{-1}$. Logo, $\mathrm{TL}_2(\mathbb{F}_p)_2 = \langle y, \gamma \rangle$ e $|\,\mathrm{TL}_2(\mathbb{F}_p)_2| = 2^{l+1}$, então $\mathrm{TL}_2(\mathbb{F}_p)_2 \cong \mathcal{Q}_{2^{l+1}}$.

(Caso 2) $p \equiv 3 \pmod 4$.

Sabemos que $\mathcal{Q}_{2(p+1)} \hookrightarrow \mathrm{SL}_2(\mathbb{F}_p)$ e $|\,\mathrm{SL}_2(\mathbb{F}_p)| = p(p-1)(p+1)$, em que $2||p-1$ e $2^{l-1}||p+1$, ou seja, $p+1 = 2^{l-1} \cdot i$, em que i é ímpar. Temos que a maior potência de 2 que divide $(p-1)(p+1)$ é 2^l, assim $|\,\mathrm{SL}_2(\mathbb{F}_p)_2| = 2^l$. Além disso, sabemos que $\mathcal{Q}_{2(p+1)} = \langle y, x \rangle$, em que $o(x) = p+1$ e $o(y) = 4$, portanto, ao considerarmos $\mathcal{Q}_{2^l}$, temos que $\mathcal{Q}_{2^l} = \langle y, x^i \rangle$. Como em $\mathcal{Q}_{2(p+1)}$ vale a relação que $yxy^{-1} = x^{-1}$, é claro que valerá que $yx^iy^{-1} = x^{-i}$ em $\mathcal{Q}_{2^l}$. E ainda, $y^2 = (x^i)^{2^{l-2}}$ que em $\mathcal{Q}_{2(q+1)}$ é o mesmo que $y^2 = x^{(q+1)/2}$, assim $\mathrm{SL}_2(\mathbb{F}_\mathrm{q})_2 = \langle y, x^i \rangle$. E temos que $y\gamma y^{-1} = \gamma^{-1}$ pelo caso anterior. Portanto, $\mathrm{TL}_2(\mathbb{F}_p)_2 = \langle y, \gamma^i \rangle$ e $|\,\mathrm{TL}_2(\mathbb{F}_p)_2| = 2^{l+1}$, ou seja, $\mathrm{TL}_2(\mathbb{F}_p)_2 \cong \mathcal{Q}_{2^{l+1}}$.

Assim, pelo proposição 5.7 temos portanto que $\mathrm{TL}_2(\mathbb{F}_p)$ possui cohomologia periódica. □

5.2 O Teorema de Suzuki-Zassenhaus

É possível classificar completamente as famílias de grupos finitos que possuem cohomologia periódica, mas para isso, é necessário usar algumas outras técnicas que não foram possíveis estudar no tempo que tivemos.

Teorema 5.9. *(Teorema de Suzuki-Zassenhaus) Um grupo finito possui cohomologia periódica se, e somente se, ele pertence a alguma das famílias abaixo, em que p primo*

Grupos	Condição
$\mathbb{Z}_a \rtimes_\alpha \mathbb{Z}_b$	$\mathrm{mdc}(a,b) = 1$
$\mathbb{Z}_a \rtimes_\beta (\mathbb{Z}_b \times \mathcal{Q}_{2^i})$	$\mathrm{mdc}(a,b) = \mathrm{mdc}(ab,2) = 1$
$\mathbb{Z}_a \rtimes_\gamma (\mathbb{Z}_b \times T_i)$	$\mathrm{mdc}(a,b) = \mathrm{mdc}(ab,6) = 1$
$\mathbb{Z}_a \rtimes_\tau (\mathbb{Z}_b \times \mathcal{O}_i^*)$	$\mathrm{mdc}(a,b) = \mathrm{mdc}(ab,6) = 1$
$(\mathbb{Z}_a \rtimes_\alpha \mathbb{Z}_b) \times SL_2(\mathbb{F}_p)$	$\mathrm{mdc}(a,b) = \mathrm{mdc}(ab, p(p^2-1)) = 1$
$\mathbb{Z}_a \rtimes_\mu (\mathbb{Z}_b \times \mathrm{TL}_2(\mathbb{F}_p))$	$\mathrm{mdc}(a,b) = \mathrm{mdc}(ab, p(p^2-1)) = 1$

Para mais detalhes veja [12] e [13].

REFERÊNCIAS

[1] SWAN, R. G. Periodic resolutions for finite groups. *Ann. of Math. (2)*, v. 72, p. 267–291, 1960.

[2] ADEM, A.; SMITH, J. H. Periodic complexes and group actions. *Annals of Mathematics*, v. 154, 09 2001.

[3] CONNOLLY, F. X.; PRASSIDIS, S. Groups which act freely on $\mathbb{R}^m \times S^{n-1}$. *Topology*, v. 28, n. 2, p. 133–148, 1989.

[4] GOLASIŃSKI, M.; GONÇALVES, D. L.; JIMENEZ, R. Free and properly discontinuous actions of groups on homotopy $2n$-spheres. *Proc. Edinb. Math. Soc. (2)*, v. 61, n. 2, p. 305–327, 2018.

[5] BROWN, K. *Cohomology of groups*. 1st edition. ed., Graduate Texts in Mathematics. Springer-Verlag Berlin and Heidelberg GmbH e Co. K, 1982.

[6] EILENBERG, S.; MACLANE, S. Cohomology theory in abstract groups. i. *Annals of Mathematics*, v. 48, n. 1, p. 51–78, 1947.

[7] HALL, M. *The theory of groups*. 4th edition. ed. Macmillan, 1959.

[8] TOMODA, S.; ZVENGROWSKI, P. Remarks on the cohomology of finite fundamental groups of 3-manifolds. In: *The Zieschang Gedenkschrift*. Geom. Topol. Publ., Coventry, 2008. v. 14 of *Geom. Topol. Monogr.*, p. 519–556.

[9] ADEM, A.; MILGRAM, R. Cohomology of finite groups. v. 309, 01 2004.

[10] GOLASIŃSKI, M.; GONÇALVES, D. L. Automorphism groups of generalized (binary) icosahedral, tetrahedral and octahedral groups. *Algebra Colloquium*, v. 18, n. 3, p. 385–396, 2011.

[11] GOLASIŃSKI, M.; GONÇALVES, D. L. Spherical space forms – homotopy self-equivalences and homotopy types, the case of the groups $\mathbb{Z}/a \rtimes (\mathbb{Z}/b \times TL_2(\mathbb{F}_p))$. *Topology Appl.*, v. 156, n. 17, p. 2726–2734, 2009.

[12] WOLF, J. A. *Spaces of constant curvature*. 6th edition. ed. AMS, 2011.

[13] DWYER, W. G.; WILKERSON, C. W. A new finite loop space at the prime two. *Journal of the American Mathematical Society*, v. 6, p. 37–64, 1993.

Apêndices

APÊNDICE A – ÁLGEBRA HOMOLÓGICA

Este apêndice contêm algumas definições e alguns teoremas que servem para relembrar assuntos que foram utilizados durante o texto.

Definição A.1. *Seja G um grupo (com notação multiplicativa). O* anel de grupo $\mathbb{Z}G$ *é definido como o $\mathbb{Z}$-módulo livre gerado pelos elementos de G. Deste modo, um elemento de $\mathbb{Z}G$ é expresso por*

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

em que $a(g) \in \mathbb{Z}$ e $a(g) = 0$ exceto para uma quantidade finita de elementos $g \in G$.

A multiplicação em G se estende unicamente para um produto bilinear $\mathbb{Z}G \times \mathbb{Z}G \to \mathbb{Z}G$. Deste modo, $\mathbb{Z}G$ se torna um anel com as operações

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

$$\left(\sum_{g\in G} a(g)g\right)\left(\sum_{h\in G} b(h)g\right) = \sum_{g,h\in G}(a(g)b(h))gh$$

e o elemento neutro é dado por $\sum_{g\in G} a(g)g$ tal que $a(1) = 1$ e $a(g) = 0$ para todo $g \neq 1$.

Definição A.2. *Seja R um anel. Um* complexo de cadeia *sobre R é um par (C, d) em que C é um R-módulo graduado e $d : C \to C$ é um morfismo de grau -1 tal que $d^2 = 0$. O morfismo d é chamado de* diferencial.

Definição A.3. *Chamaremos de* ciclo *o núcleo de uma diferencial d e denotaremos por $Z(C)$, ou seja, $Z(C) = \ker(d)$.*
Chamaremos de bordo *(ou* diferencial*) a imagem de uma diferencial d e denotaremos por $B(C)$, ou seja, $B(C) = \mathrm{im}(d)$.*
Chamaremos de homologia *o quociente do ciclo pelo bordo e denotaremos por $H(C)$, ou seja, $H(C) = \dfrac{Z(C)}{B(C)}$.*

Utilizaremos o prefixo “co” quando estivermos tratando de complexos de cocadeia.

Definição A.4. *O complexo $(\Sigma^n C, \Sigma^n d)$ definido por $(\Sigma^n C)_p = C_{p-n}$ e $\Sigma^n d = (-1)^n d$ é chamado de* suspensão.

Definição A.5. *Se (C, d) e (C', d') são complexos de cadeia, então um* morfismo de cadeia *de C para C' é um morfismo de módulos graduados $f : C \to C'$ de grau 0 tal que $d'f = fd$.*

Definição A.6. *Uma* homotopia *h de um morfismo de cadeia f para um morfismo de cadeia g é um morfismo de módulos graduados $h : C \to C'$ de grau 1 tal que $d'h + hd = f - g$. Escrevemos $f \simeq g$ e dizemos que f é* homotópico *a g se existe uma homotopia de f para g.*

Definição A.7. *Sejam C e C' (E e E', respectivamente) complexos de R-módulos à direita (à esquerda, respectivamente). Dados $u \in \mathscr{H}\!om_R(C, C')$ e $v \in \mathscr{H}\!om_R(E, E')$ o* produto tensorial

$$u \otimes v \in \mathscr{H}\!om_{\mathbb{Z}}(C \otimes_R E, C' \otimes_R E')$$

é definido por

$$\langle u \otimes v, c \otimes e\rangle = (-1)^{\deg v \cdot \deg c}\langle u, c\rangle \otimes \langle v, e\rangle \text{ para } c \in C, e \in E.$$

Proposição A.8. *Sejam u, v e $u \otimes v$ como na definição anterior. Se D é o diferencial em qualquer um dos três complexos $\mathscr{H}om$ que estamos considerando, então $D(u \otimes v) = Du \otimes v + (-1)^{\deg u} u \otimes Dv$. Em outras palavras, a operação de "produto tensorial de morfismos graduados" define um morfismo de cadeia*

$$\mathscr{H}om_R(C, C') \otimes \mathscr{H}om_R(E, E') \to \mathscr{H}om_{\mathbb{Z}}(C \otimes_R E, C' \otimes_R E').$$

Além disso, se $u\colon C \to C'$ é um morfismo de cadeia (de grau zero), então existe um morfismo de cadeia $\mathscr{H}om_R(E, E') \to \mathscr{H}om_{\mathbb{Z}}(C \otimes_R E, C' \otimes_R E')$ dado por $v \mapsto u \otimes v$. E o produto tensorial de morfismos de cadeia é compatível com a homotopia no seguinte sentido: dados morfismos de cadeia e homotopias $u_0 \simeq u_1 \colon C \to C'$ e $v_0 \simeq v_1 \colon E \to E'$, segue que $u_0 \otimes v_0 \sim u_1 \otimes v_1 \colon C \otimes_R E \to C' \otimes_R E'$.

Proposição A.9. *Se A é um $\mathbb{Z}$-módulo e $a \neq 0$, para $a \in A$, então existe um morfismo $f : A \to \mathbb{Q}/\mathbb{Z}$ tal que $f(a) \neq 0$.*

Proposição A.10. *Homotopia é uma relação de equivalência.*

Proposição A.11. *Um morfismo de cadeia $f : C \to C'$ induz um morfismo $H(f) : H(C) \to H(C')$. Além disso, $H(f) = H(g)$ se $f \simeq g$.*

Definição A.12. *Um morfismo de cadeia $f : C \to C'$ é uma* equivalência homotópica *se existe um morfismo de cadeia $f' : C' \to C$ tal que $f'f \simeq id_C$ e $ff' \simeq id_{C'}$. Além disso, um morfismo de cadeia f é uma* equivalência fraca *se $H(f) : H(C) \to H(C')$ é um isomorfismo.*

Teorema A.13. *Seja $f\colon C' \to C$ uma equivalência fraca entre complexos de R-módulos à direita. Se P é um complexo não negativo de R-módulos plano à esquerda, então $f \otimes_R P\colon C' \otimes_R P \to C \otimes_R P$ é uma equivalência fraca.*

Proposição A.14. *Qualquer equivalência homotópica é uma equivalência fraca.*

Definição A.15. *Um complexo de cadeia C é dito* contrátil *se é homotopicamente equivalente ao complexo zero, ou seja, se $id_C \simeq 0$. Uma homotopia de id_C a 0 é dita uma* homotopia de contração.

Definição A.16. *Um complexo de cadeia é dito* acíclico *se $H(C) = 0$.*

Observe que qualquer complexo de cadeia contrátil é acíclico, pois pela proposição A.11 temos que, se $\mathrm{id}_C \simeq 0$, então $H(\mathrm{id}_C) = H(0) = 0$, ou seja, $H(C) = 0$.

Proposição A.17. *Um complexo de cadeia (C, d) é contrátil se, e somente se, é acíclico e cada sequência exata $0 \to Z_{n+1} \hookrightarrow C_{n+1} \xrightarrow{\overline{p}} Z_n \to 0$ cinde, em que $\overline{p}$ é induzido por d.*

Proposição A.18. *Uma sequência exata curta $0 \to C' \xrightarrow{i} C \xrightarrow{\pi} C'' \to 0$ de complexos de cadeia dá origem a uma sequência exata longa de homologia*

$$\cdots \to H_n(C') \stackrel{H(i)}{\to} H_n(C) \stackrel{H(\pi)}{\to} H_n(C'') \stackrel{\partial}{\to} H_{n-1}(C') \to \dots .$$

O morfismo de conexão ∂ é natural no sentido que o diagrama comutativo

$$\begin{array}{ccccccccc} 0 & \longrightarrow & C' & \xrightarrow{i} & C & \xrightarrow{\pi} & C'' & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E' & \xrightarrow{i} & E & \xrightarrow{\pi} & E'' & \longrightarrow & 0 \end{array}$$

com linhas exatas nos dá um diagrama comutativo

$$\begin{tikzcd} H_n(C'') \arrow[r] \arrow[d] & H_{n-1}(C') \arrow[d] \\ H_n(E'') \arrow[r] & H_{n-1}(E') \end{tikzcd}$$

Proposição A.19. *(Fórmula de Künneth) Seja R um domínio de ideais principais e sejam C e C' complexos de cadeia tais que C é livre em cada dimensão. Existem sequências exatas naturais*

$$0 \to \oplus_{p\in\mathbb{Z}} H_p(C) \otimes_R H_{n-p}(C') \to H_n(C \otimes C') \to \oplus_{p\in\mathbb{Z}} \operatorname{Tor}_1^R(H_p(C), H_{-n-p-1}(C')) \to 0$$

e

$$0 \to \Pi_{p\in\mathbb{Z}} \operatorname{Ext}^1_R(H_p(C), H_{p+n+1}(C')) \to H_n(\mathscr{H}\!om_R(C, C')) \to \Pi_{p\in\mathbb{Z}} \operatorname{Hom}_R(H_p(C), H_{p+n}(C')) \to 0,$$

e estas sequências cindem.

Sejam R um anel com unidade e M um R-módulo (à esquerda).

Definição A.20. *Uma* resolução *de M é uma sequência exata de R-módulos*

$$\cdots \to F_2 \xrightarrow{\partial_2} F_1 \xrightarrow{\partial_1} F_0 \xrightarrow{\varepsilon} M \to 0.$$

Se cada F_i é livre, dizemos que é uma resolução livre.

Definição A.21. *Quando existe um inteiro n tal que $F_i = 0$ para $i > n$, dizemos que a resolução tem* comprimento $\geq n$. *Escreveremos então*

$$0 \to F_n \to \cdots \to F_0 \to M \to 0$$

e está implícito que a resolução continua com zeros à esquerda.

Sejam R um anel e M um R-módulo, temos que M admite diferentes resoluções livres (que são homotopicamente equivalentes).

Lema A.22. *(Lema Fundamental da Álgebra Homológica) Sejam (C, ∂) e (C', ∂') complexos de cadeia e seja r inteiro. Considere $(f_i : C_i \to C'_i)_{i\leq r}$ uma família de morfismos tais que $\partial'_i f_i = f_{i-1}\partial_i$ para $i \leq r$. Se C_i é projetivo para $i > r$ e $H_i(C') = 0$ para $i \geq r$, então $(f_i)_{i\leq r}$ se entende para um único morfismo de cadeia $f : C \to C'$ a menos de homotopia. Mais precisamente, quaisquer duas extensões são homotópicas por uma homotopia h tal que $h_i = 0$ para $i \leq r$.*

Sejam $\varepsilon : F \to M$ e $\varepsilon' : F' \to M$ duas resoluções livres (ou projetivas) de um módulo M. Podemos construir um complexo de cadeia aumentado com M na dimensão -1 e aplicar o lema A.22 com $r = -1$:

$$\begin{tikzcd} \ldots \arrow[r] & F_1 \arrow[r] \arrow[d, dashed] & F_0 \arrow[r, "\varepsilon"] \arrow[d, dashed] & M \arrow[r] \arrow[d, "\mathrm{id}_M"] & 0 \arrow[r] \arrow[d] & \ldots \\ \ldots \arrow[r] & F'_1 \arrow[r] & F'_0 \arrow[r, "\varepsilon'"] & M \arrow[r] & 0 \arrow[r] & \ldots \end{tikzcd}$$

Concluímos que existe um morfismo de cadeia $f : F \to F'$ que *preserva aumento*, ou seja, que satisfaz $\varepsilon' f = \varepsilon$ e também que f é única a menos de homotopia. Note que a homotopia h do lema A.22 no nível do complexo de cadeia aumentado nos dá a homotopia $F \to F'$, pois $h_{-1} = 0$.

Teorema A.23. *Dadas resoluções projetivas F e F' de um módulo M, existe um morfismo de cadeia $f : F \to F'$ que preserva aumento, único a menos de homotopia, e f é uma equivalência homotópica.*

Corolário A.24. *Seja $\varepsilon : F \to \mathbb{Z}$ uma resolução livre de $\mathbb{Z}$ sobre um $\mathbb{Z}$-módulo. Então ε é uma equivalência homotópica.*

Neste final, encontram-se alguns teoremas bem conhecidos que foram necessários para o desenvolvimento deste trabalho.

Lema A.25. *Todo módulo livre é projetivo.*

Lema A.26. *(a) Dado um diagrama:*

$$\begin{tikzcd} P \arrow[r, "d"] \arrow[d, dashed, "g"] & Q \arrow[d, "f"] & \\ M' \arrow[r, "d_1"] & M \arrow[r, "d_2"] & M'' \end{tikzcd}$$

em que $d_2 f d = 0$, queremos encontrar g tal que $d_1 g = fd$. Se P é projetivo e a linha de baixo é exata, então tal g existe.
(b) Dado um diagrama:

$$\begin{tikzcd} & P \arrow[r, "d"] \arrow[dl, dashed, "k"] \arrow[d, "f"] & Q \arrow[dl, "h"] \\ M' \arrow[r, "d_1"] & M \arrow[r, "d_2"] & M'' \end{tikzcd}$$

em que $d_2 h d = d_2 f$, queremos encontrar k tal que $d_1 k + hd = f$. Se P é projetivo e a linha de baixo é exata, então tal k existe.

Proposição A.27. *P é projetivo se, e somente se, para toda sobrejeção $\pi : M \to \overline{M}$ e todo morfismo $\varphi : P \to \overline{M}$ existe um único morfismo $\psi : P \to M$ tal que $\varphi = \pi\psi$.*

$$\begin{tikzcd} & P \arrow[dl, dashed, "\psi"] \arrow[d, "\varphi"] \\ M \arrow[r, "\pi"] & \overline{M}. \end{tikzcd}$$

Proposição A.28. *As seguintes condições sobre um R-módulo P são equivalentes:*
(i) P é projetivo.
(ii) Toda sequência exata $0 \to M' \to M \to P \to 0$ cinde.
(iii) P é um somando direto de um módulo livre.
(iv) Existem elementos $e_i \in P$ e $f_i \in \mathrm{Hom}_R(P, R)$ (em que os índices de i variam em algum conjunto I) tal que para todo $x \in P$, $f_i(x) = 0$ para quase todos i e $x = \sum_{i \in I} f_i(x) e_i$.

Para próxima proposição, considere $P^* = \mathrm{Hom}_R(M, P)$.

Proposição A.29. *Seja P um R-módulo à esquerda projetivo e finitamente gerado.*
(a) P^* é um R-módulo à direita projetivo e finitamente gerado.
(b) Para qualquer R-módulo à esquerda M, existe um isomorfismo

$$\varphi : P^* \otimes_R M \xrightarrow{\cong} \mathrm{Hom}_R(P, M)$$

de grupos abelianos, dado por $\varphi(u \otimes m)(x) = u(x) \cdot m$ para $u \in P^*$, $m \in M$ e $x \in P$.
(c) Para qualquer R-módulo à direta M, existe um isomorfismo

$$\varphi' : M \otimes_R P \xrightarrow{\cong} \mathrm{Hom}_R(P^*, M),$$

dado por $\varphi'(m \otimes x)(u) = m \cdot u(x)$ *para* $m \in M$, $x \in P$ *e* $u \in P^*$.
(d) Existe um isomorfismo

$$\varphi'' : P \overset{\cong}{\to} P^{**}$$

de R*-módulos à esquerda, dado por* $\varphi''(x)(u) = u(x)$ *para* $x \in P$, $u \in P^*$.