Universidade Federal de Pernambuco

Centro de Ciências Exatas e da Natureza

Programa de Pós-Graduação em Matemática

Rafael Henrique Trajano Santos

Ideais fortemente irredutíveis sobre anéis comutativos com unidade

Recife

2016

Rafael Henrique Trajano Santos

Ideais fortemente irredutíveis sobre anéis comutativos com unidade

Este trabalho foi apresentado à Pós-Graduação em Matemática do Centro de Ciências Exatas e da Natureza da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. Eduardo Shirlippe Goes Leandro

Coorientador: Prof. Dr. Jorge Nicolás Caro Montoya

Recife

2016

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

S237i Santos, Rafael Henrique Trajano
Ideais fortemente irredutíveis sobre anéis comutativos com unidade / Rafael Henrique Trajano Santos. – 2016.
55 f.

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

1. Matemática. 2. Anéis aritméticos. I. Leandro, Eduardo Shirlippe Goes (orientador). II. Título.

510 CDD (23. ed.) UFPE- MEI 2017-220

Rafael Henrique Trajano Santos

Ideais fortemente irredutíveis sobre anéis comutativos com unidade

Este trabalho foi apresentado à Pós-Graduação em Matemática do Centro de Ciências Exatas e da Natureza da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre em Matemática.

Aprovado em: 21/10/2016.

BANCA EXAMINADORA

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

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

Prof. Dr. Rodrigo José Gondim Neves
(Examinador Externo)
Universidade Federal Rural de Pernambuco

AGRADECIMENTOS

Gostaria de agradecer aos meus familiares, especialmente meus pais Nilson Maurício dos Santos Costa e Rizonete Trajano da Silva pelo empenho em me fornecer um ambiente familiar com muito amor e boa educação, pois sem vocês eu nada seria. Agradecimento especial para a minha sobrinha Grazyella e meu irmão Carlos pelos bons momentos de distração nos jogos.

Às professoras da Escola Fátima Freitas pela excelente base no infantil e ao professores do Colégio Agostinho Nunes pelo excelente ensino médio, faço menção especial ao professor Rosivaldo José que foi quem mais me incentivou no caminho da Matemática nessa fase.

À minha amada e tricampeã Pernambucana de Xadrez Universitário Aline Anjos que mostrou que existe vida além da Matemática (desde o dia 14/11/2013). Com ela tenho os melhores momentos deste curto intervalo que é a vida e espero sempre contar com seu companheirismo e amor. É muito reconfortante encontrar em uma mesma pessoa a melhor amiga, amante, amor e companheira. Mesmo que ela nunca me deixe vencer no xadrez sua presença em minha vida trouxe a soma de boas aventuras que fizeram a diferença e multiplicaram a alegria que com ela hei de dividir sempre. Amo-te muito, amor! Além dela agradeço a minha sogra, Dona Alice, pela sempre amável recepção e apoio em todos os momentos.

Aos meus amigos e colegas pelas boas histórias para contar. Menciono especialmente Jones Barros, Adelson Elias, Felipe (Fu), Carlos Hélder (Zé), Ilan Trajano, Marcos Emílio, Ivson Mota, Ernesto Lins, João Gondim, Tiago DK, Michel, Josco, Turma LM 3x8 e Thiago Fiel.

Professores da UFRPE que tanto contribuíram para a melhor graduação que eu poderia ter. Em especial Anete Soares, Maria Eulália, Tiago Dias (DK), Renato(Tatinho), Rodrigo Gondim, Paulo Santiago, Marcelo Pedro, Gabriel Guedes e Antônio (Macarrão).

Membros da banca Eduardo Leandro (orientador), Rodrigo Gondim e Marco Barone pela disposição e aconselhamentos durante o processo.

Ao professor Nicolás Caro que desde o Verão de 2012 tem uma grande influência para mim e sem o qual não teria tido êxito nessa dissertação. Sua ajuda foi indispensável e seus conselhos sobre animes também!

RESUMO

Neste trabalho apresentamos as propriedades básicas dos ideais fortemente irredutíveis sobre anéis comutativos com unidade. Apresentamos também a relação entre ideais irredutíveis, ideais fortemente irredutíveis e ideais primários. Estudamos anéis aritméticos e a relação de ordem que os ideais destes anéis devem satisfazer ao serem estendidos em localizações no anel de frações para ideais primos. Caracterizaremos os ideais fortemente irredutíveis em anéis aritméticos, domínios fatoriais e anéis noetherianos, sendo este último caso para ideais não primos. Demonstramos a importância das hipóteses para cada tipo de anel e/ou ideal por meio de contraexemplos, deste modo explorando vários tipos de particularidades que podem surgir das definições abordadas. Destaque especial para o resultado que garante que, em um anel aritmético, todo ideal fortemente irredutível possui radical primo, e para nossa construção de um ideal fortemente irredutível cujo radical não é primo (feita em um anel não-aritmético), onde fazemos uso da ferramenta de idealização de módulos abordada nas noções iniciais desta dissertação.

Palavras-chave: Ideais fortemente irredutíveis. Ideais irredutíveis. Anéis aritméticos. Anéis noetherianos.

ABSTRACT

In this work we present the basic properties of strongly irreducible ideals in commutative rings with unity. We also exhibit the relationship between irreducible, strongly irreducible and primary ideals. We study arithmetical rings and the order relation that the ideals of such rings must satisfy after extension at localization at prime ideals. We characterize strongly irreducible ideals in arithmetical rings, UFDs and Noetherian rings, the latter case being that of nonprime ideals. We show the importance of the hypotheses for each kind of ring and/or ideal through counterexamples, exploring in this way the various types of particularities that can raise from the definitions considered. Special mention for the result that guarantees that, in an arithmetical ring, every strongly irreducible ideal has prime radical, and for our construction of a strongly irreducible ideal whose radical is nonprime (in a nonarithmetical ring), where we use the machinery of idealization of modules, which is treated on the preliminaries of this dissertation.

Keywords: Strongly irreducible ideals. Irreducible ideals. Arithmetical rings. Noetherian rings.

SUMÁRIO

1 NOÇÕES PRELIMINARES

1.1 Introdução

Um ideal de um anel é dito **irredutível** quando não puder ser escrito como interseção de dois ideais que o contenham propriamente. Ideais irredutíveis aparecem naturalmente no estudo da decomposição primária em anéis noetherianos, pois a decomposição primária neste tipo de anéis se reduz a expressar um ideal como interseção finita de ideais irredutíveis (vide Teorema 1.17 e Corolário 1.16). Nesta dissertação vamos estudar a seguinte noção: um ideal I de um anel A é dito **fortemente irredutível** quando dados dois ideais J, K no anel tem-se $J \cap K \subseteq I$ somente quando se verifica $J \subseteq I$ ou $K \subseteq I$. Demonstraremos, como é esperado, que todo ideal fortemente irredutível é irredutível, e que todo ideal primo é fortemente irredutível. Também estudaremos os ideais fortemente irredutíveis em anéis aritméticos. Um anel é dito **aritmético** se dados quaisquer ideais I, J, K, então eles satisfazem a relação $(I + J) \cap K = (I \cap K) + (J \cap K)$. Veremos que nesse tipo de anel as definições de irredutível e fortemente irredutível são equivalentes. Além das noções já mencionadas vamos estudar os ideais fortemente irredutíveis de um domínio fatorial e como se relacionam os ideais fortemente irredutíveis de um anel e os fortemente irredutíveis de sua localização.

O Capítulo 1 consiste em preliminares e pode ser omitido pelos leitores familiarizados com as noções básicas de Álgebra Comutativa. Consideramos neste capítulo duas seções que podem ser consideradas de nível intermediário, a saber: As Seções 1.3 e 1.4. Na primeira destas seções trabalhamos com as chamadas famílias de Oka, que consiste numa simples definição que generaliza as demonstrações de que dado um ideal cumprindo uma determinada propriedade e maximal a esse respeito seja primo. Na outra apresentamos as definições de idealização de um módulo e a caracterização dos ideais primos, maximais e do radical dessa estrutura, assim como a definição de módulo injetivo e extensão essencial.

O capítulo 2 está baseado nos artigos (HEINZER; RATLIFF JR.; RUSH, 2002) e (JENSEN, 1966) que trabalham, respectivamente, com as definições e propriedades dos ideais fortemente irredutíveis e anéis aritméticos. Inicialmente vamos verificar as relações entre ideais fortemente irredutíveis e ideais irredutíveis, bem como as relações entre os ideais fortemente irredutíveis de A e ideais fortemente irredutíveis na localização em um conjunto multiplicativo, mais especificamente provaremos que, sendo S um conjunto multiplicativo, se I_S é fortemente irredutível, então a sua saturação também o será e se I for fortemente irredutível e primário de maneira que o radical de I não tem interseção com S, então I_S será fortemente irredutível.

Demonstraremos que em um anel aritmético, as noções de ideal irredutível e redutível coincidem e o conjunto dos divisores de zero do A-módulo A/I formam um ideal primo, além disso caracterizaremos os anéis aritméticos provando que A é aritmético se, e somente se, para todo ideal primo de A, os ideais da localização no complementar do ideal são comparáveis pela relação de inclusão. Também daremos a caracterização completa dos ideais fortemente irredutíveis em um domínio de fatorial. Neste tipo de anel veremos que um ideal I será fortemente irredutível se, e somente se, o fato dele conter um produto de fatores irredutíveis, implica que algum dos fatores nele já está e por meio desta caracterização que exibiremos um exemplo de ideal irredutível que não é fortemente irredutível (vide o Exemplo 2.17).

Exibiremos uma série de implicações e demonstraremos que suas recíprocas não se verificam, a saber: Em um anel noetheriano todo irredutível é primário; em um anel aritmético todo primário é irredutível; em um anel aritmético todo ideal fortemente irredutível vai possuir radical primo. Destaque para a construção do contra-exemplo de ideal fortemente irredutível que não possui radical primo mesmo se o anel for noetheriano (vide Exemplo 2.21).

A última seção do Capítulo 2 consiste na caracterização dos ideais fortemente irredutíveis de um anel noetheriano que não são primos.

Neste trabalho todos os anéis são comutativos com unidade

1.2 Definições básicas

Notações:

Os ideais serão denotados por $I, J, K, \ldots$. Spec(A) denotará a família dos ideais primos de A, os que por sua vez serão denotados por $\mathfrak{p}, \mathfrak{q}, \ldots$. Os ideais maximais serão denotados por $\mathfrak{m}, \mathfrak{n}, \ldots$, e o conjunto de tais ideais será denotado por m-Spec(A). Para o leitor que não está familiarizado com alguma das noções acima, recomendamos consultar os livros (BORGES; TENGAN, 2015), (EISENBUD, 1995) e/ou (ALTMAN; KLEIMAN, 2013).

Se M é um A-módulo, denotamos o fato de N ser um A-submódulo de M por $N < M$. O submódulo gerado por um subconjunto $\mathcal{B}$ de um A-módulo M será denotado por $\langle \mathcal{B} \rangle$. O quociente entre dois submódulos N, P de um A-módulo M (ou seja, o conjunto $\{a \in A : aP \subseteq N\}$) será denotado por $(N : P)$. Se $N = \langle n \rangle$, escrevemos $(N : P)$ como $(n : P)$, e similarmente se P é cíclico. O anulador $(0 : N)$ de um submódulo N de M será as vezes denotado por Ann(N), e por Ann(m) quando $N = \langle m \rangle$. O radical de

um ideal I em um anel A (ou seja, os elementos $a \in A$ tais que $a^m \in I$ para algum $m \geq 0$) será denotado por $\mathrm{Rad}(I)$.

Definição 1.1. Sejam A um anel e M um A-módulo. Um elemento $a \in A$ é dito **divisor de zero (em M)**, se existir $m \in M \setminus 0$ tal que $am = 0$. Caso contrário (isto é, se $am \neq 0$ para todo $m \in M \setminus 0$) é dito ***M*-regular**. Quando $M = A$, falamos simplesmente de divisor de zero ou de elemento regular.

Denotaremos o conjunto dos divisores de zero em M por $\mathcal{Z}_A(M)$; se $M = A$, o denotaremos simplesmente por $\mathcal{Z}(A)$. Certamente $\mathcal{Z}(A) \cap A^* = \emptyset$ (onde A^* denota o conjunto dos elementos invertíveis do anel A), pois se $a \in A^*$ e $c \in A$ satisfazem $ac = 0$, então teremos $0 = a^{-1} \cdot 0 = a^{-1}(ac) = (a^{-1}a)c = 1 \cdot c = c$. Em particular $\mathcal{Z}(A) \subsetneq A$.

Definição 1.2. Um ideal I de um anel A é dito **regular** se I possui algum elemento regular.

Para o leitor que desejar saber mais propriedades dos ideais regulares, recomendamos consultar (GILMER, 1992).

Definição 1.3. Seja A um anel. Um subconjunto $S \subseteq A$ é dito:

- **Multiplicativo fechado** (ou simplesmente multiplicativo) quando $1 \in S$ e se $s, t \in S$, então $st \in S$.
- **Saturado** quando $st \in S$, implica $s, t \in S$.

Exemplo 1.4.

i) Os conjuntos $\{0, 1\}$ e $\{1\}$ são multiplicativos, mas em geral não são saturados, pois podemos ter divisores de zero e/ou elementos invertíveis.

ii) Dado $a \in A$, o conjunto $S_a = \{1, a, a^2, \ldots\}$ é multiplicativo, porém não necessariamente saturado, pelos mesmos motivo do item anterior.

iii) Se I é um ideal, então $1 + I$ é multiplicativo (não necessariamente saturado). Ainda, o conjunto $A \setminus I$ é saturado, e será multiplicativo precisamente quando I for primo.

iv) O conjunto A^* dos elementos invertíveis do anel A é multiplicativo e saturado.

v) Se A é um domínio, o conjunto $S = \{up_1 \cdots p_m : u \in A^*, m \geq 0,$ cada p_i é primo$\}$ é multiplicativo (trivial), e também é saturado. De fato, se $st \in S$, digamos $st = up_1 \cdots p_m$, então ou bem $m = 0$, isto é, $st \in A^*$, logo $s, t \in A^*$, ou bem $m \geq 1$. Usando que cada p_i é primo (ou seja, se p_i divide ab, então p_i divide a ou p_i divide b) concluímos que (reetiquetando se necessário) vale $s = s'p_1 \cdots p_k$ e

$t = t'p_{k+1}\cdots p_m$. Substituindo na igualdade original e cancelando obtemos $s't' = u$, logo $s', t' \in A^*$, como desejado.

vi) Um subconjunto S é multiplicativo saturado se, e somente se, $A \setminus S$ for união de ideais primos. Este resultado pode ser usado para caracterizar domínios fatoriais, a saber: um domínio D é fatorial se todo ideal primo não nulo de D contém um elemento primo (o recíproco é trivial). Com efeito: Na notação do item anterior queremos provar que $S = D \setminus 0$. Ora, temos $A \setminus S = \cup_{P\in\mathcal{F}} P$ para alguma família $\mathcal{F}$ de ideais primos; mas se Q é primo não nulo então $Q \cap S \neq \emptyset$ pela hipótese, logo $Q \notin \mathcal{F}$.

vii) Dado um polinômio $f = \sum_{i=0}^{m} f_i X^i \in A[X]$, definimos o **conteúdo** de f como o ideal $c(f) = \langle f_0, \ldots, f_m\rangle$; tal f será chamado de **primitivo** se $c(f) = A$. Se $S = \{f \in A[X] : f \text{ é primitivo}\}$, então S é multiplicativo saturado. Com efeito, pela definição de multiplicação de polinômios teremos $c(fg) \subseteq c(f)c(g) \subseteq c(f) \cap c(g)$, logo $fg \in S$ implica $f, g \in S$; reciprocamente, se fg não é primitivo então existe um ideal maximal $\mathfrak{m}$ contendo $c(fg)$. Se $\theta : A[X] \to (A/\mathfrak{m})[X]$ é o homomorfismo natural ($X \mapsto X; a \in A \mapsto a + \mathfrak{m} \in A/\mathfrak{m}$), então $\theta(fg) = \theta(f)\theta(g)$; como $(A/\mathfrak{m})[X]$ é um domínio, segue que $\theta(f) = 0$ ou $\theta(g) = 0$, isto é, $c(f) \subseteq \mathfrak{m}$ ou $c(g) \subseteq \mathfrak{m}$.

viii) O conjunto $S = A \setminus \mathcal{Z}(A)$ dos elementos regulares em A é multiplicativo saturado. De fato $1 \in A^* \subseteq S$, e se $s, t \in S$, então para qualquer $c \neq 0$ temos $tc \neq 0$ (pois t é regular), logo $(st)c = s(tc) \neq 0$ (pois s é regular), o que mostra que S é multiplicativo. Por outro lado, se $st \in S$ e $b \neq 0$ então $sb, tb \neq 0$, pois do contrário $stb = 0$, contradição, e assim S é também saturado.

1.3 Anéis e módulos noetherianos

Um conjunto parcialmente ordenado $(\Sigma, \leq)$ satisfaz a **condição de cadeia ascendente**, abreviada pela sigla c.c.a., se toda cadeia de elementos $s_1 \leq s_2 \leq \cdots \leq s_k \leq \cdots$ em Σ estaciona, ou mais formalmente, existe um índice n implicando que $s_i = s_n$ para todo i com $i \geq n$.

Proposição 1.5. *As seguintes condições em um A-módulo M são equivalentes:*

a) A família dos submódulos de M, ordenada por inclusão, satisfaz c.c.a..

b) Toda família não-vazia de submódulos de M possui um elemento maximal (respeito da inclusão).

c) Todo conjunto C de geradores de um submódulo N possui um subconjunto finito C_0 que ainda gera N.

d) Todo submódulo N de M é finitamente gerado.

Demonstração.

$a) \Rightarrow b)$ Se existe alguma família não vazia de submódulos de M sem elemento maximal, dado um submódulo N na família sempre existirá outro submódulo P em tal família satisfazendo $N \subsetneq P$. Dessa forma existe[§] uma cadeia de submódulos $N_1 \subsetneq N_2 \subsetneq \cdots \subsetneq N_k \subsetneq \cdots$.

$b) \Rightarrow c)$ Seja C um conjunto de geradores de um submódulo N, e considere a família $\mathcal{F}$ dos submódulos $\langle D \rangle$, onde D é um subconjunto finito de C. Temos $\mathcal{F} \neq \emptyset$, porque $0 = \langle \emptyset \rangle \in \mathcal{F}$, logo pela hipótese existirá P maximal em $\mathcal{F}$, digamos $P = \langle C_0 \rangle$, onde C_0 é um subconjunto finito de C. Então $N = P$, pois se $m \in C$, então $P + \langle m \rangle = \langle C_0 \cup \{m\} \rangle \supseteq P$, sendo que $C_0 \cup \{m\}$ é um subconjunto finito de C, logo pela maximalidade de P teremos $P + \langle m \rangle = P$, e assim $m \in P$.

$c) \Rightarrow d)$ Tome $C = N$.

$d) \Rightarrow a)$ Considere uma cadeia $N_1 \subseteq N_2 \subseteq \cdots N_k \subseteq \cdots$ de submódulos. É fácil ver que $P = \bigcup_{j \geq 1} N_j$ é um submódulo, e devido à hipótese teremos $P = \langle m_1, m_2, \ldots, m_t \rangle$. Deduz-se que existe um índice ℓ tal que $m_j \in N_\ell$ para cada j, o que mostra que vale $P = N_\ell$, e a cadeia estaciona neste índice. □

Definição 1.6. Um A-módulo M satisfazendo alguma (portanto todas) das condições da Proposição anterior é dito ***A*-módulo noetheriano**. Se $M = A$, dizemos que A é um **anel noetheriano**, e podemos trocar "submódulo" pelo seu equivalente, a saber, "ideal", no enunciado da Proposição.

Proposição 1.7 (Teorema da base de Hilbert)**.** *Se A é um anel noetheriano, então $A[X]$ é também anel noetheriano.*

Demonstração. Suponhamos, por contradição, que exista um ideal $I \subseteq A[X]$ que não seja finitamente gerado. Claramente, por estas hipóteses, $I \neq 0$, portanto existe $f_1 \in I$ de grau mínimo, cujo coeficiente líder será denotado por a_1. Considere agora $f_2 \in I \setminus \langle f_1 \rangle \neq \emptyset$ (pois I não é finitamente gerado), de maneira que f_2 tenha grau mínimo, e seja a_2 seu coeficiente líder. Prosseguindo[†] teremos polinômios $f_1, f_2, \ldots, f_n, \ldots$ cumprindo:

- $f_i \in I \setminus \langle f_1, f_2, \ldots, f_{i-1} \rangle$.
- Denotando o grau de um polinômio g por ∂g, vamos ter $\partial f_i \leq \partial f_{i+1}$ para cada i.

[§] Usando o chamado **axioma da escolha dependente**, que afirma o seguinte: Dada uma relação $\mathcal{R}$ em um conjunto A, tal que $\mathrm{Dom}(\mathcal{R}) = A$ (ou seja, para cada $a \in A$ existe pelo menos um elemento $b \in A$ com $a\mathcal{R}b$), existe uma sequência $(a_n)_{n \geq 1}$ de elementos de A tal que $a_n \mathcal{R} a_{n+1}$ para todo n.

[†] De novo, pelo axioma da escolha dependente.

Considere a cadeia $\langle a_1\rangle \subseteq \langle a_1, a_2\rangle \subseteq \cdots \langle a_1, a_2, \cdots, a_n\rangle \subseteq \cdots$ de ideais em A. A hipótese garante a existência de $k \in \mathbb{N}$ de maneira que $a_j \in \langle a_1, \ldots, a_k\rangle$ para todo j, o que em particular nos dá $a_{k+1} = \sum_{i=1}^{k} b_i a_i$ para alguns $b_1, \ldots, b_k \in A$. Considere agora o polinômio

$$h = \sum_{i=1}^{k} b_i X^{\partial f_{k+1} - \partial f_i} f_i \,.$$

Segue que o coeficiente do termo de grau ∂f_{k+1} de h é $\sum_{i=1}^{k} b_i a_i = a_{k+1}$ e evidentemente $\partial h \leq \partial f_{k+1}$, logo h e f_{k+1} têm o mesmo grau e o mesmo coeficiente líder, e portanto $\partial(f_{k+1} - h) < \partial f_{k+1}$. Pela minimalidade de ∂f_{k+1} segue que $f_{k+1} - h \in \langle f_1, f_2, \ldots, f_k\rangle$; mas $h \in \langle f_1, f_2, \ldots, f_k\rangle$ por construção e, portanto, $f_{k+1} \in \langle f_1, f_2, \ldots, f_k\rangle$, contradição. Logo I é finitamente gerado. □

Corolário 1.8. *Se A é noetheriano, então $A[X_1, X_2, \ldots, X_n]$ é noetheriano.*

Lema 1.9. *Seja M um A-módulo, e sejam N um submódulo e $m \in M$. Seja $\{n_i + a_i m\}_{i\in I}$ um conjunto de geradores de $N + \langle m\rangle$ (onde $a_i \in A$ para cada $i \in I$), e seja $\{b_j\}_{j\in J}$ um conjunto de geradores do ideal $(N : m)$. Então $\{n_i\}_{i\in I} \cup \{b_j m\}_{j\in J}$ é um conjunto de geradores de N. Em particular, se $N + \langle m\rangle$ e $(N : m)$ são finitamente gerados, então N o será.*

Demonstração. Claramente $\left\langle \{n_i\}_{i\in I} \cup \{b_j m\}_{j\in J}\right\rangle \subseteq N$. Se $n \in N \subseteq N + \langle m\rangle$ então existem $c_i \in A$ tais que $n = \sum_{i\in I} c_i(n_i + a_i m)$, logo $\left(\sum_{i\in I} c_i a_i\right)m = n - \sum_{i\in I} c_i n_i \in N$, isto é, $\sum_{i\in I} c_i a_i \in (N : m)$. Portanto existem $d_j \in A$ tais que $\sum_{i\in I} c_i a_i = \sum_{j\in J} d_j b_j$, o que implica $n = \sum_{i\in I} c_i n_i + \sum_{j\in J} d_j(b_j m) \in \left\langle \{n_i\}_{i\in I} \cup \{b_j m\}_{j\in J}\right\rangle$. □

Pelo teorema de correspondência, se $f : A \to B$ é um homomorfismo sobrejetivo de anéis e A é noetheriano, então B também o será. Similarmente, se M é um A-módulo noetheriano (independentemente de A ser ou não anel noetheriano) e $g : M \to N$ é uma aplicação A-linear sobrejetiva, então N também será um A-módulo noetheriano. Isto, junto com o Lema anterior, será usado no resultado a seguir.

Proposição 1.10. *Se A é um anel noetheriano e M é um A-módulo finitamente gerado, então M é um A-módulo noetheriano.*

Demonstração. Por indução no número n de geradores. Se $n = 1$ então M é imagem sobrejetiva do A-módulo A, o qual é (anel) noetheriano pela hipótese, logo o resultado segue. Suponhamos então que qualquer A-módulo gerado por menos de n elementos (sendo $n > 1$ fixo) é noetheriano, e seja $M = \langle m_1, \ldots, m_{n-1}, m\rangle$. Seja $P = M/\langle m\rangle$, e considere a projeção $\pi : M \to P$. Note que vale $P = \left\langle \pi(m_1), \ldots, \pi(m_{n-1})\right\rangle$, logo P será A-módulo noetheriano pela hipótese de indução.

Se N é um submódulo de M então $\pi(N)$ o será de P, logo $\pi(N)$ será finitamente gerado. Ora, pelo teorema de correspondência, $\pi(N)$ corresponde ao submódulo

$N + \mathrm{Ker}(\pi) = N + \langle m \rangle$ de M, logo $N + \langle m \rangle$ será finitamente gerado. Como $(N : m)$ é um ideal finitamente gerado (pois A é noetheriano), concluímos do Lema 1.9 que N é finitamente gerado. □

Definição 1.11. Um ideal $I \neq A$ é dito **primário** se dados $x, y \in A$ com $xy \in I$ então ou bem $x \in I$ ou bem existe $n \geq 1$ tal que $y^n \in I$. Um ideal I é dito **$\mathfrak{p}$-primário** se I é primário e $\mathrm{Rad}(I) = \mathfrak{p}$. Convém notar que se I é primário, então $\mathrm{Rad}(I)$ é primo.

Presente na definição anterior está a generalização de aspectos relativos ao anel dos inteiros $\mathbb{Z}$. Em $\mathbb{Z}$ se p é primo e vale $p^n \mid rs$, então $p^n \mid r$ ou $p^n \mid s^k$ para algum $k \in \mathbb{N}$. Este resultado nada mais é do que um corolário do teorema fundamental da aritmética. O caso $n = 1$ nos dá p primo em $\mathbb{Z}$ e ideal primo para anéis em geral. Logo todo ideal primo é primário, mas não vice-versa. Ademais é na ideia de decomposição em fatores primos que baseia-se a ideia de decomposição primária que veremos a seguir.

Lema 1.12. *Sejam A, B anéis e $\phi : A \to B$ um homomorfismo sobrejetivo. Ainda, sejam I um ideal de B e J um ideal em A tal que $\phi(J) = I$. Então:*

a) $\phi^{-1}(I) = J + \mathrm{Ker}(\phi)$.

b) $\dfrac{A}{J + \mathrm{Ker}(\phi)} \simeq \dfrac{B}{I}$.

c) I é primário se, e somente se, $J + \mathrm{Ker}(\phi)$ é primário.

Demonstração. Dado $x \in \phi^{-1}(I)$ temos que existe $y \in J$ tal que $\phi(x) = \phi(y)$, logo $x - y \in \mathrm{Ker}(\phi)$, implicando $x \in J + \mathrm{Ker}(\phi)$. A inclusão oposta é óbvia, obtendo *a*).

Ora, o núcleo do homomorfismo composto $A \xrightarrow{\phi} B \xrightarrow{\pi} B/I$, que é sobrejetivo, é justamente $\phi^{-1}(I)$, logo *b*) segue do teorema do isomorfismo junto com *a*).

Finalmente, um ideal K em um anel R é primário se, e somente se, $R/K \neq 0$ e $\mathcal{Z}(R/K) \subseteq \mathrm{Rad}(0_{R/K})$. Ou seja, a condição de K ser primário equivale a uma condição do anel quociente R/K; como tal condição evidentemente é preservada por isomorfismo, o resultado do item *c*) segue (aplicado aos anéis quociente do item *b*)). □

Definição 1.13. Sejam A um anel e I um ideal de A. Dizemos que I admite uma **decomposição primária** se existem ideais primários $P_1, \ldots, P_n$ tais que $I = \bigcap_{i=1}^{n} P_i$.

Definição 1.14. Dado $I \subseteq A$ um ideal, I é dito **irredutível** se não puder ser escrito como interseção de dois ideais o contendo propriamente.

Proposição 1.15. *Seja $I \subseteq A$ um ideal irredutível. Então I é primário se, e somente se, para todo $a \in A$ a cadeia $I \subseteq (I : a) \subseteq (I : a^2) \subseteq \cdots \subseteq (I : a^n) \subseteq \cdots$ é estacionária.*

Demonstração. Seja $\mathrm{Rad}(I) = \mathfrak{p}$. Se I é primário, então $\mathfrak{p}$ é primo. Tomemos $a \in A$, portanto $a \in \mathfrak{p}$ ou $a \in A \setminus \mathfrak{p}$. No primeiro caso $a^n \in I$ para algum $n \in \mathbb{N}$, ocasionando $(I : a^n) = (I : a^{n+i}) = A$ para todo inteiro positivo i. Se $a \notin \mathfrak{p}$, então para cada $k \in \mathbb{N}$ vale $a^k \notin I$, portanto se $b \in (I : a^n)$, então $ba^n \in I$, logo $b \in I$ pois I é primário. Isto prova a inclusão $(I : a^n) \subseteq I$ para todo n. Como a outra inclusão é trivial, concluímos que vale $(I : a^n) = I$ para cada n.

Reciprocamente, sejam $a, b \in A$ com $b \notin I$ e $a \notin \mathfrak{p}$. Queremos provar que $ab \notin I$. Pela hipótese (do recíproco) a cadeia

$$I \subseteq (I : a) \subseteq (I : a^2) \subseteq \cdots \subseteq (I : a^k) \subseteq \cdots$$

é estacionária, e assim existe n de maneira que $(I : a^n) = (I : a^{n+1})$. Os ideais $I + \langle b \rangle$ e $I + \langle a^n \rangle$ contém propriamente o ideal I, logo pela irredutibilidade de I não podemos ter $I = (I + \langle b \rangle) \cap (I + \langle a^n \rangle)$, portanto existe $r \in \left[\left(I + \langle b \rangle\right) \cap \left(I + \langle a^n \rangle\right)\right] \setminus I$, ou seja, $r = \ell_1 + sb = \ell_2 + ta^n \notin I$ com $\ell_1, \ell_2 \in I$ e $s, t \in A$. Se fosse $ab \in I$ então $a\ell_2 + ta^{n+1} = ar = a\ell_1 + sab \in I$, e como $a\ell_2 \in I$, então $ta^{n+1} \in I$, isto é, $t \in (I : a^{n+1}) = (I : a^n)$, ocasionando $r = \ell_2 + ta^n \in I$, contradição. Segue que $ab \notin I$, o que mostra que e I é primário. □

Corolário 1.16. *Em um anel noetheriano todo ideal irredutível é primário.*

Teorema 1.17. *Se A é um anel noetheriano, então todo ideal de A admite decomposição primária.*

Demonstração. Considere a família $\mathcal{F}$ de todos os ideais que não podem ser expressos como interseção finita ideais irredutíveis. Se $\mathcal{F} \neq \emptyset$, então existe um elemento M que é maximal nesta família; tal M é em particular redutível, logo $M = J \cap K$, onde J e K são ideais e J, K contendo estritamente M. Pela maximalidade de M, segue que J, K não estão em $\mathcal{F}$ e isso nos dá que $J = \bigcap_{i=1}^{m} P_i$ e $K = \bigcap_{j=1}^{n} Q_j$, sendo cada P_i e Q_j irredutíveis. Reindexando os termos se necessário, encontramos $M = \bigcap_{k=1}^{r} P_k^*$, com cada P_k^* irredutível, uma contradição. Assim $\mathcal{F} = \emptyset$, e já que todo irredutível em um anel noetheriano é primário o resultado segue. □

Definição 1.18. Uma família de ideais $\mathcal{F}$ de um anel A é dita **família de Oka** se $A \in \mathcal{F}$ e para quaisquer $a \in A$ e qualquer ideal I em A temos que $(I : a), I + \langle a \rangle \in \mathcal{F}$ implica $I \in \mathcal{F}$.

O estudo das famílias de Oka permite generalizar muitas demonstrações importantes da Álgebra que envolvem ideais primos. Para saber mais consulte (LAM; REYES, 2009)

Dada uma família $\mathcal{F}$ de ideais em A, denotamos por $\mathcal{F}^c$ a família complementar, ou seja, a família de ideais em A que não estão em $\mathcal{F}$. Com esta notação temos o seguinte resultado:

Proposição 1.19. *Seja $\mathcal{F}$ uma família de Oka em um anel A. Se J é um ideal maximal em $\mathcal{F}^c$ (com respeito à inclusão), então J é primo.*

Demonstração. Suponhamos, por contradição, que $J \in \mathcal{F}^c$ não seja primo. Já temos $J \subsetneq A$ pois $A \in \mathcal{F}$. Pela definição de ideal primo, temos, por negação, que existem $a, b \in A$ tais que $a, b \notin J$ mas $ab \in J$. Notemos que $J \subsetneq J + \langle a \rangle$ pois $a \notin J$, e $J \subsetneq (J : a)$ pois $ab \in J$, logo $b \in (J : a)$, e por hipótese $b \notin J$. Pela maximalidade de J segue necessariamente $J + \langle a \rangle, (J : a) \in \mathcal{F}$, mas isso implicaria $J \in \mathcal{F}$, absurdo. Portanto o ideal J é primo. □

Definição 1.20. Seja M um A-módulo. Um ideal I de A é dito ***M*-anulador** se $I = \mathrm{Ann}(m)$ para algum $m \in M \setminus 0$. Quando $M = A$, falamos simplesmente de ideal anulador. Um **primo associado** de M é um ideal primo que é M-anulador; o conjunto dos primos associados de M será denotado por $\mathrm{Ass}(M)$.

Proposição 1.21. *Em cada um dos seguintes casos, os ideais correspondentes formam exemplos de famílias de Oka:*

a) Os ideais não disjuntos de um conjunto multiplicativo fixado S.

b) Os finitamente gerados.

c) Os principais.

d) Os não M-anuladores de um A-módulo M fixado.

Além disso, os complementares das famílias dos itens a), b) e c) (ordenados por inclusão), quando não vazios, satisfazem a hipótese do lema de Zorn.

Demonstração.

a) Sejam S um conjunto multiplicativo que não contenha o zero e $\mathcal{F}_S$ a família dos ideais $J \in A$ não disjuntos de S. Tomemos $a \in A$ e $I \subseteq A$ tais que $(I : a), I + \langle a \rangle \in \mathcal{F}_S$. Então existem $s \in (I : a) \cap S$ e $t \in I + \langle a \rangle$, ou seja $sa \in I$ e $t = x + ba$ com $x \in I$ e $b \in A$. Como S é multiplicativo temos que $st \in S$, todavia $st = sx + bsa \in I$, pois $x \in I$ e $sa \in I$, logo $st \in I \cap S$ e $I \in \mathcal{F}_S$.

Se $\mathcal{F}_S^c \neq \emptyset$ e $\mathcal{A}$ é uma subfamília totalmente ordenada em $\mathcal{F}_S^c$, é simples provar que $\bigcup \mathcal{A}$ é um ideal, e evidentemente $\bigcup \mathcal{A}$ é disjunto do conjunto S, logo $\bigcup \mathcal{A} \in \mathcal{F}_S^c$.

b) Seja $\mathcal{F}$ a família dos ideais finitamente gerados. Como $A = \langle 1 \rangle$, então é finitamente gerado e $A \in \mathcal{F}$. Se I é um ideal e $a \in A$ são tais que $(I : a)$ e $I + \langle a \rangle$ são finitamente gerados, então I é finitamente gerado pelo Lema 1.9.

Se $\mathcal{F}^c \neq \emptyset$, considere uma subfamília $\mathcal{A}$ totalmente ordenada em $\mathcal{F}^c$. Afirmamos que $\bigcup \mathcal{A}$ não é finitamente gerado: De fato, se $\bigcup \mathcal{A}$ fosse finitamente gerado,

digamos $\bigcup \mathcal{A} = \langle x_1, \ldots, x_n \rangle$, então existiriam ideais $I_1, \ldots, I_n$ em $\mathcal{A}$ tais que $x_i \in I_i$ para todo i. Pela ordenação total segue (reetiquetando se necessário) $x_i \in I_i$ e $I_1, I_2, \ldots, I_{n-1} \subseteq I_n$, implicando $\bigcup \mathcal{A} \subseteq \langle x_1, \ldots, x_n \rangle \subseteq I_n \subseteq \bigcup \mathcal{A}$, isto é, finitamente gerado.

c) Seja $\mathcal{F}$ a família dos ideais principais. Temos $A = \langle 1 \rangle \in \mathcal{F}$. Sejam $I \subseteq A$ e $a \in A$ tais que $I + \langle a \rangle, (I : a) \in \mathcal{F}$, digamos $I + \langle a \rangle = \langle x + ra \rangle$ e $(I : a) = \langle b \rangle$, com $x \in I$. Para quaisquer I e a vale $\big(I + \langle a \rangle\big)(I : a) \subseteq I$, o que neste caso se traduz em $\big\langle (x + ra)b \big\rangle \subseteq I$. Afirmamos que vale a inclusão oposta, do qual decorrerá que I é principal.

Ora, da prova do item anterior obtemos $I = \langle x, ba \rangle$, logo basta provar que valem $x, ba \in \big\langle (x + ra)b \big\rangle$. Como $x, a \in I + \langle a \rangle = \langle x + ra \rangle$ então existem $s, t \in A$ de maneira que

$$\begin{aligned} x &= s(x + ra)\,; \\ a &= t(x + ra)\,. \end{aligned}$$

Da segunda igualdade obtemos $ba = t(x+ra)b \in \big\langle (x+ra)b \big\rangle$, e como $x = s(x+ra)$, então basta demonstrarmos que $s \in \langle b \rangle = (I : a)$, isto é, $\boldsymbol{sa \in I}$. Ora, temos $sra = (1-s)x$ e $tx = (1-rt)a$. Estas igualdades podem se expressar matricialmente por

$$\begin{bmatrix} s-1 & sr \\ t & rt-1 \end{bmatrix} \begin{bmatrix} x \\ a \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Denotando a matriz quadrada acima por B e multiplicando por $\operatorname{cof}(B)^t$ ♠ vem que:

$$\operatorname{cof}(B)^t B = \det(B) \begin{bmatrix} x \\ a \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix},$$

e em particular $\det(B)a = 0$; por outro lado $\det(B) = 1 - s - rt$, logo

$$\begin{aligned} sa &= \big[1 - rt - (1 - s - rt)\big]a \\ &= \big[1 - rt - \det(B)\big]a \\ &= (1 - rt)a \\ &= tx \in I \quad (\text{pois } x \in I)\,. \end{aligned}$$

Finalmente, se $\mathcal{F}^c \neq \emptyset$ e $\mathcal{A}$ é uma família totalmente ordenada em $\mathcal{A}$, então $\bigcup \mathcal{A}$ não é principal, pois se existisse $a \in A$ tal que $\bigcup \mathcal{A} = \langle a \rangle$, então $a \in J$ para algum $J \in \mathcal{A}$, o que implicaria $\bigcup \mathcal{A} = \langle a \rangle$, contradição.

d) Seja $\mathcal{F}$ a família dos ideais que não são M-anuladores. Certamente $A \in \mathcal{F}$, pois $1 \in A$. Agora raciocinamos pela contrapositiva: tomemos $I \notin \mathcal{F}$, ou seja $I = \operatorname{Ann}(m)$

♠ Usamos a identidade $\operatorname{cof}(B)^t B = \det(B) I$, sendo I a matriz identidade.

para algum $m \in M \setminus 0$. Se $I + \langle a \rangle$ é M-anulador, nada temos a fazer; caso contrário $I = \mathrm{Ann}(m) \subsetneq I + \langle a \rangle$ e consequentemente $a \notin I$. Portanto $am \neq 0$, e já que $\mathrm{Ann}(am) = \{y \in A : yam = 0\} = \{y \in A : ya \in \mathrm{Ann}(m)\} = (I : a)$, concluímos que $(I : a)$ é M-anulador, isto é, $(I : a) \notin \mathcal{F}$. □

A seguir daremos uma prova alternativa (e mais fácil) do item c) da Proposição anterior [¶].

Lema 1.22. *Sejam $a, b \in A$. Então $\langle a \rangle \cap \langle b \rangle = a(b : a)$; ainda, se um ideal $I \subseteq A$ cumpre $I \subseteq \langle a \rangle$, então $I = a(I : a)$.*

Demonstração. Evidentemente $a(b : a) \subseteq \langle a \rangle \cap \langle b \rangle$. Se $x \in \langle a \rangle \cap \langle b \rangle$ então $x = ar = bs$, com $r, s \in A$. Portanto $r\langle a \rangle \subseteq \langle b \rangle$ e assim $r \in (b : a)$, logo $x = ar \in a(b : a)$.

Por outro lado, se $I \subseteq \langle a \rangle$, então para cada $x \in I$ vale $x = aw$, com $w \in A$, e portanto $w \in (x : a) \subseteq (I : a)$. Assim $x = aw \in a(I : a)$. A inclusão $a(I : a) \subseteq I$ é evidente. □

Corolário 1.23 (Demonstração alternativa). *A família dos ideais principais é de Oka.*

Demonstração. Sejam $a, b, c \in A$ e I um ideal tais que $I + \langle a \rangle = \langle b \rangle$ e $(I : a) = \langle c \rangle$. Note que $(I : b) = \big(I : I + \langle a \rangle\big) = (I : a)$. Como $I \subseteq \langle b \rangle$, então pelo Lema anterior temos $I = b(I : b) = \langle bc \rangle$, como desejado. □

Ainda como consequência da Proposição 1.21 temos os seguintes resultados:

Corolário 1.24 (Cohen)**.** *Um anel A é noetheriano se, e somente se, todo ideal primo é finitamente gerado.*

Demonstração. Se A e noetheriano o resultado segue pela condição d) da Proposição 1.5. Reciprocamente, se A não é noetheriano, então com as notações do item c) da Proposição 1.21 teremos $\mathcal{F}^c \neq \emptyset$, logo pelo mesmo item as hipóteses do lema de Zorn são satisfeitas, e desse modo $\mathcal{F}^c$ possui um elemento maximal, o qual será primo pela Proposição 1.19; em outras palavras, haverá um ideal primo que não será finitamente gerado. □

Lema 1.25. *Sejam A um anel, J um ideal fixado e $\mathbb{J} = \{I : I \text{ ideal}, I \not\supseteq J\}$. Se $\mathcal{F}$ é uma família de Oka, então $\mathcal{G} = \mathcal{F} \cup \mathbb{J}$ também o será. Ainda, se $\mathcal{G}^c \neq \emptyset$ e $\mathcal{F}^c$ satisfaz a hipótese do lema de Zorn, então $\mathcal{G}^c$ também o fará. Finalmente, todo elemento maximal em $\mathcal{G}^c$ é maximal em $\mathcal{F}^c$.*

Demonstração. Sejam I ideal em A e $a \in A$ tais que $I + \langle a \rangle$ e $(I : a)$ estão em $\mathcal{G}$. Se $I + \langle a \rangle$ e $(I : a)$ estão em $\mathcal{F}$ acabou; caso contrário $I + \langle a \rangle \in \mathbb{J}$ ou $(I : a) \in \mathbb{J}$, logo $I \not\supseteq J$, pois $I \subseteq I + \langle a \rangle, (I : a)$. Em cada um dos casos $I \in \mathcal{G}$.

[¶] A ideia do argumento já apresentado, usando "álgebra linear matricial", foi dada pelo Prof. Nicolás.

Por outro lado, se $\mathcal{G}^c \neq \emptyset$ e toda cadeia em $\mathcal{F}^c$ admite cota superior em $\mathcal{F}^c$, então toda cadeia C em $\mathcal{G}^c$ possuirá uma cota superior em $\mathcal{F}^c$ (pois $\mathcal{G}^c \subseteq \mathcal{F}^c$), digamos I; se K é algum elemento de C então $K \supseteq J$, logo $I \supseteq K \supseteq J$ e assim $I \in \mathcal{G}^c$. Finalmente, se $\mathfrak{p}$ é maximal em $\mathcal{G}^c$ e $I \in \mathcal{F}^c$ satisfaz $I \supseteq \mathfrak{p}$, então $I \supseteq J$ (pois $\mathfrak{p} \supseteq J$), logo $I \in \mathcal{G}^c$ e daí $I = \mathfrak{p}$ pela maximalidade de $\mathfrak{p}$, o que mostra que $\mathfrak{p}$ é maximal em $\mathcal{F}^c$. □

Observação 1.26. Se J é um ideal em A disjunto de um conjunto multiplicativo S então, com a notação da prova do item *a*) da Proposição 1.21, teremos $\mathcal{F}_S^c \neq \emptyset$, logo pelo Lema anterior (e com sua notação) $\mathcal{G}^c$ possuirá, pelo lema de Zorn, um membro maximal, o qual será um ideal primo (pela Proposição 1.19) disjunto de S contendo J.

Como caso particular, se $S = \{1\}$ então $\mathcal{F}_S^c$ é justamente o conjunto dos ideais que não possuem o elemento 1, isto é, os ideais próprios do anel A. Ainda, seus membros maximais são justamente os ideais maximais no sentido clássico da definição, e estes serão primos ♣.

Proposição 1.27. *O radical de um ideal J é a interseção dos primos contendo J.*

Demonstração. Se $a \in \mathrm{Rad}(J)$ então $a^n \in J$ para algum $n > 0$, logo para qualquer primo $\mathfrak{p}$ contendo J teremos $a^n \in \mathfrak{p}$, e assim $a \in \mathfrak{p}$. Reciprocamente, se $a \notin \mathrm{Rad}(J)$ então o conjunto multiplicativo $S_a = \{a^n : n \geq 0\}$ (vide o Exemplo 1.4, ii)) satisfaz $S_a \cap J = \emptyset$, logo pela Observação 1.26 existe um ideal primo $\mathfrak{p}$ disjunto de S_a com $\mathfrak{p} \supseteq J$, e em particular $a \notin \mathfrak{p}$. □

No capítulo seguinte será discutida a situação em que $\mathrm{Rad}(I)$ é um ideal primo, logo nosso objetivo agora é caracterizar esta situação.

De maneira geral, seja A um conjunto e seja $\mathcal{F}$ uma família de subconjuntos de A. Denotamos a interseção $\cap_{I \in \mathcal{F}} I$ por $\cap\mathcal{F}$ (o que certamente resolve a redundância da notação original). Gostaríamos de expressar $\cap\mathcal{F}$ usando menos elementos de $\mathcal{F}$, ou seja, queremos achar $\mathcal{G} \subseteq \mathcal{F}$ "interessante" tal que $\cap\mathcal{F} = \cap\mathcal{G}$. Ora, se $I \in \mathcal{F}$ não é minimal com respeito da inclusão, então existe $J \in \mathcal{F}$ tal que $J \subsetneq I$, e neste caso podemos tomar $\mathcal{G} = \mathcal{F} \setminus \{I\}$. Em outras palavras, podemos omitir o elemento não minimal I da família $\mathcal{F}$.

Isto sugere que podemos "retirar" todos os elementos não minimais de $\mathcal{F}$. Seja então $\mathcal{M}$ a subfamília de elementos minimais de $\mathcal{F}$ (com respeito da inclusão, é claro). Pela observação anterior parece ser verdade a igualdade $\cap\mathcal{F} = \cap\mathcal{M}$. Mas isto é falso: por exemplo se A é um conjunto infinito e $\mathcal{F}$ é a família dos subconjuntos cofinitos de A (ou seja, os subconjuntos I de A tais que $A \setminus I$ é finito), então *nenhum* elemento de $\mathcal{F}$ é minimal, e portanto neste caso teremos $\cap\mathcal{F} = \emptyset$, enquanto $\cap\mathcal{M} = \cap\emptyset = A$ ‖.

♣ Lembramos que o argumento usual para demonstrar que um ideal maximal $\mathfrak{m}$ é primo é o seguinte: $\mathfrak{m}$ é maximal $\Leftrightarrow A/\mathfrak{m}$ é corpo $\Rightarrow A/\mathfrak{m}$ é domínio $\Leftrightarrow \mathfrak{m}$ é primo.

‖ Convidamos o leitor a aplicar as definições básicas da teoria dos conjuntos para provar estas igualdades.

Qual é então o problema no nosso raciocínio? Se $I \in \mathcal{F}$ não é minimal, digamos $J \subsetneq I$ com $J \in \mathcal{F}$, o que pode ocorrer é que ao retirarmos *simultaneamente* todos os elementos minimais também retiremos o elemento J. Uma tentativa de solução então é exigir que exista algum J que não seja "retirado", ou seja, impor a hipótese de que cada $I \in \mathcal{F}$ contenha um elemento minimal de $\mathcal{F}$. Com este ajuste a redução pode ser feita:

Proposição 1.28. *Dado um conjunto A, sejam $\mathcal{F}$ uma família de subconjuntos de A, e denotemos a subfamília dos elementos minimais de $\mathcal{F}$ (com respeito à inclusão) por $\mathcal{M}$. Se cada $I \in \mathcal{F}$ contém um elemento $J \in \mathcal{M}$, então vale $\cap\mathcal{F} = \cap\mathcal{M}$. Ainda, $\cap\mathcal{F} \in \mathcal{F}$ se, e somente se, $\mathcal{F}$ possui um único elemento minimal, a saber, $\cap\mathcal{F}$.*

Demonstração. Obviamente $\cap\mathcal{F} \subseteq \cap\mathcal{M}$. Se $a \in \cap\mathcal{M}$, seja $I \in \mathcal{F}$ qualquer. Então existe $J \in \mathcal{M}$ tal que $J \subseteq I$, logo teremos $a \in J \subseteq I$, e assim $a \in I$, o que mostra a inclusão contrária.

Se $\mathcal{F}$ possui um único elemento minimal, digamos $\mathcal{M} = \{J\}$, então $\cap\mathcal{F} = J \in \mathcal{F}$. Reciprocamente, se $\cap\mathcal{F} = J \in \mathcal{F}$, então $J \subseteq I$ para cada $I \in \mathcal{M}$, logo pela minimalidade de I teremos $J = I$, o que mostra que $\mathcal{M} = \{J\}$. □

Definição 1.29. Seja I um ideal em um anel A. Um ideal primo $\mathfrak{p}$ é dito **minimal sobre *I*** se ele for minimal na família $\{\mathfrak{q} \in \operatorname{Spec}(A) : \mathfrak{q} \supseteq I\}$. Quando $I = 0$, falamos simplesmente de **primo minimal**.

Proposição 1.30. *Seja I um ideal de um anel A. Cada primo $\mathfrak{q}$ contendo I contém um primo minimal sobre I. Em particular $\operatorname{Rad}(I)$ é a interseção dos primos minimais sobre I, e $\operatorname{Rad}(I)$ é primo precisamente quando existir exatamente um primo minimal sobre I, em cujo caso será justamente $\operatorname{Rad}(I)$.*

Demonstração. Seja $\mathcal{H} = \{\mathfrak{p} \in \operatorname{Spec}(A) : \mathfrak{q} \supseteq \mathfrak{p} \supseteq I\}$. Temos $\mathfrak{q} \in \mathcal{H}$, e se $\mathcal{C}$ é uma cadeia (não vazia) em $\mathcal{H}$, então certamente $\cap\mathcal{C}$ é um ideal próprio contendo I. Ainda, se $a, b \in A \setminus \cap\mathcal{C}$, então existem $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathcal{C}$ tais que $a \notin \mathfrak{p}_1, b \notin \mathfrak{p}_2$. Como $\mathcal{C}$ é uma cadeia então temos, digamos $\mathfrak{p}_1 \subseteq \mathfrak{p}_2$, logo $a, b \notin \mathfrak{p}_1$, o que implica $ab \notin \mathfrak{p}_1$. Isto mostra que $ab \notin \cap\mathcal{C}$. Portanto $\mathcal{H}$ satisfaz as hipóteses do lema de Zorn, e o primeiro resultado segue. As outras afirmações decorrem então da primeira junto com a Proposição 1.28. □

Proposição 1.31. *Sejam A um anel noetheriano e M um A-módulo não nulo. Então M possui ao menos um primo associado. De fato, todo ideal M-anulador está contido em algum primo associado maximal de M.*

Demonstração. Seja $J = \operatorname{Ann}(m)$ com $m \in M \setminus 0$, e seja $\mathcal{F}$ a família dos ideais não M-anuladores. Se $\mathbb{J} = \{I : I \text{ ideal}, I \not\supseteq J\}$, então pela Proposição 1.21, d) e o Lema 1.25 temos que $\mathcal{G} = \mathcal{F} \cup \mathbb{J}$ é uma família de Oka. Ainda, $\mathcal{G}^c \neq \emptyset$ pois $J \in \mathcal{G}^c$, logo $\mathcal{G}^c$ vai

possuir pelo menos um elemento maximal (por A ser noetheriano) e pela Proposição 1.19 tal elemento será primo, portanto primo associado maximal de M contendo J. □

Proposição 1.32. *Se A é um anel noetheriano e $M \neq 0$ é um A-módulo finitamente gerado, então $\mathcal{Z}_A(M)$ é uma união finita de primos associados maximais de M. Isto vale em particular para $M = A$.*

Demonstração. A segunda afirmação decorre da primeira pelo fato de A ser finitamente gerado como A-módulo. Ora, seja M um A-módulo finitamente gerado. Sejam $\mathcal{F}$ a família dos ideais não M-anuladores em A e $\mathcal{H}$ a família dos ideais maximais em $\mathcal{F}^c$ (isto é, dos primos associados maximais de M). Cada $\mathfrak{p} \in \mathcal{H}$ é da forma $\mathrm{Ann}(m_\mathfrak{p})$, com $m_\mathfrak{p} \in M \setminus 0$. Considere o submódulo $N = \langle m_\mathfrak{p} : \mathfrak{p} \in \mathcal{H} \rangle$. Como M é noetheriano (pela Proposição 1.10), então pela condição c) da Proposição 1.5 existem $\mathfrak{p}_1 \ldots, \mathfrak{p}_k \in \mathcal{H}$ tais que $N = \langle m_{\mathfrak{p}_1}, \ldots, m_{\mathfrak{p}_k} \rangle$. Se $\mathfrak{p} \in \mathcal{H}$ então

$$\begin{aligned}
\mathfrak{p} &= \mathrm{Ann}(m_\mathfrak{p}) \\
&\supseteq \mathrm{Ann}(N) \quad (\text{pois } m_\mathfrak{p} \in N) \\
&= \mathrm{Ann}\big(\langle m_{\mathfrak{p}_1}, \ldots, m_{\mathfrak{p}_k} \rangle\big) \\
&= \bigcap_{i=1}^{k} \mathrm{Ann}(m_{\mathfrak{p}_i}) \\
&= \bigcap_{i=1}^{k} \mathfrak{p}_i \,,
\end{aligned}$$

logo $\mathfrak{p} \supseteq \mathfrak{p}_j$ para algum j (pois $\mathfrak{p}$ é primo); como $\mathfrak{p} \in \mathcal{F}^c$ e $\mathfrak{p}_j$ é maximal em $\mathcal{F}^c$, segue que $\mathfrak{p} = \mathfrak{p}_j$. Isto prova que $\mathcal{H} = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_k\}$. Finalmente, cada ideal M-anulador está contido em algum membro de $\mathcal{H}$ pela Proposição anterior, logo teremos $\bigcup_{m \in M \setminus 0} \mathrm{Ann}(m) = \bigcup_{\mathfrak{p} \in \mathcal{H}} \mathfrak{p}$ (esta igualdade é o análogo para uniões da Proposição 1.28), isto é, $\mathcal{Z}_A(M) = \bigcup_{i=1}^{k} \mathfrak{p}_i$. □

Corolário 1.33. *Seja A um anel noetheriano.*

a) Um ideal I em A é regular se, e somente se, $(0 : I) = 0$. Em particular, se J e I são ideais em A tais que $I \subseteq J$, então $I = (I : J) \Leftrightarrow$ o ideal J/I possui um elemento regular.

b) Se I for um ideal primo em A e $I \subsetneq J$ então $I = (I : J)$.

c) Se I, J são ideais em A tais que I é ideal próprio e $J \subseteq \mathcal{Z}_A(A/I)$, então $I \subsetneq (I : J)$. Em particular vale $I \subsetneq \big(I : \mathrm{Rad}(I)\big)$.

Demonstração.

a) A segunda equivalência segue da primeira por conta da igualdade $(I : J)/I = \big(0 : J/I\big)$. Se I é regular, então existe um elemento $x \in I$ regular, logo para todo $a \in A \setminus 0$ temos $ax \neq 0$, portanto $aI \neq 0$ e assim $(0 : I) = 0$ (note que não usamos a hipótese de A ser noetheriano). Por outro lado, se A é noetheriano e I não é regular, então $I \subseteq \mathcal{Z}(A) = \bigcup_{i=1}^{k} \mathfrak{p}_i$, com $\mathfrak{p}_i \in \mathrm{Ass}(A)$, pela Proposição anterior. Por evasão de primos (ALTMAN; KLEIMAN, 2013, Lemma 3.19) teremos $I \subseteq \mathfrak{p}_j$ para algum j; porém $\mathfrak{p}_j = \mathrm{Ann}(y)$ para algum $y \in A \setminus 0$, portanto $y \in (0 : I) \setminus 0$.

b) Neste caso A/I é um domínio, logo qualquer elemento não nulo de J/I será regular. Agora aplicamos o item anterior.

c) Neste caso todo elemento de J/I é divisor de zero no anel A/I, logo J/I não será ideal regular. Ainda, lembramos que $\mathrm{Rad}(I) \subseteq \mathcal{Z}_A(A/I)$. □

Proposição 1.34. *Sejam A um anel noetheriano, I um ideal de A e $J = \bigcup_{n\in\mathbb{N}} (0 : I^n)$. Dada uma decomposição primária $0 = \bigcap_{i=1}^{n} \mathfrak{q}_i$, com cada $\mathfrak{q}_i$ sendo $\mathfrak{p}_i$-primário, seja $\mathcal{G} = \{i : \mathfrak{p}_i \not\supseteq I\}$. Então $J = \bigcap_{i\in\mathcal{G}} \mathfrak{q}_i$.*

Demonstração. Seja $x \in J$, digamos $xI^n = 0$. Dado $i \in \mathcal{G}$, seja $z \in I \setminus \mathfrak{p}_i$ fixado (o qual existe pela hipótese sobre i). Então $z^n x = 0$ (pois $z^n \in I^n$), logo $z^n x \in \mathfrak{q}_i$. Como $z^n \notin \mathfrak{p}_i = \mathrm{Rad}(\mathfrak{q}_i)$ e $\mathfrak{q}_i$ é primário, concluímos que vale $x \in \mathfrak{q}_i$.

Reciprocamente, dado $x \in \bigcap_{i\in\mathcal{G}} \mathfrak{q}_i$, certamente teremos $xI^m \subseteq \mathfrak{q}_i$ para cada $i \in \mathcal{G}$ e para qualquer $m \in \mathbb{N}$ (pois $x \in \mathfrak{q}_i$); por outro lado, se $j \notin \mathcal{G}$ então $I \subseteq \mathfrak{p}_j = \mathrm{Rad}(\mathfrak{q}_j)$, logo existe $k_j \geq 1$ tal que $I^{k_j} \subseteq \mathfrak{q}_j$ [**], e consequentemente $xI^{k_j} \in \mathfrak{q}_j$. Tomando k como o máximo dos k_j teremos $xI^k \in \mathfrak{q}_j$ para todo j (esteja ou não tal j em $\mathcal{G}$), e assim $xI^k \in \bigcap_{i=1}^{n} \mathfrak{q}_i = 0$, provando que $x \in (0 : I^k) \subseteq J$. □

1.4 Idealizações de módulos e envelopes injetivos

Nesta seção serão apresentadas certas noções, as quais serão utilizadas na construção de um contraexemplo no próximo capítulo (vide o Exemplo 2.21). A principal noção aqui apresentada será a de **idealização** que tem muitas propriedades analisadas em (ANDERSON; WINDERS, 2009).

Definição 1.35. Sejam A um anel e M um A-módulo. Considere o conjunto $A(+)M = A \oplus M$ com soma e produto dados por $(a_1, m_1) + (a_2, m_2) = (a_1 + a_2, m_1 + m_2)$ e

[**] De fato, seja D um conjunto finito de geradores de I; existe então um inteiro positivo k tal que $d^k \in \mathfrak{q}_j$ para todo $d \in D$ (pois $I \subseteq \mathrm{Rad}(\mathfrak{q}_j)$). É fácil ver que I^m é gerado pelos produtos de m elementos (não necessariamente distintos) de D. Se $m = |D|(k-1)+1$ então em cada um destes produtos deve aparecer, forçosamente, um fator d^ℓ com $\ell \geq k$, e assim tal produto está em $\mathfrak{q}_j$.

$(a_1, m_1) \cdot (a_2, m_2) = (a_1a_2, a_1m_2 + a_2m_1)$. Com estas operações $A(+)M$ vira um anel comutativo com unidade (a unidade sendo o elemento $(1, 0)$), o qual é chamado de **idealização de M**.

Proposição 1.36. *Sejam I um ideal de A e N um submódulo de M. Então $I(+)N$ é um ideal de $A(+)M$ se e somente se vale $IM \subseteq N$; notando que esta condição implica que M/N é um A/I-módulo, com a multiplicação escalar dada por $(a + I)(m + N) = am + N$. Sob esta hipótese, as idealizações $\dfrac{A(+)M}{I(+)N}$ e $\dfrac{A}{I}(+)\dfrac{M}{N}$ são anéis isomorfos.*

Demonstração. Se $I(+)N$ é um ideal de $A(+)M$, então $I(+)N = \big[I(+)N\big] \cdot \big[A(+)M\big] = I(+)(IM + N)$, logo $IM + N = N$ e assim $IM \subseteq N$. Reciprocamente, se $IM \subseteq N$ então (como mencionado no enunciado da Proposição) M/N é um A/I-módulo via $(a + I)(m + N) = am + N$. Seja

$$\begin{aligned} \phi : A(+)M &\longrightarrow \frac{A}{I}(+)\frac{M}{N} \\ (a, m) &\longmapsto (a + I\,,\ m + N)\,. \end{aligned}$$

Então

$$\begin{aligned} \phi[(a_1, m_1) + (a_2, m_2)] &= \phi(a_1 + a_2, m_1 + m_2) \\ &= \big((a_1 + a_2) + I, (m_1 + m_2) + N\big) \\ &= (a_1 + I, m_1 + N) + (a_2 + I, m_2 + N) \\ &= \phi(a_1, m_1) + \phi(a_2, m_2)\,; \\ \phi\big[(a_1, m_1) \cdot (a_2, m_2)\big] &= \phi(a_1a_2, a_1m_2 + a_2m_1) \\ &= \big(a_1a_2 + I, (a_1m_2 + a_2m_1) + N\big) \\ &= (a_1 + I, m_1 + N) \cdot (a_2 + I, m_2 + N) \\ &= \phi(a_1, m_1) \cdot \phi(a_2, m_2)\,; \\ \phi(1_A, 0_M) &= (1 + I, 0 + N) \\ &= (1_{A/I}, 0_{M/N})\,. \end{aligned}$$

Isto prova que ϕ é um homomorfismo de anéis. Ora, ϕ é sobrejetivo e $\phi(a, m) = (0, 0)$ se, e somente se, $a \in I$ e $m \in N$, logo $I(+)N = \mathrm{Ker}(\phi)$ é um ideal em $A(+)M$. Finalmente, pelo teorema do isomorfismo teremos $\dfrac{A(+)M}{I(+)N} \simeq \dfrac{A}{I}(+)\dfrac{M}{N}$. □

Note que o resultado anterior não descreve todos os ideais de $A(+)M$, mas apenas aqueles que são produto cartesiano de um ideal e de um submódulo; contudo, provaremos a seguir que certos ideais são necessariamente desta forma:

Lema 1.37. *Os ideais de $A(+)M$ contendo $0(+)M$ são da forma $I(+)M$ para algum ideal $I \subseteq A$, e vale $\dfrac{A(+)M}{I(+)M} \simeq \dfrac{A}{I}$. Em particular $I(+)M$ é primo se e somente se I o for.*

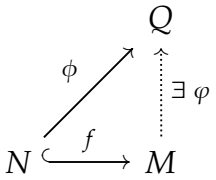
Demonstração. A projeção $\pi : A(+)M \to A$ é um homomorfismo sobrejetivo de anéis, e $(a, m) \in \mathrm{Ker}(\pi) \Leftrightarrow a = 0$, logo $\mathrm{Ker}(\pi) = 0(+)M$. Pelo teorema de correspondência, os ideais em $A(+)M$ contendo $0(+)M$ serão precisamente os da forma $\pi^{-1}(I)$, para algum ideal I em A. Como $\pi^{-1}(I) = I(+)M$, o primeiro resultado segue.

Note que π é isomorfismo se $M = 0$, ou seja $A(+)0 \simeq A$, e portanto $\dfrac{A}{I} \simeq \dfrac{A}{I}(+)\,0 \simeq \dfrac{A(+)M}{I(+)M}$ pela Proposição anterior. A última afirmação é evidente. □

Proposição 1.38. *Os ideais primos de $A(+)M$ são precisamente os da forma $\mathfrak{p}(+)M$, com $\mathfrak{p} \in \mathrm{Spec}(A)$. Ainda, $\mathfrak{p}(+)M$ será primo minimal se, e somente se, $\mathfrak{p}$ for primo minimal em A. Em particular $\mathrm{Rad}(0_{A(+)M}) \in \mathrm{Spec}\big(A(+)M\big) \Leftrightarrow \mathrm{Rad}(0_A) \in \mathrm{Spec}(A)$.*

Demonstração. Seja $\mathfrak{q} \subseteq A(+)M$ um ideal primo. Observamos que $(0, m)(0, n) = 0$ para todos $m, n \in M$, portanto $\big(0(+)M\big)^2 = 0 \subseteq \mathfrak{q}$ e assim $0(+)M \subseteq \mathfrak{q}$. Pelo Lema anterior existe um ideal primo $\mathfrak{p} \subseteq A$ tal que $\mathfrak{q} = \mathfrak{p}(+)M$. O recíproco decorre do mesmo Lema, e a afirmação sobre primos minimais segue da equivalência $I(+)M \supseteq J(+)M \Leftrightarrow I \supseteq J$. Finalmente, a equivalência da primalidade de radicais segue da afirmação anterior junto com a Proposição 1.30. □

Definição 1.39. Um A-módulo Q é dito **injetivo** se, dado um homomorfismo injetivo $f : N \to M$ e qualquer homomorfismo $\phi : N \to Q$, então existe um homomorfismo $\varphi : M \to Q$ tal que $\phi = \varphi \circ f$.



Definição 1.40. Sejam E um A-módulo e $M \subseteq E$ um submódulo. Dizemos que E é **extensão essencial de M** se todo submódulo não-nulo $N \subseteq E$ cumpre $N \cap M \neq 0$. Se E é ademais um A-módulo injetivo, dizemos que E é um **envelope injetivo de M**.

Teorema 1.41. *Todo A-módulo M admite um envelope injetivo.*

Demonstração. Vide (EISENBUD, 1995, Proposition-Definition A3.10).

1.5 Anéis e módulos de frações

Sejam A um anel e S um subconjunto multiplicativo de A. Definimos em $A \times S$ a relação $(a, s) \sim (b, r)$ se, e somente se, existe $t \in S$ de maneira que $t(ar - bs) = 0$. Esta

relação é de equivalência e representaremos suas classes de maneira canônica, ou seja, $\big[(a,s)\big] = a/s$. Definimos a soma e multiplicação destas classes por

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}\,; \quad \frac{a}{s}\cdot\frac{b}{t} = \frac{ab}{st}\,.$$

É um exercício simples verificar que as operações estão bem definidas. O conjunto dessas classes forma, com estas operações, um anel que é chamado de **anel de frações** (ou **localização**) de A em relação a S, o qual denotaremos por A_S. Em termos simples a ideia é construir um anel onde os elementos de S sejam invertíveis. Quando $S = A \setminus \mathfrak{p}$, com $\mathfrak{p} \in \operatorname{Spec}(A)$ (vide o Exemplo 1.4, iii)), denotaremos o conjunto A_S por $A_{\mathfrak{p}}$.

De maneira similar ao que foi feito para se construir o anel de frações, podemos construir, a partir de um A-módulo M, o **módulo de frações** M_S, que será conjunto das frações m/s tais que $m \in M$ e $s \in S \subseteq A$, e a igualdade de frações sendo definida de maneira análoga ao caso anterior. Segue que M_S é um A_S-módulo com as operações de soma e de múltiplo por escalar naturalmente definidas.

A aplicação $\phi_S : M \to M_S$ dada por $\phi_S(m) = m/1$ é A-linear, onde M_S é considerado A-módulo por restrição de escalares. Se $M = A$, então a aplicação é de fato um homomorfismo de anéis.

Dado outro A-módulo N e uma aplicação A-linear $f : M \to N$, então $f_S : M_S \to N_S$ dada por $f_S(m/s) = f(m)/s$, é bem definida, e será uma aplicação A_S-linear. Ainda, se P é outro A-módulo e $g : N \to P$ é A-linear, então claramente vale $(g \circ f)_S = g_S \circ f_S : M_S \to P_S$.

Definição 1.42. Seja $X \subseteq M$. A ***S*-extensão** de X é o A_S-submódulo em M_S gerado por $\phi_S(X)$, a qual será denotada por X_S. A ***S*-saturação** de X é o conjunto $X^S = \phi_S^{-1}(X_S)$. Note que sempre vale $X \subseteq X^S$. Quando ocorrer $X = X^S$ dizemos que X é ***S*-saturado**.

Observação 1.43. Se X é um A-submódulo de M, então a notação X_S é ambígua, uma vez que X_S também denotará o A_S-módulo de frações de X; esta ambiguidade será resolvida na Proposição 1.48, e por isto **não** introduziremos uma notação adicional para diferenciar as duas situações. Também observamos que as operações de extensão e saturação são claramente monótonas, ou seja, se $X \subseteq Y \subseteq M$, então valem $X_S \subseteq Y_S$ e $X^S \subseteq Y^S$.

Lema 1.44. *Sejam N um A-submódulo de M e P um A_S-submódulo de M_S.*

a) Se $L = \phi_S^{-1}(P)$, então para todos $m \in M$ e $s \in S$ vale $m/s \in P \Leftrightarrow m \in L$, e $P = \{m/s : m \in L\,, s \in S\} = L_S$; ainda, L é S-saturado.

b) Para todos $m \in M$ e $s \in S$ vale $m/s \in N_S \Leftrightarrow m \in N^S$; ainda, N^S é S-saturado, $N_S = \{m/s : m \in N^S, s \in S\}$ e $(N^S)_S = N_S$.

c) *Para todos $m \in M$ e $s \in S$ vale $m/s \in N_S \Leftrightarrow um \in N$ para algum $u \in S$; em particular $N^S = \{m \in M : um \in N \text{ para algum } u \in S\}$. Ainda, vale a igualdade $N_S = \{n/s : n \in N, s \in S\}$.*

Demonstração.

a) Para todos $m \in M$ e $s \in S$ vale $\frac{m}{s} \in P \Leftrightarrow \frac{m}{1} \in P$ (pois $\frac{s}{1} \in A_S^*$), o que prova a primeira equivalência e a igualdade $P = \{m/s : m \in L, s \in S\}$. Como $\phi_S(L) \subseteq P$ então $L_S = \langle \phi_S(L) \rangle \subseteq P$; reciprocamente, se $\frac{m}{s} \in P$ então $m \in L$, logo $\frac{m}{s} = \frac{1}{s}\phi_S(m) \in \langle \phi_S(L) \rangle = L_S$. Assim $P = L_S$, logo $L^S = \phi_S^{-1}(L_S) = \phi_S^{-1}(P) = L$, isto é, L é S-saturado.

b) Segue do item anterior tomando $P = N_S$, pois neste caso $L = \phi_S^{-1}(N_S) = N^S$.

c) Se $\frac{m}{s} \in N_S = \langle \phi_S(N) \rangle$ então $\frac{m}{s} = \sum_{i=1}^k \frac{a_i}{t_i}\frac{n_i}{1}$, com $a_i \in A, t_i \in S$ e $n_i \in N$ para cada i. Se $t = \prod_{i=1}^k t_i$ então $t \in S$ e $t = b_i t_i$ com $b_i \in S$, logo $\frac{m}{s} = \frac{n}{t}$, sendo $n = \sum_{i=1}^k a_i b_i n_i \in N$. Portanto existe $w \in S$ tal que $wtm = wsn \in N$, e assim $um \in N$ com $u = wt \in S$. Reciprocamente, se $um \in N$ para algum $u \in S$, então $\frac{m}{s} = \frac{1}{su}\phi_S(um) \in \langle \phi_S(N) \rangle = N_S$.

Disto junto com o item anterior obtemos que para todo $m \in M$ vale $m \in N^S \Leftrightarrow m/1 \in N_S \Leftrightarrow um \in N$ para algum $u \in S$, provando a primeira igualdade de conjuntos. Como $N \subseteq N^S$ então $\{n/s : n \in N, s \in S\} \subseteq N_S$ pelo item anterior; reciprocamente, se $\frac{m}{s} \in N_S$ então $m \in N^S$, logo $um = n \in N$ para algum $u \in S$, e portanto $\frac{m}{s} = \frac{n}{su}$, o que prova a segunda igualdade de conjuntos. □

Proposição 1.45. *Sejam A um anel, S um subconjunto multiplicativo de A, e M um A-módulo.*

a) *Existe uma bijeção entre a família dos A_S-submódulos de M_S e a família dos A-submódulos S-saturados de M, dada por $N \mapsto N_S; P \mapsto \phi_S^{-1}(P)$ (para $N < M, P < M_S$). Ainda, estas correspondências preservam inclusões.*

b) *Se I é um ideal primário em A com $\mathrm{Rad}(I) \cap S = \emptyset$, então I é S-saturado.*

c) *O conjunto $\mathrm{Spec}(A_S)$ está em bijeção com o conjunto dos ideais primos em A disjuntos de S, via a correspondência do item a).*

d) *Dado $\mathfrak{p} \in \mathrm{Spec}(A)$, o conjunto $\mathrm{Spec}(A_\mathfrak{p})$ está em bijeção com o conjunto $\{\mathfrak{q} \in \mathrm{Spec}(A) : \mathfrak{q} \subseteq \mathfrak{p}\}$, via a correspondência do item a).*

Demonstração.

a) Se N é A-submódulo de M então $N^S = \phi_S^{-1}(N_S)$ **por definição**, logo se N é S-saturado teremos $N = \phi_S^{-1}(N_S)$. Também, se P é A_S-submódulo de M_S, então pelo item *a*) do Lema anterior temos $P = \left(\phi_S^{-1}(P)\right)_S$, com $\phi_S^{-1}(P)$ sendo S-saturado. Como estas correspondências são dadas por imagens inversas e submódulos gerados por imagens diretas, segue que elas respeitam inclusões.

b) Já temos $I \subseteq I^S$, e se $a \in I^S$, então existe $s \in S$ tal que $as \in I$; já que I é primário e $s \notin \mathrm{Rad}(I)$ (pois $\mathrm{Rad}(I) \cap S = \emptyset$), concluímos que vale $a \in I$.

c) Se $\mathfrak{q} \in \mathrm{Spec}(A_S)$ então $\phi_S^{-1}(\mathfrak{q}) = \mathfrak{p} \in \mathrm{Spec}(A)$ (pois ϕ_S é homomorfismo de anéis), e $\mathfrak{p}$ é S-saturado pelo item *a*). Como $1 \notin \mathfrak{p} = \mathfrak{p}^S$, então para todo $s \in S$ vale $s = s \cdot 1 \notin \mathfrak{p}$, logo $\mathfrak{p} \cap S = \emptyset$. Reciprocamente, se $\mathfrak{p} \in \mathrm{Spec}(A)$ satisfaz $\mathfrak{p} \cap S = \emptyset$, então $\mathfrak{p}$ é S-saturado pelo item anterior; como $1 \in S$ então $1 \notin \mathfrak{p} = \mathfrak{p}^S$, logo $\frac{1}{1} \notin \mathfrak{p}_S$ pelo item *b*) do Lema anterior. Similarmente, se $a, b \in A$ e $s, t \in S$ satisfazem $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} \in \mathfrak{p}_S$, então pelo mesmo item temos $ab \in \mathfrak{p}^S = \mathfrak{p}$, logo $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$, e assim $\frac{a}{s} \in \mathfrak{p}_S$ ou $\frac{b}{t} \in \mathfrak{p}_S$, o que mostra que $\mathfrak{p}_S \in \mathrm{Spec}(A_S)$.

d) Imediato a partir do item anterior, tomando $S = A \setminus \mathfrak{p}$. □

Exemplo 1.46. A hipótese de I ser primário do item *b*) da Proposição anterior não pode ser removida. Considere A um domínio fatorial e p, q primos distintos, logo $\langle p \rangle$ e $\langle q \rangle$ são comaximais. É simples notar que $I = \langle pq \rangle$ não é primário, além disso $\mathrm{Rad}(I) = I$ e $S = 1 + \langle q \rangle$ cumpre $S \cap I = \emptyset$, entretanto $q \in I^S \setminus I$, pois como $\langle p \rangle + \langle q \rangle = A$ existem r, s tais que $pr + qs = 1$, logo $pr = 1 - qs$ e assim $qpr = q(1 - qs) \in I$.

Proposição 1.47. *Se a sequência de A-módulos $N \xrightarrow{f} M \xrightarrow{g} P$ é exata em M, então a sequência de A_S-módulos $N_S \xrightarrow{f_S} M_S \xrightarrow{g_S} P_S$ é exata em M_S.*

Demonstração. Como $\mathrm{Im}(f) = \mathrm{Ker}(g)$ então $g \circ f = 0$, logo $g_S \circ f_S = (g \circ f)_S = 0$, e assim $\mathrm{Im}(f_S) \subseteq \mathrm{Ker}(g_S)$. Reciprocamente, se $\frac{m}{s} \in \mathrm{Ker}(g_S)$ então $\frac{g(m)}{s} = \frac{0}{1}$, e portanto existe $t \in S$ cumprindo $tg(m) = 0$, o que nos dá $tm \in \mathrm{Ker}(g) = \mathrm{Im}(f)$, e por isto existe $n \in N$ de maneira que $tm = f(n)$, logo $\frac{m}{s} = \frac{f(n)}{st} = f_S\left(\frac{n}{st}\right) \in \mathrm{Im}(f_S)$, provando a inclusão contrária. □

Proposição 1.48. *Sejam M um A-módulo, S um subconjunto multiplicativo de A, e J um ideal em A. Então para quaisquer A-submódulos $(N_i)_{i \in I}, N, P$ tem-se:*

a) $\left(\sum_{i \in I} N_i\right)_S = \sum_{i \in i} (N_i)_S$.

b) $N_S \cap P_S = (N \cap P)_S$; $N^S \cap P^S = (N \cap P)^S$.

c) $\mathrm{Rad}(J)^S = \mathrm{Rad}(J^S)$; *em particular para quaisquer $a \in A, s \in S$ vale $a/s \in \mathrm{Rad}(J)_S \Leftrightarrow a \in \mathrm{Rad}(J^S)$, e* $\mathrm{Rad}(J_S) = \mathrm{Rad}(J)_S$.

d) O A_S-módulo N_S é isomorfo ao A_S-submódulo $\{n/s \in M_S : n \in N, s \in S\}$ de M_S, o qual também é denotado por N_S (vide a Observação 1.43). Ainda, vale $M_S/N_S \simeq (M/N)_S$ como A_S-módulos.

Demonstração.

a) Para cada $\ell \in I$ temos $N_\ell \subseteq \sum_{i\in I} N_i$, o que implica $(N_\ell)_S \subseteq \left(\sum_{i\in I} N_i\right)_S$, e assim $\sum_{i\in I}(N_i)_S \subseteq \left(\sum_{i\in I} N_i\right)_S$. Reciprocamente, se $z \in \left(\sum_{i\in I} N_i\right)_S$ então $z = \frac{m}{s}$, com $m \in \sum_{i\in I} N_i$ (pelo Lema 1.44, *c*)), digamos $m = \sum_{r=1}^{k} n_r$ para alguns $i_1, \ldots, i_k \in I$ com $n_r \in N_{i_r}$, logo $\frac{n_r}{s} \in (N_{i_r})_S$ (de novo pelo Lema 1.44, *c*)). Portanto $z = \sum_{r=1}^{k} \frac{n_r}{s} \in \sum_{i\in I}(N_i)_S$.

b) Como imagem inversa de função (neste caso a função ϕ_S) preserva interseções arbitrárias, a segunda igualdade decorre da primeira. Se $x \in N_S \cap P_S$ então $x = \frac{n}{t} = \frac{p}{u}$ com $n \in N, p \in P$ e $t, s \in S$. Logo existe $v \in S$ tal que $vun = vtp \in N \cap P$ e desse modo $x = \frac{uvn}{tuv} \in (N \cap P)_S$, pelo Lema 1.44, *c*). A outra inclusão é obvia pois $N \cap P \subseteq N, P$, logo $(N \cap P)_S \subseteq N_S \cap P_S$.

c) Afirmamos que para todo $a \in A$ e todo $n \geq 1$, vale

$$(\exists u \in S)[ua^n \in J] \Leftrightarrow (\exists s \in S)[(sa)^n \in J]\,.$$

Com efeito, a implicação direta vale tomando $s = u$, enquanto a reciproca vale tomando $u = s^n$. Consequentemente temos $\mathrm{Rad}(J^S) = \mathrm{Rad}(J)^S$.

Se $a \in M$ e $s \in S$, então pelo anterior junto com o Lema 1.44, *b*) vale $\frac{a}{s} \in \mathrm{Rad}(J)_S \Leftrightarrow a \in \mathrm{Rad}(J)^S = \mathrm{Rad}(J^S)$, e se $L = \phi_S^{-1}\left(\mathrm{Rad}(J_S)\right)$ então pelo Lema 1.44, *a*) teremos $\mathrm{Rad}(J_S) = L_S$; já que imagem inversa de homomorfismo de anel comuta com radical então $L = \mathrm{Rad}\left(\phi_S^{-1}(J_S)\right) = \mathrm{Rad}(J^S) = \mathrm{Rad}(J)^S$, logo

$$\mathrm{Rad}(J_S) = L_S = \left(\mathrm{Rad}(J)^S\right)_S = \mathrm{Rad}(J)_S\,,$$

pelo Lema 1.44, *b*).

d) A sequência $0 \to N \xrightarrow{i} M \xrightarrow{\pi} M/N \longrightarrow 0$ é exata, sendo i a inclusão e π a projeção canônicas. Pela Proposição anterior a sequência $0 \to N_S \xrightarrow{i_S} M_S \xrightarrow{\pi_S} M/N \to 0$ também será exata. Ainda, $i_S(N_S)$ será justamente o conjunto $\left\langle \phi_S(N) \right\rangle$ da Definição 1.42, o qual também foi denotado por N_S (vide a Observação 1.43). Fazendo esta identificação e usando a exatidão da nova sequência obtemos $(M/N)_S \simeq M_S/N_S$. □

Proposição 1.49. *Sejam M um A-módulo finitamente gerado, $S \subseteq A$ um conjunto multiplicativo. Então* $\mathrm{Ann}(M)_S = \mathrm{Ann}(M_S)$.

Demonstração. Se a propriedade vale para dois submódulos N, P de M, então vale para $N + P$, pois

$$\begin{aligned}
\big[\mathrm{Ann}(N+P)\big]_S &= \big[\mathrm{Ann}(N) \cap \mathrm{Ann}(P)\big]_S \\
&= \underbrace{\mathrm{Ann}(N)_S \cap \mathrm{Ann}(P)_S}_{\text{Proposição 1.48, } b)} \\
&= \underbrace{\mathrm{Ann}(N_S) \cap \mathrm{Ann}(P_S)}_{\text{Hipótese}} \\
&= \mathrm{Ann}(N_S + P_S) \\
&= \underbrace{\mathrm{Ann}\big((N+P)_S\big)}_{\text{Proposição 1.48, } a)} .
\end{aligned}$$

Assim, o caso $M = \langle m_1, m_2, \ldots, m_k\rangle = \langle m_1\rangle + \langle m_2\rangle + \cdots \langle m_k\rangle$ segue por indução, o caso base sendo $M = \langle m\rangle$, em cujo caso $M \simeq A/\mathrm{Ann}(M)$ (pelo teorema do isomorfismo, considerando a aplicação $a \in A \mapsto am \in M$); $M_S \simeq \big(A/\mathrm{Ann}(M)\big)_S \simeq A_S/\mathrm{Ann}(M)_S$ pela Proposição 1.48, d), e assim $\mathrm{Ann}(M_S) = \mathrm{Ann}(M)_S$. □

Corolário 1.50. *Sejam N, P submódulos de um A-módulo. Se P é finitamente gerado, então $(N : P)_S = (N_S : P_S)$.*

Demonstração. Temos $(N : P) = \mathrm{Ann}\left(\frac{N+P}{N}\right)$, e $\frac{N+P}{N} \simeq \frac{P}{P\cap N}$, este último sendo finitamente gerado pois P o é. Portanto

$$\begin{aligned}
(N : P)_S &= \left[\mathrm{Ann}\left(\frac{N+P}{N}\right)\right]_S \\
&= \mathrm{Ann}\left(\left(\frac{N+P}{N}\right)_S\right) \quad \text{(pela Proposição anterior)} \\
&= \mathrm{Ann}\left(\frac{N_S + P_S}{N_S}\right) \quad \text{(Proposição 1.48, } a),\ d)) \\
&= (N_S : P_S). \qquad \square
\end{aligned}$$

Definição 1.51. Sejam A um anel e $M \neq 0$ um A-módulo. Um ideal primo $\mathfrak{p}$ em A é dito **fracamente associado de M** se for minimal sobre um ideal M-anulador. O conjunto destes ideais será denotado por $\mathrm{WeakAss}(M)$.

Obviamente temos $\mathrm{Ass}(M) \subseteq \mathrm{WeakAss}(M)$. Foi provado na Proposição 1.32 que se A é noetheriano e M é A-módulo finitamente gerado, então $\mathcal{Z}_A(M)$ é união finita de primos, a saber, primos associados maximais. A demonstração usou fortemente as

hipóteses do anel de escalares ser noetheriano, junto com os resultados de famílias de Oka. No caso geral não será possível repetir este raciocínio; contudo, vale um resultado semelhante:

Proposição 1.52. *Se $M \neq 0$ então $\mathcal{Z}_A(M) = \bigcup \mathrm{WeakAss}(M)$.*

Demonstração. Se I é um ideal M-anulador então I é um ideal próprio, logo pela Proposição 1.30 existe um primo minimal sobre I, o qual será primo associado fraco. Reciprocamente, seja $m \in M \setminus 0$ e seja $\mathfrak{p}$ um primo minimal sobre $I = \mathrm{Ann}(m)$. Afirmamos que, em $A_\mathfrak{p}$, o ideal $\mathfrak{p}_\mathfrak{p}$ é o único primo contendo $I_\mathfrak{p}$. De fato, seja $S = A \setminus \mathfrak{p}$. Todo ideal primo em $A_\mathfrak{p}$ é da forma $\mathfrak{q}_\mathfrak{p}$, onde $\mathfrak{q} \in \mathrm{Spec}(A)$ satisfaz $\mathfrak{q} \subseteq \mathfrak{p}$, pela Proposição 1.45, *d*). A mesma também garante que $\mathfrak{p}$ e $\mathfrak{q}$ são S-saturados, e portanto (aplicando ϕ_S^{-1}) tem-se $I^S \subseteq \mathfrak{q} \subseteq \mathfrak{p}$. Como $I \subseteq I^S$, segue pela minimalidade de $\mathfrak{p}$ sobre I que $\mathfrak{q} = \mathfrak{p}$.

Assim, pela Proposição 1.27 teremos $\mathrm{Rad}(I_\mathfrak{p}) = \mathfrak{p}_\mathfrak{p}$, logo se $a \in \mathfrak{p}$, segue da Proposição 1.48, *c*) que $a \in \mathrm{Rad}(I^S)$. Seja $n \geq 1$ mínimo tal que $a^n \in I^S$. Então $ua^n \in I$ para algum $u \in S$, e $sa^{n-1} \notin I$ para cada $s \in S$. Como $I = \mathrm{Ann}(m)$, isto significa em particular que vale $a \in \mathrm{Ann}(\hat{m})$, sendo $\hat{m} = ua^{n-1}m \in M \setminus 0$. Isto mostra que $a \in \mathcal{Z}_A(M)$. □

Corolário 1.53. *Se I é um ideal em um anel A, então todo primo minimal sobre I está contido em $\mathcal{Z}_A(A/I)$.*

Demonstração. Decorre da Proposição anterior tomando $M = A/I$, e levando em conta que $I = \mathrm{Ann}(m)$, onde $m = 1 + I \in M \setminus 0$. □

Observação 1.54. Com as notações da prova da Proposição anterior, note que se $a \in \mathfrak{p}$ então $I + \langle a \rangle \subseteq J_0 = \mathrm{Ann}(\hat{m})$ (pois $I = \mathrm{Ann}(m) \subseteq \mathrm{Ann}(ua^{n-1}m)$). Afirmamos que vale $J_0 \subseteq \mathfrak{p}$. De fato, se $t \in A \setminus \mathfrak{p} = S$, então pela definição de n temos $tua^{n-1} \notin I$ (pois $tu \in S$), isto é, $tua^{n-1}m \neq 0$, logo $t \notin \mathrm{Ann}(\hat{m})$. Portanto $\mathfrak{p}$ é minimal sobre um ideal M-anulador contendo $I + \langle a \rangle$. Em particular, se $\mathfrak{p}$ é finitamente gerado, digamos $\mathfrak{p} = \langle a_1, \ldots, a_k \rangle$, então aplicando reiteradamente o raciocínio anterior, concluímos que existe um ideal M-anulador J tal que $I + \langle a_1, \ldots, a_k \rangle \subseteq J \subseteq \mathfrak{p}$, e assim $\mathfrak{p} = J \in \mathrm{Ass}(M)$.

Definição 1.55. Uma propriedade $\mathbb{P}$ de A-módulos é dita **local** se as condições a seguir são equivalentes, para qualquer A-módulo M:

1. M satisfaz $\mathbb{P}$.
2. O $A_\mathfrak{p}$-módulo $M_\mathfrak{p}$ satisfaz $\mathbb{P}$ para todo $\mathfrak{p} \in \mathrm{Spec}(A)$.
3. $M_\mathfrak{m}$ satisfaz $\mathbb{P}$ para todo $\mathfrak{m} \in \text{m-Spec}(A)$.

Exemplo 1.56. A propriedade de ser o módulo nulo é local; mais especificamente, dado $m \in M$, temos as seguintes condições equivalentes:

1. $m = 0$.
2. $m/1 = 0$ em $M_{\mathfrak{p}}$, para cada $\mathfrak{p} \in \operatorname{Spec}(A)$.
3. $m/1 = 0$ em $M_{\mathfrak{m}}$, para cada $\mathfrak{m} \in \text{m-Spec}(A)$.

As implicações (1) $\Rightarrow$ (2) $\Rightarrow$ (3) são óbvias, e assim basta demonstrarmos (3) $\Rightarrow$ (1). Se $m \in M \setminus 0$ então $\operatorname{Ann}(m) \subsetneq A$, logo $\operatorname{Ann}(m) \subseteq \mathfrak{n}$ para algum $\mathfrak{n} \in \text{m-Spec}(A)$, e assim para cada $s \in A \setminus \mathfrak{n}$ teremos $sm \neq 0$, o que mostra que vale $m/1 \neq 0$ em $A_{\mathfrak{n}}$.

Proposição 1.57. *Sejam N, P submódulos de um A-módulo M, então:*

$N = P$.

$N_{\mathfrak{p}} = P_{\mathfrak{p}}$ *para todo* $\mathfrak{p} \in \operatorname{Spec}(A)$.

$N_{\mathfrak{m}} = P_{\mathfrak{m}}$ *para todo* $\mathfrak{m} \in \text{m-Spec}(A)$.

Demonstração. De maneira análoga ao Exemplo anterior vamos demonstrar apenas que (3) $\Rightarrow$ (1). Suponhamos que se tenha $N_{\mathfrak{m}} = P_{\mathfrak{m}}$ para cada $\mathfrak{m} \in \text{m-Spec}(A)$, e seja $L = N + P$. Então $L_{\mathfrak{m}}/N_{\mathfrak{m}} = (N_{\mathfrak{m}} + P_{\mathfrak{m}})/N_{\mathfrak{m}} = (N_{\mathfrak{m}} + N_{\mathfrak{m}})/N_{\mathfrak{m}} = 0$, mas pelo item d) da Proposição 1.48 vale $L_{\mathfrak{m}}/N_{\mathfrak{m}} \simeq (L/N)_{\mathfrak{m}}$. Portanto $(L/N)_{\mathfrak{m}} = 0$ para cada $\mathfrak{m} \in \text{m-Spec}(A)$, logo pelo Exemplo anterior temos $L/N = 0$ e, portanto $L = N$. De maneira análoga prova-se que $L = P$ e assim $N = P$. $\square$

Definição 1.58. A **dimensão de Krull** de um anel A, denotada por $\dim(A)$, é o maior número natural n para o qual se pode formar uma cadeia

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \cdots \subsetneq \mathfrak{p}_n \,,$$

onde cada $\mathfrak{p}_i$ é um ideal primo de A. Caso não exista esse número n, então é porque podemos formar cadeias de comprimento arbitrário, e neste caso definimos $\dim(A) = \infty$.

Definição 1.59. Definimos a **altura** de um ideal primo $\mathfrak{p} \in \operatorname{Spec}(A)$ (denotada por $\operatorname{ht}(\mathfrak{p})$) por $\operatorname{ht}(\mathfrak{p}) = \dim(A_{\mathfrak{p}})$. Pela Proposição 1.45, d) teremos que $\operatorname{ht}(\mathfrak{p})$ será o maior natural n para o qual existe uma cadeia de ideais primos em A da forma

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p} \,,$$

quando tal n exista; caso contrário definimos $\operatorname{ht}(\mathfrak{p}) = \infty$. Ainda, para um ideal próprio I de A, definimos sua **altura** como sendo

$$\operatorname{ht}(I) = \operatorname{mín}\{\operatorname{ht}(\mathfrak{p}) : \mathfrak{p} \in \operatorname{Spec}(A), \mathfrak{p} \supseteq I\} \,.$$

Obviamente temos $\operatorname{ht}(I) = \operatorname{mín}\{\operatorname{ht}(\mathfrak{p}) : \mathfrak{p}$ é primo minimal sobre $I\}$.

Enunciamos a seguir o teorema da altura de Krull, cuja demonstração pode ser encontrada em (BORGES; TENGAN, 2015, Exercício 7.9)

Teorema 1.60. *Sejam A um anel noetheriano e $I = \langle a_1, a_2, ..., a_n \rangle$ um ideal próprio. Então:*

1. *$I \subseteq \mathfrak{p}$ para algum $\mathfrak{p} \in \mathrm{Spec}(A)$ com $\mathrm{ht}(\mathfrak{p}) \leq n$; em particular $\mathrm{ht}(I) \leq n$.*
2. *Se A é domínio, então para quaisquer $a \in A \setminus 0$ e $\mathfrak{q} \in \mathrm{Spec}(A)$ minimal sobre $\langle a \rangle$ vale $\mathrm{ht}(\mathfrak{q}) \leq 1$.*

1.6 Domínios de valorização discreta

Definição 1.61. Seja $\mathbb{K}$ um corpo. Uma **valorização discreta de $\mathbb{K}$** é uma função sobrejetiva $v : \mathbb{K}^* \to \mathbb{Z}$ satisfazendo, para quaisquer $a, b \in \mathbb{K}^*$:

- $v(ab) = v(a) + v(b)$; ou seja, v é um homomorfismo do grupo $(\mathbb{K}^*, \cdot)$ no grupo $(\mathbb{Z}, +)$.
- $v(a + b) \geq \mathrm{mín}\{v(a), v(b)\}$, desde que $a + b \neq 0$.

Em particular $v(1) = v(1^2) = 2v(1)$ e assim $v(1) = 0$. Analogamente $v(-1) = 0$, pois $0 = v(1) = v\big((-1)^2\big) = 2v(-1)$. Isto, junto com o fato de v ser homomorfismo de grupos, implica para todos $a, b \in \mathbb{K}^*$ as igualdades $v(a) = v(-a), v(a^{-1}) = -v(a)$ e $v(ab^{-1}) = v(a) - v(b)$.

O conjunto $A_v = \{a \in \mathbb{K} : v(a) \geq 0\} \cup \{0\}$ é chamado de **anel associado à valorização v**. Afirmamos que A_v é realmente um anel, e de fato será um anel local. Com efeito, já temos $0 \in A_v$, e se $a, b \in A_v \setminus 0$, então $v(a), v(b) \geq 0$, e assim ou bem $a + b = 0$ ou bem $v(a+b) \geq \mathrm{mín}\{v(a), v(b)\} \geq 0$, e também $v(-a) = v(a) \geq 0$ e $v(ab) = v(a)+v(b) \geq 0$, o que mostra que $a + b, ab, -a \in A_v$, isto é, A_v é subanel de $\mathbb{K}$.

A localidade de A_v é garantida, pois se $c \in A_v$ não é invertível então $c^{-1} \notin A_v$, logo $v(c^{-1}) < 0$; reciprocamente, se $c \in \mathbb{K}^*$ satisfaz $v(c) > 0$, então para todo $b \in A_v \setminus 0$ vale $v(cb) = v(c) + v(b) > 0$, logo $cb \neq 1$ (pois $v(1) = 0$). Assim, o conjunto das não unidades em A_v é precisamente $\{0\} \cup \{c \in \mathbb{K}^* : v(c) > 0\}$, o qual é um ideal em A_v (A prova é idêntica à prova acima de A_v ser subanel de $\mathbb{K}^*$).

Finalmente afirmamos que $\mathbb{K}$ é o corpo de frações de A_v: como v é sobrejetiva, então existe $x \in K$ tal que $v(x) = 1$; em particular $x \in A_v$, e para todo $y \in \mathbb{K} \setminus A_v$ teremos $v(y) = -n$, com $n > 0$, logo $v(yx^n) = 0$ e assim $c = yx^n \in A_v^*$. Portanto $y = c/x^n$, com $c, x^n \in A_v$ e $x^n \neq 0$.

Definição 1.62. Um **domínio de valorização discreta** é um domínio A tal que $A = A_v$ para alguma valorização discreta do seu corpo de frações.

A seguir apresentamos uma caracterização dos domínios de valorização discreta:

Proposição 1.63. *Seja $(A, \mathfrak{m})$ um domínio local com corpo de frações $\mathbb{K}$. As seguintes condições são equivalentes:*

a) $A = A_v$ *para alguma valorização discreta* $v : \mathbb{K}^* \to \mathbb{Z}$.

b) A *é um domínio de ideais principais que não é corpo.*

c) A *é um anel noetheriano e* $\mathfrak{m}$ *é gerado por um elemento não nulo.*

d) A *é um domínio fatorial com um único elemento irredutível a menos de associados.*

Demonstração.

$a) \Rightarrow b)$ Uma vez que v é sobrejetiva, então, em particular, $v(x) = 1$ para algum $x \in A \setminus 0$, e assim $x \in \mathfrak{m} = \{a \in \mathbb{K} : v(a) > 0\}$, logo $\mathfrak{m}$ como um ideal não-trivial de A, e por isto não é corpo. Se $I \neq 0$ é um ideal em A, seja $b \in I$ com $v(b) \in \mathbb{N}$ sendo o mínimo possível. Claramente $\langle b \rangle \subseteq I$, e se $y \in I$ então $v(y) \geq v(b)$ pela escolha de b, logo $v(yb^{-1}) = v(x) - v(b) \geq 0$, logo $xb^{-1} = a \in A_v$ e $x = ba$, provando a inclusão $I \subseteq \langle b \rangle$.

$b) \Rightarrow c)$ Obviamente A é noetheriano, e ainda $\mathfrak{m} = \langle x \rangle$ para algum elemento $x \in A \setminus 0$ (pois A não é corpo, logo $\mathfrak{m} \neq 0$).

$c) \Rightarrow d)$ Seja $\mathfrak{m} = \langle x \rangle$, com $x \neq 0$. Afirmamos que vale $\bigcap_{n=1} \langle x^n \rangle = 0$. De fato, dado $a \in \bigcap_{n=1} \langle x^n \rangle$, a cadeia de ideais $\langle a \rangle \subseteq (a : x) \subseteq (a : x^2) \cdots \subseteq (a : x^n) \cdots$ estaciona (condição a) da Proposição 1.5), digamos $(a : x^m) = (a : x^{m+1})$. Ora, $a \in \langle x^{m+1} \rangle$, digamos $a = cx^{m+1}$, com $c \in A$, e assim $c \in (a : x^{m+1}) = (a : x^m)$, logo $cx^m = ra$ para algum $r \in A$. Substituindo obtemos $a = (cx^m)x = arx$, o que implica $a = 0$, pois caso contrário teríamos $1 = rx$, isto é, $x \in A^*$, absurdo.

Consequentemente, para cada $b \in A \setminus 0$ existe $m \geq 0$ tal que $b \in \langle x^m \rangle \setminus \langle x^{m+1} \rangle$, e portanto $b = ux^m$ com $u \notin \langle x \rangle = \mathfrak{m}$, isto é, $u \in A^*$. Agora afirmamos que x é um elemento primo. Certamente $x \notin \{0\} \cup A^*$. Sejam $a, b \in A \setminus 0$, digamos $a = ux^m, b = wx^n$, com $m, n \geq 0$ e $u, w \in A^*$, e suponha $x \mid ab$. Então $ab \notin A^*$ pois $x \notin A^*$. Como $ab = uwx^{m+n}$ então necessariamente $m + n \geq 1$, logo $m \geq 1$ ou $n \geq 1$, e assim $x \mid a$ ou $x \mid b$. Isto prova que A admite fatoração **em primos**, isto é, A é fatorial. Ainda, a prova mostra que x é o único primo a menos de associados.

$d) \Rightarrow a)$ Seja x o único elemento irredutível do domínio fatorial A (a menos de associados). Todo elemento $a \in \mathbb{K}^*$ é da forma $a = b/c$ com $b, c \in A \setminus 0$, e teremos $b = ux^n$ e $c = wx^m$, com $m, n \geq 0$ e $u, w \in A^*$. Assim $a = tx^k$ com $t \in A^*$ e $k \in \mathbb{Z}$. Definimos $v : \mathbb{K}^* \to \mathbb{Z}$ por $v(a) = k$. Se $tx^k = ux^j$, com $t, u \in A^*$ e $k \leq j$, então

$x^{j-k} = tu^{-1} \in A^*$, logo necessariamente $j - k = 0$ (pois x é irredutível, logo não invertível). Isto mostra que v fica bem definida, e claramente $A = A_v$.

Resta provar que v é uma valorização discreta de K e $A_v = A$. Se $a_1 = t_1 x^{k_1}$ e $a_2 = t_2 x^{k_2}$, com $k_1 \leq k_2$ e $t_1, t_2 \in A^*$, então $v(a_1 a_2) = v(t_1 t_2 x^{k_1+k_2}) = k_1 + k_2 = v(a_1) + v(a_2)$. Também, $a_1 + a_2 = b x^{k_1}$, sendo $b = t_1 + t_2 x^{k_2-k_1} \in A$. Se $a_1 + a_2 \neq 0$ então $b \neq 0$, logo $v(b) \geq 0$, o que implica $v(a_1 + a_2) = v(b) + v(x^{k_1}) \geq v(x^{k_1}) = k_1 = \text{mín}\{v(a_1), v(a_2)\}$. □

Corolário 1.64. *Em um domínio de valorização discreta D o conjunto dos ideais é totalmente ordenado.*

Demonstração. Pela Proposição anterior existe um elemento $x \in D$ tal que todo ideal em D é da forma $\langle x^m \rangle$, com $m \in \mathbb{N}$, e obviamente vale $\langle x^m \rangle \subseteq \langle x^n \rangle \Leftrightarrow m \geq n$. □

Exemplo 1.65. Dado um anel A, seja $A((X))$ o conjunto das funções $f : \mathbb{Z} \to A$ para as quais existe $N = N(f) \in \mathbb{Z}$ tal que $f(n) = 0$ para $n < N$. Para outra função $g \in A((X))$, digamos $g(n) = 0$ para $n < M$, definimos a soma e o produto $f + g, fg : \mathbb{Z} \to A$ por

$$(f + g)(n) = f(n) + g(n)\,;\ (fg)(n) = \sum_{\substack{k,j \in \mathbb{Z} \\ k+j=n}} f(k)g(j)\,.$$

Note que se $n < \text{mín}\{N, M\}$ então $f(n) = g(n) = 0$, logo $(f + g)(n) = 0$, e assim $f + g \in A((X))$. Por outro lado, dado n, o conjunto dos pares de inteiros (k, j) com $k + j = n$ e $f(k)g(j) \neq 0$, é finito: com efeito, para tais pares teremos necessariamente $k \geq N$ e $j = n - k \geq M$, logo $N \leq k \leq n - M$. Isto mostra que a soma que define $(fg)(n)$ é finita, logo $(fg)(n)$ é de fato um elemento de A; ainda, se $n < M + N$ então a desigualdade $N \leq k \leq n - M$ é impossível, logo nenhum par (k, j) com $k + j = n$ satisfará $f(k)g(j) \neq 0$, o que mostra que vale $(fg)(n) = 0$, e portanto $fg \in A((X))$.

É fácil ver que, com estas operações, o conjunto $A((X))$ vira um anel, o qual é chamado de **anel das séries formais de Laurent sobre A**. Seus elementos $f : \mathbb{Z} \to A$ se denotam por $f = \sum_{n=N}^{\infty} f_n X^n$, onde $f_n = f(n)$ e N é tal que $f(n) = 0$ para $n < N$. Esta notação é conveniente pois permite fazer as operações usando as leis formais dos expoentes com o "símbolo" X ★, junto com a propriedade distributiva formal (para somar os coeficientes em A da mesma potência de X).

O anel $A((X))$ contém, de maneira natural, ao anel das séries formais de potências $A[[X]]$ como subanel, a saber $A[[X]] = \{f \in A((X)) : f_n = 0 \text{ para todo } n < 0\}$, o qual

★ O símbolo X pode de fato ser interpretado como um elemento de $A((X))$, a saber, $X(1) = 1_A$ e $X(n) = 0_A$ para todo $n \neq 1$. A única precaução a ser tomada é continuar interpretando a notação de soma infinita de maneira apenas formal, e manipulando X como elemento apenas quando somas e produtos finitos sejam envolvidos.

por sua vez contém como subanel ao anel $A[X]$ dos polinômios com coeficientes em A. Finalmente, $A[X]$ contém A como subanel.

Dado $f \in A((X)) \setminus 0$, seja $v(f) = \text{mín}\{n \in \mathbb{Z} : f_n \neq 0\}$. Ou seja, $f = \sum_{n=v(f)}^{\infty} f_n X^n$, com $f_{v(f)} \neq 0$. Para qualquer outro $g \neq 0$, e denotando $v(f) = N$, $v(g) = M$, teremos $f+g = \sum_{n=\text{mín}\{N,M\}}(f_n+g_n)X^n$ e $fg = \sum_{n=N+M}^{\infty} h_n X^n$. Assim $v(f+g) \geq \text{mín}\{v(f), v(g)\}$ se $f+g \neq 0$, e como $h_{N+M} = f_N g_M$ então $v(fg) \geq v(f)+v(g)$ se $fg \neq 0$. Se A é domínio então $h_{N+M} \neq 0$, logo $fg \neq 0$ e $v(fg) = v(f) + v(g)$; em particular $A((X))$ será também um domínio.

Por outro lado, f é invertível em $A((X))$ se, e somente se, f_N for invertível em A. Com efeito, se existe $g \in A((X))$ com $fg = 1$ então com as notações acima teremos $M = -N$ e $f_N g_M = 1$, logo $f_N \in A^*$; reciprocamente, se $f_N \in A^*$, então $f = f_N X^N h$, onde $h \in A[[X]]$ tem termo constante igual a 1. Definindo recursivamente g_n por $g_0 = 1$ e $g_n = -\sum_{k=0}^{n-1} g_k h_{n-k}$ para $n > 0$, obtemos $g = \sum_{n=0}^{\infty} g_n X^n \in A[[X]]$ tal que $gh = 1$, e portanto $f(f_N^{-1}X^{-N}g) = 1$, com $f_N^{-1}X^{-N}g \in A((X))$.

Todo o anterior mostra que se A é um corpo então $\mathbb{K} = A((X))$ também será um corpo, e ainda, a função $v : \mathbb{K}^* \to \mathbb{Z}$ será uma valorização discreta de $\mathbb{K}$. Note que A_v é precisamente $A[[X]]$, o que mostra que o anel de séries formais de potências com coeficientes em um corpo forma um domínio de valorização discreta.

2 IDEAIS FORTEMENTE IRREDUTÍVEIS

2.1 Propriedades básicas e exemplos

Definição 2.1. Um ideal próprio I é dito **fortemente irredutível** se dados dois ideais J, K satisfazendo $J \cap K \subseteq I$, então $J \subseteq I$ ou $K \subseteq I$.

Definição 2.2. Um anel A é dito **aritmético** se para quaisquer três ideais ideais I, J e K vale a identidade $(I + J) \cap K = (I \cap K) + (J \cap K)$.

Exemplo 2.3. Todo domínio de ideais principais D é aritmético, pois dados ideais I, J e K de D temos que existem $a, b, c \in D$ tais que $I = \langle a \rangle$, $J = \langle b \rangle$ e $K = \langle c \rangle$. Segue que

$$\begin{aligned}
(I + J) \cap K &= \big(\langle a \rangle + \langle b \rangle\big) \cap \langle c \rangle \\
&= \big\langle \mathrm{mdc}(a, b) \big\rangle \cap \langle c \rangle \\
&= \big\langle \mathrm{mmc}\big(\mathrm{mdc}(a, b), c\big) \big\rangle \\
&= \big\langle \mathrm{mdc}\big(\mathrm{mmc}(a, c), \mathrm{mmc}(b, c)\big) \big\rangle^{\S} \\
&= \big\langle \mathrm{mmc}(a, c) \big\rangle + \big\langle \mathrm{mmc}(b, c) \big\rangle \\
&= \big(\langle a \rangle \cap \langle c \rangle\big) + \big(\langle b \rangle \cap \langle c \rangle\big) \\
&= (I \cap J) + (J \cap K)\,.
\end{aligned}$$

Lema 2.4. *Um anel A é aritmético se, e somente se, para quaisquer ideais I, J e K vale a identidade* $(I \cap J) + K = (I + K) \cap (J + K)$.

Demonstração. Suponhamos que A seja aritmético. Então vale

$$\begin{aligned}
(I + K) \cap (J + K) &= \big(I \cap (J + K)\big) + \big(K \cap (J + K)\big) \\
&= \big((J + K) \cap I\big) + K \\
&= (I \cap J) + (I \cap K) + K \\
&= (I \cap J) + K\,.
\end{aligned}$$

§ Usamos a identidade $\mathrm{mmc}\big(a, \mathrm{mdc}(b, c)\big) = \mathrm{mdc}\big(\mathrm{mmc}(a, b), \mathrm{mmc}(a, c)\big)$; ou seja, mmc distribui com respeito de mdc.

Reciprocamente se para quaisquer ideais I, J e K temos $(I \cap J) + K = (I + K) \cap (J + K)$, então

$$\begin{aligned}(I \cap K) + (J \cap K) &= \big(I + (J \cap K)\big) \cap \big(K + (J \cap K)\big) \\ &= \big(I + (J \cap K)\big) \cap K \\ &= (I + J) \cap (I + K) \cap K \\ &= (I + J) \cap K\,. \quad \square\end{aligned}$$

Observação 2.5. Em qualquer anel A sempre vale a inclusão $(I+J)\cap K \supseteq (I\cap K)+(J\cap K)$. Portanto para um anel ser aritmético, basta valer $(I+J)\cap K \subseteq (I\cap K)+(J\cap K)$. A respeito da outra equivalência sempre vale $(I \cap J) + K \subseteq (I + K) \cap (J + K)$, logo um anel A é aritmético se, e somente se, $(I + J) \cap K \subseteq (I \cap K) + (J \cap K)$ para todos os ideais I, J e K em A (ou, alternativamente, $(I + K) \cap (J + K) \subseteq (I \cap K) + K$ para todos os ideais).

Dentre as propriedades básicas que demonstraremos no texto está a de que, como era de se esperar, todo ideal fortemente irredutível é irredutível; mas a recíproca não vale (vide o Exemplo 2.17). A interseção de dois ideais fortemente irredutíveis pode não ser fortemente irredutível: por exemplo $\langle 2\rangle, \langle 3\rangle \subseteq \mathbb{Z}$ são fortemente irredutíveis (vide Exemplo 2.3 e o item *d*) do Lema 2.10); porém $\langle 2\rangle \cap \langle 3\rangle = \langle 6\rangle$ não é fortemente irredutível.

Entretanto se I_1, I_2 são fortemente irredutíveis, então $I_1 \cap I_2$ cumpre o seguinte: dados três ideais $J, K, L \subseteq A$ tais que $J \cap K \cap L \subseteq I_1 \cap I_2$, então $J \cap K \subseteq I_1 \cap I_2$ ou $K \cap L \subseteq I_1 \cap I_2$ ou $J \cap L \subseteq I_1 \cap I_2$. Com efeito, temos $J \cap K \cap L \subseteq I_1, I_2$ o que nos dá pela irredutibilidade forte de I_1 e I_2 que cada um deles contém algum dos três ideais, logo $I_1 \cap I_2$ conterá a interseção de dois deles (se I_1 e I_2 contém o mesmo ideal então $I_1 \cap I_2$ conterá duas das interseções duplas).

Entre outras propriedades dos ideais fortemente irredutíveis que serão demonstradas no Lema 2.10 está a de que basta verificar a irredutibilidade forte para ideais principais, ou seja, I é fortemente irredutível, se e somente se, para cada $a, b \in A$ tais que $\langle a\rangle \cap \langle b\rangle \subseteq I$ tem-se $a \in I$ ou $b \in I$.

Lema 2.6. *Em um anel A as seguintes condições são equivalentes:*

- *Todo ideal de A é fortemente irredutível.*
- *Quaisquer dois ideais são comparáveis.*

Demonstração. Se todo ideal é fortemente irredutível, e I, J são ideais, então $I \cap J$ é fortemente irredutível, logo $I \cap J \subseteq I \cap J$ nos dá $I \subseteq I \cap J \subseteq J$ ou $J \subseteq I \cap J \subseteq I$.

Reciprocamente se quaisquer dois ideais de A são comparáveis, então dados I, J, K ideais arbitrários satisfazendo $J \cap K \subseteq I$, sem perda de generalidade podemos supor $J \subseteq K$, portanto $J \cap K = J \subseteq I$. □

Observação 2.7. Se os ideais de um anel A são linearmente ordenados pela inclusão, então o anel A é aritmético: dados $I, J, K \subseteq A$ ideais arbitrários, afirmamos que vale a igualdade $(I + J) \cap K = (I \cap K) + (J \cap K)$. Como esta igualdade é simétrica em I e J, basta prová-la nos três casos seguintes.

Se $I \subseteq J \subseteq K$ então $(I + J) \cap K = J = (I \cap K) + (J \cap K)$. Se $I \subseteq K \subseteq J$ temos $(I + J) \cap K = J \cap K = K = I + K = (I \cap K) + (J \cap K)$. Finalmente se $K \subseteq I \subseteq J$ então $(I + J) \cap K = K = K + K = (I \cap K) + (J \cap K)$. Os casos restantes decorrem da simetria em I e J.

A recíproca é falsa, por exemplo $\mathbb{Z}$ é aritmético, mas seus ideais não são linearmente ordenados; entretanto se A for local e aritmético, então todos os seus ideais são linearmente ordenados. A caracterização de ideais aritméticos e aritméticos locais do lema a seguir é devida a (JENSEN, 1966).

Lema 2.8. *Seja A um anel. Então tem-se:*

a) *Os ideais em A estão totalmente ordenados por inclusão se, e somente se, os ideais principais o estão.*

b) *A é local e aritmético se, e somente se, todos os seus ideais estão linearmente ordenados.*

c) *A é aritmético se, e somente se, para cada $\mathfrak{p} \in \operatorname{Spec}(A)$, os ideais em $A_{\mathfrak{p}}$ são totalmente ordenados pela inclusão.*

Demonstração.

a) A implicação direta é clara. Reciprocamente, suponha que para quaisquer $a, b \in A$ vale $a \mid b$ ou $b \mid a$. Se houvessem ideais I, J tais que $I \nsubseteq J$ e $J \nsubseteq I$, então existiriam $a \in I \setminus J$ e $b \in J \setminus I$; mas $a \mid b$ ou $b \mid a$, ou seja, $b \in \langle a \rangle \subseteq I$ ou $a \in \langle b \rangle \subseteq J$, contradição.

b) Pela Observação anterior a ordenação linear de ideais em um anel implica que ele é aritmético; ainda, não poderá ter mais de um ideal maximal, pois ideais maximais diferentes não são comparáveis. Agora provaremos que se A é local e aritmético, então para quaisquer dois elementos $a, b \in A$ tem-se $a \mid b$ ou $b \mid a$, logo pelo item anterior todos os ideais estarão linearmente ordenados.

Note que $\langle a \rangle \subseteq \langle b \rangle + \langle a - b \rangle$, logo por aritmeticidade $\langle a \rangle = \big(\langle b \rangle + \langle a - b \rangle\big) \cap \langle a \rangle = \big(\langle a \rangle \cap \langle b \rangle\big) + \big(\langle a \rangle \cap \langle a - b \rangle\big)$. Portanto $a = d + (a - b)c = d + ac - bc$, onde $d \in \langle a \rangle \cap \langle b \rangle$

e $ac - bc \in \langle a \rangle \cap \langle a - b \rangle$, implicando $bc \in \langle a \rangle$. Se $c \in A^*$ então $b \in \langle a \rangle$; se $c \notin A^*$, então $1 - c \in A^*$ (pois A é local), e como $a(1-c) = a - ac = d - bc \in \langle b \rangle$, concluímos que vale $a \in \langle b \rangle$.

c) Vimos na Proposição 1.48 que localizações comutam com soma e interseção de um número finito de ideais. Consequentemente, se A é aritmético, então $A_\mathfrak{p}$ é aritmético (na verdade qualquer A_S será aritmético). O recíproco também vale pois pela Proposição 1.57 temos a garantia de que a igualdade entre ideais é uma propriedade que pode ser checada localmente, logo se $A_\mathfrak{p}$ é aritmético para todo $\mathfrak{p} \in \operatorname{Spec}(A)$, então A o será. □

Observação 2.9. O Lema anterior continua válido se trocarmos "$\mathfrak{p} \in \operatorname{Spec}(A)$" por "$\mathfrak{m} \in \text{m-Spec}(A)$" (pela Proposição 1.57).

Lema 2.10. *Sejam A um anel e I um ideal em A. Então:*

a) *Todo ideal fortemente irredutível é irredutível. Além disso se A é noetheriano, então I é primário.*

b) *Todo ideal primo é fortemente irredutível.*

c) *Seja $S \subseteq A$ um conjunto multiplicativo. I_S fortemente irredutível implica I^S fortemente irredutível.*

d) *Se A é aritmético, então I é irredutível se, e somente se, I é fortemente irredutível e se, e somente se, $\mathcal{Z}_A(A/I)$ for um ideal primo de A.*

e) *Se I é fortemente irredutível e $H \subseteq I$ é um ideal, então I/H é fortemente irredutível em R/H.*

f) *Uma condição suficiente para que um ideal I seja fortemente irredutível é que dados $a, b \in A$, $\langle a \rangle \cap \langle b \rangle \subseteq I$ implique que $a \in I$ ou $b \in I$.*

g) *Se I é fortemente irredutível e primário e S for um conjunto multiplicativo tal que $\operatorname{Rad}(I) \cap S = \emptyset$, então I_S é fortemente irredutível em A_S.*

h) *Se I é $\mathfrak{p}$-primário, então $I_\mathfrak{p}$ fortemente irredutível em $A_\mathfrak{p}$ implica I fortemente irredutível em A.*

Demonstração.

a) Seja I um ideal fortemente irredutível e J, K ideais tais que $I = J \cap K$. Então já valem as inclusões $I \subseteq J$ e $I \subseteq K$. Por hipótese temos que I é fortemente irredutível, logo $J \subseteq I$ ou $K \subseteq I$. Sem perda de generalidade assumamos $J \subseteq I$ e assim $I = J$. Ademais se A é noetheriano, então I é primário pelo Corolário 1.16.

b) Sejam $\mathfrak{p}$ um ideal primo e J, K ideais cumprindo $J \cap K \subseteq \mathfrak{p}$. Logo $\mathfrak{p} \supseteq JK$ e pela definição de ideal primo, $\mathfrak{p} \supseteq J$ ou $\mathfrak{p} \supseteq K$.

c) Suponha que $I_S = \{a/s : a \in I, s \in S\}$ é fortemente irredutível em A_S. Sendo J, K ideais em A tais que $J \cap K \subseteq I^S$ vem que $(J \cap K)_S \subseteq (I^S)_S = I_S$, mas $(J \cap K)_S = J_S \cap K_S$, portanto $J_S \subseteq I_S$ ou $K_S \subseteq I_S$ o que nos dá (contraindo) $J \subseteq J^S \subseteq I^S$ ou $K \subseteq K^S \subseteq I^S$.

d) Já demonstramos que todo ideal fortemente irredutível é irredutível; demonstraremos, sob as hipóteses apresentadas, a recíproca. Suponhamos que I é irredutível e $J \cap K \subseteq I$. Com isto obtemos $(J \cap K) + I = I$, mas pela hipótese de que A é aritmético, então $I = (J \cap K) + I = (J + I) \cap (K + I)$; sendo I irredutível, segue que $I = J + I$ ou $I = I + K$ o que nos dá, respectivamente, $J \subseteq I$ ou $K \subseteq I$.

Suponhamos agora que I é fortemente irredutível e seja $\mathcal{Z} = \mathcal{Z}_A(A/I)$ o conjunto dos divisores de zero de A/I (**como *A*-módulo**). Nosso objetivo é provar que $\mathcal{Z}$ é um ideal primo. Ora, foi visto que $\mathcal{Z}$ é próprio e absorve produtos, portanto basta demonstrar que $\mathcal{Z}$ é fechado para somas.

Considere $a, b \in \mathcal{Z}$. Existem então $c, d \in A \setminus I$ de maneira que $ac, bd \in I$. Afirmamos que $\langle c \rangle \cap \langle d \rangle \nsubseteq I$, pois caso contrário, pela hipótese sobre I, teríamos $c \in \langle c \rangle \subseteq I$ ou $d \in \langle d \rangle \subseteq I$, contradição. Portanto existem $k_1, k_2 \in A$ tais que $e = ck_1 = dk_2 \in \langle c \rangle \cap \langle d \rangle \setminus I$ e assim $(a + b)e = ae + be = ack_1 + bdk_2 \in I$, o que mostra que vale $a + b \in \mathcal{Z}$.

Reciprocamente se temos $\mathcal{Z} = \mathfrak{p} \in \operatorname{Spec}(A)$, então definindo $S = A \setminus \mathfrak{p}$ temos $I = I^S$ pela Proposição 1.45, *b*). Pelo Lema 2.8 segue que os ideais de $A_\mathfrak{p}$ são totalmente ordenados pela relação de inclusão, logo todo ideal em $A_\mathfrak{p}$ é fortemente irredutível pelo Lema 2.6. Assim pelo item anterior teremos $I^S = I$ fortemente irredutível.

e) Dados $J^*, K^* \subseteq A/H$ tais que $J^* \cap K^* \subseteq I/H$ sabemos pelo teorema da correspondência que existem ideais J, K em A contendo H de maneira que $J^* = J/H, K^* = K/H$. Com as considerações feitas até aqui vamos ter $J \cap K \subseteq I$. Pela irredutibilidade forte de I segue que $J \subseteq I$ ou $K \subseteq I$, o que nos dá, respectivamente, $J^* \subseteq I/H$ ou $K^* \subseteq I/H$.

f) Sejam J, K ideais satisfazendo $J \cap K \subseteq I$. Caso $I \nsupseteq J$, considere $a \in J \setminus I$ fixado. Então para todo $b \in K$ vale $\langle a \rangle \cap \langle b \rangle \subseteq J \cap K \subseteq I$ e assim $b \in I$, pois $a \notin I$. Portanto $K \subseteq I$ o que mostra que I é fortemente irredutível.

g) Suponha que I é fortemente irredutível e primário e seja S multiplicativo com $\operatorname{Rad}(I) \cap S = \emptyset$. Sejam J^*, K^* ideais em A_S tais que $J^* \cap K^* \subseteq I_S$. Então existem ideais J, K em A tais que $J = J^S, K = K^S$, e $J^* = J_S, K^* = K_S$, o que implica $J^* \cap K^* = (J \cap K)_S$ pela Proposição 1.48, *b*), e assim $(J \cap K)_S \subseteq I_S$. Contraindo obtemos $(J \cap K)^S = J^S \cap K^S$ (Proposição 1.48, *b*)) $= J \cap K \subseteq I^S$, enquanto $I^S = I$

pela Proposição 1.45, b). Como I é fortemente irredutível então $J \subseteq I$ ou $K \subseteq I$, implicando em $J_S = J^* \subseteq I_S$ ou $K_S = K^* \subseteq I_S$. Isto mostra que I_S é fortemente irredutível.

h) Se I é $\mathfrak{p}$-primário e $I_{\mathfrak{p}}$ é fortemente irredutível, então pelo item c) segue que I^S é fortemente irredutível, onde $S = A \setminus \mathfrak{p}$; porém $I^S = I$ pela Proposição 1.45, b), portanto I é fortemente irredutível. □

Proposição 2.11. *Seja $A = B \times C$ com B, C anéis. Se J é um ideal próprio fortemente irredutível, então existem ideais I_1, I_2 fortemente irredutíveis, respectivamente, em B, C tais que $J = I_1 \times I_2$.*

Demonstração. Seja $J \subseteq A$. Vamos demonstrar que J se escreve como produto direto de ideais de B e C. Claramente $J \subseteq \pi_B(J) \times \pi_C(J)$ com $\pi_B(J)$ e $\pi_C(J)$ as projeções em B e C. Por outro lado se $(x, y) \in \pi_B(J) \times \pi_C(J)$ então existem $b \in B$, $c \in C$ tais que $(x, c), (b, y) \in J$, logo $(x, y) = (1, 0)(x, c) + (0, 1)(b, y) \in J$. Sejam I_1, I_2 tais que $J = I_1 \times I_2$. Se I_1 não fosse fortemente irredutível, então existiriam $a, b \in B \setminus I_1$ tais que $\langle a \rangle \cap \langle b \rangle \subseteq I_1$; contudo $\big(\langle a \rangle \times C\big) \cap \big(\langle b \rangle \times 0\big) = \big(\langle a \rangle \cap \langle b \rangle\big) \times 0 \subseteq J$, mas nenhum está contido em J, contradição. Assim, provamos que I_1 é fortemente irredutível, e a demonstração de que I_2 é fortemente irredutível é análoga. □

Corolário 2.12. *Seja $A = A_1 \times \cdots \times A_n$. Se J é um ideal fortemente irredutível em A, então existem $I_1, \ldots, I_n$ fortemente irredutíveis com $I_i \subseteq A_i$ tais que $J = I_1 \times \cdots \times I_n$.*

Proposição 2.13. *Seja A um domínio fatorial e $I \neq A$ um ideal. Então as seguintes condições são equivalentes:*

a) *I é fortemente irredutível.*

b) *Para todo $a, b \in A$, $\operatorname{mmc}(a, b) \in I$ implica $a \in I$ ou $b \in I$.*

c) *Dado um elemento $a = \prod_{i=1}^{k} p_i^{n_i} \in I$, onde os p_j são elementos irredutíveis não associados de A e n_j são inteiros positivos, então vale $p_j^{n_j} \in I$ para algum j.*

Além disso se I é principal, então I é fortemente irredutível, se e somente se, seu gerador é potência de algum elemento irredutível.

Demonstração.

$a) \Leftrightarrow b)$ Decorre da igualdade $\big\langle \operatorname{mmc}(a, b) \big\rangle = \langle a \rangle \cap \langle b \rangle$ junto com o item f) do Lema 2.10.

$b) \Rightarrow c)$ Como os $p_j^{n_j}$ são não associados temos que $\prod_{i=1}^{k} p_i^{n_i} = \operatorname{mmc}(p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k})$ e por aplicações sucessivas do item a) o resultado segue.

$c) \Rightarrow a)$ Tomemos $a, b \in A$ tais que $\text{mmc}(a, b) \in I$ e consideremos suas fatorações, ou seja:

$$a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} q_1^{m_1} \cdots q_r^{m_r}$$

e

$$b = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k} r_1^{j_1} \cdots r_l^{j_l},$$

logo $\text{mmc}(a, b) = p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{m_1} \cdots q_r^{m_r} r_1^{j_1} \cdots r_l^{j_l}$ onde $\alpha_i = \text{máx}\{n_i, t_i\}$ para todo i. Pela hipótese temos que alguma das três seguintes situações ocorre:

- Para algum i, $p_i^{\alpha_i} \in I$.
- Para algum i, $q_i^{m_i} \in I$.
- Para algum i, $r_i^{i_i} \in I$.

Caso $p_i^{\alpha_i} \in I$ e $\alpha_i = n_i$, então $a \in I$ e se $\alpha_i = t_i$ nós teríamos $b \in I$. Por outro lado se $q_i^{m_i} \in I$, então é evidente que $a \in I$ e, analogamente, ocorrendo $r_i^{l_i} \in I$, implica $b \in I$. Pela equivalência entre a) e b) o resultado segue.

Para provar a afirmação final, suponhamos $I = \langle a \rangle$ e $a = \prod_{i=1}^{k} p_i^{n_i}$, logo, pelo item c), para algum $j \in \mathbb{N}$ temos que $p_j^{n_j} \in I$, consequentemente $\langle p_j^{n_j} \rangle \subseteq I = \langle a \rangle$. Afirmamos que $I = \langle p_j^{n_j} \rangle$, pois $a = \prod_{i=1}^{k} p_i^{n_i} = p_j^{n_j} \prod_{i \neq j}^{k} p_i^{n_i}$ implica $\langle a \rangle \subseteq \langle p_j^{n_j} \rangle$ provando a inclusão oposta. Reciprocamente tomemos $I = \langle p^n \rangle$. Suponhamos que $\prod_{i=1}^{k} p_i^{m_i} \in I$, logo $p^n \mid \prod_{i=1}^{k} p_i^{m_i}$ e, consequentemente, $p^n \mid p_j^{m_j}$ para algum $j \in \mathbb{N}$ e desse modo $p \sim p_j$ e $m_j \leq n$. Assim $p_j^{m_j} \in I$ e por c) I é fortemente irredutível. □

Corolário 2.14. *Seja A um domínio fatorial. Então:*

a) Todo ideal principal não-nulo é fortemente irredutível se, e somente se, é primário.

b) Todo ideal fortemente irredutível não-nulo pode ser gerado por um conjunto de potências de elementos irredutíveis.

Demonstração.

$a)$ Sejam $a, b \in A \setminus 0$ tais que $ab \in I$. Como A é fatorial podemos assumir que vale $a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k} \cdots q_1^{m_1} \cdots q_r^{m_r}$ e $b = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k} \cdots r_1^{j_1} \cdots r_l^{j_l}$, portanto

$$ab = p_1^{n_1+t_1} p_2^{n_2+t_2} \cdots p_k^{n_k+t_k} \cdots q_1^{m_1} \cdots q_r^{m_r} r_1^{j_1} \cdots r_l^{j_l} \in I.$$

Deduzimos pelo item c) da Proposição anterior que para algum i vale $p_i^{n_i+t_i} \in I$ ou $q_i^{m_i} \in I$ ou $r_i^{l_i} \in I$. No primeiro caso basta tomarmos $n \in \mathbb{N}$ tal que $nt_i \geq n_i$, pois $(n+1)t_i \geq n_i + t_i$ nos fornece $p_i^{n_i+t_i} \mid p_i^{(n+1)t_i}$, notemos que $p_i^{(n+1)t_i} \mid b^{n+1}$, logo

$p_i^{n_i+t_i} \mid b^{n+1}$, ou seja, $b^{n+1} \in I$. Nos outros casos temos, respectivamente, $a \in I$ ou $b \in I$

Reciprocamente, consideremos $I = \langle a \rangle$ não primário, com $a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$. Afirmamos que o inteiro $k = 1$, pois do contrário existiriam m e j tais que $p_j^{mn_j} \in I$, mas isso não é possível, pois desse modo $p_j^{mn_j}$ admitiria duas decomposições distintas, logo $k = 1$ e $a = p_j^{m_j}$ e $I = \langle p_j^{m_j} \rangle$. Pelo resultado da Proposição anterior para I principal, segue que I é fortemente irredutível.

b) Sejam $X \subseteq A$ um conjunto de geradores para $I \neq 0$ e $x \in X \setminus 0$. Então $x = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ e pelo item *c*) da Proposição anterior segue $p_j^{m_j} \in I$ para algum $j \in \mathbb{N}$, portanto $\langle x \rangle \subseteq \langle p_j^{m_j} \rangle \subseteq I$. Como $x \in X$ é arbitrário o resultado segue. □

No caso em que o anel em questão é noetheriano as propriedades *g*) e *h*) do Lema 2.10 são válidas para ideais irredutíveis, uma vez que todo irredutível é primário em tais anéis; porém podemos ter um ideal primário que não é irredutível, como o seguinte exemplo mostra:

Exemplo 2.15 (Ideal primário em anel noetheriano, que não é irredutível). Seja $p \in \mathbb{Z}$ primo e considere $A = \mathbb{Z}_{p^2}[X]/\langle X^3 \rangle$. O homomorfismo $i : \mathbb{Z}_{p^2} \to A$ é injetivo, pois $\mathbb{Z}_{p^2} \cap \langle X^3 \rangle = 0$. A fim de simplificar as notações vamos denotar, para $a \in \mathbb{Z}$, o elemento $i(\overline{a}) \in A$ por a e $\overline{X} := \eta$. Convém observar que A é noetheriano, e $A = \mathbb{Z}_{p^2}[\eta]$ (logo todo $a \in A$ é da forma $f(\eta)$ com $f \in \mathbb{Z}_{p^2}[X]$). Considere o ideal $I = \langle p\eta \rangle$.

Afirmação.

a) Seja $\alpha \in \mathbb{Z}_{p^2}$. Então $p \mid \alpha \Leftrightarrow p\alpha = 0 \Leftrightarrow \alpha \in \mathcal{Z}(\mathbb{Z}_{p^2})$. Como consequência, para todo $f \in \mathbb{Z}_{p^2}[X]$ tem-se $pf = 0$, se e somente se, $p \mid f$.

b) Tem-se $I = \langle p \rangle \cap \langle \eta \rangle$ e $I \subsetneq \langle p \rangle, \langle \eta \rangle$.

c) O ideal I é primário.

Demonstração.

a) A tripla equivalência decorre da igualdade $\mathcal{Z}(\mathbb{Z}_{p^2}) = \{0, p\}$, e a afirmação sobre os polinômios é obtida aplicando o primeiro resultado a cada coeficiente.

b) A inclusão $I \subseteq \langle p \rangle \cap \langle \eta \rangle$ é óbvia. Para demonstrarmos a segunda inclusão, considere $z \in \langle p \rangle \cap \langle \eta \rangle$, isto é $z = pf(\eta) = \eta g(\eta)$. Logo temos $pf(X) - Xg(X) = X^3 h(X)$ e como $X \mid X^3 h(X)$ e $X \mid Xg(X)$, então $X \mid pf(X)$, digamos $pf(X) = Xq(X)$. Multiplicando por p e lembrando que $p^2 = 0$ vem $pXq(X) = 0$, porém X é

elemento regular e portanto $pq(X) = 0$. Pelo item anterior temos $q(X) = pr(X)$, logo $z = pf(\eta) = \eta q(\eta) = p\eta r(\eta) \in \langle p\eta \rangle$.

Por outro lado se $p = p\eta f(\eta)$, seguiria $p - pXf(X) = X^3 h(X)$, o que é absurdo, pois $X^3 h(X)$ possui termo constante nulo e $p - pXf(X)$ possui termo constante p. Do mesmo modo se supomos $\eta = p\eta g(\eta)$, multiplicando por p temos $p\eta = 0$, logo $pX = X^3 h(X)$, o que implica $p = X^2 h(X)$, absurdo.

c) Observando que $I = \pi\big(\langle pX \rangle\big)$ e tomando $J = \langle pX \rangle + \langle X^3 \rangle = \langle pX, X^3 \rangle$, é suficiente, pelo Lema 1.12, provar que J é primário. Note que temos $J = \big\{pa_1X + pa_2X^2 + X^3h(X) : a_1, a_2 \in \mathbb{Z}_{p^2}, h(X) \in \mathbb{Z}_{p^2}[X]\big\}$. Se denotamos o coeficiente de grau i de um polinômio h por h_i, concluímos então que $h \in J$ se, e somente se, $h_0 = 0$ e $p \mid h_1, h_2$.

Sejam f, g tais que $fg \in J$. Então $f_0 g_0 = 0$. Se $f_0 = 0$ então $f^3 \in \langle X^3 \rangle$, implicando $f \in \mathrm{Rad}(J)$, e similarmente $g_0 = 0$ implica $g \in \mathrm{Rad}(J)$. Portanto vamos supor $f_0, g_0 \neq 0$, o que obriga a termos $f_0 = g_0 = p$ (pois $\mathcal{Z}(\mathbb{Z}_{p^2}) = \{0, p\}$), logo $(fg)_2 = pg_2 + pf_2 + f_1 g_1 = pa_2$, e assim $p \mid f_1 g_1$. Portanto, pelo item *a*) teremos $f_1 g_1 \in \mathcal{Z}(\mathbb{Z}_{p^2})$, logo $f_1 \in \mathcal{Z}(\mathbb{Z}_{p^2})$ ou $g_1 \in \mathcal{Z}(\mathbb{Z}_{p^2})$. De novo pelo mesmo item teremos $p \mid f_1$ ou $p \mid g_1$. Se $p \mid f_1$ então $f = p(1 + aX) + X^2 h$, logo $f^3 = 3(1 + aX)h^2 pX^4 + h^3 X^6 \in J$, e similarmente $p \mid g_1$ implica $g \in \mathrm{Rad}(J)$. □

Em contrapartida, nos anéis aritméticos vale a recíproca, ou seja, $I \subsetneq A$ ser primário, implica I irredutível. De fato se I é primário e $I = J \cap K$, então tomando $\mathfrak{p} = \mathrm{Rad}(I)$ temos $I_\mathfrak{p} = J_\mathfrak{p} \cap K_\mathfrak{p}$. Nesta situação o Lema 2.8 nos dá $I_\mathfrak{p} = J_\mathfrak{p}$ ou $I_\mathfrak{p} = K_\mathfrak{p}$ (pois $J_\mathfrak{p} \subseteq K_\mathfrak{p}$ ou $K_\mathfrak{p} \subseteq J_\mathfrak{p}$). Sem perda de generalidade vamos assumir $I_\mathfrak{p} = J_\mathfrak{p}$, logo $I^{S=A\setminus\mathfrak{p}} = I$ pela Proposição 1.45, *b*). Assim $I = I^S = J^S$ e como $J \subseteq J^S$ segue que $J \subseteq I$. Claramente o fato de $I = J \cap K$ nos dá que $J \supseteq I$ e assim $I = J$.

Por outro lado (em mais uma "virada" de eventos) mesmo o anel sendo aritmético, nem sempre é verdade que todo ideal irredutível seja primário:

Exemplo 2.16 (Anel aritmético com ideal irredutível que não é primário). Sejam $A = \mathbb{Z} + x\mathbb{Q}[X]$ e $\mathfrak{m} = 2\mathbb{Z} + x\mathbb{Q}[X]$. Note que $\mathfrak{m}$ é maximal, pois $\mathfrak{m} = \mathrm{Ker}(\phi)$, onde $\phi : A \to \mathbb{Z}_2$ é o homomorfismo de avaliação em 0, seguido da projeção em $\mathbb{Z}/2\mathbb{Z}$.

Afirmação. Todo elemento de $A_\mathfrak{m}$ é associado a algum elemento da forma $2^i X^j/1$, com $i \geq 0$ quando $j = 0$.

Demonstração. Note que $A_\mathfrak{m} \subseteq \mathbb{Q}(X)$, e a igualdade de frações é a usual. Seja $z \in \mathfrak{m}_\mathfrak{m}$, digamos $z = \dfrac{a + Xp(X)}{r + Xq(X)}$, com $r, a \in \mathbb{Z}$, r ímpar, e $p(X), q(X) \in \mathbb{Q}[X]$. Desejamos obter uma igualdade da forma

$$\frac{a + Xp(X)}{r + Xq(X)} = \frac{2^i X^j}{1} \frac{s + X\ell(X)}{t + Xu(X)},$$

para alguns i, j, alguns s, t inteiros ímpares, e alguns $\ell(X), u(X) \in \mathbb{Q}[X]$. Se $a \neq 0$ então $a = 2^n b$ para algum $n \geq 0$ e algum b ímpar, logo a igualdade desejada será

$$\frac{2^n\left(b + X(p(X)/2^n)\right)}{r + Xq(X)} = \frac{2^i X^j}{1}\,\frac{s + X\ell(X)}{t + Xu(X)},$$

a qual vale tomando $i = n, j = 0, s = b, t = r, \ell(X) = p(X)/2^n, u(X) = q(X)$. Note que neste caso $i \geq 0$. Por outro lado, se $a = 0$ então

$$z = \frac{X^m\left(2^n(c/d) + Xf(X)\right)}{r + Xq(X)},$$

para algum $m > 0$, alguns $n, c, d \in \mathbb{Z}$ com c, d ímpares, e algum $f(X) \in \mathbb{Q}[X]$. Agora a igualdade desejada será

$$\frac{2^n X^m\left(c + X(df(X)/2^n)\right)}{dr + Xdq(X)} = \frac{2^i X^j}{1}\,\frac{s + X\ell(X)}{t + Xu(X)},$$

a qual vale tomando $i = n, j = m, s = c, t = dr, \ell(X) = df(X)/2^n$ e $u(X) = dq(X)$. □

Afirmação. O anel $A_{\mathfrak{m}}$ é aritmético.

Demonstração. Demonstraremos que os ideais principais de $A_{\mathfrak{m}}$ são totalmente ordenados por inclusão, e o resultado segue do Lema 2.8. Pela Afirmação anterior os ideais principais são justamente os gerados pelos elementos $2^i X^j/1$, com $i, j \in \mathbb{Z}$ e com $i \geq 0$ quando $j = 0$.

Seja $\mathfrak{T}_0 = \left\{\left\langle \frac{2^i}{1}\right\rangle : i \geq 0\right\}$, e para $j \geq 1$ seja $\mathfrak{T}_j = \left\{\left\langle \frac{2^i X^j}{1}\right\rangle : i \in \mathbb{Z}\right\}$. Cada subfamília $\mathfrak{T}_j$ é totalmente ordenada por inclusão, a saber, $\left\langle \frac{2^i X^j}{1}\right\rangle \subseteq \left\langle \frac{2^k X^j}{1}\right\rangle$ se $k \leq i$. Se $j \geq 0$ e $i, k \in \mathbb{Z}$, com $k \geq 0$ se $j = 0$, então vale $\left\langle \frac{2^i X^{j+1}}{1}\right\rangle \subseteq \left\langle \frac{2^k X^j}{1}\right\rangle$, pois $\frac{2^i X^{j+1}}{1} = \frac{2^k X^j}{1}\,\frac{2^{i-k}X}{1}$. □

Afirmação. O ideal $I = \langle 2X/1\rangle$ é fortemente irredutível, mas não é primário.

Demonstração. A irredutibilidade forte de I decorre da ordenação demonstrada na Afirmação anterior. Note que $(2/1)(X/1) \in I$, mas $2/1 \notin I$ e $(X/1) \notin \mathrm{Rad}(I)$. Com efeito, se fosse $2/1 = 2Xp(X)/q(X)$, então retirando denominadores e avaliando em $X = 0$ seguiria $q(0) = 0$, absurdo, pois $q(X)$ tem termo independente ímpar. Também, se fosse $X^n/1 = 2Xp(X)/q(X)$ para algum $n \geq 1$, então $X^n q(X) = 2Xp(X)$, logo todos os coeficientes de $X^n q(X)$ seriam pares, e isto é absurdo pelo mesmo motivo que o caso anterior. □

Vamos dar agora um exemplo de ideal irredutível que não é fortemente irredutível. Certamente nosso candidato será um anel não aritmético pelo que foi obtido no item c) do Lema 2.10.

Exemplo 2.17 (Ideal irredutível que não é fortemente irredutível). Considere o domínio fatorial $A = \mathbb{K}[X, Y]$ com $\mathbb{K}$ um corpo e $I = \langle X^2, Y\rangle$.

Afirmação. O ideal $I = \langle X^2, Y\rangle$ é irredutível em A.

Demonstração. Tomemos J, K ideais em A tais que $J \cap K = I$. Se I fosse redutível, então existiriam $f(X, Y)$, $g(X, Y)$ tais que $f \in J \setminus I$, $g \in K \setminus I$. Reduzindo módulo I podemos tomar $f(X, Y) = a + bX$ e $g(X, Y) = c + dX$. Caso $b = 0$, então $a \in J \cap A^*$, o que implicaria $J = A$ e assim $I = K$, contradição, logo $b \neq 0$, e analogamente temos $d \neq 0$. Multiplicando por constantes convenientes podemos considerar $f(X, Y) = a + X$ e $g(X, Y) = c + X$.

Ora, $ac+(a+c)X = f(X, Y)g(X, Y)-X^2 \in JK+\langle X^2\rangle \subseteq I$, portanto $ac+(a+c)X \in I$; entretanto, se $e + fX \in I$, então $e = f = 0$. Com efeito, se $e + fX = p(X, Y)X^2 + q(X, Y)Y$, então fazendo $Y = 0$ tem-se $e + fX = p(X, 0)X^2$ e assim $e = f = 0$. Portanto $ac = 0$ e $a + c = 0$, logo $a = c = 0$, e isto implicaria $f = g = X \in J \cap K = I$, absurdo. □

Por outro lado $(X + Y)X \in \langle X^2, Y\rangle$ com $X + Y, Y$ irredutíveis em $\mathbb{K}[X, Y]$. Pelo item b) da Proposição 2.13 se $I = \langle X^2, Y\rangle$ fosse fortemente irredutível, então $X + Y \in I$ ou $Y \in I$. Mas se $X = f(X, Y)X^2 + g(X, Y)Y$, então fazendo $Y = 0$ tem-se $X = f(X, 0)X^2$, absurdo. Por outro lado, caso $X + Y = f(X, Y)X^2 + g(X, Y)Y$ implica $X\big(1 - f(X, Y)X\big) = Y\big(g(X, Y) - 1\big)$, logo $X\big(1 - f(X, 0)X\big) = 0$, absurdo.

Exemplo 2.18. Em um ideal A tal que o ideal 0 é irredutível tem-se que 0 é fortemente irredutível, pois sejam J, K cumprindo $J \cap K \subseteq 0$, então $J \cap K = 0$ e, consequentemente, $J = 0$ ou $K = 0$, logo 0 é fortemente irredutível.

Exemplo 2.19. Se D é um domínio de valorização discreta ou a imagem via um homomorfismo de um domínio de valorização discreta (pois o teorema da correspondência preserva inclusão), então todo ideal de A é fortemente irredutível. Como caso particular, se k é um corpo então o anel $k[[X]]$ de séries formais de potências com coeficientes em K é um domínio de valorização discreta (vide o Exemplo 1.65). Segue que todo ideal de $k[[X]]$ é fortemente irredutível e, para todo $n \geq 1$, todo ideal de $k[[X]]/\langle X^n\rangle$ também será fortemente irredutível.

Se I é fortemente irredutível em um anel noetheriano A, então é irredutível, logo será primário pelo Corolário 1.16, e assim $\mathrm{Rad}(I)$ é primo. Afirmamos que esta última conclusão vale também no caso em que A é aritmético.

Proposição 2.20. *Em um anel aritmético todo ideal fortemente irredutível possui radical primo.*

Demonstração. Seja I um ideal fortemente irredutível em um anel aritmético A. Pelo item d) do Lema 2.10 temos que $\mathcal{Z}_A(A/I) = \mathfrak{p}$ é primo. Pelo Lema 2.8 temos que $\mathrm{Spec}(A_\mathfrak{p})$ é totalmente ordenado por inclusão, logo pela Proposição 1.45, d) o mesmo acontece com a família $\mathcal{F}$ dos ideais primos em A contidos em $\mathfrak{p}$.

Por outro lado, se $\mathcal{M}$ é a família dos primos minimais sobre I então temos $\mathrm{Rad}(I) = \cap\mathcal{M}$ pela Proposição 1.30; mas pelo Corolário 1.53 temos $\mathfrak{q} \subseteq \mathcal{Z}_A(A/I)$ para cada $\mathfrak{q} \in \mathcal{M}$, logo $\mathcal{M} \subseteq \mathcal{F}$, e assim $\mathcal{M}$ também será uma cadeia de ideais; já que $\mathcal{M}$ consiste de ideais minimais, então necessariamente $\mathcal{M}$ só contém um membro, logo pela Proposição 1.30 obtemos que $\mathrm{Rad}(I)$ é primo. □

Exemplo 2.21 (Ideal fortemente irredutível cujo radical não é primo). Seja $(A, \mathfrak{m})$ um anel local com mais de um primo minimal, o que implica que $\mathrm{Rad}(0_A)$ não é primo, pela Proposição 1.30. Sejam $E = E(A/\mathfrak{m})$ o envelope injetivo do A-módulo $A/\mathfrak{m}$ e $R = A(+)E$ a idealização do A-módulo E. Note que $A/\mathfrak{m} \subseteq E$ e $A/\mathfrak{m}$ é um A-módulo simples (isto é, para qualquer elemento não-nulo $x \in A/\mathfrak{m}$ temos $Ax = A/\mathfrak{m}$), portanto o fato de E ser uma extensão essencial nos permite concluir que dado um submódulo $F \neq 0$ de E temos $F \cap A/\mathfrak{m} \neq 0$ e assim $A/\mathfrak{m} \subseteq F$.

Afirmação. O anulador da extensão E é trivial.

Demonstração. Suponhamos, por contradição, que exista $x \in \mathrm{Ann}(E)$ com $x \neq 0$. Definamos $\phi : \langle x \rangle \to E$ dada por $\phi(ax) = a \cdot \overline{1} = \overline{a} \in A/\mathfrak{m}$. Devemos verificar que a aplicação ϕ está bem definida, ou seja, se $ax = bx$, então $\overline{a} = \overline{b}$; mas se $(a-b)x = 0$, segue que $a - b$ não é invertível em A e portanto $a - b \in \mathfrak{m}$. Evidentemente ϕ é A-linear, e portanto pela injetividade de E temos que ϕ pode ser estendido a um homomorfismo $\varphi : A \to E$, mas seguiria então $\varphi(x) = \phi(1 \cdot x) = 1 \cdot \overline{1} = \overline{1}$, mas também $\varphi(x) = \varphi(x \cdot 1) = x\varphi(1) = 0$, pois $\varphi(1) \in E$ e $x \in \mathrm{Ann}(E)$, contradição. Logo $\mathrm{Ann}(E) = 0$. □

Afirmação. Todo ideal não-nulo de R contém $(0, \overline{1})$.

Demonstração. É suficiente demonstrar o resultado para ideais principais gerados por um elemento não-nulo. Tomemos $0 \neq (a, e) \in R$. Se $a = 0$, então $e \neq 0$, logo $Ae \neq 0$ e assim $A/\mathfrak{m} \subseteq Ae$, portanto podemos escrever $\overline{1} = ye$ com $y \in A$, logo

$$(y, 0)(a, e) = (y, 0)(0, e) = (0, ye) = (0, \overline{1}).$$

Se $a \neq 0$, então pela Afirmação anterior $aE \neq 0$ e, consequentemente, $A/\mathfrak{m} \subseteq aE$. Sendo $\overline{1} = az$ com $z \in E$ temos:

$$(0, z)(a, e) = (0, za) = (0, \overline{1}). \quad \square$$

Como consequência da última Afirmação deduzimos que o ideal 0_R é irredutível, logo fortemente irredutível pelo Exemplo 2.18. Por outro lado, da Proposição 1.38 concluímos que $\mathrm{Rad}(0_R)$ não é primo, pois $\mathrm{Rad}(0_A)$ não o é.

Para concluir o exemplo vamos apresentar um anel A satisfazendo as hipóteses, ou seja, A local com mais de um primo minimal. Considere $B = \mathbb{Z}[X]$ e os ideais $\mathfrak{p}_1 = \langle 2 \rangle, \mathfrak{p}_2 = \langle X \rangle$. Como 2 e X são primos em B segue que $\mathfrak{p}_1$ e $\mathfrak{p}_2$ são ideais primos. Convém observar que eles não são comaximais, pois $1 \notin \mathfrak{p}_1 + \mathfrak{p}_2$ uma vez que 1 é um polinômio (constante) com termo independente ímpar. Seja $J = \mathfrak{p}_1 \cap \mathfrak{p}_2$. Se $\mathfrak{p} \in \mathrm{Spec}(B)$ e $\mathfrak{p} \supseteq J$, então $\mathfrak{p} \supseteq \mathfrak{p}_1$ ou $\mathfrak{p} \supseteq \mathfrak{p}_2$, ademais se ocorresse $\mathfrak{p} \subseteq \mathfrak{p}_1$, então $\mathfrak{p}$ não poderia conter $\mathfrak{p}_2$, pois $\mathfrak{p}_1, \mathfrak{p}_2$ não estão contidos um no outro, logo $\mathfrak{p} = \mathfrak{p}_1$; analogamente, se $\mathfrak{p} \subseteq \mathfrak{p}_2$ então $\mathfrak{p} = \mathfrak{p}_2$. Concluímos então (pelo teorema da correspondência) que $\mathfrak{q}_1 = \mathfrak{p}_1/J$ e $\mathfrak{q}_2 = \mathfrak{p}_2/J$ são primos minimais e não comaximais em B/J. Tomando-se $\mathfrak{m} \in \mathrm{Spec}(B/J)$ tal que $\mathfrak{q}_1 + \mathfrak{q}_2 \subseteq \mathfrak{m}$ tem-se $(\mathfrak{q}_1)_\mathfrak{m}$ e $(\mathfrak{q}_2)_\mathfrak{m}$ primos minimais distintos no anel local $A = (B/J)_\mathfrak{m}$.

2.2 Ideais fortemente irredutíveis em anéis noetherianos

Teorema 2.22. *Seja $(A, \mathfrak{m})$ um anel local, e seja I um ideal fortemente irredutível, satisfazendo $I \subsetneq (I : \mathfrak{m})$. Então:*

a) $(I : \mathfrak{m})$ *é um ideal principal gerado por qualquer elemento de* $(I : \mathfrak{m}) \setminus I$.

b) $I = (I : \mathfrak{m})\mathfrak{m}$.

c) Para quaisquer ideal $J \subseteq A$ vale $J \subseteq I$ ou $(I : \mathfrak{m}) \subseteq J$.

Demonstração. Seja $x \in (I : \mathfrak{m}) \setminus I$ qualquer.

a) Provaremos no próximo parágrafo que vale $(I : \mathfrak{m}) = \langle x \rangle \cup I$; já que a união de dois ideais é um ideal se, e somente, se, um deles está contido no outro, segue que $(I : \mathfrak{m}) = \langle x \rangle$ ou $(I : \mathfrak{m}) = I$, logo devemos ter $(I : \mathfrak{m}) = \langle x \rangle$ pelas hipóteses.

Seja $y \in (I : \mathfrak{m}) \setminus \langle x \rangle$. Pelo Lema 1.22 vale $\langle x \rangle \cap \langle y \rangle = y\,(x : y)$; contudo $y \notin \langle x \rangle$ implica $(x : y) \neq A$ e portanto $(x : y) \subseteq \mathfrak{m}$, logo $\langle x \rangle \cap \langle y \rangle = y\,(x : y) \subseteq (I : \mathfrak{m})\mathfrak{m} \subseteq I$. Pela hipótese que I é fortemente irredutível segue que $\langle x \rangle \subseteq I$ ou $\langle y \rangle \subseteq I$, logo necessariamente $y \in I$ pois $x \notin I$.

b) Pelo fato de que $I \subseteq (I : \mathfrak{m}) = \langle x \rangle$, segue do Lema 1.22 que $I = x\,(I : x)$. Temos $\mathfrak{m} \subseteq (I : x)$, uma vez que $\mathfrak{m}\langle x \rangle = \mathfrak{m}(I : \mathfrak{m}) \subseteq I$. Assim $(I : x) = \mathfrak{m}$ ou $(I : x) = A$ (pois A é local com ideal maximal $\mathfrak{m}$); entretanto $x \cdot 1 = x \notin I$, assim $(I : x) \neq A$, o que implica $\mathfrak{m} = \big(I : x)$ e, consequentemente, $I = x\,(I : x) = x\mathfrak{m} = (I : \mathfrak{m})\mathfrak{m}$.

c) Seja J um ideal tal que $(I : \mathfrak{m}) = \langle x \rangle \nsubseteq J$. Então para qualquer $z \in J$ vale $(z : x) \neq A$, e assim vamos ter (pelo Lema 1.22) $\langle x \rangle \cap \langle z \rangle = x\,(z : x) \subseteq \langle x \rangle \mathfrak{m} = I$. Assim $\langle z \rangle \subseteq I$, pois $x \notin I$ e I é fortemente irredutível, o que prova a inclusão $J \subseteq I$. □

Uma aplicação do resultado anterior é o seguinte: Um ideal $I \subseteq A$ é dito **abrigado** se existe um elemento mínimo no conjunto dos submódulos **não-nulos** do A-módulo A/I, ou, equivalentemente, no conjunto dos ideais contendo estritamente o ideal I. Portanto, sob a hipótese de $A = (A, \mathfrak{m})$ ser local e I um ideal fortemente irredutível com $I \subsetneq (I : \mathfrak{m})$, temos que I é abrigado. De fato, o ideal $(I : \mathfrak{m})$ será o mínimo entre os ideais contendo estritamente I pelo item *c*) do Teorema anterior.

Corolário 2.23. *Sejam $(A, \mathfrak{m})$ um anel local noetheriano e $I \neq \mathfrak{m}$ um ideal fortemente irredutível e $\mathfrak{m}$-primário. Então valem*

$$I = \cup \left\{K : K \text{ é ideal e } K \subsetneq (I : \mathfrak{m})\right\};$$
$$(I : \mathfrak{m}) = \cap \left\{J : J \text{ é ideal e } I \subsetneq J\right\}.$$

Consequentemente, os ideais I e $(I : \mathfrak{m})$ são comparáveis com qualquer ideal de A.

Demonstração. Temos $I \subsetneq (I : \mathfrak{m})$ por *c*) do Corolário 1.33, e assim por *c*) do Teorema 2.22 segue que para todo ideal L em A vale $L \subseteq I$ ou $(I : \mathfrak{m}) \subseteq L$; no primeiro caso, também valerá $L \subseteq (I : \mathfrak{m})$ pois $I \subseteq (I : \mathfrak{m})$, e similarmente no segundo caso teremos $L \supseteq I$, o que demonstra a última afirmação do enunciado.

Pela hipótese I é um ideal K satisfazendo $K \subsetneq (I : \mathfrak{m})$; reciprocamente, se $K \subsetneq (I : \mathfrak{m})$ então $(I : \mathfrak{m}) \nsubseteq K$, implicando $K \subseteq I$, o que mostra a primeira igualdade. Para a segunda igualdade, se um ideal J satisfaz $I \subsetneq J$, então $J \nsubseteq I$, logo $(I : \mathfrak{m}) \subseteq J$; assim, $(I : \mathfrak{m}) \subseteq \cap \left\{J : J \text{ é ideal e } I \subsetneq J\right\}$. Como $I \subsetneq (I : \mathfrak{m})$, então a inclusão oposta se verifica e o resultado segue. □

Corolário 2.24. *Seja I um ideal fortemente irredutível em um anel noetheriano A, com $\mathrm{Rad}(I) = \mathfrak{p}$, e tal que $I \neq \mathfrak{p}$. Considerando o conjunto multiplicativo $S = A \setminus \mathfrak{p}$, então:*

a) *$(I : \mathfrak{p})_S$ é um ideal principal e $\mathrm{ht}(I) \leq 1$.*

b) *$I_S = \big((I : \mathfrak{p})\mathfrak{p}\big)_S$.*

c) *Para todo ideal $J \subseteq A$ segue que $J \subseteq I$ ou $(I : \mathfrak{p})_S \subseteq J_S$.*

Demonstração. Sendo I fortemente irredutível segue que I é irredutível, e como A é noetheriano, então I é primário, ou seja, I será $\mathfrak{p}$-primário. Pelo item *g*) do Lema 2.10 o ideal I_S será fortemente irredutível.

Por outro lado, valem $(I : \mathfrak{p})_S = (I_S : \mathfrak{p}_S)$ (Corolário 1.50) e $\big((I : \mathfrak{p})\mathfrak{p}\big)_S = (I_S : \mathfrak{p}_S)\mathfrak{p}_S$ [†]. Portanto, exceto pela a afirmação "$\operatorname{ht}(I) \leq 1$", todos os outros resultados enunciados decorrerão do Teorema 2.22, desde que a hipótese $I_S \subsetneq (I_S : \mathfrak{p}_S)$ seja satisfeita (Note: se $(I : \mathfrak{p})_S \not\subseteq J_S$, então teremos $J_S \subseteq I_S$, logo $J \subseteq J^S \subseteq I^S = I$, pela Proposição 1.45, b)). Mas isto é verdade, pois $\mathfrak{p}_S = \operatorname{Rad}(I_S)$ pela Proposição 1.48, c), logo podemos aplicar o item c) do Corolário 1.33.

Finalmente, pelo teorema da altura de Krull (Teorema 1.60), existe um ideal primo $\mathfrak{q}$ em A com $\mathfrak{q} \subseteq \mathfrak{p}$ tal que $(I : \mathfrak{p})_S \subseteq \mathfrak{q}_S$ e tal que $\operatorname{ht}(\mathfrak{q}_S) \leq 1$. Portanto $I \subseteq I^S \subseteq (I : \mathfrak{p})^S \subseteq \mathfrak{q}$, e vale $\operatorname{ht}\mathfrak{q} = \operatorname{ht}(\mathfrak{q}_S)$ (pois $A_\mathfrak{q}$ é isomorfo, como anel, a $(A_S)_{\mathfrak{q}_S}$), o que prova que $\operatorname{ht}(I) \leq 1$. □

Observação 2.25.

(1) Seja I um ideal fortemente irredutível e não primo em um anel noetheriano A. Se $\mathfrak{p} = \operatorname{Rad}(I)$, então o ideal $I_\mathfrak{p}$ em $A_\mathfrak{p}$ satisfaz:

- $(I_\mathfrak{p} : \mathfrak{p}_\mathfrak{p})$ é principal.
- $I_\mathfrak{p} = \mathfrak{p}_\mathfrak{p}(I_\mathfrak{p} : \mathfrak{p}_\mathfrak{p})$.
- $I_\mathfrak{p}$ e $(I_\mathfrak{p} : \mathfrak{p}_\mathfrak{p})$ são comparáveis com qualquer ideal de $A_\mathfrak{p}$.

Com efeito, note que I é primário, logo $\mathfrak{p}$ é primo, e assim $I \neq \mathfrak{p}$ pela hipótese. As afirmações decorrem então do Corolário 2.24.

(2) Seja I um ideal fortemente irredutível e não primo em um anel local noetheriano $(A, \mathfrak{m})$. Se I é $\mathfrak{m}$-primário, então I é comparável com qualquer ideal de A. Com efeito, como $\mathfrak{m} = \operatorname{Rad}(I)$, segue do Corolário 1.33, c) que $I \subsetneq (I : \mathfrak{m})$, e assim o resultado segue do Teorema 2.22, c). O recíproco não é verdadeiro: o ideal nulo é comparável com qualquer ideal de um anel, e pode nem ser irredutível.

Proposição 2.26. *Seja A um anel noetheriano. Um ideal I de A é não primo e fortemente irredutível se, e somente se, existem ideais L e $\mathfrak{p}$ tais que $I \subsetneq L \subseteq \mathfrak{p}$, e satisfazendo:*

(1) *$\mathfrak{p}$ é primo.*

(2) *I é $\mathfrak{p}$-primário.*

(3) *Para qualquer ideal $J \subseteq A$ temos $J \subseteq I$ ou $L_\mathfrak{p} \subseteq J_\mathfrak{p}$.*

Em tal caso vale $L_\mathfrak{p} = (I_\mathfrak{p} : \mathfrak{p}_\mathfrak{p})$.

[†] Se $I_1, \ldots, I_n$ são ideais de um anel A, então $(I_1 \cdots I_n)_S = (I_1)_S \cdots (I_n)_S$. A prova é inteiramente similar à prova do item a) da Proposição 1.48.

Demonstração. Se I é não primo e fortemente irredutível, definimos $\mathfrak{p} = \mathrm{Rad}(I)$ e $L = (I : \mathfrak{p})$. Então $I \subsetneq L$ pelo Corolário 1.33, *c*). Se fosse $L = A$ então $\mathfrak{m} \subseteq I$, logo $I = A$ ou $I = \mathfrak{m}$, o que é impossível (no primeiro caso, pela definição de ideal fortemente irredutível; no segundo caso, pela hipótese de I ser não primo). Isto mostra que vale $L \subseteq \mathfrak{p}$. A condição de comparabilidade decorre do Corolário 2.24, *c*).

Reciprocamente, sejam L um ideal, $\mathfrak{p}$ um ideal primo, e seja I cumprindo as condições (1)-(3) do enunciado. Como $I \subsetneq L \subseteq \mathfrak{p} = \mathrm{Rad}(I)$, então I não é primo. Ora, pelo item *c*) do Lema 2.10, se demonstrarmos que $I_\mathfrak{p}$ é fortemente irredutível, então I^S o será, onde $S = A \setminus \mathfrak{p}$. Como $I^S = I$ pela Proposição 1.45, *b*), nosso trabalho estará feito.

Se $I_\mathfrak{p}$ não fosse fortemente irredutível, então existiriam ideais J, K em A tais que $J_\mathfrak{p} \cap K_\mathfrak{p} \subseteq I_\mathfrak{p}$, mas $J_\mathfrak{p} \nsubseteq I_\mathfrak{p}$ e $K_\mathfrak{p} \nsubseteq I_\mathfrak{p}$. Então $J, K \nsubseteq I$, logo necessariamente $L_\mathfrak{p} \subseteq J_\mathfrak{p}, K_\mathfrak{p}$, ou seja $L_\mathfrak{p} \subseteq J_\mathfrak{p} \cap K_\mathfrak{p} \subseteq I_\mathfrak{p}$, e contraindo obteríamos $L \subseteq L^S \subseteq I^S = I$, absurdo. Finalmente, nesta situação o ideal $\hat{L} = (I : \mathfrak{p})$ também satisfará, para cada ideal J, a dicotomia $J \subseteq I$ ou $\hat{L}_\mathfrak{p} \subseteq J_\mathfrak{p}$, pelo Corolário 2.24, *c*). Como $L \nsubseteq I$ então $\hat{L}_\mathfrak{p} \subseteq L_\mathfrak{p}$, e como $\hat{L} \nsubseteq I$, então $L_\mathfrak{p} \subseteq \hat{L}_\mathfrak{p}$, o que mostra a igualdade $L_\mathfrak{p} = \hat{L}_\mathfrak{p} = (I_\mathfrak{p} : \mathfrak{p}_\mathfrak{p})$. □

Corolário 2.27. *Seja I um ideal irredutível em um anel local noetheriano $(A, \mathfrak{m})$, e suponha que I é $\mathfrak{m}$-primário. Então I é fortemente irredutível se, e somente se, I é comparável com qualquer ideal em A.*

Demonstração. Se I é primo, então $I = \mathrm{Rad}(I) = \mathfrak{m}$, e o resultado segue trivialmente, logo podemos supor que I não é primo. Neste caso, a implicação direta segue do item (2) da Observação 2.25. Para o reciproco, suponha que I é comparável com qualquer ideal em A. Mostraremos então que as condições (1)-(3) da Proposição 2.26 valem tomando $L = (I : \mathfrak{m})$ e $\mathfrak{p} = \mathfrak{m}$. As inclusões $I \subsetneq L \subseteq \mathfrak{p}$ se provam como no primeiro parágrafo da prova da Proposição 2.26, e claramente (1) e (2) são satisfeitas. Finalmente, seja J um ideal em A. Se $J \subseteq I$, estamos prontos; caso contrário, existe $z \in J$ com $\langle z \rangle \nsubseteq I$, logo $I \subsetneq \langle z \rangle$ pela hipótese de comparabilidade do ideal I. Seja $x \in (I : \mathfrak{m})$. Se $x \in I$, então $x \in \langle z \rangle$; caso contrário, teremos $\langle x \rangle \nsubseteq I$, logo $I \subsetneq \langle x \rangle$. Como I é irredutível, então $I \subsetneq \langle x \rangle \cap \langle z \rangle$, digamos $ax = bz \notin I$. Já que $x\mathfrak{m} \subseteq I$, então necessariamente vale $a \notin \mathfrak{m}$, isto é, $a \in A^*$, o que implica $x = a^{-1}bz \in \langle z \rangle$. Isto prova que vale $(I : \mathfrak{m}) \subseteq \langle z \rangle \subseteq J$. □.

Proposição 2.28. *Seja A um anel noetheriano e I um ideal fortemente irredutível. Suponhamos que* $\mathrm{Rad}(I) = \mathfrak{p} \neq I$ *e* $\mathrm{ht}(\mathfrak{p}) > 0$. *Então $I_\mathfrak{p}$ é um ideal regular.*

Demonstração. Seja $J = I_\mathfrak{p}$. Pelo item *a*) da Proposição 1.33 é necessário e suficiente provarmos que vale, na localização $A_\mathfrak{p}$, a igualdade $(0 : J) = 0$. Ora, temos que I é primário pelo Lema 2.10, *a*), logo por *g*) do mesmo segue que $J = I_\mathfrak{p}$ é fortemente irredutível. Se $\mathfrak{m} = \mathfrak{p}_\mathfrak{p}$, então também temos

- $\mathrm{ht}(\mathfrak{m}) = \mathrm{ht}(\mathfrak{p}) > 0$, pela Proposição 1.45, *b*).

- $\mathrm{Rad}(J) = \mathrm{Rad}(I)_{\mathfrak{p}} = \mathfrak{m}$, pela Proposição 1.48, *c*).
- $J \subsetneq (J : \mathfrak{m})$, por *c*) do Corolário 1.33.
- Tomando $S = A \setminus \mathfrak{p}$ temos que I e $\mathfrak{p}$ são S-saturados, por *b*) da Proposição 1.45. Como $I \subsetneq \mathfrak{p}$, segue do item *a*) da mesma Proposição que $I_S \subsetneq \mathfrak{p}_S$, isto é, $J \subsetneq \mathfrak{m}$. Consequentemente teremos $(J : \mathfrak{m}) \subseteq \mathfrak{m}$.

Seja $K = \bigcup\{(0 : J^n) : n \in \mathbb{N}\}$. Então $(J : \mathfrak{m}) \subseteq K$ ou $K \subseteq J$ pelo Teorema 2.22, *c*). Se fosse $(J : \mathfrak{m}) \subseteq K$, então pelo fato do ideal $(J : \mathfrak{m})$ ser finitamente gerado (pois $A_{\mathfrak{p}}$ é anel noetheriano) e pelo fato da união dos ideais $(0 : J^n)$ ser crescente, concluiríamos que para algum k vale $(J : \mathfrak{m}) \subseteq (0 : J^k)$, e assim $J^{k+1} \subseteq J^k(I : \mathfrak{m}) \subseteq J^k(0 : J^k) = 0$. Consequentemente $\mathrm{Rad}(0) = \mathrm{Rad}(J^{k+1}) = \mathrm{Rad}(J)$[♠] $= \mathfrak{m}$, logo $\mathfrak{m}$ seria o único primo minimal de $A_{\mathfrak{p}}$ (pela Proposição 1.30), e assim $\mathrm{ht}(\mathfrak{m}) = 0$, o que é absurdo.

Assim, temos $K \subseteq J$. Consideremos, no anel $A_{\mathfrak{p}}$, uma decomposição primária do ideal nulo, digamos $0 = \bigcap \mathfrak{q}$, e seja $\mathcal{G} = \{\mathfrak{q} : \mathrm{Rad}(\mathfrak{q}) \not\supseteq J\}$. Pela Proposição 1.34 vale $K = \bigcap_{\mathfrak{q}\in\mathcal{G}} \mathfrak{q}$. Por outro lado, o Teorema 2.22 nos dá $(J : \mathfrak{m}) = \langle x\rangle$ para algum $x \in (J : \mathfrak{m}) \subseteq \mathfrak{m}$, e portanto $0 \subseteq K \subseteq J \subseteq (J : \mathfrak{m}) = \langle x\rangle$. Se $\mathfrak{q} \in \mathcal{G}$ então $J \nsubseteq \mathrm{Rad}(\mathfrak{q})$, implicando $x \notin \mathrm{Rad}(\mathfrak{q})$. Consequentemente, para qualquer y tal que $yx \in \mathfrak{q}$ teremos $y \in \mathfrak{q}$ (pois $\mathfrak{q}$ é primário e $x \notin \mathrm{Rad}(\mathfrak{q})$). Assim, $(\mathfrak{q} : x) = \mathfrak{q}$, logo

$$\begin{aligned}(K : x) &= \left(\bigcap_{\mathfrak{q}\in\mathcal{G}} \mathfrak{q} : x\right)\\ &= \bigcap_{\mathfrak{q}\in\mathcal{G}} (\mathfrak{q} : x)\\ &= \bigcap_{\mathfrak{q}\in\mathcal{G}} \mathfrak{q}\\ &= K\,.\end{aligned}$$

Finalmente, pelo Lema 1.22 temos $K = x(K : x) = xK$; como A é local e $x \in \mathfrak{m}$, o lema de Nakayama implica $(0 : J) \subseteq K = 0$. □

Lema 2.29. *Seja A um anel local e I um ideal. Se alguma potência do ideal I é principal, então ou bem I será principal, ou bem I consistirá de divisores de zero. Equivalentemente, se I é regular então I será principal.*

Demonstração. Consulte (SALLY, 1975, Proposition 1). □

Teorema 2.30. *Seja A um anel noetheriano, e seja I um ideal não primo de A com* $\mathrm{ht}(I) > 0$. *Então I é fortemente irredutível se e somente se valem:*

♠ Usamos a identidade $\mathrm{Rad}(I_1)\cdots\mathrm{Rad}(I_n) = \mathrm{Rad}(I_1)\cap\cdots\cap\mathrm{Rad}(I_n)$.

- $\mathfrak{p} = \mathrm{Rad}(I)$ *é primo;*
- I *é* ($\mathfrak{p}$-)*primário;*
- *A localização* $A_\mathfrak{p}$ *é um domínio de valorização discreta;*
- $I = \mathfrak{p}^n$ *para algum* $n > 1$.

Demonstração.

($\Leftarrow$) Como $A_\mathfrak{p}$ é um domínio de valorização discreta, então os ideais de $A_\mathfrak{p}$ são totalmente ordenados por inclusão (pelo Corolário 1.64), e portanto $I_\mathfrak{p}$ é fortemente irredutível pelo Lema 2.6. Ainda, I será $\mathfrak{p}$-primário por a) do Lema 2.10, logo I será fortemente irredutível pelo item h) do mesmo Lema.

($\Rightarrow$) Sejam $J = I_\mathfrak{p}$ e $\mathfrak{m} = \mathfrak{p}_\mathfrak{p}$. Como I não é primo, então $I \neq \mathfrak{p} = \mathrm{Rad}(I)$, e como $\mathfrak{p} \supseteq I$, então $\mathrm{ht}(\mathfrak{p}) \geq \mathrm{ht}(I) > 0$. Isto mostra que valem as hipóteses da Proposição 2.28. Argumentando como na primeira parte da prova deste resultado, obtemos então que J é fortemente irredutível em $A_\mathfrak{p}$ (logo $\mathfrak{m}$-primário), $\mathrm{Rad}(J) = \mathfrak{m}$ e $J \subsetneq (J : \mathfrak{m}) \subseteq \mathfrak{m}$. Ainda, temos $\mathrm{ht}(J) = \mathrm{ht}(\mathfrak{q}_\mathfrak{p})$ para algum ideal primo $\mathfrak{q}$ em A contido em $\mathfrak{p}$. Tomando $S = A \setminus \mathfrak{p}$ e contraindo na inclusão $J = I_\mathfrak{p} \subseteq \mathfrak{q}_\mathfrak{p}$ obtemos $I^S \subseteq \mathfrak{q}^S$, e como $I = I^S, \mathfrak{q} = \mathfrak{q}^S$ por b) da Proposição 1.45, segue que $I \subseteq \mathfrak{q}$. Consequentemente temos $\mathrm{ht}(J) = \mathrm{ht}(\mathfrak{q}_\mathfrak{p}) = \mathrm{ht}(\mathfrak{q}) \geq \mathrm{ht}(I) > 0$.

Ora, pelo item a) do Corolário 2.24 vale $\mathrm{ht}(J) \leq 1$, logo $\mathrm{ht}(J) = 1$, e ainda J é regular pela Proposição 2.28. Como $J \subsetneq (J : \mathfrak{m})$, então pelos itens a) e b) da Proposição 2.22 valem $(J : \mathfrak{m}) = \langle x \rangle$ e $I = x\mathfrak{m}$, para algum $x \in A_\mathfrak{p} \setminus J$. Pelo teorema da interseção de Krull temos $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = 0$ (vide (EISENBUD, 1995, Corollary 5.4)), logo existe $k \geq 1$ tal que $x \in \mathfrak{m}^k \setminus \mathfrak{m}^{k+1}$, e assim $I = x\mathfrak{m} \subseteq \mathfrak{m}^{k+1}$.

Se $\mathfrak{m}^k$ não fosse principal, então existiria $y \in \mathfrak{m}^k \setminus \mathfrak{m}^{k+1}$ de modo que $x \notin \langle y \rangle$ e $y \notin \langle x \rangle$. Com efeito: como $x \in \mathfrak{m}^k$ e $\mathfrak{m}^k$ não é principal, então existe $z \in \mathfrak{m}^k \setminus \langle x \rangle$. Se $z \notin \mathfrak{m}^{k+1}$, definimos $y = z$; caso contrário, definimos $y = z + x$, e vemos facilmente que em qualquer dos dois casos vale $y \in \mathfrak{m}^k \setminus \left(\mathfrak{m}^{k+1} \cup \langle x \rangle\right)$. Finalmente, se valesse $x \in \langle y \rangle$, digamos $x = by$, então não poderíamos ter $b \in A_\mathfrak{p}^*$, pois isto implicaria $y \in \langle x \rangle$. Assim $b \in \mathfrak{m}$, logo $y \in x\mathfrak{m} \subseteq \mathfrak{m}^{k+1}$, o que é absurdo.

Como $J \subseteq \mathfrak{m}^{k+1}$ então $y \notin J$, e por construção $x \notin J$; por outro lado, vale $\langle x \rangle \cap \langle y \rangle = x(y : x)$ Pelo Lema 1.22, e como $x \in (J : \mathfrak{m})$ e $(x : y) \subseteq \mathfrak{m}$ (pois $y \notin \langle x \rangle$, logo $(x : y) \neq A_\mathfrak{p}$), segue que $\langle x \rangle \cap \langle y \rangle \subseteq (J : \mathfrak{m})\mathfrak{m} \subseteq J$, o que contradiz o fato do ideal J ser fortemente irredutível.

O anterior mostra que $\mathfrak{m}^k$ é principal, e como $\mathfrak{m} \supseteq J$ e J é um ideal regular (pela Proposição 2.28), segue que $\mathfrak{m}$ também é regular. Aplicando o Lema anterior

concluímos que $\mathfrak{m}$ é principal, logo $A_{\mathfrak{p}}$ é um domínio de valorização discreta[¶], e em particular teremos $J = \mathfrak{m}^n$ para algum $n > 1$ (lembremos que vale $J \neq \mathfrak{m}$). Se $w \in \mathfrak{p}$ é tal que o elemento $w/1$ gera o ideal $\mathfrak{m}$, isto é, $\mathfrak{m} = \langle w \rangle_S$, então contraindo obtemos $\mathfrak{p} = \mathfrak{m}^S = \langle w \rangle^S$, logo $I = J^S = \langle w^n/1 \rangle^S = \langle w^n \rangle^S = \mathfrak{p}^n$. □

[¶] Não é possível aplicar a Proposição 1.63, pois ela assume que o anel em questão já é um domínio. Para remediar isto, apelamos a um resultado mais forte, que afirma o seguinte: se um anel local é noetheriano, e seu ideal maximal é gerado por um elemento não nilpotente, então o anel será um domínio de valorização discreta. Em nossa situação o gerador do ideal $\mathfrak{m}$ não pode ser nilpotente, pois em tal caso teríamos $\mathfrak{m}^j = 0$ para algum $j \geq 1$, logo $\mathrm{Rad}(0) = \mathrm{Rad}(\mathfrak{m})^j = \mathfrak{m}$, o que é absurdo. A prova do fato mencionado encontra-se em (SERRE, 1968, Chapitre I, Proposition 2).

REFERÊNCIAS

ALTMAN, A.; KLEIMAN, S. *A Term of Commutative Algebra*. [S.l.]: Worldwide Center of Mathematics, LLC, 2013. ISBN 9780988557215. Citado 2 vezes nas páginas 9 e 22.

ANDERSON, D. D.; WINDERS, M. Idealization of a module. *Journal of Commutative Algebra*, v. 1, n. 1, p. 3–56, 2009. ISSN 1939-0807. Citado na página 22.

BORGES, H.; TENGAN, E. *Álgebra comutativa em quatro movimentos*. [S.l.]: IMPA, Rio de Janeiro, 2015. 490 p. ISBN 9788524403989. Citado 2 vezes nas páginas 9 e 32.

EISENBUD, D. *Commutative algebra*. [S.l.]: Springer-Verlag, New York, 1995. v. 150. xvi+785 p. (Graduate Texts in Mathematics, v. 150). With a view toward algebraic geometry. ISBN 0-387-94268-8; 0-387-94269-6. Citado 3 vezes nas páginas 9, 24 e 53.

GILMER, R. *Multiplicative ideal theory*. [S.l.]: Queen's University, Kingston, ON, 1992. v. 90. xii+609 p. (Queen's Papers in Pure and Applied Mathematics, v. 90). Corrected reprint of the 1972 edition. Citado na página 10.

HEINZER, W. J.; RATLIFF JR., L. J.; RUSH, D. E. Strongly irreducible ideals of a commutative ring. *Journal of Pure and Applied Algebra*, v. 166, n. 3, p. 267–275, 2002. ISSN 0022-4049. Citado na página 8.

JENSEN, C. U. Arithmetical rings. *Acta Mathematica Academiae Scientiarum Hungaricae*, v. 17, p. 115–123, 1966. ISSN 0001-5954. Citado 2 vezes nas páginas 8 e 38.

LAM, T. Y.; REYES, M. L. Oka and Ako ideal families in commutative rings. In: *Rings, modules and representations*. [S.l.]: Amer. Math. Soc., Providence, RI, 2009, (Contemp. Math., v. 480). p. 263–288. Citado na página 15.

SALLY, J. D. On the number of generators of powers of an ideal. *Proceedings of the American Mathematical Society*, v. 53, n. 1, p. 24–26, 1975. ISSN 0002-9939. Citado na página 52.

SERRE, J.-P. *Corps locaux*. [S.l.]: Hermann, Paris, 1968. 245 p. Deuxième édition, Publications de l'Université de Nancago, No. VIII. Citado na página 54.