SOBRE AS ÁLGEBRAS SIMÉTRICA E DE REES DE UM IDEAL GERADO POR UMA d-SEQÜÊNCIA

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Érika Maria Chioca Lopes e aprovada pela comissão julgadora.

Campinas, 26 de fevereiro de 1998

Prof. Dr. Paulo Roberto Brumatti
Orientador

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de MESTRE em Matemática.

Sobre as Álgebras Simétrica e de Rees de um Ideal Gerado por uma d-seqüência

Érika Maria Chioca Lopes

26 de Fevereiro de 1998

Dissertação de Mestrado defendida e aprovada em 17 de fevereiro de 1998 pela Banca Examinadora composta pelos Profs. Drs.

Prof (a). Dr (a).PAULO ROBERTO BRUMATTI

Prof (a). Dr (a). ANTONIO PAQUES

Prof (a). Dr (a). ALEXANDER ANAN'IN

Dedico esta dissertação
a José Luiz Paro Júnior

Agradecimentos

Agradeço

- a meus pais e minhas irmãs, pelo apoio e carinho em todos os momentos. Também agradeço a minha mãe pela revisão lingüística dessa dissertação.
- ao José Luiz, por estar sempre ao meu lado, pelo amor, compreensão e tentativas de me acalmar nos momentos difíceis.
- ao meu orientador Prof. Paulo Brumatti, pela paciência, profissionalismo e preocupação em me ajudar.
- aos professores da banca examinadora Prof. Alexander Ananin e Prof. Antônio Paques, pelas sugestões e correções sugeridas.
- aos queridos Elisângela, Luciane e Gabriel, minha família de Campinas, pela amizade e por tudo que aprendemos juntos nesse ano.
- aos amigos Diogo, Daniel, Marcelo, Ximena, Marcela, Luciana, Ryuichi, Marcinha, Claudião, João, Marilaine, Alvino e Victor, Sinval e Cláudia, pelo companheirismo, amizade e por me ajudarem a aprender um pouco de LATEX.
- a todos os professores do Departamento de Matemática que me ajudaram nesses dois anos.
- ao pessoal do SAT, que, com paciência e boa-vontade, sempre me ajudou a resolver os problemas que surgiram com os computadores.
- ao CNPq e à FAPESP, pelo financiamento desse projeto.

Resumo

Nesta dissertação, o objetivo foi estudar os ideais de tipo linear, que são tais que existe um isomorfismo natural entre as álgebras simétrica e de Rees desses ideais. Um primeiro teste para verificar se um ideal é de tipo linear é através do cálculo das dimensões das álgebras simétrica e de Rees desse ideal, que foi feito nesse texto. A partir desse cálculo, conseguimos uma cota superior para o número mínimo de geradores de um ideal de tipo linear. Essencialmente, estudamos o conceito de d-seqüência, que generaliza a noção de R-seqüência, e mostramos que ideais gerados por d-seqüências são de tipo linear. Obtivemos ainda uma caracterização dos anéis locais regulares.

Conteúdo

Introdução

A álgebra simétrica de um ideal $\mathfrak{a}$ de um anel comutativo R é um par $(S(\mathfrak{a}), \psi_{\mathfrak{a}})$, onde $S(\mathfrak{a})$ é uma R-álgebra e $\psi_{\mathfrak{a}} : \mathfrak{a} \rightarrow S(\mathfrak{a})$ é um R-homomorfismo, que satisfaz a uma propriedade universal. Podemos caracterizá-la através dos geradores do ideal e de relações entre eles. Por outro lado, a álgebra de Rees de $\mathfrak{a}$ é um subanel de $R[T]$. Tal álgebra é conhecida como "blowup" álgebra, pois em termos geométricos ela representa a versão algébrica da explosão de uma variedade ao longo de uma subvariedade (Veja [7] e [23]). A teoria das "blowup" álgebras tem despertado muito interesse e portanto vem se mostrando ser uma área muito ativa e bem sucedida dentro da Álgebra Comutativa. Essa teoria tenta investigar várias propriedades algébricas da álgebra de Rees de um ideal, compará-la com o anel graduado desse ideal e descrever a álgebra de Rees em termos de geradores e relações. Por isso, o estudo que aproxima as álgebras simétrica e de Rees de um ideal é relevante, já que dá uma descrição explícita da álgebra de Rees em termos dos geradores do ideal e suas relações. Nesta dissertação, estaremos interessados em estudar o epimorfismo natural definido entre essas duas álgebras. Mais precisamente, estaremos interessados no caso em que o ideal é gerado por uma d-seqüência, no qual o referido epimorfismo é um isomorfismo (sendo um isomorfismo, chamamos o ideal $\mathfrak{a}$ de ideal de tipo linear).

As álgebras simétricas começaram a ser sistematicamente estudadas nos anos 60, por Micali([16]), o qual mostrou que, quando o anel R é domínio, a condição necessária e suficiente para um ideal ser de tipo linear é que sua álgebra simétrica seja um domínio. Micali também mostrou que ideais gerados por R-seqüências são de tipo linear. Muitos autores então se preocuparam em estudar quando a álgebra simétrica de um ideal é um domínio, por exemplo [2], [6], [16], [17] e [20]. Em [16], também encontramos a caracterização dos anéis locais regulares, isto é, um domínio local $(R, \mathfrak{m})$ é regular se, e só se, $\mathfrak{m}$ é de tipo linear. Tal resultado, por exemplo, caracteriza os pontos regulares de uma variedade algébrica afim irredutível. Mais tarde, Huneke([9]) e Valla([24]) mostraram que a noção de d-seqüências estava conectada com a integridade de álgebras simétricas de ideais. No caso em que a álgebra simétrica é um domínio, outras questões foram formuladas: Barshay([2]) estudou se ela é Cohen-Macaulay, Samuel([21]) investigou se ela é fatorial e Ribenboim([19]) e Barshay([2]), se ela é integralmente fechada. Um primeiro teste para verificar se um ideal é de tipo linear é fazendo o cálculo das dimensões das álgebras simétrica e de Rees. Por isso, o cálculo da dimensão da álgebra simétrica de um ideal é importante. Isso foi feito primeiramente por Huneke e Rossi([11]), quando eles associaram a dimensão da álgebra simétrica de um módulo à cota de Forster-Swan. Isso tornou a pesquisa pelas fórmulas de dimensão para a álgebra simétrica mais fácil. Mais tarde, usando idéias um pouco diferentes, Simis e Vasconcelos([22]) também encontraram a fórmula explícita.

No Capítulo I, fazemos uma breve revisão dos principais conceitos e resultados da Álgebra Comutativa, essencialmente daqueles resultados efetivamente usados no texto. A seguir, no Capítulo II, introduzimos os conceitos das álgebras simétrica e de Rees de um ideal e fazemos os cálculos de suas dimensões. Começmos o estudo dos ideais de tipo linear no Capítulo III, onde observamos uma limitação superior para o número de geradores de um ideal de tipo linear. Preocupamo-nos principalmente com os ideais gerados por R-seqüências, que são de tipo linear. Como aplicação, obtemos a caracterização dos anéis locais regulares descrita no parágrafo anterior. Como o conceito de d-seqüência generaliza o conceito de R-seqüência, focalizamos nosso estudo no último capítulo na generalização do resultado para R-seqüências, ou seja, mostramos que ideais gerados por d-seqüências são de tipo linear. Todo o trabalho foi baseado essencialmente nos artigos [16], [9] e [25].

Capítulo I

Preliminares

Neste capítulo, revisaremos os principais conceitos e teoremas da Álgebra Comutativa, que serão usados posteriormente. A maioria das provas será omitida, pois se trata de provas de resultados clássicos de um primeiro curso em Álgebra Comutativa, mas elas podem ser encontradas nas referências [1] e [12], sendo que este resumo se baseia principalmente em [12]. Durante todo o texto, consideraremos $R \neq 0$ um anel comutativo com unidade.

I.1 Produto Tensorial e Seqüências Exatas

Definição I.1.1 *Uma seqüência de R-módulos e R-homomorfismos*

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots$$

é dita **exata em** M_i *se* $Im(f_i) = Ker(f_{i+1})$. *A seqüência é* **exata** *se ela é exata em cada* M_i.

Assim, temos:

$0 \longrightarrow M' \xrightarrow{f} M$ é exata $\Leftrightarrow f$ é injetiva
$M \xrightarrow{g} M'' \longrightarrow 0$ é exata $\Leftrightarrow g$ é sobrejetiva
$0 \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$ é exata $\Leftrightarrow f$ é injetiva, g é sobrejetiva, e $Imf = Kerg$.

Sejam M, N, P três R-módulos. Uma aplicação $f : M \times N \to P$ é dita uma aplicação R-**bilinear** se para cada $x \in M$ a aplicação de N em P tal que $y \mapsto f(x, y)$ é R-linear e para cada $y \in N$ a aplicação de M em P tal que $x \mapsto f(x, y)$ é R-linear.

Proposição I.1.2 *Sejam M, N dois R-módulos. Então, existe um par (T, g) consistindo de um R-módulo T e uma aplicação R-bilinear $g : M \times N \to T$, satisfazendo a seguinte propriedade:*

Dados qualquer R-módulo P e qualquer aplicação R-bilinear $f : M \times N \to P$, existe uma única aplicação R-linear $f' : T \to P$ tal que $f = f' \circ g$.

$$\begin{tikzcd} M \times N \arrow[r, "f"] \arrow[d, "g"'] & P \\ T \arrow[ur, "f'"'] & \end{tikzcd}$$

Além disso, se (T, g) e (T', g') são dois pares satisfazendo essa propriedade, então existe um único isomorfismo $j : T \to T'$ tal que $j \circ g = g'$.

O módulo T construído como na proposição é chamado o **produto tensorial** de M e N e é denotado por $M \otimes_R N$ ou simplesmente por $M \otimes N$. Ele é um R-módulo gerado pelos elementos $x \otimes y$, onde $x \in M$ e $y \in N$. Se $(x_i)_{i \in I}$ e $(y_j)_{j \in J}$ são famílias de geradores de M e N, respectivamente, então $x_i \otimes y_j$ geram $M \otimes N$. Em particular, $M \otimes N$ é finitamente gerado, se M e N o são.

Observação I.1.3 Podemos também definir o produto tensorial de um número finito qualquer de R-módulos, por meio de uma proposição análoga à anterior, começando com uma aplicação R -multilinear, ao invés de uma R-bilinear:

Proposição I.1.4 *Sejam $M_1, \cdots M_r$ R-módulos. Então existe um par (T, g), que consiste de um R -módulo T e uma aplicação R-multilinear $g : M_1 \times \cdots \times M_r \to T$ satisfazendo a seguinte propriedade:*

Dados qualquer R-módulo P e qualquer aplicação R-multilinear $f : M_1 \times \cdots \times M_r \to P$, existe um único R-homomorfismo $f' : T \to P$ tal que $f' \circ g = f$.

$$\begin{tikzcd} M_1 \times \cdots \times M_r \arrow[r, "f"] \arrow[d, "g"'] & P \\ T \arrow[ur, "f'"'] & \end{tikzcd}$$

Além disso, se (T, g) e (T', g') são dois pares satisfazendo essa propriedade, então existe um único isomorfismo $j : T \to T'$.

Através da propriedade universal de definição de um produto tensorial, podemos mostrar os seguintes homomorfismos e isomorfismos canônicos, onde M, N, P são R-módulos e $\mathfrak{a}$ é um ideal de R:

1. $M \otimes N \cong N \otimes M$

   $x \otimes y \mapsto y \otimes x$

2. $(M \otimes N) \otimes P \cong M \otimes (N \otimes P) \cong M \otimes N \otimes P$

   $(x \otimes y) \otimes z \mapsto x \otimes (y \otimes z) \mapsto x \otimes y \otimes z$

3. $(M \oplus N) \otimes P \cong (M \otimes P) \oplus (N \otimes P)$

   $(x, y) \otimes z \mapsto (x \otimes z, y \otimes z)$

4. $R \otimes M \cong M$

   $r \otimes x \mapsto rx$

5. $(R/\mathfrak{a}) \otimes_R M \cong M/\mathfrak{a}M$

   $\overline{r} \otimes m \mapsto \overline{rm}$

6. $(M/N) \otimes R \cong (M \otimes R)/(N \otimes R)$

   $\overline{m} \otimes r \mapsto \overline{m \otimes r}$

7. Se $u : M \to N$ e $v : M' \to P$ são R-homomorfismos, então existe um R-homomorfismo $u \otimes v : M \otimes M' \to N \otimes P$ tal que $(u \otimes v)(m \otimes m') = u(m) \otimes v(m')$.

Veremos agora uma proposição que estabelece a propriedade exata do produto tensorial:

Proposição I.1.5 *Seja*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow 0$$

uma seqüência exata de R-módulos e homomorfismos e seja N qualquer R-módulo. Então, a seqüência

$$M' \otimes N \xrightarrow{f \otimes 1} M \otimes N \xrightarrow{g \otimes 1} M'' \otimes N \to 0$$

(onde 1 denota a aplicação identidade em N) é exata.

Corolário I.1.6 *Sejam E, E', E'', F, F', F'' R-módulos e as seqüências exatas $E' \xrightarrow{u} E \xrightarrow{v} E'' \to 0$ e $F' \xrightarrow{s} F \xrightarrow{t} F'' \to 0$. Então, $v \otimes t : E \otimes F \to E'' \otimes F''$ é sobrejetivo e seu núcleo é igual a $Im(u \otimes 1_F) + Im(1_E \otimes s)$.*

Dem. : Temos que $v \otimes t = (v \otimes 1_{F''}) \circ (1_E \otimes t)$. Como, pela Proposição anterior, $v \otimes 1_{F''}$ e $1_E \otimes t$ são sobrejetivas, segue que $v \otimes t$ é sobrejetiva. Além disso, como as seqüências do enunciado são exatas, temos que $Ker(v \otimes t) = Im(1_E \otimes s) + Im(u \otimes 1_F)$. De fato, $z \in Ker(v \otimes t)$ se, e só se, $(1_E \otimes t)(z) \in Ker(v \otimes 1_{F''}) = Im(u \otimes 1_{F''})$. Como t é sobrejetivo e $u \otimes t = (u \otimes 1_{F''}) \circ (1_{E'} \otimes t)$, isso é equivalente a $(1_E \otimes t)(z)$ pertencer a $Im(u \otimes t)$, ou seja, $(1_E \otimes t)(z) = (u \otimes t)(a)$, onde $a \in E' \otimes F$. Seja $b = z - (u \otimes 1_F)(a)$. Como $(1_E \otimes t) \circ (u \otimes 1_F) = u \otimes t$, segue que $(1_E \otimes t)(b) = 0$, isto é, $b \in Ker(1_E \otimes t) = Im(1_E \otimes s)$. Assim, $z \in Ker(v \otimes t)$ se, e só se, $z = b + (u \otimes 1_F)(a) \in Im(1_E \otimes s) + Im(u \otimes 1_F)$. □

I.2 Teorema da Base de Hilbert

Também estaremos considerando R um anel **Noetheriano**, isto é, um anel cujos ideais são finitamente gerados. Da mesma forma, dizemos que um R-módulo M é **Noetheriano** se todo submódulo de M é finitamente gerado.

Exemplos de anéis Noetherianos são os domínios de ideais principais (em particular os corpos), o anel dos inteiros – representado aqui por $\mathbb{Z}$, $K[X]$, onde K é corpo e qualquer imagem homomorfa de um anel Noetheriano. Pode-se mostrar que R é Noetheriano se, e só se, qualquer cadeia de ideais primos de R é estacionária.

Teorema I.2.1 (Teorema da Base de Hilbert para anéis) *Se R é um anel Noetheriano, então $R[X]$ também é.*

Dem. : Vamos supor que $R[X]$ não é Noetheriano, ou seja, suponhamos que exista um ideal I de $R[X]$ que não é finitamente gerado. Seja $f_1 \in I$ um polinômio de menor grau. Se $f_k (k \geq 1)$ já foi escolhido, seja f_{k+1} o polinômio de menor grau em $I - (f_1, \ldots, f_k)$. Sejam $n_k \in I\!N$ o grau e $a_k \in R$ o coeficiente líder de f_k, para todo k. Pela escolha de f_k temos $n_1 \leq n_2 \leq \cdots$. Além disso, $(a_1) \subset (a_1, a_2) \subset \cdots$ é uma cadeia de ideais de R que não é estacionária e, logo, R não é Noetheriano. Com efeito, suponhamos que $(a_1, \ldots, a_k) = (a_1, \ldots, a_{k+1})$. Então temos uma equação $a_{k+1} = \sum_{i=1}^{k} b_i a_i, b_i \in R$ e $g := f_{k+1} - \sum_{i=1}^{k} b_i X^{n_{k+1} - n_i} f_i \in I - (f_1, \ldots, f_k)$ tem grau menor que f_{k+1}; ou $g = 0$, contradizendo a escolha de f_{k+1}. □

Corolário I.2.2 *Sejam R um anel Noetheriano e S um anel finitamente gerado sobre R. Então S também é Noetheriano.*

Dem. : Como S é a imagem homomorfa de $R[X_1, \ldots, X_n]$, basta mostrar que $R[X_1, \ldots, X_n]$ é Noetheriano, o que segue usando o Teorema I.2.1 e indução em n. □

Em particular, temos mais exemplos de anéis Noetherianos: $R[X_1, \ldots, X_n]$, onde R é um domínio de ideais principais, e suas imagens homomorfas, como por exemplo $\mathbb{Z}[X_1, \ldots, X_n]$ e $K[X_1, \ldots, X_n]$, com K corpo.

Teorema I.2.3 (Teorema da Base de Hilbert para módulos) *Se R é um anel Noetheriano e M é um R-módulo finitamente gerado, então M é Noetheriano.*

Dem. : Suponhamos que $M = \langle m_1, \cdots, m_n \rangle$. Então existe uma única aplicação linear sobrejetiva $\varphi : R^n \to M$ que leva e_i em m_i, onde $(e_i)_{i=1}^{n}$ é a base canônica de R^n. É suficiente mostrar que qualquer submódulo U de R^n é finitamente gerado, pois todo submódulo de M é a imagem homomorfa de um submódulo de R^n.

Para os elementos $u = (u_1, \ldots, u_n) \in U$, as primeiras componentes u_1 formam um ideal I de R. Pela hipótese, I é finitamente gerado, ou seja, $I = (u_1^{(1)}, \ldots, u_1^{(k)})$.

Para $n = 1$, terminamos.

No caso geral, consideramos elementos $u^{(i)} \in U$ com primeiras componentes $u_1^{(i)}, i = 1, \ldots, k$. Para um $u \in U$ arbitrário, seja $u_1 = \sum_{i=1}^{k} r_i u_1^{(i)}, r_i \in R$. Então $u - \sum_{i=1}^{k} r_i u^{(i)}$ é da forma $(0, u_2^*, \ldots, u_n^*)$ e, portanto, é um elemento de $U \cap R^{n-1}$, onde R^{n-1} denota o submódulo de R^n, consistindo dos elementos com primeira componente zero. Pela hipótese de indução, $U \cap R^{n-1}$ tem um sistema finito de geradores $\{v_1, \ldots, v_l\}$. Então $\{u^{(1)}, \ldots, u^{(k)}, v_1, \ldots, v_l\}$ é um sistema de geradores de U. □

Agora, usando o Teorema da Base de Hilbert para módulos, podemos definir o conceito de apresentação finita de um R-módulo M, que será utilizado futuramente para o cálculo da álgebra simétrica do módulo M.

Definições I.2.4 • *A* **apresentação** *de M relativa a um sistema de geradores $\{m_\lambda\}_{\lambda\in\Lambda}$ de M é a seqüência exata*

$$0 \to K \to R^\Lambda \xrightarrow{\alpha} M \to 0,$$

onde α leva o elemento e_λ da base canônica de R^Λ em m_λ e $K := Ker(\alpha)$.

• *Dizemos que M é um módulo* **finitamente apresentado** *ou que a seqüência é uma* **apresentação finita** *de M se existe um $n \in I\!N$ e uma seqüência exata de R-módulos*

$$0 \to K \to R^n \to M \to 0,$$

onde K é finitamente gerado.

Vamos ver que, se M é um R-módulo finitamente gerado e estamos supondo R Noetheriano, então M é finitamente apresentado.

Com efeito, suponhamos que $M = \langle m_1, \cdots, m_n\rangle$. Assim, temos a seguinte apresentação de M:

$$0 \to K \to R^n \xrightarrow{\alpha} M \to 0.$$

Como K é um submódulo de R^n e este último é Noetheriano (pelo Teorema da Base de Hilbert para módulos), segue que $K = \langle v_1, \cdots, v_m\rangle$. Logo, M é finitamente apresentado.

Vamos também associar uma matriz a essa apresentação finita de M.

Como K é finitamente gerado, podemos definir uma aplicação natural $R^m \to R^n$ que leva o i-ésimo vetor da base canônica de R^m em v_i. A essa aplicação linear está associada uma matriz A, cujas colunas são exatamente os vetores $v_1, \ldots, v_m$ que geram K. Podemos então considerar a seguinte seqüência:

$$R^m \xrightarrow{A} R^n \xrightarrow{\alpha} M \to 0,$$

que é exata, pois $Im(A) = K = Ker(\alpha)$. Essa matriz A é chamada **matriz de relação** de M.

I.3 Anéis Graduados

Definições I.3.1 **(a)** *Um* **anel graduado** *é um anel R junto com uma decomposição $R = \oplus_{i\in\mathbb{Z}} R_i$ (como um $\mathbb{Z}$-módulo) tal que $R_iR_j \subset R_{i+j}$, para todos $i,j \in \mathbb{Z}$.*

(b) *Um R-***módulo graduado** *é um R-módulo M junto com uma decomposição $M = \oplus_{i\in\mathbb{Z}} M_i$ (como um $\mathbb{Z}$-módulo) tal que $R_iM_j \subset M_{i+j}$, para todos $i,j \in \mathbb{Z}$.*

(c) *Uma R-álgebra A é* **graduada** *se $A = \oplus_{i\in\mathbb{Z}} A_i$ (como um R-módulo) e $A_iA_j \subset A_{i+j}$, para todos $i,j \in \mathbb{Z}$.*

Os elementos $x \in M_i$ são ditos **homogêneos de grau** i, os elementos $x \in R_i$ são também chamados i-**formas**. De acordo com essa definição, o elemento zero é homogêneo de grau arbitrário. O grau de um elemento homogêneo x é denotado por $gr(x)$. Um elemento arbitrário $x \in M$ tem uma única apresentação $x = \sum_i x_i$ como uma soma de elementos homogêneos $x_i \in M_i$. Os elementos x_i são ditos as **componentes homogêneas** de x.

Notemos que R_0 é um anel com $1 \in R_0$ (pois $R_0R_0 \subset R_0$ e $1 = 1.1 \in R_iR_i \subset R_{2i}$, logo, $i = 0$) , que todos os somandos M_i são R_0-módulos (pois $R_0M_i \subset M_i$), e que $M = \oplus_{i\in\mathbb{Z}}M_i$ é uma decomposição em soma direta de M como um R_0-módulo.

Definição I.3.2 *Sejam R um anel graduado, $M = \oplus_{i\in\mathbb{Z}}M_i, N = \oplus_{i\in\mathbb{Z}}N_i$ dois R-módulos graduados. Um homomorfismo $\varphi : M \to N$ é dito* **homogêneo de grau zero** *se $\varphi(M_i) \subset N_i$, para todo $i \in \mathbb{Z}$.*

Definição I.3.3 *Sejam M um R-módulo graduado e N um submódulo de M. N é dito um submódulo* **homogêneo** *se ele é um módulo graduado e a aplicação inclusão é um homomorfismo homogêneo de N em M.*

Observação I.3.4 A Definição I.3.3 é equivalente à condição $N_i = N \cap M_i, \forall i \in \mathbb{Z}$.

Com efeito, se estamos supondo que N é um submódulo homogêneo de M, então $j(N_i) \subset M_i$, onde j é a aplicação inclusão. Logo, $N_i \subset N \cap M_i$. Por outro lado, se $x \in N \cap M_i$, como N é graduado, podemos escrever $x = \sum_{k\in\mathbb{Z}} n_k = n_i + \sum_{k\neq i} n_k$, com $n_k \in N_k \subset M_k, \forall k$. Como $x, n_i \in M_i$, segue que $\sum_{k\neq i} n_k \in M_i$. Mas $\sum_{k\neq i} n_k \in \oplus_{k\neq i}N_k \subset \oplus_{k\neq i}M_k$. Logo, $\sum_{k\neq i} n_k = 0$ e $x = n_i \in N_i$. Portanto, $N_i = N \cap M_i$.

Reciprocamente, se $N_i = N \cap M_i, \forall i$, então $j(N_i) \subset M_i, \forall i$, onde j é a inclusão. Logo, N é homogêneo.

Em outras palavras, N é um submódulo homogêneo de M se, e só se, N é gerado pelos elementos homogêneos de M que pertencem a N. Em particular, se $x \in N$, então todas as componentes homogêneas de x pertencem a N. Além disso, o quociente M/N é graduado da maneira natural: $M/N = \oplus_{i\in\mathbb{Z}}M_i/(N \cap M_i)$.

Observemos que, se $\varphi : M \to N$ é um homomorfismo homogêneo, então $Ker(\varphi)$ e $Im(\varphi)$ são homogêneos: definamos $Ker(\varphi) = \oplus_{i\in\mathbb{Z}}(Ker(\varphi)) \cap M_i = \oplus_{i\in\mathbb{Z}}K_i$ e $Im(\varphi) = \oplus_{i\in\mathbb{Z}}(Im(\varphi)) \cap N_i) = \oplus_{i\in\mathbb{Z}}T_i$ e essas são de fato graduações para $Ker(\varphi)$ e $Im(\varphi)$.

Proposição I.3.5 *Para um anel $\mathbb{N}$-graduado R (isto é, $R = \oplus_{i\in\mathbb{N}}R_i$) cuja componente de grau zero é R_0, são equivalentes:*

i) *R é um anel Noetheriano.*

ii) *R_0 é Noetheriano e R é uma R_0-álgebra finitamente gerada.*

Dem. :

i) $\Rightarrow$ ii) Seja $R_+ = \oplus_{n>0}R_n$. Logo $R = R_0 \oplus R_+$ e $R_0 \cong R/R_+$.[1] Assim, R_0 é Noetheriano. Como R_+ é um ideal de R, ele é finitamente gerado, digamos $R_+ = (x_1, \ldots, x_s)$, e podemos tomar $x_1, \ldots, x_s$ elementos homogêneos de R, de graus $k_1, \ldots, k_s > 0$, respectivamente. Seja R' o subanel de R gerado por $x_1, \ldots, x_s$ sobre R_0. Queremos mostrar que $R_n \subset R', \forall n \geq 0$, onde $R = \oplus_{n\geq 0}R_n$, por indução em n. É claro que isso vale para $n = 0$.

[1]Basta definir o homomorfismo que leva $r_0 + \sum_{n>0} r_n \in R$ em r_0 e verificar que seu núcleo é R_+.

Seja $n > 0$ e seja $y \in R_n$. Como $y \in R_+$, y é uma combinação linear dos x_i, digamos $y = \sum_{i=1}^{s} a_i x_i$, onde $a_i \in R_{n-k_i}$ (convencionalmente $R_m = 0$, se $m < 0$). Como cada $k_i > 0$ (e, logo, $n - k_i < n$), a hipótese de indução mostra que cada a_i é uma polinomial nos x_i's com coeficientes em R_0. Assim, o mesmo vale para y e, portanto, $y \in R'$. Assim, $R_n \subset R'$ e, portanto, $R = R'$.

ii) $\Rightarrow$ i) Pelo Corolário I.2.2. □

Exemplo I.3.6 Dado um ideal I de um anel R, podemos definir o **anel graduado de** I, que será

$$gr_I(R) := R/I \oplus I/I^2 \oplus I^2/I^3 \oplus \cdots.$$

Ele é de fato um anel graduado: se $x = a + I^{m+1} \in I^m/I^{m+1}$ e $y = b + I^{n+1} \in I^n/I^{n+1}$, então definimos $x.y := ab + I^{n+m+1} \in I^{n+m}/I^{n+m+1}$ e esse resultado é independente da escolha dos representantes a, b de x, y. Isso define o produto de elementos homogêneos de $gr_I(R)$. Para elementos arbitrários, definimos o produto de maneira natural, tal que a lei distributiva valha.

I.4 Variedades Algébricas Afins - Espectro de um Anel

Vamos então definir alguns conceitos da Geometria Algébrica, que aqui servem como exemplos e aplicação da teoria desenvolvida.

Definição I.4.1 *Sejam $\mathbb{A}^n(L)$ o n-espaço afim sobre um corpo L e $K \subset L$ um subcorpo. Um subconjunto $V \subset \mathbb{A}^n(L)$ é chamado uma K-***variedade algébrica afim** *se existem polinômios $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ tais que V é a solução do sistema de equações*

$$f_i(X_1, \ldots, X_n) = 0 \ (i = 1, \ldots, m)$$

em $\mathbb{A}^n(L)$.

Exemplos I.4.2

- O conjunto solução de um sistema de equações lineares é chamado de **variedade linear**.
- O conjunto solução de uma equação $f(X_1, \ldots, X_n) = 0$, onde $f \in K[X_1, \ldots, X_n]$ é um polinômio não constante, é chamada de K-**hipersuperfície**.
- O conjunto solução da equação $f(X_1, X_2) = 0$, com $f \in K[X_1, X_2]$ um polinômio não constante, é chamado de **curva algébrica plana**.
- Interseções finitas e uniões finitas de K-variedades afins são variedades afins.

Definições I.4.3

- *Para um subconjunto $V \subset \mathbb{A}^n(L)$, o conjunto*

$$\mathbf{I}(V) := \{F \in K[X_1, \ldots, X_n]; F(x) = 0, \forall x \in V\}$$

é chamado o **ideal de V** *em $K[X_1, \ldots, X_n]$.*

- *O* **conjunto de zeros**, *em* $\mathbb{A}^n(L)$, **de um ideal** $I \subset K[X_1, \ldots, X_n]$ *é o conjunto*

$$\mathbf{V}(I) := \{x \in \mathbb{A}^n(L); F(x) = 0, \forall F \in I\}.$$

- *Dizemos que uma variedade* V *é* **irredutível** *quando temos: se* $V = V_1 \cup V_2$, *onde* V_1 *e* V_2 *são* K*-variedades, então* $V = V_1$ *ou* $V = V_2$.

Observação I.4.4 Podemos generalizar essa última definição: Um espaço topológico X é **irredutível** se para qualquer decomposição $X = A_1 \cup A_2$, com $A_1, A_2 \subset X$ subconjuntos fechados de X, tivermos $X = A_1$ ou $X = A_2$. Um subconjunto X' de um espaço topológico X é irredutível se X' é irredutível como um espaço com a topologia induzida. Usando os conceitos básicos da topologia, concluímos que o fecho de um subconjunto irredutível de um espaço topológico é irredutível.

Segue então:

Proposição I.4.5 *A aplicação* $V \mapsto \mathbf{I}(V)$ *do conjunto de todas as* K*-variedades* $V \subset \mathbb{A}^n(L)$ *no conjunto dos ideais* I *de* $K[X_1, \ldots, X_n]$ *com* $\sqrt{I} = I$ *é injetiva e reverte inclusão. Uma* K*-variedade* $V \subset \mathbb{A}^n(L)$ *é irredutível se, e só se, seu ideal* $\mathbf{I}(V)$ *é primo.*

Usando o Teorema da Base de Hilbert, obtemos o seguinte corolário:

Corolário I.4.6 *Para um ideal* I *de* $K[X_1, \ldots, X_n]$, $\mathbf{V}(I)$ *é uma* K*-variedade em* $\mathbb{A}^n(L)$.

Dem. : De fato, como $K[X_1, \ldots, X_n]$ é Noetheriano, temos que $I = (f_1, \ldots, f_m)$. Logo $\mathbf{V}(I)$ é o conjunto solução do sistema de equações $f_i(X_1, \ldots, X_n) = 0$ $(i = 1, \ldots, m)$. □

Também usando a definição de variedade, obtemos:

Corolário I.4.7 *Se* $(V_\lambda)_{\lambda \in \Lambda}$ *é uma família de* K*-variedades em* $\mathbb{A}^n(L)$, *então* $\cap_{\lambda \in \Lambda} V_\lambda$ *é uma* K*-variedade.*

Obtemos, portanto, que o conjunto das K-variedades formam os conjuntos fechados de uma topologia em $\mathbb{A}^n(L)$, chamada de **topologia de Zariski**. Se $V \subset \mathbb{A}^n(L)$ é uma K-variedade, então podemos munir V da topologia relativa, ou seja, os subconjuntos fechados $W \subset V$, chamados de **subvariedades**, são as K-variedades contidas em V. Obviamente, os subconjuntos da forma $\mathcal{D}(f) := V - \mathbf{V}(f)$, $f \in K[X]$, são subconjuntos abertos de V e podemos mostrar, usando as propriedades básicas dos conjuntos zeros de um ideal, que esses conjuntos formam uma base para a topologia de V, ou seja, todo aberto de V é uma união finita de subconjuntos da forma $\mathcal{D}(f)$. Vamos enunciar agora o Teorema dos Zeros de Hilbert, para concluir que a aplicação definida na Proposição I.4.5 é uma bijeção, quando L é algebricamente fechado.

Teorema I.4.8 (Teorema dos Zeros de Hilbert) *Se* L *é um corpo algebricamente fechado e* $I \neq K[X_1, \ldots, X_n]$ *é um ideal, então* $\mathbf{V}(I)$ *é não-vazio.*

Usando esse teorema, podemos demonstrar que:

Proposição I.4.9 *Seja $L|K$ uma extensão de corpos, onde L é algebricamente fechado. A aplicação $V \mapsto \mathbf{I}(V)$ define uma bijeção do conjunto das K-variedades $V \subset \mathbb{A}^n(L)$ no conjunto dos ideais I de $K[X_1, \ldots, X_n]$ com $\sqrt{I} = I$. Para qualquer ideal I de $K[X_1, \ldots, X_n]$ vale $\sqrt{I} = \mathbf{I}(\mathbf{V}(I))$.*

A partir de agora, sempre que falarmos de variedades afins, consideraremos L algebricamente fechado.

Definições I.4.10 • *Uma K-álgebra que é finitamente gerada sobre K é chamada* **K-álgebra afim.**

• *Para uma K-variedade $V \subset \mathbb{A}^n(L)$,*

$$K[V] := K[X_1, \ldots, X_n]/\mathbf{I}(V)$$

é chamado o **anel de coordenadas** *de V.*

Se $V = \mathbb{A}^n(L)$, então $K[V] = K[X_1, \ldots, X_n]$. Os elementos f do anel de coordenadas $K[V]$ de uma K-variedade $V \subset \mathbb{A}^n(L)$ podem ser considerados como funções $f : V \to L$. De fato, se $f = F + \mathbf{I}(V)$, com $F \in K[X_1, \ldots, X_n]$ e $x = (x_1, \ldots, x_n) \in V$, então definamos $f(x) = F(x_1, \ldots, x_n)$. Essa definição é independente da escolha do representante F da classe de f. A relação dada em I.4.9 pode ser generalizada considerando as K-subvariedades de uma variedade fixada V e os ideais de $K[V]$. Podemos falar no conjunto zero $\mathbf{V}_V(I)$ de I em V (uma K-subvariedade de V) e para um subconjunto $W \subset V$, podemos falar no ideal anulador $\mathbf{I}_V(W)$ de W em $K[V]$:

$$\mathbf{V}_V(I) := \{x \in V; f(x) = 0, \forall f \in I\}$$

$$\mathbf{I}_V(W) := \{f \in K[V]; f(x) = 0, \forall f \in W\}$$

Obtemos então:

Proposição I.4.11 *Seja $V \subset \mathbb{A}^n(L)$ uma K-variedade. A aplicação $W \mapsto \mathbf{I}_V(W)$ que leva cada K-variedade $W \subset V$ em seu ideal $\mathbf{I}_V(W)$ em $K[V]$ é uma bijeção que reverte inclusão do conjunto de todas as K-subvariedades de V sobre o conjunto de todos os ideais I de $K[V]$, com $\sqrt{I} = I$. Para cada ideal I de $K[V]$ temos $\sqrt{I} = \mathbf{I}_V(\mathbf{V}_V(I))$. Uma K-subvariedade $W \subset V$ é irredutível se, e só se, $\mathbf{I}_V(W)$ é um ideal primo de $K[V]$.*

Veremos agora o conceito de espectro de um anel e a relação entre uma variedade afim e o espectro do seu anel de coordenadas.

Definições I.4.12 • *$Spec(R)$ é o conjunto dos ideais primos $\mathfrak{p}$ de R, com $\mathfrak{p} \neq R$.*

• *$Max(R)$ é o conjunto dos ideais maximais $\mathfrak{m}$ de R.*

• *Se I é um ideal de R, o* **conjunto zero de** *I em $Spec(R)$ é $\mathbf{V}(I) := \{\mathfrak{p} \in Spec(R); \mathfrak{p} \supset I\}$.*

• *Dizemos que $A \subset Spec(R)$ é* **fechado** *se existe um ideal I de R tal que $A = \mathbf{V}(I)$.*

- *Portanto, está definida uma topologia em $Spec(R)$, chamada* **topologia de Zariski** *em $Spec(R)$.*

- *Para um subconjunto arbitrário $A \subset Spec(R)$, o* **ideal de** *A em R é o ideal $\mathbf{I}(A) = \bigcap_{\mathfrak{p} \in A} \mathfrak{p}$.*

Segue facilmente dessas definições que $\mathbf{V}(\mathbf{I}(A)) = \overline{A}$, para qualquer $A \subset Spec(R)$, onde $\overline{A}$ é o fecho de A em $Spec(R)$. Analogamente ao que foi feito para o Teorema dos Zeros de Hilbert, podemos mostrar que:

Proposição I.4.13 *Seja $X = Spec(R)$. Para qualquer ideal I de R, $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$. Os subconjuntos fechados de X correspondem bijetivamente aos ideais de R que são iguais aos seus radicais.*

Analogamente à Proposicao I.4.5, temos:

Proposição I.4.14 *Seja $X = Spec(R)$. Um subconjunto fechado $A \subset X$ é irredutível se, e só se, $\mathbf{I}(A)$ é um ideal primo.*

Queremos investigar a relação entre uma variedade algébrica e o espectro do seu anel de coordenadas. Sejam $L|K$ uma extensão de corpos, onde L é algebricamente fechado e $V \subset \mathbb{A}^n(L)$ uma K-variedade. Para qualquer $x \in V$, o conjunto $\mathfrak{p}_x := \mathbf{I}_V(\{x\})$ de todas as funções $f \in K[V]$ com $f(x) = 0$ é um ideal primo diferente de $K[V]$. Logo está definida uma aplicação $\varphi : V \longrightarrow Spec(K[V])$ que leva x em $\mathfrak{p}_x$ e que é contínua. Em geral, φ não é injetiva nem sobrejetiva. Queremos mostrar que $\mathfrak{p} \in Spec(K[V])$ está na $Im(\varphi)$ se, e só se, sua correspondente subvariedade $\mathbf{V}_V(\mathfrak{p}) \subset V$ tem um "ponto genérico", que é o conceito que definimos a seguir.

Definição I.4.15 *Seja A um subconjunto fechado de um espaço topológico X. Dizemos que $x \in A$ é um* **ponto genérico** *de A se $A = \overline{\{x\}}$.*

Se A tem um ponto genérico, então A é irredutível, pois $A = \overline{\{x\}}$ e $\{x\}$ é irredutível. Para $\mathfrak{p} \in Spec(K[V])$, existe um $x \in V$ com $\mathfrak{p} = \mathfrak{p}_x = \mathbf{I}_V(\{x\})$ se, e só se, $\mathbf{V}_V(\mathfrak{p}) = \overline{\{x\}}$, isto é, quando x é um ponto genérico de $\mathbf{V}_V(\mathfrak{p})$. Nem toda variedade irredutível tem um ponto genérico; por exemplo, se $L = K$, então $\overline{\{x\}} = \{x\}$, para qualquer ponto $x \in V$. Entretanto, se o grau de transcendência de L sobre K é pelo menos n, então podemos mostrar que qualquer K-variedade irredutível $V \subset \mathbb{A}^n(L)$ tem um ponto genérico.

Proposição I.4.16 *Seja $X = Spec(R)$. Qualquer subconjunto fechado não vazio e irredutível $A \subset X$ tem um único ponto genérico $\mathfrak{p}$, que é $\mathfrak{p} = \mathbf{I}(A)$.*

Dem. : Se $\mathfrak{p}$ é um ponto genérico de A, então $A = \overline{\{\mathfrak{p}\}} = \mathbf{V}(\mathbf{I}(\{\mathfrak{p}\})) = \mathbf{V}(\mathfrak{p})$, logo $\mathbf{I}(A) = \mathbf{I}(\mathbf{V}(\mathfrak{p}))$. Mas da definição de $\mathbf{V}$ e $\mathbf{I}$ segue que $\mathbf{I}(\mathbf{V}(\mathfrak{p})) = \sqrt{\mathfrak{p}} = \mathfrak{p}$. Logo, $\mathfrak{p} = \mathbf{I}(A)$.

Em geral, por I.4.14, $\mathbf{I}(A) = \bigcap_{\mathfrak{p} \in A} \mathfrak{p}$ é um ideal primo de R. Aplicando a regra $\overline{\{x\}} = \mathbf{V}(\mathbf{I}(\{x\}))$ para $x = \mathbf{I}(A)$, vemos que $\overline{\{\mathbf{I}(A)\}} = \mathbf{V}(\mathbf{I}(A)) = \overline{A} = A$, isto é, $\mathrm{I}(A)$ é um ponto genérico de A. □

Chamamos o radical do ideal zero de um anel R, denotado por $\sqrt{0}$, de **nilradical** de R. Ele consiste dos elementos nilpotentes de R. Ainda, dado um ideal I de um anel R, dizemos que o ideal primo $\mathfrak{p}$ de R é um **divisor primo de** I se $\mathfrak{p} \supset I$, e dizemos que $\mathfrak{p}$ é um **divisor primo minimal de** I se $\mathfrak{p}$ é o menor ideal primo de R que contém I. Usando a proposição anterior, podemos mostrar que, se R tem somente um número finito de ideais primos minimais $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$, então $\sqrt{0} = \bigcap_{i=1}^{s} \mathfrak{p}_i$.

I.5 Dimensão de Krull de Anéis e Altura de Ideais - Teorema do "Going-Down" - Teorema da Normalização de Noether

Definição I.5.1 *Se $X \neq \emptyset$ é um espaço topológico, a* **dimensão de Krull** *de X, denotada por $dimX$, é o supremo dos comprimentos n de todas as cadeias*

$$X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n \tag{I.1}$$

de subconjuntos fechados e irredutíveis X_i de X. Por convenção, o espaço topológico vazio tem dimensão de Krull -1. Se $Y \neq \emptyset$, a **codimensão** *$codim_X Y$ de Y em X é o supremo dos comprimentos das cadeias I.1, com $X_0 = Y$.*

Definições I.5.2 **(a)** *A* **dimensão de Krull** *de um anel R, denotada por $dimR$, é a dimensão de Krull de $Spec(R)$, ou seja, é o supremo dos comprimentos n de todas as cadeias de ideais primos*

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n \tag{I.2}$$

em $Spec(R)$.

(b) *A* **altura** *de um ideal primo $\mathfrak{p} \in Spec(R)$, denotada por $ht(\mathfrak{p})$, é o supremo dos comprimentos n das cadeias de ideais primos com $\mathfrak{p} = \mathfrak{p}_n$ em I.2. Para um ideal arbitrário $I \neq R$, a* **altura** *de I é definida como o ínfimo das alturas dos divisores primos de I, ou equivalentemente, o ínfimo das alturas dos divisores primos minimais de I.*

(c) *Chamamos $dim(I) = dim(R/I)$ a* **dimensão** *ou* **co-altura** *do ideal I.*

Segue então que $dim(\mathfrak{p}) = dim(\mathbf{V}(\mathfrak{p}))$ e $ht(\mathfrak{p}) = codim_{Spec(R)}\mathbf{V}(\mathfrak{p}), \forall \mathfrak{p} \in Spec(R)$.

Para uma K-variedade $V \subset \mathbb{A}^n(L)$, como as cadeias de subconjuntos fechados irredutíveis de V correspondem bijetivamente às cadeias de ideais primos de $Spec(K[V])$, segue que $dim(V) = dim(K[V])$.

Exemplos I.5.3 • No anel polinomial $K[X_1, \ldots, X_n]$, onde K é corpo, temos que

$$(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \subsetneq \cdots \subsetneq (X_1, \ldots, X_n)$$

é uma cadeia de ideais primos, logo $dim(K[X_1, \ldots, X_n]) \geq n$. Veremos que na verdade $dimK[X_1, \ldots, X_n] = n$, com o auxílio do Teorema da Normalização de Noether. Como conseqüência, $dim(\mathbb{A}^n(L)) = n$ e, logo, variedades afins são de dimensão finita.

- Em um domínio fatorial R, os ideais primos de altura 1 são exatamente os ideais principais gerados por elementos primos. Em particular, segue que domínios de ideais principais que não são corpos têm dimensão de Krull 1. Logo, $dim(\mathbb{Z}) = 1$ e $dim(K[X]) = 1$.

Estudaremos agora algumas proposições que nos levarão ao Teorema da Normalização de Noether, de fundamental importância para o cálculo da dimensão de álgebras afins e variedades afins. Sejam $S|R$ uma extensão de anéis e I um ideal de R.

Definição I.5.4 *Dizemos que $x \in S$ é* **integral sobre** *I se existe um polinômio mônico f de grau n, com $f - X^n \in I[X]$, tal que $f(x) = 0$. Dizemos que a extensão $S|R$ é* **inteira** *se todo $x \in S$ é integral sobre R.*

Proposição I.5.5 *Para $x \in S$ as seguintes afirmações são equivalentes:*

a) *x é integral sobre I.*

b) *$R[x]$ é finitamente gerado como um R-módulo e $x \in \sqrt{IR[x]}$.*

c) *Existe um subanel S' de S com $R[x] \subset S'$ tal que S' é finitamente gerado como um R-módulo e $x \in \sqrt{IS'}$.*

Dem. :

a) $\Rightarrow$ b) Seja $f = X^n + a_1X^{n-1} + \cdots + a_n$, com $a_i \in I$ tal que $f(x) = 0$. Todo $g \in R[X]$ pode ser dividido por f , isto é, $g = q.f + r$, com $q, r \in R[X], gr(r) < gr(f)$, ou $r = 0$. Como $g(x) = r(x)$, vemos que $\{1, x, \ldots, x^{n-1}\}$ é um sistema de geradores do R-módulo $R[X]$. De $f(x) = 0$, segue que $x^n \in IR[X]$, logo, $x \in \sqrt{IR[X]}$.

b) $\Rightarrow$ c) Basta colocar $S' = R[x]$.

c) $\Rightarrow$ a) Se $\{w_1, \ldots, w_l\}$ é um sistema de geradores do R-módulo S' e $x^m \in IS'$, então podemos escrever

$$x^m w_i = \sum_{k=1}^{l} \rho_{ik} w_k$$

ou

$$\sum_{k=1}^{l} (x^m \delta_{ik} - \rho_{ik}) w_k = 0 \ (i = 1, \ldots, l).$$

Além disso, $1 = \sum_{k=1}^{l} b_k w_k$, para alguns $b_k \in R$ e logo $det(x^m \delta_{ik} - \rho_{ik}) = 0$. A expansão completa do determinante resulta em

$$x^n + a_1x^{n-1} + \cdots + a_n = 0,$$

onde $n = m.l$ e $a_i \in I$. □

Corolário I.5.6 *Se $x_1, \ldots, x_n \in S$ são integrais sobre I, então $R[x_1, \ldots, x_n]$ é um R-módulo finitamente gerado e $x_i \in \sqrt{IR[x_1, \ldots, x_n]}$, para $i = 1, \ldots, n$.*

Dem. : Basta usar a Proposição I.5.5 e indução. □

Corolário I.5.7 *O conjunto* $\overline{R}$ *de todos os elementos de* S *que são integrais sobre* R *é um subanel de* S. $\sqrt{I\overline{R}}$ *é o conjunto dos elementos de* S *que são integrais sobre* I.

Dem. : Para $x, y \in \overline{R}$, $R[x,y]$ é um R-módulo finitamente gerado. Pela Proposição I.5.5, $x+y, x-y, x.y \in \overline{R}$. Se $x \in S$ é integral sobre I, então $x \in \sqrt{IR[x]} \subset \sqrt{I\overline{R}}$, por I.5.5.

Reciprocamente, se $x \in \sqrt{I\overline{R}}$, então $x^m \in IR[x_1, \ldots, x_n]$, para adequados $x_1, \ldots, x_n \in \overline{R}$. Como $R[x_1, \ldots, x_n]$ é um R-módulo finitamente gerado, por I.5.5 segue que x é integral sobre I. □

Definição I.5.8 *Dizemos que* $\overline{R}$ *é o* **fecho integral de** R **em** S. *Dizemos que* R *é* **integralmente fechado em** S *se* $\overline{R} = R$. *Um domínio que é integralmente fechado no seu corpo de frações é dito* **normal**.

Exemplo I.5.9 Qualquer domínio fatorial R é normal. Em particular, $\mathbb{Z}$ e $R[X_1, \ldots, X_n]$, se R é fatorial, são normais.

De fato, sejam K o corpo de frações de R e $x \in K$ integral sobre R. Consideramos a equação

$$x^n + r_1 x^{n-1} + \cdots + r_n = 0 \ (r_i \in R)$$

e uma representação $x = r/s, r, s \in R, s \neq 0$, onde r e s são primos entre si. Depois de multiplicar a equação por s^n, obtemos:

$$r^n + r_1 s r^{n-1} + \ldots + r_n s^n = 0.$$

Se existisse um elemento primo de R que divide s, então ele também dividiria r, uma contradição. Portanto, s é uma unidade de R e $x \in R$.

Para uma extensão inteira de anéis $S|R$, existe uma íntima relação entre as cadeias de ideais primos de R e aquelas de S. Essa relação é dada pela Teoremas de Cohen-Seidenberg ("Going-Up" e "Going-Down"), que iremos apenas enunciar. Seja

$$\begin{array}{rccc} \varphi: & Spec(S) & \to & Spec(R) \\ & \mathfrak{q} & \mapsto & \mathfrak{q} \cap R \end{array}$$

que é uma aplicação contínua. Se $\mathfrak{q} \in Spec(S)$ e $\mathfrak{p} = \mathfrak{q} \cap R$, dizemos que $\mathfrak{q}$ **está sobre** $\mathfrak{p}$.

Proposição I.5.10 *Seja* $S|R$ *uma extensão inteira de anéis.*

1. *Se* $\mathfrak{q} \subsetneq \mathfrak{q}'$, *com* $\mathfrak{q}, \mathfrak{q}' \in Spec(S)$, *então* $\mathfrak{p} = \mathfrak{q} \cap R \subsetneq \mathfrak{p}' = \mathfrak{q}' \cap R$.

2. *Se* $\mathfrak{p} \in Spec(R)$, *então existe* $\mathfrak{q} \in Spec(S)$ *tal que* $\mathfrak{q} \cap R = \mathfrak{p}$.

Teorema I.5.11 (Teorema do "Going-Up") *Seja* $S|R$ *uma extensão inteira de anéis. Para qualquer cadeia de ideais primos* $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ *em* R *e para qualquer* $\mathfrak{q}_0$ *que está sobre* $\mathfrak{p}_0$, S *contém uma cadeia de ideais primos* $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$, *com* $\mathfrak{q}_i \cap R = \mathfrak{p}_i (i = 0, \ldots, n)$.

Corolário I.5.12 *Seja $S|R$ uma extensão inteira de anéis. Então $dim(S) = dim(R)$.*

Proposição I.5.13 (Teorema de "Going-Down") *Seja $S|R$ uma extensão inteira de anéis, onde R e S são domínios e R é normal. Seja $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$ uma cadeia de primos em $Spec(R)$ e $\mathfrak{q}_1$ um ideal primo de S que está sobre $\mathfrak{p}_1$. Então, existe um $\mathfrak{q}_0 \in Spec(S)$ com $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1$ e $\mathfrak{q}_0 \cap R = \mathfrak{p}_0$.*

Por fim, enunciaremos o Teorema da Normalização de Noether, cuja prova omitiremos por ser muito extensa. Antes, porém, veremos os conceitos de elementos algebricamente independentes e grau de transcendência, usados no referido Teorema.

Sejam S um conjunto e R um anel comutativo. Denotaremos por $R[S]$ o anel polinomial de S sobre R; seus elementos são da forma $\sum a_{(v)} M_{(v)}(S) = \sum a_{(v)} \prod_{x \in S} x^{v(x)}$, onde (v) varia entre as aplicações de S em $\mathbb{N}$ que é 0, para quase todo x, e $a_{(v)} = 0$, para quase todo (v).

Em particular, se $S = \{X_1, \ldots, X_n\}$. então $R[S] = R[X_1, \ldots, X_n]$.

Definição I.5.14 *Sejam $K|k$ uma extensão de corpos e $S \subset K$. Dizemos que os elementos S (ou S) são* **algebricamente independentes sobre** *k se sempre que $\sum a_{(v)} M_{(v)}(S) = 0$ — onde $a_{(v)} \in k$ e quase todo $a_{(v)} = 0$ — tivermos todo $a_{(v)} = 0$.*

Podemos colocar uma ordem parcial no conjunto dos subconjuntos algebricamente independentes de K pela inclusão. Pelo Lema de Zorn, existem elementos maximais nesse conjunto.

Definição I.5.15 *Um subconjunto S de K que é algebricamente independente sobre k e é maximal com relação à inclusão será chamado* **base transcendente de K sobre k**.

Observação I.5.16 **a)** Se $K = k(T)$, então T contém uma base transcendente de K sobre k.

b) Se S é uma base transcendente de K sobre k, então K é algébrico sobre $k(S)$.

Podemos mostrar que

Teorema I.5.17 *Seja $K|k$ uma extensão de corpos. Quaisquer duas bases transcendentes de K sobre k têm a mesma cardinalidade.*

A partir desse resultado, podemos definir:

Definição I.5.18 *O* **grau de transcendência de K sobre k** *é a cardinalidade de uma base transcendente de K sobre k.*

Teorema I.5.19 (Teorema da Normalização de Noether) *Sejam A uma álgebra afim sobre um corpo K, $I \subset A$ um ideal com $I \neq A$. Existem naturais $\delta \leq d$ e elementos $Y_1, \ldots, Y_d \in A$ tais que:*

a) *$Y_1, \ldots, Y_d$ são algebricamente independentes sobre K.*

b) *A é finitamente gerado como um $K[Y_1, \ldots, Y_d]$-módulo.*

c) $I \cap K[Y_1, \ldots, Y_d] = (Y_{\delta+1}, \ldots, Y_d)$ *em* $K[Y_1, \ldots, Y_d]$.

Se K é infinito e $A = K[x_1, \ldots, x_n]$, também temos:

d) *Para $i = 1, \ldots, \delta, Y_i$ é da forma $Y_i = \sum_{k=1}^{n} a_{ik}x_k, a_{ik} \in K$.*

Definição I.5.20 *Para uma K-álgebra afim $A \neq 0$, $K[Y_1, \ldots, Y_d] \subset A$ é dita uma* **normalização Noetheriana**, *se $Y_1, \ldots, Y_d$ são elementos algebricamente independentes sobre K e A é um $K[Y_1, \ldots, Y_d]$-módulo finitamente gerado.*

Do Teorema da Normalização de Noether e dos Teoremas de Cohen-Seidenberg seguem importantes resultados a respeito das dimensões de álgebras afins e suas cadeias de ideais primos. Dizemos que uma cadeia de ideais primos é **maximal** se não existe uma cadeia de comprimento maior que o dessa cadeia e que contenha todos os ideais primos dessa cadeia dada.

Proposição I.5.21 *Seja A uma K-álgebra afim. Se $K[Y_1, \ldots, Y_d] \subset A$ é uma normalização Noetheriana, então $dim(A) = d$. Além disso, se A é um domínio, então todas as cadeias maximais de ideais primos de A têm o mesmo comprimento d. (Em particular, isso vale para a álgebra polinomial $K[Y_1, \ldots, Y_d]$.)*

Em particular, segue que álgebras afins sempre têm dimensão de Krull finita.

Corolário I.5.22 *Sejam $\mathfrak{p} \subset \mathfrak{q}$ ideais primos da álgebra afim A, com $\mathfrak{q} \neq A$. Todas as cadeias maximais de ideais primos que começam com $\mathfrak{p}$ e terminam com $\mathfrak{q}$ têm o mesmo comprimento, que é $dim(A/\mathfrak{p}) - dim(A/\mathfrak{q})$.*

Corolário I.5.23 *Sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ ideais primos minimais da K-álgebra afim A e seja L_i o corpo de frações de $A/\mathfrak{p}_i, i = 1, \ldots, s$. Então:*

a) *$dim(A) = max_{i=1,\ldots,s}\{gr.tr._K(L_i)\}$. Em particular, $dim(A) = gr.tr._K(L)$, se A é um domínio com corpo de frações L.*

b) *Se $dim(A/\mathfrak{p}_i)$ é independente de $i = 1, \ldots, s$, então para todo $\mathfrak{p} \in Spec(A)$:*

$$dim(A) = ht(\mathfrak{p}) + dim(A/\mathfrak{p}).$$

Dem. : Como toda cadeia maximal de ideais primos de A começa com um dos $\mathfrak{p}_i$, é suficiente mostrar as afirmações para domínios. Se A é domínio e $K[Y_1, \ldots, Y_d] \subset A$ é uma normalização Noetheriana, então, como $A|K[Y_1, \ldots, Y_d]$ é inteira, $dim(A) = d = gr.tr._K K[Y_1, \ldots, Y_d] = gr.tr._K L$. A fórmula $dim(A) = ht(\mathfrak{p}) + dim(A/\mathfrak{p})$ segue de I.5.22. □

Corolário I.5.24 *Se A é uma K-álgebra afim, então $dim(A)$ é o número máximo de elementos de A que são algebricamente independentes sobre K. Se $B \subset A$ é outra K-álgebra afim, então $dim(B) \leq dim(A)$.*

Em particular, se $B \subset A$ são duas K-álgebras afins, então $gr.tr._B(A) = dim(A) - dim(B)$.

I.6 Localização

Sejam R um anel, $S \subset R$ um subconjunto fechado multiplicativamente (por convenção, $1 \in S$) e M um R-módulo. Denotaremos, para cada $r \in R$, por $\mu_r : M \to M$ a aplicação tal que $\mu_r(m) = rm$. Queremos introduzir os conceitos de módulo e anel de frações, assim como o que existe para o corpo de frações de um domínio.

Definição I.6.1 *Um R-módulo M junto com uma aplicação linear $i : M \to M_S$ é chamado um* **módulo de fraçõesde M com conjunto denominador S** *(ou* **por S***) se:*

1. *Para todo $s \in S, \mu_s : M_S \to M_S$ é bijetiva.*
2. *Se N é qualquer R-módulo para o qual $\mu_s : N \to N$ é bijetiva, para todo $s \in S$, e se $j : M \to N$ é qualquer aplicação linear, então existe uma única aplicação linear $l : M_S \to N$ com $j = l \circ i$.*

$$\begin{tikzcd} M \arrow[r, "j"] \arrow[d, "i"'] & N \\ M_S \arrow[ur, "l"'] & \end{tikzcd}$$

A aplicação i é dita a **aplicação canônica** *no módulo de frações.*

Para construir o módulo de frações de um R-módulo M, denotado por M_S, consideramos a relação de equivalência em $M \times S$

$$(m, s) \sim (m', s') \Leftrightarrow \exists s'' \in S; s''(ms' - sm') = 0.$$

e denotamos por $\frac{m}{s}$ a classe de equivalência do representante (m, s). M_S será o conjunto das classes de equivalência e $i : M \to M_S$ a aplicação natural $m \mapsto m/1, \forall m \in M$. Define-se naturalmente a soma e o produto em M_S:

$$\frac{m}{s} + \frac{m'}{s'} := \frac{s'm + sm'}{ss'} \qquad \text{e} \qquad r.\frac{m}{s} := \frac{rm}{s}, r \in R$$

e verifica-se que essa construção resulta realmente no módulo de frações de M por S.

No caso especial em que $M = R$, temos o **anel de frações de R por S**.

Exemplos I.6.2

- Se $R \neq 0$ é um domínio e $S = R - \{0\}$, então R_S é o corpo de frações de R e $i : R \to R_S$ é a imersão de R no corpo de frações que identifica $r \in R$ com a "fração imprópria" $\frac{r}{1}$.
- Sejam $R \neq 0$ um anel e S o subconjunto fechado multiplicativamente dos elementos regulares de R. Nesse caso, R_S é chamado **anel total de frações de R**, denotado por $Q(R)$.
- Sejam R um anel e g um elemento de R. Temos que $S = \{1, g, g^2, \ldots, \}$ é um subconjunto fechado multiplicativamente de R. Nesse caso, o módulo de frações de M por S será denotado por M_g e o anel de frações de R por S, por R_g.

- Seja R qualquer anel. Temos que $S := R - \mathfrak{p}$ é fechado multiplicativamente. O anel de frações de R por S será denotado por $R_{\mathfrak{p}}$ e será chamado de **anel local do ideal primo** $\mathfrak{p}$ de R ou a **localização de** R **em** $\mathfrak{p}$. $R_{\mathfrak{p}}$ é, de fato, um anel local. Seu ideal maximal $\mathfrak{m}_{\mathfrak{p}}$ consiste dos elementos p/s, com $p \in \mathfrak{p}, s \in S$ e é claro que esses elementos formam um ideal de R. Além disso, se $r/s \in R_{\mathfrak{p}} - \mathfrak{m}_{\mathfrak{p}}$ é dado, então $r \notin \mathfrak{p}$ e r/s é uma unidade de $R_{\mathfrak{p}}$ com inverso s/r. Portanto, $\mathfrak{m}_{\mathfrak{p}}$ é um ideal maximal de $R_{\mathfrak{p}}$, e não existem outros.

Usando a propriedade universal de definição do módulo de frações, podemos mostrar que se M é um R-módulo e $S \subset R$ é um subconjunto fechado multiplicativamente de R, então $M_S \cong R_S \otimes_R M$.

Vamos estudar agora as principais propriedades dos módulos e anéis de frações. Consideraremos R um anel, M um R-módulo e $S \subset R$ fechado multiplicativamente.

Definições I.6.3 • *O* **submódulo de torção** *de M é o conjunto*

$$T(M) = \{m \in M; \exists s \in R \text{ regular tal que } sm = 0\}.$$

- *Dizemos que M é* **livre de torção** *se $T(M) = 0$.*
- *Dizemos que um elemento $u \in M$ é um* **elemento de torção** *de M se $u \in T(M)$.*

Podemos relacionar esse conceito com a aplicação natural $i : M \to M_S$, quando considerarmos S o conjunto dos elementos regulares de R. Como $Ker(i) = \{m \in M; \exists s \in S \text{ com } sm = 0\}$, então nesse caso $Ker(i) = T(M)$. Logo, M é livre de torção se, e só se, i é injetiva. Em geral, $i : R \to R_S$ é injetiva se, e só se, S não tem divisores de zero de R.

Podemos conseguir informações locais-globais, ou seja, obter informações globais a partir das informações em cada localização:

Proposição I.6.4 *$M = 0$ se, e só se, $M_{\mathfrak{m}} = 0$, para todo $\mathfrak{m} \in Max(R)$.*

Dem. : Se $M_{\mathfrak{m}} = 0$, para todo $\mathfrak{m} \in Max(R)$ e $n \in M$ é dado, então existe $s \in R - \mathfrak{m}$ tal que $sn = 0$. Logo, $Ann(n)$ não está contido em nenhum ideal maximal de R. Portanto, $Ann(n) = R$ e, logo, $1 \in Ann(n)$, o que significa que $n = 0$. □

Definição I.6.5 *O* **suporte** *de M é o conjunto*

$$Supp(M) := \{\mathfrak{p} \in Spec(R); M_{\mathfrak{p}} \neq 0\}.$$

Proposição I.6.6 *Se M é finitamente gerado, então*

$$Supp(M) = \mathbf{V}(Ann(M)) = \{\mathfrak{p} \in Spec(R); \mathfrak{p} \supset Ann(M)\}.$$

Em particular, $Supp(M)$ é um subconjunto fechado de $Spec(R)$.

Podemos mostrar que:

Proposição I.6.7 *Se M é um R-módulo Noetheriano, então M_S é um R_S-módulo Noetheriano. Se R é um anel Noetheriano, então R_S também é Noetheriano.*

Proposição I.6.8 *Seja $i : R \to R_S$ a aplicação canônica, Σ o conjunto de todos os $\mathfrak{p} \in Spec(R)$ com $\mathfrak{p} \cap S = \emptyset$. Então:*

a) *Todo $\mathfrak{q} \in Spec(R_S)$ é da forma $\mathfrak{q} = \mathfrak{p}_S$, para um $\mathfrak{p} \in \Sigma$ unicamente determinado.*

b) *$Spec(i) : Spec(R_S) \to Spec(R)$ define um homeomorfismo de $Spec(R_S)$ sobre Σ, considerado com a topologia relativa da topologia de Zariski.*

c) *Para todo $\mathfrak{p} \in \Sigma$, temos $ht(\mathfrak{p}_S) = ht(\mathfrak{p})$ e para qualquer ideal I de R com $I_S \neq R_S$ temos $ht(I_S) \geq ht(I)$.*

d) *$dim(R_S) \leq dim(R)$.*

e) *Se R é um anel fatorial e $0 \notin S$, então R_S também é fatorial.*

Corolário I.6.9 *Para qualquer $\mathfrak{p} \in Spec(R), Spec(R_{\mathfrak{p}}) \to Spec(R)$ define um homeomorfismo de $Spec(R_{\mathfrak{p}})$ sobre o conjunto de todos os ideais primos contidos em $\mathfrak{p}$. Temos $ht(\mathfrak{p}) = dim(R_{\mathfrak{p}})$.*

Usando a propriedade universal de definição do módulo de frações, temos:

Proposição I.6.10 *As seguintes regras são válidas:*

- *Se $U \subset M$ são dois R-módulos, então $(M/U)_S \cong M_S/U_S$.*
- *Se I é um ideal de R e S' é a imagem de S em R/I, então $(R/I)_{S'} \cong R_S/I_S$.*
- *Se $M \xrightarrow{\alpha} N \xrightarrow{\beta} P$ é uma seqüência exata de R-módulos e aplicações lineares, então a seqüência de R_S-módulos $M_S \xrightarrow{\alpha_S} N_S \xrightarrow{\beta_S} P_S$ é exata.*

Exemplos I.6.11 1. Sejam I um ideal de R, $\mathfrak{p} \in Spec(R)$ contendo I e $\mathfrak{p}'$ a imagem de $\mathfrak{p}$ em R/I. Temos o seguinte isomorfismo canônico:

$$(R/I)_{\mathfrak{p}'} \cong R_{\mathfrak{p}}/I_{\mathfrak{p}}.$$

No caso $I = \mathfrak{p}$ resulta no isomorfismo:

$$Q(R/\mathfrak{p}) \cong R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}.$$

O corpo residual do anel local $R_{\mathfrak{p}}$ pelo ideal maximal $\mathfrak{p}R_{\mathfrak{p}}$ é portanto isomorfo ao corpo de frações de $R/\mathfrak{p}$.

2. Se $R \neq 0$ é um domínio e $\mathfrak{q} \in Spec(R)$, então existe um isomorfismo canônico

$$Q(R) \cong Q(R_{\mathfrak{q}}).$$

Aqui $R_{\mathfrak{q}}$ se identifica com o conjunto dos $r/s \in Q(R)$, com $r \in R$ e $s \in R - \mathfrak{q}$. Podemos considerar os anéis locais como subanéis de $Q(R)$; naturalmente eles têm o mesmo corpo de frações.

Proposição I.6.12 *Se P, Q são submódulos de M, então $P = Q$ se, e só se, $P_{\mathfrak{m}} = Q_{\mathfrak{m}}$, para todo $\mathfrak{m} \in Max(R)$.*

Dem. : Temos $((P+Q)/Q)_{\mathfrak{m}} \cong (P_{\mathfrak{m}} + Q_{\mathfrak{m}})/P_{\mathfrak{m}}$ e $((P+Q)/P)_{\mathfrak{m}} \cong (P_{\mathfrak{m}} + Q_{\mathfrak{m}})/P_{\mathfrak{m}}$. Se $P_{\mathfrak{m}} = Q_{\mathfrak{m}}, \forall \mathfrak{m} \in Max(R)$, então $(P+Q)/Q = (P+Q)/P = 0$, por I.6.4. Logo, $P = Q$. □

Corolário I.6.13 *Uma seqüência de R-módulos e aplicações lineares $M \xrightarrow{\alpha} N \xrightarrow{\beta} P$ é exata se, e só se, para todo $\mathfrak{m} \in Max(R)$, a seqüência $M_{\mathfrak{m}} \xrightarrow{\alpha_{\mathfrak{m}}} N_{\mathfrak{m}} \xrightarrow{\beta_{\mathfrak{m}}} P_{\mathfrak{m}}$ é exata.*

Dem. : Se $K := Ker(\beta)$ e $U := Im(\alpha)$, vemos facilmente, usando as definições, que $K_{\mathfrak{m}} = Ker(\beta_{\mathfrak{m}})$ e $U_{\mathfrak{m}} = Im(\alpha_{\mathfrak{m}})$. Por I.6.12, $K = U$ se, e só se, $K_{\mathfrak{m}} = U_{\mathfrak{m}}, \forall \mathfrak{m} \in Max(R)$. □

I.7 Lema de Nakayama - Cota de Forster-Swan

Definição I.7.1 *Sejam R um anel e M um R-módulo finitamente gerado. Um sistema de geradores de M com o menor número de elementos dentre os sistemas de geradores de M é dito um* **sistema minimal de geradores** *de M e seu número de elementos é denotado por $\mu(M)$.*

Quando trabalhamos com módulos sobre anéis locais, o seguinte lema é de fundamental importância:

Lema I.7.2 (Lema de Nakayama) *Seja I um ideal de R que está contido na interseção de todos os ideais maximais de R. Sejam M um R-módulo qualquer e $N \subset M$ um submódulo tal que M/N é finitamente gerado. Se $M = N + IM$, então $M = N$.*

Dem. : $\overline{M} := M/N$ tem um sistema minimal de geradores $\{m_1, \ldots, m_t\}$. Suponhamos $t > 0$. Como $\overline{M} = I\overline{M}$, existe uma equação

$$m_t = \sum_{j=1}^{t} a_j m_j \ (a_j \in I, j = 1, \ldots, t).$$

Como $a_t \in I \subset \mathfrak{m}$, para todo $\mathfrak{m} \in Max(R)$, então $1 - a_t$ é uma unidade em R. De $(1 - a_t)m_t = \sum_{j=1}^{t-1} a_j m_j$, segue que $m_t \in \langle m_1, \cdots, m_{t-1} \rangle$. Isso contradiz a hipótese de minimalidade do sistema de geradores. Portanto $t = 0$, logo $M = N$. □

Corolário I.7.3 *Sejam $(R, \mathfrak{m})$ um anel local, $K = R/\mathfrak{m}$ seu corpo residual e M um R-módulo finitamente gerado. Para elementos $m_1, \cdots, m_t \in M$, as seguintes afirmações são equivalentes:*

(a) $M = \langle m_1, \cdots, m_t \rangle$.

(b) *As classes residuais* $\overline{m_1}, \cdots, \overline{m_t} \in M/\mathfrak{m}M$ *dos* m_i *formam um sistema de geradores do* K*-espaço vetorial* $M/\mathfrak{m}M$.

Dem. : De $M/\mathfrak{m}M = \langle \overline{m_1}, \cdots, \overline{m_t} \rangle$ segue que $M = \langle m_1, \cdots, m_t \rangle + \mathfrak{m}M$ e assim $M = \langle m_1, \cdots, m_t \rangle$, pelo Lema de Nakayama. □

Do corolário anterior e dos fatos conhecidos sobre espaços vetoriais, resulta:

Corolário I.7.4 *Sob as mesmas hipóteses do lema anterior, temos:*

(a) $\mu(M) = dim_K(M/\mathfrak{m}M)$.

(b) $m_1, \cdots, m_t \in M$ *formam um sistema minimal de geradores de* M *se, e só se, suas classes residuais* $\overline{m_1}, \cdots, \overline{m_t} \in M/\mathfrak{m}M$ *formam uma base de* $M/\mathfrak{m}M$.

(c) *Se* $m_1, \cdots, m_t$ *é um sistema minimal de geradores de* M *e se*

$$\sum_{i=1}^{t} r_i m_i = 0 \ (r_i \in R)$$

então $r_i \in \mathfrak{m}$, *para* $i = 1, \cdots, t$.

(d) *Qualquer sistema de geradores de* M *contém um sistema minimal.*

(e) *Os elementos* $m_1, \cdots m_r \in M$ *podem ser estendidos a um sistema minimal de geradores de* M *se, e só se, suas classes residuais* $\overline{m_1}, \cdots, \overline{m_r} \in M/\mathfrak{m}M$ *são linearmente independentes sobre* K.

Esses resultados nos dão informações sobre a geração de módulos sobre anéis locais. Passamos agora para anéis globais.

Definição I.7.5 *Para* $\mathfrak{p} \in Spec(R)$, *denotamos por* $\mu_{\mathfrak{p}}(M)$ *o número mínimo de elementos em um menor sistema de geradores do* $R_{\mathfrak{p}}$*-módulo* $M_{\mathfrak{p}}$.

Podemos mostrar que

Teorema I.7.6 *Sejam* $X = Spec(R)$ *Noetheriano e de dimensão de Krull finita e* M *um* R*-módulo. Então*

$$\mu(M) \leq b(M) := max\{\mu_{\mathfrak{p}}(M) + dim\mathbf{V}(\mathfrak{p}); \mathfrak{p} \in X \cap Supp(M)\},$$

onde $b(M)$ *é chamado a* **cota de Forster-Swan**.

I.8 Teorema do Ideal Principal de Krull - Aplicações - Anéis Locais Regulares

O Teorema do Ideal Principal de Krull dará uma cota inferior para o número de geradores de um ideal em um anel Noetheriano.

Teorema I.8.1 (Teorema do Ideal Principal de Krull) *Sejam R um anel Noetheriano e $(a) \neq R$ um ideal principal de R. Então $ht(\mathfrak{p}) \leq 1$, para qualquer divisor primo minimal $\mathfrak{p}$ de (a), e $ht(\mathfrak{p}) = 1$ se a não é um divisor de zero de R.*

Sua generalização é a seguinte:

Teorema I.8.2 (Teorema Generalizado do Teorema do Ideal Principal de Krull) *Sejam R um anel Noetheriano e $I \neq R$ um ideal gerado por m elementos. Para qualquer divisor primo minimal $\mathfrak{p}$ de I, $ht(\mathfrak{p}) \leq m$.*

Como a altura de um ideal $I \neq (1)$ é definida como o ínfimo das alturas dos divisores primos de I, segue pelo Teorema Generalizado de Krull que um ideal $I \neq (1)$ em um anel Noetheriano sempre tem altura finita, pois $ht(I) \leq \mu(I)$.

Definições I.8.3 *Seja $I \neq R$ um ideal em um anel Noetheriano R.*

a) *Dizemos que I é uma* **interseção completa** *se $ht(I) = \mu(I)$.*

b) *Dizemos que I é* **localmente uma interseção completa** *se $I_{\mathfrak{m}}$ é uma interseção completa em $R_{\mathfrak{m}}$, para todo $\mathfrak{m} \in Max(R)$ com $I \subset \mathfrak{m}$.*

Definição I.8.4 *Um ideal $\mathfrak{q}$ de um anel R é chamado* **primário** *se qualquer divisor de zero de $R/\mathfrak{q}$ é nilpotente.*

Equivalentemente, se $a, b \in R$ com $a.b \in \mathfrak{q}$ e $a \notin \mathfrak{q}$, então existe um $n \in I\!N$ com $b^n \in \mathfrak{q}$.

Observação I.8.5 Podemos mostrar, usando as definições, que o radical de um ideal primário é um ideal primo. Se $\mathfrak{q}$ é primário e $\mathfrak{p} = \sqrt{\mathfrak{q}}$, dizemos que $\mathfrak{q}$ é um ideal **$\mathfrak{p}$-primário**.

Proposição I.8.6 Sejam $(R, \mathfrak{m})$ um anel Noetheriano local, $\mathfrak{q}$ um ideal $\mathfrak{m}$-primário. Então $\mu(\mathfrak{q}) \geq dim(R)$. Em particular, $\mu(\mathfrak{m}) \geq dim(R)$.

Dem. : Como $\mathfrak{m} = \sqrt{\mathfrak{q}}$ é a interseção dos ideais primos que contêm $\mathfrak{q}$, supondo que $\mathfrak{p}$ é um divisor primo minimal de $\mathfrak{q}$, temos que $\mathfrak{m} \subset \mathfrak{p}$. Como $\mathfrak{m}$ é maximal, segue que $\mathfrak{m} = \mathfrak{p}$. Logo, $\mathfrak{m}$ é o único divisor primo minimal de $\mathfrak{q}$. Pelo Teorema Generalizado de Krull, segue que $\mu(\mathfrak{q}) \geq ht(\mathfrak{m}) = dim(R)$. □

Definição I.8.7 *Se $(R, \mathfrak{m})$ é um anel Noetheriano local, então $\mu(\mathfrak{m})$ é chamada a* **dimensão de mergulho** *de R, e é denotada por $edim(R)$.*

Como acabamos de ver, $edim(R) \geq dim(R)$.

Temos a recíproca do Teorema Generalizado de Krull:

Proposição I.8.8 *Seja R um anel Noetheriano. Se $\mathfrak{p} \in Spec(R)$ tem altura m, então existem elementos $a_1, \ldots, a_m \in \mathfrak{p}$ tais que $\mathfrak{p}$ é um divisor primo minimal de $(a_1, \ldots, a_m)$.*

Para a dimensão de Krull de anéis locais Noetherianos, temos a seguinte descrição:

Corolário I.8.9 *Em um anel Noetheriano local $(R, \mathfrak{m})$ existe um ideal $\mathfrak{m}$-primário $\mathfrak{q}$ que é uma interseção completa: $\mu(idq) = dim(R)$. Temos $dim(R) = min\{\mu(\mathfrak{q}); \mathfrak{q}$ é $\mathfrak{m}$-primário$\}$.*

Dem. : Seja $m := dim(R) = ht(\mathfrak{m})$. Pela Proposição I.8.8 existem elementos $a_1, \ldots, a_m \in \mathfrak{m}$ tais que $\mathfrak{m}$ é o único divisor primo minimal de $\mathfrak{q} := (a_1, \ldots, a_m)$. Logo, $Spec(R/\mathfrak{q})$ tem somente um elemento, que é $\mathfrak{m}/\mathfrak{q}$. Como $\mathfrak{m}/\mathfrak{q}$ é o nilradical de $R/\mathfrak{q}$, os elementos de $\mathfrak{m}/\mathfrak{q}$ são nilpotentes e os elementos fora de $\mathfrak{m}/\mathfrak{q}$ são unidades. Logo, os divisores de zero de $R/\mathfrak{q}$ são nilpotentes e portanto $\mathfrak{q}$ é primário. Como $\mathfrak{m}$ é o único divisor primo minimal de $\mathfrak{q}$, segue que $\sqrt{\mathfrak{q}} = \mathfrak{m}$. Assim, $\mu(\mathfrak{q}) \leq m = dim(R) \;_{I.8.6} \leq \mu(\mathfrak{q})$, ou seja, $\mu(\mathfrak{q}) = dim(R)$. Portanto $\mathfrak{q}$ é uma interseção completa. Como $\mu(\mathfrak{q}') \geq dim(R)$, para qualquer ideal $\mathfrak{m}$-primário $\mathfrak{q}'$, a fórmula da dimensão também segue. □

Definição I.8.10 *Um conjunto $\{a_1, \ldots, a_d\}$ de elementos de um anel Noetheriano local $(R, \mathfrak{m})$ de dimensão d é chamado um* **sistema de parâmetros de** *R se ele gera um ideal $\mathfrak{m}$-primário.*

Pelo Corolário I.8.9, tal sistema sempre existe.

Queremos obter uma caracterização das interseções completas de anéis Noetherianos arbitrários.

Definição I.8.11 *Um sistema de elementos $\{a_1, \ldots, a_m\}, m \geq 0$ de um anel R é chamado* **independente** *se as seguintes condições são válidas:*

a) *$(a_1, \ldots, a_m) \neq R$.*

b) *Se $F \in R[X_1, \ldots, X_m]$ é um polinômio homogêneo com $F(a_1, \ldots, a_m) = 0$, então todos os coeficientes de F estão contidos no $\sqrt{(a_1, \ldots, a_m)}$.*

Lema I.8.12 *Seja $R[X]$ o anel polinomial sobre um anel Noetheriano R. Para qualquer ideal I de R com $I \neq R$, temos $ht(IR[X]) = ht(I), ht((I, X)R[X]) = ht(I) + 1$ e se $dimR < \infty$, então $dimR[X] = dimR + 1$.*

Teorema I.8.13 *Em um anel Noetheriano R, seja $I = (a_1, \ldots, a_m) \neq R$ dado. Então $ht(I) = m$ (e logo I é uma interseção completa) se, e só se, $\{a_1, \ldots, a_m\}$ é independente.*

Corolário I.8.14 *Sejam $a_1, \ldots, a_d$ elementos no ideal maximal de um anel Noetheriano local $(R, \mathfrak{m})$ de dimensão d. $\{a_1, \ldots, a_d\}$ é um sistema de parâmetros de R se, e só se, $\{a_1, \ldots, a_d\}$ é independente.*

Vamos agora fazer um estudo dos anéis locais regulares.

Definição I.8.15 *Um anel Noetheriano local R é chamado* **regular** *se $edim(R) = dim(R)$, ou seja, se o ideal maximal de R é gerado por $dim(R)$ elementos.*

Nessa terminologia, podemos definir o conceito de ponto regular de uma variedade. Considere uma variedade afim $V \subset \mathbb{A}^n$ e um ponto $x \in V$. Ao ponto $x = (a_1, \ldots, a_n)$ está associado o ideal maximal $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n) \supset \mathbf{I}(V)$. Dizemos que x é **regular** se $K[V]_{\overline{\mathfrak{m}}}$ é um anel regular, onde $\overline{\mathfrak{m}} = \mathfrak{m}/\mathbf{I}(V)$.

Exemplos I.8.16 Exemplos de anéis locais regulares são os corpos e os anéis locais $R_{(\pi)}$, onde R é um anel fatorial e π é um elemento primo de R, pois $dimR_{(\pi)} = 1$ e o ideal maximal de $R_{(\pi)}$ é gerado por π. Em particular, os anéis locais $\mathbb{Z}_{(p)}$, onde p é um número primo, são regulares.

Mais exemplos são obtidos a partir do seguinte resultado:

Proposição I.8.17 *Se $(R, \mathfrak{m})$ é um anel local regular, então $R[X]_{\mathfrak{q}}$ também é regular, para todo $\mathfrak{q} \in Spec(R[X])$, com $\mathfrak{q} \cap R = \mathfrak{m}$.*

Corolário I.8.18 *Se K é um domínio de ideais principais, então $K[X_1, \ldots, X_n]_{\mathfrak{q}}$ é regular, para qualquer $\mathfrak{q} \in Spec(K[X_1, \ldots, X_n])$.*

Em particular, se $R = K[X_1, \ldots, X_n]$, onde K é corpo, então $R_{\mathfrak{p}}$ é regular, para todo $\mathfrak{p} \in Spec(R)$.

Observação I.8.19 Anéis locais regulares são domínios e integralmente fechados em seu corpo de frações.

Definição I.8.20 *Seja M um R-módulo. Dizemos que $a \in R$ é um* **elemento** M**-regular** *(ou* **não é um divisor de zero de** M*) se $ax = 0$, com $x \in M$ implica que $x = 0$. Uma seqüência $\{a_1, \ldots, a_m\}, m \geq 0$ de elementos de R é chamada uma* **seqüência** M**-regular** *se:*

a) $M \neq (a_1, \ldots, a_m)M$.

b) *Para $i = 0, \ldots, m-1, a_{i+1}$ não é um divisor de zero de $M/(a_1, \ldots, a_i)M$.*

No caso em que $M = R$, também dizemos que $a_1, \ldots, a_m$ é uma R**-seqüência.**

Observação I.8.21 Se $a_1, \ldots, a_n$ são algebricamente independentes sobre o corpo K, então eles formam uma $K[a_1, \ldots, a_n]$-seqüência.

De fato, primeiro observamos que a_1 não é divisor de zero de $R = K[a_1, \ldots, a_n]$:

$$a_1 f(a_1, \ldots, a_n) = 0 \Rightarrow f = 0.$$

Suponhamos agora que a_i não seja divisor de zero de $R/(a_1,\ldots,a_{i-1})R$. Podemos definir a aplicação

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & K[a_{i+1},\ldots,a_n] \\ a_j & \mapsto & \begin{cases} 0 & \text{se } j=1,\ldots,i \\ a_j & \text{se } j=i+1,\ldots,n \end{cases} \end{array}$$

cujo núcleo será o ideal $(a_1,\ldots,a_i)$ de R.

Logo, $R/(a_1,\ldots,a_i)R \cong K[a_{i+1},\ldots,a_n]$, que é domínio.

Portanto, supondo que $a_{i+1}\overline{f_{i+1}} = 0$ em $R/(a_1,\ldots,a_i)R$, devemos ter $\overline{f_{i+1}} = 0$ e segue que a_{i+1} não é divisor de zero de $R/(a_1,\ldots,a_i)R$.

Observação I.8.22 1. Se $(R,\mathfrak{m})$ é um anel local regular, então qualquer sistema minimal de geradores $\{a_1,\ldots,a_d\}$ de $\mathfrak{m}$ é um sistema de parâmetros de R e uma R-seqüência. Qualquer subsistema $\{a_{i_1},\ldots,a_{i_d}\}$ gera um ideal primo de R.

2. $(R,\mathfrak{m})$ é local regular se, e só se, qualquer sistema minimal $a_1,\ldots,a_n$ de geradores de $\mathfrak{m}$ é independente.

   De fato, se $(R,\mathfrak{m})$ é regular, então $a_1,\ldots,a_n$ é um sistema de parâmetros de R e pelo Corolário I.8.14, $\{a_1,\ldots,a_n\}$ é independente.

   Reciprocamente, se $a_1,\ldots,a_n$ são independentes, então, pelo Teorema I.8.13, $ht(\mathfrak{m}) = n$ e, logo, R é regular.

I.9 Anéis Cohen-Macaulay

Sejam M um módulo finitamente gerado sobre um anel Noetheriano R e I um ideal de R com $IM \neq M$. Para qualquer R-seqüência $\{a_1,\ldots,a_m\}$ temos $(a_1,\ldots,a_i)M \neq (a_1,\ldots,a_{i+1})M$, para $i = 0,\ldots,m-1$. Como M é um módulo Noetheriano, segue que qualquer R-seqüência $\{a_1,\ldots,a_m\}$, com $a_i \in I$ pode ser estendida a uma seqüência **maximal**, isto é, uma seqüência M-regular $\{a_1,\ldots,a_n\} \subset I, n \geq m$ tal que qualquer $a \in I$ é um divisor de zero de $M/(a_1,\ldots,a_n)M$. Podemos mostrar que

Proposição I.9.1 *Quaisquer duas seqüências maximais M-regulares em I têm o mesmo número de elementos.*

Definição I.9.2 *Sejam R um anel Noetheriano, I um ideal de R com $IM \neq M$ e M um R-módulo finitamente gerado. O número de elementos de uma seqüência M-regular em I maximal é chamado a* **I-profundidade de M**, *denotada por $d(I,M)$ ou a* **graduação de M com relação a** *I. Se R é local e I é seu ideal maximal, então chamamos $d(I,M)$ simplesmente de* **profundidade de** *M e escrevemos $d(M)$. Em particular, está definido $d(R)$.*

Com esse conceito, obtemos o seguinte critério para interseções completas:

Proposição I.9.3 *Sejam R um anel Noetheriano e $I \neq R$ um ideal de R com $\sqrt{I} = I$. I é uma interseção completa em R se, e só se, I é gerado por uma R-seqüência. Em particular, uma variedade afim é uma interseção completa se, e só se, seu ideal no anel polinomial é gerado por uma seqüência regular.*

Vamos agora discutir a relação entre a profundidade de um módulo e sua dimensão de Krull.

Definição I.9.4 *A* **dimensão** *de um módulo M sobre um anel R é a dimensão de Krull de $R/Ann(M)$.*

É claro que para $M = R$, não há nada de novo. Se M é um R-módulo finitamente gerado, então os divisores primos minimais de $Ann(M)$ são também os elementos primos de $Supp(M)$. Assim, temos a fórmula:

$$dim(M) = sup_{\mathfrak{p} \in Supp(M)}\{dim R/\mathfrak{p}\}.$$

Proposição I.9.5 *Seja $(R, \mathfrak{m})$ um anel Noetheriano local e $M \neq 0$ um R-módulo finitamente gerado. Então*

$$d(M) \leq dim(M).$$

Definição I.9.6 *Seja M um módulo finitamente gerado sobre um anel Noetheriano R. Se R é local, dizemos que M é um* **módulo Cohen-Macaulay** *se $M = 0$ ou se $d(M) = dim(M)$. No caso geral, M é um* **módulo Cohen-Macaulay** *se $M_{\mathfrak{m}}$, considerado como um $R_{\mathfrak{m}}$-módulo, é Cohen-Macaulay, para todo $\mathfrak{m} \in Max(R)$. R é chamado um* **anel Cohen-Macaulay** *se, como um R-módulo, R é Cohen-Macaulay.*

Com esse conceito e alguns resultados que não convém mostrar aqui, concluímos que

Proposição I.9.7 *Sejam $(R, \mathfrak{m})$ um anel Cohen-Macaulay e $\{a_1, \ldots, a_m\}$ um sistema de elementos em $\mathfrak{m}$. Então $\{a_1, \ldots, a_m\}$ é uma R-seqüência se, e só se, $\{a_1, \ldots, a_m\}$ pode ser estendido a um sistema de parâmetros de R. Em particular, os sistemas de parâmetros de R são exatamente as R-seqüências maximais em $\mathfrak{m}$.*

Exemplos I.9.8

1. Qualquer módulo finitamente gerado de dimensão 0 sobre um anel Noetheriano é Cohen-Macaulay; em particular, qualquer anel Noetheriano de dimensão 0 é Cohen-Macaulay.

   Com efeito, pela Proposição I.9.5, $d(M_{\mathfrak{m}}) \leq dim(M_{\mathfrak{m}}) = 0$; logo, $d(M_{\mathfrak{m}}) = 0, \forall \mathfrak{m} \in Max(R)$. Assim, $M_{\mathfrak{m}}$ é Cohen-Macaulay, $\forall \mathfrak{m} \in Max(R)$.

2. Qualquer anel Noetheriano regular é Cohen-Macaulay.

   De fato, se R é regular, ou seja, se $R_{\mathfrak{m}}$ é regular, $\forall \mathfrak{m} \in Max(R)$, então $\mathfrak{m}R_{\mathfrak{m}}$ é uma interseção completa, logo $\mathfrak{m}R_{\mathfrak{m}}$ é gerado por uma seqüência regular de comprimento $dim(R_{\mathfrak{m}})$. Assim, $d(\mathfrak{m}R_{\mathfrak{m}}) \geq dim(R_{\mathfrak{m}})$ e logo vale a igualdade.

3. Se K é um corpo, então $R = K[X_1, X_2]/(X_1^2, X_1X_2)$ não é Cohen-Macaulay.

   De fato, se m é o ideal gerado pelas imagens de X_1 e X_2 em R, então é claro que m contém estritamente o ideal de R gerado pela imagem de X_1; logo, $dim(R_m) \geq 1$. Por outo lado, como X_1 e X_2 são divisores de zero de R, segue que mR_m só tem divisores de zero, logo, $d(mR_m) = 0$. Portanto, R não é uma interseção completa.

Capítulo II

As Álgebras Simétrica e de Rees de um Ideal

Neste capítulo, vamos ver as definições da álgebra simétrica de um módulo e da álgebra de Rees de um ideal, além de suas principais propriedades. Por fim, faremos o cálculo das dimensões das álgebras simétrica e de Rees, esta última no caso em que o anel R é domínio.

II.1 A Álgebra Simétrica de um Módulo

Esta seção introduz o conceito da álgebra simétrica de um módulo e estabelece os principais resultados ligados a essa definição, bem como fornece o cálculo da álgebra simétrica de um módulo qualquer num anel Noetheriano.

Definição II.1.1 *Dados um anel R e um R-módulo M, a* **álgebra simétrica** *de M é uma R-álgebra $S(M)$ junto com um homomorfismo de R-módulos $\psi_M : M \to S(M)$ que satisfaz a seguinte propriedade universal: Para qualquer R-álgebra comutativa A e qualquer homomorfismo de R-módulos $\varphi : M \to A$, existe um único homomorfismo de R-álgebras $\phi : S(M) \to A$ tal que o diagrama abaixo é comutativo.*

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\psi_M"'] & A \\ S(M) \arrow[ur, "\phi"'] & \end{tikzcd}$$

Observação II.1.2 1. Se (S', ψ') for uma R-álgebra que também satisfaz a propriedade universal de definição da álgebra simétrica, então existe um único isomorfismo ϕ de $S(M)$ em S' tal que $\phi \circ \psi_M = \psi'$. (Por isso, podemos usar a notação $S(M)$ para a álgebra simétrica de M.) De fato, como (S', ψ') e $(S(M), \psi_M)$ satisfazem a propriedade universal das álgebras simétricas, temos que existem $\varphi : S' \to S(M)$ e $\phi : S(M) \to S'$ tais que os seguintes diagramas são comutativos:

$$\begin{tikzcd} M \arrow[r, "\psi_M"] \arrow[d, "\psi'"'] & S(M) \\ S' \arrow[ur, "\varphi"'] & \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, "\psi'"] \arrow[d, "\psi_M"'] & S' \\ S(M) \arrow[ur, "\phi"'] & \end{tikzcd}$$

Logo, temos:

$\psi_M = \varphi \circ \psi' = (\varphi \circ \phi) \circ \psi_M$

e

$\psi' = \phi \circ \psi_M = (\phi \circ \varphi) \circ \psi'$.

Obviamente, os diagramas abaixo também são comutativos:

$$\begin{tikzcd} M \arrow[r, "\psi_M"] \arrow[d, "\psi_M"'] & S(M) \\ S(M) \arrow[ur, "id"] & \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, "\psi'"] \arrow[d, "\psi'"'] & S' \\ S' \arrow[ur, "id"] & \end{tikzcd}$$

Pela unicidade da definição de álgebra simétrica, devemos ter $\varphi \circ \phi = id = \phi \circ \varphi$, ou seja, ϕ é um isomorfismo.

2. Se $(S(M), \psi_M)$ é a álgebra simétrica de M, então $\psi_M(M)$ é um conjunto de geradores da álgebra $S(M)$.
   De fato, considere S' a subálgebra de $S(M)$ gerada por $\psi_M(M)$. Existe $\phi : S(M) \to S'$ tal que $\phi \circ \psi_M = \psi_M$. Podemos considerar $\phi : S(M) \to S(M)$. Como $id \circ \psi_M = \psi_M$, pela unicidade devemos ter $\phi = id$. Logo, $S(M) = S'$.

$$\begin{tikzcd} M \arrow[r, "\psi_M"] \arrow[d, "\psi_M"'] & S' \\ S(M) \arrow[ur, "\phi"] & \end{tikzcd}$$

Vamos mostrar que, dado qualquer R-módulo M, existe uma álgebra simétrica de M. Para isso, precisamos definir e mostrar a existência da álgebra tensorial de M.

Definição II.1.3 *Sejam R um anel e M um R-módulo. Sejam dados uma R-álgebra não-comutativa $\mathcal{T}(M)$ e um homomorfismo de R-módulos $\theta_M : M \to \mathcal{T}(M)$. Dizemos que $(\mathcal{T}(M), \theta_M)$ é uma* **álgebra tensorial** *de M se a seguinte condição é satisfeita: Se φ é qualquer homomorfismo de R-módulos de M em uma R-álgebra A, então existe um único homomorfismo τ da álgebra $\mathcal{T}(M)$ em A tal que $\tau \circ \theta_M = \varphi$.*

$$\begin{tikzcd} M \arrow[r, "\phi"] \arrow[d, "\theta_M"'] & A \\ \mathcal{T}(M) \arrow[ur, "\tau"] & \end{tikzcd}$$

Observação II.1.4 De forma análoga à que foi mostrada para a álgebra simétrica, podemos mostrar que:

1. Se (T', θ') é uma R-álgebra que também satisfaz a condição de definição da álgebra tensorial, então existe um único isomorfismo $\delta : \mathcal{T}(M) \to T'$ tal que $\delta \circ \theta_M = \theta'$.

2. Se $(\mathcal{T}(M), \theta_M)$ é uma álgebra tensorial de M, então $\theta_M(M)$ é um conjunto de geradores da álgebra $\mathcal{T}(M)$.

Afirmação: Dado qualquer R-módulo M, existe uma álgebra tensorial em M.

De fato, consideremos para cada $n \in I\!N$ o R-módulo $\mathcal{T}^n(M) = \underbrace{M \otimes \cdots \otimes M}_{n\text{vezes}}$ e seja $\mathcal{T}(M) = \oplus_{n\geq 0}\mathcal{T}^n(M)$, onde $\mathcal{T}^0(M) = R, \mathcal{T}^1(M) = M$. Então,

- $\mathcal{T}(M)$ tem uma estrutura de R-álgebra:
  Para cada par de inteiros $n, m \geq 0$, definimos uma aplicação linear $\rho_{nm} : \mathcal{T}^n(M) \otimes \mathcal{T}^m(M) \to \mathcal{T}^{n+m}(M)$, que é a associatividade, se $m, n > 0$, e é a multiplicação por escalar canônica, se $m = 0$ ou $n = 0$. Logo, definimos para $x_i \in M, \alpha \in R$, que

$$\begin{aligned}
(x_1 \otimes \cdots \otimes x_n).(x_{n+1} \otimes \cdots \otimes x_{n+m}) &= x_1 \otimes \cdots \otimes x_n \otimes x_{n+1} \otimes \cdots \otimes x_{n+m} \quad \text{(II.1)}\\
\alpha.(x_1 \otimes \cdots \otimes x_n) &= \alpha(x_1 \otimes \cdots \otimes x_n) \quad \text{(II.2)}
\end{aligned}$$

  e definimos por linearidade uma multiplicação em $\mathcal{T}(M)$. Essa multiplicação é associativa e tem elemento unidade $1 \in R = \mathcal{T}^0(M)$.

- Definamos o homomorfismo de R-módulos

$$\begin{aligned}
\theta_M : M \to & \quad \mathcal{T}(M)\\
x \mapsto & \quad (0, x, 0, \ldots)
\end{aligned}$$

  Então θ_M é um isomorfismo de M sobre um submódulo de $\mathcal{T}(M)$, pois θ_M é injetiva.

Para mostrar que $(\mathcal{T}(M), \theta_M)$ é uma álgebra tensorial em M, seja $\varphi : M \to A$ um homomorfismo de R-módulos, onde A é uma R-álgebra qualquer. Vamos definir uma aplicação $\tau : \mathcal{T}(M) \to A$, tal que o diagrama abaixo seja comutativo.

$$\begin{tikzcd}
M \arrow[r, "\varphi"] \arrow[d, "\theta_M"'] & A \\
\mathcal{T}(M) \arrow[ur, "\tau"'] &
\end{tikzcd}$$

Para qualquer $n > 0$, a aplicação

$$\begin{aligned}
\varphi_n : \underbrace{M \times \cdots \times M}_{n\text{vezes}} \to & \quad A\\
(x_1, \ldots, x_n) \mapsto & \quad \varphi(x_1). \cdots .\varphi(x_n)
\end{aligned}$$

é R-multilinear.

Pela propriedade de produto tensorial, existe uma aplicação R-linear

$$\begin{aligned}
\tau_n : \mathcal{T}^n(M) \to & \quad A\\
x_1 \otimes \cdots \otimes x_n \mapsto & \quad \varphi(x_1). \cdots .\varphi(x_n)
\end{aligned}$$

e também definamos

$$\begin{aligned}\tau_0 : R \to \quad & A \\ \alpha \mapsto \quad & \alpha.1\end{aligned}$$

Seja

$$\begin{aligned}\tau : \mathcal{T}(M) \to \quad & A \\ \sum_{i=0}^{\infty} y_i \mapsto \quad & \sum_{i=0}^{\infty} \tau_i(y_i)\end{aligned}$$

Então:

- $\tau \circ \theta_M = \varphi$:
  $\tau \circ \theta_M(x) = \tau(0, x, 0, \ldots) = \tau_1(x) = \varphi(x)$.

- τ é um homomorfismo de R-álgebras:
  Pela construção, $\tau(1) = 1$, logo por linearidade, é suficiente mostrar que $\tau(xy) = \tau(x)\tau(y)$, para $x \in \mathcal{T}^n(M)$ e $y \in \mathcal{T}^m(M)$ $(n, m > 0)$ e também podemos supor que $x = x_1 \otimes \cdots \otimes x_n$ e $y = x_{n+1} \otimes \cdots \otimes x_{n+m}$. Pela fórmula II.1, $\tau(x)\tau(y) = [\varphi(x_1) \cdots \varphi(x_n)].[\varphi(x_{n+1}) \cdots \varphi(x_{n+m})] = \varphi(x_1) \cdots \varphi(x_{n+m}) = \tau(xy)$. Se $n = 0$ ou $m = 0$, podemos supor que $x = \alpha \in R$ e $y = x_1 \otimes \cdots \otimes x_n \in \mathcal{T}^n(M)$ e pela fórmula II.2, $\tau(x)\tau(y) = \alpha.(x_1 \otimes \cdots \otimes x_n) = \alpha(x_1 \otimes \cdots \otimes x_n) = \tau(xy)$.

- Unicidade de τ:
  Para cada família finita $(x_i)_{i=1}^n$ de elementos de M temos, pela definição de produto em $\mathcal{T}(M)$, que $x_1 \otimes \cdots \otimes x_n = \theta_M(x_1) \cdots \theta_M(x_n)$. De fato, se $n = 0$, isso é verdade. Suponhamos que $n > 0$ e essa igualdade válida para $n - 1$. Daí, $\theta_M(x_1) \cdots \theta_M(x_n) = [\theta_M(x_1) \cdots \theta_M(x_{n-1})]\theta_M(x_n) = (x_1 \otimes \cdots \otimes x_{n-1}) \otimes x_n = x_1 \otimes \cdots \otimes x_n$. Como $\tau \circ \theta_M = \varphi$, temos $\tau(x_1 \otimes \cdots \otimes x_n) = \varphi(x_1) \cdots \varphi(x_n)$, para $n \geq 1$ e $\tau(\alpha) = \alpha.1$, logo temos a unicidade de τ determinada por φ.

Portanto, $(\mathcal{T}(M), \theta_M)$ é uma álgebra tensorial de M.

Observação II.1.5 $\mathcal{T}(M)$ é uma álgebra graduada, pois $\mathcal{T}(M) = \oplus_{n \geq 0} \mathcal{T}^n(M)$ e $\mathcal{T}^n(M).\mathcal{T}^m(M) \subset \mathcal{T}^{n+m}(M)$.

Proposição II.1.6 *Sejam M um R-módulo, $(\mathcal{T}(M), \theta_M)$ uma álgebra tensorial de M. Suponha que $\varphi : M \to A$ é uma aplicação linear, onde A é uma álgebra graduada, e que os elementos de $\varphi(M)$ são homogêneos de grau 1 em A. Então existe um único homomorfismo $\tau : \mathcal{T}(M) \to A$ tal que $\tau \circ \theta_M = \varphi$ e τ é homogêneo de grau 0.*

Dem. : Se $x_1, \cdots, x_n \in M$, então $\tau(x_1 \otimes \cdots \otimes x_n) = \varphi(x_1) \cdots \varphi(x_n)$ é homogêneo de grau n em A. Segue que os elementos de $\tau(\mathcal{T}^n(M))$ são homogêneos de grau n, se $n > 0$, e τ é homogêneo. □

Finalmente, vamos mostrar que dado um R-módulo M, existe uma álgebra simétrica de M. Seja $(\mathcal{T}(M), \theta_M)$ uma álgebra tensorial de M. Denote por K_M o ideal gerado em $\mathcal{T}(M)$ pelos elementos $\theta_M(x)\theta_M(y) - \theta_M(y)\theta_M(x)$, para quaisquer $x, y \in M$. Sejam $S(M)$ a álgebra $\mathcal{T}(M)/K_M$ e $\pi : \mathcal{T}(M) \to S(M)$ a projeção canônica.

Sejam $\psi_M = \pi \circ \theta_M$, A uma álgebra comutativa e $\varphi : M \to A$ um homomorfismo de R-módulos. Como $(\mathcal{T}(M), \theta_M)$ é uma álgebra tensorial em M, existe um homomorfismo de R-álgebras τ de $\mathcal{T}(M)$ em A tal que $\tau \circ \theta_M = \varphi$.

$$\begin{tikzcd} M \arrow[r, "\theta_M"] \arrow[dr, "\varphi"'] & \mathcal{T}(M) \arrow[r, "\pi"] \arrow[d, "\tau"'] & S(M) \arrow[dl, "\phi"] \\ & A & \end{tikzcd}$$

Se $x, y \in M$, então $\tau(\theta_M(x)\theta_M(y) - \theta_M(y)\theta_M(x)) = \varphi(x)\varphi(y) - \varphi(y)\varphi(x) = 0$. Logo, o núcleo de τ contém o conjunto dos geradores de K_M, e, logo, contém K_M. Assim, existe um homomorfismo de R-álgebras $\phi : S(M) \to A$ tal que $\tau = \phi \circ \pi$, definido por $t + K_M \mapsto \tau(t), t \in \mathcal{T}(M)$ (ϕ está bem definido pois $K_M \subset Ker(\tau)$).

Temos $\phi \circ \psi_M = \phi \circ \pi \circ \theta_M = \tau \circ \theta_M = \varphi$. Como $\theta_M(M)$ é um conjunto de geradores de $\mathcal{T}(M)$, $\psi_M(M) = \pi(\theta_M(M))$ é um conjunto de geradores de $S(M)$ (pois π é sobrejetiva) e, portanto, não pode existir mais que um homomorfismo ϕ de $S(M)$ em A tal que $\phi \circ \psi_M = \varphi$ (pois $\phi \circ \psi_M = \varphi = \phi' \circ \psi_M \Rightarrow \phi(s) = \phi(\psi_M(m)) = \varphi(m) = \phi'(\psi_M(m)) = \phi'(s), \forall s \in S(M) \Rightarrow \phi = \phi'$).

Portanto, $(S(M), \psi_M)$ é uma álgebra simétrica de M.

Observação II.1.7 1. $S(M)$ é uma álgebra comutativa.

De fato, para quaisquer $x, y \in M$, temos: $\psi_M(x)\psi_M(y) = \pi(\theta_M(x)\theta_M(y)) = \pi(\theta_M(y)\theta_M(x)) = \psi_M(y)\psi_M(x)$ e como $\psi_M(M)$ gera $S(M)$, temos que $S(M)$ é comutativa.

2. $S(M)$ é uma álgebra graduada. De fato, como $S(M) = \mathcal{T}(M)/K_M$ e K_M é gerado por elementos homogêneos de grau 2, então K_M é um ideal homogêneo e como $\mathcal{T}(M)$ é graduado, segue que $S(M)$ é graduado.

3. Se A é uma R-álgebra graduada e $\varphi : M \to A$ é um homomorfismo de R-módulos, então ϕ é um homomorfismo homogêneo, se supusermos que os elementos de $\varphi(M)$ são homogêneos de grau 1 de A.

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[d, "\psi_M"'] & A \\ S(M) \arrow[ur, "\phi"] & \end{tikzcd}$$

De fato, $\phi(x_1 \otimes \cdots \otimes x_n) = \varphi(x_1) \cdots \varphi(x_n)$ é homogêneo de grau n em A. Logo os elementos de $\phi(S^n(M))$ são homogêneos de grau n em A. Portanto, ϕ é homogêneo.

Exemplo II.1.8 Se M é um R-módulo livre finitamente gerado de posto n, então $S(M)$ é o anel polinomial $R[T_1, \ldots, T_n]$.

De fato, temos que $M \cong R^n$ e consideremos $\psi_M : M \to R[T_1, \ldots, T_n]$ um homomorfismo de R-módulos definido por $e_i \mapsto T_i$, onde $\{e_i; 1 \leq i \leq n\}$ é a base canônica de M. Observe que ψ está bem definido, pois M é livre.

Considere qualquer R-álgebra comutativa A e qualquer homomorfismo de R-módulos $\varphi : M \to A$.

$$\begin{array}{ccc} M & \xrightarrow{\varphi} & A \\ {\scriptstyle\psi_M}\big\downarrow & \nearrow{\scriptstyle\phi} & \\ R[T_1, \cdots, T_n] & & \end{array}$$

Definamos $\phi : R[T_1, \ldots, T_n] \to A$ por $f(T_1, \ldots, T_n) \mapsto f(\varphi(e_1), \ldots, \varphi(e_n))$. Temos que $\phi(\psi_M(e_i)) = \phi(T_i) = \varphi(e_i)$, isto é, $\phi \circ \psi_M = \varphi$. Como $\phi(T_i) = \varphi(e_i)$, então ϕ é unicamente determinado por $\phi \circ \psi_M = \varphi$. Logo, $S(M) = R[T_1, \ldots, T_n]$.

Queremos calcular a álgebra simétrica de um módulo qualquer, como fizemos no exemplo anterior. Para isso, as próximas proposições serão fundamentais.

Proposição II.1.9 *Sejam R um anel, M, N dois R-módulos e $u : M \to N$ um homomorfismo de R-módulos. Então, existe um único homomorfismo de R-álgebras $u' : S(M) \to S(N)$ tal que o diagrama abaixo é comutativo.*

$$\begin{array}{ccc} M & \xrightarrow{u} & N \\ {\scriptstyle\psi_M}\big\downarrow & & \big\downarrow{\scriptstyle\psi_N} \\ S(M) & \xrightarrow{u'} & S(N) \end{array}$$

Dem. :

$$\begin{array}{ccc} M & \xrightarrow{\psi_N \circ u} & S(N) \\ {\scriptstyle\psi_M}\big\downarrow & \nearrow{\scriptstyle u'} & \\ S(M) & & \end{array}$$

Como $(S(M), \psi_M)$ é a álgebra simétrica de M e $S(N)$ é uma álgebra comutativa, segue que existe um único homomorfismo de R-álgebras $u' : S(M) \to S(N)$ tal que o diagrama acima é comutativo, donde segue a proposição. $\square$

Observação II.1.10 1. O homomorfismo u' definido na proposição anterior será denotado por $S(u)$.

2. Analogamente, definimos o homomorfismo $\mathcal{T}(u) : \mathcal{T}(M) \to \mathcal{T}(N)$.

Proposição II.1.11 *Se $u : M \to N$ é um homomorfismo sobrejetivo de R-módulos, então $\mathcal{T}(u) : \mathcal{T}(M) \to \mathcal{T}(N)$ é sobrejetivo e seu núcleo é o ideal de $\mathcal{T}(M)$ gerado pelo núcleo $\mathfrak{p}$ de u.*

$$\begin{array}{ccc} M & \xrightarrow{u} & N \\ {\scriptstyle\theta_M}\big\downarrow & & \big\downarrow{\scriptstyle\theta_N} \\ \mathcal{T}(M) & \xrightarrow{\mathcal{T}(u)} & \mathcal{T}(N) \end{array}$$

Dem. :

$$\begin{array}{ccc} M & \xrightarrow{u} & N \\ {\scriptstyle\theta_M}\downarrow & \overset{\theta_N \circ u}{\searrow} & \downarrow{\scriptstyle\theta_N} \\ \mathcal{T}(M) & \xrightarrow{\mathcal{T}(u)} & \mathcal{T}(N) \end{array}$$

Temos $\mathcal{T}^n(u) : \mathcal{T}^n(M) \to \mathcal{T}^n(N)$, onde $\mathcal{T}^n(u) = \underbrace{u \otimes \cdots \otimes u}_{n\,\text{vezes}}$ é sobrejetivo e $\mathcal{T}^0(u) : \mathcal{T}^0(M) \to \mathcal{T}^0(N)$ é bijetivo. Além disso, o núcleo τ_n de $\mathcal{T}^n(u)$ é o submódulo de $\mathcal{T}^n(M)$ gerado pelos produtos $x_1 \otimes \cdots \otimes x_n$, onde pelo menos um dos x_i pertence a $\mathfrak{p}$. Isso mostra que o núcleo $\tau = \oplus_{n\geq 1}\tau_n$ de $\mathcal{T}(u)$ é o ideal gerado por $\mathfrak{p}$ em $\mathcal{T}(M)$. □

Proposição II.1.12 *Se $u : M \to N$ é um homomorfismo de R-módulos sobrejetivo, então $S(u) : S(M) \to S(N)$ é sobrejetivo e seu núcleo é o ideal de $S(M)$ gerado pelo núcleo $\mathfrak{p}$ de u.*

Dem. : Ponhamos $v = \mathcal{T}(u) : \mathcal{T}(M) \to \mathcal{T}(N)$, que é sobrejetiva. Temos que $v(K_M) = K_N$. De fato,

- $v(\theta_M(x)\theta_M(y) - \theta_M(y)\theta_M(x)) = \theta_N(u(x))\theta_N(u(y)) - \theta_N(u(y))\theta_N(u(x)) \Rightarrow v(K_M) \subset K_N$
- $\theta_N(x')\theta_N(y') - \theta_N(y')\theta_N(x') = \theta_N(u(x))\theta_N(u(y)) - \theta_N(u(y))\theta_N(u(x)) = v(\theta_M(x))v(\theta_M(y)) - v(\theta_M(y))v(\theta_M(x)) = v(\theta_M(x)\theta_M(y) - \theta_M(y)\theta_M(x)) \Rightarrow K_N \subset v(K_M)$.

Se $I = Ker(v)$, temos que $v^{-1}(K_N) = I + K_M$. Como $S(u) : T(M)/K_M \to T(N)/K_N$, deduz-se de v por passagem ao quociente que $S(u)$ é um homomorfismo sobrejetivo cujo núcleo é $I' = (I + K_M)/K_M$. Como I é gerado pelo núcleo $\mathfrak{p}$ de u, o mesmo vale para I'. □

Proposição II.1.13 *Se $M = \langle m_1, \ldots, m_n \rangle$, então*

$$S(M) \cong R[X_1, \ldots, X_n]/\mathfrak{q} = R[X_1, \ldots, X_n]/(\sum_{i=1}^{n} a_{ij}X_i),$$

onde $A = (a_{ij})_{n\times m}$ è a matriz de relação de M e $\mathfrak{q} = (\sum_{i=1}^n c_i X_i; \sum_{i=1}^n c_i m_i = 0)$.

Dem. : Seja $M = \langle m_1, \cdots, m_n \rangle$, com R Noetheriano. Temos uma apresentação finita de M:

$$\begin{array}{ccccccc} R^m & \xrightarrow{\psi} & R^n & \xrightarrow{\varphi} & M & \longrightarrow & 0 \\ & & e_i & \mapsto & m_i & & \end{array}$$

onde $A = (a_{ij})_{n\times m}$ é a matriz de relação de M, $\{f_j; 1 \leq j \leq m\}$ e $\{e_i; 1 \leq i \leq n\}$ são as bases canônicas de R^m e R^n, respectivamente. Pelas proposições vistas acima, temos o diagrama abaixo com as linhas exatas:

$$\begin{array}{ccccccc} R^m & \xrightarrow{\psi} & R^n & \xrightarrow{\varphi} & M & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \\ & & R[X_1, \cdots, X_n] & \longrightarrow & S(M) & \longrightarrow & 0 \end{array}$$

Logo, $S(M) \cong R[X_1, \ldots, X_n]/J$, onde J é o ideal de $R[X_1, \ldots, X_n]$ gerado por $\sum_{i=1}^n c_i X_i$ tais que $\sum_{i=1}^n c_i m_i = 0$. Logo,

$$\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \in Ker(\varphi) = Im(\psi) \Rightarrow \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = A. \begin{pmatrix} d_1 \\ \vdots \\ d_n \end{pmatrix} \Rightarrow c_i = \sum_{j=1}^m a_{ij} d_j \Rightarrow \sum_{i=1}^n c_i X_i = \sum_{i=1}^n (\sum_{j=1}^m a_{ij} d_j) X_i$$

$= \sum_{j=1}^m (\sum_{i=1}^n a_{ij} X_i) d_j \Rightarrow J \subset$ (ideal gerado pelas colunas de A) $= (\sum_{i=1}^n a_{ij} X_i)$

Por outro lado, $A.f_j = \sum_{i=1}^n a_{ij} e_i$ é uma coluna de A e $A.f_j \in Im(\psi) = Ker(\varphi)$; logo, $\sum_{i=1}^n a_{ij} m_i = \varphi(A.f_j) = 0$ e, portanto, $\sum_{i=1}^n a_{ij} X_i \in J$.

Assim, $J = (\sum_{i=1}^n a_{ij} X_i)$. □

Como aqui estamos sempre considerando os anéis Noetherianos, essa é a descrição da álgebra simétrica de um módulo que usaremos daqui para a frente. A partir disso, podemos tirar duas propriedades importantes da álgebra simétrica: Dados M um R-módulo, $\mathfrak{p}$ um ideal de R e S' um subconjunto fechado multiplicativamente de R, temos:

- $S_R(M) \otimes R/\mathfrak{p} \cong S_{R/\mathfrak{p}}(M/\mathfrak{p}M)$

  A partir da apresentação finita de M, podemos concluir, usando as propriedades do produto tensorial, que:

  $$R^m \xrightarrow{\psi} R^n \xrightarrow{\varphi} M \to 0 \qquad \Rightarrow \qquad R^m \otimes R/\mathfrak{p} \xrightarrow{\overline{\psi}} R^n \otimes R/\mathfrak{p} \xrightarrow{\overline{\varphi}} M \otimes R/\mathfrak{p} \to 0$$

  onde $\overline{\psi} = \psi \otimes 1$, $\overline{\varphi} = \varphi \otimes 1$, $A = (a_{ij})_{n\times m}$ é a matriz de relação de M e $\overline{A}$ é a matriz de relação de $M \otimes R/\mathfrak{p} \cong M/\mathfrak{p}M$. Então, considerando $\{f_j; 1 \leq j \leq m\}$ e $\{e_i; 1 \leq i \leq n\}$ as bases canônicas de R^m e R^n, respectivamente, temos:

  $$\overline{\psi}(f_j \otimes 1) = (\sum_{i=1}^n a_{ij} e_i) \otimes 1 = \sum_{i=1}^n a_{ij}(e_i \otimes 1) = \sum_{i=1}^n a_{ij} \overline{e_i} = \sum_{i=1}^n \overline{a_{ij} e_i}$$

  Logo, $\overline{A} = (\overline{a_{ij}})_{n\times m}$ e pelo exemplo II.1.13:

  $$S_{R/\mathfrak{p}}(M/\mathfrak{p}M) = \frac{R/\mathfrak{p}[X_1, \ldots, X_n]}{(\sum_{i=1}^n \overline{a_{ij}} X_i)} = \frac{R[X_1, \ldots, X_n]}{(\sum_{i=1}^n a_{ij} X_i)} \otimes R/\mathfrak{p} = S_R(M) \otimes R/\mathfrak{p}.$$

- $S_R(M) \otimes R_{S'} \cong S_{R_{S'}}(M_{S'})$

  De novo, pela apresentação finita de M e propriedades do produto tensorial e da localização, temos:

  $$R^m \xrightarrow{\psi} R^n \xrightarrow{\varphi} M \to 0 \qquad \Rightarrow \qquad R^m \otimes R_{S'} \xrightarrow{\overline{\psi}} R^n \otimes R_{S'} \xrightarrow{\overline{\varphi}} M \otimes R_{S'} \to 0$$

  onde $\overline{\psi} = \psi \otimes 1$, $\overline{\varphi} = \varphi \otimes 1$, $A = (a_{ij})_{n\times m}$ é a matriz de relação de M e $\overline{A}$ é a matriz de relação de $M \otimes R_{S'} \cong M_{S'}$. Então, considerando as mesmas bases canônicas do caso anterior, temos:

  $$\overline{\psi}(f_j \otimes 1) = (\sum_{i=1}^n a_{ij} e_i) \otimes 1 = \sum_{i=1}^n a_{ij}(e_i \otimes 1) = \sum_{i=1}^n \frac{a_{ij}}{1} \overline{e_i}$$

Logo, $\overline{A} = (\frac{a_{ij}}{1})_{n\times m}$ e

$$S_{R_{S'}}(M_{S'}) = \frac{R_{S'}[X_1,\ldots,X_n]}{(\sum_{i=1}^n \frac{a_{ij}}{1}X_i)} = \frac{R[X_1,\ldots,X_n]_{S'}}{(\sum_{i=1}^n a_{ij}X_i)_{S'}} = \frac{R[X_1,\ldots,X_n]}{(\sum_{i=1}^n a_{ij}X_i)} \otimes R_{S'} = S_R(M)\otimes R_{S'}$$

II.2 A Álgebra de Rees de um Ideal

Definição II.2.1 *Dados um anel R e um ideal $\mathfrak{a}$ de R, chamamos a* **álgebra de Rees** *de $\mathfrak{a}$ ao conjunto $\mathcal{R}_R(\mathfrak{a}) = \{c_0 + c_1T + \cdots + c_nT^n \in R[T]; c_i \in \mathfrak{a}^i, \forall i \geq 0\}$, onde $\mathfrak{a}^0 = R$ e $\mathfrak{a}^1 = \mathfrak{a}$.*

Quando está claro qual é o anel R, denotamos a álgebra de Rees simplesmente por $\mathcal{R}(\mathfrak{a})$. $\mathcal{R}(\mathfrak{a})$ é de fato uma R-álgebra:

- $b, c \in \mathcal{R}(\mathfrak{a}) \Rightarrow b + c \in \mathcal{R}(\mathfrak{a})$.
  De fato, $b = b_0 + b_1T + \cdots + b_nT^n, c = c_0 + c_1T + \cdots + c_mT^m$, com $b_i, c_i \in \mathfrak{a}^i$. Assim, $b + c = (b_0 + c_0) + (b_1 + c_1)T + \cdots + (b_s + c_s)T^s$, onde $s = max\{n, m\}$ e $b_i = 0, \forall i > n, c_i = 0, \forall i > m$. Como $b_i, c_i \in \mathfrak{a}^i$, temos $b_i + c_i \in \mathfrak{a}^i$. Logo, $b + c \in \mathcal{R}(\mathfrak{a})$.

- $1 \in \mathcal{R}(\mathfrak{a})$, pois $1 \in R = \mathfrak{a}^0$.

- $b, c \in \mathcal{R}(\mathfrak{a}) \Rightarrow b.c \in \mathcal{R}(\mathfrak{a})$.
  De fato, $b = b_0 + b_1T + \cdots + b_nT^n, c = c_0 + c_1T + \cdots + c_mT^m$, com $b_i, c_i \in \mathfrak{a}^i$. Logo, $b.c = a_0 + a_1T + \cdots + a_{n+m}T^{n+m}$, onde $a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0$. Como $b_i, c_i \in \mathfrak{a}^i$, então $b_ic_{k-i} \in \mathfrak{a}^i$ e, logo, $a_k \in \mathfrak{a}^k$ e $b.c \in \mathcal{R}(\mathfrak{a})$.

- $b = b_0 + b_1T + \cdots + b_nT^n \in \mathcal{R}(\mathfrak{a}),\ r \in R \Rightarrow r.b \in \mathcal{R}(\mathfrak{a})$:
  Como $r.b = rb_0 + rb_1T + \cdots + rb_nT^n$ e $rb_i \in \mathfrak{a}^i$, então $r.b \in \mathcal{R}(\mathfrak{a})$.

Como, pela definição, $\mathcal{R}(\mathfrak{a}) = R \oplus \mathfrak{a}T \oplus \mathfrak{a}^2T^2 \oplus \cdots$, segue imediatamente que ela é uma álgebra graduada.

Se $\mathfrak{a} = (a_1, \ldots, a_n)$, então $\mathcal{R}(\mathfrak{a}) = R[a_1T, \ldots, a_nT]$. Como estamos supondo R Noetheriano, então teremos $\mathcal{R}(\mathfrak{a})$ também Noetheriano, para cada ideal $\mathfrak{a}$ de R. Nesse caso, podemos definir o epimorfismo homogêneo

$$\begin{array}{rcl} R[X_1, \ldots, X_n] & \to & \mathcal{R}(\mathfrak{a}) \\ X_i & \mapsto & a_iT \end{array}$$

Denotamos o núcleo desse epimorfismo por $\mathfrak{q}_\infty$ e sabemos que $\mathfrak{q}_\infty$ é um ideal homogêneo. Seja f um polinômio homogêneo de $R[X_1, \ldots, X_n]$, isto é, $f = \sum_{v_1+\cdots+v_n=d} \rho_{v_1,\cdots,v_n} X_1^{v_1} \cdots X_n^{v_n}$. Logo, $f(a_1T, \ldots, a_nT) = (\sum_{v_1+\cdots+v_n=d} \rho_{v_1,\cdots,v_n} a_1^{v_1} \cdots a_n^{v_n})T^d = f(a_1, \ldots, a_n)T^d$ e segue que $f \in \mathfrak{q}_\infty \Leftrightarrow f(a_1, \ldots, a_n) = 0$.

Definição II.2.2 *Dado um ideal $\mathfrak{a}$ de um anel R, chamamos $\mathcal{R}(\mathfrak{a})[T^{-1}]$ de* **anel de Rees generalizado** *de $\mathfrak{a}$.*

Temos que $\mathcal{R}(\mathfrak{a})[T^{-1}]$ é um subanel de $R[T,T^{-1}]$. Afirmamos que:

$$\mathcal{R}(\mathfrak{a})[T^{-1}] = \{b_{-r}T^{-r} + \cdots + b_{-1}T^{-1} + b_0 + b_1T + \cdots + b_sT^s; s, r \in \mathbb{N}, b_j \in \mathfrak{a}^j, b_{-j} \in R\}.$$

Com efeito, vamos chamar tal conjunto de B. É óbvio que $\mathcal{R}(\mathfrak{a}) \subset B$ e que $T^{-1} \in B$. Logo, $\mathcal{R}(\mathfrak{a})[T^{-1}] \subset B$. Por outro lado, dado $b = b_{-r}T^{-r} + \cdots + b_{-1}T^{-1} + b_0 + b_1T + \cdots + b_sT^s$, com $b_j \in \mathfrak{a}^j, b_{-j} \in R$, temos $b_0 + b_1T + \cdots + b_sT^s \in \mathcal{R}(\mathfrak{a})$ e $b_{-j} \in R \subset \mathcal{R}(\mathfrak{a})$. Assim, $b \in \mathcal{R}(\mathfrak{a})[T^{-1}]$.

II.3 Dimensões da Álgebra Simétrica e da Álgebra de Rees

Proposição II.3.1 *Seja $\phi : A \to B$ um homomorfismo de anéis Noetherianos. Sejam $\mathfrak{p} \in Spec(B)$ e $\mathfrak{q} = \phi^{-1}(\mathfrak{p})$ (que denotaremos por $\mathfrak{p} \cap A$). Então*

$$ht(\mathfrak{p}) \leq ht(\mathfrak{q}) + ht(\mathfrak{p}/\mathfrak{q}B).$$

Dem. : Substituindo A por $A_\mathfrak{q}$ e B por $B_\mathfrak{p}$, podemos supor que $(A, \mathfrak{q})$ e $(B, \mathfrak{p})$ são anéis locais tais que $\mathfrak{p} \cap A = \mathfrak{q}$. De fato, supondo que $ht(\mathfrak{p}B_\mathfrak{p}) \leq ht(\mathfrak{q}A_\mathfrak{q}) + ht(\mathfrak{p}B_\mathfrak{p}/\mathfrak{q}B_\mathfrak{p})$, como $ht(\mathfrak{p}) = ht(\mathfrak{p}B_\mathfrak{p}), ht(\mathfrak{q}) = ht(\mathfrak{q}A_\mathfrak{q})$ e $ht(\mathfrak{p}B_\mathfrak{p}/\mathfrak{q}B_\mathfrak{p}) = ht((\mathfrak{p}/\mathfrak{q}B)_\mathfrak{p}) = ht(\mathfrak{p}/\mathfrak{q}B)$, então, substituindo na desigualdade anterior, teremos $ht(\mathfrak{p}) \leq ht(\mathfrak{q}) + ht(\mathfrak{p}/\mathfrak{q}B)$. A partir dessa redução, devemos mostrar que $dim(B) \leq dim(A) + dim(B/\mathfrak{q}B)$.

Seja $a_1, \ldots, a_r$ um sistema de parâmetros de A e ponhamos $I = (a_1, \ldots, a_r)$. Como $\sqrt{I} = \mathfrak{q}$ e $\mathfrak{q}$ é finitamente gerado, então $\mathfrak{q}^n \subset I$, para algum $n > 0$. Logo, $\mathfrak{q}^nB \subset IB \subset \mathfrak{q}B$. Assim, os ideais $\mathfrak{q}B$ e IB têm o mesmo radical. Segue da definição que $dim(B/\mathfrak{q}B) = dim(B/IB)$. Se $dim(B/IB) = s$ e se $\{\overline{b_1}, \ldots, \overline{b_s}\}$ é um sistema de parâmetros de B/IB, então $b_1, \ldots, b_s, a_1, \ldots, a_r$ é um sistema de parâmetros de B. Assim, $dim(B) \leq r + s$. □

Lema II.3.2 *Sejam A um subdomínio Noetheriano e B um domínio finitamente gerado sobre A. Sejam $\mathfrak{p} \in Spec(B)$ e $\mathfrak{q} = \mathfrak{p} \cap A$. Então,*

$$ht(\mathfrak{p}) \leq ht(\mathfrak{q}) + gr.tr._A B - gr.tr._{K(\mathfrak{q})} K(\mathfrak{p})$$

onde $gr.tr._A B$ é o grau de transcendência do corpo de frações de B sobre o corpo de frações de A, $K(\mathfrak{p}) = c.fr.(B/\mathfrak{p})$ e $K(\mathfrak{q}) = c.fr.(A/\mathfrak{q}) = A_\mathfrak{q}/\mathfrak{q}A_\mathfrak{q}$.

Dem. : Seja $B = A[x_1, \ldots, x_n]$.

Por indução em n, é suficiente considerar o caso $n = 1$. Com efeito, suponhamos que o lema esteja mostrado para $B' = A[x_1, \ldots, x_{n-1}]$. Sendo $B = A[x_1, \ldots, x_n] = A[x_1, \ldots, x_{n-1}][x_n] = B'[x_n]$, temos que B é finitamente gerado sobre B' e, pelo Teorema da Base de Hilbert, B' é um domínio Noetheriano. Aplicando o caso $n = 1$, concluímos que, para $\mathfrak{q}' = \mathfrak{p} \cap B'$, vale:

$$ht(\mathfrak{p}) \leq ht(\mathfrak{q}') + gr.tr._{B'} B - gr.tr._{K(\mathfrak{q}')} K(\mathfrak{p}).$$

Como $\mathfrak{q} = \mathfrak{p} \cap A = \mathfrak{q}' \cap A$, aplicando a hipótese de indução, vale:

$$ht(\mathfrak{q}') \leq ht(\mathfrak{q}) + gr.tr._A B' - gr.tr._{K(\mathfrak{q})} K(\mathfrak{q}').$$

Como $gr.tr._A B = gr.t._{B'}B + gr.tr._A B'$ e $gr.tr._{K(\mathfrak{q})}K(\mathfrak{p}) = gr.tr._{K(\mathfrak{q}')}K(\mathfrak{p}) + gr.tr._{K(\mathfrak{q})}K(\mathfrak{q}')$, então

$$ht(\mathfrak{p}) \leq ht(\mathfrak{q}) + gr.tr._A B - gr.tr._{K(\mathfrak{q})}K(\mathfrak{p}).$$

Então, seja $B = A[x]$.

Substituindo A por $A_\mathfrak{q}$ e B por $B_\mathfrak{q} = A_\mathfrak{q}[x]$, podemos supor que $(A, \mathfrak{q})$ é um anel local. De fato, suponhamos que a desigualdade foi mostrada para os anéis locais, ou seja,

$$ht(\mathfrak{p}B_\mathfrak{q}) \leq ht(\mathfrak{q}A_\mathfrak{q}) + gr.tr._{A_\mathfrak{q}}B_\mathfrak{q} - gr.tr._{K(\mathfrak{q}A_\mathfrak{q})}K(\mathfrak{p}B_\mathfrak{q}).$$

Como $ht(\mathfrak{p}) = ht(\mathfrak{p}B_\mathfrak{q})$, $ht(\mathfrak{q}) = ht(\mathfrak{q}A_\mathfrak{q})$, $gr.tr._{A_\mathfrak{q}}B_\mathfrak{q} = gr.tr._A B$, $K(\mathfrak{q}A_\mathfrak{q}) = c.fr.(A_\mathfrak{q}/\mathfrak{q}A_\mathfrak{q}) = k(\mathfrak{q})$, $K(\mathfrak{p}B_\mathfrak{q}) = c.fr.(B_\mathfrak{q}/\mathfrak{p}B_\mathfrak{q}) = c.fr.(B/\mathfrak{p}) = K(\mathfrak{p})$, segue, substituindo na desigualdade acima, que

$$ht(\mathfrak{p}) \leq ht(\mathfrak{q}) + gr.tr._A B - gr.tr._{K(\mathfrak{q})}K(\mathfrak{p}).$$

Sejam $k = K(\mathfrak{q}) = A/\mathfrak{q}$ e $I = \{f(X) \in A[X]; f(X) = 0\}$. Assim, $B = A[X]/I$.

Caso 1: $I = (0)$

Então $B = A[X], gr.tr._A B = 1$ e $B/\mathfrak{q}B = A[X]/\mathfrak{q}A[X] = (A/\mathfrak{q})[X] = k[X]$ (e logo $\mathfrak{q}B$ é primo). Portanto, $ht(\mathfrak{p}/\mathfrak{q}B) \leq dim(B/\mathfrak{q}B) = 1$, isto é,

$$ht(\mathfrak{p}/\mathfrak{q}B) = \begin{cases} 1, & \text{se } \mathfrak{p} \supsetneqq \mathfrak{q}B \\ 0, & \text{se } \mathfrak{p} = \mathfrak{q}B \end{cases}$$

No primeiro caso, $gr.tr._k K(\mathfrak{p}) = 0$. De fato, se $\mathfrak{q}B \subsetneqq \mathfrak{p}$, então $(0) \subsetneqq \overline{\mathfrak{p}} = \mathfrak{p}/\mathfrak{q}B \subsetneqq B/\mathfrak{q}B \cong k[X]$. Como k é corpo, $k[X]$ é um domínio de ideais principais e portanto $\overline{\mathfrak{p}} = (\overline{f(X)})$. Assim, $k[X]/\overline{\mathfrak{p}} \cong k[x]$, onde x é uma raiz de $\overline{f}$, ou seja, $k[X]/\overline{\mathfrak{p}}$ é algébrico sobre k. Por outro lado,

$$k[X]/\overline{\mathfrak{p}} = \frac{B/\mathfrak{q}B}{\mathfrak{p}/\mathfrak{q}B} = B/\mathfrak{p}.$$

Logo, $gr.tr._k K(\mathfrak{p}) = gr.tr._k(c.fr.(B/\mathfrak{p})) = gr.tr._k(c.fr.(k[X]/\overline{\mathfrak{p}})) = 0$.

No caso em que $\mathfrak{p} = \mathfrak{q}B$, temos que $gr.tr._k K(\mathfrak{p}) = 1$. De fato, como $B/\mathfrak{q}B = k[X]$, segue que $1 = dim_k(B/\mathfrak{q}B) = gr.tr._k(c.fr.(B/\mathfrak{q}B)) = gr.tr._k(c.fr.(B/\mathfrak{p})) = gr.tr._k K(\mathfrak{p})$.

Logo, $ht(\mathfrak{p}/\mathfrak{q}B) = 1 - gr.tr._k K(\mathfrak{p})$. Por outro lado, por II.3.1, $ht(\mathfrak{p}) \leq ht(\mathfrak{q}) + ht(\mathfrak{p}/\mathfrak{q}B)$. Logo, vale a desigualdade $ht(\mathfrak{p}) \leq ht(\mathfrak{q}) + 1 - gr.tr._k K(\mathfrak{p})$.

Caso 2: $I \neq (0)$

Então $gr.tr._A B = 0$, pois, pela hipótese, existe $f \in A[X] - \{0\}$ tal que $f(x) = 0$, isto é, x é algébrico sobre A. Seja $\mathfrak{p}^*$ a imagem inversa de $\mathfrak{p}$ em $A[X]$ pela projeção canônica $A[X] \xrightarrow{\pi} A[X]/I$. Logo, $\mathfrak{p} = \mathfrak{p}^*/I$ e $K(\mathfrak{p}) = c.fr.(B/\mathfrak{p}) = c.fr.(\frac{A[X]/I}{\mathfrak{p}^*/I}) = c.fr.(A[X]/\mathfrak{p}^*) = K(\mathfrak{p}^*)$. Temos que $A \cap I = (0)$ (pois $i \in A \cap I \Rightarrow i = \pi(i) = 0$), logo π é injetora em A (pois $\pi(a) = \pi(a') \Rightarrow a - a' \in I \cap A \Rightarrow a = a'$). Portanto, se $K = c.fr.(A)$, então

$ht(I) = ht(IK[X]) \leq dim(K[X]) = 1$. Como $I \neq (0)$ e I é primo, temos $ht(I) = 1$. Assim, pela Proposição II.3.1, $ht(\mathfrak{p}) \leq ht(\mathfrak{p}^*) - ht(I) = ht(\mathfrak{p}^*) - 1$. Por outro lado, como $\mathfrak{p}^* \cap A = \mathfrak{q}$,[1] temos pelo Caso 1 que $ht(\mathfrak{p}^*) \leq ht(\mathfrak{q}) + 1 - gr.tr._k K(\mathfrak{p}^*)$ e como já mostramos que $K(\mathfrak{p}^*) = K(\mathfrak{p})$, segue a afirmação. □

Lema II.3.3 *Seja B um domínio Noetheriano que é finitamente gerado sobre um subanel A. Suponhamos que exista um ideal primo $\mathfrak{q}$ de B tal que $B = A + \mathfrak{q}$ e $A \cap \mathfrak{q} = 0$. Então:*

$$dim(B) = dim(A) + ht(\mathfrak{q}) = dim(A) + gr.tr._A B$$

Dem. : Podemos supor que $dim(A)$ é finita.

- Primeiramente, vamos supor que $A = k$, onde k é corpo e vamos mostrar que $ht(\mathfrak{q}) = gr.tr._k B$.

  Como $B = k[x_1, \ldots, x_n]$, pelo Teorema da Normalização de Noether, existem $Y_1', \ldots, Y_m' \in B$ algebricamente independentes sobre k tais que a extensão $B \mid k[Y_1', \ldots, Y_m']$ é inteira. Como $B = k \oplus \mathfrak{q}$, então $Y_i' = Y_i + a_i$, com $Y_i \in \mathfrak{q}$ e $a_i \in k$. Logo, $Y_1, \ldots, Y_m$ são algebricamente independentes sobre k, $k[Y_1', \ldots, Y_m'] = k[Y_1, \ldots, Y_m]$ e $(Y_1, \ldots, Y_m) \subset \mathfrak{q}$. Portanto, $(Y_1, \ldots, Y_m) \subset \mathfrak{q} \cap k[Y_1, \ldots, Y_m]$ e como $(Y_1, \ldots, Y_m)$ é ideal maximal de $k[Y_1, \ldots, Y_m]$, segue que $(Y_1, \ldots, Y_m) = \mathfrak{q} \cap k[Y_1, \ldots, Y_m]$. Como $ht(Y_1, \ldots, Y_m) = m$ e $k[Y_1, \ldots, Y_m]$ é normal (pois é fatorial), pelo Teorema do "Going-Down", temos que $ht(\mathfrak{q}) \geq m$. Por outro lado, $ht(\mathfrak{q}) \leq dim(B) = gr.tr._k B = m$. Logo, $ht(\mathfrak{q}) = m = gr.tr._k B$.

- Agora, vamos supor que A é qualquer subanel e vamos mostrar que $ht(\mathfrak{q}) = gr.tr._A B$.

  Como $B = A \oplus \mathfrak{q}$, localizando em $S = A - \{0\}$, teremos $B_S = A_S \oplus \mathfrak{q}_S = k \oplus \mathfrak{q} B_S$, onde k é o corpo de frações de A. Como $\mathfrak{q} \cap S = \emptyset$, então $ht(\mathfrak{q}) = ht(\mathfrak{q}_S) = gr.tr._k B_S = gr.tr._A B$.

- Finalmente, vamos mostrar o lema.

  Por hipótese, $B = A \oplus \mathfrak{q}$, logo $B/\mathfrak{q} \cong A$ e portanto $dim(A) = dim(B/\mathfrak{q}) \leq dim(B) - ht(\mathfrak{q})$, ou seja, $dim(B) \geq dim(A) + ht(\mathfrak{q})$.

  Por outro lado, consideremos $\mathfrak{q}' \in Spec(B)$ tal que $ht(\mathfrak{q}') = dim(B)$ (cuja existência é garantida pelo fato de B ser Noetheriano). De acordo com o Lema II.3.2, temos

  $dim(B) = ht(\mathfrak{q}') \leq ht(\mathfrak{q}' \cap A) + gr.tr._A B - gr.tr._{K(\mathfrak{q}' \cap A)} K(\mathfrak{q}') \leq dim(A) + gr.tr._A B = dim(A) + ht(\mathfrak{q})$.

  Portanto, $dim(B) = dim(A) + ht(\mathfrak{q})$. □

Teorema II.3.4 *Se R é um domínio Noetheriano e I é um ideal não-nulo de R, então*

$$dim(\mathcal{R}(I)) = dim(R) + 1.$$

[1]Como $\mathfrak{q}$ é o ideal maximal de A, temos que $\mathfrak{p}^* \cap A \subset \mathfrak{q}$. Por outro lado, se $y \in \mathfrak{q} = \mathfrak{p} \cap A$, como π é injetora em A, então $\pi^{-1}(y) = y \in \mathfrak{p}^* \cap A$, ou seja, $\mathfrak{q} \subset \mathfrak{p}^* \cap A$.

Dem. : Sabemos que $\mathcal{R}(I) = R \oplus IT \oplus I^2T^2 \oplus \cdots$ e tomemos $\mathfrak{q} = IT \oplus I^2T^2 \oplus \cdots$, ou seja, $\mathcal{R}(I) = \mathfrak{q} \oplus R$. Logo, $\mathcal{R}(I)/\mathfrak{q} \cong R$ e como estamos supondo R domínio, segue que $\mathfrak{q}$ é primo. Pelo Lema II.3.3,

$$dim(\mathcal{R}(I)) = dim(R) + ht(\mathfrak{q}) = dim(R) + gr.tr._R\mathcal{R}(I).$$

Como $R \subset \mathcal{R}(I) \subset R[T]$ e $T \in c.fr.(\mathcal{R}(I))$, segue que $c.fr.(\mathcal{R}(I)) = c.fr.(R[T]) = K(T)$, onde $K = c.fr.(R)$. Logo, $gr.tr._R(\mathcal{R}(I)) = 1$ e portanto $dim(\mathcal{R}(I)) = dim(R) + 1$. □

Observação II.3.5 Vamos considerar B um domínio Noetheriano $\mathbb{N}$-graduado e A sua componente de grau 0. Nesse caso, $B = A \oplus \mathfrak{p}$, onde $\mathfrak{p} = \{\sum_{i=0}^{\infty} x_i; x_0 = 0\}$ é ideal primo de B e pela Proposição I.3.5, B é finitamente gerado sobre A. Pelo Lema II.3.3, para $\mathfrak{p} \in Spec(B)$ e $\mathfrak{q} = \mathfrak{p} \cap A$, temos

$$\begin{aligned} dim(B/\mathfrak{p}) &= dim(A/\mathfrak{q}) + gr.tr._{A/\mathfrak{q}}B/\mathfrak{p} \\ dim(B_\mathfrak{q}) &= dim(A_\mathfrak{q}) + gr.tr._{A_\mathfrak{q}}B_\mathfrak{q}. \end{aligned}$$

Como $c.fr.(B/\mathfrak{p}) = K(\mathfrak{p})$, $c.fr.(A/\mathfrak{q}) = K(\mathfrak{q})$, $c.fr.(B_\mathfrak{q}) = c.fr.(B)$ e $c.fr.(A_\mathfrak{q}) = c.fr.(A)$, temos:

$$dim(B/\mathfrak{p}) = dim(A/\mathfrak{q}) + gr.tr._{K(\mathfrak{q})}K(\mathfrak{p}) \tag{II.3}$$

$$dim(B_\mathfrak{q}) = dim(A_\mathfrak{q}) + gr.tr._A B \tag{II.4}$$

Estamos interessados em calcular a dimensão da álgebra simétrica $S_R(M)$, onde M é um módulo finitamente gerado sobre um anel Noetheriano R. Observamos primeiramente que, se R é um domínio, então o R-submódulo de torção T da álgebra simétrica $S(M)$ é um ideal primo de $S(M)$. Com efeito, por definição $T = \{x \in S(M); \exists r \in \dot{R} \text{ com } rx = 0\}$. Sendo $K = c.fr.(R) = R_{S'}$, onde $S' = R - \{0\}$, temos que $(S_R(M))_{S'} = S_R(M) \otimes R_{S'} = S_{R_{S'}}(M \otimes R_{S'}) = S_{R_{S'}}(M_{S'})$, onde $M_{S'} = M \otimes R_{S'} = M \otimes K$ é um espaço vetorial de dimensão finita n sobre K. Logo, $M_{S'}$ é um módulo livre de posto n. Portanto, $S_{R_{S'}}(M_{S'}) = K[T_1, \ldots, T_n]$, que é domínio. Temos uma aplicação canônica

$$\begin{aligned} S(M) &\xrightarrow{\varphi} (S(M))_{S'} \\ x &\mapsto x/1 \end{aligned}$$

e $Ker(\varphi) = \{x \in S(M); x/1 = 0/1\} = \{x \in S(M); \exists s \in R - \{0\} \text{ com } sx = 0\} = T$. Portanto, temos uma imersão canônica $S(M)/T \hookrightarrow (S(M))_{S'}$, ou seja, podemos considerar $S(M)/T$ um subanel de $(S(M))_{S'}$, que é domínio. Logo, $S(M)/T$ é domínio, ou seja, T é ideal primo de $S(M)$.

Seja $\mathfrak{p}$ um ideal primo de R. Denote por $\overline{T(\mathfrak{p})}$ o $R/\mathfrak{p}$-submódulo de torção de $S(M) \otimes R/\mathfrak{p} = S_{R/\mathfrak{p}}(M/\mathfrak{p}M)$. Como $R/\mathfrak{p}$ é domínio, $\overline{T(\mathfrak{p})}$ é ideal primo de $S_{R/\mathfrak{p}}(M/\mathfrak{p}M)$. O submódulo de torção de $S(M)$ é simplesmente $\overline{T(0)}$. Sabemos que existe uma projeção canônica

$$S_R(M) \to S_{R/\mathfrak{p}}(M/\mathfrak{p}M) \cong \frac{S_R(M)}{\mathfrak{p}S_R(M)},$$

logo $\overline{T(\mathfrak{p})} = T(\mathfrak{p})/\mathfrak{p}S_R(M)$, onde $T(\mathfrak{p}) = \{x \in S(M); \exists r \notin \mathfrak{p} \text{ com } rx \in \mathfrak{p}S(M)\}$. Assim, $T(\mathfrak{p})$ é ideal primo de $S(M)$.

Teorema II.3.6 *Sejam R um anel Noetheriano e M um R-módulo. Então*

$$dim(S(M)) = b(M)$$

onde $b(M) := sup_{\mathfrak{p}\in Spec(R)}\{dim(R/\mathfrak{p}) + \mu(M_\mathfrak{p})\}$ é a cota de Forster-Swan.

Dem. : Seja $\mathfrak{p}$ um ideal primo de R. Vamos mostrar primeiro que $gr.tr._{R/\mathfrak{p}}S(M)/T(\mathfrak{p}) = \mu(M_\mathfrak{p})$. Temos que

$$\begin{aligned}
\frac{S(M)}{T(\mathfrak{p})} \otimes R_\mathfrak{p} &= \left(\frac{S(M)}{T(\mathfrak{p})}\right)_\mathfrak{p} = \frac{S(M)_\mathfrak{p}}{T(\mathfrak{p})_\mathfrak{p}} = \frac{S(M)_\mathfrak{p}}{\mathfrak{p}S(M)_\mathfrak{p}} = S(M) \otimes \frac{R_\mathfrak{p}}{\mathfrak{p}R_\mathfrak{p}} = S(M) \otimes R_\mathfrak{p} \otimes K(\mathfrak{p}) \\
&= S(M_\mathfrak{p}) \otimes K(\mathfrak{p}) = S_{K(\mathfrak{p})}(M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}) = K(\mathfrak{p})[T_1, \ldots, T_n]
\end{aligned}$$

pois $M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}$ é um $K(\mathfrak{p})$-espaço vetorial, logo é um módulo finitamente gerado e então $n = dim_{K(\mathfrak{p})}(M_\mathfrak{p}/\mathfrak{p}M_\mathfrak{p}) = \mu(M_\mathfrak{p})$.

Agora, $c.fr.((S(M)/T(\mathfrak{p}))\otimes R_\mathfrak{p}) = c.fr.((S(M)/T(\mathfrak{p}))_\mathfrak{p}) = c.fr.(S(M)/T(\mathfrak{p}))$, pois $S(M)/T(\mathfrak{p})$ é domínio e $\mathfrak{p} \subset T(\mathfrak{p})$. Assim,

$$\mu(M_\mathfrak{p}) = n = gr.tr._{K(\mathfrak{p})}K(\mathfrak{p})[T_1, \ldots, T_n] = gr.tr._{K(\mathfrak{p})}(S(M)/T(\mathfrak{p}) \otimes R_\mathfrak{p}) = gr.tr._{K(\mathfrak{p})}S(M)/T(\mathfrak{p}).$$

Pela fórmula II.3, temos $dim(S(M)/T(\mathfrak{p})) = dim(R/\mathfrak{p}) + gr.tr._{R/\mathfrak{p}}S(M)/T(\mathfrak{p}) = dim(R/\mathfrak{p}) + \mu(M_\mathfrak{p})$ e segue que $dim(S(M)) \geq dim(S(M)/T(\mathfrak{p})) = dim(R/\mathfrak{p}) + \mu(M_\mathfrak{p})$. Logo, $dim(S(M)) \geq b(M)$.

Reciprocamente, seja $\mathfrak{p}$ um ideal primo de $S(M)$ e ponha $\mathfrak{q} = \mathfrak{p} \cap R$. É claro que $T(\mathfrak{q}) \subset \mathfrak{p}$, pois $\mathfrak{p}$ é ideal primo e

$$x \in T(\mathfrak{q}) \Rightarrow \overline{x} \in S_{R/\mathfrak{q}}(M/\mathfrak{q}M) \text{ e } \exists r \notin \mathfrak{q}; \overline{rx} = 0 \Rightarrow rx \in \mathfrak{q} \subset \mathfrak{p} \Rightarrow x \in \mathfrak{p}.$$

Logo, escolhendo $\mathfrak{p}$ minimal tal que $dim(S(M)/\mathfrak{p}) = dim(S(M))$, temos que $dim(S(M)) = dim(S(M)/\mathfrak{p}) \leq dim(S(M)/T(\mathfrak{q})) = dim(R/\mathfrak{q}) + \mu(M_\mathfrak{q})$ e logo $dim(S(M)) \leq b(M)$. □

Capítulo III

As Álgebras Simétrica e de Rees de um Ideal Gerado por uma R-seqüência

Vamos agora definir uma aplicação da álgebra simétrica de um ideal qualquer para a sua álgebra de Rees e queremos estudar os ideais para os quais essa aplicação é um isomorfismo, que serão chamados de ideais de tipo linear de R. Veremos que esses ideais têm no máximo $dim(R) + 1$ geradores minimais, quando R é um domínio. O objetivo deste capítulo é demonstrar que ideais gerados por R-seqüências são de tipo linear. Daremos exemplos desse resultado e contra-exemplos da sua recíproca e, por último, uma caracterização de anéis locais regulares usando o conceito de álgebra simétrica.

III.1 Comparação das Álgebras Simétrica e de Rees de um Ideal Gerado por uma R-seqüência

Sejam $\mathfrak{a}$ um ideal de R, $\mathcal{R}(\mathfrak{a})$ sua álgebra de Rees e $S(\mathfrak{a})$ sua álgebra simétrica. Pela definição de $S(\mathfrak{a})$, a aplicação φ de $\mathfrak{a}$ em $\mathcal{R}(\mathfrak{a})$ que leva $c \in \mathfrak{a}$ em $cT \in \mathcal{R}(\mathfrak{a})$ se prolonga a um único homomorfismo ϕ de $S(\mathfrak{a})$ em $\mathcal{R}(\mathfrak{a})$ tal que $\phi \circ \psi_{\mathfrak{a}} = \varphi$, onde $\psi_{\mathfrak{a}} : \mathfrak{a} \to S(\mathfrak{a})$ é a aplicação que define a álgebra simétrica de $\mathfrak{a}$.

$$\begin{tikzcd}
\mathfrak{a} \arrow[r, "\varphi"] \arrow[d, "\psi_{\mathfrak{a}}"'] & \mathcal{R}(\mathfrak{a}) \\
S(\mathfrak{a}) \arrow[ur, "\phi"'] &
\end{tikzcd}$$

Vamos ver que ϕ é uma aplicação sobrejetiva. Os elementos homogêneos de grau 0 de $\mathcal{R}(\mathfrak{a})$ são os elementos de R, e é claro que $\phi(R) = R$. Seja então $cT^n \in \mathcal{R}(\mathfrak{a})$ um elemento homogêneo de grau n. Logo, $c \in \mathfrak{a}^n$ e, usando o fato de que ϕ é um homomorfismo de R-álgebras, podemos supor que $c = c_1 . \cdots . c_n$, onde $c_i \in \mathfrak{a}$. Assim, $\phi(c_1 . \cdots . c_n) = c_1 T . \cdots . c_n T = c_1 . \cdots . c_n T^n = cT^n$.

Definição III.1.1 *No caso em que a aplicação $\phi : \mathfrak{a} \to S(\mathfrak{a})$ definida acima á uma bijeção, dizemos que $\mathfrak{a}$ é um* **ideal de tipo linear**.

Como conseqüência dessa definição e dos Teoremas II.3.6 e II.3.4, obtemos:

Corolário III.1.2 *Sejam I um ideal de R, com R domínio de dimensão n. Se $S(I) \cong \mathcal{R}(I)$, então $\mu(I) \leq n+1$.*

Dem. : Temos $\mu(I) \leq b(I) = dim(S(I)) = dim(\mathcal{R}(I)) = n+1$. □

Lema III.1.3 *Sejam R um domínio e $\mathfrak{a}$ um ideal de R. Então $Ker(\phi)$ é o submódulo de torção de $S(\mathfrak{a})$.*

Dem. : Suponhamos que $\mathfrak{a} = (a_1, \ldots, a_n) \neq 0$ e que $a_n \neq 0$. Sabemos que $S(\mathfrak{a}) = R[X_1, \ldots, X_n]/\mathfrak{q}$, onde $\mathfrak{q}$ é o ideal de $R[X_1, \ldots, X_n]$ gerado pelas formas lineares $\sum_{i=1}^n b_i X_i$ tais que $\sum_{i=1}^n b_i a_i = 0$ e que $\mathcal{R}(\mathfrak{a}) = R[X_1, \ldots, X_n]/\mathfrak{q}_\infty$, onde, para $f \in R[X_1, \ldots, X_n]$ homogêneo, temos $f \in \mathfrak{q}_\infty \Leftrightarrow f(a_1, \ldots, a_n) = 0$, como foi visto na Seção II.2. Logo, $\mathfrak{q} \subset \mathfrak{q}_\infty$ e $Ker(\phi) = \mathfrak{q}_\infty/\mathfrak{q}$.

$$R[X_1, \ldots, X_n]/\mathfrak{q} = S(\mathfrak{a}) \xrightarrow{\phi} \mathcal{R}(\mathfrak{a}) = R[X_1, \ldots, X_n]/\mathfrak{q}_\infty$$

Para mostrar que $Ker(\phi) = T(S(\mathfrak{a}))$, vamos mostrar que para todo $f \in \mathfrak{q}_\infty$, existe um $c \in R - \{0\}$ tal que $cf \in \mathfrak{q}$. Como o ideal $\mathfrak{q}_\infty$ é homogêneo, basta tomar $f \in \mathfrak{q}_\infty$ homogêneo. Vamos usar indução no grau m de f

- Como todo elemento homogêneo de grau 1 de $\mathfrak{q}_\infty$ pertence a $\mathfrak{q}$, o lema vale para $m = 1$ e $c = 1 \neq 0$.

- Suponhamos que o lema é verdadeiro para todo polinômio homogêneo de grau $\leq m-1$ de $\mathfrak{q}_\infty$. Temos:

  $$f(X_1, \ldots, X_n) = X_1 f_1(X_1, \ldots, X_n) + X_2 f_2(X_2, \ldots, X_n) + \cdots + X_n f_n(X_n)$$

  onde os f_i são homogêneos de grau $m-1$. Consideremos o polinômio homogêneo

  $$g(X_1, \ldots, X_n) = X_1 f_1(a_1, \ldots, a_n) + X_2 f_2(a_2, \ldots, a_n) + \cdots + X_n f_n(a_n).$$

  Como $g(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) = 0$, segue que $g \in \mathfrak{q}_\infty$ e, como g tem grau 1, segue que $g \in \mathfrak{q}$. Por outro lado,

  $$\begin{aligned}
  & a_n^{m-1} f - X_n^{m-1} g = \\
  & \quad a_n^{m-1} X_1 f_1(X_1, \ldots, X_n) + a_n^{m-1} X_2 f_2(X_2, \ldots, X_n) + \cdots + a_n^{m-1} X_n f_n(X_n) \\
  & \quad - X_n^{m-1} X_1 f_1(a_1, \ldots, a_n) - X_n^{m-1} X_2 f_2(a_2, \ldots, a_n) - \cdots - X_n^{m-1} X_n f_n(a_n) \\
  & \qquad = X_1[a_n^{m-1} f_1(X_1, \ldots, X_n) - X_n^{m-1} f_1(a_1, \ldots, a_n)] + \\
  & \qquad + X_2[a_n^{m-1} f_2(X_2, \ldots, X_n) - X_n^{m-1} f_2(a_2, \ldots, a_n)] + \cdots + \\
  & \qquad + X_{n-1}[a_n^{m-1} f_{n-1}(X_{n-1}, X_n) - X_n^{m-1} f_{n-1}(a_{n-1}, a_n)] + \\
  & \qquad + a_n^{m-1} X_n f_n(X_n) - X_n^m f_n(a_n)
  \end{aligned}$$

Como $f_n(X_n) = rX_n^{m-1}$, então $a_n^{m-1}X_nf_n(X_n) - X_n^m f_n(a_n) = a_n^{m-1}X_nrX_n^{m-1} - X_n^m r a_n^{m-1} = 0$. Logo,

$$a_n^{m-1}f - X_n^{m-1}g = X_1g_1(X_1,\dots,X_n) + \cdots + X_{n-1}g_{n-1}(X_{n-1},X_n),$$

onde os g_i são polinômios homogêneos de grau $m-1$ que anulam $a_1,\dots,a_n$ e, logo, que pertencem a $\mathfrak{q}_\infty$. Pela hipótese de indução, para cada $i=1,\dots,n$, existe um $c_i \in R-\{0\}$ tal que $c_ig_i \in \mathfrak{q}$. Logo, $c_iX_ig_i \in \mathfrak{q}$ e $c_1\cdots c_{n-1}(a_n^{m-1}f - X_n^{m-1}g) \in \mathfrak{q}$. Portanto,

$$(c_1\cdots c_{n-1}a_n^{m-1})f = \underbrace{c_1\cdots c_{n-1}(a_n^{m-1}f - X_n^{m-1}g)}_{\in\, \mathfrak{q}} + \underbrace{c_1\cdots c_{n-1}X_n^{m-1}g}_{\in\, \mathfrak{q}} \in \mathfrak{q}.$$

□

Proposição III.1.4 *Sejam R um domínio e $\mathfrak{a}$ um ideal de R. As seguintes afirmações são equivalentes:*

i) *$S(\mathfrak{a})$ é um domínio*

ii) *$S(\mathfrak{a})$ é livre de torção*

iii) *$\mathfrak{a}$ é de tipo linear*

Dem. :

i) $\Rightarrow$ ii) O submódulo de torção de $S(\mathfrak{a})$ é $T(S(\mathfrak{a})) = \{u \in S(\mathfrak{a}) / \exists v \in \dot{R}; u.v = 0\}$. Portanto: $S(\mathfrak{a})$ domínio $\Rightarrow T(S(\mathfrak{a})) = 0 \Rightarrow S(\mathfrak{a})$ é livre de torção.

ii) $\Rightarrow$ iii) Lema III.1.3

iii) $\Rightarrow$ i) Se $u.v = 0$ em $S(\mathfrak{a})$, aplicando ϕ à equação, teremos $0 = \phi(u.v) = \phi(u).\phi(v)$ em $\mathcal{R}(\mathfrak{a})$, que é um domínio, pois $R[T]$ é domínio. Logo, $\phi(u) = 0$ ou $\phi(v) = 0$ e como estamos supondo ϕ injetiva, segue que $u = 0$ ou $v = 0$. Logo, $S(\mathfrak{a})$ é domínio. □

Suponhamos agora que $\mathfrak{a} = (a_1,\dots,a_n)$ e consideremos o homomorfismo homogêneo

$$\begin{array}{rcl} R[X_1,\dots,X_n,T] & \to & R[T] \\ X_i & \mapsto & a_iT \\ T & \mapsto & T \end{array}$$

Seu núcleo J é o ideal de $R[X_1,\dots,X_n,T]$ gerado pelos $X_i - a_iT, i = 1,\dots,n$.

De fato, como J é um ideal homogêneo, basta considerar seus elementos homogêneos. Seja então

$$f = \sum_{v_1+\cdots+v_n+v=d} \rho_{v_1,\dots,v_n,v} X_1^{v_1}\cdots X_n^{v_n}T^v \in R[X_1,\dots,X_n,T].$$

Temos que

$$f(a_1T,\dots,a_nT,T) = (\sum_{v_1+\cdots+v_n+v=d} \rho_{v_1,\dots,v_n,v} a_1^{v_1}\cdots a_n^{v_n})T^d = f(a_1,\dots,a_n,1)T^d.$$

Logo,

$$f \in J \Leftrightarrow f(a_1T,\dots,a_nT,T) = 0 \Leftrightarrow f(a_1,\dots,a_n,1) = 0.$$

Consideremos $I = (X_1 - a_1T,\dots,X_n - a_nT)$. Daí:
- $f \in I \Rightarrow f(a_1,\dots,a_n,1) = 0 \Rightarrow f \in J$
- $f \in J \Rightarrow f(a_1,\dots,a_n,1) = 0$. Podemos escrever

$$\begin{array}{rcl} f = F_1(X_1,\dots,X_n,T).(X_1 - a_1T) + r_1(X_2,\dots,X_n,T) & e & 0 = f(a_1,\dots,a_n,1) = r_1(a_2,\dots,a_n,1) \\ r_1 = F_2(X_2,\dots,X_n,T).(X_2 - a_2T) + r_2(X_3,\dots,X_n,T) & e & 0 = r_1(a_2,\dots,a_n,1) = r_2(a_3,\dots,a_n,1) \\ \vdots & & \vdots \\ r_{n-1} = F_n(X_n,T).(X_n - a_nT) + r_n(T) & e & 0 = r_{n-1}(a_n,1) = r_n(1) \\ r_n = F_{n+1}(T).(T-1) + s & e & 0 = r_n(1) = s \end{array}$$

Logo,

$$\begin{aligned} f &= F_1(X_1,\dots,X_n,T).(X_1 - a_1T) + F_2(X_2,\dots,X_n,T).(X_2 - a_2T) + \cdots + F_n(X_n,T).(X_n - a_nT) + \\ &\quad + F_{n+1}(T).(T-1). \end{aligned}$$

Como $f \in J$, então $0 = f(a_1T,\dots,a_nT,T) = (T-1)F_{n+1}(T)$. Logo, $F_{n+1}(T) = 0$, o que implica que

$$f = F_1(X_1,\dots,X_n,T).(X_1 - a_1T) + F_2(X_2,\dots,X_n,T).(X_2 - a_2T) + \cdots + F_n(X_n,T).(X_n - a_nT)$$

Portanto, $f \in I$.

Além disso, é claro que $J \cap R[X_1,\dots,X_n] = \mathfrak{q}_\infty$, pela definição de $\mathfrak{q}_\infty$.

Definamos $\mathfrak{q}_s = \{\sum_{i=1}^n (X_i - a_iT)f_i \in \mathfrak{q}_\infty; gr_T(f_i) \leq s, \forall i = 1,\dots,n\}$, onde $gr_T(f_i)$ é o grau de f_i em relação a T.

1. $\mathfrak{q}_s$ é um ideal homogêneo de $R[X_1,\dots,X_n]$:

   - $\sum_{i=1}^n (X_i - a_iT)f_i, \sum_{i=1}^n (X_i - a_iT)g_i \in \mathfrak{q}_s \Rightarrow gr_T(f_i), gr_T(g_i) \leq s \Rightarrow \sum_{i=1}^n (X_i - a_iT)f_i + \sum_{i=1}^n (X_i - a_iT)g_i = \sum_{i=1}^n (X_i - a_iT)(f_i + g_i)$, com $gr_T(f_i + g_i) \leq max\{gr_T(f_i), gr_T(g_i)\} \leq s$ $\Rightarrow \sum_{i=1}^n (X_i - a_iT)f_i + \sum_{i=1}^n (X_i - a_iT)g_i \in \mathfrak{q}_s$
   - $\sum_{i=1}^n (X_i - a_iT)f_i \in \mathfrak{q}_s, f \in R[X_1,\dots,X_n] \Rightarrow f.(\sum_{i=1}^n (X_i - a_iT)f_i) = \sum_{i=1}^n (X_i - a_iT)f_i f$, onde $gr_T(f_i f) = gr_T(f_i) + gr_T(f) \leq s + 0 = s \Rightarrow f.(\sum_{i=1}^n (X_i - a_iT)f_i) \in \mathfrak{q}_s$
   - $\sum_{i=1}^n (X_i - a_iT)f_i \in \mathfrak{q}_s \Rightarrow gr_T(f_i) \leq s$ e escrevendo f_i em componentes homogêneas, temos $f_i = f_{0i} + f_{1i} + \cdots + f_{r_i i}$, onde cada f_{ji} é homogêneo de grau j e $gr_T(f_{ji}) \leq gr_T(f_i) \leq s$ $\Rightarrow \sum_{i=1}^n (X_i - a_iT)f_{ji} \in \mathfrak{q}_s, \forall j = 1,\dots,r_i \Rightarrow \sum_{i=1}^n (X_i - a_iT)f_i = \sum_{i=1}^n (X_i - a_iT)f_{0i} + \sum_{i=1}^n (X_i - a_iT)f_{1i} + \cdots + \sum_{i=1}^n (X_i - a_iT)f_{r_i i}$, onde cada parcela da soma é uma parte homogênea da soma $\sum_{i=1}^n (X_i - a_iT)f_i$.

2. Em $R[X_1, \ldots, X_n]$, temos

$$\mathfrak{q} \subset \mathfrak{q}_0 \subset \mathfrak{q}_1 \subset \cdots \subset \mathfrak{q}_s \cdots \subset \mathfrak{q}_\infty$$

Basta ver a primeira inclusão: Temos que

$$\mathfrak{q}_0 = \{\sum_{i=1}^{n}(X_i - a_iT)f_i \in \mathfrak{q}_\infty; gr_T(f_i) = 0, \forall i = 1, \ldots, n\} \text{ e } \mathfrak{q} = (\sum_{i=1}^{n} b_iX_i; \sum_{i=1}^{n} b_ia_i = 0).$$

Logo, para os geradores de $\mathfrak{q}$, como $b_i \in R$, podemos escrever

$$\sum_{i=1}^{n} b_iX_i = b_1(X_1-a_1T)+\cdots+b_n(X_n-a_nT)+(\sum_{i=1}^{n} b_ia_i)T = b_1(X_1-a_1T)+\cdots+b_n(X_n-a_nT) \in \mathfrak{q}_0$$

e, para um elemento qualquer x de $\mathfrak{q}$, temos $x = \sum_{i=1}^{r}(b_{i1}X_1 + \cdots b_{in}X_n)f_i$, $f_i \in R[X_1, \ldots, X_n]$. Assim, $gr_T(f_i) = 0$ e já sabemos que $b_{i1}X_1 + \cdots + b_{in}X_n \in \mathfrak{q}_0, \forall i = 1, \ldots, n$. Portanto, $x \in \mathfrak{q}_0$.

3. $\mathfrak{q}_0 = \{\sum_{i=1}^{n} X_if_i \in R[X_1, \ldots, X_n]; f_i \in R[X_1, \ldots, X_n] \text{ e } \sum_{i=1}^{n} a_if_i = 0\}$

Dado $f \in \mathfrak{q}_0$, temos que $f = \sum_{i=1}^{n}(X_i - a_iT)f_i \in \mathfrak{q}_\infty$, onde $gr_T(f_i) = 0, \forall i$. Assim, $f_i \in R[X_1, \ldots, X_n]$ e $f = \sum_{i=1}^{n} X_if_i - T(\sum_{i=1}^{n} a_if_i)$. Como $f \in \mathfrak{q}_\infty \subset R[X_1, \ldots, X_n]$, devemos ter $\sum_{i=1}^{n} a_if_i = 0$ e $f = \sum_{i=1}^{n} X_if_i$.

4. $\mathfrak{q}_0 = \mathfrak{q}$

$f \in \mathfrak{q}_0 \Rightarrow f = \sum_{i=1}^{n} X_if_i$, onde $\sum_{i=1}^{n} a_if_i = 0, f_i \in R[X_1, \ldots, X_n] \Rightarrow f_i = \sum_j c_{ij}m_j(X)$, onde $c_{ij} \in R$ e $m_j(X)$ é um monômio em $X_1, \ldots, X_n \Rightarrow 0 = \sum_{i=1}^{n} a_if_i = \sum_{i=1}^{n} a_i \sum_j c_{ij}m_j(X) = \sum_j(\sum_{i=1}^{n} a_ic_{ij})m_j(X) \Rightarrow \sum_{i=1}^{n} a_ic_{ij} = 0, \forall j \Rightarrow \sum_{i=1}^{n} c_{ij}X_i \in \mathfrak{q}, \forall j \Rightarrow f = \sum_{i=1}^{n} X_if_i = \sum_{i=1}^{n} X_i \sum_j c_{ij}m_j(X) = \sum_j \underbrace{(\sum_{i=1}^{n} c_{ij}X_i)}_{\in \mathfrak{q}} m_j(X) \in \mathfrak{q}$.

5. Se $\mathfrak{q}_s = \mathfrak{q}_{s+1}$, para algum inteiro $s \geq 0$, então $\mathfrak{q}_s = \mathfrak{q}_{s+r}, \forall r \geq 1$.

Vamos usar indução em r. Por hipótese, $\mathfrak{q}_s = \mathfrak{q}_{s+1}$. Suponhamos que $\mathfrak{q}_s = \mathfrak{q}_{s+r-1}$ e vamos mostrar que $\mathfrak{q}_s = \mathfrak{q}_{s+r}$.

$f \in \mathfrak{q}_{s+r} \Rightarrow f = \sum_{i=1}^{n}(X_i - a_iT)f_i \in \mathfrak{q}_\infty$, com $gr_T(f_i) \leq s + r, \forall i \Rightarrow f_i = Tf_i' + r_i(X_1, \ldots, X_n)$, onde $gr_T(f_i') \leq s + r - 1$ e $gr_T(r_i) = 0 \Rightarrow f = \sum_{i=1}^{n}(X_i - a_iT)Tf_i' + \sum_{i=1}^{n}(X_i - a_iT)r_i \Rightarrow T(\sum_{i=1}^{n}(X_i - a_iT)f_i' - \sum_{i=1}^{n} a_ir_i) = \sum_{i=1}^{n}(X_i - a_iT)Tf_i' - \sum_{i=1}^{n} a_iTr_i = f - \sum_{i=1}^{n} X_ir_i \in R[X_1, \ldots, X_n] \Rightarrow \sum_{i=1}^{n}(X_i - a_iT)f_i' = \sum_{i=1}^{n} a_ir_i \in R[X_1, \ldots, X_n] \cap J = \mathfrak{q}_\infty \Rightarrow \sum_{i=1}^{n}(X_i - a_iT)f_i' \in \mathfrak{q}_{s+r-1}, \sum_{i=1}^{n}(X_i - a_iT)r_i \in \mathfrak{q}_0 \subset \mathfrak{q}_{s+r-1} \Rightarrow f = T(\sum_{i=1}^{n}(X_i - a_iT)f_i') + \sum_{i=1}^{n}(X_i - a_iT)r_i \in \mathfrak{q}_{s+r-1} = \mathfrak{q}_s$

Definição III.1.5 *Sejam $\mathfrak{a} = (a_1, \ldots, a_n)$ um ideal de R e $S(\mathfrak{a})$ sua álgebra simétrica. Dizemos que o ideal $\mathfrak{a}$* **obedece à condição (I)** *se sempre que tivermos $\sum_{i=1}^{n} a_if_i \in \mathfrak{q}$, com $f_i \in R[X_1, \ldots, X_n]$, isso implicar que $\sum_{i=1}^{n} X_if_i \in \mathfrak{q}$.*

Exemplo III.1.6 Suponhamos que os geradores do ideal $\mathfrak{a}$ formem uma R-seqüência. Provaremos adiante que, nesse caso, o ideal $\mathfrak{a}$ obedece à condição (I).

Proposição III.1.7 *Sejam R um anel e $\mathfrak{a} = (a_1, \dots, a_n)$ um ideal de R. As seguintes afirmações são equivalentes:*

i) *$\mathfrak{a}$ é de tipo linear*

ii) $\mathfrak{q} = \mathfrak{q}_\infty$

iii) $\mathfrak{q} = \mathfrak{q}_1$

iv) *$\mathfrak{a}$ obedece à condição (I)*

Dem. :

i) $\Leftrightarrow$ ii) pois $Ker(\phi) = \mathfrak{q}_\infty/\mathfrak{q}$.

ii) $\Rightarrow$ iii) é trivial.

iii) $\Rightarrow$ ii) Se $\mathfrak{q} = \mathfrak{q}_1$, como já sabemos que $\mathfrak{q}_i = \mathfrak{q}_{i+1}, \forall i \geq 0$, segue que $\mathfrak{q}_i = \mathfrak{q}, \forall i \geq 0$. Então teremos $\mathfrak{q} = \mathfrak{q}_\infty$. Com efeito,

$f \in \mathfrak{q}_\infty \Rightarrow f = \sum_{i=1}^n (X_i - a_i T) f_i$, onde $f_i \in R[X_1, \dots, X_n, T] \Rightarrow gr_T(f_i) \leq s, \forall i,$ onde $s = max\{gr_T(f_j); 1 \leq j \leq n\} \Rightarrow f \in \mathfrak{q}_s = \mathfrak{q}$.

iv) $\Rightarrow$ ii) Basta provar que $\mathfrak{q}_\infty \subset \mathfrak{q}$. Como $\mathfrak{q}_\infty$ é um polinômio homogêneo, basta tomar $f \in \mathfrak{q}_\infty$ homogêneo de grau m. Logo, $f = \sum_{i=1}^n (X_i - a_i T) f_i$, onde os $f_i \in R[X_1, \dots, X_n, T]$ são homogêneos de grau $m-1$, isto é, $f_i = b_{0,i}T^{m-1} + b_{1,i}T^{m-2} + \cdots + b_{m-2,i}T + b_{m-1,i}$, onde $b_{j,i} \in R[X_1, \dots, X_n]$ é homogêneo de grau j. Assim,

$$\begin{aligned} f &= \sum_{i=1}^n (X_i - a_i T)(b_{0,i}T^{m-1} + b_{1,i}T^{m-2} + \cdots + b_{m-2,i}T + b_{m-1,i}) \\ &= (-\sum_{i=1}^n b_{0,i}a_i)T^m + (\sum_{i=1}^n b_{0,i}X_i - \sum_{i=1}^n b_{1,i}a_i)T^{m-1} + (\sum_{i=1}^n b_{1,i}X_i - \sum_{i=1}^n b_{2,i}a_i)T^{m-2} + \cdots + \\ &\quad + (\sum_{i=1}^n b_{m-2,i}X_i - \sum_{i=1}^n b_{m-1,i}a_i)T + \sum_{i=1}^n b_{m-1,i}X_i \end{aligned}$$

e como $f \in R[X_1, \dots, X_n]$, temos

$$f = \sum_{i=1}^n b_{m-1,i}X_i, \sum_{i=1}^n b_{m-1,i}a_i = \sum_{i=1}^n b_{m-2,i}X_i, \quad \dots, \sum_{i=1}^n b_{2,i}a_i = \sum_{i=1}^n b_{1,i}X_i,$$
$$\sum_{i=1}^n b_{1,i}a_i = \sum_{i=1}^n b_{0,i}X_i \qquad \text{e} \qquad \sum_{i=1}^n b_{0,i}a_i = 0.$$

Pela hipótese, temos:

$$\sum_{i=1}^n b_{0,i}a_i = 0 \in \mathfrak{q} \Rightarrow \sum_{i=1}^n b_{1,i}a_i = \sum_{i=1}^n b_{0,i}X_i \in \mathfrak{q} \Rightarrow \sum_{i=1}^n b_{2,i}a_i = \sum_{i=1}^n b_{1,i}X_i \in \mathfrak{q} \Rightarrow \cdots \Rightarrow f \in \mathfrak{q}$$

Portanto, $\mathfrak{q} = \mathfrak{q}_\infty$.

ii) $\Rightarrow$ iv) Suponhamos que a condição (I) não é verificada. Então, existem $f_i \in R[X_1, \dots, X_n]$, $i = 1, \dots, n$ tais que $\sum_{i=1}^n a_i f_i \in \mathfrak{q}$ e $\sum_{i=1}^n X_i f_i \notin \mathfrak{q}$. Como $\sum_{i=1}^n (X_i - a_i T) f_i \in J$, $\sum_{i=1}^n a_i f_i \in \mathfrak{q} \subset \mathfrak{q}_\infty \subset J$ e $\sum_{i=1}^n X_i f_i = \sum_{i=1}^n (X_i - a_i T) f_i + T(\sum_{i=1}^n a_i f_i)$, então $\sum_{i=1}^n X_i f_i \in J \cap R[X_1, \dots, X_n] = \mathfrak{q}_\infty$. Logo, $\sum_{i=1}^n X_i f_i \in \mathfrak{q}_\infty - \mathfrak{q}$ e $\mathfrak{q}_\infty \neq \mathfrak{q}$. □

Lema III.1.8 *Sejam $\mathfrak{a} = (a_1, \dots, a_n)$ um ideal de R e $S(\mathfrak{a}) = R[X_1, \dots, X_n]/\mathfrak{q}$ sua álgebra simétrica. Se $a_1, \dots, a_n$ é uma R-seqüência, então $\mathfrak{q}$ é o ideal de $R[X_1, \dots, X_n]$ gerado pelos $a_i X_j - a_j X_i$, $(i < j)$.*

Dem. : Sabemos que $\mathfrak{q} = (\sum_{i=1}^n b_i X_i; \sum_{i=1}^n b_i a_i = 0)$. Logo, tomando $f = \sum_{i=1}^n b_i X_i \in \mathfrak{q}$, temos $b_n a_n \in (a_1, \dots, a_{n-1})R$ e como a_n não é divisor de zero módulo $(a_1, \dots, a_{n-1})R$, devemos ter $b_n \in (a_1, \dots, a_{n-1})R$, isto é, $b_n = \sum_{i=1}^{n-1} c_{i,n} a_i$, onde $c_{i,n} \in R, i = 1, \dots, n-1$. Agora,

$$\begin{aligned} b_{n-1}a_{n-1} &= -(\sum_{i=1}^{n-2} b_i a_i) - b_n a_n = -(\sum_{i=1}^{n-2} b_i a_i) - (\sum_{i=1}^{n-1} c_{i,n} a_i) a_n \\ &\Rightarrow \quad a_{n-1}(b_{n-1} + c_{n-1,n} a_n) = -(\sum_{i=1}^{n-2} (b_i + c_{i,n} a_n) a_i) \in (a_1, \dots, a_{n-2})R. \end{aligned}$$

Como a_{n-1} não é divisor de zero módulo $(a_1, \dots, a_{n-2})R$, temos que $b_{n-1} + c_{n-1,n} a_n \in (a_1, \dots, a_{n-2})R$, isto é, $b_{n-1} = -c_{n-1,n} a_n + \sum_{i=1}^{n-2} c_{i,n-1} a_i$, com $c_{i,n-1} \in R, i = 1, \dots, n-2$. Por indução em n, obtemos $b_j = -(\sum_{i=j+1}^n c_{j,i} a_i) + \sum_{i=1}^{j-1} c_{i,j} a_i, j = 1, \dots, n$. Logo,

$$\begin{aligned} \sum_{j=1}^n b_j X_j &= -\sum_{j=1}^n \sum_{i=j+1}^n c_{j,i} a_i X_j + \sum_{j=1}^n \sum_{i=1}^{j+1} c_{i,j} a_i X_j \\ &= -\sum_{i=1}^n \sum_{j=i+1}^n c_{i,j} a_j X_i + \sum_{j=1}^n \sum_{i=1}^{j+1} c_{i,j} a_i X_j \text{(trocando i por j na primeira soma)} \\ &= -\sum_{i<j} c_{i,j} a_j X_i + \sum_{i<j} c_{i,j} a_i X_j \\ &= \sum_{i<j} c_{i,j}(a_i X_j - a_j X_i) \end{aligned}$$

□

Teorema III.1.9 *Seja R um anel. Para cada ideal $\mathfrak{a}$ de R gerado por uma R-seqüência, temos $S(\mathfrak{a}) \cong \mathcal{R}(\mathfrak{a})$.*

Dem. : De acordo com a Proposição III.1.7, devemos mostrar que a condição (I) é verificada. Seja $\sum_{i=1}^n a_i f_i \in \mathfrak{q}$, com $f_i \in R[X_1, \dots, X_n], i = 1, \dots, n$ e vamos mostrar que $\sum_{i=1}^n X_i f_i \in \mathfrak{q}$. Pelo Lema III.1.8, temos $\sum_{i=1}^n a_i f_i = \sum_{i<j} f_{i,j}(a_i X_j - a_j X_i)$, com $f_{i,j} \in R[X_1, \dots, X_n]$. Então,

$$\begin{aligned}
\sum_{i=1}^{n} a_i f_i &= f_{1,2}(a_1X_2 - a_2X_1) + f_{1,3}(a_1X_3 - a_3X_1) + \cdots + f_{1,n}(a_1X_n - a_nX_1) + \\
&+ f_{2,3}(a_2X_3 - a_3X_2) + \cdots + f_{2,n}(a_2X_n - a_nX_2) + \cdots + \\
&+ f_{n-1,n}(a_{n-1}X_n - a_nX_{n-1}) \\
&= -a_n(\sum_{i=1}^{n-1} f_{i,n}X_i) + \sum_{i<j=2}^{n-1} f_{i,j}(a_iX_j - a_jX_i) + \sum_{i=1}^{n-1} f_{i,n}a_iX_n
\end{aligned}$$

Assim,

$$a_n(f_n + \sum_{i=1}^{n-1} f_{i,n}X_i) = -\sum_{i=1}^{n-1} a_if_i + \sum_{i<j=2}^{n-1} f_{i,j}(a_iX_j - a_jX_i) + \sum_{i=1}^{n-1} f_{i,n}a_iX_i \in (a_1, \ldots, a_{n-1})R[X_1, \ldots, X_n].$$

Como a_n não é divisor de zero módulo o ideal $(a_1, \ldots, a_{n-1})R$, então a_n também não é divisor de zero módulo o ideal $(a_1, \ldots, a_{n-1})R[X_1, \ldots, X_n]$ e, portanto, $f_n = -\sum_{i=1}^{n-1} f_{i,n}X_i + \sum_{i=1}^{n-1} a_ig_{i,n}$, com $g_{i,n} \in R[X_1, \ldots, X_n]$. Por indução em n, como a_i não é divisor de zero módulo o ideal $(a_1, \ldots, a_{i-1})R[X_1, \ldots, X_n]$, para $i = 1, \ldots, n$, devemos ter $f_j = -\sum_{i=1}^{j-1} f_{i,j}X_i + \sum_{i=1}^{j-1} a_ig_{i,j} + \sum_{i=j+1}^{n} f_{j,i}X_i - \sum_{i=j+1}^{n} a_ig_{j,i}$, com $g_{j,i} \in R[X_1, \ldots, X_n]$. Portanto,

$$\begin{aligned}
\sum_{j=1}^{n} X_jf_j &= -\sum_{j=1}^{n}\sum_{i=1}^{j-1} X_iX_jf_{i,j} + \sum_{j=1}^{n}\sum_{i=1}^{j-1} a_ig_{i,j}X_j + \sum_{j=1}^{n}\sum_{i=j+1}^{n} X_iX_jf_{j,i} - \sum_{j=1}^{n}\sum_{i=j+1}^{n} a_ig_{j,i}X_j \\
&= -\sum_{i<j} X_iX_jf_{i,j} + \sum_{i<j} a_ig_{i,j}X_j + \sum_{i=1}^{n}\sum_{j=i+1}^{n} X_jX_if_{i,j} - \sum_{i=1}^{n}\sum_{j=i+1}^{n} a_jg_{i,j}X_i \\
&= -\sum_{i<j} X_iX_jf_{i,j} + \sum_{i<j} a_ig_{i,j}X_j + \sum_{i<j} X_iX_jf_{i,j} - \sum_{i<j} a_jg_{i,j}X_i \\
&= -\sum_{i<j} g_{i,j}(a_iX_j - a_jX_i)
\end{aligned}$$

Logo, de novo pelo Lema III.1.8, $\sum_{j=1}^{n} X_jf_j \in \mathfrak{q}$ e a condição (I) é verificada. □

Exemplo III.1.10 Sejam $R = K[X, Y, Z]$ e $\mathfrak{a} = (X, Y, Z)$, onde K é corpo. Como X, Y, Z é uma seqüência regular, veremos no próximo capítulo que $S(\mathfrak{a}) \cong \mathcal{R}(\mathfrak{a})$. Mas $\mathfrak{a}^2 = (X^2, Y^2, Z^2, XY, XZ, YZ)$ não tem suas ágebras simétrica e de Rees isomorfas, pois $\mu(\mathfrak{a}^2) = 6 \geq 4 = dim R + 1$.

III.2 Exemplo

Vamos mostrar nesta seção um exemplo de ideal de tipo linear num determinado anel e também vamos aplicar o Lema III.1.8 para calcular a dimensão de uma certa variedade. Para isso, precisaremos de um lema auxiliar, que será provado também nesta seção.

Exemplo III.2.1 Sejam K um corpo, $a_1, \ldots, a_n$ elementos algebricamente independentes sobre K, $R = K[a_1, \ldots, a_n]$, $\mathfrak{a} = (a_1, \ldots, a_n)$ ideal de R. Então $S(\mathfrak{a}) \cong \mathcal{R}(\mathfrak{a})$.

Com efeito, sabemos que $S(\mathfrak{a}) = R[X_1, \ldots, X_n]/\mathfrak{q}$, onde $\mathfrak{q}$ é o ideal do anel $R[X_1, \ldots, X_n]$ gerado pelas formas lineares $\sum_{i=1}^n b_i X_i$ tais que $\sum_{i=1}^n b_i a_i = 0$. Como os elementos a_i são algebricamente independentes sobre K, então $a_1, \ldots, a_n$ formam uma R-seqüência e pelo Teorema III.1.9 segue que $S(\mathfrak{a}) \cong \mathcal{R}(\mathfrak{a})$.

Vamos agora demonstrar o referido lema.

Lema III.2.2 *Sejam $x_1, \ldots, x_n, u, v$ elementos algebricamente independentes sobre um corpo K, V a variedade do ponto genérico $(ux_1, \ldots, ux_n, vx_1, \ldots, vx_n)$ e $\mathfrak{p}$ o ideal do anel $K[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$ gerado pelos determinantes $X_iY_j - X_jY_i, i < j$. Então, $\mathfrak{p}$ é o ideal da variedade irredutível V e, portanto, $\mathfrak{p}$ é primo.*

Dem. : Seja $I_K(V)$ o ideal da variedade V. Temos

$$f \in \mathfrak{p} \Rightarrow f(ux; vx) = \sum_{i<j} c_{i,j}(ux_i vx_j - ux_j vx_i) = 0 \Rightarrow f \in I_K(V).$$

Por outro lado, se $f \in I_K(V)$, sejam $f_{r,s}$ suas componentes homogêneas de grau r nos X_i e de grau s nos Y_j. Como $f = \sum f_{r,s}$, temos $0 = f(ux; vx) = \sum f_{r,s}(x; x)u^r v^s$ e portanto $f_{r,s}(x; x) = 0$. Observamos que $f_{r,s}(x; x) = 0 \Leftrightarrow f_{r,s}(ux; vx) = 0$. Portanto, podemos supor que f é homogêneo de grau (r, s). Para mostrar que $f \in \mathfrak{p}$, vamos usar indução sobre o grau total $r + s$ de f.

- Se $r + s = 1$, temos que f é um polinômio em uma variável e que satisfaz $f(x; x) = 0$. Logo, $f = 0 \in \mathfrak{p}$.

- Suponhamos que $r, s \geq 1$. Em $f(x; x)$, o termo em $x_1^{t_1} \cdots x_n^{t_n}$ provém dos monômios do tipo $X_1^{i_1} \cdots X_n^{i_n} Y_1^{j_1} \cdots Y_n^{j_n}$ tais que $i_1 + j_1 = t_1, \ldots, i_n + j_n = t_n$ e se designarmos por $c_{i,j}$ o coeficiente de um monômio desse tipo em f, então $f(x; x) = 0 \Rightarrow \sum c_{i,j} x^i x^j = 0 \Rightarrow \sum c_{i,j} = 0$ (onde a soma é feita nas n-uplas $i = (i_1, \ldots, i_n)$ e $j = (j_1, \ldots, j_n)$ tais que $i_1 + j_1 = t_1, \ldots, i_n + j_n = t_n$). Também temos $i_1 = \cdots + i_n = r$ e $j_1 = \cdots + j_n = s$. Fixemos $X_1^{p_1} \cdots X_n^{p_n} Y_1^{q_1} \cdots Y_n^{q_n}$, onde $p_1 + q_1 = t_1, \ldots, p_n + q_n = t_n, p_1 = \cdots + p_n = r, q_1 = \cdots + q_n = s$. Seu coeficiente $c_{p,q}$ satisfaz $c_{p,q} = -\sum_{i \neq p, j \neq q} c_{i,j}$. Logo,

$$\begin{aligned} f &= c_{p,q} X_1^{p_1} \cdots X_n^{p_n} Y_1^{q_1} \cdots Y_n^{q_n} + \sum_{i \neq p, j \neq q} c_{i,j} X_1^{i_1} \cdots X_n^{i_n} Y_1^{j_1} \cdots Y_n^{j_n} \\ &= - \sum_{i \neq p, j \neq q} c_{i,j} X_1^{p_1} \cdots X_n^{p_n} Y_1^{q_1} \cdots Y_n^{q_n} + \sum_{i \neq p, j \neq q} c_{i,j} X_1^{i_1} \cdots X_n^{i_n} Y_1^{j_1} \cdots Y_n^{j_n} \\ &= - \sum_{i \neq p, j \neq q} c_{i,j} (X_1^{p_1} \cdots X_n^{p_n} Y_1^{q_1} \cdots Y_n^{q_n} - X_1^{i_1} \cdots X_n^{i_n} Y_1^{j_1} \cdots Y_n^{j_n}) \end{aligned}$$

  O polinômio

  $$g = X_1^{p_1} \cdots X_n^{p_n} Y_1^{q_1} \cdots Y_n^{q_n} - X_1^{i_1} \cdots X_n^{i_n} Y_1^{j_1} \cdots Y_n^{j_n}$$

  satisfaz

  $$g(x, x) = x_1^{p_1} \cdots x_n^{p_n} x_1^{q_1} \cdots x_n^{q_n} - x_1^{i_1} \cdots x_n^{i_n} x_1^{j_1} \cdots x_n^{j_n} = x_1^{p_1+q_1} \cdots x_n^{p_n+q_n} - x_1^{i_1+j_1} \cdots x_n^{i_n+j_n} = 0.$$

  É suficiente mostrar que $g \in \mathfrak{p}$.

1. Se g é múltiplo de uma indeterminada, por exemplo de X_1, então $g = X_1 h$ e como x_1 é regular (pois é algebricamente independente sobre k), segue que $h(x,x) = 0$. Usando a hipótese de indução no grau total, temos que $h \in \mathfrak{p}$ e logo $g \in \mathfrak{p}$.

2. Suponhamos que g não é múltiplo de nenhuma indeterminada. Sejam

$$M = \{k \in \{1, \ldots, n\}; p_k > 0\} \text{ e } M' = \{k \in \{1, \ldots, n\}; q_k > 0\}.$$

Assim,

$k \in M \Rightarrow p_k > 0 \Rightarrow i_k = 0$ (pois, caso contrário, X_k seria um fator de g)

$k \in M' \Rightarrow q_k > 0 \Rightarrow j_k = 0$ (pois, caso contrário, Y_k seria um fator de g)

$k \in \{1, \ldots, n\} \Rightarrow p_k + q_k = i_k + j_k = t_k$

Logo, $M \cap M' = \emptyset$. De fato,

$$k \in M \cap M' \Rightarrow p_k, q_k > 0 \Rightarrow i_k = j_k = 0 \Rightarrow 0 = i_k + j_k = t_k = p_k + q_k > 0,$$

absurdo.

Após uma reenumeração, podemos supor que $M = \{1, \ldots, m\}$ e $M' = \{m+1, \ldots, m'\}$, onde $1 \leq m \leq m' \leq n$. Temos:

$$k \notin M \cap M' \Rightarrow p_k = q_k = 0 \Rightarrow 0 = p_k + q_k = t_k = i_k + j_k \Rightarrow i_k = j_k = 0$$

Logo,

$$\begin{aligned}
g &= X_1^{p_1} \cdots X_m^{p_m} Y_{m+1}^{q_{m+1}} \cdots Y_{m'}^{q_{m'}} - Y_1^{j_1} \cdots Y_m^{j_m} X_{m+1}^{i_{m+1}} \cdots X_{m'}^{i_{m'}} \\
&= X_1^{p_1+q_1} \cdots X_m^{p_m+q_m} Y_{m+1}^{p_{m+1}+q_{m+1}} \cdots Y_{m'}^{p_{m'}+q_{m'}} - Y_1^{i_1+j_1} \cdots Y_m^{i_m+j_m} X_{m+1}^{i_{m+1}+j_{m+1}} \cdots X_{m'}^{i_{m'}+j_{m'}} \\
&= X_1^{t_1} \cdots X_m^{t_m} Y_{m+1}^{t_{m+1}} \cdots Y_{m'}^{t_{m'}} - Y_1^{t_1} \cdots Y_m^{t_m} X_{m+1}^{t_{m+1}} \cdots X_{m'}^{t_{m'}}
\end{aligned}$$

Além disso, $r = t_1 + \cdots + t_m = t_{m+1} + \cdots + t_{m'} = s$. Como $r, s \geq 1$, podemos supor que $t_1 \geq 1$ e $t_{m'} \geq 1$. Logo,

$$g = (X_1 Y_{m'} - X_{m'} Y_1) g_1 + Y_1 X_{m'} g_2,$$

onde

$$\begin{aligned}
g_1 &= X_1^{t_1-1} X_2^{t_2} \cdots X_m^{t_m} Y_{m+1}^{t_{m+1}} \cdots Y_{m'-1}^{t_{m'-1}} Y_{m'}^{t_{m'}-1} \text{ e} \\
g_2 &= X_1^{t_1-1} X_2^{t_2} \cdots X_m^{t_m} Y_{m+1}^{t_{m+1}} \cdots Y_{m'-1}^{t_{m'-1}} Y_{m'}^{t_{m'}-1} - Y_1^{t_1-1} Y_2^{t_2} \cdots Y_m^{t_m} X_{m+1}^{t_{m+1}} \cdots X_{m'-1}^{t_{m'-1}} X_{m'}^{t_{m'}-1}
\end{aligned}$$

Com efeito,

$$\begin{aligned}
&(X_1 Y_{m'} - X_{m'} Y_1) g_1 + Y_1 X_{m'} g_2 = \\
&(X_1 Y_{m'} - X_{m'} Y_1) X_1^{t_1-1} X_2^{t_2} \cdots X_m^{t_m} Y_{m+1}^{t_{m+1}} \cdots Y_{m'-1}^{t_{m'-1}} Y_{m'}^{t_{m'}-1} + \\
&+ Y_1 X_{m'} (X_1^{t_1-1} X_2^{t_2} \cdots X_m^{t_m} Y_{m+1}^{t_{m+1}} \cdots Y_{m'-1}^{q_{m'-1}} Y_{m'}^{t_{m'}-1} - Y_1^{t_1-1} Y_2^{t_2} \cdots Y_m^{t_m} X_{m+1}^{t_{m+1}} \cdots X_{m'-1}^{t_{m'-1}} X_{m'}^{t_{m'}-1}) \\
&= X_1^{t_1} \cdots X_m^{t_m} Y_{m+1}^{t_{m+1}} \cdots Y_{m'}^{t_{m'}} - X_1^{t_1-1} X_2^{t_2} \cdots X_m^{t_m} X_{m'} Y_1 Y_{m+1}^{t_{m+1}} \cdots Y_{m'-1}^{t_{m'-1}} Y_{m'}^{t_{m'}-1} + \\
&+ X_1^{t_1-1} X_2^{t_2} \cdots X_m^{t_m} X_{m'} Y_1 Y_{m+1}^{t_{m+1}} \cdots Y_{m'-1}^{t_{m'-1}} Y_{m'}^{t_{m'}-1} - Y_1^{t_1} \cdots Y_m^{t_m} X_{m+1}^{t_{m+1}} \cdots X_{m'}^{t_{m'}} \\
&= X_1^{t_1} \cdots X_m^{t_m} Y_{m+1}^{t_{m+1}} \cdots Y_{m'}^{t_{m'}} - Y_1^{t_1} \cdots Y_m^{t_m} X_{m+1}^{t_{m+1}} \cdots X_{m'}^{t_{m'}} = g.
\end{aligned}$$

Além disso,

$$0 = g(x;x) = (x_1 x_{m'} - x_{m'} x_1) g_1(x;x) + x_1 x_{m'} g_2(x;x) = x_1 x_{m'} g_2(x;x) \Rightarrow g_2(x;x) = 0,$$

pois x_1 e $x_{m'}$ são regulares.

Como g_2 é homogêneo nos X_i e nos Y_j, pela hipótese de indução no grau total, segue que $g_2 \in \mathfrak{p}$. Como $X_1Y_{m'} - X_{m'}Y_1 \in \mathfrak{p}$, segue que $g \in \mathfrak{p}$. □

Considerando então V a variedade definida no Lema anterior, o anel de coordenadas de V é $K[V] = K[X_1, \dots, X_n, Y_1, \dots, Y_n]/I_K(V)$. Por outro lado, já que $X_1, \dots, X_n$ formam uma $K[X_1, \dots, X_n]$-seqüência, então, pelo Lema III.1.8, $S((X_1, \dots, X_n)) = K[X_1, \dots, X_n, Y_1, \dots, Y_n]/\mathfrak{p}$, onde $\mathfrak{p}$ é o ideal do anel $K[X_1, \dots, X_n, Y_1, \dots, Y_n]$ gerado pelos determinantes $X_iY_j - X_jY_i, (i < j)$. Pelo Lema III.2.2, $K[V] = S((X_1, \dots, X_n))$, isto é, o anel de coordenadas de uma variedade V sobre K nada mais é do que a álgebra simétrica do ideal $(X_1, \dots, X_n)$ do anel polinomial $K[X_1, \dots, X_n]$.

Com isso, podemos calcular a dimensão da variedade afim V. Afirmamos que

$$dim(V) = dim(k[V]) = n + 1.$$

De fato, $dim(K[X_1, \dots, X_n, Y_1, \dots, Y_n]) = 2n$ e $ht(\mathfrak{p}) = n - 1$.[1] Logo, $dim(V) = dim(K[V]) = dimS((X_1, \dots, X_n)) = dim(K[X_1, \dots, X_n, Y_1, \dots, Y_n]) - ht(\mathfrak{p}) = 2n - (n-1) = n + 1$.

III.3 Contra-Exemplos

Vamos dar alguns exemplos mostrando que em geral a álgebra simétrica não é domínio.

1. Sejam K um corpo, $\mathfrak{p}$ um ideal primo homogêneo do anel polinomial $K[U_1, \dots, U_n]$ tal que $\mathfrak{p} \subset (U_1, \dots, U_n)^2, R = K[U_1, \dots, U_n]/\mathfrak{p} = K[u_1, \dots, u_n]$, onde $u_i = U_i + \mathfrak{p}, \mathfrak{a} = (u_1, \dots, u_n)$ ideal de R. Vamos mostrar que $Ker(\phi) \neq 0$ (onde ϕ é a aplicação de $S(\mathfrak{a})$ em $\mathcal{R}(\mathfrak{a})$ definida no início da Seção III.1).

   Temos que $S(\mathfrak{a}) = R[X_1, \dots, X_n]/\mathfrak{q}$, onde $\mathfrak{q} = (\sum_{i=1}^n b_iX_i; \sum_{i=1}^n b_iu_i = 0)$. Tomemos $f = \sum_{i=1}^n b_iX_i \in \mathfrak{q}$, considerando $\alpha : K[U_1, \dots, U_n] \to R$ o epimorfismo canônico, temos que $b_i = \alpha(f_i)$, com $f_i \in K[U_1, \dots, U_n]$. Logo,

   $$0 = \textstyle\sum_{i=1}^n b_iu_i = \sum_{i=1}^n \alpha(f_i)\alpha(U_i) = (\sum_{i=1}^n U_if_i) + \mathfrak{p}, \qquad \text{isto é,} \qquad \sum_{i=1}^n U_if_i \in \mathfrak{p}.$$

   Como $\mathfrak{p} \subset (U_1, \dots, U_n)^2$, então cada f_i é linear nas variáveis $U_j, \forall j$ e portanto $b_i = \alpha(f_i) \in \mathfrak{a}, \forall i$. Então, mostramos que $\mathfrak{q} \subset \mathfrak{a}[X_1, \dots, X_n]$.

   A cada polinômio $f = \sum a_{i_1,\dots,i_n} U_1^{i_1} \cdots U_n^{i_n} \in K[U_1, \dots, U_n]$, associamos o polinômio

   $$\tilde{f} = \sum \alpha(a_{i_1,\dots,i_n}) X_1^{i_1} \cdots X_n^{i_n} \in R[X_1, \dots, X_n].$$

   Seja $\tilde{\mathfrak{p}} = \{\tilde{f}; f \in \mathfrak{p}\}$.

[1] Como $\mathfrak{p}$ é gerado por $X_iY_j - X_jY_i, (i < j)$, então $\mathfrak{p} \subset (X_1, \dots, X_n)$ e logo $ht(\mathfrak{p}) \leq ht(X_1, \dots, X_n) = n$. Se $\mathfrak{p} = (X_1, \dots, X_n)$, então $X_iY_j \in \mathfrak{p}$, o que é absurdo, pois $X_iY_j \notin I_K(V) = \mathfrak{p}$. Logo, $\mathfrak{p} \subsetneq (X_1, \dots, X_n)$. Afirmamos que não existe um ideal primo $\mathfrak{q}$ tal que $\mathfrak{p} \subset (\mathfrak{p}, X_n) \subsetneq \mathfrak{q} \subsetneq (X_1, \dots, X_n)$. De fato, $X_iY_n - X_nY_i \in (\mathfrak{p}, X_n) \subset \mathfrak{q} \Rightarrow X_iY_n \in \mathfrak{q}$ (pois $X_n \in \mathfrak{q}$) $\Rightarrow X_i \in \mathfrak{q}, i = 1, \dots, n-1$ (pois $Y_n \notin (X_1, \dots, X_n) \Rightarrow Y_n \notin \mathfrak{q}$) $\Rightarrow \mathfrak{q} = (X_1, \dots, X_n)$. Portanto, o único ideal primo entre $\mathfrak{p}$ e $(X_1, \dots, X_n)$ é $(X_1, \dots, X_n)$. Como $\mathfrak{p}$ é primo, $ht(\mathfrak{p}) = n - 1$.

- $\tilde{\mathfrak{p}}$ é um ideal de $R[X_1, \ldots, X_n]$.
  - $\tilde{f}, \tilde{g} \in \tilde{\mathfrak{p}} \Rightarrow f, g \in \mathfrak{p} \Rightarrow f + g \in \mathfrak{p} \Rightarrow \widetilde{f+g} = \tilde{f} + \tilde{g} \in \tilde{\mathfrak{p}}$
  - $\tilde{f} \in \tilde{\mathfrak{p}}, g \in R[X_1, \ldots, X_n]$

$$\Rightarrow \begin{cases} \tilde{f} = \sum \alpha(a_{i_1,\ldots,i_n}) X_1^{i_1} \cdots X_n^{i_n}, & \text{onde } f = \sum a_{i_1,\ldots,i_n} U_1^{i_1} \cdots U_n^{i_n} \in \mathfrak{p} \\ g = \sum \rho'_{j_1,\ldots,j_n} X_1^{j_1} \cdots X_n^{j_n}, & \text{onde } \rho'_{j_1,\ldots,j_n} \in R \Rightarrow \rho'_{j_1,\ldots,j_n} = \alpha(\rho_{j_1,\ldots,j_n}) \end{cases}$$

$$\begin{aligned} \Rightarrow \tilde{f}g &= (\sum \alpha(a_{i_1,\ldots,i_n}) X_1^{i_1} \cdots X_n^{i_n})(\sum \alpha(\rho_{j_1,\ldots,j_n}) X_1^{j_1} \cdots X_n^{j_n}) \\ &= \sum_{i,j} \alpha(a_{i_1,\ldots,i_n}) \alpha(\rho_{j_1,\ldots,j_n}) X_1^{i_1+j_1} \cdots X_n^{i_n+j_n} \\ &= \sum_{i,j} \alpha(a_{i_1,\ldots,i_n} . \rho_{j_1,\ldots,j_n}) X_1^{i_1+j_1} \cdots X_n^{i_n+j_n} = \tilde{h} \end{aligned}$$

onde

$$h = \sum_{i,j} a_{i_1,\ldots,i_n} \rho_{j_1,\ldots,j_n} U_1^{i_1+j_1} \cdots U_n^{i_n+j_n} = (\sum_i a_{i_1,\ldots,i_n} U_1^{i_1} \cdots U_n^{i_n})(\sum_j \rho_{j_1,\ldots,j_n} U_1^{j_1} \cdots U_n^{j_n})$$

isto é, $h = f.g' \in \mathfrak{p}$, pois $f \in \mathfrak{p}$. Logo, $\tilde{f}g = \tilde{h} \in \tilde{\mathfrak{p}}$.

- $\tilde{\mathfrak{p}} \cap \mathfrak{a}[X_1, \ldots, X_n] = (0)$.

Temos a seqüência exata

$$\begin{array}{ccccccccc} 0 & \to & (U_1, \ldots, U_n) & \longrightarrow & K[U_1, \ldots, U_n] & \longrightarrow & K & \longrightarrow & 0 \\ & & & & f(U_1, \ldots, U_n) & \mapsto & f(0, \ldots, 0) & & \end{array}$$

Tomando o quociente dessa seqüência por $\mathfrak{p}$, obtemos a seqüência exata

$$(0) \to \mathfrak{a} \to R \xrightarrow{\psi} K \to (0)$$

Temos $K \xrightarrow{\alpha|_K} R \xrightarrow{\psi} K$ e essa composição resulta na aplicação identidade. Assim,

$\tilde{f} \in \tilde{\mathfrak{p}} \cap \mathfrak{a}[X_1, \ldots, X_n] \Rightarrow \tilde{f} = \sum \alpha(a_{i_1,\ldots,i_n}) X_1^{i_1} \cdots X_n^{i_n}$, com $\alpha(a_{i_1,\ldots,i_n}) \in \mathfrak{a} = Ker(\psi) \Rightarrow$ $a_{i_1,\ldots,i_n} = \psi(\alpha(a_{i_1,\ldots,i_n})) = 0, \forall (i_1, \ldots, i_n) \Rightarrow \tilde{f} = 0$.

Considere o homomorfismo $\phi : S(\mathfrak{a}) \to \mathcal{R}(\mathfrak{a})$ definido por $X_i + \mathfrak{q} \mapsto u_i X$.

Seja $f = \sum b_{i_1,\ldots,i_n} U_1^{i_1} \cdots U_n^{i_n} \in \mathfrak{p} - \{0\}$ homogêneo de grau m, isto é, $i_1 + \cdots + i_n = m$. Como $f \in \mathfrak{p} = Ker(\alpha)$, temos $0 = \alpha(f) = \sum \alpha(b_{i_1,\ldots,i_n}) u_1^{i_1} \cdots u_n^{i_n}$. Por outro lado, $\tilde{f} = \sum \alpha(b_{i_1,\ldots,i_n}) X_1^{i_1} \cdots X_n^{i_n} \neq 0$. Como $\tilde{\mathfrak{p}} \cap \mathfrak{a}[X_1, \ldots, X_n] = (0)$ e $\tilde{f} \in \tilde{\mathfrak{p}}$, então $\tilde{f} \notin \mathfrak{a}[X_1, \ldots, X_n]$, logo $\tilde{f} \notin \mathfrak{q}$ (pois $\mathfrak{q} \subset \mathfrak{a}[X_1, \ldots, X_n]$). Assim, $\tilde{f} \pmod{\mathfrak{q}} \neq 0$ e

$$\phi(\tilde{f} \pmod{\mathfrak{q}}) = \sum \alpha(b_{i_1,\ldots,i_n})(u_1X)^{i_1} \cdots (u_nX)^{i_n} = (\sum \alpha(b_{i_1,\ldots,i_n}) u_1^{i_1} \cdots u_n^{i_n}) X^m = \alpha(f) X^m = 0.$$

Logo, ϕ não é injetiva.

2. Sejam K um corpo, $R = K[u, v]$ um anel com a relação $u^3 + u^2 + v^2 = 0$ e $\mathfrak{p} = (u, v)$ ideal de R. Vamos mostrar que $S(\mathfrak{p})$ não é domínio.

   Temos $S(\mathfrak{p}) = R[X, Y]/\mathfrak{q}$, onde $\mathfrak{q} = (aX + bY; au + bv = 0)$. Logo, $vX - uY, u(u+1)X + vY \in \mathfrak{q}$, o que implica que $[u(u+1)X + vY]X - (vX - uY)Y = u((u+1)X^2 + Y^2) \in \mathfrak{q}$. Temos $\mathfrak{q} \subset \mathfrak{p}[X, Y]$.[2] Logo, como $u + 1 \notin \mathfrak{p}$, segue que $(u+1)X^2 + Y^2 \notin \mathfrak{q}$ e pela definição, u é um elemento de torção de $S(\mathfrak{p})$. Analogamente, mostramos que v é um elemento de torção de $S(\mathfrak{p})$. Por outro lado, como $R = K[U, V]/(U^3 + U^2 + V^2)$ e $U^3 + U^2 + V^2$ é irredutível[3], temos que R é um domínio. Observemos que $R = K[U, V]/(U^3 + U^2 + V^2)$ é o anel de coordenadas da variedade definida pelo ideal $(U^3 + U^2 + V^2)$.

3. Mais geralmente, sejam K um corpo, V uma variedade, $K[V]$ seu anel de coordenadas, $p \in V$ um ponto e $\mathfrak{p} = I_K(p) = \{f; f(p) = 0\}$ um ideal primo de $K[V] = R$. É fácil ver que, se o ponto p não é regular, então $S(\mathfrak{p})$ não é domínio. Para isso, vamos usar o Teorema III.4.3 da próxima seção.

   De fato, se $S(\mathfrak{p})$ é domínio, como $S(\mathfrak{p})_{\mathfrak{p}} = S(\mathfrak{p}R_{\mathfrak{p}})$, temos que $S(\mathfrak{p}R_{\mathfrak{p}})$ é domínio, e pelo Teorema III.4.3, $R_{\mathfrak{p}}$ é regular, isto é, o ponto p é regular.

III.4 Uma Caracterização dos Anéis Locais Regulares

Um caso particular da Definição I.8.11 é a seguinte:

Definição III.4.1 *Sejam $(R, \mathfrak{m})$ um anel local, $k = R/\mathfrak{m}$ seu corpo residual e $a_1, \ldots, a_n$ um sistema minimal de geradores de $\mathfrak{m}$. Dizemos que $c_1, \ldots, c_t \in \mathfrak{m}$ são* **analiticamente independentes** *se para cada polinômio homogêneo f de $R[X_1, \ldots, X_t]$ tal que $f(c_1, \ldots, c_t) = 0$, todos os coeficientes de f estão no ideal $\mathfrak{m}$, isto é, $f \in \mathfrak{m}[X_1, \ldots, X_t]$.*

Observação III.4.2 Do Capítulo I, temos

1. $(R, \mathfrak{m})$ é um anel local regular se, e só se, $a_1, \ldots, a_n$ são analiticamente independentes.

2. Se R é um anel local regular, então $a_1, \ldots, a_n$ formam uma R-seqüência.

Teorema III.4.3 *O anel R é local regular se, e só se, a álgebra simétrica $S(\mathfrak{m})$ do R-módulo $\mathfrak{m}$ é domínio.*

Dem. : Se R é local regular, então $a_1, \ldots, a_n$ é uma R-seqüência e pelo Teorema III.1.9, segue que $S(\mathfrak{m}) \cong \mathcal{R}(\mathfrak{m})$; logo, é domínio (pois já sabemos que R, sendo local regular, é domínio).

[2] Como $R = K[U, V]/(U^3 + U^2 + V^2)$, existe um epimorfismo canônico $\alpha : K[U, V] \to R$. Temos que $\mathfrak{p} = (aX + bY; au + bv = 0)$. Logo, $a = \alpha(a'), b = \alpha(b')$ e $0 = au + bv = \alpha(a')\alpha(U) + \alpha(b')\alpha(V) = a'U + b'V + (U^3 + U^2 + V^2)$. Assim, $a'U + b'V \in (U^3 + U^2 + V^2)$ e como $U, V \notin (U^3 + U^2 + V^2)$, segue que a' e b' não têm termo constante, isto é, $a = \alpha(a'), b = \alpha(b') \in \mathfrak{p} = (u, v)$. Portanto, $\mathfrak{q} \subset \mathfrak{p}[X, Y]$.

[3] Como $U^3 + U^2 + V^2 = V^2 + U^2(U + 1)$ e $U + 1$ é um elemento irredutível de $K[U]$, pelo Critério de Eisenstein segue que $U^3 + U^2 + V^2$ é irredutível em $K[U, V]$.

Suponhamos agora que a álgebra $S(\mathfrak{m})$ é domínio. Então, $S(\mathfrak{m}) = R[X_1, \dots, X_n]/\mathfrak{q}$, onde $\mathfrak{q} = (\sum_{i=1}^n b_i X_i; \sum_{i=1}^n b_i a_i = 0)$. Logo, $\mathfrak{q} \subset \mathfrak{m}[X_1, \dots, X_n]$, pois caso contrário, existiria $b_i \notin \mathfrak{m}$, ou seja, b_i seria uma unidade de R e como $b_i a_i = -\sum_{j \neq i} b_j a_j$, teríamos $a_i \in (a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n)$, o que é absurdo, pois $a_1, \dots, a_n$ é minimal. Agora, como R e $S(\mathfrak{m})$ são domínios, segue, pelas Proposições III.1.4 e III.1.7, que para qualquer polinômio homogêneo $f \in R[X_1, \dots, X_n]$, vale $f \in \mathfrak{q} \Leftrightarrow f(a_1, \dots, a_n) = 0$. Assim, $a_1, \dots, a_n$ são analiticamente independentes e portanto R é local regular. $\square$

Sejam R um anel Noetheriano e $\mathfrak{p}$ um ideal primo de R. Como $S(\mathfrak{p})_{\mathfrak{p}} = S(\mathfrak{p} R_{\mathfrak{p}})$, se $S(\mathfrak{p})$ é um domínio, segue pelo Teorema III.4.3 que $R_{\mathfrak{p}}$ é local regular. A recíproca dessa afirmação é falsa, em geral. Para ver um contra-exemplo, vamos demonstrar a seguinte proposição:

Proposição III.4.4 *Sejam K um corpo, $R = K[X_1, \dots, X_n]$, $\mathfrak{p}$ um ideal homogêneo de R e $a_1, \dots, a_m$ um sistema minimal de geradores homogêneos de $\mathfrak{p}$. Se a álgebra simétrica $S(\mathfrak{p})$ é um domínio, então $a_1, \dots, a_m$ são algebricamente independentes sobre K.*

Dem. : Temos que $S(\mathfrak{p}) = R[Y_1, \dots, Y_m]/(\sum_{i=1}^m b_i Y_i; \sum_{i=1}^m b_i a_i = 0)$.

Ordenando os a_i's pelos graus, $1 < gr(a_1) \leq \dots \leq gr(a_m)$, teremos $\mathfrak{q} \subset (X_1, \dots, X_n)[Y_1, \dots, Y_m]$. De fato, supondo que $b_j \notin (X_1, \dots, X_n)R$, para algum $1 \leq j \leq m$, seja $s \geq j$ o maior inteiro tal que $gr(a_j) = gr(a_s)$. A relação $\sum_{i=1}^m b_i a_i = 0$ nos dá $\sum_{i=1}^s c_i a_i = 0$, onde $c_i \in R$, para $i = 1, \dots, j-1$ e $c_i \in K$, para $i = j, j+1, \dots, s$.[4] Logo, $a_j = -\sum_{i \neq j, i=1}^s (c_i/c_j) a_i$, pois $c_j \neq 0$ e isso contradiz a minimalidade de $a_1, \dots, a_n$.

[4] Escreva

$$b_j = \alpha_0^{(j)} + h^{(j)}(X_1, \dots, X_n), \text{com } \alpha_0^{(j)} \neq 0, gr(h^{(j)}) \geq 1$$
$$b_l = \alpha_0^{(l)} + h^{(l)}(X_1, \dots, X_n), \text{com } \alpha_0^{(l)} \in K, gr(h^{(l)}) \geq 1, l = j+1, \dots, s$$

Como $b_1 a_1 + \dots + b_{j-1} a_{j-1} + b_j a_j + \dots + b_s a_s + b_{s+1} a_{s+1} + \dots + b_m a_m = 0$, substituindo as expressões acima, teremos:

$$b_1 a_1 + \dots + b_{j-1} a_{j-1} + \underbrace{\alpha_0^{(j)} a_j + \alpha_0^{(j+1)} a_{j+1} + \dots + \alpha_0^{(s)} a_s}_{\text{tem grau } gr(a_j)} + \underbrace{a_j h^{(j)} + a_{j+1} h^{(j+1)} + \dots + a_s h^{(s)} + \sum_{i=s+1}^m b_i a_i}_{\text{tem grau } > gr(a_j)} = 0$$

Agora escreva
$b_i = b_0^{(i)} + b_1^{(i)} + \dots + b_{gr(a_j)-gr(a_i)}^{(i)} + h^{(i)}, i = 1, \dots, j-1$, onde $b_k^{(i)}$ é a componente homogênea de grau k de b_i e $gr(h^{(i)}) > gr(a_j) - gr(a_i)$. Logo,

$$b_i a_i = \underbrace{b_0^{(i)} a_i + b_1^{(i)} a_i + \dots}_{\text{tem grau } < gr(a_j)} + \underbrace{b_{gr(a_j)-gr(a_i)}^{(i)} a_i}_{\text{tem grau } = gr(a_j)} + \underbrace{a_i h^{(i)}}_{\text{tem grau } > gr(a_j)}, i = 1, \dots, j-1$$

Analisando somente a componente homogênea de grau $gr(a_j)$ da soma, teremos

$$\alpha_0^{(j)} a_j + \alpha_0^{(j+1)} a_{j+1} + \dots + \alpha_0^{(s)} a_s + b_{gr(a_j)-gr(a_1)}^{(1)} a_1 + \dots + b_{gr(a_j)-gr(a_{j-1})}^{(j-1)} a_{j-1} = 0$$

Então tomemos $c_i = \begin{cases} \alpha_0^{(i)} & \in K, \quad \text{para } i = j, \dots, s \\ b_{gr(a_j)-gr(a_i)}^{(i)} & \in R, \quad \text{para } i = 1, \dots, j-1 \end{cases}$ Temos que $c_j = \alpha_0^{(j)} \neq 0$ e $\sum_{i=1}^s c_i a_i = 0$.

Como $S(\mathfrak{p})$ é domínio, temos, pelas proposições III.1.4 e III.1.7, que para qualquer $f \in R[Y_1, \dots, Y_m]$ homogêneo, $f \in \mathfrak{q} \Leftrightarrow f(a_1, \dots, a_n) = 0$. Assim, para cada polinômio homogêneo $f \in R[Y_1, \dots, Y_m]$ tal que $f(a_1, \dots, a_n) = 0$, temos que $f \in (X_1, \dots, X_n)[Y_1, \dots, Y_m]$.

Suponhamos que exista um polinômio não-nulo $f = \sum c_{i_1,\dots,i_m} Y_1^{i_1} \cdots, Y_m^{i_m} \in K[Y_1, \dots, Y_m]$ tal que $f(a_1, \dots, a_m) = 0$. Seja $(j_1, \dots, j_m)$ uma m-upla entre as $(i_1, \dots, i_m)$ tal que $j_1 + \cdots + j_m$ tenha o menor valor possível e consideremos o polinômio homogêneo de grau $j_1 + \cdots + j_m$:

$$g = c_{j_1,\dots,j_m} Y_1^{j_1} \cdots Y_m^{j_m} + \sum c_{i_1,\dots,i_m} a_s^{i_1+\cdots+i_s-(j_1+\cdots+j_m)} a_{s+1}^{i_{s+1}} \cdots a_m^{i_m} Y_1^{i_1} \cdots Y_{s-1}^{i_{s-1}} Y_s^{(j_1+\cdots+j_m)-(i_1+\cdots+i_{s-1})}$$

(onde a soma é feita nas m-uplas $(i_1, \dots, i_m)$ tais que $(i_1, \dots, i_m) \neq (j_1, \dots, j_m)$ e $i_1 + \cdots + i_m \geq j_1 + \cdots + j_m$) e onde $i_1 + \cdots + i_s$ é o menor entre os inteiros $i_1, i_1 + i_2, i_1 + i_2 + i_3, \dots, i_1 + \cdots + i_m$ que são maiores que $j_1 + \cdots + j_m$. Temos

$$\begin{aligned}
g(a_1, \dots, a_m) &= \\
&= c_{j_1,\dots,j_m} a_1^{j_1} \cdots a_m^{j_m} + \sum c_{i_1,\dots,i_m} a_s^{i_1+\cdots+i_s-(j_1+\cdots+j_m)} a_{s+1}^{i_{s+1}} \cdots a_m^{i_m} a_1^{i_1} \cdots a_{s-1}^{i_{s-1}} a_s^{(j_1+\cdots+j_m)-(i_1+\cdots+i_{s-1})} \\
&= c_{j_1,\dots,j_m} a_1^{j_1} \cdots a_m^{j_m} + \sum c_{i_1,\dots,i_m} a_1^{i_1} \cdots a_{s-1}^{i_{s-1}} a_s^{i_s} a_{s+1}^{i_{s+1}} \cdots a_m^{i_m} \\
&= f(a_1, \dots, a_m) = 0
\end{aligned}$$

Logo, $g \in \mathfrak{q}$ e todos os coeficientes de g estão em $(X_1, \dots, X_n)R$. Isso é absurdo, pois o coeficiente de $Y_1^{j_1} \dots Y_m^{j_m}$ é $c_{j_1,\dots,j_m}$, isto é, o termo $Y_1^{j_1} \dots Y_m^{j_m}$ não aparece na segunda parcela da soma de g. Caso contrário, teríamos $i_1 = j_1, \dots, i_{s-1} = j_{s-1}, i_s = (j_1 + \cdots + j_m) - (i_1 + \cdots + i_{s-1}) = j_s + \cdots + j_m, j_{s+1} = 0, \dots, j_m = 0$. Assim, $i_k = j_k, \forall k$, o que é absurdo. Portanto, teríamos que $c_{j_1,\dots,j_m} \in (X_1, \dots, X_n)$, o que também é absurdo, pois $c_{j_1,\dots,j_m} \in K$.

Portanto, $a_1, \dots, a_m$ são algebricamente independentes sobre K. □

Exemplo III.4.5 Sejam K um corpo, $R = K[X_1, \dots, X_n]$ e $\mathfrak{p} = (a_1, \dots, a_m)R$ um ideal primo homogêneo de R com $m > n$ geradores, cuja existência Macaulay([14]) demonstrou. Então $a_1, \dots, a_m$ não são algebricamente independentes sobre K, pois como $X_1, \dots, X_n$ é uma base transcendente de R sobre K, qualquer conjunto algebricamente independente sobre K tem no máximo n elementos. Pela Proposição III.4.4, $S(\mathfrak{p})$ não é domínio. No entanto, $R_{\mathfrak{p}}$ é um anel local regular, pois R é um anel polinomial.

Capítulo IV

As Álgebras Simétrica e de Rees de um Ideal Gerado por uma d-seqüência

Como vimos no capítulo anterior, ideais gerados por R-seqüências são de tipo linear. Neste último capítulo, veremos o conceito de d-seqüências, que generaliza o conceito de R-seqüências e mostraremos que ideais gerados por d-seqüências também são de tipo linear. Daremos exemplos desse fato e finalmente, exibiremos um contra-exemplo da recíproca, ou seja, exibiremos um ideal que é de tipo linear, mas não é gerado por uma d-seqüência.

IV.1 d-seqüências

Definição IV.1.1 *Uma seqüência de elementos $x_1, \ldots, x_n$ em um anel comutativo R é dita uma* **d-seqüência** *se*

i) $x_i \notin (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n), \forall i = 1, \ldots, n$.

ii) *Se $\{i_1, \ldots, i_j\} \subset \{1, \ldots, n\}$ (possivelmente vazio) e $k, m \in \{1, \ldots, n\} - \{i_1, \ldots, i_j\}$, então $((x_{i_1}, \ldots, x_{i_j}) : x_k x_m) = ((x_{i_1}, \ldots, x_{i_j}) : x_k)$.*

Observação IV.1.2 1. ii) é equivalente a valer iii) para qualquer ordem de $x_1, \ldots, x_n$, onde

iii) $\forall k \geq i+1$ e $\forall i \geq 1$, vale: $((x_1, \ldots, x_i) : x_{i+1}x_k) = ((x_1, \ldots, x_i) : x_k)$.

2. A condição iii) equivale a dizer que x_{i+1} não é divisor de zero módulo o ideal $((x_1, \ldots, x_i) : x_k)$.

   De fato, se iii) vale, então suponhamos que $x_{i+1}r \in ((x_1, \ldots, x_i) : x_k)$. Logo, $x_{i+1}rx_k \in (x_1, \ldots, x_i)$, isto é, $r \in ((x_1, \ldots, x_i) : x_{i+1}x_k) = ((x_1, \ldots, x_i) : x_k)$. Então x_{i+1} não é divisor de zero módulo $((x_1, \ldots, x_i) : x_k)$.

   Reciprocamente, se x_{i+1} não é divisor de zero módulo $((x_1, \ldots, x_i) : x_k)$, então seja $r \in ((x_1, \ldots, x_i) : x_{i+1}x_k)$. Logo, $rx_{i+1}x_k \in (x_1, \ldots, x_i)$, isto é, $rx_{i+1} \in ((x_1, \ldots, x_i) : x_k)$. Pela hipótese, temos que $r \in ((x_1, \ldots, x_i) : x_k)$. Como já sabemos que $((x_1, \ldots, x_i) : x_k) \subset ((x_1, \ldots, x_i) : x_{i+1}x_k)$, segue a igualdade.

3. Se $x_1, \ldots, x_n$ formam uma d-seqüência, então as imagens de $x_i, \ldots, x_n$ no anel $R/(x_1, \ldots, x_{i-1})$ formam uma d-seqüência.

   - Temos que $x_j \notin (x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n)$. Logo, no anel $R/(x_1, \ldots, x_{i-1})$, $\overline{x_j} \notin (\overline{x_1}, \ldots, \overline{x_{j-1}}, \overline{x_{j+1}}, \ldots, \overline{x_n}) = (\overline{x_i}, \ldots, \overline{x_{j-1}}, \overline{x_{j+1}}, \ldots, \overline{x_n}), \forall j = i, \ldots, n$.
   - Temos que $((x_1, \ldots, x_j) : x_{j+1}x_k) = ((x_1, \ldots, x_j) : x_k), \forall k \geq j+1, \forall j \geq 1$. Basta mostrar que $((\overline{x_i}, \ldots, \overline{x_j}) : \overline{x_{j+1}x_k}) \subset ((\overline{x_i}, \ldots, \overline{x_j}) : \overline{x_k})$, pois a outra inclusão é óbvia. Então
   $\overline{r} \in ((\overline{x_i}, \ldots, \overline{x_j}) : \overline{x_{j+1}x_k}) \Rightarrow \overline{rx_{j+1}x_k} \in (\overline{x_i}, \ldots, \overline{x_j}) \Rightarrow rx_{j+1}x_k + s \in (x_i, \ldots, x_j), s \in (x_1, \ldots, x_{i-1}) \Rightarrow rx_{j+1}x_k \in (x_1, \ldots, x_j) \Rightarrow r \in ((x_1, \ldots, x_j) : x_{j+1}x_k) = ((x_1, \ldots, x_j) : x_k)$ $\Rightarrow rx_k \in (x_1, \ldots, x_j) \Rightarrow rx_k + s' \in (x_i, \ldots, x_j), s' \in (x_1, \ldots, x_{i-1}) \Rightarrow \overline{rx_k} \in (\overline{x_i}, \ldots, \overline{x_j}) \Rightarrow$ $\overline{r} \in ((\overline{x_i}, \ldots, \overline{x_j}) : \overline{x_k})$.

   Portanto, $\overline{x_i}, \ldots, \overline{x_j}$ é uma d-seqüência.

4. Um único elemento x é uma d-seqüência se, e só se, $(0 : x) = (0 : x^2)$.

5. Qualquer R-seqüência que, permutada, resulta numa outra R-seqüência é uma d-seqüência.

   Seja $x_1, \ldots, x_n$ uma R-seqüência. Como podemos permutá-la, restando ainda uma R-seqüência, temos que $x_i \notin (x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$, pois podemos permutá-la considerando $x_i = x_n$ e como x_n não é divisor de zero módulo $(x_1, \ldots, x_{n-1})$, temos que $x_n \notin (x_1, \ldots, x_{n-1})$. Além disso, se $rx_{i+1} \in ((x_1, \ldots, x_i) : x_k)$, então $rx_{i+1}x_k \in (x_1, \ldots, x_i)$. Como x_{i+1} não é divisor de zero módulo o ideal $(x_1, \ldots, x_i)$, segue que $rx_k \in (x_1, \ldots, x_i)$, isto é, $r \in ((x_1, \ldots, x_i) : x_k)$. Assim, x_{i+1} não é divisor de zero módulo $((x_1, \ldots, x_i) : x_k)$. Pela Observação 1, segue que $x_1, \ldots, x_n$ é uma d-seqüência.

6. Duas d-seqüências maximais em um ideal I não precisam ter o mesmo comprimento. Por exemplo, considere o ideal (X) no anel polinomial $K[X, Y, Z]$. Certamente, X é uma d-seqüência maximal em (X), pois $f \in (0 : X^2) \Rightarrow X^2 f = 0 \Rightarrow f = 0 \Rightarrow Xf = 0 \Rightarrow f \in (0 : X)$, logo $(0 : X^2) = (0 : X)$. Entretanto, XY, XZ também formam uma d-seqüência no ideal (X), pois $(XY : XZ) = (Y)$:

$$f \in (XY : XZ) \Rightarrow fXZ = XYg \Rightarrow Y | fZ \Rightarrow Y | f \Rightarrow f \in (Y)$$

$$f \in (Y) \Rightarrow f = Yg \Rightarrow fXZ = XYZg \in (XY) \Rightarrow f \in (XY : XZ)$$

   E XZ não é divisor de zero módulo (Y).

Exemplo IV.1.3 Seja $X = (x_{ij})$ uma $n \times (n+1)$ matriz de indeterminadas sobre k, onde $k = \mathbb{Z}$ ou é um corpo. Seja μ_i o determinante da matriz formada desconsiderando a $(n+2-i)$-ésima coluna de X, chamado de menor maximal de X. Seja $R = k[x_{ij}]$. Então $\mu_1, \ldots, \mu_{n+1}$ formam uma d-seqüência.

Com efeito, como mudanças na ordem dos menores maximais $\mu_1, \ldots, \mu_{n+1}$ significam rearranjos nas colunas de X, que nada afetam, pois as entradas são variáveis, basta mostrar que $\mu_1, \ldots, \mu_{n+1}$

formam uma d-seqüência nessa ordem, isto é, $((\mu_1,\ldots,\mu_{i-1}):\mu_i\mu_k)=((\mu_1,\ldots,\mu_{i-1}):\mu_i), \forall k\geq i$, ou, pela Observação 2, que $\mu_i,\ldots,\mu_{n+1}$ não são divisores de zero módulo o ideal $((\mu_1,\ldots,\mu_{i-1}):\mu_i)$.

Seja Y a $n\times(n+2-i)$ matriz obtida desconsiderando as últimas $i-1$ colunas de X (aqui podemos supor $i\geq 2$, pois para $i=1$ temos que $\mu_1,\ldots,\mu_{n+1}$ não são divisores de zero de $(0:\mu_1)=0$, já que μ_1 é irredutível[1]). Seja λ qualquer menor maximal de Y.

Afirmação: $\lambda\in((\mu_1,\ldots,\mu_{i-1}):\mu_i)$.

Temos que λ é fixado escolhendo $n+2-i$ linhas de X. Seja σ uma tal escolha. Expandindo λ sobre a $(n+2-i)$-ésima coluna, obtemos

$$\lambda=\sum_{j\in\sigma}(-1)^{n+2-i+j}x_{j(n+2-i)}\lambda_j, \tag{IV.1}$$

onde os λ_j são menores de ordem $n+1-i$. Se $m\neq n+1,n,\ldots,n+2-i$, então $\sum_{j\in\sigma}(-1)^{n+2-i+j}x_{jm}\lambda_j=(-1)^{n+2-i}\sum_{j\in\sigma}(-1)^{j+m}x_{jm}\lambda_j=0$[2] e, portanto,

$$\sum_{j\in\sigma}(-1)^{j+m}x_{jm}\lambda_j=0. \tag{IV.2}$$

Também sabemos que $\sum_{j=1}^{n+1}(-1)^{1+j}x_{rj}\mu_{n+2-j}=0$,[3] logo

$$\sum_{j=1}^{n+1}(-1)^{r+j}x_{rj}\mu_{n+2-j}=0. \tag{IV.3}$$

Multiplicando a equação IV.3 por λ_s, onde $r=s$, temos $\sum_{j=1}^{n+1}(-1)^{s+j}\lambda_s x_{sj}\mu_{n+2-j}=0$ e somando para $s\in\sigma$, obtemos $\sum_{s\in\sigma}\lambda_s\sum_{j=1}^{n+1}(-1)^{s+j}x_{sj}\mu_{n+2-j}=0$, logo,

$$\sum_{j=1}^{n+1}\mu_{n+2-j}\Big(\sum_{s\in\sigma}(-1)^{s+j}\lambda_s x_{sj}\Big)=0. \tag{IV.4}$$

Pela equação IV.2, a soma de dentro é zero, para $j\neq n+1,n,\ldots,n+2-i$. Para $j=n+2-i$, $\sum_{s\in\sigma}(-1)^{s+j}\lambda_s x_{sj}=\lambda$. Assim, a equação IV.4 se torna

$$\mu_i\lambda+\mu_{i-1}\Big(\sum_{s\in\sigma}(-1)^{s+n+3-i}\lambda_s x_{s(n+3-i)}\Big)+\cdots+\mu_1\Big(\sum_{s\in\sigma}(-1)^{s+n+1}\lambda_s x_{s(n+1)}\Big)=0.$$

Assim, $\lambda\in((\mu_1,\ldots,\mu_{i-1}):\mu_i)$, como afirmamos.

Seja J o ideal gerado pelos menores maximais de Y.

Notemos que $J\supset(\mu_1,\ldots,\mu_{i-1})$. De fato, seja $k\in\{1,\ldots,i-1\}$. Calculando μ_k através da sua expansão pela última coluna da matriz que define μ_k, vemos que μ_k é uma combinação linear de subdeterminantes de ordem $n-1$. Fazendo a expansão de cada um deles sobre a última coluna

[1] μ_1 é um polinômio em $k[x_{ij}; j\neq n+1]$, linear em cada variável, logo é irredutível.

[2] Na matriz que tomamos para calcular λ, trocando sua $(n+2-i)$-ésima coluna pela m-ésima coluna de X, obtemos uma matriz que tem duas colunas repetidas, logo seu determinante – que, calculado sobre a coluna trocada, é $\sum_{j\in\sigma}(-1)^{n+2-i+j}x_{jm}\lambda_j$ – é zero.

[3] Basta considerar a $(n+1)\times(n+1)$ matriz que tem a primeira linha sendo a r-ésima linha de X e as outras linhas sendo todas as linhas de X. Essa matriz, por ter duas linhas repetidas, tem determinante nulo e se o calcularmos pela sua primeira linha, teremos a expressão dada.

de suas respectivas matrizes, e assim sucessivamente, vemos que μ_k é uma combinação linear dos menores maximais de Y.

Mostramos na afirmação acima que $J \subset ((\mu_1, \ldots, \mu_{i-1}) : \mu_i)$.

Notemos também que $\mu_k \not\subset J, \forall k = i, i+1, \ldots, n+1$. Com efeito, como μ_i é o determinante da matriz obtida retirando a $(n+2-i)$-ésima coluna de X, então em μ_i não aparecem as variáveis $x_{j(n+2-i)}$, para $j = 1, \ldots, n$, isto é, se pusermos $x_{j(n+2-i)} = 0, \forall j = 1, \ldots, n$, então μ_i não se altera. Se, por absurdo, $\mu_i \in J$, então $\mu_i = \sum h_k \Delta_k$, onde Δ_k é menor maximal de Y. Para calcular Δ_k, desenvolvamos em relação à coluna $n+2-i$ de Y. Então $\Delta_k \in (x_{1(n+2-i)}, \ldots, x_{n(n+2-i)})$, ou seja, $\Delta_k = 0$, se $x_{j(n+2-i)} = 0$, para $j = 1, \ldots, n$. Nesse caso, teríamos $\mu_i = 0$, o que contradiz o que vimos acima. Para $k \geq i$, vale a mesma coisa, pois a coluna $n+2-k(\leq n+2-i)$ é uma coluna de Y. Como J é um ideal primo ([8]) e $\mu_i \notin J$, então $\mu_i((\mu_1, \ldots, \mu_{i-1}) : \mu_i) \subset (\mu_1, \ldots, \mu_{i-1}) \subset J$ implica que $((\mu_1, \ldots, \mu_{i-1}) : \mu_i) \subset J$ e logo $J = ((\mu_1, \ldots, \mu_{i-1}) : \mu_i)$.

Como J é um ideal primo e $\mu_k \notin J, \forall k = i, i+1, \ldots, n+1$, então μ_k não é divisor de zero módulo J, isto é, $\mu_1, \ldots, \mu_{n+1}$ formam uma d-seqüência.

IV.2 Generalidades sobre d-seqüências

Os resultados desta Seção serão utilizados na Seção IV.3 para demonstrar o principal Teorema desse trabalho, que estabelece que ideais gerados por d-seqüências são de tipo linear.

Definição IV.2.1 *Uma seqüência de elementos $a_1, \ldots, a_n$ em um anel R é uma* **seqüência regular relativa** *se $((a_1, \ldots, a_i)I : a_{i+1}) \cap (a_1, \ldots, a_n) = (a_1, \ldots, a_i)$, onde $I = (a_1, \ldots, a_n)$. Tal seqüência é dita* **incondicionada** *se qualquer permutação dela é uma seqüência regular relativa.*

Vamos agora estudar algumas propriedades das d-seqüências.

Proposição IV.2.2 *Qualquer d-seqüência $x_1, \ldots, x_n$ é uma seqüência regular relativa.*

Dem. : Basta mostrar que se $y_1, \ldots, y_d$ é uma d-seqüência, então $(0 : y_1) \cap (y_1, \ldots, y_d) = (0)$. De fato, $((x_1, \ldots, x_i)I : x_{i+1}) \cap I = (x_1, \ldots, x_i) \Leftrightarrow (0 : \overline{x_{i+1}}) \cap (\overline{x_{i+1}}, \ldots, \overline{x_n}) = (0) \Leftrightarrow (0 : y_1) \cap (y_1, \ldots, y_d) = (0)$, onde $I = (x_1, \ldots, x_n)$, e se $x_1, \ldots, x_n$ é uma d-seqüência em R, então $y_1 = \overline{x_{i+1}}, \ldots, y_d = \overline{x_n}$ é uma d-seqüência em $R/(x_1, \ldots, x_i)$.

Vamos mostrar que se $y_1, \ldots, y_d$ é uma d-seqüência, então $(0 : y_1) \cap (y_1, \ldots, y_d) = (0)$ por indução em d.

- Se $d = 1$, $(0 : y_1) = (0 : y_1^2)$ mostra que $(0 : y_1) \cap (y_1) = (0)$:

$$x \in (0 : y_1) \cap (y_1) \Rightarrow x = y_1 r \in (0 : y_1) \Rightarrow y_1^2 r = 0 \Rightarrow r \in (0 : y_1^2) = (0 : y_1) \Rightarrow x = y_1 r = 0.$$

- Suponhamos $d > 1$ e a hipótese de indução. Seja $\sum_{i=1}^d r_i y_i \in (0 : y_1) \subset (0 : y_d y_1) = (0 : y_d)$. Logo, $r_d y_d^2 \in (y_1, \ldots, y_{d-1})$ e como $y_1, \ldots, y_d$ formam uma d-seqüência, segue que $r_d y_d \in (y_1, \ldots, y_{d-1})$, pois $((y_1, \ldots, y_{d-1}) : y_d^2) = ((y_1, \ldots, y_{d-1}) : y_d)$. Mas então $\sum_{i=1}^d r_i y_i \in (y_1, \ldots, y_{d-1}) \cap (0 : y_1) = (0)$, por indução. □

Proposição IV.2.3 *Suponhamos que $x_1, \ldots, x_d$ é uma d-seqüência em R. Então as imagens de $x_1, \ldots, x_d$ formam uma d-seqüência em $R/(0 : x_1)$.*

Dem. : É suficiente mostrar que para $k \geq j+1$, x_{j+1} não é um divisor de zero módulo o ideal $I = (((0 : x_1), x_1, \ldots, x_j) : x_k)$, e isso segue imediatamente da hipótese, se mostrarmos que $I = ((x_1, \ldots, x_j) : x_k)$.

Seja $c \in I$, isto é, existe uma equação $cx_k = \sum_{i=1}^{j} r_i x_i + w$, onde $wx_1 = 0$. Mas então $cx_k - \sum_{i=1}^{j} r_i x_i \in (x_1, \ldots, x_d) \cap (0 : x_1) = (0)$, pela Proposição IV.2.2 e isso mostra que $c \in ((x_1, \ldots, x_j) : x_k)$.

Logo, vale a igualdade, pois a outra inclusão é óbvia. □

Teorema IV.2.4 *Sejam R um anel e $x_1, \ldots, x_n$ uma d-seqüência módulo um ideal I de R. Seja $X = (x_1, \ldots, x_n)$. Então*

$$X^m \cap I \subset X^{m-1}I, \forall m \geq 1. \tag{IV.5}$$

Além disso, suponhamos que $(R, \mathfrak{m})$ é local, $I = (a_1, \ldots, a_d)$ e $x_1, \ldots, x_n$ são elementos tais que $a_1, \ldots, a_d, x_1, \ldots, x_n$ formam uma d-seqüência. Se $X = (x_1, \ldots, x_n)$, então

$$X^m \cap I \subset \mathfrak{m}X^{m-1}I, \forall m \geq 1. \tag{IV.6}$$

Dem. : (por indução em n)

- Suponhamos que $n = 1$.
  - Se $x_1^m r \in (x_1^m) \cap I$, como $(I : x_1) = (I : x_1^2)$, obtemos $x_1 r \in I$. De fato, podemos supor $m \geq 2$:

    $$x_1^m r \in I \Rightarrow x_1^{m-2} r \in (I : x_1^2) = (I : x_1) \Rightarrow x_1^{m-1} r \in I \Rightarrow \cdots \Rightarrow x_1 r \in I.$$

    Logo, $x_1^m r = x_1^{m-1}(x_1 r) \in x_1^{m-1} I$. Isso mostra o caso $n = 1$ para a fórmula IV.5.
  - Suponhamos que $I = (a_1, \ldots, a_d)$ como no enunciado.

    Afirmação: $x_1 r \in I \Rightarrow x_1 r \in \mathfrak{m}I$.

    Com efeito, $x_1 r = \sum_{i=1}^{d} s_i a_i$. Se algum $s_j \notin \mathfrak{m}$, então s_j é uma unidade e logo $a_j \in (a_1, \ldots, a_{j-1}, a_{j+1}, \ldots, a_d, x_1)$, o que contradiz o fato de $a_1, \ldots, a_d, x_1$ ser uma d-seqüência. Usando a mesma demonstração anterior, vemos que vale a fórmula IV.6 para $n = 1$.

- Agora, suponhamos que a fórmula IV.5 vale, para todo $k < n$, onde n é fixo. Sejam $J = (x_2, \ldots, x_n)$ e $x = x_1$. A hipótese de indução aplicada a (I, x) mostra que $J^m \cap (I, x) \subset J^{m-1}(I, x), \forall m \geq 1$, pois $x_2, \ldots, x_n$ é uma d-seqüência módulo (I, x). Além disso, como pela Proposição IV.2.2, $X^m \cap (I : x) \subset X \cap (I : x) \subset I$, vemos que $X^m \cap (I : x) = X^m \cap I, \forall m \geq 1$ pois $X^m \cap (I : x) \subset X^m \cap I \subset X^m \cap (I : x)$.

  Façamos indução em m:

– É claro que IV.5 vale para $m = 1$: $X \cap I \subset I$.

– Agora suponhamos que $X^{m-1} \cap I \subset X^{m-2}I$.

Seja $a \in X^m \cap I$. Como $X^m = J^m + X^{m-1}x$, segue que $a = b + cx$, onde $c \in X^{m-1}$ e $b \in J^m$. Então $b \in J^m \cap (I,x) \subset J^{m-1}(I,x)$. Escrevamos $b = u + vx$, onde $u \in J^{m-1}I$ e $v \in J^{m-1}$. Então $a = u + x(v+c)$ e logo $v + c \in (I:x) \cap X^{m-1} = X^{m-1} \cap I$, pelo que vimos acima. Pela indução em m, temos $X^{m-1} \cap I \subset X^{m-2}I$. Logo, $a = u + x(v+c) \in J^{m-1}I + xX^{m-2}I \subset X^{m-1}I$. Isso mostra a fórmula IV.5.

A prova para IV.6 é exatamente a mesma, colocando $\mathfrak{m}$ em cada passo da indução. □

Teorema IV.2.5 *Seja $(R,\mathfrak{m})$ um anel local. Suponhamos que $x_1, \ldots, x_n$ é uma d-seqüência. Então $x_1, \ldots, x_n$ são analiticamente independentes.*

Dem. : (por indução em n)

- Se $n = 1$, temos $(0 : x_1) = (0 : x_1^2)$ e segue que x_1 não é nilpotente:

  De fato, estamos supondo $x_1 \neq 0$. Fixemos $r \in \mathbb{N}$. Suponhamos que $x_1^i \neq 0, \forall i \leq r$. Então, $x_1^{r+1} = 0 \Rightarrow x_1^{r-1} \in (0 : x_1^2) = (0 : x_1) \Rightarrow x_1^r = 0$, absurdo.

  Se $F(X) = cX^s$ é um polinômio homogêneo, com $r \in R$ e $F(x_1) = cx_1^s = 0$, suponhamos por absurdo que $c \notin \mathfrak{m}$. Como $(R,\mathfrak{m})$ é local, segue que c é uma unidade em R e, logo, $cx_1^s = 0 \Rightarrow x_1^s = c^{-1}.0 = 0 \Rightarrow x_1$ é nilpotente. Absurdo.

  Portanto, x_1 é analiticamente independente.

- Suponhamos o resultado para os anéis locais e todas as d-seqüências de comprimento $< n$.

  Suponhamos que $x_1, \ldots, x_n$ não são analiticamente independentes, isto é, existe um polinômio homogêneo $F(T_1, \ldots, T_n)$ em n variáveis com um coeficiente unitário em um dos monômios tal que $F(x_1, \ldots, x_n) = 0$.

  Façamos indução no grau de F para todas as d-seqüências de comprimento n em qualquer anel local, ou seja, suponhamos que, se $G(y_1, \ldots, y_n) = 0$, onde $y_1, \ldots, y_n$ é uma d-seqüência e G é homogêneo com $gr(G) < gr(F)$, então $G \in \mathfrak{m}[T_1, \ldots, T_n]$. Podemos supor que F é uma relação de grau mínimo (escolha F de grau mínimo dentre as que satisfazem $F(x_1, \ldots, x_n) = 0$ com um dos coeficientes unitário).

  Escrevemos $F(T_1, \ldots, T_n) = T_1 G(T_1, \ldots, T_n) + H(T_2, \ldots, T_n)$, onde H é homogêneo de grau d em $T_2, \ldots, T_n$. Como $x_1, \ldots, x_n$ são uma d-seqüência, então $\overline{x_2}, \ldots, \overline{x_n}$ são uma d-seqüência em R/Rx_1; logo, pela hipótese de indução $\overline{x_2}, \ldots, \overline{x_n}$ são analiticamente independentes em R/Rx_1. Como em R/Rx_1, $H(\overline{x_2}, \ldots, \overline{x_n}) = \overline{F(x_1, x_2, \ldots, x_n)} = 0$, então $H(T_2, \ldots, T_n)$ não pode ter nenhum monômio com coeficiente unitário, isto é, $H(T_2, \ldots, T_n) \in \mathfrak{m}[T_1, \ldots, T_n]$. Portanto, $G(T_1, \ldots, T_n)$ deve ter um coeficiente unitário. Agora, a equação $H(x_2, \ldots, x_n) + x_1 G(x_1, \ldots, x_n) = 0$ mostra que $w = H(x_2, \ldots, x_n) \in J^d \cap (x_1)$, onde $J = (x_2, \ldots, x_n)$. Pelo Teorema IV.2.4, $J^d \cap (x_1) \subset \mathfrak{m}J^{d-1}x_1$, pois J é gerado por uma d-seqüência módulo (x_1). Assim, existe um polinômio homogêneo $H'(T_2,\ldots,T_n) \in \mathcal{m}[T_2,\ldots,T_n]$ de grau $d-1$ tal que $w = x_1H'(x_2,\ldots,x_n)$. Logo, $x_1,\ldots,x_n$ é uma solução da equação $T_1G(T_1,\ldots,T_n) + T_1H'(T_2,\ldots,T_n) = 0$, mas $x_1[G(x_1,\ldots,x_n) + H'(x_2,\ldots,x_n)] = 0$ implica que $G(x_1,\ldots,x_n)+H'(x_2,\ldots,x_n) \in (0 : x_1)$. Se $d > 1$, então $G(x_1,\ldots,x_n)+H'(x_2,\ldots,x_n) \in (x_1,\ldots,x_n)$, pois $G(T_1,\ldots,T_n) + H'(T_2,\ldots,T_n)$ é um polinômio homogêneo de grau $d-1$. Pela Proposição IV.2.2, temos $G(x_1,\ldots,x_n) + H'(x_2,\ldots,x_n) = 0$. Como G tem um coeficiente unitário e $H' \in \mathcal{m}[T_2,\ldots,T_n]$, então $G(T_1,\ldots,T_n)+H'(T_2,\ldots,T_n)$ tem um coeficiente unitário e tem grau estritamente menor que o grau de F, o que contradiz a indução. □

IV.3 Comparação das Álgebras Simétrica e de Rees de um Ideal Gerado por uma d-seqüência

Queremos mostrar que qualquer ideal gerado por uma d-seqüência é de tipo linear. Para isso, vamos mostrar uma proposição que generaliza o Teorema IV.2.4.

Proposição IV.3.1 *Se I é um ideal em R e as imagens de $x_1,\ldots,x_n$ são uma d-seqüência em R/I, então $I \cap (x_1,\ldots,x_n)(x_1,\ldots,x_k)^m \subset (x_1,\ldots,x_n)(x_1,\ldots,x_k)^{m-1}I$, se $0 \leq k \leq n$ e $m \geq 1$.*

Observação IV.3.2 O Teorema IV.2.4 afirma que $I \cap (x_1,\ldots,x_n)^m \subset I(x_1,\ldots,x_n)^{m-1}$.

Dem. : (por indução em $n-k$)

- Se $n-k=0$, então o Teorema IV.2.4 citado mostra a veracidade da afirmação.
- Suponhamos que a proposição foi mostrada para todo m sempre que $n-k-1 < t$. Queremos mostrar a proposição para todo m e $n-k-1 = t$.

  Seja $x = x_1$. Por indução, como $x_2,\ldots,x_n$ são uma d-seqüência módulo (I,x), podemos supor que $(I,x) \cap (x_2,\ldots,x_n)(x_2,\ldots,x_k)^m \subset (x_2,\ldots,x_n)(x_2,\ldots,x_k)^{m-1}(I,x), \forall m \geq 1$.

  Seja

  $J_u =$
  $Rx^{m+1}+x^m(x_2,\ldots,x_n)+x^{m-1}(x_2,\ldots,x_k)(x_2,\ldots,x_n)+\cdots+x^{m+1-u}(x_2,\ldots,x_k)^{u-1}(x_2,\ldots,x_n)$.

  Então afirmamos que $J_u \cap I \subset I(x_2,\ldots,x_k)^{u-2}(x_2,\ldots,x_n)x^{m+1-u} + J_{u-1} \cap I$, $1 \leq u \leq m+1$.

  - Se $u = m+1$, então

  $J_u =$
  $Rx^{m+1}+x^m(x_2,\ldots,x_n)+x^{m-1}(x_2,\ldots,x_k)(x_2,\ldots,x_n)+\cdots+x(x_2,\ldots,x_k)^{m-1}(x_2,\ldots,x_n)+$
  $(x_2,\ldots,x_k)^m(x_2,\ldots,x_n)$
  $= J_m + (x_2,\ldots,x_k)^m(x_2,\ldots,x_n)$.

  Assim, se $r \in J_m$ e $s \in (x_2,\ldots,x_k)^m(x_2,\ldots,x_n)$ são tais que $r+s \in I$, então como $J_m \subset (x) \subset (I,x)$, vemos que $s \in (x_2,\ldots,x_k)^m(x_2,\ldots,x_n) \cap (I,x) \subset (x_2,\ldots,x_k)^{m-1}(x_2,\ldots,x_n)(I,x) \subset J_m + I(x_2,\ldots,x_k)^{m-1}(x_2,\ldots,x_n)$. Logo, $r+s \in J_m \cap I + I(x_2,\ldots,x_k)^{m-1}(x_2,\ldots,x_n)$, como queríamos.

– Suponhamos que $1 < u < m+1$. Escreva $J_u = J_{u-1} + x^{m+1-u}(x_2,\ldots,x_k)^{u-1}(x_2,\ldots,x_n)$. Suponhamos que $y \in J_{u-1}, z \in x^{m+1-u}(x_2,\ldots,x_k)^{u-1}(x_2,\ldots,x_n)$ são tais que $y+z \in I$. Podemos escrever $y = x^{m+2-u}w$ e $z = x^{m+1-u}v$, onde $v \in (x_2,\ldots,x_k)^{u-1}(x_2,\ldots,x_n)$. Então, $x^{m+1-u}(v+xw) = x^{m+1-u}v + x^{m+2-u}w = z+y \in I$ e assim $x(v+xw) \in I$, pois $(I:x) = (I:x^2)$ pela definição de uma d-seqüência. Logo, $v + xw \in (I:x) \cap (x, x_2, \ldots, x_n, I) = I$, pela Proposição IV.2.2. Isso implica que

$$v \in (x_2,\ldots,x_k)^{u-1}(x_2,\ldots,x_n) \cap (I,x) \subset (x_2,\ldots,x_n)(x_2,\ldots,x_k)^{u-2}(I,x).$$

Assim,

$$z = x^{m+1-u}v \in x^{m+2-u}(x_2,\ldots,x_k)^{u-2}(x_2,\ldots,x_n) + I(x_2,\ldots,x_k)^{u-2}(x_2,\ldots,x_n)x^{m+1-u}$$

e, logo, $z \in J_{u-1} + I(x_2,\ldots,x_k)^{u-2}(x_2,\ldots,x_n)x^{m+1-u}$. Então,

$$y + z \in J_{u-1} \cap I + I(x_2,\ldots,x_k)^{u-2}(x_2,\ldots,x_n)x^{m+1-u},$$

como queríamos.

– Consideremos $J_1 = Rx^{m+1} + x^m(x_2,\ldots,x_n)$. Se $rx^{m+1} + sx^m \in J_1 \cap I$, com $s \in (x_2,\ldots,x_n)$; então, $x^m(s+rx) \in I$ implica, como fizemos acima, que $x(s+rx) \in I$, isto é, $s + rx \in (I:x) \cap (I, x, x_2, \ldots, x_n) = I$, ou seja, $s \in (I,x)$. Logo, $x^m s \in Ix^m + (x^{m+1})$ e $rx^{m+1} + sx^m \in Rx^{m+1} \cap I + Ix^m \subset Ix^m$, pelo Teorema IV.2.4. Agora,

$$\begin{aligned} J_{m+1} &= Rx^{m+1} + x^m(x_2,\ldots,x_n) + x^{m-1}(x_2,\ldots,x_k)(x_2,\ldots,x_n) + \cdots + (x_2,\ldots,x_k)^m(x_2,\ldots,x_n) \\ &= (x, x_2, \ldots, x_n)(x, x_2, \ldots, x_k)^m. \end{aligned}$$

Assim,

$$\begin{aligned} J_{m+1} \cap I = (x_1, x_2, \ldots, x_n)(x_1, x_2, \ldots, x_k)^m \cap I &\subset J_m \cap I + I(x_2,\ldots,x_k)^{m-1}(x_2,\ldots,x_n) \subset \\ &\subset J_{m-1} \cap I + I(x_2,\ldots,x_k)^{m-1}(x_2,\ldots,x_n) + I(x_2,\ldots,x_k)^{m-2}(x_2,\ldots,x_n)x \subset \\ &\subset \cdots \subset J_1 \cap I + I(x_2,\ldots,x_k)^{m-1}(x_2,\ldots,x_n) + \cdots + I(x_2,\ldots,x_n)x^{m-1} \subset \\ &\subset x^m I + I(x_2,\ldots,x_k)^{m-1}(x_2,\ldots,x_n) + \cdots + I(x_2,\ldots,x_n)x^{m-1} \subset \\ &\subset I(x, x_2, \ldots, x_n)(x, x_2, \ldots, x_k)^{m-1}, \end{aligned}$$

o que prova a proposição. □

Teorema IV.3.3 *Suponha que $I = (z_1, \ldots, z_n)$, onde $z_1, \ldots, z_n$ é uma d-seqüência. Então I é de tipo linear.*

Dem. : Precisamos mostrar que, se $H(X_1,\ldots,X_n)$ é um polinômio homogêneo tal que $H(z_1,\ldots,z_n) = 0$, então $H(X_1,\ldots,X_n) \in \mathfrak{q} = (\sum_{i=1}^n b_i X_i; \sum_{i=1}^n b_i z_i = 0)$.

Primeiro mostraremos isso se $H(X_1,\ldots,X_n)$ tem grau 1 em todas as variáveis $X_1,\ldots,X_n$. Seja H de grau d.

- Suponhamos que somente um monômio aparece em H. Então $H(X_1,\ldots,X_n) = aX_{i_1}\cdots X_{i_d}$. Como $H(z_1,\ldots,z_n) = az_{i_1}\cdots z_{i_d} = 0$, a definição de uma d-seqüência mostra que $a \in$

$(0 : z_{i_1} \cdots z_{i_d}) = (0 : z_{i_1})$ logo $az_{i_1} = 0$. Definindo $F(X_1, \ldots, X_n) = aX_{i_1}$, temos que $F(z_1, \ldots, z_n) = az_{i_1} = 0$ e logo $F \in \mathfrak{q}$. Mas $H = FX_{i_2} \cdots X_{i_d}$, logo $H \in \mathfrak{q}$.

- Agora, lexicograficamente, ordenemos os monômios que aparecem em H por

$$X_{i_1} \cdots X_{i_d} < X_{j_1} \cdots X_{j_d} \Leftrightarrow i_d = j_d, i_{d-1} = j_{d-1}, \ldots, i_{k+1} = j_{k+1}, i_k < j_k, \text{para algum } 1 \leq k \leq d.$$

Façamos indução no maior monômio que aparece em H, ou seja, suponhamos que se um monômio estritamente menor que esse aparece em H, então ele já pertence a $\mathfrak{q}$. Seja $aX_{i_1} \cdots X_{i_d}$ o monômio maximal que aparece em $H(X_1, \ldots, X_n)$ sob essa ordem (Como essa ordem monomial é total, existe um único monômio maximal). Ponhamos

$$J = (z_k; k \neq i_1, \ldots, i_d, k < i_d).$$

Agora $H(z_1, \ldots, z_n) = 0$ mostra que $az_{i_1} \cdots z_{i_d} \in J$ pois qualquer outro monômio tem pelo menos um z_k que aparece em J. Como $z_{i_1}, \ldots, z_{i_d}$ formam uma d-seqüência módulo J, vemos que $a \in (J : z_{i_1} \cdots z_{i_d}) = (J : z_{i_d})$ e logo $az_{i_d} \in J$. Então, temos uma equação $az_{i_d} = \sum_k b_k z_k$, onde $z_k \in J$. Então, o polinômio $F(X_1, \ldots, X_n) = aX_{i_d} - \sum_k b_k X_k \in \mathfrak{q}$ e, portanto, $X_{i_1} \cdots X_{i_{d-1}} F \in \mathfrak{q}$ e é suficiente mostrar que $H - X_{i_1} \cdots X_{i_{d-1}} F \in \mathfrak{q}$. Mas

$$H - X_{i_1} \cdots X_{i_{d-1}} F = \underbrace{H - aX_{i_1} \cdots X_{i_d}}_{\text{com monômios} < X_{i_1} \cdots X_{i_d}} + \underbrace{\sum b_k X_k X_{i_1} \cdots X_{i_{d-1}}}_{< X_{i_d} X_{i_1} \cdots X_{i_{d-1}}}$$

tem somente monômios que são estritamente menores que $X_{i_1} \cdots X_{i_d}$. A indução agora mostra que $H - X_{i_1} \cdots X_{i_{d-1}} F \in \mathfrak{q}$, o que mostra o teorema, se $H(X_1, \ldots, X_n)$ tem grau 1 em todas as variáveis.

Vamos proceder agora tentando "tornar" H de grau 1 em todas as variáveis.

Fazemos indução no grau de H para mostrar que $H \in \mathfrak{q}$.

Agora, suponhamos que $gr(H) = d$ e $H(z_1, \ldots, z_n) = 0$, com H de grau 1 em $X_n, \ldots, X_{i+1}$. Escrevemos $H(X_1, \ldots, X_n) = X_i F(X_1, \ldots, X_n) + G(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$, onde F e G têm grau 1 em $X_n, \ldots, X_{i+1}, gr(F) = d - 1$ e $gr(G) = d$. Como $H(z_1, \ldots, z_n) = 0$, vemos que $w = G(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_n) \in (z_i)$ e logo, como $z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_n$ são uma d-seqüência módulo (z_i), pela Proposição IV.3.1,

$$w \in (z_i) \cap (z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_n)(z_1, \ldots, z_{i-1})^{d-1} \subset z_i(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_n)(z_1, \ldots, z_{i-1})^{d-2}.$$

Assim, existe um polinômio $F'(X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n)$ de grau 1 em $X_n, \ldots, X_{i+1}$ tal que $w = z_i F'(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_n)$, onde $gr(F') = d - 1$. Agora como $H(z_1, \ldots, z_n) = 0$, temos $z_i F(z_1, \ldots, z_n) + z_i F'(z_1, \ldots, z_{i-1}, z_{i+1}, \ldots, z_n) = 0$, e $(F + F')(z_1, \ldots, z_n) \in (0 : z_i) \cap (z_1, \ldots, z_n) = 0$, por IV.2.2, isto é, $(F + F')(z_1, \ldots, z_n) = 0$ e como $gr(F + F') \leq d - 1 < d$, a indução mostra que $F + F' \in \mathfrak{q}$. Assim, $X_i F + X_i F' \in \mathfrak{q}$ e é suficiente mostrar que

$$G - X_i F' = \underbrace{(X_i F + G)}_{=H} - (X_i F + X_i F') \in \mathfrak{q}.$$

Mas G é um polinômio em $X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n$ de grau 1 em $X_n, \ldots, X_{i+1}$ e logo $G - X_iF'$ tem grau 1 em $X_n, \ldots, X_{i+1}, X_i$. Continuando, podemos cair num polinômio de grau 1 em todas as variáveis e aplicar o trabalho anterior para terminar a demonstração. $\square$

IV.4 Aplicações

O Teorema IV.3.3 pode ser usado efetivamente para calcular o anel graduado de um ideal gerado por uma d-seqüência. Vamos ilustrar isso no caso do exemplo dado na Seção IV.1, onde I é o ideal gerado pelos menores maximais de uma matriz $n \times (n+1)$ genérica X.

Primeiro, vamos mostrar alguns isomorfismos:

- Se $I = (a_1, \ldots, a_n)$, então já vimos que $\mathcal{R}(I) = R[a_1T, \ldots, a_nT] \subset R[T]$ é a álgebra de Rees de I e $B = R[a_1T, \ldots, a_nT, T^{-1}]$ é o anel de Rees generalizado. Vamos ver que

$$B/BT^{-1} \cong gr_I(R) = R/I \oplus I/I^2 \oplus I^2/I^3 \oplus \cdots.$$

De fato, também já vimos que

$$B = \{b_{-r}T^{-r} + \cdots + b_{-1}T^{-1} + b_0 + b_1T + \cdots + b_sT^s; r, s \in I\!N, b_j \in I^j, b_{-j} \in R\}.$$

Logo, definimos o homomorfismo

$$\begin{array}{ccc} B & \xrightarrow{\quad\varphi\quad} & gr_I(R) = R/I \oplus I/I^2 \oplus I^2/I^3 \oplus \cdots \\ b_{-r}T^{-r} + \cdots + b_{-1}T^{-1} + b_0 + b_1T + \cdots + b_sT^s & \longmapsto & \overline{b_0} \oplus \overline{b_1} \oplus \cdots \oplus \overline{b_s} \end{array}$$

– φ está bem definida:

Se $b = b_{-r}T^{-r} + \cdots + b_{-1}T^{-1} + b_0 + b_1T + \cdots + b_sT^s = b'_{-r'}T^{-r'} + \cdots + b'_{-1}T^{-1} + b'_0 + b'_1T + \cdots + b'_{s'}T^{s'} \in B$, suponhamos, sem perda de generalidade, que $s \leq s'$. Então

$$\begin{aligned} T^{r+r'}b &= b_{-r}T^{r'} + \cdots + b_{-1}T^{r+r'-1} + b_0T^{r+r'} + b_1T^{r+r'+1} + \cdots + b_sT^{s+r+r'} \\ &= b'_{-r'}T^{r} + \cdots + b'_{-1}T^{r+r'-1} + b'_0T^{r+r'} + b'_1T^{r+r'+1} + \cdots + b'_{s'}T^{s'+r+r'} \end{aligned}$$

Se $s < s'$ então $b_{j'} = 0$, para $j' = s+1, \ldots, s'$. Logo, podemos supor que $s = s'$ e teremos então que $b_0 = b'_0, b_1 = b'_1, \ldots, b_s = b'_{s'}$. Portanto, $\overline{b_0} \oplus \overline{b_1} \oplus \cdots \oplus \overline{b_s} = \overline{b'_0} \oplus \overline{b'_1} \oplus \cdots \oplus \overline{b'_{s'}}$.

– φ é sobrejetiva:

Dado $\sum_{i=0}^{\infty} \overline{x_i} \in gr_I(R)$, temos que $\overline{x_i} = 0$, para quase todo i. Seja $s \in I\!N$ tal que $\overline{x_i} = 0, \forall i > s$. Temos $x_j \in I^j$ e $\varphi(x_0 + x_1T + \cdots + x_sT^s) = \overline{x_0} \oplus \overline{x_1} \oplus \cdots \oplus \overline{x_s} = \sum_{i=0}^{\infty} \overline{x_i}$.

– $Ker(\varphi) = T^{-1}B$:

Se $\overline{b_0} \oplus \overline{b_1} \oplus \cdots \oplus \overline{b_s} = 0$, então $b_j \in I^{j+1}, \forall j = 0, \ldots, s$. Como $b_{-r}T^{-r} + \cdots + b_{-1}T^{-1} + b_0 + b_1T + \cdots + b_sT^s = T^{-1}g(T^{-1}) + (b_0T)T^{-1} + (b_1T^2)T^{-1} + \cdots + (b_sT^{s+1})T^{-1}$ e como $b_jT^{j+1} \in R[a_1T, \dots, a_nT, T^{-1}] \subset B$, segue que $(b_jT^{j+1})T^{-1} \in T^{-1}B$ e como $T^{-1}g(T^{-1}) \in T^{-1}B$, segue que $b_{-r}T^{-r} + \cdots + b_{-1}T^{-1} + b_0 + b_1T + \cdots + b_sT^s \in T^{-1}B$. Reciprocamente, se $b = T^{-1}g(a_1T, \dots, a_nT, T^{-1}) \in T^{-1}B$, então $g = b_{-r}T^{-r} + \cdots + b_{-1}T^{-1} + b_0 + b_1T + \cdots + b_sT^s$, com $b_j \in I^j$; logo, $T^{-1}g = b_{-r}T^{-r-1} + \cdots + b_{-1}T^{-2} + b_0T^{-1} + b_1 + b_2T + \cdots + b_sT^{s-1}$ e $\varphi(T^{-1}g) = (b_1 + I) \oplus (b_2 + I^2) \oplus \cdots \oplus (b_s + I^s) = 0$.

Portanto, $B/BT^{-1} \cong gr_I(R)$.

- Sejam R um domínio, $a, b \in R$. Consideremos o anel $B = R[a/b]$. Suponhamos que o núcleo da aplicação $\psi : R[T] \to R[a/b]$, que leva T em a/b, é gerado por polinômios lineares. Então,

$$B/B(a/b) \cong R/(a : b).$$

De fato, defina o homomorfismo $\varphi = \pi \circ i$:

$$\begin{array}{ccccc} R & \xrightarrow{i} & B = R[a/b] & \xrightarrow{\pi} & B/B(a/b) \\ c & \mapsto & c & \mapsto & \overline{c} \end{array}$$

Temos:

– φ é sobrejetiva:

$\overline{d} \in B/B(a/b) \Rightarrow d \in B \Rightarrow d = f(a/b), f \in R[T] \Rightarrow f(T) = a_0 + a_1T + \cdots + a_nT^n, a_i \in R \Rightarrow d = f(a/b) = a_0 + a_1.(a/b) + a_2.(a/b)^2 + \cdots + a_n.(a/b)^n \Rightarrow d - a_0 = (a/b).(a_1 + a_2.(a/b) + \cdots + a_n.(a/b)^{n-1}) = (a/b).g(a/b), g \in R[T] \Rightarrow d - a_0 \in B(a/b) \Rightarrow \overline{d} = \overline{a_0} = \varphi(a_0), a_0 \in R$.

– $Ker(\varphi) = (a : b)$:

- $c \in (a : b) \Rightarrow bc = ad, d \in R \subset B \Rightarrow c = (a/b).d \in Ba/b \Rightarrow \overline{c} = 0$.
- $\overline{c} = 0 \Rightarrow c \in B(a/b) \Rightarrow c = d.(a/b), d \in B \Rightarrow c = (a/b).f(a/b), f \in R[T] \Rightarrow Tf(T) - c \in Ker(\psi) = (\alpha_i + \beta_iT; 1 \leq i \leq m) \Rightarrow Tf(T) - c = \sum_{i=1}^{m} f_i(T)(\alpha_i + \beta_iT)$. Como $\alpha_i + \beta_iT \in Ker(\psi)$, então $\alpha_i + \beta_i(a/b) = 0$, ou seja, $b\alpha_i = -a\beta_i$, isto é, $\alpha_i \in (a : b)$. Logo, $Tf(T) - c = \sum_{i=1}^{m} f_i(T)(\alpha_i + \beta_iT) \Rightarrow -c = \sum_{i=1}^{m} f_i(0)\alpha_i \Rightarrow c \in (a : b)$.

Observação IV.4.1 Se $(a : b^2) = (a : b)$, então $Ker(\psi)$ é gerado por polinômios lineares: (veja a demonstração no apêndice.)

Feitos esses isomorfismos, vamos considerar o exemplo da Seção IV.1.

Sejam $X = (x_{ij})$ uma $n \times (n+1)$ matriz de indeterminadas sobre k e $R = k[x_{ij}]$. Sejam Δ'_j o menor maximal de X obtido retirando-se a j-ésima coluna de X e $I = (\Delta'_1, \dots, \Delta'_{n+1})$. A matriz X acrescida da i-ésima linha tem determinante nulo (pois tem duas linhas iguais), logo se expandirmos seu determinante em relação a essa linha, teremos $\sum_{j=1}^{n+1}(-1)^{i+j}x_{ij}\Delta'_j = 0$ e chamando $\Delta_j = (-1)^{i+j}\Delta'_j$, teremos $I = (\Delta_1, \dots, \Delta_{n+1})$ e

$$\sum_{j=1}^{n+1} x_{ij}\Delta_j = 0.$$

Seja $g_i = \sum_{j=1}^{n+1} x_{ij}\Delta_j$. É conhecido que as relações lineares nos menores maximais $\Delta'_1, \ldots, \Delta'_{n+1}$ de X são geradas pelas relações $g_i = 0$ ([10]). Assim, $S(I) = R[T_1, \ldots, T_{n+1}]/J = R[\overline{T_1}, \ldots, \overline{T_{n+1}}]$, onde J é o ideal gerado por $\sum_{j=1}^{n+1} x_{ij}T_j$. Como, pelo Teorema IV.3.3, I é de tipo linear, o isomorfismo $\phi : S(I) \to \mathcal{R}(I) = R[\Delta_1 T, \ldots, \Delta_{n+1}T] \subset R[T]$ leva $\overline{T_j}$ em $\Delta_j T$ e vamos considerar $T^{-1} = \Delta_1/\Delta_1 T = \Delta_1/\overline{T_1}$. Seja $B = S(I)[\Delta_1/\overline{T_1}]$ o anel de Rees generalizado. Queremos encontrar $gr_I(R)$ e, para isso, vamos usar os isomorfismos anteriores.

Afirmação 1: $\Delta_i\overline{T_j} = \Delta_j\overline{T_i}$

Seja $f(T_1, \ldots, T_{n+1}) = \Delta_i T_j - \Delta_j T_i$. Então $f(\Delta_1, \ldots, \Delta_{n+1}) = \Delta_i\Delta_j - \Delta_j\Delta_i = 0$ e como f é linear, segue que $f \in J$, ou seja, $\Delta_i\overline{T_j} - \Delta_j\overline{T_i} = 0$.

Afirmação 2: $(\Delta_1 : \overline{T_1}^2) = (\Delta_1 : \overline{T_1})$ em $S(I)$

Aplicando o isomorfismo ϕ, basta mostrar que $(\Delta_1 : \Delta_1^2 T^2) = (\Delta_1 : \Delta_1 T)$ em $\mathcal{R}(I)$.

É claro que $(\Delta_1 : \Delta_1 T) \subset (\Delta_1 : \Delta_1^2 T^2)$.

Seja $f \in \mathcal{R}(I)$ tal que $\Delta_1^2 T^2 f = \Delta_1 h$, com $h \in \mathcal{R}(I)$. Escrevendo $f = f_0 + f_1 T + \cdots + f_s T^s$, com $f_j \in I^j$ e $h = h_0 + h_1 T + \cdots + h_{s+2}T^{s+2}$, com $h_j \in I^j$ (já podemos supor que $gr_T(h) = 2 + gr_T(f)$ pois $\Delta_1^2 T^2 f = \Delta_1 h$), e, substituindo na igualdade, teremos

$$\Delta_1^2 f_0 T^2 + \Delta_1^2 f_1 T^3 + \cdots + \Delta_1^2 f_s T^{s+2} = \Delta_1 h_0 + \Delta_1 h_1 T + \cdots + \Delta_1 h_{s+2} T^{s+2}$$

Então:

$\Delta_1 h_0 = 0 \Rightarrow h_0 = 0$

$\Delta_1 h_1 = 0 \Rightarrow h_1 = 0$

$\Delta_1 h_2 = \Delta_1^2 f_0 \Rightarrow h_2 = \Delta_1 f_0 \Rightarrow h_2 \in (\Delta_1) \cap I^2 \subset \Delta_1 I \Rightarrow h_2 = \Delta_1 h'_2, h'_2 \in I \Rightarrow f_0 = h'_2 \in I$

$\Delta_1 h_3 = \Delta_1^2 f_1 \Rightarrow h_3 = \Delta_1 f_1 \Rightarrow h_3 \in (\Delta_1) \cap I^3 \subset \Delta_1 I^2 \Rightarrow f_1 \in I^2$

$\vdots$

Portanto, concluímos que $f_j \in I^{j+1}$. Assim,

$$\Delta_1 T f = \Delta_1 \underbrace{(T f_0 + \cdots + T^{j+1} f_j + \cdots + T^{s+1} f_s)}_{\in \mathcal{R}(I)} \in (\Delta_1) \Rightarrow f \in (\Delta_1 : \Delta_1 T).$$

Logo, $(\Delta_1 : \Delta_1^2 T^2) = (\Delta_1 : \Delta_1 T)$ em $\mathcal{R}(I)$.

Afirmação 3: $(\Delta_1 : \overline{T_1}) = (\Delta_1, \ldots, \Delta_{n+1})S(I) = IS(I)$

Pela Afirmação 1, segue que $\Delta_j \in (\Delta_1 : \overline{T_1})$, logo $IS(I) \subset (\Delta_1 : \overline{T_1})$. Por outro lado, seja $\overline{f} \in (\Delta_1 : \overline{T_1}) \subset S(I)$, ou seja, $\overline{T_1 f} = \Delta_1\overline{h}$, $\overline{h} \in S(I), h \in R[T_1, \ldots, T_{n+1}], \overline{f} = f(\overline{T_1}, \ldots, \overline{T_{n+1}})$. Podemos escrever $h = h_0 + h_1 T_1 + \cdots + h_{n+1}T_{n+1}$, com $h_0 \in R$. Da igualdade $\overline{T_1 f} = \Delta_1\overline{h}$ segue que $T_1 f - \Delta_1 h \in J$ e fazendo $T_1 = \ldots = T_{n+1} = 0$, teremos $0 = -\Delta_1 h_0$ e logo $h_0 = 0$.

Logo

$$\begin{aligned}\overline{T_1 f} = \Delta_1 \overline{h} = &\ \Delta_1 \overline{T_1 h_1} + \Delta_1 \overline{T_2 h_2} + \cdots + \Delta_1 \overline{T_{n+1} h_{n+1}} \\ =^{af.1} &\ \Delta_1 \overline{T_1 h_1} + \Delta_2 \overline{T_1 h_2} + \cdots + \Delta_{n+1} \overline{T_1 h_{n+1}} \\ = &\ \overline{T_1}(\Delta_1 \overline{h_1} + \Delta_2 \overline{h_2} + \cdots + \Delta_{n+1} \overline{h_{n+1}})\end{aligned}$$

Como $T_1 \notin J$, então $\overline{T_1} \neq 0$ e como $S(I)$ é domínio, segue que

$$\overline{f} = \Delta_1 \overline{h_1} + \Delta_2 \overline{h_2} + \cdots + \Delta_{n+1} \overline{h_{n+1}} \in IS(I).$$

Portanto, $(\Delta_1 : \overline{T_1}) = IS(I)$.

Usando a afirmação 2 e os isomorfismos mostrados anteriormente, segue que

$$gr_I(R) \cong \frac{B}{B(\Delta_1/\overline{T_1})} \cong \frac{S(I)}{(\Delta_1 : \overline{T_1})} \cong \frac{S(I)}{IS(I)} \cong \frac{R[T_1,\ldots,T_{n+1}]/J}{(\Delta_1,\ldots,\Delta_{n+1})S(I)} \cong \frac{R[T_1,\ldots,T_{n+1}]/J}{((\Delta_1,\ldots,\Delta_{n+1})+J)/J} \cong \frac{R[T_1,\ldots,T_{n+1}]}{(\Delta_1,\ldots,\Delta_{n+1})+J} \cong$$

$$\cong \frac{K[x_{ij},T_1,\ldots,T_{n+1}]}{(\Delta_1,\ldots,\Delta_{n+1},\sum_{j=1}^{n+1} x_{ij}T_j)} \cong \frac{K[x_{ij},T_1,\ldots,T_{n+1}]}{J'}.$$

Na referência [8], o seguinte resultado é provado:

Teorema IV.4.2 *Sejam $X = (x_{ij})$ uma $r \times s$ matriz de indeterminadas e $Y = (y_{jk})$ uma $s \times t$ matriz de indeterminadas. Sejam k um corpo e J o ideal em $k[x_{ij}, y_{jk}]$ gerado pelas entradas do produto matricial XY, todos os $(a+1) \times (a+1)$ menores de X e todos os $(b+1) \times (b+1)$ menores de Y. Se $a + b \leq s$, então J é primo e $k[x_{ij}, y_{jk}]/J$ é Cohen-Macaulay e integralmente fechado.*

Aplicando esse resultado a $X = (x_{ij})$, uma $n \times (n+1)$ matriz, e $Y = \begin{pmatrix} T_1 \\ \vdots \\ T_{n+1} \end{pmatrix}$, uma $(n+1) \times 1$ matriz, o ideal J' que define a álgebra graduada de I é dado pelas entradas de XY e todos os $n \times n$ menores de X. Como $n-1 \leq n+1$, podemos concluir que $gr_I(R)$ é Cohen-Macaulay e integralmente fechado.

IV.5 Contra-Exemplo da Recíproca do Teorema 4.3.3

Mostramos, na Seção IV.3, que qualquer ideal gerado por uma d-seqüência é de tipo linear. Em geral, a recíproca desse resultado é falsa, e mostraremos um contra-exemplo. Para tanto, precisaremos dos seguintes resultados:

Teorema IV.5.1 *Sejam $J \subset I$ ideais do anel R tais que $S_R(I) \cong \mathcal{R}_R(I)$. As seguintes afirmações são equivalentes:*

1. $S_{R/J}(I/J) \cong \mathcal{R}_{R/J}(I/J)$
2. $J \cap I^n = JI^{n-1}, \forall n \geq 1$.

Dem. : Consideremos $I = (\alpha_1, \ldots, \alpha_n)$. Por definição, $S_R(I) = R[T_1, \ldots, T_n]/\mathfrak{q}$, onde $\mathfrak{q} = (\sum_{i=1}^n c_iT_i; \sum_{i=1}^n c_i\alpha_i = 0)$. Como, pela hipótese, $S_R(I) \cong \mathcal{R}_R(I)$, então $\mathfrak{q} = \mathfrak{q}_\infty$, onde para $f \in R[T_1, \ldots, T_n]$ homogêneo, vale $f \in \mathfrak{q}_\infty \Leftrightarrow f(\alpha_1, \ldots, \alpha_n) = 0$.

Também pela definição, $S_{R/J}(I/J) = (R/J)[T_1, \ldots, T_n]/\mathfrak{a} = R/J[\overline{T_1}, \ldots, \overline{T_n}]$, onde $\mathfrak{a} = (\sum_{i=1}^n \overline{b_i}T_i; \sum_{i=1}^n \overline{b_i}\overline{\alpha_i} = \overline{0})$. Logo,

$$S_{R/J}(I/J) \cong R[T_1, \ldots, T_n]/(J, \mathfrak{q}'),$$

onde $\mathfrak{q}' = (\sum_{i=1}^n b_iT_i; \sum_{i=1}^n b_i\alpha_i \in J)$. De fato, vamos definir o homomorfismo sobrejetivo

$$\begin{array}{ccc} R[T_1, \ldots, T_n] & \xrightarrow{\varphi} & S_{R/J}(I/J) \\ T_i & \mapsto & \overline{T_i} \\ r & \mapsto & \overline{r} \end{array}$$

e vamos ver que $Ker(\varphi) = (J, \mathfrak{q}')$.

- $Ker(\varphi) \subset (J, \mathfrak{q}')$

  $\varphi(f(T_1, \ldots, T_n)) = \overline{0}$, com $f(T_1, \ldots, T_n) = \sum a_I T_1^{i_1} \cdots T_n^{i_n} \Rightarrow \sum \overline{a}_I \overline{T_1}^{i_1} \cdots \overline{T_n}^{i_n} = \overline{0} \Rightarrow$ $\sum \overline{a}_I T_1^{i_1} \cdots T_n^{i_n} \in \mathfrak{a} \Rightarrow \sum \overline{a}_I T_1^{i_1} \cdots T_n^{i_n} = \sum \overline{h_j}(\sum \overline{b_{ij}}T_i)$, onde $\overline{h_j}(T_1, \ldots, T_n) \in (R/J)[T_1, \ldots, T_n]$ e $\sum \overline{b_{ij}}\overline{\alpha_i} = 0 \Rightarrow \sum \overline{a}_I T_1^{i_1} \cdots T_n^{i_n} - \sum \overline{h_j}(\sum \overline{b_{ij}}T_i) = 0 \Rightarrow$
  $f - h = \sum a_I T_1^{i_1} \cdots T_n^{i_n} - \underbrace{\sum h_j(\sum b_{ij}T_i)}_{h} \in J[T_1, \ldots, T_n] \Rightarrow f = \underbrace{(f-h)}_{\in J[T_1, \ldots, T_n]} + \underbrace{h}_{\in \mathfrak{q}'} \in (J, \mathfrak{q}')$.[4]

- $(J, \mathfrak{q}') \subset Ker(\varphi)$

  $f(T_1, \ldots, T_n) \in (J, \mathfrak{q}') \Rightarrow f(T_1, \ldots, T_n) = g(T_1, \ldots, T_n) + \sum h_j(\sum b_{ij}T_i)$, com $g \in J[T_1, \ldots, T_n]$ e $\sum b_{ij}\alpha_i \in J \Rightarrow \varphi(f(T_1, \ldots, T_n)) = \varphi(g(T_1, \ldots, T_n)) + \sum(\overline{h_j(T_1, \ldots, T_n)})(\sum \overline{b_{ij}T_i})$[5] $= 0 + 0 = 0$.

Como

$$\mathcal{R}(I) = R \oplus IT \oplus I^2T^2 \oplus \cdots$$

temos

$$J\mathcal{R}(I) = J \oplus JIT \oplus JI^2T^2 \oplus \cdots$$

e, sendo $JT\mathcal{R}(I)$ o ideal gerado pelos elementos aT, com $a \in J$ temos

$$JT\mathcal{R}(I) = JT \oplus JIT^2 \oplus JI^2T^3 \oplus \cdots.$$

Logo,

$$(J, JT)\mathcal{R}(I) = J \oplus (J + JI)T \oplus (JI + JI^2)T^2 \oplus \cdots = J \oplus JT \oplus JIT^2 \oplus JI^2T^3 \oplus \cdots$$

ou seja,

$$(J, JT) = \{\sum_{n=0}^{r} c_nT^n; c_n \in JI^{n-1}\}.$$

[5]Como $\sum b_{ij}\alpha_i \in J$, então $\sum \overline{b_{ij}}\overline{\alpha_i} = 0$ e, portanto, $\sum b_{ij}\alpha_i \in \mathfrak{q}$ e $\sum \overline{b_{ij}T_i} = 0$.

Portanto,

$$\mathcal{R}(I)/(J,JT)\mathcal{R}(I) = R/J \oplus I/JT \oplus I^2/IJT^2 \oplus I^3/I^2JT^3 \oplus \cdots$$

Assim,

$$S_{R/J}(I/J) \cong \mathcal{R}_R(I)/(J,JT). \tag{IV.7}$$

Para verificar esse fato, defina o homomorfismo

$$\begin{array}{ccc} R[T_1,\ldots,T_n] & \xrightarrow{\psi} & \mathcal{R}_R(I)/(J,JT) \\ T_i & \mapsto & \overline{\alpha_i}T \\ r & \mapsto & \overline{r} \end{array}$$

Temos

- $Ker(\psi) = (J, \mathfrak{q}')$, onde $\mathfrak{q}' = (\sum_{i=1}^n b_iT_i; \sum_{i=1}^n b_i\alpha_i \in J)$.

  Como ψ é homogêneo, basta tomar elementos homogêneos.

  - $Ker(\psi) \subset (J, \mathfrak{q}')$

    Seja $f(T_1,\ldots,T_n)$ homogêneo de grau $m \geq 1$. (Se f tem grau 0, então $f = r \in R$ e $\psi(r) = \overline{r} = 0$ implica que $r \in J \subset (J,\mathfrak{q}')$.) Logo, $\psi(f(T_1,\ldots,T_n)) = f(\overline{\alpha_1},\ldots,\overline{\alpha_n})T^m = 0 \Rightarrow f(\alpha_1,\ldots,\alpha_n) \in JI^{m-1} \Rightarrow f(\alpha_1,\ldots,\alpha_n) = \sum_{j=1}^s a_jg_j(\alpha_1,\ldots,\alpha_n)$, com $a_j \in J$ e $g_j(T_1,\ldots,T_n)$ homogêneo de grau $m-1 \Rightarrow a_j = \sum_{i=1}^n b_{ij}\alpha_i \Rightarrow f(\alpha_1,\ldots,\alpha_n) = \sum_{j=1}^s\sum_{i=1}^n b_{ij}\alpha_ig_j(\alpha_1,\ldots,\alpha_n) \Rightarrow h(T_1,\ldots,T_n) = f(T_1,\ldots,T_n) - \sum_i\sum_j b_{ij}T_ig_j(T_1,\ldots,T_n)$ é um polinômio homogêneo de grau m que anula $\alpha_1,\ldots,\alpha_n \Rightarrow h \in \mathfrak{q}_\infty = \mathfrak{q} = (\sum_{i=1}^n c_iT_i; \sum_{i=1}^n c_i\alpha_i = 0) \subset \mathfrak{q}'$. Como

    $$\sum_i\sum_j b_{ij}T_ig_j(T_1,\ldots,T_n) = \sum_j g_j(T_1,\ldots,T_n)(\sum_i b_{ij}T_i) \text{ e } \sum_i b_{ij}T_i \in \mathfrak{q}'$$

    (pois $\sum_i b_{ij}\alpha_i = a_j \in J$), segue que

    $$f(T_1,\ldots,T_n) = h(T_1,\ldots,T_n) + \sum_i\sum_j b_{ij}T_ig_j(T_1,\ldots,T_n) \in \mathfrak{q}' \subset (J,\mathfrak{q}').$$

  - $(J,\mathfrak{q}') \subset Ker(\psi)$

    $f \in (J,\mathfrak{q}') \Rightarrow f(T_1,\ldots,T_n) = g(T_1,\ldots,T_n) + \sum_j h_j(T_1,\ldots,T_n)(\sum_i b_{ij}T_i)$, onde $g_j \in J[T_1,\ldots,T_n]$ e $\sum b_{ij}\alpha_i \in J \Rightarrow \psi(f(T_1,\ldots,T_n)) = f(\overline{\alpha_1}T,\ldots,\overline{\alpha_n}T) = g(\overline{\alpha_1}T,\ldots,\overline{\alpha_n}T) + \sum h_j(\overline{\alpha_1}T,\ldots,\overline{\alpha_n}T)(\sum \overline{b_{ij}}\overline{\alpha_i}T) = \overline{g(\alpha_1T,\ldots,\alpha_nT)} + \sum \overline{h_j(\alpha_1T,\ldots,\alpha_nT)}(\sum \overline{b_{ij}}\overline{\alpha_i})T = 0.$

- ψ é sobrejetiva

  Dado $\overline{r} = \overline{r_0} + \overline{r_1}T + \overline{r_2}T^2 + \cdots + \overline{r_s}T^s \in \mathcal{R}(I)/(J,JT)$, temos que $r_i \in I^i$, logo $r_i = R_i(\alpha_1,\ldots,\alpha_n)$, onde R_i é um polinômio homogêneo de grau i. Logo, $\psi(r_0 + R_1(T_1,\ldots,T_n) + R_2(T_1,\ldots,T_n) + \cdots + R_s(T_1,\ldots,T_n)) = \overline{r_0} + R_1(\overline{\alpha_1},\ldots,\overline{\alpha_n})T + R_2(\overline{\alpha_1},\ldots,\overline{\alpha_n})T^2 + \cdots + R_s(\overline{\alpha_1},\ldots,\overline{\alpha_n})T^s = \overline{r_0} + \overline{r_1}T + \overline{r_2}T^2 + \cdots + \overline{r_s}T^s = \overline{r}$.

Por outro lado, é claro que

$$\mathcal{R}_{R/J}(I/J) = \mathcal{R}_R(I)/J', \tag{IV.8}$$

onde J' é o ideal de $\mathcal{R}_R(I)$ dos elementos $\sum_{n=0}^{r} c_n T^n$ com $c_n \in J \cap I^n$. Para tanto, basta definir o homomorfismo sobrejetivo

$$\begin{array}{ccc} \mathcal{R}_R(I) & \xrightarrow{\tau} & \mathcal{R}_{R/J}(I/J) \\ \sum_{n=0}^{r} c_n T^n & \mapsto & \sum_{n=0}^{r} \overline{c_n} T^n \end{array}$$

que tem núcleo J':

$$\sum \overline{c_n} T^n = 0 \Leftrightarrow \overline{c_n} = 0 \Leftrightarrow c_n \in J \Leftrightarrow c_n \in J \cap I^n \Leftrightarrow \sum c_n T^n \in J'.$$

Observemos que $(J, JT) \subset J'$, pois $JI^{n-1} \subset J \cap I^n$.

Portanto, $S_{R/J}(I/J) \cong \mathcal{R}_{R/J}(I/J) \Leftrightarrow (J, JT) = J' \Leftrightarrow J \cap I^n = JI^{n-1}$. □

Proposição IV.5.2 *Sejam $a_1, \ldots, a_t$ uma R-seqüência e $f = \sum_{i=1}^{t} a_i b_i$ um elemento do ideal $J = (a_1, \ldots, a_t)$ tal que, para algum $j = 1, \ldots, t, (J : b_j) = J$. Então $S_{R/J}(J/(f)) \cong \mathcal{R}_{R/J}(J/(f))$.*

Dem. : Suponhamos que $f \in J^2$, isto é, $\sum_{i=1}^{t} a_i b_i = \sum_{i=1}^{t} a_i c_i$, com $c_i \in J, \forall i$. Assim, $\sum_{i=1}^{t} (b_i - c_i) a_i = 0$. Como $(b_t - c_t) a_t = -\sum_{i=1}^{t-1} (b_i - c_i) a_i \in (a_1, \ldots, a_{t-1})$ e $a_1, \ldots, a_t$ são uma R-seqüência, então $b_t - c_t = \sum_{i=1}^{t-1} d_{i,t} a_i \in J$ e como $c_t \in J$, segue que $b_t \in J$. Por indução em k, segue que $b_k - c_k \in J$ e como $c_k \in J$, segue que $b_k \in J, \forall k = 1, \ldots, t$. Isso é absurdo, pois $b_j \in J \Rightarrow 1 \in (J : b_j) = J$. Logo, a maior potência de f que pertence a J é 1. Portanto $(f) \cap J^n = (f) J^{n-1}$.[6] Pelo Teorema IV.5.1, segue que $J/(f)$ é de tipo linear, como queríamos. □

Exemplo IV.5.3 Vamos ver agora que a recíproca do Teorema IV.3.3 é falsa, com um contra-exemplo.

Sejam $R = k[X, Y, Z, T]/(XT - Y^2 Z) = k[x, y, z, t]$ e $I = (x, y) = (X, Y)/(XT - Y^2 Z)$. Pela Proposição IV.5.2, considerando $f = XT - Y^2 Z$ e $J = (X, Y)$, temos que I é de tipo linear, pois X, Y é uma $k[X, Y, Z, T]$-seqüência e $(J : T) = J$.[7]

No entanto, x, y não é uma d-seqüência, pois como $y^2 z = xt \in (x)$ então $z \in (x : y^2)$; mas $z \notin (x : y)$, pois, caso contrário, teríamos $zy = xf(x, y, z, t)$ e, logo, $ZY = Xf(X, Y, Z, T) + (XT - Y^2 Z) g(X, Y, Z, T)$. Se pusermos $X = 0$, seguiria que $ZY = -Y^2 Z g(X, Y, Z, T)$, o que é absurdo.

6

- $fr \in (f) \cap J^n \Rightarrow r \in J^{n-1} \Rightarrow fr \in (f) J^{n-1}$
- $sf.r \in (f) J^{n-1}$, $r \in J^{n-1} \Rightarrow sf.r \in (f) \cap J^n$ (pois $f \in J$)

7 É claro que $J \subset (J : T)$. Se $f \in (J : T)$, então $Tf \in J = (X, Y)$ e como X, Y, T é uma $k[X, Y, Z, T]$-seqüência, segue que $f \in J$. Logo, $J = (J : T)$.

Apêndice A

Condições para $Ker(R[T] \to R[a/b])$ ser Gerado por Polinômios Lineares

Neste apêndice, nosso objetivo é mostrar que, dados a, b elementos regulares de um anel comutativo R, T uma indeterminada e o homomorfismo natural de anéis $\psi : R[T] \to R[a/b]$ que leva T em a/b, se $(a : b^2) = (a : b)$, então $Ker(\psi)$ é gerado por polinômios lineares. Para tanto, provaremos alguns resultados.

Vamos considerar $K = Ker(\psi)$. Então, K é gerado por polinômios lineares se K é gerado por $B = \{dT - e; d, e \in R, 0 \neq be = ad\}$. Para cada $n \in I\!N$, consideremos $T_n = (b, a)^n \cap (b^{n+1} : a)$.

Teorema A.1 *As seguintes afirmações são equivalentes:*

1.i) $K = BR[T]$, *isto é, K é gerado por polinômios lineares.*

1.ii) $(K, T)R[T] \cap R = (a : b)$

1.iii) $T_n \subset (b^n), \forall n > 0$

Dem. :

1.i) $\Rightarrow$ 1.ii) $(K, T)R[T] \cap R \overset{i)}{=} (B, T)R[T] \cap R = ((a : b), T)R[T] \cap R = (a : b)$.

A segunda igualdade vale, pois:

- $f + Tg \in (B, T)R[T] \Rightarrow f = (dT - e)f', f' \in R[T]$ e $be = ad \Rightarrow f + Tg = (dT - e)f' + Tg = -ef' + T(g + df')$ e $e \in (a : b) \Rightarrow f + Tg \in ((a : b), T)R[T]$
- $rf + Tg \in ((a : b), T)R[T], r \neq 0, r \in (a : b) \Rightarrow br = as \neq, s \in R \Rightarrow rf + Tg = (sT - r)(-f) + T(sf + g) \in (B, T)R[T]$

1.ii) $\Rightarrow$ 1.iii) Seja $t \in T_n$, logo $t = r_{n+1}a^n + r_n a^{n-1}b + \cdots + r_2 ab_{n-1} + r_1 b^n, r_i \in R$ e $at/b_{n+1} = -r_0 \in R$. Seja $f(T) = r_{n+1}T^{n+1} + \cdots + r_1 T + r_0$. Temos $b_{n+1}f(a/b) = at + r_0 b^{n+1} = 0$, isto é, $f(T) \in K$. Logo, $r_0 \in (K, T)R[T] \cap R = (a : b)$ e $-br_0 = (at/b^{n+1})b \in (a)$. Assim, $t \in (b^n)$ e, portanto, $T_n \subset (b^n)$.

1.iii) $\Rightarrow$ 1.i) Seja $f(T) = r_nT^n + \cdots + r_0 \in K$. Para mostrar que $f(T) \in BR[T]$, vamos usar indução em n e podemos supor que $n > 1$. Seja $t = r_na^{n-1} + r_{n-1}a^{n-2}b + \cdots + r_2ab^{n-2} + r_1b^{n-1}$. Então, $0 = b^nf(a/b) = r_na^n + \cdots + r_1ab^{n-1} + r_0b^n = at + r_0b^n$, logo $at = -r_0b^n$, o que implica que $t \in (b^n, a)$. Portanto, $t \in T_{n-1} = (b,a)^{n-1} \cap (b^n : a) \subset (b^{n-1})$ por 1.iii) e $-r_0b/a = t/b^{n-1} \in R$. Assim, $g(T) = r_nT^{n-1} + \cdots + r_2T + (r_1 + r_0(b/a)) \in K$, pois $g(a/b) = r_n(a^{n-1}/b^{n-1}) + \cdots + r_2(a/b) + r_1 - r_n(a^{n-1}/b^{n-1}) - \cdots - r_2(ab^{n-2}/b^{n-1}) - r_1(b^{n-1}/b^{n-1}) = 0$ e pela indução $g(T) \in BR[T]$. Portanto, $f(T) = Tg(T) - (r_0(b/a)T - r_0) \in BR[T]$. □

Corolário A.2 *As seguintes afirmações são equivalentes:*

2.i) *K é gerado por polinômios lineares*

2.ii) $(a/b)R[a/b] \cap R = (a : b)$

2.iii) $\bigcup (a(b,a)^n : b^{n+1}) = (a : b)$

Dem. :

2.i) $\Leftrightarrow$ 2.ii) Pelo Teorema A.1, temos que $2.i) \Leftrightarrow 1.ii)$. Vamos então mostrar que $1.ii) \Leftrightarrow 2.ii)$.

1.ii) $\Rightarrow$ 2.ii)

- $r \in (a : b) = (K,T)R[T] \cap R \Rightarrow \psi(r) = r \in (a/b)R[a/b] \cap R$
- $a/bf(a/b) \in R \cap (a/b)R[a/b] \Rightarrow a/bf(a/b) = r \in R \Rightarrow af(a/b) = br \Rightarrow f(a/b) \in (b : a) \subset R \Rightarrow b[a/bf(a/b)] = af(a/b) \in (a) \Rightarrow a/bf(a/b) \in (a : b)$

2.ii) $\Rightarrow$ 1.ii)

- $r \in (a : b) \Rightarrow r \in a/bR[a/b] \cap R \Rightarrow r = \psi^{-1}(r) \in TR[T] \cap R \subset (K,T)R[T] \cap R$
- $r \in (K,T)R[T] \cap R \Rightarrow r = f + Tg, f \in K \Rightarrow r = \psi(r) = a/bg(a/b) \in a/bR[a/b] \cap R$

2.ii) $\Leftrightarrow$ 2.iii) Basta mostrar que $\bigcup(a(b,a)^n : b^{n+1}) = (a/b)R[a/b] \cap R$.

- $a/bf(a/b) \in R, f(T) \in R[T] \Rightarrow f(T) = \alpha_0 + \alpha_1T + \cdots + \alpha_nT^n \Rightarrow f(a/b) = \alpha_0 + \alpha_1a/b + \cdots + \alpha_n(a/b)^n \Rightarrow a/bf(a/b) = \alpha_0a/b + \alpha_1a^2/b^2 + \cdots + \alpha_na^{n+1}/b^{n+1} \Rightarrow b^{n+1}[a/bf(a/b)] = \alpha_0ab^n + \alpha_1a^2b^{n-1} + \cdots + \alpha_na^{n+1} = a(\alpha_0b^n + \alpha_1ab^{n-1} + \cdots + \alpha_na^n) \in a(b,a)^n \Rightarrow a/bf(a/b) \in \bigcup(a(b,a)^n : b^{n+1})$
- $r \in \bigcup(a(b,a)^n : b^{n+1}) \Rightarrow b^{n+1}r \in a(b,a)^n \Rightarrow b^{n+1}r = a(r_0b^n + r_1ab^{n-1} + \cdots + r_na^n) \Rightarrow r = a/b(r_0 + r_1a/b + \cdots + r_n(a/b)^n) = a/bf(a/b), f \in R[X] \Rightarrow r \in a/bR[a/b]$ □

Corolário A.3 *Se $(a : b) = (a : b^2)$, então K é gerado por polinômios lineares.*

Dem. :

Afirmação 1: $(a:b) = (a:b^2) \Rightarrow (a:b) = (a:b^n), \forall n > 1$.

De fato, é claro que $(a:b) \subset (a:b^n)$ e temos que:

$r \in (a:b^n) \Rightarrow b^n r = b^2(b^{n-2}r) \in (a) \Rightarrow b^{n-2}r \in (a:b^2) = (a:b) \Rightarrow b^{n-1}r \in (a) \Rightarrow \cdots \Rightarrow br \in (a) \Rightarrow r \in (a:b)$

Afirmação 2: $\bigcup (a(b,a)^n : b^{n+1}) = (a:b)$

- $r \in \bigcup (a(b,a)^n : b^{n+1}) \Rightarrow \exists n; b^{n+1}r = a(r_0 b^n + r_1 b^{n-1}a + \cdots + r_n a^n) \Rightarrow b^{n+1}r \in (a) \Rightarrow r \in (a:b^{n+1}) = (a:b)$.
- $r \in (a:b) \Rightarrow br \in (a) \Rightarrow br = ad, d \in R = (b,a)^0 \Rightarrow r \in (a(b,a)^0 : b) \subset \bigcup (a(b,a)^n : b^{n+1})$.

Pelo Corolário A.2, segue que K é gerado por polinômios lineares. $\square$

Bibliografia

[1] ATIYAH,M.F. E MACDONALD,I.G. *Introduction to Commutative Algebra.* Addison-Wesley Publ. Company, 1969.

[2] BARSHAY, J. Graded algebras of powers of ideals generated by A-sequences. *J. Algebra* 25. 1973, pp. 90-99.

[3] BOURBAKI,N. *Algèbre - Chapitres 1 à 3.* Hermann, Paris, 1970.

[4] BRUNS,W. E HERZOG,J. *Cohen-Macaulay Rings.* Cambridge University Press, 1994.

[5] CHEVALLEY,C. *Fundamental Concepts of Algebra.* Academic Press Inc. Publishers, New York, 1956.

[6] FIORENTINI, M. On relative regular sequences. *J. Algebra* 18. 1971, pp. 384-389.

[7] HARTSHORNE, R. *Algebraic Geometry.* Graduate Texts in Mathematics 52. Springer-Verlag, New York, Heidelberg, Berlin, 1977.

[8] HOCHSTER,M. E EAGON,J.A. Cohen-Macaulay Rings, Invariant Theory and the Generic Perfection of Determinantal loci. *American Journal of Mathematics* 93. 1971, pp. 1020-1058.

[9] HUNEKE,C. On the Symmetric and Rees algebra of an ideal generated by a d-sequence. *J.Algebra* 62. 1980, pp. 268-275.

[10] HUNEKE,C. The Theory of d-sequences and powers of ideals. *Advances in Mathematics* 46. 1982, pp. 249-279.

[11] HUNEKE,C. E ROSSI,M.E. The dimension and components of symmetric algebras, *J. Algebra* 98. 1986, pp. 200-210.

[12] KUNZ,E. *Introduction to Commutative Algebra and Algebraic Geometry.* Birkäuser Boston.Basel, Stuttgart, 1985.

[13] LANG,S. *Algebra.* Addison-Wesley Publ. Company, 1974.

[14] MACAULAY, F. S. The algebraic theory of modular systems. *Cambridge Tracts* n. 19. Cambridge University Press, 1916.

[15] MATSUMURA,H. *Commutative Algebra.* Benjamin, New York, 1970.

[16] MICALI,A. Sur les algèbres universalles. *Annales Inst. Fourier* 14. 1964, pp. 37-75.

[17] MICALI, A., SALMON, P. E SAMUEL, P. Integité et factorialité des algèbras symétriques. *Atas do IV Colóquio Brasileiro le Matematica.* São Paulo, 1965, pp. 61-75.

[18] RATLIFF,L. Conditions for $Ker(R[X] \to R[c/b])$ to have a linear base. *Proceedings of the American Mathematical Society* 39. 1973, pp. 509-514.

[19] RIBENBOIM, P. Anneaux de Rees intégralement clos. *Instituo de Mathemàtica Pura e Aplicada do Conselho Nacional de Pesquisas.* Rio de Janeiro, 1959.

[20] SALMON, P. Sulle algebre simmetricle e di Rees di un ideale. *Edizioni Scientifiche.* Genova, 1964.

[21] SAMUEL, P. Anneaux gradués factoriels et modules reflexifs. *Bull. Soc. Math. France* 92. 1964, pp. 237-249.

[22] SIMIS,A. E VASCONCELOS,W.V. The Krull dimension and integrality of symmetric algebras. *Manuscripta Math.* 61. 1988, pp. 63-78.

[23] ULRICH, B. (Reviewer) Arithmetic of blowup algebras by Wolmer V. Vasconcelos. *Bulletin of the American Mathematical Society* 34. 1997, pp. 177-181.

[24] VALLA,G. On the Symmetric and Rees Algebra of an Ideal. *Manuscripta Mathematica* 30. 1980, pp. 239-255.

[25] VASCONCELOS,W.V. Arithmetic of Blowup Algebras. *London Math.Soc.* Lectures Note Series 195. 1994.