UNIVERSIDADE FEDERAL DE MINAS GERAIS

MESTRADO EM MATEMÁTICA

TEOREMA DE GOLOD-SHAFAREVICH

Lorena Mara Costa Oliveira

Belo Horizonte - MG
2014

Lorena Mara Costa Oliveira

Teorema de Golod-Shafarevich

Dissertação submetida à banca examinadora, designada pelo Programa de Pós-Graduação em Matemática da UFMG, como requisito parcial para a obtenção do título de mestre em Matemática.

Orientador: Andre Gimenez Bueno

Universidade Federal de Minas Gerais
16 de maio de 2014

0.1 Agradecimentos

Eu gostataria de agradecer a todos que de alguma forma contribuiu para a elaboração da minha dissertação.

Primeiramente, agradeço aos meus familiares que sempre estiveram presentes nos meus momentos mais difícies mas com palavras e gestos para me incentivar a continuar na caminhada.

Agradeço imensamente a minha Orientadora da Graduação, Ana Cristina Vieira, por ter me ensinado os primeiros passosnos estudos matemáticos e que me inspirou a seguir na área algébrica. Já no meu mestrado com toda paciência e sabedoria me transmitiu parte dos seus conhecimentos para que a realização e conclusão da minha dissertação.

Agradeço ao meu orientador, Andre Gimenez Bueno, pelo empenho em passar os seus conhecimentos e pela paciência nos momentos difícies que enfretamos ao longo desse período.

Agradeço a todos os funcionários do departamento de matemática da UFMG que muito me ajudaram por todo esses meses, aos professores que compuseram a banca, Prof Ana Cristina Vieira e Prof Viktor Bekkert.

Agradeço a Capes pelo apoio financeiro.

Finalmente, agradeço a todos os meus colegas e amigos que foram fundamentais no meu desenvolvimento matemático tornando muitas vezes a minha jornada bem mais leves. Em especial ao Danilo Avelar, Pedro Henrique, Pedro Franklin, Gabriela Oliveira, Marina Muniz e Fabrício Veliq.

0.2 Abstract

Golod-Shafarevich Theorem

This thesis is about the celebrated theorem of Golod and Shafarevich. It can be viewed as a theorem on homological algebra for noncommutative local rings. However, the main motivation in finding and proving it came from number theory: if K is an algebraic number field (i.e., a finite extension of $\mathbb{Q}$), and we iterate the construction of the Hilbert class field (the maximal abelian unramified extension of K), we get the class field tower of K. The theorem shows that in general such towers can be infinite. For instance, when the discriminant of $K/\mathbb{Q}$ has at least 6 prime factors, and K is imaginary quadratic, then such tower is always infinite. For more general extensions it is still true that those towers can be infinite, provided that that discriminant has a large enough number of prime factors. Another related area where the theorem is relevant is group theory. If G is a finite p-group with d being its minimal number of generators, and r relations, the theorem asserts that $r > d^2/4$. The connection with group cohomology comes from the fact that $d = \dim H^1(G, \mathbb{Z}/p\mathbb{Z})$ and $r = \dim H^2(G, \mathbb{Z}/p\mathbb{Z})$. The theorem has an interesting application to the generalised Burnside conjecture. For each prime p there is an infinite group generated by 3 elements, in which every element is of finite order, namely a power of p. The main tools used came from homological algebra, especially group homology and cohomology.

0.3 Resumo

O teorema de Golod-Shafarevich

A dissertação é sobre o célebre teorema de Golod-Shafarevich. Este teorema pode ser visto como um teorema em álgebra homológica para anéis não-comutativos. Contudo, a principal motivação para prová-lo veio da teoria dos números: mais precisamente se K é uma extensão finita de $\mathbb{Q}$ e iterarmos a construção do corpo de classe de Hilbert (extensão maximal abeliana não-ramificada de K), obtemos a torre de corpos de classe de K. O teorema em questão demonstra de forma construtiva que em geral tais torres são infinitas. Por exemplo, se o discriminante de $K/\mathbb{Q}$ contiver pelo menos 6 fatores primos, e K for imaginário quadrático, então tal torre é sempre infinita. Para extensões gerais, a infinitude de tal torre continua valendo, desde que o discriminante contenha um número de primos suficientemente grande. Outra área na qual o teorema tem consequências importantes (e diretamente relacionado ao anterior), é na teoria dos grupos. Seja G um p-grupo finito não-trivial, com d geradores (número minimal de geradores) e r relações entre estes. Segue do teorema que $r > d^2/4$. A conexão com a cohomologia de grupos vem do fato que $d = \dim\ H^1(G, \mathbb{Z}/p\mathbb{Z})$ e $r = \dim\ H^2(G, \mathbb{Z}/p\mathbb{Z})$. Isso nos permite aplicações para a conjectura generalizada de Burnside. Por exemplo, para cada primo p será construido um grupo infinito gerado por 3 elementos, no qual todo elemento tem ordem finita, uma potência de p. As ferramentas utilizadas serão as da álgebra homológica, em especial da homologia e cohomologia de grupos.

Sumário

0.4 Introdução

Os matemáticos E.S.Golod e I.R.Shafarevich, na década de 60, provaram um importante teorema

Seja G um p-grupo finito, então

$$h_2(G) > 1/4h_1(G)^2,$$

onde $h_i(G) = \dim H^i(G, \mathbb{Z}/p\mathbb{Z})$ *para* $i \geq 0$

usando como ferramentas a álgebra homológica.

A motivação que E.S.Golod e I.R.Shafarevich tiveram para demostrarem esse teorema foi para resolverem o problema da torre de corpos de classes que ainda estava em aberto. Para compreender o problema em questão, considere a torre

$$k \subset k_1 \subset \cdots \subset k_i \subset \cdots$$

que ocorre na teoria de corpo de classe, onde k é algum corpo e cada corpo k_{i+1} é o corpo de classe de Hilbert de k_i (extensão maximal abeliana não ramificada de k_i). A união K dos corpos k_i é a extensão maximal solúvel não ramificada de k. Em 1925, Ph. Furtwängler afirmou que a extensão K/k (o problema da torre de corpos de classes) é finita.

Esse problema ficou em aberto por algumas décadas e o Teorema de Golod-Shafarevich demonstrou, em 1964, de forma construtiva que tais torres em geral são infinitas.

Nesse trabalho não trataremos sobre os corpos de classes de Hilbert que utiliza a Teoria dos Números, pois o objetivo principal aqui é provar o Teorema de Golod-Shafarevich através da álgebra homológica.

A construção feita para demonstrar o Teorema de Golod-Shafarevich, utilizando como ferramentas a álgebra homológica, e também algumas importantes aplicações desse teorema na Teoria de Grupos, bem como em Álgebras Polinomiais Não Comutativas, foram a motivação central desse trabalho que está estruturado em três capítulos. O Capítulo 1 é dedicado aos conceitos básicos necessários à compreensão do texto, tais como as definições e propriedades de uma sequência exata de Λ-módulos, do conjunto $\mathrm{Hom}_\Lambda(A, B)$, de categorias e funtores. Além disso, mostramos que os funtores, $\mathrm{Hom}_\Lambda(A, -)$ e $\mathrm{Hom}_\Lambda(-, A)$, que vão da categoria dos Λ-módulos para a categoria de grupos abelianos são funtores exatos à esquerda. Ainda nesta seção mostramos o Lema da Serpente que foi fundamental na construção dos Grupos de Tate presente no Capítulo 3. Posteriormente, dedicamos uma seção aos estudos das principais propriedades da categoria dos G-módulos, onde G é um grupo. Um resultado importante dessa seção é que o conjunto $\mathrm{Hom}_\mathbb{Z}(M, N)$ se torna um G-módulo quando é dada uma estrutura especial.

No Capítulo 2 foram feitas as construções das ferramentas necessárias para provar o Teorema de Golod-Shafarevich, isto é, os conceitos básicos e propriedades dos Grupos de Cohomologia e Homologia. Dado um complexo de cocadeias formado a partir de uma resolução injetiva de um G-módulo M, tem-se uma sequência, não necessariamente exata, e com isso definimos o Grupo de Cohomologia de G dado por $H^r(G, M) = \frac{\mathrm{Ker}(d^r)}{\mathrm{Im}(d^{r-1})}$. Como aplicação, vimos algumas propriedades dos Grupos de Cohomologia de L e $L^\times$ onde L é uma extensão finita de Galois de um corpo K e $L^\times = L - \{0\}$. Ainda neste capítulo, através das propriedades funtoriais

de Grupos de Cohomologia juntamente com o resultado do Lema do Shapiro, construímos importantes homomorfismos de Grupos de Cohomologia, tais como homomorfismos Restrição, Inflação e Corestrição. Há uma relação entre os homomorfismos Inflação e Restrição que gera uma sequência exata Inflação-Restrição. Essa sequência exata, tem um papel importante ao longo da construção para a prova do teorema central desse trabalho. Dedicamos uma seção para definir os Grupos de Homologia e apresentar algumas propriedades desses grupos. Para a construção dos Grupos de Homologia tomamos um complexo de cadeias formado a partir de uma resolução projetiva de um G-módulo M e assim, temos os Grupos de Homologia de G dados por $H_r = \frac{\mathrm{Ker}(d_r)}{\mathrm{Im}(d_{r+1})}$.

Os conceitos e propriedades dos Grupos de Cohomologia e Homologia desempenham um papel muito importante no desenvolvimento realizado no Capítulo 3 para a prova do Teorema de Golod-Shafarevich.

No Capítulo 3 foi desenvolvida a demonstração do teorema chave desse trabalho, bem como aplicações desse resultado que teve grande influência em várias áreas da Matemática e vimos sua contribuição para a Teoria de Grupos e Álgebras Polinomiais Não Comutativas. O teorema provado por Golod-Shafarevich diz que para um p-grupo G finito não trivial com d geradores (número minimal de geradores) e r relações entre eles, temos $r > d^2/4$. A relação desse teorema com os Grupos de Cohomologia vem do fato que $d = \dim H^1(G, \mathbb{Z}/p\mathbb{Z})$ e $r = \dim H^2(G, \mathbb{Z}/p\mathbb{Z})$. Uma observação a ser feita é que a referência [15], usada como base para o prova desse teorema, considera G um grupo profinito. Como ao longo desse capítulo consideramos G um grupo finito e todo grupo finito é um grupo profinito, não entramos em detalhes sobre os grupos profinitos e sua topologia envolvida. Na primeira seção tratamos de algumas propriedades de p-grupos finitos, definimos $h_i(G) = \dim H^i(G, \mathbb{Z}/p\mathbb{Z})$ e mostramos que quando $i = 1$ isto nos dá o número minimal de geradores de G e sendo $i = 2$ temos o número minimal de relações entre os geradores de G. E por último, definimos o número de Shafarevich e mostramos que tal número é não negativo. Posteriormente, foram definidos os Grupos de Tate que através do Lema da Serpente nos dá uma sequência que relaciona os Grupos de Cohomologia com os Grupos de Homologia e além disso, é uma sequência exata. Para demonstrar o teorema de Golod-Shafarevech, além de todas essas definições e propriedades, foi preciso provar dois lemas de extrema importância para essa demonstração que nos fornece resultados relevantes nos Grupos de Homologia. Uma outra observação importante é que os resultados vindo dos Grupos de Tate permitem que h_i, de uma maneira especial, nos dê a dimensão dos Grupos de Homologia e com isso, juntamente com os dois lemas, o teorema em questão consiste do comportamento da homologia de G. Assim, por construção provamos o Teorema de Golod-Shafarevich.

Esse Teorema de Golod-Shafarevich pode ser visto utilizando-se álgebras polinomiais não comutativas. Para isso, consideramos $F\langle X\rangle = F\langle x_1, \cdots, x_d\rangle$ uma álgebra polinomial nas variáveis não comutativas $x_1, \cdots, x_d$ e construimos a álgebra polinomial não comutativa $A = F\langle X\rangle/\mathfrak{A}$, onde $\mathfrak{A}$ é um ideal de $F\langle X\rangle$ gerada pelos elementos homogêneos $f_1, f_2, \cdots$. Resumidamente, o Teorema de Golod-Shafarevich é o seguinte

Para a álgebra A como descrita acima, considerando $n_i = \delta(f_i)$ o grau de cada polinômio homogêneo f_i e r_i o número de polinômios homogêneos de grau i, temos que

1. *Se para cada i, $r_i \leq [(d-1)/2]^2$, então A tem dimensão infinita sobre F.*

Em 1941, surgiu o seguinte problema de Kurosh-Levitzki

Seja K um corpo. Suponha que A seja uma álgebra finitamente gerada sobre K e que todo elemento de A seja nilpotente. A álgebra A tem dimensão finita?

O matemático Golod utilizando o Teorema de Golod-Shafarevich construiu uma álgebra nil, que apesar de ser gerada por três elementos, tem dimensão infinita. Esse resultado foi o primeiro contra exemplo para o problema de Kurosh-Levitzky.

Outra importante contribuição matemática que esse teorema proporcionou, foi dar o primeiro contra exemplo que nega a conjectura de Burnside feita em 1911:

Seja G um grupo finitamente gerado com todo elemento de ordem finita, então G é finito.

Para mostrar que essa afirmação é falsa, Golod-Shafarevich provaram o seguinte resultado

Se p um número primo qualquer, existe um grupo G infinito, gerado por três elementos em que cada elemento de G tem ordem finita e de potência de p.

Portanto, esse trabalho teve como objetivo expor e provar o poderoso Teorema de Golod-Shafarevech e mostrar algumas contribuições de relevante interesse para a matemática.

Capítulo 1

Preliminares

1.1 Módulos e Sequências Exatas

Nesta seção considere R um anel, não necessariamente comutativo, mas com unidade 1_R. Os homomorfismos de anéis $\alpha : A \to B$ sempre satisfazem $\alpha(1_A) = 1_B$.

Veremos em quais condições uma sequência de R-módulos à esquerda é uma sequência exata. Posteriormente, para todos R-módulos A e B, definiremos o conjunto $\mathrm{Hom}_R(A, B)$. Além disso, mostraremos que o funtores, $\mathrm{Hom}_R(A, -)$ e $\mathrm{Hom}_R(-, A)$, que leva uma categoria de R-módulos para uma categoria de grupos abelianos são funtores exatos.

Definição 1.1. *Uma sequência*

$$\cdots \xrightarrow{\varphi_i} A_i \xrightarrow{\varphi_{i+1}} A_{i+1} \to \cdots$$

de R-módulos é exata em A_i se $\mathrm{Ker}(\varphi_{i+1}) = \mathrm{Im}(\varphi_i)$. *Assim, uma sequência é exata se for exata em todos os elementos da sequência.*

Seja $0 \xrightarrow{\alpha} A \xrightarrow{\iota} B \xrightarrow{\pi} C \xrightarrow{\beta} 0$ uma sequência exata de R-módulos. Considere os seguintes casos:

(i) Como a sequência é exata em A, temos $\mathrm{Ker}(\iota) = \mathrm{Im}(\alpha) = 0$. Isso implica que ι é injetivo.

(ii) Com a exatidão em B, $\mathrm{Ker}(\pi) = \mathrm{Im}(\iota)$.

(iii) Sendo a sequência exata em C, então $C = \mathrm{Ker}(\beta) = \mathrm{Im}(\pi)$. Assim, π é sobrejetiva.

Note que isso implica $C \cong B/A$. Tal sequência é chamada sequência exata curta de R-módulos.

Definição 1.2. *Denote por* $\mathrm{Hom}_R(M, N)$ *o conjunto dos mapas $\alpha : M \to N$ que são R-homomorfismos.*

Definição 1.3. *Seja R um anel e $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ uma sequência exata curta de R-módulos. Se existe um R-módulo complementar de $\psi(A)$ em B então dizemos que a sequência cinde. Nesse caso, $B = \psi(A) \oplus C'$, para algum R-submódulo C' de B, e $\varphi(C') \simeq C$.*

Proposição 1.1. *(Proposição 26.10 [4]) Uma sequência exata curta* $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ *de R-módulos cinde se, e somente se, existe um homomorfismo* $\alpha : C \to B$ *de R-módulos tal que* $\varphi \circ \alpha = 1_C$.

Demonstração. Suponha $\alpha : C \to B$ um homomorfismo de R-módulos tal que $\varphi \circ \alpha = 1_C$. Seja $\alpha(C) = C'$ para algum R-submódulo C' de B . Então, $\varphi(\alpha(C)) = \varphi(C') = C$ e assim, $\varphi(C') \simeq C$. Agora mostraremos que $B = \psi(A) \oplus C'$, isto é, $\psi(A) \cap C' = 0$ e todo $b \in B$ é escrito da forma $\psi(a) + c'$ para algum $a \in A$ e $c' \in C'$.

1. $\psi(A) \cap C' = 0$
   Tome $b_1 \in \psi(A) \cap C'$. Com isso, $b_1 \in \psi(A)$, isto é, $b_1 \in \mathrm{Im}(\psi) = \mathrm{Ker}(\varphi)$. Por sua vez, $b_1 \in C' = \alpha(C)$, então existe $c \in C$ tal que $\alpha(c) = b_1$. Logo, $\varphi(b_1) = \varphi \circ \alpha(c) = 0$.

   O mapa $\varphi \circ \alpha$ é injetivo, pois $\varphi \circ \alpha$ é o mapa identidade em C. Assim, $c = 0$ e $b_1 = \alpha(0) = 0$.

2. $b = \psi(a) + c'$
   Considere $b = b - \alpha(c) + \alpha(c)$, onde $\alpha(c) = c'$ para algum $c' \in C'$. Sendo φ um mapa sobrejetivo podemos afirmar que $\varphi(b) = c$. Note que

$$\varphi(b - \alpha(c)) = \varphi(b) - \varphi(\alpha(c)) = \varphi(b) - c = c - c = 0.$$

   Assim, $b - \alpha(c) \in \mathrm{Ker}(\varphi) = \mathrm{Im}(\psi)$. Com isso, $b - \alpha(c) = \psi(a)$, para algum $a \in A$.

Portanto, a sequência cinde.

Suponha que a sequência $0 \to A \xrightarrow{\psi} B \xrightarrow{\varphi} C \to 0$ cinde, isto é, para algum R-submódulo C' de B, $B = \psi(A) \oplus C'$ e $\varphi(C') \simeq C$. Defina $\alpha = \varphi^{-1} : C \to B$, que está bem definido, pois $\varphi(C')$ é um mapa bijetivo a C e por isso, tem inversa. Logo, $\varphi \circ \alpha = 1_C$. □

Proposição 1.2. *(Proposição 29.10 [4]). Sejam D, L e N R-módulos, então temos:*

1. $\mathrm{Hom}_R(D, L \oplus N) \simeq \mathrm{Hom}_R(D, L) \oplus \mathrm{Hom}_R(D, N)$.

2. $\mathrm{Hom}_R(L \oplus N, D) \simeq \mathrm{Hom}_R(L, D) \oplus \mathrm{Hom}_R(N, D)$.

Demonstração. Seja $\pi_1 : L \oplus N \to L$ a projeção natural de $L \oplus N$ em L, ou seja, $\pi_1(l, n) = l$. Analogamente, seja π_2 a projeção natural de $L \oplus N$ em N. Se $\alpha \in \mathrm{Hom}_R(D, L \oplus N)$, então as composições $\pi_1 \circ \alpha$ e $\pi_2 \circ \alpha$ nos dão elementos em $\mathrm{Hom}_R(D, L)$ e $\mathrm{Hom}_R(D, N)$, respectivamente. Assim sendo, tome o seguinte mapa:

$$\begin{aligned} \varphi : \mathrm{Hom}_R(D, L \oplus N) &\to \mathrm{Hom}_R(D, L) \oplus \mathrm{Hom}_R(D, N) \\ \alpha &\mapsto (\pi_1 \circ \alpha, \pi_2 \circ \alpha). \end{aligned}$$

que, claramente, está bem definido.
Neste instante, considere o mapa

$$\begin{aligned} \psi : \mathrm{Hom}_R(D, L) \oplus \mathrm{Hom}_R(D, N) &\to \mathrm{Hom}_R(D, L \oplus N) \\ (\beta_1, \beta_2) &\mapsto f(d) = (\beta_1(d), \beta_2(d)) \text{ para todo } d \in D. \end{aligned}$$

Facilmente verifica-se que é um homomorfismo e, além disso, que φ e ψ são homomorfismos mutuamente inversos. Isso prova o isomorfismo em 1. Similarmente é provada a afirmação 2. □

1.1.1 Categorias e Funtores

Um conjunto $\mathfrak{C}$ para ser definido como uma categoria é necessário fornecer:

(*i*) A classe dos objetos $A, B, C, \cdots$ que pertencem a categoria $\mathfrak{C}$;

(*ii*) Para cada par de objetos A, B de $\mathfrak{C}$ um conjunto $\mathfrak{C}(A, B)$, de morfismos de A para B;

(*iii*) Para os objetos A, B, C de $\mathfrak{C}$, uma lei de composição:

$$\mathfrak{C}(A, B) \times \mathfrak{C}(B, C) \to \mathfrak{C}(A, C).$$

Para cada categoria $\mathfrak{C}$, temos os seguintes axiomas:

(*i*) Os conjuntos $\mathfrak{C}(A_1, B_1)$ e $\mathfrak{C}(A_2, B_2)$ são disjuntos, a menos que $A_1 = A_2$ e $B_1 = B_2$;

(*ii*) Dados os objetos A, B, C e D de $\mathfrak{C}$ e os morfismos $\alpha : A \to B$, $\beta : B \to C$ e $\varphi : C \to D$, temos:

$$\varphi(\beta\alpha) = (\varphi\beta)\alpha;$$

(*iii*) Para cada objeto A de $\mathfrak{C}$ existe um morfismo $1_A : A \to A$ tal que para todo $\alpha : A \to B$ e $\beta : C \to A$, temos:

$$\alpha \circ 1_A = \alpha, \quad 1_A \circ \beta = \beta.$$

Segue abaixo alguns exemplos de categorias e seus devidos conjuntos de morfismos:

1. A categoria $\mathfrak{C}$ de conjuntos e funções;
2. A categoria $\mathfrak{G}$ de grupos e homomorfismos;
3. A categoria $\mathfrak{Ab}$ de grupos abelianos e homomorfismos;
4. A categoria $\mathfrak{R}$ de anéis e homomorfismos de anéis;
5. A categoria $\mathfrak{R}_1$ de anéis com unidade 1_R e homomorfismos que preserva a identidade;
6. A categoria $\mathfrak{M}_\Lambda$ de Λ-módulos, onde Λ é um objeto de $\mathfrak{R}_1$ e homomorfismos de Λ-módulos.

Dadas duas categorias distintas $\mathfrak{C}$ e $\mathfrak{D}$, um funtor $\omega : \mathfrak{C} \to \mathfrak{D}$ é uma transformação que associa cada objeto A de $\mathfrak{C}$ um objeto $\omega(A)$ de $\mathfrak{D}$, e também associa todo morfismo α de $\mathfrak{C}(A, B)$ a um morfismo $\omega(\alpha)$ em $\mathfrak{D}(\omega(A), \omega(B))$ através de:

$$\omega(\alpha\beta) = (\omega(\alpha)\omega(\beta)), \quad \omega(1_A) = 1_{\omega(A)}.$$

Defina o funtor $\mathfrak{C}(A, -)$ como funtor covariante e o funtor $\mathfrak{C}(-, A)$ sendo funtor contravariante.

Dentre os funtores, estamos interessados nos funtores $\mathrm{Hom}_R(A, -)$ e $\mathrm{Hom}_R(-, A)$ onde A é um R-módulo.

Primeiramente, observe que o conjunto $\mathrm{Hom}_R(A, B)$, onde A e B são R-módulos, tem a estrutura de um grupo abeliano. Agora, dado um homomorfismo $\alpha : B_1 \to B_2$ de R-módulos,

temos que $\mathrm{Hom}_R(A,\alpha)$ é igual ao funtor $\mathrm{Hom}_R(A,-)$ aplicado no morfismo α e de mesmo modo, temos $\mathrm{Hom}_R(\alpha,A)$. Os funtores $\mathrm{Hom}_R(A,-)$ e $\mathrm{Hom}_R(-,A)$ vão da categoria de R-módulos para a categoria de grupos abelianos. Nesse instante, verificaremos como ocorre a indução pelo homomorfismo α.

- O funtor $\mathrm{Hom}_R(A,\alpha)$ induzido pelo homomorfismo $\alpha : B_1 \to B_2$ é dado por:

$$\begin{aligned} \alpha_* : \mathrm{Hom}_R(A,\alpha) : \mathrm{Hom}_R(A,B_1) &\to \mathrm{Hom}_R(A,B_2) \\ \varphi &\mapsto \alpha\circ\varphi. \end{aligned}$$

- Para o funtor $\mathrm{Hom}_R(\alpha,A)$, temos o induzido por α da seguinte maneira:

$$\begin{aligned} \alpha^* : \mathrm{Hom}_R(\alpha,A) : \mathrm{Hom}_R(B_2,A) &\to \mathrm{Hom}_R(B_1,A) \\ \psi &\mapsto \psi\circ\alpha. \end{aligned}$$

Teorema 1.1. *(Teorema 28.10 [4]). Sejam D, L, M e N R-módulos. Se*

$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0 \tag{1.1}$$

é exata, então a sequência

$$0 \to \mathrm{Hom}_R(D,L) \xrightarrow{\psi^*} \mathrm{Hom}_R(D,M) \xrightarrow{\varphi^*} \mathrm{Hom}_R(D,N) \tag{1.2}$$

também será exata.

Demonstração. Para mostrar a injetividade de ψ^* tome σ_1 e $\sigma_2 \in \mathrm{Hom}_R(D,L)$ tal que $\psi\circ\sigma_1(d) = \psi\circ\sigma_2(d)$ para todo $d \in D$. Sendo ψ injetivo, $\sigma_1(d) = \sigma_2(d)$ para todo $d \in D$.

Mostraremos que o $\mathrm{Ker}(\varphi^*) = \mathrm{Im}(\psi^*)$.

Tome $\alpha \in \mathrm{Ker}(\varphi^*)$ e assim, $\varphi\circ\alpha(d) = 0$ para todo $d \in D$ e $\alpha(d) \in \mathrm{Ker}(\varphi) = \mathrm{Im}(\psi)$. Então existe um $l \in L$ tal que $\alpha(d) = \psi(l)$, e como ψ é injetivo, para cada $d \in D$ temos um único $l \in L$. Dessa forma, o mapa $\alpha' : D \to L$ onde $\alpha'(d) = l$ está bem definido. Claramente, α' é um homomorfismo. Assim, $\psi^*\circ\alpha'(d) = \psi^*(l) = \alpha(d)$ e isso mostra que $\mathrm{Ker}(\varphi^*) \subseteq \mathrm{Im}(\psi^*)$. Por outro lado, tome $\alpha \in \mathrm{Im}(\psi^*)(\alpha')$, então $\varphi(\alpha(d)) = \varphi(\psi(\alpha'(d))) = 0$ para todo $d \in D$. Portanto, $\mathrm{Ker}(\varphi^*) = \mathrm{Im}(\psi^*)$, provando a exatidão da sequência 3.3. □

Proposição 1.3. *(Proposição 30.10 [4]). Seja P um R-módulo. Dessa forma, são equivalentes as seguintes afirmações:*

1. *Sejam L, M e N R-módulos. Se*

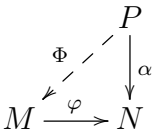
$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$$

é exata, então a sequência

$$0 \to \mathrm{Hom}_R(P,L) \xrightarrow{\psi^*} \mathrm{Hom}_R(P,M) \xrightarrow{\varphi^*} \mathrm{Hom}_R(P,N) \to 0 \tag{1.3}$$

também é uma sequência exata.

2. *Para todo M e N R-módulos, se $M \xrightarrow{\varphi} N \to 0$ é exata, então dado $\alpha \in \mathrm{Hom}_R(P, N)$ existe um levantamento $\Phi \in \mathrm{Hom}_R(P, M)$ que faz o seguinte diagrama comutar*



3. *Se P é um quociente de um R-módulo M, então P é isomorfo a um somando direto de M, isto é,*
   $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} P \to 0$ *cinde.*

4. *P é um somando direto de um R-módulo livre.*

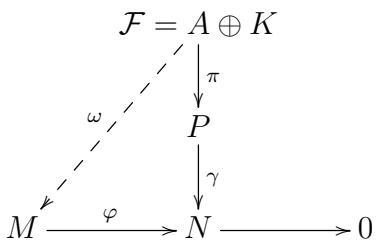
Demonstração. A equivalência de (1) para (2) segue do Teorema 1.1. Suponha que a afirmação (2) é satisfeita e considere a sequência exata $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} P \to 0$. Pela afirmação (2) o mapa identidade $id : P \to P$ levanta para um homomorfismo μ tal que $\varphi \circ \mu = 1_P$. Então, μ é um homomorfismo cindido. Isso mostra o item (3).

Todo P-módulo é quociente de um módulo livre. Dado um conjunto A, existe um $\mathcal{F}(A)$ R-módulo livre nesse conjunto. Em particular, temos $\mathcal{F}(P)$ R-módulo livre em P. Com isso, sempre existe a sequência exata

$$0 \to \mathrm{Ker}(\pi_*) \xrightarrow{\iota_*} \mathcal{F}(P) \xrightarrow{\pi_*} P \to 0.$$

Se a afirmação (3) é satisfeita para essa sequência, então ela cinde, isto é, $\mathcal{F}(P) \simeq \mathrm{Ker}(\varphi_*) \oplus P$. Assim, (4) está provada.

Para mostrar que (4) implica (2), suponha que P é um somando direto de um R-módulo livre no conjunto A, isto é, $\mathcal{F}(A) = P \oplus K$. Tome um homomorfismo $\gamma : P \to N$ e seja π a projeção natural de $\mathcal{F}(A)$ em P. Para todo $a \in A$ defina $n_a = \gamma \circ \pi(a)$. Sendo φ um mapa sobrejetivo, para todo $m_a \in M$ existe um $n_a \in N$ tal que $\varphi(m_a) = n_a$. Pela propriedade universal de módulos livres, existe um homomorfismo $\omega : \mathcal{F}(A) \to M$ com $\omega(a) = m_a$. Assim, o seguinte diagrama

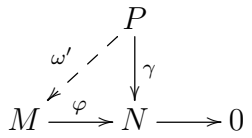


comuta, pois $\varphi \circ \omega(a) = \varphi(m_a) = n_a = \gamma \circ \pi(a)$ para todo $a \in A$.

Defina $\omega' : P \to M$ por $\omega'(p) = \omega((p, 0))$. Seja ι a inclusão natural de P em $\mathcal{F}(A)$ e sendo $\omega' = \omega \circ \iota$, então ω' é um homomorfismo. Assim,

$$\varphi \circ \omega'(p) = \varphi \circ \omega((p, 0)) = \gamma \circ \pi((p, 0)) = \gamma(p), \ \forall p \in P,$$

isto é, o diagrama



comuta.

Portanto, existe um homomorfismo ω' tal que $\varphi \circ \omega' = \gamma$, que prova que (4) implica (2). □

Teorema 1.2. *(Teorema 33.10 [4]) Para quaisquer R-módulos L, M, N e P, se*

$$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$$

é uma sequência exata curta, então

$$0 \to \mathrm{Hom}_R(N, P) \xrightarrow{\varphi^*} \mathrm{Hom}_R(M, P) \xrightarrow{\psi^*} \mathrm{Hom}_R(L, P)$$

será uma sequência exata curta.

Demonstração. Primeiro mostraremos que φ^* é injetivo.

Seja $\pi \in \mathrm{Hom}_R(N, P)$. Tome $\iota \in \mathrm{Ker}(\varphi^*)$, então $\iota \circ \varphi(m) = 0$ para todo $m \in M$. Como φ é sobrejetiva, $\iota(n) = 0$ para todo $n \in N$. Assim, $\iota = 0$.

Agora será provado que $\mathrm{Ker}(\psi^*) = \mathrm{Im}(\varphi^*)$.
Conside $\alpha \in \mathrm{Hom}_R(M, P)$ e tome $\beta \in \mathrm{Ker}(\psi^*)$, então $\beta \circ \psi(l) = 0$ para todo $l \in L$. Com isso, $\mathrm{Im}(\psi) = \mathrm{Ker}(\varphi) \in \mathrm{Ker}(\psi^*)$. Dado $n \in N$ e sendo φ sobrejetiva, existe $m \in M$ tal que $\varphi(m) = n$.

Defina $\gamma : N \to P$ por $\gamma(n) = \beta(m)$ que está bem definida, pois se $m_1 \in M$ tal que $\varphi(m) = \varphi(m_1)$, então $m - m_1 \in \mathrm{Ker}(\varphi)$. Como $\mathrm{Ker}(\varphi) \in \mathrm{Ker}(\psi^*)$, $\beta(m - m_1) = 0$. Assim, $\beta(m) = \beta(m_1)$. Logo, $\gamma(n) = \gamma(\varphi(m)) = \varphi^*(\gamma) = \beta(m)$ e $\beta \in \mathrm{Im}(\varphi^*)$. Isso mostra que $\mathrm{Ker}(\psi^*) \subseteq \mathrm{Im}(\varphi^*)$.

Observe que para $\omega \in \mathrm{Hom}_R(N, P)$

$$(\psi^* \circ \varphi^*)(\omega) = \psi^*(\omega \circ \varphi) = (\omega \circ \varphi) \circ \psi = \omega \circ (\varphi \circ \psi) = \omega \circ 0 = 0.$$

E assim, $\mathrm{Im}(\varphi^*) \subseteq \mathrm{Ker}(\psi^*)$. Portanto, $\mathrm{Hom}_R(-, P)$ é exato. □

Corolário 1. *Se a sequência exata de R-módulos*

$$0 \to M \xrightarrow{\varphi} N \xrightarrow{\psi} L \to 0$$

cinde, então a sequência

$$0 \to \mathrm{Hom}_R(L, P) \xrightarrow{\varphi^*} \mathrm{Hom}_R(N, P) \xrightarrow{\psi^*} \mathrm{Hom}_R(M, P) \to 0$$

é exata e também cinde.

Demonstração. Se a sequência exata $0 \to M \xrightarrow{\varphi} N \xrightarrow{\psi} L \to 0$ cinde, então $N = L \oplus M$. Em vista disso, $\mathrm{Hom}_R(N, P) = \mathrm{Hom}_R(L \oplus M, P)$ e pela Proposição 1.2, $\mathrm{Hom}_R(N, P) = \mathrm{Hom}_R(L \oplus M, P) = \mathrm{Hom}_R(L, P) \oplus \mathrm{Hom}_R(M, P)$. Isso induz a sequência

$$0 \to \mathrm{Hom}(L, P) \xrightarrow{\varphi^*} \mathrm{Hom}(L, P) \oplus \mathrm{Hom}(M, P) \xrightarrow{\psi^*} \mathrm{Hom}_R(M, P) \to 0.$$

Para provar sua exatidão, basta mostrar que ψ^* é sobrejetiva, pois as outras condições para essa sequência ser exata foram provadas no teorema 1.2. Note que,

$$\begin{array}{ccc} \mathrm{Hom}_R(L,P) \oplus \mathrm{Hom}_R(N,P) & \stackrel{\psi^*}{\to} & \mathrm{Hom}_R(N,P) \\ (\alpha,\beta) & \mapsto & \beta \end{array}$$

é um mapa sobrejetivo.

Tome $\mu : \mathrm{Hom}_R(L,P) \to \mathrm{Hom}_R(L,P) \oplus \mathrm{Hom}_R(M,P)$ onde $\mu(\omega) = (\omega, 0)$. Então, $\pi^* \circ \mu(\omega) = \pi^*(\omega, 0) = \omega$ para todo $\omega \in \mathrm{Hom}_R(L,P)$. Portanto, essa sequência cinde. □

Proposição 1.4. *(Proposição 34.10 [4]) Seja P um R-módulo. Dessa maneira, são equivalentes as afirmações:*

1. *Para todo L, M e N R-módulos, se*

$$0 \to L \stackrel{\pi}{\to} M \stackrel{\varphi}{\to} N \to 0$$

é uma sequência exata curta, então

$$0 \to \mathrm{Hom}_R(N,P) \stackrel{\varphi^*}{\to} \mathrm{Hom}_R(M,P) \stackrel{\pi^*}{\to} \mathrm{Hom}_R(L,P) \to 0$$

também é uma sequência exata.

2. *Para todo L e M R-módulos, se $0 \to L \stackrel{\psi}{\to} M$ é exata, então todo homomorfismo de R-módulos de L para P levanta para um homomorfismo de R-módulos de M para P. Assim, o seguinte diagrama comuta*

$$\begin{array}{ccccc} 0 & \longrightarrow & L & \xrightarrow{\pi} & M \\ & & \downarrow{\scriptstyle \omega} & \swarrow{\scriptstyle \Phi} & \\ & & P & & \end{array}$$

3. *Se P é um submódulo de um R-módulo M, então P é um somando direto de M, isto é, toda sequência exata curta $0 \to P \to M \to N \to 0$ cinde.*

Recorde que dado $\alpha : A' \to A$ um homomorfismo de R-módulos, definimos $\mathrm{Coker}(\alpha) = A/\mathrm{Im}(\alpha)$.

Lema 1.1. *(Lema 1.3.2 de [16]). (Lema da Serpente) Se o seguinte diagrama de sequências exatas de R-módulo comuta,*

$$\begin{array}{ccccccccc} & & A' & \xrightarrow{\iota} & B' & \xrightarrow{\pi} & C' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \psi} & & \\ 0 & \longrightarrow & A & \xrightarrow{\iota'} & B & \xrightarrow{\pi'} & C & & \end{array}$$

então existe uma sequência exata

$$0 \to \mathrm{Ker}(\alpha) \to \mathrm{Ker}(\beta) \to \mathrm{Ker}(\psi) \xrightarrow{\delta} \mathrm{Coker}(\alpha) \to \mathrm{Coker}(\beta) \to \mathrm{Coker}(\psi) \to 0.$$

Demonstração. Primeiramente, dado um mapa $\varphi : M \to N$, temos que $\mathrm{Coker}(\varphi) = N/\mathrm{Im}(\varphi)$.

Agora mostraremos que δ é um homomorfismo e está bem definido. A verificação da exatidão dessa sequência, por ser bem extensa, não será exposta aqui mas pode ser visto em algumas literaturas.

O único morfismo cuja definição é não trivial é o δ. O mapa δ é definido da seguinte maneira. Tome $c \in \mathrm{Ker}(\psi)$ e assim, $\pi(b) = c$ para algum $c \in C'$, pois o mapa π é sobrejetivo. Temos que $\beta(b) \in B'$ e como $c \in \mathrm{Ker}(\psi)$, então $\pi'(\beta(b)) = \psi(\pi(b)) = \psi(c) = 0$. Com isso, $\beta(b) \in \mathrm{Ker}(\pi') = \mathrm{Im}(\iota')$. Logo, $\beta(b) = \iota'(a')$ para um único $a' \in A$, pois ι' é injetivo. Defina, $\delta(c) = a + \mathrm{Im}(\alpha),\ a \in A$ e esse δ pode ser escrito da seguinte forma

$$\delta(c) = (\iota')^{-1}(\beta(\pi^{-1}(c))).$$

Para mostrar δ que está bem definido, basta verificar que não há ambiguidade no levantamento de $c \in C'$ para B'.

Suponha que $c = \pi(b_1) = \pi(b_2)$. Diante disso, $b_1 - b_2 \in \mathrm{Ker}(\pi) = \mathrm{Im}(\iota)$, então $b_1 - b_2 = \iota(a')$ para algum $a' \in A'$. Existe um único $a_1 \in A$ tal que $\iota'(a_1) = \beta(b_1)$. Logo,

$$\iota'(\alpha(a_1)) = \beta(\iota(a')) = \beta(b_1 - b_2) = \iota'(a_1 - a_2)$$

e sendo ι injetivo, $(a_1 - a_2) = \alpha(a_1) \in \mathrm{Im}(\alpha)$. Portanto, $a_1 + \mathrm{Im}(\alpha) = a_2 + \mathrm{Im}(\alpha)$ e o mapa δ está bem definido.

Agora, mostraremos que δ é um homomorfismo. Para isso, tome $c \in \mathrm{Ker}(\psi)$ e defina $\delta(c) = \iota^{-1} \circ \beta \circ \pi^{-1}(c)$. Claramente, $\delta(c) \in A$. Tome c_1 e $c_2 \in A$, então

$$\begin{aligned} \delta(c_1 + c_2) &= \iota^{-1} \circ \beta \circ \pi^{-1}(c_1 + c_2) \\ &= \iota^{-1} \circ \beta(\pi^{-1}(c_1) + \pi^{-1}(c_2)) \\ &= \iota^{-1} \circ \beta(\pi^{-1}(c_1)) + \iota^{-1} \circ \beta(\pi^{-1}(c_2)) \\ &= \delta(c_1) + \delta(c_2) \end{aligned}$$

e assim, δ é um homomorfimo. □

1.2 A categoria dos G-módulos

Seja G um grupo. Nesta seção daremos as condições para um grupo abeliano M ser um G-módulo. Definiremos o conjunto $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ e atráves de uma estrutura esse conjunto se torna um G-módulo.

Um G-módulo M é um grupo abeliano com um mapa,

$$\begin{aligned} G \times M &\to M \\ (g, m) &\mapsto g \cdot m \end{aligned}$$

tal que para todo $g, g' \in G$ e $m, m' \in M$, temos:

- G age sobre M e, consequentemente:

(*i*) $1 \cdot m = m$

(*ii*) $(gg')m = g(g' \cdot m)$;

- A ação é compatível com a adição em M

(*iii*) $g \cdot (m + m') = g \cdot m + g \cdot m'$.

O grupo de homomorfismos de grupos abelianos de M para N será denotado por $\mathrm{Hom}_{\mathbb{Z}}(M, N)$. Um G-homomorfismo de M para N é um mapa $\alpha : M \to N$ tal que

(*i*) α é um homomorfismo de grupos abelianos:
$\alpha(m + m') = \alpha(m) + \alpha(m')$;

(*ii*) α é compatível com a ação de G em M e N:
$\alpha(gm) = g\alpha(m)$ para todo $g \in G$ e $m \in M$.

Denote por $\mathrm{Hom}_G(M, N)$ o conjunto de mapas $\alpha : M \to N$ de G-homomorfismos.

Definição 1.4. *: O anel de grupo $\mathbb{Z}[G]$ de G é um grupo abeliano livre cuja base são os elementos de G e sua operacão é determinada pela lei do grupo em G estendida distributivamente, isto é, os elementos de G comutam com os coeficientes em $\mathbb{Z}$. Então, os elementos de $\mathbb{Z}[G]$ são somas finitas*

$$\sum_{\sigma \in G} a_\sigma \sigma,\ a_\sigma \in \mathbb{Z}\ e\ \sigma \in G,$$

com produto dado por:

$$(\sum_{\sigma \in G} a_\sigma \sigma)(\sum_{\tau \in G} b_\tau \tau) = \sum_{\sigma,\tau} a_\sigma b_\tau (\sigma\tau)$$

Uma estrutura de G-módulos no grupo abeliano M estende de maneira única para a estrutura de $\mathbb{Z}[G]$-módulos.

Dado um G-módulo M, ele se torna um $\mathbb{Z}[G]$-módulo via:

$$(\sum n_\sigma \sigma) \cdot m = \sum n_\sigma (\sigma \cdot m).$$

Observe que um homomorfismo de grupos abelianos é um homomorfismo de G-módulos se, e somente se, é um homomorfismo de $\mathbb{Z}[G]$-módulos.

Portanto, a categoria dos G-módulos, Mod_G, pode ser identificada com a categoria de módulos sobre o anel $\mathbb{Z}[G]$.

Se M e N são G-módulos, então o conjunto $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ se torna um G-módulo com a estrutura:

(*i*) $(\varphi + \varphi')(m) = \varphi(m) + \varphi'(m)$.

(*ii*) $(\sigma\varphi)(m) = \sigma(\varphi(\sigma^{-1}m))$

Para verificar essa afirmação, tome $\varphi, \varphi' \in \mathrm{Hom}_G(M, N)$, $\sigma, \sigma_1, \sigma_2 \in G$ e $m \in M$,

(*i*) $(1_G \cdot \varphi) = \varphi$.
$(1_G \cdot \varphi)(m) = 1_G\varphi(1_G^{-1}m) = 1_G\varphi(m) = \varphi(m)$ para todo $m \in M$.

(*ii*) $((\sigma_1\sigma_2)\varphi) = \sigma_1(\sigma_2\varphi)$.
Observe que

$$((\sigma_1\sigma_2)\varphi)(m) = \sigma_1\sigma_2\varphi((\sigma_1\sigma_2)^{-1}m) = \sigma_1\sigma_2\varphi(\sigma_2^{-1}\sigma_1^{-1}m)$$

e por outro lado,

$$(\sigma_1(\sigma_2\varphi)(m)) = \sigma_1(\sigma_2\varphi)(\sigma_1^{-1}m) = \sigma_1\sigma_2\varphi(\sigma_2^{-1}(\sigma_1^{-1}m)).$$

Assim, $((\sigma_1\sigma_2)\varphi)(m) = \sigma_1(\sigma_2\varphi)(m)$ para todo $m \in M$.

(*iii*) $(\sigma(\varphi + \varphi')) = \sigma \cdot \varphi + \sigma \cdot \varphi'$.
Note que,

$$\begin{aligned}(\sigma(\varphi + \varphi'))(m) &= \sigma \cdot [(\varphi + \varphi')(\sigma^{-1}m)] \\ &= \sigma \cdot [\varphi(\sigma^{-1}m) + \varphi'(\sigma^{-1}m)]\end{aligned}$$

e sendo N um G-módulo,

$$\begin{aligned}\sigma \cdot [\varphi(\sigma^{-1}(m) + \varphi'(\sigma^{-1}m)] &= \sigma \cdot \varphi(\sigma^{-1}m) + \sigma \cdot \varphi'(\sigma^{-1}m) \\ &= (\sigma \cdot \varphi)(m) + (\sigma \cdot \varphi')(m) \\ &= (\sigma \cdot \varphi + \sigma \cdot \varphi')(m).\end{aligned}$$

Logo, $(\sigma \cdot (\varphi + \varphi'))(m) = (\sigma \cdot \varphi + \sigma \cdot \varphi')(m)$, $\forall m \in M$

1.3 Módulos Induzidos e Módulos Injetivos

Seja H um subgrupo do grupo G. Observe que se N é um G-módulo então N também é um H-módulo. Vamos ver que a partir de um H-módulo podemos construir um G-módulo.

Seja M um H-módulo. Defina,

$$\mathrm{Ind}_H^G(M) = \{\varphi : G \to M | \varphi(\tau\sigma) = \tau\varphi(\sigma), \forall \tau \in H\}.$$

O conjunto $\mathrm{Ind}_H^G(M)$ se torna um G-módulo via:

(*i*) $(\varphi + \varphi')(x) = \varphi(x) + \varphi'(x)$.

(*ii*) $(\sigma\varphi)(x) = \varphi(x\sigma)$.

Um homomorfismo $\alpha : M \to N$ de H-módulos, define um homomorfismo de G-módulos, através de:

$$\begin{aligned}\alpha_* : \mathrm{Ind}_H^G(M) &\to \mathrm{Ind}_H^G(N) \\ \varphi &\mapsto \alpha \circ \varphi\end{aligned}$$

Lema 1.2. *(Lema 1.2.2 de [13]).*

1. *Para todo G-módulo M e H-módulo N,*

$$\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \simeq \mathrm{Hom}_H(M, N).$$

Demonstração. Tome $\alpha : M \to \mathrm{Ind}_H^G(N)$ um homomorfismo de G-módulos. Defina $\beta : M \to N$ por $\beta(m) = \alpha(m)(1_G)$. Para todo $\sigma \in G$,

$$\beta(\sigma m) = (\alpha(\sigma m))(1_G) = (\sigma(\alpha(m)))(1_G) = \alpha(m)(1_G\sigma) = \alpha(m)(\sigma).$$

Por hipótese, $\alpha(m) \in \mathrm{Ind}_H^G$, se $\sigma \in H$ então,

$$\beta(\sigma m) = \alpha(m)(1_G\sigma) = \sigma(\alpha(m)(1_G)) = \sigma(\beta(m)).$$

Com isso, $\beta(\sigma m) = \sigma(\beta(m))$ e assim, $\beta : M \to N$ é um H-homomorfismo.

Agora, tome $\beta : M \to N$ um H-homomorfismo e defina $\alpha : M \to \mathrm{Ind}_H^G(N)$ tal que, $\alpha(m)(\sigma) = \beta(\sigma m)$. Para todo $\tau \in G$,

$$\sigma\alpha(m)(\tau) = \alpha(m)(\tau\sigma) = \beta((\tau\sigma)m) = \beta(\tau(\sigma m)) = \alpha(\sigma m)(\tau).$$

Logo, α é um G-homomorfismo.

Mostraremos que os mapas $\alpha \mapsto \beta$ e $\beta \mapsto \alpha$ que são mutuamente inversos.

(i) Considere o mapa composto $\beta \mapsto \alpha \mapsto \beta'$.
Como visto, dado $\beta : M \to N$ definimos $\alpha(m)(\sigma) = \beta(\sigma m)$.
A imagem de β' de α é dada por $\beta'(m) = \alpha(m)(1_G)$ para todo $m \in M$. Tomando $\sigma = 1_G$, obtemos $\beta(m) = \beta'(m)$, $\forall m \in M$.

(ii) Tome o mapa composto $\alpha \mapsto \beta \mapsto \alpha'$.
A imagem de α' de β é dada por $\alpha'(m)(\sigma) = \beta(\sigma m)$. Assim,

$$\alpha'(m)(\sigma) = \beta(\sigma m) = \alpha(\sigma m)(1_G) = \sigma\alpha(m)(1_G) = \alpha(m)(1_G\sigma) = \alpha(m)(\sigma)$$

e então, $\alpha = \alpha'$.
Com isso, $\mathrm{Hom}_G(M, \mathrm{Ind}_H^G(N)) \simeq \mathrm{Hom}_H(M, N)$.

□

2. *O funtor*

$$\mathrm{Ind}_H^G : \mathrm{Mod}_H \to \mathrm{Mod}_G$$

é exato.

Demonstração. Considere a sequência exata,

$$0 \to M \xrightarrow{\iota} N \xrightarrow{\pi} P \to 0$$

Devemos provar que a sequência,

$$0 \to \mathrm{Ind}_H^G(M) \xrightarrow{\iota_*} \mathrm{Ind}_H^G(N) \xrightarrow{\pi_*} \mathrm{Ind}_H^G(P) \to 0$$

é exata.

(*i*) $\mathrm{Ker}(\pi_*) \subseteq \mathrm{Im}(\iota_*)$.
Tome $\psi \in \mathrm{Ker}(\pi_*)$ e defina $\pi_*(\psi) = \pi \circ \psi \ \forall \psi \in \mathrm{Ind}_H^G(N)$. Dessa forma,

$$\pi_*(\psi)(\sigma) = \pi \circ \psi(\sigma) = \pi(\psi(\sigma)) = 0, \ \forall \sigma \in G.$$

Assim, $\psi(\sigma) \in \mathrm{Ker}(\pi) = \mathrm{Im}(\iota)$ e com isso, $\psi(\sigma) = \iota(m_\sigma)$ para um único $m_\sigma \in M$, pois ι é injetivo.
Observe que, $\psi \in \mathrm{Im}(\iota_*) \Leftrightarrow$ existe $\alpha \in \mathrm{Ind}_H^G(M)$ tal que $\iota_*(\alpha) = \psi$.
Considere o mapa $\alpha : G \to M$ tal que $\sigma \mapsto m_\sigma$. Esse mapa está bem definido pois cada elemento $\sigma \in G$ está associado a um único elemento $m_\sigma \in M$.
Mostraremos que $\alpha \in \mathrm{Ind}_H^G(M)$. Para isso, tome $\tau \in H$ e defina $\alpha(\tau\sigma) = m_{\tau\sigma}$ tal que

$$\iota(m_{\tau\sigma}) = \psi(\tau\sigma) = \tau\psi(\sigma) = \tau\iota(m_\sigma)) = \iota(\tau m_\sigma).$$

Sendo ι injetivo, $\tau m_\sigma = m_{\tau\sigma}$, e assim, $\tau\alpha(\sigma) = \alpha(\tau\sigma)$. Logo, $\alpha \in \mathrm{Ind}_H^G(M)$.
Considere o mapa $\iota_* : \mathrm{Ind}_H^G(M) \to \mathrm{Ind}_H^G(N)$ tal que $\alpha \mapsto \iota \circ \alpha$. Para todo $\sigma \in G$, temos:

$$\iota_*(\alpha)(\sigma) = \iota(\alpha(\sigma)) = \iota(m_\sigma) = \psi(\sigma), \ \forall \sigma \in G.$$

Portanto, $\psi \in \mathrm{Im}(\iota_*)$.

(*ii*) $\mathrm{Im}(\iota_*) \subseteq \mathrm{Ker}(\pi_*)$.
Temos, $\pi_* \circ \iota_*(\psi) = (\pi \circ \iota)_*(\psi) = 0$. Logo, $\iota_*(\psi) \in \mathrm{Ker}(\pi_*)$.

(*iii*) ι_* é injetivo.
Tome $\alpha \in \mathrm{Ker}(\iota_*)$, então $\iota(\alpha(\sigma)) = 0$ para todo $\sigma \in G$ e pela injetividade de ι, $\alpha(\sigma) = 0$ para todo $\sigma \in G$. Dessa maneira, $\alpha = 0$ e $\mathrm{Ker}(\iota_*) = \{0\}$.

(*iv*) π_* é sobrejetivo.
Seja S um conjunto de representantes das classes laterais à direita de H em G, isto é
$G = \cup_{\rho \in S} H\rho$, e $\varphi \in \mathrm{Ind}_H^G$ (P). Para cada $\rho \in$ S escolha um $n(\rho) \in N$ tal que $\pi((n(\rho)) = \varphi(\rho)$.
Defina o mapa $\psi : G \to N$ por $\psi(\tau\rho) = \tau \cdot n(\rho)$, onde $\tau \in H$, então

$$\tau\psi(1_H\rho) = \tau 1_H n(\rho) = \psi(\tau\rho). \tag{1.4}$$

E assim, $\psi \in \mathrm{Ind}_H^G(N)$ e

$$\pi_*(\psi)(\tau\rho) = \pi(\psi(\tau\rho)) = \pi(\tau n(\rho)) = \tau\pi(n(\rho)) = \tau\varphi(\rho) = \varphi(\tau\rho).$$

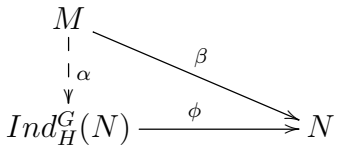
Logo, π_* é sobrejetivo.

Concluimos que o funtor $\mathrm{Ind}_H^G : \mathrm{Mod}_H \to \mathrm{Mod}_G$ é exato.

□

Seja $\Psi : \mathrm{Ind}_H^G(N) \to N$ em que $\varphi \mapsto \varphi(1_G)$ é um homomorfimo de H-módulos, e pelo Lema 1.2 $(\mathrm{Ind}_H^G(N), \varphi)$ tem seguinte propriedade universal:

Para todo H-homomorfismo $\beta : M \to N$ de um G-módulos, existe um único G-homomorfismo $\alpha : M \to \mathrm{Ind}_H^G(N)$ tal que $\Psi \circ \alpha = \beta$.



Quando $H = \{1\}$, um H-módulo é apenas um grupo abeliano e temos:

$$\begin{aligned} \mathrm{Ind}^G(M_0) &= \{\varphi : G \to M_0\} \\ &= \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}[G], M_0) \end{aligned}$$

Um G-módulo é induzido se é isomorfo a $\mathrm{Ind}^G(M_0)$, para algum grupo abeliano M_0.

Definição 1.5. *Um R-módulo P é chamado de injetivo se satisfaz quaisquer das condições de equivalência da Proposição 1.4.*

Proposição 1.5. *(Proposição 1.5.2 de [13]). A categoria Mod_G tem G-módulos injetivos suficientes, isto é, todo G-módulo M pode ser incluso em um G-módulo injetivo I, $M \hookrightarrow I$.*

Demonstração. Seja M um G-módulo. M_0 é M visto como um grupo abeliano. É sempre possível incluir M_0 em um injetivo I, $M_0 \hookrightarrow I$. Então, $\mathrm{Ind}^G(M_0) \hookrightarrow \mathrm{Ind}^G(I)$ de G-módulos. Agora, verifica-se que existe uma inclusão canônica de $M \hookrightarrow \mathrm{Ind}^G(M_0)$ de G-módulos, pois

$$\begin{aligned} M &\hookrightarrow \mathrm{Ind}^G(M_0) \\ m &\mapsto \varphi_m : \sigma \mapsto \sigma m \end{aligned}$$

Com isso, $M \hookrightarrow \mathrm{Ind}^G(M_0) \hookrightarrow \mathrm{Ind}^G(I)$.

Pelo Lema **??**, $\mathrm{Hom}_G(M, \mathrm{Ind}^G(I)) \simeq \mathrm{Hom}_{\mathbb{Z}}(M_0, I)$. Como $\mathrm{Hom}_{\mathbb{Z}}(M_0, I)$ é exato, $\mathrm{Hom}_G(-, \mathrm{Ind}^G(I))$ também será um funtor exato. Logo, $\mathrm{Ind}^G(I)$ é injetivo. □

Capítulo 2

Grupos de Cohomologia e Homologia

2.1 Grupos de Cohomologia

Trataremos aqui de um grupo muito importante para esse trabalho, os Grupos de Cohomologia. Para construir esse Grupo de Cohomologia considere G um grupo e começaremos com a definição do conjunto M^G. Mostraremos que o funtor $(-)^G$ é exato. Depois disso, definiremos um complexo de cocadeia e através de um complexo de cocadeia de uma resolução injetiva, teremos os Grupos de Cohomologia. Em seguida, daremos algumas propriedades desses grupos.

Seja M um G-módulo e defina

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

Vimos que, se M e N são G-módulos, então o conjunto $\mathrm{Hom}_{\mathbb{Z}}(M, N)$ se torna um G-módulo com a estrutrura:

(i) $(\varphi + \varphi')(m) = \varphi(m) + \varphi'(m)$.

(ii) $(\sigma\varphi)(m) = \sigma(\varphi(\sigma^{-1}m))$.

Note que segue de imediato dessa estrutura de G-módulo que

$$(\mathrm{Hom}_{\mathbb{Z}}(M, N))^G = \mathrm{Hom}_G(M, N).$$

O funtor,

$$\begin{array}{rcl} \mathrm{Mod}_G & \to & \mathrm{Mod}_{\mathbb{Z}} \\ M & \mapsto & M^G \end{array}$$

é exato à esquerda, isto é, se a sequência

$$0 \to A \to B \to C \to 0$$

é exata, então

$$0 \to A^G \to B^G \to C^G$$

será uma sequência exata.

Para isso, basta mostrar que há um isomorfismo natural $A^G \simeq \mathrm{Hom}_G(\mathbb{Z}, A)$, pois $\mathrm{Hom}_G(\mathbb{Z}, -)$ é um funtor exato à esquerda.

Considere o mapa $\mathrm{Hom}_G(\mathbb{Z}, A) \to A^G$, tal que $\alpha_a(1) = a$. Temos,

$$\sigma a = \sigma\alpha_a(1) = \alpha_a(\sigma \cdot 1) = \alpha_a(1) = a,$$

para todo $\sigma \in G$. Então, $a \in A^G$ e o mapa está bem definido.

Agora, tome o mapa $A^G \to \mathrm{Hom}_G(\mathbb{Z}, A)$ onde $a \mapsto \psi$ e defina $\psi(1) = a$. Com isso, $\psi(\sigma n) = \psi(n) = \psi(1 \cdot n) = n\psi(1) = na$ para todo $\sigma \in G$ e para todo $n \in \mathbb{Z}$. E por outro lado, $\sigma\psi(n) = \sigma(na) = \sigma(a + a + \cdots + a) = \sigma a + \sigma a + \cdots + \sigma a = na$. Logo, $\psi(\sigma n) = \sigma\psi(n)$ e o mapa está bem definido.

Mostraremos que esse mapas são mutuamente inversos.

(*i*) $\mathrm{Hom}_G(\mathbb{Z}, A) \to A^G \to \mathrm{Hom}_G(\mathbb{Z}, A)$.
$\alpha_a \mapsto a \mapsto \psi$ tal que $\psi(1) = a$. Por definição, $\alpha_a(1) = a$, então $\alpha_a = \psi$.

(*ii*) $A^G \mapsto \mathrm{Hom}_G(\mathbb{Z}, A) \mapsto A^G$.
$a \mapsto \psi \mapsto \psi(1)$ tal que $\psi(1) = a$.

Portanto, $\mathrm{Hom}_G(\mathbb{Z}, A) \simeq A^G$. Isso pode ser visto ainda mais facilmente que:

$$\mathrm{Hom}_G(\mathbb{Z}, A) = (\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A))^G \cong A^G.$$

Definição 2.1. *Seja $\mathcal{C}$ uma sequência de R-módulos*

$$0 \to C^0 \xrightarrow{d_1} C^1 \to \cdots \to C^{n-1} \xrightarrow{d_n} C^n \xrightarrow{d_{n+1}} \cdots$$

A sequência $\mathcal{C}$ é chamada complexo de cocadeia se $d_{n+1} \circ d_n = 0$ para todo n.

Definição 2.2. *Seja $\mathcal{A} = A^n$ e $\mathcal{B} = B^n$ complexos de cocadeias. Um homomorfismo de complexos $\alpha : \mathcal{A} \to \mathcal{B}$ é o conjunto de homomorfismos $\alpha_n : A^n \to B^n$ tal que para todo n o diagrama comuta:*

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & A^{n-1} & \xrightarrow{d_n} & A^n & \xrightarrow{d_{n+1}} & A^{n+1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle \alpha_{n-1}} & \circlearrowleft & \downarrow{\scriptstyle \alpha_n} & \circlearrowleft & \downarrow{\scriptstyle \alpha_{n+1}} & & \\
\cdots & \longrightarrow & B^{n-1} & \xrightarrow{d_n} & B^n & \xrightarrow{d_{n+1}} & B^{n+1} & \longrightarrow & \cdots
\end{array}$$

Seja M um G-módulo e escolha uma resolução injetiva

$$0 \to M \to I^0 \xrightarrow{d^0} I^1 \xrightarrow{d^1} I^2 \xrightarrow{d^2} \cdots$$

de M. O complexo de cocadeia

$$0 \xrightarrow{d^{-1}} (I^0)^G \xrightarrow{d^0} (I^1)^G \to \cdots \xrightarrow{d^{r-1}} (I^r)^G \xrightarrow{d^r} (I^{r+1})^G \to \cdots$$

não precisa ser uma sequência exata longa, e um r-ésimo grupo de cohomologia de G com coeficientes em M é definido por

$$\mathrm{H}^r(G, M) = \frac{\mathrm{Ker}(d^r)}{\mathrm{Im}(d^{r-1})}$$

Esse grupo tem as seguintes propriedades:

(*i*) $\mathrm{H}^0(G, M) = M^G$.

Tome a sequência exata

$$0 \to M^G \xrightarrow{\varepsilon} (I^0)^G \xrightarrow{d^0} (I^1)^G.$$

Com isso, $\mathrm{H}^0(G, M) = \frac{\mathrm{Ker}(d^0)}{\mathrm{Im}(d^{-1})} = \mathrm{Ker}(d^0) = \mathrm{Im}(\varepsilon) = M^G$.

(*ii*) Se I é um G-módulo injetivo, entao $\mathrm{H}^r(G, I) = 0$ para todo $r > 0$.

Basta notar que,

$$0 \to I \to I \to 0 \cdots$$

é uma resolusão injetiva de I.

(*iii*) Uma sequência exata

$$0 \to M' \to M \to M'' \to 0$$

de G-módulos dá origem a uma sequência exata longa,

$$0 \to \mathrm{H}^0(G, M') \to \cdots \to \mathrm{H}^r(G, M) \to \mathrm{H}^r(G, M'') \xrightarrow{\delta^r} \mathrm{H}^{r+1}(G, M') \to \cdots$$

Essa é a sequência de cohomologia.

(*iv*) Sejam $M \to I^\bullet$ e $N \to J^\bullet$ resoluções injetivas de dois G-módulos M e N. Um homomorfismo de G-módulos $\alpha : M \to N$ levanta para um mapa de complexo

$$\begin{array}{ccc} M & \longrightarrow & I^\bullet \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \alpha^\bullet} \\ N & \longrightarrow & J^\bullet \end{array}$$

e os homomorfismos,

$$H^r(\alpha^\bullet) : H^r(I^\bullet) \to H^r(J^\bullet)$$

não dependem da escolha de $\alpha^\bullet$. Assim, dado α temos que $M \mapsto \mathrm{H}^r(G, M)$ é um funtor da categoria dos G-módulos para a categoria de grupos abelianos.

Proposição 2.1. *(Lema do Shapiro)(Proposição 1.11.2 de [13]). Seja H é um subgrupo de G. Para todo H-módulo N, existe um isomorfismo canônico*

$$H^r(G, \mathrm{Ind}_H^G(N)) \simeq H^r(H, N)$$

para todo $r \geq 0$.

Demonstração. Considere os seguintes casos:

(*i*) $r = 0$ Como visto, $N^H \simeq \mathrm{Hom}_H(\mathbb{Z}, N)$ e assim,

$$H^0(H, N) = N^H \simeq \mathrm{Hom}_H(\mathbb{Z}, N) \simeq \mathrm{Hom}_G(\mathbb{Z}, \mathrm{Ind}_H^G(N)) \simeq (\mathrm{Ind}_H^G(N))^G = H^0(G, \mathrm{Ind}_H^G(N)).$$

.

(*ii*) $r > 0$ Escolha uma resolução injetiva $N \to I^\bullet$ de N. Aplicando o funtor exato Ind_H^G, obtemos a seguinte resolução injetiva:

$$\mathrm{Ind}_H^G(N) \to \mathrm{Ind}_H^G(I^\bullet).$$

Pelo resultudo acima, $(\mathrm{Ind}_H^G(I))^G \simeq I^H$ e dessa forma,

$$H^r(G, \mathrm{Ind}_H^G(N)) = H^r((\mathrm{Ind}_H^G(I))^G) \simeq H^r(I^H) = H^r(H, N).$$

□

Corolário 2. *Se M é um G-módulo induzido, então $H^r(G, M) = 0$ para $r > 0$.*

Demonstração. Se $M = \mathrm{Ind}^G(M_0)$, então pelo Lema do Shapiro

$$H^r(G, M) \simeq H^r(\{1\}, M_0) = 0 \text{ para todo } r > 0.$$

□

Seja

$$0 \to M \to J \to N \to 0$$

uma sequência exata de G-módulos. Então, essa sequência dá origem a sequência exata de cohomologia

$$0 \to H^0(G, M) \to H^0(G, J) \to H^0(G, N) \to H^1(G, M) \to H^1(G, J) \to \cdots.$$

Se $H^r(G, J) = 0$ para todo $r > 0$, então

$$0 \to H^0(G, M) \to H^0(G, J) \to H^0(G, N) \xrightarrow{\delta} H^1(G, M) \to 0$$

é uma sequência exata e além disso, temos a coleção de isomorfismos

$$H^r(G, N) \simeq H^{r+1}(G, M).$$

Exemplo 1. *Seja M um G-módulo e defina M_* como o módulo induzido $\mathrm{Ind}_H^G(M_0)$ onde M_0 é M visto como um grupo abeliano. Como visto na demonstração da Proposição 1.5, existe uma inclusão canônica $M \hookrightarrow \mathrm{Ind}^G(M_0)$ de G-módulos tal que $g \mapsto gm, m \in M$. Seja $M_\dagger = M_*/M$. Assim, a sequência*

$$0 \to M \to M_* \to M_\dagger \to 0$$

é exata e sendo $H^r(G, M_*) = 0$ para $r > 0$, então

$$H^r(G, M_\dagger) \simeq H^{r+1}(G, M), \text{ para } r \geq 1.$$

De maneira geral, uma sequência exata

$$0 \to M \xrightarrow{\alpha} J^1 \xrightarrow{\beta} J^2 \to \cdots \to J^s \to N \to 0 \tag{2.1}$$

tal que $H^r(G, J^i) = 0$ para todo $r, i > 0$, define isomorfimos

$$H^r(G, N) \simeq H^{r+s}(G, M) \text{ para todo } r \geq 1.$$

Para provar esse resultado fragmentaremos a sequência acima em sequências menores e mostraremos que são sequências exatas curtas. Primeiramente, considere a sequência

$$0 \to M \xrightarrow{\alpha} J^1 \xrightarrow{\overline{\alpha}} N^1 \to 0$$

onde $N^1 = J^1/\alpha(M)$. Claramente, $\overline{\alpha}$ é um mapa sobrejetivo. Basta mostrar que $\mathrm{Ker}(\overline{\alpha}) = \mathrm{Im}(\alpha)$. Para isso, tome $\overline{a} \in \mathrm{Ker}(\overline{\alpha})$, então $\overline{a} \in \alpha(M) = \mathrm{Im}(\alpha)$. E por outro lado, tome $b \in \mathrm{Im}(\alpha) = \alpha(M)$ e assim, $b \in \mathrm{Ker}(\overline{\alpha})$.

Agora, considere a sequência

$$0 \to N^1 \xrightarrow{\iota} J^2 \xrightarrow{\pi} N^2 \to 0$$

onde $N^2 = J^2/\iota(J^2)$. Verificaremos que o mapa ι está bem definido.

Considere o mapa induzido por β

$$\begin{aligned} \iota : J^1/\alpha(M) &\to J^2 \\ \overline{j_1} &\mapsto \beta(\overline{j_1}). \end{aligned}$$

Sendo a sequência 2.1 exata, esse mapa está bem definido, pois $\beta(\overline{j_1}) = \beta(j_1 + \alpha(M)) = \beta(j_1)$. Logo, o seguinte diagrama

$$\begin{array}{ccc} J^1 & \xrightarrow{\beta} & J^2 \\ & \searrow^{\overline{\alpha}} & \uparrow{\scriptstyle \iota} \\ & & J^1/\alpha(M) \end{array}$$

comuta. E além disso, esse mapa, ι, é injetivo, pois ao tomar $\beta(\overline{j_1}) = \beta(j_1) = 0$ temos que $j_1 \in \mathrm{Ker}(\beta) = \mathrm{Im}(\alpha)$. Assim, $j_1 = \alpha(m_1) \in \alpha(M)$ e com isso, $\overline{j_1} = \overline{0}$.

Agora, defina $N^2 = J^2/\iota(J^2)$. Assim, o mapa π é, evidentemente, sobrejetivo.

Falta mostrar que $\mathrm{Ker}(\pi) = \mathrm{Im}(\iota)$. Para isso, basta notar que $j' \in \mathrm{Ker}(\pi) \Leftrightarrow j' \in \mathrm{Im}(\iota)$.

Logo, a sequência 2.1 pode ser fragmentada em sequência menores

$$\begin{gathered} 0 \to M \to J^1 \to N^1 \to 0 \\ 0 \to N^1 \to J^2 \to N^2 \to 0 \\ \cdots \\ 0 \to N^{s-1} \to J^s \to N \to 0 \end{gathered}$$

e de modo análogo, essas sequências são construídas e verifica-se que são sequências exatas curtas.

Com isso, temos os isomorfismos

$$H^r(G, N) \simeq H^{r+1}(G, N^{s-1}) \simeq H^{r+2}(G, N^{s-2}) \simeq \cdots \simeq H^{r+s}(G, M).$$

2.2 Descrição de Grupos de Comologia através de Cocadeias

Nesta seção daremos as definições básicas de uma r-cocadeias homogêneas. E através dessas cocadeias homogênias, definiremos as r-cocadeias não homogêneas e com isso podemos dar uma outra definição para os Grupos de Cohomologia.

Como visto, $\mathrm{Hom}_{\mathbb{Z}}(M,N)$ torna-se um G-módulo via

$$(\sigma\varphi)(m) := \sigma(\varphi(\sigma^{-1}(m))),\ \forall\sigma \in G.$$

Seja P_r, $r \geq 0$ um $\mathbb{Z}$-módulo livre com base $(\sigma_0, \sigma_1, \cdots, \sigma_r)$ de elementos de G dotados da ação de G tal que

$$(\sigma\sigma_0, \sigma\sigma_1, \cdots, \sigma\sigma_r) = \sigma(\sigma_0, \sigma_1, \cdots, \sigma_r),\ \forall\sigma \in G.$$

E também, P_r é visto como um $\mathbb{Z}[G]$-módulo, com base $\{(1, \sigma_1, \sigma_2, \cdots, \sigma_r)|\sigma_i \in G\}$.
Defina um homomorfismo $d_r : P_r \to P_{r-1}$ por

$$d_r(\sigma_0, \cdots, \sigma_r) = \Sigma_{i=0}(-1)^i(\sigma_0, \cdots, \hat{\sigma_i}, \cdots, \sigma_r)$$

Lema 2.1. *(Lema 1.15.2 de [13]). O complexo $P_\bullet \xrightarrow{\varepsilon} \mathbb{Z} \to 0$ é exato.*

Demonstração. Tome $\sigma \in G$ e defina $k_r : P_r \to P_{r+1}$ por

$$k_r(\sigma_0, \sigma_1, \cdots, \sigma_r) = (\sigma, \sigma_0, \sigma_1, \cdots, \sigma_r).$$

Com isso, temos:

$$P_r \xrightarrow{k_r} P_{r+1} \xrightarrow{d_{r+1}} P_r$$
$$P_r \xrightarrow{d_r} P_{r-1} \xrightarrow{k_{r-1}} P_r$$

e verifica-se que $d_{r+1} \circ k_r + k_{r-1} \circ d_r = 1$.
Sendo $P_\bullet$ um complexo $d_{r-1} \circ d_r = 0$, então $\mathrm{Im}(d_{r+1}) \subset \mathrm{Ker}(d_r)$.
Agora, suponha que $d_r(P) = 0$ para algum $P \in P_r$, então

$$(d_{r+1} \circ k_r)(P) + (k_{r-1} \circ d_r)(P) = (d_{r+1} \circ k_r)(P) = P.$$

Com isso, $P \in \mathrm{Im}(d_{r+1})$.
Portanto, $\mathrm{Ker}(d_r) = \mathrm{Im}(d_{r+1})$ e o complexo é exato. □

Proposição 2.2. *(Proposição 1.16.2 de [13]). Para todo M G-módulo*

$$H^r(G, M) \simeq H^r(\mathrm{Hom}_G(P_\bullet, M)).$$

Sendo $P_r = \mathbb{Z}[G^{r+1}]$, podemos identificar um elemento de $\mathrm{Hom}_G(P_r, M)$ através do mapa $\phi : G^{r+1} \to M$, e ϕ é fixado por G se, e somente se,

$$\phi(\sigma\sigma_0, \cdots, \sigma\sigma_r) = \sigma(\phi(\sigma_0, \cdots, \sigma_r)), \text{ para todo } \sigma, \sigma_0, \cdots, \sigma_r \in G.$$

O conjunto dos ϕ's que satisfazem essas condições será definido por $C^r(G, M)$, e os $\phi'$$s$ serão chamados de r-homomorfismos de cocadeias de G com valores em M.
O mapa $d^r : C^r(G, M) \to C^{r+1}(G, M)$ induzido por d_r é

$$(d^r\phi)(\sigma_0,\cdots,\sigma_{r+1}) = \Sigma(-1)^i\phi(\sigma_0,\cdots,\hat{\sigma}_i,\cdots,\sigma_{r+1}).$$

Pela Proposição 2.2 temos que

$$H^r(\mathrm{Hom}_G(P_\bullet, M)) \simeq H^r(G,M) \simeq \frac{\mathrm{Ker}(d^r)}{\mathrm{Im}(d^{r-1})}.$$

Uma cocadeia homogênia $\phi : G^{r+1} \to M$ é determinada pelos elementos// $(1, \sigma_1, \sigma_1\sigma_2, \cdots, \sigma_1\sigma_2\cdots\sigma_{r+1})$

Agora, definiremos o grupo $C^r(G,M)$ das r-cocadeias não homogêneas de G com valores em M.

Seja $\varphi : G^r \to M$, onde $G^0 = \{1\}$ e $C^0(G,M) = M$, e defina

$$\varphi(\sigma_1,\cdots,\sigma_i) = \phi(1,\sigma_1,\sigma_1\sigma_2,\cdots,\sigma_1\cdots\sigma_i).$$

Em termos das cocadeias não-homogêneas, ficamos com:

$$d^r : C^r(G,M) \to C^{r+1}(G,M),$$

dado por $(d^r\varphi)(\sigma_1,\cdots,\sigma_{r+1}) =$

$$\sigma_1\varphi(\sigma_2,\cdots,\sigma_{r+1}) + \Sigma_{j=1}(-1)^j\varphi(\sigma_1,\cdots,\sigma_j\sigma_{j+1},\cdots,\sigma_{r+1}) + (-1)^{r+1}\varphi(\sigma_1,\cdots,\sigma_r).$$

Defina

$$Z^r(G,M) = \mathrm{Ker}(d^r) \quad (\textit{grupo de r-cociclos})$$

e

$$B^r(G,M) = \mathrm{Im}(d^{r-1}) \quad (\textit{grupo de r-cofronteiras}).$$

Proposição 2.3. *(Lema 1.17.2 de [13]). A sequência de mapas*

$$C^0(G,M) \overset{d^0}{\to} C^1(G,M) \overset{d^1}{\to} \cdots \overset{d^{r-1}}{\to} C^r(G,M) \overset{d^r}{\to} C^{r+1}(G,M) \to \cdots$$

é um complexo, e existe um isomorfismo canônico

$$H^r(G,M) \simeq \frac{Z^r(G,M)}{B^r(G,M)}$$

Exemplo 2. *O mapa $\varphi : G \to M$ é um homomorfismo cruzado se*

$$\varphi(\sigma\tau) = \sigma\varphi(\tau) + \varphi(\sigma),\ \forall\sigma,\tau \in G.$$

Para o elemento 1_G, identidade de G, temos

$$\varphi(1_G) = \varphi(1_G\ 1_G) = \varphi(1_G) + \varphi(1_G)$$

e assim, $\varphi(1_G) = 0$.

Para todo $m \in M$, o mapa $\sigma \mapsto \sigma m - m$ é um homomorfismo cruzado, pois

$$\varphi(\sigma\tau) = \sigma\tau m - m$$

e, por outro lado,

$$\sigma\varphi(\tau) + \varphi(\sigma) = \sigma(\tau m - m) + \sigma m - m = \sigma\tau m - m.$$

Esse mapa, $\sigma \mapsto \sigma m - m$, é chamado de homomorfismo cruzado principal.
Analisaremos o grupo de Cohomologia para $r = 1$.
Tome $\sigma_1, \sigma_2 \in G$, então

$$(d^1\varphi)(\sigma_1, \sigma_2) = \sigma_1\varphi(\sigma_2) - \varphi(\sigma_1\sigma_2) + \varphi(\sigma_1)$$

e,

$$\begin{aligned} \mathrm{Ker}(d^1\varphi) &= \{\sigma_1, \sigma_2 \in G | \sigma_1\varphi(\sigma_2) - \varphi(\sigma_1\sigma_2) + \varphi(\sigma_1) = 0\} \\ &= \{\sigma_1, \sigma_2 \in G | \varphi(\sigma_1\sigma_2) = \sigma_1\varphi(\sigma_2) + \varphi(\sigma_1)\}. \end{aligned}$$

Com isso, $\mathrm{Ker}(d^1\varphi)$ *é um homomorfismo cruzado.*

Observe que a $\mathrm{Im}(d^0) \in C^1(G, M)$ *e tome* $\varphi \in \mathrm{Im}(d^0)$ *tal que*

$$\begin{aligned} \varphi : G &\to M \\ \sigma &\mapsto \sigma m - m. \end{aligned}$$

Este mapa está bem definido, pois M é um G-módulo. Assim, $\mathrm{Im}(d^0)$ *é um homomorfismo cruzado principal.*
Portanto,

$$H^1(G, M) = \frac{\{homomorfismos \quad cruzados \quad G \to M\}}{\{homomorfismos \quad cruzados \quad principais\}}.$$

Se a ação G em M é trivial, então o homomorfismo cruzado é um homomorfismo. E sendo $\varphi(1_G) = 0$, temos

$$(d^0\varphi)(g_1) = g_1\varphi(1) - \varphi(1) = 0, \forall g_1 \in G.$$

Neste caso o homomorfismo cruzado principal é nulo, e então

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

Exemplo 3. *Seja M um grupo abeliano. Uma extensão de G por M é uma sequência exata.*

$$1 \to M \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$$

Sendo $\mathrm{Ker}(\pi) = \mathrm{Im}(\iota) = M$ *então $M \trianglelefteq E$.*

Uma seção, s, é um mapa, não necessariamente um homomorfismo, tal que $s : G \to E$ e $\pi(s(\sigma)) = \sigma$, $\forall \sigma \in G$.

Considere as seções s_1 e s_2 tal que $\pi(s_1(\sigma)) = \pi(s_2(\sigma)) = \sigma$, $\forall \sigma \in G$. Mostraremos que s_1 e s_2 diferem por um elemento $m \in M$. Observe que

$$\begin{aligned} \pi(s_1(\sigma))(\pi(s_2(\sigma))^{-1} &= \pi(s_1(\sigma))\pi(s_2(\sigma)^{-1}) \\ &= \pi(s_1(\sigma)s_2(\sigma)^{-1}) \\ &= 1. \end{aligned}$$

Como a sequência é exata, $s_1(\sigma)s_2(\sigma)^{-1} \in Ker(\pi) = Im(\iota) = M$. *Logo, existe* $m \in M$ *tal que*

$$\begin{aligned} s_1(\sigma)s_2(\sigma)^{-1} &= m \\ s_1(\sigma) &= ms_2(\sigma). \end{aligned}$$

Defina

$$\sigma m := s(\sigma)ms(\sigma)^{-1}, \quad \forall \sigma \in G \text{ e } m \in M$$

para alguma seção s. *Sendo* $M \trianglelefteq E$, *então* $s(\sigma)ms(\sigma)^{-1} \in M$. *Verificaremos que* σm *não depende da escolha da seção* s. *Para mostrar essa independência, tome duas seções* s_1 *e* s_2. *Existe* $m' \in M$ *tal que* $s_1(\sigma) = m's_2(\sigma)\ \forall \sigma \in G$. *Com isso,*

$$\begin{aligned} \sigma m &= s_1(\sigma)ms_1(\sigma)^{-1} \\ &= m's_2(\sigma)m(m's_2(\sigma))^{-1} \\ &= m's_2(\sigma)ms_2^{-1}(\sigma)m'^{-1}. \end{aligned}$$

Como $s_2(\sigma)ms_2^{-1}(\sigma) \in M$ *e* M *é abeliano,*

$$\sigma m = s_2(\sigma)ms_2^{-1}.$$

Portanto, σm *não depende da escolha da seção* s.

Dado uma seção s, σm *define uma ação de* G *em* M, *pois*

(*i*) *Tomando* $\sigma = 1_G$, $1_G \cdot m = m$;

(*ii*) *Sendo* $\sigma = \pi(s(\sigma))$ *e* $\tau = \pi(t(\tau))$. *Mostraremos que* $\sigma(\tau m) = (\sigma\tau)m$.

Dada uma seção t, $t(\tau) \cdot m \cdot t(\tau)^{-1} \in M$ *e com isso,*

$$\begin{aligned} \sigma(\tau m) &= \sigma(t(\tau) \cdot m \cdot t(\tau)^{-1}) \\ &= s(\sigma)(t(\tau) \cdot m \cdot t(\tau)^{-1})s(\sigma)^{-1}. \end{aligned}$$

Como não depende da escolha da seção, tome $t = s$. *Assim,*

$$\begin{aligned} \sigma(\tau(m)) &= s(\sigma)(s(\tau)ms(\tau)^{-1})s(\sigma)^{-1} \\ &= s(\sigma)s(\tau)ms(\tau)^{-1}s(\sigma)^{-1} \\ &= s(\sigma)s(\tau)m(s(\sigma)s(\tau))^{-1} \end{aligned} \tag{2.2}$$

e por sua vez,

$$(\sigma\tau)m = s(\sigma\tau)ms(\sigma\tau)^{-1}.$$

Observe que $\pi(s(\sigma\tau)) = \sigma\tau$ *e por outro lado,* $\pi(s(\sigma)s(\tau)) = \pi(s(\sigma))\pi(s(\tau)) = \sigma\tau$. *Logo,* $\pi(s(\sigma\tau) = \pi(s(\sigma)s(\tau))$ *e por isso, existe* $m_1 \in M$ *tal que* $s(\sigma\tau) = m_1s(\sigma)s(\tau)$. *Dessa maneira,*

$$\begin{aligned} (\sigma\tau)m &= s(\sigma\tau)ms(\sigma\tau)^{-1} \\ &= m_1s(\sigma)s(\tau)m[m_1s(\sigma)s(\tau)]^{-1} \\ &= m_1s(\sigma)s(\tau)ms(\tau)^{-1}s(\sigma)^{-1}m_1^{-1}. \end{aligned}$$

Como $s(\sigma)s(\tau)ms(\tau)^{-1}s(\sigma)^{-1} \in M$, *temos*

$$(\sigma\tau)m = s(\sigma)s(\tau)ms(\tau)^{-1}s(\sigma)^{-1}.$$

Portanto, $(\sigma\tau)m = \sigma(\tau m)$.

Tome $\varphi(\sigma,\tau) \in M$ *tal que* $s(\sigma)s(\tau) = \varphi(\sigma,\tau)s(\sigma\tau)$. *Mostraremos que* $\varphi \in \mathbb{Z}^2(G,M)$. *Pela associatividade em* E *e por* $s(\sigma)s(\tau) = \varphi(\sigma,\tau)s(\sigma\tau)$, *temos*

$$\begin{aligned}
s(\sigma)(s(\tau)s(\rho)) &= (s(\sigma)s(\tau))s(\rho)\\
s(\sigma)\varphi(\tau,\rho)s(\tau\rho) &= \varphi(\sigma,\tau)s(\sigma\tau)s(\rho)\\
\sigma\varphi(\tau,\rho)s(\sigma)s(\tau\rho) &= \varphi(\sigma,\tau)s(\sigma\tau)s(\rho)\\
\sigma\varphi(\tau,\rho)\varphi(\sigma,\tau\rho)s(\sigma\tau\rho) &= \varphi(\sigma,\tau)\varphi(\sigma\tau,\rho)s(\sigma\tau\rho)\\
\sigma\varphi(\tau,\rho)\varphi(\sigma,\tau\rho) &= \varphi(\sigma,\tau)\varphi(\sigma\tau,\rho).
\end{aligned}$$

Assim, na forma multiplicatica temos

$$\sigma\varphi(\tau,\rho)\varphi(\sigma,\tau\rho)\varphi(\sigma,\tau)^{-1}\varphi(\sigma\tau,\rho)^{-1} = 1$$

e aditivamente,

$$\sigma\varphi(\tau,\rho) - \varphi(\sigma\tau,\rho) + \varphi(\sigma,\tau\rho) - \varphi(\sigma,\tau) = 0.$$

Logo, $\varphi \in \mathbb{Z}^2(G,M)$, *onde* $\varphi : G \times G \to M$.

Dada duas seções s_1 *e* s_2 *tal que* $\pi(s_1(\sigma)) = \pi(s_2(\sigma)) = \sigma$, *existe* $f(\sigma) \in M$ *e,* $s_1(\sigma) = f(\sigma)s_2(\sigma)$. *Neste caso, também podemos de duas formas que* $f \in B^2(G,M)$. *Da forma multiplicativa,*

$$\begin{aligned}
s_1(\sigma)s_1(\tau) &= \varphi'(\sigma,\tau)s_1(\sigma\tau)\\
f(\sigma)s_2(\sigma)f(\tau)s_2(\tau) &= \varphi'(\sigma,\tau)f(\sigma\tau)s_2(\sigma\tau)\\
f(\sigma)\sigma f(\tau)s_2(\sigma)s_2(\tau) &= \varphi'(\sigma,\tau)f(\sigma\tau)s_2(\sigma\tau)\\
f(\sigma)\sigma f(\tau)\varphi(\sigma,\tau)s(\sigma\tau) &= \varphi'(\sigma,\tau)f(\sigma\tau)s(\sigma\tau)\\
f(\sigma)\sigma f(\tau)\varphi(\sigma,\tau) &= \varphi'(\sigma,\tau)f(\sigma\tau)
\end{aligned}$$

e aditivamente,

$$\varphi'(\sigma,\tau) - \varphi(\sigma,\tau) = f(\sigma) + \sigma f(\tau) - f(\sigma\tau).$$

Logo, $f(\sigma,\tau) = f(\sigma) + \sigma f(\tau) - f(\sigma\tau) \in \mathrm{B}^2(G,M)$.

Exemplo 4. *Seja* $\varphi : G \to M$ *um homomorfismo cruzado,*

$$\varphi(\sigma\tau) = \sigma\varphi(\tau) + \varphi(\sigma), \forall\sigma,\tau \in G$$

Tomando $\tau = \sigma$, $\varphi(\sigma^2) = \sigma\varphi(\sigma) + \varphi(\sigma)$ *temos,*

$$\begin{aligned}
\varphi(\sigma\sigma^2) &= \sigma\varphi(\sigma^2) + \varphi(\sigma)\\
&= \sigma[\sigma\varphi(\sigma) + \varphi(\sigma)] + \varphi(\sigma)\\
&= \sigma^2\varphi(\sigma) + \sigma\varphi(\sigma) + \varphi(\sigma).
\end{aligned}$$

e para qualquer $n \geq 1$,

$$\varphi(\sigma^n) = \sigma^{n-1}\varphi(\sigma) + \sigma^{n-2}\varphi(\sigma) + \cdots + \sigma\varphi(\sigma) + \varphi(\sigma).$$

Suponha que G *seja um grupo finito e cíclico de ordem* n *gerado por* σ, *então* $\sigma^n = 1$ *e*

$$0 = \varphi(1_G) = \varphi(\sigma^n) = \sigma^{n-1}\varphi(\sigma) + \sigma^{n-2}\varphi(\sigma) + \cdots + \sigma\varphi(\sigma) + \varphi(\sigma).$$

Com isso, o homomorfismo cruzado φ é determinado por $m \in M$ onde $\varphi(\sigma) = m$, e

$$\sigma^{n-1}m + \cdots + \sigma m + m = 0. \tag{2.3}$$

Reciprocamente, dado $m \in M$ tal que $\sigma^{n-1}m + \cdots + \sigma m + m = 0$, verifica-se que $\varphi(\sigma^i) = \sigma^{i-1}m + \cdots + \sigma m + m$ define um homomorfismo cruzado $\varphi : G \to M$. Além disso,

$$\varphi \text{ é principal} \Leftrightarrow m = \sigma x - x \text{ para algum } x \in M.$$

Defina

$$\begin{aligned} \mathrm{Nm}_G : M &\to M \\ m &\mapsto \sum_{\sigma\in G} \sigma m \end{aligned}$$

e

$$\begin{aligned} \sigma - 1 : M &\to M \\ m &\mapsto \sigma m - m. \end{aligned}$$

Para um grupo G cíclico, finito de ordem n e gerado por σ, temos que

$$\begin{aligned} \mathrm{Ker}(\mathrm{Nm}_G) &= \{m \in M : \sum_{\sigma\in G} \sigma m = 0\} \\ &= \{m \in M : \sigma^1 m + \sigma^2 m + \cdots + \sigma^{n-1} m = 0\} \end{aligned}$$

define um homomorfismo cruzado. E claramante, $(\sigma - 1)M$ é um homomorfismo cruzado principal.

Portanto,

$$H^1(G, M) \simeq \frac{Z^1(G, M)}{B^1(G, M)} \simeq \frac{\mathrm{Ker}(\mathrm{Nm}_G)}{(\sigma - 1)M}$$

2.3 A Cohomologia de L e $L^\times$

Seja L uma extensão finita de Galois do corpo K, e seja $G = \mathrm{Gal}(L/K)$. Então, L e $L^\times = L - \{0\}$ são G-módulos.

Proposição 2.4. *(Preposição 1.22.2 de [13]). Seja L/K uma extensão finita de Galois com grupo de Galois G. Então, $H^1(G, L^\times) = 0$.*

Demonstração. Seja $\varphi : G \to L^\times$ um homomorfismo cruzado. Na notação multiplicativa, temos

$$\varphi(\sigma\tau) = \sigma\varphi(\tau) \cdot \varphi(\sigma) \quad \sigma, \tau \in G.$$

Mostraremos que φ é um homomorfismo cruzado principal, isto é, que existe $\gamma \in L^\times$ tal que, $\varphi(\gamma) = \frac{\sigma\gamma}{\gamma} \quad \forall \sigma \in G$.

O Teorema de Dedekind, sobre a independência de caracteres, garante que se L é um corpo e H um grupo, então todo conjunto finito $\{\psi_i\}$ de homomorfismo distintos, $H \to L^\times$, é linearmente independentes, isto é

$$\sum_i a_i \psi_i(n) = 0, \ \forall h \in H \Rightarrow a_1 = a_2 = \cdots = a_n = 0.$$

Sendo $\varphi(\tau), \tau \in G$ não nulo, então o Teorema de Dedekind garante que

$$\sum_{\tau \in G} \varphi(\tau)\tau : L^\times \to L^\times$$

é um mapa não nulo. Assim, existe um $\alpha \in L^\times$ tal que

$$\beta \overset{def}{=} \sum_{\tau \in G} \varphi(\tau)\tau(\alpha) \neq 0.$$

Tome $\sigma \in G$, então

$$\begin{aligned} \sigma\beta &= \sum_{\tau \in G} \sigma\varphi(\tau)\sigma\tau(\alpha) \\ &= \sum_{\tau \in G} \varphi(\sigma)^{-1}\varphi(\sigma\tau)\sigma\tau(\alpha) \\ &= \varphi(\sigma)^{-1} \sum_{\tau \in G} \varphi(\sigma\tau)\sigma\tau(\alpha) \end{aligned}$$

Sendo G um grupo fechado pela multiplicação dos seus elemetos, isto é, $\sigma\tau \in G, \ \forall \sigma, \tau \in G$, e como τ percorre todo o grupo G,

$$\beta = \sum_{\tau \in G} \varphi(\tau)\tau(\alpha) = \sum_{\tau \in G} \varphi(\sigma\tau)\sigma\tau(\alpha).$$

Logo, $\sigma\beta = \varphi(\sigma)^{-1}\beta$ e

$$\varphi(\sigma) = \tfrac{\beta}{\sigma\beta}.$$

Basta tomar $\beta = \gamma^{-1}$ e teremos $\varphi(\sigma) = \frac{\sigma\gamma}{\gamma}$. Mediante esse resultado, φ é também um homomorfismo cruzado principal. Portanto, $H^1(G, L^\times) = 0$. □

Corolário 3. *Seja L/K uma extensão cíclica e σ o gerador de* $\mathrm{Gal}(L/K)$. *Se* $\mathrm{Nm}_G(a) = 1$, *então a é da forma $\frac{\sigma b}{b}$.*

Demonstração. Suponha que a ordem da extensão cíclica seja n. Por hipótese,

$$\mathrm{Nm}_G(a) = \sum_{\sigma \in G} \sigma(a) = 1.$$

sendo a extensão cíclica,

$$\sum_{\sigma \in G} \sigma(a) = a \cdot \sigma a \cdot \sigma^2 a \cdots \sigma^{n-1} a = 1$$

temos que $\varphi : G \to L^\times$ é um homomorfismo cruzado definido por

$$\varphi(\sigma^i) = \sigma^{i-1}a \cdots \sigma a \cdot a$$

Com isso, φ é um homomorfismo cruzado principal e $a = \frac{\sigma b}{b}$, para algum $b \in L^\times$. □

Proposição 2.5. *(Proposição 1.24.2 de [13]). Seja L/K uma extensão finita de Galois com grupo de Galois G. Então, $H^r(G, L) = 0$ para todo $r > 0$.*

2.4 Cohomologia de Produtos

Seja $M = \prod_i M_i$ de G-módulo. M é um G-módulo via a ação diagonal:

$$\sigma(m_1, \ldots, m_i, \ldots) = (m_1, \cdots, \sigma m_i, \ldots).$$

Proposição 2.6. *(Proposição 1.25.2 de [13]). Para todo M_i G-módulos, temos*

$$H^r(G, \textstyle\prod_i M_i) \simeq \prod_i H^r(G, M_i).$$

Demonstração. O produto de sequências exatas de grupos abelianos é também exata. Com isso, o produto $I = \prod_i I_i$, onde cada I_i é um G-módulo injetivo, será injetivo pois

$$\mathrm{Hom}_G(-, I) \simeq \textstyle\prod_i \mathrm{Hom}_G(-, I_i)$$

é exato. Seja $M_i \to I_i^\bullet$ uma resolução injetiva de M_i. Então, $\prod_i M_i \to \prod_i I_i^\bullet$ é uma resolução injetiva de $\prod_i M_i$. Assim,

$$H^r(G, \textstyle\prod_i M_i) \simeq H^r((\prod_i I_i^\bullet)^G) \simeq H^r(\prod_i (I_i^\bullet)^G) \simeq \prod_i H^r(I_i^{\bullet G}) \simeq \prod_i H^r(G, M_i).$$

□

2.5 Propriedades Funtoriais de Cohomologia de Grupos

Veremos que dois homomorfismos compatíveis um homomorfismo de complexos. Assim, teremos homomorfismos entre dois Grupos de Cohomologia. E entre esses homomorfismos e sob condições especiais, definiremos os homomorfismos restrição, inflação, corestrição. E além disso, mostraremos algumas relações existentes entre esses homomorfismos. Uma relação importante entre os homomorfimos, inflação e restrição é que eles formaram uma sequência exata.

Sejam G-módulo M e H-módulo N. Os homomorfismos

$$\alpha : H \to G, \quad \beta : M \to N$$

são chamados compatíveis se

$$\beta(\alpha(g')m) = g'(\beta(m)),\ \forall g' \in H \ e\ m \in M.$$

Assim, (α, β) define homomorfismos de complexos

$$\begin{aligned} C^\bullet(G, M) &\to C^\bullet(H, N) \\ \varphi &\mapsto \beta \circ \varphi \circ \alpha^r, \end{aligned}$$

bem como os homomorfismos

$$H^r(G, M) \to H^r(H, N).$$

Exemplo 5. *Seja H um subgrupo de G. Tome um H-módulo M e considere o mapa*

$$\begin{aligned} \alpha : \mathrm{Ind}_H^G(M) &\to M \\ \varphi &\mapsto \varphi(1_G) \end{aligned}$$

e a inclusão natural

$$\begin{aligned} \beta : H &\hookrightarrow G \\ h &\mapsto h. \end{aligned}$$

Os mapas α e β são compatíveis, pois

$$\beta(\alpha(\varphi)h) = \beta(\varphi(1_G)h) = \varphi(1_G)h = \varphi(h)$$

e, por outro lado,

$$\varphi(\beta(h)) = \varphi(h).$$

Então, (α, β) induz o homomorfismo

$$H^r(G, \mathrm{Ind}_H^G(M)) \to H^r(H, M)$$

e o Lema de Shapiro garante que são isomorfos.

Exemplo 6. *Seja H um subgrupo de G. Considere $\alpha : H \hookrightarrow G$, e β é o mapa identidade no M G-módulo. Os mapas α e β são compatíveis, pois $\beta(\alpha(h)m) = \beta(hm) = hm = h\beta(m)$. Com isso, (α, β) define o homomorfismo restrição*

$$\mathrm{Res} : H^r(G, M) \to H^r(H, M).$$

Esse homomorfismo restrição também pode ser construído da seguinte maneira:
Tome o mapa

$$\begin{aligned} \psi : M &\to \mathrm{Ind}_H^G(M) \\ m &\mapsto \psi_m : g \to gm \end{aligned}$$

$$H^r(G, M) \to H^r(G, \mathrm{Ind}_H^G(M))$$

e, pelo Lema de Shapiro, $H^r(G, \mathrm{Ind}_H^G(M)) \simeq H^r(H, M)$.
Portanto, é uma mapa restrição.

Exemplo 7. *Seja H um subgrupo normal de G. Considere o mapa quociente $\alpha : G \to G/H$, e $\beta : M^H \hookrightarrow M$. Verifica-se que $\beta(\alpha(g)m) = \beta((g + H)m) = \beta(gm) = gm = g\beta(m)$. Assim, (α, β) são compatíveis e definem o homomorfismo inflação*

$$\mathrm{Inf} : H^r(G/H, M^r) \to H^r(G, M).$$

Exemplo 8. *Tome $g_0 \in G$ e sejam $\alpha : G \to G$, $\sigma \mapsto g_0\sigma g_0^{-1}$, e $\beta : M \to M$, $m \mapsto g_0^{-1}m$ homomorfismos. Observe que*

$$\beta(\alpha(\sigma)m) = \beta(g_0\sigma g_0^{-1}m) = g_0^{-1}g_0\sigma g_0^{-1}m = \sigma g_0^{-1}m = \sigma\beta(m).$$

Com isso, (α, β) são compatíveis e definem o homomorfismo

$$H^r(G, M) \to H^r(G, M).$$

Provaremos que é o mapa identidade.

Para $r = 0$ temos o homomorfismo

$$\begin{aligned} \varphi : M^G &\to M^G \\ m &\mapsto g_0^{-1}m \end{aligned}$$

que, claramente, é o mapa identidade.

Seja $r > 0$ e suponha que a afirmação é válida para $r - 1$.

Tome a sequência 1

$$0 \to M \to M_* \to M_\dagger \to 0$$

onde $M_* = \mathrm{Ind}^G(M_0)$. Assim, obtemos o seguinte diagrama

$$\begin{array}{ccccccc} H^{r-1}(G, M_*) & \longrightarrow & H^{r-1}(G, M_\dagger) & \xrightarrow{\delta} & H^r(G, M) & \longrightarrow & 0 \\ \downarrow & & \downarrow & & \downarrow & & \\ H^{r-1}(G, M_*) & \longrightarrow & H^{r-1}(G, M_\dagger) & \xrightarrow{\delta} & H^r(G, M) & \longrightarrow & 0 \end{array}$$

Temos que $H^{r-1}(G, M_*) = 0$ e os mapas verticais são definidos pelo par (α, β). Verifica-se que esse diagrama comuta e por hipótese, o mapa do meio é a identidade. Logo, $H^r(G, M) \to H^r(G, M)$ também será o mapa identidade.

Exemplo 9. *Seja H um subgrupo de indice finito de G, e seja S um conjunto de representantes da classe lateral à esquerda de H em G, $G = \bigcup_{s\in S} sH$. Seja M um G-módulo. Para todo $m \in M^H$,*

$$\mathrm{Nm}_{G/H}m := \sum_{s\in S} sm$$

é independente da escolha de S e além disso, é fixado por G. Para verificar essa afirmação, tome $m \in M^H$ e $g \in G$ e assim $g(sm) = (gs)m$. Sendo $gs \in G$, existe $h \in H$ tal que $gs = s'h$ para algum $s' \in S$, então

$$g(sm) = (gs)m = (s'h)m = s'(hm) = s'm$$

Assim, $\mathrm{Nm}_{G/H}$ é um homomorfismo de M^H para M^G.

Esse resultado pode ser extendido para o homomorfismo de corestrição

$$\mathrm{Cor} : H^r(H, M) \to H^r(G, M)$$

para todo r. Para isso, dado M G-módulo, exite um homomorfismo canônico de G-módulo

$$\begin{aligned} \mathrm{Ind}_H^G M &\to M \\ \varphi &\mapsto \sum_{s\in S} s\varphi(s^{-1}). \end{aligned}$$

Então, $H^r(G, \mathrm{Ind}_H^G M) \to H^r(G, M)$ e pelo Lema de Shapiro,

$$H^r(H, M) \simeq H^r(G, \mathrm{Ind}_H^G M) \to H^r(G, M).$$

Proposição 2.7. *Seja H um subgrupo de G de índice finito. A composição*

$$\mathrm{Cor} \circ \mathrm{Res} : H^r(G, M) \to H^r(G, M)$$

é a multiplicação pelo índice de H em G, $[G : M]$.

Demonstração. Para todo $m \in M$, considere o mapa

$$\begin{aligned} \varphi_m : G &\to M \\ g &\mapsto gm. \end{aligned}$$

Tome $h \in H$, então $\varphi_m(hg) = (hg)m = h(gm) = h\varphi_m(g)$. Logo, $\varphi_m \in \mathrm{Ind}_H^G M$ e Cor $\circ$ Res, é o mapa na Cohomologia definido pela composição

$$M \to \mathrm{Ind}_H^G M \to M,$$

onde

$$m \mapsto \varphi_m \mapsto \sum_{s\in S} s\varphi(s^{-1}) = \sum_{s\in S} ss^{-1}m = \sum_{s\in S} m = (G : H)m.$$

□

Corolário 4. *Se $[G : 1] = m$, então $mH^r(G, M) = 0$ para $r > 0$.*

Demonstração. Pela Proposição 2.7, multiplicando por m o mapa composto

$$H^r(G, M) \overset{Res}{\to} H^r(1, M) \overset{Cor}{\to} H^r(G, M),$$

e sabendo que $H^r(1, M) = 0$, então $mH^r(G, M) = 0$ para $r > 0$. □

2.5.1 A Sequência Inflação-Restrição

Proposição 2.8. *(Proposição 1.34.2 de [13]). Seja H um subgrupo normal de G e M um G-módulo. Seja r um inteiro maior que 0. Se $H^i(H, M) = 0$ para todo i com $0 < i < r$, então a sequência*

$$0 \to H^r(G/H, M^H) \overset{Inf}{\to} H^r(G, M) \overset{Res}{\to} H^r(H, M) \tag{2.4}$$

é exata.

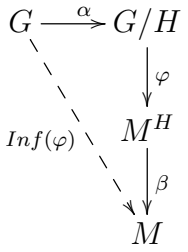
Demonstração. Observa-se que, para $r = 1$ a hipótese $H^i(H, M)$ é vazia, isto é, não podemos afirmar que a sequência é exata para $r = 1$. Diante disso, verificaremos que é válido para $r = 1$.

(i) Exatidão em $H^1(G/H, M^H)$.

Mostraremos que o mapa Inf é injetivo.

A inflação é definida pelos mapas compatíveis, (α, β), onde $\alpha : G \to G/H$ e $\beta : M^H \to M$ é o mapa inclusão.

O mapa $\varphi : G/H \to M^H$ induz o mapa inflação da seguinte forma



onde $Inf(\varphi) = \beta(\varphi(\alpha))$.

Tome $\varphi' \in \mathrm{Ker}(Inf)$ e com isso, $Inf(\varphi') \in H^1(G, M)$ é um homomorfismo principal, isto é, $Inf(\varphi')(\sigma) = \sigma m - m$ para algum $m \in M$ e para todo $\sigma \in G$. Diante disso,

$$Inf(\varphi')(\sigma) = \beta(\varphi'(\alpha))(\sigma) = \beta(\varphi'(\overline{\sigma})) = \varphi'(\overline{\sigma}) = \sigma m - m.$$

E por outro lado,

$$\varphi'(\overline{\tau}) = 0 = \tau m - m \quad \text{para todo } \tau \in H.$$

Assim, $m \in M^H$ e φ' é um homomorfismo principal. Portanto, Inf é um mapa injetivo.

(ii) $Res \circ Inf = 0$. Tome $\varphi : G \to M$ é 1-cociclo, então $\varphi|_H : H \to M$ é a restrição da classe de φ. Dessa maneira, suponha que $\varphi = Inf$, então a Inf restrita a H é igual a $\varphi(0) = 0$

(iii) Exatidão em $H^1(G, M)$. Seja $\varphi : G \to M$ tal que φ é um homorfismo cruzado e φ restrito a H é um homomorfismo cruzado principal. Então, $\varphi(h) = hm_0 - m_0$, para algum $m_0 \in M$. Defina $\varphi' : G \to M$ tal que $\varphi'(\sigma) = \varphi(\sigma) - (\sigma m_0 - m_0)$. Temos que φ' é um homomorfismo cruzado, pois

$$\varphi'(\tau\sigma) = \varphi(\tau\sigma) - (\tau\sigma m_0 - m_0) = \tau\varphi(\sigma) + \varphi(\tau) - (\tau\sigma m_0 - m_0) \quad \forall \quad \tau, \sigma \in G$$

e por outro lado,

$$\begin{aligned} \tau\varphi'(\sigma) + \varphi'(\tau) &= \tau[\varphi(\sigma) - (\sigma m_0 - m_0)] + \varphi(\tau) - (\tau m_0 - m_0) \\ &= \tau\varphi(\sigma) - \tau\sigma m_0 + \varphi(\tau) + m_0. \end{aligned}$$

Assim, $\varphi'(\tau\sigma) = \tau\varphi'(\sigma) + \varphi'(\tau)$.

Agora tome $h \in H$, $\varphi'(h) = \varphi(h) - (hm_0 - m_0) = 0$, pois φ é homomorfismo principal em H. Logo, $\varphi'(h) = 0$, $\forall h \in H$.

Defina $\varphi'' : G/H \to M^H$ via $\varphi''(\overline{\sigma}) = \varphi'(\sigma)$, $\forall \sigma \in G$. Tome $\tau \in H$, então $\varphi'(\sigma\tau) = \sigma\varphi'(\tau) + \varphi'(\sigma) = \varphi'(\sigma)$, para todo $\sigma \in G$. Mostraremos que φ'' está bem definido. Para isso, tome $\rho \in H$ e então

$$\rho\varphi''(\sigma H) = \rho\varphi'(\sigma) = \varphi'(\rho\sigma) - \varphi'(\rho) = \varphi'(\rho\sigma).$$

Note que, $\sigma = \sigma\rho'$, onde $\rho' = \sigma^{-1}\rho\sigma \in H$, pois $H \lhd G$.
Logo,

$$\rho\varphi''(\sigma H) = \varphi'(\rho\sigma) = \varphi'(\sigma\rho') = \varphi'(\sigma) = \varphi''(\sigma H)$$

e $\varphi''(\sigma H) \in M^H$. Com isso, temos a exatidão de $H^1(G, M)$.

Assuma que $r > 1$ e que a afirmação é válida para $r - 1$. Tome a sequência exata

$$0 \to M \to M_* \to M_\dagger \to 0.$$

Então,

$$H^i(H, M_\dagger) \simeq H^{i+1}(H, M),\ i > 0,$$

e assim, $H^i(H, M_\dagger) = 0$ para $0 < i < r - 1$. Por hipótese, a sequência

$$0 \to H^{r-1}(G/H, M_\dagger^H) \overset{Inf}{\to} H^{r-1}(G, M_\dagger) \overset{Res}{\to} H^{r-1}(H, M)$$

é exata, e é isomorfa a sequência

$$H^r(G/H, M_\dagger^H) \overset{Inf}{\to} H^r(G, M_\dagger) \overset{Res}{\to} H^r(H, M).$$

□

2.6 Definição de Homologia de Grupos

Dado um G-módulo M, defina M_G como o maior quociente de M sobre o qual G age trivialmente. Então, M_G é o quociente de M pelo subgrupo gerado por $\{gm - m | g \in G, \quad m \in M\}$. Para identificar o módulo M_G com um produto tensorial, lembramos do seguinte isomorfismo bem conhecido.

Proposição 2.9. *Dado um A-módulo M e $\mathfrak{a}$ um ideal de A, então*

$$\frac{M}{\mathfrak{a}M} \simeq M \otimes_A \frac{A}{\mathfrak{a}}$$

onde $\mathfrak{a}M = \{\Sigma_i a_i m_i \mid a_i \in \mathfrak{a} \quad \forall i\}$.

Demonstração. Considere o seguinte mapa

$$\begin{array}{rcl} \dfrac{M}{\mathfrak{a}M} & \to & M \otimes \dfrac{A}{\mathfrak{a}} \\ \overline{m} & \mapsto & m \otimes_A \overline{1} \end{array}$$

Note que, $m \equiv m' \mathrm{mod}\mathfrak{a} \Leftrightarrow m = m' + \Sigma_i a_i m_i$. Aplicando o funtor $- \otimes_A \overline{1}$ em $m' + \Sigma_i a_i m_i$ temos,

$$m' \otimes_A \overline{1} + \Sigma_i a_i m_i \otimes_A \overline{1} = m' \otimes_A \overline{1} + \Sigma_i m_i \otimes \overline{a}_i = m' \otimes_A \overline{1},$$

pois $\overline{a}_i = 0$. Isso mostra que o mapa está bem definido.

Tome o mapa

$$\begin{array}{rcl} M \otimes \dfrac{A}{\mathfrak{a}} & \to & \dfrac{M}{\mathfrak{a}M} \\ \Sigma_i m_i \otimes_A \overline{a}_i & \mapsto & \Sigma_i a_i m_i + \mathfrak{a}M \end{array}$$

que, claramente, está bem definido.

Verifica-se que os mapas acima são mutuamente inversos, pois

$$\begin{array}{rcl} \dfrac{M}{\mathfrak{a}M} & \to & M \otimes \dfrac{A}{\mathfrak{a}} \to \dfrac{M}{\mathfrak{a}M} \\ \overline{m} & \mapsto & m \otimes_A \overline{1} \mapsto \overline{1m} \end{array}$$

e por sua vez,

$$\begin{array}{rcl} M \otimes \dfrac{A}{\mathfrak{a}} & \to & \dfrac{M}{\mathfrak{a}M} \to M \otimes \dfrac{A}{\mathfrak{a}} \\ \Sigma_i m_i \otimes_A \overline{a}_i & \mapsto & \Sigma_i a_i m_i + \mathfrak{a}M \end{array}$$

e

$$\Sigma_i a_i m_i + \mathfrak{a}M \;\mapsto\; \Sigma_i a_i m_i \otimes_A \overline{1} = \Sigma_i m_i \otimes_A \overline{a}_i.$$

Portanto, $\frac{M}{\mathfrak{a}M} \simeq M \otimes_A \frac{A}{\mathfrak{a}}$. □

Definimos o mapa aumento por

$$\begin{array}{rcl} \varepsilon : \mathbb{Z}[G] & \to & \mathbb{Z} \\ \Sigma n_g g & \mapsto & \Sigma n_g. \end{array}$$

Dado $n_g \in \mathbb{Z}$ existe $n_g g \in \mathbb{Z}[G]$ tal que $\varepsilon(n_g g) = n_g$, então ε é um mapa sobrejetivo.

O núcleo desse mapa é chamado ideal de aumento e é denotado por I_G. Claramente, I_G é um $\mathbb{Z}$-submódulo livre de $\mathbb{Z}[G]$ com base $\{g - 1 | g \in G, g \neq 1\}$. Logo, pelo Primeiro Teorema do Isomorfismo

$$\frac{\mathbb{Z}[G]}{I_G} \simeq \mathbb{Z}.$$

Com isso, e pelo resultado da Proposição 2.9

$$M_G \simeq \frac{M}{I_G M} \simeq M \otimes_{\mathbb{Z}[G]} \frac{\mathbb{Z}[G]}{I_G} \simeq M \otimes_{\mathbb{Z}[G]} \mathbb{Z}.$$

Proposição 2.10. *O funtor,*

$$\begin{array}{rcl} \mathrm{Mod}_G & \to & \mathrm{Mod}_{\mathbb{Z}} \\ M & \mapsto & M_G \end{array}$$

é exato à direita, isto é, se

$$0 \to M' \to M \to M'' \to 0$$

é exata, então

$$M'_G \to M_G \to M''_G \to 0$$

é exata.

Demonstração. Sendo o funtor $M \mapsto M \otimes_{\mathbb{Z}[G]} \mathbb{Z}$ exato e isomorfo ao funtor $M \mapsto M_G$, então a sequência $M'_G \to M_G \to M''_G \to 0$ é exata. □

Definição 2.3. *Um objeto P na categoria abeliana é dito projetivo se satisfaz qualquer uma das afirmações:*

1. *Sejam D, L, M e N R-módulos. Se*

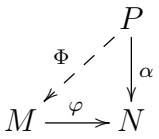
   $$0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} N \to 0$$

   é exata, então a sequência

   $$0 \to \mathrm{Hom}_R(P, L) \xrightarrow{\psi^*} \mathrm{Hom}_R(P, M) \xrightarrow{\varphi^*} \mathrm{Hom}_R(P, N) \to 0 \tag{2.5}$$

   também é uma sequência exata.

2. *Para todo M e N R-módulos, se $M \xrightarrow{\varphi} N \to 0$ é exata, então dado $\alpha \in \mathrm{Hom}_R(P, N)$ existe um levantamento $\Phi \in \mathrm{Hom}_R(P, M)$ que faz o seguinte diagrama comutar*

3. *Se P é um quociente de um R-módulos M, então P é isomorfo a um somando direto de M, isto é,*
   $0 \to L \xrightarrow{\psi} M \xrightarrow{\varphi} P \to 0$ cinde.

4. *P é a somando direto de um R-módulo livre.*

Vimos na Proposição 1.3 que essas relações são equivalentes.

Seja M um G-módulo e tome uma resolução projetiva

$$\cdots \to P_2 \xrightarrow{d_2} P_1 \xrightarrow{d_1} P_0 \xrightarrow{d_0} M \to 0$$

de M. O complexo

$$\cdots \to (P_2)_G \xrightarrow{d_2} (P_1)_G \xrightarrow{d_1} (P_0)_G \to 0$$

não é necessariamente uma sequência exata longa. O conjunto definido por

$$H_r(G, M) = \frac{\mathrm{Ker}(d_r)}{\mathrm{Im}(d_{r+1})}$$

é r-ésimo grupo de homologia de G.

Esses grupos tem as seguintes propriedades básicas:

(*i*) Temos um isomorfismo natural $H_0(G, M) = M_G$.

(*ii*) Se P é um G-módulo projetivo, então $H_r(G, P) = 0$ para todo $r > 0$, pois

$$\cdots \to 0 \to P \to P \to 0$$

é uma resolução projetiva.

(*iii*) Sejam $P_\bullet \to M$ e $Q_\bullet \to N$ resoluções projetivas de doisn G-módulos M e N, respectivamente. Dado $\alpha : M \to N$ homomorfismo de G-módulos estende para um morfismo de complexos

$$\begin{array}{ccc} P_\bullet & \longrightarrow & M \\ {\scriptstyle \alpha_\bullet}\downarrow & & \downarrow{\scriptstyle \alpha} \\ Q_\bullet & \longrightarrow & N \end{array}$$

e os homomorfismos

$$H_r(\alpha_\bullet) : H_r(P_\bullet) \to H_r(Q_\bullet)$$

não dependem da escolha de $\alpha_\bullet$. Note que isso aplicado à identidade $M \to M$ nos diz que os $H_r(G, M)$ estão bem-definidos.

(*iv*) Uma sequência exata curta

$$0 \to M' \to M \to M'' \to 0$$

de G-módulos induz a exatidão da sequência longa

$$\cdots \to H_r(G, M) \to H_r(G, M'') \xrightarrow{\delta_r} H_{r-1}(G, M') \to \cdots \to H_0(G, M'') \to 0.$$

Considere a sequência exata curta

$$0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z}$$

que induz a sequência exata longa dada por

$$\cdots \to H_1(G, I_G) \to H_1(G, \mathbb{Z}[G]) \to H_1(G, \mathbb{Z}) \xrightarrow{\delta} H_0(G, I_G) \to H_0(G, \mathbb{Z}[G]) \to H_0(G, \mathbb{Z}) \to 0.$$

O $\mathbb{Z}[G]$ é um G-módulo livre e então, $\mathbb{Z}[G]$ é projetivo. Assim, $H_1(G, \mathbb{Z}[G]) = 0$. E além disso, o mapa $H_0(G, I_G) \to H_0(G, \mathbb{Z}[G])$ é nulo, pois esse mapa pode ser visto como

$$\frac{I_G}{I_G I_G} \to \frac{\mathbb{Z}[G]}{I_G \mathbb{Z}[G]},$$

e é induzido pela inclusão $I_G \hookrightarrow \mathbb{Z}[G]$. Com isso, temos

$$0 \to H_1(G,\mathbb{Z}) \stackrel{\delta}{\to} \frac{I_G}{I_G I_G} \to 0$$

isto é, $H_1(G,\mathbb{Z}) \simeq \frac{I_G}{I_G I_G}$ e

$$0 \to H_0(G,\mathbb{Z}[G]) \to H_0(G,Z) \to 0$$

implica que $\mathbb{Z}[G]_G \simeq \mathbb{Z}$.

Considere $I_G^2 := I_G \cdot I_G$ é o $\mathbb{Z}$-submódulo de $\mathbb{Z}[G]$ gerado pelos elementos da forma

$$(g-1)(g'-1),\ g,g' \in G.$$

Lema 2.2. *(Lema 2.6.2 de [13]). Seja G' o subgrupo comutador de G. O mapa $g \mapsto (g-1)+I_G^2$ induz o isomorfismo*

$$\frac{G}{G'} \to \frac{I_G}{I_G^2}.$$

Demonstração. O subgrupo comutador de G é gerado por $[\sigma_1,\sigma_2]$, onde $[\sigma_1,\sigma_2] = \sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}$ e sabemos que G/G' é o maior quociente abeliano de G.

Considere o homomorfismo $\psi : G \to A$, onde A é um grupo abeliano aditivo. Tome $[\sigma_1,\sigma_2] \in G'$, então

$$\psi(\sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}) = \psi(\sigma_1)+\psi(\sigma_2)-\psi(\sigma_1)-\psi(\sigma_2) = 0.$$

Logo, o mapa ψ induz $\overline{\psi} : G/G' \to A$ tal que $gG' \mapsto \psi(g)$.

Mostraremos que o mapa $\overline{\varphi} : G/G' \to I_G/I_G^2$ é induzido pelo mapa

$$\begin{aligned} \varphi : G &\to I_G/I_G^2 \\ g &\mapsto (g-1)+I_G^2. \end{aligned}$$

através do resultado acima.

O mapa φ é um homomorfismo, pois

$$\varphi(\sigma_1\sigma_2)-(\varphi(\sigma_1)+\varphi(\sigma_2)) = [\sigma_1\sigma_2-1-((\sigma_1-1)+(\sigma_2-1))]+I_G^2 = (\sigma_1-1)(\sigma_2-1)+I_G^2.$$

Com isso, $\varphi(\sigma_1\sigma_2) \equiv \varphi(\sigma_1)+\varphi(\sigma_2) \text{mod } I_G^2$.

Obeerve que $G' \subset \text{Ker}(\varphi)$, pois I_G/I_G^2 é abeliano. Dessa forma, o mapa φ induz o mapa

$$\begin{aligned} \overline{\varphi} : G/G' &\to I_G/I_G^2 \\ gG' &\mapsto \varphi(g) = (g-1)+I_G^2. \end{aligned}$$

Agora, considere o seguinte mapa

$$\begin{aligned} \psi : I_G/I_G^2 &\to G/G' \\ \Sigma_{g\in G} n_g(g-1)+I_G^2 &\mapsto \Pi_{g\in G} g^{n_g}G' \end{aligned}$$

que, claramente, é um homomorfismo. Tome $(\sigma_1-1)(\sigma_2-1) = (\sigma_1\sigma_2-1)-(\sigma_1-1)-(\sigma_2-1) \in I_G^2$ e assim,

$$\psi[(\sigma_1-1)(\sigma_2-1)] = (\sigma_1\sigma_2)(\sigma_1)^{-1}(\sigma_2)^{-1}G' = \sigma_1\sigma_2\sigma_1^{-1}\sigma_2^{-1}G' = G'.$$

Com isso, o mapa ψ está bem definido.

Falta mostrar que os mapas φ e ψ são mutuamentes inversos. Para isso, considere os casos:

1. $G/G' \to I_G/I_G^2 \to G/G'$
   $\sigma G' \mapsto (\sigma - 1) + I_G^2 \mapsto \sigma G'$.

2. $I_G/I_G^2 \to G/G' \to I_G/I_G^2$
   $(\sigma - 1) + I_G^2 \mapsto \sigma G' \mapsto (\sigma - 1) + I_G^2$.

Portanto, $G/G' \simeq I_G/I_G^2$. □

Capítulo 3

Teorema de Golod-Shafarevich

Neste capítulo daremos algumas propriedades de p-grupos que são essenciais para a demonstração do Teorema de Golod-Shafarevich. Depois, definiremos os Grupos de Tate e mostraremos que os Grupos de Cohomologia e Homologia estão relacionados e formam uma sequência exata. Além disso, provaremos dois lemas chaves para essa demonstração que dão resultados nos Grupos de Homologia e com isso, provaremos o poderoso Teorema de Golod-Shafarevich. Por fim, veremos como esse teorema trouxe grandes contribuições em várias áreas da matemática, bem como o primeiro contra exemplo que mostra que a conjectura de Burnside(1911) é falsa e também um contra exemplo para o problema de Kurosh-Levitzki.

3.1 A estrutura de p-grupos finitos

Lema 3.1. *(Lema 2.2 de [15]). Seja H é um subgrupo próprio de um p-grupo finito G. Existe um elemento não nulo $\chi \in H^1(G, \mathbb{Z}/p\mathbb{Z})$ tal que $\chi\,|_H = 0$*

Demonstração. Como H é um subgrupo próprio de G, existe um subgrupo normal U tal que o mapa $\pi : G \to G/U$, onde $\pi(H) \neq G/U$ está bem definido. Seja $\pi(H) = H_0$. Sendo G/U um p-grupo finito, então G/U é solúvel. Com isso, existe uma cadeia, $\{1\} \leq G_1 \leq G_2 \leq \cdots \leq G_n = G/U$, de subgrupos de G/U onde $G_i \triangleleft G_{i+1}$ e $\frac{G_{i+1}}{G_i}$ são abelianos para todo $i = 1, \ldots, n$. Assim, existe um subgrupo normal N de G/U tal que $[G/U : N] = p$ e $H_0 \subseteq N$.

Como visto, $\chi \in H^1(G, \mathbb{Z}/p\mathbb{Z}) = \{\frac{homomorfismos \quad cruzados}{homomorfismos \quad principais}\}$ e sendo ação a de G em $\mathbb{Z}/p\mathbb{Z}$ trival, então $H^1(G, \mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Z}/p\mathbb{Z})$.

Agora, considere a sequência de homomorfismos

$$G \overset{\pi}{\to} G/U \overset{\iota}{\to} \frac{G/U}{N} \simeq \mathbb{Z}/p\mathbb{Z}$$

e defina $\chi = \iota \circ \pi$. Assim,

$$\chi(H) = \iota \circ \pi(H) = \iota(H_0) = 0$$

pois $H_0 \subseteq N$. □

Definição 3.1. *O subgrupo de Frattini de G é denotado por G^*, é definido como a interseção de todos os subgrupos maximais de G. Caso G não possua subgrupos maximais, definimos $G^* = G$.*

Temos também a seguinte definição equivalante quando G é um p-grupo finito:

$$G^* = \cap\{\mathrm{Ker}(\chi)|\chi \in H^1(G, \mathbb{Z}/p\mathbb{Z})\}.$$

Definição 3.2. *Um caracter χ de G é um homomorfismo de G para $\mathbb{C}^\times$ com $|\chi(\sigma)| = 1$. Defina a estrutura de grupo no conjunto $X(G)$ de todos os caracteres de G por*

$$\chi_1\chi_2(\sigma) := \chi_1(\sigma)\chi_2(\sigma) \text{ para todo } \chi_1, \chi_2 \in X(G).$$

E além disso, $X(G)$ é chamado de grupo de caracteres ou grupo dual de Pontryagin de G.

Teorema 3.1. *(Teorema A3.1 de [12])(Teorema da dualidade de Pontryagin)*

1. *Seja H um subgrupo de G. Seja $X(H) \simeq X(G)/\{\chi|\chi(H) = 1\}$. Assim, $H \to X(H)$ é uma correspondência injetiva entre os subgrupos de G e os grupos quocientes de $X(G)$.*
2. *Seja $\varphi : G \to X(X(G))$ um homomorfismo tal que $\varphi(\sigma)(\chi) = \chi(\sigma)$ para todo $\sigma \in G$. Então φ é um isomorfismo de G em $X(X(G))$.*

Proposição 3.1. *(Proposição 22 de [15]). O subgrupo de Frattini, G^*, de um p-grupo G tem as seguintes propriedades:*

1. *$G^* = G^P \cdot G'$.*
2. *G/G^* é dual de Pontrjagin para $H^1(G, \mathbb{Z}/p\mathbb{Z})$.*
3. *Se H é um subgrupo G, então $H = G$ se, e somente se, $HG^* = G$.*
4. *Um homomorfismo $\phi : G \to H$ de p-grupos induz um homomorfismo correspondente $\phi_* : G/G^* \to H/H^*$. Além disso, o homomorfismo ϕ é sobrejetivo se, e somente se, ϕ_* é sobrejetivo.*

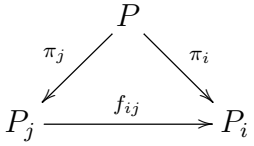
Nesse instante, definiremos o p-grupo livre, $F_p(X)$, em X. Para isso, precisamos de algumas definições que serão dadas abaixo, tais como, conjuntos direcionados e limite inverso. Vale ressaltar que também é possível definir o limite direto, mas pelos objetivos desse trabalho, isso não será feito aqui. Caso tenha interesse, é possível ver a definição de limite direto em [15].

Seja I um conjunto direcionado com relação a $\leq$. Isso significa que $\leq$ é reflexiva e transitiva e para todo $i_1, i_2 \in I$, existe um $i \in I$ tal que $i \geq i_1$ e $i \geq i_2$.

Considere uma categoria $\mathfrak{C}$ e seja $\{P_i\}_{i\in I}$ uma família de objetos de $\mathfrak{C}$, onde I é um conjunto direcionado. Assim, temos um conjunto de morfismos, $\{f_{ij} : P_j \to P_i | i \leq j; i, j \in I\}$, que satisfazem as seguintes propriedades:

- $f_{ii} = 1_{P_i}$;
- $f_{ij} \circ f_{jk} = f_{ik}$, para todo $i \leq j \leq k$.

Seja $\pi_i : \Pi_{i\in I} P_i \to P_i$ um mapa restrição e seja $P = \{(P_i)_{i\in I} \in \Pi P_i | P_i = f_{ij}(P_j), i \leq j\}$. Diremos que P é o limite inverso dos $\{P_i\}_{i\in I}$ e denotamos por $\varprojlim P_i = P$. Dessa forma, o seguinte diagrama comuta



Seja $F(X)$ um grupo livre em X. Tome um subgrupo normal U de $F(X)$ tal que o grupo $F(X)/U$ seja finito e $F(X)/U$ seja um p-grupo. Então, $F_p(X) = \varprojlim F(X)/U$ e $F_p(X)$ é um p-grupo livre em X.

Definição 3.3. *A dimensão cohomológica de G é menor ou igual a n, denotada por $cd(G) \leq n$, se, e somente se, $H^r(G, A) = 0$ para todo $r > n$ e todo G-módulo de torsão A. O ínfimo m sobre todos os $n's$ tais que $cd(G) \leq n$ é dita a dimensão cohomológica de G e assim $cd(G) = m$.*

Proposição 3.2. *(Proposição 23 de [15]). Seja G um p-grupo e X um conjunto finito. Se $\phi : H^1(G, \mathbb{Z}/p\mathbb{Z}) \to \amalg_X \mathbb{Z}/\mathrm{p}\mathbb{Z}$ um homomorfismo de espaços vetoriais, então existe um homomorfismo de grupos correspondente $\pi : F_p(X) \to G$ tal que $H^1(\pi, \mathbb{Z}/p\mathbb{Z})$ é o mapa ϕ.*

Corolário 5. *Seja G um p-grupo e X finito é um conjunto. Se $H^1(G, \mathbb{Z}/p\mathbb{Z})$ tem uma base tal que sua dimensão é menor ou igual a $|X|$, então p-grupo G é um quociente de $F_p(X)$ para o conjunto X.*

Proposição 3.3. *(Proposição 24 de [15]) Seja G um p-grupo e $\sigma_1, \sigma_2, \cdots, \sigma_n$ um conjunto de elementos de G. As seguintes afirmações são equivalentes:*

1. *$\sigma_1, \sigma_2, \cdots, \sigma_n$ geram G.*
2. *O homomorfismo $F_p(X) \to G$ induzido por $\sigma_1, \sigma_2, \cdots, \sigma_n$, onde $\mid X \mid = n$, é sobrejetivo.*
3. *Os elementos $\overline{\sigma_1}, \overline{\sigma_2}, \cdots, \overline{\sigma_n}$ de G/G^* geram G/G^*.*
4. *Cada $\chi \in H^1(G, \mathbb{Z}/p\mathbb{Z})$ que se anula em $\sigma_j (j = 1, \cdots, n)$ é identicamente nulo.*

Corolário 6. *(Exemplo 2.5 de [3]). O número mínimo de geradores de G é a dimensão de $H^1(G, \mathbb{Z}/p\mathbb{Z})$.*

Definição 3.4. *Dado um grupo livre F a dimensão de $H^1(N, \mathbb{Z}/p\mathbb{Z})^{F/N}$ é denotadoa por $r_F(N)$, que representa o número minimal de elementos, $\tau_1, \ldots, \tau_n$, que podem gerar N como subgrupo normal de F.*

Definição 3.5. *Defina $h_i(G) = \dim H^i(G, \mathbb{Z}/p\mathbb{Z})$ para todo $i > 0$, e todo p-grupo finito G.*

Neste instante, denotaremos o p-grupo livre $F_p(X)$ por F.

Proposição 3.4. *(Proposição 26 de [15]) Se G é um p-grupo que é finitamente gerado, e se a sequência*

$$0 \to N \to F \to G \to 0 \tag{3.1}$$

é exata para algum conjunto finito X de cardinalidade n e N é um subgrupo normal em F, então $r_F(N)$ é finito, se e somente se, $h_2(G)$ é finito. Além disso, nesse caso, temos a equação

$$r_F(N) = n - h_1(G) + h_2(G).$$

Demonstração. A sequência inflação-restrição

$$0 \to H^1(F/N, \mathbb{Z}/p\mathbb{Z}^N) \overset{Inf}{\to} H^1(F, \mathbb{Z}/p\mathbb{Z}) \overset{Res}{\to} H^1(N, \mathbb{Z}/p\mathbb{Z})^{F/N} \to H^2(F/N, \mathbb{Z}/p\mathbb{Z}^N) \to H^2(F, \mathbb{Z}/p\mathbb{Z})$$

é uma sequência exata de espaços vetoriais sobre $\mathbb{Z}/p\mathbb{Z}$.

Sendo a sequência 3.1 exata, temos $F/N \simeq G$. E além disso, como a ação de N em $\mathbb{Z}/p\mathbb{Z}$ é trivial, então $n\overline{z} = \overline{z}$ para todo $n \in N$ e $\overline{z} \in \mathbb{Z}/p\mathbb{Z}$, isto é, $(\mathbb{Z}/p\mathbb{Z})^N = \mathbb{Z}/p\mathbb{Z}$. Temos que cd $G(F_p(X)) = 1$, ver referência Corolário 1, (capítulo III, de [15]) e com isso, $H^2(F, \mathbb{Z}/p\mathbb{Z}) = 0$. Assim, temos a sequência exata

$$0 \to H^1(G, \mathbb{Z}/p\mathbb{Z}) \overset{Inf}{\to} H^1(F, \mathbb{Z}/p\mathbb{Z}) \overset{Res}{\to} H^1(N, \mathbb{Z}/p\mathbb{Z})^{F/N} \to H^2(G, \mathbb{Z}/p\mathbb{Z}) \to 0.$$

Pela soma alternada das dimensões dos espaços vetoriais

$$h_1(G) - n + r_F(N) - h_2(G) = 0.$$

Logo, $r_F(N) = n - h_1(G) + h_2(G)$ e $r_F(N)$ é finito se, e somente se, $h_2(G)$ é finito. □

Corolário 7. *Seja G um p-grupo finito e finitamente gerado, e seja B é uma base para $H^1(G, \mathbb{Z}/p\mathbb{Z})$. Então na representação canônica*

$$0 \to N \to F_p(B) \to G \to 0,$$

o inteiro $r_F(N)$ é exatamente $h_2(G)$.

Demonstração. Suponha que a dimensão de B seja n, então $h_1(G) = n$. E por outro lado, a dimensão de $F_p(B)$ também é n.
Sendo $r_F(N) = n - h_1(G) + h_2(G)$, temos que $r_F(N) = h_2(G)$. Portanto, $h_2(G)$ é o número de relações entre qualquer conjunto mínimo de geradores que definem G. □

Definição 3.6. *O número inteiro definido por, $\sigma(G) = h_2(G) - h_1(G)$, é chamado de número de Shafarevich de G.*

Proposição 3.5. *(Proposição 27 de [15]). Para todo p-grupo G, o número de Shafarevich é não negativo. Além disso, $\sigma(G)$ é o posto de $H^3(G, \mathbb{Z})$, isto é, o número de fatores cíclicos de $H^3(G, \mathbb{Z})$.*

Demonstração. Considere a seguinte sequência exata

$$0 \to \mathbb{Z} \overset{p}{\to} \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z},$$

e aplicando a cohomologia temos a sequência exata longa

$$0 \to H^0(G, \mathbb{Z}) \overset{p}{\to} H^0(G, \mathbb{Z}) \to H^0(G, \mathbb{Z}/p\mathbb{Z}) \to H^1(G, \mathbb{Z}) \overset{p}{\to} H^1(G, \mathbb{Z}) \to H^1(G, \mathbb{Z}/p\mathbb{Z}) \to$$
$$H^2(G, \mathbb{Z}) \overset{p}{\to} H^2(G, \mathbb{Z}) \to H^2(G, \mathbb{Z}/p\mathbb{Z}) \to H^3(G, \mathbb{Z}) \overset{p}{\to} H^3(G, \mathbb{Z}) \to \cdots.$$

Como a ação de G em $\mathbb{Z}$ é trivial, então $H^1(G, \mathbb{Z}) = \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Z})$. E sendo G um p-grupo e $\mathbb{Z}$ é livre de torção, $\mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Z}) = 0$.
Considere $H^3(G, \mathbb{Z})_p = \mathrm{Ker}(H^3(G, \mathbb{Z}) \overset{p}{\to} H^3(G, \mathbb{Z}))$, e assim temos a sequência exata

$$0 \to H^1(G, \mathbb{Z}/p\mathbb{Z}) \to H^2(G, \mathbb{Z}) \overset{p}{\to} H^2(G, \mathbb{Z}) \to H^2(G, \mathbb{Z}/p\mathbb{Z}) \to H^3(G, \mathbb{Z})_p \to 0.$$

Note que $H^2(G,\mathbb{Z})$ é o dual de G/G'. Com isso, é um grupo finito. E pela exatidão da sequência, $H^3(G,\mathbb{Z})_p$ também é um grupo finito.

De modo análogo como temos a soma alternada das dimensões dos espaços vetoriais, temos o produto alternado das ordens dos grupos. E nesse caso, esse produto alternado é dado por

$$\frac{p^{h_1(G)} \cdot |H^2(G,\mathbb{Z})| \cdot p^t}{|H^2(G,\mathbb{Z})| \cdot p^{h_2(G)}} = 1$$

onde $t = \dim H^3(G,\mathbb{Z})_p$. Tomando o logarítimo na base p no produto acima, encontramos

$$\sigma(G) = h_2(G) - h_1(G) = t \geq 0.$$

E para finalizar, falta mostrar que t é o número de fatores cíclicos de $H^3(G,\mathbb{Z})$, isto é,
$t = \dim H^3(G,\mathbb{Z})_p =$ posto de $H^3(G,\mathbb{Z})$.
Suponha que $|G| = p^k$ para algum $k > 0$. Pelo corolário 4, $p^k H^3(G,\mathbb{Z}) = 0$ e isso implica que $H^3(G,\mathbb{Z})$ é um p-grupo abeliano. Tomando a decomposição de fatores cíclicos do grupo $H^3(G,\mathbb{Z})$ temos

$$H^3(G,\mathbb{Z}) = \langle \tau_1 \rangle \times \cdots \times \langle \tau_n \rangle$$

onde $\tau_i^{p^{\alpha_i}} = 1$ para todo $i = 1, \cdots, n$. Por outro lado, $pH^3(G,\mathbb{Z})_p = 0$ pois
$H^3(G,\mathbb{Z})_p = \mathrm{Ker}(H^3(G,\mathbb{Z}) \xrightarrow{p} H^3(G,\mathbb{Z}))$. Com isso, $H^3(G,\mathbb{Z})_p \subset H^3(G,\mathbb{Z})$ e a base de $H^3(G,\mathbb{Z})_p$ será

$$\{\tau_1^{p^{\alpha_1 - 1}}, \cdots, \tau_n^{p^{\alpha_n - 1}}\}.$$

Portanto, $\dim H^3(G,\mathbb{Z})_p =$ posto de $H^3(G,\mathbb{Z})$.
Voltando ao nosso caso, $\sigma(G) = t = \dim H^3(G,\mathbb{Z})_p =$ posto $H^3(G,\mathbb{Z})$. □

3.2 Grupos de Tate

Ao longo dessa seção G é um grupo finito.

Para todo G-módulo M, o mapa norma é definido por

$$\begin{aligned} \mathrm{Nm}_G : M &\to M \\ m &\mapsto \Sigma_{\sigma \in G} \sigma m. \end{aligned}$$

Tome $\sigma' \in G$ e sendo G fechado pela multiplição dos seus elementos, então

$$\sigma'(\mathrm{Nm}_G(m)) = \sigma' \Sigma_{\sigma \in G} \sigma m = \Sigma_{\sigma \in G} \sigma' \sigma m.$$

Como σ percorre todos os elementos de G, verifica-se que

$$\Sigma_{\sigma \in G} \sigma' \sigma m = \Sigma_{\sigma \in G} \sigma m = \mathrm{Nm}_G(m).$$

Com isso,

$$\sigma'(\mathrm{Nm}_G(m)) = \mathrm{Nm}_G(m) = \mathrm{Nm}_G(\sigma' m).$$

Através desse resultado, $\mathrm{Im}(\mathrm{Nm}_G) \subset M^G$.

Agora, mostraremos que $I_G M \subset \mathrm{Ker}(\mathrm{Nm}_G)$, onde I_G é o ideal de aumento. Assim, $I_G M = \{\sigma m - m | \sigma \in G, m \in M\}$. Tome $m' \in I_G M$, então

$$\mathrm{Nm}_G(m') = \mathrm{Nm}_G(\sigma m' - m') = \mathrm{Nm}_G(\sigma m') - \mathrm{Nm}_G(m') = 0.$$

Portanto, podemos tomar a sequência exata

$$0 \to \mathrm{Ker}(\mathrm{Nm}_G)/I_G M \xrightarrow{\iota} M/I_G M \overset{\mathrm{Nm}_G}{\to} M^G \xrightarrow{\pi} M^G/\mathrm{Nm}_G(M) \to 0.$$

Claramente, os mapas ι e π estão bem definidos. Para verificar que Nm_G está bem definido, tome $\overline{m} \in M/I_G M$ e assim,

$$\mathrm{Nm}_G(m + I_G M) = \mathrm{Nm}_G(m) + \mathrm{Nm}_G(I_G M) = \mathrm{Nm}_G(m).$$

O mapa fica bem definido pois $\mathrm{Im}(\mathrm{Nm_G}) \subset M^G$.

Sendo $H_0(G, M) = M/I_G M$ e $H^0(G, M) = M^G$, a sequência exata acima pode ser reestrita da seguinte maneira

$$0 \to \mathrm{Ker}(\mathrm{Nm}_G)/I_G M \xrightarrow{\iota} H_0(G, M) \overset{\mathrm{Nm}_G}{\to} H^0(G, M) \xrightarrow{\pi} M^G/\mathrm{Nm}_G(M) \to 0.$$

Defina os Grupos de Tate por:

$$\begin{aligned}
\widehat{H}^0(G, M) &= M^G/\mathrm{Nm}_G(M) \\
\widehat{H}^{-1}(G, M) &= \mathrm{Ker}(\mathrm{Nm}_G(M))/I_G M \\
\widehat{H}^{-n}(G, M) &= H_{n-1}(G, M) \text{ para } n \geq 2 \\
\widehat{H}^n(G, M) &= H^n(G, M) \text{ para } n \geq 0.
\end{aligned}$$

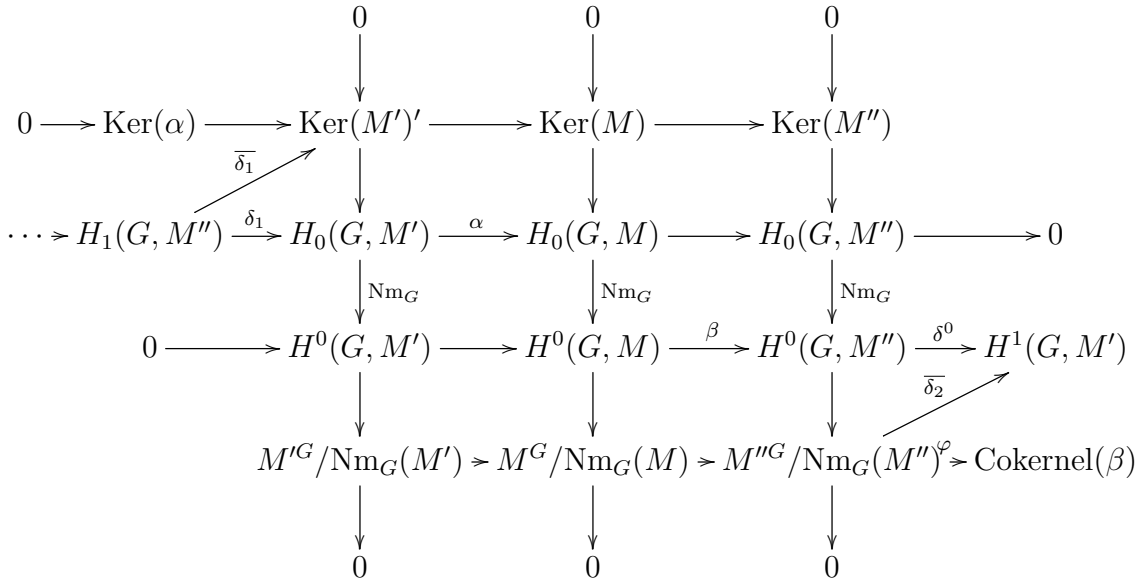
Dada qualquer sequência exata de G-módulos,

$$0 \to M' \to M \to M'' \to 0,$$

induz o seguinte diagrama comutativo

$$\begin{array}{ccccccccccc}
\cdots \longrightarrow & H_1(G, M'') & \longrightarrow & H_0(G, M') & \longrightarrow & H_0(G, M) & \longrightarrow & H_0(G, M'') & \longrightarrow & 0 & \\
 & & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & \downarrow{\scriptstyle \mathrm{Nm}_G} & & & \\
0 \longrightarrow & H^0(G, M') & \longrightarrow & H^0(G, M) & \longrightarrow & H^0(G, M'') & \longrightarrow & H^1(G, M') & \longrightarrow & \cdots &
\end{array}$$

Aplicando o Lema da Serpente na parte central desse diagrama e pelos resultados obtidos, temos o seguinte diagrama



onde $\mathrm{Ker}(M') = \mathrm{Nm}_G(M')/I_G M'$, e de modo análogo para $\mathrm{Ker}(M)$ e $\mathrm{Ker}(M'')$.

Agora, mostraremos que os mapas $\overline{\delta_1}$ e $\overline{\delta_2}$ estão bem definidos.

Primeiramente, observe que

$$\mathrm{Im}(\delta_1) = \mathrm{Ker}(\alpha) \subset \mathrm{Ker}(\mathrm{Nm}_G(M')) \subset H_0(G, M').$$

Com isso, $\overline{\delta}_1$ é o mapa induzido

$$\begin{array}{rcl} \overline{\delta}_1 : H_1(G, M'') & \to & \mathrm{Ker}(\mathrm{Nm}_G(M')) \\ \psi & \mapsto & \delta_1(\psi) \end{array}$$

e dessa forma, está bem definido.

Sendo o mapa φ sobrejetivo,

$$\mathrm{Im}(\varphi) = \mathrm{Coker}(\beta) = H^0(G, M'')/\mathrm{Im}(\beta).$$

E por outro lado, $\mathrm{Im}(\beta) = \mathrm{Ker}(\delta^0)$ e pelo Primeiro Teorema do Isomorfismo,

$$\mathrm{Im}(\varphi) = H^0(G, M'')/\mathrm{Ker}(\delta^0) \simeq H^1(G, M').$$

Assim, $\overline{\delta_2}$ é o mapa

$$\begin{array}{rcl} \overline{\delta_2} : M''^G/\mathrm{Nm}_G(M'') & \to & H^1(G, M') \\ \overline{m} & \mapsto & \delta^0(\overline{m}) \end{array}$$

induzido por δ^0 e por isso, está bem definido.

Portanto, com esses resultados, temos a sequência exata

$$\cdots \to \widehat{H}^{-n}(G, M'') \to \widehat{H}^{-n+1}(G, M') \to \widehat{H}^{-n+1}(G, M) \to \cdots \to \widehat{H}^0(G, M) \to \cdots \to$$
$$\to \widehat{H}^n(G, M'') \to \widehat{H}^{n+1}(G, M') \to \cdots .$$

Teorema 3.2. *(Teorema 17 de [15]). Seja A um G-módulo para um grupo finito G. Então existe um isomorfismo*

$$\widehat{H}^{r-1}(G, A^D) \simeq \widehat{H}^r(G, A)^D$$

onde $()^D$ significa o dual de Pontrjagin de $()$.

Teorema 3.3. *(Teorema 18 de [15]). Se G é um grupo finito, então existe um isomorfismo*

$$\widehat{H}^{-r}(G, \mathbb{Z}) \simeq \widehat{H}^r(G, \mathbb{Z})^D.$$

3.3 O Teorema de Golod-Shafarevich

Lema 3.2. *Seja G um p-grupo finito e A um G-módulo tal que $pA = 0$. Então as seguintes afirmações são equivalentes:*

(i) $A = 0$.

(ii) $H^0(G, A) = 0$

(iii) $H_0(G, A) = 0$

Demonstração. Claramente se $A = 0$, então $H^0(G, A) = H_0(G, A) = 0$. Para completar a demonstração considere os seguintes casos:

- $(ii) \to (i)$.

  Suponha que $A \neq 0$. Seja x um elemento não nulo de A e assim, o G-submódulo B de A gerado por x é finito de ordem p^k para algum k.

  Considere a ação de G em B dada por

  $$\begin{aligned} G \times B &\to B \\ (g, b) &\mapsto g \cdot b. \end{aligned}$$

  Com isso, temos a órbita da ação, $\mathrm{Orb}_G(b) = \{g \cdot b | g \in G\}$, e o estabilizador, $\mathrm{Stab}_G(b) = \{g \in G | g \cdot b = b\}$.

  Pelo Teorema da Órbita-Estabilizador, $[G : \mathrm{Stab}_G(b)] = |\mathrm{Orb}_G(b)|$ e assim, $|\mathrm{Orb}_G(b)| = p^{k_i}$, para todo $b \in B$ e para algum $k_i < k$. Além disso, $B = \amalg_{b \in B} \mathrm{Orb}_G(b)$.

  Suponha que G tenha apenas um ponto fixo, $b = 0$, então

  $$p^k = 1 + p^{k_1} + p^{k_2} + \cdots + p^{k_n}.$$

  Essa igualdade é um absurdo e só é válida quando G tem pelo menos p pontos fixos. Portanto, $H^0(G, A) = A^G \neq 0$.

- $(iii) \to (i)$

  Por hipótese, A é um G-módulo tal que $pA = 0$. Por meio disso, mostraremos que A pode ser visto como um espaço vetorial sobre $\mathbb{F}_p$. Para isso, considere o mapa

  $$\begin{aligned} \mathbb{F}_p \times A &\to A \\ (\overline{m}, a) &\mapsto m \cdot a. \end{aligned}$$

Para mostrar que esse mapa está bem definido, suponha que exista $m' \in \mathbb{Z}$ tal que $m' = m + pr$, para algum $r \in \mathbb{Z}$. Assim,

$$m'a = ma + pra = ma + rpa = ma$$

e esse mapa define a ação de $\mathbb{F}_p$ em A. Portanto, como $(a_1 + a_2) \in A$, para todo $a_1, a_2 \in A$ e $ma \in A$, para todo $m \in \mathbb{F}_p$, então A é um espaço vetorial sobre $\mathbb{F}_p$.

Agora, será mostrado que $\mathrm{Hom}_{\mathbb{F}_p}(A, \mathbb{F}_p) = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Z}_p)$, onde A é o definido acima. Tome $\varphi \in \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{Z}_p)$, então

$$\lambda\varphi(a) = \varphi(\lambda a) = \varphi(\overline{\lambda}a) = \overline{\lambda}\varphi(a)$$

para todo $\lambda \in \mathbb{Z}$ e $\overline{\lambda} \in \mathbb{F}_p$.

Diante desses resultados, seja $A' = \mathrm{Hom}_{\mathbb{Z}}(A, \mathbb{F}_p)$ é o dual de A, considerando como espaço vetorial sobre $\mathbb{F}_p$, isto é,

$$\begin{array}{rcl} A' \times A & \to & \mathbb{F}_p \\ (\varphi, a) & \mapsto & \varphi(a) \end{array}$$

onde φ é linear em cada argumento e não degenerada.

Já foi visto que,

$$H^0(G, A') = (A')^G = \mathrm{Hom}_G(A, \mathbb{F}_p).$$

Com isso, mostraremos que $H^0(G, A')$ é dual a $H_0(G, A) = A/IA$. Para isso, considere

$$\begin{array}{rcl} \mathrm{Hom}_G(A, \mathbb{F}_p) \times A/IA & \to & \mathbb{F}_p \\ (\varphi, \overline{a}) & \mapsto & \varphi(a). \end{array}$$

Pela dualidade entre A e A' temos que φ é linear, então falta mostrar que φ é não degenerada. Tome $(\sigma - 1)a \in IA$ e assim, $\varphi((\sigma - 1)a) = (\sigma - 1)\varphi(a) = \varphi(a) - \varphi(a) = 0$. Logo, o mapa $(\varphi, \overline{a}) \mapsto \varphi(a)$ está bem definido.

Por hipótese, $H_0(G, A) = 0$ e pela dualidade, $H^0(G, A') = 0$ e isso implica que $A' = 0$. Portanto, pela dualidade entre A e A', $A = 0$.

□

Lema 3.3. *(Lema 4.2 de [15]). Seja G um p-grupo finito e $\Lambda = \mathbb{Z}[G]$ o anel de grupo. Seja A um G-módulo com $pA = (0)$, $\Lambda/p\Lambda$ o anel de grupo sobre $\mathbb{Z}/p\mathbb{Z}$ e I o ideal de aumento de Λ. Então o número minimal de geradores de A como G-módulo é a dimensão de $H_0(G, A) = A/IA$. Isso significa que $a_1, \cdots, a_n$ geram A como G-módulo se, e somente se, $\overline{a_1}, \cdots, \overline{a_n}$ geram A/IA como espaço vetorial sobre $\mathbb{Z}/p\mathbb{Z}$.*

Demonstração. Claramente, se $a_1, \cdots, a_n$ geram A como G-módulo, então $\overline{a_1}, \cdots, \overline{a_n}$ geram A/IA como espaço vetorial sobre $\mathbb{Z}/p\mathbb{Z}$. Para provar a afirmação contrária, suponha que $\overline{a_1}, \cdots, \overline{a_n}$ geram A/IA como espaço vetorial sobre $\mathbb{Z}/p\mathbb{Z}$ e seja B um submódulo de A gerado pelas pré-imagens $a_1, \cdots, a_n$ em A. Considere a sequência exata

$$0 \to B \to A \to A/B \to 0$$

e tome sua sequência homológica

$$\cdots \to H_0(G,B) \to H_0(G,A) \to H_0(G,A/B) \to 0.$$

Observe que o mapa $H^0(G,B) \to H^0(G,A)$ definido por

$$\begin{array}{ccc} B/IB & \to & A/IA \\ \overline{a_1}, \cdots, \overline{a_n} & \mapsto & \overline{a_1}, \cdots, \overline{a_n} \end{array}$$

é, claramente, sobrejetivo. Pela exatidão em $H_0(G,A/B)$ e com o Primeiro Teorema do Isomorfismo, $H_0(G,A/B) = 0$. E pelo Lema 3.2, implica que $A/B = 0$, isto é, $A = B$. □

Lema 3.4. *(Lema 5.2 de [15]). Seja G um p-grupo finito e A um G-módulo com $pA = (0)$. Então existe uma resolução, isto é, uma sequência exata*

$$\cdots \to Y_3 \to Y_2 \to Y_1 \to Y_0 \to A \to 0$$

com as seguintes propriedades:

1. *Cada Y_n é livre sobre $\Lambda/p\Lambda$.*

2. *O número de geradores livres de Y_n sobre $\Lambda/p\Lambda$ é precisamente a dimensão de $H_n(G,A)$ sobre $\mathbb{Z}/p\mathbb{Z}$.*

3. *A imagem de Y_{n+1} em Y_n está contida em $I_G Y_n$.*

Demonstração. Suponha que dim $H^0(G,A) = d$, então pelo Lema 3.3 é o número minimal de geradores de A como G-módulo. Além disso, existe um Λ-módulo livre de posto d, X, tal que a sequência

$$X \to A \to 0$$

é exata. Seja Y_0 o cokernel do mapa $X \xrightarrow{p} X$, isto é, $Y_0 = X/pX$. Então Y_0 é um $\Lambda/p\Lambda$-módulo livre de posto d.

Agora mostraremos que $H_n(G,Y_0) = 0$ para $n \geq 1$. Tome a sequência exata

$$0 \to X \xrightarrow{p} X \to 0$$

e aplicando a homologia temos a sequência exata longa

$$\cdots \to H_{n+1}(X) \to H_{n+1}(Y_0) \to \cdots \to H_1(X) \to H_1(Y_0) \to H_0(X) \xrightarrow{p} H_0(X) \to H_0(Y_0) \to 0.$$

Como X é um Λ-módulo livre, então X é projetivo. Com isso, $H_n(X) = 0$ para todo $n > 0$ e a sequência acima é dada por

$$\cdots 0 \to H_{n+1}(Y_0) \to 0 \to \cdots 0 \to H_1(X) \to H_1(Y_0) \to H_0(X) \xrightarrow{p} H_0(X) \to H_0(Y_0) \to 0.$$

Isso implica que $H_n(Y_0) = 0$ para $n \geq 2$ e nos dá a sequência exata

$$0 \to H_1(X) \to H_1(Y_0) \xrightarrow{\iota} X/I_G X \xrightarrow{p} X/I_G X \to H_0(Y_0) \to 0. \tag{3.2}$$

Para mostrar que $H_1(Y_0) = 0$ observe que

$$X/I_GX = X \otimes_{\mathbb{Z}[G]} (\mathbb{Z}[G]/I_G) = X \otimes_{\mathbb{Z}[G]} \mathbb{Z}$$

e, sendo X um Λ-módulo de posto d e aplicando as propriedades produto tensorial temos

$$X/I_GX = X \otimes_{\mathbb{Z}[G]} \mathbb{Z} = \mathbb{Z}[G]^{\oplus d} \otimes_{\mathbb{Z}[G]} \mathbb{Z} = (\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} \mathbb{Z}) \oplus (\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} \mathbb{Z}) \oplus \cdots \oplus (\mathbb{Z}[G] \otimes_{\mathbb{Z}[G]} \mathbb{Z}).$$

Assim, $X/I_GX = \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z} = \mathbb{Z}^{\oplus d}$.

A exatidão da sequência 3.2 em X/I_GX implica que $\mathrm{Ker}\{X/I_GX \xrightarrow{p} X/I_G\} = \mathrm{Im}(\iota) = 0$ pois $X/I_GX = \mathbb{Z}^{\oplus d}$ é livre de torção. Como o mapa $H_1(Y_0) \to X/I_GX$ é injetivo, $H_1(Y_0) \simeq \mathrm{Im}(\iota) = 0$. Portanto, $H_1(Y_0) = 0$.

Seja $B = \mathrm{Ker}(Y_0 \to A)$ tal que a sequência

$$0 \to B \to Y_0 \to A \to 0.$$

é exata. Mostraremos que o mapa de $Y_0 \to A$ está bem definido. Para isso, seja $\varphi : X \to A$ e defina $\overline{\varphi} : X/pX \to A$ por $\overline{\varphi}(x + pX) = \varphi(x)$. Suponha que existe $x' \in X$ tal que $x' = x + px''$, isto é, $x' + pX = x + pX$. Assim,

$$\varphi(x') = \varphi(x) + \varphi(px'') = \varphi(x) + p\varphi(x'')$$

e sendo $\varphi(x'') \in A$ e $pA = 0$, $\varphi(x') = \varphi(x)$.

A sequência de homologia será

$$\cdots \to 0 \to H_{n+1}(A) \to H_n(B) \to \cdots \to 0 \to H_1(A) \to H_0(B) \to H_0(Y_0) \to H_0(A) \to 0 \quad (3.3)$$

pois $H_n(Y_0) = 0$ para todo $n \geq 1$. Com isso, $H_{n+1}(A) \simeq H_n(B)$ para todo $n \geq 0$.

Verificaremos que $H_0(Y_0) \simeq H_0(A)$. Note que $H_0(Y_0)$ é um espaço vetorial sobre $\mathbb{Z}/p\mathbb{Z}$. Para ver isso, basta observar que

$$Y_0 = X/pX = X \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} = \Lambda^{\oplus d} \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}$$

e por outro lado

$$Y_0/I_GY_0 = Y_0 \otimes_{\mathbb{Z}[G]} \mathbb{Z} = (\Lambda^{\oplus d} \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z}) \otimes_{\Lambda} \mathbb{Z} = (\Lambda^{\oplus d} \otimes_{\Lambda} \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}^{\oplus d} \otimes_{\mathbb{Z}} \mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z})^{\oplus d}.$$

Como visto, A também é um espaço vetorial de dimensão d sobre $\mathbb{Z}/p\mathbb{Z}$. Assim, sendo a sequência 3.3 exata, o mapa $H_0(Y_0) \to H_0(A)$ é sobrejetiva, e como a dimensão desses espaços são iguais, então $H_0(Y_0) \simeq H_0(A)$ como espaços vetoriais. Pelo Lema 3.3, $H_0(Y_0) \simeq H_0(A)$ como G-módulo. Portanto, o mapa

$$B/I_GB = H_0(B) \to H_0(Y_0) = Y_0/I_GY_0$$

é nulo e segue que $B \subseteq I_GY_0$.

Aplicaremos o mesmo procedimento acima para B. Observe que se $pY_0 = (0)$ então $pB = 0$. Com isso, obtemos o módulo livre Y_1 e a sequência exata

$$0 \to C \to Y_1 \to B \to 0.$$

Portanto, $H_n(C) \simeq H_{n+1}(B) \simeq H_{n+2}(A)$, para todo $n \geq 0$ e $C \subseteq I_GY_1$. De modo análogo, verifica-se que o módulo Y_1 tem posto igual a dimensão de $H_0(B)$ que por sua vez, tem a mesma dimensão de $H_1(A)$. Através do mapa $Y_1 \to Y_0$, obtemos por composição o mapa $Y_1 \to B \to Y_0$ cuja imagem é B que está contida em I_GY_0. Com isso, esse procedimento pode ser estendido por indução e assim temos o esperado resultado. □

Teorema 3.4. *(Golod-Shafarevich)(Teorema 19 de [15]) Seja G um p-grupo finito, então*

$$h_2(G) > 1/4h_1(G)^2.$$

Demonstração. Pelo teorema de dualidade da cohomologia de p-grupos aplicada no módulo $\mathbb{Z}/p\mathbb{Z}$ temos

$$\widehat{H}^{r-1}(G, \mathbb{Z}/p\mathbb{Z}) \simeq \widehat{H}^{-r}(G, \mathbb{Z}/p\mathbb{Z})^D.$$

Note que $(\mathbb{Z}/p\mathbb{Z})^D = (\mathbb{Z}/p\mathbb{Z})$, então a dimensão de $\widehat{H}^{r-1}(G, \mathbb{Z}/p\mathbb{Z})$ é a mesma de $\widehat{H}^{-r}(G, \mathbb{Z}/p\mathbb{Z})$. Tome $r = 2$ e assim,

$$h_1(G) = \dim\, \widehat{H}^{-2}(G, \mathbb{Z}/p\mathbb{Z}) = \dim\, H_1(G, \mathbb{Z}/p\mathbb{Z}),$$

e quando $r = 3$, temos

$$h_2(G) = \dim \widehat{H}^{-3}(G, \mathbb{Z}/p\mathbb{Z}) = \dim\, H_2(G, \mathbb{Z}/p\mathbb{Z}).$$

Dessa maneira, o teorema em questão consiste do comportamento da homologia de G com coeficientes em $\mathbb{Z}/p\mathbb{Z}$.

Agora aplicaremos o Lema 3.4 no G-módulo $\mathbb{Z}/p\mathbb{Z}$. Sendo a ação de G em $\mathbb{Z}/p\mathbb{Z}$ é trivial, $H_0(G, \mathbb{Z}/p\mathbb{Z}) = \mathbb{Z}/p\mathbb{Z}$ e assim, tem dimensão um sobre $\mathbb{Z}/p\mathbb{Z}$. Com isso, é possível encontrar Y_0 sobre $\Lambda/p\Lambda$ tal que o mapa $Y_0 \to \mathbb{Z}/p\mathbb{Z}$ é sobrejetivo cujo kernel está contido em $I_G Y_0$. Portanto, como espaços vetoriais sobre $\mathbb{Z}/p\mathbb{Z}$, os grupos $Y_0/I_G Y_0$ e $\mathbb{Z}/p\mathbb{Z}$ são isomorfos. E pelo Lema 3.3, $Y_0/I_G Y_0$ e $\mathbb{Z}/p\mathbb{Z}$ são isomorfos como G-módulos. Assim,

$$0 \to I_G Y_0 \to Y_0 \to \mathbb{Z}/p\mathbb{Z} \to 0$$

é uma sequência exata. Pelo Lema 3.4 a sequência

$$Y_2 \to Y_1 \to I_G Y_0 \to 0$$

é exata. Seja $Y_2 = R$, $Y_1 = D$, $Y_0 = E$, então R, D, E são $\Lambda/p\Lambda$-módulos de posto $h_2(G)$, $h_1(G)$ e 1 respectivamente. Logo, a sequência

$$R \to D \to I_G E \to 0 \tag{3.4}$$

é exata.

Agora, para um G-módulo finito A com $pA = (0)$, introduziremos o polinômio de Poincaré e para isso, considere o grupo graduado

$$gr(A) = \amalg_{n=0} I^n A/I^{n+1}A,$$

onde $I^n A/I^{n+1}A$ é $I^n/In + 1 \otimes_{\Lambda/p\Lambda} A$. Como visto, I/I^2 é isomorfo a G/G' e como p-grupos são solúveis, existe um inteiro N tal que $I^m A/I^{m+1}A = (0)$ para todo $m > N$. Os grupos $I^n A/I^{n+1}A$ são espaços vetoriais sobre $\mathbb{Z}/p\mathbb{Z}$. Defina $c_n(A)$ como a dimensão de $I^n A/I^{n+1}A$ sobre $\mathbb{Z}/p\mathbb{Z}$. O polinômio de Poincaré é dado por

$$\chi_A(t) = \Sigma_{n=0} c_n(A) t^n$$

Note que essa soma é finita pois $I^mA/I^{m+1}A = (0)$ para todo $m > N$.

Seja $\chi(t)$ igual a $\chi_E(t)$. Se F é um $\Lambda/p\Lambda$-módulo livre, então $\chi_F(t) = n\chi(t)$ pois dimensão de $Y_0 = E$ é igual a um. Assim, podemos deduzir que

$$\chi_D(t) = h_1(G)\chi(t); \quad \chi_R(t) = h_2(G)\chi(t).$$

Portanto, $c_0(E) = \dim E/IE = 1$, e $c_n(IE) = \dim I^n(IE)/I^{n+1}(IE) = \dim I^{n+1}E/I^{n+2}E$. Com isso, $c_n(IE) = c_{n+1}(E)$ e observe que

$$\chi_{IE}(t) = \Sigma_{n=0}c_{n+1}(E)t^n = c_1(E)t + c_2(E)t + c_3(E)t^2 + \cdots$$

e por outro lado

$$\frac{\chi(t)-1}{t} = \Sigma_{n=0}(\frac{c_n(E)t^n}{t}) - \frac{1}{t} = (\frac{1}{t} + c_1(E)t + c_2(E)t + c_3(E)t^2 + \cdots) - \frac{1}{t}.$$

Logo, $\chi_{IE}(t) = \frac{\chi(t)-1}{t}$.

Em particular, se $0 < t < 1$ é uma variável real, então

$$\chi_A(t)\frac{1}{1-t} = \chi_A(t)\Sigma_{j=0}t^j = \Sigma_{n=0}c_n(A)t^n\Sigma_{j=0}t^j.$$

E com algumas manipulações algébricas,

$$\chi_A(t)\frac{1}{1-t} = \Sigma_{r=0}(\Sigma_{n=0}c_n(A))t^r = \Sigma_{r=0}s_r(A)t^r,$$

onde $r = n + j$ e $s_r(A) = \Sigma_{n=0}c_n(A)$. Por isso,

$$s_r(A) = \dim\frac{A}{IA} + \dim\frac{IA}{I^2A} + \cdots + \dim\frac{I^rA}{I^{r+1}A}$$

e usando as somas altenardas das dimensões dos espaços vetoriais, $s_r(A) = \dim A/I^{n+1}A$ sobre $\mathbb{Z}/p\mathbb{Z}$. Suponha que $s_{-1}(A) = 0$, então

$$\chi_A(t)\frac{t}{1-t} = \Sigma_{r=0}s_{r-1}(A)t^r$$

Sendo a sequência 3.4 exata, o mapa $I^{n+1}D \to I^{n+2}E$ é sobrejetivo.

Seja R_{n+1} é a imagem inversa de I^{n+1} em D, isto é, $R_{n+1} = \varphi^{-1}(I^{n+1}D)$. Assim, a sequência

$$0 \to \frac{R}{R_{n+1}} \xrightarrow{\overline{\varphi}} \frac{D}{I^{n+1}D} \xrightarrow{\overline{\psi}} \frac{IE}{I^{n+2}E} \to 0$$

é exata. Para ver isso, defina o mapa $\overline{\varphi}(\overline{r}) = \varphi(r) + I^{n+1}D$ e note que está bem definido, pois ao tomar $r' = r + r''$, onde $r, r'' \in R$ e $r'' \in R_{n+1}$ temos $\varphi(r') + I^{n+1}D = (\varphi(r) + \varphi(r'')) + I^{n+1}D$, e sendo $\varphi(r'') \in I^{n+1}D$, $\varphi(r') + I^{n+1}D = \varphi(r) + I^{n+1}D$. De modo análogo, defina $\overline{\psi}(\overline{d}) = \psi(d)$ e verifica-se que está bem definido. Pela exatidão da sequência 3.4 $\mathrm{Ker}(\overline{\psi}) = \mathrm{Im}(\overline{\varphi})$ e ao tomar $\xi \in IE$, existe $d \in D$ tal que $\psi(d) = \xi$ e por definição, $\overline{\psi}(\overline{d}) = \psi(d) = \xi$. Logo, $\overline{\psi}$ é sobrejetivo. Para mostrar que $\overline{\varphi}$ é injetivo suponha que $\overline{\varphi} = 0$. Então, $\overline{\varphi}(\overline{r}) = \varphi(r) \in I^{n+1}D$ e assim, $r \in \varphi^{-1}(I^{n+1}D) = R_{n+1}$, isto é, $\overline{r} = \overline{0}$. Portanto,

$$s_n(D) = s_n(IE) + \dim_{\mathbb{Z}/p\mathbb{Z}}(R/R_{n+1})$$

Pelo Lema 3.4 a imagem de R está contida em ID, então a imagem de I^nR está contida em $I^{n+1}D$. Assim, $I^nR \subseteq R_{n+1}$ e com isso, a $\dim R/R_{n+1} \leq \dim R/I^nR = s_{n-1}(R)$. Dessa forma,

$$s_n(D) \leq s_n(IE) + s_{n-1}(R).$$

Voltando para a série de potência de Poincaré onde $0 < t < 1$ e pelos resultados anteriores

$$\chi_D(t)\frac{1}{1-t} \leq \chi_{IE}\frac{1}{1-t} + \chi_R(t)\frac{t}{1-t}.$$

Com isso,

$$h_1(G)\chi(t)\frac{1}{1-t} \leq \frac{\chi(t)-1}{t}\frac{1}{1-t} + h_2(G)\chi(t)\frac{t}{1-t}.$$

Assim, podemos deduzir a equação

$$1 \leq \chi(t)(1 - th_1(G) + t^2h_2(G)), \quad 0 < t < 1. \tag{3.5}$$

A equação 3.5 é chamada Lema de Golod. Sendo $\chi(t)$ uma função positiva para valores positivos de t, então

$$1 - th_1(G) + t^2h_2(G) > 0, \quad 0 < t < 1.$$

Como visto, $h_2(G) \geq h_1(G)$ e assim, $2h_2(G) > h_1(G)$ tal que $0 < \frac{h_1(G)}{2h_2(G)} < 1$.

Tomando $t = \frac{h_1(G)}{2h_2(G)}$ na inequação acima obtemos,

$$h_2(G) > 1/4(h_1(G))^2.$$

□

3.4 Aplicação do Teorema de Golod-Shafarevich

Para darmos uma aplicação do Teorema de Golod-Shafarevich, definiremos a álgebra polinomial não comutativa e enunciaremos o Teorema de Golod-Shafarevich para uma álgebra polinomial não comutativa. Posteriormente, mostraremos os dois contra exemplos que negam a conjectura de Burnside e também o problema de Kurosh-Levitzky.

Definição 3.7. *Seja F um corpo qualquer, $X = \{x_1, \cdots, x_n\}$ um conjunto finito e denote por $F\langle X\rangle = F\langle x_1, \cdots, x_d\rangle$ a F-álgebra associativa em X, isto é, a álgebra de polinômios nas variávies não comutativas $(x_1, \cdots, x_d)$ com coeficiente em F. Seja $F\langle X\rangle_n$ as componentes homogêneas de grau n de $F\langle X\rangle$ tal que $F\langle X\rangle = T_0 \oplus T_1 \oplus \cdots \oplus T_n \oplus \cdots$, onde $T_0 = F$, são as constantes, T_1 são todas as combinações F lineares de $x_1, \cdots, x_d$, T_2 são as combinações F lineares de todos os monônios quádricos e assim segue para todos os $F\langle X\rangle_n's$.*

Seja $F\langle X\rangle = F\langle x_1, \cdots, x_d\rangle$ uma álgebra polinomial não comutativa nas variáveis $x_1, \cdots, x_d$. Considere $R = \{f_1, f_2, \cdots\}$ um subconjunto de $F\langle X\rangle$. Seja $\mathfrak{A} = (f_1, f_2, \cdots)$ um ideal bilateral de $F\langle X\rangle$, gerado pelos elementos homogêneos de R de grau $2 \leq n_1 \leq n_2 \leq \cdots$, respectivamente.

Para cada $n \geq 2 \in \mathbb{N}$, r_n é o número de elementos de R que tem grau n.

Seja A uma F-álgebra dada por $A = F\langle X\rangle/\mathfrak{A}$.

Observe que o ideal $\mathfrak{A}$ é um ideal graduado, isto é, $\mathfrak{A} = \oplus\mathfrak{A}_n$ onde $\mathfrak{A}_n = \mathfrak{A} \cap F\langle X\rangle_n$. E além disso, A é uma álgebra graduada, $A = \oplus A_n$ onde $A_n = F_n\langle X\rangle_n/\mathfrak{A}_n$, $n \geq 0$.

Seja $b_n = \dim_F(A_n)$.

O teorema abaixo nos dá condições suficientes para que A tenha dimensão infinita sobre F.

Teorema 3.5. *(Golod-Shafarevich)(Teorema 8.1.1 de [8]). Para a álgebra A como descrita acima, considerando $n_i = \delta(f_i)$ o grau de cada polinômio homogêneo f_i e r_i o número de polinômios homogêneos de grau i, temos*

1. *$b_n \geq db_{n-1} - \Sigma_{n_i \leq n} b_{n-n_i}$ para $n \geq 1$.*
2. *Se para cada i $r_i \leq [(d-1)/2]^2$, então A tem dimensão infinita sobre F.*

Definição 3.8. *Seja A uma álgebra. Diremos que A é uma álgebra nilpotente se existe $m \in \mathbb{N}$ tal que $A^m = 0$, isto é, $a_1 \cdot \cdots \cdot a_m = 0$ para todo $a_i \in A$. E A é uma álgebra nil se para cada $a \in A$ existe $m \in \mathbb{N}$ tal que $a^m = 0$, ou seja, todo elemento de A é nilpotente.*

Usando os resultados do Teorema 3.5, o matemático Golod construiu uma álgebra nilpotente, que apesar de ser gerada por três elementos, tem dimensão infinita. Esse resultado foi o primeiro contra exemplo para o problema de Kurosh-Levitzki(1941)

Seja K um corpo. Suponha que A seja uma álgebra finitamente gerada sobre K e que seja uma nil álgebra. Então A tem dimensão finita?

Segue abaixo a construção feita por Golod que nega essa afirmação.

Teorema 3.6. *(Teorema 8.1.3 de [8]). Se F é qualquer corpo enumerável, então existe uma nil álgebra de dimensão infinita sobre F gerada por três elementos.*

Demonstração. Seja $T = F\langle x_1, x_2, x_3\rangle$ uma álgebra polinomial sobre F nas três variáveis não comutativas, x_1, x_2, x_3. Com isso, $T = F \oplus T_1 \oplus \cdots \oplus T_n \oplus \cdots$, onde os elementos de T_i são homogêneos de grau i.

O ideal $T' = T_1 \oplus \cdots \oplus T_n \oplus \cdots$ é contável e por isso, é possível enumerar os seus elementos $\{s_1, s_2, \cdots\}$.

Veremos agora como cada s_i é construído.

Tome $m_1 \geq 2$ e defina

$$s_1^{m_1} = s_{12} + s_{13} + \cdots + s_{1k_1},$$

onde $s_{1j} \in T_j$ e $m_1 \leq \delta(s_{1j}) < \delta(s_{1,j+1})$.

Suponha que $\delta(s_{1k_1}) = M$. Assim,

$$s_2^{M+1} = s_{2k_1+1} + \cdots + s_{2k_2}$$

onde $s_{2,j} \in T_j$ e $M \leq \delta(s_{2j}) < \delta(s_{2,j+1})$.

Esse processo é realizado para todo s_i e assim, teremos uma coleção de polinômios homogêneos s_{ij} onde cada s_{ij} tem grau maior ou igual a m_1. Além disso, para cada grau temos no máximo um polinômio.

Dessa maneira, temos a álgebra $A = \oplus A_i$ onde $A_i = \frac{T_i}{\mathfrak{A} \cap T_i}$ e $\mathfrak{A}$ um ideal de T gerado por $\{s_{ij}\}$.

Sendo $r_i = 1$ ou $r_i = 0$ para cada i, então $r_i \leq 1 \leq [(d-1)/2]^2$. Pelo Teorema 3.5 parte (ii), a álgebra A tem dimensão infinita sobre F.

Agora, considere a álgebra $B = T'/\mathfrak{A}$. Mostraremos que B é uma nil álgebra finitamente gerada e que tem dimensão infinita.

- $B = T'/\mathfrak{A}$ tem dimensão infinita.

  Como $\mathfrak{A} \subset T' \subset T$,

  $$0 \to T'/\mathfrak{A} \to T/\mathfrak{A} \to T/T'$$

  é uma sequência exata de espaços vetoriais e sendo T/T' de dimensão finita, então $T'/\mathfrak{A}$ tem dimensão infinita.

- $B = T'/\mathfrak{A}$ é finitamente gerada por $x_1 + \mathfrak{A}, x_2 + \mathfrak{A}, x_3 + \mathfrak{A}$.

- $B = T'/\mathfrak{A}$ é uma nil álgebra.

  Tome $b \in B$, então

  $$b = (f_1 + f_2 + \cdots + f_n) + \mathfrak{A},$$

  onde $f_i \in T_i$. Como o elemento b não tem termos constantes implica que f_i também não tem termos constantes para cada i. Assim, para cada f_i existe um $n_i \in \mathbb{N}$ tal que $f_i^{n_i} \in \mathfrak{A}$.

  Tome $N = \max\{n_i\}$, então

  $$b^N \in \mathfrak{A} \Rightarrow b^N = 0.$$

  Logo, B é uma nil álgebra.

□

A conjectura de Burnside (1911) era a seguinte

Se G é um grupo finitamente gerado com todo elemento de ordem finita, então G tem ordem finita?

E o seguinte resultado dado por Golod-Shafarevich é o primeiro contra exemplo que nega essa conjectura.

Teorema 3.7. *(Teorema 8.1.4 de [8]). Se p um número primo qualquer, existe um grupo G infinito, gerado por três elementos em que cada elemento de G tem ordem finita de potência de p.*

Demonstração. Seja F o corpo com p elementos e $T = F < x_1, x_2, x_3 >$ a álgebra polinomial sobre F nas variáveis não comutativas x_1, x_2, x_3. Considere $\mathfrak{A}$ o ideal de T construído na demonstração do Teorema 3.6 e assim, temos $A = T/\mathfrak{A}$ a álgebra polinomial não comutativa gerada pelos elementos de $x_1 + \mathfrak{A}, x_2 + \mathfrak{A}, x_3 + \mathfrak{A}$.

Considere G um monóide multiplicativo em A gerado por $1+a_1, 1+a_2, 1+a_3$, onde a_1, a_2, a_3 são elementos de $x_1+\mathfrak{A}, x_2+\mathfrak{A}, x_3+\mathfrak{A}$, respectivamente. Observe que, qualquer elemento em G é da forma $1+a$, onde $a \in T'/\mathfrak{A}$, então a é nilpotente. Diante disso, para um n suficientemente grande, $a^{p^n} = 0$ e assim, $(1+a)^{p^n} = 1 + a^{p^n} = 1$. Logo, $1 + a$ tem inverso em G e assim G é um grupo. Com isso, todo elemento de G tem ordem potência de p.

Suponha que G seja finito e assim, as combinações lineares dos seus elementos formam uma álgebra B de dimensão finita sobre F. Como $1, 1 + a_i$ são elementos de G então, $(1 + a_i) - 1 = a_i \in B$. Logo, $B = A$ contrariando o fato de A ter dimensão infinita. Portanto, G é um grupo infinito.

Portanto, com esse resultado Golod-Shafaverich mostraram que a conjectura de Burnside é falsa.

□

Referências Bibliográficas

[1] E. Artin, *Geometric Algebra*, Interscience Publishers, 1957.

[2] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley Publishing Company, Inc., 1969.

[3] J. W. S. Cassels, A. Fröhlich, *Algebraic Number Theory*, Academic Press, 1967.

[4] D. S. Dummit, R. M. Foote, *Abstract Albegra*, Jonh Wiley and Sons, Inc., 2004.

[5] I. Gelfand, Y. Manin, *Methods of Homological Algebra*, Encyclopaedia of Mathematical Sciences, Springer, 1988.

[6] R. Godement, *Algebra*, Hermann, 1968.

[7] E. S. Golod, I. R. Shafarevich, *On the class field tower*, Izv. Akad. Nauk. 28, 1964, 261-272.

[8] I. N Herstein, *Noncommutative rings*, The Mathematical Association of America, 1968.

[9] P.J. Hilton, U. Stammbach, *A course in Homological Algebra*, Graduate Texts in Mathematics, 1970.

[10] A. Knapp, *Basic Algebra*, Bizkhauser, 2006.

[11] A. Knapp, *Advanced Algebra*, Bizkhauser, 2007.

[12] H. Koch, *Algebric Number Theory*, Springer, 1988.

[13] J. Milne, *Class Field Theory*, Notas de Aula, disponíveis em www.jmilne.org.

[14] P. Roquette, *On class field towers*, in *Algebraic Number Theory*, J. Cassels and A. Fröhlich (eds), Academic Press, London, 1967.

[15] S. Schatz, *Profinite Groups, Arithmetic and Geometry*, Princeton University Press, 1972.

[16] A. Weibel, *An Introduction to Homological Albegra*, Cambridg University Press, 1994.

[17] E. Weiss, *Cohomology of Groups*, Academic Press, New York and London, 1969.