Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós–Graduação em Matemática
Mestrado em Matemática

Cohomologia Local de Módulos sobre Anéis Invariantes

Pedro Henrique Oliveira Pantoja

João Pessoa – PB
Julho de 2017

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós–Graduação em Matemática
Mestrado em Matemática

Cohomologia Local de Módulos Sobre Anéis Invariantes

por

Pedro Henrique Oliveira Pantoja.

sob a orientação do

Prof. Dr. Roberto Callejas Bedregal

e coorientação do

Prof. Dr. Napoleón Caro Tuesta

João Pessoa – PB
14 de Julho de 2017

Catalogação na publicação
Seção de Catalogação e Classificação

P198c Pantoja, Pedro Henrique Oliveira.
Cohomologia local de módulos sobre anéis invariantes / Pedro Henrique Oliveira Pantoja. - João Pessoa, 2017.
94 f.

Orientador: Roberto Callejas Bedregal.
Coorientador: Napoleón Caro Tuesta.
Dissertação (Mestrado) - UFPB/CCEN

1. Matemática. 2. Cohomologia local. 3. Anéis invariantes. 4. Anéis Gorenstein. I. Título.

UFPB/BC

Cohomologia Local de Módulos Sobre Anéis Invariantes

por

Pedro Henrique Oliveira Pantoja [1]

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática da Universidade Federal da Paraíba como requisito parcial para a obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra.

Aprovada em 14 de Julho de 2017.

Banca Examinadora:

Prof. Dr. Roberto Callejas Bedregal – UFPB
(Orientador)

Prof. Dr. Napoleón Caro Tuesta
(Examinador Interno)

Luis A. Alba S.

Prof. Dr. Luis Alba Sarria –
(Examinador Externo)

[1]O autor foi bolsista do CNPq/CAPES durante a elaboração desta dissertação.

*"Ao querido amigo Dr.
Luis Alberto Alba Sarria,
pela inestimável ajuda na
realização deste presente
trabalho ".*

Agradecimentos

Primeiramente gostaria de agradecer à Deus, pois sem ele nem existiria. Agradeço a minha querida mãe Rosangêla e a todos os meus familiares pelo cuidado, amor e dedicação em todos esses anos de convivência.

Agradeço ao meu orientador Roberto, coorientador Napoleon, pela confiança depositada e pela ajuda acadêmica.

Gostaria de compartilhar minha felicidade junto aos meus inúmeros amigos que fiz em João Pessoa: Luis, Raiza, Zé, Poli, Tony, Rich, Wendy, Tarcy, Cris, Cássio, Manu, Licy, Rebeca, Igor, Itallo, Ianne, Fernando, Fernanda, Tião, Nildo, Mauri, Fran, Txutxu, Belly, Sally, Alan, Sérgio, Marcius, Maria, Lucas, Marcos, Raoni, Clecle e Mariana.

Aos amigos de Natal: Pardal, Volpato, Was, Nandinho, Tetê, Deilton, Thais, Tufão, Paulo, Renato, FK, Yuri (171), Carol e Nane. Aos Amigos de Araruna: Neymar, Carmem, Ceará e Pedro.

Não poderia me esquecer dos amigos que fiz em Portugal: Hugo, Társio, Dénis (acento agudo mesmo!), James, Camila, Daniel, Regina e Mara.

Agradeço aos meus professores do Mestrado pelo conhecimento adquirido: Elisandra, Andrade, Adriano, Cleto, Mirian, Manassés e Hinojosa. Agradeço também à secretária Roseli.

Também gostaria de lembrar alguns professores da UFRN que marcaram minha trajetória na graduação: Ronaldo, C. Gomes, Júlia e Jonas. Em especial aos professores: Iesus, Benedito e Nir Cohen. Agradeço à Pedro Duarte (Universidade de Lisboa).

Meus sinceros agradecimento ao Pr. Alcimar pela amizade ao longo de mais de 14 anos e à família Vasconcelos.

Gostaria de Dedicar também essa realização ao Professor Elmano, que já faleceu há alguns anos, todavia marcou muito a minha formação matemática quando fui seu aluno pela primeira vez em 2005.

Finalmente, agradeço à CAPES e ao CNPq pelo apoio financeiro.

"Eu posso aceitar o fracasso. Todo mundo falha em alguma coisa. Mas eu não posso aceitar não tentar".

Michael Jordan

Resumo

Neste trabalho estudamos cohomologia local de módulos sobre anéis invariantes inspirados nos resultados de Sharp, Huneke e Lyubeznik. De fato, o principal resultado foi demonstrado por Tony J. Puthenpurakal:

Sejam K um corpo e R um domínio regular contendo K. Seja G um subgrupo finito do grupo dos automorfismos de R. Suponhamos que $|G|$ é inversível em K. Seja R^G o anel dos invariantes de G. Seja I um ideal de R^G. Fixe $i \geq 0$, se R^G é Gorenstein então:

(I) $injdim_{R^G} H^i_I(R^G) \leq dimsupp\ H^i_I(R^G)$;

(II) $H^j_{\mathfrak{m}}(H^i_I(R^G))$ é injetivo, onde $\mathfrak{m}$ é um ideal maximal de R^G;

(III) $\mu_j(P, H^i_I(R^G)) = \mu_j(P', H^i_{IR}(R))$ onde P' é qualquer ideal primo sobre P.

Também iremos demonstrar que se P é um ideal primo de R^G com R^G_P não Gorenstein então os números de Bass $\mu_j(P, H^i_I(R^G))$ são zero para todo j ou existe c tal que $\mu_j(P, H^i_I(R^G)) = 0$ para $j < c$ e $\mu_j(P, H^i_I(R^G)) > 0$ para todo $j \geq c$.

Palavras Chaves: Cohomologia Local, Anéis Gorenstein, Anéis Invariantes.

Abstract

In this work we study local cohomology of modules on invariant rings inspired by the results of Sharp, Huneke and Lyubeznik. In fact the main result was demonstrated by Tony J. Puthenpurakal:

Let K be a field and let R be a regular domain containing K. Let G be a finite subgroup of the group of automorphisms of R. We assume that $|G|$ is invertible in K. Let R^G be the ring of invariants of G. Let I be an ideal in R^G. Fix $i \geq 0$, if R^G is Gorenstein then:

(I) $injdim_{R^G} H^i_I(R^G) \leq dimsupp\ H^i_I(R^G)$;

(II) $H^j_{\mathfrak{m}}(H^i_I(R^G))$ is injective, where $\mathfrak{m}$ is any maximal ideal of R^G;

(III) $\mu_j(P, H^i_I(R^G)) = \mu_j(P', H^i_{IR}(R))$ where P' is any prime in R lying above.

We also prove that if P is a prime ideal in R^G with R^G_P not Gorenstein then either the Bass number $\mu_j(P, H^i_I(R^G))$is zero for all j or there exists c such that $\mu_j(P, H^i_I(R^G)) = 0$ for $j < c$ and $\mu_j(P, H^i_I(R^G)) > 0$ for all $j \geq c$.

Keywords: Local Cohomology, Gorenstein Ring, Invariant Ring.

Notações

A seguir, listamos algumas notações utilizadas neste trabalho.

• $\mathfrak{m}, \mathfrak{n}$, denotam ideais maximais de um anel;

• $\mathfrak{p}, \mathfrak{q}$, denotam ideais primos de um anel;

• id denota a aplicação identidade;

• $\square$ denota o final de uma demonstração;

• $ht(I)$ denota a altura de um ideal I;

• $Ass(M)$ denota o conjunto dos primos associados do módulo M;

• $dim(A)$ denota a dimensão (de Krull) de um anel A;

• $Spec(A)$ denota o conjunto de todos os ideais primos de um anel A;

• $Aut(A)$ denota o conjunto de todos os automorfismos de A;

• $Supp(M)$ denota o suporte de um A-módulo, i.e., $\{P \in spec(A) \mid M_P \neq 0\}$;

• $J(A)$ denota o radical de Jacobson de A;

• $char(A)$ denota a característica de A;

• $Var(I)$ denota a variedade de I, isto é, o conjunto $\{\mathfrak{p} \in Spec(A) \mid \mathfrak{p} \supseteq I\}$;

• $1_A, 1_G$ denotam as identidades do anel A e do grupo G, respectivamente.

• $\mathcal{M}_{n\times n}(R)$ denota o conjunto de todas as matrizes quadradas de ordem n e entradas no anel R;

Sumário

Introdução

Historicamente, Hilbert, em sua célebre lista de problemas, no ínicio do século XX elaborou uma lista de 23 problemas que iriam desafiar os matemáticos por um longo período. O 14° problema pode ser formulado como: Sejam K um corpo e $x_1, ..., x_n$ elementos algebricamentes independentes sobre K. Seja L um subcorpo de $K[x_1, ..., x_n]$ contendo K. É o anel $K[x_1, ..., x_n] \cap L$ finitamente gerado sobre K? O matemático japonês Masayoshi Nagata em 1958 deu uma resposta negativa a essa afirmação. Em tal complicado e longo contraexemplo figura-se um polinômio de 32 variáveis!!!

Uma pergunta interessante seria em que casos menos gerais do anterior teríamos uma resposta positiva. No seguinte caso especial do 14° problema obtemos isso: Seja R um anel de polinômios em n variáveis sobre o corpo dos complexos $\mathbb{C}$ e G um grupo finito, denotemos R^G o subanel dos polinômios G-invariantes, i.e., os polinômios $f(x)$ tais que $f(gx) = f(x),\ \forall\ g\ \in\ G\ e\ x\ \in\ \mathbb{C}^n$. Então R^G é finitamente gerada como $\mathbb{C}$-álgebra.

Neste trabalho, com base no artigo de Tony J. Puthenpurakal ([20]), estudamos questões relacionadas a cohomologia local de módulos sobre anéis invariantes. Neste texto R será um anel comutativo Noetheriano. Se M é um R-módulo e se $\mathfrak{a}$ é um ideal de R, denotemos por $H^i_{\mathfrak{a}}(M)$ o i-ésimo módulo de cohomologia local com respeito a $\mathfrak{a}$. No artigo clássico ([10]), Sharp e Huneke provaram que se R é um anel regular contendo um corpo de característica $p > 0$, e se $\mathfrak{a}$ é um ideal de R então os módulos de cohomologia local de R com respeito a $\mathfrak{a}$ têm as seguintes propriedades:

(i) $H^i_{\mathfrak{m}}(H^j_{\mathfrak{a}}(R))$ é injetivo, onde $\mathfrak{m}$ é qualquer ideal maximal de R;

(ii) $injdim_R H^i_{\mathfrak{a}}(R) \leq \dim \operatorname{Supp} H^i_{\mathfrak{a}}(R)$;

(iii) Os números de Bass de $H^i_{\mathfrak{a}}(R)$ são finitos;

(iv) O conjunto dos primos associados de $H^i_{\mathfrak{a}}(R)$ é finito. (isso segue de (iii). Com efeito, temos que $\mathfrak{p} \in AssM \Leftrightarrow \mu^0(\mathfrak{p}, M) > 0$.)

Aqui $injdim_R H^i_{\mathfrak{a}}$ denota a dimesão injetiva de $H^i_{\mathfrak{a}}(R)$. Também $\operatorname{Supp} M = \{P \in Spec(R \mid M_P \neq 0)\}$ denota o suporte do R-módulo M. O j-ésimo número de Bass do

R-módulo M com respeito ao ideal primo P é definido como

$$\mu_j(P,M) = \dim_{k(P)} \operatorname{Ext}^j_{R_P}(k(P), M_P) \quad \textit{onde } k(P) \textit{ denota o corpo residual de } R_P.$$

Em um outro notável artigo, para anéis regulares de característica zero, Lyubeznik foi capaz de estabelecer as propriedades acima para uma classe consideravelmente maior de funtores, do que apenas os módulos de cohomologia local, vide ([16]). Em particular para os ideais $\mathfrak{a}_1, \mathfrak{a}_2, ..., \mathfrak{a}_n$ em R e $T(R) = H^{i_1}_{\mathfrak{a}_1}(H^{i_2}_{\mathfrak{a}_2}(\cdots H^{i_n}_{\mathfrak{a}_n}(R)\cdots))$, então $T(R)$ satisfaz as seguintes propriedades:
(i) $H^j_{\mathfrak{m}}(T(R))$ é injetivo, onde $\mathfrak{m}$ é qualquer ideal maximal de R;
(ii) $injdim_R T(R) \leq \dim \operatorname{Supp} T(R)$;
(iii) Para todo ideal maximal $\mathfrak{m}$, o número de primos associados de $T(R)$ contido em $\mathfrak{m}$ é finito;
(iv) Os números de Bass de $T(R)$ são finitos.

É importante salientar que para qualquer ideal maximal $\mathfrak{m}$ de R o resultado acima implica que $H^i_{\mathfrak{m}}(T(R))$ é uma soma direta em um número finito de cópias de $E_R(R/\mathfrak{m})$. Com efeito, por (i) $H^i_{\mathfrak{m}}(T(R))$ é injetivo, daí uma soma direta de cópias de $E_R(R/\mathfrak{m})$. Esse número de cópias é igual a $s = \mu_0(\mathfrak{m}, H^i_{\mathfrak{m}}(T(R)))$ que é finito por (iv). Em suma,

$$H^i_{\mathfrak{m}}(T(R)) = E_R(R/\mathfrak{m})^s. \tag{1}$$

Isto, por sua vez, levantou a questão de se os resultados (i)$-$(iv) de Huneke e Sharp (na característica $p > 0$) poderia ser estendida a esta classe maior de funtores. Em ([17]), Lyubeznik prova isso. Para anéis singulares resultados análogos como esse em geral são falsos. Hartshorne deu um exemplo de um anel singular R, um ideal $\mathfrak{a}$ e um ideal maximal $\mathfrak{m}$ de R tal que $\mu_0(\mathfrak{m}, H^2_{\mathfrak{a}}(R))$ é infinito, vide ([11], seção 3). Singh deu um primeiro exemplo de um anel singular R tendo um ideal $\mathfrak{a}$ para o qual $Ass_R(H^i_{\mathfrak{a}}(R))$ é infinito, vide ([31]). Neste exemplo o anel R não está contido em um corpo. Mais tarde, Katzman, vide ([14]), deu um exemplo de uma álgebra afim R sobre um corpo (e também de um anel local contendo um corpo) possuindo um ideal $\mathfrak{a}$ tal que $\operatorname{Ass}_R H^i_{\mathfrak{a}}(R)$ é infinito. Depois Singh e Swanson deram exemplos parecidos de anéis tendo somente singularidades racionais, vide ([32]).

Em um artigo interessante Núñez-Betancourt, provaram que se $S \to R$ é um homomorfismo Noetheriano de anéis que cinde, então para todo ideal $\mathfrak{a}$ em S e todo inteiro não nagativo i, se $\operatorname{Ass}_R H^i_{\mathfrak{a}R}(R)$ é finito então $\operatorname{Ass}_R H^i_{\mathfrak{a}}(R)$ também o é. Além do mais se, R é Cohen-Macaulay e finitamente gerado como um S-módulo e todos os números de Bass do R-módulo $H^i_{\mathfrak{a}R}$ são finitos, então todos os números de Bass do S-módulo $H^i_{\mathfrak{a}}(S)$ também são finitos.

Um caso em que o resultado acima é válido é quando R é um domínio regular contendo um corpo K e G é um grupo finito agindo em R com $|G|$ inversível em K e $S = R^G$. Nesse caso, o resultado é mais forte:

Teorema 0.1. *Sejam K um corpo e R um domínio regular contendo K. Seja G um subgrupo finito dos grupos dos automorfismos de R. Admita que $|G|$ é inversível em K. Considere R^G o anel dos invariantes de G e $\mathfrak{a}_1, \mathfrak{a}_2, ..., \mathfrak{a}_r$ ideais em R^G. Chamamos $T(R) = H^{i_1}_{\mathfrak{a}_1}(H^{i_2}_{\mathfrak{a}_2}(\cdots H^{i_r}_{\mathfrak{a}_r}(R^G)\cdots)$ para alguns $i_1, ..., i_r \geq 0$.*
(i) Se R^G é Gorenstein então;
(a) $injdim_{R^G} T(R^G) \leq \dim \operatorname{Supp} T(R^G)$;
(b) Seja $P \in Spec(R^G)$. Então $\mu_j(P, T(R^G)) = \mu_j(P', T(R))$ onde
$T(R) = H^{i_1}_{\mathfrak{a}_1}(H^{i_2}_{\mathfrak{a}_2 R}(\cdots H^{\mathfrak{a}_r}_{\mathfrak{a}_r R}(R)\cdots)$ e P' um ideal primo qualquer sobre P.
(ii) Seja $P \in Spec(R^G)$, com R^G_P não Gorenstein. Então para todo $j \geq 0$ os números de Bass $\mu_j(P, T(R^G))$ são zero para todo j ou existe c tal que $\mu_j(P, T(R^G)) = 0$ para $j < c$ e $\mu_j(P, T(R^G)) > 0$ para todo $j \geq c$.

O principal exemplo em que o Teorema se aplica é quando $R = K[X_1, ..., X_n]$ ou $R = K[[X_1, ..., X_n]]$ e G um subgrupo finito de $GL_n(K)$ agindo linearmente em R, com $|G|$ inversível em K. Neste caso, devemos observar que, por um resultado K. Watanabe, R^G é Gorenstein se $G \subseteq SL_n(K)$; vide ([33]). Seja $R = K[X_1, ..., X_n]$ onde K é um corpo de característica zero e G é um subgrupo finito de $GL_n(K)$ agindo linearmente sobre R. Seja $D(R)$ o anel dos operadores K-lineares diferenciaveis em R. É bem conhecido que $D(R)$ é isomorfo a $A_n(K)$, a n-ésima álgebra de Weyl sobre K.

Teorema 0.2. *(Com as hipóteses acima). Seja $\mathfrak{a}$ um ideal em R^G. Então para todo $i \geq 0$, $H^i_{\mathfrak{a}}(R^G)$ possui comprimento finito como $D(R^G)$-módulo.*

Nosso trabalho, está dividido:

- No *Capítulo* 1, estudamos algumas ferramentas necessárias ao desenvolvimento do capítulo 2, tais como funtor torção, cohomologia local e dual de Matlis;
- O *Capítulo* 2 é dedicado aos resultados de anéis invariantes;
- O *Capítulo* 3 é dedicado aos resultados de cohomologia local relacionados aos anéis invariantes;
- No *Apêndice A*, falamos sucintamente de módulos injetivos;
- Finalmente, o *Apêndice B* discutimos brevemente sobre os anéis dos operadores diferenciáveis, os anéis e módulos Cohen Macaulay, anéis Gorenstein.

A grande maioria dos resultados do Capítulo 1 e Apêndice B não são demonstrados e tão poucos explorados em sua total generalidade, para evitar que esse texto seja demasiadamente extenso e cansativo. Recomendamos ao leitor interessado que busque mais sobre o assunto nas referências.

Capítulo 1

Preliminares

Neste capítulo inicial, apresentamos o funtor torção, que nos permite calcular um dos objetos principais de estudo deste trabalho, o *módulo de cohomologia local.* Por fim, apresentamos algumas propriedades do funtor dual de Matlis que serão relevantes nos próximos capítulos. Todos os anéis aqui serão comutativos e com identidade.

1.1 Funtor Torção

Definição 1.1. Para cada R-módulo M, o módulo *torção de M* é definido por:

$$\Gamma_{\mathfrak{a}}(M) := \{m \in M : \mathfrak{a}^n m = 0 \text{ para algum } \ n \in \mathbb{N}\} = \bigcup_{n\in\mathbb{N}} (0 :_M \mathfrak{a}^n)$$

Observe que $\Gamma_{\mathfrak{a}}(M)$ é um submódulo de M. Além disso,

$$\Gamma_{\mathfrak{a}}(M) = \{m \in M / Var(\text{Ann}M) \subseteq Var(\mathfrak{a})\}.$$

De fato, se $m \in \Gamma_{\mathfrak{a}}(M)$, então $\mathfrak{a}^n m = 0$ para algum $n \in \mathbb{N}$, ou seja, $\mathfrak{a}^n \subseteq \text{Ann}(m)$. Daí, $Var(\text{Ann}(m)) \subseteq Var(\mathfrak{a}^n) = Var(\mathfrak{a})$. Reciprocamente, se $Var(\text{Ann}(m)) \subseteq Var(\mathfrak{a})$, então $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}} \subseteq \sqrt{Ann(m)}$. Como R é noetheriano , segue que $\mathfrak{a}^n m = 0$ para algum $n \in \mathbb{N}$.

Cada homomorfismo de R-módulos $f : M \to N$ induz um homomorfismo de R-módulos:

$$\Gamma_{\mathfrak{a}}(f) : \Gamma_{\mathfrak{a}}(M) \to \Gamma_{\mathfrak{a}}(N),$$

definido por $\Gamma_{\mathfrak{a}}(f)(m) = f(m)$, ou seja $\Gamma_{\mathfrak{a}}(f) = f\mid_{\Gamma_{\mathfrak{a}}(M)}$. Notemos que $\Gamma_{\mathfrak{a}}(f)$ está bem definida pois $\text{Ann}f(m) \supseteq \text{Ann}(m) \Rightarrow Var(\text{Ann}f(m)) \subseteq Var(\text{Ann}(m))$.

Isto define um funtor linear $\Gamma_{\mathfrak{a}}(-)$ sobre a categoria dos R-módulos, chamado *funtor $\mathfrak{a}$-torção.* Agora observe que

$$(0:_M \mathfrak{a}^n) \cong Hom\left(\frac{R}{\mathfrak{a}^n}, M\right), \tag{1.1}$$

em particular,

$$Hom_R(R, M) \cong M. \tag{1.2}$$

Obviamente temos as inclusões:

$$(0:_M \mathfrak{a}^n) \subseteq (0:_M \mathfrak{a}^{n+1}) \subseteq ...$$

Portanto, temos um sistema direto de Hom's e consequentemente o funtor torção pode ser escrito como limite direto: $\Gamma_{\mathfrak{a}}(M) \cong \varinjlim_n \mathrm{Hom}_R(R/\mathfrak{a}^n, M)$. O último isomorfismo é válido em virtude de (1.1) e também porque o seguinte diagrama comuta para todo $n \in \mathbb{N}$:

$$\begin{tikzcd}
(0:_M \mathfrak{a}^n) \arrow[r, "\iota_n"] \arrow[d, "\tau_n"] & (0:_M \mathfrak{a}^{n+1}) \arrow[d, "\tau_{n+1}"] \\
Hom_R\left(\frac{R}{\mathfrak{a}^n}, M\right) \arrow[r, "\pi_n^*"] & Hom_R\left(\frac{R}{\mathfrak{a}^{n+1}}, M\right).
\end{tikzcd}$$

Para cada R-módulo M, seja DZ_R o conjunto dos divisores de zero de R em M e seja NDZ_R o conjunto dos não divisores de zero de R em M. Em outras palavras,

$$DZ_R := \{x \in R \mid \exists\ m \in M \backslash \{0\} : xm = 0\};$$

$$NDZ_R := R \backslash DZ_R.$$

Temos o seguinte:

Lema 1.2. Seja M um R-módulo.
(a) Se $\Gamma_{\mathfrak{a}}(M) \neq 0$, então, $\mathfrak{a} \subseteq DZ_R(M)$.
(b) Sejam R um anel noetheriano e M um R-módulo finitamente gerado. Se $\mathfrak{a} \subseteq DZ_R(M)$, então, $\Gamma_{\mathfrak{a}}(M) \neq 0$.

Demonstração. (a) Trivial.
(b) Como M é noetheriano o conjunto $Ass_R(M)$ é finito, assim podemos escrever $Ass_R(M) = \{\mathfrak{p}_1, ..., \mathfrak{p}_r\}$. Entretanto

$$DZ_R = \bigcup_{\mathfrak{p} \in Ass_R(M)} \mathfrak{p}$$

donde $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$. Pelo lema da esquiva (Prime Avoidance) existe $i \in \{1, ..., r\}$ com $\mathfrak{a} \subseteq \mathfrak{p}_i$. Como $\mathfrak{p}_i \in Ass_R(M)$ existe algum $0 \neq v \in M$ tal que $\mathfrak{p}_i = (0 :_R Rv)$. Portanto, $\mathfrak{a}v \subseteq \mathfrak{p}_i v = 0 \Rightarrow v \in \Gamma_{\mathfrak{a}}(M) \backslash \{0\}$. □

Observação 1.3 (Propriedades do Funtor Torção). Sejam M um R-módulo e $\mathfrak{a}$, $\mathfrak{b}$ ideais de R.

1) $\Gamma_0(M) = M$ e $\Gamma_R(M) = 0$
2) Se $\mathfrak{b} \subseteq \mathfrak{a}$, então, $\Gamma_{\mathfrak{a}}(M) \subseteq \Gamma_{\mathfrak{b}}(M)$
3) Se R é noetheriano e $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$, então, $\Gamma_{\mathfrak{a}}(M) = \Gamma_{\mathfrak{b}}(M)$
4) $\Gamma_{\mathfrak{a}+\mathfrak{b}}(M) = \Gamma_{\mathfrak{a}}(M) \cap \Gamma_{\mathfrak{b}}(M) = \Gamma_{\mathfrak{a}}(\Gamma_{\mathfrak{b}}(M))$
5) Se M é noetheriano, então existe $n \in \mathbb{N}$ tal que $\Gamma_{\mathfrak{a}}(M) = (0 :_M \mathfrak{a}^n)$.
6) Se R é noetheriano e M é finitamente gerado, então existe $n \in \mathbb{N}$ tal que $\mathfrak{a}^n M \cap \Gamma_{\mathfrak{a}}(M) = 0$.

Definição 1.4. Um R-módulo M é chamado $\mathfrak{a}$-*torção* se $\Gamma_{\mathfrak{a}}(M) = M$ e é chamado *livre de* $\mathfrak{a}$-*torção* se $\Gamma_{\mathfrak{a}}(M) = 0$.

Observação 1.5. (i) Na propriedade 5, tomando $\mathfrak{a} = \mathfrak{b}$, temos $\Gamma_{\mathfrak{a}}(\Gamma_{\mathfrak{a}}(M)) = \Gamma_{\mathfrak{a}}(M)$. Logo, $\Gamma_{\mathfrak{a}}(M)$ é $\mathfrak{a}$-torção.

(ii) Se M é de $\mathfrak{a}$-torção e N um submódulo de M, então N e M/N são de $\mathfrak{a}$-torção. Reciprocamente, se R é noetheriano e N é um submódulo de M tal que N e M/N são $\mathfrak{a}$-torção, então M é de $\mathfrak{a}$-torção.

(iii) Sejam $r \in \mathfrak{a}$ e M um R-módulo $\mathfrak{a}$-torção, então $M \xrightarrow{\cdot r} M$ é injetivo $\Leftrightarrow M = 0$.

Proposição 1.6. O funtor $\mathfrak{a}$-torção $\Gamma_{\mathfrak{a}}(-)$ é exato à esquerda.

Demonstração. Seja $0 \to L \xrightarrow{f} M \xrightarrow{g} N \to 0$ uma sequência exata de R-módulos. Queremos mostrar que

$$0 \to \Gamma_{\mathfrak{a}}(L) \xrightarrow{\Gamma_{\mathfrak{a}}(f)} \Gamma_{\mathfrak{a}}(M) \xrightarrow{\Gamma_{\mathfrak{a}}(g)} \Gamma_{\mathfrak{a}}(N) \text{ é exato.}$$

Como f é um homomorfismo injetivo, então, $\Gamma_{\mathfrak{a}}(f)$ claramente é injetivo. Por outro lado, $\Gamma_{\mathfrak{a}}(g) \circ \Gamma_{\mathfrak{a}}(f) = 0$, pois $g \circ f = 0$. Portanto im $(\Gamma_{\mathfrak{a}}(f)) \subseteq \ker(\Gamma_{\mathfrak{a}}(g))$. Para provar a inclusão contrária, seja $m \in \ker(\Gamma_{\mathfrak{a}}(g))$, isto é, $g(m) = 0$ e $m \in \Gamma_{\mathfrak{a}}(M)$, então existe $n \in \mathbb{N}$ tal que $\mathfrak{a}^n m = 0$. Como $\ker g = \operatorname{im} f$, então $f(l) = m$ para algum $l \in L$. Note que $l \in \Gamma_{\mathfrak{a}}(L)$, de fato, para cada $r \in \mathfrak{a}^n$ temos $f(rl) = rf(l) = rm = 0 \Rightarrow rl = 0$ pois f é um homomorfismo injetor. Assim $\mathfrak{a}^n l = 0$. □

Observação 1.7. (i) Seja N uma extensão essencial (vide apêndice) de M. Então, $\Gamma_{\mathfrak{a}}(N)$ é uma extensão essencial de $\Gamma_{\mathfrak{a}}(M)$. De fato, seja $0 \neq H \leq \Gamma_{\mathfrak{a}}(N)$. Em particular, $0 \neq H \leq N$, logo existe $0 \neq h \in H \cap M$, então existe $n \in \mathbb{N}$ tal que $\mathfrak{a}^n h = 0$, portanto $h \in H \cap \Gamma_{\mathfrak{a}}(M)$

(ii) Sejam R noetheriano, E um R-módulo injetivo (vide apêndice), então $\Gamma_{\mathfrak{a}}(E)$ é um R-módulo injetivo ([4], Prop. 2.1.4).

(iii) Seja R noetheriano. Se $E(M)$ denota a envoltória injetiva (vide apêndice) de um R-módulo M, então:

$$\Gamma_{\mathfrak{a}}(E(M)) = E(\Gamma_{\mathfrak{a}}(M))$$

De fato, por (i), $\Gamma_{\mathfrak{a}}(E(M))$ é extensão essencial de $\Gamma_{\mathfrak{a}}(M)$, Além disso, por (ii), $\Gamma_{\mathfrak{a}}(E(M))$ é injetivo. Logo, $\Gamma_{\mathfrak{a}}(E((M))$ é a envoltória injetiva de $\Gamma_{\mathfrak{a}}(M)$.

Exemplo 1.8. Sejam $\mathfrak{p}, \mathfrak{q}$ ideais primos de R. Temos:

$$\Gamma_{\mathfrak{p}}(R/\mathfrak{q}) = \begin{cases} R/\mathfrak{q} & se\ \mathfrak{p} \supseteq \mathfrak{q} \\ 0 & se\ \mathfrak{p} \not\supseteq \mathfrak{q} \end{cases}$$

Solução 1.9. Com efeito, $\Gamma_{\mathfrak{p}}(R/\mathfrak{q}) = \{r + \mathfrak{q} \mid \mathfrak{p}^n r \subseteq \mathfrak{q}\ \exists n \geq 1\}$. Assim se $\mathfrak{p} \not\subseteq \mathfrak{q} \Rightarrow \mathfrak{p}^n \not\subseteq \mathfrak{q}$ logo $r \in \mathfrak{q} \Rightarrow r + \mathfrak{q} = 0$, ou seja, $\Gamma_{\mathfrak{p}}(R/\mathfrak{q}) = 0$. Se $\mathfrak{p} \subseteq \mathfrak{q} \Rightarrow \mathfrak{p}^n r \subseteq \mathfrak{q}$, para todo r, donde $\Gamma_{\mathfrak{p}}(R/\mathfrak{q}) = R/\mathfrak{q}$. A prova está completa.

Lema 1.10. Sejam R noetheriano, M um R-módulo, o módulo $M/\Gamma_{\mathfrak{a}}(M)$ é livre de $\mathfrak{a}$-torção.

Demonstração. Queremos mostrar que $\Gamma_{\mathfrak{a}}(M/\Gamma_{\mathfrak{a}}(M)) = 0$. Seja $m \in M$ tal que o elemento $m + \Gamma_{\mathfrak{a}}(M) \in M/\Gamma_{\mathfrak{a}}(M)$ é anulado por $\mathfrak{a}^n$ para algum $n \in \mathbb{N}$. Queremos mostrar que $m + \Gamma_{\mathfrak{a}}(M) = 0$, ou seja, $m \in \Gamma_{\mathfrak{a}}(M)$. Assim $\mathfrak{a}^n(m + \Gamma_{\mathfrak{a}}(M)) = 0 \Rightarrow \mathfrak{a}^n m \subseteq \Gamma_{\mathfrak{a}}(M)$. Desde que $\mathfrak{a}^n m$ é um submódulo finitamente gerado de $\Gamma_{\mathfrak{a}}(M)$ e cada elemento de $\mathfrak{a}^n m$ é anulado por alguma potência de $\mathfrak{a}$ segue que existe $t \in \mathbb{N}$ tal que $\mathfrak{a}^t \mathfrak{a}^n m = 0$. Portanto $m \in (0 :_M \mathfrak{a}^{t+n}) \subseteq \Gamma_{\mathfrak{a}}(M)$. □

Lema 1.11. Sejam R um anel noetheriano e M um R-módulo $\mathfrak{a}$-torção finitamente gerado. Então $Ass_R(M) = Ass_R(0 :_M \mathfrak{a})$.

Demonstração. Por (1.3, item 5) existe $m \in \mathbb{N}$ tal que $M = \Gamma_{\mathfrak{a}}(M) = (0 :_M \mathfrak{a}^m)$. Portanto,

$$Ass_R(M) = Ass_R(0 :_M \mathfrak{a}^m) = Ass_R\left(Hom_R\left(\frac{R}{\mathfrak{a}^m}, M\right)\right) = Supp\left(\frac{R}{\mathfrak{a}^m}\right) \cap Ass_R(M)$$

$$= Supp\left(\frac{R}{\mathfrak{a}}\right) \cap Ass_R(M) = Ass_R\left(Hom_R\left(\frac{R}{\mathfrak{a}}, M\right)\right) = Ass_R(0 :_M \mathfrak{a}).$$

□

Proposição 1.12. Seja M um R-módulo noetheriano. Então:
(a) $Ass_R(\Gamma_{\mathfrak{a}}(M)) = Ass_R(M) \cap Var(\mathfrak{a})$.
(b) Se R é noetheriano, então $Ass_R(M/\Gamma_{\mathfrak{a}}(M)) = Ass_R(M) \backslash Var(\mathfrak{a})$.

Demonstração. (a) ($\subseteq$) Seja $\mathfrak{p} \in Ass_R(\Gamma_{\mathfrak{a}}(M))$. Como $\Gamma_{\mathfrak{a}}(M)$ é submódulo de M tem-se $\mathfrak{p} \in Ass_R(M)$. Como M é noetheriano existe $n \in \mathbb{N}$ tal que $\mathfrak{a}^n\Gamma_{\mathfrak{a}}(M) = 0 \Rightarrow \mathfrak{a}^n \subseteq (0 :_R \Gamma_{\mathfrak{a}}(M))$ portanto[1] $\mathfrak{a}^n \subseteq \mathfrak{p} \Rightarrow \mathfrak{a} \subseteq \mathfrak{p}$, pois $\mathfrak{p}$ é primo. Logo $\mathfrak{p} \in Var(\mathfrak{a})$.
($\supseteq$) Seja $\mathfrak{p} \in Ass_R(M) \cap Var(\mathfrak{a})$. Então, existe algum $v \in M$ com $(0 :_R Rv) = \mathfrak{p}$. Como $\mathfrak{a} \subseteq \mathfrak{p}$ então $\mathfrak{a}v = 0$ daí $v \in \Gamma_{\mathfrak{a}}(M)$. Segue que $\mathfrak{p} \in Ass_R(\Gamma_{\mathfrak{a}}(M))$.
(b) ($\supseteq$) Seja $\mathfrak{p} \in Ass_R(M)$. Portanto $\mathfrak{p} \in Ass_R(\Gamma_{\mathfrak{a}}(M)) \cup Ass_R(M/\Gamma_{\mathfrak{a}}(M))$. Se $\mathfrak{p} \notin Var(\mathfrak{a})$, então, $\mathfrak{p} \notin Ass_R(\Gamma_{\mathfrak{a}}(M))$ daí $\mathfrak{p} \in Ass_R(M/\Gamma_{\mathfrak{a}}(M))$.
($\subseteq$) Seja $\mathfrak{p} \in Ass_R(M/\Gamma_{\mathfrak{a}}(M))$. Por (1.10) e pelo fato de $M/\Gamma_{\mathfrak{a}}(M)$ ser noetheriano, existe algum $x \in NDZ_R(M/\Gamma_{\mathfrak{a}}(M)) \cap \mathfrak{a}$ (1.2). Agora $\mathfrak{p} \subseteq DZ_R(M/\Gamma_{\mathfrak{a}}(M))$ segue que $x \notin \mathfrak{p}$.

Pela nossa escolha de $\mathfrak{p}$ encontramos um $\overline{v} \in M/\Gamma_{\mathfrak{a}}(M)$ com $(0 :_R R\overline{v}) = \mathfrak{p}$. Seja $v \in M$ tal que $\overline{v} = v + \Gamma_{\mathfrak{a}}(M)$. Assim $\mathfrak{p}\overline{v} = 0 \Rightarrow \mathfrak{p}v \subseteq \Gamma_{\mathfrak{a}}(M)$. Mas M é noetheriano $\exists\ n \in \mathbb{N} : \mathfrak{a}^n\Gamma_{\mathfrak{a}}(M) = 0 \Rightarrow \mathfrak{p}(Rx^nv) = x^n\mathfrak{p}v \subseteq \mathfrak{a}^n\Gamma_{\mathfrak{a}}(M) = 0$ donde $\mathfrak{p} \subseteq (0 :_R Rx^nv)$. Seja $a \in (0 :_R Rx^nv) \Rightarrow (ax^n)v = a(x^nv) = 0 \in \Gamma_{\mathfrak{a}}(M) \Rightarrow ax^n\overline{v} = 0 \Rightarrow ax^n \in (0 :_R R\overline{v}) = \mathfrak{p}$. Como $x \notin \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ daí $(0 :_R Rx^nv) \subseteq \mathfrak{p}$. Logo $\mathfrak{p} = (0 :_R Rx^nv) \Rightarrow \mathfrak{p} \in Ass_R(M)$. Finalmente como $\mathfrak{p} \in \mathfrak{a}$ tem-se $\mathfrak{p} \in Var(\mathfrak{a})$.

□

Os seguintes fatos (que podem ser encontrados em [?]), serão úteis na demonstração de (1.15).

Lema 1.13. Sejam A um anel, S um conjunto multiplicativo. Então o módulo M tem uma estrutura compatível de um $S^{-1}A$-módulo se, e somente se, para todo $s \in S$, o mapa multiplicação por s, $\mu_s : M \to M$ é uma bijeção.

Lema 1.14. Sejam A um anel, S um conjunto multiplicativo e M um A-módulo. Então $M = S^{-1}M$ se, e somente se, M é um $S^{-1}A$-módulo.

A última proposição desta seção será usada com frequência no capítulo 3.

Proposição 1.15. Sejam A um anel noetheriano e $\mathfrak{m}$ um ideal maximal em A. Seja M um A-módulo $\mathfrak{m}$-torção (M não necessita ser finitamente gerado). Então $M = M_{\mathfrak{m}}$.

[1] já que $Ass_R(\Gamma_{\mathfrak{a}}(M)) \subseteq Var(0 :_R \Gamma_{\mathfrak{a}}(M))$.

Demonstração. Pelos resultados anteriores é suficiente provar que para todo $s \in A \backslash \mathfrak{m}$ o mapa $\mu_s : M \to M$, pela multiplicação por s, é um isomorfismo. Primeiramente, provaremos que μ_s é sobrejetivo. Seja $t \in M$. Como M é um módulo $\mathfrak{m}$-torção existe $n \geq 1$ tal que $\mathfrak{m}^n t = 0$. Observe que $\mathfrak{m} \subsetneq \mathfrak{m} + As \subseteq A \Rightarrow \mathfrak{m} + As = A$, donde $\mathfrak{m}^n + As = A$.[2] Seja $1 = \xi + as$ onde $\xi \in \mathfrak{m}^n$ e $a \in A$. Assim $t = \xi t + ast = ast \Rightarrow \mu_s(at) = t$, donde μ_s é sobrejetiva. Para mostrar a injetividade de μ_s, digamos que $\mu_s(t) = 0 \Rightarrow st = 0$. De $\mathfrak{m}^n t = 0$, e $1 = \xi + as$, onde $\xi \in \mathfrak{m}^n, a \in A$ tem-se $t = \xi t + ast = 0$. Daí μ_s é injetiva, e portanto $M = M_{\mathfrak{m}}$, como se buscava. □

1.2 Módulo de Cohomologia Local

Definição 1.16. Seja $i \geq 0$, o i-ésimo funtor derivado a direita de $\Gamma_{\mathfrak{a}}(-)$ é denotado por $H^i_{\mathfrak{a}}(-)$ e é chamado *i-ésimo funtor de Cohomologia Local* com respeito ao ideal $\mathfrak{a}$. Isto é, para cada R-módulo M,

$$H^i_{\mathfrak{a}}(M) = H^i(\Gamma_{\mathfrak{a}}(E^\bullet)),$$

onde $E^\bullet$ é uma resolução injetiva de M.

Para calcular $H^i_{\mathfrak{a}}(M)$ procedemos da seguinte forma: Tome uma resolução injetiva de M:

$$0 \to M \xrightarrow{\alpha} E^0 \xrightarrow{d^0} E^1 \to \cdots \to E^n \xrightarrow{d^n} E^{n+1} \to \cdots$$

Aplique o funtor $\Gamma_{\mathfrak{a}}(-)$ para obter:

$$0 \to \Gamma_{\mathfrak{a}}(E^0) \xrightarrow{\Gamma_{\mathfrak{a}}(d^0)} \cdots \to \Gamma_{\mathfrak{a}}(E^n) \xrightarrow{\Gamma_{\mathfrak{a}}(d^n)} \Gamma_{\mathfrak{a}}(E^{n+1}) \to \cdots$$

Tomando a i-ésima cohomologia deste complexo, obtemos:

$$H^i_{\mathfrak{a}}(M) = \ker(\Gamma_{\mathfrak{a}}(d^i))/\mathrm{im}\,(\Gamma_{\mathfrak{a}}(d^{i-1})).$$

Quando $M = R$, escreveremos apenas $H^c_{\mathfrak{a}}(R) := H^c_{\mathfrak{a}}$.

Proposição 1.17. Seja M um R-módulo e $\mathfrak{a}$ e $\mathfrak{b}$ ideais de R.

a) $H^0_{\mathfrak{a}}(M) \simeq \Gamma_{\mathfrak{a}}(M)$ e $H^i_{\mathfrak{a}}(M)$ é $\mathfrak{a}$-torção para cada $i > 0$.

b) Se R é noetheriano e $\sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}$, então $H^i_{\mathfrak{a}}(M) = H^i_{\mathfrak{b}}(M)$ para cada $i > 0$. Em particular, $H^i_{\mathfrak{a}\mathfrak{b}}(M) = H^i_{\mathfrak{a}\cap\mathfrak{b}}(M)$ para cada $i > 0$.

[2] Já que se I, J são ideais de um anel A, $\sqrt{I} + \sqrt{J} = A \Rightarrow I + J = A$, e obviamente $\sqrt{\mathfrak{m}^n} = \mathfrak{m}$.

c) Seja $\{M_\lambda\}$ uma família de R-módulos. Para cada inteiro n, temos

$$H^n_{\mathfrak{a}}(\bigoplus_\lambda M_\lambda) = \bigoplus_\lambda H^n_{\mathfrak{a}}(M_\lambda)$$

d) Uma sequência exata de R-módulos $0 \to M' \to M \to M'' \to 0$ induz uma sequência exata em cohomologia local

$$\cdots H^n_{\mathfrak{a}}(M') \to H^n_{\mathfrak{a}}(M) \to H^n_{\mathfrak{a}}(M'') \to H^{n+1}_{\mathfrak{a}}(M') \to \cdots$$

Demonstração. Ver ([13], Prop. 7.3). □

Lema 1.18. Sejam $\mathfrak{a}$ um ideal e M um R-módulo.
(a) Se M é $\mathfrak{a}$-torção então $H^i_{\mathfrak{a}}(M) = 0$ para todo $i > 0$.
(b) Para cada R-módulo N e cada $i > 0$ tem-se

$$H^i_{\mathfrak{a}}(\Gamma_{\mathfrak{a}}(N)) = 0 \ \ e \ \ H^i_{\mathfrak{a}}(N) \cong H^i_{\mathfrak{a}}(N/\Gamma_{\mathfrak{a}}(N)).$$

Demonstração. Vide ([4], Corolário 2.1.7). □

Seja M um R-módulo, um elemento $x \in R$ é dito *regular* se $xm \neq 0$ para todo $0 \neq m \in M$. Uma sequência $x_1, \ldots, x_n$ de elementos de R é uma *M-sequência* (de comprimento n) se:

(1) x_1 é M-regular, x_2 é (M/x_1M)-regular, x_n é $M/(x_1, ..., x_{n-1})M$-regular

(2) $(M/(x_1, ..., x_n)M) \neq 0$

Dizemos que uma M-sequência $x_1, \cdots x_n \in \mathfrak{a}$ é *máxima* (em $\mathfrak{a}$) se, para qualquer $x_{n+1} \in \mathfrak{a}$, a sequência $x_1, \cdots, x_{n+1} \in \mathfrak{a}$ não é uma M-sequência. Dizemos que uma *M-sequência fraca* se satisfaz apenas a condição (1) acima.

Lema 1.19. Sejam R um anel, e M, N R-módulos. Considere $\mathfrak{a} = (0 : N)$.
(a) Se $\mathfrak{a}$ contém um elemento M-regular, então, $Hom_R(N, M) = 0$.
(b) Inversamente, se R é noetheriano e M, N são finitamente gerados, com $Hom_R(N, M) = 0$, então, $\mathfrak{a}$ contém um elemento M-regular.

Demonstração. Vide ([6], prop. 1.2.3). □

Lema 1.20. Sejam R um anel, e M, N R-módulos e $\underline{x} = x_1, \cdots x_n$ uma M-sequência fraca em $(0 : N)$. Então:

$$Hom_R\left(N, \frac{M}{\underline{x}M}\right) \cong Ext^n_R(N, M).$$

Demonstração. A prova é por indução em n. O caso $n = 0$ é fácil já que $Hom_R(N, M) \cong Ext_R^0(N, M)$. Suponhamos que o resultado vale para todo natural menor que n. É claro que $\underline{x'} = x_1, ..., x_{n-1}$ é uma M-sequência fraca e daí

$$Hom_R\left(N, \frac{M}{\underline{x'}M}\right) \cong Ext_R^{n-1}(N, M).$$

Por outro lado x_n não é divisor de zero de $\frac{M}{\underline{x'}M}$ e $x_n \in (0 : N)$ donde,

$$Hom_R\left(N, \frac{M}{\underline{x'}M}\right) = 0 \Rightarrow Ext_R^{n-1}(N, M) = 0.$$

Consideremos a sequência exata

$$0 \to M \xrightarrow{\cdot x_1} M \to \frac{M}{x_1 M} \to 0.$$

Pela sequência longa dos ext's tem-se:

$$0 = Ext_R^{n-1}(N, M) \to Ext_R^{n-1}\left(N, \frac{M}{x_1 M}\right) \xrightarrow{\partial} Ext_R^n(N, M) \xrightarrow{\delta}$$

$$Ext_R^n(N, M) \to Ext_R^n\left(N, \frac{M}{x_1 M}\right) \to ...$$

Assim sendo δ induzida pela multiplicação por $x_1 \in (0 : N) \Rightarrow \delta \equiv 0$.

Portanto, $Ext_R^{n-1}(N, \frac{M}{x_1 M}) \cong Ext_R^n(N, M)$ via ∂. Em virtude de $x_1, ..., x_n$ ser M-sequência fraca, a hipótese de indução implica $Ext_R^{n-1}(N, \frac{M}{x_1 M}) \cong Hom_R(N, \frac{M}{\underline{x}M})$ nos garante o isomorfismo $Ext_R^n(N, M) \cong Hom_R(N, \frac{M}{\underline{x}M})$.

$\square$

Teorema 1.21 (Rees)**.** *Seja R um anel noetheriano, M um R-módulo finitamente gerado, e $\mathfrak{a}$ um ideal de R tal que $\mathfrak{a}M \neq M$. Então todas as M-sequências máximas em $\mathfrak{a}$ têm o mesmo comprimento n dado por*

$$n = \min\{i : \mathrm{Ext}_R^i(R/\mathfrak{a}, M) \neq 0\}.$$

Demonstração. Sejam $\underline{x} = x_1, ..., x_n$ uma M-sequência maximal em $\mathfrak{a}$ e $\overline{M} = \frac{M}{(x_1, ..., x_n)M}$. Como $\mathfrak{a}$ contém um elemento $\overline{M}$-regular para $i = 1, ..., n$ tem-se

$$Ext_R^{i-1}\left(\frac{R}{\mathfrak{a}}, M\right) \cong Hom_R\left(\frac{R}{\mathfrak{a}}, \overline{M}\right) = 0.$$

Logo,

$$Ext_R^j\left(\frac{R}{\mathfrak{a}}, M\right) = 0 \ \forall \ j \leq n-1.$$

e mais por (1.19),

$$Ext_R^n\left(\frac{R}{\mathfrak{a}}, M\right) \cong Hom_R\left(\frac{R}{\mathfrak{a}}, \frac{M}{\underline{x}M}\right) \neq 0.$$

provando o teorema.

□

Este resultado nos permite introduzir a seguinte definição.

Definição 1.22. Sejam M um R-módulo e a um ideal de R tal que $\mathfrak{a}M \neq M$. Definimos a $\mathfrak{a}$-*profundidade* de M como sendo o maior comprimento de uma M-sequência com elementos em $\mathfrak{a}$. Denotamos a $\mathfrak{a}$-profundidade de M como grade$(\mathfrak{a}, M)$. No caso em que $M = R$, escrevemos a $\mathfrak{a}$-profundidade de R como grade $\mathfrak{a}$.

Definição 1.23. Seja $(R, \mathfrak{m})$ anel noetheriano local e M um R-módulo finitamente gerado então o $\mathfrak{m}$-profundidade de M é chamado profundidade de M, denotado por $profM$.

Proposição 1.24. Seja R um anel noetheriano, $\mathfrak{a}$ ideal de R e M um R-módulo finitamente gerado. Então:

a) grade$(\mathfrak{a}, M) = \inf\{profM_{\mathfrak{p}} : \mathfrak{p} \in Var(\mathfrak{a})\}$

b) grade$(\mathfrak{a}, M) =$ grade$(\sqrt{\mathfrak{a}}, M)$

c) Se $x = x_1, \cdots, x_n$ é uma M-sequência em a, então

$$\text{grade}(\mathfrak{a}, M/xM) = \text{grade}(\mathfrak{a}, M) - n.$$

Demonstração. Vide ([6], 1.2.10). □

Exemplo 1.25. Sejam M um R-módulo e $(x_1, ..., x_n)$ uma M-sequência em $\mathfrak{a}$. Então:

$$H_{\mathfrak{a}}^i(M) = 0, \ \textit{para todo} \ i < r.$$

Existe uma caracterização de grade envolvendo cohomologia local.

Teorema 1.26. *Seja M um R-módulo finitamente gerado tal que $\mathfrak{a}M \neq M$. Então* grade$(\mathfrak{a}, M) = min\{i \ \in \mathbb{N} \mid H_{\mathfrak{a}}^i(M) \neq 0\}$.

Demonstração. Seja $c = \operatorname{grade}(\mathfrak{a}, M)$. Usaremos indução em c. Quando $c = 0$, todo elemento de $\mathfrak{a}$ deve ser um divisor de zero de M e então $\Gamma_{\mathfrak{a}}(M) \neq 0$ pelo lema (1.2). Agora suponha que $c > 0$ e que este resultado vale para cada R-módulo N finitamente gerado e com $\mathfrak{a}N \neq N$ e $\operatorname{grade}(\mathfrak{a}, N) < c$.

Existe $x_1 \in \mathfrak{a}$ tal que x_1 é um não divisor de zero de M. Seja $M_1 := M/x_1M$. Observe que $x_1M_1 \neq M_1$ e $\operatorname{grade}(\mathfrak{a}, M_1) = c - 1$. Portanto, pela hipótese de indução, $H^i_{\mathfrak{a}}(M_1) = 0$ para todo $i < c - 1$, enquanto $H^{c-1}_{\mathfrak{a}}(M_1) \neq 0$. A sequência exata

$$0 \to M \xrightarrow{.x_1} M \to M_1 \to 0$$

induz uma sequência exata longa

$$H^{i-1}_{\mathfrak{a}}(M) \to H^{i-1}_{\mathfrak{a}}(M_1) \to H^i_{\mathfrak{a}}(M) \xrightarrow{.x_1} H^i_{\mathfrak{a}}(M)$$

Isto mostra que para $i < c$, o elemento x_1 é um não divisor de zero em $H^i_{\mathfrak{a}}(M)$, como este módulo é a-torção, ele deve ser zero (1.5), (iii)). Temos portanto a sequência exata

$$0 \to H^{c-1}_{\mathfrak{a}}(M_1) \to H^c_{\mathfrak{a}}(M)$$

E desde que $H^{c-1}_{\mathfrak{a}}(M_1) \neq 0$, segue que $H^c_{\mathfrak{a}}(M_1) \neq 0$. □

Seja M um R-módulo não nulo. A dimensão de Krull, $\dim M$ ou $\dim_R M$ de M é o supremo do comprimento das medidas das cadeias de ideais primos no suporte de M, se esse supremo existe, e é igual a ∞, caso contrário. Quando M é finitamente gerado a dimensão de M coincide com $\dim R/ann(M)$, isto é, a dimensão do anel $R/ann(M)$. Os próximos dois teoremas encontram-se em ([4]).

Teorema 1.27. *(**Teorema de Anulamento de Grothendieck**) Seja M um R-módulo. Então, $H^i_{\mathfrak{a}}(M) = 0$ para todo $i > \dim M$.*

Teorema 1.28. *(**Teorema de Não Anulamento**) Sejam $(R, \mathfrak{m})$ local e M um R-módulo não nulo finitamente gerado de dimensão d. Então, $H^d_{\mathfrak{m}}(M) \neq 0$.*

Assim nas hipóteses do teorema acima, em vista do teorema de anulamento de Grothendieck, $d = dimM$ é o menor inteiro para o qual $H^i_{\mathfrak{m}}(M) \neq 0$.

Definição 1.29. Seja x um elemento de R e seja R_x a localização de R em x. O complexo de Čech em x é o complexo:

$$\check{C}^{\bullet}_x : 0 \to R \xrightarrow{\iota} R_x \to 0,$$

com o módulo R de grau 0 e R_x de grau -1, onde $\iota(r) = r/1$ é a aplicação canônica. Para uma sequência $\underline{x} = x_1, \ldots, x_n$ de elementos em R. Definimos o *Complexo de Čech em* $\underline{x}$ como sendo:

$$\check{C}^{\bullet}_{\underline{x}} = \check{C}^{\bullet}_{x_n} \otimes_R \cdots \otimes_R \check{C}^{\bullet}_{x_n}$$

Explicitamente

$$\begin{aligned} \check{C}^{\bullet}_{\underline{x}} \;&:= \\ & 0 \to R \to \bigoplus_{1}^{n} R_{x_i} \to \bigoplus_{i<j} R_{x_i x_j} \to \cdots \to R_{x_1 \cdots x_n} \to 0 \end{aligned}.$$

Exemplo 1.30. (Complexo de Čech para $n = 2$) Vamos estudar efetivamente o caso $n = 2$.

Solução 1.31. Sejam

$$\check{C}^{\bullet}_{x} := \; 0 \to R \xrightarrow{\iota_x} R_x \to 0,$$

$$\check{C}^{\bullet}_{y} := \; 0 \to R \xrightarrow{\iota_y} R_y \to 0.$$

Então:

$$\check{C}^{\bullet}_{x} \otimes \check{C}^{\bullet}_{y} := \; 0 \to R \otimes R \xrightarrow{\iota^*} (R \otimes R_y) \oplus (R_x \otimes R) \xrightarrow{\tau^*} R_x \otimes R_y \to 0,$$

onde definimos $\iota^*(a \otimes b) = (a \otimes \frac{b}{1}, \frac{a}{1} \otimes b)$ e $\tau^*(a \otimes \frac{b}{y^m}, \frac{c}{x^m} \otimes d) = \frac{a}{1} \otimes \frac{b}{y^m} - \frac{c}{x^m} \otimes \frac{d}{1}$. Podem-se mostrar os isomorfismos $R \otimes R \cong R, R \otimes R_y \cong R_y, R_x \otimes R \cong R_x$ *e* $R_x \otimes R_y \cong R_{xy}$. De sorte que

$$\check{C}^{\bullet}_{x} \otimes \check{C}^{\bullet}_{y} := \; 0 \to R \to R_x \otimes R_y \to R_{xy} \to 0.$$

Para um R-módulo M, seja

$$\check{C}^{\bullet}_{\underline{x}}(M) = \check{C}^{\bullet}_{\underline{x}} \otimes_R M$$

O R-módulo

$$\check{H}^{i}_{\underline{x}}(M) = H^i(\check{C}^{\bullet}_{\underline{x}}(M))$$

é a *i-ésima cohomologia de Čech* de $\underline{x}$ em M.

Teorema 1.32. *Sejam M um R-módulo, $\mathfrak{a}$ ideal de R e $\underline{x} = x_1, \ldots, x_n$ um sistema de elementos tais que $\sqrt{(\underline{x})} = \sqrt{\mathfrak{a}}$. Então:*

$$H^i_{\mathfrak{a}}(M) \simeq H^i(\check{C}_{\underline{x}} \otimes M)$$

Demonstração. Para demonstração deste teorema, ver ([13], Teorema 7.13). □

Proposição 1.33. O funtor $H^i_{\mathfrak{a}}(-), i \geq 0$, comuta com limites diretos, isto é, se $\{M_\lambda : \lambda \in \Lambda\}$ é um sistema direto de R-módulos, então existe um isomorfismo natural:

$$H^i_{\mathfrak{a}}(\varinjlim_{\lambda} M_\lambda) \simeq \varinjlim_{\lambda} H^i_{\mathfrak{a}}(M_\lambda)$$

para qualquer $i \geq 0$

Demonstração. Segue diretamente do teorema (1.32), e do fato que o limite direto comuta com produto tensorial. □

Agora vamos descrever um método para calcular a cohomologia local a partir do limite direto de certo sistema direto de R-módulos.

Teorema 1.34. *Seja $\mathfrak{a}$ ideal de R. Para cada R-módulo M e para cada $j \geq 0$, existe isomorfismo natural:*

$$\varinjlim_{t} \operatorname{Ext}^j_R(R/\mathfrak{a}^t, M) \simeq H^j_{\mathfrak{a}}(M)$$

.

Demonstração. Já vimos que

$$\varinjlim_{t} \operatorname{Hom}_R(R/\mathfrak{a}^t, M) = \Gamma_{\mathfrak{a}}(M)$$

Seja $M^\bullet$ uma resolução injetiva de M. Então,

$$\varinjlim_{t} \operatorname{Hom}_R(R/\mathfrak{a}^t, M^\bullet) = \Gamma_{\mathfrak{a}}(M^\bullet)$$

Desde que $H^j(-)$ comuta com limite direto, a identificação anterior resulta num isomorfismo natural:

$$\varinjlim_{t} \operatorname{Ext}^j_R(R/\mathfrak{a}^t, M) = \varinjlim_{t} H^j(\operatorname{Hom}_R(R/\mathfrak{a}^t, M^\bullet)) \simeq H^j(\Gamma_{\mathfrak{a}}(M^\bullet)) = H^j_{\mathfrak{a}}(M)$$

□

Proposição 1.35. Seja M um R-módulo finitamente gerado. Então

$$H^i_{\mathfrak{m}}(M) \simeq H^i_{\mathfrak{m}}(M) \otimes_R \hat{R} \simeq H^i_{\hat{\mathfrak{m}}}(\hat{M}),$$

onde $\hat{M}$ denota o completamento $\mathfrak{m}$-ádico de M.

Demonstração. Como $H^i_{\mathfrak{m}}(M)$ é artiniano ([4], Teorema 7.1.3), podemos escrevê-lo como limite direto de submódulos N_j de comprimento finito[3] e para cada N_j temos

[3]Todo módulo tem-se $M = \varinjlim M_\lambda$, com M_λ finitamente gerado.

$N_j \otimes_R \hat{R} \simeq N_j$ ([24], Lemma 2.1). Assim,

$$H^i_{\mathfrak{m}}(M) \simeq \varinjlim N_j \simeq \varinjlim (N_j \otimes_R \hat{R}) \simeq (\varinjlim N_j) \otimes_R \hat{R} \simeq H^i_{\mathfrak{m}}(M) \otimes_R \hat{R}.$$

Usando o teorema anterior e a platitude de $\hat{R}$, temos:

$$H^i_{\mathfrak{m}}(M) \otimes_R \hat{R} \simeq \varinjlim_t \operatorname{Ext}^i_R(R/\hat{\mathfrak{m}}^t, M) \otimes_R \hat{R} \simeq \varinjlim_t \operatorname{Ext}^i_{\hat{R}}(\hat{R}/\hat{\mathfrak{m}}^t, \hat{M}) \simeq H^i_{\hat{\mathfrak{m}}}(\hat{M})$$

. □

O próximo teorema encontra-se demonstrado em ([4]).

Teorema 1.36. *Sejam $f : R \to S$ um homomorfismo de anéis noetherianos, $\mathfrak{a}$ um ideal de R e $i \in \mathbb{Z}$.*
(1) (Teorema da independência) Seja M um S-módulo. Então $H^i_{\mathfrak{a}}(M) \cong H^i_{\mathfrak{a}S}(M)$ como S-módulos. (a primeira cohomologia local é considerada sobre o anel R).
(2) (Teorema da mudança de base plana) Assuma que f é um homomorfismo plano e M um R-módulo. Então existe um isomorfismo

$$H^i_{\mathfrak{a}}(M) \otimes_R S \cong H^i_{\mathfrak{a}S}(M \otimes_R S).$$

Observação 1.37. Note que os homomorfismos $R \to \widehat{R}$ e $R \to R_{\mathfrak{p}}$ são planos e pelo item 2 do teorema acima tem-se:

$$H^i_{\mathfrak{a}}(M) \otimes_R \widehat{R} \cong H^i_{a\widehat{R}}(M \otimes_R \widehat{R})$$

e

$$H^i_{\mathfrak{a}}(M) \otimes_R R_{\mathfrak{p}} \cong H^i_{\mathfrak{a}R_{\mathfrak{p}}}(M \otimes_R R_{\mathfrak{p}}).$$

1.3 Dualidade de Matlis

Seja $(R, \mathfrak{m})$ anel local, $E = E_R(R/\mathfrak{m})$ a envoltória injetiva do corpo residual $k = R/\mathfrak{m}$. Usaremos $\hat{R}$ para denotar o completamento $\mathfrak{m}$-ádico $\varprojlim_{n\in\mathbb{N}} R/\mathfrak{m}^n$ e $(-)^\vee$ o funtor R-linear, exato e contravariante $\operatorname{Hom}(-, E)$. Para cada R-módulo M, chamaremos $(M)^\vee$ o *Dual de Matlis* de M. Note que $(R)^\vee = \operatorname{Hom}(R, E) \simeq E$.

Proposição 1.38. O homomorfismo natural $\hat{R} \to E^\vee = \operatorname{Hom}(E, E)$ é um isomorfismo.

Em sua tese de doutorado na Universidade de Chicago, Eben Matlis demonstrou o seguinte resultado fundamental de dualidade:

Teorema 1.39. *Sejam $(R, \mathfrak{m})$ anel noetheriano local completo, N um R-módulo Artiniano e M um R-módulo finitamente gerado. Então*

a) $R^\vee = E$ *e* $E^\vee = R$

b) $M^\vee$ *é artiniano e* $N^\vee$ *é finitamente gerado*

b) $N^{\vee\vee} \simeq N$ *e* $M^{\vee\vee} \simeq M$

Demonstração. Vide ([6], teorema 3.2.13). □

Aqui listamos outras propriedades do funtor dual de Matlis.

Proposição 1.40. Sejam M um R-módulo injetivo e N um R-módulo plano. Então:

a) $(M)^\vee$ é um R-módulo plano

b) $(N)^\vee$ é um R-módulo injetivo

Demonstração. a) Pelo critério de platitude ([19], Teorema 7.7), basta analisarmos $(M)^\vee$ para um ideal finitamente gerado $\mathfrak{a} \subseteq R$. Considere a sequência exata $0 \to \mathfrak{a} \to R$ aplicando o funtor contravariante $\mathrm{Hom}(-, M)$, exato pois M é injetivo, temos $\mathrm{Hom}(R, M) \to \mathrm{Hom}(\mathfrak{a}, M) \to 0$ que aplicando o funtor contravariante $(-)^\vee$ tem-se

$$0 \to \mathrm{Hom}(\mathrm{Hom}(\mathfrak{a}, M), E) \to \mathrm{Hom}(\mathrm{Hom}(R, M), E)$$

Sendo que

$$\mathrm{Hom}(\mathrm{Hom}(\mathfrak{a}, M), E) \simeq \mathfrak{a} \otimes \mathrm{Hom}(M, E) \text{ e } \mathrm{Hom}(\mathrm{Hom}(R, M), E) \simeq R \otimes \mathrm{Hom}(M, E)$$

Com isso, tem-se

$$0 \to \mathfrak{a} \otimes \mathrm{Hom}(M, E) \to R \otimes \mathrm{Hom}(M, E)$$

ou seja, $(M)^\vee$ é um R-módulo plano.

b) Considere uma sequência exata de R-módulos $0 \to L \to P$, Sendo N é R-módulo plano, temos:

$$0 \to L \otimes N \to P \otimes N$$

Aplicando o funtor contravariante $(-)^\vee$ tem-se

$$\mathrm{Hom}(P \otimes N, E) \to \mathrm{Hom}(L \otimes N, E) \to 0$$

Pelo isomorfismo de adjunção:

$$\mathrm{Hom}(P \otimes N, E) \simeq \mathrm{Hom}(P, (N)^\vee) \ \text{ e } \ \mathrm{Hom}(L \otimes N, E) \simeq \mathrm{Hom}(L, (N)^\vee)$$

Logo,

$$\mathrm{Hom}(P, (N)^\vee) \to \mathrm{Hom}(L, (N)^\vee) \to 0$$

ou seja, $\mathrm{Hom}(-, (N)^\vee)$ é exato daí segue que $(N)^\vee$ é injetivo.

$\square$

Proposição 1.41. Seja $f : M \to N$ um homomorfismo de R-módulos. Então:

$$f \text{ é um isomorfismo} \Leftrightarrow (f)^\vee : (N)^\vee \to (M)^\vee \quad \text{é um isomorfismo.}$$

Demonstração. Como $(-)^\vee$ é um funtor,

$$f : M \to N \text{ é isomorfismo} \Rightarrow D(f) : D(N) \to D(M) \text{ é um isomorfismo.}$$

Reciprocamente, o homomorfismo de R-módulos $f : M \to N$ induz a sequência exata:

$$0 \to \ker f \to M \to N \to \operatorname{coker} f \to 0$$

Aplicando o funtor exato contravariante $D(-)$:

$$0 \to D(\operatorname{coker} f) \to D(N) \xrightarrow{D(f)} D(M) \to D(\ker f) \to 0$$

Assim, $D(\operatorname{coker} f) = \ker D(f)$ e $D(\ker f) = \operatorname{coker} D(f)$. Sendo $D(f)$ um isomorfismo, $\ker D(f) = 0 = \operatorname{coker} D(f)$ Isto implica que $\ker f = 0 = \operatorname{coker} f$, ou seja $f : M \to N$ é um isomorfismo. $\square$

Proposição 1.42. Sejam M e N dois R-módulos. Então:

a) $(\mathrm{Tor}_i^R(M, N))^\vee \simeq \mathrm{Ext}_R^i(M, (N)^\vee)$

b) Assumindo que M seja finitamente gerado, $(\mathrm{Ext}_R^i(M, N))^\vee \simeq \mathrm{Tor}_i^R(M, (N)^\vee)$.

Demonstração. a) Seja $\mathbb{F}$ resolução livre de M. Então $\mathrm{Tor}_i^R(M, N) = H_i(\mathbb{F} \otimes N)$. Com isso, $(\mathrm{Tor}_i^R(M, N))^\vee = DH_i(\mathbb{F} \otimes N))^\vee \simeq H^i((\mathbb{F} \otimes N)^\vee)$

Por outro lado,

$$\begin{aligned} (\mathbb{F} \otimes N)^\vee = & \ \mathrm{Hom}_R(\mathbb{F} \otimes N, E) \\ \simeq & \ \mathrm{Hom}_R(\mathbb{F}, \mathrm{Hom}(N, E)) \\ \simeq & \ \mathrm{Hom}_R(\mathbb{F}, (N)^\vee) \end{aligned}$$

Tomando as cohomologias obtemos: $H^i((\mathbb{F}\otimes N)^\vee) \simeq H^i(\mathrm{Hom}_R(\mathbb{F},(N)^\vee)$.

Assim, $(\mathrm{Tor}_i^R(M,N))^\vee \simeq H^i((\mathbb{F}\otimes N)^\vee) \simeq H^i(\mathrm{Hom}_R(\mathbb{F},(N)^\vee) \simeq \mathrm{Ext}_R^i(M,(N)^\vee)$.

b) Seja $\mathbb{F}$ resolução livre de M. Como M é finitamente gerado, cada termo de $\mathbb{F}$ pode ser escolhido de posto finito. Então

$$\begin{aligned}
\mathrm{Tor}_i^R(M,(N)^\vee) &= H_i(\mathbb{F}\otimes (N)^\vee) \\
&= H_i(\mathbb{F}\otimes \mathrm{Hom}(N,E)) \\
&\simeq H_i(\mathrm{Hom}_R(\mathrm{Hom}_R(\mathbb{F},N),E)) \\
&\simeq H_i((\mathrm{Hom}(\mathbb{F},N)^\vee)) \\
&\simeq (H^i(\mathrm{Hom}(\mathbb{F},N)))^\vee \\
&\simeq (\mathrm{Ext}_R^i(M,N))^\vee
\end{aligned}$$

□

Capítulo 2

Anéis Invariantes

2.1 Grupo Agindo sobre um Anel

Nesta seção A é um anel (não necessariamente comutativo) e G é um subgrupo finito de $Aut(A)$; o grupo dos automorfismos de G (sob a operação de composição de funções). Seja $\varphi : G \to Aut(A)$ um homomorfismo de grupos. Suponhamos que $|G|$ é inversível em A. Nesta seção iremos descrever algumas propriedades básicas de grupos agindo sobre um anel $A *_\varphi G$ ao qual iremos necessitar no futuro.

Definição 2.1. Um grupo agindo sobre um anel A induzido por φ é o anel das somas formais

$$A *_\varphi G = \left\{ \sum_{\sigma \in G} a_\sigma \sigma \mid a_\sigma \ \in A \right\}.$$

A operação de soma feita componente a componente, ou seja,

$$\sum_{\sigma \in G} a_\sigma \sigma + \sum_{\sigma \in G} b_\sigma \sigma = \sum_{\sigma \in G} (a_\sigma + b_\sigma)\sigma.$$

A operação de multiplicação é definida por

$$(a_\sigma \sigma)(a_\tau \tau) = a_\sigma \varphi(\sigma)(a_\sigma)\sigma\tau.$$

Observação 2.2. Por questão de comodidade de notação, escrevemos $\varphi(\sigma)(a_\sigma) = \varphi_\sigma(a_\sigma)$. Quando não houver perigo de confusão, escrevemos $A *_\varphi G = A * G$.

Proposição 2.3. Com as operações acima, temos que $A * G$ é um anel.

Demonstração. Por construção, já temos um grupo Abeliano $(A, +)$. Resta verificar que os axiomas da multiplicação são compatíveis com os da soma. Sejam $a_\sigma, b_\tau, c_\upsilon \in A$

e $\sigma, \tau, \upsilon \in G$. Para facilitar a escrita, fazemos $a_\sigma = a, b_\tau = b, c_\upsilon = c$. Notemos que:

$$(a\sigma \cdot b\tau) \cdot c\upsilon = (a\varphi_\sigma(b)\sigma\tau) \cdot c\upsilon = a\varphi_\sigma(b)\varphi_{\sigma\tau}(c)\sigma\tau\upsilon = a\varphi_\sigma(b\varphi_\tau(c))a\sigma\upsilon = a\sigma \cdot (b\varphi_\tau(c)\tau\upsilon)$$

$$= a\sigma \cdot (b\tau \cdot c\upsilon),$$

onde na terceira igualdade usamos o fato de φ ser um homomorfismo de grupos. Portanto, provamos a associatividade da multiplicação. Além disso, tem-se

$$a\sigma \cdot 1_A 1_G = a\varphi_\sigma(1_A)\sigma 1_G = a\sigma = 1_A \varphi_{1_G}(a) 1_G \sigma = 1_R 1_G \cdot a\sigma.$$

Então, $A * G$ contém identidade para a operação de multiplicação. Agora iremos provar que a multiplicação é distributiva em relação à soma. Para todos $a, b, c \in A$ e $\sigma, \tau, \upsilon \in G$ tem-se

$$a\sigma \cdot (b\tau + c\upsilon) = a(\varphi_\sigma(b)\sigma\tau + \varphi_\sigma(c)\sigma\upsilon) = a\varphi_\sigma(b)\sigma\tau + a\varphi_\sigma(c)\sigma\upsilon = a\sigma \cdot b\tau + a\sigma \cdot c\upsilon,$$

$$(b\tau + c\upsilon) \cdot a\sigma = (b\varphi_\tau(a)\tau + c\varphi_\upsilon(a)\upsilon)\sigma = b\varphi_\tau(a)\tau\sigma + c\varphi_\upsilon(a)\upsilon\sigma = b\tau \cdot a\sigma + c\upsilon \cdot a\sigma.$$

Portanto todos os axiomas de anel são verificados e a prova está completa.

□

Exemplo 2.4. (Anel de grupo) Seja R um anel e G um grupo finito. Quando o homomorfismo de grupos ϕ é trivial, isto é,

$$\phi : G \to Aut(R), \quad g \longmapsto id_R, \ \forall \ g \ \in \ G,$$

então $R *_\varphi G$ é chamado anel de grupo e denotado por $R[G]$.

Exemplo 2.5. (Polinômio de Laurent) Seja A um anel. Recordemos que o anel dos polinômios de Laurent com coeficientes em A é dado por $R[x, x^{-1}] = \{a_{-m}x^{-m} + \cdots + a_{-1}x^{-1} + a_0 + a_1 x + \cdots + a_n x^n : m, n \in \mathbb{N}, a_i \in A\}$ onde a soma é definida componente a componente, e a multiplicação é dada por $a_m x^m \cdot a_n x^n = a_m b_n x^{m+n}$. Agora suponhamos que existe um homomorfismo de grupos $\varphi : \mathbb{Z} \to Aut(A)$, digamos $n \mapsto (a \mapsto na)$. Define-se por anel de grupo de Polinômios de Laurent induzido por φ como sendo o anel $A[x, x^{-1}, \varphi]$ cujo grupo Abeliano é $A[x, x^{-1}]$ e a multiplicação é definida por $a_m x^m b_n x^n = a_m \varphi(m)(b) x^{m+n}$.

Exemplo 2.6. Sejam R um anel comutativo e $G = \langle g \rangle$ um grupo cíclico de ordem n. Tem-se o seguinte homomorfismo de grupos:

$$\varphi : G \to Aut(R^n) \quad g \mapsto ((a_1, a_2, ..., a_n) \mapsto (a_n, a_1, a_2, ..., a_{n-1})).$$

Pode-se provar (com um pouco de trabalho algébrico) que $R^n *_\varphi G \cong \mathcal{M}_{n\times n}(R)$.

Observação 2.7. Dizemos que M é um $A*G$-módulo $\Leftrightarrow$ M é um A-módulo, G age sobre M (visto como grupo Abeliano) e para todo $a \in A$ e $m \in M$, $\sigma \in G$: $\widetilde{\varphi}(\sigma)(am) = \varphi(\sigma)(a)\widetilde{\varphi}(\sigma)(m)$, onde $\widetilde{\varphi} : G \to Aut_{\mathbb{Z}}(M)$. Para facilitar a escrita, a partir de agora iremos denotar $\widetilde{\varphi}(\sigma)(m) = \sigma(m)$.

Definição 2.8. Seja M um $A * G$-módulo. Então

$$M^G = \{m \in M \mid \sigma(m) = m, \forall\ \sigma \in G\}.$$

em particular, o conjunto $A^G = \{a \in A \mid \sigma(a) = a,\ \forall\ \sigma\ \in G\}$ é o anel dos invariantes de G.

Claramente, M^G é um A^G-módulo. Com efeito, dados $a, b \in A^G, m, n \in M^G, \sigma \in G$ verificamos que

$$\begin{aligned}\sigma((a+b)m) &= \sigma(am+bm) = \sigma(am)+\sigma(bm)\\ &= \sigma(a)\sigma(m)+\sigma(b)\sigma(m)\\ &= am+bm\\ &= (a+b)m,\end{aligned}$$

analogamente, $\sigma(a(m+n)) = a(m+n)$, etc.

Pode-se mostrar que um homomorfismo $f : M \to M'$ de $A * G$-módulos é uma aplicação tal que

- $f(m+m') = f(m)+f(m'),\ \forall\ m, m' \in M$;
- $f(am) = af(m),\ \forall\ m \in M, a\ \in A$;
- $\sigma(f(m)) = f(\sigma(m)),\ \forall\ m \in M,\ \sigma \in G$;

Também é fácil verificar que se $\mu : M \to N$ é $A * G$-linear então $\mu(M^G) \subseteq N^G$ e a restrição ao mapa $\widetilde{\mu} : M^G \to N^G$ é A^G-linear. Então temos o functor $(-)^G$: $mod(A * G) \to mod(A^G)$.

Exemplo 2.9. A é um $A * G$-módulo.

Solução 2.10. Tem-se a identificação

$$\left(\sum_{\sigma\in G} a_\sigma \sigma\right)\alpha = \sum_{\sigma\in G} a_\sigma\sigma(\alpha),\ onde\ \alpha\ \in\ A.$$

Os demais detalhes são deixados a cargo do leitor.

Agora defina

$$\begin{array}{rcccl} \psi_1 & : & M^G & \longrightarrow & Hom_{A*G}(A, M) \\ & & m & \longmapsto & \phi_m : A \to M \end{array}$$

onde $\phi_m(r) = rm$. Essa última aplicação satisfaz $\phi_m(\sigma(r)) = \sigma(r)m = \sigma(r)\sigma(m) = \sigma(rm) = \sigma(\phi_m(r))$. Definimos também

$$\begin{array}{rcccl} \psi_2 & : & Hom_{A*G}(A, M) & \longrightarrow & M^G \\ & & \phi & \longmapsto & \phi(1) \end{array}.$$

Temos que ψ_2 satisfaz $\sigma(\phi(1)) = \phi(\sigma(1)) = \phi(1)$. É fácil ver que elas são inversas uma da outra e portanto $M^G \cong Hom_{A*G}(A, M)$.

Assim provamos o isomorfismo:

Proposição 2.11. $(-)^G \cong Hom_{A*G}(A, -)$.

Para qualquer M, um $A * G$-módulo considere o operador Reynolds

$$\begin{array}{rcccl} \rho^M & : & M & \longrightarrow & M^G \\ & & m & \longmapsto & \frac{1}{|G|}\sum_{\sigma \in G} \sigma(m) \end{array}$$

Note que $\rho^M(m) = m$ para todo $m \in M^G$, isso porque

$$\frac{1}{|G|}\sum_{\sigma \in G} \sigma(m) = \frac{1}{|G|}\sum_{\sigma \in G} m = \frac{|G|m}{|G|} = m.$$

Também ρ^M é A^G-linear e cinde com a inclusão $M^G \to M$.
Neste momento, iremos mostrar que módulos invariantes é um funtor exato.

Lema 2.12. Seja $0 \to M_1 \xrightarrow{\mu_1} M_2 \xrightarrow{\mu_2} M_3 \to 0$ uma sequência exata curta de $A * G$-módulos. Então a sequência induzida

$$0 \to M_1^G \xrightarrow{\widetilde{\mu_1}} M_2^G \xrightarrow{\widetilde{\mu_2}} M_3^G \to 0$$

também é exata.

Demonstração. No parágrafo acima comentamos que o funtor "invariante" é exato à esquerda (2.11). Logo é suficiente mostrar que $\widetilde{\mu_2}$ é sobrejetiva. Seja $\xi \in M_3^G$. Como μ_2 é sobrejetiva existe $t \in M_2$ com $\mu_2(t) = \xi$. Para qualquer $\sigma \in G$ note que (**??**)

$$\mu_2(\sigma t) = \sigma\mu_2(t) = \sigma\xi = \xi.$$

Segue que

$$\mu_2(\rho^{M_2}(t)) = \mu_2\left(\frac{1}{|G|}\sum_{\sigma\in G}\sigma(t)\right) = \frac{1}{|G|}\sum_{\sigma\in G}\mu_2(\sigma(t)) = \frac{1}{|G|}\sum_{\sigma\in G}\xi = \xi.$$

Portanto $\widetilde{\mu_2}$ é sobrejetiva.

□

O próximo resultado é interessante.

Lema 2.13. Seja M um $A*G$-módulo simples. Então $M^G = 0$ ou M é um A^G-módulo simples.

Demonstração. Suponhamos que $M^G \neq 0$. Seja $N \neq 0$ um A^G-submódulo arbitrário de M^G. Considere $t \in N$ não nulo. Seja $\xi \in M^G$ arbitrário e não nulo.
Como M é um $A * G$-módulo simples tem-se $M = A * Gt$.[1] Assim $\xi = \alpha t$ para algum $\alpha \in A * G$, digamos $\alpha = \sum_{\sigma\in G} a_\sigma\sigma$. Portanto

$$\xi = \alpha t = \sum_{\sigma\in G} a_\sigma\sigma t = \left(\sum_{\sigma\in G} a_\sigma\right) t.$$

A última igualdade ocorre desde que $\sigma(t) = t$ para todo $\sigma \in G$. Seja $d = \sum_{\sigma\in G} a_\sigma$. Logo $\xi = dt$, daí para qualquer $\sigma \in G$

$$\xi = \sigma(\xi) = \sigma(d)\sigma(t) = \sigma(d)t.$$

Portanto

$$\xi = \frac{1}{|G|}\sum_{\sigma\in G}\sigma(\xi) = \frac{1}{|G|}\sum_{\sigma\in G}(\sigma(d)t) = \left(\frac{1}{|G|}\sum_{\sigma\in G}\sigma(d)\right)t.$$

De sorte que $\xi = \rho^A(d)t$ e então $\xi \in N$. Portanto $N = M^G$. Segue que M^G é um A^G-módulo simples, como se queria.

□

Uma consequência imediata do lema anterior é o

Corolário 2.14. Seja M um $A * G$-módulo de comprimento finito. Então M^G possui comprimento finito como um A^G-módulo.

Demonstração. Em virtude do $A * G$-módulo M ter comprimento finito, existe uma série de composição

$$0 = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_{n-1} \subseteq M_n = M,$$

[1] Pois $t \neq 0 \Rightarrow 0 \neq At$ é submódulo de $M \Rightarrow At = M$.

tal que M_i/M_{i-1} é simples como $A*G$-módulo para $i = 1, ..., n$. Observe que $0 = M_0^G \subseteq M_1^G \subseteq M_2^G \subseteq \cdots \subseteq M_{n-1}^G \subseteq M_n^G = M^G$ é uma série de composição de M^G como um A^G-módulo. Pelo Lema (2.12), a sequência exata

$$0 \to M_{i-1} \to M_i \to M_i/M_{i-1} \to 0,$$

induz a sequência exata

$$0 \to M_{i-1}^G \to M_i^G \to (M_i/M_{i-1})^G \to 0.$$

Pelo lema (2.13), $(M_{i-1}/M_i)^G$ é nulo ou um A^G-módulo simples, daí M^G tem comprimento finito como A^G-módulo. $\square$

O exemplo abaixo segue facilmente de (2.13).

Exemplo 2.15. Seja M um R-módulo. Então $l(M) \geq l(M^G)$, onde $l(M)$ denota o comprimento do R-módulo M.

O teorema abaixo mostra o complexo "invariante" preserva as homologias. Mais precisamente,

Teorema 2.16. *Sejam* $\boldsymbol{C} : \cdots \to M_n \xrightarrow{\mu_n} M_{n-1} \xrightarrow{\mu_{n-1}} M_{n-2} \to \cdots$ *complexos de* $A * G$*-módulos. Considere*

$$\boldsymbol{C}^{\,G} : \cdots \to M_n^G \xrightarrow{\widetilde{\mu_n}} M_{n-1}^G \xrightarrow{\widetilde{\mu_{n-1}}} M_{n-2}^G \to \cdots$$

Então:
(1) $\boldsymbol{C}^{\,G}$ *é um complexo de* A^G*-módulos;*
(2) Para cada $n \in \mathbb{Z}$ *existe uma aplicação* A^G*-linear* $\psi_n : H_n(\boldsymbol{C}^{\,G}) \to H_n(\boldsymbol{C})$*;*
(3) Para todo n *a aplicação* ψ_n *é injetiva;*
(4) Para todo $n \in \mathbb{Z}$ *tem-se* $Im(\psi_n) = H_n(\boldsymbol{C})^G$*;*
(5) Para todo $n \in \mathbb{Z}$ *tem-se* $H_n(\boldsymbol{C}^{\,G}) \cong H_n(\boldsymbol{C})^G$ *como* A^G*-módulo.*

Demonstração. (1) Segue do fato que $\mu_n \circ \mu_{n+1} = 0 \Rightarrow \widetilde{\mu_n} \circ \widetilde{\mu_n} = 0$.
(2) Fixe $n \in \mathbb{Z}$. Seja $z \in Z_n(\mathbf{C}^G) \Rightarrow \widetilde{\mu_n(z)} = 0 \Rightarrow \mu_n(z) = 0$. Logo $z \in Z_n(\mathbf{C})$. Por outro lado se $b \in B_n(\mathbf{C}^G)$ então seja $\widetilde{\mu_{n+1}}(t) = b \Rightarrow \mu_{n+1}(t) = b$ daí $b \in B_n(\mathbf{C})$. Desse modo a aplicação

$$\begin{array}{cccc} \psi : & H_n(\mathbf{C}^G) & \longrightarrow & H_n(\mathbf{C}) \\ & z + B_n(\mathbf{C}^G) & \longmapsto & z + B_n(\mathbf{C}) \end{array}$$

está bem definido e é A^G-linear[2]

[2] Já que ψ é A-linear e $H_n(\mathbf{C}^G)$ é um A^G-módulo.

(3) Fixe $n \in \mathbb{Z}$. Seja $\xi \in H_n(\mathbf{C}^G)$ tal que $\psi_n(\xi) = 0$, digamos $\xi = z + B_n(\mathbf{C}^G) \Rightarrow \psi_n(\xi) = z + B_n(\mathbf{C})$, logo $z \in B_n(\mathbf{C})$. Assim existe $t \in M_{n+1}$ tal que $\mu_{n+1}(t) = z$. Seja $\sigma \in G$. Note que

$$\mu_{n+1}(\sigma t) = \sigma\mu_{n+1}(t) = \sigma z = z.$$

Assim $\mu_{n+1}(\sigma t) = z$, para todo $\sigma \in G$. Portanto, $\mu_{n+1}(d) = z$, onde $d = \rho^{M_{n+1}}(t)$. Como $d \in M_{n+1}^G$ tem-se $\widetilde{\mu_{n+1}}(d) = z \Rightarrow z \in B_n(\mathbf{C}^G)$. Logo $\xi = 0$, e assim ψ é uma aplicação injetiva.

(4) É claro que $Im(\phi_n) \subseteq H_n(\mathbf{C})^G$. Suponha que $\xi \in H_n(\mathbf{C})^G$. Digamos $\xi = z + B_n(\mathbf{C})$. Seja $\sigma \in G$. Como $\sigma\xi = \xi$ tem-se $\xi = z + b$ onde $b \in B_n(\mathbf{C}) \Rightarrow \xi = \sigma\xi = \sigma(z + b)$. Logo $z + b = \sigma(z) + \sigma(b) \Rightarrow \sigma(z) = z + (b - \sigma(b)) = z + v_\sigma$[3], onde $v_\sigma \in B_n(\mathbf{C})$. Segue que

$$\frac{1}{|G|}\sum_{\sigma \in G}\sigma(z) = \frac{1}{|G|}\sum_{\sigma \in G}(z + v_\sigma) \Rightarrow$$

$$y = \rho^{M_n}(z) = z + v, \quad onde\ v = \frac{1}{|G|}\sum_{\sigma \in G} v_\sigma \in B_n(\mathbf{C}).$$

Claramente $y \in Z_n(\mathbf{C}^G)$. Note que

$$\phi_n(y + B_n(\mathbf{C}^G)) = y + B_n(\mathbf{C}) = z + B_n(\mathbf{C}) = \xi.$$

(5) Segue imediatamente dos itens anteriores e do primeiro teorema do isomorfismo de módulos.

$\square$

A partir de agora iremos supor que A seja um anel noetheriano comutativo.

Lema 2.17. Sejam M um $A * G$-módulo e $S \subseteq A^G$ um conjunto multiplicativo. Então:
(a) $S^{-1}M$ é um $A * G$-módulo;
(b) $S^{-1}M^G$ pode ser naturalmente identificado como um subconjunto de $S^{-1}M$, e com essa identificação tem-se $(S^{-1}M)^G = S^{-1}M^G$.

Demonstração. (a) Primeiramente vamos definir G-ação em $S^{-1}M$. Seja $\sigma \in G$ e seja $\xi \in S^{-1}M$. Se $\xi = m/s$, com $m \in M, s \in S$ então defina $\sigma(\xi) = \sigma(m)/s$. Esta G-ação esta bem definida: de fato, se $\xi = m_1/s_1 = m_2/s_2$ então existe $s_3 \in S$ com $s_3(s_2m_1 - s_1m_2) = 0 \Rightarrow s_3s_2m_1 = s_3s_1m_2$. Como $S \subseteq A^G$ tem-se $\sigma(s_3s_2m_1) = \sigma(s_3s_1m_2) \Rightarrow s_3s_2\sigma(m_1) = s_3s_1\sigma(m_2)$. Assim $\sigma(m_1)/s_1 = \sigma(m_2)/s_2$ em $S^{-1}M$. É fácil ver que isso é

[3]pois $b - \sigma(b) = \mu_{n+1}(i) - \sigma\mu_{n+1}(i) = \mu_{n+1}(i) - \mu_{n+1}\sigma(i) = \mu_{n+1}(i - \sigma(i)) \in B_n(\mathbf{C})$.

uma G-ação em $S^{-1}M$. Com efeito,

$$\begin{array}{rcccl} \phi & : & G \times S^{-1}M & \longrightarrow & S^{-1}M \\ & & (\sigma, m/s) & \longmapsto & \sigma(m/s) = \sigma(m)/s \end{array}$$

satisfaz: $\forall\, \sigma, \sigma' \in G, \forall\, m/s \in S^{-1}M$, $\sigma'(\sigma(m/s)) = (\sigma'\sigma)(m/s)$, e $\forall\, m/s \in S^{-1}M$, $e_G(m/s) = e_G(m)/s = m/s$, onde e_G é o elemento neutro do grupo G. Sejam $a \in A$ e $\xi \in S^{-1}M$, digamos $\xi = m/s$. Então:

$$\sigma(a\xi) = \sigma(am)/s = \sigma(a)\sigma(m)/s = \sigma(a)\sigma(\xi.)$$

Segue que $S^{-1}M$ é um $A * G$-módulo.

(b) Temos que $M^G \subseteq M$ e essa inclusão é A^G-linear. Como localização preserva inclusões, tem-se $S^{-1}M^G \subseteq S^{-1}M$. Afirmamos que $S^{-1}M^G \subseteq (S^{-1}M)^G$. De fato, $S^{-1}M^G = \{m/s : m \in M^G, s \in S\}$ e $\sigma(m/s) = \sigma(m)/s = m/s \Rightarrow m/s \in (S^{-1}M)^G$. Agora vamos mostrar a inclusão contrária. Seja $\xi \in (S^{-1}M)^G$, digamos $\xi = m/s$. Então para todo $\sigma \in G$ tem-se $\sigma(m/s) = m/s \Rightarrow \sigma(m)/s = m/s$. Portanto existe $s'_\sigma \in S$ tal que $s'_\sigma s\sigma(m) = s'_\sigma sm$. Considere $s_\sigma = s'_\sigma s \in S$, e notando que $\sigma(s_\sigma m) = s_\sigma m$,[4] ponhamos

$$\theta = \prod_{\sigma \in G} s_\sigma \in S.$$

Por indução em $|G|$, obtém-se $\sigma(\theta m) = \theta m$ para todo $\sigma \in G$. Assim $\theta m \in M^G$. Finalmente,

$$\xi = m/s = (\theta m)/(\theta s) \in S^{-1}M^G,$$

pois $\theta s \in S$, e o lema está demonstrado. □

Uma propriedade fundamental que iremos usar é que funtores aditivos levam sequências exatas cindidas em sequências exatas cindidas ([22], Corolário 5.88). Em particular, como a sequência exata $0 \to M_1 \to M_1 \oplus M_2 \to M_2 \to 0$ cinde, a sequência exata induzida $0 \to M_1^G \to (M_1 \oplus M_2)^G \to M_2^G \to 0$ irá cindir. Assim obtemos um isomorfismo $(M_1 \oplus M_2)^G \cong M_1^G \oplus M_2^G$. Por indução simples temos o seguinte:

Lema 2.18. Sejam $M_1, ..., M_r$ $A * G$-módulos. Então

$$\left(\bigoplus_{i=1}^{r} M_i\right)^G \cong \bigoplus_{i=1}^{r} M_i^G.$$

Lema 2.19. Sejam A um domínio e $G \subseteq Aut(A)$ um grupo finito. Seja S um conjunto multiplicativo contido em A^G. Considere a ação de G em $S^{-1}A$ como no lema (2.17).

[4]pois $S \subseteq A^G$.

Então o mapa natural

$$\begin{array}{ccc} G & \longrightarrow & Aut(S^{-1}A) \\ \sigma & \longmapsto & \widetilde{\sigma} \end{array}$$

é injetivo.

Demonstração. Primeiramente,

$$\begin{array}{cccc} \widetilde{\sigma} & : & S^{-1}A & \longrightarrow & S^{-1}A \\ & & a/s & \longmapsto & \widetilde{\sigma}(a/s) = \sigma(a)/s \end{array}$$

é um automorfismo: se $\sigma(a)/s = 0/1 \Rightarrow \exists\ t \in S \subseteq A^G : t\sigma(a) = 0 \Rightarrow \sigma(ta) = 0 \Rightarrow ta = 0 \Rightarrow a/1 = 0/1$, donde $\widetilde{\sigma}$ é injetiva. A sobrejetividade é óbvia. Também é claro que

$$\widetilde{\sigma}\left(\frac{a}{s} + \frac{b}{t}\right) = \widetilde{\sigma}\left(\frac{at + bs}{st}\right) = \frac{\sigma(ta + bs)}{st} = \frac{\sigma(a)}{s} + \frac{\sigma(b)}{t} = \widetilde{\sigma}\left(\frac{a}{s}\right) + \widetilde{\sigma}\left(\frac{b}{t}\right).$$

Agora note que dados $\sigma, \tau \in G$ implica $\sigma \circ \tau \in G$, e $\widetilde{(\sigma \circ \tau)}(a/s) = \sigma \circ \tau(a)/s = \widetilde{\sigma}\left(\tau(a)/s\right) = \widetilde{\sigma}\left(\widetilde{\tau}\left(\frac{a}{s}\right)\right) = \widetilde{\sigma} \circ \widetilde{\tau}\left(\frac{a}{s}\right)$ (Homomorfismo de grupos). Por fim para provar a injetividade do mapa natural, suponha que $\sigma \in G$ é tal que o mapa $\sigma : S^{-1}A \longrightarrow S^{-1}A$ é a identidade. Logo $\sigma(\xi) = \xi$ para todo $\xi \in S^{-1}A$. Seja $a \in A \Rightarrow \sigma(a/1) = a/1$, donde $\sigma(a)/1 = a/1$, como A é um domínio de integridade tem-se $\sigma(a) = a$. Portanto σ é a identidade. □

Antes de finalizar esta seção vamos estudar um lema que relacionado com módulos injetivos (para mais detalhes sobre módulos injetivos consulte o Apêndice).

Observação 2.20. Claramente $A * G$ é um A-módulo à esquerda livre. Note que

$$\begin{array}{ccccc} A^n & \longrightarrow & A^n & \longrightarrow & A * G \\ (a_1, ..., a_n) & \longmapsto & (\sigma_1(a_1), ..., \sigma_n(a_n)) & \longmapsto & \sigma(a_1)\sigma_1 + \cdots + \sigma(a_n)\sigma_n \end{array}.$$

Onde para qualquer $a \in A$ e $\sigma \in G$ tem-se $\sigma a = \sigma(a)\sigma$, também $\sigma : A \to A$ é um automorfismo. Daí $A * G$ também é um A-módulo livre à direita.

Uma consequência significativa da observação acima é o seguinte:

Lema 2.21. Seja E um $A * G$-módulo injetivo. Então E é injetivo como A-módulo.

Demonstração. Em virtude de ([22], prop. 3.25) é suficiente ver que $Hom_A(-, E)$ é exato. Por adjunção ([22], 2.75) e (1.2) tem-se

$$Hom_A(-, E) \cong Hom_A(-, Hom_{A*G}(A * G, E)) \cong Hom_{A*G}(A * G \otimes_A -, E).$$

Como $A * G$ é um A-módulo livre à direita tem-se $A * G \otimes_A -$ é um funtor exato da categoria $Mod(A)$ a categoria $Mod(A*G)$. Por hipótese E é injetivo como $A*G$-módulo, portanto $Hom_A(-, E)$ é exato. Assim E é injetivo como A-módulo. □

2.2 Anel dos Invariantes dos Operadores Diferenciais

Nesta seção iremos discorrer brevemente sobre o anel dos operadores diferenciais. Para mais detalhes recomendamos ao leitor o Apêndice. Sejam K um corpo de característica zero e $R = K[X_1, ..., X_n]$. Seja G um subgrupo finito de $GL_n(K)$ agindo linearmente em R. Seja R^G o anel dos invariantes de R. Considere $D(R)$ o anel dos operadores diferenciais K-lineares em R. Note que $D(R) \cong A_n(K)$ a n-ésima álgebra de Weyl sobre K. Recordemos a ação natural de G em $D(R)$ vide ([33], seção 1) e então considere o anel dos invariantes $D(R)^G$.

• Primeiramente recordemos a construção de $D(R)$ como sendo um subanel de $S = \mathrm{Hom}_K(R, R)$. A composição de dois elementos P, Q de S é denotada por $P \cdot Q$. O comutador de P, Q é

$$[P, Q] = P \cdot Q - Q \cdot P.$$

Temos a inclusão natural $\eta : R \longrightarrow S$ onde $\eta(r) : R \longrightarrow R$ é a multiplicação por r. Seja $D_0(R) = R$ visto como um subanel de S. Para $i \geq 0$ seja

$$D_i(R) = \{P \in S \mid [P, r] \in D_{i-1}(R)\}.$$

Os elementos de $D_i(R)$ são ditos de operadores diferenciais de R de grau menor ou igual a i. Note que $D_{i+1} \supseteq D_i(R)$ para todo $i \geq 0$. Vamos mostrar isso por indução: para $i = 0$ seja $\theta \in D_0(R) \Rightarrow \theta = s \in R$. $[\theta, r] = \mu_s\mu_r - \mu_r\mu_s = 0 \in R = D_0(R) \Rightarrow \theta \in D_1(R)$. Supondo por hipótese de indução que $D_{i-1}(R) \subseteq D_i(R)$ e sendo $\theta \in D_i(R)$ tem-se $[\theta, r] \in D_{i-1}(R)\ \forall\ r \in R \Rightarrow [\theta, r] \in D_i(R)\ \forall\ r \in R \Rightarrow \theta D_{i+1}(R)$. Seja agora

$$D(R) = \bigcup_{i \geq 0} D_i(R).$$

Este é o anel dos K-operadores diferenciais de R. Com efeito, $\theta, \tau D(R) \Rightarrow \theta \in D_i(R)$ e $\tau \in D_j(R)$ podemos supor que $\theta, \tau \in D_i(R)$, agora $[\theta + \tau, r] = (\theta + \tau)r - r(\theta + \tau) = \theta r + \tau r - r\theta - r\tau = [\theta, r] + [\tau, r] \in D_{i-1}(R)$ logo $\theta + \tau \in D_i(R) \subset D(R)$.

Observação 2.22. Note que $D_0(R) = R$ é aditivo. Supondo por indução que $D_i(R)$ é aditivo tem-se $\theta, \tau \in D_{i+1}(R)$ implica

$$[\theta+\tau, r] = [\theta, r] + [\tau, r] \in D_i(R),$$

donde $D_i(R)$ é aditivo para todo $i \geq 0$.

Pode-se mostrar que $D(R) \cong A_n(K)$.

Seja $D(R)_{-1} = 0$. Note que o anel graduado

$$\mathfrak{gr}(D(R)) = \bigoplus_{i\geq 0} D(R)_i/D(R)_{i-1} = R[\overline{\partial_1}, \cdots, \overline{\partial_n}],$$

é isomorfo ao anel de polinômios em n variaveis sobre R.

Observação 2.23. Defina uma ação de G em $D(R)$ como segue. Sejam $\theta \in D(R)_i$ e $g \in G$. Então:

$$\begin{array}{rccc} g\theta & : & R & \longrightarrow & R \\ & & r & \longmapsto & g\cdot\theta(g^{-1}r). \end{array}$$

Pode-se verificar que $g\theta \in D(R)_i$. Então obtemos uma ação de G em $D(R)$. Pode-se verificar facilmente que $G \hookrightarrow Aut(D(R))$.

Observação 2.24. (i) Sejam $s \in R$ e $\mu_s : R \to R$ a multiplicação por s. Então $g\mu_s = \mu_{gs}$.
(ii) Seja $g \in G \subset GL_n(K)$ dado pela matriz T_g podemos verificar que

$$g\begin{bmatrix} \partial_1 \\ \cdots \\ \partial_n \end{bmatrix} = (T_g^{-1})^t \begin{bmatrix} \partial_1 \\ \cdots \\ \partial_n \end{bmatrix}.$$

Onde $(-)^t$ indica a matriz transposta. Note que $g\partial_i$ é uma derivação para todo $g \in G$, e todo i.

• Seja $D(R)^G$ o anel dos invariantes de G. Para $i \geq 0$ seja $(F)_i = D(R) \cap D(R)^G$. Pela Observação (2.24) tem-se $\mathcal{F}_0 = R^G$. O anel graduado $\mathfrak{gr}(\mathcal{F})$ é um subanel de $\mathfrak{gr}(D(R))$. Pelo ([33], Teorema 1) existem uma G-ação natural em $\mathfrak{gr}(D(R)$ com $\mathfrak{gr}(D(R))^G = \mathfrak{gr}(\mathcal{F})$. Daí segue que:
(i) $D(R)^G$ é Noetheriano, desde que $\mathfrak{gr}(\mathcal{F})$ é Noetheriano;
(ii) $\mathfrak{gr}(D(R))$ é finitamente gerado como $\mathfrak{gr}(\mathcal{F})$-módulo. Assim $D(R)$ é finitamente gerado como um $D(R)^G$-módulo. Apesar de não usar esses fatos nesse texto, é conveniente citá-los aqui.

• Seja $D(R) * G$ um anel de grupo de $D(R)$ com respeito a G. Seja $D(R)^G$ o anel dos invariantes. Claramente $D(R)$ é um $D(R) * G$-módulo.

Proposição 2.25. *R é um $D(R) * G$-módulo.*

Demonstração. Claramente R é um $D(R)$-módulo e que G é uma ação em R. Portanto da observação 2.1 é suficiente verificar que para quaisquer $\theta \in D(R), g \in G$ e $r \in R$ tem-se $g(\theta \cdot r) = g(\theta) \cdot g(r)$. Observe que $\theta \cdot r = \theta(r)$ para qualquer $\theta \in D(R)$. Então

$$g(\theta \cdot r) = g(\theta(r))$$

enquanto que

$$\begin{aligned} g(\theta) \cdot g(r) &= g(\theta)[g(r)] \\ &= g[\theta(g^{-1}gr)] \\ &= g(\theta(r)), \end{aligned}$$

pela observação (2.23). Portanto R é um $D(R) * G$-módulo. □

Observação 2.26. Notemos que o anel $R * G$ é claramente um subanel de $D(R) * G$. Então os $D(R) * G$-módulos são naturalmente $R * G$-módulos. Sejam M um $D(R) * G$-módulo e $f \in R^G$. Temos uma G-ação natural em M_f, veja (2.17). Sabe-se que M_f é um $D(R)$-módulo.

Com isso temos a

Proposição 2.27. (Com as hipóteses acima). *M_f é um $D(R) * G$-módulo.*

Demonstração. Temos que provar que para todos $\sigma \in G, \theta \in D(R)$ e $\xi \in M_f$ que

$$\sigma(\theta\xi) = \sigma(\theta)\sigma(\xi). \tag{2.1}$$

Como $D(R)$ é gerado por R e derivações é suficiente provar (2.1) quando $\theta \in R$ ou é uma derivação. Quando $\theta \in R$ então claramente (2.1) vale, vide (2.17). Agora assuma que θ é uma derivação. Pela Observação (2.24, ii), $\sigma(\theta)$ também é uma derivação. Seja $\xi = m/f^i$, calculamos:

$$\begin{aligned} \sigma(\theta\xi) &= \sigma(\theta(m/f^i)), \\ &= \sigma\left(\frac{f^i\theta(m) - m(if^{i-1}\theta(f))}{f^if^i}\right) \\ &= \sigma\left(\frac{f^{i-1} \cdot f\theta(m) - m(if^{i-1}\theta(f))}{f^if \cdot f^{i-1}}\right) \\ &= \sigma\left(\frac{\theta m}{f^i} - \frac{i(\theta(f))(m)}{f^{i+1}}\right) \\ &= \frac{\sigma(\theta m)}{f^i} - \frac{i\sigma(\theta(f))\sigma(m)}{f^{i+1}}. \end{aligned}$$

O próximo passo é calcular $\sigma(\theta)\sigma(\xi)$. Como $\sigma(\theta)$ é uma derivação obtém-se

$$\sigma(\theta)\sigma(\xi) = \sigma(\theta)\left(\frac{\sigma(m)}{f^i}\right),$$

$$= \frac{\sigma(\theta)\sigma(m)}{f^i} - \frac{i\sigma(\theta(f))\sigma(m)}{f^{i+1}}.$$

Note que:
(1) $\sigma(\theta m) = \sigma(\theta)\sigma(m)$;
(2) $\sigma(\theta)(f) = \sigma(\theta(\sigma^{-1}f)) = \sigma(\theta(f))$; desde que $f \in R^G$ $(\sigma f = f \Rightarrow f = \sigma^{-1}f)$
Então $\sigma(\theta\xi) = \sigma(\theta)\sigma(\xi)$. Segue que M_f é um $D(R) * G$-módulo.

□

2.3 Anéis Invariantes Cohen-Macaulay

Para encerrar este capítulo vejamos alguns resultados que relacionam o anel dos invariantes e os anéis *Cohen-Macaulay.* O leitor poderá consultar as definições e resultados pertinentes de anéis Cohen-Macaulay no Apêndice. Começamos com um resultado auxiliar:

Lema 2.28. Sejam R um anel, G um subgrupo finito dos automorfismos de R com $|G|$ inversível em R. Então:
(i) $IR \cap R^G = I$, para todo ideal I de R^G.
(ii) Se R é noetheriano, assim também o é R^G.

Demonstração. Seja $\rho : R \to R^G$ o operador de Reynold. i) $(\subset)$ Se $\Sigma a_i r_i \in R^G$ onde $a_i \in I, r_i \in R$ então

$$\Sigma a_i r_i = \rho(\Sigma a_i r_i) = \Sigma a_i \rho(r_i) \in I.$$

$(\supset)$ Óbvia.

ii) Sejam $I_2 \subset I_2 \subset ... \subset I_n \subset ...$ uma cadeia ascendente de ideais em R^G. Então, $I_{n_0}R = I_{n_0+1}R = I_{n_0+2}R...$ para algum $n_0 \in \mathbb{N}$, desde que R é Noetheriano. Portanto,

$$I_{n_0}R \cap R^G = I_{n_0+1}R \cap R^G = I_{n_0+2}R \cap R^G = ...$$

então, pelo item a) tem-se

$$I_{n_0} = I_{n_0+1} = I_{n_0+2} = ...$$

ou seja, R^G é noetheriano.

□

Agora iremos verificar explicitamente um exemplo em que R^G é Cohen-Macaulay.

Exemplo 2.29. Seja $G = \{1, -1\} \subset k\backslash\{0\}$, onde k é um corpo qualquer. Considere o anel de polinômio $R = k[r, s]$. Então R^G é Cohen-Macaulay.

Solução 2.30. Sabemos que $R^G = \{f(r, s) \in k[r, s] : \sigma(f(r, s)) = f(r, s), \forall\ \sigma\ \in\ G\}$. A ação $G \times R \to R$ é dada por $1 \cdot f(r, s) = f(r, s)$ e $-1 \cdot f(r, s) = f(-r, -s)$. Portanto, $R^G = k[r^2, rs, s^2]$. Considere a sobrejeção

$$\begin{array}{cccc} \phi\ :\ k[X,Y,Z] & \longrightarrow & k[r^2, rs, s^2] \\ X & \longmapsto & r^2 \\ Y & \longmapsto & rs \\ Z & \longmapsto & s^2 \end{array}$$

Temos que $ker(\phi) = (Y^2 - XZ) \Rightarrow k[r^2, rs, s^2] \cong k[X, Y, Z]/(Y^2 - XZ)$ é um domínio, logo o ideal $(Y^2 - XZ)$ não é um divisor de zero, daí é uma $k[X, Y, Z]$-sequência e pelo (B.1) $k[X, Y, Z]/(Y^2 - XZ)$ é Cohen-Macaulay. Portanto R^G é Cohen-Macaulay.

O próximo teorema é conhecido como Teorema da finitude de Hilbert.

Teorema 2.31. *Seja G um subgrupo de $GL_n(k)$ agindo sobre $k[x] = R$. Considere que $S = k[x]^G$ e que existe o operador de Reynolds $\rho : R \to S$. Então S é finitamente gerado como k-álgebra.*

Corolário 2.32. Seja G um subgrupo de $GL_n(k)$ agindo sobre $k[x] = R$. Suponhamos que $mdc(|G|, char K) = 1$. Então $k[x]^G$ é finitamente gerado como k-álgebra.

O teorema abaixo foi demonstrado por Hochster-Eagon em 1971. Eis-o:

Teorema 2.33. *Seja $G \subset GL_n(K)$ um grupo de ordem não divisível pela característica do corpo K, i.e, $mdc(|G|, char K) = 1$. Então $k[x]^G$ é Cohen-Macaulay.*

Demonstração. Sejam $R = k[x]$ e $S = k[x]^G$. Considere $\rho : R \to S$ o operador de Reynold. Seja I um ideal de S. Sabemos que $IR \cap S = I$ (2.28). Seja $k[x_1, ..., x_n]$ a normalização de Noether (2.31) do anel graduado S, os $x_i \in k[x]^G$ são algebricamente independentes. Sabemos que a extensão $k[x_1, ..., x_n] \to k[x]$ é inteira[5]. Seja $(x_1, ..., x_n) \subset k[x_1, ..., x_n]$ maximal. Sabe-se que $\sqrt{(x_1, ..., x_n)k[x]}$ é igual a uma interseção de primos minimais, e cada um desses primos minimais $\mathfrak{p}_i$ satisfazem $\mathfrak{p}_i \cap k[x_1, ..., x_n] = (x_1, ..., x_n)$ daí pela maximalidade todos os $\mathfrak{p}_i's$ são iguais ao ideal irrelevante $(x) = R_+$. Em suma $(x_1, ..., x_n)R$ é R_+-primário. Como R é Cohen-Macaulay[6] segue que $\underline{x} = x_1, ..., x_n$ é uma R-sequência. Afirmamos que $\underline{x}$ é uma S-sequência. Suponhamos que $1 \leq i \leq n$, $s \in S$ com $sx_i = \overline{0}$ em $S/(x_1, ..., x_n)S \Rightarrow sx_i \in (x_1, ..., x_{i-1})S$, então $sx_i \in (x_1, ..., x_{i-1})R$, daí

[5]note que $k[x] \longrightarrow k[x]^G$ é inteira, vide ([7], 11.1.1, 1).
[6]já que todo corpo é Cohen-Macaulay e usando (B.44).

$s \in (x_1, ..., x_{i-1})R \cap S = (x_1, ..., x_{i-1})$. Portanto $\underline{x}$ é uma S-sequência, donde $S = R^G$ é Cohen-Macaulay. □

Exemplo 2.34. A hipótese $mdc(|G|, char K) = 1$ é essencial.

Solução 2.35. De fato o seguinte contraexemplo mostra que quando $char K$ divide $|G|$ tem-se que R^G não é necessariamente Cohen-Macaulay:
Tome $G = \mathbb{Z}/4\mathbb{Z}$ e $R = k[x, y, z, w]$, onde $k = \mathbb{Z}/2\mathbb{Z}$ (Entretanto nesse caso, pode-se mostrar que R^G é um domínio de fatoração única, Vide ([35]) para mais detalhes).

O teorema abaixo pode ser encontrado em ([37]).

Teorema 2.36. *Sejam R um anel noetheriano e G um grupo finito tal que $|G|$ é inversível em R. Se R é Cohen-Macaulay então R^G é Cohen-Macaulay.*

Capítulo 3

Cohomologia Local de Anéis Invariantes

3.1 Cohomologia Local Associada

Sejam A um anel noetheriano comutativo e $G \subseteq Aut(A)$ um grupo finito com $|G|$ inversível em A. Seja A^G o anel dos invariantes de G. Seja $A * G$ um grupo agindo sobre um anel A com respeito a G. Nesta seção iremos mostrar que certos módulos de cohomologia local sobre A tem uma estrutura natural de $A * G$-módulo, com isso, investigaremos algumas dessas propriedades. Começamos com:

Teorema 3.1. *Sejam M um $A * G$-módulo e I um ideal em A^G. Então*
(1) $H^i_{IA}(M)$ é um $A * G$-módulo para todo $i \geq 0$.
(2) $H^i_{IA}(M)^G \cong H^i_I(M^G)$ para todo $i \geq 0$.

Demonstração. (1) Seja $I = (f_1, ..., f_s)$[1]. Considera o complexo de Čech (modificado)

$$\mathbf{C} : 0 \to M \to \bigoplus_{i=1}^{s} M_{f_i} \to \cdots \to M_{f_1 \cdots f_s} \to 0.$$

Afirmação: $\mathbf{C}$ é um complexo de $A * G$-módulos. Em virtude do lema (2.17), cada módulo em $\mathbf{C}$ é um $A * G$-módulo. Assim necessitamos provar que cada diferencial em $\mathbf{C}$ é $A * G$-linear. Para mostrar isso devemos verificar que se $f, g \in A^G$ então o mapa natural (onde $M_f = \{1, f, f^2, f^3, ..., \}$)

$$\begin{array}{cccc} \eta : & M_f & \longrightarrow & M_{fg} \\ & m/f^n & \longmapsto & (g^n m)/((fg)^n) \end{array}$$

[1] já que A^G é noetheriano (2.28)

é $A * G$-linear. Claramente η é A-linear:

$$\eta\left(a \cdot \frac{m}{f^n}\right) = \eta\left(\frac{am}{f^n}\right) = \frac{g^n am}{(fg)^n} = a \cdot \frac{g^n m}{(fg)^n} = a \cdot \eta(\frac{m}{f^n})$$

e da mesma forma,

$$\eta\left(\frac{m}{f^n} + \frac{m'}{f^{n'}}\right) = \eta\left(\frac{f^{n'}m + f^n m'}{f^{n+n'}}\right) = \frac{g^{n+n'}(f^{n'}m + f^n m')}{(fg)^{n+n'}}$$

$$= \frac{g^{n+n'}f^{n'}m}{(fg)^{n+n'}} + \frac{g^{n+n'}f^n m'}{(fg)^{n+n'}} = \eta\left(\frac{m}{f^n}\right) + \eta\left(\frac{m'}{f^{m'}}\right).$$

Agora seja $\xi \in M_f$ digamos $\xi = m/f^i \Rightarrow \sigma\xi = \sigma(m)/f^i \Rightarrow \eta(\sigma\xi) = g^i\sigma(m)/f^i g^i$. Note que,

$$\sigma\eta(\xi) = \sigma(g^i m/f^i g^i) = g^i\sigma(m)/f^i g^i = \eta(\sigma\xi).$$

Então η é $A*G$-linear. Assim $\mathbf{C}$ é um complexo de $A*G$-módulos, segue que $H^i_{IA}(M)$ é um $A * G$-módulo para todo $i \geq 0$.
(2) *Afirmação:* O complexo $\mathbf{C}^G$ como definido no teorema (2.16) é um complexo de Čech em M^G. De fato,

$$\mathbf{C}^G : 0 \to M^G \to \left(\bigoplus_{i=1}^{s} M_{f_i}\right)^G \to \cdots \to (M_{f_1\cdots f_s})^G \to 0$$

isso nos dá (2.18)

$$\mathbf{C}^G : 0 \to M^G \to \bigoplus_{i=1}^{s} (M_{f_i})^G \to \cdots \to (M_{f_1\cdots f_s})^G \to 0$$

entretanto pelo lema (2.17), tem-se

$$\mathbf{C}^G : 0 \to M^G \to \bigoplus_{i=1}^{s} M^G_{f_i} \to \cdots \to M^G_{f_1\cdots f_s} \to 0.$$

Com isso concluímos que $H^i(\check{C}_{\underline{f}} \otimes M)^G) \cong H^i(\check{C}_{\underline{f}} \otimes M^G)$, onde $\underline{f} = f_1, ..., f_s$. Agora usando o teorema (1.32) tem-se,

$$H^i(\check{C}_{\underline{f}} \otimes M^G) \cong H^i_I(M^G),$$

e por outro lado usando (1.36)

$$H^i_{IA}(M)^G \cong H^i_I(M)^G \cong (H^i(\check{C}_{\underline{f}} \otimes M))^G \cong H^i((\check{C}_{\underline{f}} \otimes M)^G) \cong H^i(\check{C}_{\underline{f}} \otimes M^G)$$

No penúltimo isomorfismo usamos (2.16, 5). Portanto $H^i_{IA}(M)^G \cong H^i_I(M^G)$ para todo $i \geq 0$.

□

Como uma consequência do teorema anterior tem-se, o

Corolário 3.2. Sejam $I, I_1, I_2, ..., I_r$ ideais em A^G. Então:
(1) $H^i_{IA}(A)$ é um $A * G$-módulo para todo $i \geq 0$. Além disso,

$$H^i_{IA}(A)^G \cong H^i_I(A^G);$$

(2) Para todos $i_j \geq 0$, onde $j = 1, ..., r$, $H^{i_1}_{I_1A}(H^{i_2}_{I_2A}(\cdots H^{i_r}_{I_rA}(A)\cdots)$ é um $A*G$-módulo. Além disso,

$$H^{i_1}_{I_1A}(H^{i_2}_{I_2A}(\cdots H^{i_r}_{I_rA}(A)\cdots)^G \cong H^{i_1}_{I_1A}(H^{i_2}_{I_2A}(\cdots H^{i_r}_{I_rA}(A^G)\cdots).$$

Demonstração. (1) É uma consequência imediata do teorema (2.16), desde que A é um $A * G$-módulo.
(2) Vamos provar o resultado por indução em r. Para $r = 1$ é justamente a parte 1. Assuma que o resultado vale para $r - 1$ onde $r \geq 2$. Fixe $i_1, ..., i_r \geq 0$. Seja

$$M = H^{i_2}_{I_2A}(\cdots H^{i_r}_{I_rA}(A)\cdots).$$

Por hipótese de indução M é um $A * G$-módulo e

$$M^G \cong H^{i_2}_{I_2}(\cdots H^{i_r}_{I_r}(A^G)\cdots).$$

Pelo Teorema (3.1) segue que para todo $i_1 \geq 0$, $H^{i_1}_{I_1A}(M)$ é um $A * G$-módulo e

$$H^{i_1}_{I_1A}(M)^G \cong H^{i_1}_{I_1}(M^G).$$

O resultado segue imediatamente.

□

O leitor poderá revisar os conceitos e os resultados de anéis de operadores diferenciais que foram introduzidos no capítulo 2 e no Apêndice. Neste momento iremos provar um resultado análogo ao teorema (3.1).

Teorema 3.3. *Seja M um $D(R) * G$-módulo. Seja I um ideal em R^G. então:*
(1) H^i_{IR} é um $D(R) * G$-módulo para todo $i \geq 0$;
(2) $H^i_{IR}(M)^G \cong H^i_I(M^G)$ para todo $i \geq 0$.

Demonstração. (1) Seja $I = (f_1, ..., f_s)$. Considera o complexo de Čech (modificado)

$$\mathbf{C} : 0 \to M \to \bigoplus_{i=1}^{s} M_{f_i} \to \cdots \to M_{f_1 \cdots f_s} \to 0.$$

Afirmação: $\mathbf{C}$ é um complexo de $D(R) * G$-módulos. Pela proposição anterior (2.27) cada módulo em $\mathbf{C}$ é um $D(R)*G$-módulo. Assim, temos que provar que cada diferencial em $\mathbf{C}$ é $D(R)*G$-linear. Para mostrar isso é suficiente ver que se $f, g \in R^G$ então o mapa natural $\eta : M_f \to M_{fg}$ (como no teorema 3.1) é $D(R)*G$-linear. Claramente η é $D(R)$-linear. Por um argumento análogo ao teorema (3.1) tem-se que $\eta(\sigma\xi) = \sigma(\eta(\xi))$ para qualquer $\sigma \in G$ e $\xi \in M_f$. Portanto η é $D(R) * G$-linear, e segue que $\mathbf{C}$ é um complexo de $D(R)*G$-módulos. Daí $H^i_{IR}(M)$ é um $D(R)*G$-módulo para todo $i \geq 0$.
(2) Note que o complexo $\mathbf{C}^G$ definido no teorema (2.16) é um complexo de Čech em M^G. Pelo teorema (2.16) segue que $H^i_{IA}(M)^G \cong H^i_I(M^G)$ para todo $i \geq 0$.

□

Como consequência trivial obtemos a prova do teorema (0.1).

Teorema 3.4. *(Com as hipóteses acima). Seja I um ideal em R^G. Então para todo $i \geq 0$, $H^i_I(R^G)$ possui comprimento finito como $D(R^G)$-módulo.*

Demonstração. Vamos aplicar o teorema (3.3) no caso em que $M = R$. Notemos que $H^i_{IR}(R)$ é um $D(R)$-módulo Holonômico ([16], página 46). Assim possui comprimento finito como $D(R)$-módulo (B.16). Segue que $H^i_{IR}(R)$ tem comprimento finito como $D(R) * G$-módulo. Logo pelo corolário (2.14) tem-se $H^i_l(R^G) = H^i_{IR}(R)^G$ possui comprimento finito como um $D(R)^G$-módulo. □

3.2 Resolução Injetiva Equivariante

Nesta seção A é um domínio normal comutativo com corpo de frações L. Também G é um subgrupo finito do grupo dos automorfismos de A. Assuma que $|G|$ é inversível sobre A. Seja A^G o anel dos invariantes de G. Então A^G é normal (vide [6], 6.4.1). Recorde também que todo domínio regular é normal. Seja F o corpo de frações de A^G. Note que G age em L e $L^G = F$. Assim L é uma extensão de Galois de F e o seu grupo de Galois é G. Seja $\mathfrak{m}$ um ideal maximal de A^G. Considere $\mathfrak{n}_1, ..., \mathfrak{n}_r$ todos os ideais maximais[2] sobre $\mathfrak{m}$. Por ([19], 8.3) para i, j existe $\sigma_i^j(\mathfrak{n}_i) = \mathfrak{n}_j$. Nosso principal resultado nessa seção é o seguinte:

[2]Essa quantidade de ideais maximais é finita em virtude de ([25], 8.1.17).

Teorema 3.5. *(com as hipóteses acima) Seja M um $A*G$-módulo. Então para todo $n \geq 0$,*
(1) O módulo de cohomologia local $H^n_{\mathfrak{m}A}(M)$ é um $A*G$-módulo.
(2) Como A-módulo, tem-se

$$H^n_{\mathfrak{m}A}(M) = \bigoplus_{i=1}^{r} \Gamma_{n_i}(H^n_{\mathfrak{m}A}(M)).$$

(3) Para $i = 1, ..., r$;

$$\Gamma_{n_i}(H^n_{\mathfrak{m}A}(M)) \cong H^n_{n_i}(M).$$

(4) Se $\sigma_i^j(\mathfrak{n}_i) = \mathfrak{n}_j$ então,

$$\sigma_i^j(\Gamma_{n_i}(H^n_{\mathfrak{m}A}(M))) = \Gamma_{n_j}(H^n_{\mathfrak{m}A}(M)).$$

Antes da demonstração, porém, precisamos do lema abaixo. Seu ingrediente fudamental é a sequência de Mayer–Vietoris bastante difundida em cohomologia local e topologia algébrica, sugerimos a ótima referência ([4]) para mais pormenores.

Lema 3.6. Sejam $\mathfrak{a}, \mathfrak{b}$ ideais de um anel R e M um R-módulo. Se $\mathfrak{a}, \mathfrak{b}$ são comaximais então temos um isomorfismo, $\Gamma_{\mathfrak{a}}(M) \oplus \Gamma_{\mathfrak{b}}(M) \cong \Gamma_{\mathfrak{a}\cdot\mathfrak{b}}(M)$.

Demonstração. Pela sequência de Mayer–Vietoris temos

$$0 \to \Gamma_{\mathfrak{a}+\mathfrak{b}}(M) \to \Gamma_{\mathfrak{a}}(M) \oplus \Gamma_{\mathfrak{b}}(M) \to \Gamma_{\mathfrak{a}\cap\mathfrak{b}}(M) \to H^1_{\mathfrak{a}+\mathfrak{b}}(M) \to ...$$

Como $\mathfrak{a}, \mathfrak{b}$ são comaximais então $\mathfrak{a} + \mathfrak{b} = R$ daí $\Gamma_{\mathfrak{a}+\mathfrak{b}}(M) = H^1_{\mathfrak{a}+\mathfrak{b}}(M) = 0$, e o resultado segue-se. □

Por indução, podemos provar que se $\mathfrak{a}_1, ..., \mathfrak{a}_n$ são comaximais então

$$\Gamma_{\mathfrak{a}_1\cdots\mathfrak{a}_n}(M) = \bigoplus_{i=1}^{n} \Gamma_{\mathfrak{a}_i}(M).$$

Finalmente vamos fornecer a prova de (3.5):

Demonstração. (Do teorema 3.5) A afirmação feita no item (1) segue do teorema (3.1). Seja $\mathbb{E}$ uma resolução injetiva de M como um $A*G$-módulo. Pelo lema (2.21) $\mathbb{E}$ também é uma resolução injetiva de M como um A-módulo. Observe que $\sqrt{\mathfrak{m}A} = \mathfrak{n}_1 \cdots \mathfrak{n}_r$. De fato, extensão $A^G \to A$ é inteira e $\mathfrak{n}_i \cap A^G = \mathfrak{m}$ para $i = 1, ..., r$. Afirmamos que $Var(\mathfrak{m}A) = \{\mathfrak{n}_1, ..., \mathfrak{n}_r\}$. Se $\mathfrak{q} \in Spec(A)$ e $\mathfrak{q} \supset \mathfrak{m}A$ então $\mathfrak{q} \cap A^G \supset \mathfrak{m}A \cap A^G = \mathfrak{m}$ (2.28). Portanto, $\mathfrak{m} = \mathfrak{q} \cap A^G \Rightarrow \mathfrak{q} = \mathfrak{n}_i$, para algum i. Logo, $Var(\mathfrak{m}A) = \{\mathfrak{n}_1, ..., \mathfrak{n}_r\}$ e

$$\sqrt{\mathfrak{m}A} = \bigcap_{\mathfrak{q} \in Var(\mathfrak{m}A)} \mathfrak{q} = \mathfrak{n}_1 \cap \cdots \cap \mathfrak{n}_r = \mathfrak{n}_1 \cdots \mathfrak{n}_r.$$

Note que os $\mathfrak{n}_i$ são comaximais (1.3) donde

$$\Gamma_{\mathfrak{m}A}(\mathbb{E}^n) = \bigoplus_{i=1}^{r} \Gamma_{\mathfrak{n}_i}(\mathbb{E}^n).$$

Seja d^n o n-ésimo diferencial do complexo $\Gamma_{\mathfrak{m}A}(\mathbb{E})$. Escreva $d^n = (\mu_{i,n}^j)$ onde $\mu_{i,n}^j : \Gamma_{\mathfrak{n}_i}(\mathbb{E}^n) \longrightarrow \Gamma_{\mathfrak{n}_j}(\mathbb{E}^{n+1})$ é A-linear.

Afirmação 1: $\mu_{i,n}^j = 0$ para $i \neq j$.

Prova da Afirmação 1: Seja $a \in \Gamma_{\mathfrak{n}_i}(\mathbb{E}^n)$. Então $\mu_{i,n}^j(a) \in \Gamma_{\mathfrak{n}_j}(\mathbb{E}^{n+1})$. Então existem t_1, t_2 tais que $\mathfrak{n}_i^{t_1} a = 0$ e $\mathfrak{n}_j^{t_2} \mu_{i,n}^j(a) = 0$. Como $i \neq j$ tem-se $\mathfrak{n}_i^{t_1} + \mathfrak{n}_j^{t_2} = A \Rightarrow 1 = c_i + c_j$ onde $c_i \in \mathfrak{n}_i^{t_1}$ e $c_j \in \mathfrak{n}_j^{t_2}$ daí $a = ac_i + ac_j = c_j a$. Portanto,

$$\mu_{i,n}^j(a) = c_j \mu_{i,n}^j(a) = 0.$$

□

Como consequência da afirmação 1 obtemos o módulo de n-co-ciclos:

$$Z^n(\Gamma_{\mathfrak{m}A}(\mathbb{E})) = \bigoplus_{i=1}^{r} Z^n(\Gamma_{\mathfrak{n}_i}(\mathbb{E})),$$

e os módulos de co-fronteiras:

$$B^n(\Gamma_{\mathfrak{m}A}(\mathbb{E}) = \bigoplus_{i=1}^{r} B^n(\Gamma_{\mathfrak{n}_i}(\mathbb{E})).$$

segue que

$$H^n_{\mathfrak{m}A}(M) = \bigoplus_{i=1}^{r} H^n_{\mathfrak{n}_i}(M).$$

Agora (2) e (3) segue do fato que $\Gamma_{\mathfrak{n}_i}(H^n_{\mathfrak{m}A}(M)) = H^n_{\mathfrak{n}_i}(M)$.

(4) Seja $\sigma_i^j(\mathfrak{n}_i) = \mathfrak{n}_j$. Antes de tudo vamos mostrar que $\sigma_i^j(\Gamma_{\mathfrak{n}_i}(\mathbb{E}^n)) = \Gamma_{\mathfrak{n}_j}(\mathbb{E}^n)$. Seja $\xi \in \Gamma_{\mathfrak{n}_i}(\mathbb{E})$, assim $\mathfrak{n}_i^s \xi = 0$ para algum $s \geq 1$. Note que $\sigma_i^j(\mathfrak{n}_i^s) = \mathfrak{n}_j^s$. Seja $b \in \mathfrak{n}_j^s$, portanto existe $a \in \mathfrak{n}_i^s$ com $\sigma_i^j(a) = b$. Observe que

$$b\sigma_i^j(\xi) = \sigma_i^j(a)\sigma_i^j(\xi) = \sigma_i^j(a\xi) = 0.$$

Consequentemente $\sigma_i^j(\xi) \in \Gamma_{\mathfrak{n}_j}(\mathbb{E}^n) \Rightarrow \sigma_i^j(\Gamma_{\mathfrak{n}_i}(\mathbb{E}^n)) \subseteq \Gamma_{\mathfrak{n}_j}(\mathbb{E}^n)$. Considerando $(\sigma_i^j)^{-1}$ obtém-se $(\sigma_i^j)^{-1}(\Gamma_{\mathfrak{n}_i}(\mathbb{E}^n)) \subseteq \Gamma_{\mathfrak{n}_j}(\mathbb{E}^n)$.
Como d^n é $A * G$-linear, decorre que o seguinte diagrama é comutativo:

$$\begin{tikzcd}
\Gamma_{\mathfrak{n}_i}(\mathbb{E}^n) \arrow[r, "\mu_{i,n}^i"] \arrow[d, "\sigma_i^j"] & \Gamma_{\mathfrak{n}_i}(\mathbb{E}^{n+1}) \arrow[d, "\sigma_i^j"] \\
\Gamma_{\mathfrak{n}_j}(\mathbb{E}^n) \arrow[r, "\mu_{i,n}^i"] & \Gamma_{\mathfrak{n}_j}(\mathbb{E}^{n+1}).
\end{tikzcd}$$

Com um argumento semelhante pode-se provar que

$$\sigma_i^j(Z^n(\Gamma_{\mathfrak{n}_i}(\mathbb{E}))) = Z^n(\Gamma_{\mathfrak{n}_j}(\mathbb{E})) \quad e \quad \sigma_i^j(B^n(\Gamma_{\mathfrak{n}_i}(\mathbb{E}))) = B^n(\Gamma_{\mathfrak{n}_j}(\mathbb{E})).$$

Portanto

$$\sigma_i^j(H^n_{\mathfrak{n}_i}(M)) = H^n_{\mathfrak{n}_j}(M).$$

□

3.3 Um Resultado Crucial

Nesta seção iremos provar um teorema que será fundamental na prova do teorema (0.1). Eis-o.

Teorema 3.7. *Sejam K um corpo e R um domínio regular contendo K. Seja G um subgrupo finito dos grupos dos automorfismos de R. Admita que $|G|$ é inversível em K. Considere R^G o anel dos invariantes de G e $I_1, I_2, ..., I_r$ ideais em R^G. Chamamos $T(R) = H^{i_1}_{I_1}(H^{i_2}_{I_2}(\cdots H^{i_r}_{I_r}(R^G)\cdots)$ para alguns $i_1, ..., i_r \geq 0$. Seja P um ideal primo de R^G com $ht(P) = g$. Então para todo $j \geq 0$,*

$$\left(H^j_P(T(R^G))\right)_P = H^g_{PR^G_P}(R^G_P)^s,$$

para algum $s \geq 0$ finito.

Demonstração. Sejam L o corpo de frações de R e F o corpo de frações de R^G. Note que L é uma extensão de Galois de F com grupo de Galois G. É claro que R^G é normal e que seu fecho inteiro de R^G em L é R. Seja

$$T(R) = H^{i_1}_{I_1R}(H^{i_2}_{I_2R}(\cdots H^{i_r}_{I_rR}(R)\cdots)).$$

Seja $A = R_P$,[3] então pelo lema (2.19), G age via o automorfismo em A e $A^G = R^G_P$

[3]Na realidade $A = S^{-1}R$, com $S = R^G \backslash P$ portanto R_P não é local.

é local; vide o lema (2.17) e o lema (2.19). Observe que A^G é normal e o seu fecho inteiro de A^G em L é A, vide ([1], 5.2). Note que PA^G é o único ideal maximal de A^G. Sejam $P_1, ..., P_r$ ideais maximais de A sobre P. Podemos verificar que $ht(P_l) = g$, para $l = 1, ..., r$. De fato, a desigualdade $ht(P_l) \leq ht(P) = g$ é satisfeita em virtude[4] da extensão inteira $R^G \to R$. A desigualdade oposta segue do fato que R é regular.[5] Por ([19], 9.3), para k, l; existe $\sigma_k^l \in G$ tal que $\sigma_k^l(P_k) = P_l$. Seja $M = T(A) = H^{i_1}_{I_1 A}(H^{i_2}_{I_2 A}(\cdots H^{i_r}_{I_r A}(A)\cdots))$. Então M é um $A * G$-módulo, assim pelo teorema (3.5) tem-se

$$H^j_{PA}(M) = \bigoplus_{l=1}^{r} H^j_{P_l}(M) \ \ e\ \sigma_k^l(H^j_{P_k}(M)) = H^j_{P_l}(M) \ \ para\ todos\ l, k.$$

Agora notemos que $T(R)_P = M$. Pela proposição (1.15)

$$\begin{aligned} H^j_{P_l}(M) &= H^j_{P_l}(M)_{P_l} \\ &= H^j_{P_l A_{P_l}}(M_{P_l}) \qquad\qquad por\ (1.36) \\ &= H^j_{P_l R_{P_l}}(T(R)_{P_l}) \\ &= H^l_{P_l}(H^{i_1}_{I_1 R}(H^{i_2}_{I_2 R}(\cdots H^{i_r}_{I_r R}(R)\cdots)))_{P_l}. \end{aligned}$$

Segue dos resultados de Lyubeznik ([16], 3.4) em característica zero e por ([17], 1.5, 2.14) em característica $p > 0$, que (1)

$$H^l_{I_l}(H^{i_1}_{I_1 R}(H^{i_2}_{I_2 R}(\cdots H^{i_r}_{I_r R}(R)\cdots)))_{P_l} = E_R(R/P_l)^{t_l}_{P_l} \quad para\ algum\ t_l \geq 0\ finito.$$

Também pela proposição (1.15),

$$H^g_{P_l A}(A) = H^g_{P_l A_{P_l}}(A_{P_l}) = E_R(R/P_l)_{P_l}.$$

Portanto

$$H^j_{PA}(M) = \bigoplus_{l=1}^{r} H^g_{P_l A}(A)^{t_l}.$$

Observe também que

$$\sigma_k^l(H^g_{P_l A}(A)^{t_l}) = H^g_{P_k A}(A)^{t_k} \quad para\ todos\ l, k.$$

daí concluímos que $t_1 = t_2 = \cdots = t_r$, pois σ é um automorfismo[6]. Ponhamos $s = t_1$.

[4]Ver ([19], Exercício 9.8).
[5]Ver ([19], Exercício 9.9, Teorema 9.4) e que todo domínio regular é normal.
[6]Isso implica $H^g_{P_l A}(A)^{t_l} = H^g_{P_k A}(A)^{t_k}$ donde $t_l = t_k$ para todos l, k.

então

$$H^j_P(M) = \left(\bigoplus_{l=1}^{r} H^g_{P_lA}(A)\right)^s \cong H^g_{PA}(A)^s;$$

como $A * G$-módulos. Tomando invariantes tem-se

$$H^j_{PA^G}(M^G) \cong H^P_{PA^G}(A^G)^s \cong H^g_{PR^G_P}(R^G_P)^s.$$

Por fim notando que

$$H^j_{PA^G}(M^G) \cong (H^j_P(T(R^G)))_P.$$

o resultado segue.

□

Observação 3.8. (Com as hipótese acima) Seja $A = R_P$. Se $N = T(R)_P$ e se $P_1, ..., P_r$ são ideais primos em R sobre P então mostramos que

$$H^j_{PA}(N) \cong \bigoplus_{l=1}^{r} H^g_{P_l}(A)^s$$

e

$$H^j_P(T(R^G)_P) \cong H^g_{PR^G_P}(R^G_P)^s.$$

é importante notar que a mesma constante aparece em ambas as equações acima.

O próximo lema pode ser encontrado em ([29]). Ele é fundamental para a demonstração do último teorema desta seção.

Lema 3.9. Sejam $(A, \mathfrak{m}, k)$ um anel Local noetheriano e $E = E_R(\frac{R}{\mathfrak{m}})$. Então:
(a) O módulo E é artiniano;
(b) O módulo M é artiniano $\Leftrightarrow M \subset E^n$, para algum $n \geq 1$.

3.4 O Caso em que R^G é Gorenstein

Nesta seção iremos provar a primeira parte do teorema (0.1).

Teorema 3.10. *Sejam K um corpo e R um domínio regular contendo K. Seja G um subgrupo finito dos grupos dos automorfismos de R. Admita que $|G|$ é inversível em K. Considere R^G o anel dos invariantes de G. Além disso, suponha que R^G é Gorenstein. Sejam $I_1, I_2, ..., I_r$ ideais em R^G. Chamamos $T(R^G) = H^{i_1}_{I_1}(H^{i_2}_{I_2}(\cdots H^{i_r}_{I_r}(R^G)\cdots)$ e $T(R) = H^{i_1}_{I_1R}(H^{i_2}_{I_2R}(\cdots H^{i_r}_{I_rR}(R)\cdots)$ para alguns $i_1, ..., i_r \geq 0$. Então:*
(i) $injdim_{R^G}(T(R^G)) \leq dim\ SuppT(R^G)$;
(ii) Seja P um ideal primo em R^G. Então $\mu_j(P, T(R^G)) = \mu_j(P', T(R))$ onde P' é qualquer ideal primo de R sobre P.

Para tanto invocamos o lema ([16], 1.4).

Lema 3.11. Seja A um anel noetheriano e M um A-módulo (M não necessita ser finitamente gerado). Seja P um ideal primo em A. Se $(H^j_P(M))_P$ é injetivo para todo $j \geq 0$ então $\mu_j(P, M) = \mu_0(P, H^j_P(M))$.

Agora fornecemos a

Demonstração. (Do teorema 3.10). Ponha $M = T(R^G)$ Seja P um ideal primo de R^G de altura igual a g.
(i) Pelo Teorema (3.3) tem-se

$$H^j_P(M)_P = H^g_{PR^G_P}(R^G_P)^s \quad para\ algum\ s \geq 0\ finito.$$

Como R^G é Gorenstein tem-se que R^G_P é um anel local Gorenstein. Assim

$$g = ht(PR^G_P) = dim(R^G_P) = H^g_{PR^G_P}(R^G_P \cong E_{R^G_P}(R^G_P/PR^G_P) \cong E_{R^G}(R^G/P),$$

daí $H^j_P(M)_P \cong E_{R^G}(R^G/P)^s$ é um R^G-módulo injetivo.

Então pelo lema (3.11) temos que

$$\mu_j(P, M) = \mu_0(P, H^j_P(M)).$$

Pelo teorema de anulamenento de Grothendieck (1.27) $H^j_P(M) = 0$ para $j > dim\ Supp\ M$. então $\mu_j(P, M) = 0$ para todo $j > dim\ Supp\ M$ para qualquer idela primo P de R^G. Assim se $\mathbb{E}$ é uma resolução injetiva minimal de M tem-se $\mathbb{E}^j = 0$ para $j > dim\ Supp\ M$. Então

$$injdim\ M \leq dim\ Supp\ M.$$

(ii) A idéia é localizar em P e usar o resultado (3.8). Note que

$$H^j_{PR_P}(T(R)_P) \cong \bigoplus_{l=1}^{r} H^g_{P'_l} H^g_{P'_l}(R_P)^s \cong \bigoplus_{l=1}^{r} E_R\left(\frac{R}{P'_l}\right)^s$$

donde $\mu_0(P'_l, H^J_{PR^P}(T(R)_P)) = \mu_j(P', T(R)) = s$. Da mesma maneira,

$$H^j_P(T(R^G)_P) \cong H^g_{PR^G_P}(R^G_P)^s \cong E_{R^G}(R^G/P)^s,$$

donde $\mu_0(P, H^j_P(T(R^G)_P)) = \mu_j(P, T(R^G)) = s.$ □

3.5 O Caso em que R^G não é Gorenstein

Nesta seção provamos a segunda parte do teorema (0.1).

Teorema 3.12. *Sejam K um corpo e R um domínio regular contendo K. Seja G um subgrupo finito dos grupos dos automorfismos de R. Admita que $|G|$ é inversível em K. Considere R^G o anel dos invariantes de G. Sejam $I_1, I_2, ..., I_r$ ideais em R^G. Chamamos $T(R^G) = H^{i_1}_{I_1}(H^{i_2}_{I_2}(\cdots H^{i_r}_{I_r}(R^G)\cdots)$ para alguns $i_1, ..., i_r \geq 0$. Seja P um ideal primo de R^G com R^G_P não Gorenstein. Então para todo $j \geq 0$, os números de Bass $\mu_j(P, H^i_I(R^G))$ são zero para todo j ou existe c tal que $\mu_j(P, H^i_I(R^G)) = 0$ para $j < c$ e $\mu_j(P, H^i_I(R^G)) > 0$ para todo $j \geq c$.*

Demonstração. Após localizarmos, é suficiente provar o resultado para ideais maximais, vide (2.17) e (2.19). Sejam $\mathfrak{m}$ um ideal maximal em R^G e $d = ht(\mathfrak{m})$. Sejam $M = T(R^G), E = E_{R^G}(R^G/\mathfrak{m})$ e $l = R^G/\mathfrak{m}$. Seja $\mathbb{G}$ uma resolução injetiva minimal de M. Sabemos que $\mathbb{G}^j = \bigoplus_{\mathfrak{p}\in Spec(R^G)} E_{R^G}\left(\frac{R^G}{\mathfrak{p}}\right)^{\mu_i(\mathfrak{p},M)}$. Assim podemos escrever

$$\mathbb{G}^j = \widetilde{\mathbb{G}^j} \oplus E^{r_j}, \qquad com\ \mathfrak{m} \notin Ass(\widetilde{\mathbb{G}^j})^7.$$

Então, $\mu_j(\mathfrak{m}, M) = r_j$ para $j \geq 0$. Sabemos que r_j é finito para todo $j \geq 0$, a justificativa vem de (3.9). Suponhamos que existe j tal que $r_j > 0$. Seja $c = \min\{j \mid r_j > 0\}$. Iremos mostrar que

$$r_j > 0,\ para\ todo\ j \geq c. \tag{3.1}$$

Seja $\mathbb{E} = \Gamma_\mathfrak{m}(\mathbb{G})$. Primeiramente temos:

Afirmação 3.13. $\mathbb{E}^j = E^{r_j}$ para todo $j \geq 0$.

Prova 1: $\mathbb{E}^j = \Gamma_\mathfrak{m}(\mathbb{G}^j) = \Gamma_\mathfrak{m}(\widetilde{\mathbb{G}^j} \oplus E^{r_j}) = \Gamma_\mathfrak{m}(\widetilde{\mathbb{G}^j}) \oplus \Gamma_\mathfrak{m}(E^{r_j}) = 0 \oplus E^{r_j} = E^{r_j}$, já que usando-se (1.12) e o fato que $\mathfrak{m} \notin Ass(\mathbb{G}^j)$ vem $Ass(\Gamma_\mathfrak{m}(\widetilde{\mathbb{G}^j})) = 0 \Rightarrow \Gamma_\mathfrak{m}(\widetilde{\mathbb{G}^j}) = 0$. A outra parte, usou-se o seguinte fato $\Gamma_\mathfrak{a}(M) = M \Leftrightarrow Ass(M) = Var(\mathfrak{a})$. □

Prova 2: Temos

$$\mathbb{E}^j = \Gamma_\mathfrak{m}(\mathbb{G}^j) = \Gamma_\mathfrak{m}\left(E_{R^G}\left(\frac{R^G}{\mathfrak{m}}\right)\right)^{r_j} \cong E_{R^G}\left(\Gamma_\mathfrak{m}(R^G/\mathfrak{m})\right)^{r_j} = E_{R^G}(R^G/\mathfrak{m})^{r_j} = E^{r_j},$$

onde usamos (1.8). □

Além disso pelo lema (3.3) e a proposição (1.15) tem-se,

$$H^j(\mathbb{E}) = H^j(\Gamma_\mathfrak{m}(\mathbb{G})) = H^j_\mathfrak{m}(M) = H^j_\mathfrak{m}(T(R^G)) \cong H^j_\mathfrak{m}(T(R^G))_\mathfrak{m} \cong H^d_{\mathfrak{m}R^G_\mathfrak{m}}(R^G_\mathfrak{m})^{s_{ij}}$$

$$\cong H^d_{\mathfrak{m}R^G_\mathfrak{m}}(R^G_\mathfrak{m} \otimes R^G_\mathfrak{m})^{s_{ij}} \cong H^d_\mathfrak{m}(R^G)^{s_{ij}} \otimes_{R^G} R^G_\mathfrak{m} \cong (H^d_\mathfrak{m}(R^G)^{s_{ij}})_\mathfrak{m}$$

[7] já que $Ass(\bigoplus M_i) = \bigcup Ass(M_i)$ e $Ass(E_R(R/\mathfrak{p})) = \{\mathfrak{p}\}$.

$$\cong H^d_{\mathfrak{m}}(R^G)^{s_{ij}} \quad \textit{para algum } s_{ij} \geq 0 \textit{ finito}[8].$$

Considere S o completamento de R^G em $\mathfrak{m}$, ou seja, $S = \varprojlim_{n\in\mathbb{N}} R^G/\mathfrak{m}^n := \bigwedge_{\mathfrak{m}}(R^G)$. Notemos que

$$E_{R^G}\left(\frac{R^G}{\mathfrak{m}}\right) = E_{R^G_{\mathfrak{m}}}\left(\frac{R^G_{\mathfrak{m}}}{\mathfrak{m}R^G_{\mathfrak{m}}}\right)$$

e

$$E_S\left(\frac{S}{\mathfrak{m}S}\right) = E_{\bigwedge_{\mathfrak{m}R^G_{\mathfrak{m}}}(R^G_{\mathfrak{m}})}\left(\frac{\bigwedge_{\mathfrak{m}R^G_{\mathfrak{m}}}(R^G_{\mathfrak{m}})}{\mathfrak{m}R^G\bigwedge_{\mathfrak{m}R^G_{\mathfrak{m}}}(R^G_{\mathfrak{m}})}\right).$$

O isomorfismo $\bigwedge_{\mathfrak{m}}(R^G) \cong \bigwedge_{\mathfrak{m}R^G_{\mathfrak{m}}}(R^G_{\mathfrak{m}})$, decorre de $R^G/\mathfrak{m}^n \cong R^G_{\mathfrak{m}}/\mathfrak{m}^n R^G_{\mathfrak{m}}$ e do fato que o seguinte diagrama é comutativo:

$$\begin{array}{ccc} \dfrac{R^G}{\mathfrak{m}^{n+1}} & \longrightarrow & \dfrac{R^G_{\mathfrak{m}}}{\mathfrak{m}^{n+1}R^G_{\mathfrak{m}}} \\ \downarrow & & \downarrow \\ \dfrac{R^G}{\mathfrak{m}^{n}} & \longrightarrow & \dfrac{R^G_{\mathfrak{m}}}{\mathfrak{m}^{n}R^G_{\mathfrak{m}}}. \end{array}$$

Portanto,

$$E_{R^G_{\mathfrak{m}}}\left(\frac{R^G_{\mathfrak{m}}}{\mathfrak{m}R^G_{\mathfrak{m}}}\right) = E_{\bigwedge_{\mathfrak{m}R^G_{\mathfrak{m}}}(R^G_{\mathfrak{m}})}\left(\frac{\bigwedge_{\mathfrak{m}R^G_{\mathfrak{m}}}(R^G_{\mathfrak{m}})}{\mathfrak{m}R^G\bigwedge_{\mathfrak{m}R^G_{\mathfrak{m}}}(R^G_{\mathfrak{m}})}\right).$$

Conclusão, $E = E_S(S/\mathfrak{m}S)$. Sejam $(-)^\vee = Hom_S(-, E_S)$ o dual de Matlis do funtor S e $Z^j = Ker(\delta^j), B^j = Im(\delta^{j-1})$ os módulos dos j-co-ciclos e j-co-fronteira do complexo $\mathbb{E} : \cdots \to E^{j-1} \overset{\delta^{j-1}}{\to} E^j \overset{\delta^j}{\to} E^{j+1} \to \cdots$. Vamos provar as seguintes afirmações por indução em $j \geq c$:

(i) $Z^j \neq 0$;

(ii) injdim $Z^j = \infty$;

(iii) $(Z^j)^\vee$ é um S-módulo não livre Cohen Macaulay maximal;

(iv) $B^{j+1} \neq 0$;

(v) injdim$B^{j+1} = \infty$;

(vi) $(B^{j+1})^\vee$ é um S-módulo não livre Cohen Macaulay maximal.

é conveniente provar todas as afirmações juntas para $j \geq c$. Note que (i) implicará nossa afirmação. Vamos provar o resultado para $j = c$. Note que como $\mathbb{G}$ é uma resolução injetiva minimal de $M = T(R)$ tem-se que a aplicação

[8]recorde $S^{-1}R \otimes M \cong S^{-1}M$ e (1.36) .

$$Hom_{R^G_{\mathfrak{m}}}\left(\frac{R^G_{\mathfrak{m}}}{\mathfrak{m}R^G_{\mathfrak{m}}}, \mathbb{G}^j_{\mathfrak{m}}\right) \longrightarrow Hom_{R^G_{\mathfrak{m}}}\left(\frac{R^G_{\mathfrak{m}}}{\mathfrak{m}R^G_{\mathfrak{m}}}, \mathbb{G}^{j+1}_{\mathfrak{m}}\right)$$

é a aplicação nula. Mas

$$Hom_{R^G_{\mathfrak{m}}}\left(\frac{R^G_{\mathfrak{m}}}{\mathfrak{m}R^G_{\mathfrak{m}}}, \mathbb{G}^j_{\mathfrak{m}}\right) = Hom_{R^G}\left(\frac{R^G}{\mathfrak{m}}, \mathbb{G}^j\right)_{\mathfrak{m}}$$

donde pelo princípio local-global tem-se que a aplicação abaixo é nula:

$$Hom_{R_G}(l, \mathbb{G}^j) \longrightarrow Hom_{R_G}(l, \mathbb{G}^{j+1}),$$

recorde que $l = R^G/\mathfrak{m}$.

Desde que $Hom_{R_G}(l, \widetilde{\mathbb{G}^j}) = 0$ para todo $j \geq 0$[9] obtemos que a aplicação abaixo é nula

$$Hom_{R_G}(l, \widetilde{\mathbb{G}^j} \oplus E^{r_j}) \longrightarrow Hom_{R_G}(l, \widetilde{\mathbb{G}^{j+1}} \oplus E^{r_{j+1}})$$

e por sua vez,

$$Hom_{R_G}(l, E^{r_j}) \longrightarrow Hom_{R_G}(l, E^{r_{j+1}}) \; \forall \; j \geq 0$$

é a aplicação nula também. Se $Z^c = 0$ consideramos a sequência $0 \to E^c \to E^{c+1}$ e aplicando o funtor Hom: $0 \to Hom_{R^G}(l, E^c) \to Hom_{R^G}(l, E^{c+1})$ tem-se $Hom_{R^G}(l, E^c) = (0 :_{E^c} \mathfrak{m}) = 0$ mas $E^c = E_{R^G}\left(\frac{R^G}{\mathfrak{m}}\right)^c \supseteq \left(\frac{R^G}{\mathfrak{m}}\right)^c$ seria tal que $(0 :_{E^c} \mathfrak{m}) \neq 0$, logo $Z^c \neq 0$.

Também $Z^c = Ker(\delta^c)$ e já vimos que $H^d_{\mathfrak{m}}(M) = H^d_{\mathfrak{m}}(R^G)^{s_{ij}}$. Agora dado o complexo: $\cdots \mathbb{G}^{c-1} \to \mathbb{G}^c \to \mathbb{G}^{c+1} \to \cdots$ aplicando $\Gamma_{\mathfrak{m}}(-)$ tem-se:

$$\cdots \to \Gamma_{\mathfrak{m}}(\mathbb{G}^{c-1}) \to \Gamma_{\mathfrak{m}}(\mathbb{G}^c) \to \Gamma_{\mathfrak{m}}(\mathbb{G}^{c+1}) \to \cdots$$

ou seja,

$$\cdots \to 0 \overset{\delta^{c-1}}{\to} E^c \overset{\delta^c}{\to} E^{c+1} \to \cdots$$

daí $H^c_{\mathfrak{m}}(T(R^G)) = Ker(\delta^c)/Im(\delta^{c-1}) = Ker(\delta^c) = Z^c$. Conclusão $Z^c = H^d_{\mathfrak{m}}(R^G)^{s_{ij}}$ para algum $s_{ij} > 0$ finito. Agora

$$H^d_{\mathfrak{m}}(R^G) \cong (H^d_{\mathfrak{m}}(R^G))_{\mathfrak{m}} \cong H^d_{\mathfrak{m}R^G_{\mathfrak{m}}}(R^G_{\mathfrak{m}}) \cong H^d_{\mathfrak{m}R^G_{\mathfrak{m}}}(R^G_{\mathfrak{m}}) \otimes_{R^G_{\mathfrak{m}}} \bigwedge_{\mathfrak{m}R^G_{\mathfrak{m}}}(R^G_{\mathfrak{m}})$$

$$\cong H^d_{\mathfrak{m}\bigwedge_{\mathfrak{m}R^G_{\mathfrak{m}}}(R^G_{\mathfrak{m}})}\left(\bigwedge_{\mathfrak{m}R^G_{\mathfrak{m}}}(R^G_{\mathfrak{m}})\right) \cong H^d_{\mathfrak{m}S}(S) \cong H^d_{\mathfrak{m}}(S),$$

[9] $Ass\left(Hom_{R^G}\left(\frac{R^G}{\mathfrak{m}}, \widetilde{\mathbb{G}}^j\right)\right) = Supp\left(\frac{R^G}{\mathfrak{m}}\right) \cap Ass(\widetilde{\mathbb{G}}^j) = Var(\mathfrak{m}) \cap \{\mathfrak{p} \in Spec(R) \mid \mathfrak{p} \neq \mathfrak{m}\} = \emptyset.$

onde usamos sucessivamente (dentre outras coisas) a proposição (1.15) e ([6], 3.5.4(d)). Como S não é Gorenstein segue que $H^d_{\mathfrak{m}}(S)$ não é injetivo (B.62). Além disso $H^d_{\mathfrak{m}}(S)^\vee = \omega$ o módulo canônico de S é um S-módulo não livre[10] Cohen Macaulay maximal.

Afirmação 3.14. Z^c possui dimensão injetiva infinita.

Justificativa: Sabemos que $\Gamma_{\mathfrak{m}}(E^j(S)) = 0 \,\forall\, j < c$ e $0 \to H^d_{\mathfrak{m}}(S) \to \Gamma_{\mathfrak{m}}(E^d(S)) \to \Gamma_{\mathfrak{m}}(E^{d+1}(S)) \to \cdots$ é uma resolução injetiva infinita minimal assim $0 \to Z^c \to \Gamma_{\mathfrak{m}}(E^d(S))^{s_{ij}} \to \Gamma_{\mathfrak{m}}(E^{d+1}(S))^{s_{ij}} \to \cdots$ é uma resolução injetiva infinita minimal. □

Note que $(Z^c)^\vee = \omega^{s_{ij}}$ é um S-módulo não livre Cohen Macaulay maximal. Considere a sequência exata

$$0 \longrightarrow Z^c \longrightarrow E^{r_c} \longrightarrow B^{c+1} \longrightarrow 0.$$

Em virtude de injdim$Z^c = \infty$ segue que $B^{c+1} \neq 0$ (caso contrário $Z^c \cong E^{r_c}$ absurdo) e B^{c+1} possui dimensão injetiva infinita. Aplicando o dual de Matlis obtem-se, a sequência exata

$$0 \longrightarrow (B^{c+1})^\vee \longrightarrow S^{r_c} \longrightarrow (Z^c)^\vee \longrightarrow 0.$$

Portanto $(B^{c+1})^\vee$ é um S-módulo não livre ((1.40)) Cohen Macaulay maximal (B.45).

Agora assuma que o resultado vale para $j = n$, vamos provar para $j = n+1$. Considere a sequência exata

$$0 \longrightarrow B^{n+1} \longrightarrow Z^{n+1} \longrightarrow H^{n+1}(\mathbb{E}) \longrightarrow 0.$$

Por razões óbvias $Z^{n+1} \neq 0$. Se $H^{n+1}(\mathbb{E}) = 0$ então claramente Z^{n+1} satisfaz as propriedades (2) e (3). Se $H^{n+1}(\mathbb{E}) \neq 0$ então $H^{n+1}(\mathbb{E})$ é isomorfo a $H^d_{\mathfrak{m}}(S)^{s_n}$ para algum $s_n > 0$ finito. Tomando o dual de Matlis obtém-se

$$0 \longrightarrow \omega^{s_n} \longrightarrow (Z^{n+1})^\vee \longrightarrow (B^{n+1})^\vee \longrightarrow 0.$$

Mas para qualquer S-módulo Cohen Macaulay maximal N tem-se $Ext^1_S(N, \omega) = 0$ [6][Teorema 3.3.10]. Segue que (A.12)

$$(Z^{n+1})^\vee \cong \omega^{s_n} \oplus (B^{n+1})^\vee.$$

Disso segue que $(Z^{n+1})^\vee$ é um S-módulo não livre[11] Cohen Macaulay maximal. Também

[10] De fato, se fosse livre seria plano e dual de plano é injetivo (1.40), uma contradição.

[11] Caso não fosse livre teríamos tanto ω^{s_n} como $(B^{n+1})^\vee$ módulos projetivos donde livres, absurdo.

tomando o dual de Matlis obtém-se (1.39)

$$Z^{n+1} \cong B^{n+1} \oplus H^d_{\mathfrak{m}}(S)^{s_n};$$

tem dimensão injetiva infinita. Considere a sequência exata

$$0 \longrightarrow Z^{n+1} \longrightarrow E^{r_{n+1}} \longrightarrow B^{n+2} \longrightarrow 0.$$

Como $\text{injdim} Z^{n+1} = \infty \Rightarrow B^{n+2} \neq 0$ e possui dimensão injetiva infinita. Finalmente tomando o dual de Matlis obtém-se a sequência exata

$$0 \longrightarrow (B^{n+2})^{\vee} \longrightarrow S^{r_{n+1}} \longrightarrow (Z^{n+1})^{\vee} \longrightarrow 0.$$

Portanto $(B^{n+2})^{\vee}$ é um S-módulo não livre Cohen Macaulay maximal (B.45). Finalmente, provamos que $Z^j \neq 0$ para $j \geq c$ e isso termina a demonstração pois, a partir da sequência $0 \to Z^c \to E^{r_c} \to B^{c+1} \to 0$ tem-se $Z^c \neq 0 \Rightarrow E^{r_c} \neq 0 \Rightarrow r_c > 0$. (3.1)

□

Apêndice A

Módulos Injetivos

Neste apêndice, R denotará um anel comutativo. Se M e N são R-módulos, "M é um submódulo de N" (notação $M \subseteq N$) e "existe um homomorfismo injetor $\iota : M \to N$" são equivalentes e serão usadas neste texto de maneira indistinta, identificando-se assim o módulo M com sua imagem $\iota(M)$ em N.

A.1 Módulos Injetivos

Um R-módulo E é dito *injetivo* se para cada homomorfismo injetivo $\alpha : M' \to M$ e cada homomorfismo $f : M' \to E$, existe um *levantamento* $g : M \to E$ (isto é, $g\alpha = f$).

$$\begin{tikzcd} M' \arrow[r, "\alpha"] \arrow[d, "f"'] & M \arrow[dl, dotted, "g"] \\ E & \end{tikzcd}$$

Equivalentemente, o R-módulo E é injetivo quando o funtor contravariante $\mathrm{Hom}_R(-, E) : R\text{-mód} \to \text{R-mód}$ é *exato*, isto é, $\mathrm{Hom}_R(-, E)$ transforma sequências exatas curtas em sequências exatas curtas (observe que $\mathrm{Hom}_R(\alpha, E)(g) = g\alpha$ para quaisquer morfismos $\alpha : M' \to M$ e $g : M \to E$).

Se $E = \prod_{i \in \Lambda} E_i$, então, E é injetivo se, e somente se, cada E_i for injetivo. Isto vem do fato de que todo homomorfismo $M' \to E$ é determinado de maneira única pelas projeções $M' \to E_i$.

Na prática, não é necessário testar todos os homomorfismos possíveis entre R-módulos para comprovar injetividade.

Lema A.1. (Critério de Baer) Um R-módulo E é injetivo se, e somente se, todo homomorfismo $\mathfrak{b} \to E$ estende a um homomorfismo $R \to E$ para todo ideal $\mathfrak{b}$ de R.

Demonstração. Se E é injetivo, então, todo homomorfismo $\mathfrak{b} \to E$ estende a um homomorfismo $R \to E$ para todo ideal $\mathfrak{b}$ de R: faça $M' = \mathfrak{b}$, $M = R$ e $\alpha = \iota$ a inclusão.

Reciprocamente, considere um homomorfismo injetivo $\alpha : M' \to M$ e um homomorfismo $f : M' \to E$. Considere também a família de pares

$$\mathscr{F} = \{(N, g_N) : \alpha(M') \subseteq N \subseteq M \text{ e } g_N : N \to E \text{ é tal que } g_N\alpha = f\}.$$

Esta família satisfaz as hipóteses do Lema de Zorn[1] com a ordem $(N, g_N) \leq (N', g_{N'})$ quando $N \subseteq N'$ e $g_{N'}|_N = g_N$. Isto define uma ordem parcial, de fato:
(Reflexividade):

$$\begin{tikzcd} N \arrow[r, "Id_N"] \arrow[d, "g_N"'] & N \arrow[dl, dotted, "g_N"] \\ E & \end{tikzcd}$$

(Antissimetria): Se

$$\begin{tikzcd} N' \arrow[r, "\iota'"] \arrow[d, "g_{N'}"'] & N \arrow[dl, dotted, "g_N"] \\ E & \end{tikzcd} \qquad e \qquad \begin{tikzcd} N \arrow[r, "\iota"] \arrow[d, "g_N"'] & N' \arrow[dl, dotted, "g_{N'}"] \\ E & \end{tikzcd}$$

então $g_N(n) = g_{N'}(\iota(n)) = g_{N'}(n)$ para todo $n \in N$.

(Transitividade): trivial.

Defina o conjunto

$$\{(N_\lambda, g_{N_\lambda})_{\lambda\in\Lambda} : (N_\lambda, g_{N_\lambda}) \leq (N_{\lambda'}, g_{n_{\lambda'}}) \textit{ quando } \lambda \leq \lambda', \Lambda \textit{ totalmente ordenado}\}$$

e $N = \bigcup_{\lambda\in\Lambda} N_\lambda$, $g_N : N \to E$ definida por $n \longmapsto g_N(n) = g_{N_\lambda}(n)$ se $n \in N_\lambda$ é uma cota superior.

Então, existe um elemento maximal (H, g). Se $H \neq M$, considere $x \in M - H$ e $\mathfrak{b} = (H :_R x)$. Existe uma aplicação

$$\varphi : \mathfrak{b} \xrightarrow{\mu_x} H \xrightarrow{g} E.$$

Logo, esta aplicação estende a $\tilde{\varphi} : R \to E$. Defina $\psi : H + Rx \to E$ como $\psi(h + rx) = g(h) + \tilde{\varphi}(r)$. Observemos que ψ está bem definida: se $h + rx = h' + r'x$, então, $h - h' = (r' - r)x$ e $g(h) - g(h') = g((r' - r)x)$. Por outro lado, $r' - r \in \mathfrak{b} \Rightarrow (r' - r)x \in H$ e $\tilde{\varphi}(r') - \tilde{\varphi}(r) = \tilde{\varphi}(r' - r) = g((r' - r)x)$. Logo, $g(h) + \tilde{\varphi}(r) = g(h') + \tilde{\varphi}(r')$. Além disso, ψ é um homomorfismo, $H \subsetneq H + Rx$ e $\psi|_H = g$, o que é uma contradição com

[1] Se, em um conjunto não-vazio e parcialmente ordenado, todo subconjunto não-vazio totalmente ordenado tem uma cota superior, então o conjunto tem um elemento maximal.

a maximalidade do par (H, g). $\square$

Seja D um grupo abeliano. Dizemos que D é *divisível* se para cada $d \in D$ e cada $n \in \mathbb{N} - \{0\}$, existe $d' \in D$ tal que $d = nd'$.

Existem vários exemplos de grupos abelianos divisíveis:

Exemplo A.2. O grupo abeliano $\mathbb{Q}$ dos números racionais é divisível.

Exemplo A.3. Somas diretas e produtos diretos de grupos abelianos divisíveis são divisíveis.

Solução A.4. Com efeito, seja $d \in \oplus_{i=1}^{n} D_i$ e $n \in \mathbb{N} \backslash \{0\}$, como cada D_i é divisível $d_i = nd_i'$ então $d = (d_1, ..., d_n) = n(d_1', ..., d_n') = nd'$, onde $d' = (d_1', ..., d_n')$.

Exemplo A.5. Quocientes de grupos abelianos divisíveis são divisíveis.

Solução A.6. Com efeito, se D é divisível e sendo $D' \leq D$ dado $d \in D$ e $n \in \mathbb{N} \backslash \{0\}$, existe $d' \in D$ tal que $d = nd'$ logo $d + D' \in D/D' \Rightarrow d + D' = nd' + D' = n(d' + D')$, como se queria.

Esta nova definição fornece outra caracterização no contexto.

Proposição A.7. Um grupo abeliano D é injetivo (isto é, um $\mathbb{Z}$-módulo injetivo) se, e somente se, é divisível.

Demonstração. Se D é injetivo, considere $e \in D$ e $n \in \mathbb{N} - \{0\}$. Fica definido um homomorfismo $f : n\mathbb{Z} \to D$ por $f(rn) = re$ para cada $r \in \mathbb{Z}$. Logo, existe uma extensão $h : \mathbb{Z} \to D$, isto é, $h(rn) = f(rn)$ para cada $r \in \mathbb{Z}$. Assim, $e = f(n) = h(n) = nh(1)$, donde D é divisível.

Reciprocamente, suponha que D é divisível e considere um homomorfismo $f : n\mathbb{Z} \to D$ onde $n \in \mathbb{N} - \{0\}$. Assim, existe $e \in D$ tal que $f(n) = ne$. Defina $h : \mathbb{Z} \to E$ por $h(r) = re$. Deste modo, h é um homomorfismo que estende f. Pelo Critério de Baer, D é injetivo. $\square$

Procedemos à primeira parte da existência de módulos injetivos.

Proposição A.8. Todo grupo abeliano é subgrupo de um grupo abeliano injetivo.

Demonstração. Podemos ver o grupo abeliano $G = \sum_{g \in G} \mathbb{Z}g$. Consideremos o grupo livre $F = \bigoplus_{g \in G} \mathbb{Z}$. Deste modo, $G \cong \frac{F}{N}$. Mas $F \subseteq D$, onde $D = \bigoplus_{g \in G} \mathbb{Q}$ é divisível, já que $\mathbb{Q}$ o é. Portanto, $G \subseteq \frac{D}{N}$ e o enunciado segue do exemplo 3 e da Proposição (A.7). $\square$

Lema A.9. Se D é um grupo abeliano divisível, então, $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ é um R-módulo injetivo.

Demonstração. O grupo abeliano $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ torna-se um R-módulo definindo $rf : a \mapsto f(ar)$ para cada $r \in R$ e cada $f \in \mathrm{Hom}_{\mathbb{Z}}(R, D)$. Agora, o funtor $\mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbb{Z}}(R, D))$ é naturalmente equivalente à composição $\mathrm{Hom}_{\mathbb{Z}}(-, D) \circ (R \otimes_R -)$. O funtor $R \otimes_R -$ é naturalmente equivalente ao funtor id, logo exato, e o funtor $\mathrm{Hom}_{\mathbb{Z}}(-, D)$ é exato porque D é injetivo. Portanto, o funtor $\mathrm{Hom}_R(-, \mathrm{Hom}_{\mathbb{Z}}(R, D))$ é exato, donde $\mathrm{Hom}_{\mathbb{Z}}(R, D)$ é um R-módulo injetivo. $\square$

Concluímos desta forma que a categoria dos R-módulos possui injetivos suficientes.

Teorema A.10. *Todo módulo é submódulo de um módulo injetivo.*

Demonstração. Defina $\varphi : M \to \mathrm{Hom}_{\mathbb{Z}}(R, M)$ como $m \mapsto \varphi_m$ onde $\varphi_m : R \to M$ é definida como $r \mapsto \varphi_m(r) = rm$. Observe que φ é um homomorfismo injetor de grupos. Também, existe um grupo abeliano injetivo D e um homomorfismo injetor de grupos $\iota : M \to D$. Agora, $\mathrm{Hom}_{\mathbb{Z}}(R, \iota) : \mathrm{Hom}_{\mathbb{Z}}(R, M) \to \mathrm{Hom}_{\mathbb{Z}}(R, D)$ é um homomorfismo injetor. Mais ainda, $\mathrm{Hom}_{\mathbb{Z}}(R, \iota)\varphi : M \to \mathrm{Hom}_{\mathbb{Z}}(R, D)$ é um homomorfismo de R-módulos: de fato, $\mathrm{Hom}_{\mathbb{Z}}(R, \iota)\varphi(rm) = \mathrm{Hom}_{\mathbb{Z}}(R, \iota)(\varphi_{rm}) = \iota\varphi_{rm} : a \mapsto \iota(arm)$. Por outro lado, $r\mathrm{Hom}_{\mathbb{Z}}(R, \iota)\varphi(m) = r\iota\varphi_m$ e $r\iota\varphi_m(a) = \iota\varphi_m(ar) = \iota(arm)$ para cada $a \in R$, concluindo o requerido. $\square$

Uma sequência exata curta

$$0 \longrightarrow M' \xrightarrow{\iota} M \xrightarrow{\pi} M'' \longrightarrow 0$$

é dita *"cindida"* (*splits* ou *is split*) se existe um homomorfismo $j : M'' \to M$ tal que $\pi j = \mathrm{id}_{M''}$. Equivalentemente, tal sequência cinde se, e somente se, existe um homomorfismo $q : M \to M'$ tal que $q\iota = \mathrm{id}_{M'}$.
De fato, defina $q(m) = \iota^{-1}(m - j\pi(m))$ para cada $m \in M$, expressão que faz sentido pois $\pi(m - j\pi(m)) = \pi(m) - \pi(m) = 0$ donde $m - j\pi(m) \in ker(\pi) = im(\iota)$. Reciprocamente, defina $j(m'') = m - \iota q(m)$ onde $m \in \pi^{-1}(m'')$. O homomorfismo j é bem definido pois se $\pi(m) = m'' = \pi(n)$, então, $\pi(m - n) = 0 \Rightarrow m - n \in \ker(\pi) = im\iota$ e existe um único $m' \in M'$ com $\iota(m') = m - n$. Logo, $m' = q(m - n) = q(m) - q(n)$ e $m - n = \iota q(m) - \iota q(n)$, donde $m - \iota q(m) = n - \iota q(n)$. Falta agora verificar que j é um homomorfismo: de fato, sejam $a, b \in M''$ então existem $c \in \pi^{-1}(a), d \in \pi^{-1}(b), e \in \pi^{-1}(a + b)$ podemos escolher $e = c + d$ donde $j(a + b) = c + d - \iota q(c + d) = c - \iota q(c) + d - \iota q(d) = j(a) + j(b)$. Finalmente, $j(ra) = rc - \iota q(rc) = rc - r\iota q(c) = r(c - \iota q(c)) = rj(a)$, onde r pertence ao anel.

Observe também que se dita sequência cinde, então, $M \cong M' \oplus M''$ via os isomorfismos

$$\begin{aligned} \alpha : M &\longrightarrow M' \oplus M'' \\ m &\longmapsto (q(m), \pi(m)) \end{aligned}$$

e

$$\begin{array}{rccc} \beta : & M' \oplus M'' & \longrightarrow & M \\ & (a,b) & \longmapsto & \iota(a) + j(b) \end{array}$$

Com efeito, $\beta\alpha(m) = \beta(q(m), \pi(m)) = \iota q(m) + j\pi(m) = m$, pois $q(m) = \iota^{-1}(m - j\pi(m))$. e $\alpha\beta(a,b) = \alpha(\iota(a) + j(b)) = (q(\iota(a) + j(b)), \pi(\iota(a) + j(b))) = (q(\iota(a)) + qj(b), \pi\iota(a) + \pi j(b)) = (a + 0, 0 + b) = (a,b)$, pois $qj(b) = \iota^{-1}(j(b) - j\pi(j(b))) = \iota^{-1}(j(b) - j(b)) = \iota^{-1}(0) = 0$. Portanto α e β são inversas uma da outra. Obviamente eles são homomorfismos. A conclusão segue-se.

Existe mais uma caracterização de módulos injetivos via sequências cindidas.

Lema A.11. Um módulo E é injetivo se, e somente se, toda sequência exata curta $0 \to E \to M \to M'' \to 0$ cinde.

Demonstração. Se E é injetivo e $\iota : E \to M$ é um homomorfismo injetor, então, existe um homomorfismo $q : M \to E$ tal que $q\iota = \mathrm{id}_E$.

Reciprocamente, existem um módulo injetivo E' e um homomorfismo injetor $\iota : E \to E'$ pelo Teorema (A.10). Logo, a sequência exata

$$0 \to E \to E' \to E'/E \to 0$$

cinde e, $E' = E \oplus \frac{E'}{E} = E \times \frac{E'}{E}$, donde E é injetivo (como também E'/E). □

O anterior lema permite-nos concluir que um módulo injetivo E é somando direto de qualquer módulo que o contém.

Proposição A.12. Se $Ext^1_R(M,N) = 0$, então toda extensão de N para M cinde.

Demonstração. Vide ([22], prop. 7.24). □

A.2 Extensões Essenciais

Sejam $M \subseteq N$ módulos. N é uma *extensão essencial* de M (denotamos $M \subseteq_e N$) se todo submódulo não-nulo H de N satisfaz $H \cap M \neq 0$. Tal extensão essencial é dita *própria* se $M \subsetneq N$ (trivialmente, M sempre é extensão essencial de si mesmo, inclusive quando $M = 0$). Existem outras formas de verificar se uma extensão é essencial.

Lema A.13. Sejam $M \subseteq N$ módulos. As condições são equivalentes:

1. N é uma extensão essencial de M.

2. Todo elemento não-nulo $n \in N$ possui um múltiplo não-nulo $rn \in M$, onde $r \in R$.

3. Se $\varphi : N \to M'$ é um homomorfismo tal que $\varphi|_M := \varphi\iota$ é injetivo, então, φ é injetivo.

Demonstração. Suponha que N é uma extensão essencial de M e seja n um elemento não-nulo de N. Logo, Rn é um submódulo não-nulo de N e existe $r \in R$ tal que $0 \neq rn \in M$.

Se a condição 2 é satisfeita e $\varphi : N \to M'$ é um homomorfismo tal que $\varphi|_M$ é injetor, considere um elemento não-nulo $h \in \ker \varphi$. Então, $rh \in M - \{0\}$ para algum $r \in R$. Assim, $0 = r\varphi(h) = \varphi(rh) \neq 0$, o que é absurdo.

Agora, se a condição 3 é satisfeita e H é um submódulo de N, considere a projeção $\pi : N \to \frac{N}{H}$. Então, $\ker \pi|_M = H \cap M$. Se $H \cap M = 0$, então, $\pi|_M$ é injetor, donde π é injetor e $0 = \ker \pi = H$. Logo, N é uma extensão essencial de M. □

Exemplo A.14. Se $M_i \subseteq_e E$ para $1 \leq i \leq n$ então $\bigcap_{i=1}^{n} M_i \subseteq_e E$.

Solução A.15. Seja $e \in E \backslash \{0\}$. Desde que $M_1 \subseteq_e E$ existe $r_1 \in R$ tal que $er_1 \in M_1 \backslash \{0\}$. Desde que $M_2 \subseteq_e E$ existe $r_2 \in R$ tal que $er_1r_2 \in M_2 \backslash \{0\}$. Repetindo esse argumento um número finito de vezes obtemos $er_1r_2 \cdots r_n \in M_n \backslash \{0\}$ para $r_i \in R$. Claramente $er_1r_2 \cdots r_n \in \bigcap_{i=1}^{n} M_i$.
Para uma família infinita o resultado não vale. De fato, considere o módulo livre $E = \mathbb{Z}$ sobre $R = \mathbb{Z}$. E é essencial sobre os submódulos $M_i = i\mathbb{Z}$ $(i = 1, 2, ...)$, entretanto E não é essencial sobre $\bigcap_{i=1}^{n} M_i = 0$.

Se M é um submódulo de N, a existência de extensões essenciais maximais de M em N fica garantida graças ao Lema de Zorn. Os módulos injetivos ficam caracterizados pela não existência de extensões essenciais próprias.

Lema A.16. Um módulo é injetivo se, e somente se, não possui extensões essenciais próprias.

Demonstração. Se E é injetivo e $E \subseteq M$, então, $M = E \oplus M''$ (daí automaticamente $E \cap M = 0$) para algum submódulo M'' de M pelo Lema (A.11). Se $E \neq M$, então, $M'' \neq 0$ e M não é uma extensão essencial de E.

Reciprocamente, se E não possui extensões essenciais próprias, considere $E \subsetneq M$, onde M é injetivo graças ao teorema (A.10). Então, existe um submódulo não-nulo H de M tal que $H \cap E = 0$. Pelo Lema de Zorn, existe um submódulo maximal N de M tal que $H \subseteq N$ e $N \cap E = 0$. Agora, existe um homomorfismo injetor natural $E \to \frac{M}{N}$[2] que, de fato, define uma extensão essencial $E \subseteq \frac{M}{N}$ pelo lema (A.13). Deste modo, $E = \frac{M}{N}$. Portanto, $E + N = M$, donde $M = E \oplus N$ e E é injetivo. □

[2] pois seu núcleo é N$\cap E = 0$

Deste modo, se M é submódulo de um módulo injetivo E, então, todas as extensões essenciais possíveis de M devem estar contidas em E. Assim, não é mais necessário especificar "o contexto" de M estar contido em módulo algum graças ao Teorema (A.10).

Proposição A.17. Se N é uma extensão essencial maximal de M, então, N é injetivo.

Demonstração. Suponha que N possui uma extensão essencial Q. Então, Q é uma extensão essencial de M. Logo, $N = Q$, pois N é extensão essencial maximal de M. Deste modo, N não possui extensões essenciais próprias, logo, N é injetivo pelo Lema (A.16). □

Mais ainda, quaisquer duas extensões essenciais maximais de um módulo M devem ser isomorfas.

Teorema A.18. *Se N e N' são duas extensões essenciais maximais de M, então, $N \cong N'$.*

Demonstração. Sejam $\alpha : M \to N$ e $\beta : M \to N'$ homomorfismo injetor. Logo, α estende para um homomorfismo injetor $\varphi : N' \to N$ pelo Lema (A.13) e pela Proposição (A.17), isto é, $\alpha = \varphi\beta$. Logo, N' é um submódulo de N(pois ψ é injetora), donde $N' \cong N$ (pela maximalidade). □

Chamamos de *envoltória injetiva* (*injective hull*) de M qualquer extensão essencial maximal de M a qual é denotada por $E_R(M)$.

Recolhemos a seguir uma série de exemplos elementares de extensões essenciais e envoltórias injetivas:

Exemplo A.19. Todo anel comutativo é extensão essencial de cada um de seus ideais que contêm pelo menos um elemento regular.

Solução A.20. De fato, dizemos que um elemento $a \in R$ é regular se para todo $r \in R$, $ar = 0$ implica $a = 0$. Seja $\mathfrak{a}$ ideal de R e $a \in \mathfrak{a}$ regular. Seja $\mathfrak{b}$ ideal de R não nulo e seja $0 \neq b \in \mathfrak{b}$ como a é regular $ab \neq 0$, mas $ab \in \mathfrak{a} \cap \mathfrak{b}$ e a conclusão segue.

Exemplo A.21. Se R é um anel comutativo, denote por S o conjunto de todos os elementos regulares de R. Verifica-se que $S^{-1}R$ é uma extensão essencial de R.

Solução A.22. De fato, como S é o conjunto de todos os elementos regulares de R segue que $R \to S^{-1}R$ é injetor e daí podemos ver que R é submódulo de $S^{-1}R$. Dado $\frac{0}{1} \neq \frac{a}{s} \in S^{-1}R$ temos que $(a/s)\dot{s} = a \neq 0 \in R$ donde $S^{-1}R$ é essencial.

Exemplo A.23. Mais ainda, se R é um domínio de integridade, então, seu corpo de frações é um R-módulo injetivo.

Solução A.24. De fato, se $\mathfrak{b}$ é um ideal (não-nulo) de R e $\varphi : \mathfrak{b} \to \mathrm{Frac}(R)$ é um homomorfismo, fixe $i \in \mathfrak{b} - \{0\}$ e defina $\psi : R \to \mathrm{Frac}(R)$ como $\psi(r) = \frac{\varphi(ri)}{i}$. Observa-se que ψ é um homomorfismo que estende φ. Concluímos assim que $E_R(R) = \mathrm{Frac}(R)$ quando R é um domínio de integridade.

Exemplo A.25. Se $N \subseteq M$, então, $E_R(N) \subseteq E_R(M)$.

Solução A.26. De fato, a composição injetora $N \to M \to E_R(M)$ e a injeção $N \to E_R(N)$ induzem um homomorfismo injetor $E_R(N) \to E_R(M)$. Por outro lado, obtemos também um homomorfismo não-nulo $E_R(M) \to E_R(N)$. Além disso, se M é uma extensão essencial de N, então, $E_R(M) = E_R(N)$.

Exemplo A.27. De maneira similar ao exemplo anterior, pode-se concluir que se $M \subseteq M_1 \oplus \cdots \oplus M_s$, então, $E_R(M) \subseteq E_R(M_1) \oplus \cdots \oplus E_R(M_s)$.

Solução A.28. De fato, pode-se mostrar que se $M \subseteq_e M'$ e $N \subseteq_e N'$ então $M \oplus N \subseteq_e M' \oplus N'$. Também é válida a igualdade: $E(M \oplus N) = E(M) \oplus E(N)$.

A.3 Resoluções Injetivas

Seja M um R-módulo. Então, é possível construir uma seqüência exata de R-módulos $0 \to M \to E^0 \to E^1 \to \cdots$ onde cada E^i é injetivo graças ao Teorema (A.10). Toda esta situação motiva algumas definições.

Definição A.29. Seja $\mathcal{X}$ uma classe de módulos. Dizemos que existem *$\mathcal{X}$-módulos suficientes* quando, para cada módulo M, existem um módulo X da classe $\mathcal{X}$ (doravante, X é um *$\mathcal{X}$-módulo*) e um homomorfismo injetor $M \to X$. Uma *$\mathcal{X}$-resolução de M* é um cocomplexo $\mathbf{X}(M)$ de $\mathcal{X}$-módulos

$$0 \longrightarrow X^0 \xrightarrow{d^0} X^1 \xrightarrow{d^1} X^2 \longrightarrow \cdots$$

tal que $H^0(\mathbf{X}(M)) = \ker d^0 = M$ e $H^i(\mathbf{X}(M)) = 0$ para cada $i \geq 1$(por exemplo, $H^1(\mathbf{X}(M)) = kerd^1/imd^0 = 0$, etc...).

Para cada $i \geq 0$, o quociente $V^i = \frac{X^i}{\ker d^i}$ é chamado de *i-ésima cosizígia de* $\mathbf{X}(M)$. Assim, o homomorfismo $d^i : X^i \to X^{i+1}$ fica fatorado como $d_i = \bar{d}^i \pi^i$ onde $\bar{d}^i : V^i \to X^{i+1}$ é um homomorfismo injetor e $\pi^i : X^i \to V^i$ é um epimorfismo para cada $i \geq 0$.

Neste texto, consideraremos de maneira exclusiva a classe $\mathcal{X}$ dos módulos injetivos. Se $f : M \to N$ é um homomorfismo de módulos e $\mathbf{X}(M)$ e $\mathbf{X}(N)$ são, respectivamente, resoluções injetivas

$$0 \longrightarrow D^0 \xrightarrow{d^0} D^1 \xrightarrow{d^1} D^2 \longrightarrow \cdots$$

e

$$0 \longrightarrow E^0 \xrightarrow{e^0} E^1 \xrightarrow{e^1} E^2 \longrightarrow \cdots$$

de M e N, então, pode-se construir uma aplicação de cadeias

$$\begin{tikzcd}
0 \arrow[r] & N \arrow[r, "\beta"] & E^0 \arrow[r, "e^0"] & E^1 \arrow[r, "e^1"] & E^2 \arrow[r] & \cdots \\
0 \arrow[r] & M \arrow[u, "f"] \arrow[r, "\alpha"] & D^0 \arrow[u, "f^0"] \arrow[r, "d^0"] & D^1 \arrow[u, "f^1"] \arrow[r, "d^1"] & D^2 \arrow[u, "f^2"] \arrow[r] & \cdots .
\end{tikzcd}$$

que será chamada de *resolução de f*. Aqui, α e β são os homomorfismo injetor que fazem que as linhas do diagrama sejam exatas. De fato, f^0 é um levantamento de βf via o homomorfismo injetor α, pois E^0 é injetivo. Supondo que foram encontradas todos os homomorfismos até $f^n : D^n \to E^n$, temos um homomorfismo injetor $\bar{d}_n : V_M^n \to D^{n+1}$ induzido por d^n, mais exatamente, $\bar{d}^n\pi^n = d^n$ onde $\pi^n : D^n \to V_M^n$ é a projeção canônica. Define-se, também, um homomorfismo (é, de fato, bem definido!) $\lambda^n : V_M^n \to E^{n+1}$ como $\lambda^n(a + \ker d^n) = e^n f^n(a)$. Portanto, existe $f^{n+1} : D^{n+1} \to E^{n+1}$ tal que $f^{n+1}\bar{d}^n = \lambda^n$. Assim, $f^{n+1}d^n = f^{n+1}\bar{d}^n\pi^n = \lambda^n\pi^n = e^n f^n$.

Observe, também, que se fora construída outra resolução $(g^i)_{i\geq 0}$ de f, então, ambas aplicações de cadeias são *homotópicas*, isto é, existe uma aplicação $t = (t^n : D^n \to E^{n-1})$ de grau 1 (ou cograu -1) tal que $f^n - g^n = e^{n-1}t^n + t^{n+1}d^n$.

$$\begin{tikzcd}
0 \arrow[r, "e^{-1}"] & E^0 \arrow[r, "e^0"] & E^1 \arrow[r, "e^1"] & E^2 \arrow[r] & \cdots \\
0 \arrow[r, "d^{-1}"] & D^0 \arrow[ul, "t^0"] \arrow[u, "f^0-g^0"'] \arrow[r, "d^0"] & D^1 \arrow[ul, "t^1"] \arrow[u, "f^1-g^1"'] \arrow[r, "d^1"] & D^2 \arrow[ul, "t^2"] \arrow[u, "f^2-g^2"'] \arrow[r] & \cdots
\end{tikzcd}$$

De fato, observe que $M \cong \operatorname{im}\alpha \subseteq \ker(f^0 - g^0)$ e defina $\lambda^0 : V_M^0 \to E^0$ como $\lambda^0(a + \ker d^0) = (f^0 - g^0)(a)$, isto é, $\lambda^0\pi^0 = f^0 - g^0$, onde $\pi^0 : D^0 \to V_M^0$ é a projeção natural. Mas $\bar{d}^0\pi^0(x) = d^0(x)$ para todo $x \in E^0$. Por ser E^0 injetivo, defina $t^1 : D^1 \to E^0$ estendendo λ^0, ou seja, $\lambda^0 = t^1\bar{d}^0$. Logo, $f^0 - g^0 = \lambda^0\pi^0 = e^{-1}t^0 + t^1d^0$.

Supondo que já foram encontrados todos os homomorfismos até $t^n : D^n \to E^{n-1}$, considere, análogo ao primeiro passo, o homomorfismo $\lambda^n : V_M^n \to E^n$ definido por $\lambda^n\pi^n = f^n - g^n - e^{n-1}t^n$. Define-se um levantamento $t^{n+1} : D^{n+1} \to E^n$ de λ^n via $\bar{d}^n$ (isto é, $t^{n+1}\bar{d}_n = \lambda^n$) e verifica-se que $f^n - g^n = e^{n-1}t^n + t^{n+1}d^n$.

Fica, então, demonstrado o seguinte resultado.

Proposição A.30. Quaisquer duas resoluções injetivas de um mesmo módulo são *homotopicamente equivalentes*, isto é, se $\mathbf{E}(M)$ e $\mathbf{D}(M)$ são resoluções injetivas de M, então, existem aplicações de cadeias $f : \mathbf{E}(M) \to \mathbf{D}(M)$ e $g : \mathbf{D}(M) \to \mathbf{E}(M)$ tais que fg é homotópica a $\mathrm{id}_{\mathbf{D}(M)}$ e gf é homotópica a $\mathrm{id}_{\mathbf{E}(M)}$.

Uma resolução injetiva $\mathbf{E}(M) = (E^i(M), d^i)_{i\geq 0}$ de M é *minimal* se o termo de cograu n é extensão essencial da $(n-1)$-ésima cosizígia para cada $n \geq 0$ (convencionamos $V^{-1} = M$).

Existem muitas razões para as resoluções injetivas minimais terem este nome. Uma delas é a seguinte.

Proposição A.31. Sejam $\mathbf{D}(M)$ e $\mathbf{E}(M)$ duas resoluções injetivas de M, sendo a segunda delas minimal. Então, para cada $n \geq 0$, cada termo de $\mathbf{E}(M)$ de cograu n é somando direto do termo de $\mathbf{D}(M)$ do mesmo cograu. Em particular, para cada $n \geq 0$, os termos de cograu n de quaisquer duas resoluções injetivas minimais do mesmo módulo são isomorfos.

Demonstração. Construiremos uma aplicação de cadeias $(\mathrm{id}^i_M)_{i\geq 0} : (\mathbf{E}(M), e) \to (\mathbf{D}(M), d)$ induzida pelo isomorfismo identidade $\mathrm{id}_M : M \to M$ e injetora. De fato, id^0_M satisfaz $\mathrm{id}^0_M\alpha = \beta\mathrm{id}_M$, sendo o lado direito um homomorfismo injetor. Logo, id^0_M é injetora pelo Lema (A.13) e E^0 é somando direto de D^0.

Suponha, agora, que id^i_M é injetora para cada $i \in \{0, \ldots, n\}$. Observe que $x \in \ker e^i$ se, e somente se, $\mathrm{id}^i_M(x) \in \ker d^i$. Defina $\lambda^n : V^n_{\mathbf{E}} \to D^{n+1}$ como $\lambda^n(a + \ker e^n) = d^n\mathrm{id}^n_M(a)$. Verifica-se que λ^n é injetora: de fato, $\mathrm{id}^n_M(a) \in \ker d^n$ se, e somente se, $a \in \ker e^n$. Deste modo, λ^n estende-se a um homomorfismo injetor $\mathrm{id}^{n+1}_M : E^{n+1} \to D^{n+1}$ pois $\bar{e}^n : V^n_{\mathbf{E}} \to E^{n+1}$ é uma extensão essencial. Portanto, E^n é somando direto de D^n para cada $n \geq 0$ pelo Lema (A.11).

Observe que ficam definidas sequências exatas curtas

$$0 \longrightarrow E^i \underset{q^i}{\overset{\mathrm{id}^i_M}{\rightleftarrows}} D^i \underset{\tau^i}{\overset{p^i}{\rightleftarrows}} \frac{D^i}{\mathrm{im}\,\mathrm{id}^i_M} \longrightarrow 0$$

e diagramas comutativos

$$\begin{tikzcd}
\frac{D^{i-1}}{\mathrm{im}\,\mathrm{id}^{i-1}_M} \arrow[r, "j^{i-1}"] & \frac{D^i}{\mathrm{im}\,\mathrm{id}^i_M} \\
D^{i-1} \arrow[u, "p^{i-1}"] \arrow[r, "d^{i-1}"] & D^i \arrow[u, "p^i"']
\end{tikzcd}$$

Defina $\lambda^n : V^n \to D^{n+1}$ como $\lambda^n(a + \ker e^n) = d^n\mathrm{id}^n_M(a)$. Verifica-se que λ^n é injetora: se $\mathrm{id}^n_M(a) \in \ker d^n$, então, existe $b \in D^{n-1}$ tal que $\mathrm{id}^n_M(a) = d^{n-1}(b)$. Assim, $a =$

$q^n d^{n-1}(b)$. Por outro lado, $e^{n-1}q^{n-1}(b) = q^n d^{n-1}\mathrm{id}_M^{n-1}q^{n-1}(b)$. Logo, $a - e^{n-1}q^{n-1}(b) = q^n d^{n-1}(b - \mathrm{id}_M^{n-1}q^{n-1}(b))$. Como $q^{n-1}(b - \mathrm{id}_M^{n-1}q^{n-1}(b)) = 0$, segue que $b - \mathrm{id}_M^{n-1}q^{n-1}(b) = \tau^{n-1}(c)$ para algum $c \in \frac{D^{n-1}}{\mathrm{im}\,\mathrm{id}_M^{n-1}}$. Logo, $d^{n-1}(b - \mathrm{id}_M^{n-1}q^{n-1}(b)) = d^{n-1}\tau^{n-1}(c)$, sendo o termo da direita um elemento de $\frac{D^n}{\mathrm{im}\,\mathrm{id}_M^n}$, donde $q^n d^{n-1}(b - \mathrm{id}_M^{n-1}q^{n-1}(b)) = 0$. Portanto, $a \in \mathrm{im}\, e^{n-1} = \ker e^n$ e λ^n é injetora. Deste modo, sua extensão $\mathrm{id}_M^{n+1} : E^{n+1} \to D^{n+1}$ também é injetora, donde E^{n+1} é somando direto de D^{n+1}. $\square$

A.4 Módulos Injetivos sobre um Anel Comutativo Noetheriano

Antes de continuarmos com o estudo de módulos injetivos, lembremos algumas propriedades dos módulos de homomorfismos. Para qualquer conjunto de índices I, existe um homomorfismo injetor de grupos $\varphi : \bigoplus_{i \in I} \mathrm{Hom}_R(M, N_i) \to \mathrm{Hom}_R\left(M, \bigoplus_{i \in I} N_i\right)$ dado por $\varphi(f_{i_1} + \cdots + f_{i_s}) = f_{i_1} + \cdots + f_{i_s} : M \to \bigoplus_{i \in I} N_i$ quando $f_{i_j} \in \mathrm{Hom}_R(M, N_{i_j})$. Observa-se que φ é um isomorfismo quando M é finitamente gerado: de fato, a imagem de $f \in \mathrm{Hom}_R\left(M, \bigoplus_{i \in I} N_i\right)$ está contida numa quantidade finita de N_i neste caso, logo, $f \in \mathrm{Hom}_R\left(M, \bigoplus_{i \in F} N_i\right)$ onde F é um subconjunto finito de I. Mas neste último caso, o homomorfismo injetor $\varphi|_F : \bigoplus_{i \in F} \mathrm{Hom}_R(M, N_i) \to \mathrm{Hom}_R\left(M, \bigoplus_{i \in F} N_i\right)$ é, de fato, um isomorfismo (independente de M ser finitamente gerado). Assim, existe $g \in \bigoplus_{i \in F} \mathrm{Hom}_R(M, N_i) \subseteq \bigoplus_{i \in I} \mathrm{Hom}_R(M, N_i)$ tal que $\varphi(g) = \varphi|_F(g) = f$.

Os anéis noetherianos ficam caracterizados pelo comportamento dos módulos injetivos.

Proposição A.32. Um anel é noetheriano se, e somente se, toda soma direta de módulos injetivos é injetiva.

Demonstração. Seja $E = \bigoplus_{i \in I} E_i$ uma soma direta de módulos injetivos e considere um ideal $\mathfrak{a}$ de um anel noetheriano R. A inclusão $\mathfrak{a} \to R$ induz um homomorfismo $\mathrm{Hom}_R(R, E) \to \mathrm{Hom}_R(\mathfrak{a}, E)$. Como cada E_i é injetivo, temos também que cada homomorfismo $\mathrm{Hom}_R(R, E_i) \to \mathrm{Hom}_R(\mathfrak{a}, E_i)$ é sobrejetor. Logo, $\bigoplus_{i \in I} \mathrm{Hom}_R(R, E_i) \to \bigoplus_{i \in I} \mathrm{Hom}_R(\mathfrak{a}, E_i)$ é sobrejetor. Como $\mathfrak{a}$ é finitamente gerado, temos o isomorfismo natural $\bigoplus_{i \in I} \mathrm{Hom}_R(\mathfrak{a}, E_i) \cong \mathrm{Hom}_R\left(\mathfrak{a}, \bigoplus_{i \in I} E_i\right)$. Portanto, o homomorfismo $\mathrm{Hom}_R(R, E) \to$

$\mathrm{Hom}_R(\mathfrak{a}, E)$ é sobrejetor, donde E é um módulo injetivo pelo Critério de Baer.

Reciprocamente, suponha que R não é noetheriano. Exibiremos uma soma direta de módulos injetivos que não é injetiva. Existe uma cadeia ascendente $\mathfrak{a}_1 \subsetneq \mathfrak{a}_2 \subsetneq \cdots$ de ideais de R. Seja $\mathfrak{a} = \bigcup_{i \geq 1} \mathfrak{a}_i$. Existem projeções naturais $\pi_i : \mathfrak{a} \to E_R\left(\dfrac{R}{\mathfrak{a}_i}\right)$ para cada $i \geq 1$, donde obtemos um homomorfismo $\pi : \mathfrak{a} \to \prod_{i \geq 1} E_R\left(\dfrac{R}{\mathfrak{a}_i}\right)$. Se $a \in \mathfrak{a}$, então, $a \in \mathfrak{a}_j$ para algum inteiro $j \geq 1$. Assim, $\pi_i(a) = 0$ quando $i \geq j$. Portanto, o contradomínio de π é o submódulo $\bigoplus_{i \geq 1} E_R\left(\dfrac{R}{\mathfrak{a}_i}\right)$ de $\prod_{i \geq 1} E_R\left(\dfrac{R}{\mathfrak{a}_i}\right)$. Se existisse $\psi : R \to \bigoplus_{i \geq 1} E_R\left(\dfrac{R}{\mathfrak{a}_i}\right)$ estendendo π, então, $\psi(1) = e_1 + \cdots + e_s$ para alguns $e_i \in E_R\left(\frac{R}{\mathfrak{a}_i}\right)$ e $s \geq 1$. Agora, $\pi(a) = a\psi(1)$ para cada $a \in \mathfrak{a}$. Mas se $a \in \mathfrak{a}_{s+2} - \mathfrak{a}_{s+1}$, então, $\pi_{s+1}(a) \neq 0$ e chegamos a uma contradição. $\square$

Lembremos que um módulo é dito *simples* quando não tem submódulos não-triviais. Um módulo será dito *indecomponível* quando não for uma soma direta de submódulos não-triviais. Um módulo será dito *uniforme* quando satisfizer alguma das condições equivalentes:

1. Não contém somas diretas não-triviais.

2. Todo submódulo não-nulo é indecomponível.

3. É extensão essencial de cada um de seus submódulos não-nulos.

Todo módulo simples é uniforme e todo módulo uniforme é indecomponível. Agora provaremos que todo módulo injetivo indecomponível é uniforme.

Teorema A.33. *Seja E um módulo injetivo. As condições são equivalentes:*

1. *E é indecomponível.*

2. *$E \neq 0$ e $E = E_R(M)$ para qualquer submódulo não-nulo M de E.*

3. *$E = E_R(U)$ para algum submódulo uniforme U de E.*

4. *$E = E_R\left(\frac{R}{\mathfrak{a}}\right)$ onde $\mathfrak{a}$ é* irredutível*, isto é, se $\mathfrak{b} \cap \mathfrak{b}' = \mathfrak{a}$, então, $\mathfrak{b} = \mathfrak{a}$ ou $\mathfrak{b}' = \mathfrak{a}$.*

5. *O anel* $\mathrm{End}_R(E)$ *dos endomorfismos do R-módulo E é local.*

Demonstração. Se E é um módulo injetivo e $0 \neq M \subseteq E$, então, toda extensão essencial de M está contida em E. Em particular, $E_R(M) \subseteq E$, donde $E_R(M) = E$, pois E é indecomponível. Deste modo, a condição 1 implica na condição 2.

Se $E = E_R(M)$ para qualquer submódulo não-nulo M de E, então, E é uniforme. Assim, $U = E$ satisfaz a condição 3 quando E satisfaz a condição 2.

Suponha que $E = E_R(U)$ para algum submódulo uniforme U de E e considere um submódulo cíclico V de U, isto é, $V = \frac{R}{\mathfrak{a}}$ para algum ideal $\mathfrak{a}$ de R. Como U é uniforme, temos que U é uma extensão essencial de V. Portanto, $E_R(U)$ é uma extensão essencial de V. Finalmente, se $\mathfrak{b} \cap \mathfrak{b}' = \mathfrak{a}$, considere os submódulos cíclicos $W = \frac{\mathfrak{b}}{\mathfrak{a}}$ e $W' = \frac{\mathfrak{b}'}{\mathfrak{a}}$ de $V \subseteq U$. Se $W \neq 0$, então, $W' = 0$, pois $W \cap W' = 0$ e U é uniforme. Fica demonstrado deste modo que a condição 3 implica na condição 4.

Seja $E = E_R\left(\frac{R}{\mathfrak{a}}\right)$ onde $\mathfrak{a}$ é irredutível. Observe que o módulo $U = \frac{R}{\mathfrak{a}}$ é uniforme. Considere um elemento não-invertível $\alpha \in \mathrm{End}_R(E)$. Então, $\ker \alpha \neq 0$, pois caso contrário, $E \cong \operatorname{im} \alpha \subsetneq E$, o que é absurdo, pois E é injetivo. Assim, $U \cap \ker \alpha \neq 0$. Considerando outro elemento não-invertível $\beta \in \mathrm{End}_R(E)$, obtemos igualmente que $U \cap \ker \beta \neq 0$. Logo, $\ker \alpha + \beta \supseteq \ker \alpha \cap \ker \beta \supseteq (U \cap \ker \alpha) \cap (U \cap \ker \beta) \neq 0$. Portanto, o conjunto dos elementos não-invertíveis de $\mathrm{End}_R(E)$ é um ideal, concluindo assim que a condição 4 implica na condição 5.

Finalmente, se $E = E_1 \oplus E_2$, então, $\mathrm{id}_{E_1} \oplus 0$ e $0 \oplus \mathrm{id}_{E_2}$ são elementos idempotentes de $\mathrm{End}_R(E)$. Assim, a condição 5 implica na condição 1 e o enunciado fica estabelecido. $\square$

Um módulo N é dito *primo* se $\mathrm{Ann}(N') = \mathrm{Ann}(N)$ para todo submódulo não-nulo N' de N. Pode-se demonstrar que o ideal $\mathrm{Ann}(N)$ é primo sob esta condição: de fato, se $ab \in \mathrm{Ann}(N)$ e $a \notin \mathrm{Ann}(N)$, considere $n \in N$ tal que $na \neq 0$. Assim, o submódulo $N' = naR$ de N deve satisfazer $\mathrm{Ann}(N') = \mathrm{Ann}(N)$. Como $b \in \mathrm{Ann}(N')$, a afirmação segue.

Um ideal primo $\mathfrak{p}$ é dito *associado* ao módulo (à direita) M quando $\mathfrak{p} = \mathrm{Ann}(N)$ para algum submódulo primo N de M e o conjunto de ideais primos associados de M é denotado por $\mathrm{Ass}(M)$. Observe que a presente definição de ideal primo associado coincide com a usual no caso comutativo.

Uma das vantagens de considerarmos estas novas definições é a seguinte.

Lema A.34. Se E é uma extensão essencial de M, então, $\mathrm{Ass}(E) = \mathrm{Ass}(M)$. Em particular, $\mathrm{Ass}(E_R(M)) = \mathrm{Ass}(M)$.

Demonstração. Seja H um submódulo primo de E. Então, $H \cap M \neq 0$, donde $\mathfrak{p} = \mathrm{Ann}(H) = \mathrm{Ann}(H \cap M)$. Agora, $H \cap M$ é um submódulo primo de M. Assim, $\mathfrak{p} \in \mathrm{Ass}(M)$. A recíproca é tranquila. $\square$

Se $\mathfrak{p}$ é um ideal primo de um anel comutativo R, então, o R-módulo $\frac{R}{\mathfrak{p}}$ é uniforme, donde $E_R\left(\frac{R}{\mathfrak{p}}\right)$ é indecomponível pelo Teorema (A.33). Observe que $\mathrm{Ass}_R\left(\frac{R}{\mathfrak{p}}\right) = \{\mathfrak{p}\}$. De fato, todos os módulos uniformes satisfazem esta condição.

Lema A.35. Todo módulo uniforme possui, no máximo, um ideal primo associado.

Demonstração. Suponha que $\mathrm{Ann}(H_1)$ e $\mathrm{Ann}(H_2)$ são ideais primos associados de um módulo uniforme U, onde H_1 e H_2 são submódulos primos de U. Então, $H_1 \cap H_2 \neq 0$ e $\mathrm{Ann}(H_1) = \mathrm{Ann}(H_1 \cap H_2) = \mathrm{Ann}(H_2)$. □

O objetivo agora é decompor todo módulo injetivo em indecomponíveis. Isto pode ser feito no contexto comutativo noetheriano e o anel base terá estas características daqui para frente.

Teorema A.36. *Seja E um módulo injetivo não-nulo sobre um anel comutativo noetheriano R. Então, $E \cong \bigoplus_i E_R\left(\frac{R}{\mathfrak{p}_i}\right)$ onde cada $\mathfrak{p}_i$ é um ideal primo de R.*

Demonstração. Observe que se E é um módulo injetivo indecomponível, então, $E = E_R\left(\frac{R}{\mathfrak{a}}\right)$ onde $\mathfrak{a}$ é um ideal irredutível. Demonstraremos que se R é comutativo noetheriano, então, $\mathfrak{a}$ pode ser escolhido como um ideal primo. Seja $\mathfrak{p} \in \mathrm{Ass}(E)$. Então, existe um homomorfismo injetor $\frac{R}{\mathfrak{p}} \to E$. Como E é indecomponível, temos que E é uma extensão essencial de $\frac{R}{\mathfrak{p}}$ pelo Teorema (A.33), donde $E = E_R\left(\frac{R}{\mathfrak{p}}\right)$.

Em geral, seja $e \in E$ e considere $\mathfrak{a} = \mathrm{Ann}(e)$. Então, $\mathfrak{a} = \mathfrak{a}_1 \cap \cdots \cap \mathfrak{a}_s$ onde cada $\mathfrak{a}_i$ é um ideal irredutível veja ([19], página 40). Logo, $Re = \frac{R}{\mathfrak{a}} \subseteq \frac{R}{\mathfrak{a}_1} \oplus \cdots \oplus \frac{R}{\mathfrak{a}_s}$, donde $Re \subseteq E_R\left(\frac{R}{\mathfrak{a}_1}\right) \oplus \cdots \oplus E_R\left(\frac{R}{\mathfrak{a}_s}\right)$. Como cada $\mathfrak{a}_i$ é irredutível, existem ideais primos $\mathfrak{p}_i$ tais que $E_R\left(\frac{R}{\mathfrak{a}_i}\right) = E_R\left(\frac{R}{\mathfrak{p}_i}\right)$ para cada i pelo argumento anterior e concluímos o enunciado. □

Deste modo, o conjunto $\left\{E_R\left(\frac{R}{\mathfrak{p}}\right)\right\}_{\mathfrak{p}\in R}$ fornece uma lista completa dos módulos injetivos indecomponíveis sobre o anel comutativo noetheriano R. Assim, dados dois ideais primos, $\mathfrak{p}$ e $\mathfrak{q}$, de R, teremos que $E_R\left(\frac{R}{\mathfrak{p}}\right) = E_R\left(\frac{R}{\mathfrak{q}}\right)$ se, e somente se, $\mathfrak{p} = \mathfrak{q}$: de fato, se $x \in \mathfrak{p} - \mathfrak{q}$, então, a multiplicação por x é um automorfismo em $E_R\left(\frac{R}{\mathfrak{q}}\right)$ e não é um automorfismo em $E_R\left(\frac{R}{\mathfrak{p}}\right)$.

Extensões essenciais e injetividade são preservadas via localização.

Lema A.37. Considere um conjunto multiplicativo S de um anel comutativo noetheriano R. Se E é um R-módulo injetivo, então, $S^{-1}E$ é injetivo como $S^{-1}R$-módulo e como R-módulo.

Demonstração. Se $\mathfrak{a}$ é um ideal de $S^{-1}R$, então, $\mathfrak{a} = S^{-1}\mathfrak{b}$ para algum ideal $\mathfrak{b}$ de R. Temos a seqüência exata $\mathrm{Hom}_R(R, E) \to \mathrm{Hom}_R(\mathfrak{b}, E) \to 0$. Como $S^{-1}(-)$ é um funtor exato da categoria dos R-módulos à categoria dos $S^{-1}R$-módulos, obtemos a seqüência exata $S^{-1}\mathrm{Hom}_R(R, E) \to S^{-1}\mathrm{Hom}_R(\mathfrak{b}, E) \to 0$. Agora, como R é noetheriano, todos seus ideais são de apresentação finita e a seqüência anterior transforma-se em $\mathrm{Hom}_{S^{-1}R}(S^{-1}R, S^{-1}E) \to \mathrm{Hom}_{S^{-1}R}(S^{-1}\mathfrak{b}, S^{-1}E) \to 0$ via isomorfismos naturais veja ([15], Prop. 12.21). Deste modo, $S^{-1}E$ é um $S^{-1}R$-módulo injetivo pelo Critério de Baer.

Finalmente, considere dois R-módulos $M \subseteq N$ e um homomorfismo de R-módulos $\lambda : M \to S^{-1}E$. O homomorfismo canônico $\psi : S^{-1}E \to S^{-1}E$ é um isomorfismo de $S^{-1}R$-módulos. Deste modo, $\psi^{-1}S^{-1}\lambda : S^{-1}M \to S^{-1}E$ é um homomorfismo de $S^{-1}R$-módulos. Agora, existe um homomorfismo de $S^{-1}R$-módulos $\mu' : S^{-1}N \to S^{-1}E$ que estende $\psi^{-1}S^{-1}\lambda$. Deste modo, o homomorfismo canônico $\theta : N \to S^{-1}N$ induz um homomorfismo de R-módulos $\mu'\theta : N \to S^{-1}E$ que estende λ concluindo que $S^{-1}E$ é também R-injetivo.

$$\begin{tikzcd}
 & & S^{-1}E \arrow[dd, "J_{S^{-1}E}"] & \\
0 \arrow[r] & M \arrow[ur, "\lambda"] \arrow[rr, "\alpha"'] \arrow[dd, "J_M"] & & N \arrow[ul, dotted, "\mu"'] \arrow[dd, "J_N"] \\
 & & S^{-1}E & \\
0 \arrow[r] & S^{-1}M \arrow[ur, "S^{-1}\lambda"] \arrow[rr, "S^{-1}\alpha"'] & & S^{-1}N \arrow[ul, "\beta"']
\end{tikzcd}$$

□

Lema A.38. Seja S um conjunto multiplicativo de um anel comutativo noetheriano R e considere um homomorfismo de R-módulos $f : L \to M$ tal que $\operatorname{im} f \subseteq M$ é uma extensão essencial. Então, $S^{-1}M$ é uma extensão essencial de $\operatorname{im} S^{-1}f$.

Demonstração. Seja $\frac{x}{s}$ um elemento não-nulo de $S^{-1}M$. Logo, existe $\mathfrak{p} \in \operatorname{Ass}(Rx)$ tal que $\mathfrak{p} \cap S = \emptyset$. Assim, $\mathfrak{p} = \operatorname{Ann}(rx)$ para algum $r \in R$, isto é, podemos escolher $r \in R$ de maneira que Rrx seja um R-módulo primo. Como M é uma extensão essencial de $\operatorname{im} f$, existe $r' \in R$ tal que $0 \neq r'rx = f(y)$ para algum $y \in L$. Como Rrx é um R-submódulo primo de Rx, temos que $\operatorname{Ann}(r'rx) = \mathfrak{p}$, donde $0 \neq \frac{r'r}{1}\frac{x}{s} = \frac{f(y)}{s} = S^{-1}f\left(\frac{y}{s}\right)$. Conclui-se que $S^{-1}M$ é uma extensão essencial de $\operatorname{im} S^{-1}f$. □

Lema A.39. Considere um conjunto multiplicativo S de um anel comutativo noetheriano R. Então, os $S^{-1}R$-módulos injetivos indecomponíveis são os módulos $E_R\left(\frac{R}{\mathfrak{p}}\right)$, com $\mathfrak{p}$ primo, tais que $\mathfrak{p} \cap S = \emptyset$.

Demonstração. Pelo Teorema (A.36), os $S^{-1}R$-módulos injetivos indecomponíveis são os módulos $E_{S^{-1}R}\left(\frac{S^{-1}R}{S^{-1}\mathfrak{p}}\right)$ onde $\mathfrak{p}$ é um ideal primo de R tal que $\mathfrak{p} \cap S = \emptyset$. Agora, $E_{S^{-1}R}\left(\frac{S^{-1}R}{S^{-1}\mathfrak{p}}\right) = S^{-1}E_R\left(\frac{R}{\mathfrak{p}}\right)$, pois $S^{-1}E_R\left(\frac{R}{\mathfrak{p}}\right)$ é $S^{-1}R$-injetivo pelo Lema (A.37) e uma extensão essencial do $S^{-1}R$-módulo $S^{-1}\left(\frac{R}{\mathfrak{p}}\right) = \frac{S^{-1}R}{S^{-1}\mathfrak{p}}$ pelo Lema (A.38). Afirmamos que, quando $\mathfrak{p} \cap S = \emptyset$, o R-módulo $E_R\left(\frac{R}{\mathfrak{p}}\right)$ possui estrutura de $S^{-1}R$-módulo e, além disso, que é isomorfo ao $S^{-1}R$-módulo $E_{S^{-1}R}\left(\frac{S^{-1}R}{S^{-1}\mathfrak{p}}\right)$: de fato, a primeira afirmação segue porque a multiplicação por qualquer elemento $s \in S$ é um automorfismo em $E_R\left(\frac{R}{\mathfrak{p}}\right)$, ficando definido $\frac{e}{s} = \mu_s^{-1}(e)$ para cada $e \in E_R\left(\frac{R}{\mathfrak{p}}\right)$ e cada $s \in S$. Quanto à segunda afirmação, note que a estrutura de $S^{-1}R$-módulo em $E_R\left(\frac{R}{\mathfrak{p}}\right)$ é única veja ([15], Prop. 12.1). Deste modo, $E_R\left(\frac{R}{\mathfrak{p}}\right) = S^{-1}E_R\left(\frac{R}{\mathfrak{p}}\right) = E_{S^{-1}R}\left(\frac{S^{-1}R}{S^{-1}\mathfrak{p}}\right)$ e conclui-se o requerido. □

Proposição A.40. Seja $\mathfrak{p}$ um ideal primo de um anel comutativo noetheriano R e considere os módulos $E = E_R\left(\frac{R}{\mathfrak{p}}\right)$ e $\kappa(\mathfrak{p}) = \mathrm{Frac}\left(\frac{R}{\mathfrak{p}}\right) = \frac{R_\mathfrak{p}}{\mathfrak{p}R_\mathfrak{p}}$. Então, $\mathrm{Hom}_{R_\mathfrak{p}}(\kappa(\mathfrak{p}), E) = \kappa(\mathfrak{p})$ e $\mathrm{Hom}_{R_\mathfrak{p}}\left(\kappa(\mathfrak{p}), E_R\left(\frac{R}{\mathfrak{q}}\right)_\mathfrak{p}\right) = 0$ para todo ideal primo $\mathfrak{q} \neq \mathfrak{p}$.

Demonstração. Observe que $\mathrm{Hom}_{R_\mathfrak{p}}(\kappa(\mathfrak{p}), E) = (0 :_E \mathfrak{p}R_\mathfrak{p})$.[3] Afirmamos que $(0 :_E \mathfrak{p}R_\mathfrak{p}) = \kappa(\mathfrak{p})$: de fato, $\kappa(\mathfrak{p}) \subseteq (0 :_E \mathfrak{p}R_\mathfrak{p})$ e $(0 :_E \mathfrak{p}R_\mathfrak{p})$ é um $\kappa(\mathfrak{p})$-espaço vetorial, donde $\kappa(\mathfrak{p})$ é somando direto de $(0 :_E \mathfrak{p}R_\mathfrak{p})$. Por outro lado, E é extensão essencial de todos seus submódulos não-nulos pelo Lema (A.39). Assim, $(0 :_E \mathfrak{p}R_\mathfrak{p}) = \kappa(\mathfrak{p})$.

Para o segundo isomorfismo, consideremos primeiro um ideal primo $\mathfrak{q} \not\subseteq \mathfrak{p}$. Assim, $E_R\left(\frac{R}{\mathfrak{q}}\right)_\mathfrak{p}$ é uma extensão essencial de $\left(\frac{R}{\mathfrak{q}}\right)_\mathfrak{p} = 0$ pelo Lema (A.38). Se $\mathfrak{q} \subseteq \mathfrak{p}$, então, $\mathrm{Hom}_{R_\mathfrak{p}}\left(\kappa(\mathfrak{p}), E_R\left(\frac{R}{\mathfrak{q}}\right)_\mathfrak{p}\right) = (0 :_{E_R\left(\frac{R}{\mathfrak{q}}\right)_\mathfrak{p}} \mathfrak{p}R_\mathfrak{p}) = (0 :_{E_R\left(\frac{R}{\mathfrak{q}}\right)} \mathfrak{p}R_\mathfrak{p})$, a última igualdade vinda do Lema (A.39). Se $(0 :_{E_R\left(\frac{R}{\mathfrak{q}}\right)} \mathfrak{p}R_\mathfrak{p}) \neq 0$, então, $\mathfrak{q} = \mathfrak{p}$, pois $\mathrm{Ass}\left(E_R\left(\frac{R}{\mathfrak{q}}\right)\right) = \{\mathfrak{q}\}$ pelo Lema (A.34). □

A.5 Números de Bass

Análogo aos números de Betti das resoluções livres, encontramos invariantes no contexto comutativo noetheriano.

Teorema A.41. *Seja E um módulo injetivo. Então, $E = \bigoplus_{\mathfrak{p}\in R} E_R\left(\frac{R}{\mathfrak{p}}\right)^{\alpha_\mathfrak{p}}$, onde cada $\alpha_\mathfrak{p}$ depende somente de $\mathfrak{p}$.*

Demonstração. Lembremos que $E = \bigoplus_i E_R\left(\frac{R}{\mathfrak{p}_i}\right)$ onde $\mathfrak{p}_i$ é um ideal primo de R para cada i. Lembremos, também, que existe um isomorfismo natural $\bigoplus_i \mathrm{Hom}(N, M_i) \cong \mathrm{Hom}\left(N, \bigoplus_i M_i\right)$ quando N é finitamente gerado. Fixando o ideal primo $\mathfrak{p}$, a Proposição (A.40) implica em $\mathrm{Hom}_{R_\mathfrak{p}}(\kappa(\mathfrak{p}), E) = \kappa(\mathfrak{p})^{\alpha_\mathfrak{p}}$, onde $\alpha_\mathfrak{p}$ é o número (possivelmente infinito) de vezes que aparece $\mathfrak{p}$ numa decomposição de E em indecomponíveis. □

[3]pois $Hom(R/I, M) \cong (0 :_M I)$.

Podemos definir os números de Bass a seguir.

Definição A.42. Seja M um módulo e considere uma resolução injetiva minimal $\mathbf{E}(M)$ de M. Assim, $E^i(M) = \bigoplus_{\mathfrak{p}\in R} E_R\left(\frac{R}{\mathfrak{p}}\right)^{\mu^i(\mathfrak{p},M)}$ e o número $\mu^i(\mathfrak{p}, M)$ é o *i-ésimo número de Bass de M com respeito a $\mathfrak{p}$.*

Como já vimos na Proposição (A.31), estes números estão bem definidos. O próximo resultado dá uma fórmula para calculá-los.

Teorema A.43. *Para cada módulo M, cada primo $\mathfrak{p}$ e cada número inteiro $i \geq 0$, $\mu^i(\mathfrak{p}, M) = \dim_{\kappa(\mathfrak{p})} \operatorname{Ext}^i_{R_\mathfrak{p}}(\kappa(\mathfrak{p}), M_\mathfrak{p})$. Em particular, os números de Bass com respeito a $\mathfrak{p}$ de um módulo finitamente gerado são finitos.*

Demonstração. Vide ([4], teorema 11.1.8). □

Apêndice B

Alguns Fundamentos

Este breve apêndice não tem por objetivo desenvolver por completo os tópicos aqui elucidados, mas sim de expor de forma resumida e sintética outras ferramentas abordadas no capítulo 2 do presente trabalho. Para uma descrição mais completa recomendamos: [2], [23] e [6] para as 3 primeiras seções abaixo, respectivamente.

B.1 Anéis dos Operadores Diferenciais

Seja K um corpo comutativo de característica zero e $K[x] = K[x_1, ..., x_n]$ o anel de polinômios em n variáveis com coeficientes em K, onde n é um inteiro positivo. Em $K[x]$ temos a derivação k-linear usual $\partial/\partial x_1 \cdots \partial/\partial x_n$. A aplicação K-linear $\partial/\partial x_i$ que transforma um dado polinômio p em $\partial p/\partial x_1$ é chamado de derivada parcial com respeito a x_i.
Iremos usar a notação $\partial_i = \partial/\partial x_i$ assim $\partial_i(p) = \partial p/\partial x_i$.
Desde que $\partial_i(\partial_k(p)) = \partial^2 p/\partial x_i \partial x_k = \partial^2 p/\partial x_k \partial x_i = \partial_k(\partial_i(p))$ para todos os polinômios p, segue que $\partial_1 \cdots \partial_n$ são dois a dois operadores k-lineares comutativos em K$[x]$.
a multiplicação do anel em $K[x]$ também nos dá operadores K-lineares. Isto é, se $p \in K[x]$ define o operador multiplicação $\mu_p(q) = pq$ para todo polinômio $q \in K[x]$.

Definição B.1. O anel dos operadores K-lineares em $K[x]$ é o anel gerado pelas derivações $\partial_1 \cdots \partial_n$ e a multiplicação μ pelos polinômios em $K[x]$, este anel é chamado o anel dos operadores diferenciais K-lineares em $K[x]$. Denotemos este anel por $A_n(K)$, e chamamos de álgebra de Weyl em n variáveis e com coeficientes em K.

Desde que $x_1 \cdots x_n$ geram a K-álgebra $K[x]$ vemos que a K-álgebra $A_n(K)$ é gerada pelos operadores multiplicação $x_1 \cdots x_n$ e as derivações $\partial_1 \cdots \partial_n$. Isto sugere a notação $A_n(K) = \langle x_1, \cdots x_n, \partial_1, \cdots \partial_n \rangle$ onde $\langle\ \ \rangle$ indica que os geradores não comutam.

Observação B.2. *Notação.* $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ e $\partial^\beta = \partial_1^{\beta_1} \cdots \partial_n^{\beta_n}$. Também $|\beta| = \beta_1 + \cdots + \beta_n$ e $|\alpha| = \alpha_1 + \cdots + \alpha_n$.

Proposição B.3. Todo elemento em $A_n(K)$ pode ser escrito de modo único como uma soma finita $\sum K_{\alpha\beta}x^\alpha\partial^\beta$ onde $K_{\alpha\beta} \in K$. Isto é, a família $\{x^\alpha\partial^\beta\}$ é uma base quando $A_n(K)$ é considerado como espaço vetorial sobre K.

Proposição B.4. Se $v \geq 0$ considere $\mathcal{F}_v$ o espaço vetorial sobre K que é gerado pelo conjunto $\{x^\alpha\partial^\beta : \ |\alpha| + |\beta| \leq v\}$. Obviamente $\mathcal{F}_0 = K$[1] e $\mathcal{F}_1 = K + Kx_1 + \cdots + Kx_n + K\partial_1 + \cdots + K\partial_n$ e assim sucessivamente. Temos que $\mathcal{F}_0 \subset \mathcal{F}_1 \subset \mathcal{F}_2 \subset \cdots$ é uma cadeia crescente de K-espaços vetoriais de dimensão finita e $\bigcup \mathcal{F}_v = A_n(K)$ e $\mathcal{F}_v\mathcal{F}_k \subset \mathcal{F}_{v+k}$ para todos v, k. Em suma, $\mathcal{F} = \{\mathcal{F}_v\}$ é uma filtração do anel $A_n(K)$ e $\mathcal{F}$ é chamada filtração de Bernstein sobre $A_n(K)$. Introduziremos a soma direta (anel graduado associado) $\mathcal{F}_0 \oplus \frac{\mathcal{F}_1}{\mathcal{F}_0} \oplus \frac{\mathcal{F}_2}{\mathcal{F}_1} \oplus \cdots$. Isto é um espaço vetorial sobre K ao qual denotamos por $\mathfrak{gr}(A_n(K))$. Vide ([2]) para mais detalhes. Existe também a noção de filtração de um módulo. Os detalhes encontram-se na literatura relatada.

Proposição B.5. $\mathfrak{gr}(A_n(K))$ é um anel de polinômios em $2n$ variáveis com coeficientes em K.

Definição B.6. Uma filtração Γ em um $A_n(K)$-módulo à esquerda M é boa se $gr_\Gamma(M)$ é finitamente gerada como $gr(A_n(K))$-módulo.

Proposição B.7. Se M é um $A_n(K)$-módulo à esquerda ao qual pode ser equipado com uma filtração boa, então M é um $A_n(K)$-módulo finitamente gerado.

Reciprocamente podemos provar que:

Proposição B.8. Um $A_n(K)$-módulo à esquerda finitamente gerado M pode ser equipado com uma filtração boa.

Em geral, seja K um corpo comutativo e $K[x_1, .., x_N]$ um anel de polinômio em N variáveis onde N é um inteiro. Um $K[x_1, .., x_N]$-módulo graduado é um $K[x_1, .., x_N]$-módulo S que possui a decomposição $S = \bigoplus S(v)$ onde $S(v)$ são K-subespaços de S e $x_jS(v) \subset S(v+1)$ para cada $1 \leq j \leq N$ e todo v.

Teorema B.9. *Seja $S = \bigoplus S(v)$ um $K[x_1, .., x_N]$-módulo graduado e finitamente gerado. Então existem $a_1, ..., a_d \in \mathbb{Q}$ tais que*

$$\sum_{j \leq v} dim_K(S(j)) = a_dv^d + a_{d-1}v^{d-1} + \cdots + a_1v + a_0$$

para todo v suficientemente grande.

[1] $|\alpha| + |\beta| \leq 0 \Rightarrow \alpha = \beta = 0$.

Observação B.10. O polinômio $H(v) = a_d v^d + a_{d-1} v^{d-1} + \cdots + a_1 v + a_0$ que aparece em (B.9) é chamado polinômio de Hilbert de S. Então pode-se mostrar que $0 \leq d \leq N$ e $d = d(S)$ é chamado dimensão do $K[x_1, .., x_N]$-módulo graduado.

Corolário B.11. Seja Γ uma filtração *boa* de um $A_n(K)$-módulo à esquerda M finitamente gerado. Então existem um $d \geq 0$ e $a_0, ..., a_d$ tais que $dim_K(\Gamma_v) = a_d v^d + \cdots + a_0$ quando v é suficientemente grande.

Lema B.12. Sejam Γ e Ω duas filtrações de um $A_n(K)$-módulo à esquerda M e admita que Γ é boa. Então existe um inteiro w tal que $\Gamma_v \subset \Omega_{v+w}$ para todo v.

Corolário B.13. Se Γ e Γ' duas filtrações boas em um $A_n(K)$-módulo à esquerda M, então existem um inteiro w tal que $\Gamma_v \subset \Gamma'_{v+w}$ e $\Gamma'_v \subset \Gamma_{v+w}$ para todo v.

Usando (B.13) vemos que $d_\Gamma(M)$ é o mesmo para todas as filtrações boas em um dado $A_n(K)$-módulo M finitamente gerado. Ponhamos $d_\Gamma(M) = d(M)$ é chamada dimensão de Bernstein de M.

O próximo teorema é a importante desigualdade de Bernstein.

Teorema B.14. *$d(M) \geq n$ para todo M não nulo e finitamente gerado $A_n(K)$- módulo à esquerda.*

Isto permite dar a seguinte definição:

Definição B.15. Dizemos que um $A_n(K)$-módulo à esquerda finitamente gerado M é *holonômico* quando $d(M) \leq n$, ou seja, $d(M) = n$.

A seguir uma propriedade dos módulos holonômicos.

Proposição B.16. Seja M um módulo holonômico. Então M possui comprimento finito como $A_n(K)$-módulo à esquerda.

B.2 Anéis e Módulos Cohen-Macaulay

Definição B.17. Sejam R um anel comutativo com identidade noetheriano e M um R-módulo não-nulo finitamente gerado. Sejam $a_1, ..., a_n \in R$. Dizemos que $a_1, ..., a_n$ formam uma M-sequência (ou uma sequência regular) quando:
(i) $M \neq (a_1, ..., a_n)M$;
(ii) a_i *não é um divisor de zero de* $M/((a_1, ..., a_{i-1})M)$ $\forall\ i = 1, ..., n$.

Exemplo B.18. A sequência das indeterminadas $x_1, ..., x_n$ de um anel de polinômios $R = K[x_1, ..., x_n]$ é uma R-sequência.

O próximo lema é útil em argumentos de indução.

Lema B.19. Sejam R um anel comutativo com identidade noetheriano e M um R-módulo não-nulo finitamente gerado. Sejam $n \in \mathbb{N}, n > 1$ e $a_1, ..., a_n \in R$. Considere que $h \in \mathbb{N}$ com $1 \leq h < n$. Então $(a_i)_{i=1}^n$ é uma M-sequência se, e somente se,
(a) $(a_i)_{i=1}^h$ é uma M-sequência;
(b) $(a_i)_{i=h+1}^n$ é uma $M/(a_1, ..., a_h)M$-sequência.

A ordem dos termos em sequências regulares é fundamental como mostra o seguinte exemplo.

Exemplo B.20. Sejam K um corpo e R o anel $k[x, y, z]$. Então:
(i) $x, y(1-x), z(1-x)$ é uma R-sequência;
(ii) $y(1-x), z(1-x), x$ não é uma R-sequência.

Entretanto, se o anel for local qualquer permutação de uma sequência regular continua sendo regular. Mais geralmente temos o seguinte resultado:

Teorema B.21. *Sejam R um anel comutativo com identidade noetheriano e M um R-módulo não-nulo finitamente gerado. Seja $(a_i)_{i=1}^n$ uma M-sequência de elementos do radical de Jacobson $J(R)$, onde $n > 1$. Se σ é uma permutação qualquer do conjunto $\{1, ..., n\}$, então $(a_{\sigma(i)})_{i=1}^n$ também é uma M-sequência.*

Proposição B.22. Sejam R um anel comutativo com identidade noetheriano e M um R-módulo não-nulo finitamente gerado. Então não existe uma sequência infinita $(a_i)_{i=1}^\infty$ de elementos de R tal que, para todo n, a sequência finita $(a_i)_{i=1}^n$ seja uma M-sequência.

Demonstração. Suponhamos que tal sequência exista. Então, para cada $n \in \mathbb{N}$, temos $(a_1, \cdots, a_n) \subset (a_1, \cdots, a_n, a_{n+1})$, pois caso contrário teríamos a igualdade e daí $a_{n+1} \in (a_1, \cdots, a_n)$ e assim a_{n+1} seria um divisor de zero do R-módulo não nulo $M/(a_1, \cdots, a_n)M$. Então,

$$(a_1) \subset (a_1, a_2) \subset (a_1, \cdots, a_n) \subset \cdots$$

Seria uma cadeia ascendente infinita de ideais de R, contrariando o fato de R ser noetheriano. □

Definição B.23. Sejam R um anel comutativo com identidade noetheriano e M um R-módulo não-nulo finitamente gerado. Sejam I um ideal de R tal que $IM \neq M$ e $a_1, ..., a_n$ uma M-sequência de elementos de I. Dizemos que $(a_i)_{i=1}^n$ é uma M-sequência maximal em I se é impossível encontrar um elemento $a_{n+1} \in I$ tal que $a_1, ..., a_n, a_{n+1}$

formam uma M-sequência de tamanho $n+1$. É fácil ver que isso é equivalente a $I \subseteq DZ_R(M/(a_1, ..., a_n)M)$.

Teorema B.24. *Sejam R um anel comutativo com identidade noetheriano, M um R-módulo não-nulo finitamente gerado e I um ideal de R tal que $IM \neq M$. Então quaisquer duas sequências maximais em I tem o mesmo comprimento.*

Definição B.25. Sejam R um anel comutativo com identidade noetheriano, M um R-módulo não-nulo finitamente gerado e I um ideal de R tal que $IM \neq M$. A medida comum do comprimento de todas as sequências maximais em I é chamado *grade* de I em M, denotado por $grade(I, M)$. Quando $M = R$ simplesmente escrevemos $grade(I)$. Quando $(R, \mathfrak{m})$ é local, escrevemos $grade(\mathfrak{m}, R) = prof(\mathfrak{m})$.

O próximo resultado é útil em muitas situações, em sua demonstração usa-se o teorema do ideal principal de Krull generalizado.

Proposição B.26. Sejam R um anel comutativo com identidade noetheriano e J um ideal de R que é gerado por uma R-sequência de tamanho n. Então $ht(J) = n$.

Corolário B.27. Seja I um ideal próprio de um anel comutativo com identidade noetheriano R. então $grade(I) \leq ht(I)$.

Demonstração. Sejam $grade(I) = n$ e $(a_i)_{i=1}^n$ uma R-sequência maximal contida em I. Então $(a_1, \cdots a_n) \subseteq I$ e tendo em vista o resultado anterior tem-se,

$$grade(I) = n = ht(a_1, ..., a_n) \leq ht(I).$$

□

Proposição B.28. Seja I um ideal próprio de um anel comutativo com identidade noetheriano R. então $grade(I) = grade(\sqrt{I})$.

Demonstração. Como $I \subseteq \sqrt{I}$ tem-se $grade(I) \leq grade(\sqrt{I})$ (note que $\sqrt{I}$ é um ideal próprio de R). Sejam $n = grade(\sqrt{I})$ e $(a_i)_{i=1}^n$ uma R-sequência contida em $\sqrt{I}$. Existe $t \in \mathbb{N}$ tal que $a_i^t \in I \ \forall\ i = 1, ..., n$. Sabe-se que $(a_i^t)_{i=1}^n$ forma uma R-sequência, donde $grade(I) \geq n = grade(\sqrt{I})$.

□

Corolário B.29. Sejam I, J ideais próprios de um anel comutativo com identidade noetheriano R. então $grade(IJ) = grade(I \cap J) = min\{grade(I), grade(J)\}$.

Demonstração. Como $\sqrt{IJ} = \sqrt{I \cap J}$ segue que $grade(IJ) = grade(I \cap J)$. Além disso, $I \cap J \subseteq I \Rightarrow grade(I \cap J) \leq grade(I)$. Analogamente $grade(I \cap J) \leq grade(J)$.

Suponhamos por absurdo que $grade(I \cap J) < min\{grade(I), grade(J)\}$. Sejam $n = grade(I \cap J)$ e $(a_i)_{i=1}^n$ uma R-sequência maximal em $I \cap J$. Então $(a_i)_{i=1}^n$ é uma R-sequência em I e por hipótese existe $a_{n+1} \in I$ tal que $(a_i)_{i=1}^{n+1}$ é uma R-sequência. Analogamente, existe $a'_{n+1} \in J$ tal que $a_1, \cdots a_n, a'_{n+1}$ formam uma R-sequência. Logo $a_{n+1}, a'_{n+1} \in NDZ_R\left(\frac{R}{(a_1,\ldots,a_n)}\right)$, e o mesmo é verdade para $a_{n+1}a'_{n+1}$. Entretanto $a_{n+1}a'_{n+1} \in I \cap J$ e daí $a_1, \cdots a_n, a_{n+1}a'_{n+1}$ formam uma R-sequência contida em $I \cap J$ de comprimento $n+1$ o que contradiz o fato de $n = grade(I \cap J)$. Portanto $min\{grade(I), grade(J)\} = n$. □

Sejam R um anel comutativo com identidade noetheriano, M um R-módulo não-nulo finitamente gerado e S um conjunto multiplicativo tal que $S^{-1}M \neq 0$. Pode-se provar que se $(a_i)_{i=1}^n$ é uma M-sequência então a sequência $(a_i/1)_{i=1}^n$ de elementos de $S^{-1}R$ é uma $S^{-1}M$-sequência, supondo apenas que $S^{-1}M \neq (a_1/1, \cdots a_n/1)S^{-1}M$.

Corolário B.30. Sejam R um anel comutativo com identidade noetheriano, I um ideal de R, e S um conjunto multiplicativo tal que $I \cap S = \emptyset$. Então $grade(I) \leq grade(S^{-1}I, S^{-1}R)$.

A seguir daremos uma prova onde usamos o resultado de Inschebeck[2], vide ([19]).

Teorema B.31. *Sejam $(R, \mathfrak{m})$ um anel local noetheriano, G um R-módulo não nulo e finitamente gerado. Então,*

$$prof G \leq dim R/P, \quad \forall\ P\ \in\ Ass(G).$$

Demonstração. Suponhamos por absurdo que existe um $P \in Ass(G)$ tal que $Prof(G) > dim(R/P)$ então por Inschebeck

$$Ext_R^i(R/P, M) = 0\ \forall\ i < prof(G) - dim(R/P) \geq 1 \overset{\text{i=0}}{\Longrightarrow} Hom_R(R/P, M) = 0.$$

Por outro lado, $P \in Ass(G)$ implica que existe uma injeção R-linear $A/P \hookrightarrow M$ donde $Hom_R(R/P, M) \neq 0$, contradição. □

Corolário B.32. Sejam R um anel local noetheriano e G um R-módulo não nulo e finitamente gerado. Então $prof G \leq dim G$.

Demonstração. Como M é não nulo existe $\mathfrak{p} \in Ass(M)$. Logo $\mathfrak{p} \in Supp_R(M)$ implica $\mathfrak{p} \supseteq (0 : M)$ e obtém-se a sobrejeção de anéis $\frac{R}{(0:M)} \to \frac{R}{\mathfrak{p}}$ logo, por (B.31)

$$dim(R/\mathfrak{p}) \leq dim(R/(0 : M) = dim M.$$

[2]Sejam $M, N R$-módulos finitamente gerados então $Ext_R^i(N, M) = 0\ \forall\ i < prof(M) - dim(N)$.

Portanto $profM \leq dimM$. $\square$

Definição B.33. Um anel comutativo com identidade noetheriano R é dito *Cohen-Macaulay* quando $grade(I) = ht(I)$ para todo ideal próprio $I \subset R$. Um ideal próprio I de um anel comutativo com identidade noetheriano R é dito *unmixed* quando todos os primos associados de I tem a mesma altura.

Teorema B.34. *Seja R um anel comutativo com identidade noetheriano. Então R é Cohen-Macaulay se, e somente se, todo ideal gerado por uma R-sequência é unmixed.*

Definição B.35. Seja $(R, \mathfrak{m})$ um anel local noetheriano. Dizemos que R é *semiregular* quando $profR = dimR$.

Note que isso é equivalente a $grade(\mathfrak{m}) = ht(\mathfrak{m})$. É fácil mostrar que anéis regulares locais são semiregulares, na realidade temos que:

Proposição B.36. Seja $(R, \mathfrak{m})$ um anel local noetheriano. Então R é Cohen-Macaulay se, e somente se, é semiregular.

Também é fácil ver que anéis locais regulares são Cohen-Macaulay.

Exemplo B.37. O anel $R = \frac{\mathbb{C}[[x,y]]}{(x^2,xy)}$ não é Cohen-Macaulay.

Solução B.38. De fato, ele possui dimensão 1 e profundidade 0.

Teorema B.39. *Seja R um anel comutativo com identidade noetheriano. Então são equivalentes:*
(i) R é Cohen-Macaulay;
(ii) $grade(\mathfrak{p}) = ht(\mathfrak{p})$ $\forall$ $\mathfrak{p} \in Spec(R)$;
(iii) $grade(\mathfrak{m}) = ht(\mathfrak{m})$, para todo ideal maximal $\mathfrak{m}$ de R;
(iv) $R_\mathfrak{p}$ é Cohen-Macaulay para todo $\mathfrak{p} \in Spec(R)$;
(v) $R_\mathfrak{m}$ é Cohen-Macaulay para todo ideal maximal $\mathfrak{m}$ de R.

Demonstração. A título de exemplo vamos provar que $(v) \Rightarrow (ii)$: Sejam $\mathfrak{p}$ um ideal primo de R, $n = grade(\mathfrak{p})$ e $(a_i)_{i=1}^n$ uma R-sequência maximal contida em $\mathfrak{p}$. Considere $J = (a_1, ..., a_n)$. Como $\mathfrak{p} \subseteq DZ_R(R/J)$ então $\mathfrak{p} \subseteq \bigcup_{P' \in Ass(R/J)} P'$ portanto pelo lema da esquiva $\mathfrak{p} \subseteq P''$ com $P'' \in Ass(R/J)$. Seja $\mathfrak{m}$ um ideal maximal que contém P'. Por hipótese, $R_\mathfrak{m}$ é Cohen-Macaulay local. Então os elementos $a_1/1, \cdots, a_n/1$ do anel local $R_\mathfrak{m}$ formam uma $R_\mathfrak{m}$-sequência contida em $\mathfrak{p}R_\mathfrak{m} \subseteq P'R_\mathfrak{m}$. Agora temos um isomorfismo:

$$R_\mathfrak{m}/(a_1/1, \cdots, a_n/1) = R_\mathfrak{m}/(a_1, ..., a_n)R_\mathfrak{m} = R_\mathfrak{m}/(JR)_\mathfrak{m} \cong (R/J)_\mathfrak{m}.$$

Entretanto,

$$P'R_{\mathfrak{m}} \in Ass_{R_{\mathfrak{m}}}((R/J)_{\mathfrak{m}}) = Ass_{R_{\mathfrak{m}}}(R_{\mathfrak{m}}/(a_1/1, \cdots, a_n/1)).$$[3]

daí $\mathfrak{p}R_{\mathfrak{m}} \subseteq P'R_{\mathfrak{m}} \subseteq DZ_R(R_{\mathfrak{m}}/(a_1/1, \cdots, a_n/1))$, e consequentemente os elementos $a_1/1, \cdots, a_n/1$ de $R_{\mathfrak{m}}$ formam uma $R_{\mathfrak{m}}$-sequência contida em $\mathfrak{p}R_{\mathfrak{m}}$. Portanto $grade(\mathfrak{p}R_{\mathfrak{m}}, R_{\mathfrak{m}}) = n$, mas $R_{\mathfrak{m}}$ é Cohen-Macaulay: $ht(\mathfrak{p}R_{\mathfrak{m}}) = n \Rightarrow ht(\mathfrak{p}) = n = grade(\mathfrak{p})$. □

Em particular todo anel de frações de um anel Cohen-Macaulay é Cohen-Macaulay.

Exemplo B.40. Todo anel comutativo com identidade artiniano R é Cohen-Macaulay. Em particular, para cada $n \in \mathbb{N}$ com $n > 1$ o anel $\mathbb{Z}/n\mathbb{Z}$ é Cohen-Macaulay.

Proposição B.41. Suponhamos que o anel local (R,m) é Cohen Macaulay. Então

$$ht(\mathfrak{p}) + dim(R/\mathfrak{p}) = dimR \quad \forall\, \mathfrak{p} \in Spec(R).$$

Teorema B.42. *Sejam R um anel comutativo com identidade noetheriano e $a \in J(R)$ tal que a forma uma R-sequência (de tamanho 1). Então R é Cohen-Macaulay se, e somente se, $R/(a)$ é Cohen-Macaulay.*

Pode-se mostrar que se R é um anel comutativo com identidade noetheriano Cohen-Macaulay e sendo $a_1, ..., a_n$ uma R-sequência então

$$R/(a_1, ..., a_n) \text{ é } Cohen - Macaulay. \tag{B.1}$$

Corolário B.43. Seja R um anel comutativo com identidade noetheriano. Então o anel das séries formais $R[[x_1, ..., x_n]]$ sobre R e n indeterminadas $x_1, ..., x_n$ é Cohen-Macaulay se, e somente se, R é Cohen-Macaulay.

Demonstração. Pelo teorema da base de Hilbert $R[[x_1, .., x_n]]$ é noetheriano. Quando $n > 1$, $R[[x_1, ..., x_n]] \cong R[[x_1, ..., x_{n-1}]][[x_n]]$. Um simples argumento indutivo mostra que é suficiente mostrar o resultado para $n = 1$. Nesse caso escreva x para x_1. A aplicação

$$\begin{array}{cccc} h: & R[[x]] & \longrightarrow & R \\ & \sum_{j=0}^{\infty} x^j & \longmapsto & r_0 \end{array}$$

é um epimorfismo com núcleo $xR[[x]]$; daí existe um isomorfismo $R \cong R[[x]]/xR[[x]]$. Desde que x é claramente um não divisor de zero em $R[[x]]$ vemos que x forma uma $R[[x]]$-sequência. Além disso, para todo $f \in R[[x]]$ o elemento $1 - xf$ é uma unidade em $R[[x]]$ donde $x \in J(R)$. O resultado segue do teorema anterior. □

[3]em virtude da igualdade: $Ass_{S^{-1}R}(S^{-1}M) = \{PS^{-1}R : P \in Ass_R(M) \text{ e } P \cap S = \emptyset\}$.

Teorema B.44. *Seja R um anel comutativo com identidade noetheriano. Então o anel de polinômios $R[x_1, ..., x_n]$ sobre R e n indeterminadas $x_1, ..., x_n$ é Cohen-Macaulay se, e somente se, R é Cohen-Macaulay.*

Proposição B.45. Seja $0 \to L \to M \to N \to 0$ uma sequência exata de R-módulos. Então:
(a) Se L e N são Cohen-Macaulay assim o é M.
(b) Se M e N são Cohen-Macaulay assim o é L.

Observação B.46. Não é verdade que se L e M são Cohen-Macaulay então N o é. O resultado (B.45) vale para módulos Cohen-Macaulay maximais.

Definição B.47. Um sistema de parâmetros para um anel local $(R, \mathfrak{m})$ é uma sequência $x_1, ..., x_n$ contida em $\mathfrak{m}$ tal que $n = ht(\mathfrak{m})$ e $\mathfrak{m}$ é o único ideal primo contendo $x_1, ..., x_n$. Isso é equivalente a dizer que

$$Ass(R/(x_1, ..., x_n)) = \mathfrak{m}.$$

Note que todo anel local noetheriano possui um sistema de parâmetros (que não é único). Sistemas de parâmetros têm uma relação intíma com anéis Cohen-Macaulay:

Proposição B.48. Um anel local noetheriano R é Cohen-Macaulay se, e somente se, todo sistema de parâmetros é uma R-sequência.

Sejam R anel local noetheriano e $\widehat{R}$ seu completamento. Pode-se provar que $dimR = dim\widehat{R}$ e que $profR = prof\widehat{R}$, portanto tem-se:

Teorema B.49. *Seja R anel local noetheriano então R é Cohen-Macaulay se, e somente se, $\widehat{R}$ é Cohen-Macaulay.*

Por fim um resultado relacionado com cohomologia local.

Teorema B.50. *Sejam $(R, \mathfrak{m}, k)$ um anel local noetheriano e M um R-módulo. São equivalentes:*
(a) M é Cohen-Macaulay;
(b) $Ext^i_R(k, M) = 0$, para $i < dimR$;
(c) $H^i_{\mathfrak{m}}(M) = 0$, para $i \neq dimR$.

Para mais detalhes veja ([12]) e ([8]).

B.3 Anéis Gorenstein

Antes de tudo, vamos começar com um resultado útil de módulos injetivos, a saber:

Proposição B.51. Sejam R um anel e N um R-módulo. São equivalentes:
(1) N é injetivo;
(2) $Ext^i_R(M,N)=0$ para todo R-módulo M e todo $i\geq 0$;
(3) $Ext^1_R(M,N)=0$ para todo R-módulo M;
(4) $Ext^1_R(M,N)=0$ para todo R-módulo M finitamente gerado;
(5) $Ext^1_R(R/I,N)=0$ para todo ideal I de R.

Demonstração. É suficiente provar (5) $\Rightarrow$ (1): Vamos usar o critério de Baer (A.1). Devemos mostrar que para cada ideal $I\subseteq R$ o homomorfismo de R-módulos $\phi: I\to N$ pode ser estendido ao homomorfismo de R-módulos $\psi: R\to N$. Isto é o mesmo que dizer que a aplicação

$$Hom_R(R,N)\rightarrowtail Hom_R(I,N)$$

é sobrejetiva. Considere a sequência exata curta:

$$0\to I\to R\to R/I\to 0.$$

Aplicando a sequência exata longa de Ext's:

$$0\to Hom_R(R/I,N)\to Hom_R(R,N)\to Hom_R(I,N)\to Ext^1_R(R/I,N)=0\to\cdots$$

donde segue que N é injetivo.

□

Definição B.52. Seja R um anel e M um R-módulo. A dimenção injetiva de M, denotada por $inj\ dim_R M = inj\ dim(M)$ é o menor inteiro positivo n para o qual existe uma resolução injetiva $I^\bullet$ de M com $I^m=0$ para $m>n$. Se não existe tal m dizemos que a dimesão injetiva de M é infinita.

A seguinte proposição segue de (A.37) e da exatidão da localização:

Proposição B.53. Seja R um anel comutativo com identidade noetheriano, M um R-módulo e S um conjunto multiplicativo. Então $inj\ dim_{S^{-1}R}(S^{-1}M)\leq inj\ dim_R(M)$.

A próxima proposição caracteriza dimensão injetiva homologicamente.

Proposição B.54. Seja R um anel, M um R-módulo. São equivalentes:
(i) $inj\ dimM\leq n$;

(ii) $Ext_R^{n+1}(N, M) = 0$ para todo R-módulo N;
(iii) $Ext_R^{n+1}(R/J, M) = 0$ para todo ideal J de R.

A proposição acima pode ser melhorada no caso em que R é Noetheriano. De fato, é notável dizer que neste caso, sendo M um R-módulo a condição (i) acima é equivalente a $Ext_R^{n+1}(R/\mathfrak{p}, M) = 0$ para todo $\mathfrak{p} \in Spec(R)$. A proposição abaixo nos dá uma fórmula para a dimesão injetiva no caso local Noetheriano:

Proposição B.55. Sejam $(R, \mathfrak{m}, k)$ local noetheriano e M um R-módulo finitamente gerado. Então

$$inj \dim M = sup\{i \mid Ext_R^i(k, M) \neq 0\}.$$

O seguinte resultado é importantíssimo.

Teorema B.56. *Sejam $(R, \mathfrak{m}, k)$ um anel local noetheriano e M um R-módulo finitamente gerado com dimensão injetiva finita. Então $dimM \leq inj\ dimM = profR$.*

Agora estamos em condições de definir uma classe importante de anéis locais.

Definição B.57. Um anel local noetheriano R é dito *Gorenstein* quando $inj\ dimR < \infty$. Um anel noetheriano é dito *Gorenstein* se sua localização a todo ideal maximal é um anel local Gorenstein.

Sejam $(R, \mathfrak{m}, k)$ um anel local noetheriano e M um R-módulo, definimos o tipo de M como sendo:

$$tipo(M) = dim_k(Ext_R^n(k, M)).$$

Proposição B.58. R é um anel Gorenstein se, e somente se, R é Cohen-Macaulay de tipo 1.

Assim anéis Gorenstein são Cohen-Macaulay também, e portanto valem todas as propriedades já vistas na seção anterior. O próximo resultado envolve sistemas de parâmetros.

Proposição B.59. Um anel local noetheriano R é Gorenstein se, e somente se, todo ideal gerado por um sistema de parâmetros é irredutível.[4]

É bom ter em mente que anéis regulares são Gorenstein e que R é Gorenstein $\Leftrightarrow \widehat{R}$ é Gorenstein.

Sabemos que em geral (vide apêncide de módulos injetivos)

$$E^i(M) = \bigoplus_{\mathfrak{p} \in Spec(R)} E(R/\mathfrak{p})^{\mu_i(\mathfrak{p}, M)},$$

[4] I é um ideal irredutível quando $I \subset R$ e $I = I_1 \cap I_2 \Rightarrow I = I_1$ ou $I = I_2$.

no caso em que R é Gorenstein pode-se mostrar ([4]) que

$$E^i(M) = \bigoplus_{\substack{\mathfrak{p}\in Spec(R)\\ ht(\mathfrak{p})=i}} E(R/\mathfrak{p}).$$

Em resumo, pode-se depreender que o número de Bass (no caso Gorenstein) fica:

$$\mu_i(\mathfrak{p}, R) = \begin{cases} 0 & se \quad i \neq ht(\mathfrak{p}) \\ 1 & se \quad i = ht(\mathfrak{p}) \end{cases}.$$

Definição B.60. O módulo canônico para um anel R é um R-módulo finitamente gerado ω tal que $Hom_R(\omega, E_R(R/\mathfrak{m})) \cong H^n_{\mathfrak{m}}(R)$. Em particular se R é Gorenstein, $\omega = R$.

É notável dizer que existe um resultado para anéis invariantes no contexto de anéis Gorenstein.

Teorema B.61. *Sejam R um anel noetheriano, G um subgrupo finito dos automorfismos de R e suponha que $|G|$ é inversível em R. Se $G \subset SL_n(K)$,*[5] *então R^G é Gorenstein.*

Demonstração. Vide [37]. □

Para finalizar iremos dar uma caracterização de anéis Gorenstein envolvendo dual de Matlis.

Teorema B.62. *Um anel local $(R, \mathfrak{m}, k)$ noetheriano de dimensão d é Gorenstein se, e somente se, R é Cohen-Macaulay e $H^d_{\mathfrak{m}}(R) \cong E$ (ou equivalentemente $(H^d_{\mathfrak{m}}(R))^\vee \cong \widehat{R}$).*

Demonstração. Vide ([9], Definição 4.3). □

[5] $\mathrm{SL}_n(K) = \{M \in \mathcal{M}_n(K) \mid det(M) = 1\}$.

Referências Bibliográficas

[1] ATIYAH, M. F. AND MACDONALD, I. G., *Introduction to commutative algebra*, Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont. 1969.

[2] BJÖRK, J. E., *Rings of Differential Operators.* Elsevier.

[3] BOUBARKI, *Commutative Algebra*, Hermann, Paris, 1972.

[4] BRODMANN, M. AND SHARP, R. Y., *Local Cohomology: an algebraic introduction with geometric applications*, Cambridge Univ. Press, 60, Cambridge, (1998).

[5] BASS, H., *On the ubiquity of Gorenstein rings*, Math. Z. 82 (1963), 8-28.

[6] BRUNS, W. AND HERZOG J., *Cohen- Macaulay ring*, Cambridge Studies in Advanced Mathematics 39, Revised Edition (Cambridge Univ. Press, Cambridge, 1998).

[7] BORGES, H., TENGAN, E., *Álgebra comutativa em quatros movimentos*, Projeto Euclides, IMPA, 2015.

[8] GROTHENDIECK, A., *Local cohomology*, Notes by R. Hartshorne, Lect. Notes in Math., 20, Springer, (1966).

[9] HUNEKE, CRAIG, *Lectures on Local cohomology*, Contemporary Mathematics.

[10] HUNEKE, C. AND SHARP, R., *Bass numbers of local cohomology modules*, AMS Transactions 339 (1993), 765-779.

[11] HARTSHORNE, R., *Affine duality and cofiniteness*, Invent. Math. 9 1969/1970 145-164.

[12] HERZOG J. AND KUNZ, E., *"Der kanonische Modul eines Cohen-Macaulay-Rings"*, Lecture Notes in Math. vol. 238, Springer Verlag, 1971.

[13] IYENGAR, S., LEUSCHKE, G., LEYKIN, A., MILLER, C., AND MILLER, E.. *Twenty-four hours of local cohomology.* Graduate Studies in Mathematics. American Mathematical Society, 2007.

[14] KATZMAN, M., *An example of an infinite set of associated primes of a local cohomology module*, J. Algebra 252 (2002), no. 1, 161-166.

[15] KLEIMAN, STEVEN, ALTMAN, ALLEN, *A Term of Commutative Algebra.*

[16] LYUBEZNIK, G. , *Finiteness Properties of Local Cohomology Modules (an Application of D-modules to Commutative Algebra)*, Inv. Math. 113 (1993), 41-55.

[17] LYUBEZNIK, G. , *F-modules: applications to local cohomology and D-modules in characteristic* $p = 0$, J. Reine Angew. Math. 491 (1997), 65-130.

[18] MATLIS, E., *Injective modules over notherian rings*, Pacific J. Math. 8 (1958), 511-528.

[19] MATSUMURA, H, *Commutative ring theory*, Cambridge Univ. Press, (1986).

[20] PUTHENPURAKAL, TONY J., *Local Cohomology Modules of Invariant Rings.* Cambridge Philosophical Society, 2015.

[21] POON, EDWARD, *Skew Group Rings,* Class Note, Summer 2016.

[22] ROTMAN, J., *An Introduction to Homological Algebra*, Academic Press, Orlando, FL, 1979.

[23] SHARP, R. Y., *Steps in commutative algebra: Second edition*, London Mathematical Society Student Texts 51 (Cambridge University Press, Cambridge, 2000).

[24] SHARP, R. Y., *On The Attached Prime Ideals of Certain Artinian Local Cohomology Modules*, 1979.

[25] SARRIA., LUIS, TUESTA., CARO , *Álgebra Comutativa: Uma Introdução.* Notas de Aula. UFPB. 2017.

[26] SHARP, R. Y., *Some results on the vanishing of local cohomology modules*, Proc. London Math. Soc. 30 (1975) 177–195.

[27] SHARP, R. Y., *Secondary representations for injective modules over commutative Noetherian rings*, Proc. Edinburgh Math. Soc. (2) 20 (1976), 143-151.

[28] SHARP, R. Y., *Local Cohomology theory in Commutative Algebra*, Quart. J. Math. (Oxford) (2) 21 (1970) 425-34.

[29] SCOTT, M. OSBORNE., *Basic homology Algebra*, Graduate texts in Mathematics, Springer, (196) (2000).

[30] SHARP, D. W. AND VÁMOS, P., *Injective modules*, Cambridge tracts in mathematics and mathematical physics No. 62, Cambridge University Press, (1972).

[31] SINGH, A., *p-torsion elements in local cohomology modules*, Math. Res. Lett. 7 (2000), no. 2-3, 165-176

[32] SINGH, A. AND SWANSON, I., *Associated primes of local cohomology modules and of Frobenius powers*, Int. Math. Res. Not. 2004, no. 33, 1703-1733.

[33] TRAVES, W., *W. Traves, Differential operators on orbifolds*, J. Symbolic Comput. 41 (2006), no. 12, 1295- 1308.

[34] VERMA, J. K., *Rings of Invariats of Finite Groups.* 18-19.

[35] WINFRIED, BRUNS., *Rings of invariants.* Notes Class. 2008.

[36] WEIBEL, C., *An introduction to homological algebra*, Cambridge Univ. Press, Cambridge, 1994.

[37] WATANABE, K., *K. Watanabe, Certain invariant subrings are Gorenstein.* I, Osaka J. Math. 11 (1974), 1-8.