FUNÇÕES DE HILBERT

1. Comprimento

Seja $M \neq 0$ um R-módulo. M é dito *simples* (ou *irredutível*), se 0 e M são os únicos R-submódulos de M. Uma cadeia de submódulos

$$0 \subset M_1 \subset M_2 \subset \cdots \subset M_r = M$$

é dito série de composição de comprimento r para M se M_i/M_{i+1} são simples. O comprimento $\operatorname{len} M$ de M é definida como o mínimo entre os comprimentos de séries de composição de M. O comprimento de M é infinito se M não possui séries de composição finita.

Exemplo 1. Se k é um corpo, então k-módulos são espaços vetoriais, e $\operatorname{len} V = \dim V$ para todo k-espaço V.

Lemma 2. *M é simples se e somente se $M \cong R/\mathfrak{m}$ com algum ideal maximal $\mathfrak{m}$ de R.*

Proof. Se $\mathfrak{m}$ é maximal, então $R/\mathfrak{m}$ é simples, pelo Teorema de Correspondência. Seja M simples. Existe $m \in M$ tal que $Rm \neq 0$. Como Rm é um submódulo de M, temos que $Rm = M$. Defina $\psi : R \to M$, por $r \mapsto rm$. Então ψ é sobrejetiva, e $M \cong R/\ker\psi$. Pela simplicidade de M, temos que $\ker\psi$ é maximal. □

Theorem 3. *As seguintes propriedades são válidas.*

(1) *$\operatorname{len} M$ é finita se e somente se M é noetheriano e artiniano.*
(2) *Se $\operatorname{len} M$ é finita, então toda série de composição tem comprimento $\operatorname{len} M$.*
(3) *Se*

$$0 \to N \to M \to P \to 0$$

é uma sequência exata de R-módulos, então $\operatorname{len} M = \operatorname{len} N + \operatorname{len} P$.

Proof. (1) Exercício.

(2) Indução por $\operatorname{len} M$. Se $\operatorname{len} M = 0$, então $M = 0$ e o teorema está trivialmente válido. Assuma que

$$0 \subset M_1 \subset M_2 \subset \cdots \subset M_r = M$$

é uma série de composição para M. Então $\operatorname{len} M \leq r$. Além disso, M_1 é simples e

$$0 = M_1/M_1 \subset M_2/M_1 \subset \cdots \subset M_r/M_1 = M/M_1$$

é uma série de composição para M/M_1. Pela definição do comprimento, $\operatorname{len} M/M_1 \leq r-1$ e pela hipótese de indução $\operatorname{len} M/M_1 = r-1$ e toda série de composição de M/M_1 tem comprimento $r-1$.

Assuma que

$$0 \subset N_1 \subset \cdots \subset N_k = M.$$

é uma série de composição para M. Assuma que i é minimal tal que $N_i \cap M_1 \neq 0$. Pela simplicidade de M_1, temos que $N_i \cap M_1 = M_1$; ou seja $M_1 \subseteq N_i$. Então afirmamos que

eq:comp

$$0 \subset (N_1 + M_1)/M_1 \subset \cdots \subset (N_{i-1} + M_1)/M_1 \subseteq N_i/M_1 \subset \cdots \subset N_k/M_1 = M/M_1 \tag{1}$$

é uma série de composição para M/M_1 com comprimento $r - 1$ (ou seja a inclusão $\subseteq$ no meio é $=$). Considerando um quociente para $j < i$, temos que $N_j \cap M_1 = N_{j-1} \cap M_1 = 0$ e assim $(N_j + M_1)/M_1 \cong N_j/(N_j \cap M_1) = N_j$ e $(N_{j+1} + M_1)/M_1 \cong N_{j+1}/(N_{j+1} \cap M_1) = N_{j+1}$. Portanto

$$((N_j + M_1)/M_1)/((N_{j-1} + M_1)/M_1) \cong N_j/N_{j-1}$$

que é simples. Se $j \geq i$, então

$$(N_{j+1}/M_1)/(N_j/M_1) \cong N_{j+1}/N_j$$

é simples. Finalmente

$$(N_i/M_1)/((N_{i-1} + M_1)/M_1) \cong N_i/(N_{i-1} + M_1).$$

Mas $N_{i-1} \subset N_{i-1} + M_1 \subseteq N_i$. Como N_i/N_{i-1} é simples, temos que $N_{i-1} + M_1 = N_i$. Ou seja, $N_i/(N_{i-1} + M_1) = 0$. Logo (??) é uma séria de composição para M/M_1 de comprimento $r - 1$. Assim $k - 1 = r - 1$ e $r = k$.

(3) Exercício. $\square$

2. Polinômios binomiais

Um polinômio binomial é um polinômio na forma

$$\binom{x}{d} = \frac{x(x-1)\cdots(x-d+1)}{d!}$$

onde $d \geq 0$.

Lemma 4. *(1) Seja $p(x) \in \mathbb{Q}[x]$ um polinômio de grau d. Temos que $p(n) \in \mathbb{Z}$ para todo $n \in \mathbb{N}$ suficientemente grande se e somente se*

$$p(x) = a_d\binom{x}{d} + a_{d-1}\binom{x}{d-1} + \cdots + a_0\binom{x}{0}.$$

com $a_i \in$.

(2) Assuma que $f : \mathbb{N} \to \mathbb{N}$ é uma função. Suponha que existe um polinômio $q(t) \in \mathbb{Q}[t]$ de grau $k - 1$ tal que

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

para todo natural n suficientemente grande. Então existe um polinômio $p(t) \in \mathbb{Q}[t]$ de grau k tal que $f(n) = p(n)$ para todo natural n suficientemente grande.

3. Anéis graduados

Um anel R é dito *graduado* se

$$R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots$$

como um grupo abeliano onde $R_i R_j \subseteq R_{i+j}$. Em particular, R_0 é um anel, R_i é um R_0-módulo para todo $i \geq 0$ e R é uma R_0-álgebra. Os R_i são chamados de *componentes homegêneos* de R e um elemento $f \in R_i$ é dito *homogêneo* de grau i.

Seja R um anel. Considere a cadeia F_i de ideais

$$R = F_0 \supset F_1 \supset F_2 \supset \cdots$$

tal que $F_i F_j \subseteq F_{i+j}$. Uma tal cadeia chama-se *filtração* sobre R. Dada uma filtração como na linha destacada anterior, podemos definir

$$R_{\mathrm{gr}} = \bigoplus_{i \geq 0} F_i / F_{i+1}$$

como um grupo abeliano e um produto em R_{gr} pela regra

$$(x_i + F_{i+1})(x_j + F_{j+1}) = x_i x_j + F_{i+j+1}$$

para $x_i \in F_i$ e $x_j \in F_j$ e estender estes produtos linearmente para R_{gr}.

Se R é uma S-álgebra, então tomamos S-módulos R_i na definição de graduação. Em particular, se R é uma k-álgebra com um corpo k, então R_i é um k-espaço vetorial.

Exemplo 5. A álgebra $R = k[x_1, \ldots, x_n]$ de polinômios é uma k-álgebra graduada com a graduação na qual R_i é o k-espaço de polinômios com grau (total) i.

Exemplo 6. Um ideal $I \subseteq R$ de um anel graduado é dito *homogêneo* se

$$I = I_0 \oplus I_1 \oplus I_2 \oplus \cdots$$

onde $I_i = I \cap R_i$. Se I é um ideal homogêneo, então

$$R/I = \left(\bigoplus_{i \geq 0} R_i \right) / I = \bigoplus_{i \geq 0} ((R_i + I)/I) \cong \bigoplus_{i \geq 0} (R_i / I_i).$$

Se $r_i \in R_i/I_i \cong (R_i + I)/I$ e $r_j \in R_j/I_j \cong (R_j + I)/I$ então

$$r_i r_j \in (R_i R_j + I)/I \subseteq (R_{i+j} + I)/I \cong R_{i+j}/I_{i+j}.$$

Ou seja, o quociente R/I é graduado.

Exemplo 7. Seja $(R, \mathfrak{m}, k)$ um anel local noetheriano. Considere a filtração

$$R \supset \mathfrak{m} \supset \mathfrak{m}^2 \supset \cdots .$$

Podemos definir

$$R_{\mathrm{gr}} = k + \mathfrak{m}/\mathfrak{m}^2 \oplus \mathfrak{m}^2/\mathfrak{m}^3 \oplus \cdots$$

com a multiplicação como acima. Então $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ são k-espaços vetoriais e R_{gr} é uma soma direta de k-espaços vetoriais. Assim R_{gr} é uma k-álgebra graduada. Assuma que

$m_1, \dots, m_r \in m$ é um sistema gerador do ideal $\mathfrak{m}$. Então $m_1+\mathfrak{m}^2, \dots, m_r+\mathfrak{m}^2$ é um sistema gerador para R_{gr}. Em particular, R_{gr} é quociente do anel $k[x_1, \dots, x_r]$ de polinômios de posto r.

Exercício 8. *Mostre que um ideal $I \subseteq k[x_1, \dots, x_n]$ é homogêneo se e somente se I é gerado por $f_1, \dots, f_k$ onde f_i são polinômios homogêneos.*

Se R é um anel graduado e M é um R-módulo, então dizemos que M é *graduado* se M pode ser escrito como

$$M = M_0 \oplus M_1 \oplus \cdots$$

como um grupo abeliano em tal forma que $R_i M_j \subseteq M_{i+j}$ para todo $i, j \geq 0$.

Assuma que $R = k[x_1, \dots, x_n]/I$ com um ideal graduado I e seja M um R-módulo graduado finitamente gerado. Definimos a função de Hilbert

$$\chi_M(n) = \dim_k M_n.$$

Exercício 9. *Mostre que $\chi_M(n) < \infty$ para todo n.*

Um morfismo *homogêneo* de R-módulos graduados M e N é um morfismos $\varphi : M \to N$ que satisfaz a condição $\varphi(M_i) \subseteq N_i$.

Theorem 10. *Seja $R = k[x_1, \dots, x_n]/I$ onde I é um ideal homogêneo (e assim R é graduado). Seja M um R-módulo graduado. Então existe um polinômio $p_M(t) \in \mathbb{Q}[t]$ de grau menor ou igual a $n-1$ tal que $\chi_M(m) = \dim M_m = p_M(m)$ para todo $m \in \mathbb{N}$ suficientemente grande.*

Proof. Indução por n. Se $n = 0$, então $R = k$ e temos que M é um k-espaço vetorial de dimensão finita e podemos tomar $p_M(t) = 0$.

Assuma que $n \geq 1$ e o teorema está verdadeiro para $n-1$. Seja $M[1]$ o R-módulo graduado tal que $M[1] = M$ como R-módulos e $M[1]_i = M_{i+1}$ para todo i. É fácil verificar que $M[1]$ é um R-módulo graduado. Seja $\mu : M \to M[1]$ dado por $m \mapsto x_n \cdot m$ (multiplicação por x_n). Então μ é um morfismo homogêneo de R-módulos graduados. Temos a seguinte sequência exata de R-módulos

$$0 \to N \to M \to M[1] \to P \to 0$$

onde N e P são o núcleo e conúcleo de μ. Note que N e P são finitamente gerados sobre R, pois R é noetheriano. Além disso, N, $M[1]$ e P são graduados, o morfismo μ é homogêneo, e temos as seguintes sequências exatas de k-espaços para todo $m \geq 0$:

$$0 \to N_m \to M_m \to (M[1])_m \to P_m \to 0.$$

Olhando nas dimensões obtemos

$$\dim_k P_m = \dim_k N_m - \dim_k M_m + \dim_k M_{m+1};$$

ou seja

$$\chi_M(m+1) - \chi_M(m) = \chi_P(m) - \chi_N(m).$$

Considere $R_1 = R/(x_r) \cong R/(I + (x_r))$. Então x_r anula P e N e podemos considerar P e N como R_1-módulos finitamente gerados. Assim $\chi_N(t)$ e $\chi_P(t)$ são funções polinomiais de grau menor ou igaul a $n-2$. Assim $\chi_M(t)$ é polinomial de grau menor ou igual a $n-1$. □

Seja $(R, \mathfrak{m}, k)$ um anel local noetheriano. Para $n \geq 0$, definimos

$$\lambda_R(n) = \operatorname{len} A/\mathfrak{m}^n$$

onde $\mathfrak{m}^0 = A$.

Theorem 11. *Assuma que $(R, \mathfrak{m}, k)$ é um anel local noetheriano. Então*

$$\Delta\lambda_R(n) = \dim_k \mathfrak{m}^n/\mathfrak{m}^{n+1}.$$

Existe um polinômio $p(t) \in \mathbb{Q}[t]$ tal que $\lambda_A(n) = p(n)$ para todo $n \in \mathbb{N}$ suficientemente grande.

Proof. Primeiro

$$\operatorname{len} A/\mathfrak{m}^{n+1} = \operatorname{len} A/\mathfrak{m} + \operatorname{len} \mathfrak{m}/\mathfrak{m}^2 + \cdots + \operatorname{len} \mathfrak{m}^n/\mathfrak{m}^{n+1}$$

e

$$\Delta\lambda_R(n) = \lambda_R(n+1) - \lambda_R(n) = \operatorname{len} \mathfrak{m}^n/\mathfrak{m}^{n+1}.$$

Como $\mathfrak{m}$ anula $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ para todo i, temos que $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ pode ser visto como um k-espaço e os R-submódulos de $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ são precisamente os k-subespaços. Assim $\operatorname{len} \mathfrak{m}^i/\mathfrak{m}^{i+1} = \dim_k \mathfrak{m}^i/\mathfrak{m}^{i+1}$. □

O polinômio $p(n)$ no teorema anteirior chama-se o polinômio de *Hilbert–Samuel* do anel local R.