UNIVERSIDADE FEDERAL DE SERGIPE
DEPARTAMENTO DE MATEMÁTICA

NATAN VINÍCIUS DE ARAÚJO LIMA

Função de Hilbert e suas conexões com outros invariantes

São Cristóvão, SE
2023.

UNIVERSIDADE FEDERAL DE SERGIPE
DEPARTAMENTO DE MATEMÁTICA

Função de Hilbert e suas conexões com outros invariantes

Dissertação apresentada ao Departamento de Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do título de Mestre em Matemática.

Natan Vinícius de Araújo Lima

Orientador: Zaqueu Alves Ramos

São Cristóvão, SE
2023.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Lima, Natan Vinícius de Araújo
L732f Função de Hilbert e suas conexões com outros invariantes / Natan Vinícius de Araújo Lima ; orientador Zaqueu Alves Ramos. – São Cristóvão, 2023.
60 f.

Dissertação (mestrado em Matemática) – Universidade Federal de Sergipe, 2023.

1. Hilbert, Espaço de. 2. Polinômios. 3. Álgebra comutativa. I. Ramos, Zaqueu Alves orient. II. Título.

CDU 517.98

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Função de Hilbert e suas conexões com outros invariantes

por

Natan Vinicius de Araujo Lima

Aprovada pela banca examinadora:

Prof. Dr. Zaqueu Alves Ramos - UFS
Orientador

Prof. Dr. Aislan Leal Fontes - UFS
Primeiro Examinador

Prof. Dr. Thiago Henrique de Freitas - UTFPR
Segundo Examinador

São Cristóvão, 31 de Janeiro de 2023

AGRADECIMENTOS

- À Deus primeiramente, por me permitir trilhar este caminho com saúde e força para superar todos obstáculos e dificuldades.
- Aos meus pais e irmãos, por todo apoio moral e financeiro. Além de todo o incentivo para conquistar meus objetivos.
- Aos meus antigos professores do IFS por me proporcionar todo conhecimento necessário para chegar até aqui. Em especial, a Crislene Paixão pelo incentivo no Mestrado. E em especial também a Lenira Pereira, que foi minha orientadora de monitoria e de trabalhos acadêmicos durante toda graduação, por toda amizade e conselhos.
- Aos meus amigos de graduação e futuros mestres Antonio Joaquim e Erika Félix, por toda amizade, companheirismo e risadas durante todos esses anos.
- Ao meu companheiro Gustavo Pereira, que me deu todo suporte emocional e soube compreender minhas dificuldades e ausências durante todo esse tempo. Te amo!
- Aos professores do PROMAT, que mesmo em período de pandemia se esforçaram para compartilhar seus conhecimentos.
- Em especial ao meu orientador Zaqueu, por toda paciência, compreensão e suporte dado durante todo o período de construção desta dissertação. Agradeço também por toda fundamentação básica, sem a qual este trabalho não seria escrito.
- Agradeço a CAPES pela bolsa concebida durante o curso.
- Por fim, agradeço a mim mesmo por ter conseguido conquistar esse objetivo, superando todas dificuldades e obstáculos. Por aguentar as noites sem dormir, os dias de estudos cansativos e as viagens intermunicipais diárias. Por todas vezes que tive abrir mão de algo para chegar até aqui. E por toda maturidade conquistada durante esses 2 anos de Mestrado. Que nunca duvidemos da força que temos.

"O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001."

RESUMO

Um importante invariante associado a um módulo graduado é a função de Hilbert. Através dele surgem outros invariantes, tais como o polinômio e a série de Hilbert. Um fato notável sobre esses três conceitos é que eles se relacionam com diversas outras informações do módulo graduado, a exemplo da dimensão de Krull, multiplicidade, resolução livre graduada, etc. Nesse trabalho de dissertação nosso objetivo é estudar propriedades sobre a função, o polinômio e a série de Hilbert bem como apresentar a conexão desses conceitos com outros como os já mencionados.

Palavras Chave: Função de Hilbert, Polinômio de Hilbert, Série de Hilbert, Resolução Livre Graduada, Multiplicidade.

ABSTRACT

An important invariant associated with a graded module is the Hilbert function. Through it other invariants arise, such as the polynomial and the Hilbert series. A notable fact about these three concepts is that they relate to various other information of the graded module, the example of the Krull dimension, multiplicity, graded free resolution, etc. In this work of dissertation our objective is to study properties of the function, the polynomial and the Hilbert series as well as presenting the connection of these concepts with others like those already mentioned.

Key-words: Hilbert Function, Hilbert Polynomial, Hilbert Series, Graded Free Resolution, Multiplicity.

Lista de símbolos

Símbolo	**Descrição**
$\ker \varphi$	núcleo de um homomorfismo φ
$\operatorname{Im} \varphi$	imagem de um homomorfismo φ
$\operatorname{ht} I$	altura de um ideal I
$\ell(M)$	comprimento de um módulo M.
I_i	componente homogênea (ou parte homogênea) de grau i do ideal I
Z	sizígia de M
$\mathcal{K}(f)$	sizígia de Koszul
e_i	i-ésimo vetor da base canônica de um módulo livre de posto finito.
$I_t(\Psi)$	ideal gerado pelos menores de ordem t de uma matriz Ψ
$\operatorname{Supp}(M)$	suporte do módulo M
$\operatorname{Ass}_R(M)$	conjunto dos primos associados de um R-módulo M
$\operatorname{posto}(\Psi)$	posto de uma matriz Ψ
$\dim M$	dimensão de Krull do módulo M
$h_R(M,-)$	função de Hilbert de um módulo graduado M
$P_M(t)$	polinômio de Hilbert de um módulo graduado M
$H_M(t)$	série de Hilbert de um módulo graduado M
$Z_R(M)$	conjunto dos divisores de zero de um R-módulo M
$\operatorname{Min}_A(M)$	coleção dos primos associados mínimos de M
$\operatorname{depth}_I(M)$	profundidade de M
$T_R(M)$	álgebra tensorial de um R-módulo M

Conteúdo

Introdução

Existem dois tipos de ambientes onde a álgebra comutativa se desenvolve de forma mais eficaz: o local e o graduado. Essa dissertação concentra-se nesse segundo ambiente. A grosso modo, os módulos graduados são objetos que se decompõe em pedaços menores que possuem uma boa estrutura. Do ponto de vista geométrico, eles são o lugar natural onde a geometria algébrica projetiva é descrita em termos algébricos.

Uma situação de destaque do ponto de vista algébrico e geométrico é quando os pedaços menores nos quais um módulo graduado M se decompõe são espaços vetoriais de dimensão finita M_n indexados pelo conjunto dos números inteiros $\mathbb{Z}$. Nesse caso, podemos estabelecer a função numérica $n \mapsto \dim_k M_n$. Essa função é justamente o que chamamos de *função de Hilbert* do módulo graduado M.

Por vários anos, funções de Hilbert têm sido objetos centrais e ferramentas frutíferas em vários campos, incluindo geometria algébrica, combinatória, álgebra comutativa e álgebra computacional. Houve um aumento no interesse e na pesquisa nos últimos anos; uma variedade de novas ideias e técnicas foram introduzidas e progressos substanciais foram feitos. Nessa dissertação nos concentraremos em escrever sobre alguns fatos dessas funções.

A seguir descrevemos brevemente o conteúdo de cada capítulo.

O primeiro capítulo é de preliminares. Nele fazemos um apanhado sucinto sobre conceitos de álgebra comutativa tais como: decomposição primária e primos associados, altura, dimensão de Krull, sistema de parâmetros, sequência regular, profundidade, módulos Cohen-Macaulay e sequências exatas. Esses conceitos serão importantes para o desenvolvimento do trabalho.

O capítulo 2 apresentamos o tipo de ambiente onde os conceitos de função, polinômio e série de Hilbert são definidos. Precisamente, tais conceitos fazem sentido no contexto dos módulos graduados. Assim, nos dedicamos nessa parte do trabalho em definir o que são módulos graduados, dar exemplos e demonstrar algumas propriedades básicas.

O capítulo 3 é onde iniciamos o conteúdo principal do trabalho. É feita a definição dos conceitos de função, polinômio e série de Hilbert. Um resultado central desse capítulo é o Teorema 3.2.5, o qual fundamenta a existência do polinômio de Hilbert e relaciona seu grau com a dimensão do módulo. Outro resultado importante é o Teorema 3.2.7, que fornece uma representação alternativa

para a série de Hilbert de um módulo graduado M como quociente $Q_M(t)/(1-t)^t$ onde $Q_M(t)$ é um elemento em $\mathbb{Z}[t, t^{-1}]$ unicamente determinado pelo módulo M. Finalizamos o capítulo discutindo a função de Hilbert dos ideais de pontos do plano projetivo.

O propósito do quarto capítulo é exibir relações entre a resolução livre graduada de um módulo e a função de Hilbert. Para isso definimos o que é uma resolução livre e graduada e como ela pode ser construída. Alguns exemplos de ideais onde a resolução livre e graduada é conhecida são apresentados. O Teorema 4.3.2 mostra como a série de Hilbert pode ser escrita em termos da resolução livre e graduada. Como uma aplicação desse resultado descrevemos uma curiosa relação entre os números de Betti e os *shifts* de uma resolução pura. Finalizamos o capítulo discutindo sobre o número de postulação.

Capítulo 1

Preliminares

O objetivo desse capítulo é fornecer material preliminar de álgebra comutativa que será útil para a parte principal do trabalho. Aqui não iremos priorizar a demonstração dos resultados, simplesmente faremos menção às referências. Em compensação, iremos dar prioridade ao cálculo de alguns exemplos. Este será um diferencial. Para as definições e resultados enunciados seguiremos de perto o livro [9], do professor Aron Simis.

1.1 Primos associados e decomposição primária

Seja M um módulo sobre um anel R. Um ideal primo P de R é dito *primo associado* de M se existe um elemento x de M tal que $P = 0 :_R x$. O conjunto de todos os primos associados de M será denotado por $\mathrm{Ass}_R(M)$. Os elementos minimais de $\mathrm{Ass}_R(M)$, com respeito a relação de inclusão, são chamados de *primos associados mínimos* de M. Denotaremos a coleção dos primos associados mínimos de M por $\mathrm{Min}_R(M)$. Os primos associados de M que não pertencem a $\mathrm{Min}_R(M)$ serão chamados de *primos associados imersos* de M.

Na proposição a seguir, bem como em todo o texto, usaremos $Z_R(M)$ para denotar o conjunto dos divisores de zero de um R-módulo M (recordemos que, por definição, $Z_R(M)$ é o conjunto de todos os elementos $a \in R$ tal que $ax = 0$ para algum $x \in M$ não nulo).

Proposição 1.1.1. *Sejam R um anel noetheriano e M um R-módulo finitamente gerado. Então:*

(a) $\mathrm{Ass}_R(M)$ *é vazio se, e somente se,* $M = 0$.

(b) $\mathrm{Ass}_R(M)$ *é um conjunto finito.*

(c) $Z_R(M) = \bigcup_{P \in \mathrm{Ass}_R(M)} P$.

(d) *Se N é um submódulo de M então* $\mathrm{Ass}_R(N) \subset \mathrm{Ass}_R(M) \subset \mathrm{Ass}_R(N) \cup \mathrm{Ass}_R(M/N)$.

Prova. Ver [8, Theorem 6.1, 6.3, 6.5]. □

Sejam M um módulo sobre um anel R e N um submódulo de M. É verificável que as seguintes condições são equivalentes:

(a) $\mathrm{Ass}_R(M/N)$ tem um único elemento.

(b) $Z_R(M/N) = \sqrt{N : M}$.

(c) Dados $a \in R$ e $x \in M$ tais que $ax \in N$ então $a \in \sqrt{N : M}$ ou $x \in N$.

Se N satisfaz uma (e portanto todas) dessas condições dizemos que N é um *submódulo primário* de M. Além disso, se P é o único primo de $\mathrm{Ass}_R(M/N)$, também dizemos que N é submódulo P-*primário* de M.

Observação 1.1.2. Seja I um ideal de um anel R. Dizer que I é um *ideal primário* de R significa que I é um submódulo primário de R. Observe que $I : R = I$. Assim, I é ideal primário se satisfaz uma (e portanto todas) das seguintes condições:

(a) $\mathrm{Ass}_R(R/I)$ tem um único elemento.

(b) $Z_R(R/I) = \sqrt{I}$.

(c) Dados $a, x \in R$ tais que $ax \in I$ então $a \in \sqrt{I}$ ou $x \in I$.

Exemplo 1.1.3. Seja P um ideal primo de um anel R. Notemos que nesse caso a condição (c) da Observação 1.1.2 é automática. Assim, todo ideal primo é primário.

Exemplo 1.1.4. Seja $\mathfrak{m}$ um ideal maximal de um anel R. Afirmamos que para qualquer inteiro positivo n o ideal $\mathfrak{m}^n$ é primário. Para provar essa afirmação iniciamos observando que $\mathrm{Ass}_R(R/\mathfrak{m}^n)$ é não vazio pois $R/\mathfrak{m}^n \neq \{0\}$. Dito isso, suponhamos P sendo um primo associado de $R/\mathfrak{m}^n$. Então, $P = 0 : x$ para algum $x \in R/\mathfrak{m}^n$ não nulo. Em particular, temos $\mathfrak{m}^n x = \{0\}$, ou seja, $\mathfrak{m}^n \subset P$. Como P é primo, segue dessa inclusão que $\mathfrak{m} \subset P$. Pela maximalidade de $\mathfrak{m}$ segue que $P = \mathfrak{m}$. Dessa forma, $\mathrm{Ass}_R(R/\mathfrak{m}^n) = \{\mathfrak{m}\}$. Portanto, da Observação 1.1.2(a) segue o afirmado.

Definição 1.1.5. Seja N um submódulo de um R-módulo M. Uma *decomposição primária* de N em M é uma interseção $N = \bigcap_{i=1}^{r} Q_i$ onde cada Q_i é submódulo P_i-primário de M. A decomposição primária $N = \bigcap_{i=1}^{r} Q_i$ é dita *reduzida* se $\mathrm{Ass}_R(M/Q_i) \neq \mathrm{Ass}_R(M/Q_j)$ sempre que $i \neq j$ e N não pode ser expresso como interseção de uma subcoleção própria dos Q_i.

Exemplo 1.1.6. Sejam $R = k[x, y, z]$ um anel de polinômios em três variáveis com coeficientes sobre um corpo k e $I = \langle xy, xz, yz \rangle$. Claramente, cada gerador do ideal I pertence a interseção

$\langle x, y\rangle \cap \langle x, z\rangle \cap \langle y, z\rangle$. Agora, suponhamos que f é um elemento arbitrário da interseção $\langle x, y\rangle \cap \langle x, z\rangle \cap \langle y, z\rangle$. Em particular, existem $a_i, b_i \in R$, com $1 \leqslant i \leqslant 3$, tais que

$$f = a_1x + b_1y = a_2x + b_2z = a_3y + b_3z.$$

Dessas igualdades segue, por exemplo, que:

$$a_1x = (a_3 - b_1)y + b_3z \quad \text{e} \quad b_1y = (a_1 - a_2)x + b_2z.$$

Logo, $a_1x \in \langle y, z\rangle$ e $b_1y \in \langle x, z\rangle$. Como $\langle y, z\rangle$ e $\langle x, z\rangle$ são ideais primos de R com $x \notin \langle y, z\rangle$ e $y \notin \langle x, z\rangle$ então $a_1 \in \langle y, z\rangle$ e $b_1 \in \langle x, z\rangle$. Assim, existem $\alpha_i, \beta_i \in R$, com $i = 1$ ou 2, tais que $a_1 = \alpha_1 y + \alpha_2 z$ e $b_1 = \beta_1 x + \beta_2 z$. Desse modo, $f = (\alpha_1 + \beta_1)xy + \alpha_2 xz + \beta_2 yz$, ou seja, $f \in I$. Com isso segue que a interseção $\langle x, y\rangle \cap \langle x, y\rangle \cap \langle x, y\rangle$ está contida no ideal I. Portanto, temos a igualdade

$$I = \langle x, y\rangle \cap \langle x, z\rangle \cap \langle y, z\rangle.$$

Como cada membro dessa interseção é ideal primo, segue que esta é uma decomposição primária para o ideal I.

Exemplo 1.1.7. Sejam $R = k[x, y]$ um anel de polinômios em duas variáveis sobre um corpo k e $I = \langle x^2, xy\rangle$. Considere a interseção $\langle x\rangle \cap \langle x, y\rangle^2$. Claramente, os geradores de I pertencem a interseção citada. Além disso, seja $f \in \langle x\rangle \cap \langle x, y\rangle^2$. Observe que $\langle x, y\rangle^2 = \langle x^2, y^2, xy\rangle$, assim, existem $a, b, c, d \in A$, tais que

$$f = ax = bx^2 + cy^2 + dxy.$$

Desse modo:

$$cy^2 = ax - bx^2 - dxy.$$

Então, $cy^2 \in \langle x\rangle$. Como $\langle x\rangle$ é primo e $y^2 \notin \langle x\rangle$, temos que $c \in \langle x\rangle$. Logo, existe $p \in A$, tal que $c = px$. Então, $f = bx^2 + cy^2 + dxy = bx^2 + pxy^2 + dxy \in \langle x^2, xy\rangle = I$. Desse modo,

$$I = \langle x\rangle \cap \langle x, y\rangle^2.$$

Pelo Exemplo 1.1.3 segue que $\langle x\rangle$ é primário e pelo Exemplo 1.1.4 segue que $\langle x, y\rangle^2$ também é primário. Portanto, $I = \langle x\rangle \cap \langle x, y\rangle^2$ é uma decomposição primária de I.

Teorema 1.1.8. *Sejam M um módulo finitamente gerado sobre um anel noetheriano R e N um submódulo de M. Então N admite uma decomposição primária reduzida $N = \bigcap_{i=1}^{r} Q_i$. Além disso,*

(i) $\mathrm{Ass}_R(M/N) = \{\sqrt{Q_1 : M}, \ldots, \sqrt{Q_r : M}\}$. *Em particular, os radicais* $\sqrt{Q_i : M}$ *em uma decomposição primária reduzida de* N *em* M *são unicamente determinados pelo quociente* M/N.

(ii) *Os submódulos primários* Q_i *que correspondem aos primos associados mínimos de* M/N *são unicamente determinados pelo quociente* M/N.

Prova. Ver [7, Theorem 3.2]. □

Exemplo 1.1.9. Sejam $R = k[x, y, z]$ um anel de polinômios em três variáveis com coeficientes sobre um corpo k e $I = \langle xy, xz, yz\rangle$. No Exemplo 1.1.6 vimos que uma decomposição primária de I é:

$$I = \langle x, y\rangle \cap \langle x, z\rangle \cap \langle y, z\rangle.$$

É imediato observar que essa é de fato uma decomposição primária reduzida. Segue do teorema da decomposição primária que para esse exemplo temos:

$$\mathrm{Ass}_R(R/I) = \mathrm{Min}_R(R/I) = \{(x, y), (x, z), (y, z)\}.$$

Observação 1.1.10. Sejam R um anel noetheriano e I um ideal de R. Afirmamos que um ideal primo P é primo associado mínimo de R/I se, e somente se, P é mínimo (com respeito a ordem de inclusão) entre os ideais primos de R que contém I. Com efeito, suponhamos que $I = \bigcap_{i=1}^{r} Q_i$ seja uma decomposição primária de I. Se P é um elemento mínimo na coleção dos ideais que contem I então, em particular, $P \supset \bigcap_{i=1}^{r} Q_i$. Como P é ideal primo, P contém um certo Q_i. Logo, $P = \sqrt{P} \supset \sqrt{Q_i}$. Como $\sqrt{Q_i}$ é ideal primo e contém I segue da minimalidade de P que $P = \sqrt{Q_i}$. Obviamente, $\sqrt{Q_i}$ é primo associado mínimo, pois caso contrário, isso contrariaria a minimalidade de P. Por outro lado, consideremos $\sqrt{Q_i}$ sendo um primo associado mínimo de R/I. Seja P_1 um ideal primo tal que $I = \bigcap_{i=1}^{r} Q_i \subset P_1 \subset \sqrt{Q_i}$. Da primalidade de P_1 segue que $Q_j \subset P_1$ para algum j. Logo, $\sqrt{Q_j} \subset P_1 \subset \sqrt{Q_i}$. Como $\sqrt{Q_i}$ é primo associado mínimo devemos ter $\sqrt{Q_i} = \sqrt{Q_j}$, ou seja, $P_1 = \sqrt{Q_i}$. Sendo assim, $\sqrt{Q_i}$ é minimo entre os ideais primos que contém I.

1.2 Altura e Dimensão de Krull

Seja R um anel. Uma sequência de inclusões de ideais primos

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n$$

de R é chamada uma *cadeia de ideais primos* de R. A quantidade de inclusões em uma cadeia de ideais primos de R é chamada de *comprimento* da cadeia de ideais primos de R.

Definição 1.2.1. Seja P um ideal primo de um anel R. A *altura* de P, denotada $\operatorname{ht} P$, é o supremo dos comprimentos das cadeias de ideais primos

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P.$$

Podemos ver facilmente que para domínios de ideais principais a altura de um ideal primo não nulo é sempre 1. Contudo, situações como essa são muito raras. Tipicamente, determinar a altura dos ideias primos de um anel não é uma tarefa fácil. Veremos abaixo um exemplo simples, onde uma estimativa para altura à luz da definição é trivial, mas a determinação do seu valor exato faz uso de resultados mais sutis.

Exemplo 1.2.2. Sejam k um corpo e R o anel de polinômios $k[x_1, \ldots, x_n]$. Para cada $1 \leqslant i \leqslant n$, considere o ideal primo $P_i = (x_1, \ldots, x_i)$. Temos a seguinte cadeia de ideais primos

$$(0) \subsetneq P_1 \subsetneq \cdots \subsetneq P_i.$$

Com essa cadeia podemos concluir que $\operatorname{ht} P_i \geqslant i$.

O conceito de altura pode ser estendido para um ideal arbitrário I do anel R da seguinte maneira:

$$\operatorname{ht} I = \min\{\operatorname{ht} P \mid P \text{ é ideal primo de } R \text{ que contém } I\}.$$

Obviamente, não precisamos calcular a altura de um ideal I olhando para todos os ideais primos de R que contém I. De fato, é suficiente avaliarmos o que acontece no *conjunto dos primos mínimos* de I, denotato, $\operatorname{Min}(I)$. Este conjunto é formado por todos os ideais primos que contém I e é mínimo, com respeito a ordem de inclusão, com essa propriedade.

Exemplo 1.2.3. Seja $I = (xy, xz, yz) \subset R = k[x, y, z]$. Obviamente, $(x, y), (x, z), (y, z)$ são ideais primos de R que contém I. Por outro lado, considere P um ideal primo de R que contém I. Em particular, $xy \in P$. Desse modo, x ou $y \in P$. Se ambos pertencem a P então $(x, y) \subset P$. Caso contrário, digamos que $y \notin P$. Então, como $yz \in P$ segue que $(x, z) \subset P$. Assim, P contém um dos 3 ideais $(x, y), (x, z), (y, z)$. Concluímos com isso que $\operatorname{Min}(I) = \{(x, y), (x, z), (y, z)\}$. Assim, para calcular a altura do ideal I é suficiente calcular a altura dos ideais $(x, y), (x, z), (y, z)$.

Um dos resultados mais fundamentais para a altura de ideais é:

Teorema 1.2.4 (Teorema do ideal primo de Krull)**.** *Sejam R um anel noetheriano e I um ideal gerado por n elementos. Então qualquer primo mínimo de I tem altura $\leqslant n$.*

Prova. Ver [9, Theorem 2.5.27]. □

Observe que, através do Teorema do ideal primo de Krull podemos concluir que a altura do ideal P_i no Exemplo 1.2.2 é exatamente i. Em particular, podemos concluir com isso que a altura do ideal $I = (xy, xz, yz) \subset R = k[x, y, z]$ no Exemplo 1.2.3 é exatamente 2.

Definição 1.2.5. Seja R um anel. A *dimensão de Krull* de R (ou simplesmente dimensão de R), denotada $\dim R$, é o supremo das alturas dos ideais primos de R, ou seja,

$$\dim R = \sup\{\operatorname{ht} P \mid P \text{ é ideal primo de } R\}.$$

A dimensão de Krull de um anel pode não ser finita mesmo para anéis noetherianos. Embora não exista uma cadeia de ideais primos infinita em um anel noetheriano, pode acontecer de existir cadeias com comprimentos finitos tão grande quanto se queira. Um exemplo desse fenômeno foi observado por Nagata (ver por exemplo [3, Exercise 9.6]).

Observação 1.2.6. Seja P um ideal primo de um anel R. Das propriedades básicas de localização segue que as cadeias de ideais primos $Q_0 \subsetneq Q_1 \subsetneq \cdots \subsetneq Q_n = P_P$ de R_P estão em correspondência biunívoca com as cadeias de ideais primos $P_0 \subseteq P_1 \subsetneq \cdots \subsetneq P_n = P$ de R. Em particular, podemos concluir com isso que $\operatorname{ht} P = \dim R_P$.

Exemplo 1.2.7. Seja R o anel de polinômios $k[x_1, \ldots, x_n]$ localizado no ideal maximal $(x_1, \ldots, x_n)$. Pela observação acima e pelos comentários logo após o Teorema 1.2.4 segue que $\dim R = n$.

Proposição 1.2.8. *Sejam* R *um anel e* I *um ideal de* R. *Então:*

$$\dim R/I + \operatorname{ht} I \leqslant \dim R. \tag{1.1}$$

Prova. Seja $\overline{P}$ um ideal primo de R/I. Então $\overline{P} = P/I$ para algum ideal primo P de R que contém I. Digamos que

$$\overline{P}_0 \subsetneq \cdots \subsetneq \overline{P}_n$$

seja uma cadeia de ideais primos de R/I. Pelo teorema da correspondência, $\overline{P}_i = P_i/I$ para únicos ideais primos P_i de R contendo I. Temos assim a cadeia

$$I \subset P_0 \subsetneq \cdots \subsetneq P_n.$$

Por outro lado, como $I \subset P_0$, é possível obter um cadeia $Q_0 \subsetneq \cdots \subsetneq Q_r = P_0$ de ideais primos de R tal que $r \geqslant \operatorname{ht} I$. Assim, temos a cadeia

$$Q_0 \subsetneq \cdots \subsetneq Q_r = P_0 \subsetneq \cdots \subsetneq P_n$$

cujo comprimento é $\geqslant n + \operatorname{ht} I$. Com isso, segue que o comprimento das cadeias de ideais primos construídas dessa maneira é $\geqslant \dim R/I + \operatorname{ht} I$. Em particular, segue o resultado. □

Observação 1.2.9. Existem diversas classes de anéis em que a desigualdade (1.1) é uma igualdade. Um exemplo disso são os anéis de polinômios e suas localizações.

O conceito de dimensão de Krull também se estende aos módulos. De fato, dado um R-módulo M definimos a dimensão de Krull de M como a dimensão de Krull do anel residual $R/0 :_R M$, onde $0 :_R M := \{a \in R \mid ax = 0 \text{ para todo } x \in M\}$.

1.3 Sistema de Parâmetros

Seja $M \neq \{0\}$ um módulo finitamente gerado sobre um anel local $(R, \mathfrak{m})$.

Definição 1.3.1. Um *sistema de parâmetros* de M é um conjunto de elementos $a_1, \ldots, a_s \in R$, com s menor possível, tal que $\dim M/(a_1, \ldots, a_s)M = 0$.

Denotaremos a cardinalidade de um sistema de parâmetros de um módulo M por $s(M)$.

Teorema 1.3.2 (Krull-Chevalley)**.** *Seja M um módulo finitamente gerado sobre um anel local $(R, \mathfrak{m})$. Então $s(M) = \dim M$.*

Prova. Ver [9, Theorem 5.1.11]. □

Observação 1.3.3. Um aspecto importante da demonstração do teorema de Krull-Chevalley é que é ensinado como calcular um sistema de parâmetros de um módulo finitamente gerado $M \neq \{0\}$ sobre um anel local $(R, \mathfrak{m})$. Precisamente, o primeiro elemento a_1 é escolhido no complementar em $\mathfrak{m}$ da união de todos os primos mínimos P de M tal que $\dim M = \dim M/PM$. Para essa escolha, temos $\dim M/(a_1)M = \dim M - 1$. O segundo elemento a_2 é escolhido no complementar em $\mathfrak{m}$ da união de todos os primos mínimos P de $\overline{M} := M/(a_1)M$ tal que $\dim \overline{M} = \overline{M}/P\overline{M}$. Continuamos a escolha dos demais a_i de forma indutiva.

Ilustramos esse método de calcular os elementos de um sistema de parâmetros no seguinte exemplo:

Exemplo 1.3.4. Consideremos o anel local $R = k[x, y, z]_{\mathfrak{m}}/(xy, xz, yz)_{\mathfrak{m}}$, onde $\mathfrak{m} = (x, y, z)$. Observe que

$$\begin{aligned} \dim R &= \dim k[x, y, z]_{\mathfrak{m}} - \operatorname{ht}(xy, xz, yz)_{\mathfrak{m}} \quad \text{(Observação 1.2.9)} \\ &= 3 - 2 \quad \text{(Observação 1.2.6 e comentário após Teorema 1.2.4)} \\ &= 1 \end{aligned}$$

Assim, um sistema de parâmetros de R é formado por um único elemento. Observe que o conjunto dos primos mínimos P de R tais que $\dim R = \dim P$ é $\{(x,y)_m, (x,z)_m, (y,z)_m\}$. Desse modo, pela observação anterior, para obter um elemento de R que constitui um sistema de parâmetros de R é suficiente encontrar um elemento f que não pertença aos ideais do conjunto $\{(x,y)_m, (x,z)_m, (y,z)_m\}$. Nesse caso, uma escolha possível é $f = x + y + z$.

1.4 Anéis e Módulos Cohen-Macaulay

Definição 1.4.1. Sejam R um anel noetheriano e M um R-módulo finitamente gerado. Um sequência de elementos $f_1, \ldots, f_m \in R$ é chamada *sequência regular* sobre M se satisfaz as seguintes condições:

(a) $M \neq (f_1, \ldots, f_m)M$.

(b) f_1 não é um divisor de zero de M e, para cada $1 \leqslant i \leqslant m-1$, f_{i+1} não é um divisor de zero de $M/(f_1, \ldots, f_i)M$

Um exemplo típico de sequência regular é a sequência de variáveis $x_1, \ldots, x_n$ em um anel de polinômios $D[x_1, \ldots, x_n]$ com coeficientes em um domínio D. De fato, x_1 é não divisor de zero de $D[x_1, \ldots, x_n]$ pois $D[x_1, \ldots, x_n]$ é domínio. De maneira similar, para cada $1 \leqslant i \leqslant n-1$, x_{i+1} não é divisor de zero de $D[x_1, \ldots, x_n]/(x_1, \ldots, x_i) \simeq D[x_{i+1}, \ldots, x_n]$ pois $D[x_{i+1}, \ldots, x_n]$ é domínio.

Definição 1.4.2. Sejam R um anel noetheriano, M um R-módulo finitamente gerado e I um ideal de R. A *profundidade* de M sobre I é o máximo comprimento de uma sequência regular sobre M contida em I.

Denotaremos a profundidade de M sobre I por $\operatorname{depth}_I(M)$.

Dizemos que uma sequência regular sobre M contida em I é de *comprimento maximal* se não existe nenhuma outra sequência regular em I a contendo propriamente. Obviamente, para calcularmos a profundidade de M sobre I é suficiente conhecermos as sequências regulares de comprimento maximal. O próximo resultado nos garantirá que não é necessário conhecermos todas as sequências regulares de comprimento maximal para podermos determinar $\operatorname{depth}_I(M)$.

Teorema 1.4.3. *Sejam R um anel noetheriano, M um R-módulo finitamente gerado e I um ideal de R tal que $IM \neq M$. Então:*

(a) *Qualquer sequência regular sobre M contida em I está contida em uma sequência regular de comprimento maximal.*

(b) *Quaisquer duas sequências regulares sobre M contida em I de comprimento maximal tem o mesmo comprimento.*

Em particular, $\operatorname{depth}_I(M)$ *é finito e é atingido como comprimento de qualquer sequência regular sobre* M *de comprimento maximal em* I.

Prova. Ver [9, Theorem 5.3.5]. □

Seja $(R, \mathfrak{m})$ é um anel noetheriano local com ideal maximal $\mathfrak{m}$. Usaremos a notação simplificada $\operatorname{depth}(M)$ para denotar a profundidade de M sobre o ideal maximal $\mathfrak{m}$.

Observe pela Proposição 1.1.1(c) que para obtermos uma sequência regular $a_1, \ldots, a_n \in R$ sobre um R-módulo M devemos, para cada $1 \leqslant i \leqslant n$, escolher a_i de modo que não pertença a nenhum primo associado P do R-módulo $M/(a_1, \ldots, a_{i-1})M$. Por mais forte razão, cada a_i deverá ser escolhido de modo a evitar todos os primos associados de $M/(a_1, \ldots, a_{i-1})M$ tais que $\dim M/(a_1, \ldots, a_{i-1})M = \dim M - (i-1)$. Assim, em virtude da Observação 1.3.3 segue o seguinte fato:

Proposição 1.4.4. *Sejam* $(R, \mathfrak{m})$ *um anel noetheriano local e* M *um* R*-módulo finitamente gerado. Então toda sequência regular* $a_1, \ldots, a_n$ *sobre* M *é parte de um sistema de parâmetros de* M. *Em particular,* $\operatorname{depth} M \leqslant \dim M$.

Apresentamos a seguir o principal conceito dessa seção.

Definição 1.4.5. Sejam $(R, \mathfrak{m})$ um anel noetheriano local e M um R-módulo finitamente gerado. Dizemos que M é um *módulo Cohen-Macaulay* se $\operatorname{depth} M = \dim M$. Diremos que o anel R é *anel Cohen-Macaulay* se ele o for como R-módulo.

Em geral, para um anel noetheriano R e um R-módulo finitamente gerado M diremos que M é módulo Cohen-Macaulay se $M_{\mathfrak{m}}$ é $R_{\mathfrak{m}}$-módulo Cohen-Macaulay para todo ideal maximal $\mathfrak{m}$ de R.

Exemplo 1.4.6. Seja k um corpo e $R = k[x_1, \ldots, x_n]_{(x_1,\ldots,x_n)}$. Pela Observação 1.2.6 temos $\dim R = \operatorname{ht}(x_1, \ldots, x_n) = n$. Como visto acima, $x_1, \ldots, x_n \in (x_1, \ldots, x_n)_{(x_1,\ldots,x_n)}$ é uma sequência regular sobre R. Assim, $n \leqslant \operatorname{depth} R$. Por outro lado, pela Proposição 1.4.4, $\operatorname{depth} \leqslant \dim R = n$. Portanto, $\operatorname{depth} R = \dim R = n$ e, consequentemente, R é anel Cohen-Macaulay.

1.5 Sequências exatas

Seja R um anel. Uma sequência finita ou infinita de homomorfismos de R-módulos

$$\cdots \longrightarrow M_{i+1} \xrightarrow{\varphi_{i+1}} M_i \xrightarrow{\varphi_i} M_{i-1} \xrightarrow{\varphi_{i-1}} \cdots$$

é chamada de *sequência exata* se $\operatorname{Im}\varphi_{i+1} = \ker \varphi_i$ para cada i.

Alguns fatos básicos sobre sequências exatas estão contidos na seguinte proposição.

Proposição 1.5.1. *Sejam* M *e* N *módulos sobre um anel* R*. Então:*

(a) *A sequência* $0 \longrightarrow \mathrm{M} \xrightarrow{\varphi} \mathrm{N}$ *é exata se, e somente se,* φ *é homomorfismo injetor.*

(b) *A sequência* $\mathrm{M} \xrightarrow{\varphi} \mathrm{N} \longrightarrow 0$ *é exata se, e somente se,* φ *é homomorfismo sobrejetor.*

(c) *A sequência* $0 \longrightarrow \mathrm{M} \xrightarrow{\varphi} \mathrm{N} \longrightarrow 0$ *é exata se, e somente se,* φ *é isomorfismo.*

Demonstração. (a) Suponhamos que a sequência $0 \to \mathrm{M} \xrightarrow{\varphi} \mathrm{N}$ é exata. Então $\ker \varphi = \mathrm{Im}(0 \to \mathrm{M}) = 0$. Logo, φ é um homomorfismo injetor. Reciprocamente, suponhamos que φ seja um homomorfismo injetor. Então $\ker \varphi = 0 = \mathrm{Im}(0 \to \mathrm{M})$. Portanto, a sequência $0 \to \mathrm{M} \xrightarrow{\varphi} \mathrm{N}$ é exata.

(b) Suponhamos que a sequência $\mathrm{M} \xrightarrow{\varphi} \mathrm{N} \to 0$ é exata. Então $\mathrm{Im}\varphi = \ker(\mathrm{N} \to 0) = \mathrm{N}$. Portanto, φ é um homomorfismo sobrejetor. Reciprocamente, suponhamos que φ seja um homomorfismo sobrejetor. Então $\mathrm{Im}\varphi = \mathrm{N} = \ker(\mathrm{N} \to 0)$. Portanto, a sequência $\mathrm{M} \xrightarrow{\varphi} \mathrm{N} \to 0$ é exata.

(c) Pelos itens (a) e (b) acima, φ é um homomorfismo injetor e sobrejetor. Logo, φ é um isomorfismo. □

Capítulo 2

Anéis e módulos graduados

Objetos muito importantes para a álgebra comutativa e geometria algébrica são a função e o polinômio de Hilbert de um módulo graduado. Estes são invariantes do módulo que codificam diversas informações tais como: dimensão, multiplicidade, números de Betti, etc. Nesse capítulo iniciaremos explicando em qual tipo de ambiente faz sentido falar da função e polinômio de Hilbert. Em seguida, apresentaremos suas definições e algumas propriedades básicas. Usamos como principal referência nesse capítulo o livro [1].

2.1 Conceitos básicos

Seja $(G, +)$ um *monóide comutativo*, isto é, um conjunto munido com uma operação associativa, comutativa e possuindo elemento neutro. Um anel R é dito G-*graduado* se seu grupo aditivo $(R, +)$ admite uma decomposição em soma direta de subgrupos abelianos R_g

$$R = \bigoplus_{g \in G} R_g$$

satisfazendo $R_g R_h \subseteq R_{g+h}$, para todos $g, h \in G$.

Os elementos R_g são chamados de *elementos homogêneos de grau* g do anel graduado R. Em particular, todo elemento $a \in R$ pode ser escrito de forma única como uma soma finita $a = \sum_{g \in G} a_g$ de elementos homogêneos $a_g \in R_g$. Dizemos nesse caso que a_g é a *componente homogênea de grau* g de a.

Tipicamente, iremos considerar nesse trabalho anéis graduados em que $G = \mathbb{N}$, $\mathbb{Z}$, $\mathbb{N}^n$ ou $\mathbb{Z}^n$.

Observação 2.1.1. Qualquer anel R admite ao menos uma G-graduação. Para isso, basta considerarmos $R_0 = R$ e $R_g = 0$ para cada $g \neq 0$. Chamamos esta de *graduação trivial* de R. Certamente, esta é uma graduação "grosseira"que não produz nenhuma informação adicional.

Exemplo 2.1.2. Seja S um anel. O exemplo padrão de anel $\mathbb{N}$-graduado é o anel de polinômios $R = S[x_1, \ldots, x_n]$. Sua $\mathbb{N}$-graduação usual é dada pela seguinte decomposição

$$R = \bigoplus_{d \geqslant 0} R_d,$$

onde R_d é o S-módulo livre de posto $\binom{n+d-1}{d-1}$ com base formada por todos os monômios de grau d.

Exemplo 2.1.3. Considere o polinômio $f(x, y, z) = x + 2y - z + x^2 + xy + y^3 + \frac{1}{2}zx^3 \in R = \mathbb{Q}[x, y, z]$. Usando a graduação de R descrita no Exemplo 2.1.2 temos que a escrita de f como soma de polinômios homogêneos f_i de grau i é da seguinte forma:

$$f = f_1 + f_2 + f_3 + f_4$$

onde $f_1 = x + 2y - z$, $f_2 = x^2 + xy$, $f_3 = y^3$ e $f_4 = \frac{1}{2}zx^3$.

Fixado um monóide comutativo G, podemos notar os anéis G-graduados como os objetos de uma categoria onde os morfismos são definidos da seguinte maneira.

Definição 2.1.4. Um morfismo $\varphi : R \to S$ entre dois anéis G-graduados é dito ser *morfismo graduado* se preserva gradução, isto é, se $\varphi(R_g) \subseteq S_g$ para todo $g \in G$.

É de imediata observação que:

1. Se R é um anel G-graduado então o mapa identidade $\mathrm{id}_R : R \to R$ é um morfismo graduado.
2. Se $\varphi : R \to S$ e $\psi : S \to T$ são morfismos graduados então $\psi \circ \varphi : R \to T$ é um morfismo graduado.

A associatividade entre os morfismos é consequência da associatividade de funções. Portanto, como afirmado anteriormente, o conjunto dos anéis G-graduados junto com a coleção dos morfismos de módulos graduados é de fato uma categoria.

Seja R um anel G-graduado. Dizemos que um R-módulo M é G-*graduado* se $(M, +)$ admite uma decomposição em soma direta de subgrupos abelianos M_g

$$M = \bigoplus_{g \in G} M_g$$

compatível com a graduação de R, ou seja, $R_g.M_h \subseteq M_{g+h}$ para todos $g, h \in G$.

Tal como no caso dos anéis graduados, os elementos em M_g são chamados de *homogêneos de grau* g e todo elemento em M pode ser escrito de forma única como soma de elementos homogêneos. Além disso, um morfismo de R-módulos será dito *graduado* se preserva graduação.

Dado um R-módulo G-graduado M e um elemento $d \in G$ podemos definir um novo R-módulo graduado da seguinte maneira

Definição 2.1.5. O *deslocamento* de M pelo elemento d, denotado $M(d)$, é o R-módulo G-graduado onde $M(d)_i = M_{i+d}$ para cada $i \in G$. O número d será chamado *shift* do deslocamento.

Exemplo 2.1.6. Seja S um anel. Considere o anel de polinômios em n variáveis $R = S[x_1, \ldots, x_n]$ pensado com a $\mathbb{N}$-graduação descrita no Exemplo 2.1.2. Se pensamos R como R-módulo com a graduação usual temos que os elementos constantes de R tem grau zero. Todavia, quando pensamos em termos de $R(-2)$ os elementos constantes tem grau 2.

Dado $R = \bigoplus_{n\in\mathbb{Z}} R_n$ um anel $\mathbb{Z}$-graduado, podemos notar R_0 como subanel de R. Sendo assim, podemos enxergar R como álgebra sobre R_0. Além disso, cada componente M_n de um R-módulo graduado M pode ser considerada como R_0-módulo.

2.2 Propriedades básicas

Abaixo seguem algumas propriedades sobre anéis e módulos $\mathbb{N}$-graduados.

Proposição 2.2.1. *Seja* $R = \bigoplus_{d\in\mathbb{N}} R_d$ *um anel graduado. Então* R *é noetheriano se, e só se,* R_0 *é noetheriano e* R *é finitamente gerado como álgebra sobre* R_0.

Prova. Se R é finitamente gerado como álgebra sobre R_0 então R é isomorfo a um quociente do anel de polinômios $R_0[x_1, \ldots, x_n]$. Como R_0 é noetheriano então pelo teorema da base de Hilbert, segue que R é noetheriano. Reciprocamente, se R é noetheriano, então R_0 é noetheriano, pois $R_0 \cong R/I$, onde I é o ideal $\bigoplus_{d\geqslant 1} R_d$. Agora, mostraremos que R é finitamente gerado sobre R_0. Para isso, necessitamos da seguinte afirmação:

Afirmação. Existe um conjunto finito de elementos homogêneos de R que geram I.

Como R é noetheriano, então existe um conjunto finito $\{b_1, \ldots, b_s\}$ de elementos em R que gera I. Como $I = \bigoplus_{d\geqslant 1} R_d$ então podemos escrever cada b_i da seguinte maneira:

$$b_i = a_{i,1} + \cdots + a_{i,d_i}$$

onde $a_{i,j} \in R_j \subset I$ para cada $j = 1, \ldots, d_i$. Assim, dado $b \in I$ temos:

$$b = \sum c_i b_i = \sum_{i=1}^{s} c_i(a_{i,1} + \cdots + a_{i,d_i})$$

Portanto, $\{a_{1,1},\dots,a_{1,d_1}\}\cup\cdots\cup\{a_{s,1},\dots,a_{s,d_s}\}$ é um conjunto finito de geradores homogêneos de I.

Da afirmação anterior podemos supor $a_1,\dots,a_r$ elementos homogêneos de R, com respectivos graus $n_1,\dots,n_r$, que geram I. Seja, $R' = R_0[a_1,\dots,a_n]$. Mostraremos que $R = R'$. Para tal, é suficiente mostrar que $R_n \subseteq R'$, para todo $n \geqslant 0$. Pela definição de R', temos que $R_0 \subseteq R'$. Por indução, assuma que $R_d \subseteq R'$ para todo $d \leqslant n-1$, e $n > 0$. Se $a \in R_n \subseteq I$, então a pode ser escrito na forma $a = c_1a_1 + \cdots + c_ra_r$, onde cada c_i é um elemento homogêneo de grau $n - n_i < n$. Por hipótese de indução temos que $c_i \in R'$, e como $a_i \in R'$, segue que $a \in R'$. □

Proposição 2.2.2. *Seja* $R = \bigoplus_{n\in\mathbb{N}} R_n$ *um anel graduado. Assuma que* R_0 *é artiniano e* R *é finitamente gerado como álgebra sobre* R_0. *Se* $M = \bigoplus_{n\in\mathbb{N}} M_n$ *é um* R*-módulo graduado finitamente gerado, então cada* M_n *é finitamente gerado como* R_0*-módulo.*

Prova. Temos em particular que R_0 é noetheriano. Como R é finitamente gerado como R_0-álgebra, segue pela Proposição 2.2.1 que R é noetheriano, donde M é R-módulo noetheriano. Seja $N_n = M_n \oplus (\bigoplus_{m>n} M_m)$. Desse modo, N_n é finitamente gerado sobre R, digamos por $x_1, x_2, \dots, x_t$. Por definição de N_n, cada x_i pode ser escrito como $x_i = y_i + z_i$, com $y_i \in M_n$ e $z_i \in \bigoplus_{m>n} M_m$. Mostraremos que $y_1,\dots,y_t$ geram M_n sobre R_0. Com efeito, se $y \in M_n$, então y é da forma

$$y = \sum_{i=1}^{t} a_i x_i \qquad (a_i \in R).$$

Pela graduação de R, podemos escrever $a_i = b_i + c_i$ com $a_i \in R_0$ e $c_i \in (\bigoplus_{j>0} R_j)$. Dessa forma, teremos

$$y = \sum_{i=1}^{t} (b_i + c_i)(y_i + z_i) = \sum_{i=1}^{t} b_i y_i,$$

pois os elementos b_iz_i, c_iy_i e c_iz_i estão em $\bigoplus_{m>n} M_m$. □

Corolário 2.2.3. *Com as mesmas hipóteses da* Proposição 2.2.2*, o comprimento* $\ell_{R_0}(M_n)$ *do* R_0*-módulo* M_n *é finito para todo* $n \geqslant 0$.

Prova. Como R_0 é artiniano (noetheriano), M_n é artiniano (noetheriano), e pela Proposição 2.2.2, M_n é R_0-módulo finitamente gerado, segue que $\ell_{R_0}(M_n) < \infty$. □

Definição 2.2.4. Considere R um anel G-graduado e M um R-módulo G-graduado. Um submódulo $N \subseteq M$ é dito G-*graduado* se N herda a graduação de M, isto quer dizer que, $(N, +)$ se decompõe como

$$N = \bigoplus_{g\in G} N \cap M_g$$

Em especial, um ideal $I \subseteq R$ é dito ser *ideal homogêneo* se I é submódulo graduado de R, visto como R-módulo.

Segue direto da Definição 2.2.4 que o quociente de M por N admite uma graduação de maneira natural

$$\frac{M}{N} = \bigoplus_{g \in G} \frac{M_g}{N \cap M_g}.$$

Além disso, também temos a sequência exata de módulos G-graduados

$$0 \to N \to M \to M/N \to 0.$$

A próxima proposição caracteriza ideais homogêneos em termos de elementos homogêneos.

Proposição 2.2.5. *Considere* $(G, +)$ *um grupo abeliano,* $R = \bigoplus_{g \in G} R_g$ *um anel* G*-graduado e* $I \subseteq R$ *um ideal. Então, são equivalentes:*

(a) I *é ideal homogêneo.*

(b) *Para todo* $a = \sum_{g \in G} a_g$ *em* R*,* a *pertence a* I *se, e somente se,* $a_g \in I$ *para todo* $g \in G$.

(c) I *é gerado por elementos homogêneos.*

Demonstração. A equivalência entre (a) e (b), e a implicação de (b) para (a), seguem simplesmente das definições. Para a implicação de (c) para (a) suponha que I seja gerado pelos elementos homogêneos a_i. Daí, para cada $a \in I$ podemos escrever $a = b_1 a_{i_1} + \cdots + b_n a_{i_n}$ com $b_i \in R$. Escreva cada $b_i = \sum_{g \in G} b_{i,g}$, com $b_{i,g} \in R_g$. Assim, o termo de grau g em a é

$$a_g = b_{1,g-\deg(a_{i_1})} a_{i_1} + \cdots + b_{n,g-\deg(a_{i_n})} a_{i_n},$$

donde $a_g \in I$. □

Capítulo 3

Função e polinômio de Hilbert

Neste capítulo fazemos a definição dos conceitos de função, polinômio e série de Hilbert. Um resultado central desse capítulo é o Teorema 3.2.5, o qual fundamenta a existência do polinômio de Hilbert e relaciona seu grau com a dimensão do módulo. Outro resultado importante é o Teorema 3.2.7, que fornece uma representação alternativa para a série de Hilbert de um módulo graduado M como quociente $Q_M(t)/(1-t)^t$ onde $Q_M(t)$ é um elemento em $\mathbb{Z}[t, t^-1]$ unicamente determinado pelo módulo M. Finalizamos o capítulo discutindo a função de Hilbert dos ideais de pontos do plano projetivo.

3.1 O operador diferença

Definição 3.1.1. Definimos o *operador diferença* (ou *derivada discreta*) de uma função $f : \mathbb{Z} \to \mathbb{Q}$ por

$$\Delta f(n) = f(n+1) - f(n).$$

Se $d \geqslant 0$ denotaremos as d iterações do operador diferença por $\Delta^d f$, convencionando $\Delta^0 f = f$.

Definição 3.1.2. Um *polinômio binomial* é um polinômio em $\mathbb{Q}[x]$ da forma, $(d \in \mathbb{Z})$

$$\binom{x}{d} = \begin{cases} \dfrac{x(x-1)(x-2)\cdots(x-d+1)}{d!}, & \text{se } d \geqslant 0; \\ 0, & \text{se } d < 0; \end{cases}$$

Observe que $\binom{x}{d}$ é um polinômio de grau d para cada $d \in \mathbb{N}$.

Observação 3.1.3. Como é bem conhecido, $\binom{n+1}{d} = \binom{n}{d} + \binom{n}{d-1}$ para cada $n \in \mathbb{N}$. Assim, o polinômio $p(x) = \binom{x+1}{d} - \binom{x}{d} - \binom{x}{d-1}$ possui infinitas raízes em $\mathbb{Q}$. Logo, $p(x)$ deve ser o

polinômio nulo, ou seja,

$$\Delta\binom{x}{d} = \binom{x}{d-1}.$$

Definição 3.1.4. Uma função $f : \mathbb{Z} \to \mathbb{Q}$ é dita de *tipo-polinomial* se assintoticamente concorda com um polinômio $g(x) \in \mathbb{Q}[x]$, isto é, $f(n) = g(n)$ para todo inteiro $n \gg 0$. O *grau* de f será tomado como o grau de g.

Note que o grau de f está bem definido. Com efeito, se tivéssemos dois polinômios concordando com f para valores suficientemente grandes, então a diferença entre eles seria um polinômio com infinitas raízes, logo seria o polinômio nulo. Convencionaremos que o grau do polinômio nulo é igual a -1.

Proposição 3.1.5. *As seguintes propriedades são verificadas:*

(a) *Seja* $p(x) \in \mathbb{Q}[x]$ *um polinômio de grau* d. *Então* $p(n) \in \mathbb{Z}$ *para todo inteiro* $n \gg 0$ *se, e só se,* $p(x)$ *é uma combinação* $\mathbb{Z}$*-linear de polinômios binomiais.*

(b) *Considere uma função* $f : \mathbb{Z} \to \mathbb{Z}$. *Então* f *é de tipo-polinomial de grau* d *se, e só se,* Δf *é de tipo-polinomial de grau* $d - 1$.

Demonstração. (a) De fato, qualquer combinação $\mathbb{Z}$-linear de polinômios binomiais assume valores inteiros. Suponha então, que $p(n) \in \mathbb{Z}$ para todo inteiro $n \gg 0$. Argumentaremos por indução sobre d que $p(x)$ é uma combinação $\mathbb{Z}$-linear de polinômios binomiais. Se $d = 0$, o resultado é claro. Suponha $d > 0$. Os polinômios binomiais $\binom{x}{i}$ formam uma $\mathbb{Q}$-base de $\mathbb{Q}[x]$, e assim podemos escrever

$$p(x) = a_d\binom{x}{d} + a_{d-1}\binom{x}{d-1} + \cdots + a_1\binom{x}{1} + a_0\binom{x}{0} \qquad (a_i \in \mathbb{Q}).$$

Devemos mostrar que $a_i \in \mathbb{Z}$. Para tal, considere a derivada discreta

$$\Delta p(x) = a_d\binom{x}{d-1} + a_{d-1}\binom{x}{d-2} + \cdots + a_1\binom{x}{0}.$$

Por hipótese, $\Delta p(n) = p(n+1) - p(n) \in \mathbb{Z}$ para todo $n \gg 0$. Então, pela hipótese de indução $a_d, \ldots, a_1 \in \mathbb{Z}$. Daí,

$$a_0 = p(x) - a_d\binom{x}{d} - a_{d-1}\binom{x}{d-1} - \cdots - a_1\binom{x}{1}$$

é um polinômio constante que assume valores inteiros. Portanto, $a_0 \in \mathbb{Z}$.

(b) Se f é de tipo-polinomial de grau d, pelo item anterior podemos escrever seu polinômio correspondente da forma

$$p(x) = a_d\binom{x}{d} + a_{d-1}\binom{x}{d-1} + \cdots + a_1\binom{x}{1} + a_0\binom{x}{0} \qquad (a_i \in \mathbb{Z}).$$

Pela Observação 3.1.3,

$$\Delta p(x) = a_d\binom{x}{d-1} + a_{d-1}\binom{x}{d-2} + \cdots + a_1\binom{x}{0}.$$

Portanto, Δf é de tipo-polinomial de grau $d-1$. Para a recíproca, suponha que $q(x)$ é o polinômio correspondente a Δf. Utilizando o item anterior novamente podemos escrever

$$q(x) = a_d\binom{x}{d-1} + a_{d-1}\binom{x}{d-2} + \cdots + a_1\binom{x}{0} \qquad (a_i \in \mathbb{Z}).$$

Consideremos a "integral discreta" de $q(x)$:

$$r(x) = a_d\binom{x}{d} + a_{d-1}\binom{x}{d-1} + \cdots + a_1\binom{x}{1}.$$

Pela Observação 3.1.3, $\Delta r(x) = q(x)$. Logo, $\Delta(f-r)(n) = 0$ para todo $n \gg 0$, ou seja, uma constante $a_0 = f(n) - r(n)$. Assim, se consideramos $p(x) = r(x) + a_0$, temos um polinômio de grau d e ainda para todo $n \gg 0$, $p(n) = r(n) + f(n) - r(n) = f(n)$. □

Utilizando o princípio de indução e a parte (b) da proposição anterior temos o seguinte:

Corolário 3.1.6. *Sejam $f : \mathbb{Z} \to \mathbb{Z}$ uma função numérica e $d \geqslant 0$ um inteiro. As seguintes condições são equivalentes:*

(a) $\Delta^d f(n) = c$, $c \neq 0$ *e* $n \gg 0$.

(b) *f é de tipo-polinomial de grau* d.

Prova. A implicação de (b) para (a) é clara, uma vez que se escrevemos o polinômio correspondente a f em termos de polinômios binomiais, a cada iteração do operador diferença o grau deste decai em 1. Por indução em d provaremos a outra implicação. Se $d = 0$, então o corolário é trivialmente satisfeito. Suponha agora $d > 0$. Como $\Delta^d f(n) = \Delta^{d-1}(\Delta f(n)) = c$, $c \neq 0$ e $n \gg 0$, por hipótese de indução $\Delta f(n)$ é de tipo-polinomial de grau $d-1$ e dessa forma, pela Proposição 3.1.5, f é de tipo-polinomial de grau d. □

3.2 Função de Hilbert

Definição 3.2.1. Sejam $R = \bigoplus_{n\in\mathbb{Z}} R_n$ um anel graduado e $M = \bigoplus_{n\in\mathbb{Z}} M_n$ um R-módulo graduado cujas componentes possuem comprimento finito para todo n. A *função de Hilbert* é definida por

$$h_R(M,n) = \ell_{R_0}(M_n)$$

Exemplo 3.2.2. Seja k um corpo e $R = k[x_1,\dots,x_r]$. Então uma k-base de R_n é formada pelos monômios de grau n em $x_1,\dots,x_r$. Daí,

$$h(R,n) = \ell_k(R_n) = \dim_k R_n = \binom{n+r-1}{r-1}$$

é uma função polinomial de grau $r-1$.

Mostraremos que sob certas condições que a função de Hilbert é de tipo-polinomial. Para isto, precisamos de mais alguns preparativos. Começamos com a seguinte proposição:

Proposição 3.2.3 (**Aditividade do Comprimento).** *Suponha que temos uma sequência exata de* R*-módulos*

$$0 \to A_n \xrightarrow{d_{n-1}} A_{n-1} \to \cdots \xrightarrow{d_1} A_1 \to 0$$

com todos os comprimentos finitos. Então, temos a aditividade do comprimento, isto é,

$$\ell(A_1) - \ell(A_2) + \cdots + (-1)^{n-1}\ell(A_n) = 0.$$

Prova. A sequência exata dada pode ser decomposta nas seguintes sequências exatas:

$$0 \to \ker d_1 \to A_2 \to A_1 \to 0,$$

$$0 \to \ker d_2 \to A_3 \to \ker d_1 \to 0,$$

$$\vdots$$

$$0 \to \ker d_i \to A_{i+1} \to \ker d_{i-1} \to 0,$$

$$\vdots$$

$$0 \to \ker d_{n-2} \to A_{n-1} \to \ker d_{d-3} \to 0,$$

$$0 \to A_n \to \ker d_{n-2} \to 0.$$

Mas, para uma sequência exata $0 \to N \to M \to Q \to 0$ de módulos de comprimento finito é conhecido que $\ell(M) = \ell(N) + \ell(Q)$. Assim, aplicando esse fato nas sequências exatas acima

obtemos:

$$\ell(A_1) + \ell(\ker d_1) - \ell(A_2) = 0,$$

$$\ell(A_3) - \ell(\ker d_1) - \ell(\ker d_2) = 0,$$

$$\vdots$$

$$(-1)^{i+1}(\ell(A_{i+1} - \ell(\ker d_i) - \ell(\ker d_{i+1})) = 0,$$

$$\vdots$$

$$(-1)^{n-1}(\ell(A_{n-1} - \ell(\ker d_{n-2}) - \ell(\ker d_{n-3})) = 0,$$

$$(-1)^{n-1}(\ell(A_n - \ell(\ker d_{n-2})) = 0.$$

Somando todas essas igualdades membro a membro e efetuando os devidos cancelamentos obtemos o resultado desejado. □

O próximo teorema nos diz condições suficientes para que a função de Hilbert seja de tipo-polinomial.

Teorema 3.2.4 (Hilbert). *Seja* $R = \bigoplus_{n\geqslant 0} R_n$ *um anel graduado. Assuma que* R_0 *é artiniano e* R *é finitamente gerado como álgebra sobre* R_0*, com todos os geradores* $a_1, \ldots, a_r$ *pertencentes a* R_1*. Se* M *é* R*-módulo graduado finitamente gerado, então sua função de Hilbert é do tipo-polinomial de grau no máximo* $r - 1$.

Prova. Utilizaremos indução sobre r. Se $r = 0$, então $R = R_0$. Escolha um conjunto finito de geradores homogêneos de M sobre R. Se d é o máximo dos graus desses geradores, então $M_n = 0$ para todo $n > d$, implicando que $h(M, n) = 0$. Assim, a função de Hilbert concorda com o polinômio nulo para valores suficientemente grandes. Suponha então $r > 0$. Sejam $a_r \in R_1$ e $\lambda_r : M_n \to M_{n+1}$ a multiplicação por a_r. Denote por K_n o kernel de λ_r e por C_n o cokernel[1] de λ_r. Então, temos a sequência exata

$$0 \longrightarrow K_n \longrightarrow M \xrightarrow{\lambda_r} M_{n+1} \longrightarrow C_n \longrightarrow 0.$$

Sejam $K = \oplus_{n\geqslant 0} K_n$ e $C = \oplus_{n\geqslant 0} C_n$. Assim, K é submódulo de M e C é um quociente de M, logo são finitamente gerados. Então pelo Corolário 2.2.3, $h(K, n) < \infty$ e $h(C, n) < \infty$. Pela Proposição 3.2.3, temos

$$h(K, n) - h(M, n) + h(M, n + 1) - h(C, n) = 0.$$

Daí, $\Delta h(M, n) = h(C, n) - h(K, n)$ Por outro lado, observe que a_r anula K e C, logo K e C são

[1] Relembremos que o cokernel de um homomorfismo $\varphi : M \to N$ de R-módulos é o R-módulo quociente $N/\mathrm{Im}(\varphi)$

finitamente gerados como T-módulos, onde T é o subanel gerado por $a_1, \ldots, a_{r-1}$. Por hipótese de indução, $h(K, n)$ e $h(C, n)$ são de tipo-polinomial de graus no máximo $r-2$, implicando que $\Delta h(M, n)$ também é. Donde pela Proposição 3.1.5, $h(M, n)$ é de tipo-polinomial de grau no máximo $r-1$. □

Um anel como no Teorema 3.2.4, adicionado com a localidade na componente de grau zero é chamado de *anel homogêneo*. Veremos abaixo que a desigualdade obtida no Teorema de Hilbert passa a ser igualdade no caso de anéis homogêneos.

Teorema 3.2.5. *Seja* R *um anel homogêneo e* M *um* R*-módulo graduado finitamente gerado de dimensão* d*. Então a função de Hilbert* $h(M, n)$ *é de tipo-polinomial de grau* $d-1$.

Prova. Se $M = 0$, o polinômio nulo (de grau -1), satisfaz o teorema. Então, assuma $M \neq 0$. Dessa forma, escolha $P_1 \in \operatorname{Ass}(M)$. Então, P_1 é ideal homogêneo e existe submódulo graduado $N_1 \subseteq M$ tal que $N_1 \cong (R/P_1)(a_1)$. Se $N_1 \neq M$, escolhamos $P_2 \in \operatorname{Ass}(M/N_1)$. Como antes, existe submódulo graduado $N_2 \subseteq M$, com $N_2/N_1 \cong (R/P_2)(a_2)$. Continuando dessa maneira, como M é noetheriano conseguimos uma cadeia finita

$$0 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_m = M$$

de submódulos graduados de M tais que $N_{i+1}/N_i \cong (R/P_i)(a_i)$, para cada $i = 1, \ldots, m$. Assim, por definição $h(M, n) = \sum_{i=1}^{m} h((R/P_i)(a_i), n)$. Observe que $d = \sup\{\dim(R/P_i)\}$. Como os valores da função de Hilbert só assume valores não-negativos para $n \gg 0$, então o polinômio que a descreve é o nulo ou possui coeficiente líder não-negativo, e como consequência o grau da soma desses polinômios é o máximo dos graus. Assim, basta provar o teorema para o caso $M = R/P$, para P um ideal primo homogêneo. Argumentaremos por indução em $\dim R/P = d$. Se $\dim R/P = 0$, então R/P é corpo e P é o único ideal homogêneo maximal $m_0 \oplus_{n>0} R_n$ de R, onde m_0 é o ideal maximal de R_0. Logo, para todo $n > 0$, $h(R/P, n) = \ell(R_n/P_n) = 0$. Se $\dim R/P > 0$, como R é homogêneo, podemos escolher um elemento homogêneo $x \neq 0$ em R/P de grau 1. Donde a sequência

$$0 \longrightarrow (R/P)(-1) \xrightarrow{x} R/P \longrightarrow R/(x, P) \longrightarrow 0$$

é exata. Pela Proposição 3.2.3, temos

$$\Delta h(R/P, n) = h(R/P, n+1) - h(R/P, n) = h(R/(x, P), n+1).$$

Uma vez que R/P é domínio, a Observação 1.3.3 juntamente com o Teorema 1.4.4 nos garante que $\dim R/(x, P) = d-1$. A hipótese de indução nos diz que $\Delta h(R/P, n)$ é de tipo-polinomial de grau $d-2$. Se $d > 1$, o Corolário 3.1.6 implica que $\Delta^{d-1}(h(R/P, n)) = \Delta^{d-2}(\Delta h(R/P, n))$ é uma

constante não-nula para valores suficientemente grandes de n. Se $d = 1$, então $\Delta^{d-1}(h(R/P, n)) = h(R/P, n) = h(R/P, 0) + \sum_{i=1}^{n} h(R/(x, P), i)$ é constante para $n \gg 0$, pois $h(R/(x, P), i) = 0$, para $i \gg 0$ e essa constante é não-nula pois $h(R/P, 0) \neq 0$. Em qualquer caso, o Corolário 3.1.6 conclui o desejado. □

Alguns conceitos subjacentes à função de Hilbert são:

Definição 3.2.6. Seja M um R-módulo graduado finitamente gerado de dimensão d. O único polinômio $P_M(X) \in \mathbb{Q}[X]$ para o qual $h(M, n) = P_M(n)$ para todo $n \gg 0$ é chamado de *polinômio de Hilbert* de M. A série de potências $H_M(t) = \sum_{n\in\mathbb{Z}} h(M, n)t^n$ é chamada de *série de Hilbert* de M.

Teorema 3.2.7. *Seja M um R-módulo graduado finitamente gerado de dimensão d. Então existe um único $Q_M(t) \in \mathbb{Z}[t, t^{-1}]$, com $Q(1) \neq 0$ tal que*

$$H_M(t) = \frac{Q_M(t)}{(1-t)^d}$$

Prova. Temos

$$(1-t)^d H_M(t) = \sum_{n\in\mathbb{Z}} \Delta^d h(M, n-d)t^n.$$

Como $h(M, n-d)$ é de tipo polinomial de grau $d-1$ (Teorema 3.2.4), segue pelo Corolário 3.1.6 que $(1-t)^d H_M(t) \in \mathbb{Z}[t, t^{-1}]$. Definamos então $Q_M(t) = \sum_{n\in\mathbb{Z}} \Delta^d h(M, n-d)t^n$. Provaremos agora que $Q_M(1) \neq 0$. Para isso, argumentaremos por contradição. Assim, suponha que $Q_M(1) = 0$. Então:

$$0 = \sum \Delta^d h(M, n-d) = \sum (\Delta^{d-1} h(M, n+1-d) - \Delta^{d-1} h(M, n-d)) = \Delta^d h(M, m)$$

para um m suficientemente grande. Mas isso contradiz o Corolário 3.1.6(a). □

3.3 Ideais de pontos planos

Determinar a função, polinômio ou série de Hilbert de um módulo graduado explicitamente é na maioria das vezes uma tarefa muito difícil. De fato, é um problema que já se mostra complexo mesmo para módulos cuja dimensão de Krull é baixa.

Por exemplo, dado um módulo graduado M de dimensão de Krull 1 sabemos pelo Teorema 3.2.5 que o polinômio de Hilbert de M será um polinômio constante. Contudo, mesmo nesse caso os desafios são grandes. A seguir apresentaremos exemplos especiais desse caso, os chamados *ideais de pontos planos*.

Seja k um corpo. O plano projetivo sobre k, denotado por $\mathbb{P}^2_k$ (ou simplesmente $\mathbb{P}^2$ quando o corpo k estiver subentendido), é o espaço quociente do conjunto $k^3 \setminus \{(0,0,0)\}$ pela relação de *homotetia*, ou seja: $(a_1, b_1, c_1) \sim (a_2, b_2, c_2)$ se, e somente se, $(a_1, b_1, c_1) = \lambda(a_2, b_2, c_2)$ para algum $\lambda \in k$ não nulo. Representamos a classe de equivalência de um elemento $(a, b, c) \in k^3 \setminus \{(0,0,0)\}$ por $(a : b : c)$. Cada classe $(a : b : c)$ será chamada um *ponto* do plano projetivo $\mathbb{P}^2$.

Seja $F(x, y, z)$ um polinômio em $R = k[x, y, z]$. Dizemos que $F(x, y, z)$ se anula em ponto $p = (a : b : c) \in \mathbb{P}^2$ se $F(\lambda a, \lambda b, \lambda c) = 0$ para cada $\lambda \in k$ não nulo.

Proposição 3.3.1. *Seja* $p = (a : b : c)$ *um ponto do plano projetivo* $\mathbb{P}^2$. *Denotemos por* $I(p)$ *o conjunto de todos os polinômios de* $R = k[x, y, z]$ *que se anulam em* p. *Então* $I(p)$ *é um ideal homogêneo de* R *gerados por dois polinômios homogêneos de grau* 1.

Prova. Primeiro mostraremos que $I(p)$ é um ideal. Obviamente, o polinômio nulo se anula em p. Agora, considere $f, g \in R$ tais que $f(\lambda a, \lambda b, \lambda c) = g(\lambda a, \lambda b, \lambda c) = 0$ para cada $\lambda \in k$ não nulo. Então, $(f + g)(\lambda a, \lambda b, \lambda c) = f(\lambda a, \lambda b, \lambda c) + g(\lambda a, \lambda b, \lambda c) = 0$ para cada $\lambda \in k$ não nulo. Logo, $f + g \in I(p)$. Finalmente, dado $f \in R$ e $g \in I(p)$ temos $(fg)(\lambda a, \lambda b, \lambda c) = f(\lambda a, \lambda b, \lambda c)g(\lambda a, \lambda b, \lambda c) = f(\lambda a, \lambda b, \lambda c) \cdot 0 = 0$ para cada $\lambda \in k$ não nulo; em particular, $fg \in I(p)$. Portanto, $I(p)$ é ideal de R.

Agora mostraremos que $I(p)$ é gerado por dois polinômios homogêneos de grau 1. Sem perda de generalidade, digamos que $a \neq 0$. Afirmamos que $I(p) = (bx - ay, cx - az)$. Inicialmente observe que

$$b(\lambda a) - a(\lambda b) = 0 \quad \text{e} \quad c(\lambda a) - a(\lambda c) = 0,$$

para cada $\lambda \in k$ não nulo. Isso nos mostra que $bx - ay, cx - az \in I(p)$, ou seja, $(bx - ay, cx - az) \subset I(p)$. Para mostrar a inclusão contrária, considere $f \in I(p)$. Dividindo f por $bx - ay$ obtemos

$$f = (bx - ay)q + r,$$

onde $q, r \in R$ com r dependendo apenas das variáveis x, z. Dividindo agora r por $cx - az$ obtemos

$$f = (bx - ay)q + (cx - az)q' + r',$$

onde $q', r' \in R$ com r dependendo apenas da variável x. Agora, para cada $\lambda \in k$ não nulo temos

$$0 = f(\lambda a, \lambda b, \lambda c) = 0 \cdot q(\lambda a, \lambda b, \lambda c) + 0 \cdot q'(\lambda a, \lambda b, \lambda c) + r'(\lambda a).$$

Com isso, obtemos $r' = 0$. Logo,

$$f = (bx - ay)q + (cx - az)q',$$

ou seja, $f \in (bx - ay, cx - az)$. Dessa forma, concluímos a igualdade desejada e a prova da proposição. □

Dada um conjunto de pontos $\mathbf{p} = \{p_1, \ldots, p_n\} \subset \mathbb{P}^2$ temos que $I(p_1) \cap \cdots \cap I(p_n)$ é o ideal de $R = k[x, y, z]$ que reúne todos os polinômios $F \in R$ que se anula em todos os pontos do conjunto $\mathbf{p}$. Denotaremos esse ideal por $I(\mathbf{p})$.

Dado um ponto $p = (a : b : c) \in \mathbb{P}^2$ temos $R/I(p) \simeq k[x]$. Em particular,

$$h(R/I(p), d) = h(k[x], d) = 1,$$

para cada inteiro não negativo d. Equivalentemente,

$$h(I(p), d) = \binom{d+2}{2} - 1 \tag{3.1}$$

para cada inteiro positivo d.

Proposição 3.3.2. *Seja* $\mathbf{p} = \{p_1, \ldots, p_n\}$ *um conjunto de pontos do plano projetivo* $\mathbb{P}^2$. *Então:*

(i) *Para cada inteiro positivo* d, $h(I(\mathbf{p}), d) \geqslant \binom{d+2}{2} - n$.

(ii) *Para cada inteiro* $d \geqslant n - 1$, $h(I(\mathbf{p}), d) = \binom{d+2}{2} - n$.

(iii) *O polinômio de Hilbert da* k*-álgebra graduada* $R/I(\mathbf{p})$ *é o polinômio constante* $P_{R/I(\mathbf{p})}(X) = n$.

Prova. (i) A prova será por indução na quantidade n de pontos. Para $n = 1$ o resultado segue de (3.1). Suponha agora $n > 1$ e que o resultado seja verdadeiro para $n - 1$ pontos. Denotemos por $\mathbf{p}'$ o conjunto formado pelos $n - 1$ primeiros elementos de $\mathbf{p}$. A afirmação segue das seguintes estimativas

$$\begin{aligned}
h(I(\mathbf{p}), d) &= h(I(\mathbf{p}'), d) + h(I(p_n), d) - \dim_k(I(\mathbf{p}')_d + I(p_n)_d) && \text{(fórmula de Grassmann)} \\
&\geqslant \binom{d+2}{2} - (n-1) + \binom{d+2}{2} - 1 - \dim_k(I(\mathbf{p}')_d + I(p_n)_d) && \text{(hipótese de indução)} \\
&\geqslant \binom{d+2}{2} - (n-1) + \binom{d+2}{2} - 1 - \binom{d+2}{2} && \text{(pois } I(\mathbf{p}')_d + I(p_n)_d \text{ é subespaço de } R_d\text{)} \\
&= \binom{d+2}{2} - n. && (3.2)
\end{aligned}$$

(ii) A prova desse item também será por indução sob a quantidade n de pontos. Para $n = 1$ o resultado segue de (3.1). Dado $n > 1$, iremos considerar $\mathbf{p}'$ como na demonstração do item anterior. Por indução e pelo princípio da indução é suficiente provar que $I(\mathbf{p})_d \neq I(\mathbf{p}')_d$. Pelo Lema da Esquiva, como $p_i \neq p_j$ sempre que $i \neq j$, segue que para cada $1 \leqslant i \leqslant n$ existe uma polinômio homogêneo L_i de grau 1 tal que $L_i \in I(p_i) \setminus I(p_j)$ sempre que $j \neq i$. Além disso, também pelo Lema da Esquiva, exite polinômios homogêneo L_0 de grau 1 tal que $L \notin I(p_i)$ para

qualquer $1 \leqslant i \leqslant n$. Desse modo, o polinômio $F = L_1 \cdots L_{n-1} L_0^{d-n+1} \in I(\mathbf{p}') \setminus I(\mathbf{p})$ e com isso concluímos a demonstração.

(iii) Como $[R/I(\mathbf{p})]_d = R_d/I(\mathbf{p})_d$ para cada $d \geqslant 0$ segue que

$$h(R/I(\mathbf{p}), d) = h(R, d) - h(I(\mathbf{p}), d),$$

para cada $d \geqslant 0$. Assim, pelo item (ii), para $d \geqslant n-1$ temos

$$h(R/I(\mathbf{p}), d) = \binom{d+2}{2} - \binom{d+2}{2} + n = n.$$

Logo, da definição de polinômio de Hilbert segue que $P_{R/I(\mathbf{p})}(X) = n$. □

Mendiante a proposição acima vemos que o polinômio de Hilbert $P_{R/I(\mathbf{p})}(X)$ com respeito a subconjunto finito $\mathbf{p}$ de pontos do plano projetivo $\mathbb{P}^2$ depende somente da quantidade de pontos do conjunto $\mathbf{p}$, ou seja, não depende das coordenadas dos pontos. Todavia, veremos nos dois exemplos a seguir que isso não é verdade para a função de Hilbert de $R/I(\mathbf{p})$.

Exemplo 3.3.3. Seja $\mathbf{p} = \{(1:0:0), (0:1:0), (0:0:1)\} \subset \mathbb{P}^2$. Suponha que $L = ax+by+cz \in I(\mathbf{p})_1$. Então:

$$\begin{cases} a \cdot 1 + b \cdot 0 + c \cdot 0 = 0 \\ a \cdot 0 + b \cdot 1 + c \cdot 0 = 0 \\ a \cdot 0 + b \cdot 0 + c \cdot 1 = 0 \end{cases}.$$

Logo, $L = 0$. Concluímos com isso que $h(I(\mathbf{p}), 1) = 0$, ou equivalentemente,

$$h(R/I(\mathbf{p}), 1) = h(R, 1) - h(I(\mathbf{p}), 1) = 3.$$

Exemplo 3.3.4. Seja $\mathbf{p} = \{(1:0:0), (0:1:0), (1:1:0)\} \subset \mathbb{P}^2$. Nesse caso temos que $z \in I(\mathbf{p})_1$. Em particular,

$$h(R/I(\mathbf{p}), 1) = h(R, 1) - h(I(\mathbf{p}), 1) \leqslant 2.$$

Capítulo 4

Resoluções livres graduadas

Uma forma eficiente de entender um módulo graduado M sobre um anel R é através do conceito de *resolução livre graduada*. Nesse capítulo apresentaremos esse conceito, alguns exemplos de módulos/ideais onde resoluções livres graduadas são satisfatoriamente conhecidas e a relação entre resolução livre graduada e a função/polinômio de Hilbert.

4.1 Generalidades

Sejam $R = \bigoplus_{n\in\mathbb{Z}} R_n$ uma R_0-álgebra graduada e $M = \bigoplus_{n\in\mathbb{Z}} M_n$ um R-módulo graduado. Uma sequência exata

$$F_\bullet : \cdots \to F_n \xrightarrow{d_n} \cdots \to F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0 \tag{4.1}$$

é dita uma *resolução livre graduada* de M se cada F_i é um módulo livre graduado e cada d_i é um homomorfismo graduado. Se existe um índice p tal que $F_n = 0$ para cada $n \geqslant p$, dizemos que a resolução livre graduada $F_\bullet$ é *finita* e a escrevemos como

$$F_\bullet : 0 \to F_p \xrightarrow{d_p} \cdots \to F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0. \tag{4.2}$$

Uma resolução livre graduada de um módulo graduado M é construído de forma recursiva da seguinte maneira.

(a) Seja I_0 um conjunto de índices que indexa um conjunto de geradores homogêneos $\{g_i \,|\, i \in I_0\}$ de M. Considere o módulo livre graduado $F_0 = \bigoplus_{i\in I_0} R(-\deg(g_i))$. Defina agora o homomorfismo graduado e sobrejetor $d_0 : F_0 \mapsto M$ que envia o i-ésimo vetor e_i da base canônica de F_0 em g_i. Temos então a sequência exata

$$F_0 \xrightarrow{d_0} M \to 0.$$

(b) Considere agora I_1 um conjunto de índices que indexa um conjunto de geradores homogêneos $\{g_i \mid i \in I_1\}$ de $Z_1 := \ker d_0$. Considere o módulo livre graduado $F_1 = \bigoplus_{i\in I_1} R(-\deg(g_i))$. Defina o homomorfismo graduado sobrejetor $d_1 : F_1 \to Z_1$ que envia o i-ésimo vetor e_i da base canônica de F_1 em g_i. Temos então a sequência exata

$$F_1 \xrightarrow{d_1} F_0 \xrightarrow{d_0} M \to 0.$$

Seguimos a construção dos Z_i, F_i e $d_i : F_i \twoheadrightarrow Z_i$ de forma sucessiva obtendo a resolução livre e graduada desejada. Na decomposição $F_i = \bigoplus_{i\in I_i} R(-\deg(g_i))$ podemos juntar os somandos que têm o mesmo deslocamento escrevendo $F_i = \bigoplus_j R(-j)^{\beta_{i,j}}$.

Nesse trabalho estaremos particularmente interessados nas resoluções livres e graduadas quando $R = k[x_1, \ldots, x_n]$ é um anel de polinômios em n variáveis com coeficientes sobre um corpo k com sua graduação usual e M é um R-módulo graduado finitamente gerado. Nesse caso, denotando por $\mathfrak{m}$ o ideal maximal e homogêneo $(x_1, \ldots, x_n)$, temos os seguintes conceitos e fatos:

Definição 4.1.1. A resolução livre e graduada $F_\bullet$ é dita *minimal* se $\operatorname{Im} d_i \subset \mathfrak{m}F_{i-1}$ para cada i.

Teorema 4.1.2 (Teorema das Sizígias de Hilbert)**.** *M possui uma resolução livre graduada e minimal da forma*

$$0 \to \bigoplus_j R(-j)^{\beta_{p,j}} \to \cdots \to \bigoplus_j R(-j)^{\beta_{1,j}} \to \bigoplus_j R(-j)^{\beta_{0,j}} \to M \to 0$$

onde os números p e $\beta_{i,j}$ dependem apenas do R-módulo M.

Prova. Ver [4, Theorem 1.1]. □

Chamamos p como no teorema acima de *dimensão projetiva* de M, e o denotemos por $\dim.\mathrm{proj}(M)$. Os números $\beta_{i,j}$ são chamados de *números graduados de Betti* do módulo M.

Teorema 4.1.3. *Se $I \subset R = k[x_1, \ldots, x_n]$ é um ideal homogêneo e R/I é Cohen-Macaulay então*

$$\dim.\mathrm{proj}(M) = n - \dim R/I = \operatorname{ht} I.$$

Prova. Ver [1, Theorem 1.3.3]. □

Ilustramos as discussões acima com o seguinte exemplo concreto.

Exemplo 4.1.4. Seja k um corpo e R o anel de polinômios $k[x, y, z]$. Considere o ideal $I = \langle xy, xz, yz\rangle \subset R$. Iniciamos considerando o homomorfismo sobrejetor

$$d_0 : R(-2)^3 \twoheadrightarrow I, \quad e_1 \mapsto xy,\ e_2 \mapsto xz,\ e_3 \mapsto yz.$$

Nesse caso, dado $u = (\alpha, \beta, \gamma) \in R^3$ temos $d_0(u) = \alpha xy + \beta xz + \gamma yz$. Afirmamos que $Z_1 := \ker d_0$ é gerado pelos vetores $v_1 = (0, y, -x)$ e $v_2 = (z, 0, -x)$. A inclusão $\langle v_1, v_2 \rangle \subset Z_1$ é um cálculo direto. Para a inclusão contrária considere $u = (\alpha, \beta, \gamma) \in Z_1$. Então $\alpha xy + \beta xz + \gamma yz = 0$. Equivalentemente, $\alpha xy = -z(\beta x + \gamma y)$. Como z é elemento primo de R segue que $\alpha = pz$ para algum $p \in R$. Substituindo essa expressão de α na igualdade $\alpha xy = -z(\beta x + \gamma y)$ e efetuando os devidos cancelamentos obtemos $pxy = -\beta x - \gamma y$. Por conseguinte, essa igualdade pode ser reescrita como $\beta x = -y(px + \gamma)$. Agora, dessa igualdade e da primalidade de y em R segue que $\beta = qy$ para algum $q \in R$. Substituindo essa expressão de β em $\beta x = -y(px + \gamma)$ e efetuando cancelamentos obtemos $qx = -px - \gamma$, ou seja, $\gamma = -(q + p)x$. Assim, temos

$$u = (\alpha, \beta, \gamma) = (pz, qy, -(q + p)x) = q \cdot (0, y, -x) + p \cdot (z, 0, -x) = qv_1 + pv_2.$$

Logo, $u \in \langle v_1, v_2 \rangle$. Consequentemente, $Z_1 = \langle v_1, v_2 \rangle$. Agora consideramos o homomorfismo sobrejetor

$$d_1 : R(-3)^2 \twoheadrightarrow Z_1, \quad e_1 \mapsto v_1, \quad e_2 \mapsto v_2.$$

Dado $(\alpha_1, \alpha_2) \in R^2$ temos $d_1(\alpha_1, \alpha_2) = (\alpha_2 z, \alpha_1 y, -(\alpha_1 + \alpha_2)x)$. Em particular,

$$(\alpha_1, \alpha_2) \in \ker d_1 \Leftrightarrow \alpha_2 z = \alpha_1 y = -(\alpha_1 + \alpha_2)x = 0 \Leftrightarrow \alpha_1 = \alpha_2 = 0.$$

Assim, $\ker d_1 = \{0\}$. Concluímos assim a seguinte resolução livre e graduada para I

$$0 \to R(-3)^2 \xrightarrow{d_1} R(-2)^3 \to I \to 0.$$

Observe que os números de Betti aqui são:

$$\beta_{0,2} = 3 \qquad \text{e} \qquad \beta_{1,3} = 2.$$

4.2 Exemplos

Determinar a resolução livre graduada ou mesmo informações parciais sobre ela é, tipicamente, muito difícil. Não à toa, existem diversas conjecturas sobre o tema que perduram ao logo do tempo. Nessa seção exibiremos alguns exemplos importantes de módulos/ideais em que uma resolução livre graduada é conhecida.

4.2.1 Complexo de Koszul

Sejam R um anel e M um R-módulo. Para cada inteiro positivo i, denotamos o produto tensorial $M \otimes \cdots \otimes M$ de i fatores M por $M^{\otimes i}$. Por convenção, definiremos $M^{\otimes 0} = R$. Podemos dar ao R-módulo $T(M) = \bigoplus_{i \in \mathbb{N}} M^{\otimes i}$ uma estrutura de R-álgebra $\mathbb{N}$-graduada definindo uma multiplicação da seguinte maneira: para $f = u_1 \otimes \cdots \otimes u_i \in M^{\otimes i}$ e $g = v_1 \otimes \cdots v_j \in M^{\otimes j}$ definimos

$$f \cdot g := u_1 \otimes \cdots \otimes u_i \otimes v_1 \otimes \cdots v_j \in M^{i+j}.$$

Em seguida, estendemos a definição para elementos arbitrários de $T(M)$ por meio da distributividade. É possível demonstrar que essa multiplicação está bem definida e que o R-módulo $T(M)$ com esta operação é uma R-álgebra $\mathbb{N}$-graduada (não comutativa!). A chamamos de *álgebra tensorial* do R-módulo M.

Algumas álgebras importantes são obtidas como quocientes da álgebra tensorial. Um exemplo disso é a *álgebra exterior*. A álgebra exterior de um R-módulo M, denotado $\bigwedge_R M$ (ou simplesmente $\bigwedge M$ quando o anel base estiver subentendido), é o quociente da álgebra tensorial $T_R(M)$ pelo ideal bilateral $\mathfrak{I}$ gerado pelos elementos $x \otimes x$ com $x \in M$. Como $\mathfrak{I}$ é ideal homogêneo, pois ele é gerado por elementos homogêneos de grau 2, então $\bigwedge M$ é também uma álgebra graduada. Denotaremos sua i-ésima componente homogênea por $\bigwedge^i M$ e a chamamos de i-*ésima potência exterior* do módulo M. O produto de dois elementos $f, g \in \bigwedge M$ é denotado por $f \wedge g$.

Proposição 4.2.1. (a) *Se M é R-módulo gerado por elementos $x_1, \ldots, x_m$ então $\bigwedge^r M$ é R-módulo gerado pelos elementos $x_{j_1} \wedge \cdots \wedge x_{j_m}$ com $1 \leqslant j_1 < \cdots < j_r \leqslant m$.*

(b) *Se M é R-módulo livre com base $e_1, \ldots, e_m$ então $\bigwedge^r M$ é $\bigwedge^r M$ é R-módulo livre com base $e_{j_1} \wedge \cdots \wedge e_{j_m}$; em particular, $\bigwedge^r M \simeq R^{\binom{m}{r}}$.*

Prova. Ver [7, Chapter XIX, Proposition 1.1]. □

Dado um homomorfismo de R-módulos $\varphi : R^m \to R$, a correspondência

$$(u_1, \ldots, u_n) \mapsto \sum_{i=1}^{n} (-1)^{i+1} \varphi(u_i) u_1 \wedge \cdots \wedge \widehat{u}_i \wedge \cdots \wedge u_n$$

define uma aplicação R-linear de $R^m \times \cdots \times R^m$ (n fatores) em $\bigwedge^{n-1} R^m$ ($\widehat{u}_i$ indica que u_i foi omitido). Pela propriedade universal da n-ésima potência exterior, existe um mapa R-linear $d_\varphi^{(n)} : \bigwedge^n R^m \to \bigwedge^{n-1} R^m$ satisfazendo

$$d_\varphi^{(n)}(u_1 \wedge \cdots \wedge u_n) = \sum_{i=1}^{n} (-1)^{i+1} \varphi(u_i) u_1 \wedge \cdots \wedge \widehat{u}_i \wedge \cdots \wedge u_n$$

para cada $u_1, \ldots, u_n \in R^m$. A coleção dos mapas $d_\varphi^{(n)}$ define um homomorfismo de álgebras graduadas

$$d_\varphi : \bigwedge R^m(-1) \to \bigwedge R^m.$$

Por um cálculo direto podemos verificar que

$$d_f \circ d_f = 0 \quad \text{e} \quad d_f(u \wedge v) = d_f(u) \wedge v + (-1)^{\deg u} u \wedge d_f(y)$$

para todo elemento homogêneo $u \in \bigwedge R^m$. A igualdade $d_f \circ d_f = 0$ implica que a sequência

$$\mathcal{K}(\varphi): \quad 0 \to \bigwedge^m R^m \xrightarrow{d_f^{(m)}} \bigwedge^{m-1} R^m \xrightarrow{d_f^{(m-1)}} \cdots \longrightarrow \bigwedge^2 R^m \xrightarrow{d_f^{(2)}} R^m \xrightarrow{f=:d_f^{(1)}} R \tag{4.3}$$

é um *complexo*, i.e., $\operatorname{Im}(d_f^{(i+1)}) \subset \ker d_f^{(i)}$ para cada $i = 1, \ldots, m-1$. Chamamos $\mathcal{K}(\varphi)$ de *complexo de Koszul* do homomorfismo φ.

Dada uma sequência $\mathbf{f} = f_1, \ldots, f_m$ em um anel noetheriano R podemos considerar o homomorfismo sobrejetor

$$\varphi : R^n \twoheadrightarrow (f_1, \ldots, f_m) \subset R, \quad e_i \mapsto f_i.$$

Chamaremos o complexo de Koszul desse homomorfismo φ de *complexo de Koszul da sequência* $\mathbf{f}$ e o denotamos por $\mathcal{K}_\mathbf{f}$. O próximo resultado nos revela o que acontece com o complexo de Koszul de uma sequência quando ela é suposta regular.

Teorema 4.2.2. *Se* $\mathbf{f} = \{f_1, \ldots, f_m\}$ *é uma sequência regular de* R *então o complexo de Koszul* $\mathcal{K}_\mathbf{f}$ *é uma sequência exata.*

Prova. Ver [1, Corollary 1.6.19]. □

Corolário 4.2.3. *Sejam* R *uma álgebra* $\mathbb{Z}$*-graduada e* $f_1, \ldots, f_m$ *uma sequência regular de* R *de elementos homogêneos de mesmo grau* d. *Então uma resolução livre e graduada do ideal* $(f_1, \ldots, f_m)$ *é:*

$$0 \to R(-md) \to \cdots \to R(-id)^{\binom{m}{i}} \to \cdots \to R(-2d)^{\binom{m}{2}} \to R(-d)^m \to (f_1, \ldots, f_n) \to 0.$$

Prova. Pelo Teorema 4.2.2 temos que o complexo

$$0 \to \bigwedge^m R^m \xrightarrow{d_f^{(m)}} \cdots \xrightarrow{d_f^{(i+1)}} \bigwedge^i R^m \xrightarrow{d_f^{(i)}} \cdots \longrightarrow \bigwedge^2 R^m \xrightarrow{d_f^{(2)}} R^m \xrightarrow{f=:d_f^{(1)}} (f_1, \ldots, f_n) \to 0$$

é uma sequência exata. Por outro lado, pela Proposição 4.2.1, temos $R^{\binom{m}{r}} \simeq \bigwedge^r R^m$. Assim, segue a sequência exata

$$0 \to R \to \cdots \to R^{\binom{m}{i}} \to \cdots \to R^{\binom{m}{2}} \to R^m \to (f_1, \ldots, f_n) \to 0.$$

Agora, para concluir o desejado é suficiente mostrar os *shifts* da resolução. Mostraremos isso por indução no índice $1 \leqslant r \leqslant m$ do módulo livre $R^{\binom{m}{r}} \simeq \bigwedge^r R^m$. Para $r = 1$ o resultado segue do fato que cada f_i tem grau d. Suponha agora o resultado verdadeiro para $r-1$. Então, o $r-1$ módulo com *shift* é $R((r-1)d)^{\binom{m}{r-1}}$. Pela definição dos mapas, para cada $1 \leqslant i_1 < \cdots < i_r \leqslant m$, o $(i_1, \ldots, i_r)$-ésimo vetor da base canônica de $R^{\binom{m}{r}}$ é enviado $\sum_{i=1}^{n}(-1)^r f_{i_j} e_{i_1} \wedge \cdots \wedge \widehat{e}_{i_j} \wedge \cdots \wedge i_{i_r}$, um elemento de grau rd em $R((r-1)d)^{\binom{m}{r-1}}$. Assim, segue que o *shift* para o módulo livre $R^{\binom{m}{r}}$ é $-rd$ e isso conclui a demonstração. □

Exemplo 4.2.4. Seja k um corpo e R o anel de polinômios $k[x_1, \ldots, x_n]$. Como mencionado acima, a sequência $x_1, \ldots, x_n$ é uma sequência regular de R. Assim, pelo Corolário 4.2.3 uma resolução livre graduada do ideal $(x_1, \ldots, x_n)$ é

$$0 \to R(-n) \to \cdots \to R(-i)^{\binom{n}{i}} \to \cdots \to R(-2)^{\binom{n}{2}} \to R(-1)^n \to (x_1, \ldots, x_n) \to 0.$$

4.2.2 Teorema de Hilbert-Burch

Seja R um anel e φ uma matriz de ordem $m \times r$ com entradas em R. Para cada $1 \leqslant t \leqslant \min\{m, r\}$, denotaremos por $I_t(\varphi)$ o ideal de R gerado por todos os menores de ordem t da matriz φ. Nessa subseção estamos interessados na situação em que $m = r + 1$ e $t = r$. Digamos, por exemplo, que

$$\varphi = \begin{pmatrix} a_{1,1} & \cdots & a_{1,r} \\ a_{2,1} & \cdots & a_{2,r} \\ \vdots & \ddots & \vdots \\ a_{r+1,1} & \cdots & a_{r+1,r} \end{pmatrix}.$$

Considere agora a matriz quadrada de ordem $(r+1) \times (r+1)$ obtida pela concatenação de φ com a j-ésima coluna c_j de φ

$$[\varphi \,|\, c_j] = \left(\begin{array}{ccc|c} a_{1,1} & \cdots & a_{1,r} & a_{1,j} \\ a_{2,1} & \cdots & a_{2,r} & a_{2,j} \\ \vdots & \ddots & \vdots & \vdots \\ a_{n+1,1} & \cdots & a_{r+1,r} & a_{r+1,j} \end{array}\right).$$

Como $[\varphi \,|\, c_j]$ possui duas colunas iguais então

$$\det[\varphi \,|\, c_j] = 0.$$

Desenvolvendo $\det[\varphi \mid c_j]$ por Laplace ao longo da última coluna obtemos:

$$a_{1,j}(-1)^1\Delta_1 + \cdots + a_{r+1,j}(-1)^{r+1}\Delta_{r+1} = 0. \tag{4.4}$$

Assim, se consideramos a matriz $\boldsymbol{\Delta} = \begin{bmatrix} (-1)^1\Delta_1 & \cdots & (-1)^{r+1}\Delta_{r+1} \end{bmatrix}$ de ordem $1 \times (r+1)$ segue que a sequência

$$0 \to R^r \xrightarrow{\varphi} R^{r+1} \xrightarrow{\boldsymbol{\Delta}} I_r(\varphi) \to 0 \tag{4.5}$$

satisfaz:

(i) $\boldsymbol{\Delta}$ é sobrejetora pois suas entradas geram $I_r(\varphi)$.

(ii) Por (4.4), $\operatorname{Im}(\varphi) \subset \ker \boldsymbol{\Delta}$.

Teorema 4.2.5 (Teorema de Hilbert-Burch)**.** *Seja* R *um anel Cohen-Macaulay e* φ *uma matriz de ordem* $(r+1) \times r$ *com entradas em* R. *Se* $\operatorname{ht} I_r(\varphi) \geqslant 2$ *então* $\ker \varphi = \mathbf{0}$ *e* $\operatorname{Im}(\varphi) = \ker \boldsymbol{\Delta}$.

Prova. Ver [1, Theorem 1.4.17]. □

Exemplo 4.2.6. Sejam k um corpo e R o anel de polinômios $k[x, y, z]$. Consideremos mais uma vez o ideal $I = \langle xy, xz, yz \rangle$. Observe que os geradores de I são os 2-menores ordenados e com sinal da matriz

$$\varphi = \begin{pmatrix} 0 & z \\ -y & 0 \\ -x & -x \end{pmatrix},$$

ou seja, $I = I_2(\varphi)$. Além disso, $\operatorname{ht} I = 2$. Assim, de acordo com o Teorema de Hilbert-Burch a sequência

$$0 \to R^2 \xrightarrow{\varphi} R^3 \to I \to 0$$

é exata. Agora, levando em consideração os graus essa sequência exata produz a seguinte resolução livre graduada e mínima:

$$0 \to R(-3)^2 \xrightarrow{\varphi} R(-2)^3 \to I \to 0.$$

4.3 Série de Hilbert versus resoluções livres graduadas

Iniciamos essa seção com o seguinte exemplo:

Exemplo 4.3.1. Seja k um corpo e $R = k[x_1, \ldots, x_r]$. Pelo que vimos no Exemplo 3.2.2,

$$P_R(n) = \binom{n+r-1}{r-1},$$

é um polinômio de grau $r-1$. Além disso, como sabemos da teoria de série de potências, a série de Hilbert

$$H_R(t) = \sum_{n \geqslant 0} \binom{n+r-1}{r-1} t^n$$

tem como função geradora $\frac{1}{(1-t)^r}$. Assim, podemos escrever

$$H_R(t) = \frac{1}{(1-t)^r}.$$

No próximo resultado veremos que para todo módulo graduado e finitamente gerado M sobre um anel homogêneo R é sempre possível representar sua série de Hilbert em termos de uma função geradora que é uma função racional.

Teorema 4.3.2. *Seja M um R-módulo graduado finitamente gerado. Considere*

$$0 \to \bigoplus_j R(-j)^{\beta_{pj}} \to \cdots \to \bigoplus R(-j)^{\beta_{0,j}} \to M \to 0$$

uma resolução livre graduada de M. Então

$$H_M(t) = S_M(t) H_R(t),$$

onde $S_M(t) = \sum_{i,j} (-1)^i \beta_{i,j} t^j$. Em particular, se $R = k[x_1, \ldots, x_n]$ é um anel de polinômios com coeficientes sobre um corpo k então

$$H_M(t) = \frac{S_M(t)}{(1-t)^n}.$$

Prova. Para cada inteiro positivo d, a resolução livre graduada

$$0 \to \bigoplus_j R(-j)^{\beta_{pj}} \to \cdots \to \bigoplus R(-j)^{\beta_{0,j}} \to M \to 0$$

induz a seguinte exata de k-espaços vetoriais

$$0 \to \left[\bigoplus_j R(-j)^{\beta_{pj}}\right]_d \to \cdots \to \left[\bigoplus R(-j)^{\beta_{0,j}}\right]_d \to M_d \to 0.$$

Assim, pela Proposição 3.2.3,

$$\begin{aligned} h_R(M,d) &= \sum_{i=1}^{p}(-1)^i h_R(\bigoplus_j R(-j)^{\beta_{ij}},d) \\ &= \sum_{i,j}(-1)^i\beta_{i,j}h_R(R,d-j). \end{aligned} \tag{4.6}$$

Logo,

$$\begin{aligned} H_M(t) &= \sum_{d\geqslant 0} h_R(M,d)t^d \\ &= \sum_{d\geqslant 0}\sum_{i,j}(-1)^i\beta_{i,j}h_R(R,d-j)t^d \\ &= \sum_{d\geqslant 0} h_R(R,d-j)t^{d-j} \\ &= \sum_{i,j}(-1)^i\beta_{i,j}t^j\sum_{d\geqslant 0} h_R(R,d-j)t^{d-j} \\ &= S_M(t)H_R(t). \end{aligned} \tag{4.7}$$

A parte suplementar do teorema é consequência do que foi observado no Exemplo 4.3.1 □

Exemplo 4.3.3. Sejam $R = k[x,y,z]$ com k sendo um corpo e $I = (xy, xz, yz) \subset R$.

$$\beta_{0,0} = 1, \quad \beta_{1,2} = 3 \quad \text{e} \quad \beta_{2,3} = 2.$$

Assim,

$$S_{R/I}(t) = 1 - 3t^2 + 2t^3$$

e

$$H_{R/I}(t) = \frac{1-3t^2+2t^3}{(1-t)^3}.$$

Exemplo 4.3.4. Sejam k um corpo, R o anel de polinômios $k[x_1,\ldots,x_n]$ e $f_1,\ldots,f_m$ polinômios homogêneos de mesmo grau d formando uma sequência regular sobre R. Seja I o ideal gerado por $f_1,\ldots,f_m$. De acordo com o Exemplo 4.2.3, a resolução livre graduada de R/I é

$$0 \to R(-md) \to \cdots \to R(-id)^{\binom{m}{i}} \to \cdots \to R(-2d)^{\binom{m}{2}} \to R(-d)^m \to R \to R/I \to 0.$$

Assim,

$$S_{R/I}(t) = \sum_{i=0}^{m}(-1)^i\binom{m}{i}t^{di} = (1-t^d)^m.$$

Portanto,

$$H_{R/I}(t) = \frac{(1-t^d)^m}{(1-t)^d}.$$

Sejam $R = k[x_1, \ldots, x_n]$ um anel de polinômios sobre um corpo k e I um ideal homogêneo de R. Dizemos que R/I tem uma *resolução pura* de tipo $(d_1, \ldots, d_p)$ se sua resolução livre graduada e minimal tem a forma:

$$0 \to R(-d_p)^{\beta_p} \to \cdots \to R(-d_1)^{\beta_1} \to R \to R/I \to 0.$$

Observe que, como a resolução é minimal devemos ter necessariamente $d_1 < \cdots < d_p$. O próximo teorema é uma aplicação do Teorema 4.3.2 para as resoluções puras.

Teorema 4.3.5. *Suponha que* R/I *é Cohen-Macaulay e tem resolução pura de tipo* $(d_1, \ldots, d_p)$. *Então*

$$\beta_i = (-1)^{i+1} \prod_{j \neq i} \frac{d_j}{d_j - d_i}.$$

Prova. O Teoremas 3.2.7 e 4.3.2 nos dão a seguinte igualdade

$$\frac{S_{R/I}(t)}{(1-t)^n} = \frac{Q_{R/I}(t)}{(1-t)^d}.$$

Logo,

$$S_{R/I}(t) = (1-t)^{n-d} Q_{R/I}(t).$$

Como R/I é Cohen-Macaulay então, pelo Teorema 4.1.3, $n - d = p$. Assim,

$$S_{R/I}(t) = (1-t)^p Q_{R/I}(t). \tag{4.8}$$

Desse modo, de (4.8) segue que

$$S^{(j)}_{R/I}(1) = 0, \qquad j = 1, \cdots, p-1 \tag{4.9}$$

onde $S^{(j)}_{R/I}(t)$ significa a j-ésima derivada de $S_{R/I}(t)$. Por outro lado, pelo Teorema 4.3.2 temos

$$S_{R/I}(t) = 1 - \beta_1 t^{d_1} + \cdots + (-1)^p \beta_p t^{d_p}. \tag{4.10}$$

De (4.9) e (4.10) obtemos o seguinte sistema:

$$\begin{cases} -\beta_1 & + & \beta_2 & + & \cdots & + & (-1)^p\beta_p & = & -1 \\ -d_1\beta_1 & + & d_2\beta_2 & + & \cdots & + & (-1)^p d_p\beta_p & = & 0 \\ -d_1(d_1-1)\beta_1 & + & d_2(d_2-1)\beta_2 & + & \cdots & + & (-1)^p d_p(d_p-1)\beta_p & = & 0 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ -\frac{d_1!}{(d_1-p+1)!}\beta_1 & + & \frac{d_2!}{(d_2-p+1)!}\beta_2 & + & \cdots & + & (-1)^p\frac{d_p!}{(d_p-p+1)!}\beta_p & = & 0 \end{cases}.$$

Note que somando a segunda equação desse sistema à terceira obtemos

$$\begin{cases} -\beta_1 & + & \beta_2 & + & \cdots & + & (-1)^p\beta_p & = & -1 \\ -d_1\beta_1 & + & d_2\beta_2 & + & \cdots & + & (-1)^p d_p\beta_p & = & 0 \\ -d_1^2\beta_1 & + & d_2^2\beta_2 & + & \cdots & + & (-1)^p d_p^2\beta_p & = & 0 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ -\frac{d_1!}{(d_1-p+1)!}\beta_1 & + & \frac{d_2!}{(d_2-p+1)!}\beta_2 & + & \cdots & + & (-1)^p\frac{d_p!}{(d_p-p+1)!}\beta_p & = & 0 \end{cases}.$$

Observe que o i-ésimo coeficiente da j-ésima equação é expressão polinomial em d_i, com coeficiente líder ± 1 e de grau $j-1$. Assim, indutivamente, após operações elementares podemos reescrever o sistema como

$$\begin{cases} -\beta_1 & + & \beta_2 & + & \cdots & + & (-1)^p\beta_p & = & -1 \\ -d_1\beta_1 & + & d_2\beta_2 & + & \cdots & + & (-1)^p d_p\beta_p & = & 0 \\ -d_1^2\beta_1 & + & d_2^2\beta_2 & + & \cdots & + & (-1)^p d_p^2\beta_p & = & 0 \\ \vdots & & \vdots & & & & \vdots & & \vdots \\ -d_1^{p-1}\beta_1 & + & d_2^{p-1}\beta_2 & + & \cdots & + & (-1)^p d_p^{p-1}\beta_p & = & 0 \end{cases}.$$

Assim, pela regra de Cramer temos

$$(-1)^i\beta_i = \frac{\det V_i}{\det V},$$

onde

$$V_i = \begin{pmatrix} d_1 & \cdots & d_{i-1} & d_{i+1} & \cdots & d_p \\ d_1^2 & \cdots & d_{i-1}^2 & d_{i+1}^2 & \cdots & d_p^2 \\ \vdots & & \vdots & \vdots & & \vdots \\ d_1^{p-1} & \cdots & d_{i-1}^{p-1} & d_{i+1} & \cdots & d_p^{p-1} \end{pmatrix} \quad \text{e} \quad V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ d_1 & d_2 & \cdots & d_p \\ \vdots & \vdots & & \vdots \\ d_1^{p-1} & d_2^{p-1} & \cdots & d_p^{p-1} \end{pmatrix}.$$

Observe que essas são matrizes de Vandermonde. Como é bem conhecido, seus determinantes são:

$$\det V_i = \prod_{\substack{1\leqslant j\leqslant p-1 \\ j\neq i}} d_j \cdot \prod_{\substack{1\leqslant j<r\leqslant p-1 \\ j,r\neq i}} (\alpha_j - \alpha_r)$$

e

$$\det V = \prod_{1 \leqslant j < r \leqslant p-1} (\alpha_j - \alpha_r).$$

Assim,

$$\beta_i = (-1)^{i+1} \prod_{j \neq i} \frac{d_j}{d_j - d_i}$$

como desejado.

□

4.4 Número de postulação

De acordo com o Teorema 3.2.5, dado um anel homogêneo R e um R-módulo graduado M, a função de Hilbert de M coincide assintoticamente com o polinômio de Hilbert de M. Assim, uma pergunta natural é qual o primeiro valor n_0 onde essa coincidência ocorre. Esse valor n_0 constitui um invariante do R-módulo graduado M e o chamamos de *número de postulação* do R-módulo graduado M. Nesse trabalho o indicaremos por $\rho(M)$. O objetivo dessa seção é estabelecer uma estimativa para o número de postulação em termos da resolução livre e graduada de M quando R é um anel de polinômios com coeficientes sobre um corpo.

Proposição 4.4.1. *Suponha que* $R = k[x_1, \ldots, x_r]$*, com* k *sendo um corpo. Se o* R*-módulo graduado* M *possui resolução livre finita*

$$0 \longrightarrow F_m \xrightarrow{\varphi_m} F_{m-1} \longrightarrow \cdots \longrightarrow F_1 \xrightarrow{\varphi_1} F_0 \to M \to 0$$

com cada $F_i = \bigoplus_j R(-a_{i,j})$*, então*

$$h(M, d) = \sum_{i=0}^{m} (-1)^i \sum_j \binom{r - 1 + d - a_{i,j}}{r - 1}.$$

Prova. Como no Exemplo 3.2.2, sabemos que $h(R, d) = \binom{r-1+d}{r}$. Deslocando por $a_{i,j}$, obtemos $h(R(-a_{i,j}), n) = \binom{r-1+d-a_{i,j}}{r-1}$. Daí, para cada i, $h(F_i, d) = \sum_j \binom{r-1+d-a_{i,j}}{r-1}$. Pelo que vimos acima, temos então

$$h(M, d) = \sum_{i=0}^{m} (-1)^i h(F_i, d) = \sum_{i=0}^{m} (-1)^i \sum_j \binom{r - 1 + d - a_{i,j}}{r - 1},$$

como desejávamos. □

Corolário 4.4.2. *Se* M *possui uma resolução livre como na* Proposição 4.4.1 *então* $h(M,d) = P_M(d)$ *para cada* $d \geqslant \max\{a_{i,j} - r + 1\}$. *Em particular,* $\rho(M) \leqslant \max\{a_{i,j} - r + 1\}$.

Prova. Basta notar que se $d + r - 1 - a_{i,j} \geqslant 0$, então

$$\binom{r-1+d-a_{i,j}}{r-1}$$

é um polinômio binomial de grau $r-1$ em d, e assim o resultado segue da Proposição 4.4.1. □

Exemplo 4.4.3. Seja $R = k[x_1, x_2, x_3, x_4]$ com k um corpo. Consideremos o ideal $I \subset R$ gerado por todos os menores de ordem 2 da seguinte matriz de ordem 3×2 :

$$\varphi = \begin{pmatrix} x_1 & x_2 \\ x_2 & x_3 \\ x_3 & x_4 \end{pmatrix}.$$

Observe que $f = x_1x_3 - x_2^2$ e $g = x_1x_4 - x_2x_3$ são elementos de I. O elemento f é irredutível (por exemplo, aplicando o critério de Eisenstein). Assim, o ideal $P = (f)$ e ideal primo e está contido propriamente em I. Com isso concluímos que $\operatorname{ht} I \geqslant 2$. Assim, pelo Teorema de Hilbert-Burch segue que uma resolução livre e graduada do ideal I é da forma:

$$0 \to R(-3)^2 \xrightarrow{\varphi} R(-2)^3 \xrightarrow{\Delta} I \to 0.$$

Podemos aumentar essa resolução livre graduada de I para uma resolução livre e graduada de R/I da seguinte maneira

$$0 \to R(-3)^2 \xrightarrow{\varphi} R(-2)^3 \xrightarrow{\Delta} R \xrightarrow{\pi} R/I \to 0,$$

onde π é a projeção canônica de R sobre R/I. De posse dessa resolução livre e graduada de R/I e da Proposição 4.4.1 obtemos

$$\begin{aligned} h(R/I,d) &= (-1)^0\binom{d+3-0}{3} + (-1)^1 \cdot 3\binom{d+3-2}{3} + (-1)^2 \cdot 2\binom{d+3-3}{3} \\ &= \binom{d+3}{3} - 3\binom{d+1}{3} + 2\binom{d}{3} \\ &= \frac{(d+3)(d+2)(d+1)}{3!} - 3\frac{(d+1)d(d-1)}{3!} + 2\frac{d(d-1)(d-2)}{3!} \\ &= 3d+1. \end{aligned}$$

Além disso, o Corolário 4.4.2 nos diz que para $d \geqslant 0$, temos a concordância entre a função de

Hilbert e seu polinômio

$$h(R/I, d) = P_{R/I}(d) = 3d + 1.$$

Bibliografia

[1] W. Bruns and J. Herzog, *Cohen-Macaulay Rings*, Cambridge Studies in Advanced Mathematics, **60**, Cambridge Unniversity Press, 1993.

[2] W. Bruns and U. Vetter, *Determinantal Rings*, Lecture Notes in Mathematics, Vol. 1327 Springer-Verlag, 1988.

[3] D. Eisenbud, *Commutative Algebra With A View Toward Algebraic Geometry*. Graduate Texts in Mathematics, 150, New York, Springer-Verlag, 1995.

[4] D. Eisenbud, *The geometry of syzygies: A second course in commutative algebra and algebraic geometry*, vol. 229 of Graduate Texts in Mathematics. Springer-Verlag, New York, 2005.

[5] J. Herzog and T. Hibi, *Monomial Ideals*, Grad. Texts in Math. 260, Springer, London, 2010.

[6] C. Huneke and I. Swanson, *Integral Closure of Ideals, Rings, and Modules*, London Math. Society, Lecture Notes Series **336**, Cambridge University Press (2006).

[7] S. Lang, *Algebra*. Graduate Texts in Mathematics, 211 (Revised third ed.), New York, Springer-Verlag, 2002.

[8] H. Matsumura, *Commutative ring theory*, Cambridge University Press, 1986.

[9] A. Simis, *Commutative Algebra*, De Gruyter Textbook, 2020.