Universidade Federal de Pernambuco
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática

THIAGO FIEL DA COSTA CABRAL

GERADORES DE D-MÓDULOS EM CARACTERÍSTICA POSITIVA

Recife
2016

Thiago Fiel da Costa Cabral

Geradores de D-módulos em Característica Positiva

Trabalho apresentado ao Programa de Pós-graduação em Matemática, do Departamento de Matemática da Universidade Federal de Pernambuco, como requisito parcial para obtenção do grau de Mestre em Matemática.

ORIENTADOR: **Prof. Eduardo Shirlippe Góes Leandro**
CO-ORIENTADOR: Prof. **Jorge Nicolás Caro Montoya**

Recife
2016

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

C117g Cabral, Thiago Fiel da Costa
Geradores de D-módulos em característica positiva / Thiago Fiel da Costa Cabral. – 2016.
56 f.

Orientador: Eduardo Shirlippe Góes Leandro.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CCEN, Matemática, Recife, 2016.
Inclui referências e apêndices.

1. Matemática. 2. Operador diferencial. I. Leandro, Eduardo Shirlippe Góes (orientador). II. Título.

510 CDD (23. ed.) UFPE- MEI 2017-165

THIAGO FIEL DA COSTA CABRAL

GERADORES DE D-MÓDULOS EM CARACTERÍSTICA POSITIVA

Dissertação apresentada ao Programa de Pós-graduação do Departamento de Matemática da Universidade Federal de Pernambuco, como requisito parcial para a obtenção do título de Mestrado em Matemática.

Aprovado em: 28/07/2016

BANCA EXAMINADORA

Prof. Dr. Eduardo Shirlippe Góes Leandro (Orientador)
Universidade Federal de Pernambuco

Prof. Dr. Marco Barone (Examinador Interno)
Universidade Federal de Pernambuco

Prof. Dr. Cleto Brasileiro Miranda Neto (Examinador Externo)
Universidade Federal da Paraíba

Resumo

Sejam $R = k[x_1,...,x_d]$ ou $R = k[[x_1,...,x_d]]$ um anel de polinômios ou um anel de séries de potências formais em um número finito de variáveis sobre um corpo k de característica positiva $p > 0$ e $D_{R|k}$ o anel de operadores diferenciais k-lineares de R. Nesta dissertação será provado que, se f é um elemento não-nulo de R, então R_f, o anel de frações obtido de R por inverter f, é gerado como um $D_{R|k}$-módulo por $\frac{1}{f}$. Esse resultado é impressionante, considerando que em característica zero é falso. Será provado também um resultado análogo para uma vasta classe de anéis R e $D_{R|k}$-módulos, com o auxílio da teoria de $R[F]$-módulos unitários e da Descida de Frobenius. E por último, mostraremos que os módulos de cohomologia local de um R-módulo finitamente gerado tem comprimento finito na categoria de $D_{R|k}$-módulos, para essa vasta classe de anéis R, utilizando complexos de Čech, uma ferramenta bastante útil em álgebra homológica.

Palavras-chave: Operador Diferencial. $R[F]$-módulo unitário. Cohomologia Local.

Abstract

Let $R = k[x_1,...,x_d]$ or $R = k[[x_1,...,x_d]]$ be either a polynomial or formal power series ring in a finite number of variables over a field k of positive characteristic $p > 0$ and let $D_{R|k}$ be the ring of k-linear differential operators of R. In this dissertation will be proved that if f is a non-zero element of R then R_f, the ring of fractions obtained from R by inverting f, is generated as a $D_{R|k}$-module by $\frac{1}{f}$. This is an amazing fact considering that the corresponding characteristic zero statement is false. Will be proved an analog of this result for a considerably wider class of rings R and a considerably wider class of $D_{R|k}$-modules, with the support of the unit $R[F]$-modules theory and of the Frobenius Descent. Finally, we will show that the local cohomology modules of a R-module finitely generated have finite length in the category of $D_{R|k}$-modules, for this considerably wider class of rings, using Čech complexes, A very useful tool in homological algebra.

Keywords: Differential Operator. Unit $R[F]$-module. Local Cohomology.

Sumário

Capítulo 1

Introdução

Neste trabalho de dissertação, exibimos com mais detalhes os resultados desenvolvidos no artigo intitulado *Generators of D-modules in positive characteristic*, dos autores Josep Alvarez-Montaner, Manuel Blickle e Gennady Lyubeznik, do ano de 2005 [**?**], e damos uma aplicação desses resultados a cohomologia local.

Seja k um corpo e seja $R = k[x_1,...,x_d]$ ou $k[[x_1,...,x_d]]$ um anel de polinômios ou um anel de séries de potências formais em um número finito de variáveis sobre k. Seja $D_{R|k}$ o anel de operadores diferenciais k-lineares em R. Para todo $f \in R$ não-nulo, a ação natural de $D_{R|k}$ em R induz, de maneira única, uma ação no anel de frações R_f, via a conhecida regra do quociente. Disto, R_f adquire uma estrutura natural de $D_{R|k}$-módulo. Um conhecido fato sobre R_f, é que ele tem comprimento finito na categoria de $D_{R|k}$-módulos. Esse fato foi provado para um anel de polinômios sobre um corpo de característica zero por Bernstein ([**?**], Cor. 1.4) e, também em característica zero, para um anel de séries de potências formais por Björk ([**?**], Thm. 2.7.12, 3.3.2). Em característica positiva, o caso polinomial foi dado por Bogvad ([**?**], Prop. 3.2) e para o caso de séries de potências formais por Lyubeznik ([**?**], Thm. 5.9). Consequentemente, a cadeia crescente de $D_{R|k}$-módulos

$$D_{R|k} \cdot \frac{1}{f} \subseteq D_{R|k} \cdot \frac{1}{f^2} \subseteq \cdots \subseteq D_{R|k} \cdot \frac{1}{f^i} \subseteq \cdots \subseteq R_f$$

estabiliza, isto é, R_f é gerado por $\frac{1}{f^i}$, para algum i. Daí, nos perguntamos: Qual o menor i tal que $\frac{1}{f^i}$ gera R_f como um $D_{R|k}$-módulo?

Se k é um corpo de característica zero e $f \in R$ é um polinômio não-nulo, a resposta para essa questão é conhecida: Teorema 1' de [**?**] mostra que existe um polinômio mônico $b_f(s) \in k[s]$ é um operador diferencial $Q(s) \in D_{R|k}[s]$ tais que

$$Q(s) \cdot f^{s+1} = b_f(s) \cdot f^s$$

para todo s. O polinômio $b_f(s)$ é chamado de polinômio Bernstein-Sato de f. Seja $-i$ a raiz inteira negativa de $b_f(s)$ de maior valor absoluto (essa raiz existe, pois -1 é sempre raiz de $b_f(s)$). Então, $b_f(s) \neq 0$ para todo $s < -i$, daí $f^s \in D_{R|k} \cdot f^{s+1}$, implicando $\frac{1}{f^s} \in D_{R|k} \cdot \frac{1}{f^i}$, para todo $s > i$. Em particular, R_f é gerado por $\frac{1}{f^i}$ como $D_{R|k}$-módulo, e é visto em ([?], Lem. 1.3), que R_f não pode ser gerado por $\frac{1}{f^j}$, para $j < i$. Isso nos dá uma resposta completa para a questão, em característica zero.

Por exemplo, considere o polinômio $f = x_1^2 + \cdots + x_{2n}^2$. Então, equação

$$\frac{1}{4}\left(\frac{\partial^2}{\partial x_1^2} + \cdots + \frac{\partial^2}{\partial x_{2n}^2}\right) \cdot f^{s+1} = (s+1)(s+n) \cdot f^s$$

mostra que o polinômio Bernstein-Sato de f é $b_f(s) = (s+1)(s+n)$ ([?], Cor. 3.17). Disto, R_f é gerado por $\frac{1}{f^n}$, mas não por $\frac{1}{f^j}$, para $j < n$.

O primeiro objetivo nesta dissertação é provar:

Teorema 1.0.1. *Seja $R = k[x_1, ..., x_d]$ ou $R = k[[x_1, ..., x_d]]$ um anel de polinômios ou anel de séries de potências formais sobre um corpo de característica $p > 0$ e seja $f \in R$ não-nulo. Então R_f é gerado por $\frac{1}{f}$ como $D_{R|k}$-módulo.*

De fato, provamos esse resultado para uma vasta classe de anéis R e $D_{R|k}$-módulos. O segundo objetivo é mostrar que os módulos de cohomologia local de um R-módulo finitamente gerado, em relação a qualquer ideal de R, têm comprimento finito na categoria de $D_{R|k}$-módulos, para uma classe de anéis R.

No capítulo 1, coletamos resultados básicos (e não tão básicos) sobre $D_{R|k}$-módulos em característica $p > 0$, juntamente com a definição e propriedades do funtor Frobenius e suas iterações, como também de $R[F]$-módulos unitários. E concluímos com a Descida de Frobenius. Esses fatos iniciais serão cruciais no desenvolvimento do capítulo 2.

No Capítulo 2, atacamos o teorema acima. Começamos definindo uma cadeia descendente de ideais associados a um elemento f de um anel regular F-finito R de característica $p > 0$, consequentemente, mostramos que essa cadeia estabiliza se, e somente se, R_f é gerado por $\frac{1}{f}$ como $D_{R|k}$-módulo. Verificamos que para o caso em que $R = k[x_1, ..., x_d]$ a prova é de fácil entendimento. Depois estendemos para o caso em que R é uma álgebra regular finitamente gerada sobre um anel local regular F-finito de característica $p > 0$, onde usamos fortemente os resultados obtidos no Capítulo 1, em especial a Descida de Frobenius e o Teorema de Lyubeznik (1.3.10). Por fim, verificamos o caso em que R é uma álgebra finitamente gerada sobre $R = k[[x_1, ..., x_d]]$, um anel de séries de potências formais sobre um corpo k de característica $p > 0$ (o caso k perfeito é coberto pelo caso anterior).

Por último, no Capítulo 3, exibimos a definição e propriedades básicas do funtor de cohomologia local com respeito a um ideal I de um anel Noetheriano R. Em seguida, definimos o complexo de Čech de um R-módulo em relação a uma sequência $a_1, ..., a_n$ de elementos de R, e exibimos um resultado que relaciona a cohomologia no complexo de Čech com módulos de cohomologia local. Disto, provamos que módulos de cohomologia local de um R-módulo finitamente gerado, com respeito a qualquer ideal de R, tem comprimento finito na categoria de $D_{R|k}$-módulos, para uma classe de anéis R.

No apêndice A, exibimos de maneira objetiva os conceitos básicos da teoria de categorias, a definição e propriedades básicas do produto tensorial entre módulos e a definição de anéis regulares, para o leitor que não tem familiaridade com tais. Também exibimos, no apêndice B, a parte introdutória da teoria de operadores diferenciais em característica zero. No apêndice C, demonstramos um teorema muito importante do capítulo 1.

Capítulo 2

Preliminares

2.1 Módulos sobre anéis de operadores diferenciais em característica positiva

Nesta seção, será visto a definição e propriedades básicas de operadores diferenciais de um anel R, onde R é um anel comutativo que contém um corpo k de característica $p > 0$. Exibimos a estrutura usual de D_R-módulo do anel R_f. Por fim, verificamos a estrutura de D_R-módulo, dada pelo Teorema 1.1.4, para $R = k[x_1, ..., x_d]$, um anel de polinômios sobre um corpo k de característica $p > 0$.

Definição 2.1.1. Um operador diferencial $\delta : R \to R$ de ordem $\leq n$, onde n é um inteiro não-negativo, é definido indutivamente como segue. Um operador diferencial de ordem 0 é apenas a multiplicação por um elemento de R. Um operador de ordem $\leq n$ é um mapa aditivo $\delta : R \to R$ tal que, para todo $r \in R$, o comutador $[\delta, \tilde{r}] = \delta \circ \tilde{r} - \tilde{r} \circ \delta$ é um operador diferencial de ordem $\leq n-1$, onde $\tilde{r} : R \to R$ é a multiplicação por r (Compare com o apêndice B).

É fácil verificar que a soma de dois operadores diferenciais é um operador diferencial, devido à biaditividade do comutador, e a ordem da soma é a maior entre as ordens das parcelas. Sejam $r \in R$ e δ, τ operadores diferenciais de ordem $\leq n$, $\leq m$, respectivamente. Temos

$$[\delta \circ \tau, \tilde{r}] = \delta \circ [\tau, \tilde{r}] + [\delta, \tilde{r}] \circ \tau,$$

portanto, por indução em $n+m$, pode-se verificar que a composição também é um operador diferencial de ordem $\leq n+m$. Daí os operadores diferenciais formam um anel que é subanel de $\mathrm{End}_{\mathbb{Z}} R$. Denotamos este anel por D_R.

Se $k \subset R$ é um subanel, denotamos por $D_{R|k} \subset D_R$ o subanel de D_R consistindo de todos os operadores diferenciais que são k-lineares. Visto que todo mapa em $\mathrm{End}_{\mathbb{Z}} R$ é $\mathbb{Z}/p\mathbb{Z}$-linear, temos que $D_R = D_{R|(\mathbb{Z}/p\mathbb{Z})}$, isto é, D_R é um caso especial de $D_{R|k}$. O monomorfismo de anéis $R \to D_{R|k}$, que manda $r \in R$ para a multiplicação por r, faz de R um subanel de $D_{R|k}$.

Por um $D_{R|k}$-módulo entendemos um $D_{R|k}$-módulo à esquerda.

Exemplo 2.1.2. (a) R com a ação natural de $D_{R|k}$ é um $D_{R|k}$-módulo. Sejam $\delta \in D_{R|k}$ e $r \in R$, temos

$$\delta \cdot r := \delta(r).$$

(b) Se M é um $D_{R|k}$-módulo e $S \subset R$ um conjunto multiplicativamente fechado, então $S^{-1}M$ tem uma única estrutura de $D_{R|k}$-módulo tal que a localização natural $M \to S^{-1}M$ é um homomorfismo de $D_{R|k}$-módulos.

De fato, existe uma única estrutura de R-módulo em $S^{-1}M$ tal que o mapa natural $M \to S^{-1}M$ seja um homomorfismo de R-módulos, dado por $r(x/s) = (rx)/s$ para todo $r \in R$, $s \in S$ e $x \in M$. Se a ação de operadores diferenciais de ordem $\leq n-1$ em $S^{-1}M$ está definida, então existe uma única maneira de estender a uma ação de operadores diferenciais de ordem $\leq n$ que seja compatível com as relações da forma $[s,\delta] = s\delta - \delta s$, onde $s \in S$ e δ é um operador diferencial de ordem $\leq n$, dada por

$$\delta\left(\frac{x}{s}\right) := \frac{[s,\delta]\left(\frac{x}{s}\right) + \delta(x)}{s},$$

ou seja, $\delta = s^{-1}([s,\delta] + \delta s)$. Isto faz sentido, pois $[s,\delta]$ é um operador de ordem $\leq n-1$, daí sua ação em M_S está definida, por hipótese. Sejam $\delta \in D_{R|k}$ e $x/s = y/t \in S^{-1}M$, então:

$$\begin{aligned}
\delta\left(\frac{y}{t}\right) &= t^{-1}\left([t,\delta]\left(\frac{y}{t}\right) + \delta(y)\right) \\
&= t^{-1}\left((t\delta - \delta t)\left(\frac{x}{s}\right) + \delta(y)\right) \\
&= t^{-1}\left(t\delta\left(\frac{x}{s}\right) - \delta\left(\frac{tx}{s}\right) + \delta(y)\right) \\
&= \delta\left(\frac{x}{s}\right) - t^{-1}\delta\left(\frac{y}{1}\right) + t^{-1}\delta(y) \\
&= \delta\left(\frac{x}{s}\right),
\end{aligned}$$

disto, vemos que a ação está bem definida. Esta ação é compatível com a operação de adição em M e $D_{R|k}$, como também a operação de multiplicação em $D_{R|k}$. Com isto, a estrutura de $D_{R|k}$-módulo em $S^{-1}M$ está definida. Em particular, R_f carrega uma estrutura natural de $D_{R|k}$-módulo para todo $f \in R$.

Seja $R^{p^s} \subset R$ o subanel consistindo de todas as p^s-ésimas potências de todos os elementos de R.

Proposição 2.1.3. *Todo operador diferencial $\delta \in D_R$ de ordem $\leq p^s - 1$ é R^{p^s}-linear, para todo s.*

Demonstração. Seja $r \in R$, definimos o mapa $\tau_r : D_R \to D_R$, dado por $\tau_r(\delta) = [\delta, \tilde{r}]$. Note que

$$\tau_r^k(\delta) = \sum_{i=0}^{k} \binom{k}{i} (-1)^i r^i \delta r^{k-i}.$$

Assim, se $\delta \in D_R$ de ordem $\leq p^s - 1$, então $\tau_r^{p^s}(\delta) = 0$, pela definição de operador diferencial. Como R contém um corpo de característica $p > 0$,

$$0 = \tau_r^{p^s}(\delta) = \delta r^{p^s} - r^{p^s}\delta.$$

□

Em outras palavras, D_R é um subanel do anel

$$\bigcup_s D_R^{(s)}$$

onde $D_R^{(s)} = \mathrm{End}_{R^{p^s}}(R)$, anel dos endomorfismos R^{p^s}-lineares de R. Em particular, isso implica que, se k não for apenas $\mathbb{Z}/p\mathbb{Z}$, mas qualquer subcorpo perfeito de R, isto é, $k \subset R^{p^s}$ para todo s, então todo $\delta \in D_R$ é k-linear, ou seja, $D_R = D_{R|k}$.

Observação 2.1.4. Um corpo perfeito é um corpo em que todas as raízes p-ésimas de seus elementos estão nele, ou seja, $k = k^p$

Seja $k[R^{p^s}]$ a k-subálgebra de R gerada pelas p^s-ésimas potências de todos os elementos de R.

Teorema 2.1.5. *Se R é $k[R^p]$-módulo finitamente gerado, então*

$$D_{R|k} = \bigcup_s \mathrm{End}_{k[R^{p^s}]}(R).$$

Demonstração. A demonstração está no Apêndice C. □

O anel R é chamado *F-finito*, se R é finitamente gerado como R^p-módulo. Daí, $D_R = D_{R|(\mathbb{Z}/p\mathbb{Z})}$ e $(\mathbb{Z}/p\mathbb{Z})[R^{p^s}] = R^{p^s}$. Segue que, se R é F-finito, então

$$D_R = \bigcup_s D_R^{(s)}.$$

Exemplo 2.1.6. Se $R = k[x_1, ..., x_d]$ é o anel de polinômios sobre um corpo k de característica $p > 0$, então $D_{R|k}$ é a extensão de R gerada pelos operadores diferenciais $D_{t,i} = \frac{1}{t!}\frac{\partial^t}{\partial x_i^t}$, onde $\frac{\partial^t}{\partial x_i^t}$ é a t-ésima derivação parcial k-linear de x_i, isto é, $D_{t,i}(x_i^n) = 0$ se $n < t$ e $D_{t,i}(x_i^n) = \binom{n}{t} x_i^{n-t}$ se $n \geq t$.

De fato, R é um $k[R^{p^s}]$-módulo livre de posto dp^s, cujos geradores livres são os monômios $x_1^{i_1} \cdots x_d^{i_d}$, onde $0 \leq i_j \leq p^s - 1$, para todo j. Seja $\delta_{i_1,...,i_d}^{i'_1,...,i'_d} : R \to R$ o mapa

$k[R^{p^s}]$-linear que manda o gerador livre $x_1^{i_1}\cdots x_d^{i_d}$ no gerador livre $x_1^{i'_1}\cdots x_d^{i'_d}$ e manda os outros geradores livres, acima mencionados, em zero. Claramente, $\mathrm{End}_{k[R^{p^s}]}(R)$ é gerado por esses elementos $\delta_{i_1,\ldots,i_d}^{i'_1,\ldots,i'_d}$ como $k[R^{p^s}]$-módulo. Não é difícil checar que

$$\delta_{p^s-1,\ldots,p^s-1}^{0,\ldots,0} = D_{p^s-1,1}\cdots D_{p^s-1,d}.$$

Isso implica que

$$\delta_{i_1,\ldots,i_d}^{i'_1,\ldots,i'_d} = x_1^{i'_1}\cdots x_d^{i'_d} D_{p^s-1,1}\cdots D_{p^s-1,d} x_1^{p^s-1-i_1}\cdots x_d^{p^s-1-i_d}$$

para todo $\delta_{i_1,\ldots,i_d}^{i'_1,\ldots,i'_d}$. Logo, se k é perfeito, isto é, $\bigcup_s D_R^{(s)} = D_R = D_{R|k}$, então $D_R^{(s)}$ é a extensão de R gerada pelos operadores $D_{t,i}$ com $t < p^s$.

2.2 O Funtor Frobenius

Definimos aqui o funtor Frobenius e listamos algumas propriedades que serão utilizadas nas próximas seções. E por fim, damos uma condição para que o funtor Frobenius seja exato.

Seja R um anel comutativo de característica $p > 0$. O *homomorfismo de Frobenius* é o mapa $F_R : R \to R$, dado por $F_R(r) = r^p$. Via F_R, podemos considerar R como uma R-álgebra de maneira não-trivial. O ponto crucial na construção do funtor Frobenius é tratar R com duas estruturas de R-módulo essencialmente diferentes. Denotamos por $R^{(s)}$ o R-R-bimódulo que, como R-módulo à esquerda é R, e a estrutura à direita é dada pela s-ésima iteração do homomorfismo de Frobenius: para $a \in R^{(s)}$ e $r \in R$, temos $a \cdot r = F^s(r)a = r^{p^s}a$, para s inteiro positivo.

Seja M um R-módulo (à esquerda). Então tomamos o produto tensorial $R^{(s)} \otimes_R M$, com $R^{(s)}$ como um R-módulo à direita, isto é

$$a \otimes rx = a \cdot r \otimes x = r^{p^s} a \otimes x$$

onde $a \in R^{(s)}$, $r \in R$ e $x \in M$. A estrutura de R-módulo à esquerda de $R^{(s)}$ induz em $R^{(s)} \otimes_R M$ uma estrutura de R-módulo à esquerda, dado por $r(a \otimes x) = ra \otimes x$.

Observação 2.2.1. Este produto tensorial é meramente biaditivo, a bilinearidade é perdida porque em geral $a \cdot r \neq ra$, para $a \in R^{(s)}$ e $r \in R$.

Definição 2.2.2. O *funtor Frobenius* é o funtor da categoria de R-módulos nela mesma

$$F_R^* : R\text{−mod} \longrightarrow R\text{−mod}$$

que manda M em $F_R^*(M) = R^{(1)} \otimes_R M$, e para $\varphi : M \to N$, temos $F_R^*(\varphi) = id_{R^{(1)}} \otimes_R \varphi$. E sua s-ésima iteração é $F_R^{s*}(M) = R^{(s)} \otimes M$. Se não tiver confusão, escrevemos F^{s*} em vez de F_R^{s*}.

É fácil verificar que o funtor Frobenius é um funtor covariante, exato à direita e aditivo, da categoria de R-módulos nela mesma. Queremos obter alguns resultados especificos de F^{s*}. Primeiro, vemos que $F^{s*}(R) = R^{(s)} \otimes_R R \cong R^{(s)}$ como R-módulo à esquerda, então $F^{s*}(R) \cong R$; pela aditividade temos ainda, $F^{s*}(R^n) \cong R^n$. Para um R-módulo cíclico R/I, $F^{s*}(R/I) = R^{(s)} \otimes_R R/I \cong R^{(s)}/I^{[p^s]}$, onde $I^{[p^s]}$ é o ideal gerado pelas p^s-ésimas potências dos elementos de I, visto como R-módulo. Assim, temos

Proposição 2.2.3. *Seja R um anel comutativo de característica $p > 0$. Então*

(a) *$F^{s*}(R^n) = R^n$ para todo n, e se $e_1,...,e_n$ é uma base de R^n, $1 \otimes e_1,...,1 \otimes e_n$ é uma base de $F^{s*}(R^n)$;*

(b) *$F^{s*}(R/I) = R^{(s)}/I^{[p^s]}$ para todo ideal I de R ($I^{[p^s]}$ é chamado a p^s-ésima potência Frobenius de I).*

Proposição 2.2.4. *Seja R um anel comutativo de característica $p > 0$, M e N R-módulos, e $\varphi : M \to N$ um mapa R-linear. Então*

(a) *$F^{s*}(r\varphi) = r^{p^s} F^{s*}(\varphi)$ para todo $r \in R$;*

(b) *Se $\varphi(x) = \sum r_i y_i$ para $x \in M$, $r_i \in R$, $y_i \in N$, então $F^{s*}(\varphi)(1 \otimes x) = \sum r_i^{p^s}(1 \otimes y_i)$;*

(c) *O mapa $M \to F^{s*}(M)$, dado por $x \mapsto 1 \otimes x$, não é linear em geral, mas $(rx) \mapsto r^{p^s}(1 \otimes x)$.*

Proposição 2.2.5. *$F^{s*}(F^{t*}(N)) \cong F^{(t+s)*}(N)$, para todo R-módulo N.*

Demonstração. Consideremos os mapas

$$\Phi : R^{(s)} \otimes_R (R^{(t)} \otimes_R N) \to R^{(t+s)} \otimes_R N$$

dado por $a \otimes (b \otimes n) \mapsto ab^{p^s} \otimes n$, e

$$\Psi : R^{(t+s)} \otimes_R N \to R^{(s)} \otimes_R (R^{(t)} \otimes_R N)$$

dado por $a \otimes n \mapsto a \otimes (1 \otimes n)$. Seja $a \otimes (b \otimes n) \in R^{(s)} \otimes_R (R^{(t)} \otimes_R N)$, então

$$\begin{aligned} \Psi(\Phi(a \otimes (b \otimes n))) &= \Psi(ab^{p^s} \otimes n) \\ &= ab^{p^s} \otimes (1 \otimes n) \\ &= a \otimes (b(1 \otimes n)) \\ &= a \otimes (b \otimes n). \end{aligned}$$

Agora seja $a \otimes n \in R^{(t+s)} \otimes_R (N)$, então

$$\Phi(\Psi(a \otimes n)) = \Phi(a \otimes (1 \otimes n)) = a \otimes n.$$

É fácil verificar que estão bem definidos. □

Podemos agora dar uma descrição de F^{s*} em termos de geradores e relações.

Proposição 2.2.6. *Seja R um anel comutativo de característica $p > 0$ e M um R-módulo de apresentação finita, digamos $R^m \xrightarrow{\varphi} R^n \to M \to 0$. Então:*

(a) *$F^{s*}(M)$ é R-módulo de apresentação finita; ainda mais, $R^m \overset{F^{s*}(\varphi)}{\to} R^n \to F^{s*}(M) \to 0$ é exata;*

(b) *Mais ainda, se φ é dado pela matriz (r_{ij}), então $F^{s*}(\varphi)$ é dado pela matriz $(r_{ij}^{p^s})$.*

A parte (a) segue do fato que F^{s*} é exato à direita e $F^{s*}(R^n) = R^n$. E a parte (b) segue da proposição anterior.

A próxima proposição trata do comportamento do funtor Frobenius com relação a localização.

Proposição 2.2.7. *Seja R um anel comutativo de característica $p > 0$. O funtor Frobenius comuta com anéis de fração: $S^{-1}F_R^{t*}(M) = F_{S^{-1}R}^{t*}(S^{-1}M)$ para todo R-módulo M, e analogamente para mapas R-lineares.*

Demonstração. Note que no enunciado da proposição o produto tensorial citado é R-bilinear, e M um R-módulo.

Temos que

$$S^{-1}F_R^{t*}(M) = S^{-1}R \otimes_R F_R^{t*}(M) = S^{-1}R \otimes_R (R^{(t)} \otimes_R M) = (S^{-1}R \otimes R^{(t)}) \otimes_R M,$$

e

$$F_{S^{-1}R}^{t*}(S^{-1}M) = F_{S^{-1}R}^{t*}(S^{-1}R \otimes_R M) = (S^{-1}R)^{(t)} \otimes_R (S^{-1}R \otimes_R M) =$$
$$((S^{-1}R)^{(t)} \otimes_R S^{-1}R) \otimes_R M = (S^{-1}R)^{(t)} \otimes_R M.$$

Como $S^{-1}R$-módulos, $S^{-1}R \otimes_R R^{(t)} \cong S^{-1}R \otimes_R R \cong S^{-1}R$ e $(S^{-1}R)^{(t)}$ são naturalmente isomorfos. Esse isomorfismo é também um isomorfismo de R-módulos à direita, tomando $(x/s \otimes a) \cdot r = x/s \otimes ra$, lembrando que este produto tensorial é o do enunciado, ou seja, R-bilinear. □

Concluímos nossa lista com a chamada *planitude de Frobenius*.

Teorema 2.2.8 (Kunz)**.** *Seja R é anel regular de característica p. Então $R^{(s)}$ é R-módulo à direita plano; equivalentemente, a s-ésima iteração do funtor Frobenius é exata, para todo s.*

Já vimos que o funtor Frobenius é exato à direita, e pela hipótese de R ser regular, temos que $R^{(s)}$ é R-módulo à direita plano, pelo Teorema 2.1 de [**?**], portanto garantimos a exatidão à esquerda de F^*, e também de F^{s*}, para todo $s \in \mathbb{N}$. A prova desse fato também é dada no corolário 8.2.8 de [**?**].

2.3 Definição e propriedades básicas de $R[F]$-módulos unitários

Nesta seção, R é um anel comutativo regular de característica $p > 0$. Serão dadas a definição e as propriedades básicas de $R[F]$-módulos unitários, e que esta estrutura induz uma estrutura natural de D_R-módulo. Damos uma condição para que um $R[F]$-módulo unitário seja finitamente gerado. Exibimos a estrutura de $R[F]$-módulo unitário de R_f e vemos que a estrutura natural de D_R-módulo induzida, é a mesma do exemplo 1.1.2(b). Depois mostramos que R_f é $R[F]$-gerado por $\frac{1}{f}$. Concluímos esta seção com um resultado importante sobre $R[F]$-módulos unitários finitamente gerados, que eles tem comprimento finito na categoria de D_R-módulos, ou seja, R_f tem comprimento finito na categoria de D_R-módulos, para uma classe de anéis R.

Definição 2.3.1. Um $R[F^s]$-*módulo* é um R-módulo M, junto com um mapa R-linear

$$\vartheta_M^s : F^{s*}M \to M,$$

com $F^{s*}M = R^{(s)} \otimes_R M$, como na seção 1.2.

Um morfismo entre dois $R[F^s]$-módulos (M, ϑ_M^s) e (N, ϑ_N^s) é um mapa R-linear $\varphi : M \to N$, tal que o seguinte diagrama comuta:

$$\begin{tikzcd} F^{s*}M \arrow[r, "F^{s*}(\varphi)"] \arrow[d, "\vartheta_M^s"'] & F^{s*}N \arrow[d, "\vartheta_N^s"] \\ M \arrow[r, "\varphi"] & N \end{tikzcd}$$

A categoria de todos os $R[F^s]$-módulos junto com seus morfismos, será denotada por $R[F^s]$-mod.

De outra maneira, podemos obter o anel $R[F^s]$ como a extensão de R gerada pela variável F^s, sujeita às relações $F^s r = r^{p^s} F^s$, para todo $r \in R$. Claramente, um módulo M sobre o anel $R[F^s]$ é um R-módulo com um mapa aditivo de grupos abelianos $F_M^s : M \to M$ tal que $F_M^s \circ \tilde{r} = \tilde{r}^{p^s} \circ F_M^s$, onde $\tilde{r} : M \to M$ é a multiplicação por r. Então um $R[F^s]$-módulo, como definido neste parágrafo, é apenas um módulo sobre este anel (não-comutativo) $R[F^s]$. Mais precisamente, vamos mostrar que essas duas definições são equivalentes.

Proposição 2.3.2. *A categoria $R[F^s]$-mod é equivalente à categoria de módulos sobre o anel $R[F^s]$.*

Demonstração. Seja M um módulo sobre o anel $R[F^s]$. Então M é um R-módulo com um mapa aditivo de grupos abelianos $F_M^s : M \to M$, tal que $F_M^s \circ \tilde{r} = \widetilde{r^{p^s}} \circ F_M^s$, para todo $r \in R$. Daí, os módulos sobre o anel $R[F^s]$ podem ser associados aos pares (M, ϑ_M^s), onde $\vartheta_M^s : F^{s*}M \to M$, é dada por $r \otimes m \mapsto rF_M^s(m)$, que é R-linear. Sejam M e N dois módulos sobre o anel $R[F^s]$, e $\varphi : M \to N$ um mapa $R[F^s]$-linear, portanto R-linear. Temos

$$\vartheta_N^s(F^{s*}(\varphi)(r \otimes m)) = \vartheta_N^s(r \otimes \varphi(m)) = rF_N^s(\varphi(m)).$$

Por outro lado,

$$\varphi(\vartheta^s_M(r\otimes m)) = \varphi(rF^s_M(m)) = r\varphi(F^s_M(m)).$$

Como φ é $R[F^s]$-linear, segue que o mapa abaixo comuta

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "F^s_M"'] & N \arrow[d, "F^s_N"] \\ M \arrow[r, "\varphi"] & N \end{tikzcd}$$

Assim, cada módulo sobre o anel $R[F^s]$ está associado a um módulo em $R[F^s]$-mod. Seja (M,ϑ^s_M) em $R[F^s]$-mod. Damos uma estrutura de módulo sobre o anel $R[F^s]$, tomando M com o mapa $F^s_M : M \to M$, que manda m em $\vartheta^s_M(1\otimes m)$. De fato, para $r\in R$ e $m \in M$, temos:

$$F^s_M(rm) = \vartheta^s_M(1\otimes rm) = \vartheta^s_M(r^{p^s}\otimes m) = \vartheta^s_M(r^{p^s}(1\otimes m)) = r^{p^s}\vartheta^s_M(1\otimes m) = r^{p^s}F^s_M(m),$$

portanto, $F^s_M \circ \tilde{r} = \widetilde{r^{p^s}} \circ F^s_M$.

Seja $\varphi : M \to N$ morfismo em $R[F^s]$-mod. Este mapa está em correspondência com o mapa $\varphi : M \to N$, de módulos sobre o anel $R[F^s]$, se $F^s_N \circ \varphi = \varphi \circ F^s_M$. Assim,

$$F^s_N(\varphi(m)) = \vartheta^s_N(1\otimes\varphi(m)) = \vartheta^s_N(F^{s*}(\varphi)(1\otimes m)) = \varphi(\vartheta^s_M(1\otimes m)) = \varphi(F^s_M(m)).$$

□

Definição 2.3.3. Um $R[F^s]$-módulo (M,ϑ^s) é chamado $R[F^s]$-*módulo unitário* se

$$\vartheta^s : F^{s*}M \to M$$

é um isomorfismo.

Exemplo 2.3.4. (a) Sabendo que $F^{s*}R$ é isomorfo à R como R-módulos, temos que R é um $R[F^s]$-módulo unitário, sendo $F^s_R : R \to R$, que manda $r \in R$ em r^{p^s}. Um ideal $I \subset R$ é um $R[F^s]$-submódulo de R, visto que $F^{s*}I = I^{[p^s]} \subset I$. Em geral, I não é um $R[F^s]$-módulo unitário, pois a inclusão $I^{[p^s]} \subset I$ é geralmente estrita.

(b) Seja $S \subset R$ um subconjunto multiplicativamente fechado de R. Então $S^{-1}R$ é naturalmente um $R[F^s]$-módulo unitário, onde $\vartheta^s_{S^{-1}R} : F^{s*}(S^{-1}R) \to S^{-1}R$ manda $r'\otimes\frac{r}{s}$ em $\frac{r'r^{p^s}}{s^{p^s}}$, note que $F^s_{S^{-1}R} : S^{-1}R \to S^{-1}R$, manda $x \in S^{-1}R$ em x^{p^s}. O mapa inverso é dado por $\frac{r}{s} \mapsto s^{p^s-1}r\otimes\frac{1}{s}$. Mais ainda, o mapa natural $R \to S^{-1}R$ é um mapa de $R[F^s]$-módulos unitários.

Um $R[F^s]$-módulo unitário carrega uma estrutura natural de $\bigcup_s D^{(s)}_R$-módulo, e portanto, de D_R-módulo pois D_R é subanel de $\bigcup_s D^{(s)}_R = \bigcup_s \mathrm{End}_{R^{p^s}}(R)$.

Considere,

$$\vartheta^{(s)}_l = F^{s(l-1)*}((\vartheta^s_M)^{-1}) \circ F^{s(l-2)*}((\vartheta^s_M)^{-1}) \circ \cdots \circ (\vartheta^s_M)^{-1} : M \longrightarrow F^{(sl)*}M.$$

Todo $u \in D_R^{(sl)}$ atua em $F^{(sl)*}M = R^{(sl)} \otimes_R M$ via $u \otimes_R id_M$. Assim, u age em M via $(\vartheta_l^{(s)})^{-1} \circ (u \otimes_R id_M) \circ \vartheta_l^{(s)}$. Esta ação está bem-definida, isto é, ela só depende de u, e não de l.

De fato, seja $l' > l$. queremos mostrar que

$$(\vartheta_l^{(s)})^{-1} \circ (u \otimes_R id_M) \circ \vartheta_l^{(s)} = (\vartheta_{l'}^{(s)})^{-1} \circ (u \otimes_R id_M) \circ \vartheta_{l'}^{(s)}.$$

Visto que $\vartheta_{l'}^{(s)} = \theta_{l'-l}^{l} \circ \vartheta_l^{(s)}$, onde

$$\theta_{l'-l}^{l} = F^{s(l'-1)*}((\vartheta_M^s)^{-1}) \circ \cdots \circ F^{(sl)*}((\vartheta_M^s)^{-1}) : F^{(sl)*}(M) \to F^{(sl')*}(M),$$

isto reduz a checar que

$$u \otimes_R id_M = (\theta_{l'-l}^{l})^{-1} \circ (u \otimes_R id_M) \circ \theta_{l'-l}^{l}, \;\; em \;\; F^{(sl)*}(M).$$

Note que

$$\theta_{l'-l}^{l} = F^{(sl)*}(\vartheta_{l'-l}^{(s)}) = id_{R^{(sl)}} \otimes_R \vartheta_{l'-l}^{(s)} : R^{(sl)} \otimes_R M \to R^{(sl)} \otimes_R F^{s(l'-l)*}(M)$$

e daí a ação de u em $F^{(sl')*}M = R^{(sl')} \otimes_R M$ via $u \otimes_R id_M$ é a mesma ação em $F^{(sl')*}M = F^{(sl)*}(F^{s(l'-l)*}M) = R^{(sl)} \otimes_R F^{s(l'-l)*}M$, via $u \otimes_R id_{F^{s(l'-l)*}M}$, pois u é $R^{p^{sl}}$-linear, e assim, basta ver que

$$u \otimes_R id_M = (id_{R^{(sl)}} \otimes_R \vartheta_{l'-l}^{(s)})^{-1} \circ (u \otimes_R id_{F^{s(l'-l)*}M}) \circ (id_{R^{(sl)}} \otimes_R \vartheta_{l'-l}^{(s)})$$

que é claro.

Exemplo 2.3.5. A estrutura usual de D_R-módulo de R_f (exemplo 1.1.2(b)) é a mesma estrutura, definida acima, induzida pela estrutura de $R[F]$-módulo unitário $F : R_f \to R_f$ de R_f, que manda $x \in R_f$ em x^p.

De fato,

$$\vartheta_t = F^{(t-1)*}(\vartheta^{-1}) \circ F^{(t-2)*}(\vartheta^{-1}) \circ \cdots \circ \vartheta^{-1} : R_f \to F^{t*}R_f,$$

onde $\vartheta : F^*R_f \to R_f$ é dado por $\vartheta(a \otimes \frac{r}{s}) = aF(\frac{r}{s}) = \frac{ar^p}{s^p}$, ou seja, a estrutura de $R[F]$-módulo unitário de R_f. Temos ainda que $\vartheta^{-1}(\frac{r}{s}) = s^{p-1} \otimes \frac{1}{s}$. Assim,

$$\vartheta_t\left(\frac{r}{s}\right) = s^{p^t-1} r \otimes \frac{1}{s}$$

e

$$\vartheta_t^{-1}\left(a \otimes \frac{r}{s}\right) = \frac{ar^{p^t}}{s^{p^t}},$$

pelo fato que $F^*(F^*R_f) \cong F^{(2)*}R_f$ via $a \otimes (b \otimes \frac{r}{s}) \mapsto ab^p \otimes \frac{r}{s}$ (Proposição 1.2.5).

Seja $\delta \in D_R^{(t)}$ e $\frac{r}{s} \in R_f$, então

$$\begin{aligned}
\delta \cdot \frac{r}{s} &= \vartheta_t^{-1} \circ (\delta \otimes_R id_{R_f}) \circ \vartheta_t\left(\frac{r}{s}\right) \\
&= \vartheta_t^{-1} \circ (\delta \otimes_R id_{R_f})\left(s^{p^t-1} r \otimes \frac{1}{s}\right) \\
&= \vartheta_t^{-1}\left(\delta(s^{p^t-1} r) \otimes \frac{1}{s}\right) \\
&= \frac{\delta(s^{p^t-1} r)}{s^{p^t}}
\end{aligned}$$

que é a estrutura usual de D_R-módulo de R_f, visto que $[s^{p^t}, \delta] = 0$, pois δ é R^{p^s}-linear.

Seja (M, ϑ^s) um $R[F^s]$-módulo e N um R-submódulo de M. Então o conjunto $F^s(N)$ é um subconjunto de M consistindo dos elementos $\{F^s(n); n \in N\}$. Por abuso de notação, $F^s(N)$ irá denotar o R-submódulo de M gerado por esse conjunto. Como $F^{s*}N \subset F^{s*}M$, pois R é regular (Proposição 1.2.8), temos que $F^s(N) = \vartheta^s(F^{s*}N)$.

Proposição 2.3.6. *Seja (M, ϑ^s) um $R[F^s]$-módulo tal que ϑ^s é sobrejetivo. Então M é finitamente gerado como $R[F^s]$-módulo se, e somente se, existe um R-módulo finitamente gerado M_0 tal que $M_0 \subseteq F^s(M_0)$ e $M = \bigcup_l F^{sl}(M_0)$.*

Demonstração. Vamos começar com a volta. Primeiro note que a imagem dos R-geradores de M_0 são R-geradores de $F^{sl}(M_0)$, via F^{sl}. Isto implica que $M = \bigcup_l F^{sl}(M_0)$ é gerado como $R[F^s]$-módulo pelos R-geradores de M_0.

Reciprocamente, assuma que M é finitamente gerado como $R[F^s]$-módulo. Seja M' o R-módulo gerado por um conjunto finito de geradores de M como $R[F^s]$-módulo. Em outras palavras,

$$R[F^s]M' = \sum_{l=0}^{\infty} F^{sl}(M') = M,$$

com $F^0(M') = M'$. Visto que ϑ^s é sobrejetiva, temos que $M = F^s(M)$. Aplicando F^s à igualdade acima obtemos $M = F^s(M) = F^s(\sum_{l=0}^{\infty} F^{sl}(M')) = \sum_{l=1}^{\infty} F^{sl}(M')$. Como M' é finitamente gerado, então está contido em uma parte finita desta soma, digamos $M' \subseteq \sum_{l=1}^{t} F^{sl}(M')$. Agora, chame $M_0 = \sum_{l=0}^{t-1} F^{sl}(M')$ e veja que $M_0 \subseteq F^s(M_0)$ e também

$$M_0 \subseteq F^s(M_0) \subseteq F^{2s}(M_0) \subseteq F^{3s}(M_0) \subseteq \cdots$$

cuja união é M, pois M' está contido em M_0. □

Definição 2.3.7. Um R-submódulo M_0 de um $R[F^s]$-módulo unitário M é dito ser uma *raiz*, se M_0 é finitamente gerado como R-módulo, $M_0 \subseteq F^{s*}(M_0)$ e $\bigcup_l F^{(sl)*}(M_0) = M$.

Pela Proposição 1.3.6, a existência de uma raiz para um $R[F^s]$-módulo unitário M é equivalente a dizer que M é finitamene gerado como um $R[F^s]$-módulo unitário, visto que $F^{(sl)*}(M_0)$ é isomorfo à $F^{sl}(M_0)$ via ϑ^{sl}. Assim,

Corolário 2.3.8. *Seja M é um $R[F^s]$-módulo unitário. Então, M é finitamente gerado como $R[F^s]$-módulo se, e somente se, M possui uma raiz.*

Exemplo 2.3.9. R_f é gerado por $\frac{1}{f}$ como $R[F]$-módulo unitário, ou seja, R_f tem como raiz o R-submódulo gerado por $\frac{1}{f}$. De fato, temos que $R\cdot\frac{1}{f} \subseteq F^*(R\cdot\frac{1}{f}) = R\cdot\frac{1}{f^p}$, pois $f^{p-1}\in R$, $f^{p-1}\cdot\frac{1}{f^p} = \frac{1}{f}$. Visto que $\frac{1}{f^{p^s}} \in F^{s*}(R\cdot\frac{1}{f})$ para todo s, temos $\bigcup_s F^{s*}(R\cdot\frac{1}{f}) = R_f$. Assim, o R-submódulo gerado por $\frac{1}{f}$ é uma raiz de R_f. Pelo corolário anterior, R_f é $R[F]$-módulo unitário finitamente gerado, mais ainda, pela demonstração da Proposição 1.3.6, $\frac{1}{f}$ é $R[F]$-gerador de R_f.

Por fim, concluímos esta seção com enunciando o teorema, que será de grande importância.

Teorema 2.3.10 (Lyubeznik)**.** *Seja R uma álgebra finitamente gerada sobre um anel local regular Noetheriano F-finito A de característica $p>0$. Um $R[F]$-módulo unitário finitamente gerado M tem comprimento finito na categoria de D_R-módulos. Em particular, R_f com sua estrutura usual de D_R-módulo tem comprimento finito na categoria de D_R-módulos, para todo $f\in R$.*

Demonstração. A demonstração desse teorema é dada em [**?**], Corolário 5.8. □

2.4 Descida de Frobenius

Esta seção é baseada no Capítulo 3.2 de [**?**]. Começamos expondo uma forma simples da Descida de Frobenius, para um anel R e a álgebra das matrizes $n\times n$ com entradas em R. De maneira análoga a essa versão, mostramos uma equivalência entre a categoria de R-módulos e a categoria de $D_R^{(s)}$-módulos, e depois que a s-ésima iteração do funtor Frobenius F^{s*} é uma equivalência da categoria de D_R-módulos nela mesma, para todo s. No final, obtemos que a estrutura de $R[F]$-módulos unitários ϑ é um mapa de D_R-módulos.

A forma básica da descida de Frobenius usada aqui se baseia no fato que o anel R e a álgebra das matrizes $n\times n$ com entradas em R são equivalentes à Morita, isto é, a categoria dos módulos sobre R é equivalente à categoria dos módulos sobre $\mathrm{Mat}_{n\times n}(R)$. Sabemos que $\mathrm{Mat}_{1\times n}(R)$, a linha de comprimento n com entradas em R (respectivamente $\mathrm{Mat}_{n\times 1}(R)$, a coluna de comprimento n com entradas em R), é um R-$\mathrm{Mat}_{n\times n}(R)$-bimódulo (respectivamente um $\mathrm{Mat}_{n\times n}(R)$-$R$-bimódulo) e os mapas

$$\mathrm{Mat}_{1\times n}(R)\otimes_{\mathrm{Mat}_{n\times n}(R)}\mathrm{Mat}_{n\times 1}(R)\to R$$

e

$$\mathrm{Mat}_{n\times 1}(R)\otimes_R\mathrm{Mat}_{1\times n}(R)\to\mathrm{Mat}_{n\times n}(R),$$

que mandam $A\otimes B$ no produto de matrizes AB, são isomorfismos de R-módulos e de $\mathrm{Mat}_{n\times n}(R)$-módulos, respectivamente. Daí, os funtores

$$\mathrm{Mat}_{1\times n}(R)\otimes_{\mathrm{Mat}_{n\times n}(R)}(-):\mathrm{Mat}_{n\times n}(R)-\mathrm{mod}\to R-\mathrm{mod}$$

e

$$\mathrm{Mat}_{n\times 1}(R)\otimes_R(-):R-\mathrm{mod}\to \mathrm{Mat}_{n\times n}(R)-\mathrm{mod}$$

são inversos e estabelecem uma equivalência de categorias.

De fato, para M um R-módulo (à esquerda), e para N um $\mathrm{Mat}_{n\times n}(R)$-módulo, temos

$$\begin{aligned}\mathrm{Mat}_{1\times n}(R)\otimes_{\mathrm{Mat}_{n\times n}(R)}[\mathrm{Mat}_{n\times 1}(R)\otimes_R M] &= [\mathrm{Mat}_{1\times n}(R)\otimes_{\mathrm{Mat}_{n\times n}(R)}\mathrm{Mat}_{n\times 1}(R)]\otimes_R M\\ &= R\otimes_R M\\ &= M\end{aligned}$$

e

$$\begin{aligned}\mathrm{Mat}_{n\times 1}(R)\otimes_R[\mathrm{Mat}_{1\times n}(R)\otimes_{\mathrm{Mat}_{n\times n}(R)}N] &= [\mathrm{Mat}_{n\times 1}(R)\otimes_R \mathrm{Mat}_{1\times n}(R)]\otimes_{\mathrm{Mat}_{n\times n}(R)}N\\ &= \mathrm{Mat}_{n\times n}(R)\otimes_{\mathrm{Mat}_{n\times n}(R)}N\\ &= N.\end{aligned}$$

Seja $R^{(s)}$ como definido na seção 1.2. Como R tem estrutura de $D_R^{(s)}$-módulo à esquerda, temos que $R^{(s)}$ tem estrutura de $D_R^{(s)}$-R-bimódulo.

De fato, para $r\in R$, $r'\in R^{(s)}$ e $\delta\in D_R^{(s)}$, temos

$$\begin{aligned}\delta\cdot(r'\cdot r) &= \delta(r^{p^s}r')\\ &= r^{p^s}\delta(r')\\ &= (\delta\cdot r')\cdot r,\end{aligned}$$

devido δ ser R^{p^s}-linear.

Definimos uma estrutura de R-$D_R^{(s)}$-bimódulo em $\mathrm{Hom}_R^r(R^{(s)},R)$, onde Hom^r denota os homomorfismos na categoria de R-módulos à direita, como segue. Para $\delta\in D_R^{(s)}$, $\varphi\in \mathrm{Hom}_R^r(R^{(s)},R)$ e $r\in R$ o produto $r\cdot\varphi\cdot\delta$ é a composição $\tilde r\circ\varphi\circ\delta$, onde δ age à esquerda em $R^{(s)}$ e $\tilde r$ é a multiplicação por r em R. A identificação de $D_R^{(s)}$ com $\mathrm{Hom}_R^r(R^{(s)},R^{(s)})$ mostra que $\tilde r\circ\varphi\circ\delta$ está em $\mathrm{Hom}_R^r(R^{(s)},R)$.

Daí, temos os funtores

$$F^{s*}(-)=R^{(s)}\otimes_R(-):R-\mathrm{mod}\to D_R^{(s)}-\mathrm{mod}$$

e

$$T^s(-)=\mathrm{Hom}_R^r(R^{(s)},R)\otimes_{D_R^{(s)}}(-):D_R^{(s)}-\mathrm{mod}\to R-\mathrm{mod}.$$

O primeiro é a s-ésima iteração do funtor Frobenius de R-módulos em $D_R^{(s)}$-módulos, pois $R^{(s)}$ tem estrutura de $D_R^{(s)}$-módulo à esquerda. O segundo, dado um $D_R^{(s)}$-módulo à esquerda N, $T^sN = \mathrm{Hom}^r_R(R^{(s)}, R) \otimes_{D_R^{(s)}} N$ é o produto tensorial com $\mathrm{Hom}^r_R(R^{(s)}, R)$ como um $D_R^{(s)}$-módulo à direita, e devido a estrutura de R-módulo à esquerda de $\mathrm{Hom}^r_R(R^{(s)}, R)$, T^sN é um R-módulo.

Proposição 2.4.1 (Descida de Frobenius)**.** *Se R é regular e F-finito, os funtores $F^{s*}(-)$ e $T^s(-)$ são inversos. Consequentemente, eles induzem uma equivalência entre a categoria de R-módulos e a categoria de $D_R^{(s)}$-módulos.*

Demonstração. Seja
$$\Phi : R^{(s)} \otimes_R \mathrm{Hom}^r_R(R^{(s)}, R) \to D_R^{(s)}$$
que manda $a \otimes \varphi$ em $\tilde{a} \circ F^s \circ \varphi$, onde $\tilde{a}$ é a multiplicação à esquerda por a, e $F^s : R \to R^{(s)}$ é o mapa de R-módulos à direita induzido pela s-ésima iteração do homomorfismo Frobenius de R, dado por $F^s(r) = 1 \cdot r \; (= r^{p^s})$.

Seja $r \in R$ e $r' \in R^{(s)}$. Então

$$\begin{aligned}
(\tilde{a} \circ F^s \circ \varphi)(r' \cdot r) &= aF^s(\varphi(r' \cdot r)) \\
&= a\varphi(r' \cdot r)^{p^s} \\
&= ar^{p^s}\varphi(r')^{p^s} \\
&= (a\varphi(r')^{p^s}) \cdot r \\
&= (\tilde{a} \circ F^s \circ \varphi)(r') \cdot r
\end{aligned}$$

portanto, $\tilde{a} \circ F^s \circ \varphi \in D_R^{(s)}$, e Φ está bem-definido.

Seja também
$$\Psi : \mathrm{Hom}^r_R(R^{(s)}, R) \otimes_{D_R^{(s)}} R^{(s)} \to R$$
que manda $\varphi \otimes a$ em $\varphi(a)$.

Para mostrar que $F^{s*}(-)$ e $T^s(-)$ são inversos, é suficiente mostrar que os mapas Φ e Ψ são isomorfismos. E, Φ e Ψ são isomorfos se, e somente se, eles são localmente isomorfos.

Lema 2.4.2. *$R^{(s)}$ é R-módulo à direita localmente livre de posto finito.*

Demonstração. Pelo Teorema 1.2.8, $R^{(s)}$ é R-módulo à direita plano, e finitamente gerado, pois R é F-finito. Assim, localmente, $R^{(s)}$ é livre e de posto finito, vide [**?**] Thm. 7.10. □

Como $R^{(s)}$ é finitamente gerado como R-módulo à direita, temos que $\mathrm{Hom}^r_R(R^{(s)}, R)$ e $D_R^{(s)} = \mathrm{Hom}^r_R(R^{(s)}, R^{(s)})$ comutam com localização, vide [**?**] Thm. 7.11. Pelo lema acima, podemos assumir $R^{(s)}$ como um R-módulo livre de posto finito. Fixada uma R-base de $R^{(s)}$, podemos tratar $R^{(s)}$ como uma matriz linha com entradas em R representando os elementos de $R^{(s)}$ com respeito a essa R-base, e $\mathrm{Hom}^r_R(R^{(s)}, R)$ como a matriz coluna, com respeito a base dual, e ainda, $D_R^{(s)}$ é a álgebra das matrizes sobre

R. Basta ver que os mapas Φ e Ψ agem como o produto matricial, para que $R^{(s)}$ e $D_R^{(s)}$ sejam Morita equivalentes, e assim terminamos a demonstração.

Sejam $\{e_1, e_2, ...\}$ R-base para $R^{(s)}$ e $\{e_1^*, e_2^*, ...\}$ R-base dual para $\mathrm{Hom}_R^r(R^{(s)}, R)$. Assim, basta ver que

$$\Phi(e_i \otimes e_j^*)(e_k) = \begin{cases} e_i, & se\, j = k \\ 0, & se\, j \neq k \end{cases}$$

e

$$\Psi(e_j^* \otimes e_i) = \begin{cases} 1, & se\, j = i \\ 0, & se\, j \neq i \end{cases},$$

que é de fácil verificação. □

A proposição acima implica que as categorias de $D_R^{(s)}$-módulos, para todo s, são equivalentes, visto que cada uma delas é equivalente a R-mod. O funtor que dá a equivalência entre $D_R^{(t)}$-mod e $D_R^{(t+s)}$-mod é F^{s*}, ou seja,

$$F^{s*}(-) : D_R^{(t)}\text{–mod} \to D_R^{(t+s)}\text{–mod}$$

$$M \mapsto F^{s*}(M) = R^{(s)} \otimes_R M$$

Para entender melhor a estrutura de $D_R^{(t+s)}$-módulo em $F^{s*}(M)$, para um $D_R^{(t)}$-módulo M, escrevemos $M \cong F^{t*}(N)$, com $N = T^t(M)$. Portanto, $F^{s*}(M) = F^{(t+s)*}(N)$ carrega claramente um estrutura de $D_R^{(t+s)}$-módulo com $\delta \in D_R^{(t+s)}$ agindo via $\delta \otimes id_N$. Assim,

Proposição 2.4.3. *Seja R regular e F-finito. Então F^{s*} é uma equivalência da categoria de D_R-módulos nela mesma.*

Demonstração. Vimos que F^{s*} é uma equivalência entre a categoria de $D_R^{(t)}$-módulos e a categoria de $D_R^{(t+s)}$-módulos, para todo s. Visto que um D_R-módulo M é um $D_R^{(t)}$-módulo para todo t, segue que $F^{s*}M$ é um $D_R^{(t+s)}$-módulo, para todo s. Essas estruturas de vários níveis são compatíveis com a inclusão $D_R^{(t)} \subseteq D_R^{(t')}$ para $t \leq t'$, e daí temos uma estrutura natural de D_R-módulo em $F^{s*}M$. Para verificar essa compatibilidade basta lembrar que $F^{s*} \circ T^s$ é isomorfo ao funtor identidade, ou seja, $M = F^{s*}(T^s M)$ para todo s. Seja $\delta \in D_R^{(t+s)}$, vimos que a ação de δ em $F^{s*}M$ é dada pelo diagrama abaixo:

$$\begin{tikzcd} F^{(t+s)*}(T^t M) \arrow[r, equal] \arrow[d, "\delta \otimes_R id_{T^t M}"'] & F^{s*}M \arrow[d, dashed, "\delta"] \\ F^{(t+s)*}(T^t M) \arrow[r, equal] & F^{s*}M \end{tikzcd}$$

Esta ação só depende de δ e não de $t+s$. A verificação deste fato é bastante similar a compatibilidade da estrutura de D_R-módulo em um $R[F^{s*}]$-módulo unitário (seção 1.3). □

Corolário 2.4.4. *Seja R um anel regular F-finito e M um $R[F^s]$-módulo unitário. Então $\vartheta_M^s : F^{s*}M \to M$ é um mapa de D_R-módulos.*

Demonstração. Sabendo que M tem uma estrutura natural de D_R-módulo, F^*M também possui, pela Descida de Frobenius. Temos que mostrar que o mapa ϑ^s_M é D_R-linear. Considere

$$F^{(sl)*}(T^{s(l-1)}M) \cong F^{s*}M \xrightarrow{\vartheta^s_M} M \cong F^{(sl)*}(T^{sl}M)$$

onde o primeiro e o terceiro isomorfismo são de $D_R^{(sl)}$-módulos, para l inteiro não-negativo. Então, ϑ^s_M é D_R-linear se a composição desses isomorfismos é D_R-linear (Note que, por ϑ^s_M ser R-linear, essa composição é R-linear). Assim, se chamamos essa composição de Ψ, temos

$$\Psi(\delta \cdot a \otimes n) = \Psi(\delta(a) \otimes n) = \Psi(\delta(a) \cdot 1 \otimes n) = \delta(a)\Psi(1 \otimes n) =$$

$$(\delta \cdot \tilde{a}) \cdot \Psi(1 \otimes n) = \delta \cdot (a\Psi(1 \otimes n)) = \delta \cdot (\Psi(a \otimes n)),$$

para $\delta \in D_R^{(sl)}$ e $a \otimes n \in F^{sl*}(T^{s(l-1)}M)$. $\square$

Capítulo 3

Geradores de D-módulos

3.1 Uma cadeia de ideais associados a um elemento de um anel regular F-finito

Nesta seção, R é um anel regular F-finito de característica $p > 0$. Para um elemento $f \in R$ não-nulo qualquer, iremos definir uma cadeia descendente de ideais $I_s(f)$ indexado por um inteiro positivo s, e relacionar esta cadeia com a estrutura de D_R-módulo de R_f.

Vamos assumir que R é livre como R^{p^s}-módulo. Seja $\{c_1^{p^s}, c_2^{p^s}, ...\} \subset R^{p^s}$ o conjunto das coordenadas de $f \in R$ com respeito a alguma R^{p^s}-base de R. Definimos $I_s(f)$ como sendo o ideal de R gerado pelo conjunto $\{c_1, c_2, ...\}$. Essa definição independe da escolha da base, pois as coordenadas de f com respeito a uma base são combinações lineares com coeficientes de R^{p^s} das coordenadas de f com respeito a uma outra base, daí os ideais correspondentes são os mesmos.

Visto que qualquer anel R regular F-finito é R^p-módulo livre localmente finito, Spec$R$ é coberto por um número finito de abertos afins SpecR_r, com $r \in$ Spec$R$, tal que R_r é um R^p-módulo livre (e consequentemente R_r é livre como R^{p^s}-módulo, para todo s). Daí definimos $I_s(f)$ em R colando os ideais locais definidos acima. Isto é possível devido a independência de escolha de base na construção.

Uma consequência de R ser F-finito, é que o anel de operadores diferenciais de R é $\bigcup_s D_R^{(s)}$, onde $D_R^{(s)} = \mathrm{End}_{R^{p^s}}(R)$. Veremos algumas relações entre os ideais $I_s(f)$ e operadores diferenciais.

Lema 3.1.1. *$D_R(s) \cdot f = I_s(f)^{[p^s]}$, onde $D_R(s) \cdot f = \{\delta(f); \delta \in D_R^{(s)}\} \subseteq R$ e $I_s(f)^{[p^s]}$ é o ideal gerado pelas p^s-ésimas potências dos elementos de $I_s(f)$, equivalentemente, pelas p^s-ésimas potências de um conjunto gerador de $I_s(f)$.*

Demonstração. Visto que R é finitamente gerado como R^{p^s}-módulo, $D_R^{(s)} = \mathrm{End}_{R^{p^s}}(R)$ comuta com localização com respeito a qualquer subconjunto multiplicativamente fechado de R^{p^s}, vide [?] Thm. 7.11. Disto, podemos assumir que R é R^{p^s}-módulo livre. Nesse caso, $f = \sum_i c_i^{p^s} e_i$, onde $\{e_1, e_2, ...\}$ é uma R^{p^s}-base de R e $\{c_1^{p^s}, c_2^{p^s}, ...\}$ são as coordenadas de f com respeito a essa base. Visto que, $\delta(f) = \sum_i c_i^{p^s} \delta(e_i) \in I_s(f)^{[p^s]} = (c_1^{p^s}, c_2^{p^s}, ...)$ para todo $\delta \in D_R^{(s)}$, segue $D_R(s) \cdot f \subseteq I_s(f)^{[p^s]}$. Reciprocamente, seja $\delta_i \in D_R^{(s)}$ o mapa R^{p^s}-linear que manda e_i em 1 e e_j em 0, para todo $j \neq i$. Temos $\delta_i(f) = c_i^{p^s}$, isto é, todos os geradores de $I_s(f)^{[p^s]}$ estão em $D_R^{(s)} \cdot f$. □

Lema 3.1.2. $I_s(f) = I_{s+1}(f^p)$.

Demonstração. É suficiente provar para localizações em ideais maximais de R, daí assumimos que R é anel local, e temos que R é R^p-módulo livre. Como (R, m) é anel local, (R^p, m^p) é local. Pelo *lema de Nakayama*, temos que $1 \notin m^p R$, e assim podemos obter uma R^p-base de R tal que 1 faz parte, digamos $\{e_1, e_2, ...\}$, com $e_1 = 1$.

Agora seja $\{\tilde{e}_j\}$ uma R^{p^s}-base de R. Então o conjunto dos produtos $\{e_{j,i} = \tilde{e}_j{}^p e_i\}$ é uma $R^{p^{s+1}}$-base para R.

De fato, seja $r \in R$

$$
\begin{aligned}
b = \sum_i b_i^p e_i \implies b &= \sum_i \left(\sum_j b_{j,i}^{p^s} \tilde{e}_j \right)^p e_i \\
\implies b &= \sum_i \sum_j b_{j,i}^{p^{s+1}} \tilde{e}_j{}^p e_i \\
\implies b &= \sum_i \sum_j b_{j,i}^{p^{s+1}} e_{j,i},
\end{aligned}
$$

onde $b_i, b_{j,i} \in R$. Assim $\{e_{j,i}\}$ gera R como $R^{p^{s+1}}$-módulo. Seja $\sum_{i,j} c_{j,i}^{p^{s+1}} e_{j,i} = 0$, então

$$
\begin{aligned}
\sum_{i,j} c_{j,i}^{p^{s+1}} e_{j,i} = 0 \implies & \sum_{i,j} c_{j,i}^{p^{s+1}} \tilde{e}_j{}^p e_i = 0 \\
\implies & \sum_i \left(\sum_j c_{j,i}^{p^s} \tilde{e}_j \right)^p e_i = 0 \\
\implies & \sum_j c_{j,i}^{p^s} \tilde{e}_j = 0 \ , \ \ pois \ \{e_i\} \ R^p - base \ de \ R \\
\implies & c_{j,i} = 0 \ , \ \ pois \ \{\tilde{e}_j\} \ R^{p^s} - base \ de \ R,
\end{aligned}
$$

logo $\{e_{j,i}\}$ é $R^{p^{s+1}}$-base de R.

Assim, se $f = \sum_j c_j^{p^s} \tilde{e}_j$, temos $f^p = \sum_j c_j^{p^{s+1}} \tilde{e}_j{}^p$. Mas $\tilde{e}_j{}^p = \tilde{e}_j{}^p \cdot 1 = \tilde{e}_j{}^p \cdot e_1 = e_{j,1}$, daí a (j,i)-ésima coordenada de f^p com respeito a base $\{e_{j,i}\}$ é $c_j^{p^{s+1}}$ se $i = 1$, e 0 se $i \neq 1$. Portanto, $I_s(f)$ e $I_{s+1}(f^p)$ são gerados pelos mesmos elementos. □

Lema 3.1.3. *$I_s(f\tilde{f}) \subseteq I_s(f)I_s(\tilde{f}) \subseteq I_s(f)$, para todo $\tilde{f} \in R$.*

Demonstração. Como antes, assumimos que R é um R^{p^s}-módulo livre em alguma base $\{e_1, e_2, ...\}$. Multiplicando as igualdades $f = \sum_i c_i^{p^s} e_i$ e $\tilde{f} = \sum_i \tilde{c_i}^{p^s} e_i$, temos $f\tilde{f} = \sum_{i,j} c_i^{p^s} \tilde{c_j}^{p^s} e_i e_j$. Escrevendo $e_i e_j = \sum_q \bar{c_q}^{p^s} e_q$ e substituindo na igualdade anterior vemos que todas as coordenadas de $f\tilde{f}$ com respeito a base $\{e_i\}$ são combinações lineares (com coeficientes em R^{p^s}) dos produtos $c_i^{p^s} \tilde{c_j}^{p^s}$. Isto implica que $I_s(f\tilde{f})$ é gerado por combinações lineares (com coeficientes em R) dos produtos $c_i \tilde{c}_j$, daí $I_s(f\tilde{f}) \subseteq I_s(f)I_s(\tilde{f}) \subseteq I_s(f)$. □

Lema 3.1.4. *$I_{s+1}(f^{p^{s+1}-1}) \subseteq I_s(f^{p^s-1})$.*

Demonstração. Como $f^{p^{s+1}-1} = f^{p^{s+1}-p} f^{p-1}$, temos $I_{s+1}(f^{p^{s+1}-1}) \subseteq I_{s+1}(f^{p^{s+1}-p})$ pelo Lema 2.1.3. Visto que $f^{p^{s+1}-p} = (f^{p^s-1})^p$, concluímos a demonstração pelo Lema 2.1.2. □

Proposição 3.1.5. *A cadeia descendente de ideais*

$$I_1(f^{p-1}) \supseteq I_2(f^{p^2-1}) \supseteq \cdots$$

estabiliza em s, isto é, $I_s(f^{p^s-1}) = I_{s+1}(f^{p^{s+1}-1}) = I_{s+2}(f^{p^{s+2}-1}) = \cdots$ se, e somente se, existe $\delta \in D_R^{(s+1)}$ tal que $\delta\left(\frac{1}{f}\right) = \frac{1}{f^p}$.

Demonstração. Assuma que $I_s(f^{p^s-1}) = I_{s+1}(f^{p^{s+1}-1})$. Por outro lado, o lema 2.1.2 implica que $I_s(f^{p^s-1}) = I_{s+1}(f^{p^{s+1}-p})$. Daí

$$I_{s+1}(f^{p^{s+1}-p}) = I_{s+1}(f^{p^{s+1}-1})$$

e consequentemente $I_{s+1}(f^{p^{s+1}-p})^{[p^{s+1}]} = I_{s+1}(f^{p^{s+1}-1})^{[p^{s+1}]}$. Isto implica que $D_R^{(s+1)} \cdot f^{p^{s+1}-p} = D_R^{(s+1)} \cdot f^{p^{s+1}-1}$ pelo lema 2.1.1. Logo

$$f^{p^{s+1}-p} \in D_R^{(s+1)} \cdot f^{p^{s+1}-1}$$

isto é, existe $\delta \in D_R^{(s+1)}$ tal que $\delta(f^{p^{s+1}-1}) = f^{p^{s+1}-p}$. Dividindo esta igualdade por $f^{p^{s+1}}$ e considerando que $\delta \in D_R^{(s+1)}$ comuta com todo elemento de $R^{p^{s+1}}$, temos $\delta\left(\frac{f^{p^{s+1}-1}}{f^{p^{s+1}}}\right) = \frac{f^{p^{s+1}-p}}{f^{p^{s+1}}}$, isto é, $\delta\left(\frac{1}{f}\right) = \frac{1}{f^p}$.

Reciprocamente, assuma que exista $\delta \in D_R^{(s+1)}$ tal que $\delta\left(\frac{1}{f}\right) = \frac{1}{f^p}$. Multiplicando essa igualdade por $f^{p^{s+1}}$, temos $\delta(f^{p^{s+1}-1}) = f^{p^{s+1}-p}$. Isto implica que

$$D_R^{(s+1)} \cdot f^{p^{s+1}-p} = D_R^{(s+1)} \cdot (\delta(f^{p^{s+1}-1})) = (D_R^{(s+1)} \cdot \delta)(f^{p^{s+1}-1}) \subseteq D_R^{(s+1)} \cdot f^{p^{s+1}-1}.$$

Daí $I_{s+1}(f^{p^{s+1}-p})^{[p^{s+1}]} \subseteq I_{s+1}(f^{p^{s+1}-1})^{[p^{s+1}]}$ pelo lema 2.1.1. Como será mostrado no último paragrafo desta demonstração, isto implica que $I_{s+1}(f^{p^{s+1}-p}) \subseteq I_{s+1}(f^{p^{s+1}-1})$. Agora o lema 2.1.2 implica $I_s(f^{p^s-1}) \subseteq I_{s+1}(f^{p^{s+1}-1})$ visto que $f^{p^{s+1}-p} = (f^{p^s-1})^p$. Isto junto com o lema 2.1.4 implica que $I_s(f^{p^s-1}) = I_{s+1}(f^{p^{s+1}-1})$.

Provamos que a existência de $\delta \in D_R^{(s+1)}$ tal que $\delta\left(\frac{1}{f}\right) = \frac{1}{f^p}$ é equivalente a igualdade $I_s(f^{p^s-1}) = I_{s+1}(f^{p^{s+1}-1})$. Agora segue que $I_s(f^{p^s-1}) = I_{s+1}(f^{p^{s+1}-1})$ é equivalente à $I_s(f^{p^s-1}) = I_{s'}(f^{p^{s'}-1})$ para todo $s' > s$, pois todo $\delta \in D_R^{(s+1)}$ automaticamente pertence a $D_R^{(s')}$ para $s' > s$.

Mostremos agora que se $\mathcal{I}$ e $\mathcal{J}$ são dois ideais de R tais que $\mathcal{I}^{[p^{s+1}]} \subset \mathcal{J}^{[p^{s+1}]}$, então $\mathcal{I} \subset \mathcal{J}$. De fato, é suficiente mostrar localmente, daí podemos assumir, como no Lema 2.1.2, que R é um $R^{p^{s+1}}$-módulo livre e $e_1 = 1$ é um dos geradores livres, isto é, $R = R^{p^{s+1}} \oplus M$, onde M é um $R^{p^{s+1}}$-módulo livre. Seja $\varphi : R \to R^{p^{s+1}}$ o mapa que manda $r \in R$ para $r^{p^{s+1}}$. Claramente, $\mathcal{I}^{[p^{s+1}]} = \varphi(\mathcal{I})R$, daí $\mathcal{I}^{[p^{s+1}]} \cap R^{p^{s+1}} = \varphi(\mathcal{I})R \cap R^{p^{s+1}} = (\varphi(\mathcal{I}) \oplus \varphi(\mathcal{I})M) \cap R^{p^{s+1}} = \varphi(\mathcal{I})$, e o mesmo acontece trocando $\mathcal{I}$ por $\mathcal{J}$. Assim, tomando interseção por $R^{p^{s+1}}$, temos que $\mathcal{I}^{[p^{s+1}]} \subset \mathcal{J}^{[p^{s+1}]}$ implica $\varphi(\mathcal{I}) \subset \varphi(\mathcal{J})$, que implica $\mathcal{I} \subset \mathcal{J}$, pois R, localmente, é um domínio, e assim, φ é um isomorfismo de anéis. □

Note que a demonstração mostra que a cadeia descendente de ideais estabiliza no primeiro inteiro s tal que $I_s(f^{p^s-1}) = I_{s+1}(f^{p^{s+1}-1})$.

Corolário 3.1.6. *A cadeia de ideais $I_1(f^{p-1}) \supseteq I_2(f^{p^2-1}) \supseteq \cdots$ estabiliza se, e somente se, $\frac{1}{f}$ gera R_f como D_R-módulo.*

Demonstração. Se $\frac{1}{f}$ gera R_f como D_R-módulo, então $\frac{1}{f^p} \in D_R \cdot \frac{1}{f}$, isto é, existe $\delta \in D_R$ tal que $\frac{1}{f^p} = \delta\left(\frac{1}{f}\right)$. Visto que $\delta \in D_R^{(s+1)}$ para algum s, a proposição anterior mostra que a cadeia de ideais estabiliza em s.

Reciprocamente, se a cadeia de ideais estabiliza em s, a proposição anterior diz que existe $\delta \in D_R^{(s+1)}$ tal que $\delta\left(\frac{1}{f}\right) = \frac{1}{f^p}$. Como foi visto demonstração do Lema 2.1.2, localmente o elemento 1 pode sempre ser tomado como um elemento de uma R^p-base de R, daí R/R^p é um R^p-módulo localmente livre de posto finito, portanto projetivo ([**?**], Thm. 7.12). Da sobrejeção natural $R \to R/R^p$, segue que existe um isomorfismo de R^p-módulos $R \cong R^p \oplus R/R^p$.

Seja $\delta' \in D_R^{(s+2)}$ definido por $\delta(x^p \oplus y) = \delta(x)^p$ para todo $x \in R$ e $y \in R/R^p \subseteq R$.

De fato, seja $r \in R$, então

$$\begin{aligned}
\delta'(r^{p^{s+2}} \cdot (x^p \oplus y)) &= \delta'(r^{p^{s+2}} x^p \oplus r^{p^{s+2}} y) \\
&= \delta'((r^{p^{s+1}} x)^p \oplus r^{p^{s+2}} y) \\
&= \delta(r^{p^{s+1}} x)^p \\
&= (r^{p^{s+1}} \delta(x))^p \\
&= r^{p^{s+2}} \delta(x)^p \\
&= r^{p^{s+2}} \delta'(x^p \oplus y).
\end{aligned}$$

Então $\delta'\left(\frac{1}{f^p}\right) = \left(\delta\left(\frac{1}{f}\right)\right)^p = \left(\frac{1}{f^p}\right)^p = \frac{1}{f^{p^2}}$, isto é, $\frac{1}{f^{p^2}} \in D_R \cdot \frac{1}{f}$. Disto, mostramos que para qualquer f tal que $\frac{1}{f^p} \in D_R \cdot \frac{1}{f}$, implica $\frac{1}{f^{p^2}} \in D_R \cdot \frac{1}{f}$. Daí, $\frac{1}{f^{p^s}} \in D_R \cdot \frac{1}{f}$ para todo s, por indução em s. O conjunto $\{\frac{1}{f^{p^s}}\}_s$, com s inteiro positivo, gera R_f como R-módulo. □

Observação 3.1.7 (Problema em aberto)**.** Seja R um anel regular F-finito de característica $p > 0$ e seja $f \in R$ um elemento não-nulo. A cadeia de ideais $I_1(f^{p-1}) \supseteq I_2(f^{p^2-1}) \supseteq \cdots$ estabiliza? Equivalentemente, R_f é gerado por $\frac{1}{f}$ como um D_R-módulo?

Para um anel regular F-finito R arbitrário, o problema está em aberto. Mas nas próximas seções mostramos que para uma classe de anéis regulares F-finitos a resposta é afirmativa.

3.2 O caso de um anel de polinômios

Seja $R = k[x_1, x_2, ..., x_n]$ o anel de polinômios sobre k, onde k é um corpo de característica $p > 0$. Um operador diferencial $\delta \in D_R$ será escrito na forma normal à direita, isto é, $\delta = \sum a_{\alpha\beta} x^\alpha D_\beta$, onde x^α é o monômio $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, D_β denotará o operador diferencial $D_\beta := D_{\beta_1,1} \cdots D_{\beta_n,n}$ (Exemplo 1.1.5) e $a_{\alpha\beta} \in k$ diferente de zero para um número finito.

Teorema 3.2.1. *Seja $R = k[x_1, x_2, ..., x_d]$ o anel de polinômios nas variáveis $x_1, x_2, ..., x_d$ sobre um corpo perfeito k de característica $p > 0$ e $f \in R$ um elemento não-nulo. A cadeia de ideais $I_1(f^{p-1}) \supseteq I_2(f^{p^2-1}) \supseteq \cdots$ estabiliza.*

Demonstração. Os monômios $\{x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}; 0 \le \alpha_i \le p^s - 1\}$ formam uma R^{p^s}-base de R. Seja $f^{p^s-1} = \sum_\alpha c_\alpha^{p^s} x^\alpha$, então $I_s(f^{p^s-1})$ é gerado pelo conjunto $\{c_\alpha\}$. Note que o grau de cada $c_\alpha^{p^s} x^\alpha$ é dado por $\deg(c_\alpha^{p^s} x^\alpha) = p^s \cdot \deg(c_\alpha) + \deg(x^\alpha)$. Assim, nenhum monômio no lado direito da equação $f^{p^s-1} = \sum_\alpha c_\alpha^{p^s} x^\alpha$ se cancela como um resultado de redução de termos similares, daí $\deg(f^{p^s-1}) \ge \deg(c_\alpha^{p^s})$ para todo α. Desta desigualdade temos $(p^s - 1)\deg(f) \ge p^s \deg(c_\alpha)$, ou seja, $\deg(c_\alpha) \le \frac{p^s-1}{p^s} \deg(f)$. Daí $\deg(c_\alpha) < \deg(f)$. Concluímos que os ideais $I_s(f^{p^s-1})$, para todo s, são gerados por polinômios de graus menores do que o grau de f, e este fato independe de s. O conjunto de polinômios de grau menor que $\deg(f)$ é um k-espaço vetorial de dimensão finita e as interseções dos ideais $I_s(f^{p^s-1})$ com este espaço vetorial forma uma cadeia descendente de subespaços que estabiliza, pois o espaço tem dimensão finita. Portanto, $I_1(f^{p-1}) \supseteq I_2(f^{p^2-1}) \supseteq \cdots$ estabiliza. □

Corolário 3.2.2. *Seja $R = k[x_1, x_2, ..., x_d]$ o anel de polinômios nas variáveis $x_1, x_2, ..., x_d$ sobre um corpo arbitrário de característica $p > 0$ e $f \in R$ um elemento não-nulo. Então R_f é gerado por $\frac{1}{f}$ como um D_R-módulo.*

Demonstração. Se k é perfeito, o Corolário 2.1.6 e o teorema anterior garantem o resultado. No caso geral, seja K o fecho perfeito de k. Visto que K é perfeito, existe um operador diferencial $\delta = \sum a_{\alpha\beta} x^\alpha D_\beta$ com coeficientes $a_{\alpha\beta} \in K$ tal que $\delta\left(\frac{1}{f}\right) = \frac{1}{f^p}$. Isto é equivalente ao fato que um sistema de um número finito de equações lineares com coeficientes em k tem soluções em K, onde os coeficientes $a_{\alpha\beta}$ de δ são as incógnitas do sistema. (Por exemplo, se $f = x_1$, nós podemos procurar uma solução na forma $\delta = aD_{p-1,1}$, e temos uma equação $\delta\left(\frac{1}{x_1}\right) = \frac{1}{x_1^p}$. Visto que $\delta\left(\frac{1}{x_1}\right) = a\frac{1}{x_1^p}$, o sistema linear correspondente é apenas uma equação $a = 1$.) O sistema tem uma solução em K, que são os coeficientes de δ. Portanto, devemos ter soluções em k, porque os coeficientes do sistema linear estão em k (eles dependem unicamente dos coeficientes de f). Daí, existe um operador diferencial δ' com coeficientes em k tal que $\delta'\left(\frac{1}{f}\right) = \frac{1}{f^p}$. □

Exemplo 3.2.3. Seja $R = k[x_1, x_2, x_3, x_4]$ onde k é um corpo de característica $p > 0$ e seja $f = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Em característica 0, como é pontuado na Introdução, $\frac{1}{f^2}$ não pertence ao D_R-submódulo de R_f gerado por $\frac{1}{f}$. Mas em característica $p > 0$, encontraremos um operador diferencial $\delta \in D_R$ tal que $\delta\left(\frac{1}{f}\right) = \frac{1}{f^p}$, apenas investigando monômios que aparecem em f^{p-1}.

- Se 4 divide $p-1$, então f^{p-1} contém o termo $a_\alpha x^\alpha$, onde

$$a_\alpha = \frac{(p-1)!}{\left(\frac{p-1}{4}!\right)^4} \neq 0 \text{ e } \alpha = \left(\frac{p-1}{2}, \frac{p-1}{2}, \frac{p-1}{2}, \frac{p-1}{2}\right);$$

- Se 4 não divide $p-1$, então f^{p-1} contém o termo $a_\alpha x^\alpha$, onde

$$a_\alpha = \frac{(p-1)!}{\left(\frac{p+1}{4}!\right)^2\left(\frac{p-3}{4}!\right)^2} \neq 0 \text{ e } \alpha = \left(\frac{p+1}{2}, \frac{p+1}{2}, \frac{p-3}{2}, \frac{p-3}{2}\right).$$

Note que $\frac{1}{a_\alpha} D_\alpha(f^{p-1}) = 1$, pois todos os outros monômios que aparecem em f^{p-1} contém algum x_i com potência menor do que a potência de $\frac{\partial_i}{\partial x_i}$ em D_α, daí D_α anula todos os outros monômios. O operador diferencial $\delta = \frac{1}{a_\alpha} D_\alpha(f^{p-1})$ comuta com f^p, logo, dividindo a equação $\delta(f^{p-1}) = 1$ por f^p, temos o resultado desejado.

3.3 O caso de uma álgebra regular finitamente gerada sobre um anel local regular F-finito

Aqui damos a demonstração do resultado central desta dissertação [?], ou seja, que R_f é gerado por $\frac{1}{f}$ como D_R-módulo, para o caso em que R é uma álgebra regular finitamente gerada sobre um anel local regular F-finito, e generalizamos para o caso de um $R[F]$-módulo unitário finitamente gerado. Para isso usamos as técnicas desenvolvidas no Capítulo 1.

Seja R uma álgebra finitamente gerada sobre um anel F-finito A de característica $p > 0$. Note que R é $A[R^p]$-módulo finitamente gerado, e como A é F-finito, temos que R é R^p-módulo finitamente gerado, ou seja, R é F-finito.

Lema 3.3.1. *$R^{(s)}$ é R-módulo à direita fielmente plano.*

Demonstração. Seja $N \neq 0$ um R-módulo (à esquerda). Localmente, temos que $R^{(s)} \otimes_R N \neq 0$, pois $R^{(s)}$ é livre, portanto fielmente plano. Logo, $R^{(s)} \otimes_R N \neq 0$ ([?], Thm. 7.2(2)) □

Teorema 3.3.2. *Seja R uma álgebra regular finitamente gerada sobre um anel local regular F-finito de característica $p > 0$. Seja $f \in R$ um elemento não-nulo. Então o D_R-módulo R_f é gerado por $\frac{1}{f}$.*

Demonstração. Para um D_R-módulo $M \subseteq R_f$, identificamos F^*M com sua imagem isomorfa em R_f, via o isomorfismo natural de D_R-módulos $\vartheta : F^*R_f \to R_f$ do Corolário 1.4.4 (com R_f visto como um $R[F]$-módulo unitário, onde $F : R_f \to R_f$ manda $x \in R_f$ em x^p). Então, F^*M é R-gerado por elementos m^p, para $m \in M \subseteq R_f$, visto que $\vartheta(r \otimes m) = rm^p$. Pela Descida de Frobenius (Proposição 1.4.1), F^*M é um D_R-submódulo de R_f.

Seja $M = D_R \cdot \frac{1}{f}$. Afirmamos que $M \subseteq F^*M$. Visto que F^*M é um D_R-submódulo de R_f, é suficiente mostrar que $\frac{1}{f} \in F^*M$. Mas $\frac{1}{f} \in M$ implica que $\left(\frac{1}{p}\right)^p = \frac{1}{f^p} \in F^*M$. Daí $f^{p-1} \cdot \frac{1}{f^p} = \frac{1}{f} \in F^*M$. Isto prova a afirmação.

Agora tomamos a cadeia ascendente de D_R-submódulos de R_f:

$$M \subseteq F^*M \subseteq F^{2*}M \subseteq F^{3*}M \subseteq \cdots$$

Pelo fato que $\frac{1}{f} \in M$ implica $\frac{1}{f^{p^s}} = F^s\left(\frac{1}{f}\right) \in F^{s*}M$, temos que a união dos submédulos desta cadeia é todo R_f, pois o conjunto $\{\frac{1}{f^{p^s}}\}_s$ gera R_f como R-módulo. Disto, é suficiente mostrar que $M = F^*M$, daí $M = F^{s*}M$ para todo s, e assim obtemos que $M = R_f$. Assuma que $M \subsetneq F^*M$, ou seja, a inclusão é estrita. Então todas as inclusões da cadeia acima são estritas, pois $F^{s*}(-) = R^{(s)} \otimes_R (-)$ e $R^{(s)}$ é R-módulo fielmente plano. Mas isso contradiz o fato que, pelo Teorema 1.3.10, o comprimento de R_f como D_R-módulo é finito. □

Corolário 3.3.3. *Seja R uma álgebra regular finitamente gerada sobre um anel local regular F-finito de característica $p > 0$. Seja $f \in R$ elemento não-nulo. A cadeia descendente de ideais $I_1(f^{p-1}) \supseteq I_2(f^{p^2-1}) \supseteq \cdots$, definida na seção 2.1, estabiliza.*

Demonstração. Segue do Teorema 2.3.2 e do Corolário 2.1.6. □

Do Teorema 2.3.2 segue também uma observação mais geral, que se temos $F^*M \subseteq M$ então M é também um $R[F]$-módulo unitário.

Teorema 3.3.4. *Seja R uma álgebra regular finitamente gerada sobre um anel local regular F-finito de característica $p > 0$. Seja N um $R[F]$-módulo unitário finitamente gerado. Suponha que $M \subseteq N$ é um D_R-submódulo tal que $M \subseteq F^*M$ (identificamos $F^*M \subseteq F^*N$ com sua imagem em N via o isomorfismo estrutural $\vartheta : F^*N \to N$ de N). Então M é um $R[F]$-submódulo unitário.*

Demonstração. Para M ser um $R[F]$-submódulo de N basta mostrar que a inclusão $M \subseteq F^*M$ é de fato uma igualdade. Se a inclusão for estrita, então todas as inclusões $F^{s*}M \subseteq F^{(s+1)*}M$ são estritas, pois são obtidas por tensorizar $M \subseteq F^*M$ pelo R-módulo fielmente plano $R^{(s)}$. Resultando na cadeia estritamente crescente infinita

$$M \subsetneq F^*M \subsetneq F^{2*}M \subsetneq F^{3*}M \subsetneq \cdots$$

contradizendo a finitude do comprimento de N como D_R-módulo, Teorema 1.3.10. □

Para obter o Teorema 2.3.2 deste fato, note que $M = D_R \cdot \frac{1}{f}$ satisfaz $M \subseteq F^*M$ e contém o $R[F]$-módulo gerado por $\frac{1}{f}$ de R_f.

Um R-submódulo N_0 de um $R[F]$-módulo unitário N é chamado uma *raiz*, se N_0 é finitamente gerado como R-módulo, $N_0 \subseteq F^*N_0$ e $\bigcup_s F^{s*}N_0 = N$ (Definição 1.3.7). A existência de uma raiz é equivalente a dizer que N é finitamente gerado como um $R[F]$-módulo, pelo Corolário 1.3.8.

Corolário 3.3.5. *Com as hipóteses do Teorema 2.3.4, se $n_1, ..., n_t$ são geradores de uma raiz de um $R[F]$-módulo unitário finitamente gerado N, então $n_1, ..., n_t$ geram N como um D_R-módulo.*

Demonstração. Pelo Teorema 2.3.4, é suficiente mostrar que o D_R-submódulo $M = D_R \cdot \langle n_1, ..., n_t \rangle$ satisfaz $M \subseteq F^*M$ e contém os $R[F]$-geradores $n_1, ..., n_t$ de N. A segunda afirmação é trivial, para a primeira observe que, pela definição de raiz, $n_i = \sum r_j F(n_j)$ para $r_j \in R$. Note que $F(n_j) \in F^*M$, portanto $n_i \in F^*M$ para todo i. □

O corolário acima é uma generalização do Teorema 2.3.2, em que R_f é $R[F]$-módulo finitamente gerado, com gerador $n = \frac{1}{f}$.

3.4 O caso de uma álgebra finitamente gerada sobre um anel de séries de potências formais

O propósito desta seção é mostrar que R_f é $D_{R|k}$-gerado por $\frac{1}{f}$ em um importante caso que não é coberto pelas seções anteriores. Seja R uma álgebra finitamente gerada sobre um anel de séries de potências formais $A = k[[x_1, ..., x_n]]$ sobre um corpo k de característica $p > 0$. O interessante neste caso é que não assumiremos que k é corpo perfeito.

Vamos supor a princípio que k é finitamente gerado como k^p-módulo. Então temos que A é finitamente gerado como $k[A^p]$-módulo, mais ainda R é $k[R^p]$-módulo finitamente gerado. Pelo Teorema 1.1.4, $D_{R|k} = \bigcup_s \mathrm{End}_{k[R^p]}(R)$. Porém, se k não é finitamente gerado como k^p-módulo, então R nem sempre é $k[R^p]$-módulo finitamente gerado, logo não podemos aplicar a fórmula acima neste caso.

Sem nenhuma suposição sobre k, denotamos por $k[[A^{p^s}]] = k[[x_1^{p^s}, ..., x_n^{p^s}]]$ a k-subálgebra de A consistindo de todas as séries de potências formais em $x_1^{p^s}, ..., x_n^{p^s}$ com coeficientes em k, e denotamos por $k[[A^{p^s}]][R^{p^s}]$ a $k[[A^{p^s}]]$-subálgebra de R gerada pelas p^s-ésimas potências de todos os elementos de R. O fato que A é finitamente gerado como $k[[A^{p^s}]]$-módulo para todo s, implica que R é um $k[[A^{p^s}]][R^{p^s}]$-módulo finitamente gerado. Disto, o anel de operadores diferenciais $k[[A^{p^s}]][R^{p^s}]$-lineares de R é $\mathrm{End}_{k[[A^{p^s}]][R^{p^s}]}(R)$, devido ao Teorema 1.1.4. Todo operador diferencial $k[[A^{p^s}]][R^{p^s}]$-linear de R é k-linear, portanto $D_{R|k} \supseteq V(R,k)$, onde

$$V(R,k) = \bigcup_s \mathrm{End}_{k[[A^{p^s}]][R^{p^s}]}(R).$$

Sejam $k^* = k^{\frac{1}{p^\infty}}$ o fecho perfeito de k, $A^* = k^*[[x_1, ..., x_n]]$ e $R^* = A^* \otimes_A R$, onde A^* é visto como uma A-álgebra via a inclusão natural $k[[x_1, ..., x_n]] \subseteq k^*[[x_1, ..., x_n]]$. Sendo R finitamente gerado como A-álgebra, temos R^* finitamente gerado como A^*-álgebra, e portanto noetheriano, pois A^* é noetheriano.

Lema 3.4.1. *A^* é fielmente plano sobre A.*

Demonstração. A^* é plano sobre A, por [**?**] Thm 22.3(β)(1)(3'), e local ([**?**] Thm.7.2(3)). □

Proposição 3.4.2. *Com a notação acima, seja R uma A-álgebra finitamente gerada tal que R^* é regular. Então R^* é F-finito e $D_{R^*} = R^* \otimes_R V(R,k)$.*

Demonstração. Seja $R(k,s) = k[[A^{p^s}]][R^{p^s}]$. Visto que A^* é fielmente plano sobre A, o homomorfismo $R \to R^*$ induzido pela inclusão natural $A \to A^*$ é injetivo ([**?**], Thm. 7.5(i)). Consideramos R como um subanel de R^* via esse homomorfismo. Então

$k^*[[A^{*^{p^s}}]][R^{*^{p^s}}] = k^*[[A^{*^{p^s}}]][R^{p^s}]$, a $k^*[[A^{*^{p^s}}]]$-subálgebra de R^* gerada pelos elementos de R^{p^s}. Visto que k^* é perfeito,

$$k^*[[A^{*^{p^s}}]][R^{*^{p^s}}] = R^{*^{p^s}}, \quad e \quad k^*[[A^{*^{p^s}}]][R^{p^s}] = R^{*^{p^s}},$$

ou seja, R^* é F-finito.

O homomorfismo de anéis

$$\phi : k^*[[A^{*^{p^s}}]] \otimes_{k[[A^{p^s}]]} R(k,s) \overset{a\otimes r\mapsto ar}{\longrightarrow} R^{*^{p^s}}$$

é claramente sobrejetivo. Afirmamos que ϕ é um isomorfismo. De fato, o homomorfismo de anéis $R^* = A^* \otimes_A R \overset{a\otimes r\mapsto a^{p^s}\otimes r^{p^s}}{\rightarrow} k^*[[A^{*^{p^s}}]] \otimes_{k[[A^{p^s}]]} R(k,s)$ é sobrejetivo, pois cada elemento de $k^*[[A^{*^{p^s}}]] \otimes_{k[[A^{p^s}]]} R(k,s)$ é da forma $\sum_i a_i \otimes a_i' r_i^{p^s} = \sum_i a_i a_i' \otimes r^{p^s}$, onde $a_i \in k^*[[A^{*^{p^s}}]], a_i' \in k[[A^{p^s}]], r_i \in R$ e $a_i a_i' \in k^*[[A^{*^{p^s}}]]$ tem uma p^s-ésima raiz em A^* (visto que todo elemento de $k^*[[A^{*^{p^s}}]]$ tem). A composição desse homomorfismo com ϕ produz o homomorfismo de Frobenius $R^* \overset{r\mapsto r^{p^s}}{\rightarrow} R^{*^{p^s}}$. Visto que R^* é regular, logo localmente um domínio, esse homomorfismo de Frobenius é injetivo, então ϕ é injetivo. Disto

$$R^{*^{p^s}} = k^*[[A^{*^{p^s}}]] \otimes_{k[[A^{p^s}]]} R(k,s).$$

Isto implica que $R^{*^{p^s}}$ é fielmente plano sobre $R(k,s)$ (visto que $k^*[[A^{*^{p^s}}]]$ é fielmente plano sobre $k[[A^{p^s}]]$, Lema 2.4.1).

É fácil verificar que $A^* = k^*[[A^{*^{p^s}}]] \otimes_{k[[A^{p^s}]]} A$, então

$$\begin{aligned}
R^* \otimes_R (-) &= A^* \otimes_A R \otimes_R (-) \\
&= A^* \otimes_A (-) \\
&= k^*[[A^{*^{p^s}}]] \otimes_{k[[A^{p^s}]]} (-) \\
&= k^*[[A^{*^{p^s}}]] \otimes_{k[[A^{p^s}]]} R(k,s) \otimes_{R(k,s)} (-) \\
&= R^{*^{p^s}} \otimes_{R(k,s)} (-).
\end{aligned}$$

Em particular,

$$R^* = R^* \otimes_R R = R^{*^{p^s}} \otimes_{R(k,s)} R.$$

Vimos que R é finitamente gerado como $R(k,s)$-módulo. Afirmamos que R é $R(k,s)$-módulo projetivo. Visto que $R^{*^{p^s}}$ é fielmente plano como $R(k,s)$, é suficiente mostrar que $R^* = R^{*^{p^s}} \otimes_{R(k,s)} R$ é um $R^{*^{p^s}}$-módulo projetivo. Sendo R^* regular F-finito, temos que R^* é localmente $R^{*^{p^s}}$-módulo livre de posto finito, logo projetivo, vide [**?**] Thm. 7.12.

Se $S \to T$ é um homomorfismo de aneis Noetherianos comutativos e M, N são S-módulos, temos o homomorfismo de T-módulos

$$\tau(M,N) : T \otimes_S \mathrm{Hom}_S(M,N) \overset{t\otimes f\mapsto(t'\otimes x\mapsto tt'\otimes f(x))}{\longrightarrow} \mathrm{Hom}_T(T \otimes_S M, T \otimes_S N)$$

que é um isomorfismo se M é um S-módulo finitamente gerado e projetivo. De fato, Isto é claro se M é finitamente gerado e livre. Em geral, $M \oplus M'$ é finitamente gerado e livre para algum S-módulo, então $\tau(M \oplus M', N)\tau(M,N) \oplus \tau(M', N)$, e $\tau(M,N)$ é um isomorfismo.

Aplicando a $S = R(k,s), T = R^{*^{p^s}}$ e $M = N = R$, temos

$$\mathrm{Hom}_{R^{*p^s}}(R^*, R^*) = R^{*^{p^s}} \otimes_{R(k,s)} \mathrm{Hom}_{R(k,s)}(R,R) = R^* \otimes_R \mathrm{Hom}_{R(k,s)}(R,R).$$

Visto que R^* é finitamente gerado como R^{*^p}-módulo, pela formula do Teorema 1.1.4 temos

$$D_{R^*} = \bigcup_s \mathrm{Hom}_{R^{*p^s}}(R^*, R^*) = \bigcup_s R^* \otimes_R \mathrm{Hom}_{R(k,s)}(R,R).$$

Isto implica que $D_{R^*} = R^* \otimes_R \bigcup_s \mathrm{Hom}_{R(k,s)}(R,R) = R^* \otimes_R V(R,k)$, visto que produto tensorial comuta com limites indutivos. □

Teorema 3.4.3. *Com a notação acima, seja R uma A-álgebra finitamente gerada tal que R^* é regular. Temos que R_f é gerado por $\frac{1}{f}$ como $D_{R|k}$-módulo.*

Demonstração. Visto que $V(R,k)$ é subanel de $D_{R|k}$, é suficiente mostrar que $\frac{1}{f}$ gera R_f como $V(R,k)$-módulo. De acordo com a proposição anterior,

$$D_{R^*} = R^* \otimes_R V(R,k)$$

e existe um funtor

$$V(R,k) - mod \overset{N \mapsto R^* \otimes_R N}{\longrightarrow} D_{R^*} - mod$$

onde para cada $V(R,k)$-módulo N, a estrutura de D_{R^*}-módulo em $R^* \otimes_R N$ é definida como segue: se $\delta \in D_{R^*}, r \otimes n \in R^* \otimes_R N$ e $\delta \cdot r = \sum_i (r_i \otimes v_i)$, onde $r_i \in R^*, v_i \in V(R,k)$, então $\delta(r \otimes n) = \sum_i (r_i \otimes v_i(n))$ (note que $\delta \cdot r$ é multiplicação de operadores diferenciais).

Sendo A^* fielmente plano sobre A, temos $R^* = A^* \otimes_A R$ fielmente plano sobre R. Seja $M \subset R_f$ o $V(R,k)$-submódulo gerado por $\frac{1}{f}$. Tomando o produto tensorial $R^*_f = R^* \otimes_R R_f$, concluímos que $R^* \otimes M$ é um D_{R^*}-submódulo de R^*_f contendo $\frac{1}{f}$ (identificamos $1 \otimes f$ com f). Pelo Teorema 2.3.2, $R^* \otimes_R M = R^*_f$. Portanto, como R^* é fielmente plano sobre R, temos que $M = R_f$. □

Teorema 3.4.4. *Com a notação acima, seja R uma A-álgebra finitamente gerada tal que R^* é regular. Se $n_1, ..., n_t$ são geradores de uma raiz de um $R[F]$-módulo unitário finitamente gerado N, então $n_1, ..., n_t$ geram N como um $D_{R|k}$-módulo.*

Demonstração. É suficiente mostrar que $n_1, ..., n_t$ geram N como um $V(R,k)$-módulo. Se não, Seja $M \subseteq N$ o $V(R,k)$-submódulo de N gerado por $n_1, ..., n_t$. Sendo R^* fielmente plano sobre R, temos que $R^* \otimes_R M$ é um D_{R^*}-submódulo de $R^* \otimes_R N$ diferente de $R^* \otimes_R N$. Mas isso contradiz o Corolário 2.3.5, pois $R^* \otimes_R M$ contém $1 \otimes n_1, ..., 1 \otimes n_t$ e esses elementos geram uma raiz de $R^* \otimes_R N$. □

O seguinte caso especial dos Teoremas 2.4.3 e 2.4.4 deve ser enunciado separadamente.

Corolário 3.4.5. *Seja R uma álgebra finitamente gerada por sobre um corpo k de característica $p > 0$ tal que $k^{\frac{1}{p^\infty}} \otimes_k R$ é regular. Então*

(a) *R_f, para qualquer $f \in R$, é gerado por $\frac{1}{f}$ como um $D_{R|k}$-módulo;*

(b) *Mais geralmente, se $n_1, ..., n_t$ são geradores de uma raiz de um $R[F]$-módulo unitário finitamente gerado N, então $n_1, ..., n_t$ geram N como um $D_{R|k}$-módulo.*

Capítulo 4

Uma aplicação à cohomologia local

4.1 Módulos de cohomologia local

Vamos definir o funtor I-torsão Γ (em toda seção, I sempre denota um ideal de um anel comutativo Noetheriano R) e seus funtores derivados à direita H_I^i $(i \geq 0)$, chamados funtores de cohomologia local com respeito a I. Para finalizar, exibimos algumas propriedades. Denotaremos por $\mathbb{N}$, os inteiros positivos, e por $\mathbb{N}_0$, os inteiros não-negativos.

Definição 4.1.1. Para cada R-módulo M, definimos $\Gamma_I(M) = \bigcup_{n\in\mathbb{N}}(0 :_M I^n)$, o conjunto de elementos de M que são anulados por alguma potência de I. Note que $\Gamma_I(M)$ é um submódulo de M. Para um homomorfismo $f : M \to N$ de R-modulos, temos $f(\Gamma_I(M)) \subseteq \Gamma_I(N)$, assim existe um mapa $\Gamma_I(f) : \Gamma_I(M) \to \Gamma_I(N)$ que concorda com f em cada elemento de $\Gamma_I(M)$.

É claro que, se $g : M \to N$ e $h : N \to L$ são mais homomorfismos de R-módulos e $r \in R$, então $\Gamma_I(h \circ f) = \Gamma_I(h) \circ \Gamma_I(f)$, $\Gamma_I(f + g) = \Gamma_I(f) + \Gamma_I(g)$, $\Gamma_I(rf) = r\Gamma_I(f)$ e $\Gamma_I(id_M) = id_{\Gamma_I(M)}$. Disto, Γ_I é um funtor covariante R-linear da categoria de R-módulos nela mesma. (Dizemos que um funtor $T : R-\text{mod} \to R-\text{mod}$ é R-linear quando ele é aditivo e $T(rf) = rT(f)$ para todo $r \in R$ para todo homomorfismo f de R-módulos.) Chamamos Γ_I o *funtor I-torsão*.

Lema 4.1.2. *O funtor I-torsão* $\Gamma_I : R-\text{mod} \to R-\text{mod}$ *é exato à esquerda.*

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

$$0 \to \Gamma_I(L) \xrightarrow{\Gamma_I(f)} \Gamma_I(M) \xrightarrow{\Gamma_I(g)} \Gamma_I(N)$$

ainda é exata. É claro que $\Gamma_I(f)$ é monomorfismo e segue imediatamente de 3.1.1 que $\Gamma_I(g) \circ \Gamma_I(f) = 0$, logo

$$\mathrm{Im}(\Gamma_I(f)) \subseteq \mathrm{Ker}(\Gamma_I(g)).$$

Para mostrar a outra inclusão, tome $m \in \mathrm{Ker}(\Gamma_I(g))$. Disto $m \in \Gamma_I(M)$, então existe $n \in \mathbb{N}$ tal que $I^n m = 0$, e $g(m) = 0$. Agora existe $l \in L$ tal que $f(l) = m$, basta mostrar que $l \in \Gamma_I(L)$. Note que, para cada $r \in I^n$, temos $f(rl) = rf(l) = rm = 0$, logo $rl = 0$ pois f é monomorfismo. Portanto $I^n l = 0$. □

Definição 4.1.3. Para $i \in \mathbb{N}_0$, o i-ésimo funtor derivado à direita de Γ_I é denotado por H^i_I e o chamamos de *i-ésimo funtor de cohomologia local com respeito a I.*

Para um R-módulo M, chamados $H^i_I(M)$ de i-ésimo módulo de cohomologia local de M com respeito a I, e $\Gamma_I(M)$ de submódulo de I-torsão de M. Dizemos que M é *livre de I-torsão* quando $\Gamma_I(M) = 0$, e que M é *I-torsão* quando $\Gamma_I(M) = M$, isto é, se, e somente se, cada elemento de M é anulado por alguma potência de I.

Visto que Γ_I é covariante e R-linear, automaticamente os funtores de cohomologia local H^i_I ($i \in \mathbb{N}_0$) são covariantes e R-lineares. E como Γ_I é exato à esquerda, H^0_I é naturalmente equivalente a Γ_I.

Seja M um R-módulo arbitrário. Para calcular $H^i_I(M)$ procedemos da seguinte forma. Tomamos uma resolução injetiva

$$Q^\bullet : 0 \xrightarrow{d^{-1}} Q^0 \xrightarrow{d^0} Q^1 \to \cdots \to Q^i \xrightarrow{d^i} Q^{i+1} \to \cdots$$

de M, ou seja, existe um R-homomorfismo $\alpha : M \to I^0$ tal que a sequência

$$0 \to M \xrightarrow{\alpha} Q^0 \xrightarrow{d^0} Q^1 \to \cdots \to Q^i \xrightarrow{d^i} Q^{i+1} \to \cdots$$

seja exata. Aplicamos o funtor Γ_I ao complexo $Q^\bullet$ para obter

$$0 \xrightarrow{d^{-1}} \Gamma_I(Q^0) \xrightarrow{\Gamma_I(d^0)} \Gamma_I(Q^1) \to \cdots \to \Gamma_I(Q^i) \xrightarrow{\Gamma_I(d^i)} \Gamma_I(Q^{i+1}) \to \cdots$$

e tomamos o i-ésimo módulo de cohomologia desse complexo; o resultado,

$$\mathrm{Ker}(\Gamma_I(d^i))/\mathrm{Im}(\Gamma_I(d^{i-1})),$$

é $H^i_I(M)$. Note que, por um fato clássico de álgebra homológica, $H^i_I(M)$ independe (a menos de R-isomorfismo) da escolha de resolução injetiva $Q^\bullet$ de M.

4.2 Complexo de Čech e finitude do comprimento na categoria dos D-módulos

Nesta seção, $a_1, a_2, ..., a_n$ (onde $n > 0$) denotam n elementos que geram I, e M um R-módulo arbitrário. Iremos definir o complexo de Čech $C(M)^\bullet$ de M com respeito a sequência $a_1, a_2, ..., a_n$. Esse complexo tem a forma

$$0 \to C(M)^0 \xrightarrow{d^0} C(M)^1 \to \cdots \to C(M)^{n-1} \xrightarrow{d^{n-1}} C(M)^n \to 0.$$

No final, vamos mostrar que, dado um R-módulo finitamente gerado M, então os módulos de cohomologia local de M tem comprimento finito na categoria de D_R-módulos. Para $a \in R$, as notações R_a e M_a denotam, o anel e o módulo de frações de R e M com respeito ao conjunto multiplicativamente fechado $\{a^i : i \in \mathbb{N}_0\}$ de R.

Lema 4.2.1. *Sejam $a,b \in R$. Existe um isomorfismo de R-módulos $\mu : M_{ab} \to (M_a)_b$ dado por $\mu(m/(ab)^i) = (m/a^i)/b^i$ para todo $m \in M$ e todo $i \in \mathbb{N}_0$.*

Demonstração. Suponha que $m,y \in M$ e $i,j \in \mathbb{N}_0$ são tais que $m/(ab)^i = y/(ab)^j$ em M_{ab}. Então existe $k \in \mathbb{N}_0$ tal que

$$(ab)^k((ab)^j m - (ab)^i y) = 0.$$

Disto, em M_a, temos $b^{k+j}m/a^i = b^{k+i}y/a^j$, e $(m/a^i)/b^i = (y/a^j)/b^j$ em $(M_a)_b$. Portanto, existe, de fato, um mapa $\mu : M_{ab} \to (M_a)_b$ dado pela fórmula do enunciado do lema. É fácil verificar que μ é R-isomorfismo. □

Observação 4.2.2. Devido ao Lema 3.2.1, usamos μ para identificar os R-módulos M_{ab} e $(M_a)_b$. Daí, quando falamos do R-homomorfismo natural $\omega : M_a \to M_{ab}$, estamos nos referindo ao R-homomorfismo natural de M_a para $(M_a)_b$, onde $\omega(m/a^i) = b^i m/(ab)^i$ para todo $m \in M$ e $i \in \mathbb{N}_0$.

Notação 4.2.3. Para $k \in \mathbb{N}$ com $1 \le k \le n$, escrevemos

$$\mathcal{I}(k,n) := \{(i(1),...,i(k)) \in \mathbb{N}^k : 1 \le i(1) < i(2) < \cdots < i(k) \le n\},$$

o conjunto de todas as sequências estritamente crescente de comprimento k de inteiros positivos tomados do conjunto $\{1,...,n\}$. Para $i \in \mathcal{I}(k,n)$ e $1 \le j \le k$, denotamos o j-ésimo componente de i por $i(j)$, tal que $i = (i(1),...,i(k))$.

Agora suponha que $k < n$ e $s \in \mathbb{N}$ com $1 \le s \le k+1$. Seja $j \in \mathcal{I}(k+1,n)$. Então

$$j^{\hat{s}} \;\; ou \;\; (j(1),...,\widehat{j(s)},...,j(k+1))$$

é a sequência $(j(1),...,j(s-1),j(s+1),...,j(k+1))$ de $\mathcal{I}(k,n)$ obtido por omitir o s-ésimo componente de j. Mais ainda, se $t \in \mathbb{N}$ com $1 \le t < s$, então $(j^{\hat{s}})^{\hat{t}} = (j^{\hat{t}})^{\widehat{s-1}}$.

Novamente assumindo $k < n$, tome $i \in \mathcal{I}(k,n)$. O *n-complemento* de i é a sequência $j \in \mathcal{I}(n-k,n)$ tal que

$$\{1,...,n\} = \{i(1),...,i(k),j(1),...,j(n-k)\}.$$

Agora vamos definir o complexo de Čech de um R-módulo M com respeito a sequência $a_1,a_2,...,a_n \in R$.

Proposição 4.2.4 (Definição)**.** *Definimos a sequência $C(M)^\bullet$ de R-módulos e R-homomorfismos*

$$0 \to C(M)^0 \xrightarrow{d^0} C(M)^1 \to \cdots \to C(M)^{n-1} \xrightarrow{d^{n-1}} C(M)^n \to 0.$$

como segue:

(a) *$C(M)^0 := M$;*

(b) *para $k = 1,...,n$ e com a notação 2.2.3,*

$$C(M)^k = \oplus_{i\in\mathcal{I}(k,n)} M_{a_{i(1)}\cdots a_{i(k)}};$$

(c) *$d^0 : C(M)^0 \to C(M)^1$ é tal que, para cada $h = 1,...,n$, a composição de d^0 com a projeção canônica de $C(M)^1$ em M_{a_h} é o mapa natural de M para M_{a_h}; e*

(d) *para $k = 1,...,n-1$, $i \in \mathcal{I}(k,n)$ e $j \in \mathcal{I}(k+1,n)$, a composição*

$$M_{a_{i(1)}\cdots a_{i(k)}} \to C(M)^k \xrightarrow{d^k} C(M)^{k+1} \to M_{a_{j(1)}\cdots a_{j(k+1)}}$$

(onde o primeiro e o terceiro mapas são a injeção canônica e a projeção canônica, respectivamente) é o mapa natural de $M_{a_{i(1)}\cdots a_{i(k)}}$ para $M_{a_{i(1)}\cdots a_{i(k)}a_{j(s)}}$ multiplicado por $(-1)^{s-1}$, se $i = j^{\hat{s}}$, para todo s com $1 \le s \le k+1$, e 0 caso contrário.

Então $C(M)^\bullet$ é um complexo, e chamamos o complexo de Čech estendido de M com respeito a $a_1,...,a_n$. (Vamos omitir a palavra 'estendido'.)

Denotamos $C(R)^\bullet$ por

$$C^\bullet : 0 \to C^0 \xrightarrow{d^0} C^1 \to \cdots \to C^i \xrightarrow{d^i} C^{i+1} \to \cdots \to C^n \to 0.$$

Demonstração. Temos que provar que $d^{k+1} \circ d^k = 0$, para todo $k = 0,...,n-2$. Seja $m \in M$. Para mostrar que $d^1 \circ d^0 = 0$, é suficiente mostrar que, para cada $i \in \mathcal{I}(2,n)$, o componente de $d^1 \circ d^0(m)$ na parcela $M_{a_{i(1)}a_{i(2)}}$ de $C(M)^2$ é 0. As únicas contribuições para esse componente que poderiam ser não-nulos, devem vir das parcelas $M_{a_{i(1)}}$ e $M_{a_{i(2)}}$ de $C(M)^1$. Segue que, a componente de $d^1 \circ d^0(m)$ na parcela $M_{a_{i(1)}a_{i(2)}}$ de $C(M)^2$ é $(-1)(m/1) + (m/1) = 0$. Daí $d^1 \circ d^0(m) = 0$.

Agora, considere o casa onde $1 \le k \le n-2$. Para mostrar que $d^{k+1} \circ d^k = 0$, é suficiente mostrar que, para cada $i \in \mathcal{I}(k,n)$, a restrição de $d^{k+1} \circ d^k$ à parcela $M_{a_{i(1)}...a_{i(k)}}$ de $C(M)^k$ é zero. Seja $m \in M, e \in \mathbb{N}_0$ e $j \in \mathcal{I}(k+2,n)$: calculamos a componente de

$$d^{k+1} \circ d^k \left(\frac{m}{(a_{i(1)}...a_{i(k)})^e} \right)$$

na parcela $M_{a_{i(1)}...a_{i(k)}}$ de $C(M)^{k+2}$. Esse componente será não-nulo somente se $i = (j^{\hat{s}})^{\hat{t}}$, para alguns inteiros s,t com $1 \le t < s \le k+2$, e, quando forem, temos

$$\frac{(-1)^{t-1}(-1)^{s-2} a_{j(t)}^e a_{j(s)}^e m}{(a_{j(1)}...a_{j(k+2)})^e} + \frac{(-1)^{s-2}(-1)^{t-1} a_{j(s)}^e a_{j(t)}^e m}{(a_{j(1)}...a_{j(k+2)})^e}$$

que é zero. Daí $d^{k+1} \circ d^k = 0$, e a prova está completa. □

Exemplo 4.2.5. Vamos escrever explicitamente o complexo de Čech $C^\bullet = C(R)^\bullet$ de R com respeito a $a_1, ..., a_n$, no caso que $n = 3$. O complexo é

$$0 \to R \xrightarrow{d^0} R_{a_1} \oplus R_{a_2} \oplus R_{a_3} \xrightarrow{d^1} R_{a_2a_3} \oplus R_{a_1a_3} \oplus R_{a_1a_2} \xrightarrow{d^2} R_{a_1a_2a_3} \to 0$$

onde os d^i ($i = 0,1,2$) são descritos como segue. Para $r, r_1, r_2, r_3 \in R$ e $e_1, e_2, e_3 \in \mathbb{N}_0$,

$$d^0(r) = \left(\frac{r}{1}, \frac{r}{1}, \frac{r}{1}\right),$$

$$d^1\left(\left(\frac{r_1}{a_1^{e_1}}, \frac{r_2}{a_2^{e_2}}, \frac{r_3}{a_3^{e_3}}\right)\right) = \left(\frac{a_2^{e_3} r_3}{(a_2a_3)^{e_3}} - \frac{a_3^{e_2} r_2}{(a_2a_3)^{e_2}}, \frac{a_1^{e_3} r_3}{(a_1a_3)^{e_3}} - \frac{a_3^{e_1} r_1}{(a_1a_3)^{e_1}}, \frac{a_1^{e_2} r_2}{(a_1a_2)^{e_2}} - \frac{a_2^{e_1} r_1}{(a_1a_2)^{e_1}}\right)$$

e

$$d^2\left(\left(\frac{r_1}{(a_2a_3)^{e_1}}, \frac{r_2}{(a_1a_3)^{e_2}}, \frac{r_3}{(a_1a_2)^{e_3}}\right)\right) = \frac{a_1^{e_1} r_1}{(a_1a_2a_3)^{e_1}} - \frac{a_2^{e_2} r_2}{(a_1a_2a_3)^{e_2}} + \frac{a_3^{e_3} r_3}{(a_1a_2a_3)^{e_3}}.$$

Teorema 4.2.6. *Sejam $a_1, ..., a_n$ os n geradores do ideal I de R. Existem isomorfismos naturais*

$$(\gamma^i)_{i\in\mathbb{N}_0} : (H^i(C(-)^\bullet))_{i\in\mathbb{N}_0} \xrightarrow{\cong} (H_I^i)_{i\in\mathbb{N}_0},$$

ou seja, os módulos de cohomologia local são dados pela cohomologia do complexo de Čech.

Demonstração. A demonstração desse teorema é dada em [**?**], Thm. 5.1.20. □

Corolário 4.2.7. *Seja M um R-módulo finitamente gerado, onde R é uma álgebra regular finitamente gerada sobre um anel local regular F-finito de característica $p > 0$. Então, os módulos de cohomologia local de M, com respeito a qualquer ideal de R, tem comprimento finito na categoria de D_R-módulos.*

Demonstração. Pelo teorema anterior, temos que $H_I^i(M) \cong H^i(C(M)^\bullet)$, para todo ideal I de R. Então basta ver que os componentes do complexo de Čech de M, com respeito a sequência $a_1, ..., a_n$ de geradores de I, tem comprimento finito na categoria de D_R-módulos. Tais componentes são soma diretas de localizações de M com respeito a elementos de R, logo temos a igualdade $C(M)^\bullet = C^\bullet \otimes_R M$, onde $C^\bullet = C(R)^\bullet$. Assim,

$$C(M)^0 = C(R)^0 \otimes_R M = R \otimes_R M \ \ e$$

$$C(M)^k = C(R)^k \otimes_R M = \left(\oplus_{i\in\mathcal{I}(k,n)} R_{a_{i(1)}\dots a_{i(k)}}\right) \otimes_R M,$$

onde a estrutura de D_R-módulo de $C(M)^0$ vem de R, e para $C(M)^k$ vem das localizações $R_{a_{i(1)}\dots a_{i(k)}}$ para $i \in \mathcal{I}(k,n)$. Temos ainda, pelo Teorema 1.3.10, que $R_{a_{i(1)}\dots a_{i(k)}}$ tem comprimento finito na categoria D_R-módulos, portanto $\oplus_{i\in\mathcal{I}(k,n)} R_{a_{i(1)}\dots a_{i(k)}}$ também. Como M é finitamente gerado como R-módulo, temos que $C(M)^k = C(R)^k \otimes_R M$ tem comprimento finito na categoria de D_R-módulos, para todo k. Disto, segue que os módulos de cohomologia local de M tem comprimento finito na categoria de D_R-módulos. □

Corolário 4.2.8. *Seja M um R-módulo finitamente gerado, onde R é uma álgebra finitamente gerada sobre $A = k[[x_1,...,x_d]]$, um anel de séries de potências formais sobre um corpo k de característica $p > 0$, como na notação da seção 2.4. Suponha que $R^* = A^* \otimes_A R$ é regular. Então, os módulos de cohomologia local de M, com respeito a qualquer ideal de R, tem comprimento finito na categoria de $D_{R|k}$-módulos.*

Demonstração. Segue de [[**?**], thm. 5.8(a)] que R_f tem comprimento finito na categoria de $D_{R|k}$-módulos. □

Referências

[ABL05] ALVAREZ-MONTANER, J., BLICKLE, M. and LYUBEZNIK, G., *Generators of D-modules in positive characteristic*, Mathematical Research Letters, v. 12, p. 459 - 473, 2005.

[Ber72] BERNSTEIN, I. N., *Analytic continuation of generalized functions with respect to a parameter*, Funkcional. Anal. i Priložen., v. 6, no. 4, p. 26 - 40, 1972.

[Bjö79] BJÖRK, J. E., *Ring of differential operators*, North Holland Mathematics Library, v. 21, North-Holland Publishing Co., Amsterdam-New York, 1979.

[Bli01] BLICKLE, M., *The intersection homology D-module in finite characteristic*, Ph.D thesis, University of Michigan, 2001, arXiv:math.AG/0110244.

[Bog95] BOGVAD, R., *Some results on D-modules on Borel varieties in characteristic* $p > 0$, J. Algebra, v. 173, no. 3, p. 638 - 667, 1995.

[BrS13] BRODMANN, M. P. and SHARP, R. Y., *Local cohomology, as algebraic introduction with geometric applicatins*, Second Edition, Cambridge University Press, Cambridge, 2013.

[BHr98] BRUNS, W. and HERZOG, J., *Cohen-Macaulay rings*, Cambridge Studies in Advanced Mathematics 39, Revised Edition (Cambridge University Press, Cambridge, 1998).

[Mil99] MILIČIĆ, D., *Lectures on algebraic theory of D-Modules*, <https://www.math.utah.edu/ milicic/>, 1999.

[Kun69] KUNZ, E., *Characterization of regular locals rings in characteristic p*, Amer J. Math, v. 91, p. 772 - 784, 1969.

[Lyu97] LYUBEZNIK, G., *F-modules: an application to local cohomology and D-modules in characteristic* $p > 0$, J. Reine Angew, v. 491, p. 65-130, 1997.

[Mat92] MATSUMURA, H., *Commutative Ring Theory*. Cambridge Studies in Advanced Mathematics, 8, Cambridge University Press, 1992.

[Wal05] WALTHER, U., *Bernstein-Sato polynomials versus cohomology of the Milnor fiber for generic hyperplane arrangements*, Compositio Math, v. 141, no. 1, p. 121 - 145, 2005.

[Yan78] YANO, T., *On the theory of b-functions*, Publ. Res. Inst. Math. Sci., v. 14, no. 1, p. 111 - 202, 1978.

[Yek92] YEKUTIELI, A., *An explicit construction of the Grothendieck residue complex*, appendix by Pramathanath Sastry. Astérisque No. 208, 1992.

Apêndice A : Conceitos básicos

A.1 Categorias

Uma **categoria** consiste de uma coleção de **objetos**, e para cada par de objetos, um conjunto de **morfismos** (ou setas) entre eles. A coleção de objetos de uma categoria C é frequentemente denotada por $\mathrm{obj}(C)$, mas denotaremos apenas por C. Se $A, B \in C$, então o conjunto de morfismos de A para B é denotado por $\mathrm{Mor}(A,B)$. Um morfismo é frequentemente escrito $f : A \to B$. Existe uma composição entre morfismos $\mathrm{Mor}(B,C) \times \mathrm{Mor}(A,B) \to \mathrm{Mor}(A,C)$, e se $f \in \mathrm{Mor}(A,B)$ e $g \in \mathrm{Mor}(B,C)$, então a composição denotada por $g \circ f \in \mathrm{Mor}(A,C)$. A composição é associativa: se $f \in \mathrm{Mor}(A,B)$, $g \in \mathrm{Mor}(B,C)$ e $h \in \mathrm{Mor}(C,D)$, então $h \circ (g \circ f) = (h \circ g) \circ f$. Para cada objeto $A \in C$, existe sempre o morfismo **identidade** $id_A : A \to A$, tal que a composição, pela direita ou pela esquerda, de um morfismo com o morfismo identidade, obtemos o mesmo morfismo, ou seja, para quaiquer morfismos $f : A \to B$ e $g : B \to C$, $id_B \circ f = f$ e $g \circ id_B = g$. Note que o morfismo identidade é único.

Temos uma noção de **isomorfismo** entre dois objetos de uma categoria (um morfismo $f : A \to B$ tal que existe algum, não necessariamente único, morfismo $g : B \to A$, onde $f \circ g = id_B$ e $g \circ f = id_A$).

Exemplo A.1.1 (Grupos abelianos)**.** Os grupos abelianos, junto com os homomorfismos de grupo, formam a categoria $\mathcal{A}b$.

Exemplo A.1.2 (Módulos sobre um anel)**.** Se A é um anel, então os A-módulos formam junto com os mapas A-lineares formam a categoria Mod_A. Tomando $A = k$ um corpo, temos a categoria Vec_k de espaços vetoriais sobre k; e tomando $A = \mathbb{Z}$ temos $\mathcal{A}b$.

Definição A.1.3. Uma **subcategoria** $\mathcal{A}$ de uma categoria $\mathcal{B}$ tem como seus objetos alguns objetos de $\mathcal{B}$, e alguns de seus morfismos, tal que os morfismos de $\mathcal{A}$ inclui o morfismo identidade dos objetos de $\mathcal{A}$, e são fechados para composição.

Um **funtor covariante** F da categoria $\mathcal{A}$ para a categoria $\mathcal{B}$, denotado por $F : \mathcal{A} \to \mathcal{B}$, é definido da seguinte maneira: F é um mapa de objetos $F : \mathrm{obj}(\mathcal{A}) \to \mathrm{obj}(\mathcal{B})$, para cada $A_1, A_2 \in \mathcal{A}$ e morfismo $m : A_1 \to A_2$, temos que F é um mapeia m no morfismo $F(m) : F(A_1) \to F(A_2)$ de $\mathcal{B}$. F preserva morfismos identidade (para $A \in \mathcal{A}, F(id_A) = id_{F(A)}$), e preserva composição ($F(m \circ m_1) = F(m_2) \circ F(m_1)$). Note que F manda isomorfismos em isomorfismos. Um exemplo simple é o funtor identidade $id : \mathcal{A} \to \mathcal{A}$.

Se $F : \mathcal{A} \to \mathcal{B}$ e $G : \mathcal{B} \to \mathcal{C}$ são funtores covariantes, podemos definir a composição $G \circ F : \mathcal{A} \to \mathcal{C}$ de maneira óbvia.

Um **funtor contravariante** é definido da mesma maneira que o funtor covariante, exceto o sentido dos morfismos ($F(A_1 \to A_2)$ agora é um morfismo de $F(A_2)$ para $F(A_1)$). Daí $F(m_2 \circ m_1) = F(m_1) \circ F(m_2)$, e não $F(m_2) \circ F(m_1)$.

Exemplo A.1.4 (Álgebra linear)**.** Se Vec_k é a categoria dos espaços vetoriais sobre o corpo k, então tomar o dual é um funtor contravariante $(\cdot)^* : Vec_k \to Vec_k$. De fato, para cada transformação linear $f : V \to W$, temos a transformação dual $f^* : W^* \to V^*$, e $(f \circ g)^* = g^* \circ f^*$.

Sejam F e G dois funtores covariantes de $\mathcal{A}$ para $\mathcal{B}$. Uma **transformação natural de funtores covariantes** $F \to G$ é definido da seguinte maneira: para cada $A \in \mathcal{A}$ temos um morfismo $m_A : F(A) \to G(A)$ em $\mathcal{B}$, tal que para cada morfismo $f : A \to A'$ em $\mathcal{A}$, o diagrama

$$\begin{tikzcd} F(A) \arrow[r, "F"] \arrow[d, "m_A"'] & F(A') \arrow[d, "m_{A'}"] \\ G(A) \arrow[r, "G(f)"] & G(A') \end{tikzcd}$$

comuta. Um **isomorfismo natural** de funtores é uma tranformação natural tal que cada m_A é um isomorfismo. Seja $F : \mathcal{A} \to \mathcal{B}$, e suponha que exista $F' : \mathcal{B} \to \mathcal{A}$ tal que $F \circ F'$ é naturalmente isomorfo ao funtor identidade $id_{\mathcal{B}}$ e $F' \circ F$ é naturalmente isomorfo a $id_{\mathcal{A}}$, dizemos que F é uma **equivalência de categorias**. Equivalência de categorias é uma relação de equivalência em categorias. A noção de quando duas categorias são "essencialmente a mesma"não é isomorfismo (um funtor dando bijeções de objetos e morfismos), mas equivalência.

Exemplo A.1.5. Seja $\mathcal{V}$ a categoria cujos objetos são os k-espaços vetoriais k^n, para $n \geq 0$, junto com as transformações lineares entre eles. Os objetos de $\mathcal{V}$ podem ser k-espaços vetorias com bases, e os morfismos como matrizes. Temos que $\mathcal{V} \to f.d.Vec_k$ é uma equivalência de categorias, onde $f.d.Vec_k$ é a categoria dos k-espaços vetoriais de dimensão finita, e é óbvio que $\mathcal{V}$ é uma subcategoria estrita de $f.d.Vec_k$.

A.2 Produto tensorial

Seja A um anel e L, M e N A-módulos. Dizemos que um mapa $\varphi : M \times N \to L$ é *bilinear* se fixando uma das entradas ele é A-linear na outra, isto é, se

$$\varphi(x + x', y) = \varphi(x, y) + \varphi(x', y), \quad \varphi(ax, y) = a\varphi(x, y);$$

$$\varphi(x, y + y') = \varphi(x, y) + \varphi(x, y'), \quad \varphi(x, ay) = a\varphi(x, y).$$

Escrevemos $\mathcal{L}(M, N; L)$ ou $\mathcal{L}_A(M, N; L)$ para denotar o conjunto de todos os mapas bilineares de $M \times N$ para L, e esse conjunto tem estrutura de A-módulo (visto que A é comutativo).

Se $g : L \to L'$ é um mapa A-linear e $\varphi \in \mathcal{L}(M,N;L)$, então $g \circ \varphi \in \mathcal{L}(M,N;L')$. Com isso em mente, dados M e N, considere um mapa bilinear $\otimes : M \times N \to L_0$ tendo a seguinte propriedade, onde escrevemos $x \otimes y$ ao invés de $\otimes(x,y)$: Para cada A-módulo L e qualquer $\varphi \in \mathcal{L}(M,N;L)$, existe um único mapa A-linear $g : L_0 \to L$ satisfazendo

$$g(x \otimes y) = \varphi(x,y).$$

Se isso acontece, dizemos que L_0 é o *produto tensorial* de M e N sobre A, e escrevemos $L_0 = M \otimes_A N$; as vezes omitimos A e escrevemos $M \otimes N$. Assumindo sua existência, é unicamente determinado, a menos de isomorfismo. Para provar a existência, escreva F o A-módulo livre com base o conjunto $M \times N$, ou seja, os elementos de F são combinações lineares formais dos elementos de $M \times N$, isto é, expressões da forma $\sum_{i=1}^{n} a_i(x_i,y_i)$, com $a_i \in A, x_i \in M$ e $y_i \in N$. Seja $R \subset F$ o submódulo gerado por todos os elementos da forma

$$(x+x',y)-(x,y)-(x',y), \quad (ax,y)-a(x,y),$$

$$(x,y+y')-(x,y)-(x,y'), \quad (x,ay)-a(x,y).$$

Então $M \otimes N = F/R$ e escrevemos $x \otimes y$ para denotar a imagem em $M \otimes N$ de $(x,y) \in F$. Note que em geral um elemento de $M \otimes N$ é uma soma da forma $\sum x_i \otimes y_i$. Para A-módulos M,N e L, a definição de produto tensorial nos dá:

Fórmula 1. $\mathrm{Hom}_A(M \otimes N, L) \cong \mathcal{L}(M,N;L)$.

Podemos definir mapas multilineares de um produto de A-módulos $M_1,...,M_r$ para um A-módulo L como no caso bilinear, e tomar os módulos $\mathcal{L}(M_1,...,M_r;L)$ e $M_1 \otimes_A \cdots \otimes_A M_r$; e obtemos 'associatividade':

Fórmula 2. $(M \otimes_A M') \otimes_A M" = M \otimes_A M' \otimes_A M" = M \otimes_A (M' \otimes_A M")$.

E também:

Fórmula 3. $M \otimes_A N \cong N \otimes_A M$;

Fórmula 4. $M \otimes_A A = M$;

Fórmula 5. $\left(\bigoplus_\lambda M_\lambda\right) \otimes_A N = \bigoplus_\lambda (M_\lambda \otimes_A N)$.

Se $f : M \to M'$ e $g : N \to N'$ são mapas A-lineares, então $(x,y) \mapsto f(x) \otimes g(y)$ é mapa bilinear de $M \times N$ para $M' \otimes_A N'$, disto podemos definir um mapa linear $M \otimes_A N \to M' \otimes_A N'$, denotado por $f \otimes g$:

Fórmula 6. $(f \otimes g)(\sum_i x_i \otimes y_i) = \sum_i f(x_i) \otimes g(y_i)$.

Se a sequência $M_1 \xrightarrow{f} M_2 \xrightarrow{g} M_3 \to 0$ é exata, então

$$M_1 \otimes N \xrightarrow{f\otimes 1} M_2 \otimes N \xrightarrow{g\otimes 1} M_3 \otimes N \to 0$$

também é exata, onde $1(= id_N)$ é o mapa identidade em N. Ou seja:

Fórmula 7. (Tomar produto tensorial é exato à direita)

Em geral, se $f : M \to M'$ é injetivo, $f \otimes 1 : M \otimes N \to M' \otimes N$ não necessariamente é injetivo. Se $f \otimes 1 : M \otimes N \to M' \otimes N$ é injetivo, sempre que $f : M \to M'$ for, então dizemos que o A-módulo N é *plano*.

Exemplo A.2.1. Seja $A = \mathbb{Z}$ e $N = \mathbb{Z}/n\mathbb{Z}$ para algum $n > 1$. Seja o mapa injetivo $f : \mathbb{Z} \to \mathbb{Z}$ dado pela multiplicação por n; Então $\mathbb{Z} \otimes_{\mathbb{Z}} N \cong N \neq 0$, mas $f \otimes 1 : N \xrightarrow{n} N$ é o mapa nulo. Portanto, $f \otimes 1$ não é injetivo.

Sejam A e B anéis, e P um A-B-bimódulo; isto é, para $a \in A, b \in B$ e $x \in P$ os produtos ax e $x \cdot b$ estão definidos, e são compatíveis, ou seja

$$(ax) \cdot b = a(x \cdot b).$$

Então a multiplicação por um elemento $b \in B$ induz um mapa A-linear de P nele mesmo, que vamos denotar por b. Isso determina um mapa $1 \otimes b : M \otimes_A P \to M \otimes_A P$ para qualquer A-módulo M, e por definição temos uma multiplicação por b em $M \otimes_A P$,

$$(\sum y_i \otimes x_i) \cdot b = \sum y_i \otimes x_i b$$

para todo $y_i \in M$ e $x_i \in P$, ou seja, uma estrutura de B-módulo. Disto, é fácil verificar

Fórmula 8. $(M \otimes_A P) \otimes_B N \cong M \otimes_A (P \otimes_B) N$, para todo B-módulo N.

Sejam $f : A \to B$ homomorfismo de anéis e M A-módulo. Note que B é um A-B-módulo, com $a \cdot b = f(a)b$. Então $B \otimes_A M$ é um B-módulo, chamado *extensão de escalares* em M de A para B.

Fórmula 9. $(M \otimes_A B) \otimes_B (M' \otimes_A B) \cong (M \otimes_A M') \otimes_A B$

Uma A-*álgebra* B é um anel B junto com um homomorfismo de anéis $f : A \to B$. Seja C com $g : A \to C$, uma outra A-ágebra. Dizemos que $\lambda B \to C$ é um homomorfismo de A-álgebras se for um homomorfismo de anéis e satisfaz $g = \lambda \circ f$, ou seja, se λ for A-linear também. Podemos tomar o produto tensorial $B \otimes_A C$, B e C como A-módulos, e ainda temos uma A-álgebra, com produto

$$\left(\sum_i b_i \otimes c_i\right)\left(\sum_j b_j \otimes c_j\right) = \sum_{i,j} b_i b_j \otimes c_i c_j,$$

e o homomorfismo de anéis $A \to B \otimes_A C$ dado por $a \mapsto a \otimes 1 (= 1 \otimes a)$.

Exemplo A.2.2. Se B é uma A-álgebra e $A[X]$ é o anel de polinômios sobre A, então $B \otimes_A A[X]$ pode ser identificado com $B[X]$.

A.3 Anéis regulares

Seja A um anel local Noetheriano com ideal maximal $\mathbf{m}$. Seja $k = A/\mathbf{m}$ o corpo residual de A. Como A é Noetheriano, $\mathbf{m}$ é finitamente gerado, digamos por $a_1, a_2, ..., a_p$. Temos que, as classes $\bar{a}_1, \bar{a}_2, ..., \bar{a}_p$ geram $\mathbf{m}/\mathbf{m}^2$, como k-espaço vetorial, disto temos que $dim_k(\mathbf{m}/\mathbf{m}^2) < +\infty$.

Lema A.3.1. *$dim_k(\mathbf{m}/\mathbf{m}^2)$ é o menor número de geradores de $\mathbf{m}$.*

Demonstração. Seja $s = dim_k(\mathbf{m}/\mathbf{m}^2)$. Então podemos encontrar $a_1, a_2, ..., a_s \in \mathbf{m}$ tais que $\bar{a}_1, \bar{a}_2, ..., \bar{a}_s$ formam uma base para $\mathbf{m}/\mathbf{m}^2$. Vamos mostrar que esses elementos geram $\mathbf{m}$. Seja I o ideal gerado por $a_1, a_2, ..., a_s$. Então $I + \mathbf{m}^2 = \mathbf{m}$ e $\mathbf{m}(\mathbf{m}/I) = \mathbf{m}/I$. Daí, por *Nakayama*, temos que $\mathbf{m}/I = 0$. □

Para qualquer s-úpla $(a_1, a_2, ..., a_s)$ de elementos de $\mathbf{m}$ tal que $(\bar{a}_1, \bar{a}_2, ..., \bar{a}_s)$ forma uma base para $\mathbf{m}/\mathbf{m}^2$, chamamos um *sistema de coordenadas* em A.

Considere a filtração $\mathbf{m} \supset \mathbf{m}^2 \supset \mathbf{m}^3 \supset \mathbf{m}^4 \supset ...$ de A. Então podemos formar o anel graduado $\mathrm{Gr}A = \oplus_{p=o}^{\infty} \mathbf{m}^p/\mathbf{m}^{p+1}$. Afirmamos que $\mathrm{Gr}A$ é k-álgebra finitamente gerada, e portanto, anel graduado Noetheriano, vide Lema1.1 de [Dra99]. Mais ainda, o mapa $X_i \mapsto \bar{a}_i \in \mathbf{m}/\mathbf{m}^2 \subset \mathrm{Gr}A$ se estende a um epimorfismo de $k[X_1, X_2, ..., X_s]$ em $\mathrm{Gr}A$.

Definição A.3.2. Dizemos que o anel local Noetheriano A é dito *regular* se $\mathrm{Gr}A$ e $k[X_1, X_2, ..., X_s]$ são isomorfos.

Teorema A.3.3. *Seja A um anel local regular. Então A é um domínio.*

Demonstração. Sejam $a, b \in A$ com $a \neq 0$, $b \neq 0$. Então podemos encontrar $p, q \in \mathbb{Z}_+$ tais que $a \in \mathbf{m}^p$, $a \notin \mathbf{m}^{p+1}$ e $b \in \mathbf{m}^q$, $b \notin \mathbf{m}^{q+1}$. Então suas imagens $\bar{a} \in \mathbf{m}^p/\mathbf{m}^{p+1}$ e $\bar{b} \in \mathbf{m}^q/\mathbf{m}^{q+1}$ são diferentes de zero, como $\mathrm{Gr}A$ é inteiro, temos que $\bar{a}\bar{b} \neq 0$. Portanto, $ab \neq 0$. □

Exemplo A.3.4. Sejam k um corpo, $A = k[X_1, X_2, ..., X_n]$ o anel de polinômios em n-variáveis com coeficientes em k e $\hat{A} = k[[X_1, X_2, ..., X_n]]$ o anel de séries de potências formais em n-variáveis com coeficientes em k. É fácil verificar que $\hat{A}$ é um anel local Noetheriano com ideal maximal $\hat{\mathbf{m}}$ gerado por $X_1, X_2, ..., X_n$. E também, que o mapa canônico de $k[X_1, X_2, ..., X_n]$ em $\mathrm{Gr}\hat{A}$ é claramente um isomorfismo.

Teorema A.3.5 (Serre)**.** *Seja A um anel local regular e P um ideal primo, então A_P é regular.*

Demonstração. Theorem 19.3 de [**?**]. □

Definição A.3.6. Um anel Noetheriano R é dito *regular* se a localização em cada ideal primo é regular. E pelo teorema anterior, R é regular se a localização em cada ideal maximal for regular.

Exemplo A.3.7. Para cada $x \in k^n$, denotamos por $\mathbf{m}_x$ o ideal maximal de A gerado por $X_1 - x_1, X_2 - x_2, ..., X_n - x_n$; e A_x a localização de A nesse ideal maximal. Temos que, A_x é um anel local Noetheriano com ideal maximal $\mathbf{n}_x = (\mathbf{m}_x)_x$. O automorfismo de A definito por $X_i \mapsto X_i - x_i$, $1 \leq i \leq n$, nos fornece um isomorfismo de A_0 em A_x para cada $x \in k^n$. por outro lado, o homomorfismo natural de A em estende a um monomorfismo de A_0 em $\hat{A}$. Esse monomorfismo preserva filtrações e induz um isomorfismo canônico de $\mathrm{Gr}A_0$ em $\mathrm{Gr}\hat{A}$. Portanto, os anéis A_x, $x \in k^n$, são anéis locais regulares, ou seja, A é anel regular.

Por fim, a importância de anéis regulares nesta dissertação é devido a este resultado crucial:

Teorema A.3.8 (Kunz)**.** *Seja R anel local regular de característica p, então R é módulo plano sobre o anel R^{p^s}, para todo $s \in \mathbb{Z}_+$.*

Demonstração. [**?**] □

Apêndice B : Operadores diferenciais

B.1 Operadores diferenciais em característica zero

Sejam k um corpo de característica zero e A uma álgebra sobre k. Seja $\mathrm{End}_k(A)$ a álgebra dos endomorfismos k-lineares de A. Consideramos o comutador $[S,T] = ST - TS$ em $\mathrm{End}_k(A)$. Claramente, $\mathrm{End}_k(A)$ contém, como uma subálgebra, o conjunto $\mathrm{End}_A(A)$ dos endomorfismos A-lineares. Identificando cada elemento $a \in A$ com o endomorfismo A-linear $b \mapsto ab$ de $\mathrm{End}_A(A)$, e todo $T \in \mathrm{End}_k(A)$ com $T(1) \in A$, temos que A e $\mathrm{End}_A(A)$ são isomorfos e podemos considerar A como subálgebra de $\mathrm{End}_k(A)$.

Uma k-derivação de A é um $T \in \mathrm{End}_k(A)$ tal que

$$T(ab) = T(a)b + aT(b)$$

para todo $a,b \in A$. Em particular, $[T,a](b) = T(ab) - aT(b)$, isto é, $[T,a] = T(a) \in A$ para todo $a \in A$. Isso implica que $[[T,a_0],a_1] = 0$, para todo $a_0,a_1 \in A$. Esse fato nos motiva dar a seguinte definição. Seja $n \in \mathbb{Z}_+$. Dizemos que um elemento $T \in \mathrm{End}_k(A)$ é um *operador diferencial* ($k - linear$) em A de *ordem* $\leq n$ se

$$[...[[T,a_0],a_1],...,a_n] = 0$$

para todo $a_0,a_1,...,a_n \in A$. Denotamos por $\mathrm{Diff}_k(A)$ o k-espaço dos operadores diferenciais em A.

Teorema B.1.1. *Seja T,S dois operadores diferenciais de ordens $\leq n$, $\leq m$ respectivamente. Então TS é um operador diferencial de ordem $\leq n+m$.*

Demonstração. Provamos por indução em $n+m$. Se $n = m = 0$, $T,S \in \mathrm{End}_A(A)$, daí $TS \in \mathrm{End}_A(A)$, ou seja, um operador diferencial de ordem 0. Assuma que vale para $n+m-1$. Então

$$[TS,a] = TS(a) - aTS = T[S,a] + [T,a]S,$$

e $[T,a]$ e $[S,a]$ são operadores diferenciais de ordem $\leq n-1$ e $\leq m-1$ respectivamente. Por indução, $[TS,a]$ é um operador diferencial de ordem $\leq n+m-1$. Portanto, TS é de ordem $\leq n+m$. □

Disto temos que $\mathrm{Diff}_k(A)$ é uma subálgebra de $\mathrm{End}_k(A)$, chamamos *álgebra dos operadores diferenciais k-lineares* de A. Façamos $\mathrm{F}_n\mathrm{Diff}_k(A) = \{0\}$ para $n < 0$ e

$$\mathrm{F}_n\mathrm{Diff}_k(A) = \{T \in \mathrm{Diff}_k(A); \mathrm{ordem}(T) \leq n\}$$

para $n \geq 0$. Claramente, vemos que os $\mathrm{F}_n\mathrm{Diff}_k(A)$ formam uma filtração crescente exaustiva ($\bigcup_{n\in\mathbb{Z}} \mathrm{F}_n\mathrm{Diff}_k(A) = \mathrm{Diff}_k(A)$) de $\mathrm{Diff}_k(A)$ por espaços vetoriais sobre k. Essa filtração é compatível com a estrutura de anel de $\mathrm{Diff}_k(A)$, ou seja, ela satisfaz

$$\mathrm{F}_n\mathrm{Diff}_k(A) \circ \mathrm{F}_m\mathrm{Diff}_k(A) \subset \mathrm{F}_{n+m}\mathrm{Diff}_k(A)$$

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

Lema B.1.2. **(i)** $\mathrm{F}_0\mathrm{Diff}_k(A) = A$*;*

(ii) $\mathrm{F}_1\mathrm{Diff}_k(A) = \mathrm{Der}_k(A) \oplus A$*;*

(iii) $[\mathrm{F}_n\mathrm{Diff}_k(A), \mathrm{F}_m\mathrm{Diff}_k(A)] \subset \mathrm{F}_{n+m-1}\mathrm{Diff}_k(A)$*, para todo* $n, m \in \mathbb{Z}_+$*.*

Demonstração. (i) é claro. (ii) Como vimos antes, $\mathrm{Der}_k(A) \subset \mathrm{F}_1\mathrm{Diff}_k(A)$. Para todo $T \in \mathrm{Der}_k(A)$, temos $T(1) = T(1 \cdot 1) = 2T(1)$, daí $T(1) = 0$. Isso implica que $\mathrm{Der}_k(A) \cap A = \{0\}$. Seja $S \in \mathrm{F}_1\mathrm{Diff}_k(A)$ e $T = S - S(1)$. Então, $T(a) = [T, a](1)$, e

$$\begin{aligned} T(ab) &= [T, ab](1) \\ &= ([T, a]b)(1) + (a[T, b])(1) \\ &= (b[T, a])(1) + (a[T, b])(1) \\ &= T(a)b + aT(b), \end{aligned}$$

ou seja, $T \in \mathrm{Der}_k(A)$.

(iii) Sejam T, S de ordem $\leq n, \leq m$ respectivamente. Vamos mostrar que $[T, S]$ é de ordem $\leq n + m - 1$. Provamos por indução em $n + m$. Se $n = m = 0$, não há nada a provar. Em geral, pela identidade de *Jacobi*, temos

$$[[T, S], a] = [[T, a], S] + [T, [S, a]]$$

onde $[T, a]$ e $[S, a]$ são de ordem $\leq n - 1$ e $\leq m - 1$ respectivamente. Daí, por indução, $[[T, S], a]$ é de ordem $\leq n + m - 2$ e $[T, S]$ de ordem $\leq n + m - 1$. □

Seja $A = k[X_1, X_2, ..., X_n]$. Então denotamos $D(n) = \mathrm{Diff}_k(A)$. Dizemos que $D(n)$ é a *álgebra dos operadores diferenciais em* k^n. Sejam $\partial_1, \partial_2, ..., \partial_n$ as derivações parciais de A. Para $I, J \in \mathbb{Z}_+^n$ façamos

$$X^I = X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$$

e

$$\partial^J = \partial_1^{j_1} \partial_2^{j_2} \cdots \partial_n^{j_n}.$$

Então $X^I\partial^J \in D(n)$, e tem ordem $\leq |J| = j_1 + j_2 + \cdots + j_n$. Mais ainda, se T é um operador diferencial dado por

$$T = \sum_{|I|\leq p} P_I(X_1, X_2, ..., X_n)\partial^I,$$

onde $P_I \in A$, temos que T é de ordem $\leq p$.

Lema B.1.3. *As derivações $\partial_1, \partial_2, ..., \partial_n$ formam uma base para o A-módulo livre $Der_k(A)$.*

Demonstração. Seja $T \in \mathrm{Der}_k(A)$. Tome $P_i = T(X_i)$, para $1 \leq i \leq n$, e defina $S = \sum_{i=1}^n P_i\partial_i$. Claramente,

$$S(X_i) = \sum_{j=1}^{n} P_j\partial_j(X_i) = P_i = T(X_i)$$

para todo $1 \leq i \leq n$. Visto que $X_1, X_2, ..., X_n$ geram A como uma k-álgebra, segue que $T = S$. Portanto, $\partial_1, \partial_2, ..., \partial_n$ geram o A-módulo $\mathrm{Der}_k(A)$. Suponha que $\sum_{i=1}^n Q_i\partial_i = 0$ para certos $Q_i \in A$. Então $0 = \left(\sum_{j=1}^n Q_j\partial_j\right)(X_i) = Q_i$, para todo $1 \leq i \leq n$. Isso implica que $\partial_1, \partial_2, ..., \partial_n$ são geradores livres de $\mathrm{Der}_k(A)$. □

Por fim, temos uma caracterização de $D(n)$ que é frequentemente usada, cuja demonstração será omitida.

Teorema B.1.4. *A k-álgebra $D(n)$ é a k-álgebra gerada por $X_1, X_2, ..., X_n$ e $\partial_1, \partial_2, ..., \partial_n$, satifazendo as seguintes relações*

$$[X_i, X_j] = 0 \ \ , \ \ [\partial_i, \partial_j] = 0 \ \ e \ \ [\partial_i, X_j] = \delta_{ij}$$

para todo $1 \leq i \leq n$.

Demonstração. [$Mil99$]. □

B.2 Demonstração do Teorema 1.1.4

Neste apêndice damos uma demonstração do Teorema 1.1.4, baseada no texto [**?**].

Seja I_R o núcleo do mapa $R \otimes_k R \to R$, $x \otimes y \mapsto xy$, onde k é um anel comutativo e R uma k-álgebra comutativa. Defina $\mathcal{P}^n_{R/k} := R \otimes_k R/I_R^{n+1}$. Considere $\mathcal{P}^n_{R/k}$ como uma R-álgebra via $r \to \overline{r \otimes 1}$, e tome $d^n(r) := \overline{1 \otimes r}$. d^n define uma estrutura de R-módulo à direita em $\mathcal{P}^n_{R/k}$, ou seja, $a \cdot r := ad^n(r)$, para todo $a \in \mathcal{P}^n_{R/k}$ e $r \in R$.

Proposição B.2.1. *Sejam k um anel comutativo, R uma k-álgebra comutativa e $\mathrm{Diff}^n_{R/k}(R)$ o R-módulo dos operadores diferenciais k-lineares de ordem $\leq n$ de R. Então,*

$$\mathrm{Hom}_R(\mathcal{P}^n_{R/k}, R) \cong \mathrm{Diff}^n_{R/k}(R).$$

Demonstração. Considere o mapa $\phi : \mathrm{Hom}_R(\mathcal{P}^n_{R/k}, R) \to \mathrm{Diff}^n_{R/k}(R)$, dado por $\phi(T) = T \circ d^n$. O objetivo é mostrar que ϕ é isomorfismo de R-módulos, e que seu inverso é $\psi : \mathrm{Diff}^n_{R/k}(R) \to \mathrm{Hom}_R(\mathcal{P}^n_{R/k}, R)$, dado por $\psi(\delta) = \delta^*$, com $\delta^*(\overline{x \otimes y}) := x\delta(y)$.

Seja $T \in \mathrm{Hom}_R(\mathcal{P}^n_{R/k}, R)$, então

$$T \overset{\phi}{\mapsto} T \circ d^n \overset{\psi}{\mapsto} (T \circ d^n)^*,$$

onde $(T \circ d^n)^*(\overline{x \otimes y}) = xT(d^n(y)) = T(\overline{x \otimes y})$, logo $\psi \circ \phi = id_{\mathrm{Hom}_R(\mathcal{P}^n_{R/k}, R)}$. Seja $\delta \in \mathrm{Diff}^n_{R/k}(R)$, então

$$\delta \overset{\psi}{\mapsto} \delta^* \overset{\phi}{\mapsto} \delta^* \circ d^n,$$

onde $\delta^* \circ d^n(r) = \delta^*(\overline{1 \otimes r}) = \delta(r)$, logo $\phi \circ \psi = id_{\mathrm{Diff}^n_{R/k}(R)}$. Basta verificar a boa-definição de ϕ e ψ.

Primeiro temos que mostrar que $T \circ d^n$ é um operador diferencial k-linear de ordem $\leq n$ de R, para todo $T \in \mathrm{Hom}_R(\mathcal{P}^n_{R/k}, R)$. Visto que T é R-linear e que $[T \circ d^n, \tilde{r}] = T \circ [d^n, \tilde{r}]$, é suficiente mostrar que $d^n \in \mathrm{Diff}^n_{R/k}(R, \mathcal{P}^n_{R/k})$, ou seja, $[...[[d^n, \tilde{r_0}], \tilde{r_1}], ..., \tilde{r_n}] = 0$, para todo $r_0, ..., r_n \in R$.

Observação B.2.2. $\mathrm{Diff}^n_{R/k}(R, \mathcal{P}^n_{R/k})$ é definido de maneira análoga à $\mathrm{Diff}^n_{R/k}(R)$, onde $\tilde{r}$ é a multiplicação à esquerda por r, ora em R, ora em $\mathcal{P}^n_{R/k}$, veja a seção 1.4 de [**?**].

Seja $x \in R$.

$$\begin{aligned}
& [...[[d^n, \tilde{r_0}], \tilde{r_1}], ..., \tilde{r_n}](x) \\
= \;& d^n\left(\left(\prod_{i=0}^n r_i\right)x\right) - \sum_{i=0}^n r_i \cdot d^n\left(\left(\prod_{j\neq i} r_j\right)x\right) + ... + (-1)^{n+1}\left(\prod_{i=0}^n r_i\right) \cdot d^n(x) \\
= \;& \overline{1 \otimes \left(\prod_{i=0}^n r_i\right)x} - \overline{\left(\sum_{i=0}^n r_i\right) \otimes \left(\prod_{j\neq i} r_j\right)x} + ... + (-1)^{n+1}\overline{\left(\prod_{i=0}^n r_i\right) \otimes x} \\
= \;& \left[\overline{1 \otimes \left(\prod_{i=0}^n r_i\right)} - \overline{\left(\sum_{i=0}^n r_i\right) \otimes \left(\prod_{j\neq i} r_j\right)} + ... + (-1)^{n+1}\overline{\left(\left(\prod_{i=0}^n r_i\right) \otimes 1\right)}\right] d^n(x) \\
= \;& \left(\prod_{i=0}^n (1 \otimes r_i - r_i \otimes 1)\right) d^n(x) \\
= \;& 0,
\end{aligned}$$

na última igualdade temos que $\prod_{i=0}^n (1 \otimes r_i - r_i \otimes 1) \in I_R^{n+1}$.

Por δ ser k-linear, temos que δ^* é k-linear pela definição de produto tensorial, e

$$\delta^*(r \cdot (\overline{x \otimes y})) = \delta^*(\overline{(rx) \otimes y}) = (rx)\delta(y) = r(x\delta(y)) = r\delta^*(\overline{x \otimes y}),$$

ou seja, δ^* é R-linear. Agora seja $\prod_{i=0}^{n} x_i \otimes y_i \in I_R^{n+1}$,onde $x_i y_i = 0$ para cada i. Então

$$\begin{aligned}
& \delta^*\left(\overline{\prod_{i=0}^{n} x_i \otimes y_i}\right) \\
= \; & \delta^*\left(\overline{\left(\prod_{i=0}^{n} x_i\right) \otimes \left(\prod_{i=0}^{n} y_i\right)}\right) \\
= \; & \left(\prod_{i=0}^{n} x_i\right) \delta\left(\prod_{i=0}^{n} y_i\right) \\
= \; & \left(\prod_{i=0}^{n} x_i\right)\left[\sum_{i=0}^{n} y_i \delta\left(\prod_{j\neq i} y_j\right) - \sum_{i,j} y_i y_j \delta\left(\prod_{k\neq i, k\neq j} y_k\right) + \ldots + (-1)^{n+1} \prod_{i=0}^{n} y_i \delta(1)\right] \\
= \; & 0,
\end{aligned}$$

na terceira igualdade usamos o fato de δ ser operador diferencial k-linear de ordem $\leq n$ de R, $[...[[\delta, y_0], y_1], ..., y_n](1) = 0$ em R, e na quarta igualdade o fato que cada $x_i y_i = 0$. □

Lema B.2.3. *Seja k anel comutativo e R uma k-álgebra comutativa gerada por $r_1, ..., r_l$. Então I_R é gerado por $\{1 \otimes r_i - r_i \otimes 1\}_{i=1}^{l}$ como R-módulo.*

Demonstração. Como R é finitamente gerado por $r_1, ..., r_l$ como k-álgebra, temos o isomorfismo de k-álgebras $R \otimes_k R \cong k[r_1 \otimes 1, ..., r_l \otimes 1, 1 \otimes r_1, ..., 1 \otimes r_l]$. Assim o mapa $R \otimes_k R \to R$ dado por $x \otimes y \mapsto xy$, pode ser visto da seguinte forma,

$$k[r_1 \otimes 1, ..., r_l \otimes 1, 1 \otimes r_1, ..., 1 \otimes r_l] \to k[r_1, ..., r_l],$$

$$r_i \otimes 1 \mapsto r_i$$

$$1 \otimes r_i \mapsto r_i.$$

$R \otimes_k R$ tem estrutura de R-álgebra via $r \mapsto r \otimes 1$. Portanto, $R \otimes_k R \cong R[1 \otimes r_1, ..., 1 \otimes r_l]$ como R-álgebra. Disto, segue que o mapa acima fica

$$R[1 \otimes r_1, ..., 1 \otimes r_l] \to R$$

$$1 \otimes r_i \mapsto r_i.$$

Logo $I_R = \ker(R \otimes_k R \to R) = (R[1 \otimes r_1, ..., 1 \otimes r_l] \to R)$ é gerado como R-módulo por $\{1 \otimes r_i - r_i\}_{i=1}^{l}$, sendo r_i visto em $R \otimes_k R$, ou seja, $\{1 \otimes r_i - r_i \otimes 1\}_{i=1}^{l}$. □

Seja agora R um anel comutativo contendo um corpo k de característica $p > 0$. Temos

Lema B.2.4. *Seja R um $k[R^p]$-módulo finito com geradores $r_1, ..., r_l$. Então R é gerado por $r_1, ..., r_l$ como $k[R^{p^s}]$-álgebra, para todo $s > 0$.*

Demonstração. Indução em s. Como R é $k[R^p]$-módulo finito, $R = k[R^p][r_1,...,r_l]$. Suponha $R = k[R^{p^s}][r_1,...,r_l]$, para $s > 1$, queremos mostrar que $R = k[R^{p^{s+1}}][r_1,...,r_l]$. Basta ver que $R^{p^s} \subseteq k[R^{p^{s+1}}][r_1,...,r_l]$. Se $x \in R$, então $x = p(r_1,...,r_l)$, onde $p(r_1,...,r_l)$ é um polinômio nas variáveis $r_1,...,r_l$ sobre $k[R^{p^s}]$, pois $R = k[R^{p^s}][r_1,...,r_l]$ pela hipótese de indução. Portanto, $x^{p^s} = p(r_1,...,r_l)^{p^s}$ é um polinômio em $p(r_1,...,r_l)$ com coeficientes em $k[R^{p^{s+1}}]$, devido à característica de k ser $p > 0$. □

Lema B.2.5. $\mathrm{End}_{k[R^{p^s}]}(R) \cong \mathrm{Hom}_R(R \otimes_{k[R^{p^s}]} R, R)$.

Demonstração. É fácil ver que o mapa

$$\phi : \mathrm{End}_{k[R^{p^s}]}(R) \to \mathrm{Hom}_R(R \otimes_{k[R^{p^s}]} R, R),$$

dado por $\phi(T)(x \otimes y) = xT(y)$ está bem definido, e tem como inverso o mapa

$$\psi : \mathrm{Hom}_R(R \otimes_{k[R^{p^s}]} R, R) \to \mathrm{End}_{k[R^{p^s}]}(R),$$

dado por $\psi(\tau)(r) = \tau(1 \otimes r)$, que também está bem definido. □

Teorema B.2.6. *Se R é $k[R^p]$-módulo finito, então*

$$D_{R|k} = \bigcup_s \mathrm{End}_{k[R^{p^s}]}(R).$$

Demonstração. Digamos que R é gerado por $r_1,...,r_l$ como $k[R^p]$-módulo. Então esses elementos também geram R como $k[R^{p^s}]$-álgebra, para todo $s \geq 0$. Para $s > 0$ faça $t := l(p^s - 1)$, e $B := k[R^{p^s}]$. O ideal $J := \ker(R \otimes_B R \to R)$ é gerado por $\{1 \otimes r_i - r_i \otimes 1\}_{i=1}^l$ como R-módulo. Visto que

$$(1 \otimes r_i - r_i \otimes 1)^{p^s} = 1 \otimes r_i^{p^s} - r_i^{p^s} \otimes 1 = 0,$$

temos que $J^{t+1} = 0$. E portanto $\mathcal{P}^t_{R/B} = R \otimes_B R$ e

$$\begin{aligned} \mathrm{End}_{k[R^{p^s}]}(R) &\cong \mathrm{Hom}_R(R \otimes_B R, R) \\ &= \mathrm{Hom}_R(\mathcal{P}^t_{R/B}, R) \\ &\cong Diff^t_{R/B}(R) \\ &\subseteq Diff^t_{R/k}(R), \end{aligned}$$

Portanto,

$$\bigcup_s \mathrm{End}_{k[R^{p^s}]}(R) \subseteq D_{R|k}.$$

Por outro lado,

$$D_{R|k} \subseteq D_R \subseteq \bigcup_s \mathrm{End}_{R^{p^s}}(R).$$

Logo $D_{R|k} \subseteq \bigcup_s \mathrm{End}_{k[R^{p^s}]}(R)$, pois os elementos de $D_{R|k}$ são k-lineares. □