Álgebra Comutativa

Notas de Aula

Maria Eugenia Martin

Universidade de São Paulo
São Paulo, 23 de novembro de 2014

SUMÁRIO

INTRODUÇÃO

Este texto corresponde à versão preliminar das notas de aula do curso MAT5737-Introdução à Álgebra Comutativa ministrado no 2º Semestre de 2014, no Instituto de Matemática e Estatística da Universidade de São Paulo, IME-USP.

O autor ficaria muito grato se lhe fossem enviadas sugestões de melhorias ou que lhe fossem apontados erros porventura encontrados.

1

ANÉIS E IDEAIS

Aula 1

AULA 1: 11/08/2014

Vamos começar revendo rapidamente as definições e propriedades elementares de anéis, ideais primos e maximais e várias operações elementares que podem ser realizadas em ideais.

Definição 1. Um **anel** A é um conjunto com duas operações binárias: soma e multiplicação, denotadas por $(+, \cdot)$ respetivamente e tais que:

a. A é um grupo abeliano em relação a operação de soma "$+$" (logo A tem um elemento nulo, 0, e todo $a \in A$ tem um inverso aditivo, $-a$.)

b. A multiplicação "$\cdot$" em A é associativa ($(a \cdot b) \cdot c = a \cdot (b \cdot c)$) e distributiva em relação à adição ($a \cdot (b + c) = a \cdot b + a \cdot c$ e $(b + c) \cdot a = b \cdot a + c \cdot a$)

   Neste curso *somente* consideraremos anéis comutativos,isto é tais que:

c. $a \cdot b = b \cdot a$ para todos $a, b \in A$

   e que contenham um elemento identidade (denotado por 1):

d. $\exists 1 \in A$ tal que $a \cdot 1 = 1 \cdot a = a$ para todo $a \in A$. (Isto implica que o elemento identidade é único)

Observação. a. Segue de imediato das definições acima que$-1 \cdot a = -a$ e $0 \cdot a = 0$ para todo elemento $a \in A$.

b. Não excluímos a possibilidade de $1 = 0$. Se isto acontecer então para qualquer $a \in A$ temos $a = a \cdot 1 = a \cdot 0 = 0$ e logo A tem um único elemento, 0. Neste caso A é denominado **anel nulo** e denotado por 0.

Definição 2. Um **homomorfismo de anéis** é uma aplicação f de um anel A em um anel B tal que:

a. $f(a + b) = f(a) + f(b)$ (logo f é um homomorfismo de grupos abelianos e logo também $f(a - b) = f(a) - f(b)$, $f(-a) = -f(a)$, $f(0) = 0$),

b. $f(a \cdot b) = f(a) \cdot f(b)$,

c. $f(1_A) = 1_B$.

Em outras palavras, f respeita adição, multiplicação e o elemento identidade.

Um homomorfismo injetor e sobrejetor é chamado de **isomorfismo**.

Um subconjunto S de um anel A é um **subanel** de A se S é fechado sob adição e multiplicação e contém o elemento identidade de A. A aplicação identidade de S em A é então um homomorfismo de anéis injetivo que chamaremos de "**inclusão**".

Se $f : A \to B$, $g : B \to C$ são homomorfismos de anéis então sua composição $g \circ f : A \to C$ é também um homomorfismo de anéis.

Definição 3. Um **ideal** I de um anel A é um subconjunto de A que é um subgrupo aditivo e é tal que $AI \subseteq I$ ou seja se $a \in A$ e $b \in I$ implica que $a \cdot b \in I$. Um ideal I é dito **próprio** se $I \neq A$ ou equivalentemente se $1 \notin I$. Os múltiplos $x \cdot a$ de um elemento $a \in A$ formam um **ideal principal**, denotado por (a). De modo mais geral, podemos definir o **ideal de** A **gerado** pelo subconjunto $S \subseteq A$, denotado por $\langle S \rangle$, como sendo o conjunto gerado por todas as combinações A-lineares finitas:

$$\langle S \rangle = \{a_1 \cdot s_1 + \cdots + a_n \cdot s_n \text{ onde } n \in \mathbb{N}, a_i \in A \text{ e } s_i \in S\}.$$

Exercício 1. Verifique que $\langle S \rangle$ é um ideal de A e que é o "menor" ideal de A que contém o subconjunto S.

O grupo quociente $A/I = \{\overline{a} = a + I \mid a \in A\}$, onde $a + I = b + I$ se e somente se $a - b \in I$, herda uma multiplicação de A definida de maneira única como: $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$ o que o torna um anel (comutativo com unidade), chamado de **anel quociente** e denotado por A/I. A aplicação $\pi : A \to A/I$ que leva cada $a \in A$ em sua classe $\overline{a}$ é um homomorfismo de anéis sobrejetivo que chamaremos de **projeção canônica**.

Usaremos frequentemente o seguinte fato (conhecido como "Teorema de Correspondência entre Ideais", TCI):

Teorema 4. *(***Teorema de Correspondência entre Ideais***) Existe uma correspondência (que preserva ordem) um-a-um entre os ideais J de A que contém I, e os ideais $\overline{J}$ de A/I, dada por $J = \pi^{-1}(\overline{J})$.*

Se $f : A \to B$ é um homomorfismo de anéis e J é um ideal de B, então a pré-imagem $f^{-1}(J)$ é sempre um ideal de A. Mas se I é um ideal de A, o conjunto $f(I)$ não necessariamente é um ideal de B, para que isso aconteça f deve ser sobrejetor. (prova: **Exercício 2.**)

Exemplo 5. Seja f a inclusão de $\mathbb{Z}$ em $\mathbb{Q}$ e seja $I = (3)$ o ideal principal não nulo de $\mathbb{Z}$ gerado por 3, então $f(I) \subseteq \mathbb{Q}$ é o próprio I. Se I for um ideal de $\mathbb{Q}$ então $\mathbb{Q}I \subseteq I$ mas $\frac{1}{2} \cdot 3 = \frac{3}{2} \notin (3) = \{0, \pm 3, \pm 6, \pm 9, \pm 12, \dots\}$. Logo $f(I)$ não é um ideal de $\mathbb{Q}$.

Como consequência o **kernel** de f, $\mathrm{Ker}(f) = f^{-1}(0)$, é um ideal de A mas só podemos afirmar que a **imagem** de f, $\mathrm{Im}(f) = f(A)$, é um subanel de B. O homomorfismo f induz um isomorfismo de anéis $A/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$.

Definição 6.

a. Um **divisor de zero** num anel A é um elemento $a \in A$ o qual "divide 0", i.e., para o qual existe $b \neq 0$ em A tal que $a \cdot b = 0$. Um anel sem divisores de zero não nulos (e no qual $1 \neq 0$) é chamado de **domínio de integridade** (ou seja, num domínio de integridade se $a \cdot b = 0$ então ou $a = 0$ ou $b = 0$).

b. Uma **unidade** em A é um elemento $a \in A$ o qual "divide 1", i.e., para o qual existe $b \in A$ tal que $a \cdot b = 1$. O elemento b é determinado de maneira única por a e é denotado por a^{-1}. As unidades em A formam um grupo abeliano (multiplicativo), $A^{\times}$. Um **corpo** é um anel $\mathbf{k}$ no qual $1 \neq 0$ e todo elemento não nulo é uma unidade.

Exemplo 7. Seja $\mathbf{k}$ um corpo, então $\mathbf{k}$ e $\mathbf{k}[x_1, \ldots, x_n]$ (x_i indeterminadas) são domínios de integridade. $\mathbb{Z}$ é um domínio de integridade mas não é um corpo.

O elemento $a \in A$ é uma unidade se e somente se $(a) = A = (1)$. (prova: **Exercício 3.**)

Proposição 8. *Seja A um anel não nulo. Então as seguintes afirmações são equivalentes:*

a. A é um corpo;

b. os únicos ideais de A são 0 e A;

c. todo homomorfismo de A num anel não nulo B é injetivo.

Demonstração. **Exercício 4.** □

Definição 9. Um **ideal** $\mathfrak{p}$ de A é dito **primo** se $\mathfrak{p} \neq A$ e se $a \cdot b \in p \Rightarrow$ ou $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. Um **ideal** $\mathfrak{m}$ de A é dito **maximal** se $\mathfrak{m} \neq A$ e se sempre que exista um outro ideal I tal que $\mathfrak{m} \subseteq I \subseteq A$ então ou $I = A$ ou $I = \mathfrak{m}$.[1]

Equivalentemente às definições temos:

Proposição 10.

a. $\mathfrak{p}$ é um ideal primo se e somente se $A/\mathfrak{p}$ é um domínio de integridade.

b. $\mathfrak{m}$ é um ideal maximal se e somente se $A/\mathfrak{m}$ é um corpo.

1 Note que por definição ideais primos e maximais são ideais **próprios**.

Demonstração.

a. **Exercício 5.**

b. Suponha que $\mathfrak{m}$ é um ideal maximal de A. Seja $\overline{J} \subseteq A/\mathfrak{m}$ um ideal de $A/\mathfrak{m}$, pelo TCI (Teorema 4) $J = \pi^{-1}(\overline{J})$ é um ideal de A que contém $\mathfrak{m}$, ou seja $\mathfrak{m} \subseteq J \subseteq A$. Da maximalidade de $\mathfrak{m}$ segue que ou $J = \mathfrak{m}$ ou $J = A$, logo ou $\overline{J} = 0$ ou $\overline{J} = A/\mathfrak{m}$. Portanto os únicos ideais de $A/\mathfrak{m}$ são 0 e o próprio $A/\mathfrak{m}$. Segue da Proposição 8 que $A/\mathfrak{m}$ é um corpo.

   Suponha agora que $A/\mathfrak{m}$ é um corpo[2]. Seja J um ideal de A tal que $\mathfrak{m} \subseteq J \subseteq A$, logo $\overline{J} = J/\mathfrak{m}$ é um ideal de $A/\mathfrak{m}$ que é um corpo. Da Proposição 8 segue que ou $\overline{J} = 0$ ou $\overline{J} = A/\mathfrak{m}$, logo $J = \mathfrak{m}$ ou $J = A$ o que implica que $\mathfrak{m}$ é um ideal maximal de A.

□

Como consequências temos: o ideal zero $(0) = 0$ é primo se e somente se A é um domínio de integridade; o ideal zero (0) é maximal se e somente se A é um corpo; e se $\mathfrak{m}$ é um ideal maximal$\Rightarrow A/\mathfrak{m}$ é um corpo$\Rightarrow A/\mathfrak{m}$ é um domínio de integridade$\Rightarrow\mathfrak{m}$ é um ideal primo, ressaltamos porém que a recíproca não é verdadeira.

Proposição 11. *Se $f : A \to B$ é um homomorfismo de anéis e $\mathfrak{q}$ é um ideal primo em B, então $f^{-1}(\mathfrak{q})$ é um ideal primo em A.*

Demonstração. Como vimos anteriormente $f^{-1}(\mathfrak{q})$ é de fato um ideal de A. Vejamos agora que é próprio: de fato se $1_A \in f^{-1}(\mathfrak{q})$ então $f(1_A) = 1_B \in \mathfrak{q}$ contrariando o fato de $\mathfrak{q}$ ser próprio. Por outro lado, se $a \cdot b \in f^{-1}(\mathfrak{q})$ então $f(a \cdot b) = f(a) \cdot f(b) \in \mathfrak{q}$, como $\mathfrak{q}$ é primo segue que ou $f(a) \in \mathfrak{q}$ ou $f(b) \in \mathfrak{q}$, i.e., ou $a \in f^{-1}(\mathfrak{q})$ ou $b \in f^{-1}(\mathfrak{q})$, o que implica por definição que $f^{-1}(\mathfrak{q})$ é um ideal primo de A. □

A proposição anterior se torna falsa se trocamos "ideal primo" por "ideal maximal", vejamos o seguinte contraexemplo:

Exemplo 12. Seja $f : \mathbb{Z} \hookrightarrow \mathbb{Q}$ o homomorfismo de anéis "inclusão". Como $\mathbb{Q}$ é um corpo, o ideal (0) de $\mathbb{Q}$ é maximal. Segue do fato de f ser injetora que o ideal $f^{-1}(0) = \mathrm{Ker}(f) = (0)$, mas (0) não é um ideal maximal de $\mathbb{Z}$ pois $\mathbb{Z}$ não é um corpo. Por outro lado, como $\mathbb{Z}$ é um domínio de integridade então $(0) = f^{-1}(0)$ é um ideal primo.

Ideais primos são fundamentalmente importantes na álgebra comutativa. O próximo teorema garante que ideais maximais (e portanto primos) existem

2 E logo por definição $1 \neq 0$, o que implica $A/\mathfrak{m} \neq 0$ ou seja $A \neq \mathfrak{m}$. Precisamos esta condição para $\mathfrak{m}$ ser maximal.

em abundância. A prova de dito teorema é uma aplicação padrão do famoso *Lema de Zorn*. Para isso lembraremos rapidamente os conceitos necessários.

Um conjunto não vazio Ω é dito **parcialmente ordenado** se for dada uma relação $\leq$ em Ω a qual é reflexiva, transitiva e tal que se $x \leq y$ e $y \leq x$ então $x = y$. Um subconjunto $S \subseteq \Omega$ é uma **cadeia** se para todo par de elementos $x, y \in S$ temos $x \leq y$ ou $y \leq x$. O *Lema de Zorn* pode ser enunciado como segue:

Lema 13. *Se toda cadeia $S \subseteq \Omega$ de um conjunto parcialmente ordenado $\Omega \neq \emptyset$ tem uma cota superior em Ω (i.e., existe $x \in \Omega$ tal que $y \leq x$ para todo $y \in S$), então Ω possui pelo menos um elemento maximal.*

Passamos agora ao enunciado do Teorema:

Teorema 14. *Todo anel não nulo $A \neq 0$ possui pelo menos um ideal maximal.*

Demonstração. Seja Ω o conjunto de todos os ideais próprios de A parcialmente ordenados por inclusão ($\subseteq$). Como $A \neq 0$, Ω é não vazio pois $(0) \in \Omega$. Devemos mostrar que Ω possui um elemento maximal e faremos isso aplicando o Lema de Zorn. Para isso, devemos mostrar que toda cadeia $S \subseteq \Omega$ tem uma cota superior em Ω. Seja $S = (I_\alpha)$ uma cadeia de ideais em Ω, então para cada par de índices α, β temos uma das possibilidades: ou $I_\alpha \subseteq I_\beta$ ou $I_\beta \subseteq I_\alpha$. Denotemos por $\mathfrak{m} = \bigcup_\alpha I_\alpha$, este será o nosso candidato a cota superior de S em Ω.

Vejamos primeiramente que $\mathfrak{m} \in \Omega$, i.e., que $\mathfrak{m}$ é um ideal próprio de A. Sejam $x, y \in \mathfrak{m}$ então existem índices α, β tal que $x \in I_\alpha$ e $y \in I_\beta$, sem perda de generalidade podemos supor que $I_\alpha \subseteq I_\beta$ logo $x + y \in I_\beta \subseteq \mathfrak{m}$. Por outro lado, seja $a \in A$ então $a \cdot x \in I_\alpha \subseteq \mathfrak{m}$. Isto mostra que $\mathfrak{m}$ é um ideal de A. Para ver que ele é próprio só basta observar que $1 \notin \mathfrak{m}$ pois $1 \notin I_\alpha$ para todo α.

Por último, só resta observar que $I_\alpha \subseteq \mathfrak{m}$ para todo α, logo $\mathfrak{m}$ é uma cota superior de S. □

AULA 2

AULA 2: 13/08/2014

Lembrando a última aula. Um conjunto não vazio Ω é dito **parcialmente ordenado** se for dada uma relação $\leq$ em Ω a qual é reflexiva, transitiva e tal que se $x \leq y$ e $y \leq x$ então $x = y$. Um subconjunto $S \subseteq \Omega$ é uma **cadeia** se para todo par de elementos $x, y \in S$ temos $x \leq y$ ou $y \leq x$.

O *Lema de Zorn* pode ser enunciado como segue:

Lema. *Se toda cadeia $S \subseteq \Omega$ de um conjunto parcialmente ordenado $\Omega \neq \emptyset$ tem uma cota superior em Ω (i.e., existe $x \in \Omega$ tal que $y \leq x$ para todo $y \in S$), então Ω possui pelo menos um elemento maximal.*

Teorema. *Todo anel não nulo $A \neq 0$ possui pelo menos um ideal maximal.*

Como aplicações diretas do teorema anterior temos os seguintes corolários:

Corolário 15. *Todo ideal próprio I de A está contido num ideal maximal.*

Demonstração. **Exercício 6.** Basta aplicar o Teorema 14 para o anel A/I no lugar de A e usar o TCI. □

Corolário 16. *Todo elemento de A que não é uma unidade está contido num ideal maximal.*

Operações com ideais

Dados dois ideais I e J de um anel A, definimos os seguintes ideais:

a. A **soma** de I e J é o conjunto de todos os elementos $x + y$ onde $x \in I$ e $y \in J$. É o menor ideal que contém I e J, em outras palavras é o ideal gerado pela união $I \cup J$. Analogamente, podemos definir a soma $\sum_{\alpha \in \Lambda} I_\alpha$ de qualquer família de ideais I_α de A cujos elementos são todas as somas $\sum x_\alpha$ onde $x_\alpha \in I_\alpha$ para todo $\alpha \in \Lambda$ e quase todos os x_α (i.e., todos exceto um conjunto finito) são zero. É o menor ideal que contém todos os ideais I_α.

b. A **interseção** de qualquer família de $(I_\alpha)_{\alpha \in \Lambda}$ ideais é um ideal.

c. O **produto** de dois ideais I, J de A é o ideal $I \cdot J$ gerado por todos os produtos $x \cdot y$, onde $x \in I$ e $y \in J$. É o conjunto de todas as somas finitas $\sum x_i y_j$ onde cada $x_i \in I$ e cada $y_j \in J$. Analogamente definimos o produto de qualquer família finita de ideais. Em particular, são definidas as potências I^n $(n > 0)$ de um ideal I. Por convenção $I^0 = (1)$ e I^n é o ideal gerado por todos os produtos $x_1 \cdot x_2 \cdot \cdots \cdot x_n$ onde cada $x_i \in I$.

Observação.

a. Em geral a união de dois ideais $I \cup J$ não é um ideal.

b. As três operações são comutativas e associativas. Também existe uma lei distributiva $I \cdot (J + K) = I \cdot J + I \cdot K$.

c. *Lei Modular:* Se $J \subseteq I$ ou $K \subseteq I$ então $I \cap (J + K) = I \cap J + I \cap K$. (**Exercício 7.**)

d. Pela lei distributiva $(I + J) \cdot (I \cap J) = I \cdot (I \cap J) + J \cdot (I \cap J) \subseteq I \cdot J$, esta última inclusão devido a que $I \cap J \subseteq J$ e $I \cap J \subseteq I$.

e. Sempre temos a inclusão $I \cdot J \subseteq I \cap J$, a igualdade acontece se $I + J = A$.

Definição 17. Dois ideais I, J são ditos **coprimos** se $I + J = A$.

Logo para ideais coprimos temos a igualdade $I \cap J = I \cdot J$. Claramente dois ideais I e J são coprimos se e somente se existe $a \in I$ e $b \in J$ tal que $a + b = 1$.

Existem anéis com exatamente um ideal maximal, como os corpos. Esta ideia levou à seguinte definição.

Definição 18. Um anel A que possui exatamente um ideal maximal $\mathfrak{m}$ é chamado de **anel local**. O corpo $\mathbf{k} = A/\mathfrak{m}$ é chamado de **corpo de resíduos** de A.

Proposição 19.

a. *Seja A um anel e $\mathfrak{m}$ um ideal próprio de A tal que todo $a \in A - \mathfrak{m}$ é uma unidade de A. Então A é um anel local e $\mathfrak{m}$ seu ideal maximal.*

b. *Seja A um anel e $\mathfrak{m}$ um ideal maximal de A, tal que todo elemento de $1 + \mathfrak{m}$ (i.e., todo $1 + a$ onde $a \in \mathfrak{m}$) é uma unidade de A. Então A é um anel local.*

Demonstração. Suponha que existe um ideal I tal que $\mathfrak{m} \subseteq I \subseteq A$. Então ou $I = A$ ou I é próprio e logo consiste de elementos que não são unidades, logo (por hipótese) está contido em $\mathfrak{m}$ e por tanto $I = \mathfrak{m}$. Por definição $\mathfrak{m}$ é maximal. Suponha que exista outro ideal maximal $\mathfrak{m}' \subseteq A$, como ele é próprio consiste de elementos que não são unidades logo $\mathfrak{m}' \subseteq \mathfrak{m} \subseteq A$, da maximalidade de $\mathfrak{m}'$ e do fato de $\mathfrak{m}$ ser próprio por hipótese, segue que $\mathfrak{m}' = \mathfrak{m}$ e A é um anel local. Isto prova (a.). Para provar (b.) vamos usar o item (a.), logo considere $a \in A - \mathfrak{m}$. Logo $\mathfrak{m} \subsetneq \langle a, \mathfrak{m} \rangle \subseteq A$, onde $\langle a, \mathfrak{m} \rangle$ é o ideal gerado por a e $\mathfrak{m}$. Então da maximalidade de $\mathfrak{m}$ segue que $\langle a, \mathfrak{m} \rangle = A$. Logo existe $b \in A$ e $t \in \mathfrak{m}$ tal que $a \cdot b + t = 1$ o que implica que $a \cdot b = 1 - t \in 1 + \mathfrak{m}$ e por hipótese é uma unidade , logo a é uma unidade. Pelo item (a.) A é um anel local. □

Exemplo 20. Todo ideal em $\mathbb{Z}$ é principal, ou seja é da forma (m) para algum $m \geq 0$. O ideal (m) é primo se e somente se $m = 0$ ou um número primo. Todos os ideais (p), onde p é um número primo, são maximais pois $\mathbb{Z}/(p) = \mathbb{Z}_p$ é o corpo com p elementos.

Isto nos motiva à seguinte definição.

Definição 21. Um **domínio de ideais principais** (DIP) é um domínio de integridade no qual todo ideal é principal.

Em tal anel todo ideal primo não nulo é maximal: seja $(a) \neq 0$ um ideal primo e suponha que $(a) \subseteq (b) \subseteq A$, logo $a \in (b)$ assim $a = b \cdot c$. Mas então

$b \cdot c \in (a)$. Suponha que $(a) \subsetneq (b)$ então $b \notin (a)$ mas (a) é primo então deve ser $c \in (a)$ assim $c = d \cdot a$. Então $a = b \cdot c = b \cdot d \cdot a$. Isto implica que

$$0 = b \cdot d \cdot a - a = (b \cdot d - 1) \cdot a,$$

como por hipótese $a \neq 0$ e o anel A é um domínio então deve ser $(b \cdot d - 1) = 0$, logo $b \cdot d = 1$ e por tanto $(b) = A$. Logo (a) é maximal.

Assim provamos a seguinte proposição:

Proposição 22. *Seja A um DIP e $I \neq 0$ um ideal não nulo de A. Então I é primo se e somente se I é maximal.*

Definição 23. Um elemento $a \in A$ é **nilpotente** se $a^n = 0$ para algum $n > 0$. O conjunto $\mathfrak{N}$ de todos os elementos nilpotentes de um anel A é um ideal (**Exercício 8.** dica: use o Binômio de Newton) chamado de **nilradical** de A.

Seja $\overline{a}$ um elemento nilpotente do anel quociente $A/\mathfrak{N}$, então existe $n > 0$ tal que $0 = \overline{a}^n = \overline{a^n}$ ou seja $a^n \in \mathfrak{N}$. Logo existe $k > 0$ tal que $(a^n)^k = 0$, i.e., $a^{nk} = 0$ e portanto $a \in \mathfrak{N}$ ou seja $\overline{a} = 0$. Assim provamos que o anel quociente $A/\mathfrak{N}$ não tem elementos nilpotentes não nulos.

A seguinte proposição da uma definição alternativa de nilradical:

Proposição 24. *O nilradical de A é a interseção de todos os ideais primos de A.*

Demonstração. Denotemos por $\mathfrak{N}'$ à interseção de todos os ideais primos de A. Seja $a \in \mathfrak{N}$ e $\mathfrak{p}$ qualquer ideal primo de A. Então existe $n > 0$ tal que $a^n = 0$, mas como $0 \in \mathfrak{p}$ temos que $a^n \in \mathfrak{p}$, segue do fato de $\mathfrak{p}$ ser primo que ou $a \in \mathfrak{p}$ ou $a^{n-1} \in \mathfrak{p}$ (se continuarmos com o mesmo raciocínio neste último caso chegaremos a que $a^2 \in \mathfrak{p}$) e logo $a \in \mathfrak{p}$ para todo $\mathfrak{p}$ ideal primo de A, o que implica que $a \in \mathfrak{N}'$. Provamos $\mathfrak{N} \subseteq \mathfrak{N}'$.

Por outro lado, suponha que $a \notin \mathfrak{N}$ (ou seja para todo $n > 0$, $a^n \neq 0$). Seja Ω o conjunto dos ideais I com a seguinte propriedade "Se $n > 0$ então $a^n \notin I$". Observe que $\Omega \neq \emptyset$ pois $(0) \in \Omega$. Queremos aplicar o Lema de Zorn ao conjunto não vazio Ω parcialmente ordenado por inclusão, seguindo o raciocínio da prova do Teorema 14. Então seja $S = (I_\alpha)$ uma cadeia de ideais em Ω e denotemos por $I = \bigcup_\alpha I_\alpha$. Como provamos anteriormente I é um ideal[3] de A e como para cada $n > 0$, $a^n \notin I_\alpha$ para todo α então $a^n \notin I$ e logo $I \in \Omega$ e claramente é uma cota superior da cadeia S. O Lema de Zorn nos garante que Ω tem um elemento maximal $\mathfrak{p}$. Queremos provar que $\mathfrak{p}$ é um ideal primo. Sejam $x, y \notin \mathfrak{p}$, então $\mathfrak{p}$ está estritamente contido nos ideais $\mathfrak{p} + (x)$ e $\mathfrak{p} + (y)$, logo ambos ideais não pertencem a Ω (pois isto seria uma contradição ao fato de $\mathfrak{p}$ ser um elemento maximal de Ω), isto significa que existem $m, n > 0$ tal que $a^m \in \mathfrak{p} + (x)$ e $a^n \in \mathfrak{p} + (y)$, ou seja

3 Observe que em geral união de ideais não é ideal mas aqui os ideais pertencem a uma *cadeia* e é este fato que faz a união ser um ideal.

podemos escrever $a^m = p' + x'$ e $a^n = p'' + y'$, onde $p', p'' \in \mathfrak{p}$, $x' \in (x)$ e $y' \in (y)$. Assim

$$a^m \cdot a^n = p' \cdot p'' + p' \cdot y' + x' \cdot p'' + x' \cdot y' = p''' + x' \cdot y',$$

segue que $a^{m+n} \in \mathfrak{p} + (x \cdot y)$ o que implica que o ideal $\mathfrak{p} + (x \cdot y)$ não pertence a Ω, logo $x \cdot y \notin \mathfrak{p}$ (caso contrário, se $x \cdot y \in \mathfrak{p}$ então $(x \cdot y) \subseteq \mathfrak{p}$, logo $\mathfrak{p} + (x \cdot y) = \mathfrak{p} \in \Omega$) e $\mathfrak{p}$ é primo. Portanto, existe um ideal primo $\mathfrak{p}$ tal que $a \notin \mathfrak{p}$ logo $a \notin \mathfrak{N}'$. Com isto provamos que $\mathfrak{N}' \subseteq \mathfrak{N}$. □

Definição 25. O **radical de Jacobson** $\mathfrak{R}$ de A é definido como sendo a interseção de todos os ideais maximais de A.

A seguinte proposição caracteriza o radical de Jacobson.

Proposição 26. *$a \in \mathfrak{R}$ se e somente se $1 - a \cdot b$ é uma unidade de A para todo $b \in A$.*

Demonstração. ($\Rightarrow$) Suponha que $1 - a \cdot b$ não é uma unidade. Então do Corolário 16 temos que $1 - a \cdot b$ pertence a algum ideal maximal $\mathfrak{m}$; mas $a \in \mathfrak{R} \subseteq \mathfrak{m}$, logo $a \cdot b \in \mathfrak{m}$ e portanto $1 \in \mathfrak{m}$ o que é uma contradição ao fato de $\mathfrak{m}$ ser maximal e logo próprio.

($\Leftarrow$) Suponha que $a \notin \mathfrak{R}$ ou seja existe $\mathfrak{m}$ um ideal maximal de A tal que $a \notin \mathfrak{m}$. Logo $\mathfrak{m} \subsetneq \langle \mathfrak{m}, a \rangle \subseteq A$ o que implica que $\langle \mathfrak{m}, a \rangle = A$, então existem $m \in \mathfrak{m}$ e $b \in A$ tal que $1 = m + a \cdot b$. Logo $1 - a \cdot b \in \mathfrak{m}$ e portanto não é uma unidade (se for, $\mathfrak{m}$ não seria próprio). □

Aula 3

aula 3: 22/08/2014

Lembrando a última aula. O conjunto $\mathfrak{N}$ de todos os elementos nilpotentes de um anel A é chamado de **nilradical** de A.

Proposição. *O nilradical de A é a interseção de todos os ideais primos de A.*

Definição 27. Definimos o **radical** do ideal I de A como sendo $\sqrt{I} = \{a \in A \mid a^n \in I \text{ para algum } n > 0\}$.

Se $\pi : A \to A/I$ é o homomorfismo projeção, então $\sqrt{I} = \pi^{-1}(\mathfrak{N}_{A/I})$ (provar **Exercício 9.**) e logo $\sqrt{I}$ é um ideal (pelo Exercício 2: pré-imagem de ideal é ideal).

Proposição 28. *O radical de um ideal I é a interseção de todos os ideais primos de A que contêm I.*

Demonstração. Aplicando a Proposição 24 a $\dot{A/I}$ temos

$$\mathfrak{N}_{A/I} = \bigcap_{\overline{\mathfrak{p}} \text{ ideal primo de } A/I} \overline{\mathfrak{p}},$$

logo

$$\begin{aligned}\sqrt{I} &= \pi^{-1}(\mathfrak{N}_{A/I}) \\ &= \bigcap_{\overline{\mathfrak{p}} \text{ ideal primo de } A/I} \pi^{-1}(\overline{\mathfrak{p}}) \\ &= \bigcap_{\mathfrak{p} \text{ ideal primo de } A \text{ que contém } I} \mathfrak{p},\end{aligned}$$

onde na última igualdade aplicamos o TCI e a Proposição 11 (pré-imagem de ideal primo é ideal primo). □

Proposição 29.

a. *Sejam $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ ideais primos e seja I um ideal contido em $\bigcup_{i=1}^n \mathfrak{p}_i$. Então $I \subseteq \mathfrak{p}_i$ para algum i.*

b. *Sejam $I_1, \ldots, I_n$ ideais e seja $\mathfrak{p}$ um ideal primo contendo $\bigcap_{i=1}^n I_i$. Então $\mathfrak{p} \supseteq I_i$ para algum i. Se $\mathfrak{p} = \bigcap_{i=1}^n I_i$ então $\mathfrak{p} = I_i$ para algum i.*

Demonstração. O primeiro item é provado por contra-positiva e indução em n, i.e. provaremos que

$$I \nsubseteq \mathfrak{p}_i \, (1 \leq i \leq n) \Rightarrow I \nsubseteq \bigcup_{i=1}^{n} \mathfrak{p}_i.$$

Claramente é verdadeiro para $n = 1$. Se $n > 1$ e o resultado verdadeiro para $n - 1$ (ou seja é verdadeiro se considerarmos quaisquer $n - 1$ $\mathfrak{p}_i$'s), então para cada i existe $a_i \in I$ tal que $a_i \notin \mathfrak{p}_j$ sempre que $j \neq i$. Agora temos duas possibilidades, se para algum i temos $a_i \notin \mathfrak{p}_i$ então acabou. Mas se $a_i \in \mathfrak{p}_i$ para todo i, então considere o elemento $b = \sum_{i=1}^n a_1 \cdot a_2 \cdots \widehat{a_i} \cdots a_n \in I$ e suponha que existe i_0 tal que $b \in \mathfrak{p}_{i_0}$. Então

$$a_1 a_2 \cdots \widehat{a_{i_0}} \cdots a_n = b - \sum_{\substack{i=1 \\ i \neq i_0}}^{n} a_1 \cdot a_2 \cdots a_{i_0} \cdots \widehat{a_i} \cdots a_n \in \mathfrak{p}_{i_0},$$

como $\mathfrak{p}_{i_0}$ é primo então pelo menos um dos a_i com $i \neq i_0$ deve pertencer a $\mathfrak{p}_{i_0}$o que é uma contradição. Logo $b \notin \mathfrak{p}_i$ para todo $1 \leq i \leq n$, portanto $I \nsubseteq \bigcup_{i=1}^n \mathfrak{p}_i$.

Para provar o segundo item suponha que $\mathfrak{p} \not\supseteq I_i$ para todo i. Então para cada i existe $a_i \in I_i$ tal que $a_i \notin \mathfrak{p}$, mas $\mathfrak{p}$ é primo logo $a_1 a_2 \dots a_n \notin \mathfrak{p}$. Por outro lado $a_1 \cdot a_2 \cdots a_n \in \prod_{i=1}^n I_i \subseteq \bigcap_{i=1}^n I_i \subseteq \mathfrak{p}$ o que é uma contradição.

Por último se $\mathfrak{p} = \bigcap_{i=1}^n I_i$ então $\mathfrak{p} \subseteq I_i$ para todo i. Se supomos que essa inclusão é estrita para todo i, seguindo o raciocínio do caso anterior chegaremos a uma contradição, logo $\mathfrak{p} = I_i$ para algum i. □

Definição 30. Definimos o **ideal quociente** dos ideais I e J de A, como sendo o ideal $(I : J) = \{a \in A \mid a \cdot J \subseteq I\}$.

Em particular $(0 : J)$ é chamado de aniquilador de J e é frequentemente denotado por $\mathrm{Ann}(J)$, consiste dos elementos $a \in A$ tais que $a \cdot J = 0$.

Se J é um ideal principal (a) escreveremos $(I : a)$ ao invés de $(I : (a))$.

1.1 TEOREMA CHINÊS DOS RESTOS

Definimos o **produto direto** dos anéis $A_1, \dots, A_n$

$$A = \prod_{i=1}^{n} A_i$$

como sendo o conjunto de todas as sequências $a = (a_1, \dots, a_n)$ com $a_i \in A_i$ $(1 \leq i \leq n)$ e adição e multiplicação componente a componente. Com essas operações A é um anel comutativo com elemento identidade $(1, 1, \dots, 1)$. As projeções $p_i : A \to A_i$ definidas por $p_i(a) = a_i$ são homomorfismos de anéis sobrejetores.

O seguinte teorema é uma generalização do *Teorema Chinês dos Restos* da teoria dos números, o qual na sua versão original afirma que, dados inteiros $m_1, m_2, \dots, m_r$ dois a dois coprimos (i.e., $\mathrm{mdc}(m_i, m_j) = 1$ se $i \neq j$) então o sistema de congruências

$$\begin{aligned} x &\equiv a_1 (\mathrm{mod}\, m_1) \\ x &\equiv a_2 (\mathrm{mod}\, m_2) \\ &\vdots \\ x &\equiv a_r (\mathrm{mod}\, m_r) \end{aligned}$$

admite solução em x que é única módulo $m_1 \cdot m_2 \dots m_r$. Na linguagem da álgebra comutativa isto se traduz como: *existe um isomorfismo de anéis*

$$\begin{aligned} \frac{\mathbb{Z}}{(m_1)} \times \frac{\mathbb{Z}}{(m_2)} \times \cdots \times \frac{\mathbb{Z}}{(m_r)} &\xrightarrow{\cong} \frac{\mathbb{Z}}{(m_1 \cdot m_2 \dots m_r)} \\ (x \bmod m_1, x \bmod m_2, \dots, x \bmod m_r) &\longmapsto x \bmod (m_1 \cdot m_2 \dots m_r). \end{aligned}$$

O isomorfismo ainda existe quando consideramos um anel qualquer e ideais coprimos.

Teorema 31. (**Teorema Chinês dos Restos**) *Seja A um anel e sejam $I_1, \ldots, I_n$ ideais dois a dois coprimos (i.e., $I_i + I_j = A$ para $i \neq j$). Então:*

a. $I_1 \cap \cdots \cap I_n = I_1 \ldots I_n$

b. $\dfrac{A}{I_1 \cdot I_2 \cdot \ldots \cdot I_n} \simeq \dfrac{A}{I_1} \times \dfrac{A}{I_2} \times \cdots \times \dfrac{A}{I_n}$

Demonstração.

a. Claramente para quaisquer ideais I_i, sempre temos $I_1 \ldots I_n \subseteq I_1 \cap \cdots \cap I_n$. Para mostrar a inclusão oposta, procedemos por indução em n sendo o caso $n = 1$ trivial. Para $n = 2$, como I_1 e I_2 são coprimos existem $a_i \in I_i$ tais que $1 = a_1 + a_2$. Assim, seja $c \in I_1 \cap I_2$ então $c = c \cdot a_1 + c \cdot a_2 \in I_1 \cdot I_2$ como desejado. Vamos supor que é verdade para $n - 1$, queremos provar que vale para n. Para isso basta mostrar que os ideais $I_1 \ldots I_{n-1}$ e I_n são coprimos pois com isso e a hipótese de indução teremos

$$(I_1 \cap \cdots \cap I_{n-1}) \cap I_n \overset{HI}{=} (I_1 \ldots I_{n-1}) \cap I_n \overset{n=2}{=} (I_1 \ldots I_{n-1}) \cdot I_n.$$

Como I_i e I_n são coprimos para $i < n$, existem $a_i \in I_i$ e $b_i \in I_n$ tais que $a_i + b_i = 1$ para $i = 1, \ldots, n-1$. Assim,

$$\begin{aligned} 1 &= (a_1 + b_1) \ldots (a_{n-1} + b_{n-1}) \\ &= a_1 \cdot a_2 \ldots a_{n-1} + \sum b_j(\sharp) \in I_1 \ldots I_{n-1} + I_n \end{aligned}$$

o que mostra que $I_1 \ldots I_{n-1} + I_n = A$ e logo $I_1 \ldots I_{n-1}$ e I_n são coprimos.

b. Para mostrar (b.) observaremos primeiramente que todo homomorfismo de anéis $f : A \to B$ induz um isomorfismo de anéis $\overline{f} : A/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ dado por $\overline{f}(\overline{a}) = f(a)$. (**Exercício 10.**)
Seja $\varphi : A \to \frac{A}{I_1} \times \frac{A}{I_2} \times \cdots \times \frac{A}{I_n}$ definida por $a \mapsto (a + I_1, a + I_2, \ldots, a + I_n)$. Logo $a \in \operatorname{Ker}(\varphi) \Leftrightarrow \varphi(a) = 0 \Leftrightarrow a \in I_i$ para todo $i = 1, \ldots, n \Leftrightarrow a \in I_1 \cap \cdots \cap I_n \overset{(a.)}{=} I_1 \ldots I_n$. Logo $\operatorname{Ker}(\varphi) = I_1 \ldots I_n$. Mostraremos a seguir que φ é sobrejetor. Para isso observamos que pelo item anterior os ideais I_i e $I_1 \cap I_2 \cap \cdots \cap \widehat{I_i} \cap \cdots \cap I_n$ são coprimos, logo para cada $i = 1, \ldots, n$ existem $e_i \in I_1 \cap I_2 \cap \cdots \cap \widehat{I_i} \cap \cdots \cap I_n$ (i.e., $e_i \in I_j$ para todo $1 \leq j \leq n$ com $j \neq i$) e $c_i \in I_i$ tal que $1 = e_i + c_i$, assim $\overline{e_i} = 0 + I_j$ para todo $j \neq i$ e por outro lado $e_i - 1 = -c_i \in I_i$, logo $\overline{e_i} = 1 + I_i$. Dito

isto, seja $(\overline{b_1}, \ldots, \overline{b_n}) \in \frac{A}{I_1} \times \frac{A}{I_2} \times \cdots \times \frac{A}{I_n}$ onde $\overline{b_i} = b_i + I_i$ com $b_i \in A$ para todo i. Então existe $a \in A$ dado por $a = b_1e_1 + \cdots + b_ne_n$ tal que

$$\begin{aligned}\varphi(a) &= (a + I_1, a + I_2, \ldots, a + I_n) \\ &= ((b_1e_1 + \cdots + b_ne_n) + I_1, \ldots, (b_1e_1 + \cdots + b_ne_n) + I_n) \\ &= (b_1e_1 + I_1, \ldots, b_ie_i + I_i, \ldots, b_ne_n + I_n) \\ &= (\overline{b_1}, \ldots, \overline{b_n})\end{aligned}$$

Logo φ é sobre. Segue da observação que o homomorfismo induzido $\overline{\varphi} : A/\operatorname{Ker}(\varphi) \to \operatorname{Im}(\varphi)$ é um isomorfismo, logo

$$A/\operatorname{Ker}(\varphi) \simeq \operatorname{Im}(\varphi),$$

ou seja

$$\frac{A}{I_1 \ldots I_n} \simeq \frac{A}{I_1} \times \frac{A}{I_2} \times \cdots \times \frac{A}{I_n}$$

□

Exemplo 32. Considere o anel dos polinômios com coeficientes no corpo dos números complexos $\mathbb{C}[x]$ e mostre que $\frac{\mathbb{C}[x]}{\langle x^2-3\rangle} \simeq \frac{\mathbb{C}[x]}{\langle x+\sqrt{3}\rangle} \times \frac{\mathbb{C}[x]}{\langle x-\sqrt{3}\rangle}$. Observe que se $a, b \in A$ então $\langle a \cdot b\rangle = \langle a\rangle \cdot \langle b\rangle$ (**Exercício 11.**). Como $x^2 - 3 = (x + \sqrt{3})(x - \sqrt{3}) \in \mathbb{C}[x]$ logo temos $\left\langle x^2 - 3\right\rangle = \left\langle x + \sqrt{3}\right\rangle \cdot \left\langle x - \sqrt{3}\right\rangle$. Agora observe que

$$1 = \frac{(x + \sqrt{3}) - (x - \sqrt{3})}{2\sqrt{3}} \in \left\langle x + \sqrt{3}\right\rangle + \left\langle x - \sqrt{3}\right\rangle$$

o que implica que os ideais $\left\langle x + \sqrt{3}\right\rangle$ e $\left\langle x - \sqrt{3}\right\rangle$ são coprimos. Logo pelo TCR

$$\frac{\mathbb{C}[x]}{\langle x^2 - 3\rangle} = \frac{\mathbb{C}[x]}{\left\langle x + \sqrt{3}\right\rangle \cdot \left\langle x - \sqrt{3}\right\rangle} \simeq \frac{\mathbb{C}[x]}{\left\langle x + \sqrt{3}\right\rangle} \times \frac{\mathbb{C}[x]}{\left\langle x - \sqrt{3}\right\rangle}.$$

1.2 EXERCÍCIOS

Ex. 1 — Seja $S \subseteq A$ um subconjunto de um anel A. Mostre que:

1. $\langle S\rangle$ é um ideal de A .
2. $\langle S\rangle$ é o menor ideal de A que contém o subconjunto S.
3. Se $a, b \in A$ então $\langle a \cdot b\rangle = \langle a\rangle \cdot \langle b\rangle$.

Ex. 2 — Se $f : A \to B$ é um homomorfismo de anéis e J um ideal de B, então a pré-imagem $f^{-1}(J)$ é um ideal de A.

Ex. 3 — O elemento $a \in A$ é uma unidade se e somente se $\langle a \rangle = A = \langle 1 \rangle$.

Ex. 4 — Prove o *Teorema da Correspondência de Ideais*: os ideais de A/I estão em bijeção com os ideais de A que contém I. Mostre que esta bijeção preserva ideais primos e maximais.

Ex. 5 — Prove que todo ideal próprio I de A está contido num ideal maximal.

Ex. 6 — Seja A um anel não nulo. Mostre que as seguintes afirmações são equivalentes:

a. A é um corpo;

b. os únicos ideais de A são 0 e A;

c. todo homomorfismo de A num anel não nulo B é injetivo.

Ex. 7 — Mostre que $\mathfrak{p}$ é um ideal primo se e somente se $A/\mathfrak{p}$ é um domínio de integridade.

Ex. 8 — Demonstre que todo homomorfismo de anéis $f : A \to B$ induz um isomorfismo de anéis $\overline{f} : A/\operatorname{Ker}(f) \to \operatorname{Im}(f)$ dado por $\overline{f}(\overline{a}) = f(a)$.

Ex. 9 — Seja A um anel, mostre que $\frac{A[x_1,\ldots,x_n]}{\langle x_1-a_1,\ldots,x_n-a_n\rangle} \simeq A$.

Ex. 10 — Seja $\mathbf{k}$ um corpo e seja $f(x) \in \mathbf{k}[x]$ um polinômio não nulo com fatoração

$$f(x) = a \cdot p_1(x)^{e_1} \cdots p_r(x)^{e_r},$$

em potências de polinômios mônicos irredutíveis distintos $p_i(x)$.

1. Mostre que:

$$\frac{\mathbf{k}[x]}{\langle f(x)\rangle} \simeq \frac{\mathbf{k}[x]}{\langle p_1(x)^{e_1}\rangle} \times \cdots \times \frac{\mathbf{k}[x]}{\langle p_r(x)^{e_r}\rangle}.$$

2. Conclua que $\frac{\mathbb{F}_q[x]}{\langle x^q-x\rangle} \simeq \underbrace{\mathbb{F}_q \times \cdots \times \mathbb{F}_q}_{q \text{ vezes}}$

Ex. 11 — Sejam I, J e K ideais de A. Mostre que:

1. $I + J$ é o menor ideal de A contendo I e J.
2. $I \cap J$ é ideal de A
3. $I \cdot J \subseteq I \cap J$
4. Se $I + J = A$, então $I \cdot J = I \cap J$
5. $I \cdot (J + K) = I \cdot J + I \cdot K$
6. Se $J \subseteq I$ ou $K \subseteq I$ então $I \cap (J + K) = I \cap J + I \cap K$ (Lei Modular).

Ex. 12 — Seja A um anel e $f = a_0 + a_1 x + \ldots a_n x^n \in A[x]$, mostre que:

1. f é unidade em $A[x]$ se e somente se a_0 é unidade em A e $a_1, \ldots, a_n$ forem nilpotentes.
2. f é nilpotente em $A[x]$ se e somente se $a_0, a_1, \ldots, a_n$ forem nilpotentes.
3. f é um divisor de zero em $A[x]$ se e somente se existe $a \neq 0$ em A tal que $af = 0$.

Ex. 13 — Seja $\mathfrak{p}$ um ideal primo e sejam I_i ideais quaisquer do anel A. Mostre que $\mathfrak{p} \supseteq I_1 I_2 \cdots I_n \iff \mathfrak{p} \supseteq I_i$ para algum i.

Ex. 14 — Seja A o anel das funções reais contínuas em $[0, 1]$, i.e,

$$A = \{f : [0,1] \to \mathbb{R} | \quad f \text{ é contínua}\}.$$

Mostre que qualquer ideal maximal de A é da forma

$$I_x = \{f \in A | f(x) = 0\}$$

para algum $x \in [0, 1]$. Conclua que existe uma bijeção entre pontos $x \in [0, 1]$ e ideais maximais de A.

Ex. 15 — Mostre que o **nilradical**

$$\mathfrak{N}(A) := \{a \in A, \exists n \in \mathbb{N} > 0 : a^n = 0\}$$

é um ideal de A.

Ex. 16 — Se I é ideal de um anel A, definimos o **radical** de I por

$$\sqrt{I} = \{a \in A | a^n \in I, \text{ para algum } n > 0\}$$

1. Mostre que $\sqrt{I}$ é um ideal de A contendo I.
2. Dado $\pi : A \to A/I$ a projeção canônica. Mostre que $\sqrt{I} = \pi^{-1}(\mathfrak{N}(A/I))$
3. Mostre que $\sqrt{\sqrt{I}} = \sqrt{I}$

4. Mostre que $\sqrt{I \cdot J} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.
5. Mostre que se I é primo então $\sqrt{I^n} = I$ para todo $n \in \mathbb{N}$.

Ex. 17 — Um ideal I de um anel A é dito radical se $\sqrt{I} = I$. Mostre que

1. Todo ideal primo é radical.
2. (0) é ideal radical de $\mathbb{Z}/n\mathbb{Z}$ se, e somente se, n é livre de quadrados.[4] Deduza que $\langle n \rangle$ é ideal radical de $\mathbb{Z}$ se, e somente se, n é livre de quadrados.

Ex. 18 — Dado A um anel e $\mathfrak{N}$ o seu nilradical. Mostre que são equivalentes:

a. A possui apenas um ideal primo;

b. Todo elemento de A ou é uma unidade ou nilpotente;

c. $A/\mathfrak{N}$ é um corpo.

Ex. 19 — Sejam I, J e K ideais de A. Mostre que:

$$\sqrt{I + J \cdot K} = \sqrt{I + J \cap K} = \sqrt{I + J} \cap \sqrt{I + K}$$

Ex. 20 — Sejam I, I_i, J, J_i e K ideais de A. Definimos o **ideal quociente** de I por J como sendo $(I : J) = \{a \in A \mid a \cdot J \subseteq I\}$. Mostre que:

1. $(I : J)$ é um ideal de A que contém I.
2. $((I : J) : K) = (I : J \cdot K) = ((I : K) : J)$
3. $(\bigcap_i I_i : J) = \bigcap_i (I_i : J)$
4. $(I : \sum_i J_i) = \bigcap_i (I : J_i)$

4 Um número natural é dito **livre de quadrados** se não for divisível pelo quadrado de nenhum número inteiro diferente de 1.

2

VARIEDADES

2.1 ESPECTRO

Definição 33. Definimos o **espectro** de um anel A, $\mathrm{Spec}(A)$, como sendo o conjunto de todos os ideais primos de A.

Se $\phi : A \to B$ é um homomorfismo de anéis, denotamos por

$$\begin{aligned} \mathrm{Spec}(\phi) : \mathrm{Spec}(B) &\to \mathrm{Spec}(A) \\ \mathfrak{q} &\mapsto \phi^{-1}(\mathfrak{q}) \end{aligned}$$

o morfismo entre espectros induzido por ϕ. Note que $\mathrm{Spec}(\phi)$ está bem definido pois da Proposição 11, $\phi^{-1}(\mathfrak{q})$ é um ideal primo de A.

Lema 34. *Seja A um anel.*

a. $\mathrm{Spec}(A) = \emptyset$ *se e somente se* $A = 0$.

b. Seja I um ideal qualquer do anel A e $\pi : A \to A/I$ o homomorfismo projeção. Então $\mathrm{Spec}(\pi) : \mathrm{Spec}(A/I) \to \mathrm{Spec}(A)$ *é injetor e sua imagem é dada por*

$$V(I) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \supseteq I\}$$

de modo que temos uma identificação natural $\mathrm{Spec}(A/I) = V(I)$.

Demonstração. A primeira afirmação é consequência do Teorema 14 (Todo anel não nulo possui pelo menos um ideal maximal e portanto primo) e o segundo é consequência do TCI e do fato dessa "correspondência" preservar ideais primos. □

Mostraremos a seguir que os conjuntos da forma $V(I)$, para I um ideal qualquer de A, são os fechados de uma topologia em $\mathrm{Spec}(A)$, chamada **Topologia de Zariski**.

Lema 35. *Seja A um anel, I, J e I_i ideais de A. Então:*

a. $V((0)) = \mathrm{Spec}(A)$ *e* $V(A) = \emptyset$;

b. $V(I) \cup V(J) = V(I \cdot J)$;

c. $\bigcap_{i \in \Lambda} V(I_i) = V(\sum_{i \in \Lambda} I_i)$.

Demonstração. O primeiro item é trivial. Para ver (b.) Seja $\mathfrak{p} \in V(I) \cup V(J)$ logo ou $\mathfrak{p} \in V(I)$ ou $\mathfrak{p} \in V(J)$, ou seja, ou $I \subseteq \mathfrak{p}$ ou $J \subseteq \mathfrak{p}$. Logo $I \cdot J \subseteq \mathfrak{p}$ o que implica $\mathfrak{p} \in V(I \cdot J)$. Reciprocamente, seja $\mathfrak{p} \in V(I \cdot J)$ isto significa que $I \cdot J \subseteq \mathfrak{p}$. Suponha que $I \nsubseteq \mathfrak{p}$ logo existe $a \in I$ tal que $a \notin \mathfrak{p}$. Seja $b \in J$ um elemento qualquer então $a \cdot b \in I \cdot J \subseteq \mathfrak{p}$, como $\mathfrak{p}$ é primo e $a \notin \mathfrak{p}$ então necessariamente $b \in \mathfrak{p}$ e logo $J \subseteq \mathfrak{p}$, logo $\mathfrak{p} \in V(J)$ e portanto $\mathfrak{p} \in V(I) \cup V(J)$. Para ver (c.) lembre que, por definição, $\sum_{i\in\Lambda} I_i$ é o menor ideal que contém todos os I_i, logo

$$\begin{aligned}\mathfrak{p} \in V(\sum_{i\in\Lambda} I_i) &\Leftrightarrow \sum_{i\in\Lambda} I_i \subseteq \mathfrak{p} \Leftrightarrow I_i \subseteq \mathfrak{p} \text{ para todo } i \in \Lambda \\ &\Leftrightarrow \mathfrak{p} \in V(I_i) \text{ para todo } i \in \Lambda \Leftrightarrow \mathfrak{p} \in \bigcap_{i\in\Lambda} V(I_i).\end{aligned}$$

□

Aula 4

aula 4: 27/08/2014

Lembrando a última aula. Definimos o **espectro** de um anel A, $\operatorname{Spec}(A)$, como sendo o conjunto de todos os ideais primos de A.

Se $\phi : A \to B$ é um homomorfismo de anéis, denotamos por

$$\begin{aligned}\operatorname{Spec}(\phi) : \operatorname{Spec}(B) &\to \operatorname{Spec}(A) \\ \mathfrak{q} &\mapsto \phi^{-1}(\mathfrak{q})\end{aligned}$$

o mapa entre espectros induzido por ϕ.

Seja I um ideal qualquer do anel A definimos $V(I) := \{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{p} \supseteq I\}$, provamos que os conjuntos das forma $V(I)$ são os fechados de uma topologia em $\operatorname{Spec}(A)$, chamada **Topologia de Zariski**.

Lema. *Seja A um anel, I, J e I_i ideais de A. Então:*

a. $V((0)) = \operatorname{Spec}(A)$ *e* $V(A) = \emptyset$;

b. $V(I) \cup V(J) = V(I \cdot J)$;

c. $\bigcap_{i\in\Lambda} V(I_i) = V(\sum_{i\in\Lambda} I_i)$.

Demonstração. Restava provar (c.). Lembre que, por definição, $\sum_{i\in\Lambda} I_i$ é o menor ideal que contém todos os I_i, logo

$$\begin{aligned}\mathfrak{p} \in V(\sum_{i\in\Lambda} I_i) &\Leftrightarrow \sum_{i\in\Lambda} I_i \subseteq \mathfrak{p} \Leftrightarrow I_i \subseteq \mathfrak{p} \text{ para todo } i \in \Lambda \\ &\Leftrightarrow \mathfrak{p} \in V(I_i) \text{ para todo } i \in \Lambda \Leftrightarrow \mathfrak{p} \in \bigcap_{i\in\Lambda} V(I_i).\end{aligned}$$

□

Queremos ver agora algumas propriedades da Topologia de Zariski, para isso dado um elemento $a \in A$ definimos o conjunto

$$D(a) := \{\mathfrak{p} \in \operatorname{Spec}(A) \mid a \notin \mathfrak{p}\}.$$

Teorema 36. *(***Topologia de Zariski***) Seja A um anel. Temos:*

a. *A família de subconjuntos $\{D(a)\}_{a\in A}$ de $\operatorname{Spec}(A)$ é uma base de abertos da topologia de Zariski.*

b. *$D(a \cdot b) = D(a) \cap D(b)$.*

c. *Se $f : A \to B$ é um homomorfismo de anéis, então $\operatorname{Spec}(f) : \operatorname{Spec}(B) \to \operatorname{Spec}(A)$ é contínuo.*

d. *Se $\mathfrak{p} \in \operatorname{Spec}(A)$ temos $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$ (fecho topológico). Em particular,*

   a) $\mathfrak{m} \in \operatorname{Spec}(A)$ é um ponto fechado se, e somente se, $\mathfrak{m}$ é um ideal maximal;

   b) se A é um domínio de integridade, (0) é um ponto denso.

e. *$\operatorname{Spec}(A)$ é compacto.*

Demonstração.

a. Veja que os conjuntos $D(a)$ são abertos (**Exercício 1.**). Uma família de subconjuntos é uma base de abertos para uma topologia se todo aberto pode ser escrito como união de alguns subconjuntos da família. Todo aberto da topologia de Zariski de $\operatorname{Spec}(A)$ é da forma $\operatorname{Spec}(A) \setminus V(I)$ para algum ideal I de A, ou seja é o conjunto dos ideais primos de A que não contem I. Seja $\mathfrak{p} \in \operatorname{Spec}(A) \setminus V(I)$, então existe $a \in I$ tal que $a \notin \mathfrak{p}$ logo $\mathfrak{p} \in D(a)$ o que implica que $\mathfrak{p} \in \bigcup_{a\in I} D(a)$. Reciprocamente, seja $\mathfrak{p} \in \bigcup_{a\in I} D(a)$ então existe $a \in I$ tal que $\mathfrak{p} \in D(a)$, logo $\mathfrak{p} \in \operatorname{Spec}(A)$ e $a \notin \mathfrak{p}$, logo $I \nsubseteq \mathfrak{p}$ e portanto $\mathfrak{p} \notin V(I)$ ou seja $\mathfrak{p} \in \operatorname{Spec}(A) \setminus V(I)$. Logo todo aberto da topologia de Zariski de $\operatorname{Spec}(A)$ se escreve como uma união de alguns $D(a)$.

b. **Exercício 2.**

c. Lembre que um aplicação é contínua se e somente se pré-imagem de aberto é aberto. Segue do item (a.) que $\{D(a)\}_{a\in A}$ é uma base de abertos da topologia de $\operatorname{Spec}(A)$, logo basta provar que $(\operatorname{Spec}(f))^{-1}(D(a))$ é aberto. Temos

$$\begin{aligned}&\mathfrak{p} \in (\operatorname{Spec}(f))^{-1}(D(a)) \Leftrightarrow \operatorname{Spec}(f)(\mathfrak{p}) \in D(a)\\ &\Leftrightarrow f^{-1}(\mathfrak{p}) \in D(a) \Leftrightarrow a \notin f^{-1}(\mathfrak{p}) \Leftrightarrow f(a) \notin \mathfrak{p} \Leftrightarrow \mathfrak{p} \in D(f(a))\end{aligned}$$

Logo $(\mathrm{Spec}(f))^{-1}(D(a)) = D(f(a))$ é aberto e portanto $\mathrm{Spec}(f)$ é contínuo.

d. Lembramos também que o fecho topológico de um conjunto é a intersecção de todos os fechados que o contem, assim

$$\overline{\{\mathfrak{p}\}} = \bigcap_{\mathfrak{p}\in V(I)} V(I) = \bigcap_{I\subseteq\mathfrak{p}} V(I) \overset{(c.)}{=} V(\sum_{I\subseteq\mathfrak{p}} I),$$

agora veja que $\mathfrak{p} \subseteq \sum_{I\subseteq\mathfrak{p}} I$ e também $\mathfrak{p}$ contém todos os I's, mas $\sum_{I\subseteq\mathfrak{p}} I$ é o menor ideal com essa propriedade, logo $\sum_{I\subseteq\mathfrak{p}} I \subseteq \mathfrak{p}$ o que implica $\mathfrak{p} = \sum_{I\subseteq\mathfrak{p}} I$ e portanto $\overline{\{\mathfrak{p}\}} = V(\mathfrak{p})$.

   a) Seja $\mathfrak{m} \in \mathrm{Spec}(A)$ um ideal maximal então $V(\mathfrak{m}) = \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \supseteq \mathfrak{m}\} = \{\mathfrak{m}\} = \overline{\{\mathfrak{m}\}}$, logo $\mathfrak{m}$ é um ponto fechado. Reciprocamente, se $\mathfrak{m} \in \mathrm{Spec}(A)$ é um ideal próprio, logo está contido em algum ideal maximal $\mathfrak{m}'$ (Corolário 15 e Exercício 5 da Lista 1) logo $\mathfrak{m}' \in V(\mathfrak{m}) = \overline{\{\mathfrak{m}\}} = \{\mathfrak{m}\}$, por tanto $\mathfrak{m}$ é maximal.

   b) Se A é um domínio de integridade então (0) é um ideal primo, logo $\overline{\{(0)\}} = V((0)) = \mathrm{Spec}(A)$.

e. Pelo item (a.), é suficiente provar que toda cobertura de $\mathrm{Spec}(A)$ por uma família de abertos básicos $\{D(a_\alpha), \alpha \in \Lambda\}$, admite subcobertura finita. Assim, se $\mathfrak{p} \in \mathrm{Spec}(A)$ então existe $\alpha \in \Lambda$ tal que $\mathfrak{p} \in D(a_\alpha)$, ou seja $a_\alpha \notin \mathfrak{p}$. Considere então o ideal $I = \langle a_\alpha, \alpha \in \Lambda\rangle$, logo $I \nsubseteq \mathfrak{p}$ para todo $\mathfrak{p} \in \mathrm{Spec}(A)$. Em particular I não vai estar contido em nenhum ideal maximal, logo segue do Corolário 15 (Exercício 5 da Lista 1) que I não é próprio, assim $A = \langle a_\alpha, \alpha \in \Lambda\rangle$ e portanto podemos escrever $1 = \sum_{i=1}^n b_i \cdot a_{\alpha_i}$ como combinação A-linear finita de elementos a_{α_i}, o que implica que $A = \langle a_{\alpha_i}, 1 \le i \le n\rangle$. Mas então cada $a_\alpha = \sum_{i=1}^n c_i \cdot a_{\alpha_i}$, logo se $a_\alpha \notin \mathfrak{p}$ então existe $1 \le i \le n$ tal que $c_i \cdot a_{\alpha_i} \notin \mathfrak{p}$ o que implica que $\mathfrak{p} \in D(c_i \cdot a_{\alpha_i}) = D(c_i) \cap D(a_{\alpha_i})$. Em conclusão, para cada $\mathfrak{p} \in \mathrm{Spec}(A)$ existe $1 \le i \le n$ tal que $\mathfrak{p} \in D(a_{\alpha_i})$, logo $\mathrm{Spec}(A) = \bigcup_{i=1}^n D(a_{\alpha_i})$.

□

Vejamos alguns exemplos:

Exemplo 37.

a. $(0) \in \mathrm{Spec}(A)$ se, e somente se, A é um domínio.

b. Se $A = \mathbf{k}$ é um corpo, então é um domínio e os únicos ideais são (0) e $\mathbf{k}$, logo $\mathrm{Spec}(\mathbf{k}) = \{(0)\}$.

c. Seja A um DIP. Então um ideal (a) não nulo é primo se, e somente se, a é irredutível (**Exercício 3.**) (i.e., Se A for um domínio um elemento $a \neq 0$ e $a \notin A^\times$ é dito **irredutível** se sempre que $a = b \cdot c$ então $b \in A^\times$ ou $c \in A^\times$). Logo $\text{Spec}(A) = \{(0)\} \cup \{(a) \mid a \text{ é irredutível}\}$.

d. Se A for um DFU, (Domínio de Fatoração Única, i.e., se todo elemento não nulo $a \in A$ pode ser escrito como produto $a = b_1 b_2 \dots b_m$ com b_i irredutíveis e se também $a = c_1 c_2 \dots c_n$ com c_i irredutíveis então $m = n$ e existe uma permutação $\sigma : \{1, 2, \dots, m\} \to \{1, 2, \dots, m\}$ tal que $b_i = u c_{\sigma(i)}$ para algum $u \in A^\times$ para todo $i = 1, 2, \dots, m$) então também todo ideal principal (a) não nulo é primo se, e somente se, a é irredutível. Entretanto um DFU em geral possui diversos ideais primos que não são principais: se $A = \mathbf{k}$ for um corpo, então $(x_1), (x_1, x_2), \dots, (x_1, x_2, \dots, x_n) \in \text{Spec}(\mathbf{k}[x_1, \dots, x_n])$ já que os anéis quociente $\frac{\mathbf{k}[x_1, x_2, \dots, x_n]}{(x_1, \dots, x_i)}$ são domínios, pois:

$$\frac{\mathbf{k}[x_1, x_2, \dots, x_n]}{(x_1, \dots, x_i)} \simeq \frac{\mathbf{k}[x_1, \dots, x_i]}{(x_1, \dots, x_i)}[x_{i+1}, \dots, x_n] \simeq \mathbf{k}[x_{i+1}, \dots, x_n].$$

e. Seja $A = \mathbf{k} \times \mathbf{k}$ então os ideais de a são: $(0) \times (0)$, $(0) \times \mathbf{k}$, $\mathbf{k} \times (0)$, $\mathbf{k} \times \mathbf{k}$. Observe que A não é um domínio pois $(0,0) = (1,0) \cdot (0,1)$ logo $(0) \times (0) \notin \text{Spec}(A)$, também $\mathbf{k} \times \mathbf{k} \notin \text{Spec}(A)$ pois não é próprio. Vejamos que $(0) \times \mathbf{k}$ é primo, seja $a \cdot b \in (0) \times \mathbf{k}$ logo existe $a_1, a_2, b_1, b_2, c \in \mathbf{k}$ tal que $a \cdot b = (a_1, a_2) \cdot (b_1, b_2) = (0, c)$, logo $a_1 \cdot b_1 = 0$ e como $\mathbf{k}$ é corpo então ou $a_1 = 0$ ou $b_1 = 0$ logo ou $a \in (0) \times \mathbf{k}$ ou $b \in (0) \times \mathbf{k}$. Analogamente vemos que $\mathbf{k} \times (0)$ é primo. Logo $\text{Spec}(\mathbf{k} \times \mathbf{k}) = \{(0) \times \mathbf{k}, \mathbf{k} \times (0)\}$. Observe que ambos os ideais são maximais e portanto fechados e logo abertos.

Generalizando este caso temos o seguinte exemplo

f. (**Exercício 4.**) Mostre que:

a) Os ideais de $A \times B$ são da forma $I \times J$ onde I é um ideal de A e J é um ideal de B.

b) Conclua que os ideais primos de $A \times B$ são da forma $\mathfrak{p} \times B$ e $A \times \mathfrak{q}$ com $\mathfrak{p} \in \text{Spec}(A)$ e $\mathfrak{q} \in \text{Spec}(B)$. Assim temos,

$$\text{Spec}(A \times B) = \text{Spec}(A) \bigsqcup \text{Spec}(B)$$

em que identificamos $\mathfrak{p} \times B$ com $\mathfrak{p}$ e $A \times \mathfrak{q}$ com $\mathfrak{q}$.

g. Como $\mathbf{k}[t]$ é um DIP, os conjuntos $V((f)) = \{(p) \mid p \text{ é um fator irredutível de } f\}$ para $f \in \mathbf{k}[t]$ não nulo. Logo os fechados em $\text{Spec}(\mathbf{k}[t])$ são $\emptyset$,

$\mathrm{Spec}(\mathbf{k}[t])$ e uniões de um número finito de pontos (pontos=ideais primos) .

h. Seja $A = \mathbf{k}[[t]]$ o anel das séries formais $f(t) = a_0 + a_1 t + \cdots + a_n t^n + \cdots$. Então f é uma unidade se, e somente se, a_0 é uma unidade. Como $\mathbf{k}[[t]]$ é DIP, o ideal (0) é primo. Provaremos agora que (t) é maximal. Seja I um ideal qualquer e seja $h = c_0 + c_1 t + \cdots + c_n t^n + \cdots \in I$, então se $c_0 \neq 0$ (logo c_0 é uma unidade) h é uma unidade e $I = \mathbf{k}[[t]]$. Mas se $c_0 = 0$ então $h \in (t)$ logo $I \subseteq (t)$ o que implica que (t) é maximal e portanto primo. Seja agora I um outro ideal primo com $h \in I$ então $c_0 = 0$ pois I é próprio. Logo existe $r \geq 1$ tal que $h = t^r \cdot (b_r + b_{r+1} t + \cdots)$ com $b_r \neq 0$. Se $b_r + b_{r+1} t + \cdots \in I$ como esse elemento é uma unidade $I = \mathbf{k}[[t]]$ o que é uma contradição, logo como I é primo necessariamente $t^r \in I$ do que segue que $t \in I$ e portanto $(t) \subseteq I$, mas como (t) é maximal temos $I = (t)$ e por tanto (t) é o único ideal primo. Assim $\mathrm{Spec}(\mathbf{k}[[t]]) = \{(0)\} \cup \{(t)\}$. Por outro lado, temos que (t) é um ponto fechado (pois é maximal) enquanto que (0) é um ponto denso (pois $\mathbf{k}[[t]]$ é um domínio). Assim os fechados de $\mathrm{Spec}(\mathbf{k}[[t]])$ são: $\emptyset$, $\mathrm{Spec}(\mathbf{k}[[t]])$ e $\{(t)\}$

Aula 5

aula 5: 29/08/2014

No Exemplo 5 da aula passada, (**Exercício 4.**) Mostre que:

a. Os ideais de $A \times B$ são da forma $I \times J$ onde I é um ideal de A e J é um ideal de B.

b. Conclua que os ideais primos de $A \times B$ *"são da forma* $\mathfrak{p} \times (0)$ *e* $(0) \times \mathfrak{q}$ *com* $\mathfrak{p} \in \mathrm{Spec}(A)$ *e* $\mathfrak{q} \in \mathrm{Spec}(B)$*"* deve-se trocar por ***"são da forma*** $\mathfrak{p} \times B$ ***e*** $A \times \mathfrak{q}$ ***com*** $\mathfrak{p} \in \mathrm{Spec}(A)$ ***e*** $\mathfrak{q} \in \mathrm{Spec}(B)$***"***. Assim temos,

$$\mathrm{Spec}(A \times B) = \mathrm{Spec}(A) \bigsqcup \mathrm{Spec}(B)$$

"em que identificamos $\mathfrak{p} \times (0)$ *com* $\mathfrak{p}$ *e* $(0) \times \mathfrak{q}$ *com* $\mathfrak{q}$*"* trocar por ***"em que identificamos*** $\mathfrak{p} \times B$ ***com*** $\mathfrak{p}$ ***e*** $A \times \mathfrak{q}$ ***com*** $\mathfrak{q}$***"***.

A forma anterior não funciona pois temos o seguinte **contraexemplo:** Seja $A = \mathbf{k} \times \mathbf{k}$ então os ideais de a são: $(0) \times (0)$, $(0) \times \mathbf{k}$, $\mathbf{k} \times (0)$, $\mathbf{k} \times \mathbf{k}$. Dado que $\mathrm{Spec}(\mathbf{k}) = \{(0)\}$ então, de acordo à primeira identificação, teríamos que o único ideal primo de $\mathbf{k} \times \mathbf{k}$ seria $(0) \times (0)$. Mas $\mathbf{k} \times \mathbf{k}$ não é um domínio pois $(0,0) = (1,0) \cdot (0,1)$ logo $(0) \times (0) \notin \mathrm{Spec}(\mathbf{k} \times \mathbf{k})$. Vejamos então que os ideais primos de $A \times B$ de fato são dessa forma.

Seja então $I \times J$ um ideal $A \times B$, então temos um isomorfismo $\frac{A \times B}{I \times J} \xrightarrow{\simeq} \frac{A}{I} \times \frac{B}{J}$ dado por $(a,b) + (I \times J) \mapsto (a + I, b + J)$. Agora observe que $A \times B$

é um domínio se e somente se ($A = 0$ e B é um domínio) ou ($B = 0$ e A é um domínio). Assim $I \times J$ um ideal primo $A \times B \Leftrightarrow \frac{A\times B}{I\times J}$ é um domínio$\Leftrightarrow$ $\frac{A}{I} \times \frac{B}{J}$ é um domínio $\Leftrightarrow$ ($\frac{A}{I} = 0$ e $\frac{B}{J}$ é um domínio) ou ($\frac{B}{J} = 0$ e $\frac{A}{I}$ é um domínio) $\Leftrightarrow$ ($A = I$ e J é primo) ou ($B = J$ e I é primo).

Exemplo 38. (Exemplo 8) Seja $A = \mathbb{C}[x, y]/(y^2 - x^3 + x)$. Mostraremos que

$$\operatorname{Spec}(A) = \left\{(\overline{0})\right\} \cup \left\{ \langle \overline{x} - a, \overline{y} - b\rangle \mid b^2 = a^3 - a \right\}.$$

Para isso seja $B = \mathbb{C}[x]$, então existe um homomorfismo $\varphi : B \to A$, dado por $x \mapsto \overline{x}$. Note que φ é injetor pois nenhum polinômio na variável x pode ser múltiplo de $y^2 - x^3 + x$. Utilizando a relação $\overline{y}^2 = \overline{x}^3 - \overline{x}$, temos um conjunto de representantes de classe $\frac{\mathbb{C}[x,y]}{(y^2-x^3+x)} = \mathbb{C}[\overline{x}] + \mathbb{C}[\overline{x}] \cdot \overline{y}$ formado pelos polinômios $p(\overline{x}) + q(\overline{x})\overline{y}$ de grau no máximo 1 em y. Observe que $y^2 - x^3 + x$ é um polinômio irredutível no DFU $\mathbb{C}[x, y]$ e assim $(y^2 - x^3 + x) \subseteq \mathbb{C}[x, y]$ é um ideal primo e logo $A = \mathbb{C}[x, y]/(y^2 - x^3 + x)$ é um domínio. Por tanto $(\overline{0}) \in \operatorname{Spec}(A)$.

Seja $\operatorname{Spec}(\varphi) : \operatorname{Spec}(A) \to \operatorname{Spec}(B)$ o morfismo entre espectros induzido por φ e seja $\mathfrak{q} \in \operatorname{Spec}(A)$. Como B é um DIP, segue do Exemplo (c.) que $\operatorname{Spec}(B) = \{(0)\} \cup \{(x - a)\}$, já que os elementos irredutíveis de B são da forma $x - a$, para $a \in \mathbb{C}$. Logo temos dois casos a analisar:

a. $\operatorname{Spec}(\varphi)(\overline{\mathfrak{q}}) = (0)$, ou seja $\varphi^{-1}(\overline{\mathfrak{q}}) = (0)$ o que implica que $\overline{\mathfrak{q}} \cap \mathbb{C}[\overline{x}] = (\overline{0})$. Vamos mostrar que $\overline{\mathfrak{q}} = (\overline{0})$. Seja $a(\overline{x}) + b(\overline{x})\overline{y} \in \overline{\mathfrak{q}}$ multiplicando pelo seu "conjugado", obtemos

$$\begin{aligned} \overline{\mathfrak{q}} &\ni (a(\overline{x}) + b(\overline{x})\overline{y}) \cdot (a(\overline{x}) - b(\overline{x})\overline{y}) = a(\overline{x})^2 - b(\overline{x})^2\overline{y}^2 \\ &= a(\overline{x})^2 - b(\overline{x})^2(\overline{x}^3 - \overline{x}) \in \mathbb{C}[\overline{x}], \end{aligned}$$

como $\overline{\mathfrak{q}} \cap \mathbb{C}[\overline{x}] = (\overline{0})$ e A é um domínio então $a(\overline{x}) = \overline{0}$ e $b(\overline{x}) = \overline{0}$ logo $\overline{\mathfrak{q}} = (\overline{0})$.

b. $\operatorname{Spec}(\varphi)(\overline{\mathfrak{q}}) = (x - a)$ para algum $a \in \mathbb{C}$, ou seja $\varphi^{-1}(\overline{\mathfrak{q}}) = (x - a)$ o que implica que $\overline{\mathfrak{q}} \cap \mathbb{C}[\overline{x}] = (\overline{x} - a) \subseteq \overline{\mathfrak{q}}$. Vamos calcular o $\operatorname{Spec}(A/(\overline{x} - a))$, pois estamos interessados em ideais primos $\overline{\mathfrak{q}}$ de A que contém $(\overline{x} - a)$. Seja $b \in \mathbb{C}$ tal que $b^2 = a^3 - a$, de modo que temos um isomorfismo

$$\frac{A}{(\overline{x} - a)} \simeq \frac{\mathbb{C}[x, y]}{\langle y^2 - x^3 + x, x - a\rangle} \overset{\overline{x}\mapsto a}{\simeq} \frac{\mathbb{C}[y]}{(y^2 - a^3 + a)} = \frac{\mathbb{C}[y]}{(y^2 - b^2)}.$$

Temos alguns sub-casos de acordo com a fatoração de $y^2 - b^2$. Primeiro, se $b \neq 0$, pelo Teorema Chinês dos Restos (Teorema 31) temos

$$\frac{\mathbb{C}[y]}{(y^2 - b^2)} = \frac{\mathbb{C}[y]}{(y-b)} \times \frac{\mathbb{C}[y]}{(y+b)} \simeq \mathbb{C} \times \mathbb{C}$$

que possui somente dois ideais primos: $(0) \times \mathbb{C}$ e $\mathbb{C} \times (0)$ que identificamos (Exemplo f.) com os ideais primos $(\overline{0})$ de $\frac{\mathbb{C}[y]}{(y+b)}$ e $(\overline{0})$ de $\frac{\mathbb{C}[y]}{(y-b)}$. Mas esses ideais correspondem aos ideais primos $(\overline{y} + b)$ e $(\overline{y} - b)$ de $\frac{A}{(\overline{x}-a)}$ que a sua vez correspondem aos ideais primos $\langle \overline{y} - b, \overline{x} - a \rangle$ e $\langle \overline{y} + b, \overline{x} - a \rangle$ de A. Logo neste caso $\overline{\mathfrak{q}}$ é da forma $\langle \overline{y} - b, \overline{x} - a \rangle$ com $b^2 = a^3 - a \neq 0$.

Segundo se $b = 0$ (i.e., $a^3 - a = 0 \Leftrightarrow a = 0$ ou $a = \pm 1$) então

$$\frac{A}{(\overline{x} - a)} = \frac{\mathbb{C}[y]}{(y^2)}$$

logo os ideais primos de $\frac{A}{(\overline{x}-a)}$ correspondem aos ideais primos de $\mathbb{C}[y]$ que contém (y^2) neste caso só há um primo (y) que corresponde ao ideal primo $(\overline{y}, \overline{x} - a)$ de A.

Resumindo: $\mathrm{Spec}(\mathbb{C}[x,y]/\langle y^2 - x^3 + x \rangle)$ consiste no ideal $(\overline{0})$ e nos ideais $\langle \overline{y} - b, \overline{x} - a \rangle$ que estão em bijeção com os pontos (a, b) da curva $y^2 = x^3 - x$.

O subespaço de $\mathrm{Spec}(A)$ consistindo dos ideais maximais de A com a topologia induzida, é chamado de **espectro maximal** de A e é denotado por $\mathrm{Specm}(A)$. Para anéis comutativos arbitrários $\mathrm{Specm}(A)$ não tem as propriedades funtoriais de $\mathrm{Spec}(A)$ por causa que a imagem inversa de um ideal maximal sob um homomorfismo de anéis não é necessariamente maximal.

Como consequência do teorema de existência de ideais maximais temos que $A = 0$ se e somente se $\mathrm{Specm}(A) = \emptyset$ e dado um ideal I qualquer de A segue do TCI que existe uma bijeção natural

$$\mathrm{Specm}(A/I) = \{\mathfrak{m} \in \mathrm{Specm}(A) \mid \mathfrak{m} \supseteq I\}. \tag{1}$$

Do Exercício 9 da Lista 1 existe um isomorfismo $\alpha : \frac{A[x_1,\ldots,x_n]}{\langle x_1 - a_1, \ldots, x_n - a_n \rangle} \to A$, dado por $\overline{x_i} \mapsto a_i$. Seja I um ideal de $A[x_1, \ldots, x_n]$, dados $a_1, \ldots, a_n \in A$ vamos mostrar que $I \subseteq \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ se e somente se $f(a_1, \ldots, a_n) = 0$ para todo $f(x_1, \ldots, x_n) \in I$ de modo que $\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subseteq A[x_1, \ldots, x_n]$ é um ideal de $A[x_1, \ldots, x_n]/I$ se, e somente se, $(a_1, \ldots, a_n) \in A^n$ é um ponto do **conjunto de zeros** $Z(I)$ de I, definido por

$$Z(I) := \{(a_1, \ldots, a_n) \in A^n \mid f(a_1, \ldots, a_n) = 0 \text{ para todo } f(x_1, \ldots, x_n) \in I\}.$$

De fato, temos $I \subseteq \langle x_1 - a_1, \ldots, x_n - a_n\rangle \Leftrightarrow$para cada $f(x_1, \ldots, x_n) \in I$, $\overline{f(x_1, \ldots, x_n)} = \overline{0}$ em $\frac{A[x_1,\ldots,x_n]}{\langle x_1-a_1,\ldots,x_n-a_n\rangle} \Leftrightarrow$para cada $f(x_1, \ldots, x_n) \in I$, $\alpha\left(\overline{f(x_1, \ldots, x_n)}\right) = 0$ em $A \Leftrightarrow$para cada $f(x_1, \ldots, x_n) \in I$, $f(a_1, \ldots, a_n) = 0 \Leftrightarrow (a_1, \ldots, a_n) \in Z(I)$.

Em particular se $A = \mathbf{k}$ for um corpo, $\langle x_1 - a_1, \ldots, x_n - a_n\rangle \in \text{Specm}(\mathbf{k}[x_1, \ldots, x_n])$ para quaisquer n elementos a_i de $\mathbf{k}$. E logo pelo TCI temos que para todo ponto $(a_1, \ldots, a_n) \in Z(I)$, $\langle\overline{x_1 - a_1}, \ldots, \overline{x_n - a_n}\rangle \in \text{Specm}(\mathbf{k}[x_1, \ldots, x_n]/I)$.

Mais tarde, veremos que se $\mathbf{k}$ for algebricamente fechado, a recíproca em ambos casos também é verdadeira (Nullstellensatz Hilberts). Ou seja, todo ideal maximal de $\mathbf{k}[x_1, \ldots, x_n]$ é da forma $\langle x_1 - a_1, \ldots, x_n - a_n\rangle$ para $a_1, \ldots, a_n \in \mathbf{k}$. E, todo ideal maximal de $\mathbf{k}[x_1, \ldots, x_n]/I$ é da forma $\langle\overline{x_1 - a_1}, \ldots, \overline{x_n - a_n}\rangle$ para $(a_1, \ldots, a_n) \in Z(I)$, por tanto temos uma bijeção entre $\text{Specm}(\mathbf{k}[x_1, \ldots, x_n]/I)$ e o conjunto dos zeros $Z(I)$ de I. Mas para isso precisaremos de alguns conceitos da Geometria Algébrica...

2.2 INTRODUÇÃO À GEOMETRIA ALGÉBRICA

Nesta seção $\mathbf{k}$ denotará um **corpo algebricamente fechado**.

Definição 39.

a. O **espaço afim** $\mathbb{A}^n_{\mathbf{k}}$ de dimensão n sobre o corpo $\mathbf{k}$ é o conjunto

$$\mathbb{A}^n_{\mathbf{k}} := \mathbf{k}^n = \underbrace{\mathbf{k} \times \cdots \times \mathbf{k}}_{n \text{ vezes}}.$$

b. Seja $S \subseteq \mathbf{k}[x_1, \ldots, x_n]$ um conjunto de polinômios. O **conjunto algébrico afim** definido por S é o subconjunto $Z(S) \subseteq \mathbb{A}^n_{\mathbf{k}}$ dos zeros comuns de todos os polinômios em S:

$$Z(S) := \{(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbf{k}} \mid f(a_1, \ldots, a_n) = 0 \text{ para todo } f \in S\}.$$

Note que $Z(-)$ reverte inclusões: $S \subseteq T$ então $Z(S) \supseteq Z(T)$. Além disso, se $I \subseteq \mathbf{k}[x_1, \ldots, x_n]$ é o ideal gerado por S, então $Z(S) = Z(I)$. Assim não há perda de generalidade em definir um conjunto algébrico como o conjunto de zeros de um ideal, o que faremos de agora em diante. Mais tarde veremos que todo ideal de $\mathbf{k}[x_1, \ldots, x_n]$ é finitamente gerado (pelo Teorema da Base de Hilbert, Teorema 119) e assim todo conjunto algébrico é o conjunto de zeros de um número *finito* de polinômios.

Podemos definir também uma topologia em $\mathbb{A}^n_{\mathbf{k}}$ (e, por conseguinte, também nos conjuntos algébricos) de acordo com o seguinte Lema:

Lema 40. *Os conjuntos algébricos têm as seguintes propriedades:*

a. $Z((0)) = \mathbb{A}^n_{\mathbf{k}}$ *e* $Z(\mathbf{k}[x_1, \ldots, x_n]) = \emptyset$

b. $Z(I) \cup Z(J) = Z(I \cdot J)$

c. $\bigcap_{i \in \Lambda} Z(I_i) = Z(\sum_{i \in \Lambda} I_i)$.

Assim, os conjuntos algébricos são os fechados de uma topologia de $\mathbb{A}^n_{\mathbf{k}}$*, chamada também de* ***Topologia de Zariski****.*

Demonstração. **Exercício 5.** □

Aula 6

AULA 6: 10/09/2014

Lembrando a última aula. Introdução à Geometria Algébrica.

k denotará um **corpo algebricamente fechado**. Definimos o **espaço afim** $\mathbb{A}^n_{\mathbf{k}}$ de dimensão n sobre o corpo **k** como sendo o conjunto $\mathbb{A}^n_{\mathbf{k}} := \mathbf{k}^n = \underbrace{\mathbf{k} \times \cdots \times \mathbf{k}}_{n \text{ vezes}}$. Definimos um **conjunto algébrico afim** como sendo o conjunto dos zeros comuns de um ideal $I \subseteq \mathbf{k}[x_1, \ldots, x_n]$

$$Z(I) := \{(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbf{k}} \mid f(a_1, \ldots, a_n) = 0 \text{ para todo } f \in I\}.$$

Os conjuntos algébricos são os fechados de uma topologia de $\mathbb{A}^n_{\mathbf{k}}$, chamada também de **Topologia de Zariski**.

Lembramos que um espaço topológico é dito **irredutível** se não pode ser escrito como união de dois fechados próprios, isto implica que quaisquer dois abertos não vazios se interceptam, logo todo aberto não vazio em um espaço irredutível X é denso.

Definição 41. Uma **variedade algébrica** é um conjunto algébrico irredutível.

O espaço afim $\mathbb{A}^n_{\mathbf{k}}$ para $n \geq 1$ é uma variedade. Para ver isso precisamos de seguinte fato: (**Exercício 6.**) Se **k** é um corpo infinito e $f \in \mathbf{k}[x_1, \ldots, x_n]$ é tal que $f(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbf{k}}$ então $f = 0$. Observe que como **k** é algebricamente fechado ele é infinito, pois suponha que ele é finito $\mathbf{k} = \{a_1, \ldots, a_n\}$ então o polinômio $f(x) = (x - a_1)(x - a_2) \ldots (x - a_n) + 1$ não tem raiz em **k**, contradição. Segue que nenhum polinômio não nulo se anula identicamente em todo $\mathbb{A}^n_{\mathbf{k}}$. Assim $Z(I) \subsetneq \mathbb{A}^n_{\mathbf{k}}$ é um fechado próprio se, e somente se, $I \neq (0)$. Logo se $\mathbb{A}^n_{\mathbf{k}} = Z(I) \cup Z(J) = Z(I \cdot J)$ então $I \cdot J = 0$ e como $\mathbf{k}[x_1, \ldots, x_n]$ é um domínio então ou $I = 0$ ou $J = 0$, o que mostra que $\mathbb{A}^n_{\mathbf{k}}$ não é união de dois fechados próprios.

Definição 42. Sejam $X \subseteq \mathbb{A}^m_{\mathbf{k}}$ e $Y \subseteq \mathbb{A}^n_{\mathbf{k}}$ dois conjuntos algébricos afins. Um **morfismo** de conjuntos algébricos $f : X \to Y$ é uma função para a qual existem polinômios $p_1, \ldots, p_n \in \mathbf{k}[x_1, \ldots, x_m]$ tais que

$$f(a_1, \ldots, a_m) = (p_1(a_1, \ldots, a_m), \ldots, p_n(a_1, \ldots, a_m)) \in Y$$

para todo $(a_1, \ldots, a_m) \in X$.

Observamos que composição de morfismos de conjuntos algébricos é também um morfismo de conjuntos algébricos.

Os polinômios p_i não são unicamente determinados por f: se $X = Z(I)$, então somando a cada p_i um elemento de I ainda obtemos a mesma função f. Em outras palavras, os polinômios p_i só estão determinados "módulo polinômios que se anulam sobre todo o X". Isto nos leva a introduzir a seguinte definição:

Definição 43. Seja $X \subseteq \mathbb{A}^n_{\mathbf{k}}$ um conjunto algébrico. O anel (com a soma e o produto de funções induzidos pelas respetivas operações em $\mathbf{k}$)

$$\mathbf{k}[X] := \left\{ f : X \to \mathbb{A}^1_{\mathbf{k}} = \mathbf{k} \mid f \text{ é um morfismo de conjuntos algébricos} \right\}$$

é chamado de **anel de funções regulares** em X.

Existe um morfismo sobrejetor $\mathbf{k}[x_1, \ldots, x_n] \to \mathbf{k}[X]$ que leva um polinômio no morfismo correspondente. O kernel $I(X)$ deste morfismo, i.e.,

$$I(X) := \{ f \in \mathbf{k}[x_1, \ldots, x_n] \mid f(a_1, \ldots, a_n) = 0 \text{ para todo } (a_1, \ldots, a_n) \in X \}$$

é chamado de **ideal do conjunto algébrico** X. Pelo Teorema do Isomorfismo (Exercício 8 Lista 1) temos $\mathbf{k}[X] \simeq \frac{\mathbf{k}[x_1, \ldots, x_n]}{I(X)}$.

Proposição 44. *Sejam $X, Y \subseteq \mathbb{A}^n_{\mathbf{k}}$ conjuntos algébricos temos:*

a. $X \subseteq Y$ *então* $I(X) \supseteq I(Y)$*;*

b. Para um ideal J de $\mathbf{k}[x_1, \ldots, x_n]$ *temos* $J \subseteq I(Z(J))$*.*

c. $X = Z(I(X))$

Demonstração. Os itens a. e b. são triviais. A inclusão $\subseteq$ em c. é clara, enquanto que b. implica que $Z(I(Z(J))) \subseteq Z(J)$, logo se X é conjunto algébrico então $Z(I(X)) \subseteq X$. □

Em geral a inclusão em b. é estrita: considere por exemplo o ideal $J = (x^2) \subseteq \mathbf{k}[x]$, então $Z(x^2) = \left\{ a \in \mathbb{A}^1_{\mathbf{k}} = \mathbf{k} \mid a^2 = 0 \right\} = 0$ logo $I(Z(J)) = I(Z(x^2)) = I(0) = \{ f \in \mathbf{k}[x] \mid f(0) = 0 \}$, ou seja são os polinômios em uma variável com termo constante nulo. Logo $x \in I(Z(J))$ mas $x \notin (x^2) = J$.

Diversas propriedades geométricas de um conjunto algébrico X se traduzem em propriedades algébricas de seu anel de funções regulares $\mathbf{k}[X]$ e vice-versa. Como um primeiro exemplo temos a seguinte proposição:

Proposição 45. *Seja X um conjunto algébrico, então são equivalentes:*

a. X *é uma variedade;*

b. $\mathbf{k}[X]$ *é um domínio;*

c. $I(X)$ *é um ideal primo.*

Demonstração. É claro que $\mathbf{k}[X]$ é um domínio $\Leftrightarrow$ $I(X)$ é um ideal primo. Suponha, então, que $X \subseteq \mathbb{A}^n_{\mathbf{k}}$ não seja uma variedade, i.e., X é união de dois fechados próprios:

$$\begin{aligned} X &= (X \cap Z(I)) \cup (X \cap Z(J)) = X \cap (Z(I) \cup Z(J)) \\ &\Leftrightarrow X \subseteq Z(I) \cup Z(J) = Z(I \cdot J) \end{aligned}$$

onde I e J são ideais de $\mathbf{k}[x_1, \ldots, x_n]$. Como estes fechados são próprios (i.e., $X \cap Z(I) \subsetneq X$ então $X \nsubseteq Z(I)$, idem com J), existem polinômios $f \in I$ e $g \in J$ que não se anulam sobre todo X, logo $f, g \notin I(X)$. Por outro lado, como $f \cdot g \in I \cdot J$, então $f \cdot g$ se anula identicamente sobre X (i.e., $f \cdot g \in I(X)$). Assim, as imagens $\overline{f}, \overline{g} \in \mathbf{k}[X] = \frac{\mathbf{k}[x_1,\ldots,x_n]}{I(X)}$ de f e g são tais que $\overline{f} \cdot \overline{g} = 0$ mas $\overline{f} \neq 0$ e $\overline{g} \neq 0$, mostrando que $\mathbf{k}[X]$ não é domínio.

Reciprocamente, suponha que $\mathbf{k}[X]$ não seja domínio e sejam $\overline{f}, \overline{g} \in \mathbf{k}[X]$ tais que $\overline{f} \cdot \overline{g} = 0$ com $\overline{f} \neq 0$ e $\overline{g} \neq 0$. Se $f, g \in \mathbf{k}[x_1, \ldots, x_n]$ são dois levantamentos de $\overline{f}, \overline{g}$ então $f \cdot g \in I(X)$ ou seja $f \cdot g$ se anula sobre todo X mas o mesmo não ocorre nem com f nem com g. Assim,

$$X \subseteq Z(f \cdot g) = Z(f) \cup Z(g) \Leftrightarrow X = (X \cap Z(f)) \cup (X \cap Z(g))$$

mostra que X é união de dois fechados próprios, ou seja, não é variedade. □

Seja $X \subseteq \mathbb{A}^n_{\mathbf{k}}$ um conjunto algébrico e seja $P = (a_1, \ldots, a_n) \in X$ um ponto[1] deste conjunto. Defina

$$\mathfrak{m}_P := I(P) = \{f \in \mathbf{k}[x_1, \ldots, x_n] \mid f(P) = f(a_1, \ldots, a_n) = 0\}.$$

Claramente, $x_i - a_i \in \mathfrak{m}_P$ para $i = 1, \ldots, n$ assim $\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subseteq \mathfrak{m}_P$. Mas $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ é um ideal maximal já que

$$\frac{\mathbf{k}[x_1, \ldots, x_n]}{\langle x_1 - a_1, \ldots, x_n - a_n \rangle} \simeq \mathbf{k}$$

é um corpo, logo $\mathfrak{m}_P = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ é um ideal maximal de $\mathbf{k}[x_1, \ldots, x_n]$ que contém $I(X)$ (pois $P \subseteq X$ implica $I(X) \subseteq I(P)$). Isto

1 Qualquer ponto $(a_1, \ldots, a_n)$ do espaço afim $\mathbb{A}^n_{\mathbf{k}}$ é um conjunto algébrico, pois $(a_1, \ldots, a_n) = Z(\langle x_1 - a_1, \ldots, x_n - a_n \rangle)$

implica que $\mathfrak{m}_P$ corresponde a um ideal maximal de $\mathbf{k}[X] \simeq \frac{\mathbf{k}[x_1,\ldots,x_n]}{I(X)}$ que denotaremos por $\overline{\mathfrak{m}}_P$. Temos então uma bijeção natural

$$X \xrightarrow{\simeq} \operatorname{Specm}(\mathbf{k}[X]) = \operatorname{Specm}(\frac{\mathbf{k}[x_1,\ldots,x_n]}{I(X)})$$
$$P = (a_1,\ldots,a_n) \longmapsto \overline{\mathfrak{m}}_P = \frac{I(P)}{I(X)} = \langle \overline{x}_1 - a_1, \ldots, \overline{x}_n - a_n \rangle$$

Esta associação é claramente injetora pois se dois pontos $P \neq Q$ diferem nas i-ésimas coordenadas $a_i \neq b_i$ então $\overline{x_i} - a_i \in \mathfrak{m}_P \backslash \mathfrak{m}_Q$. Para ver que é sobre, ou seja que $\operatorname{Specm}(\frac{\mathbf{k}[x_1,\ldots,x_n]}{I(X)}) = \{\langle \overline{x}_1 - a_1, \ldots, \overline{x}_n - a_n \rangle \mid (a_1,\ldots,a_n) \in X\}$, basta mostrar que

$$\operatorname{Specm}(\mathbf{k}[x_1,\ldots,x_n]) = \{\langle x_1 - a_1, \ldots, x_n - a_n \rangle \mid a_i \in \mathbf{k}\}$$

pois como observamos na aula passada: "$\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subseteq \mathbf{k}[x_1,\ldots,x_n]$ corresponde a um ideal de $\mathbf{k}[x_1,\ldots,x_n]/I(X)$ se, e somente se, $(a_1,\ldots,a_n) \in Z(I(X)) = X$". Mas esse resultado é conhecido como **Nullstellensatz**[2] **Hilberts** ou **Teorema dos Zeros de Hilbert.**

Teorema 46. *(***Nullstellensatz Hilberts***) Seja* $\mathbf{k}$ *um corpo algebricamente fechado.*

a. *Todo ideal maximal do anel* $\mathbf{k}[x_1,\ldots,x_n]$ *é da forma* $\mathfrak{m}_P = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ *para algum ponto* $P = (a_1,\ldots,a_n) \in \mathbb{A}^n_{\mathbf{k}}$.

b. *Seja* $J \subsetneq \mathbf{k}[x_1,\ldots,x_n]$ *um ideal próprio então* $Z(J) \neq \emptyset$.

c. *Para qualquer* $J \subseteq \mathbf{k}[x_1,\ldots,x_n]$ *temos* $I(Z(J)) = \sqrt{J}$.

A parte essencial do teorema é o item b. , o qual nos diz que se um ideal J não é o anel todo $\mathbf{k}[x_1,\ldots,x_n]$ então ele tem zeros em $\mathbb{A}^n_{\mathbf{k}}$. Note também que b. é completamente falso se $\mathbf{k}$ não é algebricamente fechado, pois se $f \in \mathbf{k}[x]$ é um polinômio não-constante então ele pode não gerar o anel todo $\mathbf{k}[x]$ como um ideal, mas $Z(f) = \emptyset$ é perfeitamente possível.

Demonstração. Para provar o teorema vamos assumir o seguinte fato que provaremos mas tarde (veja Teorema 190):

Fato: "Seja $\mathbf{k}$ um corpo e $A = \mathbf{k}[a_1,\ldots,a_n]$ um anel finitamente gerado[3] (f.g.) sobre $\mathbf{k}$. Se A é um corpo então A é uma extensão algébrica[4] de $\mathbf{k}$."

2 Satz=Teorema, Nullstellen=dos zeros

3 i.e., existe um número finito de elementos $a_1,\ldots,a_n$ tal que A é gerado como anel por $\mathbf{k}$ e $a_1,\ldots,a_n$. Ou sejam os elementos de A são expressões polinomiais nos a_i's.

4 Uma extensão $A \supseteq \mathbf{k}$ é dita algébrica se para todo elemento $a \in A$ existe um polinômio $f \in \mathbf{k}[x]$ não nulo tal que $f(a) = 0$

a. Seja $\mathfrak{m} \subseteq \mathbf{k}[x_1, \ldots, x_n]$ um ideal maximal, como $\mathbf{k}[x_1, \ldots, x_n]$ é um anel f.g. sobre $\mathbf{k}$ então $K = \mathbf{k}[x_1, \ldots, x_n]/\mathfrak{m}$ é um corpo (pois $\mathfrak{m}$ é maximal) f.g. sobre $\mathbf{k}$ (pois é gerado pelos $\overline{x}_i$'s). Logo segue do "**Fato**" que K é uma extensão algébrica de $\mathbf{k}$, mas $\mathbf{k}$ é algebricamente fechado, logo $\mathbf{k} = K$. Assim, existem $a_i \in \mathbf{k}$ tais que $x_i \equiv a_i \bmod(\mathfrak{m})$ logo $x_i - a_i \in \mathfrak{m}$ para todo $i = 1, \ldots, n$. Ou seja, $\langle x_1 - a_1, \ldots, x_n - a_n \rangle \subseteq \mathfrak{m}$, mas como já vimos $\langle x_1 - a_1, \ldots, x_n - a_n \rangle$ é um ideal maximal (Exercício 9 da Lista 1 para $A = \mathbf{k}$), logo $\langle x_1 - a_1, \ldots, x_n - a_n \rangle = \mathfrak{m}$.

b. Se $J \subsetneq \mathbf{k}[x_1, \ldots, x_n]$ é um ideal próprio então existe um ideal maximal $\mathfrak{m}$ de $\mathbf{k}[x_1, \ldots, x_n]$ tal que $J \subseteq \mathfrak{m}$. Pelo item a. $\mathfrak{m}$ é da forma $\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$ para certos a_i's $\in \mathbf{k}$. Logo $J \subseteq \mathfrak{m}$ implica que $f(a_1, \ldots, a_n) = 0$ para todo $f \in J$. Logo $(a_1, \ldots, a_n) \in Z(J)$.

c. É claro que $\sqrt{J} \subseteq I(Z(J))$: se $f^n \in J \subseteq I(Z(J))$ (pela Proposição 44 b.) então $\overline{f}^n = 0$ em $\mathbf{k}[X] = \frac{\mathbf{k}[x_1, \ldots, x_n]}{I(Z(J))}$ onde $X = Z(J)$. Logo para todo $(a_1, \ldots, a_n) \in X$, $(\overline{f(a_1, \ldots, a_n)})^n = 0 \in \mathbf{k} = \mathbb{A}^1_{\mathbf{k}}$ o que implica que $\overline{f(a_1, \ldots, a_n)} = 0$ (pois $\mathbf{k}$ é um corpo e o único elemento nilpotente é o 0). Assim $\overline{f} = 0$ em $\mathbf{k}[X]$ (como morfismo que leva todos os elementos do domínio em 0), ou seja $f \in I(X)$.

   Para ver $I(Z(J)) \subseteq \sqrt{J}$ tome $f \in I(Z(J))$. Introduza uma outra variável y e considere o novo ideal $J_1 = \langle J, f \cdot y - 1 \rangle \subseteq \mathbf{k}[x_1, \ldots, x_n, y]$ gerado por J e $f \cdot y - 1$. Um ponto $Q \in Z(J_1) \subseteq \mathbb{A}^{n+1}_{\mathbf{k}}$ é uma $(n+1)$-tupla $Q = (a_1, \ldots, a_n, b)$ tal que $g(a_1, \ldots, a_n) = 0$ para toda $g \in J$, i.e., $(a_1, \ldots, a_n) \in Z(J)$ e $f(a_1, \ldots, a_n) \cdot b = 1$, ou seja $f(a_1, \ldots, a_n) \neq 0$ e $b = f(a_1, \ldots, a_n)^{-1}$.

   Mas como $f \in I(Z(J))$, a primeira condição acima implica que $f(a_1, \ldots, a_n) = 0$ o que contradiz a segunda, então $Z(J_1) = \emptyset$. Segue do item b. que $1 \in J_1$, i.e., existe uma expressão

$$1 = \sum g_i f_i + g_0(f \cdot y - 1) \in \mathbf{k}[x_1, \ldots, x_n, y]$$

   com $f_i \in J$ e $g_0, g_i \in \mathbf{k}[x_1, \ldots, x_n, y]$. Agora suponha que y^N é a maior potência de y aparecendo em qualquer um dos g_0, g_i então multiplicando ambos lados por f^N temos

$$f^N = \sum G_i(x_1, \ldots, x_n, f \cdot y) f_i + G_0(x_1, \ldots, x_n, f \cdot y)(f \cdot y - 1)$$

onde G_i é $f^N g_i$ escrito como um polinômio em $x_1, \ldots, x_n$ e $(f \cdot y)$, da seguinte forma:

$$\begin{aligned} G_i(x_1, \ldots, x_n, f \cdot y) &= f^N g_i(x_1, \ldots, x_n, y) \\ &= f^N \sum_{(\alpha_1, \ldots, \alpha_n, j)} p^i_{\alpha_1 \ldots \alpha_n j} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \cdot y^j \\ &= \sum_{(\alpha_1, \ldots, \alpha_n, j)} p^i_{\alpha_1 \ldots \alpha_n j} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \cdot f^{N-j} \cdot (f \cdot y)^j \end{aligned}$$

Podemos reduzir esta igualdade de polinômios em $\mathbf{k}[x_1, \ldots, x_n, y]$ módulo $\langle f \cdot y - 1 \rangle$, logo $\overline{f \cdot y} = \overline{1}$ assim $\overline{G_i}(x_1, \ldots, x_n, f \cdot y) = \overline{h_i}(x_1, \ldots, x_n)$ e obtemos

$$\overline{f}^N = \sum \overline{h}_i(x_1, \ldots, x_n)\overline{f}_i \in \mathbf{k}[x_1, \ldots, x_n, y] / \langle f \cdot y - 1 \rangle ;$$

ambos os lados da igualdade são imagens de elementos de $\mathbf{k}[x_1, \ldots, x_n]$. Como o homomorfismo canônico $\mathbf{k}[x_1, \ldots, x_n] \hookrightarrow \mathbf{k}[x_1, \ldots, x_n, y] / \langle f \cdot y - 1 \rangle$ é injetivo segue que

$$f^N = \sum h_i(x_1, \ldots, x_n) f_i \in \mathbf{k}[x_1, \ldots, x_n]$$

ou seja $f^N \in J$ pois $f_i \in J$, logo $f \in \sqrt{J}$.

□

Aula 7

AULA 7: 12/09/2014

Como consequência do Teorema dos Zeros de Hilbert temos:

Corolário 47. *As correspondências Z e I dadas por:*

$$\begin{aligned} \{\textit{ideais } J \subseteq \mathbf{k}[x_1, \ldots, x_n]\} &\xrightarrow{Z} \{\textit{subconjuntos } X \subseteq \mathbb{A}^n_{\mathbf{k}}\} \\ J &\mapsto Z(J) \\ \{\textit{ideais } J \subseteq \mathbf{k}[x_1, \ldots, x_n]\} &\xleftarrow{I} \{\textit{subconjuntos } X \subseteq \mathbb{A}^n_{\mathbf{k}}\} \\ I(X) &\hookleftarrow X \end{aligned}$$

induzem as seguintes bijeções:

$$\begin{array}{ccc} \{\textit{ideais radicais } J \subseteq \mathbf{k}[x_1, \ldots, x_n]\} & \xleftrightarrow{Z,I} & \{\textit{conjuntos algébricos } X \subseteq \mathbb{A}^n_{\mathbf{k}}\} \\ \cup & & \cup \\ \{\textit{ideais primos } J \subseteq \mathbf{k}[x_1, \ldots, x_n]\} & \xleftrightarrow{Z,I} & \{\textit{variedades } X \subseteq \mathbb{A}^n_{\mathbf{k}}\} \end{array}$$

A primeira bijeção segue dos fatos $Z(I(X)) = X$ para qualquer conjunto algébrico X (Proposição 44 c.) e $I(Z(J)) = J$ para qualquer ideal radical J (i.e., qualquer ideal J tal que $J = \sqrt{J}$) (Teorema 46 c.). A segunda segue do fato de variedades serem conjuntos algébricos e ideais primos serem radicais (Exercício 17 Lista 1) e da Proposição 45: X é variedade se, e somente se, $I(X)$ é um ideal primo.

A próxima proposição mostra que a topologia de Zariski do espaço afim $\mathbb{A}^n_{\mathbf{k}}$ é na verdade a topologia induzida do subespaço $\mathrm{Specm}(\mathbf{k}[X])$ de $\mathrm{Spec}(\mathbf{k}[X])$ via identificação $X = \mathrm{Specm}(\mathbf{k}[X])$ de um conjunto algébrico com o espectro maximal de seu anel de funções regulares.

Proposição 48. *Seja* $\mathbf{k}$ *um corpo algebricamente fechado, seja* $X \subseteq \mathbb{A}^n_{\mathbf{k}}$ *um conjunto algébrico e seja* $\mathbf{k}[X] = \mathbf{k}[x_1, \ldots, x_n]/I(X)$ *seu anel de funções regulares. Se* $\overline{J} \subseteq \mathbf{k}[X]$ *é um ideal qualquer de* $\mathbf{k}[X]$ *com ideal correspondente* $J \subseteq \mathbf{k}[x_1, \ldots, x_n]$ *no anel de polinômios, temos*

$$Z(J) \cap X = V(\overline{J}) \cap \mathrm{Specm}(\mathbf{k}[X])$$

via identificação $X = \mathrm{Specm}(\mathbf{k}[X])$ *dada por* $P \mapsto \overline{\mathfrak{m}}_P$. *Assim, a topologia de subespaço de* $\mathrm{Specm}(\mathbf{k}[X]) \subseteq \mathrm{Spec}(\mathbf{k}[X])$ *coincide com a topologia de Zariski de* X *como conjunto algébrico.*

Demonstração. Seja $P = (a_1, \ldots, a_n) \in X$, temos que o ideal maximal correspondente é $\overline{\mathfrak{m}}_P = \langle \overline{x}_1 - a_1, \ldots, \overline{x}_n - a_n \rangle \subseteq \mathbf{k}[X]$ e portanto

$$\begin{aligned} \overline{\mathfrak{m}}_P \in V(\overline{J}) &\Leftrightarrow \overline{\mathfrak{m}}_P \supseteq \overline{J} \text{ em } \mathbf{k}[X] = \mathbf{k}[x_1, \ldots, x_n]/I(X) \\ &\Leftrightarrow \langle x_1 - a_1, \ldots, x_n - a_n \rangle \supseteq J \text{ em } \mathbf{k}[x_1, \ldots, x_n] \\ &\Leftrightarrow P = (a_1, \ldots, a_n) \in Z(J) \end{aligned}$$

□

2.3 EXERCÍCIOS

Ex. 21 — Mostre que todo anel A possui um ideal primo minimal, ou seja, um ideal primo p tal que se $q \in \mathrm{Spec}(A)$ e $q \subseteq p \Longrightarrow q = p$. Quais são os primos minimais de $\dfrac{\mathbb{C}[x,y]}{(x^2 - y^2)}$?

Ex. 22 — Seja A um anel. Para um subconjunto $S \subseteq A$, defina

$$V(S) := \{p \in \mathrm{Spec}(A) \mid p \supseteq S\}$$

como o conjunto de todos os ideais primos de A que contêm S. Prove que $V(S) = V(I) = V(\sqrt{I})$, onde I representa o ideal gerado por S em A.

Ex. 23 — Seja A um anel. Para $a \in A$, defina o conjunto $D(a) := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid a \notin \mathfrak{p}\}$. Mostre que os conjuntos $D(a)$ com $a \in A$ são abertos e formam uma base para a topologia de Zariski de $\mathrm{Spec}(A)$. Além disso, dados $a, b \in A$ mostre que:

1. $D(a) \cap D(b) = D(a \cdot b)$.
2. $D(a) = \emptyset \iff a$ é nilpotente.
3. $D(a) = \mathrm{Spec}(A) \iff a$ é unidade.
4. $D(a) = D(b) \iff \sqrt{\langle a \rangle} = \sqrt{\langle b \rangle}$.

Ex. 24 — Seja A um anel e $I \subseteq A$ um ideal qualquer. Prove que o morfismo entre espectros

$$\mathrm{Spec}(\pi) : \mathrm{Spec}(A/I) \to V(I) \subseteq \mathrm{Spec}(A)$$

induzido pela projeção canônica $\pi : A \to A/I$ é um homeomorfismo.

Ex. 25 — Um espaço topológico X é dito irredutível se $X \neq \emptyset$ e se todo par de conjuntos abertos não vazios em X se interceptam, ou equivalentemente, todo aberto não vazio é denso em X. Mostre que $\mathrm{Spec}(A)$ é irredutível se e somente se o nilradical de A, $\mathfrak{N}(A)$, é um ideal primo.

Ex. 26 — Sejam A e B dois anéis. Mostre que:

1. $A \times B$ é um domínio se e somente se $A = 0$ e B é um domínio ou $B = 0$ e A é um domínio.
2. Os ideais de $A \times B$ são da forma $I \times J$ onde I é um ideal de A e J é um ideal de B.
3. $\mathrm{Spec}(A \times B) = \mathrm{Spec}(A) \bigsqcup \mathrm{Spec}(B)$.

Ex. 27 — Mostre que

1. Se A é um Domínio de Fatoração Única (DFU), então um ideal principal (a) não nulo é primo se, e somente se, a é irredutível.
2. Todo Domínio de Ideais Principais (DIP) é DFU.
3. Conclua que $\mathrm{Spec}(\mathrm{DIP}) = \{(0)\} \cup \{(a) \mid a \text{ é irredutível}\}$.

Ex. 28 — Mostre que os conjuntos algébricos são os fechados de uma topologia de $\mathbb{A}^n_{\mathbf{k}}$ (Topologia de Zariski), i.e., têm as seguintes propriedades:

1. $Z((0)) = \mathbb{A}^n_{\mathbf{k}}$ e $Z(\mathbf{k}[x_1, \ldots, x_n]) = \emptyset$

2. $Z(I) \cup Z(J) = Z(I \cdot J)$
3. $\bigcap_{i \in \Lambda} Z(I_i) = Z(\sum_{i \in \Lambda} I_i)$.

Ex. 29 — Seja $\mathbf{k}$ um corpo infinito e $f \in \mathbf{k}[x_1, \ldots, x_n]$. Mostre que se $f(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbf{k}}$ então $f = 0$. Encontre um contraexemplo no caso em que $\mathbf{k}$ é um corpo finito.

Ex. 30 — Seja $\mathbf{k}$ um corpo algebricamente fechado, $f \in \mathbf{k}[x_1, \ldots, x_n]$. Prove que o conjunto algébrico $Z(f) \subseteq \mathbb{A}^n_{\mathbf{k}}$ é uma variedade se, e somente se, existe um polinômio irredutível $g \in \mathbf{k}[x_1, \ldots, x_n]$ tal que $f = g^n$ para algum $n > 0$.

Ex. 31 — Para cada um dois anéis A a seguir determine o grupo das unidades de A, $\mathrm{Spec}(A)$, ideais maximais e os abertos e fechados do $\mathrm{Spec}(A)$.

1. $\mathbb{Z}$
2. $\mathbb{Z}/3\mathbb{Z}$
3. $\mathbb{Z}/6\mathbb{Z}$
4. $\mathbb{C}[x]$
5. $\mathbb{C}[x]/\langle x^{13} \rangle$
6. $\mathbb{R}[x]/\langle x^2 + 1 \rangle$
7. $\mathbb{C}[[x]]/\langle x^2 + 1 \rangle$
8. $\mathbb{Z}[x]/\langle x^2 + 1 \rangle$
9. $\mathbb{C}[x, y]/\langle x^2 + y^2 + 1 \rangle$
10. $\mathbb{R}[x, y]/\langle x^2 + y^2 + 1 \rangle$

3

MÓDULOS

Definição 49. Seja A um anel. Um A**-módulo** é um par (M, μ) onde M é um grupo abeliano e $\mu : A \times M \to M$ é uma aplicação que leva $(a, m) \mapsto am$ e satisfaz:

$$\begin{aligned} a(m+n) &= am + an \\ (a+b)m &= am + bm \\ (ab)m &= a(bm) \\ 1m &= m \end{aligned}$$

para todo $a, b \in A$ e $m, n \in M$.

Ou, equivalentemente, M é um grupo abeliano juntamente com um homomorfismo de anéis $A \to \mathrm{End}(M)$ onde $\mathrm{End}(M)$ é o anel dos endomorfismos do grupo abeliano M.

Exemplo 50.

a. Um ideal I de A é um A-módulo. Em particular, A é um A-módulo.

b. Se $A = \mathbf{k}$ é um corpo, então um A-módulo é um $\mathbf{k}$-espaço vetorial.

c. Se $A = \mathbb{Z}$ então um A-módulo é um grupo abeliano, onde definimos $nm = \underbrace{m + \cdots + m}_{n \text{ vezes}}$.

d. Se $A = \mathbf{k}[x]$ onde $\mathbf{k}$ é um corpo, então um A-módulo é um $\mathbf{k}$-espaço vetorial com uma transformação linear.

Sejam M e N dois A-módulos. Uma aplicação $f : M \to N$ é um **homomorfismo** de A-módulos (ou um A**-homomorfismo**) se

$$\begin{aligned} f(m_1 + m_2) &= f(m_1) + f(m_2) \\ f(am_1) &= af(m_1) \end{aligned}$$

para todo $a \in A$ e $m_1, m_2 \in M$. Ou seja, f é um homomorfismo de grupos abelianos que comuta com a ação de cada $a \in A$.

O conjunto de todos os homomorfismos de A-módulos de M em N pode ser visto como um A-módulo se definimos soma e produto pelas regras

$$\begin{aligned} (f+g)(m) &= f(m) + g(m) \\ (af)(m) &= af(m) \end{aligned}$$

para todo $m \in M$. Denotamos este A-módulo por $\mathrm{Hom}_A(M, N)$.

Sejam $u : M' \to M$ e $v : N \to N''$ dois homomorfismos de A-módulos, então eles induzem aplicações

$$\overline{u} : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M', N) \text{ e } \overline{v} : \mathrm{Hom}_A(M, N) \to \mathrm{Hom}_A(M, N'')$$

definidas como $\overline{u}(f) = f \circ u$ e $\overline{v}(f) = v \circ f$. Estas aplicações são também homomorfismos de A-módulos.

Para todo módulo M existe um isomorfismo natural $\mathrm{Hom}_A(A, M) \simeq M$ pois todo homomorfismo de A-módulos $f : A \to M$ é determinado de maneira única por $f(1) \in M$.

Definição 51. Um **submódulo** M' de M é um subgrupo de M que é fechado em relação à multiplicação por elementos de A.

O grupo abeliano M/M' herda uma estrutura de A-módulo de M, definida por $a(m + M') = am + M'$. Logo M/M' é o A-módulo **quociente** de M por M'.

O TCI é um caso particular do seguinte fato: a projeção canônica $M \to M/M'$ é um homomorfismo de A-módulos que induz uma correspondência um-a-um (que preserva ordem) entre submódulos de M que contém M' e submódulos de M/M'.

Se $f : M \to N$ é um homomorfismo de A-módulos, então o $\mathrm{Ker}(f)$ é um submódulo de M e a $\mathrm{Im}(f)$ é um submódulo de N. Denotamos o **cokernel** de f como sendo $\mathrm{Coker}(f) = N/\mathrm{Im}(f)$.

Se $M' \subseteq M$ é um submódulo de M tal que $M' \subseteq \mathrm{Ker}(f)$ então f induz um homomorfismo $\overline{f} : M/M' \to N$ definido como segue: se $\overline{m} \in M/M'$ é imagem de $m \in M$ então $\overline{f}(\overline{m}) = f(m)$. O $\mathrm{Ker}(\overline{f}) = \mathrm{Ker}(f)/M'$, em particular tomando $M' = \mathrm{Ker}(f)$ temos um isomorfismo de A-módulos

$$\frac{M}{\mathrm{Ker}(f)} \simeq \mathrm{Im}(f).$$

Definição 52. Seja M um A-módulo e $(M_i)_{i \in I}$ uma família de submódulos de M. Definimos

a. A **soma** $\sum M_i$ como sendo o conjunto de todas as somas (finitas) Σm_i, onde $m_i \in M_i$ para todo $i \in I$ e quase todos (i.e., todos exceto um número finito) os m_i são zero. A soma $\sum M_i$ é o menor submódulo de M que contém todos os M_i.

b. A **interseção** $\bigcap M_i$ é um submódulo de M.

c. Em geral não podemos definir o produto de dois submódulos, mas podemos definir o **produto** IM onde I é um ideal e M um A-módulo, como sendo o conjunto de todas as somas finitas $\Sigma a_i m_i$ com $a_i \in I$ e $m_i \in M_i$. O produto IM é um submódulo de M.

Proposição 53.

a. Se $L \supseteq M \supseteq N$ são A-módulos, então $(L/N)/(M/N) \simeq L/M$.

b. Se M_1 e M_2 são submódulos de M, então

$$\frac{(M_1 + M_2)}{M_1} \simeq \frac{M_2}{(M_1 \cap M_2)}.$$

Demonstração. **Exercício 1.** □

Se N, P são submódulos de M definimos $(N : P)$ como sendo o conjunto de todos os $a \in A$ tais que $aP \subseteq N$, logo $(N : P)$ é um ideal de A. Em particular, $(0 : M)$ é o conjunto de todos os $a \in A$ tais que $aM = 0$, este ideal é chamado **aniquilador** de M e é denotado por $\mathrm{Ann}(M)$. Se $I \subseteq \mathrm{Ann}(M)$ podemos considerar M como um (A/I)-módulo: se $\overline{a} \in A/I$ é representado por $a \in A$, defina $\overline{a}m$ como sendo am, $m \in M$. Observe que esta definição é independente da escolha do representante a de $\overline{a}$ pois $IM = 0$.

Definição 54. Um A-módulo M é dito **fiel** se $\mathrm{Ann}(M) = 0$.

Segue da definição que todo módulo M é fiel como um $\frac{A}{\mathrm{Ann}(M)}$-módulo.

Se m é um elemento de M, o conjunto de todos os múltiplos am, com $a \in A$, é um submódulo de M, denotado por Am ou $\langle m \rangle$. Se um módulo $M = \sum_{i \in I} Am_i$ dizemos que os m_i's formam um **conjunto de geradores** de M, isto significa que todo elemento de M pode ser expresso (não necessariamente de maneira única) como uma combinação linear finita dos m_i's com coeficientes em A. Um A-módulo é dito **finitamente gerado** (f.g.) se ele tem um conjunto finito de geradores.

Definição 55. Se $(M_i)_{i \in I}$ é uma família de A-módulos, definimos:

a. A **soma direta** $\bigoplus_{i \in I} M_i$ como sendo o conjunto das famílias $(m_i)_{i \in I}$ tais que $m_i \in M_i$ para cada $i \in I$ e quase todos os m_i's são zero.

b. O **produto direto** $\prod_{i \in I} M_i$ como sendo o conjunto das famílias $(m_i)_{i \in I}$ tais que $m_i \in M_i$ para cada $i \in I$ (aqui descartamos a restrição dos m_i's serem quase todos zero).

3.1 MÓDULOS FINITAMENTE GERADOS

Definição 56. Um A-módulo **livre** é um A-módulo isomorfo a $\bigoplus_{i \in I} M_i$ onde cada $M_i \simeq A$ como um A-módulo. Um A-módulo **livre f.g.** é isomorfo a $A^n = \underbrace{A \oplus \cdots \oplus A}_{n \text{ vezes}}$, para algum $n > 0$.

Proposição 57. *M é um A-módulo f.g. se, e somente se, M é isomorfo a um quociente de A^n para algum inteiro $n > 0$.*

Demonstração. ($\Rightarrow$) Sejam $m_1, \ldots, m_n$ os geradores de M. Defina $f : A^n \to M$ por $f(a_1, \ldots, a_n) = a_1 m_1 + \cdots + a_n m_n$. Então f é um homomorfismo de A-módulos sobrejetor e logo $M = A^n / \operatorname{Ker}(f)$.

($\Leftarrow$) Temos que $A^n/N \overset{\varphi}{\simeq} M$ para algum A-módulo N, logo existe um homomorfismo de A-módulos sobrejetor $f : A^n \to M$ onde $f = \pi \circ \varphi$ com $\pi : A^n \to A^n/N$ a projeção canônica. Se $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$ (com 1 na i-ésima posição) então e_i ($1 \leq i \leq n$) geram A^n, ou seja $A^n = Ae_1 + \cdots + Ae_n$. Como f é sobre então $f(A^n) = M = Af(e_1) + \cdots + Af(e_n)$ e logo $f(e_i)$ geram M. □

O nosso objetivo agora é provar uma versão do Lema de Nakayama, para isso precisaremos dos seguintes resultados:

Proposição 58. *Seja M um A-módulo f.g., I um ideal de A e f um endomorfismo do A-módulo M tal que $f(M) \subseteq IM$. Então f satisfaz uma equação da forma $f^n + a_1 f^{n-1} + \cdots + a_n \operatorname{id} = 0$ onde $a_i \in I$.*

Demonstração. Seja $m_1, \ldots, m_n$ o conjunto de geradores de M. Então cada $f(m_i) \in IM$ logo $f(m_i) = \sum_{j=1}^{n} a_{ij} m_j$ com $1 \leq i \leq n$ e $a_{ij} \in I$, i.e.,

$$\sum_{j=1}^{n} (\delta_{ij} f - a_{ij} \operatorname{id}) m_j = 0 \tag{2}$$

onde δ_{ij} é o delta de Kronecker. Seja B a matriz $(\delta_{ij} f - a_{ij} \operatorname{id})_{ij}$ então

$$B = \begin{bmatrix} f - a_{11}\operatorname{id} & -a_{12}\operatorname{id} & \cdots & -a_{1n}\operatorname{id} \\ -a_{21}\operatorname{id} & f - a_{22}\operatorname{id} & \cdots & -a_{2n}\operatorname{id} \\ \vdots & \vdots & \vdots & \vdots \\ -a_{n1}\operatorname{id} & -a_{n2}\operatorname{id} & \cdots & f - a_{nn}\operatorname{id} \end{bmatrix}$$

Multiplicando o lado esquerdo de (2) pela adjunta de B segue que $B \cdot \operatorname{Adj}(B) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$, mas $B \cdot \operatorname{Adj}(B) = \det(B) \cdots I_n$ isto implica que $\det(B)$ anula cada m_i, logo é o endomorfismo nulo de M. Expandindo o determinante, obtemos uma equação da forma requerida. □

Corolário 59. *Seja M um A-módulo f.g. e seja I um ideal de A tal que $IM = M$. Então existe $a \equiv 1 \bmod I$, $a \in A$, tal que $aM = 0$.*

Demonstração. Considere $f = \mathrm{id}$, então $\mathrm{id}(M) \subseteq IM$ por hipótese. Pela proposição anterior existem $a_1, \ldots, a_n \in I$ tais que $\mathrm{id} + a_1\,\mathrm{id} + \cdots + a_n\,\mathrm{id} = 0$. Seja $a = 1 + a_1 + \cdots + a_n \in A$, claramente $a \equiv 1 \bmod I$ e se $m \in M$ temos

$$am = (1 + a_1 + \cdots + a_n)m = m + a_1 m + \cdots + a_n m = (\mathrm{id} + a_1\,\mathrm{id} + \cdots + a_n\,\mathrm{id})m = 0$$

□

Aula 8

aula 8: 17/09/2014

Lembrando a última aula. Queremos provar uma versão do Lema de Nakayama, para isso precisaremos dos seguintes resultados da última aula:

a. **Proposição.** Seja M um A-módulo f.g., I um ideal de A e f um endomorfismo do A-módulo M tal que $f(M) \subseteq IM$. Então f satisfaz uma equação da forma $f^n + a_1 f^{n-1} + \cdots + a_n\,\mathrm{id} = 0$ onde $a_i \in I$.

b. **Corolário.** Seja M um A-módulo f.g. e seja I um ideal de A tal que $IM = M$. Então existe $a \equiv 1 \bmod I$, $a \in A$, tal que $aM = 0$.

E de alguns resultados das primeiras aulas como a definição do **radical de Jacobson** $\mathfrak{R}$ de um anel A: que é a interseção de todos os ideais maximais de A. E da Proposição 26 que o caracteriza:

Proposição. *$r \in \mathfrak{R}$ se e somente se $1 - r \cdot a$ é uma unidade de A para todo $a \in A$.*

Agora sim, estamos prontos para enunciar o

Lema 60. (Lema de Nakayama) *Seja M um A-módulo f.g. e I um ideal de A contido no radical de Jacobson $\mathfrak{R}$ de A. Se $IM = M$ então $M = 0$.*

Demonstração. Pelo Corolário 59 existe um elemento $a \in A$ tal que $a \equiv 1 \bmod I$, ou seja $a = 1 + r$ para algum $r \in I \subseteq \mathfrak{R}$ e a é tal que $aM = 0$. Pela Proposição 26 a é uma unidade de A, logo $M = (a^{-1}a)M = a^{-1}(aM) = 0$.

□

Como consequência do Lema de Nakayama temos:

Corolário 61. *Seja M um A-módulo f.g., N um submódulo de M, $I \subseteq \mathfrak{R}$ um ideal de A. Se $M = IM + N$ então $M = N$.*

Demonstração. Como M é f.g. então M/N também é f.g com conjunto de geradores as imagens dos geradores de M. Sabemos que $I(\frac{M}{N}) \subseteq \frac{M}{N}$ é um submódulo, queremos ver que $\frac{M}{N} \subseteq I(\frac{M}{N})$. Seja $\overline{m} \in \frac{M}{N}$, como $M = IM + N$ por hipótese, temos que $\overline{m} = \overline{\Sigma a_i m_i + n}$ logo $m - \Sigma a_i m_i - n \in N$ o que implica $m - \Sigma a_i m_i \in N$, assim $\overline{m} = \overline{\Sigma a_i m_i} = \Sigma \overline{a_i m_i} = \Sigma a_i \overline{m}_i \in I(\frac{M}{N})$ onde a última igualdade deve-se à definição de ação do módulo quociente. Segue que $I(\frac{M}{N}) = \frac{M}{N}$ e logo, pelo Lema de Nakayama (Lema 60), aplicado a $\frac{M}{N}$ temos que $\frac{M}{N} = 0$ ou seja $M = N$. □

Seja A um anel local (i.e., um anel com um único ideal maximal), $\mathfrak{m}$ seu ideal maximal e $\mathbf{k} = A/\mathfrak{m}$ seu corpo de resíduos. Seja M um A-módulo f.g., então $M/\mathfrak{m}M$ é aniquilado por $\mathfrak{m}$, logo é um $A/\mathfrak{m}$-módulo, ou seja um $\mathbf{k}$-espaço vetorial e como tal tem dimensão finita.

Proposição 62. *Sejam m_i ($1 \leq i \leq n$) os elementos de M cujas imagens em $M/\mathfrak{m}M$ formam uma base deste espaço vetorial. Então m_i geram M.*

Demonstração. Seja N o submódulo de M gerado pelos m_i e seja $f : N \subseteq M \to \frac{M}{\mathfrak{m}M}$ o homomorfismo de A-módulos dado por $n \mapsto \overline{n}$. Vejamos que f é sobrejetor: seja $\overline{m} \in \frac{M}{\mathfrak{m}M}$, como $\frac{M}{\mathfrak{m}M}$ é um $\mathbf{k}$-espaço vetorial com base $\{\overline{m}_1, \ldots, \overline{m}_n\}$ temos que existem $k_1, \ldots, k_n \in \mathbf{k}$ tais que $\overline{m} = k_1\overline{m}_1 + \cdots + k_n\overline{m}_n$. Sejam agora $a_i \in A$ representantes das classes $k_i \in A/\mathfrak{m}$ para $i = 1, \ldots, n$ então $\overline{m} = \overline{a}_1\overline{m}_1 + \cdots + \overline{a}_n\overline{m}_n$. Pela definição da ação de $A/\mathfrak{m}$ em $\frac{M}{\mathfrak{m}M}$ temos que $\overline{a}_i\overline{m}_i = a_i\overline{m}_i$ e pela ação de A em $\frac{M}{\mathfrak{m}M}$ temos $a_i\overline{m}_i = \overline{a_i m_i}$ logo $\overline{m} = \overline{a_1m_1 + \cdots + a_nm_n}$, assim existe $a_1m_1 + \cdots + a_nm_n \in N$ tal que $f(a_1m_1 + \cdots + a_nm_n) = \overline{m}$. Por outro lado, $n \in \mathrm{Ker}(f) \Leftrightarrow n \in N$ e $\overline{n} = \overline{0} \Leftrightarrow n \in N$ e $n \in \mathfrak{m}M$ logo $\mathrm{Ker}(f) = N \cap \mathfrak{m}M$. Segue do Teorema de Isomorfismos que $\frac{N}{N\cap\mathfrak{m}M} \simeq \frac{M}{\mathfrak{m}M}$ e da Proposição 53 temos que $\frac{N}{N\cap\mathfrak{m}M} \simeq \frac{\mathfrak{m}M+N}{\mathfrak{m}M}$, agora como $M \supseteq \mathfrak{m}M + N \supseteq \mathfrak{m}M$ segue também da Proposição 53 que

$$\frac{\frac{M}{\mathfrak{m}M}}{\frac{\mathfrak{m}M+N}{\mathfrak{m}M}} \simeq \frac{M}{\mathfrak{m}M + N'}$$

mas $\frac{M}{\mathfrak{m}M} \simeq \frac{\mathfrak{m}M+N}{\mathfrak{m}M}$ logo $\frac{M}{\mathfrak{m}M+N} = 0$ e $\mathfrak{m}M + N = M$. Aplicando o Corolário anterior a M e N com $I = \mathfrak{m}$ (o único ideal maximal de A) então $I \subseteq \mathfrak{R}$ (interseção de todos os ideais maximais de A) logo $M = N$. □

3.2 SEQUÊNCIAS EXATAS

Definição 63. Uma sequência de A-módulos e A-homomorfismos

$$\cdots \longrightarrow M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \longrightarrow \cdots \tag{3}$$

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

Em particular:

a. $0 \to M' \xrightarrow{f} M$ é exata $\Leftrightarrow$ f é injetiva;

b. $M \xrightarrow{g} M'' \to 0$ é exata $\Leftrightarrow$ g é sobrejetiva;

c. $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ é exata $\Leftrightarrow$ f é injetiva, g é sobrejetiva e $\mathrm{Im}(f) = \mathrm{Ker}(g)$.

Uma sequência do tipo c. é chamada de **sequência exata curta**. Toda sequência exata longa do tipo (3) pode ser dividida em sequências exatas curtas: se $N_i = \mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$ temos $0 \to N_i \overset{\text{incl}}{\hookrightarrow} M_i \overset{f_{i+1}}{\twoheadrightarrow} N_{i+1} \to 0$ para cada i.

Proposição 64.

a. Seja $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ uma sequência de A-módulos e A-homomorfismos. Então essa sequência é exata se, e somente se, para todo A-módulo N a sequência $0 \to \mathrm{Hom}_A(M'', N) \xrightarrow{\overline{v}} \mathrm{Hom}_A(M, N) \xrightarrow{\overline{u}} \mathrm{Hom}_A(M', N)$ é exata.

b. Seja $0 \to N' \xrightarrow{u} N \xrightarrow{v} N''$ uma sequência de A-módulos e A-homomorfismos. Então essa sequência é exata se, e somente se, para todo A-módulo M a sequência $0 \to \mathrm{Hom}_A(M, N') \xrightarrow{\overline{u}} \mathrm{Hom}_A(M, N) \xrightarrow{\overline{v}} \mathrm{Hom}_A(M, N'')$ é exata.

Demonstração.

a. ($\Rightarrow$) Suponha que $M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$ é uma sequência exata, queremos provar que $\overline{v}$ é injetiva e $\mathrm{Im}(\overline{v}) = \mathrm{Ker}(\overline{u})$.

   a) $\overline{v}$ é injetiva: Seja $f \in \mathrm{Ker}(\overline{v})$ então $0 = \overline{v}(f) = f \circ v : M \to N$ ou seja $f(v(M)) = 0$, mas v é sobre logo $v(M) = M''$ assim $f = 0$.

   b) $\mathrm{Im}(\overline{v}) \subseteq \mathrm{Ker}(\overline{u})$: Seja $f \in \mathrm{Im}(\overline{v})$, então existe $g : M'' \to N$ tal que $f = \overline{v}(g) = g \circ v$. Por outro lado $\overline{u}(f) = f \circ u = g \circ v \circ u$, mas $\mathrm{Im}(u) = \mathrm{Ker}(v)$ o que implica $v \circ u = 0$ logo $\overline{u}(f) = 0$ e por tanto $f \in \mathrm{Ker}(\overline{u})$.

   c) $\mathrm{Im}(\overline{v}) \supseteq \mathrm{Ker}(\overline{u})$: Seja $g \in \mathrm{Ker}(\overline{u})$, então $\overline{u}(g) = g \circ u = 0$. Queremos provar que existe $f : M'' \to N$ tal que $g = \overline{v}(f) = f \circ v$. Dado $m'' \in M''$ como v é sobre existe $m \in M$ tal que $m'' = v(m)$, defina então $f(m'') := g(m)$. Vejamos que f está bem definida. Suponha que existam $m_1, m_2 \in M$ tais que $m'' = v(m_1) = v(m_2)$, logo $m_1 - m_2 \in \mathrm{Ker}(v) = \mathrm{Im}(u)$ então existe $m' \in M'$ tal que $u(m') = m_1 - m_2$, aplicando g a ambos lados temos $0 = g \circ u(m') = g(m_1) - g(m_2)$ logo $g(m_1) = g(m_2)$. Vejamos agora que $f \in \mathrm{Hom}_A(M'', N)$: sejam $m_1'', m_2'' \in M''$ então existem $m_1, m_2 \in M$ tais que $m_i'' = v(m_i)$ o que implica que $m_1'' + m_2'' = v(m_1) + v(m_2) = v(m_1 + m_2)$ logo

$$f(m_1'' + m_2'') = g(m_1 + m_2) = g(m_1) + g(m_2) = f(m_1'') + f(m_2'').$$

Por outro lado, se $a \in A$ então $am_1'' = av(m_1) = v(am_1)$ logo

$$f(am_1'') = g(am_1) = ag(m_1) = af(m_1'').$$

($\Leftarrow$)Suponha que $0 \to \mathrm{Hom}_A(M'', N) \xrightarrow{\overline{v}} \mathrm{Hom}_A(M, N) \xrightarrow{\overline{u}} \mathrm{Hom}_A(M', N)$ é uma sequência exata para todo A-módulo N. Queremos provar que v é sobre e $\mathrm{Im}(u) = \mathrm{Ker}(v)$.

a) v é sobre: ($f : X \to Y$ é sobre $\Leftrightarrow g_1 \circ f = g_2 \circ f$ para aplicações $g_1, g_2 : Y \to Z$ implica $g_1 = g_2$). Suponha que existem homomorfismos $g_1, g_2 : M'' \to N$ tais que $g_1 \circ v = g_2 \circ v$, i.e., $\overline{v}(g_1) = \overline{v}(g_2)$ como $\overline{v}$ é injetiva então $g_1 = g_2$ e v é sobre.

b) $\mathrm{Im}(u) \subseteq \mathrm{Ker}(v)$: Temos que $\overline{u} \circ \overline{v} = 0$, i.e., $f \circ v \circ u = 0$ para todo $f : M'' \to N$. Tomando $N = M''$ e $f = \mathrm{id}$ segue que $v \circ u = 0$ e logo $\mathrm{Im}(u) \subseteq \mathrm{Ker}(v)$.

c) $\mathrm{Im}(u) \supseteq \mathrm{Ker}(v)$: Seja $N = \frac{M}{\mathrm{Im}(u)}$ e $\pi : M \to N$ a projeção canônica. Então $\overline{u}(\pi)(m') = \pi \circ u(m') = u(m') + \mathrm{Im}(u) = 0$ para todo $m' \in M'$ então $\pi \in \mathrm{Ker}(\overline{u}) = \mathrm{Im}(\overline{v})$, logo existe $f : M'' \to N$ tal que $\pi = \overline{v}(f) = f \circ v$. Consequentemente, $\mathrm{Ker}(v) \subseteq \mathrm{Ker}(\pi) = \mathrm{Im}(u)$.

b. **Exercício 2.**

□

3.3 PRODUTO TENSORIAL DE MÓDULOS

Sejam M, N, P três A-módulos. Uma aplicação $f : M \times N \to P$ é chamada A**-bilinear** se ela satisfaz:

a. $f(m + m', n) = f(m, n) + f(m', n)$

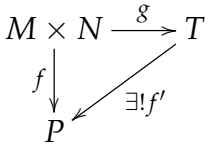
b. $f(m, n + n') = f(m, n) + f(m, n')$

c. $f(am, n) = f(m, an) = af(m, n)$

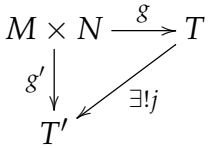
para todo $m, m' \in M$, $n, n' \in N$ e $a \in A$.

Proposição 65. *Sejam M e N dois A-módulos. Então existe um A-módulo T junto com uma aplicação A-bilinear $g : M \times N \to T$ com a seguinte propriedade: dados um A-módulo P e uma aplicação A-bilinear $f : M \times N \to P$, existe uma única aplicação A-linear $f' : T \to P$ tal que $f = f' \circ g$.*

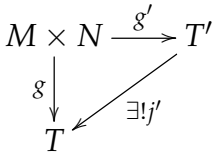
Alem disso, se (T, g) e (T', g') são dois pares que satisfazem essa propriedade, então existe um único isomorfismo $j : T \to T'$ tal que $j \circ g = g'$.



Demonstração. Unicidade. Substituindo (P, f) por (T', g') temos que existe uma única $j : T \to T'$ tal que $g' = j \circ g$.



Intercambiando os papéis de T e T' temos que existe um único $j' : T' \to T$ tal que $g = j' \circ g'$.



Logo $g' = j \circ j' \circ g'$ e $g = j' \circ j \circ g$, assim as composições $j \circ j' : T' \to T'$ e $j' \circ j : T \to T$ devem ser a identidade, logo j é um isomorfismo.

Existência. Denote por C o A-módulo livre $A^{|M \times N|}$cujos elementos são combinações lineares formais de elementos de $M \times N$ com coeficientes em A, i.e., são expressões da forma $\sum_{(m_i,n_i) \in M \times N} a_i(m_i, n_i)$ com $a_i \in A$, $m_i \in M$ e $n_i \in N$. Seja D o submódulo de C gerado por todos os elementos de C do seguinte tipo

$$\begin{aligned}
&(m + m', n) - (m, n) - (m', n)\\
&(m, n + n') - (m, n) - (m, n')\\
&(am, n) - a(m, n)\\
&(m, an) - a(m, n).
\end{aligned}$$

Seja $T = C/D$. Para cada elemento base (m, n) de C, denote por $m \otimes n$ sua imagem em T. Então T é gerado pelos elementos da forma $m \otimes n$. Estes elementos satisfazem

$$\begin{aligned}
&(m + m') \otimes n = m \otimes n + m' \otimes n \qquad m \otimes (n + n') = m \otimes n + m \otimes n'\\
&(am) \otimes n = m \otimes (an) = a(m \otimes n).
\end{aligned}$$

Equivalentemente, a aplicação $g : M \times N \to T$ definida por $g(m,n) = m \otimes n$ é A-bilinear.

Queremos ver que (T, g) satisfazem as condições da proposição. Observe que qualquer aplicação f de $M \times N$ em um A-módulo P estende-se por linearidade a um homomorfismo de A-módulos $\overline{f} : C \to P$. Suponha em particular que f é A-bilinear então, segue das definições, que $\overline{f}$ anula-se em todos os geradores de D e, logo, em todo D ou seja $D \subseteq \mathrm{Ker}(\overline{f})$. Portanto, $\overline{f}$ induz um A-homomorfismo bem definido $f' : T = C/D \to P$ tal que $f'(m \otimes n) = \overline{f}(m,n) = f(m,n)$. A aplicação f' é definida de maneira única por esta condição, e logo o par (T, g) satisfaz as condições da proposição. □

O módulo T construído na proposição anterior é chamado de **produto tensorial** de M e N, e será denotado por $M \otimes_A N$. Ele é gerado pelos elementos $m \otimes n$ com $m \in M$ e $n \in N$, chamaremos um elemento deste tipo de **tensor elementar**. Se $(m_i)_{i\in I}$ e $(n_j)_{j\in J}$ são famílias de geradores de M e N, respetivamente, então os elementos $m_i \otimes n_j$ geram $M \otimes_A N$. Em particular, se M e N são f.g. então também o é $M \otimes_A N$.

Aula 9

aula 9: 19/09/2014

Observação 66. Podemos generalizar a noção de produto tensorial a qualquer número finito de módulos, definindo aplicações multilineares $f : M_1 \times \cdots \times M_r \to P$ como sendo aplicações lineares em cada variável e seguindo a prova da Proposição 65 deveríamos chegar a um "**produto multi-tensorial**" $T = M_1 \otimes_A \cdots \otimes_A M_r$ gerado por todos os produtos $m_1 \otimes \cdots \otimes m_r$, com $m_i \in M_i$ para todo $i = 1, \ldots, r$.

Proposição 67. (Propriedades do Produto Tensorial) *Sejam M, N e P A-módulos, então:*

a. *Comutatividade:* $M \otimes_A N \simeq N \otimes_A M$;

b. *Associatividade:* $(M \otimes_A N) \otimes_A P \simeq M \otimes_A (N \otimes_A P)$;

c. *Distributividade:*$(M \oplus N) \otimes_A P \simeq (M \otimes_A P) \oplus (N \otimes_A P)$;

d. *Elemento unidade:* $A \otimes_A M \simeq M$

e. *Quocientes: Seja $I \subseteq A$ um ideal então* $M \otimes_A A/I \simeq M/IM$.

Demonstração. A técnica da demonstração é construir aplicações bilineares ou multilineares e usar a Proposição 65 para deduzir a existência de homomorfismos de produtos tensoriais e logo construir morfismos inversos explícitos para estes mapas. Os itens a. , b. e c. são deixados como **Exercício 3.**

Para ver d. defina a aplicação A-bilinear $\varphi : A \times M \to M$ dada por $(a, m) \mapsto am$. Pela Proposição 65 existe um A-homomorfismo $\varphi' : A \otimes_A M \to M$ dado por $\varphi'(a \otimes m) = am$. Seja agora o A-homomorfismo $\psi : M \to A \otimes_A M$ dado por $m \mapsto 1 \otimes m$, então $\varphi' \circ \psi : M \to M$ satisfaz $\varphi' \circ \psi(m) = \varphi'(1 \otimes m) = 1m = m$ para todo $m \in M$ logo $\varphi' \circ \psi = \mathrm{id}_M$. Por outro lado $\psi \circ \varphi' : A \otimes_A M \to A \otimes_A M$ satisfaz $\psi \circ \varphi'(a \otimes m) = \psi(am) = 1 \otimes am = a \otimes m$ para todo tensor elementar $a \otimes m$ com $a \in A$ e $m \in M$, como estes tensores elementares geram $A \otimes_A M$ temos que $\psi \circ \varphi' = \mathrm{id}_{A \otimes_A M}$. Portanto $A \otimes_A M \simeq M$.

Para provar e. defina a aplicação A-bilinear $\varphi : M \times A/I \to M/IM$ dada por $(m, \overline{a}) \mapsto \overline{am}$. Observe que esta aplicação está bem definida, i.e., o elemento $\overline{am}$ não depende da escolha do representante de classe de $\overline{a}$: Suponha que $\overline{a} = \overline{b}$ então $a - b \in I$ logo $(a - b)m \in IM$ ou seja $am - bm \in IM$ logo $\overline{am} = \overline{bm}$. Pela Proposição 65 existe um A-homomorfismo $\varphi' : M \otimes_A A/I \to M/IM$ dado por $\varphi'(m \otimes \overline{a}) = \overline{am}$. Seja agora o A-homomorfismo $\psi : M \to M \otimes_A A/I$ dado por $m \mapsto m \otimes \overline{1}$, vejamos que $IM \subseteq \mathrm{Ker}(\psi)$. Seja $m \in IM$, então $m = \Sigma a_i m_i$ com $a_i \in I$ e $m_i \in M$ logo temos

$$\begin{aligned}\psi(m) &= \psi(\sum_i a_i m_i) = (\sum_i a_i m_i) \otimes \overline{1} = \sum_i a_i (m_i \otimes \overline{1}) \\ &= \sum_i (m_i \otimes a_i \overline{1}) = \sum_i (m_i \otimes \overline{a_i}) = 0\end{aligned}$$

pois $a_i \in I$, logo $m \in \mathrm{Ker}(\psi)$. Assim ψ induz um A-homomorfismo $\overline{\psi} : M/IM \to M \otimes_A A/I$ dado por $\overline{m} \mapsto m \otimes \overline{1}$. Vejamos que φ' e $\overline{\psi}$ são inversos um do outro. Temos que $\varphi' \circ \overline{\psi} : M/IM \to M/IM$ satisfaz $\varphi' \circ \overline{\psi}(\overline{m}) = \varphi'(m \otimes \overline{1}) = \overline{1m} = \overline{m}$ para todo $\overline{m} \in M/IM$ logo $\varphi' \circ \overline{\psi} = \mathrm{id}_{M/IM}$. Por outro lado $\overline{\psi} \circ \varphi' : M \otimes_A A/I \to M \otimes_A A/I$ satisfaz $\overline{\psi} \circ \varphi'(m \otimes \overline{a}) = \overline{\psi}(\overline{am}) = am \otimes \overline{1} = m \otimes \overline{a}$ para todo tensor elementar $m \otimes \overline{a}$ com $\overline{a} \in A/I$ e $m \in M$, como estes tensores elementares geram $M \otimes_A A/I$ temos que $\overline{\psi} \circ \varphi' = \mathrm{id}_{M \otimes_A A/I}$. Portanto $M \otimes_A A/I \simeq M/IM$. □

Exemplo 68. Se m, n são coprimos então $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = 0$. Como $\mathrm{mdc}(m, n) = 1$ então existem $x, y \in \mathbb{Z}$ tais que $1 = mx + ny$. Seja agora $a \otimes b$ um gerador de $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z})$ então

$$\begin{aligned}a \otimes b &= 1(a \otimes b) = (mx + ny)(a \otimes b) \\ &= ((mx + ny)a) \otimes b = ((mx)a + (ny)a) \otimes b \\ &= (ny)a \otimes b = a \otimes (ny)b = a \otimes 0 = 0.\end{aligned}$$

Logo $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) = 0$.

Seja $f : A \to B$ um homomorfismo de anéis e seja N um B-módulo. Então N tem uma estrutura de A-módulo definida como segue: se $a \in A$ e $n \in N$

então definimos an como sendo $f(a)n$. Neste caso dizemos que o A-módulo N é obtido de N por **restrição de escalares**. Em particular, f define desta maneira uma estrutura de A-módulo em B.

Proposição 69. *Seja $f : A \to B$ um homomorfismo de anéis e seja N um B-módulo f.g. Suponha que B é f.g. como um A-módulo. Então N é f.g. como um A-módulo.*

Demonstração. Sejam $n_1, \ldots, n_r$ os geradores de N como B-módulo e sejam $b_1, \ldots, b_k$ os geradores de B como A-módulo. Então os rk produtos $n_i b_j$ são os geradores de N como A-módulo: $N \ni n = \sum_{i=1}^{r} x_i n_i$ onde $x_i \in B$, logo $x_i = \sum_{j=1}^{k} a_j^i b_j$ com $a_j^i \in A$ assim $n = \sum_{i=1}^{r} \sum_{j=1}^{k} a_j^i (b_j n_i)$. □

Seja M um A-módulo, podemos formar o A-módulo $M_B \simeq B \otimes_A M$ pois, como observamos antes, B tem estrutura de A-módulo. De fato M_B carrega também uma estrutura de B-módulo dada por $b(b' \otimes m) = bb' \otimes m$ para todo $b, b' \in B$ e $m \in M$. Dizemos que o B-módulo M_B é obtido de M por **extensão de escalares**.

Proposição 70. *Seja $f : A \to B$ um homomorfismo de anéis. Se M é um A-módulo f.g., então M_B é f.g. como um B-módulo.*

Demonstração. Sejam $m_1, \ldots, m_r$ os geradores de M sobre A e seja $b \otimes m$ um tensor elementar de M_B então $b \otimes m = b(1 \otimes m) = b(1 \otimes \sum_{i=1}^{r} a_i m_i) = \sum_{i=1}^{r} a_i b(1 \otimes m_i)$, onde a ação de A em B foi definida por $a_i b = f(a_i)b \in B$. Logo os $1 \otimes m_i$'s geram M_B sobre B. □

Proposição 71. *Sejam M, N, P A-módulos então*

$$\mathrm{Hom}_A(M \otimes_A N, P) \simeq \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P)).$$

Demonstração. Seja $f : M \times N \to P$ uma aplicação A-bilinear. Para cada $m \in M$ a aplicação $n \mapsto f(m, n)$ de N em P é A-linear (logo A-homomorfismo), logo f da origem a uma aplicação $\varphi : M \to \mathrm{Hom}_A(N, P)$ a qual é A-linear (logo A-homomorfismo) pois f é linear na variável m. Reciprocamente, qualquer A-homomorfismo $\varphi : M \to \mathrm{Hom}_A(N, P)$ define uma aplicação bilinear $f : M \times N \to P$ dada por $(m, n) \mapsto \varphi(m)(n)$. Logo o conjunto S de todas as aplicações A-bilineares $M \times N \to P$ está em correspondência um-a-um com $\mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$. Por outro lado, S está em correspondência um-a-um com $\mathrm{Hom}_A(M \otimes N, P)$ pela Proposição 65. Logo temos um isomorfismo canônico $\mathrm{Hom}_A(M \otimes_A N, P) \simeq \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$. □

Sejam $f : M \to M'$ e $g : N \to N'$ homomorfismos de A-módulos. Defina $h : M \times N \to M' \otimes_A N'$ por $h(m, n) = f(m) \otimes g(n)$, é fácil ver que h é A-bilinear e logo induz um homomorfismo de A-módulos $h' : M \otimes_A N \to M' \otimes_A N'$ tal que $h'(m \otimes n) = f(m) \otimes g(n)$ para todo $m \in M$ e $n \in N$. Denote h' por $f \otimes g$.

Em particular, fixado um A-módulo N temos um funtor $T_N = \_ \otimes_A N$ da categoria dos A-módulos e A-homomorfismos nela mesma, que associa a cada A-módulo M o A-módulo $M \otimes_A N$ e leva o A-homomorfismo $f : M \to M'$ no A-homomorfismo $f \otimes \mathrm{id} : M \otimes_A N \to M' \otimes_A N$. Uma das propriedades mais importantes deste funtor é que ele é exato à direita:

Proposição 72. ($\_ \otimes_A N$ é Exato à Direita) *Seja*

$$M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0 \tag{4}$$

uma sequência exata de A-módulos e A-homomorfismos, e seja N um A-módulo qualquer. Então a sequência

$$M' \otimes_A N \xrightarrow{f \otimes \mathrm{id}_N} M \otimes_A N \xrightarrow{g \otimes \mathrm{id}_N} M'' \otimes_A N \to 0 \tag{5}$$

é exata.

Demonstração. Denote por E a sequência (4) e por $E \otimes_A N$ a sequência (5). Seja P um A-módulo qualquer. Como E é exata, a sequência $\mathrm{Hom}_A(E, \mathrm{Hom}_A(N, P))$ é exata pela Proposição 64, logo a sequência $\mathrm{Hom}_A(E \otimes_A N, P)$ é exata pela Proposição 71. Novamente, pela Proposição 64 segue que $E \otimes_A N$ é exata. □

Em geral não é verdade que se $M' \xrightarrow{f} M \xrightarrow{g} M''$ é uma sequência exata então $M' \otimes_A N \xrightarrow{f \otimes \mathrm{id}} M \otimes_A N \xrightarrow{g \otimes \mathrm{id}} M'' \otimes_A N$ é exata, pois produtos tensoriais podem, por exemplo, destruir injetividade, vejamos:

Exemplo 73. Considere o anel $A = \mathbb{Z}$ e a sequência exata $0 \to \mathbb{Z} \xrightarrow{f} \mathbb{Z}$ onde $f(x) = 2x$ para todo $x \in \mathbb{Z}$. Seja $N = \mathbb{Z}/2\mathbb{Z}$ então a sequência $0 \to \mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \xrightarrow{f \otimes \mathrm{id}} \mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z})$ não é exata, pois para qualquer $x \otimes y \in \mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z})$ temos

$$(f \otimes \mathrm{id})(x \otimes y) = 2x \otimes y = x \otimes 2y = x \otimes 0 = 0,$$

logo $f \otimes \mathrm{id}$ é a aplicação nula enquanto que $\mathbb{Z} \otimes_{\mathbb{Z}} (\mathbb{Z}/2\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z} \neq 0$.

Definição 74. Um A-módulo M é dito **plano** se o funtor $\_ \otimes_A M$ é exato.

Note que como o produto tensorial é exato à direita, M é plano sobre A se, e somente se, o funtor $\_ \otimes_A M$ preserva injeções, ou seja, $N \hookrightarrow N'$ injetor implica $N \otimes_A M \hookrightarrow N' \otimes_A M$ injetor.

Exemplo 75.

a. Módulos livres são sempre planos: se $M = \bigoplus_{i\in I} A$, para qualquer morfismo de A-módulos $f : N \to N'$ temos a aplicação

$$N \otimes_A \left(\bigoplus_{i\in I} A\right) \xrightarrow{f\otimes \mathrm{id}} N' \otimes_A \left(\bigoplus_{i\in I} A\right), \tag{6}$$

mas pela propriedade distributiva e elemento unidade do produto tensorial (Proposição 67 c. e d.) temos: $N \otimes_A (\bigoplus_{i\in I} A) \simeq \bigoplus_{i\in I}(N \otimes_A A) \simeq \bigoplus_{i\in I} N$, assim o seguinte diagrama comuta

$$\begin{array}{ccc} N \otimes_A (\oplus_{i\in I} A) & \xrightarrow{f\otimes \mathrm{id}} & N' \otimes_A (\oplus_{i\in I} A) \\ \simeq \downarrow & & \downarrow \simeq \\ \oplus_{i\in I} N & \xrightarrow{\oplus_{i\in I} f} & \oplus_{i\in I} N' \end{array}$$

Logo se f é injetor então $\oplus f$ também é injetor o que implica que $f \otimes \mathrm{id}$ é injetor, mostrando que M é um A-módulo plano.

b. Se I é um ideal próprio de um domínio A, então A/I é um A-módulo plano se, e somente se, $I = 0$. **(Exercício 4.)**

Álgebras

Seja $f : A \to B$ um homomorfismo de anéis. Se $a \in A$ e $b \in B$ defina o produto $ab = f(a)b$. Logo B tem estrutura de A-módulo e estrutura de anel. Chamamos ao anel B equipado com sua estrutura de A-módulo de A-álgebra.

Definição 76. Uma **A-álgebra** é um anel B junto com um homomorfismo de anéis $f : A \to B$.

Se $f : A \to B$ e $g : A \to C$ são dois homomorfismos de anéis, um **homomorfismo de A-álgebras** $h : B \to C$ é um homomorfismo de anéis que também é um homomorfismo de A-módulos.

Dizemos que um homomorfismo de anéis $f : A \to B$ é **finito** e B é uma A-álgebra **finita** se B é f.g. como um A-módulo. Dizemos que o homomorfismo f é de **tipo finito** e B é uma **A-álgebra f.g.** se existe um conjunto finito de elementos $b_1, \ldots, b_n \in B$ tal que todo elemento de B pode ser escrito como um polinômio em $b_1, \ldots, b_n$ com coeficientes em $f(A)$, ou equivalentemente, se existe um homomorfismo de A-álgebras sobrejetor do anel dos polinômios $A[x_1, \ldots, x_n]$ em B.

AULA 10

Lembrando a última aula. Definimos uma A**-álgebra** como sendo um anel B equipado com uma estrutura de A-módulo definida por um homomorfismo de anéis $f : A \to B$ dada por $ab = f(a)b$.

Dadas duas A-álgebras B, C podemos formar seu produto tensorial $D = B \otimes_A C$ que é um A-módulo. Vamos definir uma multiplicação em D. Considere a aplicação $B \times C \times B \times C \to D$ definida por $(b, c, b', c') \mapsto bb' \otimes cc'$. Claramente esta aplicação é A-multilinear e logo induz um homomorfismo de A-módulos $B \otimes_A C \otimes_A B \otimes_A C \to D$, pela Proposição 67 b. podemos associar, então temos um homomorfismo de A-módulos $D \otimes_A D \to D$ que corresponde a uma aplicação A-bilinear $\mu : D \times D \to D$ tal que $\mu(b \otimes c, b' \otimes c') = bb' \otimes cc'$. Com esta multiplicação e a soma definida por $\mu^+(b \otimes c, b' \otimes c') = (b + b') \otimes (c + c')$, o produto tensorial $D = B \otimes_A C$ é um anel comutativo com elemento identidade $1 \otimes 1$. Mais ainda, D é uma A-álgebra: a aplicação $a \mapsto f(a) \otimes g(a)$ é um homomorfismo de anéis de A em D.

Definição 77. Uma A-álgebra B é **plana** se B é plano como A-módulo.

Proposição 78. *Seja $f : A \to B$ uma A-álgebra plana, $g : B \to C$ uma B-álgebra plana, então $g \circ f : A \to C$ é uma A-álgebra plana.*

Demonstração. Temos que provar que C é um A-módulo plano. É claro que C é um A-módulo com ação de A dada por $ac = g(f(a))c = (g \circ f)(a)c$, só resta provar que o funtor $\_ \otimes_A C$ é exato. Seja $j : N \hookrightarrow N'$ um homomorfismo de A-módulos injetivo, então como B é um A-módulo plano $j \otimes \mathrm{id}_B : N \otimes_A B \hookrightarrow N' \otimes_A B$ é um homomorfismo de A-módulos injetivo. Mas $N_B = N \otimes_A B$ é um B-módulo (obtido de N por extensão de escalares) com ação de B dada por $b(n \otimes b') = n \otimes bb'$ para todo $b, b' \in B$ e $n \in N$, logo $j \otimes \mathrm{id}_B : N \otimes_A B \hookrightarrow N' \otimes_A B$ é um homomorfismo de B-módulos injetivo. Como C é um B-módulo plano então $(j \otimes \mathrm{id}_B) \otimes \mathrm{id}_C : (N \otimes_A B) \otimes_B C \hookrightarrow (N' \otimes_A B) \otimes_B C$ é um homomorfismo de B-módulos injetivo. Como o seguinte diagrama

$$\begin{array}{ccc} (N \otimes_A B) \otimes_B C & \xrightarrow{(j\otimes\mathrm{id})\otimes\mathrm{id}} & (N' \otimes_A B) \otimes_B C \\ \simeq \uparrow & & \downarrow \simeq \\ N \otimes_A C & \xrightarrow{j\otimes\mathrm{id}} & N' \otimes_A C \end{array}$$

□

comuta (pelo Exercício 9 da Lista 3 : (Lei do **Cancelamento**) Seja $f : A \to B$ uma A-álgebra, M um A-módulo e N um B-módulo. Mostre que existe isomorfismo de B-módulos:$(M \otimes_A B) \otimes_B N \simeq M \otimes_A N$.) temos

que $j \otimes \mathrm{id}_C : N \otimes_A C \hookrightarrow N' \otimes_A C$ é um homomorfismo de B-módulos injetivo. Como B é uma A-álgebra todo B-módulo é um A-módulo (obtido de por restrição de escalares) com ação de A dada por $an = f(a)n$. Assim $j \otimes \mathrm{id}_C : N \otimes_A C \hookrightarrow N' \otimes_A C$ é um homomorfismo de A-módulos injetivo. Logo C é um A-módulo plano.

Proposição 79. (Mudança de Base) *Seja $f : A \to B$ uma A-álgebra plana, M um A-módulo plano então $B \otimes_A M$ é um B-módulo plano.*

Demonstração. Seja $j : N \hookrightarrow N'$ um homomorfismo de B-módulos injetivo. Como B é uma A-álgebra todo B-módulo é um A-módulo, assim $j : N \hookrightarrow N'$ é um homomorfismo de A-módulos injetivo. Como M é um A-módulo plano então $j \otimes \mathrm{id}_M : N \otimes_A M \hookrightarrow N' \otimes_A M$ é um homomorfismo de A-módulos injetivo. Mas $N \otimes_A M$ também tem estrutura de B-módulo com ação de B dada por $b(n \otimes m) = bn \otimes m$, assim $j \otimes \mathrm{id}_M : N \otimes_A M \hookrightarrow N' \otimes_A M$ é um homomorfismo de B-módulos injetivo. Analogamente à proposição anterior temos que o seguinte diagrama

$$\begin{array}{ccc} N \otimes_B (B \otimes_A M) & \xrightarrow{j\otimes\mathrm{id}} & N' \otimes_B (B \otimes_A M) \\ \downarrow \simeq & & \simeq \uparrow \\ N \otimes_A M & \xrightarrow{j\otimes\mathrm{id}} & N' \otimes_A M \end{array}$$

comuta, logo $j \otimes \mathrm{id} : N \otimes_B (B \otimes_A M) \hookrightarrow N' \otimes_B (B \otimes_A M)$ é um homomorfismo de B-módulos injetivo. Logo $B \otimes_A M$ é um B-módulo plano. □

3.4 EXERCÍCIOS

Ex. 32 — Prove que

1. Se $L \supseteq M \supseteq N$ são A-módulos, então $(L/N)/(M/N) \simeq L/M$.
2. Se M_1 e M_2 são submódulos de M, então

$$\frac{(M_1 + M_2)}{M_1} \simeq \frac{M_2}{(M_1 \cap M_2)}.$$

Ex. 33 — Seja $0 \to N' \xrightarrow{u} N \xrightarrow{v} N''$ uma sequência de A-módulos e A-homomorfismos. Mostre que essa sequência é exata se, e somente se, para todo A-módulo M a sequência

$$0 \to \mathrm{Hom}_A(M, N') \xrightarrow{\overline{u}} \mathrm{Hom}_A(M, N) \xrightarrow{\overline{v}} \mathrm{Hom}_A(M, N'')$$

é exata.

Ex. 34 — Seja $0 \to M' \to M \to M''$ uma sequência exata de A-módulos. Mostre que se M' e M'' são f.g. então M é f.g.

Ex. 35 — Seja A um anel não nulo. Mostre que se $A^m \simeq A^n$ então $m = n$.

Ex. 36 — Se I é um ideal próprio de um domínio A, então A/I é um A-módulo plano se, e somente se, $I = 0$.

Ex. 37 — (Propriedades do Produto Tensorial) Sejam M, N e P A-módulos, mostre que:

1. $M \otimes_A N \simeq N \otimes_A M$;
2. $(M \otimes_A N) \otimes_A P \simeq M \otimes_A (N \otimes_A P)$;
3. $(M \oplus N) \otimes_A P \simeq (M \otimes_A P) \oplus (N \otimes_A P)$;

Ex. 38 — (Lema de Nakayama II) Sejam A um anel local, $\mathbf{k}$ seu corpo de resíduos, M e N A-módulos f.g. Prove que:

1. Se $M \otimes_A \mathbf{k} = 0$ então $M = 0$.
2. Se $M \otimes_A N = 0$ então $M = 0$ ou $N = 0$.
3. Seja $\phi : N \to M$ um morfismo de A-álgebras. Então ϕ é sobrejetor se, e somente se, a aplicação $\mathbf{k}$-linear $\phi \otimes \mathrm{id} : N \otimes_A \mathbf{k} \to M \otimes_A \mathbf{k}$ é sobrejetora.

Ex. 39 — Seja A um anel, $f : A \to B$ uma A-álgebra, M um A-módulo e N um B-módulo. Mostre que

$$\mathrm{Hom}_B(B \otimes_A M, N) \simeq \mathrm{Hom}_A(M, N).$$

Ex. 40 — (Cancelamento) Seja $f : A \to B$ uma A-álgebra, M um A-módulo e N um B-módulo. Mostre que existe isomorfismo de B-módulos:

$$(M \otimes_A B) \otimes_B N \simeq M \otimes_A N.$$

Ex. 41 — Sejam M_i e M_i' A-módulos. Suponha que as linhas do diagrama comutativo

$$\begin{array}{ccccccc} M_1 & \xrightarrow{g} & M_2 & \xrightarrow{h} & M_3 & \xrightarrow{j} & M_4 \\ {\scriptstyle m}\downarrow & & {\scriptstyle n}\downarrow & & {\scriptstyle p}\downarrow & & \downarrow{\scriptstyle q} \\ M_1' & \xrightarrow{s} & M_2' & \xrightarrow{t} & M_3' & \xrightarrow{u} & M_4' \end{array}$$

são exatas e que m e p são A-homomorfismos sobrejetivos e q é um A-homomorfismo injetivo, mostre que n é um A-homomorfismo sobrejetivo.

Ex. 42 — Seja B uma A-álgebra e seja $f(x) \in A[x]$. Mostre que existem isomorfismos de B-álgebras:

1. $A[x] \otimes_A B \simeq B[x]$
2. $\dfrac{A[x]}{(f(x))A[x]} \otimes_A B \simeq \dfrac{B[x]}{(f(x))B[x]}$.

4

LOCALIZAÇÃO

Como uma generalização da forma em que construímos o corpo de frações de um domínio, podemos construir a localização de um subconjunto multiplicativo de um anel como sendo o anel obtido invertendo formalmente os elementos deste subconjunto.

Definição 80. Seja A um anel. Um **conjunto multiplicativo** $S \subseteq A$ é um subconjunto que é fechado por produto, ou seja se $s, t \in S$ então $st \in S$, e tal que $1 \in S$.

Defina uma relação $\equiv$ em $A \times S$ como segue:

$$(a, s) \equiv (a', s') \Leftrightarrow (as' - a's)u = 0 \text{ para algum } u \in S.$$

Claramente, esta relação é reflexiva e simétrica. Para ver que é transitiva, suponha que $(a, s) \equiv (b, t)$ e $(b, t) \equiv (c, u)$. Então existem $v, w \in S$ tais que $(at - bs)v = 0$ e $(bu - ct)w = 0$. Eliminando b destas duas equações temos $(au - cs)tvw = 0$. Como S é fechado sob multiplicação temos que $tvw \in S$, logo $(a, s) \equiv (c, u)$. Portanto, $\equiv$ é uma relação de equivalência.

Denotemos por $\frac{a}{s}$ a classe de equivalência de (a, s) e seja $S^{-1}A = (A \times S)/\equiv$ o conjunto das classes de equivalências. Vamos colocar uma estrutura de anel $S^{-1}A$ definindo adição e multiplicação da maneira usual[1]:

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2} \text{ e } \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}.$$

Com estas operações, $S^{-1}A$ é um anel comutativo com elemento nulo $\frac{0}{1}$ e elemento identidade $\frac{1}{1}$ que chamaremos de **localização** de A com respeito a S.

Associado a $S^{-1}A$ temos um homomorfismo de anéis $\rho : A \to S^{-1}A$ dado por $a \mapsto \frac{a}{1}$ chamado de **mapa de localização**.

Observação 81. Quando A é um domínio de integridade e $S = A - \{0\}$ então $S^{-1}A$ é o corpo de frações de A e neste caso o mapa de localização é a inclusão $A \subseteq S^{-1}A$. Entretanto, para anéis gerais, o mapa de localização nem sempre é injetivo.

Teorema 82. (Propriedade Universal da Localização) *Seja $g : A \to B$ um homomorfismo de anéis tal que $g(s) \in B^\times$ para todo $s \in S$. Então existe um único*

1 Estas operações estão bem definidas, i.e., não dependem dos representantes de classe utilizados. Verifique!

homomorfismo de anéis $h : S^{-1}A \to B$ tal que $g = h \circ \rho$ (onde ρ é o mapa de localização).

Demonstração. Unicidade. Se h satisfaz a condição, então $h(\frac{a}{1}) = h\rho(a) = g(a)$ para todo $a \in A$, logo se $s \in S$

$$h(\frac{1}{s}) = h((\frac{s}{1})^{-1}) = h(\frac{s}{1})^{-1} = g(s)^{-1}$$

e logo $h(\frac{a}{s}) = h(\frac{a}{1})h(\frac{1}{s}) = g(a)g(s)^{-1}$, logo h é univocamente determinado por g.

Existência. Seja $h(\frac{a}{s}) = g(a)g(s)^{-1}$. Então h será claramente um homomorfismo de anéis desde que esteja bem definido. Suponha então que $\frac{a}{s} = \frac{a'}{s'}$ então existe $t \in S$ tal que $(as' - a's)t = 0$, logo aplicando g temos

$$(g(a)g(s') - g(a')g(s))g(t) = 0,$$

agora $g(t), g(s)$ e $g(s')$ são unidades em B, então $g(a)g(s)^{-1} = g(a')g(s')^{-1}$, logo $h(\frac{a}{s}) = h(\frac{a'}{s'})$. □

O anel $S^{-1}A$ e o mapa de localização $\rho : A \to S^{-1}A$ têm as seguintes propriedades:

a. Se $s \in S$ então $\rho(s)$ é uma unidade em $S^{-1}A$;

b. Se $\rho(a) = 0$ então $as = 0$ para algum $s \in S$;

c. Todo elemento de $S^{-1}A$ é da forma $\rho(a)\rho(s)^{-1}$ para certos $a \in A$ e $s \in S$.

Reciprocamente, esta três condições determinam o anel $S^{-1}A$ a menos de isomorfismo. Mais precisamente:

Corolário 83. *Se $g : A \to B$ é um homomorfismo de anéis tal que:*

a. Se $s \in S$ então $g(s)$ é uma unidade em B;

b. Se $g(a) = 0$ então $as = 0$ para algum $s \in S$;

c. Todo elemento de B é da forma $g(a)g(s)^{-1}$ para certos $a \in A$ e $s \in S$.

Então existe um único isomorfismo $h : S^{-1}A \to B$ tal que $g = h \circ \rho$.

Demonstração. Segue do item a. e da Propriedade Universal da Localização (Teorema 82) que existe um único homomorfismo de anéis $h : S^{-1}A \to B$ definido por $h(\frac{a}{s}) = g(a)g(s)^{-1}$ tal que $g = h \circ \rho$. Vejamos que h é um isomorfismo. Pelo item c. h é sobrejetor. Para ver que h é injetor, seja $\frac{a}{s} \in \mathrm{Ker}(h)$ então $h(\frac{a}{s}) = 0$ logo $g(a) = 0$, segue do item b. que $at = 0$ para algum $t \in S$, logo $\frac{a}{s} = \frac{0}{1}$. □

Lema 84. *Seja A um anel e seja $S \subseteq A$ um conjunto multiplicativo. Então $S^{-1}A = 0$ se e somente se $0 \in S$.*

Demonstração. Temos que $S^{-1}A = 0$ se, e somente se, $\frac{0}{1} = \frac{1}{1}$ em $S^{-1}A$ (veja a Observação 2 logo após a Definição 1), ou seja, se e somente se, existe $s \in S$ tal que $(0 \cdot 1 - 1 \cdot 1) \cdot s = 0$, i.e., se e somente se, $s = 0 \in S$. □

Exemplo 85. Seja $\mathfrak{p}$ um ideal primo de A. Então $S = A \setminus \mathfrak{p}$ é um conjunto multiplicativo: $s, s' \in S$ então $s, s' \notin \mathfrak{p}$ logo $s \cdot s' \notin \mathfrak{p}$ portanto $s \cdot s' \in S$. Neste caso denotaremos por $A_{\mathfrak{p}}$ ao anel $S^{-1}A = \{\frac{a}{b} \mid a \in A, b \notin \mathfrak{p}\}$. Os elementos $\frac{a}{s}$ com $a \in \mathfrak{p}$ formam um ideal $\mathfrak{m}$ em $A_{\mathfrak{p}}$. Se $\frac{b}{t} \notin \mathfrak{m}$ então $b \notin \mathfrak{p}$, logo $b \in S$ e logo $\frac{b}{t}$ é uma unidade em $A_{\mathfrak{p}}$. Segue da Proposição 19 a. (Proposição da **Aula 2** que diz: Seja A um anel e $\mathfrak{m}$ um ideal próprio de A tal que todo $a \in A - \mathfrak{m}$ é uma unidade de A. Então A é um anel local e $\mathfrak{m}$ seu ideal maximal) que $A_{\mathfrak{p}}$ é um anel local e $\mathfrak{m}$ é seu único ideal maximal.

Podemos também localizar módulos (em particular, ideais) e álgebras: dado um A-módulo (ou A-álgebra) M, a **localização** $S^{-1}M$ de M com relação a um subconjunto multiplicativo S de A é o $S^{-1}A$-módulo (ou $S^{-1}A$-álgebra) cujos elementos são as frações $\frac{m}{s}$ com $m \in M$ e $s \in S$ com identificação:

$$\frac{m_1}{s_1} = \frac{m_2}{s_2} \text{ em } S^{-1}M \Leftrightarrow \exists t \in S \text{ tal que } t(s_2 m_1 - s_1 m_2) = 0 \text{ em } M$$

e operações de soma e multiplicação por escalar dadas por

$$\frac{m_1}{s_1} + \frac{m_2}{s_2} = \frac{s_2 m_1 + s_1 m_2}{s_1 s_2} \qquad \frac{a}{t} \cdot \frac{m}{s} = \frac{am}{ts},$$

para todo $a \in A$, $s, t \in S$ e $m_1, m_2 \in M$[2].

Dado um morfismo de A-módulos $f : M \to N$ temos um morfismo de $S^{-1}A$-módulos induzido $S^{-1}f : S^{-1}M \to S^{-1}N$ dado por $\frac{m}{s} \mapsto \frac{f(m)}{s}$ para todo $m \in M$ e $s \in S$. Este morfismo satisfaz $S^{-1}(f \circ g) = (S^{-1}f) \circ (S^{-1}g)$.

Logo "localização" é na verdade um funtor da categoria de A-módulos e na categoria de $S^{-1}A$-módulos. Uma das propriedades mais importantes deste funtor é que ele é exato:

Proposição 86. (S^{-1} é exato) *Seja A um anel, S um conjunto multiplicativo e $M' \xrightarrow{f} M \xrightarrow{g} M''$ uma sequência exata de A-módulos. Então $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ é uma sequência exata de $S^{-1}A$-módulos.*

Demonstração. Como $g \circ f = 0$ então $(S^{-1}g) \circ (S^{-1}f) = S^{-1}(g \circ f) = 0$, logo $\mathrm{Im}(S^{-1}f) \subseteq \mathrm{Ker}(S^{-1}g)$. Para mostrar a inclusão oposta, seja $\frac{m}{s} \in$

2 Verifique que estas operações estão bem definidas

$\mathrm{Ker}(S^{-1}g)$, então $\frac{g(m)}{s} = 0$ em $S^{-1}M''$, logo existe $t \in S$ tal que $tg(m) = 0$ em M''. Mas $tg(m) = g(tm)$ pois g é um homomorfismo de A-módulos, logo $tm \in \mathrm{Ker}(g) = \mathrm{Im}(f)$ e logo $tm = f(m')$ para algum $m' \in M'$. Então em $S^{-1}M$ temos $\frac{m}{s} = \frac{f(m')}{st} = (S^{-1}f)(\frac{m'}{st}) \in \mathrm{Im}(S^{-1}f)$. Logo $\mathrm{Ker}(S^{-1}g) \subseteq \mathrm{Im}(S^{-1}f)$. □

Aula 11

aula 11: 26/09/2014

Como consequências da exatidão de S^{-1} temos:

Corolário 87. *Seja A um anel, S um conjunto multiplicativo e $f : M \to N$ um A-homomorfismo. Temos:*

a. *Se f é injetor (respetivamente sobrejetor, bijetor) então $S^{-1}f$ é injetor (respetivamente sobrejetor, bijetor).*

b. *Localização comuta com kernels, cokernels e imagens, i.e., temos isomorfismos:*

   a) $\mathrm{Ker}(S^{-1}f) \simeq S^{-1}(\mathrm{Ker}(f))$

   b) $\mathrm{Coker}(S^{-1}f) \simeq S^{-1}(\mathrm{Coker}(f))$

   c) $\mathrm{Im}(S^{-1}f) \simeq S^{-1}(\mathrm{Im}(f))$

c. *Localização comuta com quocientes: Se N é um submódulo de M então* $S^{-1}(\frac{M}{N}) \simeq \frac{S^{-1}(M)}{S^{-1}(N)}$.

Demonstração. **Exercício 1.** □

Segue do primeiro item que se N é um submódulo de M a aplicação $S^{-1}N \to S^{-1}M$ é injetiva e logo $S^{-1}N$ pode ser considerado com um submódulo de $S^{-1}M$, i.e. localização preserva inclusões. Com esta convenção temos:

Corolário 88. *Se N e P são submódulos de um A-módulo M, então:*

a. $S^{-1}(N + P) = S^{-1}(N) + S^{-1}(P)$;

b. $S^{-1}(N \cap P) = S^{-1}(N) \cap S^{-1}(P)$.

Demonstração. **Exercício 2.** □

Proposição 89. *Seja M um A-módulo então existe um isomorfismo de $S^{-1}A$-módulos $S^{-1}A \otimes_A M \simeq S^{-1}M$.*

Demonstração. O anel $S^{-1}A$ junto com o homomorfismo de anéis "mapa de localização" $\rho : A \to S^{-1}A$ é uma A-álgebra e logo todo $S^{-1}A$-módulo é um A-módulo, em particular $S^{-1}M$ é um A-módulo. A aplicação $f : S^{-1}A \times M \to S^{-1}M$ definida por $(\frac{a}{s}, m) \mapsto \frac{am}{s}$ é A-bilinear e logo, pela propriedade universal do produto tensorial (Proposição 65), induz um A-homomorfismo $f' : S^{-1}A \otimes_A M \to S^{-1}M$ satisfazendo $f'(\frac{a}{s} \otimes m) = \frac{am}{s}$ para todo $a \in A$, $m \in M$ e $s \in S$. Por outro lado, $S^{-1}A \otimes_A M$ é o $S^{-1}A$-módulo obtido de M por extensão de escalares. Logo f' é um homomorfismo de $S^{-1}A$-módulos. Claramente, f' é sobrejetiva.

Seja, agora, $\Sigma_i(\frac{a_i}{s_i} \otimes m_i)$ um elemento de $S^{-1}A \otimes_A M$. Se denotamos $s = \Pi_i s_i \in S$ e $t_i = \Pi_{j \neq i} s_j$ então temos

$$\sum_i \frac{a_i}{s_i} \otimes m_i = \sum_i \frac{a_i t_i}{s} \otimes m_i = \sum_i \frac{1}{s} \otimes a_i t_i m_i = \frac{1}{s} \otimes \sum_i a_i t_i m_i,$$

logo todo elemento de $S^{-1}A \otimes_A M$ é da forma $\frac{1}{s} \otimes m$. Suponha que $f'(\frac{1}{s} \otimes m) = 0$, então $\frac{m}{s} = 0$ logo $tm = 0$ para algum $t \in S$ e portanto

$$\frac{1}{s} \otimes m = \frac{t}{st} \otimes m = \frac{1}{st} \otimes tm = \frac{1}{st} \otimes 0 = 0.$$

Logo f' é injetiva e logo é um isomorfismo de $S^{-1}A$-módulos. □

Corolário 90. *$S^{-1}A$ é um A-módulo plano.*

Demonstração. Seja $j : N \hookrightarrow N'$ um homomorfismo de A-módulos injetivo, como S^{-1} é um funtor exato (Proposição 86) então $S^{-1}j : S^{-1}N \hookrightarrow S^{-1}N'$ é um homomorfismo de $S^{-1}A$-módulos injetivo. Pela proposição anterior $N \otimes_A S^{-1}A \simeq S^{-1}N$ como $S^{-1}A$-módulos e o seguinte diagrama

$$\begin{array}{ccc} S^{-1}N & \xrightarrow{S^{-1}j} & S^{-1}N' \\ \simeq \uparrow & & \downarrow \simeq \\ N \otimes_A S^{-1}A & \xrightarrow{j \otimes \mathrm{id}} & N' \otimes_A S^{-1}A \end{array}$$

comuta. Logo $j \otimes \mathrm{id} : N \otimes_A S^{-1}A \hookrightarrow N' \otimes_A S^{-1}A$ é um homomorfismo de $S^{-1}A$-módulos injetivo. Mas $\rho : A \to S^{-1}A$ é uma A-álgebra e logo todo $S^{-1}A$-módulo é um A-módulo. Assim $j \otimes \mathrm{id} : N \otimes_A S^{-1}A \hookrightarrow N' \otimes_A S^{-1}A$ é um homomorfismo de A-módulos injetivo e por tanto $S^{-1}A$ é um A-módulo plano. □

Proposição 91. *Se M e N são A-módulos então existe um isomorfismo de $S^{-1}A$-módulos $S^{-1}(M \otimes_A N) \simeq (S^{-1}M) \otimes_{S^{-1}A} (S^{-1}N)$. Em particular, se $\mathfrak{p} \in \mathrm{Spec}(A)$ então $(M \otimes_A N)_{\mathfrak{p}} \simeq M_{\mathfrak{p}} \otimes_{A_{\mathfrak{p}}} N_{\mathfrak{p}}$ como $A_{\mathfrak{p}}$-módulos.*

Demonstração. **Exercício 3.** □

Proposição 92. *Seja M um A-módulo f.g., S um subconjunto multiplicativo de A. Então $S^{-1}(\mathrm{Ann}(M)) = \mathrm{Ann}(S^{-1}M)$.*

Demonstração. Para provar este resultado utilizaremos os seguintes fatos (verifique) onde M, N e P são A-módulos:

a. $\mathrm{Ann}(M+N) = \mathrm{Ann}(M) \cap \mathrm{Ann}(N)$.

b. $(N : P) = \mathrm{Ann}((N+P)/N)$.

Vejamos primeiramente que se o resultado vale para dois submódulos M_1 e M_2 de M então vale para a soma $M_1 + M_2$:

$$\begin{aligned} S^{-1}(\mathrm{Ann}(M_1+M_2)) &\overset{\text{fato}}{=} S^{-1}(\mathrm{Ann}(M_1) \cap \mathrm{Ann}(M_2)) \\ &\overset{\text{Cor 88}}{=} S^{-1}(\mathrm{Ann}(M_1)) \cap S^{-1}(\mathrm{Ann}(M_2)) \\ &\overset{\text{hip}}{=} \mathrm{Ann}(S^{-1}(M_1)) \cap \mathrm{Ann}(S^{-1}(M_2)) \\ &\overset{\text{fato}}{=} \mathrm{Ann}(S^{-1}M_1 + S^{-1}M_2) \\ &\overset{\text{Cor 88}}{=} \mathrm{Ann}(S^{-1}(M_1+M_2)). \end{aligned}$$

Logo é suficiente provar o resultado para um A-módulo M gerado por somente um elemento m. Seja $f : A \to M = (m)$ o homomorfismo de A-módulos dado por $a \mapsto am$ então claramente f é sobre e $\mathrm{Ker}(f) = \{a \in A \mid am = 0\} = \mathrm{Ann}(M)$, logo $M \simeq A/\mathrm{Ann}(M)$ como A-módulos. Então $S^{-1}M \simeq S^{-1}A/S^{-1}(\mathrm{Ann}(M))$ pelo Corolário 87 c. , assim $\mathrm{Ann}(S^{-1}M) = S^{-1}(\mathrm{Ann}(M))$.

□

Corolário 93. *Se N, P são submódulos de um A-módulo M e se P é f.g. então $S^{-1}(N : P) = (S^{-1}N : S^{-1}P)$.*

Demonstração. Como $(N : P) = \mathrm{Ann}((N+P)/N)$ e $(N+P)/N$ é f.g. então

$$\begin{aligned} S^{-1}(N : P) &= S^{-1}(\mathrm{Ann}((N+P)/N)) \\ &= \mathrm{Ann}(S^{-1}((N+P)/N)) \\ &= \mathrm{Ann}(S^{-1}(N+P)/S^{-1}N) \\ &= \mathrm{Ann}((S^{-1}N + S^{-1}P)/S^{-1}N) \\ &= (S^{-1}N : S^{-1}P). \end{aligned}$$

□

Uma propriedade $\mathcal{P}$ de um anel A (ou de um A-módulo M) é dita uma **propriedade local** se:

"A (ou M) tem $\mathcal{P}$ $\Leftrightarrow A_\mathfrak{p}$ (ou $M_\mathfrak{p}$) tem $\mathcal{P}$ para todo ideal $\mathfrak{p} \in \operatorname{Spec}(A)$"

As seguintes proposições são exemplos de propriedades locais:

Proposição 94. *Seja M um A-módulo, então são equivalentes:*

a. $M = 0$*;*

b. $M_\mathfrak{p} = 0$ *para todo* $\mathfrak{p} \in \operatorname{Spec}(A)$*;*

c. $M_\mathfrak{m} = 0$ *para todo* $\mathfrak{m} \in \operatorname{Specm}(A)$*;*

Demonstração. Claramente (a.)⇒(b.)⇒(c.). Suponha que acontece (c.) e que $M \neq 0$. Seja m um elemento não nulo de M e seja $I = \operatorname{Ann}(m)$ (i.e., o conjunto de todos os $a \in A$ tais que $am = 0$), então I é um ideal próprio de A e logo está contido em um ideal maximal $\mathfrak{m}$ (Corolário 15). Considere o elemento $\frac{m}{1} \in M_\mathfrak{m}$, como $M_\mathfrak{m} = 0$ temos que $\frac{m}{1} = 0$ e logo $tm = 0$ para algum $t \in S = A - \mathfrak{m}$, mas então t aniquila m e logo $t \in I \subseteq \mathfrak{m}$ o que é um contradição. □

Temos ainda uma importante recíproca da Proposição 86:

Teorema 95. *O complexo de A-módulos $M' \xrightarrow{f} M \xrightarrow{g} M''$ (i.e., uma sequência de A-módulos tal que $\operatorname{Im}(f) \subseteq \operatorname{Ker}(g)$) é exato, se e somente se, suas localizações $M'_\mathfrak{m} \xrightarrow{f_\mathfrak{m}} M_\mathfrak{m} \xrightarrow{g_m} M''_m$ são exatas para todo $\mathfrak{m} \in \operatorname{Specm}(A)$. Analogamente para todo $\mathfrak{p} \in \operatorname{Spec}(A)$.*

Demonstração. Considere o A-módulo $\operatorname{Ker}(g)/\operatorname{Im}(f)$. Segue do Corolário 87 que

$$\left(\frac{\operatorname{Ker}(g)}{\operatorname{Im}(f)}\right)_\mathfrak{m} \overset{(3)}{\simeq} \frac{(\operatorname{Ker}(g))_\mathfrak{m}}{(\operatorname{Im}(f))_\mathfrak{m}} \overset{(2)}{\simeq} \frac{\operatorname{Ker}(g_\mathfrak{m})}{\operatorname{Im}(f_\mathfrak{m})}.$$

Observe que, como o funtor localização preserva inclusões, $\operatorname{Im}(f_\mathfrak{m}) \subseteq \operatorname{Ker}(g_\mathfrak{m})$ e os quocientes acima estão bem definidos. Agora o complexo é exato se, e somente se, o A-módulo $\frac{\operatorname{Ker}(g)}{\operatorname{Im}(f)} = 0$. Segue da Proposição anterior que $\frac{\operatorname{Ker}(g)}{\operatorname{Im}(f)} = 0$ se, e somente se, $\left(\frac{\operatorname{Ker}(g)}{\operatorname{Im}(f)}\right)_\mathfrak{m} = 0$ para todo $\mathfrak{m} \in \operatorname{Specm}(A)$ se, e somente se, $\frac{\operatorname{Ker}(g_\mathfrak{m})}{\operatorname{Im}(f_\mathfrak{m})} = 0$ para todo $\mathfrak{m} \in \operatorname{Specm}(A)$ se, e somente se, $M'_\mathfrak{m} \xrightarrow{f_\mathfrak{m}} M_\mathfrak{m} \xrightarrow{g_m} M''_m$ é exata para todo $\mathfrak{m} \in \operatorname{Specm}(A)$. □

Como consequência disso temos:

Proposição 96. *Seja $f : M \to N$ um A-homomorfismo, então são equivalentes:*

a. f é injetiva (sobrejetiva, bijetiva)

b. $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ é injetiva (sobrejetiva, bijetiva) para todo $\mathfrak{p} \in \operatorname{Spec}(A)$;

c. $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_m$ é injetiva (sobrejetiva, bijetiva) para todo $\mathfrak{m} \in \operatorname{Specm}(A)$;

Demonstração. **Exercício 4.** □

A propriedade de um A-módulo ser plano é local:

Proposição 97. *Para qualquer A-módulo M, as seguintes afirmações são equivalentes:*

a. M é um A-módulo plano;

b. $M_{\mathfrak{p}}$ é um $A_{\mathfrak{p}}$-módulo plano para todo $\mathfrak{p} \in \operatorname{Spec}(A)$;

c. $M_{\mathfrak{m}}$ é um $A_{\mathfrak{m}}$-módulo plano para todo $\mathfrak{m} \in \operatorname{Specm}(A)$;

Demonstração. **Exercício 5.** □

4.2 LOCALIZAÇÃO E IDEAIS PRIMOS

Uma das ventagens da localização é que os elementos de S passam a ser unidades de $S^{-1}A$, e como consequência deste aumento de unidades temos uma redução na quantidade de ideais primos.

Teorema 98. *Seja A um anel, $S \subseteq A$ um conjunto multiplicativo e $\rho : A \to S^{-1}A$ o mapa de localização.*

a. Se $I \subseteq A$ é um ideal de A, então $S^{-1}I \subseteq S^{-1}A$ é um ideal de $S^{-1}A$. Reciprocamente, todo ideal $J \subseteq S^{-1}A$ é da forma $S^{-1}I$ para algum ideal $I \subseteq A$.

b. O mapa de espectros induzido por ρ, $\operatorname{Spec}(\rho) : \operatorname{Spec}(S^{-1}A) \hookrightarrow \operatorname{Spec}(A)$ é injetor e tem como imagem o conjunto

$$D_S := \{\mathfrak{p} \in \operatorname{Spec}(A) \mid \mathfrak{p} \cap S = \emptyset\}$$

dos primos $\mathfrak{p}$ que não interceptam S. A pré-imagem de $\mathfrak{p} \in D_S$ é dada por $S^{-1}\mathfrak{p}$. (i.e., os ideais primos de $S^{-1}A$ estão em correspondência um-a-um com os ideais primos de A que não interceptam S).

Demonstração.

a. Como localização é um funtor exato, preserva injetividade, assim se $I \subseteq A$ é um ideal de A então $S^{-1}I \subseteq S^{-1}A$ é um ideal de $S^{-1}A$. Reciprocamente, dado um ideal $J \subseteq S^{-1}A$, temos que $I = \rho^{-1}(J)$ é um ideal de A. Vejamos que $S^{-1}I = J$:

   a) $(\subseteq)$ se $\frac{a}{s} \in S^{-1}I$ com $a \in A$ e $s \in S$ então existe $i \in I$ e $s' \in S$ tal que $\frac{a}{s} = \frac{i}{s'}$. Então existe $t \in S$ tal que $tas' = tsi \in I$, logo $\rho(ats') \in J \subseteq S^{-1}A$ i.e., $\frac{ats'}{1} \in J$. Mas $ts' \in S$ é unidade em $S^{-1}A$ então posso multiplicar pelo inverso $\frac{1}{ts'}\frac{ats'}{1} \in J$ (e ainda pertence a J por ser ideal) assim $\frac{a}{1} = \rho(a) \in J$. Logo segue que $\frac{a}{s} = \frac{1}{s} \cdot \rho(a) \in J$.

   b) $(\supseteq)$ se $\frac{b}{s} \in J$ com $b \in A$ e $s \in S$ então $\rho(b) = \frac{s}{1} \cdot \frac{b}{s} \in J$, ou seja, $b \in I$ e portanto $\frac{b}{s} \in S^{-1}I$.

□

Aula 12

AULA 12: 01/10/2014

Lembrando a última aula.

Teorema. *Seja A um anel, $S \subseteq A$ um conjunto multiplicativo e $\rho : A \to S^{-1}A$ o mapa de localização.*

a. Se $I \subseteq A$ é um ideal de A, então $S^{-1}I \subseteq S^{-1}A$ é um ideal de $S^{-1}A$. Reciprocamente, todo ideal $J \subseteq S^{-1}A$ é da forma $S^{-1}I$ para algum ideal $I \subseteq A$.

b. O mapa de espectros $\mathrm{Spec}(\rho) : \mathrm{Spec}(S^{-1}A) \hookrightarrow \mathrm{Spec}(A)$ é injetor e tem como imagem o conjunto

$$D_S := \{\mathfrak{p} \in \mathrm{Spec}(A) \mid \mathfrak{p} \cap S = \emptyset\}$$

dos primos $\mathfrak{p}$ que não interceptam S. A pré-imagem de $\mathfrak{p} \in D_S$ é dada por $S^{-1}\mathfrak{p}$. (i.e., os ideais primos de $S^{-1}A$ estão em correspondência um-a-um com os ideais primos de A que não interceptam S).

Restava provar o item *b.*

Demonstração.

- Inicialmente, observe que: para $\mathfrak{p} \in D_S$, $a \in A$ e $s \in S$ temos

$$\frac{a}{s} \in S^{-1}\mathfrak{p} \Leftrightarrow a \in \mathfrak{p}. \tag{7}$$

A implicação ($\Leftarrow$) é obvia. Por outro lado, se $\frac{a}{s} \in S^{-1}\mathfrak{p}$ então existem $p \in \mathfrak{p}$ e $t \in S$ tais que $\frac{a}{s} = \frac{p}{t}$ em $S^{-1}A$, logo existe $r \in S$ tal que $r(at - ps) = 0$ logo $rta = rsp \in \mathfrak{p}$. Como $\mathfrak{p}$ é primo ou $r \in \mathfrak{p}$ ou $t \in \mathfrak{p}$ ou $a \in \mathfrak{p}$, mas $\mathfrak{p} \in D_S$ logo $\mathfrak{p} \cap S = \emptyset$ assim $r, t \notin \mathfrak{p}$ então necessariamente $a \in \mathfrak{p}$ o que prova ($\Rightarrow$).

- $\mathrm{Im}(\mathrm{Spec}(\rho)) \subseteq D_S$: seja $\mathfrak{p} \in \mathrm{Im}(\mathrm{Spec}(\rho))$, então existe $\mathfrak{q} \in \mathrm{Spec}(S^{-1}A)$ tal que $\mathfrak{p} = \mathrm{Spec}(\rho)(\mathfrak{q})$ então $\mathfrak{p} = \rho^{-1}(\mathfrak{q})$. Suponha que existe $s \in S \cap \mathfrak{p}$ então $\rho(s) \in \mathfrak{q}$, o que é absurdo pois $\rho(s) \in (S^{-1}A)^{\times}$.

- Se $\mathfrak{p} \in D_S$ então $S^{-1}\mathfrak{p} \in \mathrm{Spec}(S^{-1}A)$: note que $S^{-1}\mathfrak{p}$ é um ideal próprio de $S^{-1}A$ pois caso contrário $\frac{1}{1} \in S^{-1}\mathfrak{p}$ e isto implica pela observação inicial (7) que $1 \in \mathfrak{p}$, um absurdo. Agora, dados $a, a' \in A$ e $s, s' \in S$ temos

$$\begin{aligned} \frac{a}{s} \cdot \frac{a'}{s'} \in S^{-1}\mathfrak{p} &\Leftrightarrow \frac{aa'}{ss'} \in S^{-1}\mathfrak{p} \\ &\overset{(7)}{\Leftrightarrow} aa' \in \mathfrak{p} \\ &\Leftrightarrow a \in \mathfrak{p} \text{ ou } a' \in \mathfrak{p} \\ &\Leftrightarrow \frac{a}{s} \in S^{-1}\mathfrak{p} \text{ ou } \frac{a'}{s'} \in S^{-1}\mathfrak{p} \end{aligned}$$

  o que mostra que $S^{-1}\mathfrak{p}$ é um ideal primo de $S^{-1}A$.

- Por último, mostraremos que o mapa $\mathrm{Spec}(\rho) : \mathrm{Spec}(S^{-1}A) \to D_S$ é uma bijeção com inversa $\mathfrak{p} \mapsto S^{-1}\mathfrak{p}$: A composição

$$\begin{array}{rccl} D_S \to & \mathrm{Spec}(S^{-1}A) & \to D_S \\ \mathfrak{p} \mapsto & S^{-1}\mathfrak{p} & \mapsto \mathrm{Spec}(\rho)(S^{-1}\mathfrak{p}) \end{array}$$

  é a identidade em D_S, já que

$$\begin{aligned} \mathrm{Spec}(\rho)(S^{-1}\mathfrak{p}) = \rho^{-1}(S^{-1}\mathfrak{p}) &= \left\{ a \in A \mid \rho(a) \in S^{-1}\mathfrak{p} \right\} \\ &= \left\{ a \in A \mid \frac{a}{1} \in S^{-1}\mathfrak{p} \right\} \overset{(7)}{=} \mathfrak{p} \end{aligned}$$

  pela observação inicial. Da mesma forma, a composição

$$\begin{array}{rccl} \mathrm{Spec}(S^{-1}A) \to & D_S & \to \mathrm{Spec}(S^{-1}A) \\ \mathfrak{q} \mapsto & \rho^{-1}\mathfrak{q} & \mapsto S^{-1}(\rho^{-1}(\mathfrak{q})) \end{array}$$

  é a identidade em $\mathrm{Spec}(S^{-1}A)$, pois $\mathfrak{q} = S^{-1}(\rho^{-1}(\mathfrak{q}))$ pelo item a.

□

Corolário 99. *Seja A um anel. Se $\mathfrak{p} \in \operatorname{Spec}(A)$, temos uma bijeção*

$$\begin{aligned} \{\mathfrak{q} \in \operatorname{Spec}(A) \mid \mathfrak{q} \subseteq \mathfrak{p}\} &\xrightarrow{\simeq} \operatorname{Spec}(A_{\mathfrak{p}}) \\ \mathfrak{q} &\mapsto \mathfrak{q}A_{\mathfrak{p}}. \end{aligned}$$

Demonstração. Tome $S = A - \mathfrak{p}$ no teorema anterior. □

Como consequência a passagem de A a $A_{\mathfrak{p}}$ elimina todos os ideais primos excepto aqueles contidos em $\mathfrak{p}$. Por outro lado, a passagem de A a $A/\mathfrak{p}$ elimina todos os ideais primos excepto aqueles que contêm $\mathfrak{p}$. Logo se $\mathfrak{p}$ e $\mathfrak{q}$ são ideais primos tais que $\mathfrak{q} \subseteq \mathfrak{p}$, então localizando em relação a $\mathfrak{p}$ e tomando o quociente Mod $\mathfrak{q}$ (ou ao contrário, pois essas operações comutam), restringimos nossa atenção a aqueles ideais primos que se encontram entre $\mathfrak{p}$ e $\mathfrak{q}$. Em particular, se $\mathfrak{p} = \mathfrak{q}$ chegaremos ao corpo de resíduos do anel local $A_{\mathfrak{p}}$ o qual também pode ser obtido como o corpo de frações do domínio $A/\mathfrak{p}$.

Exemplo 100. Como $A/\mathfrak{p}$ é um domínio então a localização por $S = (A/\mathfrak{p}) - \mathfrak{p}$ coincide com o corpo de frações de $A/\mathfrak{p}$, i.e. $(A/\mathfrak{p})_{\mathfrak{p}} = \operatorname{Frac}(A/\mathfrak{p})$ (veja a Observação 81) e o mapa de localização neste caso é a inclusão. Logo, dada a composição $A \overset{\pi}{\twoheadrightarrow} A/\mathfrak{p} \overset{\rho}{\hookrightarrow} \operatorname{Frac}(A/\mathfrak{p})$ o mapa entre espectros induzido $\operatorname{Spec}(\rho \circ \pi) : \operatorname{Spec}(\operatorname{Frac}(A/\mathfrak{p})) \hookrightarrow \operatorname{Spec}(A)$ tem como imagem exatamente o primo $\mathfrak{p}$, pois $\operatorname{Spec}(\rho \circ \pi)$ é a composição

$$\operatorname{Spec}(\operatorname{Frac}(A/\mathfrak{p})) \overset{\operatorname{Spec}(\rho)}{\hookrightarrow} \operatorname{Spec}(A/\mathfrak{p}) \overset{\operatorname{Spec}(\pi)}{\hookrightarrow} \operatorname{Spec}(A)$$

(onde $\operatorname{Spec}(\rho)$ é injetor pelo teorema anterior e $\operatorname{Spec}(\pi)$ é injetor pelo Lema 34) e como $\operatorname{Frac}(A/\mathfrak{p})$ é um corpo, seu único ideal primo é (0), assim $\operatorname{Spec}(\operatorname{Frac}(A/\mathfrak{p})) = (0)$ e a imagem do primeiro mapa $\operatorname{Spec}(\rho)(0) = \rho^{-1}(0)$ é o ideal $(\overline{0})$ de $A/\mathfrak{p}$, que é levado em $\mathfrak{p}$ pelo segundo mapa. Em outras palavras, como o quociente e a localização "filtram" os primos que contêm e que estão contidos em $\mathfrak{p}$ o que sobra é apenas o primo $\mathfrak{p}$.

Para finalizar esta seção veja que podemos dar uma prova alternativa à Proposição 24 (que caracteriza o nilradical de um anel A, Aula 2.) utilizando localização. Lembremos os conceitos:

Definição. O ideal $\mathfrak{N}$ de todos os elementos nilpotentes de um anel A é chamado de **nilradical** de A.

Proposição. *O nilradical de A é a interseção de todos os ideais primos de A.*

Demonstração. A prova de que o nilradical está contido na interseção de todos os ideais primos é a mesma, mostraremos a outra inclusão. Seja $a \in A$ um elemento que não é nilpotente, vamos provar que existe um ideal

primo $\mathfrak{p}$ de A que não contem a. O conjunto $S = (a^n)_{n\geq 0}$ é um conjunto multiplicativo que não contém o elemento nulo 0. Segue do Lema 84 que o anel $S^{-1}A$ é não nulo e logo (Teorema 14) tem um ideal maximal $\mathfrak{m}$. Segue o Teorema 98 que $\mathfrak{m}$ corresponde a um ideal primo $\mathfrak{p}$ de A que não intercepta S, logo $a \notin \mathfrak{p}$. □

4.3 EXERCÍCIOS

Ex. 43 — Seja A um anel, S um conjunto multiplicativo e $f : M \to N$ um A-homomorfismo. Mostre que:

1. Se f é injetor (respetivamente sobrejetor, bijetor) então $S^{-1}f$ é injetor (respetivamente sobrejetor, bijetor).
2. Localização comuta com kernels, cokernels e imagens, i.e., temos isomorfismos:
   a) $\mathrm{Ker}(S^{-1}f) \simeq S^{-1}(\mathrm{Ker}(f))$
   b) $\mathrm{Coker}(S^{-1}f) \simeq S^{-1}(\mathrm{Coker}(f))$
   c) $\mathrm{Im}(S^{-1}f) \simeq S^{-1}(\mathrm{Im}(f))$
3. Localização comuta com quocientes: Se N é um submódulo de M então $S^{-1}\left(\frac{M}{N}\right) \simeq \frac{S^{-1}(M)}{S^{-1}(N)}$.

Ex. 44 — Se N e P são submódulos de um A-módulo M, mostre que:

1. $S^{-1}(N + P) = S^{-1}(N) + S^{-1}(P)$;
2. $S^{-1}(N \cap P) = S^{-1}(N) \cap S^{-1}(P)$.

Ex. 45 — Se M e N são A-módulos mostre que existe um isomorfismo de $S^{-1}A$-módulos $S^{-1}(M \otimes_A N) \simeq (S^{-1}M) \otimes_{S^{-1}A} (S^{-1}N)$.

Ex. 46 — Seja $f : M \to N$ um A-homomorfismo, prove que são equivalentes:

1. f é injetiva (sobrejetiva, bijetiva)
2. $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ é injetiva (sobrejetiva, bijetiva) para todo $\mathfrak{p} \in \mathrm{Spec}(A)$;
3. $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_m$ é injetiva (sobrejetiva, bijetiva) para todo $\mathfrak{m} \in \mathrm{Specm}(A)$;

Ex. 47 — Para qualquer A-módulo M, mostre que são equivalentes:

1. M é um A-módulo plano;
2. $M_{\mathfrak{p}}$ é um $A_{\mathfrak{p}}$-módulo plano para todo $\mathfrak{p} \in \mathrm{Spec}(A)$;

3. $M_{\mathfrak{m}}$ é um $A_{\mathfrak{m}}$-módulo plano para todo $\mathfrak{m} \in \mathrm{Specm}(A)$;

Ex. 48 — Seja I um ideal de A, mostre que $S^{-1}\sqrt{I} = \sqrt{S^{-1}I}$. Em particular, se $\mathfrak{N}_A$ é o nilradical de A então $\mathfrak{N}_{S^{-1}A} = S^{-1}\mathfrak{N}_A$.

Ex. 49 — Seja A um anel. Suponha que, para cada $\mathfrak{p} \in \mathrm{Spec}(A)$, o anel local $A_{\mathfrak{p}}$ não tenha elementos nilpotentes não nulos. Mostre que A não tem elementos nilpotentes não nulos. Se cada $A_{\mathfrak{p}}$ for um domínio de integridade, então necessariamente A é um domínio de integridade?

Ex. 50 — Seja M um A-módulo e I um ideal de A. Suponha que $M_{\mathfrak{m}} = 0$ para todo $\mathfrak{m} \in \mathrm{Specm}(A)$ tal que $\mathfrak{m} \supseteq I$. Prove que $M = IM$.

Ex. 51 — Seja A um anel e seja F o A-módulo livre A^n. Mostre que todo conjunto de n geradores de F é uma base de F (i.e. é LI sobre A).

5

CONDIÇÕES DE CADEIA

Seja Ω um conjunto parcialmente ordenado por uma relação $\leq$. As seguintes condições em Ω são equivalentes:

a. Toda sequência crescente $x_1 \leq x_2 \leq \cdots$ em Ω é estacionária, i.e., existe n tal que $x_n = x_{n+1} = \cdots$.

b. Todo subconjunto não vazio de Ω tem um elemento maximal.

Demonstração. (a.)$\Rightarrow$(b.) Seja T um subconjunto não vazio de Ω e seja $x_1 \in T$. Se x_1 é maximal em T acabou. Caso contrário existe $x_2 \in T$ tal que $x_1 \lneq x_2$. Se x_2 é maximal em T acabou, caso contrário repita o processo. Eventualmente, este processo termina, já que caso contrário obteríamos uma cadeia ascendente $x_1 \lneq x_2 \lneq x_3 \lneq \cdots$ estrita, o que contradiz a hipótese. Por tanto T tem um elemento maximal.

(a.)$\Leftarrow$(b.) Seja $x_1 \leq x_2 \leq \cdots$ uma sequência crescente em Ω, então o conjunto $(x_m)_{m\geq 1}$ tem um elemento maximal x_n e logo a sequência é estacionária. □

Se Ω é o conjunto de submódulos de um módulo M, ordenado pela relação $\subseteq$, então (a.) é chamada de **condição de cadeia ascendente** (cca) e (b.) de **condição maximal**. Um módulo M que satisfaz qualquer uma de estas condições equivalentes é chamado de **Noetheriano**. Se Ω é ordenado por $\supseteq$, então (a.) é chamada de **condição de cadeia descendente** (ccd) e (b.) de **condição minimal**. Um módulo M que satisfaz qualquer uma de estas condições equivalentes é chamado de **Artiniano**.

Proposição 101. *M é um A-módulo Noetheriano se e somente se todo submódulo de M é f.g.*

Demonstração. ($\Rightarrow$): Seja N um submódulo de M, e seja Ω o conjunto de todos os submódulos f.g. de N. Então Ω é um conjunto não vazio, pois $0 \in \Omega$, de submódulos de M e logo tem um elemento maximal N_0. Se $N_0 \neq N$, considere o submódulo $N_0 + An$ onde $n \in N$ e $n \notin N_0$. Este submódulo é f.g. e contém estritamente N_0 o que é uma contradição. Logo $N = N_0$ e logo N é f.g.

($\Leftarrow$): Seja $M_1 \subseteq M_2 \subseteq \cdots$ uma cadeia ascendente de submódulos de M. É fácil ver que $N = \cup_{n=1}^{\infty} M_n$ é um submódulo de M (usando a condição de cadeia) e logo é f.g. Sejam $x_1, \ldots, x_r$ os geradores de N tal que $x_i \in M_{n_i}$ e seja $n = \max_{1\leq i\leq r} n_i$. Então cada $x_i \in M_n$, logo $N = M_n$ e portanto a cadeia é estacionária. □

É esta última proposição que torna os módulos Noetherianos mais úteis que os módulos Artinianos. Porém, muitas propriedades formais elementares aplicam-se igualmente a módulos Artinianos e Noetherianos.

Proposição 102. *Seja* $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *uma sequência exata de A-módulos. Então*

a. *M é Noetheriano* $\Leftrightarrow$ *M′ e M″ são Noetherianos;*

b. *M é Artiniano* $\Leftrightarrow$ *M′ e M″ são Artinianos;*

Demonstração. Faremos a prova para módulos Noetherianos, o caso Artiniano é similar (**Exercício 1**).

($\Rightarrow$): Sejam $M_1' \subseteq M_2' \subseteq \cdots$ e $M_1'' \subseteq M_2'' \subseteq \cdots$ cadeias ascendentes de submódulos de M' e M'' respetivamente. Logo $f(M_1') \subseteq f(M_2') \subseteq \cdots$ e $g^{-1}(M_1'') \subseteq g^{-1}(M_2'') \subseteq \cdots$ são cadeias ascendentes de submódulos de M. Como M é Noetheriano estas cadeias são estacionárias logo $f(M_k') = f(M_{k+1}') = \cdots$ para algum k e $g^{-1}(M_n'') = g^{-1}(M_{n+1}'') = \cdots$ para algum n. Agora segue do fato de f ser injetiva que $f^{-1}f(M_i') = M_i'$ para todo i e logo $M_k' = M_{k+1}' = \cdots$ o que implica que M' é Noetheriano. Analogamente, como g é sobrejetiva temos $g(g^{-1}(M_i'')) = M_i''$ para todo i, assim $M_n'' = M_{n+1}'' = \cdots$ o que implica que M'' é Noetheriano.

($\Leftarrow$): Suponha que M' e M'' são Noetherianos. Seja $M_1 \subseteq M_2 \subseteq \cdots$ uma cadeia ascendente de submódulos de M; então $(f^{-1}(M_i))$ é uma cadeia em M' e $(g(M_i))$ é uma cadeia em M''. Para um n suficientemente grande ambas cadeias são estacionárias, logo $f^{-1}(M_n) = f^{-1}(M_{n+1}) = \cdots$ e $g(M_n) = g(M_{n+1}) = \cdots$. Queremos provar que sob estas condições $M_n = M_{n+1}$, mas como $M_n \subseteq M_{n+1}$ basta mostrar a inclusão oposta. Seja $x \in M_{n+1}$ então existe $y \in M_n$ tal que $g(y) = g(x)$ logo $g(x-y) = 0$ por tanto $x - y \in \mathrm{Ker}(g) = \mathrm{Im}(f)$. Isto implica que existe $z \in M'$ tal que $f(z) = x - y \in M_{n+1}$, logo $z \in f^{-1}(M_{n+1}) = f^{-1}(M_n)$ e logo $f(z) \in M_n$, i.e. $x - y \in M_n$ mas como $y \in M_n$ segue que $x \in M_n$. Logo $M_{n+1} \subseteq M_n$ e a cadeia ascendente é estacionária. Segue que M é Noetheriano. □

Aula 13

aula 13: 03/10/2014

Na última aula provamos que

Proposição. *Seja* $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ *uma sequência exata de A-módulos. Então: M é Noetheriano (Artiniano)* $\Leftrightarrow$ *M′ e M″ são Noetherianos (Artinianos).*

Note que em particular, quocientes e submódulos de módulos Noetherianos (resp. Artinianos) são Noetherianos (resp. Artinianos).

Como corolário da proposição anterior temos

Corolário 103. *Se M_i para $1 \leq i \leq n$ são A-módulos Noetherianos (resp. Artinianos) então $\bigoplus_{i=1}^{n} M_i$ é um A-módulo Noetheriano (resp. Artiniano).*

Demonstração. Faremos a prova por indução em n. O caso $n = 1$ é trivial. Suponha que o resultado vale para $n = k$, i.e. se $M_1, \cdots, M_k$ são A-módulos Noetherianos (resp. Artinianos) então $\bigoplus_{i=1}^{k} M_i$ é um A-módulo Noetheriano (resp. Artiniano). Considere, agora, a sequência

$$0 \to M_{k+1} \xrightarrow{f} \bigoplus_{i=1}^{k+1} M_i \xrightarrow{g} \bigoplus_{i=1}^{k} M_i \to 0,$$

onde f , dada por $m_{k+1} \mapsto (0, \cdots, 0, m_{k+1})$, é claramente injetiva e g, dada por $(m_1, \cdots, m_k, m_{k+1}) \mapsto (m_1, \cdots, m_k)$, é sobre. Agora, temos que $g \circ f(m_{k+1}) = g(0, \cdots, 0, m_{k+1}) = (0, \cdots, 0)$ logo $\mathrm{Im}(f) \subseteq \mathrm{Ker}(g)$. Seja $(m_1, \cdots, m_{k+1}) \in \mathrm{Ker}(g)$ então $m_i = 0$ para $i = 1, \ldots, k$ logo $(m_1, \cdots, m_{k+1}) = (0, \cdots, 0, m_{k+1}) = f(m_{k+1}) \in \mathrm{Im}(f)$. Portanto a sequência é exata. Como M_{k+1} e $\bigoplus_{i=1}^{k} M_i$ são Noetherianos (resp. Artinianos), segue da Proposição 102 que $\bigoplus_{i=1}^{k+1} M_i$ é um A-módulo Noetheriano (resp. Artiniano). □

Definição 104. Um anel A é dito **Noetheriano** (resp. **Artiniano**) se é Noetheriano (resp. Artiniano) como A-módulo, i.e., se satisfaz a cca (resp. ccd) em ideais.

Exemplo 105.

a. Todo corpo $\mathbf{k}$ é ambos Noetheriano e Artiniano, pois somente tem dois ideais (0) e $\mathbf{k}$.

b. O anel $\mathbb{Z}$ satisfaz cca mas não ccd, pois se $a \in \mathbb{Z}$ e $a \neq 0$ temos $(a) \supset (a^2) \supset \cdots \supset (a^n) \supset \cdots$ (inclusões estritas). Logo é Noetheriano mas não Artiniano.

c. Todo DIP é Noetheriano, pois todo ideal é f.g.

d. O anel dos polinômios $\mathbf{k}[x_1, x_2, \ldots, x_n, \ldots]$ em um número infinito de indeterminadas não satisfaz nenhuma das condições de cadeia: a sequência $(x_1) \subset (x_1, x_2) \subset \cdots$ é estritamente crescente e a sequência $(x_1) \supset (x_1^2) \supset (x_1^3) \supset \cdots$ é estritamente decrescente. Logo não é Noetheriano nem Artiniano.

Proposição 106. *Seja A um anel Noetheriano (resp. Artiniano), M um A-módulo f.g. Então M é Noetheriano (resp. Artiniano).*

Demonstração. Sejam $m_1, \ldots, m_n$ os geradores de M, defina $f : A^n \to M$ por $f(a_1, \ldots, a_n) = a_1 m_1 + \cdots + a_n m_n$. Então f é um homomorfismo de A-módulos sobrejetor. Segue do Corolário 103 que A^n é Noetheriano (resp. Artiniano) e logo pela Proposição 102 M é um A-módulo Noetheriano (resp. Artiniano). □

Proposição 107. *Seja A um anel Noetheriano (resp. Artiniano), I um ideal de A. Então A/I é um anel Noetheriano (resp. Artiniano).*

Demonstração. Como a projeção canônica $\pi : A \to A/I$ é um homomorfismo de A-módulos sobrejetor e A é um A-módulo Noetheriano (resp. Artiniano), segue da Proposição 102 que A/I é Noetheriano (resp. Artiniano) como um A-módulo e logo também como um A/I-módulo pois, segue do Teorema da Correspondência versão para Submódulos (Aula 7, logo após a definição de submódulo, Definição 51), que os A-submódulos de A/I correspondem aos A-submódulos de A (i.e., ideias de A) que contém I, que correspondem aos ideais de A/I. □

Uma **cadeia** de submódulos de um módulo M é uma sequência $(M_i)_{i=0}^n$ de submódulos de M tais que

$$M = M_n \supsetneq M_{n-1} \supsetneq \cdots \supsetneq M_0 = 0 \text{ (inclusões estritas).}$$

O **comprimento** da cadeia é n. Uma **série de composição** de M é uma cadeia maximal, ou seja uma cadeia na qual não podem ser insertados submódulos extras, isto é equivalente a dizer que cada quociente M_{i+1}/M_i com $0 \leq i \leq n$ é **simples** (i.e., não tem outros submódulos além de 0 e ele mesmo).

Definimos o **comprimento** de M sobre A, denotado por $\ell_A(M)$, como sendo o mínimo entre todos os comprimentos das séries de composição de M ou ∞ se M não admite série de composição.

Exemplo 108. Seja $\mathbf{k}$ um corpo. Um $\mathbf{k}$-espaço vetorial é simples se, e somente se, tem dimensão 1. Assim, uma série de composição para um espaço vetorial V é uma sequência

$$V = V_n \supsetneq V_{n-1} \supsetneq \cdots \supsetneq V_1 \supsetneq V_0 = 0$$

onde $\dim_{\mathbf{k}} V_i = i$. Logo $\ell_{\mathbf{k}}(V) = n = \dim_{\mathbf{k}} V$.

Uma importante caracterização de um módulo simples é dada pelo seguinte lema.

Lema 109. *Um A-módulo M é simples se, e somente se, $M \simeq A/\mathfrak{m}$ (como A-módulos) para algum ideal maximal $\mathfrak{m} \subset A$.*

Demonstração. Se $\mathfrak{m}$ é um ideal maximal de A, então $M = A/\mathfrak{m}$ é simples pelo Teorema da Correspondência versão para Submódulos, pois A-submódulos de $A/\mathfrak{m}$ correspondem a A-submódulos de A (ideais) que contém $\mathfrak{m}$, como $\mathfrak{m}$ é maximal estes ideais são A e $\mathfrak{m}$ e correspondem aos A-submódulos $A/\mathfrak{m}$ e 0 de $A/\mathfrak{m}$, o que implica que $A/\mathfrak{m}$ é simples. Reciprocamente, se M é simples e $m \in M$ é qualquer elemento não nulo então

$M = Am = (m)$. Logo a aplicação $f : A \to M$ dada por $a \mapsto am$ é sobrejetiva é induz um isomorfismo de A-módulos $M \simeq A/\operatorname{Ker}(f)$ e novamente pelo TCS, os A-submódulos de M (0 e M) correspondem aos A-submódulos de A (ideais) que contém $\operatorname{Ker}(f)$, logo os únicos ideais de A que contém $\operatorname{Ker}(f)$ são $\operatorname{Ker}(f)$ e A, logo $\operatorname{Ker}(f)$ deve ser maximal. □

Proposição 110. *Suponha que M tem uma série de composição de comprimento n. Então toda série de composição de M comprimento n e toda cadeia em M pode ser estendida a uma série de composição.*

Demonstração. Dividiremos a prova em quatro partes:

a. Vejamos que se $N \subsetneq M$ então $\ell_A(N) < \ell_A(M)$. Seja (M_i) uma série de composição de M de comprimento minimal, e considere os submódulos $N_i = N \cap M_i$ de N. Como $N_{i+1}/N_i \subseteq M_{i+1}/M_i$ e o último é um módulo simples, temos duas possibilidades $N_{i+1}/N_i = M_{i+1}/M_i$ ou $N_{i+1} = N_i$. Logo removendo os termos repetidos temos uma série de composição de N e logo $\ell_A(N) \leq \ell_A(M)$. Se $\ell_A(N) = \ell_A(M) = n$, então $N_{i+1}/N_i = M_{i+1}/M_i$ para cada $i = 0, \ldots, n-1$. Isto implica que $M_1 = N_1$ e logo $M_2 = N_2, \cdots$, e finalmente $M = N$.

b. Toda cadeia em M tem comprimento $\leq \ell_A(M)$. Seja $M = M_k \supsetneq M_{k-1} \supsetneq \cdots \supsetneq M_0 = 0$ uma cadeia de comprimento k. Então pelo item (a.) temos $\ell_A(M) > \ell_A(M_{k-1}) > \ell_A(M_{k-2}) > \cdots > \ell_A(M_0) = 0$, logo $\ell_A(M) \geq k$.

c. Considere qualquer série de composição de M. Se tem comprimento k então $k \leq \ell_A(M)$ pelo item (b.), mas por definição $\ell_A(M) \leq k$ logo $\ell_A(M) = k$. Segue que toda série de composição tem o mesmo comprimento.

d. Finalmente, considere qualquer cadeia. Se seu comprimento é $\ell_A(M)$ então é uma série de composição por (b.) (suponha que não é então posso insertar pelo menos um submódulo, logo essa cadeia tem comprimento maior que uma série de composição que é uma cadeia maximal, Contradição!). Se se comprimento é $< \ell_A(M)$ não é uma série de composição ou seja não é maximal e por tanto novos termos podem ser inseridos até o comprimento ser $\ell_A(M)$ e, portanto, até chegarmos a uma série de composição.

□

Aula 14

Aula 15

AULA 15: 10/10/2014

Proposição 111. *M tem uma série de composição se, e somente se, M satisfaz ambas condições de cadeia.*

Demonstração. ($\Rightarrow$) Todas as cadeias de M tem comprimento finito, logo ambas condições cca e ccd são satisfeitas.

($\Leftarrow$)Construiremos uma série de composição para M. Temos que M satisfaz a *condição maximal*: "todo subconjunto não vazio de Ω tem um elemento maximal". Em particular Ω, o conjunto de todos os submódulos de M, tem um elemento maximal. Logo M tem um submódulo maximal N, $N \subset M$. Similarmente, se considerarmos o conjunto de todos os submódulos de N, então N tem um submódulo maximal P, $P \subset N \subset M$ e assim por diante. Observe que segue do fato dos submódulos serem maximais que não podem ser insertados submódulos extras, logo os quocientes de módulos consecutivos são simples. Dando continuidade a esse processo obtemos uma cadeia estritamente descendente $M \supset N \supset P \supset \cdots$ que se interrompe pela ccd em $Q = 0$. Então essa cadeia é uma série de composição. □

Observe que a proposição anterior é equivalente a dizer que $\ell_A(M) < \infty$ se, e somente se, M é Artiniano e Noetheriano.

Definição 112. Um módulo que satisfaz ambas condições, cca e ccd, é chamado de **módulo de comprimento finito**.

Analogamente ao caso de grupos finitos podemos aplicar o Teorema de Jordan-Hölder a módulos de comprimento finito:

Teorema 113. (Teorema de Jordan-Hölder) *Seja M um módulo de comprimento finito. Se $(M_i)_{i=0}^n$ e $(M_i')_{i=0}^n$ são duas séries de composição de M então existe uma permutação σ dos índices $1, \ldots, n$ tal que $M_{i+1}/M_i \simeq M'_{\sigma(i)+1}/M'_{\sigma(i)}$ para todo $i = 1, \ldots, n$.*

Demonstração. **Exercício 2.** □

Proposição 114. *Seja $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ uma sequência exata de A-módulos. Então $\ell_A(M) < \infty$ se, e somente se, $\ell_A(M') < \infty$ e $\ell_A(M'') < \infty$. Neste caso $\ell_A(M) = \ell_A(M') + \ell_A(M'')$.*

Demonstração. Pela Proposição (102) temos que M é Noetheriano (resp. Artiniano) se, e somente se, M' e M'' são Noetherianos (resp. Artinianos). Assim pela Proposição (111), M possui comprimento finito se, e somente se, M' e M'' possuem comprimento finito. Sejam agora, $M' = M'_n \supsetneq M'_{n-1} \supsetneq \cdots \supsetneq M'_0 = 0$ e $M'' = M''_k \supsetneq M''_{k-1} \supsetneq \cdots \supsetneq M''_0 = 0$ séries de composição

de M' e M'' respetivamente. Tome a imagem por f da primeira, $(f(M'_i))_{i=0}^n$, e a imagem inversa por g da segunda, $(g^{-1}(M''_i))_{i=0}^k$. Basta combiná-las em uma cadeia de M de tamanho $n+k$:

$$\begin{aligned} M = g^{-1}(M'') = g^{-1}(M''_k) \supsetneq g^{-1}(M''_{k-1}) \supsetneq \cdots \supsetneq g^{-1}(M''_0) = g^{-1}(0) = \mathrm{Ker}(g) \\ = \mathrm{Im}(f) = f(M') = f(M'_n) \supsetneq f(M'_{n-1}) \supsetneq \cdots \supsetneq f(M'_0) = f(0) = 0. \end{aligned}$$

Vejamos que é uma série de composição de M:

a. Vejamos que não tem nenhum termo repetido, ou seja que as inclusões são mesmo estritas: como $M''_i \subsetneq M''_{i+1}$ existe $m''_{i+1} \in M''_{i+1}$ tal que $m''_{i+1} \notin M''_i$. Como g é sobre existe $m \in M$ tal que $g(m) = m''_{i+1}$, logo $m \in g^{-1}(M''_{i+1})$. Suponha que $m \in g^{-1}(M''_i)$ então $m''_{i+1} = g(m) \in M''_i$ o que é uma contradição, logo $g^{-1}(M''_i) \subsetneq g^{-1}(M''_{i+1})$, para cada $i = 0, \ldots, n-1$. Por outro lado, temos que $M'_i \subsetneq M'_{i+1}$ e logo existe $m'_{i+1} \in M'_{i+1}$ tal que $m'_{i+1} \notin M'_i$. Logo $f(m'_{i+1}) \in f(M'_{i+1})$ e suponha que também $f(m'_{i+1}) \in f(M'_i)$, isto implica que existe $m'_i \in M'_i$ tal que $f(m'_{i+1}) = f(m'_i)$. Como f é injetiva segue que $m'_{i+1} = m'_i \in M'_i$ o que é uma contradição. Logo $f(M'_i) \subsetneq f(M'_{i+1})$, para cada $i = 0, \ldots, n-1$.

b. Vejamos que a cadeia é maximal, ou seja que os quocientes de termos consecutivos são simples. Defina a aplicação sobrejetora g_i como sendo a composição das aplicações $g^{-1}(M''_{i+1}) \overset{g}{\twoheadrightarrow} M''_{i+1} \overset{\pi}{\twoheadrightarrow} M''_{i+1}/M''_i$ (onde a primeira aplicação é a restrição de g a $g^{-1}(M''_{i+1})$ e é sobre pois satisfaz $g(g^{-1}(M''_{i+1})) = M''_{i+1}$ pois g é sobre). Agora $m \in \mathrm{Ker}(g_i) \Leftrightarrow g(m) \in M''_i \Leftrightarrow m \in g^{-1}(M''_i)$, logo pelo teorema de isomorfismos $\frac{g^{-1}(M''_{i+1})}{g^{-1}(M''_i)} \simeq \frac{M''_{i+1}}{M''_i}$ como este último é simples temos que os quocientes $\frac{g^{-1}(M''_{i+1})}{g^{-1}(M''_i)}$ são simples.

   Por outro lado, defina a aplicação sobrejetora f_i como sendo a composição das aplicações $M'_{i+1} \overset{f}{\twoheadrightarrow} f(M'_{i+1}) \overset{\pi}{\twoheadrightarrow} f(M'_{i+1})/f(M'_i)$ (onde a primeira aplicação é a restrição de f a M'_{i+1} e é claramente sobre). Agora $m' \in \mathrm{Ker}(f_i) \Leftrightarrow f(m') \in f(M'_i) \Leftrightarrow m' \in f^{-1}(f(M'_i)) = M'_i$ pois f é injetiva, logo pelo teorema de isomorfismos $\frac{f(M'_{i+1})}{f(M'_i)} \simeq \frac{M'_{i+1}}{M'_i}$ como este último é simples temos que os quocientes $\frac{f(M'_{i+1})}{f(M'_i)}$ são simples.

□

5.1 ANÉIS NOETHERIANOS

Recordamos que um anel A é dito **Noetheriano** se satisfaz as seguintes três condições equivalentes:

a. Todo conjunto não vazio de ideais de A tem um elemento maximal (condição maximal).

b. Toda cadeia ascendente de ideais de A é estacionária (cca).

c. Todo ideal de A é f.g.

Vimos na aula passada que:

Proposição. *Seja A um anel Noetheriano.*

a. Se M um A-módulo f.g., então M é Noetheriano.

b. Se I um ideal de A, então A/I é um anel Noetheriano.

Provaremos que a propriedade de ser "Noetheriano" é preservada por várias outras operações.

Proposição 115. *Se A é um anel Noetheriano e $\phi : A \to B$ é um homomorfismo de anéis sobrejetor, então B é Noetheriano.*

Demonstração. Como $B \simeq A/\operatorname{Ker}(\phi)$ segue da Proposição 107 (item *b.*) que B é um anel Noetheriano. □

Proposição 116. *Seja A um subanel de B; suponha que A é Noetheriano e que B é f.g. como um A-módulo. Então B é Noetheriano como anel.*

Demonstração. Como A é um subanel de B, podemos considerar B junto com o homomorfismo inclusão como um A-módulo. Segue da Proposição 106 (item *a.*) que B é Noetheriano como um A-módulo. Mas os ideais B são B-submódulos de B por tanto também são A-submódulos de B e por tanto toda cadeia de ideais de B estabiliza-se, logo B é Noetheriano como anel. □

Proposição 117. *Se A é um anel Noetheriano e S um conjunto multiplicativo de A, então $S^{-1}A$ é Noetheriano.*

Demonstração. Pelo Teorema 98 item (a.) um ideal de $S^{-1}A$ é da forma $S^{-1}I$ para algum ideal I de A. Se I é f.g., digamos $I = \langle a_1, \ldots, a_n \rangle$ então $S^{-1}I$ também é f.g. por $\frac{a_1}{1}, \ldots, \frac{a_n}{1}$. Assim A Noetheriano implica $S^{-1}A$ Noetheriano. □

Corolário 118. *Se A é Noetheriano e $\mathfrak{p}$ é um ideal primo de A, então $A_{\mathfrak{p}}$ é Noetheriano.*

Agora sim estamos em condições de provar que conjuntos algébricos podem ser sempre definidos por um número finito de polinômios.

Lembrando: Dado um subconjunto $S \subseteq \mathbf{k}[x_1, \ldots, x_n]$, na Seção 2.2, definimos um conjunto algébrico como sendo o subconjunto $Z(S) \subseteq \mathbb{A}^n_{\mathbf{k}}$ dos zeros

comuns de todos os polinômios em S e provamos que se $I \subseteq \mathbf{k}[x_1, \ldots, x_n]$ é o ideal gerado por S, então $Z(S) = Z(I)$. Assim podemos definir um conjunto algébrico como o conjunto de zeros de um ideal. Provaremos agora que todo ideal de $\mathbf{k}[x_1, \ldots, x_n]$ é finitamente gerado e assim todo conjunto algébrico é o conjunto de zeros de um número *finito* de polinômios. Mais geralmente, provaremos que:

Teorema 119. (Teorema da Base de Hilbert) *Se A é Noetheriano, então o anel de polinômios $A[x]$ é Noetheriano.*

Demonstração. Seja I um ideal em $A[x]$, vamos mostrar que I é f.g. Seja $J_0 = I \cap A$ vejamos que J_0 é um ideal de A:

a. Se $a, b \in J_0$ então $a, b \in I$ e $a, b \in A$ logo $a + b \in I \cap A = J_0$;

b. Se $a \in J_0$ e $r \in A$ então $a \in I$, $a \in A$ e $r \in A \subset A[x]$ logo $ra \in I \cap A = J_0$.

Como A é Noetheriano J_0 é f.g., sejam $a_1, \ldots, a_n$ os geradores. Seja $I_0 = J_0 A[x]$ o ideal de $A[x]$ gerado por J_0. Agora, se $y \in I_0$ então $y = \sum_{i=1}^{l} f_i(x) j_i$, com $j_i \in J_0$ e $f_i(x) \in A[x]$. Logo $j_i = \sum_{k=1}^{n} a_k b_k^i$, com $b_k^i \in A$, assim $y = \sum_{i=1}^{l} f_i(x)(\sum_{k=1}^{n} a_k b_k^i) = \sum_{k=1}^{n}(\sum_{i=1}^{l} f_i(x) b_k^i) a_k$ onde $\sum_{i=1}^{l} f_i(x) b_k^i \in A[x]$, logo I_0 é f.g em $A[x]$ pelos $a_1, \ldots, a_n$.

Temos duas possibilidades:

a. ou $I_0 = I$ e logo I é f.g.;

b. ou $I_0 \neq I$, logo $I_0 \subsetneq I$. Seja $g \in I - I_0$ tal que o grau de g é minimal em I. Então se $g = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_0$ temos que $b_m \notin J_0$ (pois se $b_m \in J_0$ então $b_m x^m \in I_0$ e logo $g - b_m x^m \notin I_0$ contradição pois o grau de g é minimal). Seja então $J_1 = \langle J_0, b_m \rangle$ o ideal de A gerado por J_0 e b_m e seja $I_1 = J_1 A[x]$ o ideal de $A[x]$ gerado por J_1, analogamente ao caso anterior como J_1 é f.g. em A também I_1 é f.g. em $A[x]$. Novamente temos dois casos:

   a) ou $I_1 = I$ e logo I é f.g.;

   b) ou $I_1 \neq I$ e repetimos o processo obtendo, assim, uma cadeia ascendente $J_0 \subsetneq J_1 \subsetneq J_2 \subsetneq \cdots$ de ideais de A e logo, como A é Noetheriano, essa cadeia é estacionária, ou seja existe N tal que $J_N = J_{N+1} = \cdots$. Logo $J_N = \langle J_{N-1}, c_N \rangle = \langle J_N, c_{N+1} \rangle = J_{N+1}$ o que implica que $c_{N+1} \in J_N$. Suponha então que $I_N \neq I$ então, seguindo o raciocínio anterior, existe $g' \in I - I_N$ tal que o grau de g' é minimal em I e tal que c_{N+1} é o coeficiente líder de g', mas isto implica que $c_{N+1} \notin J_N$, o que é uma contradição. Logo $I_N = I$ e portanto I é f.g.

□

Corolário 120. *Se A é Noetheriano então $A[x_1, \ldots, x_n]$ é Noetheriano.*

Demonstração. Segue do teorema anterior por indução em n. □

Note que também é verdade que se A é Noetheriano então o anel das séries de potências formais em x com coeficientes em A, $A[[x]]$, é Noetheriano. A prova é análoga, excepto que deve ser considerado o coeficiente do termo de menor grau. **(Exercício 3.)**

Corolário 121. *Seja B uma A-álgebra f.g. Se A é Noetheriano, então também o é B. Em particular, todo anel e toda álgebra f.g. sobre um corpo são Noetherianos.*

Demonstração. Lembramos a definição de A-álgebra f.g. (Aula 9, logo após a Definição 76): $f : A \to B$ é uma A-álgebra f.g. se existe um conjunto finito de elementos $b_1, \ldots, b_n \in B$ tal que todo elemento de B pode ser escrito como um polinômio em $b_1, \ldots, b_n$ com coeficientes em $f(A)$, ou equivalentemente, se existe um homomorfismo de A-álgebras sobrejetor do anel dos polinômios $A[x_1, \ldots, x_n]$ em B. Esse homomorfismo $A[x_1, \ldots, x_n] \twoheadrightarrow B$ é dado por $x_i \mapsto b_i$. Como o anel de polinômios $A[x_1, \ldots, x_n]$ que é Noetheriano pelo Teorema da Base de Hilbert (Teorema 119), segue da Proposição 115 que B é um anel Noetheriano. □

AULA 16: 15/10/2014

AULA 16

5.2 ANÉIS ARTINIANOS

Recordamos que um anel A é dito **Artiniano** se satisfaz uma das seguintes condições equivalentes:

a. Todo conjunto não vazio de ideais de A tem um elemento minimal (condição minimal).

b. Toda cadeia descendente de ideais de A é estacionária (ccd).

Proposição 122. *Em um anel Artiniano A todo ideal primo é maximal. Isto é* $\mathrm{Spec}(A) = \mathrm{Specm}(A)$.

Demonstração. Seja $\mathfrak{p}$ um ideal primo de A. Então $B = A/\mathfrak{p}$ é um domínio de integridade Artiniano (pela Proposição 107). Seja $b \in B$, $b \neq 0$, então pela ccd temos que $(b^n) = (b^{n+1})$ para algum n e logo $b^n = b^{n+1}x$ para algum $x \in B$. Logo $b^n(1 - bx) = 0$, como B é um domínio e $b \neq 0$ segue $bx = 1$. Ou seja b tem um inverso em B, e portanto B é um corpo o que implica que $\mathfrak{p}$ é um ideal maximal. □

Corolário 123. *Em um anel Artiniano o nilradical $\mathfrak{N}$ é igual ao radical de Jacobson $\mathfrak{R}$.*

Lembramos uma proposição provada na Aula 3 (também é o Exercício 13 da Lista 1) que usaremos na prova da Proposição seguinte:

Proposição. *Sejam $I_1, \ldots, I_n$ ideais e seja $\mathfrak{p}$ um ideal primo contendo $\bigcap_{i=1}^{n} I_i$. Então $\mathfrak{p} \supseteq I_i$ para algum i.*

Proposição 124. *Um anel Artiniano $A \neq 0$ tem somente um número finito de ideais maximais.*

Demonstração. Considere o conjunto de todos os ideais do anel A que são interseções finitas $\mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_r$ de ideais maximais. Como A é Artiniano e este conjunto é não vazio (pois A tem pelo menos um ideal maximal) ele tem um elemento minimal: $I = \mathfrak{m}_1 \cap \mathfrak{m}_2 \cap \cdots \cap \mathfrak{m}_n$. Logo para qualquer ideal maximal $\mathfrak{m}$ temos que $\mathfrak{m} \cap I$ é uma interseção finita de ideais maximais que está contida em I, logo $\mathfrak{m} \cap I = I$ pela minimalidade de I, o que implica que $\mathfrak{m} \supseteq I$. Pela Proposição 29 temos que $\mathfrak{m} \supseteq \mathfrak{m}_i$ para algum i, e logo $\mathfrak{m} = \mathfrak{m}_i$ pois $\mathfrak{m}_i$ é maximal. □

Proposição 125. *Em um anel Artiniano o nilradical $\mathfrak{N}$ (e logo também o radical de Jacobson $\mathfrak{R}$) é nilpotente.*

Demonstração. Como as potências de $\mathfrak{N}$ formam uma cadeia descendente de ideais, pela ccd, temos que existe um $k > 0$ tal que $\mathfrak{N}^k = \mathfrak{N}^{k+1} = \cdots = I$. Suponha que $I \neq 0$ e seja Ω o conjunto de todos os ideais J de A tais que $IJ \neq 0$. Então Ω é não vazio pois $I \in \Omega$ ($I^2 = \mathfrak{N}^{2k} = I \neq 0$). Seja K o elemento minimal de Ω, então existe $x \in K$ tal que $xI \neq 0$ mas $(x) \subseteq K$ logo $(x) = K$ pela minimalidade de K. Mas $(xI)I = xI^2 = xI \neq 0$ e $xI \subseteq (x)$, logo $xI = (x)$. Isto implica que existe $y \in I$ tal que $xy = x$ e por tanto $x = xy = xy^2 = \cdots = xy^n = \cdots$, mas $y \in I = \mathfrak{N}^k \subseteq \mathfrak{N}$ e logo y é nilpotente o que implica $x = xy^n = 0$. Isto contradiz a escolha do x e portanto $I = 0$. □

Definição 126. Definimos uma **cadeia de ideais primos** de um anel A como sendo uma sequência estritamente crescente e finita $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ onde cada $\mathfrak{p}_i$ é um ideal primo de A. O **comprimento** da cadeia é n. Definimos a **dimensão** de um anel $A \neq 0$ como sendo o supremo dos comprimentos de todas as cadeias de ideais primos de A.

Assim, por exemplo um corpo tem dimensão 0 e um DIP tem dimensão 1, pois em um DIP (0) é um ideal primo e os ideais primos não nulos são maximais (Proposição 22) ou seja se $(0) \subsetneq (p) \subseteq (p_1)$ é uma cadeia de primos isto implica que $(p) = (p_1)$. Logo todas as cadeias de primos de um DIP têm comprimento ≤ 1.

Corolário 127. *Seja A um anel Artiniano então* $\dim A = 0$.

Demonstração. Segue do fato de que em um anel Artiniano todo ideal primo é maximal (Proposição 122) e logo toda cadeia de primos de A tem comprimento 0. □

5.3 EXERCÍCIOS

Ex. 52 — Seja $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ uma sequência exata de A-módulos. Mostre que M é Artiniano se, e somente se, M' e M'' são Artinianos.

Ex. 53 — (Teorema de Jordan-Hölder) Seja M um módulo de comprimento finito. Se $(M_i)_{i=0}^n$ e $(M_i')_{i=0}^n$ são duas séries de composição de M mostre que existe uma permutação σ dos índices $1, \ldots, n$ tal que $M_{i+1}/M_i \simeq M'_{\sigma(i)+1}/M'_{\sigma(i)}$ para todo $i = 1, \ldots, n$.

Ex. 54 — Mostre que se A é Noetheriano então $A[[x]]$ é Noetheriano.

Ex. 55 — Mostre que para o caso particular de módulos sobre um corpo $\mathbf{k}$, i.e., $\mathbf{k}$-espaços vetoriais V as seguintes condições são equivalentes: V tem dimensão finita $\Leftrightarrow$ V tem comprimento finito $\Leftrightarrow$ V é Noetheriano $\Leftrightarrow V$ é Artiniano.

Ex. 56 — Prove que $\mathbb{Z}[i]$, o anel dos inteiros Gaussianos, é um anel Noetheriano.

Ex. 57 — Mostre que A é um anel Artiniano e um domínio se, e somente se, A é um corpo.

Ex. 58 — Seja M um A-módulo Noetheriano. Se todo conjunto não vazio de submódulos f.g. de M tem um elemento maximal, mostre que M é Noetheriano.

Ex. 59 — Um espaço topológico X é dito **Noetheriano** se os subconjuntos abertos de X satisfazem a cca ou, equivalentemente, se os subconjuntos fechados de X satisfazem a ccd. Mostre que:

1. Se A é um anel Noetheriano então $\mathrm{Spec}(A)$ é um espaço topológico Noetheriano.
2. Se A é um anel qualquer, então $\mathrm{Spec}(A)$ é um espaço Noetheriano se, e somente se, o conjunto de ideias primos de A satisfaz a cca.

Ex. 60 — Seja A um anel Noetheriano. Mostre que:

1. Todo ideal $I \subseteq A$ contém um produto finito de ideais primos.
2. A possui apenas um número finito de ideais primos minimais.

Ex. 61 — Seja M um A-módulo Noetheriano e $f : M \to M$ um homomorfismo de A-módulos sobrejetor. Mostre que f é um isomorfismo.

Ex. 62 — Seja M um A-módulo Artiniano e $f : M \to M$ um homomorfismo de A-módulos injetor. Mostre que f é um isomorfismo.

Ex. 63 — Seja A um anel tal que:

1. o anel local $A_{\mathfrak{m}}$ é Noetheriano para todo $\mathfrak{m} \in \mathrm{Specm}(A)$ e
2. para cada $a \neq 0$ em A, o conjunto de ideais maximais de A que contém a é finito.
   Mostre que A é Noetheriano.

Ex. 64 — Prove que se todos os elementos de $\mathrm{Spec}(A)$ são f.g. então o anel A é Noetheriano.

Ex. 65 — Prove que um domínio Noetheriano A é um DIP se, e somente se, todos seus ideais primos são principais.

6

DECOMPOSIÇÃO PRIMÁRIA

A decomposição primária de um ideal é nada mais que a generalização da fatoração de um inteiro como produto de potências de números primos. Um ideal primo de um anel A é, em algum sentido, a generalização de um número primo. A correspondente generalização de uma potência de um número primo é um ideal *"primário"*:

Definição 128. Um ideal $\mathfrak{q}$ em um anel A é **primário** se $\mathfrak{q} \neq A$ e se $ab \in \mathfrak{q}$ então ou $a \in \mathfrak{q}$ ou $b^n \in \mathfrak{q}$ para algum $n > 0$.

Em outras palavras, $\mathfrak{q}$ é primário se, e somente se, $A/\mathfrak{q} \neq 0$ e todo divisor de zero em $A/\mathfrak{q}$ é nilpotente.

Segue que todo ideal primo (e maximal) é primário.

Proposição 129. *Seja $\mathfrak{q}$ um ideal primário em um anel A. Então $\sqrt{\mathfrak{q}}$ é o menor ideal primo de A contendo $\mathfrak{q}$.*

Demonstração. Como $\sqrt{\mathfrak{q}}$ é a interseção de todos os ideais primos de A que contêm $\mathfrak{q}$ (Proposição 28, Aula 3), é suficiente provar que $\sqrt{\mathfrak{q}}$ é primo. Sejam $ab \in \sqrt{\mathfrak{q}}$, então existe $m > 0$ tal que $(ab)^m \in \mathfrak{q}$. Como $\mathfrak{q}$ é primário ou $a^m \in \mathfrak{q}$ ou $b^{mn} \in \mathfrak{q}$ para algum $n > 0$, i.e. ou $a \in \sqrt{\mathfrak{q}}$ ou $b \in \sqrt{\mathfrak{q}}$. □

Se $\mathfrak{q}$ é primário e $\mathfrak{p} = \sqrt{\mathfrak{q}}$ então dizemos que $\mathfrak{q}$ é **$\mathfrak{p}$-primário**.

Exemplo 130.

a. Os ideais primários de $\mathbb{Z}$ são (0) e (p^n), onde p é um número primo.

b. Seja $A = \mathbf{k}[x, y]$ e $\mathfrak{q} = (x, y^2)$. Então $A/\mathfrak{q} \simeq \mathbf{k}[y]/(y^2)$ neste anel os divisores de zero são os múltiplos de y e logo são nilpotentes. Segue que $\mathfrak{q}$ é primário e seu radical $\mathfrak{p}$ é (x, y). Temos então que $\mathfrak{p}^2 \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$ logo um ideal primário não é necessariamente uma potência de um primo.

Proposição 131. *Se $\sqrt{I}$ é maximal, então I é primário. Em particular, as potências de um ideal maximal $\mathfrak{m}$ são $\mathfrak{m}$-primárias.*

Demonstração. Seja $\mathfrak{m} = \sqrt{I}$. Se $\pi : A \to A/I$ é o homomorfismo projeção, então segue do Exercício 16.2 da Lista 1 que $\sqrt{I} = \pi^{-1}(\mathfrak{N}_{A/I})$, ou seja a imagem de $\mathfrak{m}$ em A/I é o nilradical de A/I e logo $\mathfrak{N}_{A/I}$ é maximal. Assim dado um ideal primo $\mathfrak{p}$ de A/I segue que $\mathfrak{N}_{A/I} \subseteq \mathfrak{p}$ o que implica $\mathfrak{N}_{A/I} = \mathfrak{p}$ e logo o anel A/I tem somente um ideal primo. Então todo elemento de

A/I ou é uma unidade ou é nilpotente (Exercício 18 Lista 1), e logo todo divisor de zero de A/I é nilpotente. Isto implica que I é primário. Por outro lado se $\mathfrak{m}$ é maximal (logo primo) $\mathfrak{m} = \sqrt{\mathfrak{m}^n}$ para todo $n > 0$ (Exercício 16.5 Lista 1), logo $\mathfrak{m}^n$ é $\mathfrak{m}$-primário para todo $n > 0$. □

Por outro lado, as potências de um ideal primo não necessariamente são primárias: no anel $A = \mathbf{k}[x, y, z]/(z^2 - xy)$ o ideal $p = (\overline{x}, \overline{z})$ é primo mas p^2 não é primário.

Estudaremos a seguir presentações de um ideal como uma interseção de ideais primários. Mas antes, enunciaremos um par de lemas técnicos:

Lema 132. *Se $\mathfrak{q}_i$ com $1 \leq i \leq n$ são $\mathfrak{p}$-primários então $\mathfrak{q} = \cap_{i=1}^n \mathfrak{q}_i$ é $\mathfrak{p}$-primário.*

Demonstração. $\sqrt{\mathfrak{q}} = \sqrt{\cap_{i=1}^n \mathfrak{q}_i} \overset{\text{Ex16.4 L1}}{=} \cap_{i=1}^n \sqrt{\mathfrak{q}_i} = \mathfrak{p}$. Seja $xy \in \mathfrak{q}$ e suponha que $y \notin \mathfrak{q}$, então para algum i temos que $xy \in \mathfrak{q}_i$ e $y \notin \mathfrak{q}_i$, logo $x \in \mathfrak{p} = \sqrt{\mathfrak{q}_i} = \sqrt{\mathfrak{q}}$ (pois $\mathfrak{q}_i$ é $\mathfrak{p}$-primário) e logo $\mathfrak{q}$ é $\mathfrak{p}$-primário. □

Lema 133. *Seja $\mathfrak{q}$ um ideal $\mathfrak{p}$-primário e a um elemento de A. Então:*

a. Se $a \in \mathfrak{q}$ então $(\mathfrak{q} : a) = A$.

b. Se $a \notin \mathfrak{q}$ então $(\mathfrak{q} : a)$ é $\mathfrak{p}$-primário.

c. Se $a \notin \mathfrak{p}$ então $(\mathfrak{q} : a) = \mathfrak{q}$.

Demonstração. Como $(\mathfrak{q} : a) := \{b \in A \mid ab \in \mathfrak{q}\}$, o primeiro item segue da definição. Para o segundo, se $b \in (\mathfrak{q} : a)$ então $ab \in \mathfrak{q}$ e logo, como $a \notin \mathfrak{q}$, temos que $b \in \mathfrak{p}$. Logo $\mathfrak{q} \subseteq (\mathfrak{q} : a) \subseteq \mathfrak{p}$, tomando radicais ($\sqrt{\ }$ preserva inclusões e $\sqrt{\sqrt{I}} = \sqrt{I}$ Ex. 16 Lista 1) temos $\sqrt{(\mathfrak{q} : a)} = \mathfrak{p}$. Seja agora $bc \in (\mathfrak{q} : a)$ e suponha que $b \notin \mathfrak{p}$, então $abc \in \mathfrak{q}$ logo $ac \in \mathfrak{q}$ o que implica que $c \in (\mathfrak{q} : a)$. Logo $(\mathfrak{q} : a)$ é $\mathfrak{p}$-primário. No terceiro item, como $a \notin \mathfrak{p}$ então se $b \in (\mathfrak{q} : a)$ então $ab \in \mathfrak{q}$ logo $b \in \mathfrak{q}$. □

Definição 134. Uma **decomposição primária** de um ideal I de A é uma expressão de I como uma interseção finita de ideais primários, $I = \cap_{i=1}^n \mathfrak{q}_i$.

Note que em geral, uma tal decomposição primária não precisa existir. Diremos que um ideal I é **decomponível** se I admite uma decomposição primária.

Se um ideal I for decomponível e ainda:

a. todos os $\sqrt{\mathfrak{q}_i}$ são distintos, e

b. temos que $\cap_{j \neq i} \mathfrak{q}_j \nsubseteq \mathfrak{q}_i$ para $1 \leq i \leq n$

a decomposição primária é dita **minimal**. Em vista do Lema 132, podemos interceptar todos os ideais $\mathfrak{p}$-primários e obter um novo ideal $\mathfrak{p}$-primário tendo assim a condição (a.) satisfeita sem mudar a decomposição de I, feito isso podemos omitir qualquer termo supérfluo para obter a condição (b.) da seguinte forma: suponha que $\cap_{j\neq i}\mathfrak{q}_j \subseteq \mathfrak{q}_i$ então $\cap_{j\neq i}\mathfrak{q}_j = \cap_j \mathfrak{q}_j = I$, então podemos tirar $\mathfrak{q}_i$. Logo toda decomposição primária pode ser reduzida a uma minimal.

AULA 17: 17/10/2014

AULA 17

Lembrando a última aula. Provamos que:

Lema.

a. *Se $\mathfrak{q}_i$ com $1 \leq i \leq n$ são $\mathfrak{p}$-primários então $\mathfrak{q} = \cap_{i=1}^n \mathfrak{q}_i$ é $\mathfrak{p}$-primário.*

b. *Seja $\mathfrak{q}$ um ideal $\mathfrak{p}$-primário e $a \in A$. Então:*

   a) Se $a \in \mathfrak{q}$ então $(\mathfrak{q} : a) = A$.

   b) Se $a \notin \mathfrak{q}$ então $(\mathfrak{q} : a)$ é $\mathfrak{p}$-primário.

   c) Se $a \notin \mathfrak{p}$ então $(\mathfrak{q} : a) = \mathfrak{q}$.

Definimos uma decomposição primária de um ideal I como sendo uma expressão $I = \cap_{i=1}^n \mathfrak{q}_i$, onde os $\mathfrak{q}_i$ são primários. Diremos que I é decomponível se I admite uma decomposição primária. Neste se caso, se

a. todos os $\sqrt{\mathfrak{q}_i}$ são distintos, e

b. temos que $\cap_{j\neq i}\mathfrak{q}_j \nsubseteq \mathfrak{q}_i$ para $1 \leq i \leq n$

a decomposição primária é dita **minimal**. E observamos que, em vista do Lema anterior, toda decomposição primária pode ser reduzida a uma minimal.

Teorema 135. (1º Teorema de Unicidade) *Seja I um ideal decomponível e seja $I = \cap_{i=1}^n \mathfrak{q}_i$ uma decomposição primária minimal de I. Seja $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$ para $1 \leq i \leq n$. Então os $\mathfrak{p}_i$'s são precisamente os ideais primos que ocorrem no conjunto de ideais $\sqrt{(I : a)}$ com $a \in A$, e portanto não dependem da decomposição particular de I.*

Demonstração. Para cada $a \in A$ temos $(I : a) = (\cap_{i=1}^n \mathfrak{q}_i : a) = \cap_{i=1}^n (\mathfrak{q}_i : a)$ (Ex. 20.3 L1), logo $\sqrt{(I : a)} = \cap_{i=1}^n \sqrt{(\mathfrak{q}_i : a)} = \cap_{a\notin \mathfrak{q}_j} \mathfrak{p}_j$ (Ex. 16.4 L1 e Lema 133) . Suponha que $\sqrt{(I : a)}$ seja primo então, segue da Proposição 29 (Lembrando: Se $\mathfrak{p} = \bigcap_{i=1}^n I_i$ então $\mathfrak{p} = I_i$ para algum i), que $\sqrt{(I : a)} = \mathfrak{p}_j$ para algum j. Logo todo ideal primo da forma $\sqrt{(I : a)}$ é um dos $\mathfrak{p}_j$. Reciprocamente, para cada i existe $a_i \notin \mathfrak{q}_i$ e $a_i \in \cap_{j\neq i}\mathfrak{q}_j$ pois a decomposição é minimal, logo temos que $\sqrt{(I : a_i)} = \mathfrak{p}_i$. □

Note que não é verdade que todas as componentes primárias são independentes da decomposição. Por exemplo, $(x^2, xy) = (x) \cap (x^2, y) = (x) \cap (x, y)^2$ são duas decomposições primárias minimais distintas.

Da prova anterior, temos que para cada i existe $a_i \in A$ tal que $a_i \notin \mathfrak{q}_i$ e $a_i \in \cap_{j \neq i} \mathfrak{q}_j$ assim $(I, a_i) = \cap_{j=1}^n (\mathfrak{q}_j : a_i) = (\mathfrak{q}_i : a_i)$ pois pelo lema anterior $(\mathfrak{q}_j : a_i) = A$ para todo $j \neq i$ e logo (também pelo lema anterior) (I, a_i) é $\mathfrak{p}_i$-primário.

Dizemos que os ideais primos $\mathfrak{p}_i$ do 1º Teorema de Unicidade (Teorema 135) são **associados** a I, e os denotaremos por $\text{Assoc}(I) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. Segue que um ideal I é primário se, e somente se, ele tem um único ideal primo associado.

Os elementos minimais do conjunto $\text{Assoc}(I)$ são chamados de ideais primos **isolados** de I, i.e., um ideal primo $\mathfrak{p} \in \text{Assoc}(I)$ é isolado se sempre que exista $\mathfrak{p}' \in \text{Assoc}(I)$ tal que $\mathfrak{p}' \subseteq \mathfrak{p}$ então $\mathfrak{p}' = \mathfrak{p}$. Ideais primos de $\text{Assoc}(I)$ que não são isolados são chamados de **embutidos**. Ou seja, um ideal primo $\mathfrak{p} \in \text{Assoc}(I)$ é embutido se existe um ideal primo $\mathfrak{p}' \in \text{Assoc}(I)$ tal que $\mathfrak{p}' \subsetneq \mathfrak{p}$. Segue do fato de $\text{Assoc}(I)$ ser finito que todo ideal embutido contém um ideal isolado.

Proposição 136. *Seja I um ideal decomponível. Então todo ideal primo $\mathfrak{p} \supseteq I$ contém um ideal primo isolado associado a I. Logo os ideais primos isolados de I são precisamente os elementos minimais do conjunto $V(I)$.*

Demonstração. Se $\mathfrak{p} \supseteq I = \cap_{i=1}^n \mathfrak{q}_i$ então $\mathfrak{p} = \sqrt{\mathfrak{p}} \supseteq \cap_{i=1}^n \sqrt{\mathfrak{q}_i} = \cap_{i=1}^n \mathfrak{p}_i$. Logo temos que $\mathfrak{p} \supseteq \mathfrak{p}_i$ para algum i e portanto $\mathfrak{p}$ contém um ideal primo isolado de I. Por outro lado temos que, como $I = \cap_{i=1}^n \mathfrak{q}_i$ então $I \subseteq \sqrt{I} = \cap_{i=1}^n \mathfrak{p}_i \subseteq \mathfrak{p}_i$ para todo $i = 1, \ldots, n$. Logo $\mathfrak{p}_i \in V(I)$ para todo $i = 1, \ldots, n$. Ou seja $\text{Assoc}(I) \subseteq V(I)$. Vejamos que os isolados de I são os elementos minimais de $V(I)$. Seja $\mathfrak{p}_i$ ideal isolado de I, suponha que existe em $V(I)$ um ideal primo $\mathfrak{p}$ de A tal que $\mathfrak{p} \subseteq \mathfrak{p}_i$. Pela primeira parte desta proposição existe um ideal isolado $\mathfrak{p}_j$ tal que $\mathfrak{p}_j \subseteq \mathfrak{p} \subseteq \mathfrak{p}_i$, mas como $\mathfrak{p}_i$ é isolado temos que $\mathfrak{p}_i = \mathfrak{p}_j$ e portanto $\mathfrak{p} = \mathfrak{p}_i$. Logo $\mathfrak{p}_i$ é um elemento minimal de $V(I)$. Seja agora $\mathfrak{p}$ um elemento minimal de $V(I)$, novamente existe um isolado $\mathfrak{p}_i$ tal que $\mathfrak{p}_i \subseteq \mathfrak{p}$ mas $\mathfrak{p}_i \in V(I)$ logo pela minimalidade de $\mathfrak{p}$ devemos ter $\mathfrak{p} = \mathfrak{p}_i$. □

Exemplo 137. Queremos achar os ideais primos minimais de $A = \mathbb{C}[x, y]/(x^2, xy)$. Pelo TCI os ideais primos minimais de A correspondem aos ideais primos minimais de $\mathbb{C}[x, y]$ que contém (x^2, xy), i.e., correspondem aos elementos minimais do conjunto $V(x^2, xy)$. Segue da proposição anterior que estes elementos são os ideais isolados de (x^2, xy). Seja $(x^2, xy) = (x) \cap (x, y)^2$ uma decomposição primária minimal qualquer de (x^2, xy) (Verifique), então os ideais primos associados são:

a. $\sqrt{(x)} = (x)$ pois (x) é primo por ser x irredutível no DFU $\mathbb{C}[x, y]$.

b. $\sqrt{(x,y)^2} = (x,y)$ pois (x,y) é um ideal maximal de $\mathbb{C}[x,y]$ (Nullstellensatz Hilbert, Teorema 46) e toda potência de um maximal $\mathfrak{m}$ é $\mathfrak{m}$-primário (Proposição 131).

Logo $\text{Assoc}(x^2, xy) = \{(x), (x,y)\}$ como $(x) \subsetneq (x,y)$ temos que o único ideal isolado de (x^2, xy) é (x). Logo $(\overline{x})$ é o único ideal primo minimal de $\mathbb{C}[x,y]/(x^2, xy)$.

Proposição 138. *Seja I um ideal decomponível e $I = \cap_{i=1}^n \mathfrak{q}_i$ uma decomposição primária minimal com $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. Então $\cup_{i=1}^n \mathfrak{p}_i = \{a \in A \mid (I : a) \neq I\}$.*

Demonstração. **(Exercício 1.)** □

Logo, no caso em que o ideal zero é decomponível temos que o conjunto dos divisores de zero $D = \cup$ todos os ideais primos associados a (0) e o nilradical $\mathfrak{N} = \cap$ todos os primos isolados associados a (0). **(Exercício 2.)**

A seguinte proposição resume o comportamento de ideais primários sob localização.

Proposição 139. *Seja S um subconjunto multiplicativo de A e seja $\mathfrak{q}$ um ideal $\mathfrak{p}$-primário.*

a. Se $S \cap \mathfrak{p} \neq \emptyset$, então $S^{-1}\mathfrak{q} = S^{-1}A$.

b. Se $S \cap \mathfrak{p} = \emptyset$, então $S^{-1}\mathfrak{q}$ é $S^{-1}\mathfrak{p}$-primário.

Demonstração. Se $s \in S \cap \mathfrak{p}$ então existe $n > 0$ tal que $s^n \in S \cap \mathfrak{q}$. Logo $S^{-1}\mathfrak{q}$ contém o elemento $\frac{s^n}{1}$ que é uma unidade de $S^{-1}A$ (é uma das três propriedades do mapa de localização (Aula 10): Se $s \in S$ então $\rho(s)$ é uma unidade em $S^{-1}A$). Para o segundo item observe que $\sqrt{S^{-1}\mathfrak{q}} = S^{-1}(\sqrt{\mathfrak{q}}) = S^{-1}\mathfrak{p}$ (Ex. 6 Lista 4) e como $S \cap \mathfrak{p} = \emptyset$ segue que $S^{-1}\mathfrak{p}$ é de fato um ideal primo de $S^{-1}A$ (Teorema 98: os ideais primos de $S^{-1}A$ estão em correspondência um-a-um com os ideais primos de A que não interceptam S). Suponha agora que $\frac{a}{s}\frac{b}{t} \in S^{-1}\mathfrak{q}$, logo existe um $q \in \mathfrak{q}$ e $s' \in S$ tal que $\frac{ab}{st} = \frac{q}{s'}$ por tanto existe $t' \in S$ tal que $t'(abs' - stq) = 0$. Logo $t'abs' = t'stq \in \mathfrak{q}$, como $\mathfrak{q}$ é primário ou $ab \in \mathfrak{q}$ ou $t's' \in \mathfrak{p}$, mas por hipótese $S \cap \mathfrak{p} = \emptyset$ logo $ab \in \mathfrak{q}$. Isto implica que ou $a \in \mathfrak{q}$ ou $b \in \mathfrak{p}$ e portanto ou $\frac{a}{s} \in S^{-1}\mathfrak{q}$ ou $\frac{b}{t} \in S^{-1}\mathfrak{p} = \sqrt{S^{-1}\mathfrak{q}}$. Logo $S^{-1}\mathfrak{q}$ é $S^{-1}\mathfrak{p}$-primário. □

Proposição 140. *Seja S um subconjunto multiplicativo de A e seja I um ideal decomponível. Seja $I = \cap_{i=1}^n \mathfrak{q}_i$ uma decomposição primária minimal com $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. Suponha ainda que os $\mathfrak{q}_i$'s são numerados de tal forma que S intercepta $\mathfrak{p}_{m+1}, \ldots, \mathfrak{p}_n$ mas não intercepta $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Então $S^{-1}I = \cap_{i=1}^m S^{-1}\mathfrak{q}_i$ e essa decomposição primária é minimal.*

Demonstração. Temos que $S^{-1}I = S^{-1}(\cap_{i=1}^{n}\mathfrak{q}_i) \overset{\text{Ex2.2 L4}}{=} \cap_{i=1}^{n}S^{-1}\mathfrak{q}_i$, agora pela proposição anterior $S^{-1}\mathfrak{q}_i = S^{-1}A$ para $i = m+1,\ldots,n$. Logo $S^{-1}I = \cap_{i=1}^{m}S^{-1}\mathfrak{q}_i$ e $S^{-1}\mathfrak{q}_i$ é $S^{-1}\mathfrak{p}_i$-primário para $i = 1,\ldots,m$. Vejamos que essa decomposição é minimal:

a. Suponha que existam $1 \leq i,j \leq m$ tais que $S^{-1}\mathfrak{p}_i = S^{-1}\mathfrak{p}_j$. Como $\mathfrak{p}_i \neq \mathfrak{p}_j$ existe $a \in \mathfrak{p}_i$ tal que $a \notin \mathfrak{p}_j$, logo para $s \in S$, $\frac{a}{s} \in S^{-1}\mathfrak{p}_i = S^{-1}\mathfrak{p}_j$. Segue que existe $b \in \mathfrak{p}_j$ e $s' \in S$ tal que $\frac{a}{s} = \frac{b}{s'}$ em $S^{-1}A$, ou seja existe $t \in S$ tal que $ts'a = tsb \in \mathfrak{p}_j$, como $\mathfrak{p}_j$ é primo e $a \notin \mathfrak{p}_j$ então devemos ter $ts' \in \mathfrak{p}_j$ mas $S \cap \mathfrak{p}_j = \emptyset$, contradição. Logo os $S^{-1}\mathfrak{p}_i$'s com $1 \leq i \leq m$ são todos distintos.

b. Suponha que existe $1 \leq i \leq m$ tal que $\cap_{j\neq i}S^{-1}\mathfrak{q}_j \subseteq S^{-1}\mathfrak{q}_i$, i.e., $S^{-1}(I_i) \subseteq S^{-1}\mathfrak{q}_i$ onde $I_i = \cap_{j\neq i}\mathfrak{q}_j$. Como $I_i \nsubseteq \mathfrak{q}_i$ temos que existe $a \in I_i$ tal que $a \notin \mathfrak{q}_i$, logo para $s \in S$, $\frac{a}{s} \in S^{-1}I_i \subseteq S^{-1}\mathfrak{q}_i$. Seguindo o raciocínio anterior temos que existe $t \in S$ tal que $ta \in \mathfrak{q}_i$, como $\mathfrak{q}_i$ é primário e $a \notin \mathfrak{q}_i$ então devemos ter $t \in \mathfrak{p}_i$ mas $S \cap \mathfrak{p}_i = \emptyset$, contradição. Logo $\cap_{j\neq i}S^{-1}\mathfrak{q}_j \nsubseteq S^{-1}\mathfrak{q}_i$ para cada $i = 1,\ldots,m$.

□

AULA 18: 22/10/2014

AULA 18

- **Aviso:** Lista 5 disponível no site.

Um subconjunto $\Sigma \subseteq \text{Assoc}(I)$ do conjunto dos ideais primos associados a I é dito **isolado** se satisfaz a seguinte condição: se $\mathfrak{p}' \in \text{Assoc}(I)$ e $\mathfrak{p}' \subseteq \mathfrak{p}$ para algum $\mathfrak{p} \in \Sigma$, então $\mathfrak{p}' \in \Sigma$.

Para o que segue lembremos um resultado da Aula 3: Sejam $\mathfrak{p}_1,\ldots,\mathfrak{p}_n$ ideais primos e seja I um ideal contido em $\bigcup_{i=1}^{n}\mathfrak{p}_i$. Então $I \subseteq \mathfrak{p}_i$ para algum i.

Seja, então Σ um conjunto isolado de ideais primos associados a I e seja $S = A - \cup_{\mathfrak{p}\in\Sigma}\mathfrak{p}$. Então S é um conjunto multiplicativo e, para qualquer ideal primo $\mathfrak{p}' \in \text{Assoc}(I)$, temos que: se $\mathfrak{p}' \in \Sigma$ então $\mathfrak{p}' \cap S = \emptyset$ e se $\mathfrak{p}' \notin \Sigma$ então $\mathfrak{p}' \nsubseteq \cup_{\mathfrak{p}\in\Sigma}\mathfrak{p}$ (pois se $\mathfrak{p}' \subseteq \cup_{\mathfrak{p}\in\Sigma}\mathfrak{p}$ segue da Proposição 29 que $\mathfrak{p}' \subseteq \mathfrak{p}$ para algum $\mathfrak{p} \in \Sigma$, mas como Σ é conjunto isolado então $\mathfrak{p}' \in \Sigma$, contradição) o que implica que $\mathfrak{p}' \cap S \neq \emptyset$.

Teorema 141. (2º Teorema de Unicidade) *Seja I um ideal decomponível de um anel A, $I = \cap_{i=1}^{n}\mathfrak{q}_i$ uma decomposição primária minimal de I e $\Sigma = \{\mathfrak{p}_{i_1},\ldots,\mathfrak{p}_{i_m}\}$ um conjunto isolado de ideais primos associados a I. Então $\mathfrak{q}_{i_1} \cap \cdots \cap \mathfrak{q}_{i_m}$ é independente da decomposição.*

Demonstração. Faremos a prova em 4 partes. Para isso considere S um conjunto multiplicativo qualquer de A.

a. Vejamos que se J é um ideal de A então $\rho^{-1}(S^{-1}J) = \cup_{s\in S}(J : s)$. De fato $a \in \rho^{-1}(S^{-1}J) \Leftrightarrow \rho(a) = \frac{a}{1} \in S^{-1}J \Leftrightarrow \frac{a}{1} = \frac{x}{s}$ para algum $x \in J$ e $s \in S \Leftrightarrow (as - x)t = 0$ para algum $t \in S \Leftrightarrow ast \in J \Leftrightarrow a \in \cup_{s\in S}(J : s)$.

b. Se $\mathfrak{q}$ é um ideal $\mathfrak{p}$-primário e $S \cap \mathfrak{p} = \emptyset$ então $\rho^{-1}(S^{-1}(\mathfrak{q})) = \mathfrak{q}$. Do item anterior segue que $\rho^{-1}(S^{-1}(\mathfrak{q})) = \cup_{s\in S}(\mathfrak{q} : s)$, agora se $s \in S$ então $s \notin \mathfrak{p}$ pela hipótese, logo do Lema 133 temos que $(\mathfrak{q} : s) = \mathfrak{q}$ para todo $s \in S$. Portanto $\rho^{-1}(S^{-1}(\mathfrak{q})) = \mathfrak{q}$.

c. Suponha nas hipóteses do teorema que os $\mathfrak{q}_i$'s são numerados de tal forma que S intercepta $\mathfrak{p}_{m+1}, \ldots, \mathfrak{p}_n$ mas não intercepta $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$. Então provaremos que $\rho^{-1}(S^{-1}I) = \cap_{i=1}^{m}\mathfrak{q}_i$, de fato segue da Proposição 140 que $\rho^{-1}(S^{-1}I) = \rho^{-1}(\cap_{i=1}^{m}S^{-1}\mathfrak{q}_i) = \cap_{i=1}^{m}\rho^{-1}(S^{-1}\mathfrak{q}_i)$ e, do item anterior, $\rho^{-1}(S^{-1}\mathfrak{q}_i) = \mathfrak{q}_i$ para todo $i = 1, \ldots, m$.

d. Por último, seja $S = A - \cup_{\mathfrak{p}\in\Sigma}\mathfrak{p}$ então segue da observação prévia ao teorema que S intercepta os $\mathfrak{p} \in \mathrm{Assoc}(I) - \Sigma$ e não intercepta os $\mathfrak{p} \in \Sigma$. Logo, segue do item *c.*, que $\rho^{-1}(S^{-1}I) = \cap_{j=1}^{m}\mathfrak{q}_{i_j}$ e logo a interseção dos $\mathfrak{q}_{i_j}$ depende somente de I pois pelo 1ºTU os $\mathfrak{p}_i$'s dependem somente do ideal I e não da decomposição primária específica de I.

□

Corolário 142. *As componentes primárias isoladas (i.e., as componentes primárias $\mathfrak{q}_i$ correspondentes aos ideais primos isolados $\mathfrak{p}_i$) são univocamente determinadas por I.*

Demonstração. Aplique o teorema ao conjunto isolado $\Sigma = \{\mathfrak{p}\}$ onde $\mathfrak{p}$ é um ideal isolado de I. Neste caso a componente primária $\mathfrak{q}$ correspondente ao ideal primo isolado $\mathfrak{p}$ satisfaz $\mathfrak{q} = \rho^{-1}(I_{\mathfrak{p}})$ (aqui $S = A - \mathfrak{p}$). □

Por outro lado, as componentes primárias embutidas, em geral, não são univocamente determinadas por I. Se A é um anel Noetheriano, existe de fato uma quantidade infinita de escolhas para as componentes embutidas.

6.1 DECOMPOSIÇÃO PRIMÁRIA EM ANÉIS NOETHERIANOS

Mostraremos a seguir que todo ideal próprio em um anel Noetheriano admite decomposição primária.

Definição 143. Dizemos que um ideal I é **irredutível** se sempre que $I = J \cap K$ então ou $I = J$ ou $I = K$.

Lema 144. *Em um anel Noetheriano A todo ideal é uma interseção finita de ideais irredutíveis.*

Demonstração. Suponha que não, então o conjunto de ideais de A para os quais o lema é falso é não vazio, logo tem um elemento maximal I. Como I é redutível, temos que $I = J \cap K$ onde $J \supset I$ e $K \supset I$. Da maximalidade de I segue que J e K são interseções finitas de ideais irredutíveis e portanto o é I, contradição. □

Lema 145. *Em um anel Noetheriano todo ideal irredutível é primário.*

Demonstração. Passando ao anel quociente, é suficiente mostrar que se o ideal nulo é irredutível então ele é primário. Seja então $xy \in (0)$ com $y \neq 0$, e considere a cadeia de ideais $\mathrm{Ann}(x) \subseteq \mathrm{Ann}(x^2) \subseteq \cdots$. Pela cca, esta cadeia é estacionária, i.e., existe $n > 0$ tal que $\mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1}) = \cdots$. Segue que $(x^n) \cap (y) = (0)$ pois se $a \in (y)$ então $ax = a'yx = 0$ e se $a \in (x^n)$ então $a = bx^n$ logo $ax = bx^{n+1} = 0$ o que implica que $b \in \mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$ assim $bx^n = 0$, i.e., $a = 0$. Como (0) é irredutível e $(y) \neq 0$ então devemos ter $x^n = 0$, e isto mostra que (0) é primário. □

Segue diretamente destes dois lemas que

Teorema 146. *Em um anel Noetheriano A todo ideal admite uma decomposição primária.*

Proposição 147. *Seja A um anel Noetheriano.*

a. Todo ideal I contém uma potência de seu radical.

b. O nilradical de A é nilpotente.

Demonstração. **Exercício 3.** □

Proposição 148. *Seja I um ideal próprio de um anel Noetheriano. Então os ideais primos associados a I são precisamente os ideais primos que ocorrem no conjunto de ideais $(I : a)$ com $a \in A$.*

Demonstração. Observamos que o 1ºTU (Teorema 135) nos diz que os ideais primos associados a I são os ideais primos que ocorrem no conjunto de ideais $\sqrt{(I : a)}$ com $a \in A$. Logo se $(I : a)$ é um ideal primo $\mathfrak{p}$ de A então $\sqrt{(I : a)} = (I : a) = \mathfrak{p}$ e portanto $(I : a)$ é um ideal primo associado a I.

Reciprocamente, seja $I = \cap_{i=1}^{n} \mathfrak{q}_i$ uma decomposição primária minimal de I e seja $\mathfrak{p}_i = \sqrt{\mathfrak{q}_i}$. Denote por $I_i = \cap_{j \neq i} \mathfrak{q}_j \neq I$. Então, pela prova do 1ºTU, temos que $\mathfrak{p}_i = \sqrt{(I : a)}$ para qualquer $a \in I_i$ e $a \notin \mathfrak{q}_i$, logo $(I : a) \subseteq \mathfrak{p}_i$. Agora, como $\mathfrak{q}_i$ é $\mathfrak{p}_i$-primário e todo ideal (em um anel Noetheriano) contém uma potência de seu radical (Proposição 147) existem um inteiro m tal que $\mathfrak{p}_i^m \subseteq \mathfrak{q}_i$, e logo $I_i\mathfrak{p}_i^m \subseteq I_i \cap \mathfrak{p}_i^m \subseteq I_i \cap \mathfrak{q}_i = I$. Seja $m \geq 1$ o menor inteiro tal que $I_i\mathfrak{p}_i^m \subseteq I$ e seja $b \in I_i\mathfrak{p}_i^{m-1} \subseteq I_i \cap \mathfrak{p}_i^{m-1}$ tal que $b \notin I$. Então $\mathfrak{p}_i b \subseteq I$, logo para esse b temos $(I : b) \supseteq \mathfrak{p}_i$ e logo, como $b \in I_i$ e $b \notin I$ então $b \notin \mathfrak{q}_i$, pelo anterior $(I : b) \subseteq \mathfrak{p}_i$. □

Observação 149. Observamos que para o caso particular de módulos sobre um corpo $\mathbf{k}$, i.e. $\mathbf{k}$-espaços vetoriais V, as seguintes condições são equivalentes: V tem dimensão finita $\Leftrightarrow$ V tem comprimento finito $\Leftrightarrow$ V é Noetheriano $\Leftrightarrow$ V é Artiniano. (Exercício 4 da Lista 5)

Vejamos que existem anéis nos quais, assim como os espaços vetoriais, as condições de ser Noetheriano ou Artiniano são equivalentes. Para provar a seguinte proposição usaremos a Proposição 102 (Seja $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ uma sequência exata de A-módulos. Então: M é Noetheriano (Artiniano) $\Leftrightarrow M'$ e M'' são Noetherianos (Artinianos))

Proposição 150. *Seja A um anel no qual o ideal zero é um produto $\mathfrak{m}_1 \cdots \mathfrak{m}_n$ de ideais maximais (não necessariamente distintos). Então A é Noetheriano se, e somente se, A é Artiniano.*

Demonstração. Considere a cadeia de ideais (A-módulos): $A \supsetneq \mathfrak{m}_1 \supseteq \mathfrak{m}_1\mathfrak{m}_2 \supseteq \cdots \supseteq \mathfrak{m}_1 \cdots \mathfrak{m}_n = 0$. Denote por $M_i = \mathfrak{m}_1 \cdots \mathfrak{m}_i$, para $i = 1, \ldots, n$. Cada módulo quociente M_{i-1}/M_i é um $A/\mathfrak{m}_i$-módulo pois é um A-módulo aniquilado por $\mathfrak{m}_i$. Logo M_{i-1}/M_i é um espaço vetorial sobre o corpo $A/\mathfrak{m}_i$. Portanto, M_{i-1}/M_i é um $A/\mathfrak{m}_i$-módulo Artiniano se, e somente se, é um $A/\mathfrak{m}_i$-módulo Noetheriano (pela Observação anterior). Como seus $A/\mathfrak{m}_i$-submódulos são exatamente os mesmos que seus A-submódulos, M_{i-1}/M_i é um A-módulo Artiniano se, e somente se, é um A-módulo Noetheriano.

Considere as sequências exatas curtas:

$$
\begin{aligned}
&0 \to M_1 \xhookrightarrow{i} A \xrightarrow{\pi} A/M_1 \to 0\\
&0 \to M_2 \xhookrightarrow{i} M_1 \xrightarrow{\pi} M_1/M_2 \to 0\\
&\vdots\\
&0 \to M_i \xhookrightarrow{i} M_{i-1} \xrightarrow{\pi} M_{i-1}/M_i \to 0\\
&\vdots\\
&0 \to M_{n-1} \xhookrightarrow{i} M_{n-2} \xrightarrow{\pi} M_{n-2}/M_{n-1} \to 0\\
&0 \to M_n \xhookrightarrow{i} M_{n-1} \xrightarrow{\pi} M_{n-1}/M_n \to 0
\end{aligned}
$$

Suponha que A seja A-módulo Noetheriano então M_1 e A/M_1 são A-módulos Noetherianos, isto implica que M_2 e M_1/M_2 são A-módulos Noetherianos, continuando com esse raciocínio temos que M_i e M_{i-1}/M_i são A-módulos Noetherianos para todo $i = 1, \ldots, n$. Logo os quocientes M_{i-1}/M_i são A-módulos Artinianos para todo $i = 1, \ldots, n$. Em particular para $i = n$ temos que M_{n-1}/M_n é A-módulo Artiniano, mas $M_n = 0$ logo

M_{n-1} é A-módulo Artiniano e M_{n-2}/M_{n-1} é A-módulo Artiniano, o que implica que M_{n-2} é A-módulo Artiniano. Continuando com esse raciocínio temos que A é A-módulo Artiniano. Analogamente se trocarmos os termos "Artiniano" e "Noetheriano". □

AULA 19: 24/10/2014

Lembramos da última aula:

Proposição. *Seja A um anel no qual o ideal zero é um produto finito $\mathfrak{m}_1 \cdots \mathfrak{m}_n$ de ideais maximais (não necessariamente distintos). Então A é Noetheriano se, e somente se, A é Artiniano.*

Mostraremos a seguir que todo anel Artiniano é Noetheriano. Mas para que um anel Noetheriano seja Artiniano precisamos adicionar mais alguma condição:

Teorema 151. *A é um anel Artiniano se, e somente se, A é Noetheriano e* $\dim A = 0$.

Demonstração. ($\Rightarrow$): Como A é Artiniano segue do Corolário 127 que $\dim A = 0$ e da Proposição 124 que A tem um número finito de ideais maximais: $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. Como o radical de Jacobson $\mathfrak{R}$ de A é nilpotente (Corolário 123 e Proposição 125) existe $k > 0$ tal que $\mathfrak{R}^k = 0$. Então $\Pi_{i=1}^n \mathfrak{m}_i^k \subseteq (\cap_{i=1}^n \mathfrak{m}_i)^k = \mathfrak{R}^k = 0$, podemos escrever o zero como produto de ideais maximais (não necessariamente distintos), segue da proposição anterior que A é Noetheriano.

($\Leftarrow$): Suponha que $\mathfrak{p}$ seja um ideal primo de A e seja I um ideal próprio de A tal que $\mathfrak{p} \subseteq I$, então existe um ideal maximal $\mathfrak{m}$ tal que $\mathfrak{p} \subseteq I \subseteq \mathfrak{m}$. Segue do fato da $\dim A = 0$ que $\mathfrak{p} = \mathfrak{m} = I$, ou seja os ideais primos de A são maximais. Analogamente vemos que todos os ideais primos também são ideais primos minimais. Como A é Noetheriano, todo ideal tem decomposição primária (Teorema 146). Em particular o ideal nulo tem uma decomposição primária, logo os ideais primos isolados associados a (0) (que são os elementos minimais de $V(0) = \mathrm{Spec}(A)$ (Proposição 136)) são os ideais primos (minimais) de A, segue que A tem um número finito de ideais primos (e, portanto, maximais): $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. Assim $\mathfrak{N} = \cap_{i=1}^n \mathfrak{m}_i$. Segue da Proposição 147 que $\mathfrak{N}$ é nilpotente, logo existe $k > 0$ tal que $\Pi_{i=1}^n \mathfrak{m}_i^k \subseteq (\cap_{i=1}^n \mathfrak{m}_i)^k = \mathfrak{N}^k = 0$, ou seja, podemos escrever o zero como produto de ideais maximais, segue da proposição anterior que A é Artiniano. □

Como consequências do fato de todo anel Artiniano ser Noetheriano temos:

Corolário 152. *Em um anel Artiniano A todo ideal admite uma decomposição primária.*

Demonstração. Segue dos Teoremas 151 e 146. □

Corolário 153. *Um anel A é Artiniano se, e somente se, $\ell_A(A) < \infty$.*

Demonstração. Segue da Proposição 111 e do Teorema 151. □

Observamos que no caso de módulos o teorema anterior não é válido pois existem módulos Artinianos que não são Noetherianos, como mostra o exemplo a seguir:

Exemplo 154. Seja G o subgrupo de $\mathbb{Q}/\mathbb{Z}$ que consiste de todos os elementos de ordem potência de p, onde p é um número primo fixo. Então G tem exatamente um subgrupo G_n de ordem p^n para cada $n \geq 0$ e $G_0 \subset G_1 \subset \cdots \subset G_n \subset \cdots$ (inclusões estritas) então G não satisfaz a cca, logo não é Noetheriano como $\mathbb{Z}$-módulo. Por outro lado, os únicos subgrupos próprios de G são os G_n, logo G satisfaz a ccd e logo é Artiniano como $\mathbb{Z}$-módulo.

Proposição 155. *Seja A um anel Noetheriano local e $\mathfrak{m}$ seu ideal maximal. Então exatamente uma das seguintes condições é verdadeira:*

a. $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ *para todo n;*

b. $\mathfrak{m}^n = 0$ *para algum n, neste caso A é um anel Artiniano local.*

Demonstração. Suponha que $\mathfrak{m}^n = \mathfrak{m}^{n+1}$ para algum n. Como A é Noetheriano, $\mathfrak{m}^n$ é um ideal f.g. e como A é local $\mathfrak{R} = \mathfrak{m}$, pelo lema de Nakayama (Lema 60) com $M = \mathfrak{m}^n$ e $I = \mathfrak{m}$, temos que $\mathfrak{m}^n = 0$. Seja $\mathfrak{p}$ um ideal primo de A, como $0 \in \mathfrak{p}$ então $\mathfrak{m}^n \subseteq \mathfrak{p}$ logo, tomando radicais, temos $\sqrt{\mathfrak{m}^n} = \mathfrak{m} \subseteq \mathfrak{p} = \sqrt{\mathfrak{p}}$, da maximalidade de $\mathfrak{m}$ segue que $\mathfrak{m} = \mathfrak{p}$. Logo $\mathfrak{m}$ é o único primo de A o que implica que $\dim A = 0$, como A é Noetheriano então A é Artiniano (Teorema 151). □

Se A é um anel Artiniano local, então $\mathfrak{m}$ é o único ideal primo de A e logo $\mathfrak{m}$ é o nilradical de A. Segue que todo elemento de $\mathfrak{m}$ é nilpotente e o mesmo $\mathfrak{m}$ é nilpotente. Além disso, todo elemento de A ou é uma unidade ou é nilpotente. (Exercício 18 Lista 1).

Teorema 156. (Teorema de Estrutura de Anéis Artinianos) *Todo anel Artiniano A é um produto direto finito de anéis Artinianos locais determinados de maneira única (a menos de isomorfismo).*

Demonstração. Sejam $\mathfrak{m}_i$ com $i = 1, \ldots, n$ os ideais maximais distintos de A. Da prova do Teorema 151 temos que $\Pi_{i=1}^n \mathfrak{m}_i^k = 0$ para algum $k > 0$. Vejamos que os ideais $\mathfrak{m}_i^k$ são dois-a-dois coprimos. Primeiramente observe que:

a. $\sqrt{I} = A \Leftrightarrow I = A$ e

b. $\sqrt{I+J} = \sqrt{\sqrt{I} + \sqrt{J}}$ (Verifique!)

Seja $I = \mathfrak{m}_i + \mathfrak{m}_j$ para $i \neq j$ logo $\mathfrak{m}_i \subsetneq I$, segue da maximalidade de $\mathfrak{m}_i$ que $I = A$. Por outro lado

$$\sqrt{\mathfrak{m}_i^k + \mathfrak{m}_j^k} \overset{\text{b.}}{=} \sqrt{\sqrt{\mathfrak{m}_i^k} + \sqrt{\mathfrak{m}_j^k}} = \sqrt{\mathfrak{m}_i + \mathfrak{m}_j} = \sqrt{A} = A,$$

isto implica por a. que $\mathfrak{m}_i^k + \mathfrak{m}_j^k = A$ e logo são coprimos. Segue do Teorema Chinês dos Restos (Teorema 31) que:

a. $\cap_{i=1}^n \mathfrak{m}_i^k = \Pi_{i=1}^n \mathfrak{m}_i^k = 0$ e é uma decomposição primária minimal do 0: potências de maximais são primários, os $\sqrt{\mathfrak{m}_i^k} = \mathfrak{m}_i$ são todos distintos por hipótese e ainda se $\cap_{j\neq i}\mathfrak{m}_j^k \subseteq \mathfrak{m}_i^k$ tomando radicais teríamos $\cap_{j\neq i}\mathfrak{m}_j \subseteq \mathfrak{m}_i$ (Interseção finita de ideais contida em um primo) logo $\mathfrak{m}_j \subseteq \mathfrak{m}_i$ para algum j, como $\mathfrak{m}_j$ é maximal e $\mathfrak{m}_i \neq A$ então $\mathfrak{m}_j = \mathfrak{m}_i$, contradição. Logo $\cap_{j\neq i}\mathfrak{m}_j^k \nsubseteq \mathfrak{m}_i^k$ para todo $i = 1, \ldots, n$.

b. $A = \underbrace{\dfrac{A}{\mathfrak{m}_1^k \cdot \mathfrak{m}_2^k \cdot \ldots \cdot \mathfrak{m}_n^k}}_{=0} \simeq \dfrac{A}{\mathfrak{m}_1^k} \times \dfrac{A}{\mathfrak{m}_2^k} \times \cdots \times \dfrac{A}{\mathfrak{m}_n^k}.$

Cada quociente $A/\mathfrak{m}_i^k$ é um anel Artiniano (quociente de Artiniano por um ideal). Para ver que cada quociente é local, seja $\overline{\mathfrak{m}}$ um ideal maximal de $A/\mathfrak{m}_i^k$, então $\overline{\mathfrak{m}}$ corresponde a um ideal maximal de A que contém $\mathfrak{m}_i^k$, suponha que $\mathfrak{m}_i^k \subseteq \mathfrak{m}_j$ tomando radicais temos $\mathfrak{m}_i \subseteq \mathfrak{m}_j$ segue que $j = i$ e logo existe somente um ideal maximal de A que contém $\mathfrak{m}_i^k$ o que implica que $A/\mathfrak{m}_i^k$ é local com ideal maximal $\overline{\mathfrak{m}_i}$. Logo A é um produto direto finito de anéis Artinianos locais.

Para a unicidade, suponha que $A \simeq \Pi_{i=1}^m A_i$, onde A_i são anéis Artinianos locais. Então para cada i temos um homomorfismo sobrejetor natural $\pi_i : A \to A_i$ que é a projeção na i-ésima coordenada. Seja $I_i = \text{Ker}(\pi_i)$, então pelo teorema de isomorfismo temos $A_i \simeq A/I_i$.

Por outro lado $\cap_{i=1}^m I_i = 0$, é claro que $0_A \in I_i$ para todo i e reciprocamente se $a \in \cap_{i=1}^m I_i$ então $0_i = \pi_i(a) = a_i$ para todo i então $a = 0_A$. Vejamos que esta é uma decomposição primária do (0): seja $\mathfrak{q}_i$ o único ideal primo de A_i (veja observação previa ao teorema) e seja $\mathfrak{p}_i = \pi_i^{-1}(\mathfrak{q}_i)$ então $\mathfrak{p}_i$ é um ideal primo de A e logo maximal (Proposição 122). Como $\mathfrak{q}_i$ é o nilradical de A_i segue que I_i é $\mathfrak{p}_i$-primário, vejamos: $a \in \sqrt{I_i} \Leftrightarrow$existe $l > 0$ tal que $a^l \in I_i \Leftrightarrow 0_i = \pi_i(a^l) = \pi_i(a)^l \Leftrightarrow \pi_i(a) \in \mathfrak{q}_i \Leftrightarrow a \in \pi_i^{-1}(\mathfrak{q}_i) = \mathfrak{p}_i$. Logo $\sqrt{I_i} = \mathfrak{p}_i$ (que é maximal) logo segue da Proposição 131 (Se $\sqrt{I}$ é maximal, então I é primário) que I_i é $\mathfrak{p}_i$-primário. Isto implica que a expressão $\cap_{i=1}^m I_i = 0$ é uma decomposição primária do ideal zero de A.

Vejamos que a decomposição primária é minimal, para isso provaremos primeiramente que os $\mathfrak{p}_i$'s são coprimos dois-a-dois: seja $i \neq j$ então existe

$a = (a_1, \ldots, 1_i, \ldots, 0_j, \ldots, a_m) \in A$ tal que $\pi_i(a) = 1_i$ e $\pi_j(a) = 0_j$, logo $1_A - a \in I_i$ e $a \in I_j$ assim $1_A = (1_A - a) + a \in I_i + I_j$. Logo os I_i's são coprimos. Isto implica que para $i \neq j$, $\sqrt{\mathfrak{p}_i + \mathfrak{p}_j} = \sqrt{\sqrt{I_i} + \sqrt{I_j}} \overset{\text{b.}}{=} \sqrt{I_i + I_j} = \sqrt{A} \overset{\text{a.}}{=} A$ segue de a. que $\mathfrak{p}_i + \mathfrak{p}_j = A$ e logo os $\mathfrak{p}_i$'s são coprimos dois-a-dois. Como consequência eles são todos distintos pois se dois deles forem iguais $\mathfrak{p}_i = \mathfrak{p}_j$ então $A = \mathfrak{p}_i + \mathfrak{p}_j = \mathfrak{p}_i$, contradição. Por outro lado, $\cap_{j \neq i} I_j \nsubseteq I_i$ para cada $i = 1, \ldots, m$ pois se, para algum i, $\cap_{j \neq i} I_j \subseteq I_i$ tomando radicais temos $\cap_{j \neq i} \mathfrak{p}_j \subseteq \mathfrak{p}_i$ e logo existiria j tal que $\mathfrak{p}_j \subseteq \mathfrak{p}_i$, como $\mathfrak{p}_j$ é maximal isto implicaria $\mathfrak{p}_j = \mathfrak{p}_i$, contradição. Logo a decomposição primária $\cap_{i=1}^m I_i = 0$ é minimal.

Assim temos que $\text{Assoc}(0) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\} = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$, logo segue do 1ºTU que $m = n$. Além disso, como consequência da maximalidade dos primos associados a (0) temos que todos eles são isolados e logo todas as componentes primárias são isoladas e, consequentemente, determinadas de maneira única por A pelo 2ºTU (Teorema 141). Logo existe uma permutação σ dos índices $1, \ldots, n$ tal que $I_i \simeq \mathfrak{m}_{\sigma(i)}^k$ para todo $i = 1, \ldots, n$.

Assim os anéis Artinianos locais $A_i \simeq A/I_i \simeq A/\mathfrak{m}_{\sigma(i)}^k$ são determinados de maneira única por A, para todo $i = 1, \ldots, n$. □

Se A é um anel local, $\mathfrak{m}$ seu ideal maximal, $\mathbf{k} = A/\mathfrak{m}$ seu corpo de resíduos e M um A-módulo então o A-módulo $M/\mathfrak{m}M$ é aniquilado por $\mathfrak{m}$ e portanto tem estrutura de $\mathbf{k}$-espaço vetorial. Se, alem disso M é f.g. por m_i $(1 \leq i \leq n)$ então $M/\mathfrak{m}M$ também é f.g. como A-módulo. Assim se $x \in M/\mathfrak{m}M$ então $x = \sum_{i=1}^n a_i \overline{m_i} = \sum_{i=1}^n \overline{a}_i \overline{m}_i$ (pela definição da ação de $A/\mathfrak{m}$ em $M/\mathfrak{m}M$), logo $M/\mathfrak{m}M$ é f.g. como $\mathbf{k}$-espaço vetorial, assim $\dim_{\mathbf{k}}(M/\mathfrak{m}M) \leq n$.

Lembramos a Proposição 62, da Aula 8 que é corolário do Lema de Nakayama e diz o seguinte: Sob as hipóteses anteriores, seja M um A-módulo f.g. e sejam m_i $(1 \leq i \leq n)$ os elementos de M cujas imagens em $M/\mathfrak{m}M$ formam uma base deste espaço vetorial. Então os m_i's geram M.

Proposição 157. *Seja A um anel Artiniano local. Então são equivalentes:*

a. todo ideal de A é principal;

b. o ideal maximal $\mathfrak{m}$ é principal;

c. $\dim_{\mathbf{k}}(\mathfrak{m}/\mathfrak{m}^2) \leq 1$.

Demonstração. (a.)⇒(b.) é claro. (b.)⇒(c.) segue da observação prévia à proposição. Vejamos que (c.)⇒(a.): Se $\dim_{\mathbf{k}}(\mathfrak{m}/\mathfrak{m}^2) = 0$, então $\mathfrak{m} = \mathfrak{m}^2$ e $\mathfrak{m}$ é f.g. por A ser Artiniano (e logo Noetheriano), e por A ser local temos que $\mathfrak{m} = \mathfrak{R}$, segue do Lema de Nakayama que $\mathfrak{m} = 0$ e logo A é um corpo e seus ideias (1) e (0) são principais. Se $\dim_{\mathbf{k}}(\mathfrak{m}/\mathfrak{m}^2) = 1$, então $\mathfrak{m}$ é um

ideal principal pela Proposição 62, logo $\mathfrak{m} = (a)$. Seja $I \neq (0)$ um ideal próprio de A, então $I \subseteq \mathfrak{m}$. Temos ainda que $\mathfrak{m} \overset{\text{local}}{=} \mathfrak{R} \overset{\text{Arti}}{=} \mathfrak{N}$ e logo $\mathfrak{m}$ é nilpotente (Proposição 125), portanto existe um inteiro $r > 0$ tal que $I \subseteq \mathfrak{m}^r$ e $I \nsubseteq \mathfrak{m}^{r+1}$ (suponha que não, que para todo $r > 0$, $I \subseteq \mathfrak{m}^r$ então $I = (0)$ pela nilpotência de $\mathfrak{m}$, contradição). Logo existe $b \in I$ e $b \notin (a^{r+1}) = \mathfrak{m}^{r+1}$ com $b = xa^r$, consequentemente $x \notin (a) = \mathfrak{m}$, i.e., x não é nilpotente logo (pela observação previa à ao Teorema de Estrutura de Anéis Artinianos) x é uma unidade de A. Logo $a^r \in I$, portanto $\mathfrak{m}^r = (a^r) \subseteq I$ e logo $I = \mathfrak{m}^r = (a^r)$. Segue que I é principal. □

6.3 EXERCÍCIOS

Ex. 66 — Seja A um anel, D o conjunto dos divisores de zero de A e $\mathfrak{N}$ o nilradical de A. Mostre que:

1. $D = \cup_{a \neq 0} \sqrt{(0 : a)}$
2. $\mathfrak{N} = \sqrt{(0)}$
3. Use o item anterior para mostrar que, se o ideal zero (0) é decomponível, então:
   a) D é a união de todos os ideais primos associados a (0);
   b) $\mathfrak{N}$ é a interseção de todos os ideais primos isolados associados a (0).
4. Se I é um ideal de A decomponível então $\cup_{i=1}^{n} \mathfrak{p}_i = \{a \in A \mid (I : a) \neq I\}$, onde os $\mathfrak{p}_i$'s são os ideais primos associados a I.

Ex. 67 — Seja A um anel Noetheriano. Mostre que:

1. Todo ideal contém uma potência de seu radical.
2. O nilradical de A é nilpotente.

Ex. 68 — Seja A um anel Noetheriano, $\mathfrak{m}$ um ideal maximal de A, $\mathfrak{q}$ um ideal qualquer de A. Mostre que são equivalentes:

1. $\mathfrak{q}$ é $\mathfrak{m}$-primário;
2. $\sqrt{\mathfrak{q}} = \mathfrak{m}$;
3. $\mathfrak{m}^n \subseteq \mathfrak{q} \subseteq \mathfrak{m}$ para algum $n > 0$.

Ex. 69 — Seja A um anel Noetheriano e $\mathfrak{m}$ um ideal maximal. Mostre que $A/\mathfrak{m}^n$ é Artiniano para todo $n \geq 0$

Ex. 70 — Mostre que se I é um ideal radical (i.e., $I = \sqrt{I}$) então I é decomponível e não tem ideais primos embutidos.

Ex. 71 — Seja I um ideal decomponível de um anel A e seja $\mathfrak{p}$ um elemento maximal do conjunto de ideais $(I : a)$ onde $a \in A$ e $a \notin I$. Mostre que $\mathfrak{p}$ é um ideal primo associado a I.

Ex. 72 — Se A é um anel no qual todo ideal tem uma decomposição primária, mostre que toda localização de A por um conjunto multiplicativo S, $S^{-1}A$, tem a mesma propriedade.

Ex. 73 — Sejam $\mathfrak{p}_1 = (x, y)$, $\mathfrak{p}_2 = (x, z)$ e $\mathfrak{p}_3 = (x, y, z)$ ideais do anel de polinômios $\mathbf{k}[x, y, z]$, onde $\mathbf{k}$ é um corpo. Seja $I = \mathfrak{p}_1\mathfrak{p}_2$:

1. Mostre que $I = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \mathfrak{p}_3^2$ é uma decomposição primária minimal de I.
2. Encontre os ideais primos minimais do anel $\mathbf{k}[x, y, z]/(x, y) \cdot (x, z)$.

Ex. 74 — Seja $I = (xy, x^3 - x^2, x^2y - xy)$ um ideal do anel de polinômios $\mathbf{k}[x, y]$, onde $\mathbf{k}$ é um corpo.

1. Mostre que $I = (x) \cap (x - 1, y) \cap (x^2, y)$ é uma decomposição primária minimal de I.
2. Encontre os ideais primos minimais do anel $\mathbf{k}[x, y]/(xy, x^3 - x^2, x^2y - xy)$.

Ex. 75 — Um espaço topológico X é dito **discreto** se todo subespaço de X é fechado. Seja A um anel Noetheriano. Mostre que as seguintes condições são equivalentes:

1. A é Artiniano;
2. $\mathrm{Spec}(A)$ é finito e discreto;
3. $\mathrm{Spec}(A)$ é discreto.

Ex. 76 — Seja $A = \mathbf{k}[x_1, ..., x_n]/I$, onde I é um ideal. Mostre que $\dim(A) = 0$ se e somente se A é um $\mathbf{k}$-espaço vetorial de dimensão finita.

Ex. 77 — Seja A uma $\mathbf{k}$-álgebra Noetheriana local com ideal maximal $\mathfrak{m}$ e corpo de resíduos $\mathbf{k}$. Sabendo que $\dim_{\mathbf{k}}(\mathfrak{m}/\mathfrak{m}^2) = 2002$, qual é o número mínimo de geradores para o ideal $\mathfrak{m}$?

Ex. 78 — Seja A um anel Noetheriano e $\mathfrak{q}$ um ideal $\mathfrak{p}$-primário de A. Considere cadeias de ideais primos de $\mathfrak{q}$ até $\mathfrak{p}$. Mostre que todas tais cadeias

tem comprimento finito e que todas as cadeias maximais tem o mesmo comprimento.

7

EXTENSÕES INTEGRAIS

AULA 20: 29/10/2014

AULA 20

Extensões finitas e integrais de anéis generalizam os conceitos de extensões finitas e algébricas de corpos.

Definição 158. Seja $B \supseteq A$ uma extensão de anéis (i.e., B é um anel, A um subanel de B, de modo que $1 \in A$). Um elemento $b \in B$ é dito **integral** sobre A se b é uma raiz de um polinômio mônico com coeficientes em A, i.e., b satisfaz uma equação da forma

$$b^n + a_1 b^{n-1} + \cdots + a_n = 0 \tag{8}$$

onde os $a_i \in A$. Dizemos que a extensão $B \supseteq A$ é **integral** se todo elemento $b \in B$ é integral sobre A.

No caso geral em que $f : A \to B$ é uma A-álgebra, dizemos que f é integral e B é uma A-álgebra integral se $B \supseteq f(A)$ é uma extensão integral.

Definição 159. Uma extensão de anéis $B \supseteq A$ é dita **finita** se B, visto como A-módulo é f.g. Analogamente, uma A-álgebra $f : A \to B$ é dita **finita** se B é um A-módulo f.g.

Exemplo 160. Uma extensão integral de corpos é o mesmo que uma extensão algébrica e uma extensão de corpos $L \supseteq \mathbf{k}$ é finita se, e somente se, $[L : \mathbf{k}] = \dim_{\mathbf{k}} L < \infty$. Desta forma, as definições anteriores generalizam para anéis os conceitos familiares de elemento algébrico e extensões finitas e algébricas de corpos.

Diretamente das definições obtemos:

Lema 161.

a. *Seja I um ideal de A. O quociente A/I é uma A-álgebra finita.*

b. *Se $f : A \to B$ e $g : B \to C$ são álgebras finitas, então $g \circ f : A \to C$ é finita.*

c. *Se $f : A \to B$ é uma álgebra finita e $g : A \to C$ é uma álgebra qualquer então a álgebra obtida por mudança de base $f \otimes \mathrm{id} : A \otimes_A C \simeq C \to B \otimes_A C$ dada por $c \mapsto 1 \otimes c$ é finita. Em particular, se $S \subseteq A$ é um conjunto multiplicativo, a localização $S^{-1}f : S^{-1}A \to S^{-1}B$ é uma álgebra finita.*

Demonstração. **Exercício 1.** □

Proposição 162. *Seja $A \subseteq B$ uma extensão de anéis e seja $b \in B$. As seguintes afirmações são equivalentes:*

a. b é integral sobre A;

b. $A[b] \supseteq A$ é uma extensão finita.

c. $A[b] \subseteq C$ tal que $C \subseteq B$ é um subanel de B que é f.g. como A-módulo.

Demonstração. (a.)⇒(b.) Como b é integral sobre A, multiplicando (8) por b^r, temos $b^{n+r} = -(a_1 b^{n+r-1} + \cdots + a_n b^r)$ para todo $r \geq 0$. Logo, por indução, todas as potencias positivas de b pertencem ao A-módulo gerado por $1, b, \ldots, b^{n-1}$. Logo $A[b]$ é gerado como A-módulo por $1, b, \ldots, b^{n-1}$, i.e., $A[b] \supseteq A$ é uma extensão finita.

(b.)⇒(c.) Basta tomar $C = A[b]$.

(c.)⇒(a.) Sejam $c_1, \ldots, c_n \in C$ os geradores de C como A-módulo. Como $b \cdot c_i \in C$ para todo i (pois $b \in A[b] \subseteq C$ por hipótese), temos que $b \cdot c_i = \sum_{j=1}^{n} a_{ij} c_j$ assim temos o seguinte "sistema linear" nas "variáveis" c_i e "coeficientes" $a_{ij} \in A$:

$$\begin{aligned} b \cdot c_1 &= a_{11} c_1 + \cdots + a_{1n} c_n \\ &\vdots \\ b \cdot c_n &= a_{n1} c_1 + \cdots + a_{nn} c_n \end{aligned}$$

Logo b é raiz do polinômio característico da matriz (a_{ij}) que é mônico e possui coeficientes em A. Segue que b é integral sobre A. □

Corolário 163. *Sejam b_i com $1 \leq i \leq n$ elementos de B, cada um dos quais é integral sobre A. Então $A[b_1, \ldots, b_n] \supseteq A$ é uma extensão finita.*

Demonstração. Por indução em n. O caso $n = 1$ é a proposição anterior. Assuma $n > 1$ e seja $A_r = A[b_1, \ldots, b_r]$, então pela hipóteses indutiva $A_{n-1} \supseteq A$ é uma extensão finita. Por outro lado, como b_n é integral sobre A então é integral sobre A_{n-1}, assim pelo caso $n = 1$, $A_n = A_{n-1}[b_n] \supseteq A_{n-1}$ é uma extensão finita. Segue da transitividade do Lema 161 que $A_n \supseteq A$ é uma extensão finita. □

Corolário 164. *Se $B \supseteq A$ é uma extensão finita então é integral. Reciprocamente, se $B \supseteq A$ é integral e B é f.g. como A-álgebra, então $B \supseteq A$ é uma extensão finita.*

Demonstração. Seja $b \in B$, então $A[b] \subseteq B$ e como $A \subseteq B$ é finita B é f.g. como A-módulo, segue da Proposição 162 (c.) que b é integral sobre A. Logo a extensão $A \subseteq B$ é integral. Reciprocamente como B é uma A-álgebra f.g. existem $b_1, \ldots, b_n \in B$, cada um deles integrais sobre A por hipótese, tais que $B = A[b_1, \ldots, b_n]$. Logo segue do corolário anterior que $B \supseteq A$ é uma extensão finita. □

A seguinte definição é uma generalização da noção de fecho algébrico para extensões de corpos.

Definição 165. Seja $B \supseteq A$ uma extensão de anéis. O conjunto $\mathcal{C}(A, B)$ dos elementos de B que são integrais sobre A é chamado de **fecho integral** ou **normalização** de A em B. Se $\mathcal{C}(A, B) = A$, então A é dito **integralmente fechado** em B.

Observe que $\mathcal{C}(A, B) = B$ se, e somente se, B é integral sobre A.

Lema 166. *Seja $B \supseteq A$ uma extensão de anéis. O fecho integral de A em B, $\mathcal{C}(A, B)$, é um subanel de B que contém A.*

Demonstração. Como todo elemento de A é integral sobre A, segue $A \subseteq \mathcal{C}(A, B)$. Dados $a, b \in \mathcal{C}(A, B)$ devemos mostrar que $a \pm b$ e ab também pertencem a $\mathcal{C}(A, B)$, ou seja, são integrais sobre A. Como $a \pm b, ab \in A[a, b]$, então $A[a \pm b] \subseteq A[a, b]$ e $A[ab] \subseteq A[a, b]$. Por outro lado, como a, b são integrais sobre A, segue do Corolário 163 que $A[a, b] \supseteq A$ é uma extensão finita. Logo, da Proposição 162 (c.) segue que $a \pm b$ e ab são integrais sobre A. □

Proposição 167. *Sejam $A \subseteq B \subseteq C$ extensões de anéis. Se B é integral sobre A e C é integral sobre B então C é integral sobre A.*

Demonstração. Dado $c \in C$ devemos mostra que c é integral sobre A. Por hipótese existe uma equação $c^n + b_1 c^{n-1} + \cdots + b_n = 0$, com $b_i \in B$. Por outro lado, cada b_i é integral sobre A. Assim, segue do Corolário 163, que $A[b_1, \ldots, b_n] \supseteq A$ é uma extensão finita. Mas agora c é integral sobre $A[b_1, \ldots, b_n]$ (pois os coeficientes b_i do polinômio mônico do qual c é raiz pertencem a $A[b_1, \ldots, b_n]$), logo $A[b_1, \ldots, b_n, c] \supseteq A[b_1, \ldots, b_n]$ é uma extensão finita (Proposição 162 b.). Segue da transitividade do Lema 161 que $A[b_1, \ldots, b_n, c] \supseteq A$ é uma extensão finita. Assim $A[c]$ está contido em $A[b_1, \ldots, b_n, c]$ que é um subanel de C, f.g. como A-módulo, portanto c é integral sobre A como consequência do item (c.) da Proposição 162. □

Corolário 168. *Seja $B \supseteq A$ uma extensão de anéis. O fecho integral de A em B, $\mathcal{C}(A, B)$, é integralmente fechado em B.*

Demonstração. Queremos provar que $\mathcal{C}(\mathcal{C}(A, B), B) = \mathcal{C}(A, B)$. Sabemos pelo Lema 166 que $A \subseteq \mathcal{C}(A, B) \subseteq \mathcal{C}(\mathcal{C}(A, B), B) \subseteq B$. Seja $b \in \mathcal{C}(\mathcal{C}(A, B), B)$, então b é integral sobre $\mathcal{C}(A, B)$, ou seja $\mathcal{C}(A, B) \subseteq \mathcal{C}(\mathcal{C}(A, B), B)$ é uma extensão integral. Analogamente, se $c \in \mathcal{C}(A, B)$ então c é integral sobre A logo $A \subseteq \mathcal{C}(A, B)$ é uma extensão integral. Segue da Proposição anterior que $A \subseteq \mathcal{C}(\mathcal{C}(A, B), B)$ é uma extensão integral, o que implica que dado $d \in \mathcal{C}(\mathcal{C}(A, B), B)$ temos que d é integral sobre A, logo $d \in \mathcal{C}(A, B)$ e por tanto $\mathcal{C}(\mathcal{C}(A, B), B) \subseteq \mathcal{C}(A, B)$. □

Mostraremos a seguir que extensões integrais são preservadas por quocientes e localização:

Proposição 169. *Seja $B \supseteq A$ uma extensão integral de anéis.*

a. *Se I é um ideal de B então B/I é integral sobre $A/A \cap I$.*

b. *Se S é um subconjunto multiplicativo de A, então $S^{-1}B$ é integral sobre $S^{-1}A$.*

Demonstração.

a. Seja $\overline{b} \in B/I$, então $\overline{b} = b + I$ com $b \in B$ logo existe uma expressão $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ com $a_i \in A$. Reduzindo esta equação módulo I temos $\overline{b}^n + \overline{a}_1 \overline{b}^{n-1} + \cdots + \overline{a}_n = \overline{0}$ com $\overline{a}_i \in A/A \cap I$. Logo $\overline{b}$ é integral sobre $A/A \cap I$.

b. Seja $\frac{b}{s} \in S^{-1}B$ com $b \in B$ e $s \in S$, logo existe uma expressão $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ em B, com $a_i \in A$. Agora como $s \in S$ então $s^n \in S$ e logo $\frac{s^n}{1}$ é uma unidade em $S^{-1}B$, logo $\frac{1}{s^n}(b^n + a_1 b^{n-1} + \cdots + a_n) = 0$ em $S^{-1}B$. Assim temos a expressão $\left(\frac{b}{s}\right)^n + \frac{a_1}{s}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_n}{s^n} = 0$ onde os coeficientes $\frac{a_i}{s^i} \in S^{-1}A$. Logo $\frac{b}{s}$ é integral sobre $S^{-1}A$.

□

Proposição 170. *Sejam $A \subseteq B$ domínios de integridade, B integral sobre A. Então B é um corpo se, e somente se, A é um corpo.*

Demonstração. Suponha que A seja um corpo e seja $b \in B$, $b \neq 0$. Como B é integral sobre A, seja $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ com $a_i \in A$ uma equação para a dependência integral de b do menor grau possível. Suponha que $a_n = 0$ então $b(b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1}) = 0$, como B é um domínio de integridade e $b \neq 0$ então devemos ter $b^{n-1} + a_1 b^{n-2} + \cdots + a_{n-1} = 0$ o que contradiz o fato de n ser o grau mínimo de uma equação para a dependência integral de b, logo $a_n \neq 0$ e como A é corpo, a_n é uma unidade. Agora como $a_n = -b^n - a_1 b^{n-1} - \cdots - a_{n-1} b = b(-b^{n-1} - a_1 b^{n-2} - \cdots - a_{n-1})$ temos que $1 = b(\underbrace{-a_n^{-1} b^{n-1} - a_1 a_n^{-1} b^{n-2} - \cdots - a_{n-1} a_n^{-1}}_{\in B})$, logo b é uma unidade de B o que implica que B é um corpo.

Reciprocamente, suponha que B seja um corpo e seja $a \in A$, $a \neq 0$. Então $a^{-1} \in B$ e portanto é integral sobre A, assim temos uma equação $a^{-m} + a'_1 a^{-m+1} + \cdots + a'_m = 0$ com $a'_i \in A$. Multiplicando essa expressão por a^{m-1} temos $a^{-1} + a'_1 + a'_2 a + \cdots + a'_{m-1} a^{m-2} + a'_m a^{m-1} = 0$, logo

$$a^{-1} = -a'_1 - a'_2 a - \cdots - a'_{m-1} a^{m-2} - a'_m a^{m-1} \in A,$$

logo A é um corpo. □

Lembrando a última aula. Provamos:

Proposição. *Seja $B \supseteq A$ uma extensão integral de anéis.*

a. Se I é um ideal de B então B/I é integral sobre $A/A \cap I$.

b. Se S é um subconjunto multiplicativo de A, então $S^{-1}B$ é integral sobre $S^{-1}A$.

c. Se B é um domínio, então B é um corpo se, e somente se, A é um corpo.

Corolário 171. *Seja $B \supseteq A$ uma extensão integral. Seja $\mathfrak{q}$ um ideal primo de B e seja $\mathfrak{p} = \mathfrak{q} \cap A$. Então $\mathfrak{q}$ é maximal se, e somente se, $\mathfrak{p}$ é maximal.*

Demonstração. Primeiramente, observe que $\mathfrak{p}$ é um ideal primo de A pois se $i : A \hookrightarrow B$ é o homomorfismo inclusão então $\mathfrak{p} = \mathfrak{q} \cap A = i^{-1}(\mathfrak{q})$. Logo os anéis $B/\mathfrak{q}$ e $A/\mathfrak{p}$ são domínios de integridade e da Proposição 169 segue que $B/\mathfrak{q}$ é integral sobre $A/\mathfrak{p}$. Logo, da proposição anterior temos que $B/\mathfrak{q}$ é um corpo se, e somente se, $A/\mathfrak{p}$ é um corpo. Portanto $\mathfrak{q}$ é maximal se, e somente se, $\mathfrak{p}$ é maximal. □

Teorema 172. *(**Incomparabilidade**) Seja $A \subseteq B$ uma extensão integral. Se $\mathfrak{q} \subseteq \mathfrak{q}'$ são ideais primos de B tais que $\mathfrak{q} \cap A = \mathfrak{q}' \cap A$ então $\mathfrak{q} = \mathfrak{q}'$.*

Demonstração. Seja $\mathfrak{p} = \mathfrak{q} \cap A$, então pela prova do Corolário anterior $\mathfrak{p}$ é um ideal primo de A e seja $S = A - \mathfrak{p}$. Temos que a localização $A_{\mathfrak{p}} = S^{-1}A$ é um anel local (veja Exemplo 85 Aula 10) com único ideal maximal $S^{-1}\mathfrak{p}$: Como o único ideal maximal de $A_{\mathfrak{p}}$ é primo, ele é $S^{-1}\mathfrak{p}'$ onde $\mathfrak{p}'$ é um ideal primo de A que não intercepta S, logo $\mathfrak{p}' \subseteq \mathfrak{p}$. Como localização preserva inclusões temos que $S^{-1}\mathfrak{p}' \subseteq S^{-1}\mathfrak{p}$, segue da maximalidade de $S^{-1}\mathfrak{p}'$ que $S^{-1}\mathfrak{p}' = S^{-1}\mathfrak{p}$.

Por outro lado, segue da Proposição 169 que $S^{-1}A \subseteq S^{-1}B$ é uma extensão integral. Mais ainda, $S^{-1}\mathfrak{q} \subseteq S^{-1}\mathfrak{q}'$ são ambos ideais primos de $S^{-1}B$ já que $S \cap \mathfrak{q} = S \cap \mathfrak{q}' = \emptyset$ (suponha que existe $x \in S \cap \mathfrak{q}$ então $x \in S$ e $x \in \mathfrak{q}$ logo $x \in A$ e $x \in \mathfrak{q}$ e $x \notin \mathfrak{p}$ ou seja $x \in \mathfrak{p}$ e $x \notin \mathfrak{p}$, contradição) e $S^{-1}\mathfrak{p} = S^{-1}(\mathfrak{q} \cap A) = S^{-1}(\mathfrak{q}' \cap A)$ ou seja $S^{-1}\mathfrak{p} = S^{-1}\mathfrak{q} \cap S^{-1}A = S^{-1}\mathfrak{q}' \cap S^{-1}A$. Segue do Corolário 171 que $S^{-1}\mathfrak{q}$ e $S^{-1}\mathfrak{q}'$ são ideais maximais de $S^{-1}B$, mas $S^{-1}\mathfrak{q} \subseteq S^{-1}\mathfrak{q}'$ o que implica $S^{-1}\mathfrak{q} = S^{-1}\mathfrak{q}'$. Seja $\rho : B \to S^{-1}B$ o mapa de localização então $\rho^{-1}(S^{-1}\mathfrak{q}) = \rho^{-1}(S^{-1}\mathfrak{q}')$ segue da prova do Teorema 98 (Teorema de Localização e Ideais primos) que $\mathfrak{q} = \mathfrak{q}'$. □

Teorema 173. (Lying Over) *Seja $B \supseteq A$ uma extensão integral e seja $\mathfrak{p}$ um ideal primo de A. Então existe um ideal primo $\mathfrak{q}$ de B tal que $\mathfrak{q} \cap A = \mathfrak{p}$.*

$$\begin{array}{ccc} B & \supset & \exists \mathfrak{q}\text{-primo} \mid \mathfrak{q} \cap A = \mathfrak{p} \\ \cup & \textit{integral} & \uparrow \\ A & \supset & \mathfrak{p}\text{-primo} \end{array}$$

Demonstração. Como $\mathfrak{p}$ é um ideal primo de A então a localização de A por $S = A - \mathfrak{p}$, $A_\mathfrak{p} = S^{-1}A$ é um anel local com único ideal maximal $S^{-1}\mathfrak{p}$ (veja a prova do Teorema de Incomparabilidade).

Por outro lado, o seguinte diagrama

$$\begin{array}{ccc} A & \xhookrightarrow{\ i\ } & B \\ {\scriptstyle \rho_A}\downarrow & & \downarrow{\scriptstyle \rho_B} \\ S^{-1}A & \xhookrightarrow{\ i_S\ } & S^{-1}B \end{array}$$

comuta, i.e., $i_S \circ \rho_A = \rho_B \circ i$. Segue da Proposição 169 que $S^{-1}B$ é integral sobre $S^{-1}A$, logo se $\mathfrak{n}$ é um ideal maximal de $S^{-1}B$ ($\mathfrak{n}$ existe pois $0 \notin S = A - \mathfrak{p}$ e logo $S^{-1}B \neq 0$ e logo tem um ideal maximal) então segue do Corolário anterior que $\mathfrak{m} = \mathfrak{n} \cap S^{-1}A = i_S^{-1}(\mathfrak{n})$ é um ideal maximal de $S^{-1}A$. Como $S^{-1}A$ é local segue que $\mathfrak{m} = S^{-1}\mathfrak{p}$. Seja $\mathfrak{q} = \rho_B^{-1}(\mathfrak{n})$, então $\mathfrak{q}$ é ideal primo de B e temos que $\mathfrak{q} \cap A = i^{-1}(\mathfrak{q}) = i^{-1}(\rho_B^{-1}(\mathfrak{n})) = (\rho_B \circ i)^{-1}(\mathfrak{n}) = (i_S \circ \rho_A)^{-1}(\mathfrak{n}) = \rho_A^{-1}(i_S^{-1}(\mathfrak{n})) = \rho_A^{-1}(\mathfrak{m}) = \rho_A^{-1}(S^{-1}\mathfrak{p}) = \mathfrak{p}$ onde a última igualdade segue da prova do Teorema 98 (Teorema de Localização e Ideais primos) pois $\mathfrak{p}$ é um ideal primo de A tal que $S \cap \mathfrak{p} = \emptyset$. □

Teorema 174. (Going-Up) *Seja $B \supseteq A$ uma extensão integral. Seja $\mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ uma cadeia de ideais primos de A e $\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_m$, com $m < n$, uma cadeia de ideais primos de B tais que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para todo $i = 1, \ldots, m$. Então a cadeia $\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_m$ pode ser estendida a uma cadeia $\mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ tal que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para todo $i = 1, \ldots, n$.*

$$\begin{array}{ccccccccccccc} B & \supset & \exists \mathfrak{q}_n & \supsetneq & \cdots & & \supsetneq & \mathfrak{q}_m & \supsetneq & \cdots & \supsetneq & \mathfrak{q}_1 & \textit{primos} \\ \cup & & \textit{int} & \uparrow & & \mathfrak{q}_j \cap A = \mathfrak{p}_j & 1 \leq j \leq n & \uparrow & & \mathfrak{q}_i \cap A = \mathfrak{p}_i & 1 \leq i \leq m & \uparrow & \\ A & \supset & \mathfrak{p}_n & \supsetneq & \cdots & & \supsetneq & \mathfrak{p}_m & \supsetneq & \cdots & \supsetneq & \mathfrak{p}_1 & \textit{primos} \end{array}$$

Demonstração. Usaremos a Lei Modular: Se $J \subseteq I$ ou $K \subseteq I$ então $I \cap (J + K) = I \cap J + I \cap K$ (Aula 2 e Ex. 11.6 Lista 1). E os isomorfismo da Proposição 53: $(L/N)/(M/N) \simeq L/M$ e $\frac{(M_1+M_2)}{M_1} \simeq \frac{M_2}{(M_1 \cap M_2)}$ (Aula 7, Ex 1. Lista 3).

Por indução podemos reduzir ao caso $m = 1$ e $n = 2$. Sejam $\overline{A} = A/(\mathfrak{q}_1 \cap A)$ e $\overline{B} = B/\mathfrak{q}_1$ então $\overline{A} \subseteq \overline{B}$ e $\overline{B}$ é integral sobre $\overline{A}$ pela Proposição 169 e $\overline{\mathfrak{p}}_2 = \mathfrak{p}_2/(\mathfrak{q}_1 \cap A)$ é um ideal primo de $\overline{A}$. Logo pelo Teorema Lying Over (Teorema 173) existe um ideal primo $\overline{\mathfrak{q}}_2$ de $\overline{B}$ tal que $\overline{\mathfrak{q}}_2 \cap \overline{A} = \overline{\mathfrak{p}}_2$. Pelo TCI o ideal primo $\overline{\mathfrak{q}}_2$ de $\overline{B}$ corresponde a um ideal primo $\mathfrak{q}_2$ de B tal que $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$. Logo $(\mathfrak{q}_2/\mathfrak{q}_1) \cap (A/(\mathfrak{q}_1 \cap A)) = \mathfrak{p}_2/(\mathfrak{q}_1 \cap A)$.

Observe que como $A \cap \mathfrak{q}_1 = \mathfrak{p}_1 \subsetneq \mathfrak{p}_2$ então $\mathfrak{q}_1 \cap \mathfrak{p}_2 = \mathfrak{q}_1 \cap (\mathfrak{p}_2 \cap A) = A \cap \mathfrak{q}_1$. Agora, temos

$$\frac{\mathfrak{p}_2+\mathfrak{q}_1}{\mathfrak{q}_1} \overset{iso}{=} \frac{\mathfrak{p}_2}{\mathfrak{p}_2 \cap \mathfrak{q}_1} \overset{obs}{=} \frac{\mathfrak{p}_2}{A \cap \mathfrak{q}_1} \overset{LO}{=} \left(\frac{\mathfrak{q}_2}{\mathfrak{q}_1}\right) \cap \left(\frac{A}{\mathfrak{q}_1 \cap A}\right) \overset{iso}{=} \left(\frac{\mathfrak{q}_2}{\mathfrak{q}_1}\right) \cap \left(\frac{A+\mathfrak{q}_1}{\mathfrak{q}_1}\right) = \frac{\mathfrak{q}_2 \cap (A+\mathfrak{q}_1)}{\mathfrak{q}_1}$$

Segue do Teorema de Isomorfismos que $\mathfrak{p}_2 + \mathfrak{q}_1 = \mathfrak{q}_2 \cap (A + \mathfrak{q}_1)$(*). Vejamos que

$\mathfrak{p}_2 \overset{\mathfrak{p}_1 \subsetneq \mathfrak{p}_2}{=} \mathfrak{p}_2 + \mathfrak{p}_1 \overset{\mathfrak{p}_1 = A \cap \mathfrak{q}_1}{=} \mathfrak{p}_2 + (A \cap \mathfrak{q}_1) \overset{\mathfrak{p}_2 \subseteq A}{=} (A \cap \mathfrak{p}_2) + (A \cap \mathfrak{q}_1) \overset{LM}{=} A \cap (\mathfrak{p}_2 + \mathfrak{q}_1) \overset{(*)}{=} A \cap \mathfrak{q}_2 \cap (A + \mathfrak{q}_1) = A \cap \mathfrak{q}_2$ pois $A \cap \mathfrak{q}_2 \subseteq A \subseteq A + \mathfrak{q}_1$. □

Por último, resta ver que a inclusão $\mathfrak{q}_1 \subseteq \mathfrak{q}_2$ é estrita. Suponha que $\mathfrak{q}_1 = \mathfrak{q}_2$ então $\mathfrak{p}_1 = \mathfrak{q}_1 \cap A = \mathfrak{q}_2 \cap A = \mathfrak{p}_2$, contradição.

Corolário 175. *Seja $A \subseteq B$ uma extensão integral de anéis. Então* $\dim A = \dim B$ *(veja Definição 126).*

Demonstração. Dada uma cadeia de ideais primos em A: $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ então pelo Teorema Going-Up existe uma cadeia de ideais primos em B: $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ com $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para $i = 0, \ldots, n$ e por tanto $\dim B \geq \dim A$.

Reciprocamente, dada uma cadeia de ideais primos em B: $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$ segue da prova do Corolário 171 que os ideais $\mathfrak{p}_i = A \cap \mathfrak{q}_i$ são ideais primos de A para todo $i = 0, \ldots, n$ e claramente $\mathfrak{p}_0 \subseteq \mathfrak{p}_1 \subseteq \cdots \subseteq \mathfrak{p}_n$. Segue do Teorema de Incomparabilidade (Teorema 172) que os $\mathfrak{p}_i$'s são todos distintos e logo definem uma cadeia $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ de ideais primos de A o que mostra que $\dim A \geq \dim B$. □

Proposição 176. *Sejam $A \subseteq B$ anéis e $\mathcal{C}(A, B)$ o fecho integral de A em B. Seja S um subconjunto multiplicativo de A. Então $S^{-1}\mathcal{C}(A, B)$ é o fecho integral de $S^{-1}A$ em $S^{-1}B$.*

Demonstração. Queremos provar que $S^{-1}\mathcal{C}(A, B) = \mathcal{C}(S^{-1}A, S^{-1}B)$. Segue da definição de fecho integral que $A \subseteq \mathcal{C}(A, B)$ é uma extensão integral, logo da Proposição 169 temos que $S^{-1}A \subseteq S^{-1}\mathcal{C}(A, B)$ é também uma extensão integral. Logo dado um elemento $x \in S^{-1}\mathcal{C}(A, B) \subseteq S^{-1}B$ então x é integral sobre $S^{-1}A$ logo $x \in \mathcal{C}(S^{-1}A, S^{-1}B)$ e temos $S^{-1}\mathcal{C}(A, B) \subseteq \mathcal{C}(S^{-1}A, S^{-1}B)$. Reciprocamente, se $\frac{b}{s} \in S^{-1}B$ é integral sobre $S^{-1}A$ então existe uma equação da forma $\left(\frac{b}{s}\right)^n + \frac{a_1}{s_1}\left(\frac{b}{s}\right)^{n-1} + \cdots + \frac{a_n}{s_n} = 0$ onde $a_i \in A$ e $s_i \in S$ para todo $i = 1, \ldots, n$. Então multiplicando a equação por s^n temos $b^n + \frac{sa_1}{s_1}b^{n-1} + \cdots + \frac{s^{n-1}a_{n-1}}{s_{n-1}}b + \frac{s^n a_n}{s_n} = 0$. Seja $t = s_1 \cdot \cdots \cdot s_n$ então multiplicando novamente por t^n temos: $(bt)^n + (s(\widehat{s_1} \cdot \cdots \cdot s_n)a_1)(bt)^{n-1} + \cdots + (s^{n-1}t^{n-2}(s_1 \cdot \cdots \cdot \widehat{s_{n-1}} \cdot s_n)a_{n-1})(bt) + (s^n t^{n-1}(s_1 \cdot \cdots \cdot \widehat{s_n})a_n) = 0$ que é uma equação para a dependência integral de bt sobre A. Logo $bt \in \mathcal{C}(A, B)$ o portanto $\frac{b}{s} = \frac{bt}{st} \in S^{-1}\mathcal{C}(A, B)$, assim $\mathcal{C}(S^{-1}A, S^{-1}B) \subseteq S^{-1}\mathcal{C}(A, B)$. □

Definição 177. Um domínio de integridade A é dito **integralmente fechado** (sem qualificação) ou **normal** se ele é integralmente fechado sobre seu corpo de frações, i.e., se $\mathcal{C}(A, \mathrm{Frac}(A)) = A$.

Proposição 178. *Todo DFU é integralmente fechado.*

Demonstração. **Exercício 1.** □

Na última aula provamos que:

Proposição. *Se $A \subseteq B$ são anéis e S é um subconjunto multiplicativo de A, então $S^{-1}\mathcal{C}(A,B) = \mathcal{C}(S^{-1}A, S^{-1}B)$.*

e definimos:

Definição. Um domínio de integridade A é dito **integralmente fechado** (sem qualificação) ou **normal** se ele é integralmente fechado sobre seu corpo de frações, i.e., se $\mathcal{C}(A, \mathrm{Frac}(A)) = A$.

Provaremos a seguir que a propriedade de um domínio ser "integralmente fechado" é local.

Proposição 179. *Seja A um domínio de integridade. Então as seguintes afirmações são equivalentes:*

a. A é integralmente fechado;

b. $A_{\mathfrak{p}}$ é integralmente fechado para todo ideal primo $\mathfrak{p}$ de A;

c. $A_{\mathfrak{m}}$ é integralmente fechado para todo ideal maximal $\mathfrak{m}$ de A;

Demonstração. Primeiramente provaremos que se A é um domínio e $S \subseteq A$ um subconjunto multiplicativo tal que $0 \notin S$, então $S^{-1}A$ é também um domínio (observe que se $0 \in S$ então $S^{-1}A = 0$ que não é domínio pois $1 = 0$). Sejam $\frac{a}{s}, \frac{b}{t} \in S^{-1}A$ (com $a, b \in A$ e $s, t \in S$) elementos tais que $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} = \frac{0}{1}$ em $S^{-1}A$, então existe $s' \in S$ tal que $s'ab = 0$ em A, como A é domínio e $0 \notin S$ então ou $a = 0$ ou $b = 0$. Logo ou $\frac{a}{s} = \frac{0}{1}$ ou $\frac{b}{s} = \frac{0}{1}$ e por tanto $S^{-1}A$ é um domínio. Alem disso, o mapa de localização $\rho : A \to S^{-1}A$ é injetivo, pois se $\rho(a) = \rho(b)$ então $\frac{a}{1} = \frac{b}{1}$ em $S^{-1}A$ logo existe $s \in S$ tal que $sa = sb$ em A, logo $s(a-b) = 0$ e como A é domínio e $0 \notin S$ então $a = b$. Logo $A \simeq \rho(A) \subseteq S^{-1}A$, em particular podemos identificar os elementos $s \in S$ com $\frac{s}{1} \in \rho(S)$.

Vejamos que $S^{-1}\,\mathrm{Frac}(A) = \mathrm{Frac}(S^{-1}A)$. Chamaremos de $S_0 = A - 0$ então $\mathrm{Frac}(A) = S_0^{-1}A$ e analogamente $S_0' = S^{-1}A - \frac{0}{1}$, logo $\mathrm{Frac}(S^{-1}A) = (S_0')^{-1}(S^{-1}A)$. Observe que $\frac{a}{s} = \frac{0}{1}$ em $S^{-1}A \Leftrightarrow$existe $t \in S$ $(t \neq 0)$ tal que $ta = 0$ em A (domínio)$\Leftrightarrow a = 0$. Isto implica que $S_0' = \{\frac{a}{s}$ com $a \in S_0, s \in S\}$. Seja agora, $\frac{a}{s} \in S^{-1}\,\mathrm{Frac}(A)$ logo $s \in S$ e $a \in \mathrm{Frac}(A)$, ou seja $a = \frac{a'}{s_0}$ com $a' \in A$ e $s_0 \in S_0$. Logo $\frac{a}{s} = \frac{\frac{a'}{s_0}}{\frac{s}{1}} = \frac{a'}{s_0 s} = \frac{\frac{a'}{s}}{\frac{s_0}{1}} \in (S_0')^{-1}(S^{-1}A) = \mathrm{Frac}(S^{-1}A)$. Por outro lado se, $\frac{a}{s_0'} \in \mathrm{Frac}(S^{-1}A)$ então $a \in S^{-1}A$ e $s_0' \in S_0'$. Logo $a = \frac{a'}{s}$

com $a' \in A$ e $s \in S$ e $s'_0 = \frac{s_0}{s'}$ com $s_0 \in S_0$ e $s' \in S$, assim $\frac{a}{s'_0} = \frac{\frac{a'}{s}}{\frac{s_0}{s'}} = \frac{a's'}{ss_0} = \frac{\frac{a's'}{s_0}}{\frac{s}{1}} \in S^{-1}\operatorname{Frac}(A)$.

Segue que se A é um domínio e $S = A - \mathfrak{p}$ onde $\mathfrak{p}$ é um ideal primo de A então $0 \notin S$ e logo $S^{-1}A = A_{\mathfrak{p}}$ é um domínio, primeira condição para ser integralmente fechado.

Seja $i : A \hookrightarrow \mathcal{C}(A, \operatorname{Frac}(A))$ a inclusão de A em $\mathcal{C}(A, \operatorname{Frac}(A))$. Segue da Proposição 176 e a observação anterior que $S^{-1}\mathcal{C}(A, \operatorname{Frac}(A)) = \mathcal{C}(S^{-1}A, S^{-1}\operatorname{Frac}(A)) = \mathcal{C}(S^{-1}A, \operatorname{Frac}(S^{-1}A))$ logo $S^{-1}i : S^{-1}A \hookrightarrow \mathcal{C}(S^{-1}A, \operatorname{Frac}(S^{-1}A))$. Então A é integralmente fechado se, e somente se, $i(A) = A = \mathcal{C}(A, \operatorname{Frac}(A))$ se, e somente se, i é sobrejetiva. Segue da propriedade local dos homomorfismo sobrejetivos (Proposição 96) que i é sobrejetiva se, e somente se, $S^{-1}i$ é sobrejetiva para todo ideal primo $\mathfrak{p}$ de A, mas isto acontece se, e somente se, $S^{-1}A = A_{\mathfrak{p}}$ é integralmente fechado para todo ideal primo $\mathfrak{p}$ de A. Analogamente se considerarmos todos os ideais maximais $\mathfrak{m}$ de A. □

Definição 180. Sejam $A \subseteq B$ anéis e seja I um ideal de A. Um elemento de B é dito **integral** sobre I se satisfaz uma equação de dependência integral sobre A na qual todos os coeficientes (não "mônicos") pertencem a I. O **fecho integral** ou **normalização** $\mathcal{C}(I, B)$ do ideal I em B é o conjunto dos elementos de B que são integrais sobre I.

Lema 181. *Seja I um ideal de A com $A \subseteq B$ anéis. Então o fecho integral de I em B, $\mathcal{C}(I, B)$, é o radical de $I\mathcal{C}(A, B)$ (e logo é fechado sob adição e multiplicação, pois $\sqrt{I\mathcal{C}(A, B)}$ é um ideal de B).*

Demonstração. Seja $b \in B$ um elemento integral sobre I (i.e. $b \in \mathcal{C}(I, B)$) então temos que existe uma equação da forma $b^n + a_1 b^{n-1} + \cdots + a_n = 0$ com $a_i \in I \subseteq A \subseteq \mathcal{C}(A, B)$. Logo $b \in \mathcal{C}(A, B)$ e como $b^n = -a_1 b^{n-1} - \cdots - a_n \in I\mathcal{C}(A, B)$ (pois cada $a_i b^{n-i} \in I\mathcal{C}(A, B)$ e o termo constante $a_n = a_n 1_A \in I\mathcal{C}(A, B)$) temos que $b \in \sqrt{I\mathcal{C}(A, B)}$. Reciprocamente, se $b \in \sqrt{I\mathcal{C}(A, B)}$ então existe $n > 0$ tal que $b^n \in I\mathcal{C}(A, B)$ logo $b^n = \sum_{i=1}^{m} a_i x_i$ onde $a_i \in I$ e $x_i \in \mathcal{C}(A, B)$. Como cada x_i é integral sobre A segue do Corolário 163 que $M = A[x_1, \ldots, x_m]$ é um A-modulo f.g. Logo podemos usar a Proposição 58 (Seja M um A-módulo f.g., I um ideal de A e f um endomorfismo do A-módulo M tal que $f(M) \subseteq IM$. Então f satisfaz uma equação da forma $f^k + c_1 f^{k-1} + \cdots + c_k \operatorname{id} = 0$ onde $c_i \in I$) com $f : M \to M$ como sendo a multiplicação por b^n. Vejamos que $f(M) \subseteq IM$, seja $p(x_1, \ldots, x_m) \in M = A[x_1, \ldots, x_m]$ então $b^n p(x_1, \ldots, x_m) = \sum_{i=1}^{m} \underbrace{a_i}_{\in I} \underbrace{x_i p(x_1, \ldots, x_m)}_{\in M} \in IM$. Logo $f^k + c_1 f^{k-1} + \cdots + c_k \operatorname{id} = 0$ para certos $c_i \in I$ aplicando isto em b^n temos $b^{n^{k+1}} + c_1 b^{n^k} + \cdots + c_k b^n = 0$ logo b é integral sobre I, $b \in \mathcal{C}(I, B)$. □

Proposição 182. *Sejam $A \subseteq B$ domínios de integridade, A integralmente fechado e seja $b \in B$ um elemento integral sobre um ideal I de A. Então b é um elemento algébrico sobre o corpo de frações $\mathbf{k} = \mathrm{Frac}(A)$ de A e se seu polinômio minimal[1] sobre $\mathbf{k}$ é $p(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ então $a_1, \ldots, a_n \in \sqrt{I}$.*

Demonstração. Claramente, como b é integral sobre $I \subseteq A \subseteq \mathbf{k}$ então b é algébrico sobre $\mathbf{k}$. Seja L uma extensão de corpos de $\mathbf{k}$ a qual contem todas as raízes $b = b_1, \ldots, b_n$ de $p(x)$ em $\overline{\mathbf{k}}$ (onde $\overline{\mathbf{k}}$ é o fecho algébrico de $\mathbf{k}$). Seja $f(x)$ uma equação da dependência integral de b sobre I, então f é um polinômio em $\mathbf{k}[x]$ que tem b como raiz, logo $p(x) \mid f(x)$ em $\mathbf{k}[x]$. Como $p(b_i) = 0$ então $f(b_i) = 0$, logo b_i é integral sobre I para todo $i = 1, \ldots, n$.

Agora $p(x) = \prod_{i=1}^{n}(x - b_i) = x^n + a_1 x^{n-1} + \cdots + a_n$, então os coeficientes a_i's são polinomiais nos b_i's e pelo Lema 181 o conjunto dos elementos de B integrais sobre I é fechado sob adição e multiplicação, logo os $a_i \in \mathbf{k} = \mathrm{Frac}(A)$ são integrais sobre I e portanto integrais sobre A, assim $a_i \in \mathcal{C}(A, \mathrm{Frac}(A))$. Mas A é integralmente fechado, logo $\mathcal{C}(A, \mathrm{Frac}(A)) = A$ e $a_i \in A$ para todo $i = 1, \ldots, n$. Finalmente, aplicando novamente o Lema 181 com $B = A$ temos: $a_i \in \mathcal{C}(I, A) = \sqrt{I\mathcal{C}(A, A)} = \sqrt{IA} = \sqrt{I}$. □

A nossa intenção agora é provar o "**Teorema Going-down**", mas para isso precisaremos provar antes alguns lemas técnicos.

Vimos na Aula 1 que se $f : A \to B$ é um homomorfismo de anéis e J é um ideal de B, então a pré-imagem $f^{-1}(J)$ é sempre um ideal de A. Mas se I é um ideal de A, o conjunto $f(I)$ não necessariamente é um ideal de B. Por isso consideraremos nos lemas seguintes o ideal $Bf(I)$ que é o ideal de B gerado por $f(I)$.

Lema 183. *Seja $f : A \to B$ um homomorfismo de anéis e sejam I um ideal de A e J um ideal de B. Então:*

a. $I \subseteq f^{-1}(Bf(I))$;

b. $Bf(f^{-1}(J)) \subseteq J$;

c. $f^{-1}(J) = f^{-1}(Bf(f^{-1}(J)))$;

d. $Bf(I) = Bf(f^{-1}(Bf(I)))$;

Demonstração. Para qualquer função $f : A \to B$ e subconjuntos $I \subseteq A$ e $J \subseteq B$ vale $f(f^{-1}(J)) \subseteq J$ e $I \subseteq f^{-1}(f(I))$. Agora se I é um ideal de A então $f(I) \subseteq Bf(I)$ logo $I \subseteq f^{-1}(f(I)) \subseteq f^{-1}(Bf(I))$ e se J é um ideal de B então $Bf(f^{-1}(J)) \subseteq BJ = J$, provamos $(a.)$ e $(b.)$. Aplicando f^{-1} a $(b.)$ segue que $f^{-1}(Bf(f^{-1}(J))) \subseteq f^{-1}(J)$ e fazendo $I = f^{-1}(J)$ em $(a.)$ temos $f^{-1}(J) \subseteq f^{-1}(Bf(f^{-1}(J)))$, assim provamos o item $(c.)$. Por último, aplicando f a

1 i.e., polinômio mônico como coeficientes em $\mathbf{k}$ de menor grau que admite b como raiz. Ele é irredutível e divide qualquer outro polinômio em $\mathbf{k}[x]$ que tenha b como raiz.

$(a.)$ temos $f(I) \subseteq f(f^{-1}(Bf(I)))$ e logo $Bf(I) \subseteq Bf(f^{-1}(Bf(I)))$ e fazendo $J = Bf(I)$ em $(b.)$ segue que $Bf(f^{-1}(Bf(I))) \subseteq Bf(I)$, assim temos $(d.)$. □

Lema 184. *Seja $f : A \to B$ um homomorfismo de anéis e seja $\mathfrak{p}$ um ideal primo de A. Então $\mathfrak{p} = f^{-1}(\mathfrak{q})$ para algum ideal primo $\mathfrak{q}$ de B se, e somente se, $f^{-1}(Bf(\mathfrak{p})) = \mathfrak{p}$.*

Demonstração. Se $\mathfrak{p} = f^{-1}(\mathfrak{q})$ para algum ideal primo $\mathfrak{q}$ de B então segue do Lema 183 $(c.)$ que $f^{-1}(Bf(f^{-1}(\mathfrak{q}))) = f^{-1}(\mathfrak{q})$, ou seja $f^{-1}(Bf(\mathfrak{p})) = \mathfrak{p}$. Reciprocamente, se J denota o ideal $Bf(\mathfrak{p})$ de B, então $\mathfrak{p} = f^{-1}(J)$, mas J não é necessariamente primo. Seja $S = f(A - \mathfrak{p})$, então S é um subconjunto multiplicativo de B: sejam $s_1, s_2 \in S$ então existem $a_1, a_2 \in A - \mathfrak{p}$ tal que $s_i = f(a_i)$ para $i = 1, 2$ logo $s_1 s_2 = f(a_1)f(a_2) = f(a_1 a_2)$, como $A - \mathfrak{p}$ é um conjunto multiplicativo então $a_1 a_2 \in A - \mathfrak{p}$ logo $s_1 s_2 \in S$. Por outro lado, $S^{-1}J$ é um ideal próprio de $S^{-1}B$: suponha que $S^{-1}J = S^{-1}B$ então $\frac{1}{1} \in S^{-1}J$ logo existe $s \in S$ e $b \in J$ tal que $\frac{1}{1} = \frac{b}{s}$ logo existe $t \in S$ tal que $S \ni ts = tb \in J$ o que implica que $S \cap J \neq \emptyset$. Mas se $s \in S \cap J$ então existe $a \in A - \mathfrak{p}$ tal que $s = f(a)$ e por outro lado $a \in f^{-1}(s) \in f^{-1}(J) = \mathfrak{p}$, que é uma contradição. Logo $S^{-1}J$ é um ideal próprio de $S^{-1}B$ e $S \cap J = \emptyset$. Isto implica que $S^{-1}J$ está contido num ideal maximal $\mathfrak{m}$ de $S^{-1}B$. Seja $\mathfrak{q}$ o ideal primo de B que não intercepta S e que satisfaz $\mathfrak{m} = S^{-1}\mathfrak{q}$, queremos provar que $\mathfrak{p} = f^{-1}(\mathfrak{q})$. Vejamos que $J \subseteq \mathfrak{q}$: suponha que não, então existe $j \in J$ tal que $j \notin \mathfrak{q}$ logo $\frac{j}{1} \in S^{-1}J$ mas $\frac{j}{1} \notin S^{-1}\mathfrak{q}$ (pois se $\frac{j}{1} \in S^{-1}\mathfrak{q}$ então $\frac{j}{1} = \frac{q}{s}$ para certos $q \in \mathfrak{q}$ e $s \in S$, logo existe $t \in S$ tal que $tjs = tq \in \mathfrak{q}$ e como $j \notin \mathfrak{q}$ e $\mathfrak{q}$ é primo então necessariamente $ts \in \mathfrak{q}$ o que contradiz o fato de $\mathfrak{q} \cap S = \emptyset$), o que contradiz o fato de $S^{-1}J$ estar contido em $S^{-1}\mathfrak{q}$. Logo, temos que $\mathfrak{p} = f^{-1}(J) \subseteq f^{-1}(\mathfrak{q})$. Suponha que $\mathfrak{p} \subsetneq f^{-1}(\mathfrak{q})$, isto implica que existe $a \in f^{-1}(\mathfrak{q})$ tal que $a \notin \mathfrak{p}$, i.e., $a \in A - \mathfrak{p}$. Logo $f(a) \in \mathfrak{q}$ e $f(a) \in f(A - \mathfrak{p}) = S$, o que contradiz o fato de $\mathfrak{q} \cap S = \emptyset$. Logo $\mathfrak{p} = f^{-1}(\mathfrak{q})$. □

AULA 23: 07/11/2014

AULA 23

Na última aula provamos:

Lema 1. Seja I um ideal de A com $A \subseteq B$ anéis. Então o fecho integral de I em B, $\mathcal{C}(I, B)$, é o radical de $I\mathcal{C}(A, B)$ (e logo é fechado sob adição e multiplicação, pois $\sqrt{I\mathcal{C}(A, B)}$ é um ideal de B).

Lema 2. Seja $f : A \to B$ um homomorfismo de anéis e seja $\mathfrak{p}$ um ideal primo de A. Então $\mathfrak{p} = f^{-1}(\mathfrak{q})$ para algum ideal primo $\mathfrak{q}$ de B se, e somente se, $f^{-1}(Bf(\mathfrak{p})) = \mathfrak{p}$.

Proposição 3. Sejam $A \subseteq B$ domínios de integridade, A integralmente fechado e seja $b \in B$ um elemento integral sobre um ideal I de A. Então b é um elemento algébrico sobre o corpo de frações $\mathbf{k} = \mathrm{Frac}(A)$ de A e se seu polinômio minimal sobre $\mathbf{k}$ é $p(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ então $a_1, \ldots, a_n \in \sqrt{I}$.

Teorema 185. *(**Going-down**) Sejam $A \subseteq B$ domínios de integridade, A integralmente fechado, B integral sobre A. Seja $\mathfrak{p}_1 \supsetneq \cdots \supsetneq \mathfrak{p}_n$ uma cadeia de ideais primos de A e seja $\mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_m$ com $m < n$ uma cadeia de ideais primos de B tais que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para $i = 1, \ldots, m$. Então a cadeia $\mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_m$ pode ser estendida a uma cadeia $\mathfrak{q}_1 \supsetneq \cdots \supsetneq \mathfrak{q}_n$ tal que $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ para todo $i = 1, \ldots, n$.*

$$\begin{array}{ccccccccccccc} dom B & \supset & \mathfrak{q}_1 & \supsetneq & \cdots & & \supsetneq & \mathfrak{q}_m & \supsetneq & \cdots & \supsetneq & \exists \mathfrak{q}_n & primos \\ int\cup & & \uparrow & & \mathfrak{q}_i \cap A = \mathfrak{p}_i & 1\leq i\leq m & \uparrow & & \mathfrak{q}_i \cap A = \mathfrak{p}_i & 1\leq i\leq n & \uparrow & & \\ i.f.\ A & \supset & \mathfrak{p}_1 & \supsetneq & \cdots & & \supsetneq & \mathfrak{p}_m & \supsetneq & \cdots & \supsetneq & \mathfrak{p}_n & primos \end{array}$$

Demonstração. Como na prova do Teorema Going-Up reduzimos imediatamente ao caso $m = 1$ e $n = 2$. Então temos que mostrar que se $\mathfrak{p}_1 \supseteq \mathfrak{p}_2$ são ideais primos de A e $\mathfrak{q}_1$ um ideal primo de B tal que $\mathfrak{q}_1 \cap A = \mathfrak{p}_1$, então existe um ideal primo $\mathfrak{q}_2$ de B tal que $\mathfrak{q}_1 \supseteq \mathfrak{q}_2$ e $\mathfrak{q}_2 \cap A = \mathfrak{p}_2$. Agora, como observamos na prova da Proposição 179, B é um domínio logo o mapa de localização $\rho : B \to B_{\mathfrak{q}_1}$ é injetivo e podemos identificar $B \simeq \rho(B) \subseteq B_{\mathfrak{q}_1}$. Defina, então $f : A \hookrightarrow B_{\mathfrak{q}_1}$ como sendo a composição dos homomorfismos injetivos $A \overset{i}{\hookrightarrow} B \overset{\rho}{\hookrightarrow} B_{\mathfrak{q}_1}$. Aplicando o Lema 184 a f temos que $\mathfrak{p}_2 = f^{-1}(J_2) = \rho^{-1}(J_2) \cap A$ para algum ideal primo J_2 de $B_{\mathfrak{q}_1}$ se, e somente se, $f^{-1}(B_{\mathfrak{q}_1} f(\mathfrak{p}_2)) = \mathfrak{p}_2$. Agora, um ideal primo J_2 de $B_{\mathfrak{q}_1}$ corresponde a um ideal primo $\mathfrak{q}_2$ de B contido em $\mathfrak{q}_1$ (Corolário 99), logo $J_2 = S^{-1}\mathfrak{q}_2$ onde $S = B - \mathfrak{q}_1$. Reescrevendo o anterior temos que $\mathfrak{p}_2 = \rho^{-1}(S^{-1}\mathfrak{q}_2) \cap A = \mathfrak{q}_2 \cap A$ para algum ideal primo $\mathfrak{q}_2$ de B contido em $\mathfrak{q}_1$ se, e somente se, $f^{-1}(B_{\mathfrak{q}_1} f(\mathfrak{p}_2)) = \mathfrak{p}_2$. Sem perda de generalidade podemos supor que f é a inclusão de A em $B_{\mathfrak{q}_1}$, assim só basta provar que $\mathfrak{p}_2 = f^{-1}(B_{\mathfrak{q}_1} f(\mathfrak{p}_2)) = B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A$.

Como $\mathfrak{p}_2 \subseteq A$ e $\mathfrak{p}_2 \subseteq B_{\mathfrak{q}_1}\mathfrak{p}_2$ (que é o ideal de $B_{\mathfrak{q}_1}$ gerado por $\mathfrak{p}_2$) então claramente $\mathfrak{p}_2 \subseteq B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A$. Seja $x \in B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A$, então $x = \sum_{i=1}^{k} \frac{b_i}{s_i} p_i$ onde $b_i \in B$, $s_i \in S = B - \mathfrak{q}_1$ e $p_i \in \mathfrak{p}_2$. Logo tomando denominador comum $x = \frac{\sum_{i=1}^{k} s_1 \cdots \widehat{s_i} \cdots s_n b_i p_i}{s_1 \cdots s_n} = \frac{\sum_{i=1}^{k} b_i' p_i}{s_1 \cdots s_n}$ onde $s = s_1 \cdots s_n \in S$ e $y = \sum_{i=1}^{k} b_i' p_i \in B\mathfrak{p}_2$. Como $A \subseteq B$ é uma extensão integral e logo $\mathcal{C}(A, B) = B$, segue do Lema 181 que $\mathcal{C}(\mathfrak{p}_2, B) = \sqrt{B\mathfrak{p}_2} \supseteq B\mathfrak{p}_2 \ni y$ logo y é integral sobre $\mathfrak{p}_2$. Segue da Proposição 182 que y é um elemento algébrico sobre o corpo de frações $\mathbf{k} = \mathrm{Frac}(A)$ de A e sua equação minimal sobre $\mathbf{k}$ é da forma $y^r + u_1 y^{r-1} + \cdots + u_r = 0$(*) com $u_1, \ldots, u_r \in \sqrt{\mathfrak{p}_2} = \mathfrak{p}_2$. Agora como também $x \in A$ então $x^{-1} \in \mathbf{k}$, logo multiplicando a equação (*) por $x^{-r} \in \mathbf{k}$ obtemos $(yx^{-1})^r + u_1 x^{-1}(yx^{-1})^{r-1} + \cdots + u_r x^{-r} = 0$ com $u_i x^{-i} \in \mathbf{k}$. Seja $f(t) = t^r + u_1 x^{-1} t^{r-1} + \cdots + u_r x^{-r}$ então $f(s) = f(yx^{-1}) = 0$, logo s é um elemento algébrico sobre $\mathbf{k}$ e seu polinômio minimal $p(t) = t^m + \sum_{i=0}^{m-1} h_{m-i} t^i$ com $h_j \in \mathbf{k}$ é tal que $m \leq r$. Mas se $m < r$ então $0 = p(s) = p(yx^{-1}) = x^{-m} y^m + \sum_{i=0}^{m-1} h_{m-i} x^{-i} y^i$ contradiz que (*) é a equação minimal para a dependência integral de y sobre $\mathbf{k}$, logo o grau do polinômio minimal se s deve ser $m = r$ o que implica que $f(t)$ (polinômio mônico como coeficientes em $\mathbf{k}$ de menor grau que admite s como raiz.) é o polinômio minimal

de s. Agora $s \in B$ logo é integral sobre A, assim aplicando novamente a Proposição 182 com $I = A$ temos que $u_i x^{-i} \in \sqrt{A} = A$ para todo $i = 1, \ldots, r$.

Suponha agora que $x \notin \mathfrak{p}_2$. Então $x^i \notin \mathfrak{p}_2$, pois $\mathfrak{p}_2$ é primo de A, logo $\mathfrak{p}_2 \ni u_i = (\underbrace{u_i x^{-i}}_{\in A})\underbrace{x^i}_{\in A}$ isto implica que $u_i x^{-i} \in \mathfrak{p}_2$ (aqui usamos o que acabamos de provar, que os $u_i x^{-i} \in A$ pois como $\mathfrak{p}_2$ é primo de A precisamos que ambos fatores pertençam a A para poder concluir que um deles tem que estar em $\mathfrak{p}_2$) e segue de $f(s) = 0$ que $s^r = -u_1 x^{-1} s^{r-1} - \cdots - u_r x^{-r} \in B\mathfrak{p}_2 \subseteq B\mathfrak{p}_1 = B(\mathfrak{q}_1 \cap A) \subseteq B\mathfrak{q}_1 = \mathfrak{q}_1$ o que implica (por $\mathfrak{q}_1$ ser primo) que $s \in \mathfrak{q}_1$, contradição. Logo $x \in \mathfrak{p}_2$ e por tanto $\mathfrak{p}_2 = B_{\mathfrak{q}_1}\mathfrak{p}_2 \cap A$ como requerido. □

Por último, resta ver que a inclusão $\mathfrak{q}_2 \subseteq \mathfrak{q}_1$ é estrita. Suponha que $\mathfrak{q}_2 = \mathfrak{q}_1$ então $\mathfrak{p}_2 = \mathfrak{q}_2 \cap A = \mathfrak{q}_1 \cap A = \mathfrak{p}_1$, contradição.

Provaremos a seguir o **Teorema de Normalização de Noether** o qual descreve a estrutura básica de uma álgebra f.g. sobre um corpo, para isso precisaremos do seguinte lema.

Lema 186. *Sejam* $\mathbf{k}$ *um corpo infinito e* $f \in \mathbf{k}[x_1, \ldots, x_n]$ *qualquer polinômio homogêneo*[2] *não nulo, então existem elementos* $\lambda_1, \ldots, \lambda_{n-1} \in \mathbf{k}$ *tal que* $f(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$.

Demonstração. Note que se $f(x_1, \ldots, x_n) \in \mathbf{k}[x_1, \ldots, x_n]$ é um polinômio homogêneo de grau d não nulo então $g(x_1, \ldots, x_{n-1}) = f(x_1, \ldots, x_{n-1}, 1) \in \mathbf{k}[x_1, \ldots, x_{n-1}]$ é um polinômio não necessariamente homogêneo[3] e não nulo. Esta última condição é consequência de f ser homogêneo[4], se g for nulo então deveriam existir termos em g tais que $a x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_{n-1}^{\alpha_{n-1}} = -b x_1^{\beta_1} x_2^{\beta_2} \cdots x_{n-1}^{\beta_{n-1}}$, mas isto implica $a = b$ e $\alpha_i = \beta_i$ para todo $i = 1, \ldots, n-1$ e logo a potência de x_n em f seria a mesma em ambos termos $d - \sum_{i=1}^{n-1} \alpha_i$ e logos os termos seriam cancelados na expressão de f implicando que $f = 0$, o que é uma contradição. Segue do Execício 9 Lista 2: "Seja $\mathbf{k}$ um corpo infinito e $f \in \mathbf{k}[x_1, \ldots, x_n]$ tal que $f(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n) \in \mathbf{k}^n$ então $f = 0$" que existe $(\lambda_1, \ldots, \lambda_{n-1}) \in \mathbf{k}^{n-1}$ tal que $0 \neq g(\lambda_1, \ldots, \lambda_{n-1}) = f(\lambda_1, \ldots, \lambda_{n-1}, 1)$. □

Lembramos que uma $\mathbf{k}$-álgebra A é f.g. sobre o corpo $\mathbf{k}$ se $A = \mathbf{k}[a_1, \ldots, a_n]$ para algum conjunto finito de elementos $a_1, \ldots, a_n \in A$.

Precisaremos da seguinte definição:

2 Um polinômio homogêneo é um polinômio cujos termos não nulos tem todos o mesmo grau.

3 Por exemplo $f(x, y, z) = xyz + z^2x + xy^2$ então $f(x, y, 1) = xy + x + xy^2$ não é homogêneo.

4 Note que de fato para $f(x, y, z) = xyz - xyz^2$ não nulo e não homogêneo temos $g(x, y) = f(x, y, 1) = xy - xy = 0$.

Definição 187. Dizemos que os elementos $a_1, \ldots, a_k$ de uma álgebra sobre um corpo $\mathbf{k}$ são **algebricamente independentes** sobre $\mathbf{k}$ se $p(a_1, \ldots, a_k) \neq 0$ para qualquer polinômio não nulo $p \in \mathbf{k}[x_1, \ldots, x_k]$. No caso $k = 1$ dizemos que a_1 é **transcendente** sobre $\mathbf{k}$.

Teorema 188. *(***Teorema de Normalização de Noether***) Seja* $\mathbf{k}$ *um corpo infinito e seja* $A \neq 0$ *uma* $\mathbf{k}$*-álgebra f.g. Então existem elementos* $a_1, \ldots, a_k \in A$ *que são algebricamente independentes sobre* $\mathbf{k}$ *e tal que* A *é integral sobre* $\mathbf{k}[a_1, \ldots, a_k]$.

Demonstração. Sejam $b_1, \ldots, b_n$ os geradores de A como uma $\mathbf{k}$-álgebra. Então podemos renumerar os b_i's tal que $b_1, \ldots, b_r$ são algebricamente independentes sobre $\mathbf{k}$ mas $b_1, \ldots, b_r, b_i$ (para todo $r+1 \leq i \leq n$) não o são, ou seja existe um polinômio $p_i \in \mathbf{k}[x_1, \ldots, x_r, x_{r+1}]$ tal que $p_i(b_1, b_2, \ldots, b_r, b_i) = 0$ (para todo $r+1 \leq i \leq n$), logo $b_{r+1}, \ldots, b_n$ são algébricos sobre $\mathbf{k}[b_1, \ldots, b_r]$. Agora procedendo por indução sobre n, temos: Se $n = r$ não tem nada a fazer. Suponha então que $n > r$ e o resultado é verdadeiro para $n-1$ geradores. O gerador b_n é algébrico sobre $\mathbf{k}[b_1, \ldots, b_{n-1}]$ logo existe um polinômio $f \neq 0$ com coeficientes em $\mathbf{k}$ em n variáveis tal que $f(b_1, \ldots, b_{n-1}, b_n) = 0$. Seja F a parte homogênea de maior grau d de f, como $\mathbf{k}$ é infinito, segue do lema anterior que existem $\lambda_1, \ldots, \lambda_{n-1} \in \mathbf{k}$ tal que $F(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$. Sejam agora $b'_i = b_i - \lambda_i b_n$ para $i = 1, \ldots, n-1$. Defina $G(x_1, \ldots, x_{n-1}, x_n) = f(x_1 + \lambda_1 x_n, \ldots, x_{n-1} + \lambda_{n-1} x_n, x_n)$. Então G tem a forma

$G(x_1, \ldots, x_{n-1}, x_n) = F(\lambda_1, \ldots, \lambda_{n-1}, 1) x_n^d + p_1(x_1, \ldots, x_{n-1}) x_n^{d-1} + \cdots + p_d(x_1, \ldots, x_{n-1})$ para certos $p_1, \ldots, p_d \in \mathbf{k}[x_1, \ldots, x_{n-1}]$. Como $F(\lambda_1, \ldots, \lambda_{n-1}, 1) \neq 0$ então podemos supor G mônico pois podemos multiplicar por seu inverso. Logo $G(b'_1, \ldots, b'_{n-1}, b_n) = f(\underbrace{b'_1 + \lambda_1 b_n}_{b_1}, \ldots, \underbrace{b'_{n-1} + \lambda_{n-1} b_n}_{b_{n-1}}, b_n) = 0$ é uma equação para a dependência integral de b_n sobre $A' = \mathbf{k}[b'_1, \ldots, b'_{n-1}]$, logo b_n é integral sobre o anel $A' \subseteq A = \mathbf{k}[b_1, \ldots, b_n]$. Temos também que a $\mathbf{k}$-álgebra $A = A'[b_n]$ é gerada sobre A' pelo elemento b_n que é integral sobre A' e logo A e integral sobre A' (pela Proposição 162 Aula 20: "b_n é integral sobre $A' \Leftrightarrow A'[b_n] \supseteq A'$ é uma extensão finita"+ Corolário 164 Aula 20: "extensão finita implica integral").

Por outro lado, a hipótese indutiva fornece $a_1, \ldots, a_k \in A' \subseteq A$ algebricamente independentes sobre $\mathbf{k}$ tais que A' é integral sobre a $\mathbf{k}$-álgebra que eles geram $\mathbf{k}[a_1, \ldots, a_k]$. Assim cada extensão $\mathbf{k}[a_1, \ldots, a_k] \subseteq A' \subseteq A$ é integral e logo pela propriedade transitiva da Proposição 167 $\mathbf{k}[a_1, \ldots, a_k] \subseteq A$ é uma extensão integral. □

Ressaltamos que o Teorema de Normalização de Noether é verdadeiro para qualquer corpo $\mathbf{k}$ (não necessariamente infinito). Neste caso usamos o mesmo argumento exceto que definimos os $x'_i = x_i - x_n^{r_i}$ para inteiros r_i suficientemente grandes e adequadamente escolhidos.

Ainda, também é verdadeiro um resultado mais geral:

Teorema 189. *(***Teorema de Normalização de Noether***, versão II) Seja* $\mathbf{k}$ *um corpo e seja* $A \neq 0$ *uma* $\mathbf{k}$*-álgebra f.g. Então existem elementos* $a_1, \ldots, a_k \in A$ *que são algebricamente independentes sobre* $\mathbf{k}$ *e tal que* $\mathbf{k}[a_1, \ldots, a_k] \subseteq A$ *é uma extensão finita.*

Demonstração. **Exercício 2.** □

AULA 24: 12/11/2014

Aula 24

Lembramos a última aula: provamos o Teorema de Normalização de Noether e enunciamos uma versão mais geral:

Teorema. *(***Teorema de Normalização de Noether***, versão II) Seja* $\mathbf{k}$ *um corpo e seja* $A \neq 0$ *uma* $\mathbf{k}$*-álgebra f.g. Então existem elementos* $a_1, \ldots, a_k \in A$ *que são algebricamente independentes sobre* $\mathbf{k}$ *e tal que* $\mathbf{k}[a_1, \ldots, a_k] \subseteq A$ *é uma extensão finita.*

Na Seção 2.2: "Introdução à Geometria Algébrica" do Capítulo 2 provamos o **Teorema dos Zeros de Hilbert** ou **Nullstellensatz Hilberts** (Teorema 46) e na prova de tal teorema assumimos como verdadeiro um fato que dizemos provaríamos mais tarde. Tendo em vista o **Teorema de Normalização de Noether** (Teorema 188) estamos em condições de finalizar a prova do **Nullstellensatz** e provar o **"FATO"** o qual é chamado de "**Weak Nullstellensatz**":

Teorema 190. *(***Weak Nullstellensatz***)Seja* $\mathbf{k}$ *um corpo e* A *uma álgebra f.g. sobre* $\mathbf{k}$*. Se* A *é um corpo então* A *é uma extensão algébrica de* $\mathbf{k}$*. (mais ainda provaremos que* $\mathbf{k} \subseteq A$ *é uma extensão de corpos finita).*

Demonstração. Pelo Teorema de Normalização de Noether versão II (Teorema 189) existem elementos $a_1, \ldots, a_k \in A$ que são algebricamente independentes sobre $\mathbf{k}$ e tal que A é finita (e logo integral) sobre $\mathbf{k}[a_1, \ldots, a_k]$. Mas agora estamos na situação da Proposição 170 (Aula 20: "Sejam $A \subseteq B$ domínios de integridade, B integral sobre A. Então B é um corpo se, e somente se, A é um corpo."), logo $\mathbf{k}[a_1, \ldots, a_k]$ é um corpo. Segue do fato dos $a_1, \ldots, a_k \in A$ serem algebricamente independentes sobre $\mathbf{k}$ que $p(a_1, \ldots, a_k) \neq 0$ para qualquer polinômio não nulo $p \in \mathbf{k}[x_1, \ldots, x_k]$. Logo a aplicação $\alpha : \mathbf{k}[x_1, \ldots, x_k] \to \mathbf{k}[a_1, \ldots, a_k]$ dada por $p(x_1, \ldots, x_k) \mapsto p(a_1, \ldots, a_k)$ é claramente sobrejetora e $\mathrm{Ker}(\alpha) = 0$. Logo $\mathbf{k}[a_1, \ldots, a_k]$ é o anel dos polinômios em k indeterminadas.

Agora $\mathbf{k}[x_1, \ldots, x_k]$ é um corpo, logo todo $0 \neq f(x_1, \ldots, x_k) \in \mathbf{k}[x_1, \ldots, x_k]$ é uma unidade. Generalizando por indução em k o Exercício 12 da Lista 1, temos que f é uma unidade se, e somente se, o termo constante $b_0 \in \mathbf{k}$ é uma unidade e o resto dos coeficientes $b_i \in \mathbf{k}$ são nilpotentes, ou seja se, e somente se, $b_0 \neq 0$ e o resto dos coeficientes $b_i = 0$ (pois 0 é o único

elemento nilpotente de um corpo). Logo se $f(x_1, \ldots, x_k) \in \mathbf{k}[x_1, \ldots, x_k]$ então $f(x_1, \ldots, x_k) \in \mathbf{k}$, o que implica que $\mathbf{k}[x_1, \ldots, x_k] = \mathbf{k}$ e logo A é finito sobre o próprio $\mathbf{k}$ e por tanto $\mathbf{k} \subseteq A$ é uma extensão algébrica. □

7.1 EXERCÍCIOS

Ex. 79 — Mostre que:

1. Se I um ideal de A, então o quociente A/I é uma A-álgebra finita.
2. Se $f : A \to B$ e $g : B \to C$ são álgebras finitas, então $g \circ f : A \to C$ é finita.
3. Se $f : A \to B$ é uma álgebra finita e $g : A \to C$ é uma álgebra qualquer então a álgebra obtida por mudança de base $f \otimes \mathrm{id} : A \otimes_A C \simeq C \to B \otimes_A C$ dada por $c \mapsto 1 \otimes c$ é finita. Em particular, se $S \subseteq A$ é um conjunto multiplicativo, a localização $S^{-1}f : S^{-1}A \to S^{-1}B$ é uma álgebra finita.

Ex. 80 — Mostre que todo DFU é integralmente fechado.

Ex. 81 — Sejam $A \subseteq B \subseteq C$ anéis. Suponha que A é Noetheriano, que C é f.g. como A-álgebra e que C é f.g. como um B-módulo ou integral sobre B. Então B é f.g. como A-álgebra.

Ex. 82 — (**Teorema de Normalização de Noether**, versão II, corpo infinito) Seja $\mathbf{k}$ um corpo infinito e seja $A \neq 0$ uma $\mathbf{k}$-álgebra f.g. Prove que existem elementos $a_1, \ldots, a_k \in A$ que são algebricamente independentes sobre $\mathbf{k}$ e tal que $\mathbf{k}[a_1, \ldots, a_k] \subseteq A$ é uma extensão finita.

Ex. 83 — Sejam $B_1, B_2, \ldots, B_n$ A-álgebras integrais, mostre que $B_1 \times B_2 \times \cdots \times B_n$ é uma A-álgebra integral.

Ex. 84 — Sejam $B \supseteq A$ anéis tais que $B - A$ é um conjunto multiplicativo, então A é integralmente fechado em B.

Ex. 85 — Sejam $B \supseteq A$ uma extensão integral, $\mathfrak{m}$ um ideal maximal de B e $\mathfrak{n} = \mathfrak{m} \cap A$. Nesse caso $B_{\mathfrak{m}} \supseteq A_{\mathfrak{n}}$ é necessariamente integral?

Ex. 86 — Seja A um subanel de um domínio de integridade B e seja $\mathcal{C}(A, B)$ o fecho integral de A em B.

1. Sejam f e g polinômios mônicos em $B[x]$ tal que $f \cdot g \in \mathcal{C}(A, B)[x]$. Mostre que $f, g \in \mathcal{C}(A, B)[x]$.

2. Prove que $\mathcal{C}(A, B)[x]$ é o fecho integral de $A[x]$ em $B[x]$.

Ex. 87 — Seja $A = \mathbb{C}[x, y]/(y^2 - x^2(x + 1))$. Mostre que as localizações $A_{\mathfrak{m}}$ são integralmente fechadas para todos os ideais maximais $\mathfrak{m}$ de A com exceção de $\mathfrak{m} = (\overline{y}, \overline{x})$.

Ex. 88 — Mostre que $\mathbb{C}[x, y]/(y^2 - x^3 + x)$ é integralmente fechado.

Ex. 89 — Mostre que todas as cadeias maximais de primos de $\mathbf{k}[x_1, \ldots, x_n]$ tem o mesmo comprimento. Conclua que $\dim \mathbf{k}[x_1, \ldots, x_n] = n$.

8

TEORIA DA DIMENSÃO

Vamos lembrar a definição de dimensão de um anel dada no Capítulo 5.

Definimos uma **cadeia de ideais primos** de um anel A como sendo uma sequência estritamente crescente e finita $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n$ onde cada $\mathfrak{p}_i$ é um ideal primo de A. O **comprimento** da cadeia é n. Definimos a **dimensão** ou **dimensão de Krull** de um anel $A \neq 0$ como sendo o supremo dos comprimentos de todas as cadeias de ideais primos de A.

Se existem cadeias arbitrariamente longas de ideais primos de A, então dizemos que $\dim A = \infty$.

Assim, por exemplo um corpo tem dimensão 0, um DIP tem dimensão 1 e anéis Artinianos tem também dimensão 0. Segue do Exercício 11 da Lista 7 que $\dim \mathbf{k}[x_1, \ldots, x_n] = n$ e ainda que toda cadeia maximal de ideais primos de $\mathbf{k}[x_1, \ldots, x_n]$ tem comprimento n.

Definição 191. Seja $\mathfrak{p}$ um ideal primo de A, então a **altura** de $\mathfrak{p}$ é o comprimento da maior cadeia de ideais primos de A contidos em $\mathfrak{p}$: $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$, ou seja $\mathrm{ht}(\mathfrak{p}) = n$.

Segue diretamente da definição anterior que $\mathrm{ht}(\mathfrak{p}) = \dim A_{\mathfrak{p}}$ e que $\mathrm{ht}(\mathfrak{p}) = 0$ se, e somente se, $\mathfrak{p}$ é um ideal primo minimal de A.

Proposição 192. *Seja* $A = \mathbf{k}[x_1, \ldots, x_n]/\mathfrak{p}$ *onde* $\mathfrak{p}$ *é um ideal primo de* $\mathbf{k}[x_1, \ldots, x_n]$, *então* $\dim A = n - \mathrm{ht}(\mathfrak{p})$.

Demonstração. Como os ideais primos de A correspondem aos ideais primos de $B = \mathbf{k}[x_1, \ldots, x_n]$ que contém $\mathfrak{p}$ e $\dim B = n < \infty$ então $\dim A < \infty$, suponhamos que $\dim A = d$. Seja então $\overline{0} = \overline{\mathfrak{q}}_0 \subsetneq \overline{\mathfrak{q}}_1 \subsetneq \cdots \subsetneq \overline{\mathfrak{q}}_d$ (*) uma cadeia maximal de ideais primos de A, observamos que como $\mathfrak{p}$ é primo então A é um domínio e logo $\overline{0}$ é um ideal primo de A e ele pertence a toda cadeia maximal. Segue do TCI que os $\overline{\mathfrak{q}}_i$ correspondem a ideais primos $\mathfrak{q}_i$ de B que contém $\mathfrak{p}$: $\mathfrak{p} = \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_d$ e esse trecho de cadeia é maximal (se não fosse existiria $\mathfrak{p} \subsetneq \mathfrak{q}_i \subsetneq \mathfrak{q} \subsetneq \mathfrak{q}_{i+1}$ então $\overline{\mathfrak{q}}_i \subseteq \overline{\mathfrak{q}} \subseteq \overline{\mathfrak{q}}_{i+1}$ segue da maximalidade de (*) que ou $\overline{\mathfrak{q}}_i = \overline{\mathfrak{q}}$ ou $\overline{\mathfrak{q}}_{i+1} = \overline{\mathfrak{q}}$ mas então existiria um ideal primo de A que corresponde a dois ideais primos de B que contêm $\mathfrak{p}$, contradição). Seja $t = \mathrm{ht}(\mathfrak{p})$ (aqui de novo usamos que $\dim B < \infty$ para concluir que $\mathrm{ht}(\mathfrak{p}) < \infty$) logo existe uma cadeia maximal de ideais primos de B contidos em $\mathfrak{p}$ de comprimento t: $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_t = \mathfrak{p}$. Isto implica que existe uma cadeia maximal de ideais primos de B dada por: $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_t = \mathfrak{p} = \mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_d$, logo ela tem comprimento n (Ex 11 Lista 7) e, portanto, $n = t + d$ logo $d = n - t$, i.e., $\dim A = n - \mathrm{ht}(\mathfrak{p})$. □

O objetivo deste capítulo é provar o Teorema de Krull (veja Teorema 213) que afirma que a $\dim A$, para $(A, \mathfrak{m}, \mathbf{k})$ um anel Noetheriano local qualquer, é sempre finita e coincide com outras duas medidas: a cardinalidade mínima δ de um *sistema de parâmetros* $a_1, \ldots, a_\delta \in A$ (elementos tais que $\sqrt{(a_1, \ldots, a_\delta)} = \mathfrak{m}$) e o grau do *polinômio de Hilbert-Samuel* $h_A(n) = \ell_A(A/\mathfrak{m}^n)$ (para $n \gg 0$ natural). Para isso precisamos das seguintes definições e resultados:

8.1 ANÉIS GRADUADOS

Definição 193. Um **anel graduado** é um anel A junto com uma família $(A_n)_{n\geq 0}$ de subgrupos do grupo aditivo A, tal que $A = \bigoplus_{n=0}^{\infty} A_n$ e $A_m A_n \subseteq A_{m+n}$ para todo $m, n \geq 0$ (i.e., se $a \in A_m$ e $b \in A_n$ então $ab \in A_{m+n}$).

Segue da definição que A_0 é um subanel de A e cada A_n é um A_0-módulo.

Exemplo 194. $A = \mathbf{k}[x_1, \ldots, x_n]$ é um anel graduado $A = \bigoplus_{d=0}^{\infty} A_d$ onde cada A_d é o conjunto de todos os polinômios homogêneos de grau d, é um espaço vetorial sobre $\mathbf{k}$ (pois é A_0-módulo com $A_0 = \mathbf{k}$) e $\dim_{\mathbf{k}} A_d = \begin{pmatrix} n+d-1 \\ n-1 \end{pmatrix}$.

Exemplo 195. Dado um anel A não graduado e um ideal I de A, podemos formar um anel graduado $A^* = \bigoplus_{n=0}^{\infty} I^n$, com $I^0 = A$. Se A for Noetheriano então I é f.g. por $a_1, \ldots, a_s$, então $A^* = A[a_1, \ldots, a_s]$ é Noetheriano pelo Teorema da Base de Hilbert (Teorema 119).

Se A é um anel graduado, um **A-módulo graduado** é um A-módulo M junto com uma família $(M_n)_{n\geq 0}$ de subgrupos de M tais que $M = \bigoplus_{n=0}^{\infty} M_n$ e $A_m M_n \subseteq M_{m+n}$ para todo $m, n \geq 0$. Logo cada M_n é um A_0-módulo.

Dizemos que um elemento $m \in M$ é **homogêneo** se $m \in M_n$ para algum n, neste caso diremos que n é o **grau** de m.

Qualquer elemento $m \in M$ pode ser escrito de maneira única como uma soma $\sum_{n\geq 0} m_n$, onde $m_n \in M_n$ para todo $n \geq 0$ e todos excepto um número finito de m_n são 0. As componentes m_n não nulas são chamadas de **componentes homogêneas** de m.

Se M e N são A-módulos graduados um homomorfismo de A-módulos graduados é um homomorfismo de A-módulos $f : M \to N$ tal que $f(M_n) \subseteq N_n$ para todo $n \geq 0$.

Se A é um anel graduado definimos o ideal A_+ de A como sendo $A_+ = \bigoplus_{n>0} A_n$.

Proposição 196. *Seja A um anel graduado. Então A é Noetheriano se, e somente se, A_0 é Noetheriano e A é f.g. como uma A_0-álgebra.*

Demonstração. ($\Leftarrow$) Como A é uma A_0-álgebra f.g. e A_0 é Noetheriano segue de um Corolário do Teorema da Base de Hilbert (Corolário 121) que A é Noetheriano.

($\Rightarrow$) Como $A_0 = A/A_+$ com A Noetheriano e A_+ ideal de A, segue da Proposição 107 que A_0 é Noetheriano. Segue também que A_+ é f.g. como ideal de A por $a_1, \dots a_s \in A^+$os quais podem ser escolhidos como sendo elementos homogêneos de A (suponha que a_i não é homogêneo então a_i é soma de homogêneos, pegue as componentes homogêneas de a_i,que são finitas, como geradores), de graus $k_1, \dots, k_s > 0$. Seja A' o subanel de A gerado por $a_1, \dots, a_s$ sobre A_0, i.e. $A' = A_0[a_1, \dots, a_s]$. Mostraremos que $A_n \subseteq A'$ para todo $n \geq 0$, por indução em n. Para $n = 0$ então claramente $A_0 \subseteq A'$. Seja $n > 0$ e suponha que $A_k \subseteq A'$ para todo $k < n$. Seja $a \in A_n$, então a é homogêneo de grau n. Como $a \in A_+$ (pois $n > 0$), a é uma combinação linear dos a_i's: $a = \sum_{i=1}^{s} b_i a_i$, com $b_i \in A$. Agora $\text{grau}(a) = n = \text{grau}(b_i a_i)$, pois se os somandos não tivessem grau n então a não seria homogêneo. Logo, se $b_i a_i \neq 0$ como $a_i \in A_{k_i}$ e $b_i a_i \in A_n$ então necessariamente $b_i \in A_{n-k_i}$ (por convenção $A_m = 0$ se $m < 0$). Como cada $k_i > 0$ então $n - k_i < n$ e a hipótese indutiva mostra que $A_{n-k_i} \subseteq A'$, logo $b_i \in A'$, i.e., b_i é um polinômio nos a_j's com coeficientes em A_0. Logo o mesmo acontece com a o que implica $a \in A'$. Logo $A_n \subseteq A'$ (e isto acontece para todo $n \geq 0$) e portanto $A = A'$ e A é f.g. como A_0-álgebra. □

8.2 FUNÇÃO DE HILBERT

Definição 197. Seja C uma classe de A-módulos e seja $\lambda : C \to \mathbb{Z}$ uma função. Dizemos que a função λ é **aditiva** se, para cada sequência exata curta $0 \to M' \to M \to M'' \to 0$ na qual todos os termos pertencem a C temos $\lambda(M') - \lambda(M) + \lambda(M'') = 0$.

Segue da definição aplicada à sequência $0 \to 0 \to 0 \to 0 \to 0$ que $\lambda(0) = 0$ onde 0 é o A-módulo nulo.

Exemplo 198. Seja $\mathbf{k}$ um corpo e C a classe de todos os $\mathbf{k}$-espaços vetoriais V de dimensão finita. Então a função $\dim : C \to \mathbb{Z}$ dada por $V \mapsto \dim V$ é uma função aditiva, pois se $0 \to U \to V \to W \to 0$ é uma sequência exata pelo teorema de núcleo e da imagem segue que $\dim V = \dim U + \dim W$.

Exemplo 199. Seja C a classe de todos os A-módulos de comprimento finito. Então a função $\ell : C \to \mathbb{Z}$ dada por $M \mapsto \ell_A(M)$ é uma função aditiva como consequência da Proposição 114 (Aula 15: Seja $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ uma sequência exata de A-módulos. Então $\ell_A(M) < \infty$ se, e somente se, $\ell_A(M') < \infty$ e $\ell_A(M'') < \infty$. Neste caso $\ell_A(M) = \ell_A(M') + \ell_A(M'')$).

Proposição 200. *Seja* $0 \to M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} \dots \xrightarrow{f_n} M_n \to 0$ *uma sequência exata de* A*-módulos na qual todos os módulos* M_i *e os kernels de todos os homomorfismos pertencem a uma certa classe de* A*-módulos* C*. Então para qualquer função aditiva* λ *em* C *temos* $\sum_{i=0}^{n}(-1)^i\lambda(M_i) = 0$*.*

Demonstração. Como vimos na Aula 8, toda sequência exata pode ser dividida em sequências exatas curtas: se $N_i = \mathrm{Im}(f_i) = \mathrm{Ker}(f_{i+1})$ temos que $0 \to N_i \overset{\text{incl}}{\hookrightarrow} M_i \overset{f_{i+1}}{\twoheadrightarrow} N_{i+1} \to 0$ é exata para cada $0 \leq i \leq n$, onde $N_0 = N_{n+1} = 0$. Por hipótese, todos os M_i e os N_i pertencem a mesma classe de módulos C, então temos que $\lambda(M_i) = \lambda(N_i) + \lambda(N_{i+1})$, logo $\sum_{i=0}^{n}(-1)^i\lambda(M_i) = \sum_{i=0}^{n}(-1)^i\lambda(N_i) + \sum_{i=1}^{n+1}(-1)^{i-1}\lambda(N_i) = \lambda(N_0) + (-1)^n\lambda(N_{n+1}) = \lambda(0) + (-1)^n\lambda(0) = 0$. □

AULA 25: 14/11/2014

AULA 25

Lembramos a última aula, provamos:

Proposição 1: Seja A um anel graduado. Então A é Noetheriano se, e somente se, A_0 é Noetheriano e A é f.g. como uma A_0-álgebra.

Proposição 2: Seja $0 \to M_0 \xrightarrow{f_1} M_1 \xrightarrow{f_2} \dots \xrightarrow{f_n} M_n \to 0$ uma sequência exata de A-módulos na qual todos os módulos M_i e os kernels de todos os homomorfismos pertencem a uma certa classe de A-módulos C. Então para qualquer função aditiva λ em C temos $\sum_{i=0}^{n}(-1)^i\lambda(M_i) = 0$.

Seja $A = \bigoplus_{n=0}^{\infty} A_n$ um anel graduado Noetheriano. Segue da prova da Proposição 196 (Prop 1) que A_0 é um anel Noetheriano e A uma A_0-álgebra f.g. pelos elementos $a_1, \dots, a_s \in A$ os quais podem ser escolhidos como sendo homogêneos e de graus $k_1, \dots, k_s > 0$.

Seja M um A-módulo graduado f.g., então cada que M_n (a componente homogênea de M de grau n) é f.g. como um A_0-módulo. De fato, M é gerado sobre A por um número finito de elementos que podem ser escolhidos homogêneos $m_1, \dots, m_k$ com $r_j = \mathrm{grau}(m_j)$, $M = Am_1 + \dots + Am_k$. Agora, todo elemento y de M_n é da forma $y = \sum_{j=1}^{k} c_j m_j$ onde $c_j \in A$, então definindo b_j como o termo homogêneo de grau $n - r_j$ de c_j (com $b_j = 0$ se $n - r_j < 0$), temos $y = \sum_j b_j m_j$. Agora como os $b_j \in A = A_0[a_1, \dots, a_s]$ então $b_j = f^j(a_1, \dots, a_s)$ é um polinômio nos a_i's com coeficientes em A_0, logo y é uma combinação A_0-linear dos elementos $g^j(a_1, \dots, a_s)m_j$ onde $g^j(a_1, \dots, a_s)$ é um monômio nos a_i's de grau total $n - r_j$. Logo M_n é um A_0-módulo f.g.

Definição 201. Seja A um anel graduado Noetheriano, M um A-módulo graduado f.g. e seja λ uma função aditiva na classe de todos os A_0-módulos f.g. A **série de Poincaré** de M com respeito a λ é a série de potências $P(M, t) = \sum_{n=0}^{\infty} \lambda(M_n)t^n \in \mathbb{Z}[[t]]$.

Exemplo 202. Seja $A = \mathbf{k}[x_1, \ldots, x_n]$, segue do Exemplo 194 que $A = \bigoplus_{d=0}^{\infty} A_d$ é um anel graduado e Noetheriano onde cada termo A_d é o conjunto de todos os polinômios homogêneos de grau d e é um $A_0 = \mathbf{k}$-módulo, i.e., um espaço vetorial sobre $\mathbf{k}$ e $\dim_{\mathbf{k}} A_d = \begin{pmatrix} n+d-1 \\ n-1 \end{pmatrix} < \infty$, logo os A_d são A_0-módulos f.g. Considere $M = A$, claramente M é f.g sobre A (com gerador 1). Seja então $\lambda(A_d) = \dim_{\mathbf{k}} A_d$ temos $P(A,t) = \sum_{i=0}^{\infty} \begin{pmatrix} n+i-1 \\ n-1 \end{pmatrix} t^i = \frac{1}{(1-t)^n}$.

Teorema 203. *Sob as hipóteses anteriores, $P(M,t)$ é uma função racional em t da forma $P(M,t) = \frac{f(t)}{\prod_{i=1}^{s}(1-t^{k_i})}$ onde $f(t) \in \mathbb{Z}[t]$ e $k_i = \text{grau}(a_i)$ onde a_i são os geradores de A como A_0=álgebra, para $i = 1, \ldots, s$.*

Demonstração. Procederemos por indução em s, o número de geradores de A sobre A_0. Caso $s = 0$, isto significa que $A = A_0$, logo $A_n = 0$ para todo $n > 0$. Agora M é um A_0-módulo f.g., ou seja tem um número finito de geradores homogêneos sobre A_0, $M = A_0 m_1 + \cdots + A_0 m_k$, o que implica que $M_n = 0$ para todo $n > N$ onde $N = \max\{r_1, \ldots, r_k\}$. Logo $\lambda(M_n) = 0$ para todo $n > N$, desta forma $P(M,t) = \sum_{n=0}^{\infty} \lambda(M_n) t^n = \sum_{n=0}^{N} \lambda(M_n) t^n$ é um polinômio de grau N.

Suponha $s > 0$ e que o teorema vale para $s-1$. Considere o homomorfismo de A-módulos $\varphi_n : M_n \to M_{n+k_s}$ dado por $m \mapsto a_s m$ (φ_n é a multiplicação pelo gerador a_s de A) então temos a seguinte sequência exata $0 \to K_n = \ker \varphi_n \overset{\text{incl}}{\hookrightarrow} M_n \xrightarrow{\varphi_n} M_{n+k_s} \overset{\pi}{\twoheadrightarrow} L_{n+k_s} = \text{Coker}(\varphi_n) = \frac{M_{n+k_s}}{\varphi_n(M_n)} \to 0$.

Sejam $K = \bigoplus_{n=0}^{\infty} K_n$ e $L = \bigoplus_{n=0}^{\infty} L_n$, ambos são A-módulos f.g. pois K é um submódulo de M e $L = \bigoplus_{n=0}^{\infty} \frac{M_n}{\varphi_{n-k_s}(M_{n-k_s})} = \bigoplus_{n=0}^{\infty} \frac{M_n}{a_s M_{n-k_s}} = \bigoplus_{n=0}^{\infty} \frac{M_n}{(M_n \cap a_s M)} = \bigoplus_{n=0}^{\infty} \frac{M_n + a_s M}{a_s M} = \frac{M}{a_s M}$ é um módulo quociente de M.

Aplicando λ à sequência exata temos $\lambda(K_n) - \lambda(M_n) + \lambda(M_{n+k_s}) - \lambda(L_{n+k_s}) = 0$ (pela Proposição 200) e multiplicando por t^{n+k_s} temos: $\lambda(K_n)t^{n+k_s} - \lambda(M_n)t^{n+k_s} + \lambda(M_{n+k_s})t^{n+k_s} - \lambda(L_{n+k_s})t^{n+k_s} = 0$ para todo $n \geq 0$. Logo, somando sobre n:

$$\sum_{n=0}^{\infty} \lambda(K_n)t^{n+k_s} - \sum_{n=0}^{\infty} \lambda(M_n)t^{n+k_s} + \sum_{n=0}^{\infty} \lambda(M_{n+k_s})t^{n+k_s} - \sum_{n=0}^{\infty} \lambda(L_{n+k_s})t^{n+k_s} = 0,$$

isto é $P(K,t)t^{k_s} - P(M,t)t^{k_s} + \sum_{n=k_s}^{\infty} \lambda(M_n)t^n - \sum_{n=k_s}^{\infty} \lambda(L_n)t^n = 0$, ou seja $P(K,t)t^{k_s} - P(M,t)t^{k_s} + P(M,t) - \sum_{n=0}^{k_s} \lambda(M_n)t^n - P(L,t) = 0$, pois $L = \bigoplus_{n=0}^{\infty} \text{Coker}(\varphi_{n-k_s}) = \bigoplus_{n=k_s}^{\infty} \text{Coker}(\varphi_{n-k_s})$. Logo $P(M,t)(1-t^{k_s}) = P(L,t) + \sum_{n=0}^{k_s} \lambda(M_n)t^n - P(K,t)t^{k_s}$.

Para poder aplicar a hipótese indutiva temos que mostrar que K e L são $A_0[a_1, \ldots, a_{s-1}]$-módulos f.g. É suficiente mostrar que ambos módulos são

aniquilados por a_s pois como eles são A-módulos f.g. cada elemento se escreve como uma soma finita $\sum_{i\in I} a_0^i a_1^{\alpha_1^i}\cdots a_s^{\alpha_s^i}x_i$ onde $a_0^i \in A_0$ e $x_i \in K$ (resp. $x_i \in L$), mas $a_s x_i = 0$ logo o elemento se escreve na verdade como uma soma finita $\sum_{j\in J} a_0^j a_1^{\alpha_1^j}\cdots a_{s-1}^{\alpha_{s-1}^j}x_j$. Logo ambos módulos devem ser $A_0[a_1,\ldots,a_{s-1}]$-módulos f.g. Vejamos que, de fato $a_sK = a_sL = 0$: seja $x \in K$ então $x = \sum x_n$ com $x_n \in \ker\varphi_n$, logo $\varphi_n(x_n) = a_s x_n = 0$ portanto $a_s x = \sum a_s x_n = 0$. Seja $x \in L$, então $x = \sum \overline{x}_n$ com $\overline{x}_n \in L_n = \frac{M_n}{\varphi_{n-k_s}(M_{n-k_s})}$ tal que $\overline{x}_n = x_n + \varphi_{n-k_s}(M_{n-k_s})$ com $x_n \in M_n$. Agora $a_s x_n + a_s\underbrace{\varphi_{n-k_s}(M_{n-k_s})}_{\subseteq M_n} \in \frac{M_{n+k_s}}{\varphi_n(M_n)} = L_{n+k_s}$ pois $a_s M_n = \varphi_n(M_n)$, logo $a_s\overline{x}_n \in L_{n+k_s}$. Mas $a_s x_n = \varphi_n(x_n) \in \varphi_n(M_n)$, logo $a_s\overline{x}_n = \overline{0} \in L_{n+k_s}$, para todo $n \geq 0$. Logo $a_s x = 0$, como queríamos provar.

Aplicando então a hipótese de indução temos $P(M,t)(1-t^{k_s}) = \frac{f(t)}{\prod_{i=1}^{s-1}(1-t^{k_i})} + \underbrace{\sum_{n=0}^{k_s}\lambda(M_n)t^n}_{=h(t)} - \frac{\overbrace{g(t)t^{k_s}}^{g'(t)}}{\prod_{i=1}^{s-1}(1-t^{k_i})}$. Mas isto é $P(M,t)[1-t^{k_s}] = \frac{f(t)-g'(t)+h(t)(\prod_{i=1}^{s-1}(1-t^{k_i}))}{\prod_{i=1}^{s-1}(1-t^{k_i})} = \frac{F(t)}{\prod_{i=1}^{s-1}(1-t^{k_i})}$, logo $P(M,t) = \frac{F(t)}{\prod_{i=1}^{s}(1-t^{k_i})}$. □

Definição 204. A ordem do polo de $P(M,t)$ em $t = 1$ será denotada por $d = d(M)$.

Lembrando que uma função racional $R(t)$ tem um **polo** de ordem n em $t = a$ se podemos escrever $R(t) = \frac{1}{(t-a)^n}T(t)$ (para $t \neq a$), onde $T(t) = \frac{f(t)}{g(t)}$ é uma função racional tal que $f(a)$ é um valor finito não nulo e $t - a \nmid g(t)$.

Exemplo 205. Nas hipóteses do último exemplo, $M = A = \mathbf{k}[x_1,\ldots,x_n]$ e $\lambda(A_d) = \dim_{\mathbf{k}} A_d$ temos $P(A,t) = \frac{1}{(1-t)^n}$. Logo $d(A) = n$.

O caso em que todos os $k_i = 1$ é especialmente simples:

Corolário 206. *Se cada $k_i = 1$, então para todo n suficientemente grande, $\lambda(M_n)$ é um polinômio em n (com coeficientes racionais) de grau[1] $d-1$.*

Demonstração. Segue do teorema anterior que $P(M,t) = \frac{f(t)}{\prod_{i=1}^{s}(1-t^{k_i})} \overset{k_i=1}{=} \frac{f(t)}{\prod_{i=1}^{s}(1-t)} = \frac{f(t)}{(1-t)^s}$. Cancelando potências de $(1-t)$ assumimos que $s = d = d(M)$ e $f(1) \neq 0$. Agora $\frac{1}{(1-t)^d} = \sum_{k=0}^{\infty}\binom{d+k-1}{d-1}t^k$ e suponha que

1 aqui adotamos a convenção que o grau do polinômio nulo é -1 e também que o coeficiente binomial $\binom{n}{-1} = 0$ para todo $n \geq 0$ e $\binom{-1}{-1} = 1$.

$f(t) = \sum_{k=0}^{N} b_k t^k$ com $b_k \in \mathbb{Z}$, logo temos que $P(M,t) = (\sum_{j=0}^{N} b_j t^j)(\sum_{k=0}^{\infty} \binom{d+k-1}{d-1} t^k) = \sum_{k=0}^{\infty}(\sum_{j=0}^{N} b_j \binom{d+k-1}{d-1}) t^j t^k$. Pela definição de série de Poincaré $\lambda(M_n)$ é o coeficiente de t^n em $P(M,t)$, logo (para $k = n-j$) temos que $\lambda(M_n) = \sum_{j=0}^{N} b_j \binom{d+n-j-1}{d-1}$ para todo $n \geq N$ e a soma do lado direito é um polinômio φ em n com coeficientes racionais tal que $\varphi(x) = \frac{f(1)}{(d-1)!}x^{d-1} +$ (termos de menor grau). □

Observação 207. Para um polinômio $f(x)$ tal que $f(n)$ é um inteiro para todo inteiro n, não é necessário que todos os coeficientes de f sejam inteiros, por exemplo: $\frac{1}{2}x(x+1)$.

O polinômio do Corolário 206 é chamado de **função** ou **polinômio de Hilbert** do módulo graduado M em relação a λ.

Proposição 208. *Seja $x \in A$ um elemento homogêneo de grau positivo. Se x não é um divisor de zero de M (i.e., se $xm = 0$ então $m = 0$) então $d(M/xM) = d(M) - 1$.*

Demonstração. Considere o homomorfismo de A-módulos $\varphi_n : M_n \to M_{n+k}$ (onde $k = \text{grau}(x)$) dado por $m \mapsto xm$ então temos a seguinte sequência exata $0 \to K_n = \ker \varphi_n \overset{\text{incl}}{\hookrightarrow} M_n \xrightarrow{\varphi_n} M_{n+k} \overset{\pi}{\twoheadrightarrow} L_{n+k} = \frac{M_{n+k}}{\varphi_n(M_n)} \to 0$. Seguindo a prova do Teorema 203 temos $P(M,t)(1-t^k) = P(L,t) - P(K,t)t^k + g(t)$, mas como x não é divisor de zero $K_n = \ker \varphi_n = 0$ para todo n, logo $\lambda(K_n) = 0$ para todo n o que implica $P(K,t) = 0$. Por outro lado $1 - t^k = (1-t)(1+t+t^2+\cdots+t^{k-1}) = (1-t)f(t)$ onde $f(1) = k \neq 0$, assim $P(M,t)f(t)(1-t) - g(t) = P(L,t)$. Por tanto $d(L) = d(M) - 1$ (resultado de funções complexas), mas $L = \frac{M}{xM}$ (segue da prova do Teorema 203) logo $d(\frac{M}{xM}) = d(M) - 1$. □

AULA 26: 19/11/2014

AULA 26

Definição 209. Seja $(A, \mathfrak{m}, \mathbf{k})$ um anel local Noetheriano. Então definimos a **função de Hilbert-Samuel** como sendo $h_A(n) = \ell_A(A/\mathfrak{m}^n)$, para $n \in \mathbb{N}$.

Observe $\ell_A(A/\mathfrak{m}^n) < \infty$ para todo $n \geq 0$, pois como A é Noetheriano então $A/\mathfrak{m}^n$ é Noetheriano e pelo Exercício 4 da Lista 6 também é Artiniano, o resultado segue da Proposição 111.

Seja A um anel e I um ideal de A. Definimos o **anel graduado associado** a A como sendo $G(A) = \bigoplus_{n=0}^{\infty} G_n(A)$, onde $G_n(A) = I^n/I^{n+1}$ com $I^0 = A$. Este é um anel graduado no qual a multiplicação é dada por: para cada

$x_n \in I^n$, seja $\overline{x}_n$ a imagem de x_n em $\frac{I^n}{I^{n+1}}$, defina $\overline{x}_m\overline{x}_n = \overline{x_m x_n}$, i.e., a imagem de $x_m x_n$ em $\frac{I^{n+m}}{I^{n+m+1}}$ (verifique que o produto está bem definido, ou seja não depende da escolha dos representantes das classes).

Segue da Proposição 196 que se A é noetheriano, então $G(A)$ é Noetheriano pois $G_0(A) = A/I$ é Noetheriano por ser quociente de um anel Noetheriano por um ideal (Proposição 107). Por outro lado, um elemento de $G_n(A) = I^n/I^{n+1}$ pode ser escrito como uma combinação linear de produtos de n elementos de $G_1(A) = I/I^2$, logo $G(A)$ é gerado sobre $G_0(A)$ por elementos de $G_1(A)$. Como A é Noetheriano I é f.g. por $a_1, \ldots, a_s$ então se $\overline{a}_1, \ldots, \overline{a}_s$ são as imagens de a_i em $\frac{I}{I^2} = G_1(A)$ então $G(A)$ é gerado como uma $G_0(A)$-álgebra por $\overline{a}_1, \ldots, \overline{a}_s$ e cada $\overline{a}_i$ tem grau 1. Logo $G(A) = (A/I)[\overline{a}_1, \ldots, \overline{a}_s]$ é Noetheriano pelo Corolário 121 do Teorema da Base de Hilbert. Segue desta última observação que podemos considerar $G(A)$ como uma $G_0(A)$-álgebra f.g. por elementos que podem ser escolhidos como sendo homogêneos e de grau 1.

Agora se $(A, \mathfrak{m}, \mathbf{k})$ é um anel Noetheriano local então, fazendo $I = \mathfrak{m}$ no anel graduado associado a A temos que cada $G_n(A) = \frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}}$ é um $\mathbf{k}$-espaço vetorial de dimensão finita (como A Noetheriano então $\mathfrak{m}^n$ é f.g. como A-módulo (ideal) então $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ também é f.g. como A-módulo e como $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ é aniquilado por $\mathfrak{m}$, tem estrutura de $\mathbf{k}$-espaço vetorial e como tal tem dimensão finita), logo $\dim_{\mathbf{k}} G_n(A) < \infty$.

Proposição 210. *Seja $(A, \mathfrak{m}, \mathbf{k})$ um anel local Noetheriano.*

a. Para todo $n \geq 0$, temos $h_A(n+1) - h_A(n) = \dim_{\mathbf{k}}(\mathfrak{m}^n/\mathfrak{m}^{n+1})$.

*b. Existe um polinômio $p(x) \in \mathbb{Q}[x]$ de grau $d(G(A))$, tal que $h_A(n) = p(n)$ para $n \gg 0$. Este polinômio é chamado de **polinômio de Hilbert-Samuel**.*

Demonstração. a. Segue da sequência exata $0 \to \frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}} \overset{inc}{\hookrightarrow} \frac{A}{\mathfrak{m}^{n+1}} \to \frac{A}{\mathfrak{m}^n} \to 0$ que $\ell_A(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \ell_A(A/\mathfrak{m}^{n+1}) - \ell_A(A/\mathfrak{m}^n) = h_A(n+1) - h_A(n)$. Agora observe que $\ell_A(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \dim_{\mathbf{k}}(\mathfrak{m}^n/\mathfrak{m}^{n+1})$ já que $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ é aniquilado por $\mathfrak{m}$, e pode ser visto como um módulo sobre $\mathbf{k} = A/\mathfrak{m}$, logo toda série de composição de $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ como A-módulo é uma série de composição de $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ como $\mathbf{k}$-módulo, pois todos os A-submódulos também são aniquilados por $\mathfrak{m}$ e logo são $\mathbf{k}$-submódulos.

b. Pelo item anterior, $h_A(n+1) - h_A(n)$ é $\lambda(G_n(A))$ em relação a $\lambda = \dim_{\mathbf{k}}$. Dado que $G(A)$ é uma $\mathbf{k}$-álgebra f.g. por elementos que podem ser escolhidos como sendo homogêneos e de grau 1, segue do Corolário 206 que existe um polinômio $q(x) \in \mathbb{Q}[x]$ de grau $d(G(A)) - 1$, tal que para n suficientemente grande $q(n) = h_A(n+1) - h_A(n)$. Isto implica que existe um polinômio $p(x) \in \mathbb{Q}[x]$ de grau $d(G(A))$ tal que $h_A(n) = p(n)$ para todo inteiro $n \gg 0$ (veja Apêndice A).

□

Segue da proposição anterior que podemos escrever a função de Hilbert-Samuel como $h_A(n) = \sum_{i=0}^{n-1}[h_A(i+1) - h_A(i)] + h_A(0) = \sum_{i=0}^{n-1} \dim_{\mathbf{k}}(\mathfrak{m}^i/\mathfrak{m}^{i+1})$, já que $h_A(0) = \ell_A(A/\mathfrak{m}^0) = \ell_A(A/A) = \ell_A(0) = 0$.

Definição 211. Seja $(A, \mathfrak{m}, \mathbf{k})$ um anel local Noetheriano. Dizemos que $a_1, a_2, \ldots, a_n \in A$ é um **sistema de parâmetros** se $\sqrt{(a_1, \ldots, a_n)} = \mathfrak{m}$. Denotaremos por δ_A o tamanho mínimo de um sistema de parâmetros de A.

Note que qualquer conjunto de geradores de $\mathfrak{m}$ é um sistema de parâmetros de A. Assim segue da Proposição 62 (Sejam m_i $(1 \leq i \leq k)$ os elementos de M cujas imagens em $M/\mathfrak{m}M$ formam uma base deste espaço vetorial. Então m_i geram M), com $M = \mathfrak{m}^n$ que $\delta_A \leq \dim_{\mathbf{k}}(\frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}})$.

8.3 TEOREMA DE DIMENSÃO DE KRULL

Lema 212. (Lema principal) *Sejam $(A, \mathfrak{m}, \mathbf{k})$ um anel local Noetheriano, $a \in \mathfrak{m}$ e $B = A/aA$. Então:*

a. $d(G(B)) \geq d(G(A)) - 1$.

b. Se $a \in A$ não é divisor de zero, então $d(G(B)) = d(G(A)) - 1$.

Demonstração. Denote por $\overline{\mathfrak{m}}$ a imagem de $\mathfrak{m}$ em B. O anel B é um anel local (TCI leva maximal em maximal) Noetheriano com ideal maximal $\overline{\mathfrak{m}}$ e corpo de resíduos $B/\overline{\mathfrak{m}} = \frac{A/aA}{\mathfrak{m}/aA} = A/\mathfrak{m} = \mathbf{k}$. Temos os isomorfismos $\frac{B}{\overline{\mathfrak{m}}^n} = \frac{A/aA}{\mathfrak{m}^n + aA/aA} = \frac{A}{aA+\mathfrak{m}^n}$(**) e $\frac{aA+\mathfrak{m}^n}{\mathfrak{m}^n} = \frac{aA}{aA \cap \mathfrak{m}^n}$ e portanto uma sequência exata $0 \to \frac{aA}{aA\cap\mathfrak{m}^n} \to \frac{A}{\mathfrak{m}^n} \to \frac{B}{\overline{\mathfrak{m}}^n} \to 0$ (onde a primeira aplicação é a inclusão de $\frac{aA+\mathfrak{m}^n}{\mathfrak{m}^n} \subseteq \frac{A}{\mathfrak{m}^n}$ e a segunda é dada por $x + \mathfrak{m}^n \mapsto x + (aA + \mathfrak{m}^n)$) de modo que $\ell_A(A/\mathfrak{m}^n) = \ell_A(B/\overline{\mathfrak{m}}^n) + \ell_A(\frac{aA}{aA\cap\mathfrak{m}^n})$ i.e. $h_A(n) = h_B(n) + \ell_A(\frac{aA}{aA\cap\mathfrak{m}^n})$ (note que $\ell_A(B/\overline{\mathfrak{m}}^n) = \ell_B(B/\overline{\mathfrak{m}}^n)$ pois $\frac{B}{\overline{\mathfrak{m}}^n} = \frac{A}{aA+\mathfrak{m}^n}$ é um A-módulo que é aniquilado por a logo é um A/aA-módulo, i.e., um B-módulo e logo os comprimentos coincidem). Seja agora φ o seguinte mapa sobrejetor, induzido pela multiplicação por $a \in \mathfrak{m}$: $\varphi : \frac{A}{\mathfrak{m}^{n-1}} \to \frac{aA}{aA\cap\mathfrak{m}^n}$ dado por $x + \mathfrak{m}^{n-1} \mapsto ax + (aA \cap \mathfrak{m}^n)$. Completando a uma sequência exata temos: $0 \to \ker\varphi \overset{inc}{\hookrightarrow} \frac{A}{\mathfrak{m}^{n-1}} \overset{\varphi}{\twoheadrightarrow} \frac{aA}{aA\cap\mathfrak{m}^n} \to 0$ então para todo $n \geq 1$, temos $\ell_A(\frac{aA}{aA\cap\mathfrak{m}^n}) \leq \ell_A(\frac{A}{\mathfrak{m}^{n-1}}) = h_A(n-1)$. Assim obtemos $h_B(n) \geq h_A(n) - h_A(n-1)$ segue da prova da Proposição 210 que, para $n \gg 0$, $p_B(n) \geq q_A(n)$ onde $p_B(x)$ é o polinômio de Hilbert-Samuel de B e $q_A(x)$ é o polinômio de Hilbert do módulo graduado $G(A)$ em relação a $\lambda = \dim_{\mathbf{k}}$. Logo $\operatorname{grau}(p_B(x)) \geq \operatorname{grau} q_A(x)$, ou seja $d(G(B)) \geq d(G(A)) - 1$. A igualdade é um caso particular da Proposição 208. □

Teorema 213. (Teorema de Krull) *Seja $(A, \mathfrak{m}, \mathbf{k})$ um anel local Noetheriano. Então* $\dim A < \infty$ *e, além disso,* $\dim A = \delta_A = d(G(A))$.

Demonstração. Vamos mostrar uma sequência de desigualdades $\dim A \leq d(G(A)) \leq \delta_A \leq \dim A$. Observe que a primeira desigualdade mostra que $\dim A$ é finita.

a. Queremos provar que $\dim A \leq d(G(A))$, faremos isto por indução em $d(G(A))$. Se $d(G(A)) = 0$, então $h_A(n) = \ell_A(A/\mathfrak{m}^n)$ é constante para $n \gg 0$, i.e., $\dim_{\mathbf{k}} \frac{\mathfrak{m}^n}{\mathfrak{m}^{n+1}} = h_A(n+1) - h_A(n) = 0$ para $n \gg 0$ (Proposição 210). Logo $\mathfrak{m}^n = \mathfrak{m}^{n+1}$, segue da Proposição 155 ("Seja A um anel Noetheriano local e $\mathfrak{m}$ seu ideal maximal. Então exatamente uma das seguintes condições é verdadeira: (i) $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}$ para todo n; ou (ii) $\mathfrak{m}^n = 0$ para algum n, neste caso A é um anel Artiniano local") que $\mathfrak{m}^n = 0$ para $n \gg 0$ e A é Artiniano logo $\dim A = 0 = d(G(A))$. Suponha agora que $d(G(A)) > 0$, e seja $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ uma cadeia de ideais primos de A de comprimento r (todos os $\mathfrak{p}_i \subseteq \mathfrak{m}$, pois são ideais próprios e logo estão contidos em um maximal). Seja $A' = A/\mathfrak{p}_0$ então A' é um domínio Noetheriano local (com maximal $\overline{\mathfrak{m}} = \frac{\mathfrak{m}}{\mathfrak{p}_0}$) que contém uma cadeia de ideais primos de comprimento r: $\overline{0} \subsetneq \overline{\mathfrak{p}}_1 \subsetneq \cdots \subsetneq \overline{\mathfrak{p}}_r$ e ainda $h_{A'}(n) \leq h_A(n)$ para todo n, pois: $h_{A'}(n) = \ell_{A'}(\frac{A'}{\overline{\mathfrak{m}}^n}) \overset{(**)}{=} \ell_{A'}(\frac{A}{\mathfrak{p}_0+\mathfrak{m}^n}) = \ell_A(\frac{A}{\mathfrak{p}_0+\mathfrak{m}^n})$ (pois $\frac{A}{\mathfrak{p}_0+\mathfrak{m}^n}$ é um A-módulo que é aniquilado por $\mathfrak{p}_0$ logo é um A'-módulo), agora $\mathfrak{m}^n \subseteq \mathfrak{p}_0 + \mathfrak{m}^n$ logo se $\overline{I}$ é um ideal de $\frac{A}{\mathfrak{p}_0+\mathfrak{m}^n}$ então corresponde a um ideal de A que contém $\mathfrak{p}_0 + \mathfrak{m}^n$ e logo contém $\mathfrak{m}^n$ e logo corresponde a um ideal de $\frac{A}{\mathfrak{m}^n}$, assim $h_{A'}(n) = \ell_A(\frac{A}{\mathfrak{p}_0+\mathfrak{m}^n}) \leq \ell_A(\frac{A}{\mathfrak{m}^n}) = h_A(n)$. Logo $d(G(A')) \leq d(G(A))$. Seja $0 \neq a \in \overline{\mathfrak{p}}_1 \subseteq \overline{\mathfrak{m}}$ ($\overline{\mathfrak{p}}_1 \neq 0$ pois se não $\mathfrak{p}_1 = \mathfrak{p}_0$) e $B = A'/aA'$, como A' é um domínio a não é divisor de zero e logo, segue do Lema Principal (Lema 212) que $d(G(B)) = d(G(A')) - 1 \leq d(G(A)) - 1 < d(G(A))$. Aplicando a hipótese de indução temos que $\dim B \leq d(G(B))$. Por outro lado, as imagens de $\overline{\mathfrak{p}}_1, \ldots, \overline{\mathfrak{p}}_r$ em B formam uma cadeia de tamanho $r-1$, assim $r - 1 \leq \dim B \leq d(G(A)) - 1$ logo $r \leq d(G(A))$, em particular $\dim A \leq d(G(A))$.

b. Queremos provar que $d(G(A)) \leq \delta_A$, faremos isto por indução em δ_A. Se $\delta_A = 0$, então o sistema de parâmetros é vazio, então $\mathfrak{m} = \sqrt{(\emptyset)} = \sqrt{0} = \mathfrak{N}_A$, como A é Noetheriano, segue do Exercício 2 Lista 6 que o nilradical é nilpotente, logo existe $r \in \mathbb{N}$ tal que $\mathfrak{m}^r = 0$. Logo $h_A(n) = \ell_A(A/\mathfrak{m}^n) = \ell_A(A)$ é constante para $n \geq r$ e assim $d(G(A)) = 0$. Seja agora $\delta_A > 0$. Tome $a \in A$ pertencente a um sistema de parâmetros de cardinalidade δ_A (logo $a \in \mathfrak{m} = \sqrt{(a, a_2, \ldots, a_{\delta_A})}$) e seja $B = A/aA$. Então $\delta_B \leq \delta_A - 1$ e pela hipótese de indução $d(G(B)) \leq \delta_B$. Assim, pelo Lema Principal (Lema 212), $d(G(A)) - 1 \leq d(G(B)) \leq \delta_B \leq \delta_A - 1$, logo $d(G(A)) \leq \delta_A$.

c. Queremos provar que $\delta_A \leq \dim A$, faremos isto por indução em $\dim A$ (que já sabemos que é finita). Se $\dim A = 0$, então $\mathrm{Spec}(A) = \{\mathfrak{m}\}$ (A local e todo primo $\mathfrak{p}$ está contido em $\mathfrak{m}$), logo $\mathfrak{N} = \sqrt{0} = \mathfrak{m}$, existe um sistema de parâmetros vazio pois $0 = (\emptyset)$ e portanto $\delta_A = 0$. Agora suponha que $\dim A > 0$. Como A é Noetheriano, A possui apenas um número finito de ideais primos minimais $\mathfrak{p}_0, \ldots, \mathfrak{p}_k$ (Exercício 9.2 Lista 5). Logo como $\mathfrak{p} \subseteq \mathfrak{m}$ para todo $\mathfrak{p}$ primo então $\cup_{i=0}^{k} \mathfrak{p}_i \subseteq \mathfrak{m}$, suponha que $\cup_{i=0}^{k} \mathfrak{p}_i = \mathfrak{m}$, segue da Proposição 29 que $\mathfrak{m} \subseteq \mathfrak{p}_i$ para algum $0 \leq i \leq k$, logo $\mathfrak{m} = \mathfrak{p}_i$ é um primo minimal. Ou seja $\mathfrak{m}$ contém todos os primos e é minimal, logo $\mathfrak{m} = \mathfrak{p}$ para todo $\mathfrak{p}$ primo. Logo A tem um único primo o que implica $\dim A = 0$, contradição. Logo $\cup_{i=0}^{k} \mathfrak{p}_i \subsetneq \mathfrak{m}$, assim podemos escolher $a \in \mathfrak{m}$ que não pertence a nenhum primo minimal. Logo se $B = A/aA$, temos $\dim B \leq \dim A - 1$ (pois dada uma cadeia maximal de primos de A: $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1' \subsetneq \cdots \subsetneq \mathfrak{p}_r' = \mathfrak{m}$ ela começa em um primo minimal e acaba em $\mathfrak{m}$ e alem disso $a \in \mathfrak{m}$ e $a \notin \mathfrak{p}_0$ logo $aA \subsetneq \mathfrak{p}_0$ e portanto $\mathfrak{p}_0$ não corresponde a um primo de B, assim $\dim B \leq \dim A - 1$). Aplicando a hipótese de indução $\delta_B \leq \dim B$. Note ainda que se $a_1, \ldots, a_s \in A$ são elementos cujas imagens em B formam um sistema de parâmetros de B, então $a, a_1, \ldots, a_s$ formam um sistema de parâmetros de A, logo $\delta_A \leq \delta_B + 1$. Assim, $\delta_A - 1 \leq \delta_B \leq \dim B \leq \dim A - 1$, logo $\delta_A \leq \dim A$.

□

Um importante corolário de Teorema de Krull é o seguinte resultado conhecido como Krull Hauptidealsatz ou Teorema do Ideal Principal de Krull.

Teorema 214. (Krull Hauptidealsatz) *Seja A um anel Noetheriano e $a_1, \ldots, a_n \in A$. Seja $\mathfrak{p}$ um ideal primo de A minimal com a propriedade que $(a_1, \ldots, a_n) \subseteq \mathfrak{p}$, então $\mathrm{ht}(\mathfrak{p}) \leq n$. Em particular se $a \in A$ é um elemento que não é um divisor de zero nem uma unidade então todo ideal primo minimal que contém (a) tem altura 1.*

Demonstração. Considere $A_{\mathfrak{p}}$, que é um anel Noetheriano local com único ideal maximal $S^{-1}\mathfrak{p}$. O ideal $S^{-1}[(a_1, \ldots, a_n)A]$ é $S^{-1}\mathfrak{p}$-primário e é gerado por n elementos. Daí, pelo Teorema de Krull temos $n \geq \delta_{A_{\mathfrak{p}}} = \dim A_{\mathfrak{p}} = \mathrm{ht}(\mathfrak{p})$.

Para a segunda parte, sabemos que $\mathrm{ht}(\mathfrak{p}) \leq 1$. Suponha que $\mathrm{ht}(\mathfrak{p}) = 0$, então $\mathfrak{p}$ é um ideal primo minimal de A, i.e., $\mathfrak{p}$ é um elemento minimal de $V(0) = \mathrm{Spec}(A)$ e logo é um primo isolado associado a (0) (Proposição 136). Segue do Exercício 1 Lista 6 que todo elemento de $\mathfrak{p}$ é um divisor de zero mas $a \in \mathfrak{p}$, contradição. Logo $\mathrm{ht}(\mathfrak{p}) = 1$. □

Ex. 90 — Calcule a dimensão de $\mathbf{k}[[t]]$ e de $\mathbf{k}[x_1, x_2, \dots]$.

Ex. 91 — Seja A um anel e $\mathfrak{p} \in \operatorname{Spec}(A)$ então $\dim A \geq \operatorname{ht}(\mathfrak{p}) + \dim A/\mathfrak{p}$.

Ex. 92 — Prove que se $f \in \mathbf{k}[x_1, \dots, x_n]$ é irredutível então $\dim \mathbf{k}[x_1, \dots, x_n]/(f) = n - 1$.

Ex. 93 — Seja $A = \mathbf{k}[x_1, ..., x_n]/\mathfrak{p}$, $\mathfrak{p}$ um ideal primo de $\mathbf{k}[x_1, ..., x_n]$ e $\mathfrak{p}'$ um ideal primo de A. Mostre que $\dim(A/\mathfrak{p}') = \dim(A) - \operatorname{ht}(\mathfrak{p}')$.

Ex. 94 — Para cada um dos anéis locais Noetherianos a seguir, determine: um sistema de parâmetros minimal, o polinômio de Hilbert-Samuel e a dimensão de Krull:

1. $\mathbf{k}$ um corpo
2. $\mathbb{Z}_{(p)}$
3. $\mathbb{C}[x, y]_{(x,y)}$
4. $A_{\mathfrak{m}}$, onde $A = \mathbb{C}[x, y]/(y^2 - x^2(x+1))$ e $\mathfrak{m} = (\overline{x} + 1, \overline{y})$.
5. $A_{\mathfrak{m}}$, onde $A = \mathbb{C}[x, y]/(y^2 - x^2(x+1))$ e $\mathfrak{m} = (\overline{x}, \overline{y})$.

AULA 27: 24/11/2014 AULA DE EXERCÍCIOS

AULA 28: 26/11/2014 PROVA 2

A

IDENTIDADES BINOMIAIS

Seja $f : \mathbb{Z} \to \mathbb{Z}$ uma função. Definimos a **derivada discreta** de f , $\Delta f : \mathbb{Z} \to \mathbb{Z}$, pela regra$\Delta f(x) := f(x+1) - f(x)$. Chamamos um polinômio $p(x) \in \mathbb{Q}[x]$ de **numérico** se $p(m) \in \mathbb{Z}$ para todo $m \gg 0$ (isto significa que existe um $l \in \mathbb{Z}$ tal que $p(m) \in \mathbb{Z}$ para todo $m > l$). Definimos também um **polinômio binomial** como sendo um polinômio da forma $\binom{x}{n} := \frac{x(x-1)\cdots(x-n+1)}{n!} \in \mathbb{Q}[x]$, para algum $n \in \mathbb{Z}$ (por convenção $\binom{x}{0} = 1$ e $\binom{x}{n} = 0$ para $n < 0$).

Proposição 215. *$\binom{x}{n} \in \mathbb{Q}[x]$ é um polinômio numérico e $\Delta\binom{x}{n} = \binom{x}{n-1}$.*

Demonstração. Temos que

$$\begin{aligned}\Delta\binom{x}{n} &= \frac{(x+1)x(x-1)\cdots(x-n+2)}{n!} - \frac{x(x-1)\cdots(x-n+1)}{n!} \\ &= \frac{x(x-1)\cdots(x-n+2)}{(n-1)!} \cdot \frac{(x+1)-(x-n+1)}{n} = \binom{x}{n-1}.\end{aligned}$$

Sabemos que $\binom{m}{n} \in \mathbb{Z}$ para todo $m \geq n$ pois $\binom{m}{n}$ =nº de subconjuntos $S \subseteq \{1, \ldots, m\}$ com $|S| = n$. □

Proposição 216. *Todo polinômio numérico $p(x) \in \mathbb{Q}[x]$ tem a forma $p(x) = a_n\binom{x}{n} + a_{n-1}\binom{x}{n-1} + \cdots + a_0$ onde $a_i \in \mathbb{Z}$.*

Demonstração. Faremos a prova por indução sobre $n = \text{grau}(p)$. O caso $n = 0$ é claro. Como $\binom{x}{i} = \frac{\overbrace{x(x-1)\cdots(x-(i-1))}^{i \text{ fatores}}}{i!}$ tem grau i para $i \in \mathbb{N}$, os polinômios binomiais $\binom{x}{i}$ formam uma base de $\mathbb{Q}[x]$ sobre $\mathbb{Q}$ e assim podemos escrever

$$p(x) = a_n\binom{x}{n} + a_{n-1}\binom{x}{n-1} + \cdots + a_1\binom{x}{1} + a_0\binom{x}{0}, \text{ com } a_i \in \mathbb{Q}.$$

Temos que mostrar que $a_i \in \mathbb{Z}$, para isso considere:

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

Então $\Delta p(x)$ é um polinômio de grau $n-1$, tal que $\Delta p(m) = p(m+1) - p(m) \in \mathbb{Z}$ para todo inteiro $m \gg 0$, logo pela hipótese de indução

$a_n, \ldots, a_1 \in \mathbb{Z}$. Mas então $a_0 = p(x) - a_n\binom{x}{n} - a_{n-1}\binom{x}{n-1} - \cdots - a_1\binom{x}{1}$ é um polinômio constante que assume valores inteiros nos inteiros, logo $a_0 \in \mathbb{Z}$. □

Proposição 217. *Seja $f : \mathbb{Z} \to \mathbb{Z}$ uma função. Suponha que exista um polinômio $h(x) \in \mathbb{Q}[x]$ tal que $\Delta f(m) = h(m)$ para todo $m \gg 0$. Então existe um polinômio $p(x) \in \mathbb{Q}[x]$ tal que $\text{grau}(p) = 1 + \text{grau}(h)$ e $f(m) = p(m)$ para todo $m \gg 0$.*

Demonstração. Segue da hipótese que $h(x)$ é um polinômio numérico, logo da proposição anterior $h(x) = a_n\binom{x}{n} + a_{n-1}\binom{x}{n-1} + \cdots + a_0$ onde $a_i \in \mathbb{Z}$. Seja $q(x) := a_n\binom{x}{n+1} + a_{n-1}\binom{x}{n} + \cdots + a_0\binom{x}{1}$, então $\text{grau}(q) = n + 1 = \text{grau}(h) + 1$, $q : \mathbb{Z} \to \mathbb{Z}$ e $\Delta q(x) = h(x)$. Temos que $\Delta(f - q)(m) = 0$ para todo $m \gg 0$. Em outras palavras, $f(m) - q(m)$ é constante e inteiro para $m \gg 0$, digamos $c = f(m) - q(m)$, assim $f(m) = q(m) + c$ para $m \gg 0$, logo $p(x) = q(x) + c$ e o resultado segue. □

B

REFERÊNCIAS BIBLIOGRÁFICAS

[1] W. W. Adams e P. Loustaunau, *An introduction to gröbner bases, volume 3 of graduate studies in mathematics*, American Mathematical Society, Providence, RI, 24 (1994), p. 47.

[2] A. Ananin, *Álgebra Comutativa - Notas de Aulas*, 1998.

[3] R. B. Ash, *A course in commutative algebra*, Department of Mathematics, University of Illiois at Urbana-Champaign, 2003.

[4] M. F. Atiyah e I. G. Macdonald, *Introduction to commutative algebra*, vol. 2, Addison-Wesley Reading, 1969.

[5] N. Bourbaki, *Commutative algebra*, vol. 8, Hermann Paris, 1972.

[6] D. A. Cox, J. Little, e D. OSHEA, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*, Springer, 2007.

[7] D. Eisenbud et al., *Commutative algebra with a view toward algebraic geometry*, vol. 27, Springer New York, 1995.

[8] R. Hartshorne, *Algebraic geometry*, no. 52, Springer, 1977.

[9] G. Kemper, *A Course in Commutative Algebra*, vol. 256, Springer, 2010.

[10] E. Kunz, *Introduction to commutative algebra and algebraic geometry*, Springer, 2012.

[11] T.-Y. Lam, *Lectures on modules and rings*, no. 189, Springer, 1999.

[12] H. Matsumura, *Commutative algebra*, Benjamin/Cummings Publishing Company Reading, Massachusetts, 1980.

[13] ——, *Commutative ring theory*, vol. 8, Cambridge university press, 1989.

[14] M. Reid, *Undergraduate commutative algebra*, vol. 29, Cambridge University Press, 1995.

[15] S. Roman, *Advanced linear algebra*, vol. 135, Springer, 2007.

[16] J. J. Rotman, *Advanced modern algebra*, American Mathematical Soc., 2002.

[17] J. J. Rotman e J. J. Rotman, *An introduction to homological algebra*, vol. 2, Springer, 2009.

[18] R. Y. Sharp, *Steps in commutative algebra*, no. 51, Cambridge university press, 2000.

[19] E. Tengan, *Álgebra Comutativa: um tour ao redor dos anéis comutativos*, Em preparação, 2000.

[20] C. A. Weibel, *An introduction to homological algebra*, no. 38, Cambridge university press, 1995.

[21] O. Zariski e P. Samuel, *Commutative algebra. vol. 1. with the cooperation of is cohen. corrected reprinting of the 1958 edition*, Graduate Texts in Mathematics, 28 (1975).

[22] O. Zariski, P. Samuel, e I. S. Cohen, *Commutative algebra II*, vol. 2, Springer, 1960.

ÍNDICE REMISSIVO