Alef Alves Fidelis

Cohomologia de grupos: da construção via resoluções à interpretação via derivações

Uberlândia - Minas Gerais, Brasil

2022

Alef Alves Fidelis

Cohomologia de grupos: da construção via resoluções à interpretação via derivações

Trabalho de conclusão de curso apresentado à Faculdade de Matemática como requisito parcial para obtenção do título de Licenciado em Matemática.

Universidade Federal de Uberlândia – UFU

Faculdade de Matemática – FAMAT

Licenciatura em Matemática

Orientadora: Francielle Rodrigues de Castro Coelho

Uberlândia - Minas Gerais, Brasil

2022

Ficha Catalográfica Online do Sistema de Bibliotecas da UFU
com dados informados pelo(a) próprio(a) autor(a).

F451
2022

Fidelis, Alef Alves, 2000-
Cohomologia de grupos [recurso eletrônico] : da construção via resoluções à interpretação via derivações / Alef Alves Fidelis. - 2022.

Orientadora: Francielle Rodrigues de Castro Coelho.
Trabalho de Conclusão de Curso (graduação) - Universidade Federal de Uberlândia, Graduação em Matemática.
Modo de acesso: Internet.
Inclui bibliografia.

1. Matemática. I. Coelho, Francielle Rodrigues de Castro,1981-, (Orient.). II. Universidade Federal de Uberlândia. Graduação em Matemática. III. Título.

CDU: 51

Bibliotecários responsáveis pela estrutura de acordo com o AACR2:
Gizele Cristine Nunes do Couto - CRB6/2091
Nelson Marcos Ferreira - CRB6/3074

Alef Alves Fidelis

Cohomologia de grupos: da construção via resoluções à interpretação via derivações

Trabalho de conclusão de curso apresentado à Faculdade de Matemática como requisito parcial para obtenção do título de Licenciado em Matemática.

Trabalho _____. Uberlândia, _____ de _____ de _____:

Francielle Rodrigues de Castro Coelho
Orientadora

Ariosvaldo Marques Jatobá
Examinador 1

Ligia Laís Fêmina
Examinador 2

Uberlândia - Minas Gerais, Brasil
2022

UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Faculdade de Matemática
Av. João Naves de Àvila, 2121, Bloco 1F - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: +55 (34) 3239-4158/4156/4126 - www.famat.ufu.br - famat@ufu.br

ATA DE DEFESA - GRADUAÇÃO

Curso de Graduação em:	Matemática				
Defesa de:	Trabalho de Conclusão de Curso 2 (GMA031)				
Data:	01/04/2022	Hora de início:	15h00min	Hora de encerramento:	16h35min
Matrícula do Discente:	11811MAT001				
Nome do Discente:	Alef Alves Fidelis				
Título do Trabalho:	Cohomologia de grupos: da construção via resoluções à interpretação via derivações.				
A carga horária curricular foi cumprida integralmente?	(x) Sim ( ) Não				

Em função da pandemia mundial e da DECISÃO DO COMITÊ DE MONITORAMENTO À COVID-19/UFU, DE 16 DE MARÇO DE 2020 a respeito da suspensão de aulas e atividades acadêmicas da UFU a partir de 18 de março de 2020, a defesa de Trabalho de Conclusão de Curso ocorreu virtualmente através da plataforma Microsoft Teams, presente no Office 365 Educacional e disponibilizado de forma gratuita pela Microsoft para toda comunidade da UFU.

Reuniu-se virtualmente, a Banca Examinadora assim composta pelos Professores: Dra. Ligia Laís Fêmina – FAMAT/UFU, Dr. Ariosvaldo Marques Jatobá – FAMAT/UFU e Dra. Francielle Rodrigues de Castro Coelho – FAMAT/UFU, orientador(a) do(a) candidato(a).

Iniciando os trabalhos, o(a) presidente da mesa, Dra. Francielle Rodrigues de Castro Coelho, apresentou a Comissão Examinadora e o candidato(a), agradeceu a presença do público, e concedeu ao discente a palavra, para a exposição do seu trabalho. A duração da apresentação do discente e o tempo de arguição e resposta foram conforme as normas do curso.

A seguir o(a) senhor(a) presidente concedeu a palavra, pela ordem sucessivamente, aos(às) examinadores(as), que passaram a arguir o(a) candidato(a). Ultimada a arguição, que se desenvolveu dentro dos termos regimentais, a Banca, em sessão secreta, atribuiu o resultado final, considerando o(a) candidato(a):

(X) Aprovado(a) Nota [100] (Somente números inteiros)

OU

( ) Aprovado(a) sem nota.

Nada mais havendo a tratar foram encerrados os trabalhos. Foi lavrada a presente ata que após lida e achada conforme foi assinada pela Banca Examinadora.

Documento assinado eletronicamente por **Ariosvaldo Marques Jatoba**, **Professor(a) do Magistério Superior**, em 01/04/2022, às 16:39, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Ligia Lais Femina**, **Professor(a) do Magistério Superior**, em 01/04/2022, às 16:43, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Francielle Rodrigues de Castro Coelho**, **Professor(a) do Magistério Superior**, em 01/04/2022, às 16:50, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3474691** e o código CRC **1CD49614**.

Referência: Processo nº 23117.000257/2022-73 SEI nº 3474691

A todos os matemáticos que vieram antes de mim, que possibilitaram a construção deste trabalho. A todos os matemáticos que virão depois de mim, que este trabalho sirva como parte de um alicerce para o desenvolvimento da Matemática.

Agradecimentos

Agradeço, primeiramente, a todo e qualquer brasileiro que já existiu, seja ele natural ou assimilado. Graças à força e ao sacrifício de milhões de pessoas no decorrer da história, tive a oportunidade de estar presente nesse tempo-espaço; fui capaz de ter acesso à alimentação, à transporte, à educação, à saúde, à segurança, entre outras coisas; fui contemplado com uma graduação gratuita e de qualidade, a qual pude concluir e exercer o papel no qual foi formado à exercer.

Também agradeço a todos os professores e pedagogos que estiveram envolvidos diretamente na minha formação, desde meus 3 anos de idade até os meus 21. Neste momento concluo minha graduação como um mosaico heterogêneo de diferentes contribuições, experiências, emoções, vivências de diversas pessoas que passaram pela minha trajetória acadêmica.

Agradeço à minha orientadora Francielle Rodrigues de Castro Coelho por estar ao meu lado desde abril de 2019. Foram muitas discussões, muitos estudos e muitas produções durante esse tempo, além das indignações, desabafos, conselhos e companheirismo.

Agradeço ao Programa de Educação Tutorial de Matemática da Universidade Federal de Uberlândia - *Campus* Santa Mônica por me propiciar conhecer minha orientadora e, juntamente ao PET-SESu-MEC, o fomento a pesquisa que desenvolvi em 2019, 2020 e 2021-1 e que faz parte deste trabalho. E ao CNPq pelo atual fomento a pesquisa que realizo que também faz parte deste trabalho.

Por fim, mas não menos importante, agradeço minha mãe Ana Lúcia por todos os sacrifícios que ela fez para eu concluir minha graduação. E aos meus amigos de graduação, especialmente ao Japa, Luís, Jeje, Aline, Samir, 16, Gabriela, Leonardo e Victor, que com o apoio fizeram com que eu repensasse o abandono do curso em diversos momentos.

"Transire suum pectus mundoque potiri"
(John Charles Fields)

Resumo

Neste trabalho abordamos alguns conceitos e resultados essenciais da álgebra homológica, como o conceito de módulos, homomorfismos entre módulos, módulos livres, módulos sobre o anel RG, sequências exatas e semiexatas (tratamos aqui dos complexos de cadeias, pois os complexos de cocadeias possuem resultados análogos), módulos de homomorfismos e módulos de projetivos. No estudo dos complexos de cadeias também abordamos as transformações de cadeias e a homotopia de cadeias, essenciais para mostrar a unicidade das resoluções livres e projetivas. Tivemos com esses conceitos iniciais da álgebra homológica o objetivo de construir as resoluções livres e projetivas e mostrar sua independência por meio de uma homotopia de cadeias. Também trouxemos, como exemplos, a resolução normal, a resolução bar e a resolução bar normalizada. Dada uma resolução, que é um complexo de cadeias, aplicando $\mathrm{Hom}_R(-, A)$ obtemos um complexo de cocadeias e assim construímos os grupos de cohomologia de um grupo G, a saber $H^n(G, A)$, com $n \in \mathbb{Z}$, os quais independem da escolha da resolução pois o functor da categoria dos módulos sobre RG na categoria dos grupos abelianos preserva homotopia de cadeias. Na sequência, fazemos uma relação dos n-ésimos grupos de cohomologia de G com seus grupos de (co)invariantes e fazemos alguns cálculos relacionando $H^n(G, A)$ com A^G e com A_G. Por fim, fazemos a interpretação de $H^1(G, A)$ via grupos de derivações e de derivações principais, e calculamos alguns casos especiais como, por exemplo, quando $G = \langle t \rangle \approx \mathbb{Z}$ é o grupo cíclico infinito e quando $G = \langle t \rangle \approx \mathbb{Z}_n$ é o grupo cíclico finito de ordem n, com $n \in \mathbb{Z}_+$.

Palavras-chaves: Módulos. Resoluções livres e projetivas. Cohomologia de grupos. Grupos de derivações e derivações principais.

Abstract

In this work we approach some essential concepts and results of homological algebra, such as the concept of modules, homomorphisms between modules, free modules, modules over the RG ring, exact and semi-exact sequences (we are dealing here with chains complexes, since the cochains complexes have similar results), homomorphism modules and projective modules. In the study of chain complexes, we also approach chain transformations and chain homotopy, essential to show the uniqueness of free and projective resolutions. With these initial concepts of homological algebra, we had the objective of building free and projective resolutions and showing their independence through a homotopy of chains. We also brought, as examples, the normal resolution, the bar resolution and the normalized bar resolution. Given a resolution, which is a chains complex, applying $\mathrm{Hom}_R(-, A)$ we get a cochains complex and thus we are able to construct the cohomology groups of a group G, namely $H^n(G, A)$, with $n \in \mathbb{Z}$, which does not depend on the choice of resolution since the functor of the category of modules over RG in the category of abelian groups preserves homotopy of chains. Next, we make a relation of the n-th cohomology groups of G with their groups of (co)invariants and we make some calculations relating $H^n(G, A)$ with A^G and with A_G. Finally, we perform the interpretation of $H^1(G, A)$ via derivation groups and main derivations, and we calculate some special cases, for example, when $G = \langle t \rangle \approx \mathbb{Z}$ is the infinite cyclic group and when $G = \langle t \rangle \approx \mathbb{Z}_n$ is the finite cyclic group of order n, with $n \in \mathbb{Z}_+$.

Key-words: Modules. Free and projective resolutions. Cohomology of groups. Derivation groups and main derivations.

Sumário

Introdução

Em relação à história da álgebra homológica, podemos afirmar que:

> O início de seu desenvolvimento se deu no século XIX com os trabalhos de Georg Friedrich Bernhard Riemann, em 1857, e de Enrico Betti, em 1871, sobre "números de homologia", além do desenvolvimento extremamente rigoroso de Jules Henri Poincaré, em 1895, na noção de números de homologia. Já em 1925, Amalie Emmy Noether deslocou a atenção da álgebra homológica para os "grupos de homologia" de um espaço e, durante a década de 1930, diversas técnicas algébricas foram desenvolvidas para os cálculos desses grupos. (WEIBEL, 2021, p.1, tradução nossa).

Já, entre os anos de 1940 e 1955, tivemos que:

> [...] essas técnicas da álgebra homológica, que foram originalmente desenvolvidas por motivações topológicas, eram aplicadas para a definição e exploração das homologias e das cohomologias de diversos sistemas algébricos: extensão e torção de grupos abelianos; homologia e cohomologia de grupos; álgebras de Lie; cohomologia de álgebras associativas; entre outros. Em adição à essas aplicações, Jean Leray introduziu as noções de feixes, cohomologia de feixes e sequências espectrais. (WEIBEL, 2021, p.1, tradução nossa).

Mas a álgebra homológica ainda vivenciaria uma drástica mudança que recebeu o nome de Revolução de Cartan-Eilenberg. Sobre isso podemos afirmar que:

> Logo o campo de pesquisa da álgebra homológica mudaria completamente graças a Élie Joseph Cartan e Samuel Eilenberg. O uso de functores derivados, definidos via resoluções injetivas, uniu todas as teorias homológicas anteriores. Assim, essa mudança de paradigmas na álgebra homológica ficou conhecida como Revolução de Cartan-Eilenberg, a qual, por exemplo, na busca por definições mais gerais dos functores derivados, surgiu as noções de categorias abelianas, enquanto que a busca por exemplos não triviais de módulos projetivos levou ao surgimento das álgebras sobre um corpo. (WEIBEL, 2021, p.1, tradução nossa).

A história da álgebra homológica ainda continua, agora com uma interpretação topológica dada por Witold Hurewicz, a qual relacionou os grupos de homologia com os grupos de homotopia de espaços asféricos. Depois Samuel Eilenberg e Saunders MacLane deram um tratamento as homologias com coeficientes em um grupo abeliano qualquer que está completamente determinado por coeficientes no anel dos números inteiros. Além disso, eles correlacionaram os grupos de homologia e cohomologia de complexos de cadeias de espaços topológicos, entre outras coisas.

Muitos matemáticos estão por trás dos trabalhos de Eilenberg-MacLane, isto é, contribuíram para a desenvolvimento deles, e muitos outros estão na frente dos seus

trabalhos, isto é, utilizaram a teoria construído por Eilenberg-MacLane para desenvolver ainda mais a álgebra homológica. Porém, aqui encerramos a breve história que trouxemos, pois é esta que tange nosso trabalho; ressaltamos que essa história é extensa e que produziu inúmeras outras bases para o estudo da cohomologia de grupos e de espaços topológicos, porém não as abrangeremos aqui. Para mais informações sobre a história da álgebra homológica, veja (WEIBEL, 2021).

Neste Trabalho de Conclusão de Curso, buscamos definir e explorar resultados na cohomologia de grupos, construídos via resoluções projetivas, assim como sua interpretação via grupos de derivações e derivações principais. Para tanto o trabalho está dividido em duas partes: I - Preliminares; e II - Resoluções e cohomologia de grupos.

Parte I - Preliminares: Nesta parte nosso enfoque foi em resultados essenciais da álgebra homológica, como os conceitos de módulos, homomorfismos entre módulos, módulos livres, módulos sobre o anel RG, sequências exatas e semiexatas (tratamos aqui dos complexos de cadeias, pois os complexos de cocadeias possuem resultados análogos), módulos de homomorfismos e módulos de projetivos. Vale ressaltar que esse conceitos, mesmo sendo básicos, formam a base para o estudo da cohomologia de grupos, pois definimos e exploramos as resoluções livres e projetivas com as ferramentas que contruímos nessa parte.

Parte II - Resoluções e cohomologia de grupos: Nesta parte nosso enfoque foi na construção e na exploração de resultados sobre resoluções livres e projetivas, além de mostrarmos a independência das resoluções via homotopia de cadeias; e por fim tratamos da cohomologia de grupos, a definimos por meio das resoluções projetivas, e damos uma interpretação para os grupos de cohomologia de alguns espaços por meio dos grupos de derivações e de derivações principais.

Este trabalho é fruto de duas iniciações científicas feita pelo autor em conjunto com a orientadora. Essas iniciações estiveram sobre vigência em 2020 e 2021, respectivamente, e tiveram os títulos Introdução à Teoria de Homotopia e à Teoria de Homologia Singular, e A Cohomologia de Grupos e os Espaços de Eilenberg-MacLane do tipo $(G, 1)$, respectivamente.

Parte I

Preliminares

1 Álgebra homológica

Neste capítulo trazemos alguns conceitos e resultados fundamentais da álgebra homológica. Nosso objetivo aqui é estabelecer bases para a construção das resoluções livres e projetivas, as quais serão usadas para construir os grupos de cohomologia de um grupo G. Para tanto, fizemos uso das referências (HU, 1968), (BROWN, 1992), (CASTRO, 2006) e (FIDELIS; COELHO, 2021).

1.1 Módulos

Nessa seção, consideraremos R sendo um anel comutativo arbitrário com identidade $1 \neq 0$.

Definição 1.1.1 (Módulo)**.** *Um módulo sobre R é um grupo abeliano arbitrário X, juntamente com uma função*

$$\mu\colon R \times X \longrightarrow X,$$

satisfazendo as seguintes condições:

1. *A função μ é bi-aditiva, isto é,*

$$\mu(\alpha+\beta, x) = \mu(\alpha, x) + \mu(\beta, x) \quad e \quad \mu(\alpha, x+y) = \mu(\alpha, x) + \mu(\alpha, y),$$

   para todos $\alpha, \beta \in R$ e todos $x, y \in X$;

2. *Para arbitrários $\alpha, \beta \in R$ e qualquer $x \in X$, temos*

$$\mu[\alpha, \mu(\beta, x)] = \mu(\alpha\beta, x);$$

3. *Para todo elemento $x \in X$, temos*

$$\mu(1, x) = x.$$

A função μ é chamada de multiplicação por escalar do módulo X. Para cada $\alpha \in R$ e cada elemento $x \in X$, o elemento $\mu(\alpha, x) \in X$ é chamado de produto escalar de x por α, e é denotado por αx. Assim, com essa notação podemos escrever as condições da Definição 1.1.1 da seguinte maneira:

1. Para todos $\alpha, \beta \in R$ e todos $x, y \in X$ vale

$$(\alpha+\beta)x = \alpha x + \beta x \quad \text{e} \quad \alpha(x+y) = \alpha x + \alpha y;$$

2. Para arbitrários $\alpha, \beta \in R$ e qualquer $x \in X$ vale

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

3. Para todo elemento $x \in X$ vale

$$1x = x.$$

Exemplo 1.1.2. *Tome R como sendo o anel dos números inteiros $\mathbb{Z}$. Para qualquer grupo abeliano X, a função*

$$\mu\colon \mathbb{Z} \times X \longrightarrow X$$

definida por

$$\mu(n, x) = nx,$$

para todo $n \in \mathbb{Z}$ e todo $x \in X$ satisfaz as condições para ser uma multiplicação por escalar. Portanto, qualquer grupo abeliano pode ser considerado como um módulo sobre o anel dos inteiros $\mathbb{Z}$.

De fato, a função μ é uma multiplicação por escalar. Analisando as condições da Definição 1.1.1, podemos constatar que:

1. A função μ é bi-aditiva, ou seja,

$$\mu(n + m, x) = (n + m)x = nx + mx = \mu(n, x) + \mu(m, x),$$

e

$$\mu(n, x + y) = n(x + y) = nx + xy = \mu(n, x) + \mu(n, y),$$

para todos $n, m \in \mathbb{Z}$ e todos $x, y \in X$;

2. Para arbitrários $n, m \in \mathbb{Z}$ e qualquer $x \in X$, temos

$$\mu[n, \mu(m, x)] = \mu(n, mx) = n(mx) = (nm)x = \mu(nm, x);$$

3. Para todo elemento $x \in X$, temos

$$\mu(1, x) = 1x = x.$$

Portanto, qualquer grupo abeliano pode ser considerado como um módulo sobre o anel dos inteiros $\mathbb{Z}$.

Lema 1.1.3. *Para qualquer elemento $u \in X$, com X sendo um módulo sobre R, temos*

$$0u = 0 \quad e \quad (-1)u = -u.$$

Demonstração. Pelas condições da Definição 1.1.1 temos

$$u + 0u = (1 + 0)u = 1u = u.$$

Isso implica que $0u = 0$ no grupo abeliano X. Por outro lado, temos

$$u + (-1)u = (1 - 1)u = 0u = 0.$$

Isso implica que $(-1)u = -u$ no grupo abeliano X ■

Definição 1.1.4 (Submódulo)**.** *Seja X um módulo sobre R. Um submódulo de X é um subconjunto não vazio $A \subset X$ o qual é, por si só, um módulo sobre R. Em outras palavras, um subconjunto não vazio $A \subset X$ é um submódulo de X se, e somente se, A é um subgrupo do grupo abeliano X e ele é estável com a multiplicação por escalar de X, isto é, $\alpha x \in A$ é verdade para todo $\alpha \in R$ e para todo $x \in A$.*

Exemplo 1.1.5. *Todo ideal I de um anel comutativo R com identidade 1 é um submódulo de R considerando-o como um módulo sobre si mesmo.*

De fato, o ideal I é um submódulo de R. Primeiro, todo ideal em um anel é um subconjunto não vazio do próprio anel. Agora, veja que:

1. Para todos $\alpha, \beta \in R$ e todos $x, y \in I$ vale

$$(\alpha + \beta)x = \alpha x + \beta x \quad \text{e} \quad \alpha(x + y) = \alpha x + \alpha y;$$

2. Para arbitrários $\alpha, \beta \in R$ e qualquer $x \in I$ vale

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

3. Para todo elemento $x \in I$ vale

$$1x = x.$$

Ou ainda, se considerarmos o Lema 1.1.6, temos que, para arbitrários $\alpha \in R$ e $x, y \in I$, $x + y \in I$ e $\alpha x \in I$, pela própria definição de ideal. Em qualquer uma das verificações, fica claro que I é um submódulo de R.

Lema 1.1.6. *Um subconjunto não vazio $A \subset X$, com X um módulo sobre R, é um submódulo de X se, e somente se, para elementos arbitrários $\alpha \in R$ e $u, v \in A$, temos $u + v \in A$ e $\alpha u \in A$.*

Demonstração. Pela Definição 1.1.4, a condição necessária é evidente, pois dado A um submódulo de X, ele é, por si só, um módulo sobre R. Logo, para elementos arbitrários $\alpha \in R$ e $u, v \in A$, temos $u + v \in A$ e $\alpha u \in A$.

Falta mostrar a suficiência da afirmação. Para isso, é suficiente mostrar que o inverso $-u$, de cada elemento $u \in A$, está em A. Isto segue de

$$-u = (-1)u \in A,$$

de acordo com o Lema 1.1.3. ■

Na demonstração anterior, de fato é suficiente mostrar que o inverso de cada elemento de A está em A. Com efeito, verifiquemos que A satisfaz as condições de módulo dadas na Definição 1.1.1.

1. Para todos $\alpha, \beta \in R$ e todos $u, v \in A$ vale

$$(\alpha + \beta)u = \alpha u + \beta u \quad \text{e} \quad \alpha(u + v) = \alpha u + \alpha v,$$

pois $\gamma u \in A$ e $u + v \in A$, com $\gamma \in R$ e $u, v \in A$ arbitrários, por hipótese;

2. Para arbitrários $\alpha, \beta \in R$ e qualquer $u \in A$ vale

$$\alpha(\beta x) = (\alpha\beta)x,$$

pois $\gamma u \in A$, para todo $\gamma \in R$, por hipótese;

3. Para todo elemento $u \in A$ vale

$$1u = u.$$

Agora, vamos considerar um submódulo arbitrário A de um módulo X sobre R. Como A é um subgrupo do grupo abeliano X, o grupo quociente

$$Q = X/A$$

é um grupo abeliano bem definido. Os elementos de Q são as classes laterais distintas de A em X.

Lema 1.1.7. *Se A é um submódulo de um módulo X sobre R, então, para todo elemento $\alpha \in R$ e todo $u \in X$, temos*

$$\{\alpha(u + a) |\, a \in A\} \subset \alpha u + A.$$

Demonstração. Como A é um submódulo de X, temos que $\alpha a \in A$, para todo $a \in A$. Portanto,

$$\alpha(u + a) = \alpha u + \alpha a \in \alpha u + A$$

vale para todo $a \in A$. ■

Como consequência imediata, a classe lateral $\alpha u + A$ depende somente do elemento $\alpha \in R$ e da classe $u + A$. Logo, podemos definir uma função

$$\mu \colon R \times Q \longrightarrow Q$$

dado por

$$\mu(\alpha, u + A) = \alpha u + A,$$

para todo elemento $\alpha \in R$ e toda classe lateral $u + A \in Q$.

É possível verificar que o grupo quociente

$$Q = X/A$$

se torna um módulo sobre R com μ sendo a multiplicação por escalar. Esse módulo Q é chamado de módulo quociente do módulo X pelo seu submódulo A.

Com efeito, verifiquemos que Q satisfaz as condições de módulo dadas na Definição 1.1.1.

1. Para todos $\alpha, \beta \in R$ e todos $u + A, v + A \in Q$ vale

$$\begin{aligned} \mu(\alpha + \beta, u + A) &= (\alpha + \beta)u + A \\ &= \alpha u + \beta u + A \\ &= \alpha u + A + \beta u + A \\ &= \mu(\alpha, u + A) + \mu(\beta, u + A) \end{aligned}$$

   e

$$\begin{aligned} \mu(\alpha, u + A + v + A) &= \alpha(u + A + v + A) \\ &= \alpha(u + v) + A \\ &= \alpha u + \alpha v + A \\ &= \alpha u + A + \alpha v + A \\ &= \mu(\alpha, u + A) + \mu(\alpha, v + A); \end{aligned}$$

2. Para arbitrários $\alpha, \beta \in R$ e qualquer $u + A \in Q$ vale

$$\begin{aligned} \mu(\alpha, \beta u + A) &= \alpha(\beta u) + A \\ &= (\alpha\beta)u + A \\ &= \mu(\alpha\beta, u + A); \end{aligned}$$

3. Para todo elemento $u + A \in Q$ vale

$$\mu(1, u + A) = 1u + A = u + A.$$

Lema 1.1.8. *A interseção de qualquer família de submódulos de um módulo sobre R é um submódulo de X.*

Demonstração. Vamos considerar uma família arbitrária

$$\varphi = \{A_j \subset X | j \in J\}$$

de submódulos de um módulo X sobre R. Seja A a interseção dessa família de submódulos, isto é,

$$A = \bigcap_{j \in J} A_j.$$

Para mostrar que A é um submódulo, sejam $\alpha \in R$ e $u, v \in A$. Considere um índice arbitrário $j \in J$. Como $A \subset A_j$, temos que $u, v \in A_j$. Como A_j é um submódulo de X, segue que

$$u + v \in A_j \quad \text{e} \quad \alpha u \in A_j.$$

E isto é verdade para todo $j \in J$. Assim, temos

$$u + v \in A \quad \text{e} \quad \alpha u \in A.$$

Portanto, pelo Lema 1.1.6, A é um submódulo de X. ■

Agora, seja S um subconjunto arbitrário de um módulo X sobre R. Então, S está contido em pelo menos um submódulo de X, o próprio X. Pelo Lema 1.1.8, a interseção A de todos os submódulos de X contendo S é um submódulo de X. De fato, A é o "menor" submódulo de X que contém o subconjunto S. Esse submódulo $A \subset X$ é chamado de submódulo gerado por S. No caso que $A = X$, dizemos que S é um conjunto de geradores de X e que X é gerado por S.

Definição 1.1.9 (Combinação linear)**.** *Um elemento de $x \in X$, onde X é um módulo sobre R, é uma combinação linear de elementos em um subconjunto $S \subset X$ se, e somente se, existe uma quantidade finita de elementos de S, digamos $x_1, \cdots, x_n$, tal que*

$$x = \sum_{i=1}^{n} \alpha_i x_i,$$

com $\alpha_i \in R$, para todo $i = 1, \cdots, n$.

Proposição 1.1.10. *O submódulo de um módulo X sobre R gerado por um conjunto S consiste de todas as combinações lineares dos elementos de S.*

Demonstração. Seja A o conjunto de todas combinações lineares dos elementos de S. Podemos verificar que A é um submódulo. Com efeito, sejam $\delta \in R$ e $u, v \in A$, onde $u = \sum_{i=1}^{n} \alpha_i u_i$ e $v = \sum_{j=1}^{m} \beta_j v_j$, com $\alpha_i, \beta_j \in R$ e $u_i, v_j \in S$, para todo $i = 1, \cdots, n$ e $j = 1, \cdots, m$.

Primeiro, verifiquemos que $u+v \in A$. Para isso, defina

$$\gamma_k = \begin{cases} \alpha_k, & \text{se } k = 1, \cdots, n, \\ \beta_k, & \text{se } k = n+1, \cdots, n+m, \end{cases}$$

e

$$w_k = \begin{cases} u_k, & \text{se } k = 1, \cdots, n, \\ v_k, & \text{se } k = n+1, \cdots, n+m, \end{cases}$$

Note que, pela definição de A, temos $\sum_{k=1}^{n+m} \gamma_k w_k \in A$. Com isso, temos

$$u+v = \sum_{i=1}^{n} \alpha_i u_i + \sum_{j=1}^{m} \beta_j v_j = \sum_{k=1}^{n} \alpha_k u_k + \sum_{k=n+1}^{n+m} \beta_k v_k = \sum_{k=1}^{n+m} \gamma_k w_k.$$

Portanto, $u+v \in A$.

Agora, verifiquemos que $\delta u \in A$. Para isso, defina $\alpha_i' = \delta\alpha_i$, para todo $i = 1, \cdots, n$. Note que $\alpha_i' \in R$, para todo $i = 1, \cdots, n$, e portanto, $\sum_{i=1}^{n} \alpha_i' u_i \in A$. Temos

$$\delta u = \delta\left(\sum_{i=1}^{n} \alpha_i u_i\right) = \sum_{i=1}^{n} (\delta\alpha_i) u_i = \sum_{i=1}^{n} \alpha_i' u_i.$$

Portanto, $\delta u \in A$.

Logo, pelo Lema 1.1.6, A é de fato um submódulo de X. Além disso, para todo $x \in S$, temos $x = 1x \in A$. Logo, $S \subset A$.

Por fim, seja B um submódulo qualquer de X contendo S. Então, toda combinação linear dos elementos de S está contida em B. Isto implica em $A \subset B$, ou seja, A é o menor submódulo de X contendo S. ■

Para quaisquer dois subconjuntos $S, T \subset X$, com X sendo um módulo sobre R, a soma $S+T$ é o subconjunto de X definido por

$$S+T = \{u+v \in X \,|\, u \in S \text{ e } v \in T\}.$$

Se S e T são submódulos de X, então a soma $S+T$ também é. De fato, para verificar isso, sejam $\alpha \in R$ e $u+v, w+z \in S+T$. Então,

$$(u+v)+(w+z) = (u+w)+(v+z) \in S+T$$

e

$$\alpha(u+v) = \alpha u + \alpha v \in S+T.$$

Portanto, pelo Lema 1.1.6, a soma $S+T$ é um submódulo de X.

Por outro lado, para qualquer subconjunto $C \subset R$, CS denota o subconjunto de X definido por

$$CS = \{\alpha u \in X \,|\, \alpha \in C \text{ e } u \in S\}.$$

1.2 Homomorfismos

Definição 1.2.1 (Homomorfismo de módulos)**.** *Um homomorfismo de um módulo X sobre R em um módulo Y sobre R é uma função*

$$f\colon X \longrightarrow Y,$$

a qual é um homomorfismo do grupo abeliano X com o grupo abeliano Y e que preserva a multiplicação por escalar. Em outras palavras, f é homomorfismo do módulo X com o módulo Y se, e somente se,

$$f(u+v) = f(u) + f(v)$$
$$f(\alpha u) = \alpha f(u),$$

para todo $\alpha \in R$ e todos $u, v \in X$.

Exemplo 1.2.2. *A função inclusão $i\colon A \longrightarrow X$ de um submódulo A de qualquer módulo X sobre R no módulo X é um homomorfismo do módulo A com o módulo X. Esse homomorfismo é chamado de homomorfismo inclusão.*

Verificaremos que a função inclusão é um homomorfismo. Para todo $\alpha \in R$ e todos $u, v \in A$,

$$i(u+v) = u + v = i(u) + i(v)$$
$$i(\alpha u) = \alpha u = \alpha i(u).$$

Portanto, por definição, a função inclusão é de fato um homomorfismo de módulos sobre R.

Exemplo 1.2.3. *Um caso particular do Exemplo 1.2.2 é a função identidade $id\colon X \longrightarrow X$ em um módulo arbitrário X sobre R. Esse homomorfismo é chamado de homomorfismo identidade.*

De fato, a função identidade é um caso particular da função inclusão, basta tomar o submódulo A sendo o próprio módulo X. Portanto, segue que a função identidade é um homomorfismo de módulos sobre R.

Proposição 1.2.4. *Para módulos arbitrários X, Y e Z sobre R, a composição $g \circ f\colon X \longrightarrow Z$, de quaisquer dois homomorfismos $f\colon X \longrightarrow Y$ e $g\colon Y \longrightarrow Z$, é um homomorfismo.*

Demonstração. Sejam $\alpha \in R$ e $u, v \in X$. Como f e g são homomorfismos, temos

$$\begin{aligned}(g \circ f)(u+v) &= g[f(u+v)] \\ &= g[f(u) + f(v)] \\ &= g[f(u)] + g[f(v)] \\ &= (g \circ f)(u) + (g \circ f)(v),\end{aligned}$$

e

$$\begin{aligned}(g \circ f)(\alpha u) &= g[f(\alpha u)] \\ &= g[\alpha f(u)] \\ &= \alpha g[f(u)] \\ &= \alpha[(g \circ f)(u)].\end{aligned}$$

■

Proposição 1.2.5. *Para qualquer homomorfismo $h\colon X \longrightarrow Y$ de um módulo X sobre R em um módulo Y sobre R, a imagem*

$$h(A) = \{h(x) \in Y \,|\, x \in A\}$$

de qualquer submódulo A de X é um submódulo de Y. E a imagem inversa

$$h^{-1}(B) = \{x \in X \,|\, h(x) \in B\}$$

de qualquer submódulo B de Y é um submódulo de X.

Demonstração. Para mostrarmos que $h(A)$ é um submódulo de Y, sejam $\alpha \in R$ e $u, v \in h(A)$. Pela definição de $h(A)$, existem elementos $c, d \in A$ tais que $h(c) = u$ e $h(d) = v$. Como A é um submódulo de X, segue do Lema 1.1.6 que $c + d \in A$ e $\alpha u \in A$. Como h é um homomorfismo, temos

$$u + v = h(c) + h(d) = h(c + d) \in h(A)$$

e

$$\alpha u = \alpha h(c) = h(\alpha c) \in h(A).$$

E isto mostra que $h(A)$ é um submódulo de Y.

Para mostrarmos que $h^{-1}(B)$ é um submódulo de X, sejam $\alpha \in R$ e $u, v \in h^{-1}(B)$. Pela definição de $h^{-1}(B)$, $h(u), h(v) \in B$. Como h é um homomorfismo e B é um submódulo de Y, temos

$$h(u + v) = h(u) + h(v) \in B$$

e

$$h(\alpha u) = \alpha h(u) \in B.$$

Pela definição de $h^{-1}(B)$, isto mostra que $u+v \in h^{-1}(B)$ e $\alpha u \in h^{-1}(B)$. Portanto, $h^{-1}(B)$ é um submódulo de X. ■

Se o submódulo A de X for o próprio módulo X, a imagem

$$\mathrm{Img}(X) = h(X)$$

é um submódulo de Y e será chamado de imagem do homomorfismo $h\colon X \longrightarrow Y$. Por outro lado, se o submódulo B de Y é o submódulo trivial 0 de Y, a imagem inversa

$$\mathrm{Ker}(h) = h^{-1}(0)$$

é um submódulo de X e será chamado de núcleo do homomorfismo $h\colon X \longrightarrow Y$. Finalmente, chamaremos de coimagem e de conúcleo do homomorfismo $h\colon X \longrightarrow Y$ os módulos quocientes

$$\mathrm{Coimg}(h) = X/\mathrm{Ker}(h) \quad \text{e} \quad \mathrm{Coker}(h) = Y/\mathrm{Img}(h)$$

dos módulos X e Y, respectivamente.

Um homomorfismo $h\colon X \longrightarrow Y$ de um módulo X sobre R em um módulo Y sobre R é dito um monomorfismo se, e somente se, ele é injetivo. Além disso, h é dito um epimorfismo se, e somente se, ele é sobrejetivo. Por fim, um homomorfismo bijetivo é um isomorfismo.

Definição 1.2.6 (Isomorfismo de módulos)**.** *Dois módulos X e Y sobre R são isomorfos, $X \approx Y$, se, e somente se, existir um isomorfismo $h\colon X \longrightarrow Y$. Um homomorfismo $h\colon X \longrightarrow X$ de um módulo X sobre R consigo mesmo é um endomorfismo de X. Endomorfismos bijetores são chamados de automorfismos.*

Note que automorfismos são casos particulares de isomorfismos.

Exemplo 1.2.7. *Temos que o homomorfismo inclusão é um monomorfismo, enquanto que seu caso particular, o homomorfismo identidade, é um automorfismo.*

De fato, pela definição do homomorfismo inclusão $i\colon A \longrightarrow X$ no Exemplo 1.2.2, segue que ele é um monomorfismo, ou seja, se tomarmos $x, y \in A$ com $x \neq y$, temos

$$i(x) = x \neq y = i(y).$$

Por outro lado, se considerarmos o homomorfismo identidade $id\colon X \longrightarrow X$, ele é um epimorfismo, ou seja, dado $x \in X$, temos que existe $x \in X$ tal que $id(x) = x$. Sendo um caso particular do homomorfismo inclusão, o homomorfismo identidade é um monomorfismo, e sendo um epimorfismo e um endomorfismo (por definição), segue que ele é um automorfismo.

Proposição 1.2.8. *Um homomorfismo $h\colon X \longrightarrow Y$ de um módulo X sobre R em um módulo Y sobre R é um monomorfismo se, e somente se,* $\mathrm{Ker}(h) = \{0\}$.

Demonstração. Necessidade: Assuma que $h\colon X \longrightarrow Y$ é um monomorfismo, isto é, um homomorfismo injetivo. Como h é um homomorfismo, ele leva o elemento $0 \in X$ no elemento $0 \in Y$. Portanto, o elemento $0 \in Y$ está contido no núcleo

$$\mathrm{Ker}(h) = h^{-1}(0)$$

de h. Como h é injetivo, a imagem inversa $h^{-1}(0)$ do elemento $0 \in Y$ não pode conter mais que um elemento de X. Isso implica que $\mathrm{Ker}(h) = \{0\}$.

Suficiência: Assuma $\mathrm{Ker}(h) = \{0\}$. Sejam $u, v \in X$ com $h(u) = h(v)$. Como h é um homomorfismo, temos

$$h(u - v) = h(u) - h(v) = 0.$$

Pela definição de $\mathrm{Ker}(h)$, isso implica que $u - v \in \mathrm{Ker}(h)$. Como $\mathrm{Ker}(h) = \{0\}$, temos $u - v = 0$. Logo, $u = v$. Assim, mostramos que h é injetivo, e portanto, um monomorfismo. ■

Proposição 1.2.9. *Um homomorfismo $h\colon X \longrightarrow Y$ de um módulo X sobre R em um módulo Y sobre R é um epimorfismo se, e somente se,* $\mathrm{Coker}(h) = 0$.

Demonstração. Necessidade: Assuma que $h\colon X \longrightarrow Y$ é um epimorfismo, isto é, um homomorfismo sobrejetivo. Como h é sobrejetivo temos $\mathrm{Img}(h) = h(X) = Y$. Isto implica que

$$\mathrm{Coker}(h) = Y/\,\mathrm{Img}(h) = 0.$$

Suficiência: Assuma $\mathrm{Coker}(h) = 0$. Então, temos $h(X) = \mathrm{Img}(h) = Y$. Isto implica que h é sobrejetor, e portanto, um epimorfismo. ■

Além disso, podemos constatar que a composição de dois monomorfismos é um monomorfismo, enquanto que a composição de dois epimorfismos é um epimorfismo. E, em particular, a composição de dois isomorfismos é um isomorfismo.

Com efeito, para verificar isso, sejam $f\colon X \longrightarrow Y$ e $g\colon Y \longrightarrow Z$ homomorfismos de módulos sobre R tais que:

i. f e g são monomorfismos:

   Mostremos que $g \circ f$ é um monomorfismo também. Para isso, tomemos $u, v \in X$ tal que $u - v \neq 0$. Temos

$$\begin{aligned}(g \circ f)(u - v) &= g[f(u - v)] \\ &= g[f(u) - f(v)] \\ &= g[f(u)] - g[f(v)] \\ &= (g \circ f)(u) - (g \circ f)(v),\end{aligned}$$

   onde $(g \circ f)(u) - (g \circ f)(v) \neq 0$, pois f e g são monomorfismos. Isto mostra, portanto, que $g \circ f$ é um monomorfismo.

ii. f e g são epimorfismos:

Mostremos que $g \circ f$ é um epimorfismo também, para isto mostremos que $\text{Coker}(g \circ f) = 0$. Como f e g são epimorfismos, temos $\text{Img}(f) = Y$ e $\text{Img}(g) = Z$. Logo, $\text{Img}(g \circ f) = Z$, e portanto

$$\text{Coker}(g \circ f) = Z/\,\text{Img}(g \circ f) = 0.$$

Mostrando assim que $g \circ f$ é um epimorfismo.

Proposição 1.2.10. *Se $h = g \circ f$ é a composição de dois homomorfismos $f\colon X \longrightarrow Y$ e $g\colon Y \longrightarrow Z$ de módulos sobre R, então as seguintes afirmações são verdadeiras:*

1. *Se h é um monomorfismo, então f também é;*
2. *Se h é um epimorfismo, então g também é.*

Demonstração. 1. Sejam $f(u), f(v) \in Y$, com $f(u) = f(v)$. Mostremos que $u = v$. Para isso, apliquemos g nos dois lados da igualdade $f(u) = f(v)$, obtendo

$$h(u) = (g \circ f)(u) = (g \circ f)(v) = h(v).$$

Como h é um monomorfismo, segue que $u = v$. Portanto, f é um monomorfismo também.

2. Seja $v \in Z$. Como h é um epimorfismo, então existe $u \in X$ tal que $h(u) = v$. Porém, como $h = g \circ f$, segue $(g \circ f)(u) = g[f(u)] = v$. Portanto, g é um epimorfismo também.

E isso mostra a veracidade das afirmações. ■

Sejam X e Y módulos arbitrários sobre R. Defina o homomorfismo $h\colon X \longrightarrow Y$ dado por

$$h(x) = 0,$$

para todo $x \in X$. Esse homomorfismo é chamado de homomorfismo trivial e o denotaremos por 0.

Proposição 1.2.11. *Para um homomorfismo arbitrário $h\colon X \longrightarrow Y$ de um módulo X sobre R em um módulo Y sobre R, as seguintes afirmações são equivalentes:*

(*i*) $h = 0$;

(*ii*) $\text{Img}(h) = 0$;

(*iii*) $\text{Ker}(h) = X$.

Demonstração. Nesta demonstração mostraremos que a afirmação (i) implica na afirmação (ii), que a afirmação (ii) implica na (iii) e, por fim, que a (iii) implica na (i).

Se (i), então (ii): Se h é o homomorfismo trivial, por definição temos $h(x) = 0$, para todo $x \in X$. Portanto, $h(X) = 0$, ou ainda, $\text{Img}(h) = 0$.

Se (ii), então (iii): Se $\text{Img}(h) = 0$, temos por definição que $h(X) = 0$. Portanto, $h^{-1}(0) = X$, ou ainda, $\text{Ker}(h) = X$.

Se (iii), então (i): Se $\text{Ker}(h) = X$, ou ainda, $h^{-1}(0) = X$, por definição temos $h(X) = 0$. Portanto, $h(x) = 0$, para todo $x \in X$, ou seja, h é o homomorfismo trivial. ■

Proposição 1.2.12. *A composição $h = g \circ f$ de dois homomorfismos $f\colon X \longrightarrow Y$ e $h\colon Y \longrightarrow Z$ de módulos sobre R é o homomorfismo trivial se, e somente se,*

$$\text{Img}(f) \subset \text{Ker}(g).$$

Demonstração. Necessidade: Assuma que $h = 0$. Seja $y \in \text{Img}(f)$. Por definição, existe um elemento $x \in X$ com $f(x) = y$. Então, temos

$$g(y) = g[f(x)] = h(x) = 0.$$

Portanto, $y \in g^{-1}(0) = \text{Ker}(g)$. Isto mostra a inclusão

$$\text{Img}(f) \subset \text{Ker}(g).$$

Suficiência: Assuma $\text{Img}(f) \subset \text{Ker}(g)$. Seja $x \in X$. Então, temos $h(x) = g[f(x)]$. Como

$$f(x) \in \text{Img}(f) \subset \text{Ker}(g),$$

obtemos $g[f(x)] = 0$. Portanto, $h(x) = 0$. Como x foi tomado arbitrariamente, mostramos que $h = 0$. ■

Dado um homomorfismo $f\colon X \longrightarrow Y$ de módulos sobre R, chamaremos f de homomorfismo de saída em X e de homomorfismo de entrada em Y.

Agora, vamos considerar um submódulo arbitrário A de um módulo X sobre R juntamente com o módulo quociente

$$Q = X/A.$$

A função $p\colon X \longrightarrow Q$ definida por

$$p(x) = x + A,$$

para todo $x \in X$, é chamada de projeção natural do módulo X sobre seu módulo quociente Q. Segue que p é um epimorfismo do grupo abeliano X no grupo abeliano Q. Com efeito, consideremos $x, y \in X$ e $\alpha \in R$, temos

$$p(x + y) = (x + y) + A = x + A + y + A = p(x) + p(y),$$

e

$$p(\alpha x) = (\alpha x) + A = \alpha(x + A) = \alpha p(x).$$

Portanto p é um homomorfismo; e, dado $x + A \in Q$, tome $x \in X$, então

$$p(x) = x + A$$

e portanto p é sobrejetor.

Além disso, temos

$$A = \mathrm{Ker}(p),$$

pela própria definição da função p. Logo, todo submódulo de X é o núcleo de algum homomorfismo.

Agora, vamos considerar módulos arbitrários X e Y sobre R juntamente com os submódulos $A \subset X$ e $B \subset Y$. Sejam,

$$X^* = X/A \quad \text{e} \quad Y^* = Y/B$$

os módulos quocientes com suas respectivas projeções naturais

$$p\colon X \longrightarrow X^* \quad \text{e} \quad q\colon Y \longrightarrow Y^*.$$

Considere um homomorfismo arbitrário

$$h\colon X \longrightarrow Y$$

do módulo X no módulo Y, o qual aplica A em B. A função $h'\colon A \longrightarrow B$ definida por

$$h'(a) = h(a),$$

para todo $a \in A$, é um homomorfismo do módulo A no módulo B. De fato, para todo $\alpha \in R$ e $a, a' \in A$, temos

$$h'(a + a') = h(a + a') = h(a) + h(a') = h'(a) + h'(a')$$

e

$$h'(\alpha a) = h(\alpha a) = \alpha h(a) = \alpha h'(a).$$

Esse homomorfismo h' é chamado de homomorfismo definido por h nos seus submódulos. Quando $B = Y$, h' é chamado de homomorfismo restrição de h no submódulo A de X e é denotado por

$$h|_A\colon A \longrightarrow Y.$$

Agora, seja $x \in X$. Como

$$h(x + a) = h(x) + h(a) \in h(x) + B,$$

para todo $a \in A$, a imagem $h(x + A)$ está contida em uma única classe lateral de B em Y, ou seja,

$$h(x + A) \subset h(x) + B.$$

Portanto, a correspondência $x + A$ com $h(x) + B$ define uma função

$$h^* \colon X^* \longrightarrow Y^*.$$

Segue que h^* é um homomorfismo do grupo abeliano X^* no grupo abeliano Y^*. Com efeito, consideremos $x + A, y + A \in X^*$, temos

$$\begin{aligned} h^*[(x + A) + (y + A)] &= h^*[(x + y) + A] \\ &= h(x + y) + B \\ &= h(x) + B + h(y) + B \\ &= h^*(x + A) + h^*(y + A). \end{aligned}$$

Além disso, como, para todo $\alpha \in R$ e todo $x + A \in X^*$, temos

$$h^*(\alpha x + A) = h(\alpha x) + B = \alpha h(x) + B = \alpha h^*(x + A),$$

segue que h^* é um homomorfismo do módulo X^* no módulo Y. Esse homomorfismo h^* é chamado de homomorfismo induzido por p nos seus módulos quocientes. Consequentemente, a relação comutativa

$$q \circ h = h^* \circ p$$

é válida.

De fato, consideremos as funções $q \circ h, h^* \circ p \colon X \longrightarrow Y^*$. Para todo $x \in X$, temos

$$(q \circ h)(x) = h(x) + B$$

e

$$(h^* \circ p)(x) = g^*(x + A) = h(x) + B.$$

Portanto, a relação comutativa $q \circ h = h^* \circ p$ é verdade.

Como consequência dessa relação comutativa, temos que

$$\begin{aligned} \mathrm{Img}(h^*) &= h^*(X^*) \\ &= h^*[p(X)] \\ &= (h^* \circ p)(X) \\ &= (q \circ h)(X) = q[h(X)] \\ &= q[\mathrm{Img}(h)]; \end{aligned}$$

e

$$\begin{aligned} x + A \in \operatorname{Ker}(h^*) &\iff h^*(x + A) = B \\ &\iff h(x) + B = B \\ &\iff h(x) \in B \\ &\iff x \in h^{-1}(B) \\ &\iff x + A \in p(h^{-1}(B)). \end{aligned}$$

Ou ainda, de forma resumida,

$$\operatorname{Img}(h^*) = q[\operatorname{Img}(h)] \quad \text{e} \quad \operatorname{Ker}(h^*) = p[h^{-1}(B)].$$

Em particular, se h é for um epimorfismo, $B = 0$ e $A = \operatorname{Ker}(h)$, então $Y^* \approx Y$, ou seja, Y^* é isomorfo à X, e h^* é um isomorfismo. Neste caso, temos a seguinte relação comutativa:

$$h^* \circ p = h.$$

Proposição 1.2.13. *Para um homomorfismo $h\colon X \longrightarrow Y$ de um módulo X sobre R em um módulo Y sobre R, temos*

$$\operatorname{Coimg}(h) = X/\operatorname{Ker}(h) \approx \operatorname{Img}(h).$$

Demonstração. Mostraremos que $h^*\colon X/\operatorname{Ker}(h) \longrightarrow h(X)$ dado por

$$h^*(x + \operatorname{Ker}(h)) = h(x),$$

para todo $x \in X$, é o isomorfismo desejado.

De fato, h^* é um homomorfismo. Para mostrarmos isso, seja $A = \operatorname{Ker}(h)$. Então,

$$\begin{aligned} h^*[(x + A) + (y + A)] &= h^*[(x + y) + A] \\ &= h(x + y) \\ &= h(x) + h(y) \\ &= h^*(x + A) + h^*(y + A), \end{aligned}$$

para quaisquer $x + A, y + A \in X/A$; e

$$h^*(\alpha x + A) = h(\alpha x) = \alpha h(x) = \alpha h^*(x + A),$$

para todo $\alpha \in R$ e todo $x + A \in X/A$.

Agora, tome $x + A \in X/A$, tal que

$$h^*(x + A) = 0.$$

Então, por definição, $h(x) = 0$, o que significa que $x \in A$. Logo, h^* é um monomorfismo.

Para mostrar a sobrejetividade de h^*, tome $y \in h(X)$. Então, $y = h(x)$, para algum $x \in X$. Logo, $x + A \in X/A$ é tal que

$$h^*(x + A) = h(x) = y.$$

Logo, h^* é um epimorfismo.

Sendo o homomorfismo h^* um monomorfismo e um epimorfismo, ele é um isomorfismo. ■

Teorema 1.2.14. *Para quaisquer dois submódulos A e B de um módulo X sobre R, o homomorfismo inclusão*

$$i\colon A \longrightarrow A + B$$

leva o submódulo $A \cap B \subset A$ no submódulo $B \subset A + B$ e ele induz um isomorfismo

$$i^*\colon A/(A \cap B) \longrightarrow (A + B)/B.$$

Demonstração. Como i é o homomorfismo inclusão, é imediato que ele leva o submódulo $A \cap B$ em B e, portanto, induz um homomorfismo

$$i^*\colon A/(A \cap B) \longrightarrow (A + B)/B.$$

Para mostrar que i^* é um monomorfismo, seja $a + A \cap B \in A/(A + B)$ tal que $i^*(a + A \cap B) = i(a) + B = B$. Isto implica que $i(a) \in A \cap B$. Logo, i^* é um monomorfismo.

Para mostrar que i^* é um epimorfismo, seja $(a + b) + B \in (A + B)/B$. Como $b \in B$, temos $(a + b) + B = a + B$. Assim,

$$i^*(a + A \cap B) = i(a) + B = a + B = (a + b) + B.$$

Logo, i^* é um epimorfismo.

Sendo o homomorfismo i^* um monomorfismo e um epimorfismo, ele é um isomorfismo. ■

1.3 Produtos diretos e somas diretas

Considere uma família

$$X = \{X_i |\, i \in J\}$$

de módulos X_i sobre R e denote por

$$P = \prod_{i \in J} X_i$$

o produto cartesiano dessa família X. Por definição, um elemento de P é uma função

$$f\colon J \longrightarrow \bigcup_{i \in J} X_i$$

do conjunto de índices J na reunião dos conjuntos X_i tal que $f(i) \in X_i$, para todo $i \in J$.

Defina uma operação binária em P tomando, para quaisquer dois elementos $f, g \in P$, a função $f + g\colon J \longrightarrow \bigcup_{i \in J} X_i$ definida como

$$(f + g)(i) = f(i) + g(i),$$

para todo índice $i \in J$. O conjunto P juntamente com a operação binária $+$ torna-se um grupo abeliano. O elemento nulo de P é a função $0\colon J \longrightarrow \bigcup_{i \in J} X_i$ definida por

$$0(i) = 0_i,$$

onde 0_i é o elemento nulo de X_i, para cada $i \in J$. O elemento inverso de $f \in P$ é a função $-f\colon J \longrightarrow \bigcup_{i \in J} X_i$ definida por

$$(-f)(i) = -[f(i)].$$

Defina uma multiplicação por escalar $\mu\colon R \times P \longrightarrow P$ associando a todo $\alpha \in R$ e todo $f \in P$ a função

$$\mu(\alpha, f) = \alpha f\colon J \longrightarrow \bigcup_{i \in J} X_i$$

dada por

$$(\alpha f)(i) = \alpha[f(i)],$$

para todo $i \in J$. É possível verificar que essa multiplicação por escalar torna o grupo abeliano P em um módulo sobre R.

Vamos verificar que P juntamente com μ torna-se um módulo sobre R. Temos:

1. A função μ é bi-aditiva, isto é,

   $$\mu(\alpha + \beta, f) = (\alpha + \beta)f = \alpha f + \beta f = \mu(\alpha, f) + \mu(\beta, f)$$

   e

   $$\mu(\alpha, f + g) = \alpha(f + g) = \alpha f + \alpha g = \mu(\alpha, f) + \mu(\alpha, g),$$

   para todos $\alpha, \beta \in R$ e todos $f, g \in P$;

2. Para arbitrários $\alpha, \beta \in R$ e qualquer $f \in P$, temos

   $$\mu[\alpha, \mu(\beta, f)] = \mu(\alpha, \beta f) = \alpha\beta f = \mu(\alpha\beta, f);$$

3. Para todo elemento $f \in P$, temos

$$\mu(1, f) = 1f = f.$$

Portanto, a multiplicação por escalar torna o grupo abeliano P em um módulo sobre R.

Definição 1.3.1 (Produto direto de módulos)**.** *O módulo P sobre R construído anteriormente é chamado de produto direto da família X de módulos X_i sobre R, com $i \in J$.*

Agora, vamos considerar o subconjunto $S \subset P$ o qual consiste de todos elementos $f \in P$ tais que $f(i) = 0$, exceto para uma quantidade finita de índices $i \in J$. Podemos verificar que S é um submódulo de P.

Com efeito, sejam $\alpha \in R$ e $f, g \in S$. Suponha que existem, respectivamente, n e m índices de J tal que f e g não se anulam neles. Então,

$$f + g \in S$$

pois existem no máximo $n + m$ índices tal que $f + g$ não se anula; e

$$\alpha f \in S$$

pois existem no máximo n índices tal que αf não se anula. Assim, pelo Lema 1.1.6, segue que S é um submódulo de P.

Definição 1.3.2 (Soma direta de módulos)**.** *O submódulo S construído anteriormente é chamado de soma direta da família X de módulos X_i sobre R, com $i \in J$.*

Denotamos essa soma direta por

$$S = \sum_{i \in J} X_i.$$

Note que, se o conjunto J é finito, então temos $P = S$. Neste caso, o módulo $P = S$ sobre R pode ser chamado tanto de produto direto quanto de soma direta da família X.

Para todo índice $j \in J$, defina uma função $d_j \colon X_j \longrightarrow S$ por

$$[d_j(x)](i) = \begin{cases} x, & \text{se } i = j, \\ 0, & \text{se } i \neq j, \end{cases}$$

para todo $x \in X_j$ e todo $i \in J$. Podemos verificar que d_j é um homomorfismo do módulo X_j no módulo S. De fato, para todo $\alpha \in R$, todos $x, y \in X_j$ e todo $i \in J$,

$$\begin{aligned} [d_j(x + y)](i) &= \begin{cases} x + y, & \text{se } i = j, \\ 0, & \text{se } i \neq j. \end{cases} \\ &= \begin{cases} x, & \text{se } i = j, \\ 0, & \text{se } i \neq j. \end{cases} + \begin{cases} y, & \text{se } i = j, \\ 0, & \text{se } i \neq j. \end{cases} \\ &= [d_j(x) + d_j(y)](i); \end{aligned}$$

e

$$\begin{aligned}[d_j(\alpha x)](i) &= \begin{cases} \alpha x, & \text{se } i = j, \\ 0, & \text{se } i \neq j. \end{cases} \\ &= \alpha \begin{cases} x, & \text{se } i = j, \\ 0, & \text{se } i \neq j. \end{cases} \\ &= \alpha[d_j(x)](i). \end{aligned}$$

Portanto, d_j é um homomorfismo.

Definição 1.3.3 (Injeção natural)**.** *O homomorfismo $d_j \colon X_j \longrightarrow S$ definido por*

$$[d_j(x)](i) = \begin{cases} x, & \textit{se } i = j, \\ 0, & \textit{se } i \neq j, \end{cases}$$

para todo $x \in X_j$ e todo $i \in J$, é chamado de injeção natural do módulo X_j na soma direta S.

Por outro lado, defina uma função $p_k \colon P \longrightarrow X_k$, para todo índice $k \in K$, por

$$p_k(f) = f(k),$$

para todo $f \in P$. Podemos verificar que p_k é um homomorfismo do módulo P no módulo X_k. De fato, para todo $\alpha \in R$, todos $f, g \in P$ e todo $k \in J$,

$$p_k(f + g) = (f + g)(k) = f(k) + g(k) = p_k(f) + p_k(g);$$

e

$$p_k(\alpha f) = (\alpha f)(k) = \alpha f(k) = \alpha p_k(f).$$

Portanto, p_k é um homomorfismo.

Definição 1.3.4 (Projeção natural)**.** *O homomorfismo $p_k \colon P \longrightarrow X_k$ definido por*

$$p_k(f) = f(k)$$

para todo $f \in P$ e todo $k \in J$, é chamado de projeção natural do produto direto P no módulo X_k.

Proposição 1.3.5. *Considere $i \colon S \longrightarrow P$ o homomorfismo inclusão. A composição*

$$p_k \circ i \circ d_j \colon X_j \longrightarrow X_k$$

é o homomorfismo trivial se $j \neq k$ e é o homomorfismo identidade se $j = k$.

Demonstração. Temos que, para todo $x \in X_j$,

$$(p_k \circ i \circ d_j)(x) = (p_k \circ i)([d_j(x)](i)) = p_k([d_j(x)](i)) = [d_j(x)](k),$$

com $i \in J$. Com isso, se $j \neq k$, então

$$[d_j(x)](k) = 0$$

e, portanto, $p_k \circ i \circ d_j$ é o homomorfismo trivial. Enquanto que, se $j = k$,

$$[d_j(x)](k) = x$$

e, portanto, $p_k \circ i \circ d_j$ é o homomorfismo identidade. ■

Corolário 1.3.6. *Para todo $j \in J$, a injeção natural*

$$d_j \colon X_j \longrightarrow S$$

do módulo X_j na soma direta S é um monomorfismo.

Demonstração. Suponha que $d_j(x) = 0$. Temos que $d_j(x) = 0$ implica que $[d_j(x)](i) = 0$, para todo $i \in J$. Em particular, para $i = j$, temos

$$\begin{aligned} 0 &= [d_j(x)](j) \\ &= x, \end{aligned}$$

como queríamos. ■

Logo, podemos identificar cada módulo X_j com sua imagem $d_j(X_j) \subset S$ e considerar X_j como um submódulo da soma direta S. Após fazer isso, $d_j \colon X_j \longrightarrow S$ torna-se o homomorfismo inclusão e S é gerado pela união de todos $X_j \subset S$.

Corolário 1.3.7. *Para todo $k \in J$, a projeção natural*

$$q_k \colon S \longrightarrow X_k$$

da soma direta S no módulo X_k é um epimorfismo.

Demonstração. Seja $x_k \in X_k$. Defina a função $f \colon J \longrightarrow S$ por

$$f(i) = \begin{cases} x_k & \text{se } i = k, \\ 0 & \text{se } i \neq k. \end{cases}$$

Temos que

$$\begin{aligned} q_k(f) &= (p_k \circ i)(f) \\ &= p_k(i(f)) \\ &= p_k(f) \\ &= f(k) \\ &= x_k. \end{aligned}$$

Logo, q_k é um epimorfismo. ■

Para todo $k \in J$, seja Y_k a união de todos os submódulos

$$\mathrm{Img}(d_j) = d_j(X_j)$$

da soma direta S, com $j \neq k$.

Proposição 1.3.8. *Para todo $k \in J$, o núcleo $\mathrm{Ker}(q_k)$ da projeção natural $q_k \colon S \longrightarrow X_k$ é o submódulo da soma direta S gerado pelo subconjunto Y_k.*

Demonstração. Seja $f \in A$, onde A é o submódulo S gerado por Y_k. Então, f é uma combinação linear dos elementos de Y_k em S. Pela Definição 1.1.9. existe uma quantidade finita de elementos de Y_k tal que

$$\sum_{i=1}^{n} \alpha_i f_i,$$

com $\alpha_i \in R$ e $f_i \in Y_k$, para todo $i = 1, \cdots, n$. Segue da definição do conjunto Y_k que, para todo $i = 1, \cdots, n$, existe um índice $j_i \neq k$ e um elemento $x_i \in X_j$ tal que

$$f_i = d_{j_i}(x_i).$$

Consequentemente, obtemos

$$q_k(f) = \sum_{i=1}^{n} \alpha_i q_k(f_i) = \sum_{i=1}^{n} \alpha_i [(q_k \circ d_{j_i})(x_i)] = 0,$$

pois $j_i \neq k$, para todo $i = 1, \cdots, n$. Isto mostra que $f \in \mathrm{Ker}(q_k)$. Como $f \in A$ é um elemento arbitrário, temos $A \subset \mathrm{Ker}(q_k)$.

Agora, mostraremos que $\mathrm{Ker}(q_k) \subset A$.

Seja $f \in \mathrm{Ker}(q_k)$. Então, por definição, $q_k(f) = f(k) = 0$. Como $\mathrm{Ker}(q_k) \subset S$, temos que $f \in S$, e isso significa que existe uma quantidade finita de índices de J tal que

$$f(j_i) \neq 0,$$

para $i = 1, \cdots, n$.

Defina uma função $g \colon J \longrightarrow \bigcup_{i \in J} X_i$ por

$$g(l) = \sum_{i=1}^{n} [d_{j_i}(f(j_i))](l),$$

para todo $l \in J$. Note que $g \in S$, pois, para $l \in \{j_i \in J | \, i = 1, \cdots, n\}$, temos

$$g(l) = f(l) \neq 0,$$

enquanto que, para $l \notin \{j_i \in J | \, i = 1, \cdots, n\}$, temos

$$g(l) = 0.$$

Além disso, $g \in \mathrm{Ker}(q_k)$, pois $k \notin \{j_i \in J | \, i = 1, \cdots, n\}$.

Como $d_{j_i}(f(j_i)) \in d_{j_i}(X_j)$, g é uma combinação linear dos elementos da imagem de d_{j_i}, para $j_i \neq k$. Portanto, $g \in A$, por definição, mostrando assim que $\mathrm{Ker}(q_k) \subset A$. ■

Como consequência imediata da Proposição 1.3.8, temos que o submódulo $\mathrm{Ker}(q_k) \subset S$ é isomorfo à soma direta da família de módulos

$$X - X_k = \{X_i | \, i \in J - \{k\}\}.$$

Agora, com $X = X_i$, para todo $i \in J$, defina as função $\delta \colon X \longrightarrow P$ por

$$[\delta(x)](i) = x,$$

para todo $x \in X$ e todo $i \in J$. Podemos verificar que δ é um homomorfismo do módulo X no produto direto P. De fato, para todo $\alpha \in R$ todos $x, y \in X$ e todo $i \in J$,

$$[\delta(x+y)](i) = x + y = [\delta(x)](i) + [\delta(y)](i);$$

e

$$[\delta(\alpha x)](i) = \alpha x = \alpha[\delta(x)](i).$$

Portanto, δ é um homomorfismo.

Definição 1.3.9 (Homomorfismo diagonal)**.** *O homomorfismo $\delta \colon X \longrightarrow P$ definido por*

$$[\delta(x)](i) = x,$$

para todo $x \in X$ e todo $i \in J$, é chamado de homomorfismo diagonal do módulo X no produto direto P.

Também com $X = X_i$, para todo $i \in J$, defina a função $\sigma \colon S \longrightarrow X$ por

$$\sigma(f) = \sum_{i \in J} f(i),$$

para todo $f \in S$. Podemos verificar que σ é um homomorfismo da soma direta S no módulo X. De fato, para todo $\alpha \in R$ e todos $f, g \in X$,

$$\sigma(f+g) = \sum_{i \in J} (f+g)(i) = \sum_{i \in J} f(i) + \sum_{i \in J} g(i) = \sigma(f) + \sigma(g);$$

e

$$\sigma(\alpha f) = \sum_{i \in J} \alpha f(i) = \alpha \sum_{i \in J} f(i) = \alpha\sigma(f).$$

Portanto, σ é um homomorfismo.

Definição 1.3.10 (Homomorfismo soma)**.** *O homomorfismo $\sigma \colon S \longrightarrow X$ definido por*

$$\sigma(f) = \sum_{i \in J} f(i),$$

para todo $f \in S$, é chamado de homomorfismo soma da soma direta S no módulo X.

Agora, vamos considerar uma família de homomorfismos de módulos sobre R

$$H = \{h_i \colon X_i \longrightarrow Y_i |\, i \in J\}.$$

Defina uma função $\varphi \colon \prod_{i \in J} X_i \longrightarrow \prod_{i \in J} Y_i$ por

$$[\varphi(f)](i) = h_i[f(i)],$$

para todo $f \in \prod_{i \in J} X_i$ e todo $i \in J$. Podemos verificar que φ é um homomorfismo de módulos sobre R. De fato, para todo $\alpha \in R$, todos $f, g \in X$ e todo $i \in J$,

$$\begin{aligned}[\varphi(f+g)](i) &= h_i[(f+g)(i)] \\ &= h_i[f(i) + g(i)] \\ &= h_i[f(i)] + h_i[g(i)] \\ &= [\varphi(f)](i) + [\varphi(g)](i);\end{aligned}$$

e

$$[\varphi(\alpha f)](i) = h_i[\alpha f(i)] = \alpha h_i[f(i)] = \alpha[\varphi(f)](i).$$

Portanto, φ é um homomorfismo.

Definição 1.3.11 (Produto direto de homomorfismos)**.** *O homomorfismo* $\varphi \colon \prod_{i \in J} X_i \longrightarrow \prod_{i \in J} Y_i$ *definido por*

$$[\varphi(f)](i) = h_i[f(i)],$$

para todo $f \in \prod_{i \in J} X_i$ *e todo* $i \in J$*, é chamado de produto direto dos homomorfismos da família* $H = \{h_i \colon X_i \longrightarrow Y_i |\, i \in J\}$.

Esse produto direto de homomorfismos será denotado por

$$\varphi = \prod_{i \in J} h_i.$$

Além disso, por sua definição, segue que

$$\varphi\left(\sum_{i \in J} X_i\right) \subset \sum_{i \in J} Y_i.$$

Portanto, o homomorfismo φ define um outro homomorfismo

$$\psi \colon \sum_{i \in J} X_i \longrightarrow \sum_{i \in J} Y_i.$$

Definição 1.3.12 (Soma direta de homomorfismos)**.** *O homomorfismo* $\psi \colon \sum_{i \in J} X_i \longrightarrow \sum_{i \in J} Y_i$ *de módulos sobre* R *é chamado de soma direta dos homomorfismos da família* $H = \{h_i \colon X_i \longrightarrow Y_i |\, i \in J\}$.

Essa soma direta de homomorfismos será denotado por

$$\psi = \sum_{i \in J} h_i.$$

Note que, se o conjunto J for finito, então $\varphi = \psi$. Neste caso, o homomorfismo $\varphi = \psi$ pode ser chamado tanto de produto direto ou soma direta, ambos dos homomorfismos da família H.

No caso $X = X_i$, para todo $i \in J$, temos

$$X \xrightarrow{\delta} \prod_{i \in J} X_i \xrightarrow{\varphi} \prod_{i \in J} Y_i,$$

onde δ é o homomorfismo diagonal.

Definição 1.3.13 (Produto direto restrito de homomorfismos)**.** *A composição dos homomorfismos φ e δ da forma*

$$\varphi \circ \delta \colon X \longrightarrow \prod_{i \in J} Y_i$$

é chamado de produto direto restrito dos homomorfismos da família $H = \{h_i \colon X_i \longrightarrow Y_i | \, i \in J\}$.

Note que $\varphi \circ \delta$ é de fato um produto direto de homomorfismos. Para ver isto, seja $x \in X$ e $i \in J$. Então,

$$[\varphi(\delta(x))](i) = h_i[(\delta(x))(i)] = h_i(x).$$

Note também que, se $\varphi \circ \delta$ é um isomorfismo, então X é isomorfo a $\prod_{i \in J} Y_i$. Neste caso, dizemos que a família de homomorfismos H é uma representação projetiva de módulo X como um produto direto.

No caso $Y = Y_i$, para todo $i \in J$, temos

$$\sum_{i \in J} X_i \xrightarrow{\psi} \sum_{i \in J} X_i \xrightarrow{\sigma} Y,$$

onde σ é o homomorfismo soma.

Definição 1.3.14 (Soma direta total de homomorfismos)**.** *A composição dos homomorfismos σ e ψ da forma*

$$\sigma \circ \psi \colon \sum_{i \in J} X_i \longrightarrow Y$$

é chamado de soma direta total dos homomorfismos da família $H = \{h_i \colon X_i \longrightarrow Y_i | \, i \in J\}$.

Se $\sigma \circ \psi$ é um isomorfismo, então $\sum_{i \in J} X_i$ é isomorfo à Y. Neste caso, dizemos que a família de homomorfismos H é uma representação injetiva do módulo Y como uma soma direta.

Em particular, se X_j é um submódulo de um módulo X sobre R, para todo $j \in J$, e se a família de homomorfismos inclusão

$$H = \{i_j \colon X_j \longrightarrow X \,|\, j \in J\}$$

é uma representação injetiva do módulo X como uma soma direta, então temos

$$\sum_{J \in J} X_j \approx X.$$

Neste caso, dizemos que X é decomposto na soma direta de seus submódulos X_j, para todo $j \in J$. Outra forma de expressar isto é simplesmente dizer que X é a soma direta de seus submódulos.

Se F é uma família finita de módulos sobre R, digamos

$$F = \{X_1, X_2, \cdots, X_{n-1}, X_n\},$$

então a soma direta de F é denotada por

$$\bigoplus_{i=1}^{n} X_i \quad \text{ou} \quad X_1 \oplus \cdots \oplus X_n.$$

Além disso, se cada X_i é um submódulo de um módulo X sobre R, então

$$X = \bigoplus_{i=1}^{n} X_i$$

significa que X é a soma direta de seus submódulos X_i, para todo $i = 1, \cdots, n$.

Teorema 1.3.15. *Um módulo X sobre R é a soma direta de seus submódulos A e B se, e somente se,*

$$A + B = X \quad e \quad A \cap B = 0.$$

Demonstração. Necessidade: Assuma que X é a soma direta de A e B. Então, pela definição, o homomorfismo $\sigma \circ \psi \colon A \oplus B \longrightarrow X$ dado por

$$(\sigma \circ \psi)(a, b) = a + b,$$

para todo $(a, b) \in A \oplus B$, é um isomorfismo.

Para mostrar que $A + B = X$, seja $x \in X$. Como $\sigma \circ \psi$ é um epimorfismo, existe um elemento $(a, b) \in A \oplus B$ tal que

$$x = (\sigma \circ \psi)(a, b) = a + b.$$

Isto mostra que $x \in A + B$. Como x é qualquer elemento de $A + B$, temos $X \subset A + B$. Por outro lado, como A e B são submódulos de X, segue que $A + B \subset X$. Portanto, $A + B = X$.

Para mostrar que $A \cap B = 0$. Para isso, assuma que $A \cap B$ contém um elemento não nulo $x \in X$. Como $A \cap B$ é um submódulo de X, temos que $-x \in A \cap B$. Então, $(x, -x)$ é um elemento não nulo de $A \oplus B$. Como

$$(\sigma \circ \psi)(x, -x) = x - x = 0,$$

segue que $\sigma \circ \psi$ não é um monomorfismo. Assim, $A \cap B = 0$.

Suficiência: Assuma que $A + B = X$ e $A \cap B = 0$. Temos que mostrar que $\sigma \circ \psi$ é um isomorfismo.

Para mostrar que $\sigma \circ \psi$ é um epimorfismo, seja $x \in X$. Como $A + B = X$, existem elementos $a \in A$ e $b \in B$ com $a + b = x$. Isto implica

$$(\sigma \circ \psi)(a, b) = a + b = x,$$

e, portanto, $\sigma \circ \psi$ é um epimorfismo.

Para mostrar que $\sigma \circ \psi$ é um monomorfismo, seja $(a, b) \in \mathrm{Ker}(\sigma \circ \psi)$. Então, temos

$$a + b = (\sigma \circ \psi)(a, b) = 0.$$

Segue que $a \in A$ e $a \in B$, pois $a = -b$ e $-b \in B$. Consequentemente, $a \in A \cap B$. Como $A \cap B = 0$, isso implica que $a = 0$ e $b = -a = 0$. Logo, (a, b) é o elemento nulo $(0, 0) \in A \oplus B$. Portanto, $\mathrm{Ker}(\sigma \circ \psi) = 0$ e, consequentemente, $\sigma \circ \psi$ é um monomorfismo. ■

Teorema 1.3.16. *Se a composição $h = g \circ f$ de dois homomorfismos $f \colon X \longrightarrow Y$ e $g \colon Y \longrightarrow Z$ de módulos sobre R é um isomorfismo, então as seguintes afirmações são verdadeiras:*

1. *f é um monomorfismo;*
2. *g é um epimorfismo;*
3. *O módulo Y é decomposto na soma direta de $\mathrm{Img}(f)$ e $\mathrm{Ker}(g)$; em símbolos*

$$Y = \mathrm{Img}(f) \oplus \mathrm{Ker}(g).$$

Demonstração. Mostraremos a veracidade de cada uma das afirmações.

1. Essa afirmação é um caso particular da Proposição 1.2.10.
2. Essa afirmação também é um caso particular da Proposição 1.2.10.
3. Para mostrar que $\mathrm{Img}(f) + \mathrm{Ker}(g) = Y$, sejam $y \in Y$ e $z \in Z$, com $z = g(y)$. Como $h \colon X \longrightarrow Z$ é um isomorfismo, existe um elemento $x \in X$ com $h(x) = z$. Então, temos
$$g[y - f(x)] = g(y) - g[f(x)] = z - h(x) = 0.$$

Isso implica que $y - f(x) \in \mathrm{Ker}(g)$. Portanto, temos

$$y = f(x) + (y - f(x)) \in \mathrm{Img}(f) + \mathrm{Ker}(g).$$

Como $y \in Y$ é um elemento arbitrário, segue que $Y \subset \mathrm{Img}(f) + \mathrm{Ker}(g)$. Por outro lado, como $\mathrm{Img}(f)$ e $\mathrm{Ker}(g)$ são submódulos de Y, segue que $\mathrm{Img}(f) + \mathrm{Ker}(g) \subset Y$. Portanto, $\mathrm{Img}(f) + \mathrm{Ker}(g) = Y$.

Para mostrar $\mathrm{Img}(f) \cap \mathrm{Ker}(g) = 0$, seja $y \in \mathrm{Img}(f) \cap \mathrm{Ker}(g)$. Como $y \in \mathrm{Img}(f)$, existe um elemento $x \in X$ com $f(x) = y$. Como $y \in \mathrm{Ker}(g)$, temos $g(y) = 0$. Então, obtemos

$$h(x) = g[f(x)] = g(y) = 0.$$

Pelo fato de h ser um isomorfismo, $x = 0$. Portanto, temos

$$y = f(x) = f(0) = 0,$$

e consequentemente $\mathrm{Img}(f) \cap \mathrm{Ker}(g) = 0$.

Assim, pelo Teorema 1.3.15, Y é a soma direta de seus submódulos $\mathrm{Img}(f)$ e $\mathrm{Ker}(g)$.

Sendo cada uma das afirmações verdade, o teorema está demonstrado. ■

1.4 Módulos livres

Definição 1.4.1 (Módulo livre)**.** *Um módulo X sobre R é livre sobre um conjunto S quando X é um módulo sobre R juntamente com uma função $f\colon S \longrightarrow X$ tal que, para toda função $g\colon S \longrightarrow Y$, onde Y é um módulo sobre R, existe um único homomorfismo $h\colon X \longrightarrow Y$ satisfazendo*

$$h \circ f = g.$$

Denotamos o módulo livre X sobre um conjunto S por (X, f), onde f é a função $f\colon S \longrightarrow X$ da definição.

Teorema 1.4.2. *Se um módulo X sobre R juntamente com uma função $f\colon S \longrightarrow X$, de um conjunto S no módulo X, é um módulo livre sobre o conjunto S, então f é injetiva e sua imagem $f(S)$ gera o módulo X.*

Demonstração. Para mostrar que f é injetiva, sejam $a, b \in S$, com $a \neq b$, e Y um módulo sobre R contendo mais que um elemento. Escolha uma função $g\colon S \longrightarrow Y$ tal que $g(a) \neq g(b)$. Como

$$(h \circ f)(a) = g(a) \neq g(b) = (h \circ f)(b),$$

a função $h \circ f$ é injetora. Portanto, f é uma função injetiva, pela Proposição 1.2.10.

Para mostrar que $f(S)$ gera X, seja A o submódulo de X gerado por $f(S)$. Então, a função f define uma função $g\colon S \longrightarrow A$ com

$$i \circ g = f,$$

onde i é o homomorfismo inclusão $i\colon A \longrightarrow X$. Por definição, existe um homomorfismo $h\colon X \longrightarrow A$ tal que

$$h \circ f = g.$$

Sendo $id\colon X \longrightarrow X$ o homomorfismo identidade, temos

$$id \circ f = f$$

e

$$(i \circ h) \circ f = i \circ (h \circ f) = i \circ g = f.$$

Pela unicidade da Definição 1.4.1, devemos ter

$$i \circ h = id.$$

Sendo o homomorfismo identidade id um epimorfismo, pela Proposição 1.2.10 o homomorfismo inclusão i também deve ser. Portanto, $A = X$ e $f(S)$ gera o módulo X. ■

Teorema 1.4.3. *Se (X, f) e (X', f') são módulos livres sobre um conjunto S, então existe um único isomorfismo $j\colon X \longrightarrow X'$ do módulo X no módulo X' tal que*

$$j \circ f = f'.$$

Demonstração. Como (X, f) é um módulo livre sobre o conjunto S, segue da Definição 1.4.1 que existe um único homomorfismo $j\colon X \longrightarrow X'$ tal que

$$j \circ f = f'.$$

Analogamente, como (X', f'), existe um único homomorfismo $j'\colon X' \longrightarrow X$ tal que

$$j' \circ f' = f.$$

Agora, considerando o homomorfismo identidade do módulo X, Temos

$$id_X \circ f = f$$

e

$$(j' \circ j) \circ f = j' \circ (j \circ f) = j' \circ f' = f.$$

Pela unicidade da Definição 1.4.1, devemos ter

$$j' \circ j = id_X.$$

Sendo o homomorfismo identidade id um monomorfismo, pela Proposição 1.2.10 o homomorfismo j também deve ser.

Analogamente, considerando o homomorfismo identidade do módulo X', Temos

$$id_{X'} \circ f' = f'$$

e

$$(j \circ j') \circ f' = j \circ (j' \circ f') = j \circ f = f'.$$

Pela unicidade da Definição 1.4.1, devemos ter

$$j \circ j' = id_{X'}.$$

Sendo o homomorfismo identidade $id_{X'}$ um epimorfismo, pela Proposição 1.2.10 o homomorfismo j também deve ser.

Portanto, sendo j um monomorfismo e um epimorfismo, j é um isomorfismo. ■

Teorema 1.4.4. *Para qualquer conjunto S, sempre existe um módulo livre sobre o conjunto S.*

Demonstração. Seja X o conjunto de todas as funções $\varphi\colon S \longrightarrow R$, onde R é um anel comutativo com identidade $1 \neq 0$, satisfazendo $\varphi(s) = 0$, exceto para uma quantidade finita de elementos $s \in S$. Então, X torna-se um grupo abeliano com a soma de funções como operação binária, isto é, para quaisquer dois elementos $\varphi, \psi \in X$, o elemento $\varphi + \psi \in X$ é bem definido por

$$(\varphi + \psi)(s) = \varphi(s) + \psi(s),$$

para todo elemento $s \in S$. Além disso, X torna-se um módulo sobre R com respeito a multiplicação por escalar definida por

$$(\alpha\varphi)(s) = \alpha[\varphi(s)],$$

para todo $\alpha \in R$, todo $\varphi \in X$ e todo $s \in S$.

Agora, defina uma função $f\colon S \longrightarrow X$ tomando, para cada elemento $s \in S$, a função $f(s)\colon S \longrightarrow R$ definida por

$$[f(s)](t) = \begin{cases} 1, & \text{se } t = s, \\ 0, & \text{se } t \neq s, \end{cases}$$

para todo $t \in S$. Vamos mostrar que X juntamente com $f\colon S \longrightarrow X$ é um módulo livre sobre o conjunto S.

Para este propósito, seja $g\colon S \longrightarrow Y$ uma função arbitrária do conjunto S em um módulo Y sobre R. Defina uma função $h\colon X \longrightarrow Y$ tomando, para cada $\varphi \in X$, o elemento

$$h(\varphi) = \sum_{s \in S} \varphi(s) g(s).$$

Esta a soma está bem definida pois existe uma quantidade finita de elementos $s \in S$ tal que $\varphi(s) \neq 0$. Além disso, podemos verificar que h é um homomorfismo satisfazendo $h \circ f = g$. Com efeito,

$$\begin{aligned} h(\varphi + \psi) &= \sum_{s \in S} [\varphi + \psi](s)g(s) \\ &= \sum_{s \in S} [\varphi(s) + \psi(s)]g(s) \\ &= \sum_{s \in S} \varphi(s)g(s) + \sum_{s \in S} \psi(s)g(s) \\ &= h(\varphi) + h(\psi), \end{aligned}$$

para todos $\varphi, \psi \in X$, e

$$h(\alpha\varphi(s)) = \sum_{s \in S} \alpha\varphi(s)g(s) = \alpha h(\varphi),$$

para todo $\varphi \in X$ e todo $\alpha \in R$. Além disso,

$$(h \circ f)(t) = \sum_{s \in S} [f(t)](s)g(s) = g(t),$$

para algum $t \in S$; como $t \in S$ é arbitrário, segue que $h \circ f = g$.

Para mostrar a unicidade do homomorfismo h, sejam $h' \colon X \longrightarrow Y$ um homomorfismo arbitrário satisfazendo $h' \circ f = g$ e $\varphi \in X$. Então, pela definição da função f, temos

$$\varphi = \sum_{s \in S} \varphi(s)f(s).$$

Como h' é um homomorfismo, segue que

$$h'(\varphi) = \sum_{s \in S} \varphi(s)h'[f(s)] = \sum_{s \in S} \varphi(s)g(s) = h(\varphi).$$

Como φ é um elemento arbitrário de X, segue que $h' = h$. ■

Agora, graças ao Teorema 1.4.4, sabemos que todo conjunto S determina essencialmente um único módulo livre (X, f). Como a função

$$f \colon S \longrightarrow X$$

é injetiva, pelo Teorema 1.4.2, podemos identificar S com sua imagem $f(S) \subset X$. Feito isto, o conjunto S "torna-se" um subconjunto de X, o qual gera X. Além disso, toda função

$$g \colon S \longrightarrow Y$$

do conjunto S em um módulo arbitrário X sobre R estende-se a um único homomorfismo

$$h \colon X \longrightarrow Y$$

do módulo F sobre R com o módulo Y sobre R.

Definição 1.4.5 (Módulo livre gerado por um conjunto)**.** *O módulo X sobre R discutido anteriormente é chamado de módulo livre sobre R gerado pelo conjunto S.*

Agora, vamos considerar uma família de módulos

$$F = \{F_s | \, s \in S\}$$

indexados pelo conjunto S, onde F_s é o anel R considerado como um módulo sobre si mesmo. O módulo livre X sobre R gerado pelo conjunto S é precisamente a soma direta da família F.

Corolário 1.4.6. *A soma direta de uma família de módulos*

$$F = \{F_s | \, s \in S\}$$

com $F_s \approx R$, para todo $s \in S$, é isomorfo ao módulo livre sobre R gerado pelo conjunto S.

Demonstração. Sejam X o módulo livre sobre R gerado pelo conjunto S e X' a soma direta da família F. Temos que, como $F_s \approx R$, a reunião $\bigcup_{s \in S} F_s \approx R$. Com isso, por definição, a soma direta X' é o conjunto de todas as funções

$$f \colon S \longrightarrow R,$$

com $f(s) \neq 0$ para uma quantidade finita de elementos $s \in S$. Portanto, pela construção do conjunto X feita no Teorema 1.4.4, temos que X é isomorfo à X'. ■

Definição 1.4.7. *Um módulo X é livre sobre R se, e somente se, X é isomorfo ao módulo livre sobre R gerado por algum conjunto S.*

Corolário 1.4.8. *A soma direta de uma família de módulos livres sobre R também é um módulo livre sobre R.*

Demonstração. Pelo Corolário 1.4.6, essa soma direta é isomorfo a um módulo sobre R gerado por um conjunto S. Portanto, pela Definição 1.4.7, essa soma direta é um módulo livre sobre R. ■

Teorema 1.4.9. *Todo módulo sobre R é isomorfo a um módulo quociente de um módulo livre sobre R.*

Demonstração. Seja X um módulo sobre R. Tome um subconjunto $S \subset X$ o qual gera X. Por exemplo, podemos tomar $S = X$.

Considere o módulo livre X' sobre R gerado pelo conjunto S. Então, a função inclusão $i \colon S \longrightarrow X$ estende-se para um homomorfismo

$$f \colon X' \longrightarrow X$$

do módulo livre X' no módulo X.

Como $S = i(S) \subset f(X')$ e S gera X, temos $f(X') = X$. Portanto, f é um epimorfismo. Então, pela Proposição 1.2.13, X é isomorfo ao módulo quociente $X'/\operatorname{Ker}(f)$ do módulo livre X'. ■

Definição 1.4.10 (Conjunto linearmente independente)**.** *Um subconjunto $S \subset X$, onde X é um módulo sobre R, é linearmente independente se, e somente se, para qualquer quantidade finita de elementos distintos de S*

$$\sum_{i=0}^{n} \alpha_i s_i, = 0,$$

com $\alpha_i \in R$ e $s_i \in S$, para todo $i = 1, \cdots, n$, implicar em

$$\alpha_i = 0,$$

para todo $i = 1, \cdots, n$.

Definição 1.4.11 (Base de um módulo)**.** *Se um subconjunto $S \subset X$, onde X é um módulo sobre R, é linearmente independente e gera X, então S é chamado de base de X.*

Teorema 1.4.12. *Um subconjunto $S \subset X$, onde X é um módulo sobre R, é uma base de X se, e somente se, a função inclusão $i\colon S \longrightarrow X$ se estender a um isomorfismo $h\colon X' \longrightarrow X$ do módulo livre X' sobre R gerado pelo conjunto S com o módulo X sobre R.*

Demonstração. Pela Definição 1.4.5, a função inclusão $i\colon S \longrightarrow X$ estende a um único homomorfismo $h\colon X' \longrightarrow X$ do módulo livre X' no módulo X. Basta mostrarmos que S é uma base de X se, e somente se, h é um isomorfismo.

Necessidade: Assuma que S é uma base do módulo X. A imagem $h(X')$ é um submódulo de X contendo S. Como S gera X, isso implica que $h(X') = X$ e portanto h é um epimorfismo.

Agora, seja $\varphi \in \operatorname{Ker}(h)$. Logo, sendo $\varphi \in X'$, pelo Corolário 1.4.6 e pela Definição 1.3.2, $\varphi(s) = 0$ exceto para uma quantidade finita de elementos distintos de S. Como h é uma extensão da função inclusão, temos

$$h(\varphi) = \sum_{i=1}^{n} \varphi(s_i) s_i,$$

com $s_i \in S$, para todo $i = 1, \cdots, n$. Como $\varphi \in \operatorname{Ker}(h)$, temos por definição $h(\varphi) = 0$. Como S é linearmente independente, isso implica $\varphi(s_i) = 0$, para todo $i = 1, \cdots, n$. Portanto, $\varphi = 0$, mostrando assim que h é um monomorfismo.

Sendo h um monomorfismo e um epimorfismo, ele é um isomorfismo.

Suficiência: Assuma que h é um isomorfismo. Para mostrar que S é linearmente independente, suponha que

$$\sum_{i=1}^{n} \alpha_i s_i = 0,$$

com $\alpha_i \in R$ e $s_i \in S$, para todo $i = 1, \cdots, 0$, é válido para distintos elementos de S. Seja $\varphi\colon S \longrightarrow R$ a função definida por

$$\varphi(s) = \begin{cases} \alpha_i, & \text{se } s = s_i, \text{ para algum } i = 1, \cdots, n, \\ 0, & \text{se } s \neq s_i, \text{ para todo } i = 1, \cdots, n, \end{cases}$$

para todo $s \in S$. Então, temos

$$h(\varphi) = \sum_{i=1}^{n} \alpha_i s_i = 0.$$

Como h é um monomorfismo, isso implica que $\varphi = 0$. Portanto, obtemos que $\alpha_i = \varphi(s_i) = 0$, para cada $i = 1, \cdots, n$. Mostrando assim que S é um conjunto linearmente independente.

Agora, para mostrar que S gera X, seja $x \in X$. Como h é um epimorfismo, existe $\varphi \in X'$ com $h(\varphi) = x$. Assim, pelo Corolário 1.4.6 e pela Definição 1.3.2, $\varphi(s) = 0$ exceto para uma quantidade finita de elementos de S. Então, temos

$$x = h(\varphi) = \sum_{i=1}^{n} \varphi(s_i) s_i,$$

com $s_i \in S$, para todo $i = 1, \cdots, n$. Como $\varphi(s_i) \in R$, para todo $i = 1, \cdots, n$, isto mostra que x é uma combinação linear dos elementos de S. Portanto, S gera X. ■

Corolário 1.4.13. *Um módulo X sobre R possui uma base se, e somente se, X é livre.*

Demonstração. Necessidade: Suponha que um módulo X sobre R possui uma base S. Pelo Teorema 1.4.12, a função inclusão $i\colon S \longrightarrow X$ estende a um isomorfismo h entre o módulo livre X' sobre R gerado pelo conjunto S e o módulo X. Portanto, X é livre.

Suficiência: Suponha que (X, i) é livre, onde $i\colon S \longrightarrow X$ é a função inclusão para algum subconjunto $S \subset X$. Seja (X', f) um módulo livre sobre R gerado pelo conjunto S. Então, pelo Teorema 1.4.3, existe um único isomorfismo $h\colon X' \longrightarrow X$ tal que $h \circ f = i$. Portanto, S é uma base para o módulo X. ■

1.5 Módulos sobre o anel RG

Definição 1.5.1 (Anel RG)**.** *Seja G um grupo multiplicativo. Considere o conjunto RG cujos elementos são da forma $\sum_{g \in G} r_g g$ com $r_g \in R$, $g \in G$ onde $r_g = 0$ exceto para um número finito de elementos $g \in G$. Em RG, defina as operações:*

$$\left(\sum_{g \in G} r_g g\right) + \left(\sum_{g \in G} s_g g\right) = \sum_{g \in G} (r_g + s_g) g$$

e

$$\left(\sum_{g\in G} r_g g\right)\cdot\left(\sum_{h\in G} s_h h\right) = \sum_{g,h\in G}(r_g s_h)(gh).$$

Tais operações fazem de RG um anel com identidade $1_{RG} = 1_R 1_G$, chamado de anel grupo de G sobre R.

Definição 1.5.2 (Função aumentação)**.** *Para qualquer grupo G, podemos definir o homomorfismo de anéis $\varepsilon\colon RG \longrightarrow R$ tal que $\varepsilon(g) = 1$, para todo $g \in G$. Esse homomorfismo é chamado de função aumentação.*

Definição 1.5.3 (Ação de grupo)**.** *Sejam G um grupo multiplicativo e X um conjunto não vazio. Uma ação de G sobre X é uma função $\phi\colon G \times X \longrightarrow X$ definida como*

$$\phi(g, x) = gx,$$

para todo $g \in G$ e todo $x \in X$, satisfazendo as seguintes condições:

1. *Para todo $x \in X$, temos*
$$\phi(1, x) = x;$$
2. *Para todos $g, h \in G$ e todo $x \in X$, temos*
$$\phi[g, \phi(h, x)] = \phi(gh, x).$$

De forma equivalente, podemos definir uma ação de G sobre X como um homomorfismo $\varphi\colon G \longrightarrow S(X)$, onde $S(X)$ é o grupo das funções bijetoras de X com X, tomando, para cada $g \in G$, a função $\varphi(g)\colon X \longrightarrow X$ definida por

$$[\varphi(g)](x) = gx,$$

com $x \in X$. Neste caso, dizemos também que G atua sobre X.

Na Definição 1.5.3, se X possuir a estrutura de um grupo abeliano, e se quisermos que G preserve essa estrutura, além das condições da definição, precisamos exigir que

$$\phi[g, (x + y)] = \phi(g, x) + \phi(g, y),$$

para todo $g \in G$ e todos $x, y \in A$.

Definição 1.5.4 (Ação livre)**.** *Seja X um conjunto no qual G atua. A ação de G sobre X é livre quando*

$$\phi(g, x) = x,$$

para algum $x \in X$ se, e somente se, $g = 1$.

No caso que a ação de G sobre X é livre, dizemos que G atua livremente sobre X.

Definição 1.5.5 (Órbita)**.** *Sejam X um conjunto que G atua e $x \in X$. A órbita de x por G é o conjunto*

$$G(x) = \{gx \in X |\, g \in G\}.$$

Note que o conjunto de todas as órbitas de X por G formam uma partição de X. Primeiramente, se $x, y \in X$ com $y \notin G(x)$ (ou $x \notin G(y)$), então $G(x) \cap G(y) = \emptyset$. De fato, se existisse $z \in G(x) \cap G(y)$, então existiria $g, h \in G$ tal que

$$z = gx \quad \text{e} \quad z = hy.$$

Assim, $hy \in G(x)$ (ou $gx \in G(y)$). Como $h^{-1} \in G$ (ou $g^{-1} \in G$), teríamos $y \in G(x)$ (ou $x \in G(y)$).

Além disso, se denotarmos E como um conjunto de representantes distintos das órbitas de X por G, temos

$$X = \bigcup_{\bar{x} \in E} G(\bar{x}).$$

De fato, como $G(\bar{x}) \subset X$, para todo $\bar{x} \in E$, segue que a reunião $\bigcup_{\bar{x} \in E} G(\bar{x}) \subset X$; por outro lado, como X é um conjunto que G atua, segue que, para cada $x \in X$, $x = 1x \in G(x) = G(\bar{x})$, para $x = \bar{x}$, ou seja, $X \subset \bigcup_{\bar{x} \in E} G(\bar{x})$.

Portanto, o conjunto de todas as órbitas de X por G formam uma partição de X.

Proposição 1.5.6. *Sejam G um grupo e X um conjunto não vazio. Então X é um módulo sobre RG se, e somente se, X é um módulo sobre R munido com uma ação do grupo G.*

Demonstração. Necessidade: Se X é um módulo sobre RG então X é um módulo sobre R com

$$\alpha x = (\alpha 1_G)x,$$

para todo $\alpha \in R$ e todo $x \in X$, e a ação do grupo G é dada por

$$gx = 1_{RG}x,$$

para todo $g \in G$ e todo $x \in X$.

Suficiência: Se X é um módulo sobre R munido de uma ação do grupo G, então podemos dar a X uma estrutura de módulo sobre RG definindo

$$\left(\sum_{g \in G} \alpha_g g\right) x = \sum_{g \in G} \alpha_g (gx),$$

com $\alpha_g \in R$ e $x \in X$. ■

Corolário 1.5.7. *X é um módulo sobre $\mathbb{Z}G$ se, e somente se, X é um grupo abeliano munido de uma ação de G.*

Demonstração. Necessidade: Se X é um módulo sobre $\mathbb{Z}G$, então, pela Proposição 1.5.6, X é um módulo sobre $\mathbb{Z}$ munido com uma ação de G. Como, para ser um módulo, X deve ser um grupo abeliano, segue que ele é um grupo abeliano munido de uma ação de G.

Suficiência: Se X é um grupo abeliano, então, pelo Exemplo 1.1.2, X é um módulo sobre $\mathbb{Z}$. Sendo munido de uma ação G, X é um módulo sobre $\mathbb{Z}G$ pela Proposição 1.5.6. ■

Corolário 1.5.8. *X é um módulo sobre $\mathbb{Z}_2G$ se, e somente se, X é um módulo sobre $\mathbb{Z}_2$ munido de uma ação de G.*

Demonstração. Pela Proposição 1.5.6, X é um módulo sobre $\mathbb{Z}_2G$ se, e somente se, X é um módulo sobre $\mathbb{Z}_2$ munido de uma ação de G. ■

Sejam X um conjunto onde G atua livremente e RX o módulo livre R gerado pelos elementos de X. Podemos estender a ação de G sobre X para uma ação de G sobre RX da seguinte maneira:

$$g\left(\sum_{x\in X}\alpha_x x\right)=\sum_{x\in X}\alpha_x(gx),$$

com $g\in G$ e $\alpha_x\in R$, para todo $x\in X$.

Proposição 1.5.9. *Sejam G um grupo que atua livremente sobre X e E um conjunto de representantes distintos das órbitas de X por G. Então, RX é um módulo livre sobre RG com base E.*

Demonstração. Como o conjunto de todas as órbitas de X por G formam uma partição de X, temos $X=\bigcup_{\bar{x}\in E}G(\bar{x})$, onde se $\bar{x}\neq\bar{y}\in E$, então $G(\bar{x})\cap G(\bar{y})=\emptyset$. Assim,

$$RX=R\left(\bigcup_{\bar{x}\in E}G(\bar{x})\right)=\bigoplus_{\bar{x}\in E}RG(\bar{x}).$$

Agora, como a ação de G sobre X é livre, temos que a função $f_{\bar{x}}\colon G\longrightarrow G(\bar{x})$ dada por

$$f_{\bar{x}}(g)=g\bar{x},$$

para todo $g\in X$ e todo $\bar{x}\in E$, é uma bijeção. De fato, para $\bar{x}\in E$, seja $x\in G(\bar{x})$. Então, pela definição, $x=g\bar{x}$, para algum $g\in G$. Logo, para $g\in G$, temos

$$f_{\bar{x}}(g)=g\bar{x}=x,$$

o que mostra a sobrejetividade. Por outro lado, sejam $g,h\in G$ tais que

$$\begin{aligned}f_{\bar{x}}(g)=f_{\bar{x}}(h)&\Longrightarrow g\bar{x}=h\bar{x}\\&\Longrightarrow h^{-1}g\bar{x}=\bar{x}\\&\Longrightarrow h^{-1}g=1\\&\Longrightarrow g=h.\end{aligned}$$

Logo, $f_{\bar{x}}$ é injetiva.

Como $f_{\bar{x}}$ é uma bijeção, então $RG = RG(\bar{x})$. Portanto, $RX = \bigoplus_{\bar{x} \in E} (RG)_{\bar{x}}$. ■

Corolário 1.5.10. *Se S é um subgrupo de G, então RG é um módulo livre sobre RS com base E, onde E é um conjunto de representantes distintos das órbitas de G por S, isto é, $RG = \bigoplus_{\bar{g} \in E} (RS)_{\bar{g}}$.*

Demonstração. Temos que G é um conjunto onde S atua com a ação dada pela multiplicação dos elementos de S por elementos de G, isto é, definindo a função $\phi\colon S \times G \longrightarrow G$ como

$$\phi(s, g) = sg,$$

para todo $s \in S$ e todo $g \in G$. De fato, ϕ é uma ação de S em G:

1. Para todo $g \in G$, temos
$$\varphi(1, g) = 1g = g;$$

2. Para todos $s, t \in S$ e todo $g \in G$, temos

$$\phi[s, \phi(t, g)] = \phi(s, tg) = s(tg) = (st)g = \phi(st, g).$$

Além disso, essa ação ϕ é livre. Com efeito, seja $g \in G$. Logo, $\phi(s, g) = sg = g$, com $s \in S$, se, e somente se, $s = 1$, pois S é um subgrupo de G.

Portanto, pela Proposição 1.5.9, temos $RG = \bigoplus_{\bar{g} \in E} (RS)_{\bar{g}}$. ■

1.6 Sequências exatas

Definição 1.6.1 (Sequência exata)**.** *Uma sequência exata de módulos é uma sequência finita ou infinita*

$$\cdots \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow \cdots$$

de homomorfismos de módulos sobre R tal que a imagem do homomorfismo de entrada coincide com o núcleo do homomorfismo de saída em todo módulo, exceto nas extremidades (se essas existirem) da sequência.

No caso da definição acima, se essa sequência é exata, então, por exemplo, no módulo Y temos $\mathrm{Img}(f) = \mathrm{Ker}(g)$.

Qualquer sequência exata da forma

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$$

será chamada de sequência exata curta.

Teorema 1.6.2. *Em uma sequência exata arbitrária*

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$$

de homomorfismos de módulos sobre R, as seguintes afirmações são equivalentes:

(*i*) *f é um epimorfismo;*

(*ii*) *g é o homomorfismo trivial;*

(*iii*) *h é um monomorfismo.*

Demonstração. Nesta demonstração mostraremos que a afirmação (i) é verdadeira se, e somente se, a afirmação (ii) também é, e que a afirmação (ii) é verdadeira se, e somente se, (iii) é.

(i) se, e somente se, (ii): Por definição, f é um epimorfismo se, e somente se, $\mathrm{Img}(f) = B$. Por outro lado, g é o homomorfismo trivial se, e somente se, $\mathrm{Ker}(g) = B$. Pela exatidão da sequência, temos $\mathrm{Img}(f) = \mathrm{Ker}(g)$. Portanto, (i) se, e somente se, (ii).

(ii) se, e somente se, (iii): Por definição, g é o homomorfismo trivial se, e somente se, $\mathrm{Img}(g) = 0$. Por outro lado, h é um monomorfismo se, e somente se, $\mathrm{Ker}(h) = 0$. Pela exatidão da sequência, temos $\mathrm{Img}(g) = \mathrm{Ker}(h)$. Portanto, (ii) se, e somente se, (iii). ■

Corolário 1.6.3. *Em uma sequência exata arbitrária*

$$A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D \xrightarrow{k} E$$

de homomorfismos de módulos sobre R, $C = 0$ se, e somente se, f é um epimorfismo e k é um monomorfismo.

Demonstração. Necessidade: Assuma $C = 0$. Então, ambos g e h são homomorfismos triviais. Logo, pelo Teorema 1.6.2, f é um epimorfismo e k é um monomorfismo.

Suficiência: Assuma que f é um epimorfismo e que k é um monomorfismo. Então, g e h são homomorfismos triviais, pois $\mathrm{Ker}(g) = \mathrm{Img}(f) = B$ e $\mathrm{Ker}(h) = \mathrm{Img}(k) = 0$. Logo, pela exatidão da sequência, temos $C = \mathrm{Ker}(h) = \mathrm{Img}(g) = 0$. ■

Corolário 1.6.4. *Se uma sequência*

$$0 \longrightarrow C \longrightarrow 0$$

de homomorfismos de módulos sobre R é exata, então $C = 0$.

Demonstração. Sejam $f\colon 0 \longrightarrow C$ e $g\colon C \longrightarrow 0$ os homomorfismos da sequência. Pela exatidão da sequência, $\mathrm{Img}(f) = \mathrm{Ker}(g)$, mas $\mathrm{Img}(f) = 0$ e $\mathrm{Ker}(g) = C$. Logo, $C = 0$. ■

Por outro lado, temos o seguinte corolário:

Corolário 1.6.5. *Em uma sequência exata arbitrária*

$$A \xrightarrow{d} B \xrightarrow{f} C \xrightarrow{g} D \xrightarrow{h} E \xrightarrow{k} F$$

de homomorfismos de módulos sobre R, as seguintes afirmações são equivalentes:

(i) *g é um isomorfismo;*

(ii) *f e h são homomorfismos triviais;*

(iii) *d é um epimorfismo e k é um monomorfismo.*

Demonstração. Nesta demonstração mostraremos que a afirmação (i) é verdadeira se, e somente se, a afirmação (ii) também é, e que a afirmação (ii) é verdadeira se, e somente se, (iii) é.

(i) se, e somente se, (ii): Pelo Teorema 1.6.2, g é um monomorfismo se, e somente se, f é o homomorfismo trivial. Além disso, também pelo Teorema 1.6.2, g é um epimorfismo se, e somente, h é o homomorfismo trivial. Portanto, (i) se, e somente se, (ii).

(ii) se, e somente se, (iii): Pelo Teorema 1.6.2, f é o homomorfismo trivial se, e somente se, d é um epimorfismo. Além disso, também pelo Teorema 1.6.2, h é o homomorfismo trivial se, e somente, k é um monomorfismo. Portanto, (ii) se, e somente se, (iii). ■

Em particular, ambas as afirmações (ii) e (iii) valem quando $B = 0$ e $E = 0$. Assim, temos o seguinte corolário:

Corolário 1.6.6. *Se a sequência*

$$0 \longrightarrow C \xrightarrow{g} D \longrightarrow 0$$

de homomorfismos de módulos sobre R é exata, então g é um isomorfismo.

Demonstração. Sejam $f\colon 0 \longrightarrow C$ e $h\colon D \longrightarrow 0$ os homomorfismos da sequência. Como f e h são homomorfismos triviais segue, do Corolário 1.6.5, que g é um isomorfismo. ■

Definição 1.6.7 (Divisão de uma sequência exata)**.** *Uma sequência exata*

$$\cdots \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow \cdots$$

se divide no módulo Y se, e somente se, o submódulo

$$A = \mathrm{Img}(f) = \mathrm{Ker}(g)$$

do módulo Y é um somando direto de Y, isto é,

$$Y = A \oplus B,$$

onde B é outro submódulo de Y. Se a sequência exata se divide em cada um de seus módulos, dizemos simplesmente que ela se divide.

Em outras palavras, a sequência exata se divide no módulo Y se, e somente se, Y se decompõe como uma soma direta do módulo A e um outro submódulo de Y.

Teorema 1.6.8. *Se uma sequência exata*

$$\cdots \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow \cdots$$

de homomorfismos de módulos sobre R se divide no módulo Y, então Y é isomorfo a soma direta

$$\mathrm{Img}(f) \oplus \mathrm{Img}(g).$$

Demonstração. Por definição, Y é decomposto na soma direta do submódulo $A = \mathrm{Img}(f)$ e outro submódulo B de Y. É suficiente mostrar que $B \approx \mathrm{Img}(g)$. Para esse propósito, vamos considerar a restrição

$$g|_B \colon B \longrightarrow Z.$$

Então, $g|_B$ é um homomorfismo do módulo B no módulo Z. Como

$$\mathrm{Ker}(g) = \mathrm{Img}(f) = A \quad \text{e} \quad A \cap B = 0,$$

segue que $g|_B$ é um monomorfismo. Resta mostrarmos que $\mathrm{Img}(g|_B) = \mathrm{Img}(g)$.

Seja $z \in \mathrm{Img}(g)$. Então, existe um elemento $y \in Y$ tal que $g(y) = z$. Como $Y = A + B$, existem elementos $a \in A$ e $b \in B$ com $y = a + b$. Logo, segue que

$$\begin{aligned} z &= g(y) \\ &= g(a + b) \\ &= g(a) + g(b) \\ &= g(b) \\ &= (g|_B)(b), \end{aligned}$$

pois $a \in A$ e $b \in B$. Isto implica que $\mathrm{Img}(g|_B) = \mathrm{Img}(g)$. ■

Corolário 1.6.9. *Se uma sequência exata curta*

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$$

de homomorfismos de módulos sobre R se divide, então Y é isomorfo a soma direta $X \oplus Z$.

Demonstração. Como f é injetora, podemos identificar $\mathrm{Img}(f)$ com X. Como g é sobrejetora, podemos identificar $\mathrm{Img}(g)$ com Z. Segue do Teorema 1.6.8 que $B \approx \mathrm{Img}(f) \oplus \mathrm{Img}(g) \approx X \oplus Z$. ■

Corolário 1.6.10. *Uma sequência exata arbitrária*

$$\cdots \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow \cdots$$

de homomorfismos de módulos sobre R se divide no módulo Y se existe um homomorfismo $h\colon Y \longrightarrow X$ tal que a composição $h \circ f$ é um automorfismo do módulo X. Neste caso,

$$Y \approx \mathrm{Img}(f) \oplus \mathrm{Img}(g) \approx X \oplus \mathrm{Img}(g).$$

Demonstração. Se existe um homomorfismo $h\colon Y \longrightarrow X$ tal que $h \circ f$ é um automorfismo do módulo X, então $Y \approx \mathrm{Img}(f) \oplus \mathrm{Ker}(h)$, pelo Teorema 1.3.16. Assim, $\mathrm{Img}(f)$ é um somando direto de Y. Daí, a sequência se divide em Y. Pelo Teorema 1.6.8, $Y \approx \mathrm{Img}(f) \oplus \mathrm{Img}(g)$.

Como $h \circ f$ é um automorfismo, segue que $X \approx \mathrm{Img}(f)$ e assim,

$$Y \approx \mathrm{Img}(f) \oplus \mathrm{Img}(g) \approx X \oplus \mathrm{Img}(g).$$

Logo, o corolário é válido. ■

Corolário 1.6.11. *Uma sequência exata arbitrária*

$$\cdots \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow \cdots$$

de homomorfismos de módulos sobre R se divide no módulo Y se existe um homomorfismo $k\colon Z \longrightarrow Y$ tal que a composição $g \circ k$ é um automorfismo do módulo Z. Neste caso,

$$Y \approx \mathrm{Img}(f) \oplus \mathrm{Img}(g) \approx \mathrm{Img}(f) \oplus Z.$$

Demonstração. Se existe um homomorfismo $k\colon Z \longrightarrow Y$ tal que $g \circ k$ é um automorfismo do módulo Z, então $Y \approx \mathrm{Img}(f) \oplus \mathrm{Ker}(h)$, pelo Teorema 1.3.16. Assim, $\mathrm{Ker}(g)$ é um somando direto de Y. Daí, a sequência se divide em Y. Pelo Teorema 1.6.8, $Y \approx \mathrm{Img}(f) \oplus \mathrm{Img}(g)$.

Como $g \circ k$ é um automorfismo, segue que $Z \approx \mathrm{Img}(g)$ e assim,

$$Y \approx \mathrm{Img}(f) \oplus \mathrm{Img}(g) \approx \mathrm{Img}(f) \oplus Z.$$

Logo, o corolário é válido. ■

Seja $f\colon X \longrightarrow Y$ um homomorfismo arbitrário de um módulo X sobre R em um módulo Y sobre R. Por inversa à esquerda, referimos a um homomorfismo $h\colon Y \longrightarrow X$ tal que a composição $h \circ f$ é o automorfismo identidade do módulo X. Analogamente, por inversa à direita, referimos a um homomorfismo $k\colon Y \longrightarrow X$ tal que a composição $f \circ k$ é o automorfismo identidade do módulo Y.

Corolário 1.6.12. *Para qualquer sequência exata curta*

$$0 \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow 0$$

de homomorfismos de módulos sobre R, as seguintes afirmações são equivalentes:

(*i*) *Essa sequência se divide;*

(*ii*) *O homomorfismo f possui inversa à esquerda;*

(*iii*) *O homomorfismo g possui inversa à direita.*

Demonstração. Se (*i*), então (*ii*): Assuma que a sequência exata curta se divide. Seja $A = \mathrm{Img}(f) = \mathrm{Ker}(g)$. Por definição, o módulo Y se decompõe na soma direta de seu submódulo A e outro submódulo B de Y.

Primeiro, observe que f é um monomorfismo e portanto define um isomorfismo $i\colon X \longrightarrow A$. Seja $y \in Y$. Então, existem únicos elementos $a \in A$ e $b \in B$ tais que $y = a + b$. A associação de y a $i^{-1}(a)$ define um homomorfismo $h\colon Y \longrightarrow X$ dado por

$$h(y) = i^{-1}(a),$$

para todo $y \in Y$, o qual é a inversa à esquerda do homomorfismo f.

Se (*ii*), então (*i*): Se o homomorfismo f possui inversa à esquerda, pelo Corolário 1.6.10 temos que a sequência se divide em Y.

Se (*i*), então (*iii*): Assuma que a sequência exata curta se divide. Seja $A = \mathrm{Img}(f) = \mathrm{Ker}(g)$. Por definição, o módulo Y se decompõe na soma direta de seu submódulo A e outro submódulo B de Y.

Primeiro, observe que g é um epimorfismo com A como seu núcleo. Como $A \cap B = 0$, segue que a restrição $j = g|_B\colon B \longrightarrow Z$ é um isomorfismo. Portanto, a associação de z à $j^{-1}(z)$ define um homomorfismo $k\colon Z \longrightarrow Y$ dado por

$$k(z) = j^{-1}(z),$$

para todo $z \in Z$, o qual é a inversa à direita do homomorfismo g.

Se (*iii*), então (*i*): Se o homomorfismo g possui inversa à direita, pelo Corolário 1.6.11 temos que a sequência se divide em Y. ■

1.7 Sequências semiexatas

Definição 1.7.1 (Sequência semiexata)**.** *Uma sequência finita ou infinita*

$$\cdots \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow \cdots$$

de homomorfismos de módulos sobre R é uma sequência semiexata se, e somente se, a imagem do homomorfismo de entrada está contido no núcleo do homomorfismo de saída em todo módulo, exceto nas extremidades (se essas existirem) da sequência.

No caso da definição acima, se essa sequência é semiexata, então, por exemplo, no módulo Y temos $\mathrm{Img}(f) \subset \mathrm{Ker}(g)$.

Podemos perceber que todo sequência exata de homomorfismos de módulos sobre R é uma sequência semiexata, porém o contrário nem sempre é verdade. Para ver isto, sejam A um submódulo próprio de um módulo X sobre R, isto é, $A \subset X$ com $A \neq X$, e $i\colon A \longrightarrow X$ o homomorfismo inclusão. Então a sequência

$$0 \longrightarrow A \xrightarrow{i} X \longrightarrow 0$$

é semiexata, mas não é exata. O módulo quociente $Q = X/A$ serve como uma "medida de desvio" da exatidão. Isto sugere a seguinte definição:

Definição 1.7.2 (Módulo de desvio)**.** *Em uma sequência semiexata arbitrária dada*

$$C\colon \cdots \longrightarrow X \xrightarrow{f} Y \xrightarrow{g} Z \longrightarrow \cdots$$

de homomorfismos de módulos sobre R, o módulo quociente

$$\mathrm{Ker}(g)/\,\mathrm{Img}(f)$$

é chamado de módulo de desvio da sequência C no módulo Y.

Proposição 1.7.3. *Uma sequência semiexata de homomorfismos de módulos sobre R é exata se, e somente se, todos os seus módulos de desvio são triviais.*

Demonstração. Uma sequência é exata se, e somente se, em cada módulo, $\mathrm{Img}(f) = \mathrm{Ker}(g)$, onde f é o homomorfismo de entrada e g é o homomorfismo de saída, exceto possivelmente nos finais da sequência. Agora, em uma sequência de homomorfismos de módulos sobre R, em cada módulo, $\mathrm{Img}(f) = \mathrm{Ker}(g)$ se, e somente se, $\mathrm{Ker}(g)/\,\mathrm{Img}(f)$ é trivial, onde f é o homomorfismo de entrada e g é o homomorfismo de saída, exceto possivelmente nos finais da sequência. ■

Os módulos de uma sequência semiexata C são usualmente indexados por inteiros decrescentes ou inteiros crescentes.

Definição 1.7.4 (Complexo de cadeias)**.** *Se inteiros decrescentes são utilizados como índices, a sequência semiexata C é um complexo de cadeias de módulos sobre R e os homomorfismos em C são denotados pelo mesmo símbolo ∂. Logo, o complexo de cadeias C é da seguinte forma:*

$$C\colon \cdots \xrightarrow{\partial_{n+1}} C_n \xrightarrow{\partial_n} C_{n-1} \xrightarrow{\partial_{n-1}} \cdots,$$

com $\partial_{n-1} \circ \partial_n = 0$, para todo $n \in \mathbb{Z}$.

Neste caso, os elementos de C_n são chamados de cadeias n-dimensional de C e os homomorfismos ∂ são chamados de operadores bordo. Além disso, denotaremos tal complexo de cadeias por (C, ∂).

Definição 1.7.5 (Módulo de homologia)**.** *O núcleo de ∂ em C_n é denotado por $Z_n(C)$ e é chamado de módulo de ciclos n-dimensionais de C. A imagem de ∂ em C_n é denotada por $B_n(C)$ e é chamada de módulo de bordo n-dimensional de C. Finalmente, o módulo de desvio de C no módulo C_n é denotado por*

$$H_n(C) = Z_n(C)/B_n(C)$$

e é chamado de módulo de homologia n-dimensional de C.

Definição 1.7.6 (Complexo de cocadeias)**.** *Se inteiros crescentes são utilizados como índices, a sequência semiexata C é um complexo de cocadeias de módulos sobre R e os homomorfismos em C são denotados pelo mesmo símbolo δ. Logo, o complexo de cocadeias C é da seguinte forma:*

$$C\colon \cdots \xrightarrow{\delta^{n-1}} C^{n-1} \xrightarrow{\delta^n} C^n \xrightarrow{\delta^{n+1}} \cdots,$$

com $\delta^n \circ \delta^{n-1} = 0$, para todo $n \in \mathbb{Z}$.

Neste caso, os elementos de C^n são chamados de cocadeias n-dimensional de C e os homomorfismos δ são chamados de operadores cobordo.

Definição 1.7.7 (Módulo de cohomologia)**.** *O núcleo de δ em C^n é denotado por $Z^n(C)$ e é chamado de módulo de cociclos n-dimensionais de C. A imagem de δ em C^n é denotada por $B^n(C)$ e é chamada de módulo de cobordo n-dimensional de C. Finalmente, o módulo de desvio de C no módulo C^n é denotado por*

$$H^n(C) = Z^n(C)/B^n(C)$$

e é chamado de módulo de cohomologia n-dimensional de C.

Devido a semelhança dos complexos de cadeias e dos complexos de cocadeias, neste momento nos restringiremos aos resultados de complexos de cadeias.

Definição 1.7.8 (Transformação de cadeias)**.** *Consideremos dois complexos de cadeias quaisquer (C, ∂) e (C', ∂') de módulos sobre R. Uma transformação de cadeias $f\colon C \longrightarrow C'$ é uma família de homomorfismos*

$$f = \{f_n\colon C_n \longrightarrow C'_n \,|\, n \in \mathbb{Z}\}$$

de módulos sobre R tal que, para todo $n \in \mathbb{Z}$ vale a relação comutativa

$$\partial'_n \circ f_n = f_{n-1} \circ \partial_n,$$

como no seguinte diagrama:

$$\begin{array}{ccccccccc} \cdots & \xrightarrow{\partial_{n+1}} & C_n & \xrightarrow{\partial_n} & C_{n-1} & \xrightarrow{\partial_{n-1}} & \cdots \\ & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\ \cdots & \xrightarrow{\partial'_{n+1}} & C'_n & \xrightarrow{\partial'_n} & C'_{n-1} & \xrightarrow{\partial'_{n-1}} & \cdots \end{array}$$

Exemplo 1.7.9. *Seja (C, ∂) um complexo de cadeias. Se definirmos $id\colon C \longrightarrow C$ como a família de homomorfismos identidades*

$$id = \{id_n\colon C_n \longrightarrow C'_n \,|\, n \in \mathbb{Z}\},$$

então id é uma transformação de cadeias. Essa transformação de cadeias é chamada de transformação identidade.

Verificaremos que id é uma transformação de cadeias. De fato, para todo $n \in \mathbb{Z}$ e todo $x \in C$,

$$(\partial_n \circ id_n)(x) = \partial[(id(x)] = \partial_n(x)$$

e

$$(id_{n-1} \circ \partial_n)(x) = id_{n-1}[\partial_n(x)] = \partial_n(x).$$

Logo, a relação comutativa $\partial_n \circ id_n = id_{n-1} \circ \partial_n$ é válida para todo $n \in \mathbb{Z}$. Portanto, id é uma transformação de cadeias.

Agora, vamos considerar uma transformação de cadeias arbitrária $f\colon C \longrightarrow C'$ do complexo de cadeias C no complexo de cadeias C'. Podemos verificar que o homomorfismo $f_n\colon C_n \longrightarrow C'_n$ aplica $Z_n(C)$ em $Z_n(C')$ e $B_n(C)$ em $B_n(C')$.

Com efeito, seja $y \in Z_n(C)$. Temos que, pela relação comutativa da transformação de cadeias,

$$(\partial'_n \circ f_n)(y) = (f_{n-1} \circ \partial_n)(y) = 0,$$

ou seja, $\partial'_n \circ f_n$ é o homomorfismo trivial. Então, $\mathrm{Img}(f_n) \subset Z_n(C')$ e, portanto, f_n aplica $Z_n(C)$ em $Z_n(C')$.

Agora, seja $y \in B_n(C)$. Então, existe $x \in C_{n+1}$ tal que $\partial_{n+1}(x) = y$. Pela relação comutativa da transformação de cadeias, temos que

$$(\partial'_{n+1} \circ f_{n+1})(x) = (f_n \circ \partial_{n+1})(x) = f_n(y).$$

Como $(\partial'_{n+1} \circ f_{n+1})(x) \in B_n(C')$, segue que $f_n(y) \in B_n(C')$ e, portanto, f_n aplica $B_n(C)$ em $B_n(C')$.

Consequentemente, f_n induz um homomorfismo $H_n(f)\colon H_n(C) \longrightarrow H_n(C')$ dado por

$$[H_n(f)](z + B_n(C)) = f_n(z) + B_n(C'),$$

para todo $z \in Z_n(C)$, dos módulos de homologia n-dimensionais de C com os módulos de homologia n-dimensionais de C'. O homomorfismo $H_n(f)$ é chamado de homomorfismo n-dimensional induzido por f.

Proposição 1.7.10. *Se $id\colon C \longrightarrow C$ é a transformação identidade do complexo de cadeias C, então $H_n(id)$ é o homomorfismo identidade do módulo $H_n(C)$, para todo $n \in \mathbb{Z}$.*

Demonstração. Se id é a transformação identidade do complexo de cadeias C, então id_n é o homomorfismo identidade do módulo C_n, para todo $n \in \mathbb{Z}$. Logo, para todo $z + B_n(C) \in H_n(C)$, temos

$$\begin{aligned} H_n(id)(z + B_n(C)) &= H_n(id)(z) + H_n(id)(B_n(C)) \\ &= id_n(z) + id_n(B_n(C)) \\ &= z + B_n(C). \end{aligned}$$

Portanto, $H_n(id)$ é o homomorfismo identidade, para todo $n \in \mathbb{Z}$. ■

Agora, sejam $f\colon C \longrightarrow C'$ e $g\colon C' \longrightarrow C''$ transformações de cadeias. Então, a família de homomorfismos

$$h = \{g_n \circ f_n\colon C_n \longrightarrow C''_n |\, n \in \mathbb{Z}\}$$

é uma transformação de cadeias. Além disso, essa transformação de cadeias é chamada de composição das transformações de cadeias $f\colon C \longrightarrow C'$ e $g\colon C' \longrightarrow C''$ e é denotado por

$$g \circ f\colon C \longrightarrow C''.$$

De fato, h é uma transformação de cadeias. Verificaremos a veracidade dessa afirmação. Primeiramente, sendo f e g transformações de cadeias, h é uma família de homomorfismos. Agora, para todo $n \in \mathbb{Z}$ e todo $x \in C$, temos

$$\begin{aligned} [\partial''_n \circ (g_n \circ f_n)](x) &= [(\partial''_n \circ g_n) \circ f_n](x) \\ &= [(g_{n-1} \circ \partial'_n) \circ f_n](x) \\ &= [g_{n-1} \circ (\partial'_n \circ f_n)](x) \\ &= [g_{n-1} \circ (f_{n-1} \circ \partial_n)](x) \\ &= [(g_{n_1} \circ f_{n-1}) \circ \partial_n](x). \end{aligned}$$

Logo, a relação comutativa $\partial''_n \circ (g_n \circ f_n) = (g_{n_1} \circ f_{n-1}) \circ \partial_n$ é válida para todo $n \in \mathbb{Z}$. Portanto, $h = g \circ f$ é uma transformação de cadeias.

Proposição 1.7.11. *Se $f\colon C \longrightarrow C'$ e $g\colon C' \longrightarrow C''$ são transformações de cadeias, então*

$$H_n(g \circ f) = H_n(g) \circ H_n(f)$$

vale para todo $n \in \mathbb{Z}$.

Demonstração. Primeiro, temos que os homomorfismos $H_n(g \circ f)$ e $H_n(g) \circ H_n(f)$ possuem o mesmo domínio e o mesmo contradomínio, a saber $H_n(C)$ e $H_n(C'')$. Agora, seja $z_C + B_n(C) \in H_n(C)$. Então,

$$H_n(g \circ f)(z_C + B_n(C)) = (g \circ f)(z_C) + B_n(C'')$$

e

$$\begin{aligned}[H_n(g) \circ H_n(f)](z_C + B_n(C)) &= H_n(g)(f(z_C) + B_n(C')) \\ &= g[f(z_C)] + B_n(C'') \\ &= (g \circ f)(z_C) + B_n(C'').\end{aligned}$$

Portanto, $H_n(g \circ f) = H_n(g) \circ H_n(f)$. ■

Um complexo de cadeias trivial 0 é um complexo de cadeias tal que, para todo $n \in \mathbb{Z}$, o módulo 0_n consiste de um único elemento, a saber, o elemento nulo. Assim, todos os módulos de desvio desse complexo de cadeias são triviais. Logo, esse complexo de cadeias é uma sequência exata e, portanto,

$$H_n(0) = 0,$$

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

Seja $h\colon C \longrightarrow C'$ a família de homomorfismos triviais

$$h = \{0_n\colon C_n \longrightarrow C''_n |\, n \in \mathbb{Z}\}.$$

A família de homomorfismos h é uma transformação de cadeias, ela é chamada de transformação trivial e a denotaremos por 0.

De fato, h é uma transformação de cadeias. Para verificar isso, consideremos $n \in \mathbb{Z}$ e $x \in C$. Então,

$$(\partial'_n \circ 0_n)(x) = \partial'_n[0_n(x)] = \partial'_n(0) = 0$$

e

$$(0_{n-1} \circ \partial_n)(x) = 0_{n-1}[\partial_n(x)] = 0.$$

Como n e x foram tomados arbitrariamente, segue que a relação comutativa $\partial'_n \circ 0_n = 0_{n-1} \circ \partial_n$ vale para todo $n \in \mathbb{Z}$. Portanto, $h = 0$ é uma transformação de cadeias.

Proposição 1.7.12. *Se $h\colon C \longrightarrow C'$ é a transformação trivial do complexo de cadeias C no complexo de cadeias C', então*

$$H_n(h)\colon H_n(C) \longrightarrow H_n(C')$$

é o homomorfismo trivial, para todo $n \in \mathbb{Z}$.

Demonstração. Sejam 0 o complexo de cadeias trivial tal que 0_n consiste do elemento nulo do módulo C'_n, para todo $n \in \mathbb{Z}$, e $f\colon C \longrightarrow 0$ e $g\colon 0 \longrightarrow C'$ as transformações de cadeias unicamente determinadas. Como h é a transformação trivial, temos

$$h = g \circ f.$$

Da Proposição 1.7.11, temos

$$H_n(h) = H_n(g) \circ H_n(f),$$

para todo $n \in \mathbb{Z}$. Como $H_n(0) = 0$, segue que $H_n(h) = 0$, para todo $n \in \mathbb{Z}$. ■

Definição 1.7.13 (Homotopia de cadeias)**.** *Sejam (C, ∂) em (C', ∂') dois complexos de cadeias de módulos sobre R. Duas transformações de cadeias $f, g\colon C \longrightarrow C'$ são homotópicas se, e somente se, existe uma família de homomorfismos $h = \{h_n\colon C_n \longrightarrow C'_{n+1} \mid n \in \mathbb{Z}\}$ tal que, para todo $n \in \mathbb{Z}$, é válido*

$$\partial'_{n+1} \circ h_n + h_{n-1} \circ \partial_n = f_n - g_n,$$

como no seguinte diagrama:

$$\begin{array}{ccccccccc}
 & & \cdots & \xrightarrow{\partial_{n+1}} & C_n & \xrightarrow{\partial_n} & C_{n-1} & \xrightarrow{\partial_{n-1}} & \cdots \\
 & & & \swarrow^{h_n} & \downarrow^{g_n} \quad \downarrow^{f_n} & \swarrow^{h_{n-1}} & & & \\
\cdots & \xrightarrow{\partial'_{n+2}} & C'_{n+1} & \xrightarrow{\partial'_{n+1}} & C'_n & \xrightarrow{\partial'_n} & \cdots & &
\end{array}$$

Neste caso, a família de homomorfismos h é chamada de homotopia de cadeias entre as transformações de cadeias f e g. Em símbolos, temos

$$f \simeq g\colon C' \longrightarrow C''.$$

Proposição 1.7.14. *Se duas transformações de cadeias $f, g\colon C \longrightarrow C'$ são homotópicas, então*

$$H_n(f) = H_n(g)\colon H_n(C) \longrightarrow H_n(C'),$$

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

Demonstração. Seja h a homotopia de cadeias entre f e g. Para mostrarmos que $H_n(f) = H_n(g)$, para todo $n \in \mathbb{Z}$, seja $x \in H_n(C)$. Escolha $z \in Z_n(C)$ com $p(z) = x$, onde p é a projeção natural do módulo $Z_n(C)$ sobre seu módulo quociente $H_n(C)$. Então, temos

$$\begin{aligned} f_n(z) - g_n(z) &= (\partial'_{n+1} \circ h_n)(z) + (h_{n-1} \circ \partial_n)(z) \\ &= (\partial'_{n+1} \circ h_n)(z), \end{aligned}$$

pois $\partial_n(z) = 0$, para todo $n \in \mathbb{Z}$. Como $(\partial'_{n+1} \circ h_n)(z) \in B_n(C')$, segue que

$$[H_n(f)](x) = [H_n(g)](x),$$

para todo $n \in \mathbb{Z}$, pois se $f_n(z) - g_n(z) \in B_n(C')$, então $f_n(z) + B_n(C') = g_n(z) + B_n(C')$ e daí $[H_n(f)](x) = [H_n(g)](x)$, para todo $n \in \mathbb{Z}$. Portanto, como x foi tomado arbitrariamente, temos $H_n(f) = H_n(g)$, para todo $n \in \mathbb{Z}$. ■

1.8 Módulos de homomorfismos

Definição 1.8.1 (Módulo de homomorfismos)**.** *Sejam A e B módulos sobre R e considere o conjunto*

$$\mathrm{Hom}_R(A, B)$$

de todos os homomorfismos do módulo A no módulo B.

Defina uma operação $+\colon \mathrm{Hom}_R(A,B) \times \mathrm{Hom}_R(A,B) \longrightarrow \mathrm{Hom}_R(A,B)$ *tomando, para quaisquer dois homomorfismos $\varphi, \psi\colon A \longrightarrow B$, o elemento definido por*

$$(\varphi + \psi)(x) = \varphi(x) + \psi(x),$$

para todo $x \in A$. Essa operação $+$ torna $\mathrm{Hom}_R(A,B)$ *um grupo abeliano.*

Agora, para qualquer $\alpha \in R$ e qualquer $\varphi \in \mathrm{Hom}_R(A,B)$, considere a função $\alpha\varphi\colon A \longrightarrow B$ dada por

$$(\alpha\varphi)(x) = \alpha[\varphi(x)],$$

para todo $x \in A$. Pela comutatividade de R, $\alpha\varphi$ é um homomorfismo do módulo A no módulo B. Essa associação define uma operação por escalar $\mu\colon R \times \mathrm{Hom}_R(A,B) \longrightarrow \mathrm{Hom}_R(A,B)$ dada por

$$\mu(\alpha, \varphi) = \alpha\varphi,$$

para todo $\alpha \in R$ e todo $\varphi \in \mathrm{Hom}_R(A,B)$, no grupo abeliano $\mathrm{Hom}_R(A,B)$.

Isto faz com que $\mathrm{Hom}_R(A,B)$ *seja um módulo sobre R, o qual chamaremos de módulo de homomorfismos do módulo A no módulo B.*

Note que o elemento nulo em $\mathrm{Hom}_R(A,B)$ é o homomorfismo trivial 0.

Proposição 1.8.2. *Para qualquer módulo X sobre R, sempre é válido*

$$\mathrm{Hom}_R(R, X) \approx X.$$

Demonstração. Defina uma função $h\colon \mathrm{Hom}_R(R,X) \longrightarrow X$ dada por

$$h(\varphi) = \varphi(1),$$

para todo $\varphi \in \mathrm{Hom}_R(R,X)$. A função h é um homomorfismo de módulos.

De fato, temos

$$\begin{aligned} h(\varphi + \psi) &= (\varphi + \psi)(1) \\ &= \varphi(1) + \psi(1) \\ &= h(\varphi) + h(\psi), \end{aligned}$$

para todos $\varphi, \psi \in \mathrm{Hom}_R(R, X)$, e

$$\begin{aligned} h(\alpha\varphi) &= (\alpha\varphi)(1) \\ &= \alpha(\varphi(1)) \\ &= \alpha h(\varphi). \end{aligned}$$

Agora, para mostrar que h é um isomorfismo, seja $x \in X$. Como R é um módulo livre sobre R gerado por 1, existe um único homomorfismo $\varphi \in \mathrm{Hom}_R(R, X)$ tal que

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

Isso implica que h é um isomorfismo como queríamos. ■

Definição 1.8.3 (Homomorfismo entre módulos de homomorfismos)**.** *Sejam $f\colon A' \longrightarrow A$ e $g\colon B' \longrightarrow B$ homomorfismos de módulos sobre R e consideremos os módulos* $\mathrm{Hom}_R(A, B)$ *e* $\mathrm{Hom}_R(A', B')$*. Defina uma função $h\colon \mathrm{Hom}_R(A, B) \longrightarrow \mathrm{Hom}_R(A', B')$ dada por*

$$h(\varphi) = g \circ \varphi \circ f,$$

para todo $\varphi \in \mathrm{Hom}_R(A, B)$. Definido desta forma h é um homomorfismo do módulo $\mathrm{Hom}_R(A, B)$ *no módulo* $\mathrm{Hom}_R(A', B')$ *o qual será denotado por*

$$h = \mathrm{Hom}_R(f, g).$$

Proposição 1.8.4. *Se $id_A\colon A \longrightarrow A$ e $id_B\colon B \longrightarrow B$ são os homomorfismos identidade do módulo A e do módulo B, ambos sobre R, respectivamente, então*

$$\mathrm{Hom}_R(id_A, id_B)\colon \mathrm{Hom}_R(A, B) \longrightarrow \mathrm{Hom}_R(A, B)$$

é o homomorfismo identidade do módulo $\mathrm{Hom}_R(A, B)$*.*

Demonstração. Por definição, para todo $\varphi \in \mathrm{Hom}_R(A, B)$, temos

$$\begin{aligned} [\mathrm{Hom}_R(id_A, id_B)](\varphi) &= id_B \circ \varphi \circ id_A \\ &= id_B \circ \varphi \\ &= \varphi. \end{aligned}$$

Portanto $\mathrm{Hom}_R(id_A, id_B)$ é o homomorfismo identidade do módulo $\mathrm{Hom}_R(A, B)$. ■

Proposição 1.8.5. *Se $f\colon A' \longrightarrow A$, $f'\colon A'' \longrightarrow A'$, $g\colon B \longrightarrow B'$ e $g'\colon B' \longrightarrow B''$ são homomorfismos de módulos sobre R, então*

$$\mathrm{Hom}_R(f \circ f', g' \circ g) = \mathrm{Hom}_R(f', g') \circ \mathrm{Hom}_R(f, g).$$

Demonstração. Por definição, para todo $\varphi \in \mathrm{Hom}_R(A, B)$, temos

$$\begin{aligned}[\mathrm{Hom}_R(f \circ f', g' \circ g)](\varphi) &= (g' \circ g) \circ \varphi \circ (f \circ f') \\ &= g' \circ (g \circ \varphi \circ f) \circ f' \\ &= \mathrm{Hom}_R(f', g') \circ \mathrm{Hom}_R(f, g).\end{aligned}$$

Portanto, $\mathrm{Hom}_R(f \circ f', g' \circ g) = \mathrm{Hom}_R(f', g') \circ \mathrm{Hom}_R(f, g)$. ■

Teorema 1.8.6. *Para quaisquer homomorfismos $f\colon A' \longrightarrow A$ e $g\colon B \longrightarrow B'$ de módulos sobre R, o núcleo do homomorfismo*

$$\mathrm{Hom}_R(f, g)\colon \mathrm{Hom}_R(A, B) \longrightarrow \mathrm{Hom}_R(A', B')$$

é o submódulo K de $\mathrm{Hom}_R(A, B)$ definido por

$$K = \{\varphi \in \mathrm{Hom}_R(A, B) |\, \varphi[\mathrm{Img}(f)] \subset \mathrm{Ker}(g)\}.$$

Demonstração. Para mostrar que $K \subset \mathrm{Ker}(\mathrm{Hom}_R(f, g))$, seja $\varphi \in K$. Temos que mostrar que $[\mathrm{Hom}_R(f, g)](\varphi) = 0$. Para isso, seja $x \in A'$. Como $f(x) \in \mathrm{Img}(f)$ e $\varphi \in K$, temos que $\varphi[f(x)] \in \mathrm{Ker}(g)$. Portanto,

$$[[\mathrm{Hom}_R(f, g)](\varphi)](x) = (g \circ \varphi \circ f)(x) = 0.$$

Isso mostra que $[\mathrm{Hom}_R(f, g)](\varphi) = 0$ e, portanto, $K \subset \mathrm{Ker}(\mathrm{Hom}_R(f, g))$.

Para mostrar que $\mathrm{Ker}(\mathrm{Hom}_R(f, g)) \subset K$, seja $\varphi \in \mathrm{Ker}(\mathrm{Hom}_R(f, g))$. Então, temos

$$g \circ \varphi \circ f = [\mathrm{Hom}_R(f, g)](\varphi) = 0.$$

Pela Proposição 1.2.12, $\mathrm{Img}(\varphi \circ f) \subset \mathrm{Ker}(g)$. Por outro lado, como $\mathrm{Img}(\varphi \circ f) = \varphi[\mathrm{Img}(f)]$, segue que

$$\varphi[\mathrm{Img}(f)] \subset \mathrm{Ker}(g).$$

Isso mostra que $\varphi \in K$ e, portanto, $\mathrm{Ker}(\mathrm{Hom}_R(f, g)) \subset K$. ■

Corolário 1.8.7. *Se $f\colon A' \longrightarrow A$ é um epimorfismo e $g\colon B \longrightarrow B'$ é um monomorfismo de módulos sobre R, então*

$$\mathrm{Hom}_R(f, g)\colon \mathrm{Hom}_R(A, B) \longrightarrow \mathrm{Hom}_R(A', B')$$

é um monomorfismo.

Demonstração. Tome $k \in \mathrm{Ker}(\mathrm{Hom}_R(f, g))$. Então, pelo Teorema 1.8.6, $k \in K = \{\varphi \in \mathrm{Hom}_R(A, B) |\, \varphi[\mathrm{Img}(f)] \subset \mathrm{Ker}(g)\}$. Como g é um monomorfismo e f um epimorfismo, segue que k é um homomorfismo trivial e, portanto, $\mathrm{Hom}_R(f, g)$ é um monomorfismo. ■

Teorema 1.8.8. *Se X é um módulo sobre R e*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$$

é uma sequência exata de módulos sobre R, então a sequência

$$0 \longrightarrow \mathrm{Hom}_R(X, A) \xrightarrow{f_*} \mathrm{Hom}_R(X, B) \xrightarrow{g_*} \mathrm{Hom}_R(X, C),$$

com $f_* = \mathrm{Hom}_R(id, f)$ e $g_* = \mathrm{Hom}_R(id, g)$, onde $id\colon X \longrightarrow X$ é o homomorfismo identidade do módulo X, também é exata.

Demonstração. Como id é um epimorfismo e f um monomorfismo, segue do Corolário 1.8.7 que f_* é um monomorfismo. Como $g \circ f = 0$, segue da definição que $\mathrm{Hom}_R(id, g \circ f) = 0$. Portanto,

$$g_* \circ f_* = \mathrm{Hom}_R(id \circ id, g \circ f) = \mathrm{Hom}_R(id, g \circ f) = 0$$

pela Proposição 1.8.5. Por sua vez, pela Proposição 1.2.12, segue que

$$\mathrm{Img}(f_*) \subset \mathrm{Ker}(g_*).$$

Falta-nos mostrar a inclusão contrária. Para esse propósito, seja $\varphi \in \mathrm{Hom}_R(X, B)$ tal que $\varphi \in \mathrm{Ker}(g_*)$. Como $g_* = \mathrm{Hom}_R(id, g)$, segue do Teorema 1.8.6 que

$$\varphi(X) = \varphi[\mathrm{Img}(id)] \subset \mathrm{Ker}(g) = \mathrm{Img}(f).$$

Como f é um monomorfismo, existe um isomorfismo $j\colon \mathrm{Img}(f) \longrightarrow A$ tal que $f \circ j$ é o homomorfismo inclusão de $\mathrm{Img}(f)$ em B. Defina um homomorfismo $\psi\colon X \longrightarrow A$ por

$$\psi(x) = j[\varphi(x)],$$

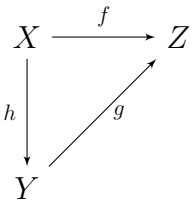
para todo $x \in X$. Então $\psi \in \mathrm{Hom}_R(X, A)$ e

$$[f_*(\psi)](x) = f(j[\varphi(x)]) = \varphi(x),$$

para todo $x \in X$. Isso mostra que $f_*(\psi) = \varphi$ e, portanto, $\varphi \in \mathrm{Img}(f_*)$. Como $\varphi \in \mathrm{Ker}(g_*)$ foi tomado arbitrariamente, temos $\mathrm{Ker}(g_*) \subset \mathrm{Img}(f_*)$. ■

1.9 Módulos projetivos

Definição 1.9.1 (Módulo projetivo)**.** *Um módulo X sobre R é projetivo quando, para todo homomorfismo $f\colon X \longrightarrow Z$ e todo epimorfismo $g\colon Y \longrightarrow Z$ de módulos sobre R, existe um homomorfismo $h\colon X \longrightarrow Y$ satisfazendo $g \circ h = f$.*



Proposição 1.9.2. *Todo módulo livre é um módulo projetivo.*

Demonstração. Considere um módulo livre arbitrário X sobre R gerado por um conjunto $S \subset X$. Seja $f\colon X \longrightarrow Z$ um homomorfismo e $g\colon Y \longrightarrow Z$ um epimorfismo de módulos sobre R.

Para qualquer $s \in S$, existe um elemento $j(s) \in Y$ com $g[j(s)] = f(s)$, pois g é um epimorfismo. A correspondência s com $j(s)$ define uma função $j\colon S \longrightarrow Y$. Como X é um módulo livre R gerado pelo conjunto $S \subset X$, j estende-se para um único homomorfismo $h\colon X \longrightarrow Y$.

Agora, falta mostrar somente que $g \circ h = f$. Para esse propósito, seja $x \in X$ um elemento arbitrário. Como X é gerado por S, x é uma combinação linear

$$x = \sum_{i=1}^{n} \alpha_i s_i,$$

com $\alpha_i \in R$ e $s_i \in S$, para todo $i = 1, \cdots, n$. Então, temos

$$\begin{aligned} g[h(x)] &= \sum_{i=1}^{n} \alpha_i g[h(s_i)] \\ &= \sum_{i=1}^{n} \alpha_i g[j(s_i)] \\ &= \sum_{i=1}^{n} \alpha_i f(s_i) \\ &= f\left(\sum_{i=1}^{n} \alpha_i s_i\right) \\ &= f(x). \end{aligned}$$

Como x foi tomado arbitrariamente, segue que $g \circ h = f$. ■

Proposição 1.9.3. *Se um módulo projetivo sobre R é uma soma direta de módulos sobre R, então os módulos que compõem essa soma também são projetivos.*

Demonstração. Assuma que a soma direta

$$X = U \oplus V$$

de dois módulos U e V sobre R é projetiva. Para mostrar que U é projetivo, sejam $f\colon U \longrightarrow Z$ um homomorfismo e $g\colon Y \longrightarrow Z$ um epimorfismo, ambos arbitrariamente

dados, $d\colon U \longrightarrow X$ a injeção natural e $p\colon X \longrightarrow U$ a projeção natural. Como X é projetivo, existe um homomorfismo $h\colon X \longrightarrow Y$ satisfazendo

$$g \circ h = f \circ p.$$

Considere a composição

$$h \circ d\colon U \longrightarrow Y.$$

Como $p \circ d$ é o homomorfismo identidade de U, temos

$$\begin{aligned} g \circ (h \circ d) &= (g \circ h) \circ d \\ &= (f \circ p) \circ d \\ &= f \circ (p \circ d) \\ &= f. \end{aligned}$$

Portanto, pela Definição 1.9.1, U é um módulo projetivo. ■

Proposição 1.9.4. *Toda soma direta de módulos projetivos sobre R também é um módulo projetivo sobre R.*

Demonstração. Considere a soma direta

$$X = \sum_{i \in J} X_i$$

de uma família $F = \{X_i | \, i \in J\}$ de módulos projetivos sobre R. Para mostrar que X é projetivo, sejam $f\colon X \longrightarrow Z$ um homomorfismo e $g\colon Y \longrightarrow Z$ um epimorfismo, ambos arbitrariamente dados. Para cada $i \in J$, seja

$$d_i\colon X_i \longrightarrow X$$

a injeção natural. Como X_i é projetivo, existe um homomorfismo $h_i\colon X_i \longrightarrow Y$ satisfazendo

$$g \circ h_i = f \circ d_i.$$

Então, obtemos o homomorfismo $h\colon X \longrightarrow Y$ dado por

$$h = \sum_{i \in J} h_i,$$

que é a soma direta de homomorfismos da família $H = \{h_i\colon X_i \longrightarrow Y | \, i \in J\}$.

Falta verificarmos que $g \circ h = f$. Para esse propósito, sejam $x \in X$ e $p_i \colon X \longrightarrow X_i$ a projeção natural para cada $i \in J$. Então, temos

$$\begin{aligned}(g \circ h)(x) &= \sum_{i \in J} [g \circ (h_i \circ p_i)](x) \\ &= \sum_{i \in J} [(g \circ h_i) \circ p_i](x) \\ &= \sum_{i \in J} [(f \circ d_i) \circ p_i](x) \\ &= f\left[\sum_{i \in J} (d_i \circ p_i)(x)\right] \\ &= f(x).\end{aligned}$$

Como x foi tomado arbitrariamente, segue que $g \circ h = f$. Assim, completamos a demonstração. ■

Teorema 1.9.5. *Para qualquer módulo X sobre R e seu homomorfismo identidade $id \colon X \longrightarrow X$, as seguintes afirmações são equivalentes:*

(*i*) *X é um módulo projetivo;*

(*ii*) *Toda sequência exata curta*

$$0 \longrightarrow U \xrightarrow{f} V \xrightarrow{g} X \longrightarrow 0$$

de módulos sobre R se divide em V;

(*iii*) *X é isomorfo à uma soma direta de módulos livres sobre R;*

(*iv*) *Para todo epimorfismo $g \colon A \longrightarrow B$,*

$$g_* = \mathrm{Hom}_R(id, g) \colon \mathrm{Hom}_R(X, A) \longrightarrow \mathrm{Hom}_R(X, B)$$

é também um epimorfismo;

(*v*) *Para toda sequência exata curta*

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

de módulos sobre R, a sequência

$$0 \longrightarrow \mathrm{Hom}_R(X, A) \xrightarrow{f_*} \mathrm{Hom}_R(X, B) \xrightarrow{g_*} \mathrm{Hom}_R(X, C) \longrightarrow 0,$$

com $f_* = \mathrm{Hom}_R(id, f)$ e $g_* = \mathrm{Hom}_R(id, g)$, também é uma sequência exata curta.

Demonstração. Se (*i*), então (*ii*): Assuma que X é um módulo projetivo e considere o diagrama:

$$\begin{array}{ccccc} & & X & & \\ & & \downarrow{\scriptstyle id} & & \\ Y & \xrightarrow{g} & X & \longrightarrow & 0 \end{array}$$

Por definição, existe um homomorfismo $h\colon X \longrightarrow Y$ satisfazendo $g \circ h = id$. Pelo Corolário 1.6.12, isso implica que a sequência exata em (ii) se divide em V.

Se (ii), então (iii): Pelo Teorema 1.4.9, X é isomorfo a um quociente de um módulo livre sobre R. Em outras palavras, existe um módulo livre F sobre R e um epimorfismo $\varepsilon\colon F \longrightarrow X$. Sendo K o núcleo de ε e $i\colon K \longrightarrow F$ o homomorfismo inclusão, obtemos a sequência exata curta

$$0 \longrightarrow K \xrightarrow{i} F \xrightarrow{\varepsilon} X \longrightarrow 0.$$

Por (ii), essa sequência se divide e daí, pelo Corolário 1.6.12, existe um homomorfismo $h\colon X \longrightarrow F$ tal que $\varepsilon \circ h$ é o automorfismo identidade de X. Pelo Teorema 1.3.16, h é um monomorfismo e

$$F \approx \mathrm{Img}(h) \oplus K.$$

Consequentemente, X é isomorfo a uma soma direta de $\mathrm{Img}(h)$ do módulo livre F sobre R.

Se (iii), então (i): Suponha que X seja isomorfo à uma soma direta de módulos livres sobre R. Sendo esses módulos livres, pela Proposição 1.9.2. eles são projetivos. Daí, segue da Proposição 1.9.4 que X é um módulo projetivo.

(i) se, e somente se, (iv): Por definição, $g_* = \mathrm{Hom}_R(id, g)$ é um epimorfismo se, e somente se, para todo elemento $f \in \mathrm{Hom}_R(X, B)$ existir um elemento $h \in \mathrm{Hom}_R(X, A)$ tal que

$$\begin{aligned} g_*(h) &= g \circ h \circ id \\ &= g \circ h \\ &= f. \end{aligned}$$

Portanto, (iv) vale se, e somente se, X for um módulo projetivo.

(iv) se, e somente se, (v): Pelo Teorema 1.8.8, g_* é um epimorfismo se, e somente se, a sequência

$$0 \longrightarrow \mathrm{Hom}_R(X, A) \xrightarrow{f_*} \mathrm{Hom}_R(X, B) \xrightarrow{g_*} \mathrm{Hom}_R(X, C) \longrightarrow 0,$$

com $f_* = \mathrm{Hom}_R(id, f)$ e $g_* = \mathrm{Hom}_R(id, g)$, é exata. ■

Lema 1.9.6. *Suponha que dado o diagrama*

$$\begin{array}{ccccc} X & \xrightarrow{d} & Y & & \\ \vdots{\scriptstyle g} & & \downarrow{\scriptstyle f} & & \\ C' & \xrightarrow{\partial_1} & C & \xrightarrow{\partial_2} & C'' \end{array}$$

onde $\partial_2 \circ (f \circ d) = 0$, desejamos determinar g tal que $\partial_1 \circ g = f \circ d$. Se X é um módulo projetivo e se

$$C' \xrightarrow{\partial_1} C \xrightarrow{\partial_2} C''$$

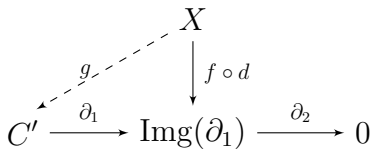
é uma sequência exata, então o homomorfismo g satisfazendo $\partial_1 \circ g = f \circ d$ existe.

Demonstração. Como $\partial_2 \circ (f \circ d) = 0$, segue que $\mathrm{Img}(f \circ d) \subset \mathrm{Ker}(\partial_2)$. Além disso, a sequência

$$C' \xrightarrow{\partial_1} C \xrightarrow{\partial_2} C''$$

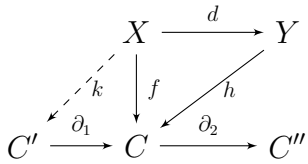
é exata e assim, $\mathrm{Img}(\partial_1) = \mathrm{Ker}(\partial_2)$. Daí, $\mathrm{Img}(f \circ g) \subset \mathrm{Img}(\partial_1)$.

Considere o diagrama:



Como X é um módulo projetivo, então existe um homomorfismo $g\colon X \longrightarrow C'$ tal que $\partial_1 \circ g = f \circ d$. ■

Lema 1.9.7. *Suponha que dado o diagrama*



onde $\partial_2 \circ (h \circ d) = \partial_2 \circ f$, desejamos determinar k tal que $\partial_1 \circ k + h \circ d = f$. Se X é um módulo projetivo e se

$$C' \xrightarrow{\partial_1} C \xrightarrow{\partial_2} C''$$

é uma sequência exata, então o homomorfismo k satisfazendo $\partial_1 \circ k + h \circ d = f$ existe.

Demonstração. Como $\partial_2 \circ (h \circ d) = \partial_2 \circ f$ segue que

$$\partial_2 \circ f - \partial \circ (h \circ d) = 0$$

implica em

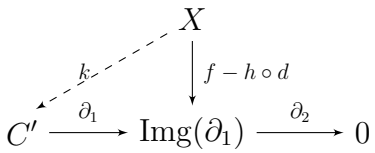
$$\partial_2 \circ (f - h \circ d) = 0.$$

Assim, $\mathrm{Img}(f - h \circ d) \subset \mathrm{Ker}(\partial_2)$. Como a sequência

$$C' \xrightarrow{\partial_1} C \xrightarrow{\partial_2} C''$$

é exata, temos que $\mathrm{Img}(\partial_1) = \mathrm{Ker}(\partial_2)$, o que implica que $\mathrm{Img}(f - h \circ d) \subset \mathrm{Img}(\partial_1)$.

Podemos então considerar o seguinte diagrama:



Como X é um módulo projetivo, segue que existe um homomorfismo $k\colon X \longrightarrow C'$ tal que $\partial_1 \circ k = f - h \circ d$. Portanto, existe um homomorfismo $k\colon X \longrightarrow C'$ satisfazendo $\partial_1 \circ k + h \circ d = f$. ■

Parte II

Resoluções e Cohomologia de grupos

2 Resoluções livres e resoluções projetivas

Neste capítulo tratamos da construção das resoluções livres e projetivas mostrando, por exemplo, que dado um módulo qualquer sempre podemos construir uma resolução sobre ele (veja a Proposição 2.1.5). Depois mostramos a independência de sua escolha via uma homotopia de cadeias (veja o Teorema 2.1.9). Por fim, apresentamos algumas resoluções: a resolução normal; a resolução bar; a resolução bar normalizada. Na obtenção desses conceitos e resultados, fazemos o uso extensivo da base de resultados construída no Capítulo 1. Para tanto, fizemos uso das referências (BROWN, 1992), (HATCHER, 2002), (CASTRO, 2006) e (FIDELIS; COELHO, 2021).

2.1 Resoluções

Definição 2.1.1 (Resolução livre)**.** *Seja A um módulo sobre R. Uma resolução livre de A sobre R é uma sequência exata de módulos sobre R da forma:*

$$\cdots \longrightarrow X_2 \xrightarrow{\partial_2} X_1 \xrightarrow{\partial_1} X_0 \xrightarrow{\varepsilon} A \longrightarrow 0,$$

com cada X_i sendo um módulo livre sobre R.

Denotamos tal resolução por $\varepsilon\colon X \longrightarrow A$.

Exemplo 2.1.2. *Considere $G = \{1\}$. Temos então que $RG \approx R$ e*

$$0 \longrightarrow R \xrightarrow{id_R} R \longrightarrow 0$$

é uma resolução livre de R sobre RG.

De fato, a sequência

$$0 \longrightarrow R \xrightarrow{id_R} R \longrightarrow 0$$

é exata e R é um módulo livre. Portanto, essa sequência é uma resolução livre.

Exemplo 2.1.3. *Seja $G \approx \mathbb{Z}_n$ o grupo cíclico finito de ordem n. Considere a sequência*

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

onde ε é a função aumentação, $t-1$ e N denotam, respectivamente, a multiplicação por $t-1$ e por $1+t+\cdots+t^{n-1}$, em cada elemento de RG, e R é visto como um módulo trivial sobre RG.

Essa sequência é uma resolução livre de R sobre RG.

De fato, RG é um módulo livre sobre RG, ε é um epimorfismo e ainda temos

$$\mathrm{Ker}(\varphi) = \mathrm{Img}(t-1) \quad \text{e} \quad \mathrm{Img}(N) = \mathrm{Ker}(t-1) \quad \text{e } \mathrm{Img}(t-1) = \mathrm{Ker}(N).$$

Exemplo 2.1.4. *Seja $G \approx \mathbb{Z}$ o grupo cíclico infinito. Considere a sequência*

$$0 \xrightarrow{t-1} RG \xrightarrow{\varepsilon} R \longrightarrow 0,$$

onde ε é a função aumentação e $t-1$ a multiplicação por $t-1$ em cada elemento de RG, e R é visto como um módulo trivial sobre RG.

Essa sequência é uma resolução livre de R sobre RG.

De fato, RG é um módulo livre sobre RG, ε é um epimorfismo e ainda temos que $t-1$ é um monomorfismo e $\mathrm{Img}(t-1) = \mathrm{Ker}(\varepsilon)$.

Proposição 2.1.5. *Dado um módulo A sobre R, sempre podemos construir uma resolução livre de A sobre R.*

Demonstração. Pelo Teorema 1.4.9, sabemos que todo módulo A sobre R é isomorfo à um módulo quociente de um módulo livre sobre R. Neste caso, então existe um módulo livre X_0 e um isomorfismo

$$\psi_0 \colon A \longrightarrow X_0/Y_0,$$

onde Y_0 é um submódulo de X_0.

Sejam $p_0 \colon X_0 \longrightarrow X_0/Y_0$ a projeção natural dada por

$$p_0(x) = x + Y_0,$$

para todo $x \in X_0$, e $\varepsilon \colon X_0 \longrightarrow A$ o homomorfismo dado por

$$\varepsilon = \psi_0^{-1} \circ p_0.$$

Temos que ε é um epimorfismo, pois tanto ψ_0^{-1} quanto p são epimorfismos. E, além disso, $\mathrm{Ker}(\varepsilon) = Y_0$.

Analogamente, o módulo $\mathrm{Ker}(\varepsilon)$ sobre R é isomorfo à um módulo quociente de um módulo livre sobre R. Digamos então que existe um módulo livre X_1 e um isomorfismo

$$\psi_1 \colon \mathrm{Ker}(\varepsilon) \longrightarrow X_1/Y_1,$$

onde Y_1 é um submódulo de X_1. Novamente, tome a projeção natural $p_1 \colon X_1 \longrightarrow X_1/Y_1$ e defina o homomorfismo $\partial_1 \colon X_1 \longrightarrow X_0$ dado por

$$\partial_1 \colon i_0 \circ \psi_1^{-1} \circ p_1,$$

onde $i_0 \colon \mathrm{Ker}(\varepsilon) \longrightarrow X_0$ é o homomorfismo inclusão.

Então,

$$\begin{aligned}\mathrm{Img}(\partial_1) &= (i_0 \circ \psi_1^{-1} \circ p_1)(X_1) \\ &= (i_0 \circ \psi_1^{-1})(X_1/Y_1) \\ &= i_0(\mathrm{Ker}(\varepsilon)) \\ &= \mathrm{Ker}(\varepsilon)\end{aligned}$$

e

$$\mathrm{Ker}(\partial_1) = \mathrm{Ker}(p_1) = Y_1,$$

pois tanto i_0 quanto ψ_1^{-1} são monomorfismos. Assim, temos a sequência exata

$$X_1 \xrightarrow{p_1} X_1/Y_1 \xrightarrow{\psi_1^{-1}} \mathrm{Ker}(\varepsilon) \xrightarrow{i_0} X_0 \xrightarrow{p_0} X_0/Y_0 \xrightarrow{\psi_0^{-1}} A \longrightarrow 0,$$

com X_0 e X_1 módulos livres sobre R.

Continuando esse processo sucessivamente, obtemos a sequência exata

$$\cdots \longrightarrow X_2 \xrightarrow{\partial_2} X_1 \xrightarrow{\partial_1} X_0 \xrightarrow{\varepsilon} A \longrightarrow 0,$$

com cada X_i sendo um módulo livre sobre R. ■

Definição 2.1.6 (Resolução projetiva)**.** *Seja A um módulo sobre R. Uma resolução projetiva de A sobre R é uma sequência exata de módulos sobre R da forma:*

$$\cdots \longrightarrow X_2 \xrightarrow{\partial_2} X_1 \xrightarrow{\partial_1} X_0 \xrightarrow{\varepsilon} A \longrightarrow 0,$$

com cada X_i sendo um módulo projetivo sobre R.

Também denotamos tal resolução por $\varepsilon\colon X \longrightarrow A$.

Lema 2.1.7. *Se $\varepsilon\colon X \longrightarrow R$ é uma resolução projetiva de R sobre RG e S é um subgrupo de G, então $\varepsilon\colon X \longrightarrow R$ também é uma resolução projetiva de R sobre RS.*

Demonstração. Seja

$$\cdots \longrightarrow X_2 \xrightarrow{\partial_2} X_1 \xrightarrow{\partial_1} X_0 \xrightarrow{\varepsilon} R \longrightarrow 0$$

uma resolução projetiva de R sobre RG. Cada módulo X_n sobre RG, com $n \in \mathbb{Z}$, pode ser visto como um módulo sobre RS, uma vez que $RS \subset RG$. Devemos mostrar então que X_n é um módulo projetivo sobre RS, para todo $n \in \mathbb{Z}$.

Como cada X_n é módulo projetivo sobre RG, pelo Teorema 1.9.5, X_n é isomorfo a uma soma direta de módulos livres sobre R. Assim,

$$X_n \oplus Y_n \simeq \bigoplus_{j \in J} (RG)_j,$$

onde Y_n é um módulo sobre RG. Pelo Corolário 1.5.10, temos que RG é um módulo livre sobre RS com base em um conjunto E de representantes para as classes laterais de S em G, isto é, $RG \simeq \bigoplus_{g \in E} (RS)_g$. Logo, obtemos

$$X_n \oplus Y_n \simeq \bigoplus_{i \in J} (RS)_i,$$

e assim, pelo Teorema 1.9.5, X_n é um módulo projetivo sobre RS, para todo $n \in \mathbb{Z}$.

Portanto, $\varepsilon\colon X \longrightarrow R$ é uma resolução projetiva de R sobre RS. ■

Podemos perceber que toda resolução livre é uma resolução projetiva. Isso é uma consequência imediata da Proposição 1.9.2, a qual nos diz que todo módulo livre é um módulo projetivo.

Lema 2.1.8. *Sejam (C, ∂) e (C', ∂') complexos de cadeias, r um inteiro e*

$$\{f_n\colon C_n \longrightarrow C'_n |\, n \leq r\}$$

uma família de funções tal que

$$\partial'_n \circ f_n = f_{n-1} \circ \partial_n,$$

para $n \leq r$. Se C_n é projetivo para $n > r$ e $H_n(C') = 0$ para $n \geq r$, então $\{f_n |\, n \leq r\}$ estende-se para uma transformação de cadeias

$$f\colon C \longrightarrow C',$$

e f é única a menos de homotopia. Mais precisamente, quaisquer duas extensões são homotópicas por uma homotopia h tal que $h_n = 0$, para $n \leq r$.

Demonstração. Suponha que f_n esteja definido para $n \leq m$, onde $m \geq r$, e que $\partial'_n \circ f_n = f_{n-1} \circ \partial_n$ vale para $n \leq m$. Então, temos

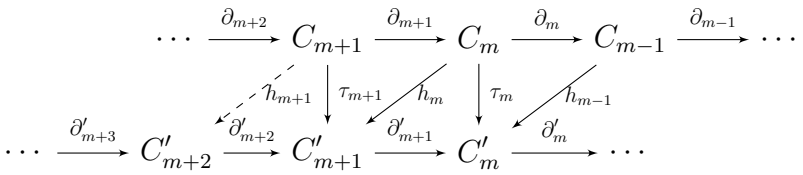
$$\begin{array}{ccccccccc}
\cdots & \xrightarrow{\partial_{m+2}} & C_{m+1} & \xrightarrow{\partial_{m+1}} & C_m & \xrightarrow{\partial_m} & C_{m-1} & \xrightarrow{\partial_{m-1}} & \cdots \\
 & & \vdots\, {\scriptstyle f_{m+1}} & & \downarrow {\scriptstyle f_m} & & \downarrow {\scriptstyle f_{m-1}} & & \\
\cdots & \xrightarrow{\partial'_{m+2}} & C'_{m+1} & \xrightarrow{\partial'_{m+1}} & C'_m & \xrightarrow{\partial'_m} & C'_{m-1} & \xrightarrow{\partial'_{m-1}} & \cdots
\end{array}$$

onde

$$\begin{aligned}
\partial'_m(\circ f_m \circ)\partial_{m+1} &= (f_{m-1} \circ \partial_m) \circ \partial_{m+1} \\
&= f_{m-1} \circ (\partial_m \circ \partial_{m+1}) \\
&= 0.
\end{aligned}$$

Portanto, pelo Lema 1.9.6, f_{m+1} também está definido.

Agora, seja g uma outra extensão de $\{f_n |\, n \leq r\}$. Devemos encontrar uma homotopia h entre f e g. Suponha que $h_n\colon C_n \longrightarrow C'_{n+1}$ esteja definido para $n \leq m$, onde $m \geq r$, e que $\partial'_n \circ h_n + h_{n-1} \circ \partial_n = f_n - g_n$ vale para $n \leq m$. Note que podemos definir $h_n = 0$, para $n \leq r$. Definindo $\tau_n = f_n - g_n$, temos



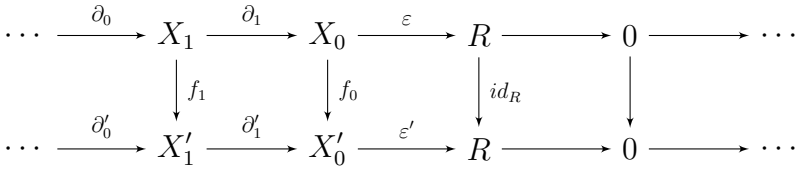
com

$$\begin{aligned}\partial'_{m+1} \circ (h_m \circ \partial_{m+1}) &= (\tau_m - h_{m-1} \circ \partial_m) \circ \partial_{m+1} \\ &= \tau_m \circ \partial_{m+1} \\ &= \partial'_{m+1} \circ \tau_{m+1}.\end{aligned}$$

Logo, pelo Lema 1.9.7, existe o homomorfismo h_{m+1} tal que $\partial'_{m+2} \circ h_{m+1} + h_m \circ \partial_{m+1} = \tau_{m+1}$. Portanto, a homotopia h entre f e g está definida. ■

Teorema 2.1.9. *Se $\varepsilon\colon X \longrightarrow R$ e $\varepsilon'\colon X' \longrightarrow R$ são resoluções projetivas de R sobre RG, então existe uma transformação de cadeias $f\colon X \longrightarrow X'$ preservando aumentação (isto é, $\varepsilon' \circ f = \varepsilon$), única a menos de homotopia e f é uma equivalência de homotopias.*

Demonstração. Sejam $\varepsilon\colon X \longrightarrow R$ e $\varepsilon'\colon X' \longrightarrow R$ resoluções projetivas de R sobre RG. Podemos formar complexos de cadeias aumentados com R na dimensão -1 e 0 nas dimensões $n < -1$:



Notemos que os complexos de cadeias são tais que $\partial'_n \circ f_n = f_{n-1} \circ \partial_n$, para $n \leq -1$, além de cada X_n ser projetivo para $n > -1$ e $H_n(X') = 0$, para $n \geq -1$, pois a sequência X' é exata.

Assim, aplicando o Lema 2.1.8 com $r = -1$, concluímos que existe uma transformação de cadeias $f\colon X \longrightarrow X'$ a qual preserva aumentação. Além disso, f é única a menos de homotopia. Note que a homotopia h dada no Lema 2.1.8 no nível dos complexos de cadeias aumentados produz uma homotopia de X em X', pois do Lema 2.1.8 segue que $h_{-1} = 0$. Da mesma forma, existe uma transformação de cadeias $f'\colon X' \longrightarrow X$ que preserva aumentação e temos $f' \circ f \simeq id_X$ e $f \circ f' \simeq id_{X'}$, onde a unicidade advém do Lema 2.1.8. ■

2.2 Resolução padrão

Sejam G um conjunto e $X_n = RS_n$ o módulo livre sobre R gerado pelo conjunto S_n, com cada S_n sendo o conjunto das $(n+1)$-uplas de elementos de G, isto é,

$$S_n = \{(g_0, g_1, \cdots, g_{n-1}, g_n) \in G^{n+1} \,|\, g_i \in G, \text{ com } i = 0, \cdots, n\}.$$

Consideremos as funções $\partial_n\colon X_n \longrightarrow X_{n-1}$, com $n \geq 1$, definidas nos geradores por

$$\partial_n(g_0, g_1, \cdots, g_{n-1}, g_n) = \sum_{i=0}^{n} (g_0, g_1, \cdots, g_{i-1}, g_{i+1}, \cdots, g_{n-1}, g_n),$$

para todo $(g_0, g_1, \cdots, g_{n-1}, g_n) \in X_n$, e $\varepsilon\colon X_0 \longrightarrow R$ definida por

$$\varepsilon(g_0) = 1_R,$$

para todo $g_0 \in X_0$, e suas respectivas extensões.

Assim, podemos construir a seguinte sequência:

$$X_*\colon \cdots \longrightarrow X_2 \xrightarrow{\partial_2} X_1 \xrightarrow{\partial_1} X_0 \xrightarrow{\varepsilon} R \longrightarrow 0.$$

A ação de G sobre X_n é obtida através da ação de G sobre S_n, isto é, para todo $s = (g_0, g_1, \cdots, g_{n-1}, g_n) \in S$, com $g_i \in G$, para todo $i = 1, \cdots, n$,

$$g\left(\sum_{s \in S_n} \alpha_s s\right) = \sum_{x \in X} \alpha_s (gs),$$

onde $gs = (gg_0, gg_1, \cdots, gg_{n-1}, gg_n)$, para todo $g \in G$ e todo $\alpha_s \in S$. Além disso, a ação de G sobre X_n é livre. Com efeito, seja $g \in G$. Logo,

$$g\left(\sum_{s \in S_n} \alpha_s s\right) = \sum_{x \in X} \alpha_s (gs) = \sum_{x \in X} \alpha_s s,$$

para algum $s = (g_0, g_1, \cdots, g_{n-1}, g_n) \in S$, com $g_i \in G$, para todo $i = 1, \cdots, n$, se, e somente se, $g = 1$, pois $gs = s$ se, e somente se, $g = 1$.

Consequentemente, pela Proposição 1.5.9, X_n é um módulo livre sobre RG com base em um conjunto de representantes distintos das órbitas de S_n por G.

Agora, vamos mostrar que a sequência X_* é exata. Consideremos o módulo $X_{-1} = R$ e a função $h_n\colon X_n \longrightarrow X_{n+1}$ definida nos geradores por

$$h_n(g_0, g_1, \cdots, g_{n-1}, g_n) = \begin{cases} (1, g_0, g_1, \cdots, g_{n-1}, g_n), & \text{se } n \geq 0, \\ 1_{X_0}, & \text{se } n = -1, \end{cases}$$

para todo $(g_0, g_1, \cdots, g_{n-1}, g_n) \in X_n$, onde, para $n = -1$, $(g_0, g_1, \cdots, g_{n-1}, g_n) = 1_R$, e suas respectivas extensões.

Ao considerar X_* como um complexo de cadeias de módulos sobre R, temos

$$\begin{aligned} \varepsilon \circ h_{-1} &= id_{X_{-1}} \\ &= id_{X_{-1}} - 0, \end{aligned}$$

além de

$$\begin{aligned} \partial_1 \circ h_{-1} + h_{-1} \circ \varepsilon &= id_{X_0} \\ &= id_{X_0} - 0, \end{aligned}$$

e

$$\begin{aligned}\partial_{n+1} \circ h_n + h_{n-1} \circ \partial_n &= id_{X_n} \\ &= id_{X_n} - 0,\end{aligned}$$

para $n \geq 1$, onde 0 sendo o homomorfismo trivial nos três casos. Logo, $h = \{h_n \colon X_n \longrightarrow X_{n+1} | \, n \in \mathbb{Z}\}$ é uma homotopia de cadeias entre o homomorfismo identidade do complexo de cadeias X_* e o homomorfismo trivial 0.

Assim, pelas Proposições 1.7.14, 1.7.10 e 1.7.12, temos que os homomorfismos n-dimensionais induzidos por $id_{X_{-1}}$ e por 0 resultam

$$id_{H_n(X_*)} = H_n(id_{X_*}) = H_n(0) = 0_n,$$

para todo $n \in \mathbb{Z}$. Consequentemente, para todo $n \in \mathbb{Z}$, $H_n(X_*) = 0$ e daí

$$\mathrm{Img}(\partial_{n+1}) = \mathrm{Ker}(\partial_n) \quad \text{e} \quad \mathrm{Img}(\partial_0) = \mathrm{Ker}(\varepsilon).$$

Portanto, X_* é uma sequência exata.

Sendo X_n um módulo livre sobre RG, para cada $n \in \mathbb{Z}$, e a sequência X_* exata, segue que

$$X_* \colon \cdots \longrightarrow X_2 \xrightarrow{\partial_2} X_1 \xrightarrow{\partial_1} X_0 \xrightarrow{\varepsilon} R \longrightarrow 0.$$

é uma resolução livre de R sobre RG. Sendo uma resolução livre, ela é portanto uma resolução projetiva. Em ambos os casos, chamaremos essa resolução de resolução padrão.

2.3 Resolução bar

Considere, na resolução padrão, o representante da órbita de $(g_0, g_1, \cdots, g_{n-1}, g_n) \in S_n$ por G o elemento

$$\begin{aligned}g_0^{-1}(g_0, g_1, \cdots, g_{n-1}, g_n) &= (1, g_0^{-1}g_1, g_0^{-1}g_2, \cdots, g_0^{-1}g_{n-1}, g_0^{-1}g_n) \\ &= (1, g_1', g_1'g_2', \cdots, g_1'g_2' \cdots g_{n-2}'g_{n-1}', g_1'g_2' \cdots g_{n-1}'g_n'),\end{aligned}$$

tal que $g_i' = g_{i-1}^{-1}g_i$, para todo $i = 1, \cdots, n$.

Vamos denotar um elemento $(1, g_1, g_1g_2, \cdots, g_1g_2 \cdots g_{n-2}g_{n-1}, g_1g_2 \cdots g_{n-1}g_n) \in X_n$ por $[g_1|g_2|\cdots|g_{n-1}|g_n]$. Esta notação é chamada de notação bar.

Utilizando a notação bar, temos que X_n é o módulo livre sobre RG gerado pelos símbolos $[g_1'|g_2'|\cdots|g_{n-1}'|g_n'] \in S_n$ e, além disso,

$$\partial_n([g_1|g_2|\cdots|g_{n-1}|g_n]) = \sum_{i=0}^{n} (-1)^i d_i([g_1|g_2|\cdots|g_{n-1}|g_n]),$$

com

$$d_i([g_1|g_2|\cdots|g_{n-1}|g_n]) = \begin{cases} g_1[g_2|g_3|\cdots|g_{n-1}|g_n], & \text{se } i=0, \\ [g_1|g_2|\cdots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\cdots|g_{n-1}|g_n], & \text{se } 1\leq i<n, \\ [g_1|g_2|g_3|\cdots|g_{n-2}|g_{n-1}], & \text{se } i=n, \end{cases}$$

para todo $[g_1|g_2|\cdots|g_{n-1}|g_n] \in X_n$ e todo $n \in \mathbb{Z}$.

Como X_0 é gerado por pelas 1-uplas dos elementos de G, na notação bar, temos que X_0 é o módulo livre sobre RG gerado pelo símbolo [ ], e assim, $X_0 \approx RG$, ou seja, eles são considerados isomorfos.

O restante da construção da resolução bar é igual à resolução normal, tendo em vista que só estamos mudando a forma de denotar os elementos do módulos X_n e, consequentemente, os homomorfismos ∂_n, para todo $n \in \mathbb{Z}$. Portanto, sendo a resolução normal uma resolução, a resolução bar também é.

Exemplo 2.3.1. *Podemos visualizar o que está acontecendo na resolução bar com, para todo* $[g_1, g_2, g_3] \in X_3$,

$$\begin{aligned} \partial_3([g_1,g_2,g_3]) &= \sum_{i=0}^{3}(-1)^i d_i([g_1|g_2|g_3]) \\ &= g_1[g_2|g_3] - [g_1g_2|g_3] + [g_1|g_2g_3] - [g_1|g_2]. \end{aligned}$$

Exemplo 2.3.2. *Agora, para todo* $[g_1, g_2] \in X_2$,

$$\begin{aligned} \partial_2([g_1,g_2]) &= \sum_{i=0}^{2}(-1)^i d_i([g_1|g_2]) \\ &= g_1[g_2] - [g_1g_2] + [g_1]. \end{aligned}$$

Exemplo 2.3.3. *Por fim, considerando o módulo* X_0 *temos, para todo* $[g_1] \in X_1$,

$$\begin{aligned} \partial_1([g_1]) &= \sum_{i=0}^{1}(-1)^i d_i([g_1]) \\ &= g_1[\,] - [\,]. \end{aligned}$$

2.4 Resolução bar normalizada

Considere o complexo de cadeias

$$\overline{X}_*\colon \cdots \longrightarrow \overline{X}_2 \xrightarrow{\bar{\partial}_2} \overline{X}_1 \xrightarrow{\bar{\partial}_1} \overline{X}_0 \xrightarrow{\varepsilon} R \longrightarrow 0.$$

de módulos sobre R, onde $\overline{X}_* = X_*/Y_*$ e Y_* é um subcomplexo de cadeias de X_*, com cada Y_n, para $n \geq 1$, sendo gerado pelos elementos $(g_0, g_1, \cdots, g_{n-1}, g_n) \in S_n$ tais que $g_i = g_{i+1}$, para algum $0 \leq i < n$, e $Y_0 = \{0\}$. Assim, temos $\overline{X}_0 \approx X_0 \approx RG$ e $\overline{X}_{-1} = R$.

Considerando então que $g_i = g_{i+1}$, temos como representante da órbita de

$$(g_0, g_1, \cdots, g_i, g_i, \cdots, g_{n-1}, g_n)$$

de Y_n por G o elemento

$$\begin{aligned} g_0^{-1}(g_0, g_1, \cdots, g_i, g_i, \cdots, g_{n-1}, g_n) &= (1, g_0^{-1}g_1, \cdots, g_0^{-1}g_i, g_0^{-1}g_i, \cdots, g_0^{-1}g_{n-1}, g_0^{-1}g_n) \\ &= (1, g_1', g_1'g_2', \cdots, g_1' \cdots g_i', g_1' \cdots g_i', \cdots, g_1' \cdots g_n'), \end{aligned}$$

tal que $g_j' = g_{j-1}^{-1}g_j$, para todo $j = 1, \cdots, n$. Na notação bar,

$$(1, g_1', g_1'g_2', \cdots, g_1' \cdots g_i', g_1' \cdots g_i', \cdots, g_1' \cdots g_n') = [g_1|g_2|\cdots|g_i|1|g_{i+2}|\cdots|g_{n-1}|g_n],$$

ou seja, Y_n é gerado pelos elementos $[g_1|g_2|\cdots|g_{n-1}|g_n]$ tais que $g_s = 1$, para algum $1 \leq s \leq n$.

Assim, cada $\overline{X}_n = X_n/Y_n$ é um módulo livre sobre RG gerado pelos elementos $[g_1|g_2|\cdots|g_{n-1}|g_n] + Y_n$, com $n \geq 1$ e $g_i \neq 1$, para todo $1 \leq i \leq n$. Note que Y_1 é gerado por $[1]$, assim $Y_1 \approx RG$ e, portanto, $\overline{X}_1 = X_1/Y_1$ é gerado pelos elementos $[g]$, com $g \in G$ tal que $g \neq 1$. Enquanto que no caso $n = 2$, Y_2 é gerado pelos elementos $[g_1|1]$ e $[1|g_2]$, com $g_1, g_2 \in G$, e, portanto, $\overline{X}_1 = X_1/Y_1$ é gerado pelos elementos $[g|h]$, com $g, h \in G$ tais que $g, h \neq 1$.

Para mostrarmos que o complexo de cadeias $\overline{X}_*$ é uma sequência exata, é suficiente mostrarmos que o homomorfismo ∂ e a homotopia de cadeias h da resolução padrão aplicam Y_* nele mesmo, mais precisamente,

$$\partial_n(Y_n) \subset Y_{n-1} \quad \text{e} \quad h_n(Y_n) \subset Y_{n+1},$$

para todo n. E isto de fato ocorre, pois dado $x \in Y_n$ podemos verificar que

$$d_j(x) \in Y_{n-1}$$

se $j \neq i$ ou $j \neq i+1$, e

$$d_i(x) = d_{i+1}(x),$$

onde

$$(-1)^i d_i(x) + (-1)^{i+1} d_{i+1}(x) = 0.$$

Logo, como

$$\partial_n(x) = \sum_{j=0}^{n} (-1)^j d_j(x),$$

temos

$$\partial_n(x) \in Y_{n-1}.$$

Além disso, temos

$$h(x) = (1, g_0, g_1, \cdots, g_i, g_i, \cdots, g_{n-1}, g_n) \in Y_{n+1}$$

Assim, ficam bem definidas as funções

$$\partial_n(\bar{x}) = \partial_n(x) + Y_{n-1} \quad \text{e} \quad h_n(\bar{x}) = h_n(x) + Y_{n+1},$$

para todo $\bar{x} \in \overline{X}_n$ e todo n. Analogamente à resolução padrão, pode-se mostrar que o homomorfismo induzido h é uma transformação de cadeias entre $id_{\overline{X}_*}$ e o homomorfismo trivial.

Desse modo, para todo n, têm-se $H_n(\overline{X}) = 0$ e daí

$$\mathrm{Ker}(\partial_n) = \mathrm{Img}(\partial_{n+1}).$$

Logo, $\overline{X}_*$ é exata.

Sendo $\overline{X}_n$ um módulo livre sobre RG, para cada $n \in \mathbb{Z}$, e a sequência $\overline{X}_*$ exata, segue que

$$\overline{X}_*\colon \cdots \longrightarrow \overline{X}_2 \xrightarrow{\bar{\partial}_2} \overline{X}_1 \xrightarrow{\bar{\partial}_1} \overline{X}_0 \xrightarrow{\varepsilon} R \longrightarrow 0.$$

é uma resolução livre de R sobre RG. Sendo uma resolução livre, ela é portanto uma resolução projetiva. Em ambos os casos, chamaremos essa resolução de resolução padrão normalizada. E quando usamos a notação bar para os elementos de $\overline{X}_n$, então essa resolução passa a ser chamada de resolução bar normalizada.

3 Cohomologia de grupos

Neste capítulo, dada uma resolução projetiva de R sobre RG aplicamos $\mathrm{Hom}_R(-, A)$ e assim obtemos um complexo de cocadeias e o n-ésimo grupo de cohomologia desse complexo de cadeias tomamos como sendo o n-ésimo grupo de cohomologia do grupo G. Na sequência, trabalhando com o grupo de (co)invariantes, conseguimos fazer uma relação entre $H^n(G, A)$ e A^G e A_G. Por fim, com a noção de grupo de derivações e de derivações principais conseguimos relacionar $H^1(G, A)$ com $\mathrm{Der}(G, A)$ e $P(G, A)$ tomando a resolução bar. Vale ressaltar que graças ao Teorema 2.1.9, os grupos de cohomologia independem da escolha da resolução pois o functor da categoria dos módulos sobre RG na categoria dos grupos abelianos preserva homotopia de cadeias. Para tanto, fizemos uso das referências (MUNKRES, 1984), (CASTRO, 2006) e (ROTMAN, 2009).

3.1 A cohomologia de grupos

Definição 3.1.1 (Grupo de cohomologia)**.** *Sejam $\varepsilon\colon X \longrightarrow R$ uma resolução projetiva de R sobre RG e A um módulo sobre RG. Considere o complexo de cocadeias*

$$\mathrm{Hom}_{RG}(X, A)\colon 0 \longrightarrow \mathrm{Hom}_{RG}(X_0, A) \xrightarrow{\delta^0} \mathrm{Hom}_{RG}(X_1, A) \xrightarrow{\delta^1} \cdots$$

com o operador cobordo δ dado por

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

para todo $f \in \mathrm{Hom}_{RG}(X_n, A)$ e todo $n \in \mathbb{Z}$.

O n-ésimo grupo de cohomologia de G com coeficientes em A é, para todo $n \in \mathbb{Z}$, definido por

$$H^n(G, A) = H^n(\mathrm{Hom}_{RG}(X, A)),$$

onde

$$H^n(\mathrm{Hom}_{RG}(X, A)) = \mathrm{Ker}(\delta^n)/\,\mathrm{Img}(\delta^{n-1}).$$

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

Note que graças ao Teorema 2.1.9, os grupos de cohomologia independem da resolução projetiva tomada. De fato, dadas $\varepsilon\colon X \longrightarrow R$ e $\varepsilon'\colon X' \longrightarrow R$ duas resoluções projetivas de R sobre RG, existe uma equivalência de homotopias $f\colon X \longrightarrow X'$. Se considerarmos o functor T da categoria dos módulos sobre RG na categoria dos grupos abelianos e os complexos de cocadeias $T(X)$ e $T(X')$, obtidos por aplicar T a X e a X',

respectivamente, então como T é aditivo, segue que T preserva homotopia de cadeias. Assim $T(f)$ é uma equivalência de homotopias.

Além disso, podemos notar que $H^n(G, A) = 0$, para todo $n \in \mathbb{Z}$, com $n < 0$. Isso advém da própria definição dos grupos de cohomologia.

Agora, para os demais resultados e exemplos faz-se necessário o conceito de grupo de (co)invariantes de um módulo sobre RG.

Definição 3.1.2 (Grupo de (co)invariantes)**.** *Sejam G um grupo e A um módulo sobre RG. O grupo de invariantes de A, denotado por A^G, é definido por*

$$A^G = \{a \in A |\, ga = a, \text{ para todo } g \in G\},$$

e o grupo de coinvariantes de A, denotado por A_G, é definido por

$$A_G = A/\langle ga - a |\, g \in G \text{ e } a \in A\rangle$$

Note que se a ação de G sobre A for trivial, isto é, $ga = a$, para todo $g \in G$, então $A^G = A = A_G$.

Note também que toda ação de G sobre A induz ação trivial de G sobre A^G e sobre A_G e assim, tanto A^G quanto A_G são módulos triviais sobre RG. E ainda, A^G é o maior submódulo de A no qual G atua trivialmente e A_G é o maior módulo quociente de A no qual G atua trivialmente.

Além disso, se A é um módulo sobre RG e considerando R como um módulo trivial sobre RG, podemos definir uma ação de G sobre $\mathrm{Hom}_R(R, A)$ de modo a torná-lo um módulo sobre RG. Essa ação é $\phi\colon G \times \mathrm{Hom}_R(R, A) \longrightarrow \mathrm{Hom}_R(R, A)$ dada por

$$\phi(g, f) = gf,$$

para todo $g \in G$ e todo $f \in \mathrm{Hom}_R(R, A)$, onde

$$(gf)(m) = gf(m),$$

para todo $m \in R$. Perceba que $(\mathrm{Hom}_R(R, A))^G = \mathrm{Hom}_{RG}(R, A)$, pois

$$\begin{aligned} gf = f &\iff (gf)(m) = f(m) \\ &\iff gf(m) = f(m) \\ &\iff gf(m) = f(gm), \end{aligned}$$

para todo $m \in R$.

Proposição 3.1.3. *Se A é um módulo sobre RG, então $H^0(G, A) \approx A^G$.*

Demonstração. Seja $\varepsilon\colon X \longrightarrow R$ uma resolução projetiva de R sobre RG. Como o functor da categoria dos módulos sobre RG na categoria dos grupos abelianos é exato, segue que a sequência

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Hom}_{RG}(R,A) & \xrightarrow{\varepsilon^*} & \mathrm{Hom}_{RG}(X_0,A) & \xrightarrow{\delta^0} & \mathrm{Hom}_{RG}(X_1,A) & \xrightarrow{\delta^1} & \cdots \\ & & & & \uparrow{\scriptstyle \delta^{-1}} & & & & \\ & & & & 0 & & & & \end{array}$$

é exata e daí ε^* é um monomorfismo e $\mathrm{Img}(\varepsilon^*) = \mathrm{Ker}(\delta^0)$. Assim,

$$\begin{aligned} H^0(G,A) &= \mathrm{Ker}(\delta^0)/\,\mathrm{Img}(\delta^{-1}) \\ &\approx \mathrm{Ker}(\delta^0) \\ &= \mathrm{Img}(\varepsilon^*) \\ &\approx \mathrm{Hom}_{RG}(R,A)/\,\mathrm{Ker}(\varepsilon^*) \\ &\approx \mathrm{Hom}_{RG}(R,A) \\ &= (\mathrm{Hom}_{RG}(R,A))^G \\ &\approx A^G, \end{aligned}$$

onde essa última passagem advém da Proposição 1.8.2. ■

Corolário 3.1.4. *Se A é um módulo trivial sobre RG, então $H^0(G,A) \approx A$.*

Demonstração. Como A é um módulo trivial sobre RG, temos que $A^G = A$. Pela Proposição 3.1.3, segue que $H^0(G,A) \approx A$. ■

Exemplo 3.1.5. *Sejam $G = \{1\}$ e A um módulo sobre RG. Então,*

$$H^n(G,A) = \begin{cases} A, & \text{se } n = 0 \\ 0, & \text{se } n > 0. \end{cases}$$

Temos que $RG \approx R$ e, pelo Exemplo 2.1.2, a sequência $0 \longrightarrow R \xrightarrow{id_R} R \longrightarrow 0$ é uma resolução livre (portanto projetiva) de R sobre RG.

Aplicando $\mathrm{Hom}_R(-, A)$, obtemos

$$0 \longrightarrow \mathrm{Hom}_R(R,A) \longrightarrow 0.$$

Mas como $\mathrm{Hom}_R(R,A) \approx A$ este complexo de cocadeias se reduz a

$$0 \longrightarrow A \longrightarrow 0.$$

Logo,

$$H^n(G,A) = \begin{cases} A^G, & \text{se } n = 0, \\ 0, & \text{se } n > 0, \end{cases}$$

mas como $A_G = A$, temos

$$H^n(G,A) = \begin{cases} A, & \text{se } n = 0, \\ 0, & \text{se } n > 0. \end{cases}$$

Exemplo 3.1.6. *Sejam $G =< t >\approx \mathbb{Z}$ o grupo cíclico infinito e A um módulo sobre RG. Então,*

$$H^n(G,A) = \begin{cases} A^G, & se\ n = 0, \\ A_G, & se\ n = 1, \\ 0, & se\ n > 1. \end{cases}$$

Pelo Exemplo 2.1.4, a sequência

$$0 \longrightarrow RG \xrightarrow{t-1} RG \xrightarrow{\varepsilon} R \longrightarrow 0,$$

com ε sendo a aplicação aumentação, é uma resolução projetiva de R sobre RG.

Aplicando $\mathrm{Hom}_R(-, A)$, obtemos o complexo de cocadeias

$$0 \xrightarrow{\delta^{-1}} \mathrm{Hom}_R(RG, A) \xrightarrow{\delta^0} \mathrm{Hom}_R(RG, A) \xrightarrow{\delta^1} 0,$$

com δ^0 sendo a multiplicação por $t-1$, pois

$$\begin{aligned} [\delta^0(f)](x) &= (f \circ (t-1))(x) \\ &= f((t-1)x) \\ &= (t-1)f(x), \end{aligned}$$

para todo $f \in \mathrm{Hom}_R(RG, A)$ e todo $x \in RG$. Mas como $\mathrm{Hom}_R(R, A) \approx A$ este complexo de cocadeias se reduz a

$$0 \xrightarrow{\delta^{-1}} A \xrightarrow{\delta^0} A \xrightarrow{\delta^1} 0.$$

Assim, $H^1(G,A) = \mathrm{Ker}(\delta^1)/\,\mathrm{Img}(\delta^0) = A/(t-1)A = A_G$ e $H^n(G,A) = 0$, para $n > 1$. Logo,

$$H^n(G,A) = \begin{cases} A^G, & \text{se } n = 0, \\ A_G, & \text{se } n = 1, \\ 0, & \text{se } n > 1. \end{cases}$$

Agora, calculemos os grupos de cohomologia de G para alguns módulos particulares:

1. Se A é um módulo trivial sobre RG, então

$$H^n(G,A) = \begin{cases} A, & \text{se } n = 0, \\ A, & \text{se } n = 1, \\ 0, & \text{se } n > 1. \end{cases}$$

2. Seja $A = \mathbb{Z}G$ visto como um módulo sobre $\mathbb{Z}G$ munido com a ação

$$t^k(rt^{k'}) = rt^{k+k'},$$

para todo $t^k, t^{k'} \in G$ e todo $r \in \mathbb{Z}$.

Então, $H^0(G,A) = A^G \approx 0$, pois $t^k t^{k'} \neq t^{k'}$ se $t^k \neq 1$.

Agora, determinemos A_G. Denotemos por $I = \langle t^k z - z |\, t^k \in G \text{ e } z \in A\rangle$ e $\overline{x} = x + I \in A/I = A_G$. Consideremos $y = t^k \in A$ com $k > 0$. Como $t^k - 1 = (t-1)(t^{k-1} + \cdots + t + 1) \in I$ segue que $\overline{t^k - 1} = \overline{0}$ e assim, $\overline{y} = \overline{t^k} = \overline{1}$ em A_G.

Por sua vez, se $y = t^{-k} \in A$ com $k > 0$, também temos $\overline{t^{-k}} = \overline{1}$, pois $t^{-k} = (1-t^k)t^{-k}+1$ e $\overline{1 - t^k} = \overline{0}$. Assim, para todo $x \in A$, com $x = r_0 t^k + r_1 t^{k+1} + \cdots + r_n t^{k+n}$ com $k, r_i \in \mathbb{Z}$, $n \geq 0$ e $i = 0, \cdots, n$, temos $\overline{x} = \overline{r_0 + r_1 + \cdots + r_n} = (r_0 + r_1 + \cdots + r_n)\overline{1}$. Daí, $H^1(G,A) = A_G \approx \mathbb{Z}$.

Portanto,

$$H^n(G,A) = \begin{cases} 0, & \text{se } n = 0, \\ \mathbb{Z}, & \text{se } n = 1, \\ 0, & \text{se } n > 1. \end{cases}$$

Proposição 3.1.7. *Se $G \approx \mathbb{Z}_n$ é um grupo cíclico finito não trivial, então não existe resolução projetiva de $\mathbb{Z}$ sobre $\mathbb{Z}G$ de comprimento finito.*

Demonstração. Suponha que exista

$$0 \longrightarrow X_k \xrightarrow{\partial_k} X_{k-1} \xrightarrow{\partial_{k-1}} \cdots \xrightarrow{\partial_2} X_1 \xrightarrow{\partial_1} X_0 \xrightarrow{\varepsilon} \mathbb{Z} \longrightarrow 0$$

uma resolução finita de $\mathbb{Z}$ sobre $\mathbb{Z}G$ de comprimento finito. Então, usando essa resolução, temos que $H^i(G,\mathbb{Z})$, para $i > k$. Mas, $H^i(G,\mathbb{Z}) \approx \mathbb{Z}_n$, para todo $i \geq 2$, o que nos dá uma contradição pois a cohomologia do grupo G independe da resolução escolhida.

Portanto, não existe resolução projetiva de $\mathbb{Z}$ sobre $\mathbb{Z}G$ de comprimento finito. ■

3.2 Uma interpretação de $H^1(G,A)$

Definição 3.2.1 (Grupo das derivações)**.** *Sejam G um grupo e A um módulo sobre RG. O grupo das derivações de G em A é definido por*

$$\mathrm{Der}(G,A) = \{d\colon G \longrightarrow A |\, d(gg') = d(g) + gd(g'),\ \textit{para todo } g, g' \in G\}$$

e o subgrupo das derivações principais por

$$P(G,A) = \{d_a \in \mathrm{Der}(G,A) |\, d_a(g) = ga - a,\ \textit{para todo } g \in G,\ \textit{com } a \in A\}.$$

Note que se $d \in \mathrm{Der}(G,A)$, então

$$\begin{aligned} d(1) &= d(1 \cdot 1) \\ &= d(1) + 1d(1) \\ &= d(1) + d(1), \end{aligned}$$

o que implica em $d(1) = 0$.

Além disso, note que se A é um módulo trivial sobre RG, então

$$\mathrm{Der}(G, A) = \mathrm{Hom}_R(G, A) \quad \text{e} \quad P(G, A) = 0.$$

Agora, faremos algumas considerações sobre a resolução bar e daremos uma interpretação de $H^1(G, A)$ em termos dos grupos de derivações e derivações principais.

Dado um grupo G, considere a resolução R sobre RG

$$X_*\colon \cdots \longrightarrow X_2 \xrightarrow{\partial_2} X_1 \xrightarrow{\partial_1} X_0 \xrightarrow{\varepsilon} R \longrightarrow 0.$$

como sendo a resolução bar. Assim, cada X_n, com $n \in \mathbb{Z}$ é um módulo livre sobre R gerado pelos símbolos

$$[g_1|\cdots|g_n]$$

e

$$\partial_n([g_1|g_2|\cdots|g_{n-1}|g_n]) = \sum_{i=0}^{n}(-1)^i d_i([g_1|g_2|\cdots|g_{n-1}|g_n]),$$

com

$$d_i([g_1|g_2|\cdots|g_{n-1}|g_n]) = \begin{cases} g_1[g_2|g_3|\cdots|g_{n-1}|g_n], & \text{se } i = 0, \\ [g_1|g_2|\cdots|g_{i-1}|g_ig_{i+1}|g_{i+2}|\cdots|g_{n-1}|g_n], & \text{se } 1 \leq i < n, \\ [g_1|g_2|g_3|\cdots|g_{n-2}|g_{n-1}], & \text{se } i = n, \end{cases}$$

para todo $[g_1|g_2|\cdots|g_{n-1}|g_n] \in X_n$ e todo $n \in \mathbb{Z}$.

Consideremos $C^*(G, A) = \mathrm{Hom}_{RG}(X_*, A)$ e $C^n(G, A) = \mathrm{Hom}_{RG}(X_n, A)$. Logo, um elemento $f \in C^n(G, A)$ é um homomorfismo $f\colon X_n \longrightarrow A$ identificando $[g_1|\cdots|g_n]$ com $(g_1, \cdots, g_n)$. Podemos enxergar $f\colon G^n \longrightarrow A$ como uma função de n variáveis. Por convenção, G^0 é um conjunto com um único elemento (por exemplo o elemento $[\,]$) de modo que $C^0(G, A) \approx A$.

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

$$(\delta^{n-1}(f))(g_1, \cdots, g_n) = f(\partial_n(g_1, \cdots, g_n)).$$

Exemplo 3.2.2. *Para $n = 1$, temos que o operador cobordo se comporta da seguinte maneira:*

$$\begin{aligned}(\delta^0(f))(g_1) &= f(\partial_1(g_1)) \\ &= g_1 f([\,]) - f([\,]),\end{aligned}$$

para todo $f \in C^1(G, A)$ e todo $g_1 \in G$.

Exemplo 3.2.3. *Para $n = 2$, temos que o operador cobordo se comporta da seguinte maneira:*

$$\begin{aligned}(\delta^1(f))(g_1, g_2) &= f(\partial_1(g_1g_2)) \\ &= g_1 f(g_2) - f(g_1g_2) + f(g_1),\end{aligned}$$

para todo $f \in C^2(G, A)$ e todos $g_1, g_2 \in G$.

Proposição 3.2.4. *Se G é um grupo e A um módulo sobre RG, então*

$$H^1(G, A) \approx \mathrm{Der}(G, A)/P(G, A).$$

Demonstração. Considere o complexo de cocadeias

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

definido anteriormente. Por definição

$$H^1(G, A) \approx \mathrm{Ker}(\delta^1)/\,\mathrm{Img}(\delta^0).$$

Temos:

1. $\mathrm{Ker}(\delta^1) = \mathrm{Der}(G, A)$:

   Seja $f \in C^1(G, A)$. Então, $f\colon G \longrightarrow A$ e $\delta^1(f)\colon G^2 \longrightarrow A$ é tal que

   $$(\delta^1(f))(g_1, g_2) = g_1 f(g_2) - f(g_1 g_2) + f(g_1),$$

   para todos $g_1, g_2 \in G$.

   Assim,

   $$\begin{aligned} f \in \mathrm{Ker}(\delta^1) &\iff \delta^1(f) = 0 \\ &\iff (\delta^1(f))(g_1, g_2) = 0 \\ &\iff f(g_1 g_2) = f(g_1) + g_1 f(g_2) \\ &\iff f \in \mathrm{Der}(G, A), \end{aligned}$$

   para todos $g_1, g_2 \in G$. Portanto, $\mathrm{Ker}(\delta^1) = \mathrm{Der}(G, A)$.

2. $\mathrm{Img}(\delta^0) = P(G, A)$:

   Se $d \in \mathrm{Img}(\delta^0)$, então existe $f\colon G^0 \longrightarrow A$ com $\delta^0(f) = d$. Assim, para todo $g_1 \in G$,

   $$\begin{aligned} d(g_1) &= (\delta^0(f))(g_1) \\ &= g_1 f([\,]) - f([\,]). \end{aligned}$$

   Como $f([\,]) \in A$, segue que $f([\,]) = a \in A$. Daí,

   $$d(g) = g_1 a - a,$$

   ou seja, $d \in P(G, A)$.

   Reciprocamente, se $d \in P(G, A)$, então $d(g_1) = g_1 a - a$, para algum $a \in A$ e todo $g_1 \in G$. Seja $f\colon G^0 \longrightarrow A$ tal que $f([\,]) = a$, para todo $[\,] \in G^0$. Logo,

   $$d(g_1) = (\delta^0(f))(g_1),$$

   para todo $g_1 \in G$ e, portanto, $d \in \mathrm{Img}(\delta^0)$.

Disso, concluímos que $H^1(G,A) \approx \mathrm{Der}(G,A)/P(G,A)$. ■

Corolário 3.2.5. *Se G é um grupo e A um módulo trivial sobre RG, então $H^1(G,A) \approx \mathrm{Hom}_R(G,A)$.*

Demonstração. Da Proposição 3.2.4 temos que $H^1(G,A) \approx \mathrm{Der}(G,A)/P(G,A)$. Como A é um módulo trivial sobre RG, temos que

$$\mathrm{Der}(G,A) = \mathrm{Hom}_R(G,A) \quad \text{e} \quad P(G,A) = 0.$$

Portanto, $H^1(G,A) \approx \mathrm{Hom}_R(G,A)$. ■

Exemplo 3.2.6. *Seja G um grupo e A um módulo trivial sobre $\mathbb{Z}G$. Temos que:*

i. Se $G = \langle t \rangle \approx \mathbb{Z}$ é o grupo cíclico infinito e $A = \mathbb{Z}_n$, com $n \in \mathbb{Z}_+^*$, então $H^1(G,A) \approx \mathbb{Z}_n$.

ii. Se $G = \langle t \rangle \approx \mathbb{Z}_n$ é o grupo cíclico finito de ordem n, com $n \in \mathbb{Z}_+$, e $A = \mathbb{Z}$, então $H^1(G,A) \approx 0$.

iii. Se $G = \langle t \rangle \approx \mathbb{Z}_n$ é o grupo cíclico finito de ordem n, com $n \in \mathbb{Z}_+$, e $A = \mathbb{Z}_2$, então $H^1(G,A) \approx \mathbb{Z}_2$.

Com efeito:

i. Como G é cíclico gerado por t os homomorfismos de G em A são dados por

$$f_i(t^k) = \overline{ik},$$

com $0 \leq i \leq n-1$, para todo $t^k \in G$. Daí, $\mathrm{Hom}_R(G,A) \approx \mathbb{Z}_n$. Logo,

$$H^1(G,A) \approx \mathrm{Der}(G,A) = \mathrm{Hom}_R(G,A) \approx \mathbb{Z}_n.$$

Portanto, $H^1(G,A) \approx \mathbb{Z}_n$.

ii. O único homomorfismo de G em A é o homomorfismo nulo, daí

$$H^1(G,A) \approx \mathrm{Der}(G,A) = \mathrm{Hom}_R(G,A) \approx 0.$$

Portanto, $H^1(G,A) \approx 0$.

iii. Temos que os homomorfismos de G em A são dados por

$$f_i(t^k) = \overline{ik},$$

com $i = 0, 1$, para todo $t^k \in G$. Assim,

$$H^1(G,A) \approx \mathrm{Der}(G,A) = \mathrm{Hom}_R(G,A) \approx \mathbb{Z}_2.$$

Portanto, $H^1(G,A) \approx \mathbb{Z}_2$.

Conclusão

Como pudemos ver, trabalhar com a cohomologia de grupos não é algo complicado, pois podemos associar $H^n(G, A)$, com $n \in \mathbb{Z}$, ao seus grupos de (co)invariantes A^G e A_G, e também conseguimos enxergar $H^1(G, A)$ com uma face mais amigável quando trabalhamos com seu grupo de derivação e de derivação principal, isto é, conseguimos estabelecer que $H^1(G, A) \approx \mathrm{Der}(G, A)/P(G, A)$, sendo G um grupo qualquer e A um módulo qualquer sobre RG. Mas para alcançar esses resultados necessitamos de um vasto arsenal de conceitos e resultados sobre álgebra homológica, principalmente os que envolvem módulos livres, módulos sobre RG, complexos de (co)cadeias, módulos de homomorfismo e módulos projetivos. Esses resultados foram essenciais para a construção do que chamamos de resoluções (livres e projetivas), que nada mais são que casos particulares de complexos de cadeias, e mostrar sua independência via homotopia de caminhos.

Porém, ainda poderíamos fazer uma abordagem da cohomologia de grupos em espaços topológicos, fazendo jus assim à motivação da construção dessa teoria, veja (WEIBEL, 2021). Nessa perspectiva utilizaríamos como ponte os espaços de Eilenberg-MacLane, que serviria como conectivos entre a álgebra homológica e a teoria de homologia singular por meio do seguinte resultado:

"Se X é um complexo de Eilenberg-MacLane do tipo $(G, 1)$ e A um módulo trivial sobre RG, então $H^*(G, A) \approx H^*(X, A)$."

Contudo, para explorar essa interpretação topológica, seria necessário a construção do que chamamos teoria de homotopia e teoria de homologia singular. Trabalharíamos assim com homotopias (que são coisas diferentes de homotopia de cadeias), espaços de recobrimento, recobrimento universal e o primeiro grupo fundamental, no que tange a teoria de homotopia; e p-simplexos, grupos de homologia de um espaço topológico, equivalência de homotopias e CW-complexos, no que tange a teoria de homologia singular.

A decisão de não abordarmos a interpretação topológica da cohomologia de grupos adveio do tamanho desse trabalho de conclusão de curso e do fato da temática abordada aqui, isto é, álgebra homológica, resoluções e cohomologia de grupos, já consistir um campo considerado avançado para a graduação. Desta forma, para os futuros matemáticos que utilizarão este material para o próprio desenvolvimento de seus trabalhos de conclusão de curso ou iniciação científica, deixamos esse caminho em aberto para ser explorado.

Referências

BROWN, K. S. *Cohomology of Groups*. Nova Iorque: Springer-Verlag, 1992.

CASTRO, F. R. de. *Cohomologia de Grupos e Algumas Aplicações*. Dissertação (Mestrado) — Universidade Estadual Paulista "Júlio de Mesquita Filho", Instituto de Biociências, Letras e Ciências Exatas, São José do Rio Preto, 2006.

FIDELIS, A. A.; COELHO, F. R. de C. Resoluções projetivas: Qual escolher? qual sua importância? In: NASCIMENTO, C. do (Ed.). *Anais da XXI SEMAT e XI SEMEST*. Faculdade de Matemática, 2021. p. 52–55. Disponível em: <https://drive.google.com/file/d/1vJZcbuC4C7cpXBVSI5VqE1PwkFDUy3z_/view>. Acesso em: 24 jan. 2022.

HATCHER, A. *Algebraic Topology*. Cambridge: Cambridge University Press, 2002.

HU, S.-T. *Introduction to Homological Algebra*. São Francisco: Holden-Day, Inc., 1968.

MUNKRES, J. R. *Elements of Algebraic Topology*. Califórnia: Addison-Wesley Publishing Company, 1984.

ROTMAN, J. J. *An Introduction to Homological Algebra*. Nova Iorque: Springer Science, 2009.

WEIBEL, C. A. *History of Homological Algebra*. 2021. 40 p. HA history. Disponível em: <https://sites.math.rutgers.edu/~weibel/HA-history.pdf>. Acesso em: 11 mar. 2022.