Universidade Federal de São Carlos
Centro de Ciências Exatas e de Tecnologia
Departamento de Matemática

Introdução à Geometria Algébrica

Autor: Fernanda Scabio Gonçalves

Orientador: Luciene Nogueira Bertoncello

Disciplina: Trabalho de Conclusão de Curso B

Profs Responsáveis: Ivo Machado da Costa
Liane Bordignon
Vera Lúcia Carbone

São Carlos, 17 de dezembro de 2010.

Introdução à Geometria Algébrica

Autor: Fernanda Scabio Gonçalves

Orientador: Luciene Nogueira Bertoncello

Disciplina: Trabalho de Conclusão de Curso B

Profs Responsáveis: Ivo Machado da Costa
Liane Bordignon
Vera Lúcia Carbone

São Carlos, 17 de dezembro de 2010.

Fernanda Scabio Gonçalves

Luciene Nogueira Bertoncello

Resumo

Este trabalho reúne os conceitos e resultados básicos de Geometria Algébrica, visando a familiaridade com esta teoria e o domínio de seus resultados fundamentais. O estudo foi desenvolvido em duas etapas. Na primeira delas, referente ao Trabalho de Conclusão de Curso A, são abordados resultados gerais de Álgebra Comutativa, como anéis e homomorfismos, ideais e operações e extensão e contração de ideais. Também são apresentados os conceitos de módulos, sequências exatas, condições de cadeia e anéis Noetherianos, com destaque ao *Teorema da Base de Hilbert*. A segunda etapa, que corresponde ao Trabalho de Conclusão de Curso B, traz os conceitos e resultados fundamentais da Geometria Algébrica, como espaços afins, conjuntos algébricos, variedades afins, o *Lema da Normalização de Noether* e o *Teorema dos Zeros de Hilbert*, também conhecido como *Nullstellensatz*.

Sumário

Introdução . . . . . **v**

1 Anéis e Ideais **1**

1.1 Anéis e Homomorfismos de Anéis 1

1.2 Anéis de Polinômios 4

1.3 Ideais e Anéis Quocientes 7

1.4 Divisores de Zero, Elementos Nilpotentes e Unidades. 10

1.5 Ideais Primos e Ideais Maximais 12

1.6 Nilradical e Radical de Jacobson 16

1.7 Operações em Ideais 17

1.8 Extensão e Contração de Ideais 23

2 Módulos **25**

2.1 Módulos e Homomorfismo de Módulos 25

2.2 Submódulos e Módulos Quocientes 27

2.3 Operações em Submódulos 27

2.4 Soma Direta e Produto Direto 29

2.5 Módulos Finitamente Gerados 30

2.6 Sequências Exatas 33

3 Anéis e Módulos de Frações **41**

3.1 Propriedades Locais 46

3.2 Extensão e Contração de Ideais em Anéis de Frações 47

3.3 Domínio de Fatoração Única 48

4 Condições de Cadeia **58**

5 Anéis Noetherianos **65**

6 Conjuntos Algébricos Afins **68**

6.1 Preliminares 68

6.2 Formas 75
6.3 Espaços Afins e Conjuntos Algébricos 77
6.4 O Ideal de um Conjunto de Pontos 80
6.5 Componentes Irredutíveis de um Conjunto Algébrico 83
6.6 Subconjuntos Algébricos do Plano 86
6.7 Elementos Inteiros 88

7 Teorema dos Zeros de Hilbert 93
7.1 Extensões de Corpos 93
7.2 Lema da Normalização de Noether 94
7.3 Teorema dos Zeros de Hilbert 96

8 Variedades Afins 99
8.1 Anéis de Coordenadas 99
8.2 Aplicações Polinomiais 100
8.3 Mudança de Coordenadas 102
8.4 Funções Racionais e Anéis Locais 102
8.5 Anéis de Valorização Discreta 104
8.6 Ideais com um Número Finito de Zeros 105

Referências Bibliográficas 109

Introdução

Quando estudamos estruturas algébricas básicas, como grupos e anéis, percebemos que determinados resultados são válidos apenas para estruturas comutativas. Este fato, aliado à possibilidade de tratarmos de duas operações simultaneamente, torna a estrutura dos anéis mais rica e interessante do que a dos grupos. A Álgebra Comutativa é, essencialmente, o estudo de anéis comutativos. Em particular, quando restrita aos anéis de polinômios, é conhecida como Geometria Algébrica.

Este trabalho reúne os principais conceitos e resultados desta teoria, distribuídos ao longo de oito capítulos. Os cinco primeiros foram desenvolvidos durante o Trabalho de Conclusão de Curso A, e tratam de resultados gerais de Álgebra Comutativa. Os demais, referentes ao Trabalho de Conclusão de Curso B, abordam resultados mais específicos de Geometria Algébrica.

No primeiro capítulo são apresentados os objetos iniciais, como anéis, homomorfismos e ideais. Também são estudados tipos especiais de ideais, como ideais principais, primos e maximais, o nilradical e radical de Jacobson; além das operações, extensão e contração de ideais. Com especial atenção, abordamos o anel de polinômios e algumas propriedades.

No Capítulo 2, retomamos vários conceitos e resultados do Capítulo 1, referente ao estudo de módulos: homomorfimos entre módulos, módulos quocientes e operações em submódulos. Além disso, apresentamos a soma direta e produto direto de módulos, módulos finitamente gerados e sequências exatas de módulos. O terceiro capítulo trata de anéis e módulos de frações, extensão e contração de ideais em anéis de frações, e o que chamamos de *propriedades locais*.

O Capítulo 4 é dedicado ao estudo das cadeias de submódulos, juntamente com as propriedades de *módulos Noetherianos*; enquanto no Capítulo 5, definimos *anéis Noetherianos* e exploramos alguns resultados envolvendo estes anéis: em particular, o famoso *Teorema da Base de Hilbert*.

No sexto capítulo são introduzidos os conceitos iniciais de Geometria Algébrica, como espaços afins, conjuntos algébricos e elementos inteiros; além

de suas propriedades e alguns resultados fundamentais.

No capítulo seguinte, apresentamos o *Lema da Normalização de Noether*, seguido da demonstração devida a Zariski do *Teorema dos Zeros de Hilbert*. O último capítulo refere-se ao estudo de variedades algébricas, abordando conceitos como anéis de coordenadas, aplicações polinomiais e funções racionais.

Por fim, temos as Considerações Finais, onde destacamos alguns pontos importantes e as principais contribuições deste trabalho.

Capítulo 1

Anéis e Ideais

Neste primeiro capítulo, definimos os conceitos básicos da Álgebra Comutativa, como anéis e ideais, e apresentamos suas propriedades elementares. Depois, passamos à discussão a respeito de ideais primos e maximais; e às operações em ideais. Ressaltamos que os exemplos são apresentados no contexto de números inteiros e polinômios.

1.1 Anéis e Homomorfismos de Anéis

Sejam $(x, y) \mapsto x + y$ e $(x, y) \mapsto xy$ leis de composição internas num conjunto $R \neq \emptyset$, usualmente chamadas de *adição* e *multiplicação*, respectivamente. Suponhamos que

1. O conjunto R é um subgrupo abeliano em relação à adição; isto é, R satisfaz as seguintes propriedades:
   - Associatividade: $\forall x, y, z \in R$, $(x + y) + z = x + (y + z)$;
   - Comutatividade: $\forall x, y \in R$, $x + y = y + x$;
   - Existe elemento neutro para esta operação, denotado por 0_R (ou simplesmente 0) e chamado de *zero* do anel, tal que para todo $x \in R$, temos $x + 0_R = x$.
   - Todo elemento de R admite um simétrico aditivo; ou seja, para todo $x \in R$ existe um elemento em R, denotado por $(-x)$ tal que $x+(-x) = 0_R$.
2. A multiplicação é associativa: $\forall x, y, z \in R$, $((xy)z) = (x(yz))$.
3. A multiplicação é distributiva em relação à adição: $\forall x, y, z \in R$, $x(y+z) = xy + xz$ e $(x + y)z = xz + yz$.

Definição 1.1 (Anel)**.** *Nas condições expostas acima, dizemos que o conjunto R é um* anel *em relação à adição e multiplicação consideradas, e denotamos por $(R, +, \cdot)$.*

Além disso, se $(R, +, .)$ também satisfaz

4. A multiplicação é comutativa: $\forall x, y \in R$, $xy = yx$;
   e

5. Existe elemento neutro da multiplicação, denotado por 1_R (ou simplesmente 1) e chamado de *um*; tal que $x1 = 1x = x$, para todo $x \in R$;

dizemos que$(R, +, \cdot)$ é um *anel comutativo com unidade.*

Vejamos alguns exemplos.

Exemplo 1.2. *Os conjuntos númericos $\mathbb{Z}$ e $\mathbb{Q}$, equipados como as operações de soma e multiplicação usuais, são anéis comutativos com unidade. As propriedades listadas acima são facilmente verificadas para estes conjuntos.*

Exemplo 1.3. *Seja $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$; e as operações:*

$$\begin{aligned} + : \mathbb{Z}[i] \times \mathbb{Z}[i] &\longrightarrow \mathbb{Z}[i] \\ ((a+bi),(c+di)) &\mapsto (a+c)+(b+d)i, \end{aligned}$$

e

$$\begin{aligned} \cdot : \mathbb{Z}[i] \times \mathbb{Z}[i] &\longrightarrow \mathbb{Z}[i] \\ ((a+bi),(c+di)) &\mapsto (ac-bd)+(ad+bc)i. \end{aligned}$$

Então $(\mathbb{Z}[i], +, \cdot)$ é uma anel comutativo com unidade, chamado de anel dos inteiros de Gauss.

Exemplo 1.4. *Sejam $M_{n\times n}(\mathbb{R})$ o conjunto das matrizes $n \times n$ com entradas em $\mathbb{R}$, $+$ a adição e $\cdot$ a multiplicação usuais de matrizes. Sabemos que $(M_{n\times n}(\mathbb{R}), +, \cdot)$ é um anel com elemento unidade, mas não é comutativo se $n \geq 2$.*

Exemplo 1.5. *Seja Γ o conjunto das funções contínuas $f : [0, 1] \to \mathbb{R}$, onde estão definidas as operações $f+g$ e fg como $(f+g)(x) = f(x)+g(x)$ e $(fg) = f(x)g(x)$. Então $(\Gamma, +, \cdot)$ é um anel comutativo com unidade, onde os elementos 0 e 1 são as funções constantes 0 e 1, respectivamente.*

Ao longo deste texto, o termo "anel" significará anel comutativo com unidade, ou seja, um anel que satisfaça os itens de (1) a (5) acima. Além disso, chamaremos o anel $(R, +, \cdot)$ apenas por R, quando não houver ambiguidade em relação às suas operações.

Notemos que não está excluída a possibilidade de que, em (5), tenhamos $1 = 0$. Neste caso, para qualquer $x \in R$, temos

$$x = x1 = x0 = 0$$

e assim, R tem apenas o elemento 0, chamado de *anel nulo* e denotado por 0.

Considerando que um anel também é um grupo em relação à adição, vários conceitos e resultados importantes para grupos, podem ser extendidos para o caso de anel. Em geral, estes resultados são os mesmos que para grupos, apenas acrescidos de condições sobre a operação de multiplicação; como é o caso das seguintes definições.

Definição 1.6 (Subanel)**.** *Um subconjunto S de um anel R é um* subanel *se é fechado em relação à adição e multiplicação e se contém o elemento* 1 *de R.*

Exemplo 1.7. *Os conjuntos $\mathbb{R}, \mathbb{Q}$ e $\mathbb{Z}$ são subanéis de $\mathbb{C}$. Também é um subanel de $\mathbb{C}$ o conjunto $\mathbb{Z}[i]$ dos inteiros de Gauss.*

Definição 1.8 (Homomorfismo de anéis)**.** *Um* homomorfismo de anéis *é uma função f de um anel R em um anel S tal que*
(i)$f(x + y) = f(x) + f(y)$;
(ii) $f(xy) = f(x)f(y)$;
(iii)$f(1_R) = 1_S$.

Notemos que a condição (i) da definição acima é equivalente a dizer que f deve ser um homomorfismo de grupos. Agora, se $f : R \to S$ é um homomorfismo de anéis, então:

(a) $f(0) = 0$. De fato, $f(0) = f(0 + 0) = f(0) + f(0)$ e assim, $f(0)$ é o elemento neutro da adição, ou seja, $f(0) = 0$.

(b) Para todo $x \in R$, $f(-x) = -f(x)$. Como $0 = f(0) = f(x + (-x)) = f(x) + f(-x)$, temos que $f(-x)$ é o simétrico aditivo de $f(x)$, ou seja, $f(-x) = -f(x)$.

(c) Para todos $x, y \in R$, $f(x-y) = f(x)-f(y)$. De fato, $f(x-y) = f(x + (-y)) = f(x) + f(-y) \overset{(b)}{=} f(x) - f(y)$.

Exemplo 1.9. *A função* $p : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, *definida por* $p(x, y) = x$ *e chamada de* projeção, *é um homomorfismo de anéis:*

$$p((x, y) + (w, z)) = p(x + w, y + z) = x + w = p(x, y) + p(w, z),$$

$$p((x, y) \cdot (w, z)) = p(xw, yz) = xw = p(x, y) \cdot p(w, z)$$

e

$$p(1, 1) = 1.$$

É fácil ver que, se $f : R \to S$, $g : S \to T$ são homomorfismos de anéis, a composição $g \circ f : R \to T$ também é homomorfismo de anéis.

Outro exemplo clássico de homomorfismo de anéis é a identidade $\iota : S \to R$, $\iota(x) = x$, onde S é *subanel* de R.

1.2 Anéis de Polinômios

Um dos mais importantes exemplos de anéis é o chamado *anel de polinômios*, apresentado mais detalhadamente nesta seção.

Seja $(R, +, \cdot)$ um anel. Um *polinômio numa variável sobre* R é uma sequência $(a_0, a_1, ..., a_n, \cdots)$, onde $a_i \in R$ para todo índice e $a_i \neq 0$ somente para um número finito de índices.

Seja $\mathcal{R}$ o conjunto dos polinômios numa variável sobre R. Em $\mathcal{R}$, definimos as seguintes operações:

$$\oplus : \mathcal{R} \times \mathcal{R} \to \mathcal{R}$$

tal que

$$(a_0, a_1, ...), (b_0, b_1, ...) \longmapsto (a_0 + b_0, a_1 + b_1, ...)$$

$$\odot : \mathcal{R} \times \mathcal{R} \to \mathcal{R}$$

tal que

$$(a_0, a_1, ...), (b_0, b_1, ...) \longmapsto (c_0, c_1, ...)$$

onde

$$\begin{cases} c_0 = a_0 b_0 \\ c_1 = a_0 b_1 + a_1 b_0 \\ \vdots \\ c_n = a_0 b_n + a_1 b_{n-1} + ... + a_{n-1} b_1 + a_n b_0 \\ \vdots \end{cases}$$

É fácil ver que $(\mathcal{R}, \oplus, \odot)$ é um anel, e que

- o elemento neutro de $\oplus$ é $(0, 0, 0, ...)$;
- o elemento neutro de $\odot$ é $(1, 0, 0, ...)$;
- o simétrico aditivo de $(a_0, a_1, ..., a_n, ...)$ com respeito a operação $\oplus$ é o elemento $(-a_0, -a_1, ..., -a_n, ...)$.

Além disso, a multiplicação de $\mathcal{R}$ é comutativa, pois a multiplicação de R é comutativa. Se $(a_0, a_1, ..., a_n, ...)$ é um elemento de $\mathcal{R}$, então o símbolo $(a_0, a_1, ..., a_n, \cdots)^n$ representa o elemento

$$\underbrace{(a_0, a_1, ..., a_n, ...) \odot (a_0, a_1, ..., a_n, ...) \odot \cdots \odot (a_0, a_1, ..., a_n, ...)}_{n \text{ vezes}}.$$

Usando as definições de $\oplus$ e $\odot$, vemos que

$$(0, ..., 0, a_n, 0, 0, ...) = (a_n, 0, ...) \odot (0, ..., \underbrace{1}_{n+1}, 0, ...),$$

e que

$$(0, ..., 0, \underbrace{1}_{n+1}, 0, ...) = (0, 1, 0, ...)^n.$$

Assim, temos

$$\begin{aligned}(a_0, a_1, ..., a_n, 0, 0, ...) \;=\; & (a_0, 0, 0, ...) \\ & \oplus[(a_1, 0, 0, ...) \odot (0, 1, 0, 0, ...)] \\ & \oplus[(a_2, 0, 0, ...) \odot (0, 1, 0, 0, ...)^2] \\ & \oplus \cdots \\ & \oplus[(a_n, 0, 0, ...) \odot (0, 1, 0, 0, ...)^n].\end{aligned}$$

Para facilitar a notação, costuma-se usar o símbolo X para designar o elemento $(0, 1, 0, ...)$, escrever apenas a_i ao invés de $(a_i, 0, 0, ...)$ e também substituir $\oplus$ e $\odot$ por $+$ e $\cdot$, respectivamente. Dessa forma, o elemento $(a_0, a_1, ..., a_n, 0, ...)$ é representado pela soma $a_0 + a_1X + ... + a_nX^n$, e então $\mathcal{R} = \{\sum_{i=0}^{n} a_iX^i : a_i \in R, n \in \mathbb{N}\}$. As operações neste anel são a soma e a multiplicação usuais em polinômios. Denotamos $(\mathcal{R}, +, \cdot)$ por $R[X]$, o *anel de polinômios numa variável sobre* R.

Definimos o *grau* do polinômio $F(X) \in R[X], F(X) \neq 0$ como o inteiro n tal que $F(X) = a_0 + a_1X + ... + a_nX^n$, com $a_n \neq 0$. O elemento a_n é chamado *coeficiente dominante* do polinômio, e o polinômio é dito *mônico* se $a_n = 1$.

De forma semelhante ao anel $\mathbb{Z}$, existe um Algoritmo da Divisão em $R[X]$, conforme o teorema a seguir.

Teorema 1.10 (Algoritmo da Divisão). *Dados* $F = a_0 + a_1X + \ldots + a_nX^n$ *e* $g = b_0 + b_1X + \ldots + b_mX^m$ *em* $R[X]$, *com* $G \neq 0$ *e seu coeficiente dominante é unidade. Então existem* $A, B \in R[X]$ *tais que* $F = G \cdot A + B$, *onde* $B = 0$ *ou* $\deg B < \deg G$.

Demonstração: Se $F = 0$, então $A = B = 0$, pois $0 = G \cdot 0 + 0$. Caso $F \neq 0$ e $\deg F < \deg G$, basta tomarmos $G = 0$ e $B = F$, pois $G \cdot 0 + F = F$ e, por hipótese, $\deg F < \deg G$.

Por fim, se $F \neq 0$ e $\deg F \geq \deg G$, procedemos por indução sobre $\deg F$. Se $\deg F = 0$, então $\deg G = 0$, e daí $F = a_0$ e $G = b_0$. Basta tomar $A = b_0^{-1}a_0$ e $B = 0$, uma vez que $a_0 = b_0(b_0^{-1}a_0) + 0$.

Suponhamos agora que $\deg F = n$ e que o teorema se verifique para todo polinômio de grau menor que n. Seja $F_1 = F - a_nb_m^{-1}X^{n-m} \cdot G$. Se $F_1 = 0$ ou $\deg F_1 < \deg G$, então $B = F_1$ e $A = a_nb_m^{-1}X^{n-m}$. Caso contrário, temos $\deg F_1 \leq n - 1$ e $\deg F_1 \geq \deg G$. Pela hipótese de indução, existem $A_1, B_1 \in R[X]$ tais que

$$F_1 = G \cdot A_1 + B_1, \text{ com } B_1 = 0 \text{ ou } \deg B_1 < \deg(G).$$

Logo

$$F - a_nb_m^{-1}X^{n-m} \cdot G = G \cdot A_1 + B_1$$

e assim

$$F = G \cdot (A_1 + a_nb_m^{-1}X^{n-m}) + B_1, \text{ com } B_1 = 0 \text{ ou } \deg B_1 < \deg G.$$

■

Por indução, podemos definir o *anel de polinômios em k variáveis sobre o anel* R do seguinte modo:

$$R[X_1, ..., X_k] = (R[X_1, ..., X_{k-1}])[X_k].$$

Examinemos mais detalhadamente o caso $k = 2$. Por definição, $R[X_1, X_2] = (R[X_1])[X_2]$, e então um elemento deste anel é da forma

$$((a_{00}, a_{01}, ..., 0, ...), ..., (a_{n0}, a_{n1}, ..., 0, ...), ..., (0, 0, ...), ...)$$

com $a_{ij} \in R \; \forall i, j$.

Representando $((0, 1, 0, ...), (0, 0, ...), ...)$ por X_1 e $((0, 0, ...), (1, 0, ...), (0, 0, ...), ...)$ por X_2; o elemento acima se escreve como

$$a_0(X_1) + a_1(X_1)X_2 + ... + a_n(X_1)X_2^n$$

onde

$$\begin{cases} a_0(X_1) = a_{00} + a_{01}X_1 + a_{02}X_1^2 + ... \\ a_1(X_1) = a_{10} + a_{11}X_1 + a_{12}X_1^2 + ... \\ \vdots \\ a_n(X_1) = a_{n0} + a_{n1}X_1 + a_{n2}X_1^2 + ... \end{cases}$$

1.3 Ideais e Anéis Quocientes

Definição 1.11 (Ideal)**.** *Um* ideal *em um anel R é um subconjunto I de R, tal que I é um subgrupo aditivo e que $RI \subseteq I$; isto é, se $x \in R$ e $y \in I$, então $xy \in I$.*

Exemplo 1.12. *Seja R um anel. Então $\{0\}$ e R são ideais em R, chamados de ideais triviais.*

Exemplo 1.13. *Seja $f : R \to S$ um homomorfismo de anéis. O* núcleo *de f, definido como o conjunto $\{x \in R : f(x) = 0\}$, denotado por* $\ker f$*, é um ideal em R. De fato,* $\ker f$ *é um subgrupo aditivo (fato já conhecido para o caso de homomorfismo de grupos) e*

$$y \in R, x \in \ker f \Rightarrow f(xy) = f(x) \cdot f(y) = 0 \cdot f(y) = 0 \Rightarrow xy \in \ker f.$$

Entretanto, a imagem de f, definido como o conjunto $\{y \in S : f(x) = y,$ para todo *$x \in R\}$, e denotado por* $\mathrm{Im}(f)$*, é um subanel de S.*

Exemplo 1.14. *O conjunto $2\mathbb{Z}$ dos inteiros pares é um ideal em $\mathbb{Z}$. Mais geralmente, o conjunto $n\mathbb{Z}$ dos múltiplos inteiros de n, são os ideais em $\mathbb{Z}$.*

Exemplo 1.15 (Ideal Principal)**.** *Seja $x \in R$, então $Rx = \{ax : a \in R\}$ é um ideal em R, denotado por (x) e chamado de* ideal gerado por x*. Se $I = (x)$ para algum $x \in R$, então dizemos que I é um* ideal principal.

Como R é anel comutativo, então o ideal I é um subgrupo normal, e portanto, R/I é um grupo quociente. Seus elementos são classes de equivalência de $x \in R$, denotados por $\overline{x} = x + I$. $\overline{x}$ também é chamado de *I-resíduo de x em R*. Definindo as operações $+$ e $\cdot$ em $\overline{R}$ como

$$\overline{x} + \overline{y} = (x + I) + (y + I) = (x + y) + I = \overline{x + y}$$

e

$$\overline{x} \cdot \overline{y} = (x + I)(y + I) = xy + I = \overline{xy},$$

temos que R/I é um anel, com $\overline{1} = 1 + I$ e $\overline{0} = I$, chamado de *anel quociente*. Algumas vezes utilizamos a notação $x \equiv y (\mathrm{mod}\ I)$ para dizer que $x - y \in I$.

Com estas operações, temos que a função $\phi : R \to R/I$, que leva cada $x \in R$ a sua classe de equivalência $x + I$, é um homomorfismo sobrejetor de anéis, chamado de *homomorfismo natural* de R em R/I. De fato, se $x, y \in R$, temos que:

$$\phi(x + y) = (x + y) + I = (x + I) + (y + I) = \phi(x) + \phi(y);$$

$$\phi(xy) = xy + I = (x + I) \cdot (y + I) = \phi(x) \cdot \phi(y)$$

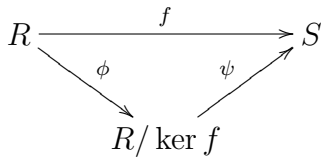
e

$$\phi(1) = 1 + I.$$

Assim como para o estudo de grupos, um resultado fundamental é o Teorema do Isomorfismo para Anéis.

Teorema 1.16 (Teorema Fundamental de Homomorfismo para Anéis Comutativos)**.** *Seja $f : R \to S$ um homomorfismo sobrejetor de anéis; e seja $\phi : R \to R/\ker f$ o homomorfismo natural. Então existe um isomorfismo $\psi : R/\ker f \to S$ tal que $\psi \circ \phi = f$.*

Demonstração: A situação descrita pode ser representada pelo seguinte diagrama:



Definindo a função $\psi : R/\ker f \to S$ como $\psi(x + \ker f) = f(x)$, temos que $\psi \circ \phi(x) = \psi(x + \ker f) = f(x)$. A função ψ está bem definida pois, se $x + \ker f = y + \ker f$, temos $x - y \in \ker f$ e, portanto, $f(x) = f(y)$. Basta agora mostrar que ψ é um isomorfismo.

ψ é homomorfismo, pois

$$\begin{aligned}
\psi((x + \ker f) + (y + \ker f)) &= \psi((x + y) + \ker f) \\
&= f(x + y) = f(x) + f(y) \\
&= \psi(x + \ker f) + \psi(y + \ker f), \\
\psi((x + \ker f)(y + \ker f)) &= \psi(xy + \ker f) \\
&= f(xy) = f(x) \cdot f(y) \\
&= \psi(x + \ker f) \cdot \psi(y + \ker f),
\end{aligned}$$

e

$$\psi(1 + \ker f) = f(1) = 1.$$

Como f é sobrejetor, para qualquer $y \in S$, existe $x \in R$ tal que $f(x) = y$. Então $\psi(x + \ker f) = f(x) = y$. Assim, ψ é sobrejetor.

Agora, suponha que $\psi(x+\ker f) = \psi(y+\ker f)$, então $f(x) = f(y)$ e $x - y \in \ker f$. Assim, $x + \ker f = y + \ker f$. Portanto, ψ é injetor.

Logo ψ é um isomorfismo de $R/\ker f$ em S, tal que $\psi \circ \phi = f$.

■

Corolário 1.17. *Qualquer imagem homomórfica de um anel R é isomorfo a um quociente R/I de R por um ideal I.*

Teorema 1.18. *Seja $f : R \to S$ um homomorfismo sobrejetor de anéis; e K seu núcleo. Então H é um subanel (ideal) de R que contém K se, e somente se, $f(H)$ é subanel (ideal) de S. Além disso, se I é um ideal de R contendo K então*

$$x + I \to f(x) + \overline{I},\ \overline{I} = f(I)$$

é um isomorfismo de R/I em $S/\overline{I}$.

Demonstração: Como a imagem por um homomorfismo é um subanel, é claro que se H é um subanel de R, então $f(H)$ é subanel de S. Se H for um ideal em R, temos que $f(H)$ é um subgrupo do grupo $(S, +)$. Se $\overline{x} \in S$, existe $x \in R$ tal que $f(x) = \overline{x}$. Assim, para $h \in H$, temos $f(h)\overline{x} = f(h)f(x) = f(hx) \in f(H)$, e portanto, $f(H)$ é um ideal.

Se $f(H)$ é um subanel (ideal) em S, então $f^{-1}(\overline{H})$ é um subgrupo do grupo $(R, +)$, e também é subanel (ideal) de R. Segue que a correspondência biunívoca entre o conjunto dos subgrupos de $(R, +)$ contendo K e dos subgrupos de S induz uma correspondência biunívoca entre os conjuntos dos subanéis e também entre os ideais contidos nos subgrupos.

Além disso, $x + I \to f(x) + \overline{I}$ é um isomorfismo de grupos entre R/I e $S/\overline{I}$, se I é um ideal em R contendo K e $\overline{I} = f(I)$. Como

$$(x + I)(y + I) = (xy + I) \to f(xy) + \overline{I} = f(x)f(y) + \overline{I} = (f(x) + \overline{I})(f(y) + \overline{I})$$

temos um isomorfismo de anéis. ■

Em particular, tomando o homomorfismo natural $\phi : R \to R/I$, temos $\ker \phi = I$. Como $\phi(J) \subseteq \phi(K)$ se $J \subseteq K$ (fato válido para funções em geral), temos o seguinte corolário.

Corolário 1.19. *Existe uma correspondência biunívoca que preserva a ordem entre os ideais J de R que contém I, e os ideais $\overline{J}$ de R/I, dada por $J = \phi^{-1}(\overline{J})$.*

Corolário 1.20. (i) *Seja $I \subset J$ ideais em um anel R. Então existe um homomorfismo natural de R/I em R/J.*

(ii) *Seja I um ideal em um anel R, e R subanel de um anel S. Então existe um homomorfismo natural de R/I em S/IS, onde IS é o ideal em S gerado por I.*

Demonstração: (i) Basta tomar $\phi : R/I \to R/J$ tal que $\phi(a+I) = a+J$. Está bem definido pois, se $a+I = b+I$, então $a-b \in J$, e $a+J = b+J$. Claramente, é homomorfismo.

(ii) A função $\psi : R/I \to S/IS$, tal que $\psi(a+I) = a+IS$ é homomorfismo, e está bem definida, uma vez que $a+I = b+I$ implica em $a-b \in I \subset IS$ e $a-b \in S$. ■

1.4 Divisores de Zero, Elementos Nilpotentes e Unidades.

Um *divisor de zero* em um anel R é um elemento x, para o qual existe $y \neq 0$ em R tal que $xy = 0$. Um anel sem divisores de zero não nulos, e com $1 \neq 0$, é chamado *domínio de integridade* (ou simplesmemte, *domínio*).

Exemplo 1.21. *Os conjuntos númericos $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$, com as operações usuais, são domínios. Também é um domínio o conjunto $\mathbb{Z}[i]$ dos inteiros de Gauss.*

Exemplo 1.22. *O conjunto Γ das funções contínuas $f : [0,1] \to \mathbb{R}$ é um anel, conforme o Exemplo 1.5. Entretanto, podemos considerar duas funções f e g em Γ assim definidas:*

$$f(x) = \begin{cases} 0, \text{ se } 0 \leq x \leq \frac{1}{2}; \\ x - \frac{1}{2}, \text{ se } \frac{1}{2} \leq x \leq 1. \end{cases}$$

$$g(x) = \begin{cases} -x + \frac{1}{2}, \text{ se } 0 \leq x \leq \frac{1}{2}; \\ 0, \text{ se } \frac{1}{2} \leq x \leq 1. \end{cases}$$

É claro que $f \not\equiv 0$ e $g \not\equiv 0$, mas $fg \equiv 0$. Portanto, Γ não é um domínio.

Em particular, existem domínios de integridade cujos ideais são todos principais, como o anel $\mathbb{Z}$ (Exemplo 1.14). Neste caso, dizemos que o domínio é um *domínio principal*.

O resultado a seguir decorre diretamente do Algoritmo de Divisão para $K[X]$, onde K é corpo, e nos fornece um exemplo de domínio principal.

Proposição 1.23. *Seja K um corpo. Então $K[X]$ é um domínio principal.*

Demonstração: Seja I um ideal em $K[X]$. Se $I = 0$, não há o que fazer. Suponhamos $I \neq 0$. Seja $F \in I$ um polinômio não nulo de menor grau possível. Afirmamos que $I = (F)$. De fato, se $G \in I$, existem polinômio A e B em $K[X]$ tais que $G = F \cdot A + B$, com $B = 0$ ou $\deg B < \deg F$. Como $B \in I$, pois $H, F \in I$, devemos ter $\deg B = 0$, pela minimalidade de $\deg F$. Logo $H = F.A$, e $H \in (F)$. A outra inclusão é óbvia e, portanto, $I = (F)$. ■

Dizemos que um elemento $x \in R$ é *nilpotente* se $x^n = 0$ para algum inteiro $n > 0$. Obviamente, se x é nilpotente, então $0 = x^n = x \cdot x^{n-1}$. Portanto, um elemento nilpotente é divisor de zero, mas a recíproca não é válida em geral.

Uma *unidade* em R é um elemento x tal que $xy = 1$ para algum $y \in R$. O elemento y é determinado de forma única por x, e é denotado por x^{-1}. As unidades em R formam um grupo abeliano U_R em relação a operação de multiplicação. De fato,

- $1 \in U_R$, obviamente;
- se $x, y \in U_R$, então $(xx^{-1})(yy^{-1}) = 1 \Rightarrow (xy)((x^{-1})(y^{-1})) = 1 \Rightarrow xy \in U_R$.
- se $x \in U_R$, então $xx^{-1} = 1 \Rightarrow x^{-1} \in U_R$.

Como exemplo, consideremos o anel $\mathbb{Z}$, cujas unidades são 1 e -1. Além disso, observemos que $(-1) = \mathbb{Z} = (1)$. Na verdade, este fato é válido para qualquer anel R: se $x \in R$ é uma unidade, então $(x) = R = (1)$. De fato, se x é unidade, então existe $x^{-1} \in R$ tal que $xx^{-1} = 1$, e logo $1 \in (x)$. Como (x) é ideal que contém 1, então $R \subseteq (x)$ e, portanto, $(x) = R$. Por outro lado, se $(x) = R$, então $1 \in (x)$. Assim, existe $y \in R$ tal que $xy = 1$, concluindo que x é uma unidade em R.

Quando R é um anel no qual $1 \neq 0$ e todo elemento não nulo é uma unidade, dizemos que R é um *corpo*. Todo corpo é domínio de integridade. Com efeito, seja R é um corpo e $x \neq 0 \in R$. Supondo que $xy = 0$, então $0 = x^{-1} \cdot 0 = x^{-1}xy = y$. Assim, x não é divisor de zero.

Entretanto, nem todo domínio de integridade é corpo: basta considerar que $\mathbb{Z}$ é um domínio de integridade, mas não é corpo, pois suas únicas unidades são 1 e -1.

O resultado a seguir nos fornece uma caracterização de um corpo em termos de ideais.

Proposição 1.24. *Seja $R \neq 0$ uma anel. Então as seguintes afirmações são equivalentes:*

(i) R é um corpo.

(ii) Os únicos ideais em R são 0 e (1).

(iii) Todo homomorfismo não nulo de R em um anel S é injetor.

Demonstração: (i) $\Rightarrow$ (ii). Seja R um corpo e $I \neq 0$ um ideal em R. Então I contém um elemento $x \neq 0$. Como R é corpo, temos que x é uma unidade e $I \supseteq (x) = (1) = R$. Logo, $I = (1) = R$.

(ii) $\Rightarrow$ (iii). Seja $f : R \to S$ homomosfismo de anéis. Então ($\ker f$ é um ideal $\neq (1)$ pois, se $\ker f = (1)$, teremos f a função identicamente nula. Assim, $\mathrm{Ker}(f) = 0$ e, portanto, f é homomorfismo injetor.

(iii) $\Rightarrow$ (i). Tomemos $x \in R$ não unidade. Então $(x) \neq (1)$, e daí $S = R/(x)$ é não nulo. Seja $\phi : R \to S$ o homomorfismo natural de R em S, com $\mathrm{Ker}(\phi) = (x)$. Por hipótese, ϕ é injetor, e assim, $(x) = 0 \Rightarrow x = 0$. Portanto, sendo 0 o único elemento que não é unidade em R, concluímos que R é corpo. ■

1.5 Ideais Primos e Ideais Maximais

Já vimos que todo ideal em $\mathbb{Z}$ é da forma (x), $x \in \mathbb{Z}$. Em particular, consideremos um ideal (p), p primo. Se $mn \in (p)$, temos $mn = kp$ e, necessariamente $m \in (p)$ ou $n \in (p)$. Além disso, se $(p) \subseteq (q)$, q inteiro; então $p \in (q)$, com $p = hq$. Sendo p primo, $h = 1$ ou $q = 1$; e logo $(p) = (q)$ ou $(q) = (1) = \mathbb{Z}$. Esta discussão motiva as duas próximas definições.

Definição 1.25 (Ideal Primo)**.** *Um ideal $\mathcal{P}$ é* primo *se $\mathcal{P} \neq (1)$ e se $xy \in \mathcal{P}$ implicar que $x \in \mathcal{P}$ ou $y \in \mathcal{P}$.*

Exemplo 1.26. *O ideal $2\mathbb{Z}$ é um ideal primo em $\mathbb{Z}$; enquanto que $4\mathbb{Z}$ não é. É claro que se $xy \in 2\mathbb{Z}$, então $xy = 2n$ para algum $n \in \mathbb{Z}$. Assim, $x \in 2\mathbb{Z}$ ou $y \in 2\mathbb{Z}$. Em relação a $4\mathbb{Z}$, basta considerar que $2 \cdot 2 = 4 \in 4\mathbb{Z}$, mas $2 \notin 4\mathbb{Z}$.*

Exemplo 1.27. *O ideal (X) é primo em $\mathbb{Z}[X]$. De fato, se $pq \in (X)$, então pq é um polinômio sem termo constante. Mas o termo constante de um produto de*

polinômio é o produto dos seus termos constantes; e assim, ou p ou q não possui termo constante, isto é, pertence a (X).

Definição 1.28 (Ideal Maximal)**.** *Um ideal* $\mathcal{M}$ *é* maximal *se* $\mathcal{M} \neq (1)$ *e se não existir um ideal* I *tal que* $\mathcal{M} \subsetneq I \subsetneq (1)$.

Exemplo 1.29. *O ideal* $2\mathbb{Z}$ *é maximal em* $\mathbb{Z}$. *De fato, suponha que exista um ideal* J *em* $\mathbb{Z}$, *tal que* $2\mathbb{Z} \subsetneq J$. *Então existe* $x \in J$ *tal que* $x \notin 2\mathbb{Z}$; *e assim* $x = 2n + 1$, *para algum* n *inteiro. Mas* $x = 2n + 1 \Rightarrow 1 = x - 2n \in J$. *Logo* $J = \mathbb{Z}$.

A proposição a seguir apresenta algumas afirmações envolvendo ideais primos e maximais e domínios de integridade.

Proposição 1.30. (i) $\mathcal{P}$ *é primo* $\Leftrightarrow$ $R/\mathcal{P}$ *é domínio de integridade.*

(ii) $\mathcal{M}$ *é maximal* $\Leftrightarrow$ $R/\mathcal{M}$ *é corpo.*

(iii) *Todo ideal maximal é primo.*

(iv) *O ideal nulo é primo* $\Leftrightarrow$ R *é domínio de integridade.*

Demonstração: (i) Tomemos $\overline{x}, \overline{y} \in R/\mathcal{P}$. Então, $\overline{xy} = \overline{0} \Leftrightarrow xy \in \mathcal{P}$ e, sendo $\mathcal{P}$ primo, temos que $x \in \mathcal{P}$ ou $y \in \mathcal{P}$. Mas isso é o mesmo que $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$; portanto, $R/\mathcal{P}$ é um domínio de integridade. Por outro lado, supondo $xy \in \mathcal{P}$ com $x, y \notin \mathcal{P}$, teremos $\overline{xy} = \overline{0}$ com $\overline{x} \neq \overline{0}$ e $\overline{y} \neq \overline{0}$, e então $R/\mathcal{P}$ não é domínio de integridade.

(ii) Considerando $\mathcal{M} \neq (1)$ maximal, existe $\overline{x} \neq \overline{0}$, $\overline{x} \in R/\mathcal{M}$. Tomemos (x) em R. Como (x) é ideal e $\mathcal{M} \subset (x)$, temos que $(x) = (1)$. Assim, $\overline{x}$ é uma unidade, e $R\,/\mathcal{M}$ é corpo. Agora, supondo $R/\mathcal{M}$ corpo, pela Proposição 1.24, seus únicos ideais são $\overline{0}$ e $(\overline{1})$. Pela Proposição 1.19, se $\mathcal{M}$ é ideal em R tal que $\mathcal{M} \subset I$, para certo ideal I, então $I = (1)$ e, portanto, $\mathcal{M}$ é maximal.

(iii) Se $\mathcal{M}$ é maximal, por (ii), $R/\mathcal{M}$ é corpo. Como todo corpo é domínio de integridade, $R/\mathcal{M}$ é domínio de integridade. Finalmente, por (i), $\mathcal{M}$ é primo.

(iv) É claro que se o ideal 0 é primo, então $xy \in 0 \Rightarrow xy = 0$, com $x \in 0$ ou $y \in 0$, significa que $x = 0$ ou $y = 0$. Logo 0 é domínio de integridade. Por outro lado, supondo que 0 não seja primo, temos que $xy \in 0$, com $x \notin 0$ e $y \notin 0$. Isto quer dizer que $xy = 0$, com $x \neq 0$ e $y \neq 0$, ou seja, que 0 possui divisores não nulos de zero, contrariando o fato de ser domínio de integridade. ■

Quando consideramos R, em particular, um domínio de ideal principal, obtemos a recíproca do item (iii). Com efeito, se $(x) \neq 0$ é um ideal primo

em R e $(x) \subsetneq (y)$, temos que $x \in (y)$, isto é, $x = yz$ para algum $z \in R$. Assim, $yz \in (x)$ e $y \notin (x)$; logo $z \in (x)$, com $z = tx$. Então $x = yz = ytx$ e $yt = 1$. Logo y é unidade e $(y) = R$.

Analisemos agora o comportamento de ideais primos e maximais sob ação de homomorfismos de anéis. Se $f : R \to S$ é um homomorfismo de anéis e $\mathcal{P}$ é um ideal primo em S, então $f^{-1}(\mathcal{P})$ é um ideal primo em R. De fato, se $xy \in f^{-1}(\mathcal{P})$, então $f(x) \cdot f(y) = f(xy) \in \mathcal{P}$. Como $\mathcal{P}$ é primo, $f(x) \in \mathcal{P}$ ou $f(y) \in \mathcal{P}$, e assim $x \in f^{-1}(\mathcal{P})$ ou $y \in f^{-1}(\mathcal{P})$. Portanto, $f^{-1}(\mathcal{P})$ é primo.

Considerando o homomorfismo

$$\begin{aligned} \psi : \ R/f^{-1}(\mathcal{P}) \ &\longrightarrow \ S/\mathcal{P} \\ \psi\left(x + f^{-1}(\mathcal{P})\right) \ &\longmapsto \ f(x) + \mathcal{P}, \end{aligned}$$

temos que $T = \mathrm{Im}(\psi) = f(R) + \mathcal{P}$ é subanel de $S/\mathcal{P}$, e portanto, $R/f^{-1}(\mathcal{P}) \cong T$. Além disso, $R/f^{-1}(\mathcal{P})$ não possui divisores não nulos de zero, pois $S/\mathcal{P}$ é domínio de integridade (item (i) da Proposição 1.30).

No entanto, se $\mathcal{M}$ é um ideal maximal em S, $f^{-1}(\mathcal{M})$ pode não ser maximal em R. Por exemplo, tome $R = \mathbb{Z}$, $S = \mathbb{Q}$ e $\mathcal{M} = 0$: 0 é maximal em $\mathbb{Q}$, pois $\mathbb{Q}$ é corpo; mas $f^{-1}(0) = 0$ não é maximal em $\mathbb{Z}$, uma vez que $0 \subset 2\mathbb{Z} \subsetneq \mathbb{Z}$.

A demonstração a seguir é uma simples aplicação do Lema de Zorn. Antes de enunciá-lo, façamos algumas considerações.

Seja S um conjunto não vazio parcialmente ordenado; isto é, existe uma relação $x \leq y$ em S que é reflexiva e transitiva, e tal que se $x \leq y$ e $y \leq x$, temos $x = y$. Um subconjunto T de S é uma *cadeia* se $x \leq y$ ou $y \leq x$ para cada par de elementos $x, y \in T$.

Lema 1.31 (Lema de Zorn)**.** *Se toda cadeia T de S possui um elemento maximal em S, então S possui ao menos um elemento maximal.*

Teorema 1.32. *Todo anel $R \neq 0$ tem ao menos um ideal maximal.*

Demonstração: Seja Σ o conjunto de todos os ideais diferentes de (1) em R. Em Σ considere a relação de ordem dada pela inclusão. Σ é não vazio, pois $0 \in \Sigma$. Para aplicar o Lema de Zorn, devemos mostrar que toda cadeia em Σ tem um limitante superior em Σ.

Seja (I_α) uma cadeia de ideais em Σ. Seja $I = \bigcup_\alpha I_\alpha$. Então $1 \notin I$, pois $1 \notin I_\alpha$ para todo α. Afirmamos que I é um ideal. De fato, como I é uma reunião de ideais, temos que:

- $0 \in I$;

- se $x, y \in I$, então $x \in I_\alpha$ e $y \in I_\beta$. Mas, como $I_\alpha \subseteq I_\beta$ ou $I_\beta \subseteq I_\alpha$, segue que $x, y \in I_\alpha$ ou $x, y \in I_\beta$, e portanto, $x + y \in I$.
- se $x \in I$, então $-x \in I$;
- $ax \in I$ para todo $a \in R$;

Assim, $I \in \Sigma$, e I é um limitante superior da cadeia. Então, pelo Lema de Zorn, Σ tem um elemento maximal. ■

Corolário 1.33. *Se $I \neq (1)$ é um ideal de R, então existe um ideal maximal de R contendo I.*

Demonstração: Consideremos R/I. Pelo Teorema 1.32, R/I contém um ideal maximal $\overline{\mathcal{M}}$; e, pelo Corolário 1.19, existe ideal $\mathcal{M}$ de R tal que $I \subset \mathcal{M} \subset R$. Tomemos um ideal J em R tal que $\mathcal{M} \subsetneq J \subset R$. Novamente utilizando o Corolário 1.19, temos $\overline{\mathcal{M}} \subsetneq \overline{J} \subset R/I$. Como $\overline{\mathcal{M}}$ é maximal, então $\overline{J} = (\overline{1})$, e assim, $J = R$. Portanto $\mathcal{M}$ é maximal em R e contém I. ■

Corolário 1.34. *Todo elemento não unidade de R está contido em um ideal maximal.*

Demonstração: Se $I \neq (1)$, então I não contém elemento unidade. Pelo corolário anterior, $I \subset \mathcal{M}$, com $\mathcal{M}$ maximal. ■

Já vimos que os únicos ideais em um corpo K são os triviais. Assim, o único ideal maximal em K é o ideal 0. Anéis com um único ideal maximal são chamado de *anéis locais*, e o corpo $K = R/\mathcal{M}$ é chamado *corpo residual*. Um anel com apenas um número finito de ideais maximais é dito *semi-local*.

A proposição a seguir fornece um método para determinar se um dado anel R é ou não anel local.

Proposição 1.35. *(i) Seja R um anel e $\mathcal{M} \neq (1)$ um ideal de R tal que todo $x \in R - \mathcal{M}$ é uma unidade em R. Então R é um anel local e $\mathcal{M}$ é seu ideal maximal.*

(ii) Seja R uma anel e $\mathcal{M}$ um ideal maximal de R, tal que todo elemento de $1+\mathcal{M} = \{1 + x : x \in \mathcal{M}\}$ é uma unidade em R. Então R é um anel local.

Demonstração: (i) Todo ideal $I \neq (1)$ consiste de não unidades e, então, estão contidos em $\mathcal{M}$. Assim, $\mathcal{M}$ é o único ideal maximal de R.

(ii) Seja $x \in R - \mathcal{M}$. Como $\mathcal{M}$ é maximal, o ideal gerado por x e $\mathcal{M}$ é (1). Daí existem $y \in R$ e $t \in \mathcal{M}$ tal que $xy+t = 1$, então $xy = 1-t \in 1+\mathcal{M}$ e assim, xy é unidade. Portanto, x é unidade e, por (i), R é anel local. ■

Exemplo 1.36. *$\mathbb{Z}_4$ é anel local, pois seu único ideal maximal é $\{\overline{0}, \overline{2}\} \cong \mathbb{Z}_2$. Com efeito, $\overline{1}$ e $\overline{3}$ são unidades em $\mathbb{Z}_4$; e pela Proposição 1.35, $\mathbb{Z}$ é local, com ideal maximal $\mathbb{Z}_2$.*

O mesmo é verificado para $\mathbb{Z}_9$, com ideal maximal $\{\overline{0}, \overline{3}, \overline{6}\} \cong \mathbb{Z}_3$. Em geral, $\mathbb{Z}_{p^2}$, p primo, é anel local, com ideal maximal $\left\{\overline{0}, \overline{p}, \overline{2p}, \cdots, \overline{(p-1)p}\right\} \cong \mathbb{Z}_p$.

1.6 Nilradical e Radical de Jacobson

Recordemos que um elemento x é nilpotente se $x^n = 0$ para algum $n > 0$ inteiro. Por exemplo, em $\mathbb{Z}$, o único elemento nilpotente é 0, que constitui o ideal trivial 0. Na verdade, o conjunto de todos os elementos nilpotentes de um anel R formam um ideal $\Re_R$, o *nilradical* de R; conforme mostra o seguinte resultado.

Proposição 1.37. *O conjunto $\Re_R$ de todos os elementos nilpotentes em um anel R é um ideal, e $R/\Re_R$ não possui elemento nilpotente não nulo.*

Demonstração: Primeiramente, vejamos que $\Re_R$ é um ideal em R:

- $0 \in \Re_R$, obviamente.
- se $x, y \in \Re_R$, com $x^m = 0$ e $y^n = 0$, então

$$\begin{aligned}(x+y)^{m+n-1} &= x^{m+n-1} + \begin{pmatrix} m+n-1 \\ 1 \end{pmatrix} x^{m+n-2}y + \cdots + \\ &\quad + \begin{pmatrix} m+n-1 \\ m+n-2 \end{pmatrix} xy^{m+n-2} + y^{m+n-1}\end{aligned}$$

  é soma de inteiros múltiplos de produtos $x^r y^s$, onde $r + s = m + n - 1$. Como não podemos ter $r < m$ e $s < n$, cada um destes produtos se anula, e assim $(x+y)^{m+n-1} = 0$. Portanto $x + y \in \Re_R$.

- se $x \in \Re_R$, então $(-x)^n = x^n = 0$, se n par; e $(-x)^n = -(x^n) = 0$, se n ímpar. Portanto, $-x \in \Re_R$.
- se $x \in \Re_R$ e $y \in R$, então $(yx)^n = y^n x^n = 0$. Logo $yx \in \Re_R$.

Agora, seja $\overline{x} \in R/\Re_R$ representado por $x \in R$. Então $\overline{x}^n$ é representado por x^n, e assim $\overline{x}^n = 0 \Rightarrow x^n \in \Re_R \Rightarrow (x^n)^k = 0$ para algum $k > 0$. Portanto $x \in \Re_R \Rightarrow \overline{x} = 0$. ■

Denotamos $\Re_R$ simplesmente por $\Re$ quando não causar ambiguidade. A seguinte proposição nos dá uma definição alternativa para $\Re$.

Proposição 1.38. *O nilradical de R é a intersecção de todos os ideais primos de R.*

Demonstração: Seja $\Re'$ a intersecção de todos os ideais primos de R. Se $f \in R$ é nilpotente e se $\mathcal{P}$ é um ideal primo, então $f^n = 0 \in \mathcal{P}$ para algum inteiro $n > 0$, e daí $f \in \mathcal{P}$, pois $\mathcal{P}$ é primo. Assim, $f \in \Re'$.

Por outro lado, suponha que f não seja nilpotente. Seja Σ o conjunto dos ideais I com a propriedade de que $n > 0 \Rightarrow f^n \notin I$. Então Σ é não vazio, pois $0 \in \Sigma$. Como na Proposição 1.32, o Lema de Zorn pode ser aplicado ao conjunto Σ, ordenado pela inclusão, garantindo que Σ tem um elemento maximal. Seja $\mathcal{P}$ um elemento maximal de Σ. Mostraremos que $\mathcal{P}$ é um ideal primo. Sejam $x, y \notin \mathcal{P}$. Então os ideais $\mathcal{P} + (x), \mathcal{P} + (y)$ contém $\mathcal{P}$ estritamente e assim não pertence a Σ. Logo $f^m \in \mathcal{P} + (x), f^n \in \mathcal{P} + (y)$ para certos m, n.

Segue que $f^{m+n} \in \mathcal{P} + (xy)$, e então o ideal $\mathcal{P} + (xy)$ não pertence a Σ e daí $xy \notin \mathcal{P}$. Assim temos um ideal primo $\mathcal{P}$ tal que $f \notin \mathcal{P}$, e portanto $f \notin \Re'$. ■

O *Radical de Jacobson* ${}_J\Re$ de R é definido como a intersecção de todos os ideais maximais de R. Também pode ser caracterizado como segue:

Proposição 1.39. *$x \in {}_J\Re \iff 1 - xy$ é uma unidade em R para todo $y \in R$.*

Demonstração: Suponha que $1-xy$ não seja unidade. Pelo Corolário 1.34, $1-xy$ pertence a um ideal maximal $\mathcal{M}$, mas $x \in {}_J\Re \subseteq \mathcal{M}$, pela definição de $\Re$. Assim $xy \in \mathcal{M}$, e então $1 \in \mathcal{M}$, o que é um absurdo.

Agora suponha $x \notin \mathcal{M}$ para algum ideal maximal $\mathcal{M}$. Então $\mathcal{M}$ e x geram o ideal (1), e temos $u + xy = 1$ para algum $u \in \mathcal{M}$ e algum $y \in R$. Assim $1 - xy \in \mathcal{M}$ e portanto, não é unidade. ■

Como todo ideal maximal é primo, então $\Re \subseteq {}_J\Re$ em todo anel R. Entretanto, se R é um domínio principal, como é o caso de $\mathbb{Z}$, todo ideal primo é maximal, e portanto, $\Re = {}_J\Re$.

1.7 Operações em Ideais

Se I e J são ideais em um anel R, sua *soma* $I + J$ é o conjunto de todos $x + y$ onde $x \in I$ e $y \in J$. Este é o menor ideal contendo I e J. Mais

geralmente, definimos a soma $\sum_{i\in I} I_i$ para qualquer família de ideais I_i de R: seus elementos são todas as somas $\sum x_i$, onde $x_i \in I_i$ para todo $i \in I$.

A *intersecção* de qualquer família $(I_i)_{i\in I}$ de ideais é um ideal. O *produto* IJ de dois ideais I, J é um ideal em R, formado por todas as somas finitas $\sum x_i y_i$ onde cada $x_i \in I$ e cada $y_i \in J$. Da mesma forma, definimos o produto de qualquer família finita de ideais. Em particular as potências $I^n (n > 0)$ de um ideal I estão definidas. Convenientemente, $I^0 = (1)$; e então $I^n (n > 0)$ é o ideal gerado por todos os produtos $x_1 x_2 ... x_n$ no qual cada fator x_i pertence a I.

Exemplo 1.40. *Se $R = \mathbb{Z}$, $I = (m)$ e $J = (n)$, então $I + J$ é o ideal gerado pelo máximo divisor comum de m e n; $I \cap J$ é o ideal gerado pelo mínimo múltiplo comum; e $IJ = (mn)$. Neste caso, $IJ = I \cap J \Leftrightarrow m, n$ são primos entre si.*

As três operações em ideais acima definidas (soma, intersecção e produto) são associativas e comutativas. Também está satisfeita a *Lei Distributiva*

$$I(J + K) = IJ + IK.$$

De fato, como $IJ \subseteq I(J + K)$ e $IK \subseteq I(J + K)$ então $IJ + IK \subseteq I(J + K)$. Por outro lado, se $x \in I(J + K)$, então $x = \sum_i a_i(b_i + c_i)$, com $a_i \in I, bi \in J$ e $c_i \in K$. Logo $x = \sum_i a_i b_i + \sum_i a_i c_i$, e $x \in IJ + IK$.

Em qualquer anel R, temos que $I \cap J \subseteq J$ e $I \cap K \subseteq K$; bem como ambas as intersecções são subconjuntos de I. Assim, $(I \cap J) + (I \cap K)$ está em $K + J$ e I, e portanto, $(I \cap J) + (I \cap K) \subseteq I \cap (J + K)$.

A inclusão contrária não é válida em geral, sendo substituído pela *Lei Modular*:

$$I \cap (J + K) = I \cap J + I \cap K$$

se $I \supseteq J$ ou $I \supseteq K$. Obviamente, se $J \subseteq I$, $I \cap J = J$, e daí $I \cap J + I \cap K = J + I \cap K \subseteq J + K$ e $J + I \cap K \subseteq I$. Logo $I \cap J + I \cap K \subseteq I \cap (J + K)$. A verificação é análoga para $I \supseteq K$.

Em particular, em $\mathbb{Z}$ não é necessário exigir que $I \supseteq K$ ou $I \supseteq J$. Isso porque se $x \in I \cap (J + K)$, e $(i) = I, (j) = (J), (k) = K$; então $x = ar$, com $r = \text{mmc}(i, d)$ e $d = \text{mdc}(j, k) = \alpha j + \beta k$, para certos $\alpha, \beta \in \mathbb{Z}$. Como também $x = bi = cd$, e $d \mid j$ e $d \mid k$; temos $i \mid cj$ e $i \mid ck$. Assim, $x = \alpha(cj) + \beta(ck) = \alpha(mi) + \beta(ni)$, para certos m, n inteiros; o que implica que $x \in (I \cap J + I \cap K)$. Portanto, no anel $\mathbb{Z}$, a intersecção e a adição de ideais são distributivas uma em relação a outra.

Em geral, $(I + J)(I \cap J) \subseteq IJ$, uma vez que $(I + J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ$. Novamente, em $\mathbb{Z}$ vale a igualdade $(I + J)(I \cap J) = IJ$,

uma vez que $\text{mmc}(i,j) \cdot \text{mdc}(i,j) = i \cdot j$.

Claramente, $IJ \subseteq I \cap J$; e então $I \cap J = IJ$ desde que $I + J = (1)$. Dizemos que os ideais I, J são *comaximais* se $I + J = (1)$. Assim, para ideais comaximais, temos que $I \cap J = IJ$. Também é fácil ver que I, J são comaximais se, e somente se, existem $x \in I$ e $y \in J$ tais que $x + y = 1$.

Proposição 1.41. *Se I_i, I_j são comaximais sempre que $i \neq j$, então $\prod I_i = \bigcap I_i$.*

Demonstração: Por indução sobre n. Para $n = 2$ a afirmação é válida, conforme visto anteriormente.

Suponha $n > 2$ e que o resultado seja válido para $I_1, ..., I_{n-1}$. Seja $J = \prod_{i+1}^{n-1} I_i = \bigcap_{i=1}^{n-1} I_i$. Como os ideias são comaximais, por hipótese, temos que $I_i + I_n = (1)$ para $1 \leq i \leq n-1$; e então existem equações do tipo $x_i + y_i = 1$, com $x_i \in I_i$ e $y_i \in I_n$. Fazendo

$$\prod_{i=1}^{n-1} x_i = \prod_{i=1}^{n-1} (1 - y_i) = 1 - \Gamma,$$

onde $\Gamma \in I_n$, pois é uma soma cujos termos são produtos de y_i. Assim,

$$\prod_{i=1}^{n-1} x_i \equiv 1 (\text{mod } I_n).$$

Como $\prod x_i = x \in J$ e $x = 1 - \Gamma$, obtemos I_n e J são comaximais; isto é, $I_n + J = (1)$. Logo, a hipótese de indução nos garante que

$$\prod_{i=1}^{n} I_i = J \cdot I_n = J \cap I_n = \bigcap_{i=1}^{n} I_i.$$

■

Sejam $R_1, ...R_n$ anéis. O *produto direto*

$$R = \prod_{i=1}^{n} R_i$$

é o conjunto de todas as sequências $x = (x_1, ..., x_n)$ com $x_i \in R_i$, com adição e multiplicação definidas componente a componente. R é um anel comutativo com elemento unidade $(1, ..., 1)$. Temos as projeções $p_i : R \to R_i$, definidas por $p_i(x) = x_i$, que são homomorfismo de anéis.

Seja R um anel e $I_1, ..., I_n$ ideais em R. Definimos o homomorfismo $\phi : R \to \prod_{i=1}^{n} (R/I_i)$ pela regra $\phi(x) = (x + I_1, ..., x + I_n)$. Para este homomorfismo, tem-se:

Proposição 1.42. (i) *ϕ é sobrejetor se, e somente se, I_i, I_j são comaximais sempre que $i \neq j$.*

(ii) *ϕ é injetor se, e somente se, $\bigcap I_i = 0$.*

Demonstração: (i) Sem perda de generalidade, mostremos que I_1 e I_2 são comaximais. Existe $x \in R$ tal que $\phi(x) = (\overline{1}, \overline{0}, ..., \overline{0})$; daí $x \equiv 1(\text{mod } I_1)$ e $x \equiv 0(\text{mod } I_2)$ de tal forma que

$$1 = (1 - x) + x \in (I_1 + I_2).$$

Por outro lado, é suficiente mostrar que, por exemplo, existe um elemento $x \in R$ tal que $\phi(x) = (1, 0, ..., 0)$. Como $I_1 + I_i = (1)(i > 1)$, temos equações $u_i + v_i = 1$, com $u_i \in I_2$ e $v_i \in I_1$. Tomemos $x = \prod_{i=2}^{n} v_i$, então $x = \prod(1 - u_i) \equiv 1(\text{mod } I_1)$ e $x \equiv 0(\text{mod } I_i)$, $i > 1$. Daí $\phi(x) = (\overline{1}, \overline{0}, ..., \overline{0})$ como desejado.

(ii) Como $x \in \ker\phi \Leftrightarrow x \equiv 0(\text{mod } I_i)(i = 1, ..., n) \Leftrightarrow x \in \bigcap I_i$, então $\ker\phi = \bigcap I_i$. Portanto, ϕ é injetora se, e somente se, $\bigcap I_i = 0$. ■

Notemos que a *união* $I \cup J$ de dois ideais, em geral, não é um ideal. Por exemplo, em $\mathbb{Z}$, o conjunto $(2) \cup (7)$ não é subgrupo aditivo, e portanto, não é ideal.

Entretanto, quando se trata de ideais primos, são feitas afirmações mais precisas, conforme a seguinte proposição.

Proposição 1.43. *(i) Sejam $\mathcal{P}_1, ..., \mathcal{P}_n$ ideais primos e seja I um ideal contido em $\bigcup_{i=1}^{n} \mathcal{P}_i$. Então $I \subseteq \mathcal{P}_i$, para algum i.*

(ii) Sejam $I_1, ..., I_n$ ideais e sejam $\mathcal{P}$ um ideal primo contendo $\bigcap_{i=1}^{n} I_i$. Então $\mathcal{P} \supseteq I_i$ para algum i. Se $\mathcal{P} = \bigcap I_i$, então $\mathcal{P} = I_i$ para algum i.

Demonstração: (i) Provaremos por indução sobre n que

$$I \nsubseteq \mathcal{P}_i(1 \leq i \leq n) \Rightarrow I \nsubseteq \bigcup_{i=1}^{n} \mathcal{P}_i.$$

Claramente, este fato é válido para $n = 1$. Suponhamos $n > 1$ e que a afirmação é verdadeira para $n - 1$, então, pela hipótese de indução, para cada i existe $x_i \in I$ tal que $x_i \notin \mathcal{P}_j$, sempre que $i \neq j$. Se para algum i tivermos $x_i \notin \mathcal{P}_i$, o resultado está provado. Se $x_i \in \mathcal{P}_i$ para todo i, consideremos o elemento

$$y = \sum_{i=1}^{n} x_1 x_2 \cdots x_{i-1} x_{i+1} x_{i+2} \cdots x_n.$$

Pela escolha dos x_i, segue que $y \in I$ e $y \notin \mathcal{P}_i(1 \leq i \leq n)$. Daí, $I \nsubseteq \bigcup_{i=1}^{n} \mathcal{P}_i$.

(ii) Suponhamos $I \nsubseteq \bigcap P_i$ para todo i. Então existe $x_i \in I_i, x_i \notin P (1 \leq i \leq n)$, e assim $\prod x_i \in \prod I_i \subseteq \bigcap I_i$, mas $\prod x_i \notin P$, já que P é primo. Logo $P \nsupseteq \bigcap I_i$. Finalmente, se $P = \bigcap I_i$, então $P \subseteq I_i$, e portanto $P = I_i$ para algum i. ■

Se I, J são ideais em um anel R, o *ideal quociente* é

$$(I : J) = \{x \in R : xy \in I, \forall y \in J\},$$

que também é um ideal. Em particular, $(0 : J) = \{x \in R : xy = 0, \forall y \in J\}$ é chamado de *anulador* de J e também denotado por $\mathrm{Ann}(J)$. Nesta notação, o conjunto de todos os divisores de zero em R é

$$D = \bigcup_{x \neq 0} \mathrm{Ann}(x).$$

Se J é um ideal principal (x), escrevemos $(I : x)$ ao invés de $(I : (x))$.

Exemplo 1.44. *Consideremos o anel* $\mathbb{Z}$, *e os ideais* (3) *e* (2). *Temos que* $(3 : 2) = \{x \in \mathbb{Z} : x \cdot 2m = 3n;$ para algum $m, n\} = (3)$, *enquanto o* $\mathrm{Ann}(2) = \{0\}$.

Observemos que multiplicando dois elementos $x, y \in R$, o produto $x \cdot y$ pertence a algum ideal I. Podemos considerar, em particular, produtos $x \cdot x \cdot ... \cdot x = x^n$. No sentido inverso, se $x^n \in I$, definimos o *radical* de I como o conjunto

$$\mathrm{Rad}(I) = \{x \in R : x^n \in I \text{ para algum } n > 0\}.$$

Seja $\phi : R \to R/I$ o homomorfismo natural. Como

$$\Re_{R/I} = \left\{\overline{x} \in R/I : \overline{x}^n = \overline{0} \text{ para algun } n\right\} = \bigcap_{\substack{\mathcal{P} \subset R/I \\ \mathcal{P} \text{ primo}}} \mathcal{P},$$

temos que $\Re_{R/I}$ é ideal em R/I. Assim,

$$\phi^{-1}(\Re_{R/I}) = \{x \in R : \overline{x}^n \in I \text{ para algum } n\} = \mathrm{Rad}(I),$$

e portanto, $\mathrm{Rad}(I)$ é ideal em R.

Proposição 1.45. $(I : J)$ *e* $\mathrm{Rad}(I)$ *satisfazem as seguintes propriedades:*

(a) $I \subseteq (I : J)$.

(b) $(I : J)J \subseteq I$.

(c) $((I : J) : K) = (I : JK) = ((I : K) : J)$.

(d) $(\cap_i I_i : J) = \cap_i (a_i : J)$

(e) $(I \sum_i J_i) = \cap_i (I : J_i)$.

(f) $\mathrm{Rad}(I) \supseteq I$.

(g) $\mathrm{Rad}(\mathrm{Rad}(I)) = \mathrm{Rad}(I)$.

(h) $\mathrm{Rad}(IJ) = \mathrm{Rad}(I \cap J) = \mathrm{Rad}(I) \cap \mathrm{Rad}(J)$.

(i) $\mathrm{Rad}(I) = (1) \Leftrightarrow I = (1)$.

(j) $\mathrm{Rad}(I + J) = \mathrm{Rad}(\mathrm{Rad}(I) + \mathrm{Rad}(J))$.

(k) *se* $\mathcal{P}$ *é primo,* $\mathrm{Rad}(\mathcal{P}^n) = \mathcal{P}$ *para todo* $n > 0$.

Demonstração: Os itens (a) - (f) decorrem diretamente da definição.

(g) Pelo item (f), basta mostrar que $\mathrm{Rad}(\mathrm{Rad}(I)) \subseteq \mathrm{Rad}(I)$. De fato,

$$x \in \mathrm{Rad}(\mathrm{Rad}(I)) \Rightarrow x^n = x^{k \cdot m} \in \mathrm{Rad}(I) \Rightarrow x^k \in \mathrm{Rad}(I) \Rightarrow x \in \mathrm{Rad}(I).$$

(h) A segunda igualdade decorre diretamente da definição de radical e intersecção de conjuntos. Mostremos que $\mathrm{Rad}(IJ) = \mathrm{Rad}(I) \cap \mathrm{Rad}(J)$.

Como $IJ \subseteq I \cap J$, então $\mathrm{Rad}(IJ) \subseteq \mathrm{Rad}(I \cap J)$. Por outro lado, tomando $x \in \mathrm{Rad}(I \cap J)$, temos que $x^n \in I$ e $x^n \in J$, para algum n. Daí, $x^n \cdot x^n = x^{2n} \in IJ$, e então $x \in \mathrm{Rad}(IJ)$.

(i) Como $\mathrm{Rad}(I) \supseteq I$, se $I = (1)$, obviamente $\mathrm{Rad}(I) = (1)$. Reciprocamente, se $I \neq (1)$, então existiria $x \in (1), x \notin I$. Assim, $x^n \notin I$, para qualquer n, e $I \neq (1)$.

(j) Como $I \subseteq \mathrm{Rad}(I)$ e $J \subseteq \mathrm{Rad}(J)$, temos que $I + J \subseteq \mathrm{Rad}(I) + \mathrm{Rad}(J) \Rightarrow \mathrm{Rad}(I+J) \subseteq \mathrm{Rad}(\mathrm{Rad}(I)+\mathrm{Rad}(J))$. Agora, pelo item (f), $r(\mathrm{Rad}(I)+\mathrm{Rad}(J)) \subseteq \mathrm{Rad}(\mathrm{Rad}(\mathrm{Rad}(I)) + \mathrm{Rad}(\mathrm{Rad}(J))) \overset{(g)}{=} \mathrm{Rad}(I + J)$.

(k) Se $x \in \mathcal{P}$, então $x^n \in \mathcal{P}^n$ e $x \in \mathrm{Rad}(\mathcal{P}^n)$. Por outro lado, se $x \in \mathrm{Rad}(\mathcal{P}^n)$, temos que $x^m \in \mathcal{P}^n$ para algum m. Como $\mathcal{P}$ é primo, $x \in \mathcal{P}^n$ para qualquer $n > 0$; e então $x \in \mathcal{P}$.

■

A proposição a seguir nos fornece uma definição de $\mathrm{Rad}(I)$ em termos de ideais primos.

Proposição 1.46. *O radical de um ideal* I *é a intersecção dos ideias primos que contêm* I.

Demonstração: Pela Proposição 1.38, o nilradical $\Re_{R/I}$ é a intersecção de todos os ideais primos $\overline{J}$ de R/I. Como $J = \phi^{-1}(\overline{J})$ também são primos em R, e contêm I (pelo Corolário 1.19); então $\mathrm{Rad}(a) = \phi^{-1}(\Re_{R/I}) = \bigcap \phi^{-1}(\overline{J}) = \bigcap J$. ■

Analogamente, definimos o radical $\mathrm{Rad}(E)$ de qualquer subconjunto E de R que, em geral, não é um ideal. Temos $\mathrm{Rad}(\cup_\alpha E_\alpha) = \cup \mathrm{Rad}(E_\alpha)$ para qualquer família de subconjuntos E_α de R.

O conjunto dos divisores de zero de um anel R pode ser caracterizado em função de $\mathrm{Rad}(\mathrm{Ann}(x))$, como segue.

Proposição 1.47. *Seja D o conjunto dos divisores de zero do anel R. Então $D = \cup_{x\neq 0}\mathrm{Rad}(\mathrm{Ann}(x))$.*

Demonstração: Como $D = \bigcup_{x\neq 0} \mathrm{Ann}(x)$, temos $\mathrm{Rad}(D) = r\left(\bigcup_{x\neq 0} \mathrm{Ann}(x)\right)$. Mas $\mathrm{Rad}(D) = D$, pois $D \subseteq \mathrm{Rad}(D)$. Tomando $x \in \mathrm{Rad}(D)$, temos $x^n \in D$; e assim $x^n y = x(x^{n-1}y) = 0$. Logo $x \in D$ e $\mathrm{Rad}(D) \subseteq D$. Portanto $D = \mathrm{Rad}(D) = r\left(\bigcup_{x\neq 0} \mathrm{Ann}(x)\right) = \bigcup_{x\neq 0} r\left(\mathrm{Ann}(x)\right)$. ■

Exemplo 1.48. *Tomemos $R = \mathbb{Z}$ e $I = (m)$. Sejam $p_i (1 \leq i \leq r)$ os primos distintos divisores de m. Então* $\mathrm{Rad}(I) = (p_1 \cdots p_r) = \bigcap_{i=1}^{r}(p_i)$.

Como visto no Exemplo 1.40, em $\mathbb{Z}$, se m, n são primos entre si, então $(m) \cap (n) = (mn)$. Assim, a segunda igualdade é uma generalização deste fato. Vejamos a primeira igualdade. Se $x \in \mathrm{Rad}(I) \Rightarrow x^n \in I \Rightarrow x^n = am$, então $x = b \cdot (p_1 \cdots p_r)$. Por outro lado, se $x \in (p_1 \cdots p_r)$, temos $x = k \cdot p_1 \cdots p_r \Rightarrow x^n = (k \cdot p_1 \cdots p_r)^n = h \cdot p_1 \cdots p_r$. Logo $x^n \in (p_1 \cdots p_r)$, e $x \in I$.

Proposição 1.49. *Sejam I, J ideais de um anel R tais que* $\mathrm{Rad}(I), \mathrm{Rad}(J)$ *são comaximais. Então I, J são comaximais.*

Demonstração: Como $\mathrm{Rad}(I) + \mathrm{Rad}(J) = (1)$, pois $\mathrm{Rad}(I)$ e $\mathrm{Rad}(J)$ são comaximais; temos $r\left(\mathrm{Rad}(I) + \mathrm{Rad}(J)\right) = \mathrm{Rad}(1)$. Mas pelas propriedades (i) e (j), obtemos $\mathrm{Rad}(I + J) = r\left(\mathrm{Rad}(I) + \mathrm{Rad}(J)\right) = \mathrm{Rad}(1) = (1)$, e portanto $I + J = (1)$. ■

1.8 Extensão e Contração de Ideais

Seja $f : R \to S$ um homomorfismo de anéis. Se I é um ideal em R, o conjunto $f(I)$ não é, necessariamente, um ideal em S. Por exemplo, considere f o mergulho de $\mathbb{Z}$ em $\mathbb{Q}$, e tome I como sendo um ideal não nulo qualquer em $\mathbb{Z}$: $f(I) \neq \{0\}$ que não é ideal em $\mathbb{Q}$, pois este é corpo.

Definimos a *extensão* I^e de I como sendo o ideal $Sf(I)$ gerado por $f(I)$ em S. Explicitamente, I^e é o conjunto de todas as somas $\sum y_i f(x_i)$, onde $x_i \in I$ e $y_i \in S$.

Se J é um ideal em S, então $f^{-1}(J)$ é um ideal em R, chamado de *contração* J^c de J. Se J é primo, então J^c é primo. Se I é primo, em geral I^e não é primo. Por exemplo, considere $f : \mathbb{Z} \to \mathbb{Q}$, $I \neq 0$; então $I^e = \mathbb{Q}$ que não é um ideal primo.

Considerando $f : R \to S$ e I, J ideais em R e S, respectivamente, temos a seguinte

Proposição 1.50. (i) $I \subseteq I^{ec}$, $J \supseteq J^{ce}$.

(ii) $J^c = J^{cec}$, $I^e = I^{ece}$.

(iii) *Se T é o conjunto dos ideais contraídos em R e se E é o conjunto dos ideais extendidos em S, então $T = \{I : I^{ec} = I\}$, $E = \{J : J^{ce} = J\}$, e $I \mapsto I^e$ é uma bijeção de T em E, cuja inversa é $J \mapsto J^c$.*

Demonstração:(i) Se $x \in I$, então $f(x) \in f(I) \Rightarrow f(x) \in I^e \Rightarrow x \in (I^e)^c$; e portanto, $I \subseteq I^{ec}$.

Agora, se $y \in J^{ce}$, $y \in \sum y_i f(f^{-1}(J)) \subseteq J$.

(ii) Como $J^c \subseteq J^{cec}$ e $I^{ece} \subseteq I^e$ segue diretamente de (i); basta mostrar as inclusões inversas. Obviamente, estas também são simples aplicações de (i):

$$J^{ce} \subseteq J \Rightarrow (J^{ce})^e \subseteq J^c$$

e

$$I^{ce} \subseteq I \Rightarrow (I^e)^{ce} \subseteq I^e.$$

(iii) Claramente, se $I \in T$, então $I = J^c$ e, por (ii), $J = J^{cec}$. Logo $I = I^{ec}$. Analogamente, se $J \in E$, $J = I^e \overset{(ii)}{=} I^{ece}$, temos que $J = I^e$.

Sejam $f : C \to E$, $I \mapsto I^e$; e $g : E \to T$, $J \mapsto J^c$. Como

$$(g \circ f)(I) = g(f(I)) = g(I^e) = I^{ec} = I$$

e

$$(f \circ g)(J) = f(g(J)) = f(J^c) = J^{ce} = J,$$

vemos que as funções são bijetoras e inversas uma da outra. ■

Capítulo 2

Módulos

Este capítulo é dedicado ao estudo de módulos e algumas de suas propriedades, uma vez que anéis, ideais e anéis quociente, são exemplos de módulos. Assim, os resultados apresentados a seguir também são válidos para estas estruturas.

2.1 Módulos e Homomorfismo de Módulos

Seja R uma anel. Um *R-módulo* é um grupo abeliano M (em relação à operação de adição) sobre o qual R age linearmente: mais precisamente, um R-módulo é um par (M, μ), onde M é um grupo abeliano e $\mu : R \times M \to M$ é uma aplicação tal que, se escrevermos ax para $\mu(a, x)$, com $a \in R, x \in M$, satisfaz os seguintes axiomas:

$$a(x + y) = ax + ay,$$

$$(a + b)x = ax + bx,$$

$$(ab)x = a(bx),$$

$$1x = x$$

para $a, b \in R$ e $x, y \in M$.

Exemplo 2.1. *Um ideal I em R é um R-módulo. Em particular, R é um R-módulo: basta considerar que a multiplicação de elementos de R satisfaz as propriedades mencionadas acima.*

Exemplo 2.2. *Se R é um corpo K, então um R-módulo é um espaço vetorial sobre K. Claramente, tomando os escalares em K, as propriedades de módulo são aquelas que definem um espaço vetorial sobre o corpo K.*

Sejam M, N dois R-módulos. Uma função $f : M \to N$ é um *homomorfismo de R-módulos* se

$$f(x+y) = f(x) + f(y)$$

$$f(ax) = a \cdot f(x)$$

para todo $a \in R$ e todo $x, y \in M$. Então f é um homomorfismo de grupos abelianos que comuta com a ação de cada $a \in R$.

Exemplo 2.3. *Se R é um corpo, um homomorfismo de R-módulos é o mesmo que uma transformação linear de espaços vetoriais.*

Como para o caso geral de anéis, a composição de um homomorfismo de R-módulos é ainda um homomorfismo de R-módulos.

O conjunto de todos os homomorfismos de R-módulos de M em N pode ser transformado em um R-módulo da seguinte maneira: defina $f+g$ e $a \cdot f$ como

$$(f+g)(x) = f(x) + g(x),$$

$$(a \cdot f)(x) = a \cdot f(x)$$

para todo $x \in M$.

Claramente, os axiomas para R-módulos estão satisfeitos.

Este R-módulo é denotado por $\mathrm{Hom}_R(M, N)$. No caso de não haver ambiguidade em relação ao anel R, denotamos apenas por $\mathrm{Hom}(M, N)$.

Os homomorfismos $u : M' \to M$ e $v : N \to N''$ induzem aplicações

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

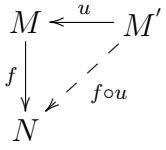
e

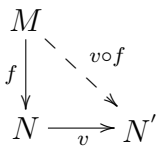
$$\overline{v} : \mathrm{Hom}(M, N) \to \mathrm{Hom}(M, N''),$$

definidos por

$$\overline{u}(f) = f \circ u,\ \overline{v}(f) = v \circ f,$$

que são homomorfismo de R-módulos. Os seguintes diagramas explicitam a definição de $\overline{u}$ e $\overline{v}$.





Para qualquer módulo M existe um homomorfismo natural $\mathrm{Hom}(R, M) \cong M$. De fato, tomemos $g : \mathrm{Hom}(R, M) \to M$ tal que $g(f) = f(1)$, onde $f : R \to M$ é homomorfismo de R-módulos. Naturalmente, g é homomorfismo e $\ker g = \{f \equiv 0\}$.

2.2 Submódulos e Módulos Quocientes

Um *submódulo* M' de M é um subgrupo de M fechado em relação à multiplicação por elementos de R. O grupo abeliano M/M' herda a estrutura de R-módulo de M, definida por $a(x+M') = ax + M'$. O R-módulo M/M' é o *quociente* de M por M'.

A função natural de M em M/M' é um homomorfismo de R-módulos. Assim, existe uma correspondência biunívoca que preserva a ordem entre submódulos de M que contém M', e submódulos de M/M'.

Se $f : M \to N$ é um homomorfismo de R-módulos, o *núcleo* de f, $\ker f = \{x \in M : f(x) = 0\}$, é um submódulo de M. A *imagem* de f, $\mathrm{Im}(f) = f(M)$, também é um submódulo de N. O *conúcleo* de f é

$$\mathrm{Coker}(f) = N/\mathrm{Im}(f)$$

que é um módulo quociente de N.

Se M' é um submódulo de M tal que $M' \subseteq \ker f$, então a aplicação

$$\begin{aligned} \overline{f} \quad : \quad & \frac{M}{M'} \longrightarrow N \\ & \overline{x} \longmapsto \overline{f}(\overline{x}) = f(x) \end{aligned}$$

está bem definida. De fato, se $\overline{x}, \overline{y} \in M/M'$ com $\overline{x} = \overline{y}$, temos $x - y \in M'$ e $f(x-y) = 0$, pois $M' \subseteq \ker f$. Como f é homomorfismo, $0 = f(x-y) = f(x) - f(y)$, e logo, $\overline{f}(\overline{x}) = f(x) = f(y) = \overline{f}(\overline{y})$. Claramente, $\overline{f}$ é um homomorfismo de R-módulos, e $\ker \overline{f} = \frac{\ker f}{M'}$.

O homomorfismo $\overline{f}$ é dito *induzido* por f. Em particular, tomando $M' = \ker f$, temos um isomorfismo de R-módulos

$$\frac{M}{\ker f} \cong \mathrm{Im}(f).$$

2.3 Operações em Submódulos

Seja M um R-módulo e seja $(M_i)_{i \in I}$ uma família de submódulos de M. A *soma* $\sum M_i$ é o conjunto de todas as somas $\sum x_i$, onde $x_i \in M_i$ para todo $i \in I$, e $x_i = 0$ a menos para um número finito de índices. $\sum M_i$ é o menor submódulo de M que contém todos os M_i, e a intersecção $\bigcap M_i$ é um submódulo de M.

Proposição 2.4. (i) *Se $L \supseteq M \supseteq N$ são R-módulos, então*

$$\frac{(L/N)}{(M/N)} \cong \frac{L}{M}.$$

(ii) *Se M_1, M_2 são submódulos de M, então*

$$\frac{M_1 + M_2}{M_1} \cong \frac{M_2}{M_1 \cap M_2}.$$

Demonstração: (i) Definindo $\theta : L/N \to L/M$ por $\theta(x + N) = x + M$, temos que θ é um homomorfismo de R-módulos de L/N em L/M, e seu núcleo é M/N. Logo, temos (i).

(ii) Consideremos a composição

$$M_2 \xrightarrow{f} M_1 + M_2 \xrightarrow{g} \frac{M_1 + M_2}{M_1}.$$

Como $\ker g \circ f = \{x \in M_2 : (g \circ f)(x) = 0\} = \{x \in M_2 : x + M_1 = 0\}$, temos que $x \in \ker g \circ f \Rightarrow x \in M_1 \cap M_2$. Além disso, $g \circ f$ é um homomorfismo sobrejetor, e portanto

$$\frac{M_2}{M_1 \cap M_2} \cong \frac{M_1 + M_2}{M_1}.$$

■

Em geral, não definimos os *produto* de dois submódulos, mas definimos o produto IM, onde I é um ideal e M um R-módulo. Este produto é o conjunto de todas as somas finitas $\sum a_i x_i$ com $a_i \in I$ e $x_i \in M$, e é um submódulo de M.

Se N, P são submódulos de M, definimos $(N : P)$ como o conjunto de todos os $a \in R$ tais que $aP \subseteq N$; e é um ideal de R. Em particular, $(0 : M)$ é o conjunto de todos os $a \in R$ tais que $aM = 0$; e este ideal é chamado de *anulador* de M e denotado por $\mathrm{Ann}(M)$. Se $I \subseteq \mathrm{Ann}(M)$, podemos considerar M como um R/I-módulo, como segue: se $\overline{x} \in R/I$ é representado por $x \in R$, definimos $\overline{x}m$ por xm $(m \in M)$. Este processo é independente da escolha dos representantes x de $\overline{x}$, uma vez que $IM = 0$. Com efeito, seja $\overline{x} = x + I = y + I$. Assim, $x - y \in I \subseteq \mathrm{Ann}(M)$ e $(x - y) \cdot m = 0$, para qualquer $m \in M$; logo $xm = ym$.

No caso de $\mathrm{Ann}(M) = 0$, dizemos que M é um R-módulo *fiel*. Se $\mathrm{Ann}(M) = I$, então M é fiel como um R/I-módulo.

A proposição a seguir apresenta algumas propriedades satisfeitas por $\mathrm{Ann}(M)$.

Proposição 2.5. (i) $\mathrm{Ann}(M + N) = \mathrm{Ann}(M) \cap \mathrm{Ann}(N)$.

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

Demonstração: (i) Se $x \in \mathrm{Ann}(M + N)$, então $x(m + n) = 0$ para quaisquer $m \in M, n \in N$. Em particular, fazendo $m = 0$, temos que $xn = 0 \Rightarrow x \in \mathrm{Ann}(N)$. Da mesma forma, se $n = 0$, $xm = 0 \Rightarrow x \in \mathrm{Ann}(M)$. Logo $x \in \mathrm{Ann}(M) \cap \mathrm{Ann}(N)$.

Por outro lado, se $x \in \text{Ann}(M) \cap \text{Ann}(N)$, temos que $xm = 0 = xn$ para quaisquer $m \in M, n \in N$. Daí $xm - xn = x(m-n) = 0$, com $m-n \in M+N$; e portanto, $x \in \text{Ann}(M+N)$.

(ii) Se $x \in (N : P)$, então $xP \subseteq N$. Como $xP \subseteq x(P+N) \subseteq N$, temos que $x \cdot \frac{P+N}{N} = 0$ e $x \in \text{Ann}\left(\frac{N+P}{N}\right)$.

Reciprocamente, $x \in \text{Ann}\left(\frac{N+P}{N}\right) \Rightarrow x \cdot \frac{P+N}{N} = 0$. Daí $x(N+P) \subseteq N$, isto é, $xN + xP \subseteq N$; e portanto $xP \subseteq N \Rightarrow x \in (N : P)$. ■

2.4 Soma Direta e Produto Direto

Se M, N são R-módulos, a *soma direta* $M \oplus N$ é o conjunto de todos os pares (x, y) com $x \in M, y \in N$. Este conjunto é um R-módulo se definirmos a adição e a multiplicação por escalar como segue:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2),$$

$$a(x, y) = (ax, ay).$$

Mais geralmente, se $(M_i)_{i \in I}$ é uma família de R-módulos, podemos definir a soma direta $\oplus_{i \in I} M_i$: seus elementos são famílias $(x_i)_{i \in I}$ tais que $x_i \in M_i$ para cada $i \in I$ e quase todos os x_i são zero.

Se não considerarmos a condição sobre a quantidade de x_i não nulos, temos o *produto direto* $\prod_{i \in I} M_i$. Dessa forma, soma e produto direto são equivalentes apenas se o conjunto de índices I for finito.

Suponha que o anel R é um produto direto $\prod_{i=1}^{n} R_i$. Então o conjunto de todos os elementos de R da forma

$$(0, ..., 0, a_i, 0, ...0)$$

com $a_i \in R_i$, é um ideal I_i de R (não é um subanel de R - exceto no caso trivial - pois não contém o elemento identidade em R). O anel R, considerado como um R-módulo, é a soma direta dos ideais $I_1, ..., I_n$.

Por outro lado, dada uma decomposição de módulo

$$R = I_1 \oplus ... \oplus I_n$$

de R como uma soma direta de ideais, temos

$$R \cong \prod_{i=1}^{n} \frac{R}{J_i}$$

onde $J_i = \oplus_{j \neq i} I_j$. Explicitamente, temos:

$$\frac{R}{J_1} = \frac{I_1 \oplus \cdots \oplus I_n}{I_2 \oplus I_3 \oplus \cdots \oplus I_n} \cong I_1;$$
$$\frac{R}{J_2} = \frac{I_1 \oplus \cdots \oplus I_n}{I_1 \oplus I_3 \oplus \cdots \oplus I_n} \cong I_2;$$
$$\vdots$$
$$\frac{R}{J_n} = \frac{I_1 \oplus \cdots \oplus I_n}{I_1 \oplus I_2 \oplus \cdots \oplus I_{n-1}} \cong I_n.$$

Assim, cada ideal I_i é um anel (isomorfo a R/J_i). O elemento identidade e_i de I_i é um elemento idempotente em R, e $I_i = (e_i)$.

2.5 Módulos Finitamente Gerados

Se x é um elemento de M, o conjunto de todos os múltiplos $ax (a \in R)$ é um submódulo de M, denotado por Rx ou (x). Se $M = \sum_{i \in I} Rx_i$, os x_i são chamados de *geradores* de M: isto significa que todo elemento de M pode ser expresso (não necessariamente de forma única) como uma combinação linear finita de x_i com coeficientes em R. Dizemos que um R-módulo M é *finitamente gerado* se possui um conjunto finito de geradores.

Exemplo 2.6. *$n\mathbb{Z}$ é um $\mathbb{Z}$-módulo finitamente gerado por $n \in \mathbb{Z}$.*

Um R-módulo *livre* é isomorfo a um R-módulo da forma $\oplus_{i \in I} M_i$, onde cada $M_i \cong R$. Assim, um R-módulo livre finitamente gerado é isomomorfo a $R \oplus \cdots \oplus R$ (n parcelas), denotado por R^n. Por convenção, R^0 é o módulo nulo, denotado por 0.

Proposição 2.7. *M é um R-módulo finitamente gerado se, e somente se, M é isomorfo a um quociente de R^n para algum inteiro $n > 0$.*

Demonstração: Sejam $x_1, \cdots, x_n$ os geradores de M. Defina $\phi : R^n \to M$ como $\phi(a_1, \cdots, a_n) = a_1x_1 + \cdots + a_nx_n$, temos que ϕ é um homomorfismo sobrejetor de R-módulos. De fato,

$$\begin{aligned} \phi\left((a_1, ..., a_n) + (b_1, ..., b_n)\right) &= \phi\left(a_1 + b_1, ..., a_n + b_n\right) \\ &= (a_1 + b_1)x_1 + \cdots + (a_n + b_n)x_n \\ &= (a_1x_1 + \cdots + a_nx_n) + (b_1x_1 + \cdots + b_nx_n) \\ &= \phi(a_1, ..., a_n) + \phi(b_1, ..., b_n) \end{aligned}$$

e

$$\begin{aligned}\phi\left(b\cdot(a_1,...,a_n)\right) &= \phi\left(ba_1,...,ba_n\right) = ba_1x_1+\cdots+ba_nx_n \\ &= b\cdot(a_1x_1+\cdots a_nx_n) = b\cdot\phi\left((a_1,...,a_n)\right)\end{aligned}$$

Além disso, dado $m\in M$, temos que $m = c_1x_1+\cdots+c_nx_n$ para certos $c_1,...,c_n\in R$; isto é, $\phi(c_1,...,c_n)=m$. Logo $M\cong\frac{R^n}{\mathrm{Ker}(\phi)}$.

Por outro lado, consideramos um homomorfismo de R-módulos sobrejetor $\phi: R^n\to M$. Se $e_i = (0,0,\cdots,0,1,0,\cdots,0)$ (com 1 na i-ésima posição), então os e_i $(1\leq i\leq n)$ são geradores de R^n. Então, $\phi(e_i)=x_i$ geram M. ■

Proposição 2.8. *Sejam M um R-módulo finitamente gerado, I um ideal de R, e ϕ um endomorfismo de R-módulos em M tal que $\phi(M)\subseteq IM$. Então ϕ satisfaz uma equação da forma*

$$\phi^n + a_1\phi^{n-1}+\cdots+a_n = 0$$

com $a_i\in I$.

Demonstração: Sejam $x_1,\cdots x_n$ geradores de M. Então cada $\phi(x_i)\in IM$, pois $\phi(M)\subseteq IM$. Assim, podemos escrever $\phi(x_i) = a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n = \sum_{j=1}^n a_{ij}x_j$, com $1\leq i\leq n$ e $a_{ij}\in I$. Isto é,

$$\phi(x_i)-\sum_{j=1}^n a_{ij}x_j = 0 \Longrightarrow \sum_{j=1}^n\left(\delta_{ij}\phi-a_{ij}\right)x_j = 0$$

onde δ_{ij} é o Delta de Kronecker.

Multiplicando o lado esquerdo pela adjunta da matriz $(\delta_{ij}\phi-a_{ij})$, obtemos $(\det(\delta_{ij}\phi-a_{ij}))(x_j)$. Segue que o determinante de $(\delta_{ij}\phi-a_{ij})$ anula cada x_i, e então é o endomorfismo nulo de M. Expandindo o determinante

$$\begin{vmatrix} \phi-a_{11} & -a_{12} & \cdots & -a_{1n} \\ -a_{21} & \phi-a_{22} & \cdots & -a_{2n} \\ \vdots & & & \vdots \\ -a_{n1} & -a_{n2} & \cdots & \phi-a_{nn}\end{vmatrix}$$

obtemos uma equação da forma desejada. ■

Corolário 2.9. *Seja M um R-módulo finitamente gerado e seja I um ideal de R tal que $IM=M$. Então existe $x\equiv 1(\mathrm{mod}\ I)$ tal que $xM=0$.*

Demonstração: Tomando ϕ como a identidade na Proposição 2.8, temos

$$\phi^n(x) + a_1\phi^{n-1}(x) + \cdots + a_n = 0 \Rightarrow 1 + a_1 + \cdots + a_n = 0.$$

Portanto, $x = a_1' + \cdots + a_n'$, onde $a_i' = -a_i \in I$. ■

A seguir, apresentamos o famoso *Lema de Nakayama* e duas demonstrações distintas.

Proposição 2.10 (Lema de Nakayama)**.** *Seja M um R-módulo finitamente gerado e I um ideal de R contido no radical de Jacobson ${}_J\Re$ de R. Então $IM = M$ implica $M = 0$.*

Primeira demonstração: Pelo resultado anterior, temos que $xM = 0$ para algum $x \equiv 1(\text{mod } {}_J\Re)$. Pela Proposição 1.39 x é uma unidade em R, e assim $M = x^{-1}xM = 0$. ■

Segunda demonstração: Suponha $M \neq 0$ e sejam $u_1, \cdots, u_n$ um conjunto mínimo de geradores de M. Então $u_n \in IM = M$, e temos uma equação da forma $u_n = a_1u_1 + \cdots a_nu_n$, com $a_i \in I$. Assim

$$(1 - a_n)u_n = a_1u_1 + \cdots + a_{n-1}u_{n-1};$$

e como $a_n \in {}_J\Re$, segue de Proposição 1.39 que $1 - a_n$ é uma unidade em R. Daí u_n pertence ao submódulo de M gerado por $u_1, \cdots u_{n-1}$; contradição. ■

Corolário 2.11. *Sejam M um R-módulo finitamente gerado, N um submódulo de M e $I \subseteq {}_J\Re$ um ideal. Então $M = IM + N \Rightarrow M = N$.*

Demonstração: Na Proposição 2.4-(ii), sejam $M_1 = N$ e $M_2 = IM$. Assim

$$\frac{M_1 + M_2}{M_1} = \frac{IM + N}{N} \cong I\frac{M}{N} = \frac{M_2}{M_1 \cap M_2}.$$

Dessa forma, $I\left(\frac{M}{N}\right) = \frac{IM+N}{N} = \frac{M}{N}$, e pelo Lema de Nakayama, $\frac{M}{N} = 0$. Portanto, $M = N$. ■

Seja R um anel local, $\mathcal{M}$ seu ideal maximal, $K = R/\mathcal{M}$ seu corpo residual. Seja M um R-módulo finitamente gerado. Como $M/\mathcal{M}M$ é anulado por $\mathcal{M}$, temos que $M/\mathcal{M}M$ é naturalmente um $\frac{R}{\mathcal{M}}$-módulo, isto é, um espaço K-vetorial de dimensão finita. De fato, tomemos $a + \mathcal{M} = \overline{a} \in \frac{R}{\mathcal{M}}$ e $x + \mathcal{M}M = \overline{x} \in \frac{M}{\mathcal{M}M}$. Assim, $\overline{a} \cdot \overline{x} = (a + \mathcal{M}) + (x + \mathcal{M}M) = ax$ é uma multiplicação bem definida.

Proposição 2.12. *Sejam $x_i (1 \leq i \leq n)$ elementos de M cujas imagems em $M/\mathcal{M}M$ formam uma base para este espaço vetorial. Então os x_i geram M.*

Demonstração: Seja N o sumbódulo de M gerado pelos x_i. Consideremos a composição

$$N \xrightarrow{\iota} M \xrightarrow{\phi} \frac{M}{\mathcal{M}M} \longrightarrow 0 \qquad (f = \phi \circ \iota)$$

onde ι é a inclusão e ϕ o homomorfismo natural. Assim, $f = \phi \circ \iota$, e $\ker f = \{x \in N : x + \mathcal{M}M = 0\} = \{x \in N : x \in \mathcal{M}M\} = N \cap \mathcal{M}M$. Logo

$$\frac{M}{\mathcal{M}M} \cong \frac{N}{N \cap \mathcal{M}M},$$

e pela Proposição 2.4-(ii)

$$\frac{N + \mathcal{M}M}{\mathcal{M}M} \cong \frac{N}{N \cap \mathcal{M}M}.$$

Por transitividade,

$$\frac{N + \mathcal{M}M}{\mathcal{M}M} \cong \frac{M}{\mathcal{M}M};$$

e assim $N + \mathcal{M}M = M$. Como $\mathcal{M} \subseteq {}_J\Re$, podemos aplicar o Corolário 2.11, obtendo $M = N$. ■

2.6 Sequências Exatas

Uma sequência de R-módulos e R-homomorfismos

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

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

(i) $0 \to M' \xrightarrow{f} M$ é exata $\iff$ f é injetora.

Obviamente, $\ker f = \{0\}$ se, e somente se, f é injetora.

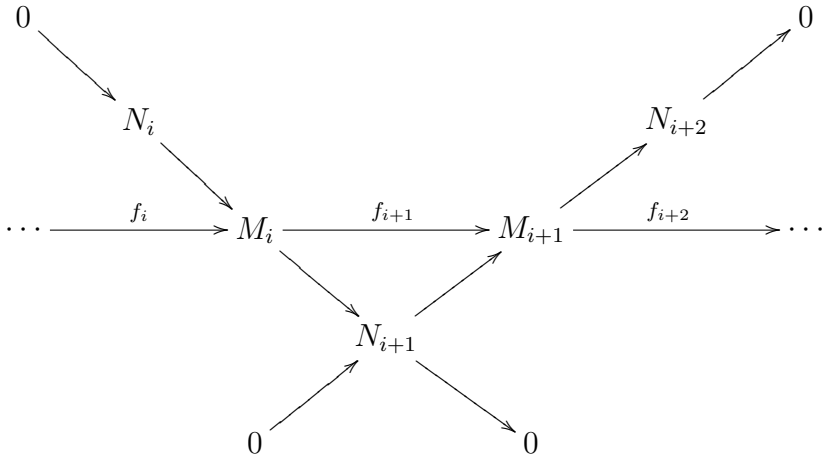
(ii) $M \xrightarrow{g} M'' \to 0$ é exata $\iff$ g é sobrejetora.

De fato, se g é sobrejetora, então $\mathrm{Im}(g) = M'' = \ker 0$; onde 0 é a função identicamente nula. Por outro lado, se a sequência é exata, $\ker 0 = M'' = \mathrm{Im}(g)$; e logo g é sobrejetora.

(iii) $0 \to M' \xrightarrow{f} M \xrightarrow{g} M'' \to 0$ é exata $\iff$ f é injetora, g é sobrejetora e g induz um homomorfismo sobrejetor de $\mathrm{Coker}(f) = M/f(M')$ em M''.

Basta verificar a equivalência para a condição $\text{Coker}(f) = M/f(M') \cong M''$. Se a sequência é exata, g homomorfismo sobrejetor e $f(M') = \text{Im}(f) = \ker g$. Daí $\frac{M}{\ker g} = \frac{M}{f(M')} \cong M''$. Reciprocamente, g é um homomorfismo sobrejetor, cujo núcleo é $\ker g = f(M') = \text{Im}(f)$.

Uma sequência como em (iii) é chamada de *sequência exata curta*. Qualquer sequência exata pode ser decomposta em sequências exatas curtas da seguinte forma: se $N_i = \text{Im}(f_i) = \text{Ker}(f_{i+1})$, temos sequências exatas curtas $0 \to N_i \to M_i \to N_{i+1} \to 0$, para cada i. O diagrama a seguir esboça esta situação:



Proposição 2.13. *(i) Seja*

$$M' \xrightarrow{u} M \xrightarrow{v} M'' \to 0$$

uma sequência de R-módulos e homomorfismos. Então esta sequência é exata $\Leftrightarrow$ para todo R-módulo N, a sequência

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

é exata.

(ii) Seja

$$0 \to N' \xrightarrow{u} N \xrightarrow{v} N''$$

uma sequência de R-módulos e homomorfismos. Então esta sequência é exata $\Leftrightarrow$ para todo R-módulo M, a sequência

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

é exata.

Demonstração: (i) [⇒] Construímos o diagrama a seguir para orientar a prova.

$$\begin{array}{ccccccc} M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow f & \swarrow g & & & \\ & & N & & & & \end{array}$$

Suponhamos que v é homomorfismo sobrejetor, e que $\ker \overline{u} = \mathrm{Im}(\overline{v})$. Primeiramente, mostremos que $\overline{v}$ é injetor, onde $\overline{v}(f) = f \circ v$. Como v é sobrejetor, para qualquer $y \in M''$, existe $x \in M$ tal que $v(x) = y$. Assim, se $\overline{v}(f)(y) = \overline{v}(h)(y)$, para qualquer $y \in M''$, então $f(y) = f \circ v(x) = h \circ v(x) = h(y)$, e $\overline{v}$ é injetor.

Agora, tomemos $f \in \ker \overline{u}$ e então, $\overline{u}(f)(x) = f \circ u(x)$ para todo $x \in M'$. Sendo v sobrejetor, para cada $y \in M''$, existe $x \in M$ tal que $v(x) = y$. Definindo

$$\begin{array}{rcl} g : M'' & \longrightarrow & N \\ y & \longmapsto & f(x) \end{array}$$

obtemos que $\overline{v}(g) = g \circ v = f$, e portanto, $f \in \mathrm{Im}(\overline{v})$. A função g está bem definida pois, se $v(x_1) = v(x_2) = y$, temos

$$v(x_1 - x_2) = v(x_1) - v(x_2) = 0 \Rightarrow x_1 - x_2 \in \ker v = \mathrm{Im}(u),$$

e daí $x_1 - x_2 = u(z)$ para algum $z \in M'$. Logo $f(x_1 - x_2) = f \circ u(z) = 0$, e $f(x_1) = f(x_2)$.

Por fim, se $f \in \mathrm{Im}(\overline{v})$, então existe $g \in \mathrm{Hom}(M'', N)$ tal que $\overline{g} = g \circ v = f$. Como

$$\overline{u}(f) = f \circ u = (g \circ v) \circ u = g \circ (v \circ u)$$

e $v \circ u \equiv 0$ pois $\ker v = \mathrm{Im}(u)$, obtemos

$$\overline{u}(f) = g \circ 0 \equiv 0.$$

Portanto, $f \in \ker \overline{u}$.

[⇐] Devemos mostrar que v é sobrejetor e que $\ker v = \mathrm{Im}(u)$. A sobrejetividade v decorre da injetividade de $\overline{v}$. De fato, se v não é sobrejetor, então existe $y \in M''$ tal que $y \neq v(x)$ para todo $x \in M$. Sejam $\alpha : M'' \to N$, e

$$\begin{array}{rcl} \beta : M'' & \longrightarrow & N \\ m & \longmapsto & \alpha(m) \ (m \neq y) \\ \beta(y) & \neq & \alpha(y) \end{array}$$

Para $x \in M$, temos:

$$\begin{aligned} \overline{v}(\alpha)(x) &= \alpha \circ v(x) \\ \overline{v}(\beta)(x) &= \beta \circ v(x) = \alpha \circ v(x) \text{ , pois } v(x) \neq y \end{aligned}$$

Logo $\overline{v}(\alpha) = \overline{v}(\beta)$ com $\alpha \neq \beta$; contrariando a injetividade de $\overline{v}$.

Tomando $N = \frac{M}{\mathrm{Im}(u)}$ e $\phi : M \to N$ o homomorfismo natural, então $\phi \in \ker \overline{u}$, uma vez que $\mathrm{Im}(u) = \ker \phi$. Como $\ker \overline{u} = \mathrm{Im}(\overline{v})$, existe $\psi : M'' \to N$, tal que $\overline{v}(\psi) = \psi \circ v = \phi$. Consequentemente, $\mathrm{Im}(u) = \ker \phi$, pela definição de ϕ, e $\ker \phi \supseteq \ker v$.

(ii)[$\Rightarrow$] Novamente, construímos um diagrama para auxiliar na demonstração.

$$\begin{array}{ccccccc} & & & & M & & \\ & & & & \downarrow f & \searrow^{g} & \\ 0 & \longrightarrow & N' & \xrightarrow[u]{} & N & \xrightarrow[v]{} & N'' \end{array}$$

Mostremos que $\overline{u}$ é injetor e que $\ker \overline{v} = \mathrm{Im}(\overline{u})$. Seja $f \in \ker \overline{u}$, isto é, $f \in \mathrm{Hom}(M, N')$ tal que $\overline{u}(f)(x) = 0$ para todo $x \in M$. Como $\overline{u}(f)(x) = u \circ f(x) = 0$ e u é injetor, $f \equiv 0$; e portanto $\overline{u}$ é injetor.

Como $v \circ u \equiv 0$, temos que $(\overline{v} \circ \overline{u})(f) = (v \circ u) \circ f \equiv 0$, para qualquer $f \in \hom(M, N')$. Assim, $\mathrm{Im}(\overline{u}) \subseteq \ker \overline{v}$.

Tomando $f \in \ker \overline{v}$, temos que $\overline{v}(f)(x) = v \circ f(x) = 0$ para todo $x \in M$. Como $\mathrm{Im}(u) = \ker v$, obviamente $f(x) \in \mathrm{Im}(u)$ e $f(x) = u(z)$ para algum $z \in N'$. Definindo a função

$$\begin{aligned} g : M &\longrightarrow N' \\ x &\longmapsto z \text{ (com } u(z) = f(x)) \end{aligned}$$

para $x \in M$, obtemos

$$\overline{u}(g)(x) = u \circ g(x) = u(g(x)) = u(z) = f(x);$$

e portanto, $f \in \mathrm{Im}(\overline{u})$. Notemos que g está bem definida, uma vez que u é injetor.

[$\Leftarrow$] Como $\overline{u}$ é injetor, então $\ker \overline{u} = \{0\}$. Vemos facilmente que $\ker u \subseteq \ker \overline{u}$, pois tomando $f \in \ker u$, temos $0 \equiv u \circ f = \overline{u}(f)$ e $f \in \ker \overline{u}$. Logo, $\ker u = \{0\}$.

Para $g \in \ker \overline{v}$, temos que $\overline{v}(g)(x) = v(g(x)) = 0$. Se $g(x) = y$, temos que $y \in \ker v$. Mas, sendo a sequência exata, temos que $\overline{u}(f) = g$ para

algum $f \in \mathrm{Hom}(M, N')$. Assim, $\overline{u}(f)(x) = (u \odot f)(x) = u(f(x)) = g(x) = y$, e logo, $y \in \mathrm{Im}(u)$. Portanto, $\ker v \subseteq \mathrm{Im}(u)$.

Como $\overline{v} \circ \overline{u} \equiv 0$, temos que $v \circ u \circ f \equiv 0$ para todo $f \in \mathrm{Hom}(M, N')$. Em particular, tomando $M = N'$ e f a identidade, concluímos que $v \circ u \equiv 0$, e assim $\mathrm{Im}(u) \subseteq \ker v$. ■

Proposição 2.14. *Seja*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \xrightarrow{u} & M & \xrightarrow{v} & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & N' & \xrightarrow[u']{} & N & \xrightarrow[v']{} & N'' & \longrightarrow & 0 \end{array}$$

um diagrama comutativo de R-módulos e homomorfismos, com as linhas exatas. Então existe uma sequência exata

$$0 \to \mathrm{Ker}(f') \xrightarrow{\overline{u}} \ker(f) \xrightarrow{\overline{v}} \mathrm{Ker}(f'') \xrightarrow{d} \mathrm{Coker}(f') \xrightarrow{\overline{u'}} \mathrm{Coker}(f) \xrightarrow{\overline{v'}} \mathrm{Coker}(f'') \to 0$$

onde $\overline{u}$, $\overline{v}$ *são restrições de* u, v; *e* $\overline{u'}, \overline{v'}$ *são induzidos por* u', v'.

O *homomorfismo de fronteira* d é definido como segue: se $x'' \in \mathrm{Ker}(f'')$, temos $x'' = v(x)$ para algum $x \in M$, e $v'(f(x)) = f''(v(x)) = 0$. Daí $f(x) \in \mathrm{Ker}(v') = \mathrm{Im}(u')$, tal que $f(x) = u'(y')$ para algum $y' \in N'$. Então $d(x'')$ é definido como sendo a imagem de y' em $\mathrm{Coker}(f')$.

Demonstração: Antes de mostrarmos que a sequência é, de fato, exata; devemos verificar que cada um de seus homomorfismos estão bem definidos.

- $\overline{u} : \ker f' \to \ker f$ está bem definido.

  Se $x \in \ker f'$, então $f'(x) = 0$. Como $f(\overline{u}(x)) = f(u(x))$, pois $\overline{u}$ é restrição de u; e pelo diagrama comutativo, $f(u(x)) = u'(f'(x)) = u'(0) = 0$, concluímos que $\overline{u}(x) \in \ker f$. Além disso, $\overline{u}$ é injetor, pois u o é.

- $\overline{v} : \ker f \to \ker f''$ está bem definido.

  Se $x \in \ker f$, então $f(x) = 0$. Como $f''(\overline{v}(x)) = f''(v(x))$, pois $\overline{v}$ é restrição de v; e pelo diagrama, $f''(v(x)) = v'(f(x)) = v'(0) = 0$, concluímos que $\overline{v}(x) \in \ker f''$.

- $d : \ker f'' \to \frac{N'}{\mathrm{Im}(f')}$ está bem definido.

Como v é sobrejetor, então $x = v(z)$ para algum $z \in M$. Assim, $v'(f(z)) = f''(v(z)) = f''(x) = 0$; e daí $f(z) \in \ker v' = \mathrm{Im}(u')$. Seja $f(z) = u'(y)$ para algum $y \in N'$.

Assim, temos a definição de d

$$\begin{array}{rccl} d : \ker f'' & \longrightarrow & \dfrac{N'}{\mathrm{Im}(f')} \\ x & \longmapsto & y + \mathrm{Im}(f') \ \text{ tal que } u'(y) = f(z). \end{array}$$

Para mostrar que está bem definida, basta mostrar que v está bem definida. Isso porque $z \overset{f}{\mapsto} f(z)$ está bem definido e $y \overset{u'}{\mapsto} f(z)$ também está, pois $f(z) \in \ker v' = \mathrm{Im}(u')$.

Assim, tomemos $z_1, z_2 \in M$ tal que $v(z_1) = v(z_2) = x$, onde $f(z_1) = u'(y_1)$ e $f(z_2) = u'(y_2)$. Então $v(z_1) - v(z_2) = v(z_1 - z_2) = 0$ e $z_1 - z_2 \in \ker v - \mathrm{Im}(u)$. Seja $z_1 - z_2 = u(w)$ para algum $w \in M'$; e daí $f(z_1 - z_2) = f(u(w)) = u'(f'(w))$. Como $f(z_1 - z_2) = u'(y_1 - y_2)$ e u' é injetor, concluímos que $y_1 - y_2 = f'(w)$. Portanto, $y_1 + \mathrm{Im}(f') = y_2 + \mathrm{Im}(f')$.

- $\overline{u'} : \frac{N'}{\mathrm{Im}(f')} \to \frac{N}{\mathrm{Im}(f)}$ está bem definido.

  Por definição, $x + \mathrm{Im}(f') \overset{\overline{u'}}{\mapsto} u'(x) + \mathrm{Im}(f)$. Suponhamos que $x_1 + \mathrm{Im}(f') = x_2 + \mathrm{Im}(f')$ para $x_1, x_2 \in N'$; ou seja, $x_1 - x_2 \in \mathrm{Im}(f')$. Assim, existe $y \in M'$ tal que $f'(y) = x_1 - x_2$. Mas $u'(x_1 - x_2) = u'(f'(y)) = f(u(y))$, e $u'(x_1 - x_2) \in \mathrm{Im}(f)$. Logo, $u'(x_1) + \mathrm{Im}(f) = u'(x_2) + \mathrm{Im}(f)$.

- $\overline{v'} : \frac{N}{\mathrm{Im}(f)} \to \frac{N''}{\mathrm{Im}(f'')}$ está bem definido.

  Por definição, $x + \mathrm{Im}(f) \overset{\overline{v'}}{\mapsto} v'(x) + \mathrm{Im}(f'')$. Caso $y_1 + \mathrm{Im}(f) = y_2 + \mathrm{Im}(f)$ para $y_1, y_2 \in N$; isto é, $y_1 - y_2 \in \mathrm{Im}(f)$. Seja $z \in M$ o elemento tal que $f(z) = y_1 - y_2$. Dessa forma, $v'(y_1) - v'(y_2) = v'(y_1 - y_2) = v'(f(z)) = f''(v(z)) \in \mathrm{Im}(f'')$; e portanto, $v'(y_1) + \mathrm{Im}(f'') = v'(y_2) + \mathrm{Im}(f'')$. Além disso, $\overline{v'}$ é sobrejetora, pois é induzida por v'.

Agora, analisemos as condições a respeito dos núcleos e imagens dos homomorfismos.

- $\mathrm{Im}(\overline{u}) = \ker \overline{v}$.

  Como $\overline{v} \circ \overline{u} = (v \circ u)|_{\ker f'}$, pois são restrições; e $v \circ u \equiv 0$ pela hipótese; temos que $\mathrm{Im}(\overline{u}) \subseteq \ker \overline{v}$. Por outro lado, se $x \in \ker \overline{v}$, então

$x \in \ker f$, pela definição de $\overline{v}$. Assim $\overline{v}(x) = v(x) = 0$, e $x = u(y)$, pois $\mathrm{Im}(u) = \ker v$. Mas $0 = f(x) = f(u(y)) = v^{'}(f^{'}(y))$, com $v^{'}$ injetor, então $f^{'}(y) = 0$. Logo $y \in \ker f^{'}$ e $\overline{u}(y) = u(y)$. Portanto $x \in \mathrm{Im}(\overline{u})$.

- $\mathrm{Im}(\overline{v}) = \ker d$.

  Se $y \in \ker d$, então $d(y) = z + \mathrm{Im}(f^{'})$, com $u^{'}(z) = f(x)$ e $v(x) = y$; e $z = f^{'}(w)$, $w \in M$. Assim, $u^{'}(z) = u^{'}(f^{'}(w)) = f(u(w))$. Calculando

$$v(x - u(w)) = v(x) - v(u(w)) = v(x)$$

  e

$$f(x - u(w)) = f(x) - f(u(w)) = u^{'}(z) - u^{'}(z) = 0,$$

  vemos que $x - u(w) \in \ker f$ e satisfaz as condições de d. Assim, tomamos $y = \overline{v}(x - u(w))$, e $y \in \mathrm{Im}(\overline{v})$.

  Se $y \in \mathrm{Im}(\overline{v})$, então $y = \overline{v}(x) \in \ker f^{''}$, com $x \in \ker f$. Calculando $d(y)$, temos que $d(y) = \mathrm{Im}(f^{'})$, pois $0 = f(x) = u^{'}(z)$, onde $0 = z \in \mathrm{Im}(f^{'})$. Logo, $y \in \ker d$.

- $\mathrm{Im}(d) = \ker \overline{u^{'}}$.

  Para $x \in \ker f^{''}$, temos

$$\overline{u^{'}} \circ d(\overline{x}) = \overline{u^{'}} \left(y + \mathrm{Im}(f^{'}) \right) = u^{'}(y) + \mathrm{Im}(f).$$

  Mas pela definição de d, $u^{'}(y) = f(x)$. Logo $\mathrm{Im}(d) \subseteq \ker \overline{u^{'}}$. Por outro lado, se $\overline{y} \in \ker \overline{u^{'}}$, então

$$\overline{u^{'}}(\overline{y}) = \overline{u^{'}} \left(y + \mathrm{Im}(f^{'}) \right) = u^{'}(y) + \mathrm{Im}(f) = \mathrm{Im}(f) \Leftrightarrow u^{'}(y) = f(x).$$

  Tomando $z = v(x)$, temos que $d(z) = y$ e $\overline{y} \in \mathrm{Im}(d)$.

- $\mathrm{Im}(\overline{u^{'}}) = \ker \overline{v^{'}}$.

  Fazendo $\overline{v^{'}} \circ \overline{u^{'}}(\overline{x})$, para $\overline{x} = x + \mathrm{Im}(f^{'})$, temos:

$$\overline{v^{'}} \left(u^{'}(x) + \mathrm{Im}(f) \right) = v^{'} \left(u^{'}(x) \right) + \mathrm{Im}(f^{''}).$$

  Como $v^{'} \circ u^{'} \equiv 0$, obtemos que $\mathrm{Im}(\overline{u^{'}}) \subseteq \ker \overline{u^{'}}$. Reciprocamente, tomando $\overline{y} \in \ker \overline{v^{'}}$, então

$$\overline{v^{'}}\,(\overline{y}) = \overline{v^{'}}\,(y + \mathrm{Im}(f)) = v^{'}(y) + \mathrm{Im}(f^{''}) = \mathrm{Im}(f^{''}) \Leftrightarrow v^{'}(y) \in \mathrm{Im}(f^{''}).$$

Assim, $v^{'}(y) = f^{''}(z)$ para algum $z \in M^{''}$; e como v é sobrejetor, $z = v(x)$ para algum $x \in M$. Fazendo

$$v^{'}(y - f(x)) = v^{'}(y) - v^{'}(f(x)) = v^{'}(y) - f^{''}(v(x)) = v^{'}(y) - f^{''}(z) = 0,$$

vemos que $y - f(x) \in \ker v^{'} = \mathrm{Im}(u^{'})$. Logo, existe $w \in N^{'}$ tal que $u^{'}(w) = y - f(x)$. Finalmente, $\overline{u^{'}}(\overline{w}) = \overline{u^{'}}(w + \mathrm{Im}(f)) = \overline{y}$, e $\ker \overline{v^{'}} \subseteq \mathrm{Im}(\overline{u^{'}})$.

■

Seja C a classe de R-módulos e seja λ um função em C com valores em $\mathbb{Z}$. A função λ é *aditiva* se, para cada sequência exata curta com termos em C, temos $\lambda(M^{'}) - \lambda(M) + \lambda(M^{''}) = 0$.

Funções aditivas são bem "comportadas" quando aplicadas a qualquer sequência exata (não necessariamente curtas), como vemos a seguir.

Proposição 2.15. *Seja*

$$0 \to M_0 \to M_1 \to \cdots \to M_n \to 0$$

uma sequência exata de R-módulos na qual todos os módulos M_i e todos os núcleos dos homomorfismos estão em T. Então para qualquer função aditiva λ em T temos

$$\sum_{i=0}^{n} (-1)^i \lambda(M_i) = 0.$$

Demonstração: Decompondo a sequência dada em sequências exatas curtas

$$0 \to N_i \to M_i \to N_{i+1} \to 0$$

com $N_0 = N_{n+1} = 0$. Então temos $\lambda(M_i) = \lambda(N_i) + \lambda(N_{i+1})$. Agora basta tomar a soma alternada de $\lambda(M_i)$, cancelando todos os termos. ■

Capítulo 3

Anéis e Módulos de Frações

O procedimento através do qual obtemos o corpo $\mathbb{Q}$ a partir do anel $\mathbb{Z}$ pode ser extendido a um domínio de integridade R, produzindo o *corpo de frações* de R. A construção consiste em tomar todos os pares (a, s), com $a \in R$ e $s \neq 0$, e definir uma relação de equivalência entre tais pares:

$$(a, s) \equiv (b, t) \Leftrightarrow at - bs = 0.$$

Notemos que este processo só é válido em domínios de integridade, pois a verificação de que esta relação é transitiva envolve cancelamento de termos, isto é, o fato de que R não possui divisores de zeros não nulos. Entretanto, pode ser generalizado como segue.

Seja R um anel. Um *sistema multiplicativo fechado* de R é um subconjunto S de R tal que $1 \in S$ e S é fechado em relação à multiplicação. Definimos uma relação $\equiv$ em $R \times S$, como

$$(a, s) \equiv (b, t) \Leftrightarrow (at - bs)u = 0 \text{ para algum } u \in S.$$

Claramente, esta relação é reflexiva e simétrica. Para verificarmos que é transitiva, supomos $(a, s) \equiv (b, t)$ e $(b, t) \equiv (c, u)$. Então existe $v, w \in S$ tal que $(at - bs)v = 0$ e $(bu - ct)w = 0$. Assim, $atv = bsv$ e $buw = ctw$, e

$$b = \frac{atv}{sv} = \frac{ctw}{uw} \Rightarrow \frac{atv}{sv} = \frac{ctw}{uw} \Rightarrow (au - cs)tvw.$$

Como S é um sistema multiplicativo fechado, temos que $tvw \in S$, e portanto, $(a, s) \equiv (c, u)$. Dessa forma, $\equiv$ é relação de equivalência.

Denotamos por a/s a classe de equivalência de (a, s), e por $S^{-1}R$ o conjunto destas classes de equivalência. Ao definir as duas operações em $S^{-1}R$

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$

e

$$\frac{a}{s}\cdot\frac{b}{t}=\frac{ab}{st},$$

este conjunto passa a ter uma estrutura de anel. Vejamos que estas operações estão bem definidas.

Tomemos $a/s \equiv a'/s'$ e $b/t \equiv b'/t'$. Assim,

$$\begin{aligned}\frac{a}{s}+\frac{b}{t}\equiv\frac{a'}{s'}+\frac{b'}{t'} &\Rightarrow \frac{at+bs}{st}\equiv\frac{a't'+b's'}{s't'}\\ &\Rightarrow \Big(s't'(at+bs)-(a't'+b's')st\Big)\,u=0 \text{ (para algum } u\in S)\\ &\Rightarrow \frac{at+bs}{st}=\frac{a't'+b's'}{s't'}.\end{aligned}$$

E também,

$$\begin{aligned}\frac{a}{s}\cdot\frac{b}{t}\equiv\frac{a'}{s'}\cdot\frac{b'}{t'} &\Rightarrow \frac{ar}{st}\equiv\frac{a'b'}{s't'}\\ &\Rightarrow \Big((s't')(ab)-(a'b')(st)\Big)\,v=0 \text{ (para algum } v\in S)\\ &\Rightarrow \frac{ab}{st}=\frac{a'b'}{s't'}.\end{aligned}$$

O anel $S^{-1}R$ é chamado de *anel de frações* de R em relação a S. Também existe um homomorfismo de anéis $f : R \to S^{-1}R$, definido por $f(x) = x/1$; em geral, não injetivo. Em particular, se R é um domínio, temos a seguinte definição.

Definição 3.1. *Se R é um domínio, dizemos que $S^{-1}R$ é o corpo de frações de R, onde $S = R - \{0\}$.*

O seguinte resultado apresenta uma propriedade universal, satisfeita por todos os anéis de frações.

Proposição 3.2. *Seja $g : R \to S$ um homomorfismo de anéis tal que $g(s)$ é uma unidade em S para todo $s \in S$. Então existe um único homomorfismo de anéis $h : S^{-1}R \to S$ tal que $g = h \circ f$.*

Demonstração: (i) Unicidade. Se h satisfaz as condições, então $h(x/1) = hf(x) = g(x)$, para todo $x \in R$. Assim, se $s \in S$,

$$h(1/s) = h((s/1)^{-1}) = g(s)^{-1};$$

logo $h(x/s) = h(x/1) \cdot h(1/s) = g(x)g(s)^{-1}$ e h unicamente determinada por g.

(ii)Existência. Seja $h(x/s) = g(x)g(s)^{-1}$. Então h será, claramente, um homomorfismo desde que esteja bem definida. Suponha que $x/s = x'/s'$; então existe $t \in S$ tal que $(xs' - x's)t = 0$, e logo

$$\Big(g(x)g(s') - g(x')g(s)\Big)\, g(t) = 0.$$

Como $g(t)$ é uma unidade em S, concluímos que $g(x)g(s)^{-1} = g(x')g(s')^{-1}$. ■

O anel $S^{-1}R$ e o homomorfismo $f : R \to S^{-1}R$ satisfazem as seguintes propriedades:

(a) $s \in S \Rightarrow f(s)$ é uma unidade em $S^{-1}R$. Como $f(s) = s/1$ e $S^{-1}R = \{a/s : a \in R, s \in S\}$, em particular, $1/s \in S^{-1}R$ e $(1/s)(s/1) = 1$.

(b)$f(a) = 0 \Rightarrow as = 0$ para algum $s \in S$. De fato, se $f(a) = 0$, então $a/1 \equiv 0/1$ e $(a \cdot 1 - 1 \cdot 0)s = 0$; logo $as = 0$ para algum $s \in S$.

(c) Todo elemento de $S^{-1}R$ é da forma $f(a)f(s)^{-1}$ para algum $a \in R$ e algum $s \in S$. Obviamente, se $x \in S^{-1}R$, então $x = a/s = (a/1) \cdot (1/s) = f(a) \cdot f(s)^{-1}$.

Por outro lado, estas três condições determinam um isomorfismo de $S^{-1}R$ em S. Mais precisamente, temos o seguinte resultado.

Corolário 3.3. *Se $g : R \to S$ é um homomorfismo de anéis tal que*

(i) *$s \in S \Rightarrow g(s)$ é uma unidade em S;*

(ii) *$g(x) = 0 \Rightarrow xs = 0$ para algum $s \in S$;*

(iii) *Todo elemento de S é da forma $g(x)g(s)^{-1}$;*

então existe um único isomorfismo $h : S^{-1}R \to S$ tal que $g = h \circ f$.

Demonstração: Pela Proposição 3.2, temos que mostrar que $h : S^{-1}R \to S$, definido por

$$h(x/s) = g(x)g(s)$$

é um isomorfismo. Notemos que esta definição para h utiliza a condição (i). Por (iii), h é sobrejetora. Para mostrar que h é injetora, analisemos o seu núcleo: se $h(x/s) = 0$, então $g(x) = 0$; e por (ii), temos $xt = 0$ para algum $t \in S$. Assim $(x, s) \equiv (1, 0)$, isto é, $x/s = 0$ em $S^{-1}R$. ■

Em particular, o resultado a seguir mostra que a partir de um homomorfimo de um domínio R em um corpo, obtemos um homomorfismo do corpo de frações de R no mesmo corpo.

Proposição 3.4. *Todo homomorfismo injetor de anéis de um domínio R em um corpo L se estende unicamente de $K = S^{-1}R$, $(S = R - \{0\})$ a L.*

Demonstração: Seja $\varphi : R \to L$ um homomorfismo injetor do anel R no corpo L. Consideremos a função

$$\begin{aligned} \overline{\varphi} : K &\longrightarrow F \\ \frac{a}{s} &\longmapsto \frac{\varphi(a)}{\varphi(s)} \end{aligned}$$

Vemos que $\overline{\varphi}$ está bem definida, pois

$$\frac{a}{s} = \frac{b}{t} \Rightarrow at - bs = 0$$

e como φ é homomorfismo, é claro que

$$\varphi(at - bs) = 0 \Leftrightarrow \varphi(a)\varphi(t) - \varphi(b)\varphi(s) = 0.$$

Daí

$$\frac{\varphi(a)}{\varphi(s)} = \frac{\varphi(b)}{\varphi(t)} \Rightarrow \overline{\varphi}\left(\frac{a}{s}\right) = \overline{\varphi}\left(\frac{b}{t}\right).$$

Além disso, $\overline{\varphi}$ também é homomorfismo:

$$\begin{aligned} \overline{\varphi}\left(\frac{a}{s} + \frac{b}{t}\right) &= \overline{\varphi}\left(\frac{at+bs}{st}\right) = \frac{\varphi(at+bs)}{\varphi(st)} = \frac{\varphi(a)\varphi(t) + \varphi(b)\varphi(s)}{\varphi(s)\varphi(t)} \\ &= \frac{\varphi(a)}{\varphi(s)} + \frac{\varphi(b)}{\varphi(t)} = \overline{\varphi}\left(\frac{a}{s}\right) + \overline{\varphi}\left(\frac{b}{t}\right), \\ \overline{\varphi}\left(\frac{a}{s} \cdot \frac{b}{t}\right) &= \overline{\varphi}\left(\frac{ab}{st}\right) = \frac{\varphi(ab)}{\varphi(st)} = \frac{\varphi(a)\varphi(b)}{\varphi(s)\varphi(t)} \\ &= \frac{\varphi(a)}{\varphi(s)} \cdot \frac{\varphi(b)}{\varphi(t)} = \overline{\varphi}\left(\frac{a}{s}\right) \cdot \overline{\varphi}\left(\frac{b}{t}\right) \end{aligned}$$

e

$$\overline{\varphi}(1) = \overline{\varphi}\left(\tfrac{1}{1}\right) = \tfrac{\varphi(1)}{\varphi(1)} = 1.$$

Agora, suponha $\psi : R \to L$ homomorfismo tal que $\psi|_R = \varphi$. Para qualquer $x \in K$, temos as seguintes possibilidades:

- Se $x = \frac{a}{1} \in R$, então $\psi(a) = \varphi(a) = \frac{\varphi(a)}{1} = \overline{\varphi}(a) \Rightarrow \psi(x) = \overline{\varphi}(x)$.
- Se $x = \frac{1}{a} \in K$, temos que $\psi(\frac{1}{a}) = \frac{1}{\psi(a)} = \frac{1}{\varphi(a)} = \overline{\varphi}(\frac{1}{a}) \Rightarrow \psi(x) = \overline{\varphi}(x)$.

  Note que esta expressão é válida, pois $\frac{1}{\psi(a)} = \psi(\frac{1}{a})$, uma vez que $1 = \psi(1) = \psi(\frac{a}{a}) = \psi(a.\frac{1}{a}) = \psi(a).\psi(\frac{1}{a})$.
- Se $x = \frac{a}{s} \in K$, então $\psi(x) = \psi(\frac{a}{s}) = \psi(a) \cdot \psi(\frac{1}{s}) = \overline{\varphi}(a) \cdot \overline{\varphi}(\frac{1}{s}) = \overline{\varphi}(\frac{a}{s})$.

Portanto, $\phi = \overline{\varphi}$. Obviamente, $\overline{\varphi}|_R = \varphi$, e portanto, $\overline{\varphi}$ é extensão de φ. ■

Os dois próximos exemplos apresentam os casos mais interessantes de anéis de frações.

Exemplo 3.5. *Seja $\mathcal{P}$ um ideal primo em R. Então $S = R - \mathcal{P}$ é um sistema multiplicativo fechado. Neste caso, escrevemos $R_{\mathcal{P}}$ para $S^{-1}R$. Os elementos x/s com $x \in \mathcal{P}$ formam um ideal $\mathcal{M}$ em $R_{\mathcal{P}}$. Se $y/t \notin \mathcal{M}$, então $y \notin \mathcal{P}$. Assim $y \in S$ e y/t é uma unidade em $R_{\mathcal{P}}$. Segue que se I é um ideal em $R_{\mathcal{P}}$ e $I \nsubseteq \mathcal{M}$, então I contém uma unidade e portanto, é todo o anel. Logo $\mathcal{M}$ é o único ideal maximal em $R_{\mathcal{P}}$; isto é, $R_{\mathcal{P}}$ é um anel local. Este processo para obter $R_{\mathcal{P}}$ é chamado de* localização.

Exemplo 3.6. *Seja $f \in R$ e $S = \{f^n\}_{n \geq 0}$. Neste caso, escrevemos R_f para $S^{-1}R$.*

A construção de $S^{-1}R$ pode ser extendida para um R-módulo M; definindo a relação $\equiv$ em $M \times S$ como

$$(m, s) \equiv (m', s') \Leftrightarrow \exists t \in S \text{ tal que } t(sm' - s'm) = 0.$$

Como antes, esta é uma relação de equivalência; m/s a classe de equivalência do par (m, s) e $S^{-1}M$ denota o conjunto de tais frações. $S^{-1}M$ é um $S^{-1}R$-módulo definido adição e multiplicação por escalar. Analogamente aos Exemplos 3.5 e 3.6, escrevemos $M_{\mathcal{P}}$ e M_f para o caso de módulos.

Seja $u : M \to N$ um homomorfismo de R-módulos. Então u origina um homomorfismo de $S^{-1}R$-módulo $S^{-1}u : S^{-1}M \to S^{-1}N$, que leva m/s em $u(m/s)$. Com esta definição, é claro que $S^{-1}(v \circ u) = (S^{-1}v) \circ (S^{-1}u)$.

A seguir, apresentamos uma importante propriedade da operação S^{-1}.

Proposição 3.7. *A operação S^{-1} é exata; isto é, se $M' \xrightarrow{f} M \xrightarrow{g} M''$ é exata em M, então $S^{-1}M' \xrightarrow{S^{-1}f} S^{-1}M \xrightarrow{S^{-1}g} S^{-1}M''$ é exata em $S^{-1}M$.*

Demonstração: Temos que $g \circ f = 0$, então $S^{-1}g \circ S^{-1}f = S^{-1}(0) = 0$, e daí $\mathrm{Im}(S^{-1}f) \subseteq \ker S^{-1}g$. Para provar a inclusão inversa, seja $m/s \in \ker S^{-1}f$, então $g(m)/s = 0$ em $S^{-1}M''$. Assim, existe $t \in S$ tal que $tg(m) = 0$ em M''. Mas $tg(m) = g(tm)$, pois g é um homomorfismo de R-módulos; logo $tm \in \ker g = \mathrm{Im}(g)$, logo $tm = f(m')$ para algum $m' \in M'$. Dessa forma, em $S^{-1}M$ temos que $m/s = f(m')/st = (S^{-1}f)(m'/st) \in \mathrm{Im}(S^{-1}f)$. Portanto $\ker S^{-1}f \subseteq \mathrm{Im}(S^{-1}f)$. ■

Em particular, segue deste resultado que se M' é um submódulo de M, a função $S^{-1}M' \to S^{-1}M$ é injetora, e assim $S^{-1}M'$ pode ser considerado como um submódulo de $S^{-1}M$. Com isso, temos o seguinte corolário.

Corolário 3.8. *Se N, P são submódulos de um R-módulo M, então*

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

(ii) $S^{-1}(N \cap P) = S^{-1}(N) \cap S^{-1}(P)$;

(iii) *os $S^{-1}R$-módulos $S^{-1}(M/N)$ e $(S^{-1}M)/(S^{-1}N)$ são isomorfos.*

Demonstração: (i) Decorre diretamente da definição, uma vez que

$$\begin{aligned} S^{-1}(N+P) &= \{x/s : x \in N+P, s \in S\} \\ &= \{(n+p)/s : n \in N, p \in P, s \in S\} \\ &= S^{-1}(N) + S^{-1}(P). \end{aligned}$$

(ii) Se $y/s = z/t$ $(y \in N; z \in P; s,t \in S)$, então $u(ty - sz) = 0$ para algum $u \in S$; e daí, $w = uty = usz \in N \cap P$ e $y/s = w/stu \in S^{-1}(N \cap P)$. Consequentemente, $(S^{-1}N \cap S^{-1}P) \subseteq S^{-1}(N \cap P)$. A inclusão inversa é óbvia, pois se $x \in S^{-1}(N \cap P)$, então $x = a/s$, com $a \in N$ e $a \in P$.

(iii) Aplicando S^{-1} à sequência exata $0 \to N \xrightarrow{\iota} M \xrightarrow{\phi} M/N \to 0$; temos que

$$0 \longrightarrow S^{-1}N \xrightarrow{S^{-1}\iota} S^{-1}M \xrightarrow{S^{-1}\phi} S^{-1}(M/N) \longrightarrow 0$$

é exata (Proposição 3.7). Como $S^{-1}\phi$ é um homomorfismo sobrejetor, e $\ker \phi = S^{-1}N$; temos que

$$S^{-1}\left(\frac{M}{N}\right) \cong \frac{S^{-1}M}{S^{-1}N}.$$

■

3.1 Propriedades Locais

Uma propriedade P de um anel R (ou de um R-módulo M) é *local* se a seguinte equivalência é verdadeira:

R (ou M) satisfaz $P \Leftrightarrow R_{\mathcal{P}}$ (ou $M_{\mathcal{P}}$) satisfaz P, para cada ideal primo $\mathcal{P}$ de R.

As proposições abaixo são exemplos de propriedades locais.

Proposição 3.9. *Seja M um R-módulo. As seguintes afirmações são equivalentes:*

(i) $M = 0$;

(ii) $M_{\mathcal{P}} = 0$ *para todos os ideais primos* $\mathcal{P}$ *de* R;

(iii) $M_{\mathcal{M}} = 0$ *para todos os ideais maximais* $\mathcal{M}$ *de* R.

Demonstração: Claramente, (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii). Suponha que (iii) esteja satisfeita e que $M \neq 0$. Seja $x \in M$ um elemento não nulo, e $I = \text{Ann}(x)$. I é um ideal $\neq (1)$, logo está contido em um ideal maximal $\mathcal{M}$ (pelo Corolário 1.33). Consideremos $x/1 \in M_{\mathcal{M}}$. Como $M_{\mathcal{M}} = 0$, necessariamente $x/1 = 0$, e assim x é anulado por algum elemento de $R - \mathcal{M}$; o que é impossível, uma vez que $\text{Ann}(x) \subseteq \mathcal{M}$. ■

Proposição 3.10. *Seja* $\phi : M \to N$ *um homomorfimos de* R*-módulos. Então são equivalentes:*

(i) ϕ *é injetor;*

(ii) $\phi_{\mathcal{P}} : M_{\mathcal{P}} \to N_{\mathcal{P}}$ *é injetor para cada ideal primo* $\mathcal{P}$*;*

(iii) $\phi_{\mathcal{M}} : M_{\mathcal{M}} \to N_{\mathcal{M}}$ *é injetor para cada ideal maximal* $\mathcal{M}$*.*

Analogamente, substituindo-se "injetor" por "sobrejetor".

Demonstração: (i) $\Rightarrow$ (ii). $0 \to M \to N$ é exata, então $0 \to M_{\mathcal{P}} \to N_{\mathcal{P}}$ é exata (Proposição 3.7). Portanto, $\phi_{\mathcal{P}}$ é injetor.

(ii) $\Rightarrow$ (iii). Obviamente, pois todo ideal maximal é primo.

(iii) $\Rightarrow$ (i). Seja $M' = \ker \phi$. Então a sequência $0 \to M' \to M \to N$ é exata, e $0 \to M'_{\mathcal{M}} \to M_{\mathcal{M}} \to N_{\mathcal{M}}$ é exata pela Proposição 3.7. Assim $M'_{\mathcal{M}} \cong \ker \phi_{\mathcal{M}} = 0$, pois $\phi_{\mathcal{M}}$ é injetor. Portanto, $M' = 0$ por 3.9, e ϕ é injetor.

Analogamente, se prova a validade da proposição para homomorfismo sobrejetor. ■

3.2 Extensão e Contração de Ideais em Anéis de Frações

Sejam T o conjunto dos ideais contraídos em R, e E o conjunto dos ideais estendidos em $S^{-1}R$. Se I é um ideal em R, sua extensão I^e em $S^{-1}R$ é $S^{-1}I$.

Proposição 3.11. (i) *Todo ideal em* $S^{-1}R$ *é um ideal estendido.*

(ii) *Se* I *é um ideal em* R*, então* $I^{ec} = \bigcup_{s \in S}(I : s)$*. Assim,* $I^e = (1)$ *se, e somente se,* I *coincide com* S*.*

(iii) $I \in C \Leftrightarrow$ *nenhum elemento de* S *é um divisor de zero em* R/I.

(iv) *Os ideais primos em* $S^{-1}(R)$ *estão em correspondência biunívoca* ($\mathcal{P} \leftrightarrow S^{-1}\mathcal{P}$) *com os ideais primos de* R *que não coincidem com* S.

Demonstração: (i) Seja J um ideal em $S^{-1}(R)$ e seja $x/s \in J$. Então $x/1 \in J$, e $x \in J^c$. Logo $x/s \in J^{ce}$. Como $J \supseteq J^{ce}$, segue que $J = J^{ce}$.

(ii) $x \in J^{ec} = (S^{-1}I)^c \Leftrightarrow x/1 = a/s$ para algum $a \in I, s \in S \Leftrightarrow (xs - a)t = 0$ para algum $t \in S \Leftrightarrow xst \in I \Leftrightarrow x \in \bigcup_{s \in S}(I : s)$.

(iii) $I \in C \Leftrightarrow I^{ec} \subseteq I \Leftrightarrow (sx \in I$ para algum $s \in S \Rightarrow x \in I) \Leftrightarrow$ nenhum $s \in S$ é um divisor de zero em R/I.

(iv) Se J é um ideal primo em $S^{-1}(R)$, então J^c é um ideal primo em R. Por outro lado, se $\mathcal{P}$ é um ideal primo em R, então $R/\mathcal{P}$ é um domínio de integridade. Se $\overline{S}$ é a imagem de S em $R/\mathcal{P}$, temos $\frac{S^{-1}R}{S^{-1}\mathcal{P}} \cong \overline{S}^{-1}(R/\mathcal{P})$, que é 0 ou está contido em um corpo de frações de $R/\mathcal{P}$; e então é um domínio de integridade. Logo $S^{-1}\mathcal{P}$ é primo ou o ideal das unidades. Por (i), esta última possibilidade ocorre se, e somente se, $\mathcal{P}$ coincide com S. ■

Corolário 3.12. *Se* $\Re$ *é o nilradical de* R, *o nilradical de* $S^{-1}R$ *é* $S^{-1}\Re$.

Demonstração: O resultado é imediato, já que o nilradical $\Re$ de R é a intersecção de todos os ideais primos em R, e estes estão em correspondência biunívoca com os ideias primos em $S^{-1}R$. ■

Corolário 3.13. *Se* $\mathcal{P}$ *é um ideal primo de* R, *os ideais primos do anel local* $R_{\mathcal{P}}$ *estão em correspondência biunívoca com os ideais primos de* R *contido em* $\mathcal{P}$.

Demonstração: Basta tomar $S = R - \mathcal{P}$ em no item (iv) da Proposição 3.11. ■

3.3 Domínio de Fatoração Única

Esta seção, embora trate de um caso particular de domínio de integridade, traz alguns resultados importantes envolvendo seu corpo de frações. Por isso, optamos por incluí-la no fim deste capítulo.

Quando consideramos o anel $\mathbb{Z}$, o Teorema Fundamental da Aritmética garante que todo número inteiro tem uma representação única como produto de números primos, a menos das unidades 1 e -1. Estas idéias de números primos e fatoração única em $\mathbb{Z}$ podem ser estendidas para um domínio de integridade A qualquer, como segue.

A partir deste momento, utilizamos a notação $x \mid y$, para dizer que x "divide" x, isto é, $y = x \cdot z$, para algum $z \in R$. Dizemos que um elemento $p \neq 0$ de R é *primo* se p não é unidade em R e se, para quaisquer $x, y \in A$ tais que $p \mid x \cdot y$, temos que $p \mid x$ ou $p \mid y$. Um elemento $x \in R$ é *irredutível* se para qualquer fatoração $x = y \cdot z$, $y, z \in R$, temos que y ou z é unidade.

Um elemento $x \in R$, não nulo, não inversível e não irredutível é chamado de *composto*. Se dois elementos $x, y \in R$ são tais que $x \mid y$ e $y \mid x$, então dizemos que x e y são *associados*, e denotamos por $x \sim y$.

Em um domínio de integridade R, um elemento d é *máximo divisor comum* de $a, b \in R$ se $d \mid a$ e $d \mid b$, e se para $d' \in R$ tal que $d' \mid a$ e $d' \mid b$, então $d' \mid d$. Se o máximo divisor comum de $a, b \in R$ é a unidade em R, dizemos que a e b são *primos entre si*.

Proposição 3.14. *Todo elemento primo de um domínio de integridade R é irredutível.*

Demonstração: Seja $p \in R$ um elemento primo. Então $p \neq 0$ e p não é unidade em R. Suponhamos $p = ab$. Como $p \mid p$, então $p \mid ab$. Assim, $p \mid a$ ou $p \mid b$.

Se $p \mid a$, então existe $t \in R$ tal que $a = pt$. Substituindo em $p = ab$, obtemos $p = p(tb)$. Logo $tb = 1$ e b é unidade.

Analogamente, se $p \mid b$, obteremos que a é unidade. Portanto, p é irredutível. ■

A recíproca desta proposição não é válida, em geral. Basta considerar o número 3 no anel $R = \mathbb{Z}[\sqrt{-5}]$: é irredutível mas não é primo. De fato, se $(a + b\sqrt{-5}) \cdot (c + d\sqrt{-5}) = 3$, com $a, b, c, d \in \mathbb{Z}$, temos

$$\begin{cases} ac - 5bd = 3 \\ bc + ad = 0 \end{cases}$$

Supondo $c \neq 0$, temos

$$b = \frac{-ad}{c} \Rightarrow ac - \frac{5ad^2}{c} = 3 \Rightarrow a \mid 3$$

e então, $a \in \{-1, 1, -3, 3\}$. Se $a = 1$, então

$$c = 3 + 5b^2c \Rightarrow c \mid 3$$

e daí $c \in \{-3, -1, 1, 3\}$. Mas de $c(1 - 5b^2) = 3$, obtemos que $c = 3$ e $b = 0$. Logo, $b = d = 0$ e $a = \pm 1$, $c = \pm 3$, ou o contrário. Assim, um dos dois elementos é unidade em $[\sqrt{-5}]$, e 3 é irredutível. Além disso, 3 divide $(2+\sqrt{-5}) \cdot (2-\sqrt{-5}) = 9$, mas não divide nenhum dos dois fatores. Portanto, 3 não é primo em $R = \mathbb{Z}[\sqrt{-5}]$.

Entretanto, se R for um domínio principal, a recíproca é verdadeira, conforme mostra o seguinte resultado:

Proposição 3.15. *Em um domínio principal R, todo elemento irredutível é primo.*

Demonstração: Seja p um elemento irredutível. Logo $p \neq 0$ e p não é unidade. Suponhamos que $p \mid ab$, com $a, b \in R$. Mostremos que p divide cada um destes elementos.

Seja $(p, a) = (d)$. Como p pertence a esse ideal, existe $q \in R$ de maneira que $p = dq$. Sendo p irredutível, então ou d é unidade, ou q é unidade.

Se d é unidade em R, então $(p, a) = R$. Logo, existem $x, y \in R$ tais que $1 = px + ay$. Multiplicando por b esta igualdade, obtemos $b = p(bx) + (ab)y$. Como p divide ambas as parcelas do segundo membro desta relação, concluímos que $p \mid b$.

Agora, se q é unidade, então de $p = dq$ segue que $d = pq^{-1}$. Como, por outro lado, $a \in (d)$, então $a = dq_1$ com $q_1 \in$. Portanto, $a = p(q^{-1}q_1)$, o que nos garante que $p \mid a$. ■

Em um domínio principal R, temos uma caracterização de um ideal próprio e primo P, explicitada abaixo.

Proposição 3.16. *Seja R um domínio principal. Seja P um ideal próprio não nulo e primo de R. Então P é gerado por um elemento irredutível.*

Demonstração: Seja $P = (a)$, $a \in R$. Mostremos que a é irredutível. Tomemos uma decomposição $a = mn$. Como $a \in P$ e P é primo, então $m \in P$ ou $n \in P$. Supondo, sem perda de generalidade, que $m \in P$, temos $m = ka$; e então, $a = kan$. Como R é domínio, obtemos $1 = kn$, isto é, n é unidade e, portanto, a é irredutível. ■

A partir destas discussões, temos a seguinte definição.

Definição 3.17 (Domínio de Fatoração Única)**.** *Um domínio R é* domínio de fatoração única *se todo elemento não nulo em R pode ser fatorado unicamente, exceto por unidades e a ordem dos fatores, em elementos irredutíveis.*

Em particular, todo elemento irredutível de um domínio de fatoração única R é primo. Com efeito, seja x um elemento irredutível de R e suponhamos que $x \mid ab$, $a, b \in R$. Assim, $a = p_1 \cdots p_r$ e $b = q_1 \cdots q_s$, com p_i, q_j

irredutíveis, e então $p_1 \cdots p_r q_1 \cdots q_s$ é a única fatoração de ab em fatores irredutíveis. Como $ab = xy$ para algum $y \in R$, considerando a fatoração irredutível $y = w_1 \cdots w_t$, temos que $p_1 \cdots p_r q_1 \cdots q_s$ e $xw_1 \cdots w_t$ são duas fatorações de ab em fatores irredutíveis. Como R é domínio de fatoração única, temos que $x = up_i$ ou $x = uq_j$ para alguma unidade u. Logo $x \mid a$ ou $x \mid b$.

Vejamos agora alguns exemplos de domínio de fatoração única.

Exemplo 3.18. *O anel $\mathbb{Z}$ é um domínio de fatoração única, pois para qualquer $n \in \mathbb{Z} - \{0\}$, temos uma decomposição única em fatores primos, que são os elementos irredutíveis deste conjunto. Claramente, n e $-n$ diferenciam-se apenas pelo elemento unidade -1.*

Exemplo 3.19. *Todo corpo é, trivialmente, um domínio de fatoração única, já que todos os seus elementos são unidades.*

Exemplo 3.20. *O anel de polinômios $\mathbb{Z}[X]$ é um domínio de fatoração única.*

De maneira geral, mostraremos que se R é um domínio de fatoração única, então $R[X]$ também é (Teorema 3.27). Para esta demonstração, serão necessários alguns lemas e a seguinte definição.

Definição 3.21. *Seja R um domínio de fatoração única. Dizemos que um polinômio $F = a_0 + a_1X + \ldots + a_nX^n$ é* primitivo *se F não é constante e se o seus coeficientes são primos entre si, isto é, admitem a unidade 1_R como máximo divisor comum.*

Lema 3.22. *Seja $F \in R[X]$ um polinômio não constante. Então existe uma polinômio primitivo $\widetilde{F} \in R[X]$ e existe um elemento $d \in R$ de maneira que $F = d \cdot \widetilde{F}$. Além disso, se $F = d_1 \cdot \widetilde{F}_1$ com $d_1 \in R$ e $\widetilde{F}_1$ primitivo em $R[X]$, então $d \sim d_1$ e $\widetilde{F} \sim \widetilde{F}_1$.*

Demonstração: Suponhamos $F = a_0 + a_1X + \ldots + a_nX^n$. Se d é um máximo divisor comum de $a_0, a_1, \ldots, a_n$, fazendo

$$\widetilde{F} = \frac{a_0}{d} + \frac{a_1}{d}X + \ldots + \frac{a_n}{d}X^n$$

temos que $F = d \cdot \widetilde{F}$ e, ainda, que $\widetilde{F}$ é primitivo, pois $\frac{a_i}{d}$ são primos entre si, para $i = 0, ..., n$.

Agora, suponhamos $F = d \cdot \widetilde{F} = d_1 \cdot \widetilde{F}_1$. Da igualdade $F = d_1 \cdot \widetilde{F}_1$ decorre que $d_1 \mid a_i$ para $i = 0, ..., n$. Logo $d_1 \mid d$, e existe $c \in A$ tal que $d = d_1c$. Retomando a igualdade $d \cdot \widetilde{F} = d_1 \cdot \widetilde{F}_1$ e levando em conta a última igualdade obtida, chegamos a $d_1c \cdot \widetilde{F} = d_1 \cdot \widetilde{F}_1$. Daí $c \cdot \widetilde{F} = \widetilde{F}_1$. Isto nos garante que c divide

todos os coeficientes de $\widetilde{F}_1$. Sendo este polinômio irredutível, a conclusão é que c é unidade. Então $d \sim d_1$ e $\widetilde{F} \sim \widetilde{F}_1$. ■

Lema 3.23. *O produto de dois polinômios primitivos sobre um anel fatorial é um polinômio primitivo.*

Demonstração: Sejam $F = a_0 + a_1X + \ldots + a_mX^m$ e $G = b_0 + b_1X + \ldots + b_nX^n$ os polinômios primitivos, de graus m e n respectivamente. Então

$$F \cdot G = c_0 + c_1X + \ldots + c_{m+n}X^{m+n}$$

onde $c_k = \sum_{i+j=k} a_ib_j$, $k = 0, 1, ..., m+n$.

Se $F \cdot G$ não fosse primitivo, existiria um elemento irredutível $p \in A$ de modo que $p \mid c_k$, $k = 0, 1, ..., m+n$. Como p divide a_0b_0 e é irredutível, então $p \mid a_0$ ou $p \mid b_0$.

Considerando a primeira alternativa, podemos dizer que existe r, $0 < r \leq m$, tal que $p \mid a_0$, $p \mid a_1$, ..., $p \mid a_{r-1}$, $p \nmid a_r$. Como

$$c_r = a_0b_r + a_1b_{r-1} + \ldots + a_rb_0$$

, com $p \mid c_r$ e $p \nmid a_r$, então $p \mid b_0$.

Logo, podemos dizer que existe s, $0 < s \leq n$, tal que $p \mid b_0$, $p \mid b_1$, ..., $p \mid b_{s-1}$, $p \nmid b_s$. Considerando que

$$c_{r+s} = a_0b_{r+s} + \ldots a_{r-1}b_{s+1} + a_rb_s + a_{r+1}b_{s-1} + \ldots a_{r+s}b_0$$

então $p \mid a_rb_s$. Assim, $p \mid a_r$ ou $p \mid b_s$; o que é um absurdo, pois f e g são primitivos. ■

Lema 3.24. *Seja K o corpo das frações de um domínio de fatoração única R. Se $f \in K[X]$ não é constante, então existem $a, b \in R$ não nulos, e um polinômio primitivo $\widetilde{F} \in R[X]$ de maneira que $f = \frac{a}{b} \cdot \widetilde{F}$. Além disso, se $f = \frac{a_1}{b_1} \cdot \widetilde{F}_1$, com $a_1, b_1 \in R$ não nulos e $\widetilde{F}_1 \in R[X]$ também primitivo, então $ab_1 \sim a_1b$ e $\widetilde{F} \sim \widetilde{F}_1$.*

Demonstração: Sendo

$$f = \frac{c_0}{d_0} + \frac{c_1}{d_1}X + \ldots + \frac{c_m}{d_m}X^m$$

e fazendo $d_0d_1 \ldots d_m = b$, então $f = \frac{1}{b} \cdot F$, com $F \in R[X]$. Pelo Lema 3.22, $f = \frac{a}{b} \cdot \widetilde{F}$, com $\widetilde{F}$ primitivo e $a \in R$, não nulo.

Por outro lado, se

$$f = \frac{a}{b} \cdot \widetilde{F} = \frac{a_1}{b_1}\widetilde{F}_1,$$

conforme o enunciado, então $ab_1 \cdot \widetilde{F} = a_1b \cdot \widetilde{F}_1$. Usando a segunda parte do Lema 3.22, concluímos que $ab_1 \sim a_1b$ e $\widetilde{F} \sim \widetilde{F}_1$. ■

Lema 3.25. *Seja F um polinômio irredutível sobre o domínio de fatoração única R. Se K é o corpo de frações de R, então F também é irredutível sobre K.*

Demonstração: Suponhamos F redutível sobre K. Então existem dois polinômios $g, h \in K[X]$, ambos de grau maior ou igual a 1, tais que $F = g \cdot h$. O Lema 3.24 nos permite o seguinte com relação a g e a h:

$g = \frac{a}{b} \cdot G$ e $h = \frac{c}{d} \cdot H$, onde $a, b, c, d \in A$, não nulos, e $G, H \in R[X]$ são primitivos.

Assim temos

$$F = \frac{ac}{bd} \cdot (G \cdot H) \text{ ou } bd \cdot F = ac \cdot (GH)$$

onde $G \cdot H$ é primitivo, devido ao Lema 3.23.

Então existe unidade u tal que $ac = u(bd)$, pois ac e bd são associados. Portanto, $F = (u \cdot G) \cdot H$. Como $\deg(u \cdot G) = \deg(G) \geq 1$ e $\deg(H) = \deg(h) \geq 1$, então a igualdade $F = (u \cdot G) \cdot H$ nos diz que F é redutível em $R[X]$, contrariando a hipótese. ■

Decorre deste resultado que se F e G são polinômios em $R[X]$ sem fatores comuns em $R[X]$, então também não possuem fatores comuns em $K[X]$.

Corolário 3.26. *Seja R um domínio de fatoração única. Então todo polinômio irredutível $F \in R[X]$ é também primo.*

Demonstração: Primeiramente, suponhamos que $F \in R$, isto é, que F é um polinômio constante. Sendo irredutível como elemento de R, então F é primo em R. Afirmamos que F é primo em $R[X]$. De fato, se $F \in R$ não fosse primo em $R[X]$, teríamos $F \mid G \cdot H$, com $F \nmid G$ e $F \nmid H$. Mas G, H são polinômios de graus maiores ou iguais a 0, e com coeficientes em R. Assim, F não divide algum dos coeficientes a_i de G e algum dos coeficientes b_j de H. Entretanto, $F \mid G \cdot H$ implica que F divide todos os coeficientes deste produto, onde cada coeficiente é da forma $c_k = \sum_{l=0}^{k} a_l b_{k-l}$ e está em R. Logo F dividiria todo produto da forma $a_i b_j$ com $F \nmid a_i$ e $F \nmid b_j$, contrariando o fato de F ser primo em R.

Supondo agora que $\deg F \geq 1$ e que $F \mid G \cdot H$ em $R[X]$. Se K é o corpo de frações de R, podemos dizer que $F \mid G \cdot H$ em $K[X]$. Como $K[X]$ é um domínio principal, e F é primo em $K[X]$ (Proposição 3.15), então $F \mid G$ ou $F \mid H$ em $K[X]$.

Consideremos que $F \mid G$. Então existe $q \in K[X]$ tal que $G = F \cdot m$. Como F é primitivo em $R[X]$ e usando as decomposições dadas pelos Lemas 3.22

e 3.24, obtemos

$$c \cdot \widetilde{G} = \frac{a}{b} \cdot F \cdot \widetilde{q}$$

onde $a, b, c \in R$ não nulos e G e $F \cdot \widetilde{m}$ são polinômios primitivos de $R[X]$. Então $bc \sim a$, o que acarreta que existe u unidade em R tal que,

$$\widetilde{G} = u \cdot F\widetilde{m}.$$

Logo $G = F \cdot (uc\widetilde{m})$, o que garante que $F \mid G$ em $R[X]$. ■

Teorema 3.27. *Seja R um domínio de fatoração única. Então $R[X]$ é domínio de fatoração única.*

Demonstração: Seja $F \in R[X]$ um elemento não nulo e tal que F não é unidade. A demonstração da decomposição será feita por indução sobre $\deg(F)$.

Se $\deg(F) = 0$, então $F \in R$. Decompondo F em fatores irredutíveis de R, já que R é domínio fatorial, obtemos a decomposição desejada, pois um elemento irredutível em R também o é em $R[X]$. Essa última afirmação é válida pois $R \subset R[X]$, e se $F = G \cdot H$, com $G, H \in R[X]$, teremos $G \in R$ e $H \in R$, uma vez que $0 = \deg F = \deg G + \deg H$, e $\deg G, \deg H \geq 0$. Logo F é irredutível em $R[X]$.

Agora suponhamos que $\deg(F) = n > 0$ e admitamos que a decomposição seja possível para todo polinômio de grau r, onde $0 \leq r < n$. Pelo Lema 3.22, podemos escrever $F = d \cdot \widetilde{F}$, com $d \in R$ e $\widetilde{F} \in R[X]$ é primitivo. Caso $\widetilde{F}$ seja irredutível, basta decompormos d em fatores irredutíveis em R, obtendo a decomposição desejada para F. Se d fosse unidade, então F também seria irredutível, e nada haveria a fazer. Caso $\widetilde{F}$ seja composto, existem $G, H \in R[X]$ de modo que $\widetilde{F} = G \cdot H$, com $1 \leq \deg(G), \deg(H) < \deg(\widetilde{F}) = \deg(F)$.

Pela hipótese de indução, G e H se decompõem em fatores irredutíveis. Assim, $F = d \cdot \widetilde{F} = d(G \cdot H)$ se decompõe em fatores irredutíves em $R[X]$, uma vez que $d \in R$ e R é domínio fatorial.

Mostremos agora a unicidade da decomposição. Seja $F = P_1 \cdot \ldots \cdot P_s = Q_1 \cdot \ldots \cdot Q_t$ $(t \geq s)$ decomposições de F em fatores irredutíveis em $R[X]$. Pelo Corolário 3.26, os $P_i, Q_j \in R[X]$ são todos primos. Assim, como $P_1 \mid F$, temos que $P_1 \mid Q_1 \cdot \ldots \cdot Q_t$. Sendo P_1 elemento primo, P_1 divide algum dos Q_j. Admitamos que $P_1 \mid Q_1$. Como Q_1 é primo, temos $P_1 \sim Q_1$.

Suponhamos $Q_1 = u_1 \cdot P_1$, com u_1 unidade em R. Então de $P_1 \cdot P_2 \cdot \ldots \cdot P_s = Q_1 \cdot Q_2 \cdot \ldots \cdot Q_t$, obtemos $P_2 \cdot P_3 \cdot \ldots \cdot P_s = (u_1 \cdot Q_2) \cdot Q_3 \cdot \ldots \cdot Q_t$. De forma análoga a P_1, obtemos $Q_2 = u_2 \cdot P_2$. Assim, $P_3 \cdot \ldots \cdot P_s = u_1(u_2 \cdot Q_3) \cdot \ldots \cdot Q_t$.

Prosseguindo com este raciocínio, obteremos $P_i \sim Q_i$, e a representação será única, a menos de unidades. ■

A aplicação sucessiva do teorema acima nos dá o corolário seguinte:

Corolário 3.28. *Seja R um domínio de fatoração única. Então $R[X_1, \ldots, X_n]$ é um domínio de fatoração única.*

Como um corpo K é sempre domínio de fatoração única, já que todos os seus elementos não nulos são unidades; temos que $K[X_1, \ldots, X_n]$ também o é, para qualquer corpo K. Em especial, $\mathbb{Q}[X]$ é um domínio de fatoração única. O corpo de frações de $K[X_1, \ldots, X_n]$ é denotado por $K(X_1, \ldots, X_n)$ e chamado de *corpo das frações racionais* em n variáveis sobre K.

Se considerarmos o corpo de frações de um domínio R, obtemos uma representação única (a menos de unidades) de seus elementos, conforme mostrado a seguir.

Proposição 3.29. *Seja R um domínio de fatoração única e K seu corpo de frações. Então todo elemento z de K pode ser escrito como $z = \frac{a}{b}$, onde $a, b \in R$ não possuem fatores em comum; e esta representação é única, a menos de unidades de R.*

Demonstração: Note que, se provarmos que todo par de elementos $x, y \in R$ admite máximo divisor comum e que, se d é o tal divisor, então $\frac{a}{d}$ e $\frac{b}{d}$ são primos entre si, este resultado estará provado; uma vez que se $z = \frac{x}{y}$, com $x = ad$ e $y = bd$, teremos $z = \frac{a}{b}$, a, b primos entre si.

Primeiramente, provemos que $x, y \in R$ admitem máximo divisor comum em R. Se $x = 0$, então y é um máximo divisor comum de x e y. Se x é unidade em R, então x é máximo divisor comum de x e y. Caso contrário, podemos decompor x e y:

$$x = up_1^{r_1}p_2^{r_2}\ldots p_n^{r_n} \text{ e } y = vp_1^{s_1}p_2^{s_2}\ldots p_n^{s_n}.$$

Seja $d = p_1^{k_1}p^{k_2}\ldots p_n^{k_n}$, onde $k_i = \min\{r_i, s_i\}$ $(i = 1, \ldots, n)$. Mostremos que d é o máximo divisor comum de x e y.

Que $d \mid x$ e $d \mid y$ é imediato. Agora, suponhamos que $d^* \in R$ com, $d^* \mid x$ e $d^* \mid y$. Então $d^* = wp_1^{t_1}p_2^{t_2}\ldots p_n^{t_n}$, w unidade em R e $t_i \leq r_i, s_i$. Logo $t_i \leq \min\{r_i, s_i\}$ $(i = 1, \ldots, n)$. Logo $d^* \mid d$.

Dessa forma, temos

$$\frac{a}{d} = up_1^{r_1-k_1}p_2^{r_2-k_2}\ldots p_n^{r_n-k_n} \text{ e } \frac{b}{d} = vp_1^{s_1-k_1}p_2^{s_2-k_2}\ldots p_n^{s_n-k_n}.$$

Como $k_i = \min\{r_i, s_i\}$, então quando não se tem $r_i - k_i = 0$, tem-se $s_i - k_i =$. Daí $p_1^0 p_2^0 \dots p_n^0 = 1$ é o máximo divisor comum de x e y.

Supondo $\frac{a}{b} = cd$, temos que $ad = bc$ e, assim, $a \mid bc$ e $b \mid ad$. Como a, b são primos entre si, então $a \mid c$ e $b \mid d$; e $c = ua$ e $d = vb$, para u, v unidade em R, pois é domínio de fatoração única. ■

Recordemos que o anel $\mathbb{Z}$ é um domínio principal, já que todos os seus ideais são da forma $I = (n)$; e, de acordo com o Exemplo 3.18, $\mathbb{Z}$ também é domínio de fatoração única. Entretanto, afirmamos que este fato é válido para todo domínio principal, conforme o resultado a seguir.

Teorema 3.30. *Todo domínio principal R é domínio de fatoração única.*

Demonstração: Mostremos que dado $a \in R$, com R domínio principal e a não nulo e não unidade, existem elementos irredutíveis $p_1, p_2, \dots, p_n$ $(n \geq 1)$ de maneira que $a = p_1 p_2 \dots p_n$, e tal decomposição é única, a menos da ordem dos fatores e de unidades.

É trivial o caso em que a é irredutível. Suponhamos a um elemento composto de R. Então existe elemento irredutível $p_1 \in R$ tal que $a = p_1 q_1$, com $q_1 \in A$. Podemos dizer que q_1 não é unidade em R pois, caso contrário, a seria irredutível. Se q_1 for irredutível, a existência da decomposição está provada com $n = 2$. Se q_1 não for irredutível, existe elemento irredutível p_2 que divide q_1, isto é, $q_1 = p_2 q_2$, $q_2 \in R$. Então $a = p_1 p_2 q_2$, com q_2 não unidade. Procedendo desta maneira, existirá um $n > 1$ de maneira que q_{n-1} é irredutível pois, caso contrário, a seria redutível. Daí $a = p_1 p_2 \cdots p_{n-1} q_{n-1}$ e, fazendo $q_{n-1} = p_n$, obtemos a decomposição $a = p_1 \dots p_n$.

A demonstração da unicidade é análoga a do Teorema 3.27, lembrando que em um domínio principal, todo elemento irredutível é primo.

■

A proposição a seguir caracteriza os ideais principais primos em um domínio de fatoração única.

Proposição 3.31. *Um ideal principal $I = (a)$ em um domínio de fatoração única R é primo se, e somente, a é irredutível.*

Demonstração: Como num domínio principal, a é primo se, e somente se, a é irredutível; basta mostarmos que $a \in R$ é primo se, e somente se, $I = (a)$ é um ideal primo não trivial.

Se a é primo, então para todo $bc \in I = (a)$ temos $bc = ma$ para algum $m \in R$. Logo $a \mid bc$, e daí, $a \mid b$ ou $a \mid c$; isto é, $b \in I$ ou $c \in I$. Portanto, $I = (a)$ é primo.

Por outro lado, se $I = (a)$ é primo, então para todo $bc \in I$, temos $b \in I$ ou $c \in I$. O que equivale a $a \mid b$ ou $a \mid c$, com $a \neq 0$ não unidade, pois I é ideal primo não trivial. ■

Capítulo 4

Condições de Cadeia

No Capítulo 1, consideramos cadeias de ideais para a aplicação do Lema de Zorn. Agora, estudaremos uma cadeia de submódulos e suas propriedades. Para tanto, definimos uma relação de ordem parcial em um conjunto.

Seja Σ um conjunto parcialmente ordenado por uma relação $\leq$; ou seja, $\leq$ é reflexixa e transitiva e é tal que se $x \leq y$ e $y \leq x$, então $x = y$.

Proposição 4.1. *As seguintes afirmações são equivalentes em Σ:*

(i) Toda sequência crescente $x_1 \leq x_2 \leq \cdots$ em Σ é estacionária (isto é, existe n tal que $x_n = x_{n+1} = \cdots$).

(ii) Todo subconjunto não vazio de Σ possui um elemento maximal.

Demonstração: Para provar que (i)⇒(ii), suponha que (ii) seja falsa. Assim, existe um subconjunto não vazio T de Σ sem nenhum elemento maximal. Então podemos construir indutivamente uma sequência infinita e estritamente crescente em T, contrariando (i).

Por outro lado, os elementos de qualquer conjunto não vazio de Σ, se ordenados, formam uma sequência estacionária como em (i). Assim, possui um maio elemento x_n. ■

Se Σ é o conjunto dos submódulos de um módulo M, ordenado pela relação $\subseteq$, então (i) é chamada de *condição de cadeia crescente*, e (ii) de *condição maximal*. Um módulo M satisfazendo uma das duas condições equivalentes é chamado de *Noetheriano*.

Se M for ordenado por $\supseteq$, então (i) é a *condição de cadeia decrescente* e (ii), a *condição mininal*. Um módulo M satisfazendo estas condições é chamado de *Artiniano*.

Exemplo 4.2. *O anel $\mathbb{Z}$ é Noetheriano, pois satisfaz a condição de cadeia crescente. Todo ideal é gerado por um número inteiro, e assim, qualquer cadeia é*

limitada pelo ideal gerado pelo máximo divisor comum dos demais geradores.

Entretanto, $\mathbb{Z}$ não é Artiniano pois, dado $n \in \mathbb{Z}$, temos $(n) \supset (n^2) \supset \cdots \supset (n^k) \supset ...$

Apesar da importância de anéis Artinianos, neste trabalho nos dedicamos apenas ao estudo de anéis Noetherianos. Assim, os próximos resultados se restrigem a anéis com esta propriedade.

A proposição a seguir apresenta uma caracterização de R-módulos Noetherianos.

Proposição 4.3. *M é um R-módulo Noetheriano $\Leftrightarrow$ todo submódulo de M é finitamente gerado.*

Demonstração: Seja N um submódulo de M, e Σ o conjunto de todos os sobmódulos finitamente gerados de N. Então $\Sigma \neq \emptyset$, pois $0 \in \Sigma$, e pelo item (ii) da Proposição 4.1, tem um elemento maximal N_0. Se $N_0 \neq N$, existe $x \in N$ tal que $x \notin N_0$. Considerando o submódulo $N_0 + Rx$, finitamente gerado e que contém N_0 estritamente; obtemos um submódulo finitamente gerado de M que contém estritamente o elemento maximal N_0: uma contradição. Portanto, $N_0 = N$ e N é finitamente gerado.

Agora suponha que M é finitamente gerado e tome $M_1 \subseteq M_2 \subseteq \cdots$ uma cadeia crescente de submódulos de M. Então $N = \bigcup_{n=1}^{\infty} M_n$ é um submódulo de M e, portanto, finitamente gerado por, digamos, $x_1, \cdots, x_r$. Digamos que $x_i \in M_{n_i}$ e seja $n = \max_{i=1}^{r} N_i$. Então cada $x_i \in M_n$, daí $M_n = N$ e, portanto, a cadeia é estacionária. ■

Vejamos como os anéis Noetherianos se comportam em sequências exatas.

Proposição 4.4. *Seja $0 \to M' \xrightarrow{\alpha} M \xrightarrow{\beta} M'' \to 0$ uma sequência exata de R-módulos. Então M é Noetheriano $\Leftrightarrow$ M' e M'' são Noetherianos.*

Demonstração: [$\Rightarrow$] Sejam $M_0' \subseteq M_1' \subseteq \cdots$ uma cadeia de submódulos de M'; e $M_0'' \subseteq M_1'' \subseteq \cdots$ uma cadeia de submódulos de M''. Então $\alpha M_0' \subseteq \alpha M_1' \subseteq \cdots$ e $\beta^{-1} M_0'' \subseteq \beta^{-1} M_1'' \subseteq \cdots$ são cadeias estacionárias em M, pois M é Noetheriano. Portanto, as cadeias também são estacionárias em M' e M''.

[$\Leftarrow$] Se $M_0 \subseteq M_1 \subseteq \cdots$ é uma cadeia de submódulos de M, então $\alpha^{-1} M_0 \subseteq \alpha^{-1} M_1 \subseteq \cdots$ é uma cadeia estacionária em M' e $\beta M_0 \subseteq \beta M_1 \subseteq \cdots$ é uma cadeia estacionária em M''. Logo, M é Noetheriano. ■

Corolário 4.5. *Se Mi* $(1 \leq i \leq n)$ *são R-módulos Noetherianos, então* $\oplus_{i=1}^{n-1} M_i$.

Demonstração: Por indução sobre n na sequência exata

$$0 \to M_n \to \oplus_{i=1}^{n} M_i \to \oplus_{i=1}^{n-1} M_i \to 0.$$

Se $n = 2$, temos a sequência

$$0 \to M_2 \to M_1 \oplus M_2 \to M_1 \to 0$$

com M_1, M_2 Noetherianos. Pela Proposição 4.4, $M_1 \oplus M_2$ é Noetheriano.

Suponhamos que $\oplus_{i=1}^{n-1} M_i$ e M_n sejam módulos Noetherianos. Então, aplicando a Proposição 4.4 na sequência

$$0 \to M_n \to \oplus_{i=1}^{n-1} M_i \oplus M_n \to \oplus_{i=1}^{n-1} M_i \to 0,$$

concluímos que $\oplus_{i=1}^{n-1} M_i$ é Noetheriano. ■

Dizemos que um anel R é Noetheriano (Artiniano) se satisfaz a condição de cadeia crescente (decrescente) para seus ideais. Por exemplo, qualquer corpo K é um anel Noetheriano e Artiniano, pois seu únicos ideais são os triviais. Vejamos mais alguns exemplos.

Exemplo 4.6. *Como consequência da Proposição 4.3, qualquer domínio principal é Noetheriano, uma vez que todos os ideais são finitamente gerados.*

Exemplo 4.7. *O anel* $K[X_1, X_2, ...]$, *K corpo, não é Noetheriano. Basta considerar a sequência* $(X_1) \subset (X_1, X_2) \subset \cdots$. *Entretanto,* $K[X_1, X_2, ...]$ *é um domínio de integridade, e assim possui um corpo de frações. Como o corpo de frações é Noetheriano e contém* $K[X_1, X_2, ...]$, *vemos que um subanel de anel Noetheriano não é, necessariamente, Noetheriano.*

Vimos que nem todo subanel de anel Noetheriano é Noetheriano. Em contrapartida, este fato é válido para R-módulos finitamente gerados, conforme o resultado abaixo.

Proposição 4.8. *Sejam R um anel Noetheriano e M um R-módulo finitamente gerado. Então M é Noetheriano.*

Demonstração: Pela Proposição 2.7, temos que M é isomorfo a um quociente de R^n para algum n. Então, temos uma sequência exata

$$0 \longrightarrow I \longrightarrow R^n \longrightarrow M \longrightarrow 0$$

onde I é o núcleo do homomorfismo de R^n em M. Como R é Noetheriano, pelo resultado anterior, R^n também o é. Assim, a Proposição 4.4 garante que M é Noetheriano. ■

Proposição 4.9. *Sejam R um anel Noetheriano e I um ideal de R. Então R/I é um anel Noetheriano.*

Demonstração: Considerando a sequência exata

$$0 \longrightarrow I \longrightarrow R \longrightarrow \frac{R}{I} \longrightarrow 0$$

e aplicando a Proposição 4.4, temos que $\frac{R}{I}$ é Noetheriano. ■

Uma *cadeia* de submódulos de um módulo M é uma sequência (M_i) $(0 \leq i \leq n)$ de submódulos de M tal que

$$M = M_0 \supset M_1 \supset \cdots \supset M_n = 0.$$

O *comprimento* da cadeia é o número de inclusões n. Uma *série de composição* de M é uma cadeia maximal, ou seja, na qual não se pode inserir nenhum submódulo extra. Isto é equivalente a dizer que cada quociente $M_{i-1}/M_i (1 \leq i \leq n)$ é *simples*; isto é, não possui nenhum submódulo não trivial.

Proposição 4.10. *Suponha que M tenha uma série de composição de comprimento n. Então toda série de composição de M tem comprimento n, e toda cadeia em M pode ser estendida a uma série de composição.*

Demonstração: Denotamos por $\ell(M)$ o maior comprimento de séries de composição de módulos de M. Esta prova será feita em três etapas.

1. Mostremos que $N \subset M \Rightarrow \ell(N) < \ell(M)$. Seja (M_i) uma série de composição em M de comprimento mínimo; e consideremos os submódulo $N_i = N \cap M_i$ de N. Como $\frac{N_{i-1}}{N_i} \subseteq \frac{M_{i-1}}{M_i}$, e $\frac{M_{i-1}}{M_i}$ é simples; temos que

$$\frac{N_{i-1}}{N_i} = \frac{M_{i-1}}{M_i} \text{ ou } N_{i-1} = N_i.$$

Se a segunda condição acontece para algum i, podemos eliminar os termos repetidos da sequência (N_i) e obtermos um série de composição em N. Mas, pelas condições acima, $\ell(N) \leq \ell(M)$. Entretanto, se $\ell(N) = \ell(M)$, então $\frac{N_{i-1}}{N_i} = \frac{M_{i-1}}{M_i}$ para cada $i = 1, 2, ..., n$. Assim, $M_{n-1} = N_{n-1}$, $M_{n-2} = N_{n-2}$, e assim por diante. Logo $M = N$.

2. Vejamos que qualquer cadeia em M tem comprimento menor ou igual a $\ell(M)$. Seja $M = M_0 \supset M_1 \supset \cdots$ uma cadeia de comprimento m. Por 1, temos que $\ell(M_0) > \ell(M_1) > \cdots > \ell(M_k) = 0$; e portanto, $m \leq \ell(M)$.

3. Consideremos qualquer série de composição de M. Se seu comprimemto for m, por 2, $m \leq \ell(M)$, e então $m = \ell(M)$. Assim, todas as séries de composições têm o mesmo comprimento. Finalmente, tomemos qualquer cadeia em M. Se seu comprimento for $\ell(M)$, então é uma série de composição. Se seu comprimento for menor do que $\ell(M)$, não é série de composições, e assim, novos termos podem ser inseridos até que seu comprimento seja $\ell(M)$. ■

Proposição 4.11. *M tem uma série de composição se, e somente se, M satisfaz as duas condições de cadeia.*

Demonstração: [⇒] Como M tem uma série de composição, pela Proposição 4.10, toda cadeia em M pode ser estendida a uma série de composição de mesmo comprimento. Assim, todas as cadeias são limitadas, e M satisfaz ambas as condições de cadeia.

[⇐] Se M satisfaz ambas as condições de cadeia, podemos construir um série de composição em M, como segue.

Como $M = M_0$ satisfaz a condição maximal, possui um submódulo maximal $M_1 \subset M_0$. Da mesma forma, M_1 tem um submódulo maximal $M_2 \subset M_1$; e assim por diante. Dessa forma, obtemos um cadeia estritamente decrescente $M = M_0 \supset M_1 \supset M_2 \supset \cdots$. Como M satisfaz a condição de cadeia decrescente, a sequência contruída é finita. Portanto, obtemos um série de composição de M.

■

Um módulo satisfazendo as condições de cadeia crescente e decrescente é chamado de *módulo de comprimento finito*. Pela Proposição 4.10, todas as séries de composição de M possuem o mesmo comprimento $\ell(M)$, chamado de *comprimento de M*.

O Teorema de Jordan-Hölder é um resultado clássico na teoria de grupos, que afirma: "toda as séries de composição de um grupo G são equivalentes". Este resultado também pode ser aplicado a módulos de comprimento finito: se $(M_i)_{0\leq i\leq n}$ e $(M_i')_{0\leq i\leq n}$ são duas séries de composição de M, existe uma correspondência biunívoca entre o conjunto dos quocientes $\left(\frac{M_{i-1}}{M_i)}\right)_{1\leq i\leq n}$ e o conjunto dos quocientes $\left(\frac{M'_{i-1}}{M'_i}\right)_{1\leq i\leq n}$, tais que os quocientes correspondentes são isomorfos.

A proposição a seguir mostra que o comprimento $\ell(M)$ é um exemplo de função aditiva.

Proposição 4.12. *O comprimento $\ell(M)$ é uma função aditiva na classe de todos os R-módulos de comprimento finito.*

Demonstração: Devemos provar que se a sequência

$$0 \longrightarrow M' \stackrel{\alpha}{\to} M \stackrel{\beta}{\to} M'' \longrightarrow 0$$

é exata, então $\ell(M) = \ell(M') + \ell(M'')$. Tomemos $\alpha(M_0') \supset \alpha(M_1') \supset \cdots \supset \alpha(M_r') = 0$, a imagem por α de uma série de composição $M' = M_0' \supset M_1' \supset \cdots \supset M_r' = 0$ em M'; e $\beta^{-1}(M_0') \supset \beta^{-1}(M_1') \supset \cdots \supset \beta^{-1}(M_s') = 0$, a imagem inversa por β de uma série de composições $M'' = M_0'' \supset M_1'' \supset \cdots \supset M_s'' = 0$ em M''.

Como $\mathrm{Im}(\alpha) = \ker\beta$, temos que $\alpha(M_0') = \beta^{-1}(M_s'')$. Assim, obtemos a série de composição em M

$$\beta^{-1}(M_0'') \supset \beta^{-1}(M_1'') \supset\supset \cdots \beta^{-1}(M_s'') = \alpha(M_0') \supset \alpha(M_1') \supset \cdots \supset \alpha(M_r') = 0$$

de comprimento $n = r + s$. ■

Considerando o caso particular de módulos sobre um corpo K, isto é, são espaços vetoriais sobre K, temos o seguinte resultado.

Proposição 4.13. *Para espaços vetoriais V sobre K, as seguintes condições são equivalentes:*

(i) dimensão finita;

(ii) comprimento finito;

(iii) condição de cadeia crescente;

(iv) condição de cadeia decrescente.

Além disso, se estas condições estão satisfeitas, temos que o comprimento é igual à dimensão.

Demonstração: (i) ⇒(ii). Se V tem dimensão finita, então todos os seus subespaços também têm. Logo, qualquer série de composição é finita.

(ii) ⇒(iii) e (ii) ⇒(iv). Seguem da Proposição 4.11.

(iii) ⇒(i). Suponha que V não tenha dimensão finita. Assim, exsite uma sequência infinita (x_n) de elementos linearmente independentes de V. Seja U_n o espaço vetorial gerado por $x_1, ..., x_n$. Então a cadeia $(U_n)_{n\geq 1}$ é infinita e estritamente crescente; e portanto, V não satisfaz a condição de cadeia crescente.

(iv) $\Rightarrow$(i). Novamente, suponha que V não tenha dimensão finita e seja gerado por (x_n). Seja V_n o espaço vetorial gerado por $x_{n+1}, x_{n+2}, ...,$. Então $(V_n)_{n\geq 1}$ é uma cadeia infinita e estritamente decrescente; contrariando (iv).

Nestas condições, seja n a dimensão de V e $x_1, x_2, ..., x_n$ seus geradores. Assim, temos a série de composição

$$V = (x_1, x_2, ..., x_n) \supset (x_1, x_2, ..., x_{n-1}) \supset \cdots \supset (x_1, x_2) \supset (x_1) \supset (0)$$

de comprimento n. ■

Capítulo 5

Anéis Noetherianos

Recordemos que um anel R é Noetheriano se satisfaz uma das seguintes condições equivalentes:

1) Todo conjunto não vazio de ideais em R tem um elemento maximal.

2) Toda cadeia crescente de ideais em R é estacionária.

3) Todo ideal em R é finitamente gerado.

A equivalência destas condições foi provada nas Proposições 4.1 e 4.3.

Os resultados deste capítulo mostram que um anel Noetheriano R reproduz anéis Noetherianos em várias situações. Em particular, apresentamos o famoso *Teorema da Base de Hilbert*.

Proposição 5.1. *Se R é Noetheriano e f um homomorfismo sobrejetor de R em um anel S, então S é Noetheriano.*

Demonstração: Como $S \cong R/I$, com $I = \ker f$; e R/I é Noetheriano pela Proposição 4.9, então S é Noetheriano. ■

Proposição 5.2. *Seja R um subanel de S, e suponha que R é Noetheriano e que S é um R-módulo finitamente gerado. Então S é um anel Noetheriano.*

Demonstração: Pela Proposição 4.8, temos que S é R-módulo Noetheriano, e portanto, é também um S-módulo Noetheriano. ■

Exemplo 5.3. *Sejam $R = \mathbb{Z}$ e $S = \mathbb{Z}[i]$. Como $\mathbb{Z}$ é anel Noetheriano e subanel de $\mathbb{Z}[i]$, e $\mathbb{Z}[i]$ é finitamente gerado por (a, b), a, b inteiros; a Proposição 5.2 garante que $\mathbb{Z}[i]$ é Noetheriano.*

Proposição 5.4. *Se R é um anel Noetheriano e S é um sistema multiplicativo fechado de R, então $S^{-1}R$ é Noetheriano.*

Demonstração: Como todo ideal em $S^{-1}R$ é um ideal estendido (Proposição 3.11 - (i)), e os ideias estendidos em $S^{-1}R$ estão em correspondência biunívoca com os ideais contraídos em R (Proposição 1.50-(iii)); então os ideais em $S^{-1}R$ satisfazem a condição maximal. ■

Em particular, se $S = R - \mathcal{P}$, onde $\mathcal{P}$ é ideal primo em R, temos o seguinte corolário.

Corolário 5.5. *Se R é Noetheriano e $\mathcal{P}$ é um ideal primo em R, então $R_{\mathcal{P}}$ é Noetheriano.*

Finalmente, apresentamos o

Teorema 5.6 (Teorema da Base de Hilbert)**.** *Se R é Noetheriano, então o anel de polinômios $R[X]$ é Noetheriano.*

Demonstração: Para que $R[X]$ seja Noetheriano, basta mostrar que qualquer ideal em $R[X]$ é finitamente gerado. Seja J um ideal arbitrário em $R[X]$; mostremos que é finitamente gerado.

Considere o conjunto formado por todos os coeficientes dominantes de polinômios em J. Este conjunto é um ideal I em R. De fato, I é um subgrupo aditivo de R:

- $0 \in I$, pois é o coeficiente dominante do polinômio nulo, e este pertence a J já que J é ideal.
- se $a_n \in I$, existe um polinônio $p(X) = a_nX^n + ... + a_0 \in J$. Como J é ideal, o polinômio $-p(X) = -a_nX^n - ... - a_0$ está em J, e portanto, $-a_n \in I$.
- se $a_n, b_m \in I$, existem polinômios $p(X) = a_nX^n + ... + a_0$ e $q(X) = b_mX^m + ... + b_0$ em J. Se $m = n$, é claro que $a_n + b_m$ é coeficiente dominante do polinômio $p(X) + q(X) \in J$. Caso contrário, supondo $m > n$, devemos considerar o polinômio $\phi(X) = X^{m-n} \in R[X]$. Fazendo $p(X) \cdot \phi(X) + q(X)$, obtemos um polinômio em J, pois J é ideal, com coeficiente dominante $a_n + b_m$.

e também satisfaz a condição relativa à multiplicação:

- se $a_n \in J$, existe polinômio $p(X) = a_nX^n + ... + a_0 \in J$. Tomando $c \in R$, temos que $c \cdot p(X) = ca_nX^n + ... + ca_0 \in J$, pois J é ideal. Assim, ca_n é coeficiente dominante de um polinômio em J e, portanto, $ca_n \in I$.

Como R é Noetheriano, todos os seus ideais são finitamente gerados. Em particular, I é finitamente gerado; e sejam $a_1, \cdots, a_n$ seus geradores. Para cada $i = 1, \cdots, n$ existe um polinômio $f_i \in R[X]$ da forma $f_i = a_i X^{r_i} + \Delta_i$, onde Δ_i é um polinômio de grau menor que r_i. Seja $r = max_{i=1}^{n} r_i$. Os f_i geram um ideal $J' \subseteq J$ em $R[X]$.

Seja $f = aX^m + \Lambda$, com Λ um polinômio de grau menor que m. f é um elemento de J, então $a \in I$ e $a = \sum_{i=1}^{n} u_i a_i; u_i \in R$. Se $m \geq r$, temos que $f - \sum u_i f_i X^{m-r_i}$ está em J e tem grau $< m$. De fato:

$$\begin{aligned} f - \sum_{i=1}^{n} u_i f_i X^{m-r_i} &= aX^m + \Lambda - \sum_{i=1}^{n} u_i (a_i X^{r_i} + \Delta_i) X^{m-r_i} \\ &= aX^m + \Lambda - \sum_{i=1}^{n} u_i (a_i X^m + (\Delta_i) X^{m-r_i} \\ &= X^m \left(a - \sum_{i=1}^{n} u_i a_i \right) + \left[\Lambda - \left(\sum_{i=1}^{n} (\Delta_i) X^{m-r_i} \right) \right] \\ &= \Lambda - \left(\sum_{i=1}^{n} (\Delta_i) X^{m-r_i} \right) \end{aligned}$$

onde o grau de $\Lambda - (\sum_{i=1}^{n} (\Delta_i) X^{m-r_i})$ é estritamente menor que m. Se o grau deste polinômio for menor que m e maior ou igual a r, através do mesmo procedimento, subtraímos elementos de J' de f até obtermos um polinômio g de grau $< r$. Então, concluímos que $f = g + h$, onde $h \in J'$.

Seja M o R-módulo finitamente gerado por $1, X, ..., X^{r-1}$. Como $J - J'$ é o ideal formado por todos os polinômios de J com grau estritamente menor que r, temos que $J - J' = (J \cap M)$, e assim, $J = (J \cap M) + J'$. Sendo M é um R-módulo finitamente gerado, pela Proposição 4.8, é Noetheriano. Considerando que $J \cap M$ é um submódulo de M, a Proposição 4.3 nos garante que $J \cap M$ é um R-módulo finitamente gerado.

Sejam $g_1, ..., g_m$ os geradores $J \cap M$. Como $J = (J \cap M) + J'$, com $(J \cap M)$ e J' disjuntos, fica claro que f_i e g_j geram J. Assim J é finitamente gerado e, portanto, $R[X]$ é Noetheriano. ■

Corolário 5.7. *Se R é Noetheriano então $R[X_1, ..., X_n]$ é Noetheriano.*

Demonstração: Por indução sobre n. Para $n = 1$, é o Teorema da Base de Hilbert. Se $n = 2$, temos $R[X_1, X_2] = (R[X_1])[X_2]$. Como $(R[X_1])$ é Noetheriano se R é Noetheriano, então $(R[X_1])[X_2]$ também é.

Suponha que $R[X_1, ..., X_{n-1}]$ seja Noetheriano. Como $R[X_1, ..., X_n] = (R[X_1, ..., X_{n-1}])[X^n]$, concluímos que $R[X_1, ..., X_n]$ é Noetheriano. ■

Capítulo 6

Conjuntos Algébricos Afins

A partir deste momento, abordaremos novos conceitos envolvendo anéis de polinômios, que constituem a base para o estudo de Geometria Algébrica. Para isto, além dos conceitos já vistos, serão necessários algumas novas definições e resultados, reunidos na seção a seguir.

6.1 Preliminares

Seja R um anel e $R[X]$ o anel de polinômios sobre a variável X e com coefientes em R. O grau de um polinômio não nulo $\sum a_i X^i$ é o maior inteiro n tal que $a_n \neq 0$; e um polinômio de grau n é mônico se $a_n = 1$.

Conforme já visto, o anel de polinômios em n variáveis sobre R é denotado por $R[X_1, ..., X_n]$ e isomorfo a $R[X_1, ..., X_{n-1}][X_n]$. Os *monômios* em $R[X_1, ..., X_n]$ são os polinômios $X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$, onde i_j são inteiros não negativos; e o *grau do monômio* é dado por $i_1 + \ldots + i_n$.

Cada elemento $F \in R[X_1, ..., X_n]$ tem uma única expressão $F = \sum a_{(i)} X^{(i)}$, onde $X^{(i)}$ são monômios e $a_{(i)} \in A$. Mais explicitamente, temos

$$F = \sum_{(i)} a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n}; (i) = (i_1, \dots, i_n).$$

Dizemos que F é *homogêneo*, ou uma *forma*, de grau n, se todos os seus coeficientes $a_{(i)}$ são nulos, exceto os coeficientes dos monômios de grau n. Desse modo, qualquer polinômio F pode ser escrito de forma única como $F = F_0 + F_1 + \ldots + F_n$, onde F_i é uma forma de grau i; e se $F_n \neq 0$, temos que o grau de F, $\deg(F)$, é n. Os termos $F_0, F_1, F_2, ...$ são chamados de constante, linear, quadrático, e assim por diante.

Proposição 6.1. *Seja R um domínio.*

(i) *Se F, G são formas de graus r, s, respectivamente, em $R[X_1, \ldots, X_n]$, então $F \cdot G$ é uma forma de grau $r + s$.*

(ii) *Qualquer fator de uma forma em $R[X_1, \ldots, X_n]$ é uma forma.*

Demonstração: (i) Temos que $F = \sum_{(i)} a_{(i)} X_1^{i_1} \ldots X_n^{i_n}$, $(i) = (i_1, \ldots, i_n)$, com $i_1 + \ldots + i_n = r$; e $G = \sum_{(j)} = b_{(j)} X_1^{j_1} \ldots X_n^{j_n}$, $(j) = (j_1, \ldots, j_n)$, com $j_1 + \ldots + j_n = s$; e $a_{(i)} \neq 0$, $b_{(j)} \neq 0$ para algum (i) e algum (j). Assim

$$F \cdot G = \sum_{(i)} \sum_{(j)} a_{(i)} b_{(j)} X_1^{i_1 + j_1} \ldots X_n^{i_n + j_n}$$

com $a_{(i)} b_{(j)} \neq 0$, para algum (i) e algum (j), e $(i_1 + j_1) + \ldots + (i_n + j_n) = r + s$. Portanto, $F \cdot G$ é uma forma de grau $r + s$.

(ii) Suponhamos que $F = G \cdot H$, onde G é forma e H não. Assim, $G = G_r$ para algum $r \neq 0$, e $H = H_s + H_t$, com $s, t \neq 0$ e $s \neq t$. Então

$$F = G \cdot H = G_r \cdot (H_s + H_t) = (G_r \cdot H_s) + (G_r \cdot H_t) = F_{r+s} + F_{r+t}$$

onde $r + s \neq 0$, $r + t \neq 0$ e $r + s \neq r + t$. Logo F não é uma forma. ■

Proposição 6.2. *Se R é um domínio, e F, G são polinômios em $R[X_1, \ldots, X_n]$, então* $\deg(F \cdot G) = \deg(F) + \deg(G)$.

Demonstração: Para o caso de polinômios sobre uma variável, temos

$$F = a_r X^r + a_{r-1} X^{r-1} + \ldots + a_1 X + a_0$$

e

$$G = b_s X^s + b_{s-1} X^{s-1} + \ldots + b_1 X + b_0$$

com graus r e s, respectivamente. Sem perda de generalidade, suponhamos que $r \leq s$. Assim

$$\begin{aligned} F \cdot G &= a_0 b_0 + (a_1 b_0 + b_1 a_0) X + \ldots + (a_r b_0 + a_{r-1} b_1 + \ldots + a_0 b_r) X^r \\ &+ \ldots + (a_0 b_s + a_1 b_{s-1} + \ldots + a_r b_{s-r}) X^s + \ldots + a_r b_s X^{r+s} \end{aligned}$$

Como R é domínio, $a_r b_s \neq 0$, pois $a_r \neq 0$ e $b_s \neq 0$. Logo, $\deg(F \cdot G) = r + s = \deg(F) + \deg(G)$.

Mais geralmente, sejam $F, G \in R[X_1, \ldots, X_n]$, com graus r, s, respectivamente. Temos $F = F_0 + F_1 + \ldots + F_r$ e $G = G_0 + G_1 + \ldots + G_s$. Supondo $r \leq s$, obtemos

$$\begin{aligned} F \cdot G &= F_0G_0 + F_1G_0 + F_0G_1 + \ldots + F_0G_s + \ldots + F_rG_{s-r} + \ldots + F_rG_s \\ &= H_0 + H_1 + \ldots + H_r + \ldots + H_s + \ldots + H_{r+s}, \end{aligned}$$

onde $H_k = \sum_{j=0}^{k} F_kG_{k-j}$, são formas de grau k, pelo o item (i) acima. Como $\deg(F) = r$ e $\deg(G) = s$, então $H_{r+s} \neq 0$; e portanto, $\deg(F \cdot G) = \deg(F) + \deg(G)$. ■

É claro que todo anel de polinômios $R[X_1, \ldots, X_n]$ contém R como subanel, pois este representa o conjunto dos polinômios constantes. Além disso, $R[X_1, \ldots, X_n]$ satisfaz a seguinte propriedade:

Proposição 6.3. *Se $\varphi : R \to S$ é um homomorfismo de anéis, e $s_1, \ldots, s_n \in S$, então existe uma única extensão de φ, denotada por $\widetilde{\varphi}$, onde $\widetilde{\varphi} : R[X_1, \ldots, X_n] \to S$ é um homomorfismo de anéis tal que $\widetilde{\varphi}(X_i) = s_i$, $i = 1, \ldots, n$. A imagem de F por $\widetilde{\varphi}$ é denotada por $F(s_1, \ldots, s_n)$.*

Demonstração: Basta considerar

$$\begin{aligned} \widetilde{\varphi} : R[X_1, \ldots, X_n] &\longrightarrow S \\ F = \sum_{(i)} a_{(i)}X^{(i)} &\longmapsto \widetilde{\varphi}(F) = \sum_{(i)} \varphi(a_{(i)})s^{(i)}, \end{aligned}$$

onde $X^{(i)} = X_1^{i_1} \ldots X_n^{i_n}$, e $s^{(i)} = s_1^{i_1} \ldots s_n^{i_n}$.

Obviamente, $\widetilde{\varphi}$ está bem definido. Além disso, $\widetilde{\varphi}$ é um homomorfismo de anéis, uma vez que φ é homorfismo.

Claramente $\widetilde{\varphi}|_R = \varphi$, logo $\widetilde{\varphi}$ é extensão de φ. Por fim, suponha $\psi : R[X_1, \ldots, X_n] \to S$, com $\psi|_R = \varphi$ e $\psi(X_i) = s_i$. Então, para $F \in R[X_1, \ldots, X_n]$ temos:

- Se $F = a \in R$, então $\psi(F) = \varphi(a) = \widetilde{\varphi}(a)$.
- Se $F = \sum_{(i)} a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$, então

$$\begin{aligned} \psi(F) &= \sum_{(i)} \psi(a_{i_1 \ldots i_n}) \psi(X_1^{i_1} \ldots X_n^{i_n}) \\ &= \sum_{(i)} \varphi(a_{i_1 \ldots i_n}) s_1^{i_1} \ldots s_n^{i_n} = \widetilde{\varphi}(F). \end{aligned}$$

Portanto, $\psi = \widetilde{\varphi}$. ■

Seja R um domínio. Definimos a *caracterísitica* de R, $\mathrm{char}(R)$, como o menor inteiro positivo c tal que $1 + \ldots + 1(c \text{ parcelas}) = 0$, se tal c existe; caso contrário, $\mathrm{char}(R) = 0$.

Proposição 6.4. *Se $char(R) = p > 0$, então p é primo.*

Demonstração: Se $\phi : \mathbb{Z} \to R$ é o homomorfismo de anéis de $\mathbb{Z}$ em R, e R é anel com característica positiva, então char(R)= p e $\ker\phi = (p)$, com p primo. De fato, seja $p = \text{char}(R)$. Mostremos que $\ker\phi = (p)$. Para $m \in \ker\phi$, temos

$$\phi(m) = 0 \Rightarrow \phi(\underbrace{1 + \ldots + 1}_{m \text{ parcelas}}) = \phi(1) + \ldots + \phi(1) = 1 + \ldots + 1 = 0$$

e assim, $m = pq + r$. Com isso, $1 + \ldots + 1$ (r parcelas) é igual a 0. Como $r < p$ e p=char(R), temos $r = 0$ e $p \mid m$, isto é, $m \in (p)$.

Por outro lado, temos que

$$0_R = \underbrace{1_R + \ldots + 1_R}_{p \text{ parcelas}} = \phi(1 + \ldots + 1) = \phi(p),$$

e logo, $p \in \ker\phi$. Para qualquer $z \in (p)$, temos $\phi(z) = \phi(a)\phi(p) = 0$. Portanto $z \in \ker\phi$.

Agora, supondo p não primo, temos $p = ab$. Daí,

$$\phi(p) = \phi(a) \cdot \phi(b) = 0 \Rightarrow \phi(a) = 0 \text{ ou } \phi(b) = 0$$

pois R é domínio. Se $\varphi(a) = 0$, então $\text{char}(R) = a$ e $a < p$; e se $\varphi(b) = 0$, char(R)=b e $b < p$, o que contraria a minimalidade de p. Logo p é primo. ■

Seja R um anel qualquer. A *derivada* de um polinômio $F = \sum a_i X^i \in R[X]$ é definida como $\sum i a_i X^{i-1}$, e denotada por F_X. Se $F \in K[X_1, \ldots, X_n]$, então F_{X_i} é definida considerando F como um polinômio em X_i com coeficientes em $R[X_1, \ldots, X_{i-1}, X_{i+1}, \ldots, X_n]$. A proposição a seguir apresenta algumas propriedades da derivada de um polinômio.

Proposição 6.5. *A derivada de um polinômio satisfaz as seguintes propriedades:*

(i) $(a \cdot F + b \cdot G)_X = (a \cdot F_X) + (b \cdot G_X)$; $a, b \in A$.

(ii) $F_X = 0$ *se* F *é constante.*

(iii) $(F \cdot G)_X = (F_X \cdot G) + (F \cdot G_X)$, *e* $(F^n)_X = n \cdot F^{n-1} \cdot F_X$.

(iv) *Se* $G_1, \ldots, G_n \in R[X]$ *e* $F \in R[X_1, \ldots, X_n]$, *então* $F(G_1, \ldots, G_n)_X = \sum_{i=1}^{n} F_{X_i}(G_1, \ldots, G_n) \cdot (G_i)_X$.

(v) $F_{X_iX_j} = F_{X_jX_i}$, *onde* $F_{X_iX_j} = (F_{X_i})_{X_j}$.

(vi) (Teorema de Euler) *Se* F *é uma forma de grau* m *em* $R[X_1, \ldots, X_n]$, *então* $mF = \sum_{j=1}^{n} X_j F_{X_j}$.

Demonstração: (i) Sejam $F = a_0+a_1X+\ldots+a_nX^n$ e $G = b_0+b_1X+\ldots+b_mX^m$, com $n \leq m$. Para $a, b \in A$, temos

$$\begin{aligned}(a \cdot F + b \cdot G)_X &= (aa_0 + aa_1X + \ldots aa_nX^n + bb_0 + bb_1X + \ldots + bb_mX^m)_X \\ &= aa_1 + \ldots + naa_nX^{n-1} + bb_1 + \ldots mbb_mX^{m-1} \\ &= a\left(a_1 + \ldots + na_nX^{n-1}\right) + b\left(b_1 + \ldots mb_mX^{m-1}\right) \\ &= (a \cdot F_X) + (b \cdot G_X)\end{aligned}$$

(ii) É óbvio.

(iii) A primeira parte será dividida em três casos:

- $F = c$ constante e G como definida em (i).

  Como $c \cdot G = cb_0 + b_1X + \ldots + cb_mX^m$, então

  $$(c \cdot G)_X = cb_1 + 2cb_2X + \ldots + mcb_mX^{m-1}.$$

  Por outro lado,

  $$c_X \cdot G + c \cdot G_X = 0 \cdot G + c(b_1 + \ldots + mb_mX^{m-1});$$

  e logo

  $$(c \cdot G)_X = c_X \cdot G + c \cdot G_X.$$

- Em particular, consideremos $F = X^n$ e $G = X^m$. Temos $F_X = nX^{n-1}$ e $G_X = mX^{m-1}$; e assim,

  $$(F_X \cdot G) + (F \cdot G_X) = nX^{m+n-1} + mX^{n+m-1} = (m+n)X^{m+n-1}.$$

  Agora, como $F \cdot G = X^{m+n}$, então $(F \cdot G)_X = (m+n)X^{m+n-1}$.

- Finalmente, sejam $F = \sum_{i=0}^{n} a_iX^i$ e $G = \sum_{j=0}^{m} b_jX^j$. Então $F \cdot G = \sum_i \sum_j a_ib_jX^iX^j$. O primeiro caso garante que

  $$(F \cdot G)_X = \sum_i \sum_j a_ib_j \left(X^iX^j\right)_X;$$

  e o segundo, que

  $$(F \cdot G)_X = \sum_i \sum_j a_ib_j \left(X^i_XX^j + X^iX^j_X\right).$$

  Daí

  $$(F \cdot G)_X = \sum_i a_i(X^i)_X \sum_j b_jX^j + \sum_i a_iX^i \sum_j b_j(X^j)_X,$$

  isto é,

  $$(F \cdot G)_X = F_XG + FG_X.$$

A demonstração de $(F^n)_X = n \cdot F^{n-1} \cdot F_X$ será feira por indução sobre n. Este fato é claramente verdadeiro para $n = 0$ ou $n = 1$. Para $n = 2$, basta considerar $F = G$ na expressão $(F \cdot G)_X = (F_X \cdot G) + (F \cdot G_X)$. De fato, $(F^2)_X = (F_X \cdot F) + (F \cdot F_X) = 2 \cdot F \cdot F_X$.

Suponhamos que tal relação seja válida para todos os naturais até n. Vejamos para $n + 1$.

É claro que

$$(F^{n+1})_X = (F^n \cdot F)_X = (F_X^n \cdot F) + (F^n \cdot F_X),$$

e usando a hipótese de indução, temos:

$$(F^{n+1})_X = \big(\big(n \cdot F^{n-1} \cdot F_X\big) \cdot F\big) + (F^n \cdot F_X) = (n+1) \cdot F^n \cdot F_X.$$

Portanto, $(F^n)_X = n \cdot F^{n-1} \cdot F_X$.

(iv) Considerando a propriedade (i), é suficiente mostrarmos para F, quando F é um monômio, isto é, $F = X_1^{k_1} \dots X_n^{k_n}$. Assim,

$$\begin{aligned}
F(G_1, \dots, G_n)_X &= (G_1^{k_1} \cdot \ldots \cdot G_n^{k_n})_X \\
&\overset{(iii)}{=} (G_1^{k_1})_X \cdot \ldots \cdot G_n^{k_n} + \ldots + G_1^{k_1} \cdot \ldots \cdot (G_n^{k_n})_X \\
&\overset{(iii)}{=} k_1 \cdot G_1^{k_1 - 1}(G_1)_X \cdot \ldots \cdot G_n^{k_n} + \ldots + G_1^{k_1} \ldots \cdot k_n G_n^{k_n - 1}(G_n)_X \\
&= F_{X_1}(G_1, \dots, G_n) \cdot (G_1)_X + \ldots + F_{X_n}(G_1, \dots, G_n) \cdot (G_n)_X \\
&= \sum_{i=1}^{n} F_{X_i}(G_1, \dots, G_n) \cdot (G_i)_X.
\end{aligned}$$

(v) Novamente por (i), basta verificar para o caso em que $F = X_1^{k_1} \cdot \ldots \cdot X_n^{K_n}$. Podemos supor, sem perda de generalidade, que $i \leq j$. Então

$$\begin{aligned}
F_{X_i X_j} &= \left(X_1^{k_1} \dots X_{i-1}^{k_{i-1}} X_i^{k_i - 1} X_{i+1}^{k_{i+1}} \dots X_n^{k_n}\right)_{X_j} \\
&= k_j k_i X_1^{k_1} \dots X_{i-1}^{k_{i-1}} X_i^{k_i - 1} X_{i+1}^{k_{i+1}} \dots X_{j-1}^{k_{j-1}} X_j^{k_j - 1} X_{j+1}^{k_{j+1}} \dots X_n^{k_n} \\
&= \left(k_j X_1^{k_1} \dots X_{j-1}^{k_{j-1}} X_j^{k_j - 1} X_{j+1}^{k_{j+1}} \dots X_n^{k_n}\right)_{X_i} \\
&= F_{X_j X_i}
\end{aligned}$$

(vi) F é uma forma de grau m, isto é, $F = \sum_{(i)} a_{(i)} X_1^{i_1} \dots X_n^{i_n}$, onde $(i) = (i_1, \dots, i_n)$ e $i_1 + \ldots i_n = m$. Assim,

$$\begin{aligned} F_{X_1} &= i_1 \sum_{(i)} a_{(i)} X_1^{i_1-1} X_2^{i_2} \dots X_n^{i_n} \\ F_{X_2} &= i_2 \sum_{(i)} a_{(i)} X_1^{i_1} X_2^{i_2-1} \dots X_n^{i_n} \\ &\vdots \\ F_{X_n} &= i_n \sum_{(i)} a_{(i)} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n-1}. \end{aligned}$$

Obviamente, $X_j F_{X_j} = i_j \sum_{(j)} F$, e então

$$\sum_{j=1}^{n} X_j F_{X_j} = (i_1 + \dots i_n)\, F = mF.$$

■

Se R é um anel, $a \in R$, $F \in R[X]$, dizemos que a é uma *raiz* de F se $F(a) = 0$. Como consequência, temos que $F = (X - a)G$, para algum $G \in R[X]$. Com efeito, o Algoritmo da Divisão em $R[X]$ garante a existência de $Q, R \in R[X]$ tais que $F = (X-a)\cdot Q + R$, com $R = 0$ ou $\deg R < \deg (X - a) = 1$. Assim, R é necessariamente uma constante, e $F(a) = 0$ implica que $R = 0$. Logo $F = (X-a)\cdot G$. Mais geralmente, para $F \in K[X_1, \dots, X_n]$, se $F(a_1, \dots, a_n) = 0$, então $F = \sum_{i=1}^{n} (X_i - a_i) G_i$, para algum $G_i \in K[X_1, \dots, X_n]$.

Um corpo K é *algebricamente fechado* se qualquer polinômio não constante $F \in K[X]$ tem raiz. Segue que $F = \alpha \prod (X - \lambda_i)^{m_i}$, $\alpha, \lambda_i \in K$, onde λ_i são as raízes distintas de F, e m_i é a *multiplicidade* de λ_i. Um polinômio de grau n tem n raízes em K, contando as multiplicidades.

As proposições seguintes apresentam algumas características de anéis de polinômios sobre um corpo K.

Proposição 6.6. *Seja K um corpo infinito, $F \in K[X_1, \dots, X_n]$. Suponha $F(a_1, \dots, a_n) = 0$ para todo $a_1, \dots, a_n \in K$. Então $F \equiv 0$.*

Demonstração: Escreva $F = \sum F_i X_n^i$, com $F_i \in K[X_1, \dots, X_{n-1}]$; prodecemos por indução sobre n. Se $n = 1$, temos que F é um polinômio em $K[X]$ e tem no máximo $\deg F$ raízes. Assim, se $F(a) = 0$ para qualquer $a \in K$, necessariamente, temos que $F \equiv 0$, pois K é infinito.

Suponhamos agora que se $G \in K[X_1, \dots, X_{n-1}]$ é tal que $G(a_1, \dots, a_{n-1}) = 0$ para quaisquer $a_1, \dots, a_{n-1} \in K$, então $G \equiv 0$.

Para $F \in K[X_1, \ldots, X_n]$, temos $F(a_1, \ldots, a_{n-1}, X_n) = \sum F_i(a_1, \ldots, a_{n-1})X_n^i$. Se para todo i, $F_i(a_1, \ldots, a_{n-1}) = 0$ para quaisquer a_1, $\ldots, a_{n-1}$, então $F_i \equiv 0$, pela hipótese de indução, e portanto, $F \equiv 0$.

Entretanto, se para algum i, tivermos $F_i(a_1, \ldots, a_{n-1}) \neq 0$, então $F(a_1, \ldots, a_{n-1}, X_n)$ é um polinômio de um variável e, assim, tem um número finito de raízes. Logo, existiria $a_n \in K$ tal que $F(a_1, \ldots, a_{n-1}, a_n) \neq 0$; absurdo.

■

Proposição 6.7. *Seja K um corpo. Então existe um número infinito de polinômios mônicos irredutíveis em $K[X]$.*

Demonstração: Suponha que $F_1, \ldots, F_n$ sejam os únicos polinômios mônicos irredutíveis de $K[X]$, e considere $G = F_1 \cdot \ldots \cdot F_n + 1$. Seja $G = u \cdot F_1^{i_1} \cdot \ldots \cdot F_n^{i_n}$ a decomposição de G em fatores irredutíveis.

Para algum $i_k \neq 0$, temos $F_k \mid F_1 \cdot \ldots \cdot F_n$ e $F_k \mid G$. Logo $F_k \mid (G - F_1 \cdot \ldots \cdot F_n) \Rightarrow F_k \mid 1$, o que é um absurdo. ■

Como aplicação do resultado anterior, temos o seguinte corolário.

Corolário 6.8. *Todo corpo algebricamente fechado é infinito.*

Demonstração: Como K é algebricamente fechado, todo polinômio $F \in K[X]$ se escreve como $F = c\prod(X - a_i)^{m_i}$, com $a_i \in K$ e m_i multiplicidade de a_i. Assim, os polinômios mônicos irredutíveis de $K[X]$ são da forma $X - a$, para $a \in K$. Pela proposição anterior, existe um número infinito de tais polinômios; e logo, K é infinito. ■

6.2 Formas

Recordemos que um forma $F \in R[X_1, \ldots, X_n]$ de grau d é um polinômio $F = \sum a_{(i)}X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$, com $i_1 + \ldots + i_n = d$, para toda n-upla $(i) = (i_1, \ldots, i_n)$.

Seja R um domínio. Se $F \in R[X_1, \ldots, X_{n+1}]$ é uma forma, definimos $F_* \in R[X_1, \ldots, X_n]$ por $F_* = F(X_1, \ldots, X_n, 1)$. Reciprocamente, para todo polinômio $f \in R[X_1, \ldots, X_n]$ de grau d, escrevemos $f = f_0 + f_1 + \ldots + f_d$, onde f_i é uma forma de grau i, e definios $f^* \in R[X_1, \ldots, X_{n+1}]$ tomando

$$f^* = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + \ldots + f_d = X_{n+1}^d f(X_1/X_{n+1}, \ldots, X_n/X_{n+1}).$$

É claro que f^* é uma forma de grau d. Estes processos podem ser chamados, respectivamente, de "desomogeneização" e "homogeneização" de

polinômios com respeito a X_{n+1}. A seguir, apresentamos as propriedades satisfeitas por F_* e f^*.

Proposição 6.9. (i)$(F \cdot G)_* = F_* \cdot G_*$; $(f \cdot g)^* = f^* \cdot g^*$.

(ii) *Se $F \neq 0$ e r é a maior potência de X_{n+1} que divide F, então* $X_{n+1}^r (F_*)^* = F$; $(f^*)_* = f$.

(iii) $(F+G)_* = F_* + G_*$; $X_{n+1}^t (f+g)^* = X_{n+1}^r (f)^* + X_{n+1}^s (g)^*$, *onde* $r = \deg(g)$, $s = \deg(f)$, *e* $t = r + s - \deg(f+g)$.

Demonstração: (i) Para as formas $F, G \in R[X_1, \ldots, X_{n+1}]$, temos:

$$(F \cdot G)_* = (F \cdot G)(X_1, \ldots, X_n, 1) = F(X_1, \ldots, X_n, 1) \cdot G(X_1, \ldots, X_n, 1) = F_* \cdot G_*.$$

Agora, para $f, g \in R[X_1, \ldots, X_n]$, com $\deg f = r$ e $\deg g = s$, temos que

$$f^* = X_{n+1}^r f\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right)$$

e

$$g^* = X_{n+1}^s g\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right);$$

então

$$f^* \cdot g^* = X_{n+1}^{r+s} (f \cdot g)\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right) = (f \cdot g)^*.$$

(ii) A primeira parte é óbvia:

$$(f^*)_* = X_{n-1}^d f_*\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right) = f(X_1, \ldots, X_n) = f.$$

Agora, escrevendo $F = X_{n+1}^r G$, temos que $F_* = G_*$, com $\deg F = \deg G + r$. Assim,

$$(F_*)^* = (G_*^* = X_{n+1}^{\deg G} G_*\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right).$$

Como $\deg G = \deg F - r$ e $G_* = F_*$, então

$$(F_*)^* = X_{n+1}^{\deg F - r} F_*\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right).$$

Multiplicando ambos os lados por X_{n+1}^r, obtemos

$$X_{n+1}^r (F_*)^* = X_{n+1}^{\deg F} F_*\left(\frac{X_1}{X_{n+1}}, \ldots, \frac{X_n}{X_{n+1}}\right) = F.$$

(iii) Usando as propriedades de polinômios, é claro que

$$(F+G)_* = (F+G)(X_1,\ldots,X_n,1) = F(X_1,\ldots,X_n,1)+G(X_1,\ldots,X_n,1) = F_*+G_*.$$

Por fim, seja $\deg f = r$ e $\deg g = s$. Então

$$f^* = X_{n+1}^r f\left(\frac{X_1}{X_{n+1}},\ldots,\frac{X_n}{X_{n+1}}\right)$$

e

$$g^* = X_{n+1}^s g\left(\frac{X_1}{X_{n+1}},\ldots,\frac{X_n}{X_{n+1}}\right).$$

Além disso, sendo $q = \deg f + g$, temos

$$\begin{aligned}(f+g)^* &= X_{n+1}^q (f+g)\left(\frac{X_1}{X_{n+1}},\ldots,\frac{X_n}{X_{n+1}}\right)\\ &= X_{n+1}^q f\left(\frac{X_1}{X_{n+1}},\ldots,\frac{X_n}{X_{n+1}}\right) + X_{n+1}^q g\left(\frac{X_1}{X_{n+1}},\ldots,\frac{X_n}{X_{n+1}}\right).\end{aligned}$$

Logo, sendo $t = r+s-q$, obtemos

$$\begin{aligned}X_{n+1}^{r+s-q}(f+g)^* &= X_{n+1}^{r+s} f\left(\frac{X_1}{X_{n+1}},\ldots,\frac{X_n}{X_{n+1}}\right) + X_{n+1}^{r+s} g\left(\frac{X_1}{X_{n+1}},\ldots,\frac{X_n}{X_{n+1}}\right)\\ &= X_{n+1}^r f^* + X_{n+1}^s g^*.\end{aligned}$$

■

6.3 Espaços Afins e Conjuntos Algébricos

Seja K um corpo. Denotamos por $\mathbb{A}^n(K)$ o produto cartesiano de K por K n vezes. Assim, $\mathbb{A}^n(K)$ é o conjunto das n-uplas de elementos de K, e é chamado de *espaço afim* de dimensão n sobre K e seus elementos são chamados de *pontos*.

Se $F \in K[X_1,\ldots,X_n]$, um ponto $P = (a_1,\ldots,a_n) \in \mathbb{A}^n(K)$ é um *zero* de F se $F(P) = F(a_1,\ldots,a_n) = 0$. Se F não é constante, o conjunto de zeros de F é chamado de *hipersuperfície* definida por F, e denotada por $\mathcal{V}(F)$. Uma hipersuperfície em $\mathbb{A}^2(K)$ é chamada *curva plana afim*. Se F é um polinômio de grau um, $\mathcal{V}(F)$ é um *hiperplano* em $\mathbb{A}^n(K)$, e se $n = 2$, é uma *linha*.

Mais geralmente, se S é um conjunto qualquer de polinômios em $K[X_1,\ldots,X_n]$, definimos $\mathcal{V}(S) = \{P \in \mathbb{A}^n(K) : F(P) = 0 \text{ para todo } F \in S\}$. Temos que $\mathcal{V}(S) = \bigcap_{F\in S}\mathcal{V}(F)$. Se $S = \{F_1,\ldots,F_r\}$, escrevemos $\mathcal{V}(F_1,\ldots,F_r)$ ao invés de $\mathcal{V}(\{F_1,\ldots,F_r\})$.

Definição 6.10 (Conjunto Algébrico)**.** *Um subconjunto $X \subset \mathbb{A}^n(K)$ é um* conjunto algébrico afim*, ou simplesmente, um* conjunto algébrico*, se $X = \mathcal{V}(S)$ para algum S.*

O resultado a seguir apresenta as propriedades satisfeitas por um conjunto algébrico em $\mathbb{A}^n$.

Proposição 6.11. (i) *Se $I \subset J$, então $\mathcal{V}(I) \supset \mathcal{V}(J)$.*

(ii) *Se I é o ideal em $R[X_1, \ldots, X_n]$ gerado por S, então $\mathcal{V}(S) = \mathcal{V}(I)$; e então todo conjunto algébrico é igual a $\mathcal{V}(I)$ para algum ideal I.*

(iii) *Se $\{I_\alpha\}$ é uma coleção qualquer de ideais, então $\mathcal{V}\left(\bigcup_\alpha I_\alpha\right) = \bigcap_\alpha \mathcal{V}(I_\alpha)$; e então a intersecção de qualquer coleção de conjuntos algébricos é um conjunto algébrico.*

(iv) *$\mathcal{V}(F \cdot G) = \mathcal{V}(f) \bigcup \mathcal{V}(G)$ para quaisquer polinômios F, G; e $\mathcal{V}(I) \bigcup \mathcal{V}(J) = \mathcal{V}(\{F \cdot G : F \in I, G \in J\})$. Então qualquer união finita de conjuntos algébricos é um conjuto algébrico.*

(v) *$\mathcal{V}(0) = \mathbb{A}^n(K)$, $\mathcal{V}(1) = \emptyset$, e $\mathcal{V}(X_1 - a_1, \ldots, X_n - a_n) = \{(a_1, \ldots, a_n)\}$ para $a_i \in K$. Então qualquer subconjunto finito de $\mathbb{A}^n(K)$ é um conjunto algébrico.*

Demonstração: (i) Temos que $\mathcal{V}(J) = \{P \in \mathbb{A}^n : F(P) = 0, \forall F \in J\}$. Como $I \subset J$, $F(P) = 0$ também é válido, em particular, para os pontos $P \in I \subset J$. Logo, se $P \in \mathcal{V}(J)$, então $P \in \mathcal{V}(I)$; e portanto, $\mathcal{V}(J) \subset \mathcal{V}(I)$.

(ii) Como $I = (S)$ temos, obviamente, $S \subset I$. Pela propriedade anterior, $\mathcal{V}(I) \subset \mathcal{V}(S)$. Agora, tomando $P \in \mathcal{V}(S)$, temos $F(P) = 0$ para todo $F \in S$. Como $I = (S)$, se $G \in I$, então $G = \sum a_i s_i$, $a_i \in R[X_1, \ldots, X_n]$ e $s_i \in S$. Assim,

$$G(P) = \sum a_i s_i(P) = \sum a_i 0 = 0.$$

Portanto, $P \in \mathcal{V}(I)$, e $\mathcal{V}(S) \subset \mathcal{V}(I)$.

(iii) Como $I_\alpha \subset \cup_\alpha I_\alpha$, para todo α, temos $\mathcal{V}(\cup_\alpha I_\alpha) \subset \mathcal{V}(I_\alpha)$ para todo α. Logo $\mathcal{V}(\cup_\alpha I_\alpha) \subset \cap_\alpha \mathcal{V}(I_\alpha)$.

Por outro lado, se $P \in \cap_\alpha \mathcal{V}(I_\alpha)$, então $P \in \mathcal{V}(I_\alpha)$ para todo α. Daí $F(P) = 0$ para todo $F \in I_\alpha$, para todo α; o que implica que $F(P) = 0$ para todo $F \in \cup_\alpha I_\alpha$. Portanto, $P \in \mathcal{V}(\cup_\alpha I_\alpha)$.

(iv) Como $(F \cdot G)(P) = F(P) \cdot G(P)$, é claro que se $P \in \mathcal{V}(F) \cup \mathcal{V}(G)$, então $P \in \mathcal{V}(FG)$. Por outro lado, se $P \in \mathcal{V}(F \cdot G)$, temos que $F(P) \cdot G(P) = 0$. Mas $F(P), G(P) \in K$, K corpo, e assim, $F(P) = 0$ ou $G(P) = 0$; isto é, $P \in \mathcal{V}(F) \cup \mathcal{V}(G)$.

Analogamente, se $P \in \mathcal{V}(\{F \cdot G : F \in I, G \in J\})$, então $F(P) = 0$ para todo $F \in I$, ou $G(P) = 0$ para todo $G \in J$. Assim $P \in \mathcal{V}(I) \cup \mathcal{V}(J)$. Também se $P \in \mathcal{V}(I) \cup \mathcal{V}(J)$, então $F(P) = 0$ para todo $F \in I$, ou $G(P) = 0$ para todo $G \in J$. Logo $P \in \mathcal{V}(\{F \cdot G : F \in I, G \in J\})$.

(v) Obviamente, o polinômio nulo é o único que se anula em todo $P \in \mathbb{A}^n$. Também é claro que um polinômio constante não nulo, não se anula em nenhum ponto de $\mathbb{A}^n$.

Agora, $P \in \mathcal{V}(X_1 - a_1, \ldots, X_n - a_n)$ se, e somente se, $P = (b_1, \ldots, b_n)$, onde $(X_i - a_i)(b_i) = 0$, isto é, se $a_i = b_i$, $i = 1, \ldots, n$. Portanto, $P \in \mathcal{V}(X_1 - a_1, \ldots, X_n - a_n)$ se, e somente se, $P = (a_1, \ldots, a_n)$. ■

Exemplo 6.12. *O conjunto* $\{(t, t^2, t^3) \in \mathbb{A}^3(K) : t \in K\}$ *é um conjunto algébrico. De fato, consideremos os polinômios* $F = X_1^2 - X_2$ *e* $G = X_1^3 - X_3$. *É claro que se* $P = (t, t^2, t^3)$, *temos* $F(P) = 0$ *e* $G(P) = 0$, *para todo* $t \in K$. *Logo, o conjunto* $\{(t, t^2, t^3) \in \mathbb{A}^3(K) : t \in K\} = \mathcal{V}(F, G)$, *e portanto, é algébrico.*

Em particular, se I, J são ideais comaximais de R, isto é, $I + J = R$, temos:

Proposição 6.13. *Seja* K *um corpo algebricamente fechado. Então dois ideais* $I, J \in K[X_1, \ldots, X_n]$ *são comaximais se, e somente se,* $\mathcal{V}(I) \cap \mathcal{V}(J) = \emptyset$.

Demonstração: Suponhamos I, J comaximais. Como $(I + J)(I \cap J) \subseteq IJ$ para quaisquer ideais I, J, temos $\mathcal{V}(IJ) \subseteq \mathcal{V}(I + J) \cap \mathcal{V}(I \cap J)$. Como $I + J = (1)$, pois são maximais, $\mathcal{V}(1) = \emptyset$ e $\mathcal{V}(iJ) = \mathcal{V}(I) \cap \mathcal{V}(J)$, então $\mathcal{V}(I) \cap \mathcal{V}(J) = \emptyset$.

Agora, suponha I, J não maximais, isto é, temos $IJ \subset I \cap J$, mas $I \cap J \not\subset IJ$. Daí, $\mathcal{V}(I) \cap \mathcal{V}(J) = \mathcal{V}(IJ) \not\subset \mathcal{V}(I \cap J)$. Assim, existe $P \in \mathcal{V}(I) \cap \mathcal{V}(J)$ tal que $P \notin \mathcal{V}(I \cap \mathcal{J})$, e $\mathcal{V}(I \cap J) \neq \emptyset$, pois K é algébrico. Logo, $\mathcal{V}(I) \cap \mathcal{V}(J) \neq \emptyset$.

■

Por outro lado, supondo que $\mathcal{V}(I) \cap \mathcal{V}(J) \neq \emptyset$, não é possível que todo polinômio em $H \in K[X_1, \ldots, X_n]$ se escreva como $H = F + G$, com $F \in I, G \in J$, pois qualquer polinômio constante não nulo não possui tal expressão. Logo, I, J não são comaximais.

A seguir, caracterizamos os conjuntos algébricos no espaço afim $\mathbb{A}^1(K)$.

Exemplo 6.14. *Os subconjuntos algébricos de* $\mathbb{A}^1(K)$ *são os subconjuntos finitos, e o próprio conjunto* $\mathbb{A}^1(K)$.

Demonstração: Pelo item (v) da Proposição 6.11, sabemos que todo subconjunto finito é algébrico, e que $\mathbb{A}^1(K)$ é um conjunto algébrico. Basta verificar que, em $\mathbb{A}^1(K)$, todo subonjunto algébrico é finito.

Seja $V \subset \mathbb{A}^1(K)$ algébrico, isto é, $V = \mathcal{V}(S)$ para algum $S \subset K[X]$. Assim, $V = \{P \in \mathcal{A}^1(K) : F(P) = 0, \forall P \in S\}$. Se V for infinito, F admitirá infinitas raízes, o que é absurdo. Logo V é finito. ■

6.4 O Ideal de um Conjunto de Pontos

Para qualquer subconjunto X de $\mathbb{A}^n(K)$, consideramos os polinômios que se anulam em X. Tais polinômios formam um ideal em $K[X_1, \ldots, X_n]$, chamado de *ideal* de X, e denotado por $\mathcal{I}(X)$. Mais explicitamente, $\mathcal{I}(X) = \{F \in K[X_1, \ldots, X_n] : F(a_1, \ldots, a_n) = 0 \text{ para todo } (a_1, \ldots, a_n) \in X\}$.

O resultado a seguir lista as propriedades satisfeitas por tais ideais.

Proposição 6.15. (i) *Se* $X \subset Y$, *então* $\mathcal{I}(X) \supset \mathcal{I}(Y)$.

(ii) $\mathcal{I}(\emptyset) = K[X_1, \ldots, X_n]$ *e* $\mathcal{I}(\mathbb{A}^n(K)) = (0)$ *se* K *é um corpo infinito.* $\mathcal{I}(\{a_1, \ldots, a_n\}) = (X_1 - a_1, \ldots, X_n - a_n)$ *para* $a_i \in K$.

(iii) $\mathcal{I}(\mathcal{V}(S)) \supset S$ *para qualquer conjunto de polinômios* S. $\mathcal{V}(\mathcal{I}(X)) \supset X$ *para qualquer conjunto de pontos* X.

(iv) $\mathcal{V}(\mathcal{I}(\mathcal{V}(S))) = \mathcal{V}(S)$ *para qualquer conjunto de polinômios* S, *e* $\mathcal{I}(\mathcal{V}(\mathcal{I}(X))) = \mathcal{I}(X)$ *para qualquer conjunto de pontos* X. *Então se* V *é um conjunto algébrico,* $V = \mathcal{V}(\mathcal{I}(V))$; *e se* I *é o ideal de um conjunto algébrico,* $I = \mathcal{I}(\mathcal{V}(I))$.

(v) $\mathcal{I}(X)$ *é um ideal radical para todo conjunto* $X \subset \mathbb{A}^n(K)$.

Demonstração: (i) Tomando $F \in \mathcal{I}(Y)$, temos $F(P) = 0$ para todo $P \in Y$. Em particular, como $X \subset Y$, $F(P) = 0$ vale para todo $P \in X$. Portanto, $F \in \mathcal{I}(X)$, e $\mathcal{I}(y) \subset \mathcal{I}(X)$.

(ii) Claramente, não existe $P \in \mathbb{A}^n$ que anule todos os polinômios em $K[X_1, \ldots, X_n]$, e o único polinômio que se anula em todo ponto P é o polinômio nulo.

Se $F \in (X_1 - a_1, \ldots, X_n - a_n)$, então $F \in \mathcal{I}(\{a_1, \ldots, a_n\})$, pois $F(P) = 0$. Por outro lado, se $F \in \mathcal{I}(\{a_1, \ldots, a_n\})$, então $F(a_1, \ldots, a_n) = 0$.

Logo, $F = \sum_{i=1}^{n}(X_i - a_i)G_i$ e $F \in (X_1 - a_1, \ldots, X_n - a_n)$.

(iii) Se $F \in S$, então $F(P) = 0$ para todo $P \in \mathcal{V}(S)$, pela definição de $\mathcal{V}(S)$. Logo, $F \in \mathcal{I}(\mathcal{V}(S))$. Analogamente, se $P \in X$, temos que $G(P) = 0$ para todo $G \in \mathcal{I}(X)$. Assim, $G \in \mathcal{V}(\mathcal{I}(X))$.

(iv) As duas igualdades seguem diretamente dos itens (i) e (iii).

(v) Lembremos que $\mathrm{Rad}(\mathcal{I}(X)) = \{F \in K[X_1, \ldots, X_n] : F^n \in \mathcal{I}(X) \text{ para algum } n\}$. Tomando $F \in \mathrm{Rad}(\mathcal{I}(X))$, temos que $F^n \in \mathcal{I}(X)$ para algum n; isto é, $F^n(P) = 0$ para todo $P \in X$. Assim, $0 = F^n(P) = F(P) \cdot \ldots \cdot F(P)$, e $F(P) = 0$. Portanto $F \in \mathcal{I}(X)$. A inclusão $\mathrm{Rad}(\mathcal{I}(X)) \subset \mathcal{I}(X)$ decorre do item (f) da Proposição 1.45. ■

Em relação ao ideais explicitados nos itens (ii) e (v) acima, temos, respectivamente, as duas seguintes proposições.

Proposição 6.16. *O ideal $I = (X_1 - a_1, \ldots, X_n - a_n) \subset K[X_1, \ldots, X_n]$ é maximal, e K é isomorfo a $K[X_1, \ldots, X_n]/I$.*

Demonstração: Seja $J \subset K[X_1, \ldots, X_n]$ um ideal tal que $I \subseteq J \subseteq K[X_1, \ldots, X_n]$. Então, pelos itens (i) e (v) da Proposição 6.11, temos $\{(a_1, \ldots, a_n)\} = \mathcal{V}(I) \supset \mathcal{V}(J)$. Dessa forma, $\mathcal{V}(J) = \emptyset$ ou $\mathcal{V}(J) = \{(a_1, \ldots, a_n)\}$. A primeira possibilidade nos dá $J = K[X_1, \ldots, X_n]$; e a segunda,$J = I$. Portanto, J é maximal.

Conside o homomorfismo natural

$$\phi : K \to \frac{K[X_1, \ldots, X_n]}{I}$$

$$a \longmapsto \overline{a} = a + I$$

Tal homomorfismo é sobrejetor por construção. Verifiquemos que é injetor. Temos que $\ker\phi = \{a \in K : a \in I\}$, mas $a \in (X_1 - a_1, \ldots, X_n - a_n)$ se, e somente se, $a = 0$. Logo $\ker\phi = \{0\}$. ■

Lema 6.17. *Sejam V, W conjuntos algébricos em $\mathbb{A}^n(K)$. Então $V = W$ se, e somente se, $\mathcal{I}(V) = \mathcal{I}(W)$.*

Demonstração: Como $V = W$, temos que $\mathcal{I}(V) \subset \mathcal{I}(W)$ e $\mathcal{I}(W) \subset \mathcal{I}(V)$. Por outro lado, como V e W são algébricos, o item (iv) da Proposição 6.15 garante que

$$\mathcal{V}(\mathcal{I}(V)) = V$$

e

$$\mathcal{V}(\mathcal{I}(W)) = W.$$

Por hipótese, $\mathcal{I}(V) = \mathcal{I}(W)$, e então $\mathcal{V}(\mathcal{I}(V)) = \mathcal{V}(\mathcal{I}(W))$. Logo $V = W$. ■

Proposição 6.18. *Se I é um ideal em $K[X_1, \ldots, X_n]$, então $\mathcal{V}(I) = \mathcal{V}(\mathrm{Rad}(I))$ e $\mathrm{Rad}(I) \subset \mathcal{I}(\mathcal{V}(I))$.*

Demonstração: Como $I \subset \mathrm{Rad}(I)$, então $\mathcal{V}(\mathrm{Rad}(I)) \subset \mathcal{V}(I)$. Tomando $P \in \mathcal{V}(I)$, temos que $F(P) = 0$ para todo $F \in I$. Em particular, se $G \in \mathrm{Rad}(I)$, temos que $G^m \in I$ para algum m, e assim, $G^m(P) = 0$. Logo $G(P) = 0$ e $P \in \mathcal{V}(\mathrm{Rad}(I))$. Por fim, como $\mathrm{Rad}(I) \subset \mathcal{I}(\mathcal{V}(\mathrm{Rad}(I)))$, temos que $\mathrm{Rad}(I) \subset \mathcal{I}(\mathcal{V}(I))$. ■

Ao definirmos conjuntos algébricos, não fizemos restrições em relação ao número de polinômios que os determinam. Entretanto, o teorema a seguir afirma que um conjunto algébrico pode ser definido a partir de um número finito de polinômios.

Teorema 6.19. *Todo conjunto algébrico é a intersecção de um número finito de hipersuperfícies.*

Demonstração: Consideremos o conjunto algébrico $\mathcal{V}(I)$ para algum ideal $I \subset K[X_1, \ldots, X_n]$. Como todo corpo é Noetheriano, pelo Teorema da Base de Hilbert (Corolário 5.7), temos que $K[X_1, \ldots, X_n]$ é Noetheriano; e portanto, I é finitamente gerado. Assim, se $I = (F_1, \ldots, F_r)$, então $\mathcal{V}(I) = \mathcal{V}(F_1) \cap \ldots \cap \mathcal{V}(F_r)$. De fato, se $P \in \mathcal{V}(F_1) \cap \ldots \cap \mathcal{V}(F_r)$, então $F_i(P) = 0$ para $i = 1, \ldots r$. Como qualquer $G \in I$ é da forma $\sum_{i=1}^{r} a_i F_i$, temos que $G(P) = \sum_{i=1}^{r} a_i F_i(P) = 0$. Logo $P \in \mathcal{V}(I)$. Reciprocamente, como $F_i \subset I$, temos que $\mathcal{V}(I) \subset \mathcal{V}(F_i)$ para para $i = 1, \ldots, r$, e assim $\mathcal{V}(I) \subset \cap \mathcal{V}(F_i)$. ■

Para finalizar esta seção, o resultado abaixo garante a existência de polinômios com certas características.

Proposição 6.20. (i) *Seja V um conjunto algébrico em $\mathbb{A}^n(K)$, e $P \in \mathbb{A}^n(K)$ tal que $P \notin V$. Então existe um polinômio $F \in K[X_1, \ldots, X_n]$ tal que $F(Q) = 0$ para todo $Q \in V$, mas $F(P) = 1$.*

(ii) *Seja $\{P_1, \ldots, P_r\}$ um conjunto finito de pontos em $\mathbb{A}^n(K)$. Então existem polinômios $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$ tais que $F_i(P_j) = 0$ se $i \neq j$, e $F_i(P_i) = 1$.*

(iii) *Seja V um conjunto algébrico em $\mathbb{A}^n(K)$, $P_1, P_2 \notin V$. Então existe um polinômio $F \in K[X_1, \ldots, X_n]$ tal que $F(P_i) \neq 0$, $i = 1, 2$, mas $F \in \mathcal{I}(V)$.*

Demonstração: (i) Temos que $V \cup \{P\}$ é um conjunto algébrico, pois é a união de conjuntos algébricos. Assim, pelo Lema 6.17, temos $\mathcal{I}(V) \neq \mathcal{I}(V \cup \{P\})$. Tomemos $G \in \mathcal{I}(V)$, tal que $G \notin \mathcal{I}(V \cup \{P\})$. Assim $G(Q) = 0$ para todo $Q \in V$, e $G(P) \neq 0$ pois, caso contrário, teríamos $G \in \mathcal{I}(V \cup \{P\})$. Agora basta tomar $F = (G(P))^{-1} \cdot G$: é claro que $F \in K[X_1, \ldots, X_n]$ e $F(P) = 1$.

(ii) Provemos por indução sobre r. Se $r = 1$, é o item anterior. Para $\{P_1, P_2\}$, temos que $\mathcal{I}(\{P_2\}) \neq \mathcal{I}(\{P_1\} \cup \{P_2\})$. Assim, por argumento análogos aos do item (i), existe $G \in \mathcal{I}(\{P_1\})$ tal que $G(P_1) = 0$ e $G_1(P_2) \neq 0$. Basta fazer $F_2 = G(P_2)^{-1}G$.

Também temos $\mathcal{I}(\{P_2\}) \neq \mathcal{I}(\{P_1\} \cup \{P_2\})$, e assim existe $H \in \mathcal{I}(\{P_2\})$ com $H(P_2) = 0$ e $H(P_2) \neq 0$. Novamente, fazemos $F_1 = H(P_1)^{-1}H$. Considerando a existência de $r - 1$ polinômios que satisfazem a condição para os pontos $P_1, \ldots, P_{r-1}$, os mesmos argumentos para $\mathcal{I}(\{P_1, \ldots, P_{r-1}\} \cup \{P_r\})$ concluem a indução.

(iii) Pelo item (ii), existem polinômios $F_1, F_2 \in K[X_1, \ldots, X_n]$ tais que $F_1(P_1) \neq 0$ e $F_2(P_2) \neq 0$. Lembrando que $F_1, F_2 \in \mathcal{I}(V)$, analisemos as três possibilidades:

- Se $F_1(P_2) \neq 0$, então tomemos $F = F_1$.
- Caso $F_2(P_1) \neq 0$, tomemos $F = F_2$.
- Por fim, se $F_1(P_2) = 0$ e $F_2(p_1) = 0$, tomemos $F = F_1 + F_2$.

Em qualquer um dos casos, $F \in \mathcal{I}(V)$ e $F(P_i) \neq 0$, $i = 1, 2$. ■

6.5 Componentes Irredutíveis de um Conjunto Algébrico

Um conjunto algébrico pode ser a união de vários conjuntos algébricos menores, como por exemplo, $\mathcal{V}(Y^2 - 2XY - X^2Y + X^3) = \mathcal{V}((Y - X^2) \cdot (Y - X)) = \mathcal{V}(Y - X^2) \cup \mathcal{V}(Y - X)$. De maneira geral, temos:

Definição 6.21. *Um conjunto algébrico $V \subset \mathbb{A}^n$ é* redutível *se $V = V_1 \cup V_2$, onde V_1, V_2 são conjuntos algébricos em $\mathbb{A}^n$, e $V_i \neq V$, $i = 1, 2$. Caso contrário, V é* irredutível.

Exemplo 6.22. *O conjunto* $\mathcal{V}(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) \subset \mathbb{A}^2(\mathbb{C})$ *é redutível, e* $\mathcal{V}(Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3) = \mathcal{V}(Y^2 - X, Y^2 + X) + \mathcal{V}(Y^2 + X, Y^2 - X^2)$.

O resultado a seguir relaciona conjuntos algébricos irredutíveis e ideais primos, o que facilita a caracaterização de tais conjuntos.

Proposição 6.23. *Um conjunto algébrico* V *é irredutível se, e somente se,* $\mathcal{I}(V)$ *é primo.*

Demonstração: Se $\mathcal{I}(V)$ não é primo, suponha $F_1 \cdot F_2 \in \mathcal{I}(V)$, $F_i \notin \mathcal{I}(V)$. Então $\mathcal{V}(F_1 \cdot F_2) \supset \mathcal{V}(\mathcal{I}(V)) = V$, e

$$V = V \cap \mathcal{V}(F_1 \cdot F_2) = V \cap (\mathcal{V}(F_1) \cup \mathcal{V}(F_2)) = (V \cap \mathcal{V}(F_1)) \cup (V \cap \mathcal{V}(F_2)).$$

Notemos que $V \cap \mathcal{V}(F_i) \subsetneq V$ pois, caso contrário, teríamos $V \subset \mathcal{V}(F_i)$ e $\mathcal{I}(V) \supset \mathcal{I}(V(F_i)) \supset F_i$. Logo V é redutível.

Reciprocamente, se $V = V_1 \cup V_2$, $V_i \subsetneq V$, então $\mathcal{I}(V_i) \supsetneq \mathcal{I}(V)$. Seja $F_i \in \mathcal{I}(V_i)$, $F_i \notin \mathcal{I}(V)$. Como $\mathcal{I}(V) = \mathcal{I}(V_1 \cup V_2)$, temos que para todo $P \in V$, $P \in V_1$ ou $P \in V_2$. Assim $F_1 \cdot F_2(P) = F_1(P) \cdot F_2(P) = 0$, e $F_1 \cdot F_2 \in \mathcal{I}(V)$. Portanto, $\mathcal{I}(V)$ não é primo. ■

Como aplicação do teorema acima, temos a seguinte corolário.

Corolário 6.24. *Se* K *é infinito, então* $\mathbb{A}^n(K)$ *é irredutível.*

Demonstração: Basta mostrar que $\mathcal{I}(\mathbb{A}^n(K))$ é primo. Como K é infinito, temos que $\mathcal{I}(\mathcal{A}^n(K)) = (0)$ (Proposição 6.15, item (ii)). Sendo $K[X_1, \ldots, X_n]$ um domínio, o item (iv) da Proposição 1.30 nos garante que (0) é um ideal primo. Portanto, $\mathbb{A}^n(K)$ é irredutível. ■

Mostraremos que um conjunto algébrico é a união de um número finito de conjuntos algébricos irredutíveis. Se V é irredutível, não há o que fazer. Se V é redutível, escrevemos $V = V_1 \cup V_2$; se V_2 é redutível, escrevemos $V_2 = V_3 \cup V_4$, e assim por diante. Nos resta mostrar que este processo termina em algum V_n.

Lema 6.25. *Seja* $\mathcal{S}$ *uma coleção qualquer não vazia de ideias em um anel Noetheriano* R. *Então* $\mathcal{S}$ *tem um elemento maximal, isto é, existe um ideal* $I \in \mathcal{S}$ *que não está contido em nenhum outro ideal de* $\mathcal{S}$.

Demonstração: Escolhemos (Axioma da Escolha) um ideal de cada subconjunto de $\mathcal{S}$. Seja I_0 o ideal escolhido para $\mathcal{S}$. Seja $\mathcal{S}_1 = \{I \in \mathcal{S} : I \supsetneq I_0\}$, e seja I_1 o ideal escolhido de $\mathcal{S}_1$. Seja $\mathcal{S}_2 = \{I \in \mathcal{S} : I \supsetneq I_1\}$, etc. É suficiente mostrar que algum $\mathcal{S}_n$ é vazio. Caso contrário, seja $I = \bigcup_{n=0}^{\infty} I_n$ um ideal de R e $F_1, \ldots, F_r$ seus geradores. Para n suficientemente grande, temos $F_i \in I_n$ para todo i. Assim $I_n = I$, e $I_{n+1} = I_n$, uma contradição. ■

Segue imediatamente deste lema que qualquer coleção de conjuntos algébricos em $\mathbb{A}^n(K)$ tem um elemento minimal. Com efeito, se $\{V_\alpha\}$ é uma tal coleção, tome um elemento maximal $\mathcal{I}(V_{a_0})$ de $\{\mathcal{I}(V_a)\}$. Como $\mathcal{I}(V_{a_0}) \supset \mathcal{I}(V_a)$, temos $V_{a_0} = \mathcal{V}(\mathcal{I}(V_{a_0})) \subset \mathcal{V}(\mathcal{I}(V_a)) = V_a$, e V_{a_0} é um elemento minimal da coleção.

A decomposição de cada conjunto algébrico em subconjuntos algébricos irredutíveis é única e finita, conforme o resultado a seguir.

Teorema 6.26. *Seja V um conjunto algébrico em $\mathbb{A}^n(K)$. Então existem únicos conjuntos algébricos irredutíveis $V_1, \ldots, V_m$ tais que $V = V_1 \cup \ldots \cup V_m$ e $V_i \subsetneq V_j$ para todo $i \neq j$.*

Demonstração: Seja $\mathcal{S} = \{\text{conjuntos algébricos } V \subset \mathbb{A}^n(K) : V \text{ não é a união de conjuntos algébricos irredutíveis}\}$. Queremos mostrar que $\mathcal{S}$ é vazio. Suponhamos o contrário e tomemos V um elemento minimal de $\mathcal{S}$. Uma vez que $V \in \mathcal{S}$, V não é irredutível, e assim $V = V_1 \cup V_2$, $V_i \subsetneq V$. Como $V_i \subsetneq V$ e V é elemento minimal de $\mathcal{S}$, temos $V_i \notin \mathcal{S}$. Então V_i é redutível, isto é, $V_i = V_{i1} \cup \ldots \cup V_{im}$, com V_{ij} irredutível para todo j. Dessa forma, concluímos que $V = \bigcup_{i,j} V_{ij}$, uma contradição. Portanto, qualquer conjunto algébrico V pode ser escrito como $V = V_1 \cup \ldots \cup V_m$, V_i irredutível.

Para obter a segunda condição, simplesmente descartamos qualquer V_i tal que $V_i \subset V_j$ para $i \neq j$. Para mostrar a unicidade, seja $V = W_1 \cup \ldots \cup W_m$ outra decomposição. Então

$$V_i = V \cap V_i = \left(\bigcup_{j=1}^{m} W_j \right) \cap V_i = \bigcup_j (W_j \cap V_i) .$$

Logo $V_i \subset W_{j(i)}$ para algum $j(i)$. Analogamente, $W_{j(i)} \subset V_k$ para algum k. Mas $V_i \subset V_k$ implica $i = k$, e assim $V_i = W_{j(i)}$. Da mesma forma, cada W_i é igual a algum $V_{i(j)}$. ■

Os conjuntos V_i são chamados *componentes irredutíveis* de V; $V = V_1 \cup \ldots \cup V_m$ é a *decomposição* de V em componentes irredutíveis.

Proposição 6.27. *Seja F um polinômio não-constante em $K[X_1, \ldots, X_n]$, K, algebricamente fechado. Então $\mathbb{A}^n - \mathcal{V}(F)$ é infinito se $n \geq 1$, e $\mathcal{V}(F)$ é infinito se $n \geq 2$.*

Demonstração: Sabemos que todo corpo algebricamente fechado é infinito. Agora, suponhamos $\mathcal{A}^n - \mathcal{V}(F) = \{a_1, \ldots, a_t\}$. Então, $\mathbb{A}^n = \mathcal{V}(F) \cup \{a_1, \ldots, a_t\}$, uma reunião de conjuntos algébricos, e logo, $\mathbb{A}^n$ é algébrico e redutível. Entretanto, $\mathbb{A}^n(K)$ é irredutível quando K é infinito, pela Proposição 6.24. Portanto, $\mathcal{A}^n(K) - \mathcal{V}(F)$ é infinito.

A prova da segunda afirmação é feita por indução sobre n, $n \geq 2$. Para $n = 2$, temos que $F \in K[X, Y]$ pode ser escrita como $F = \sum_{i=0}^{m} F_i Y^i$, para $F_i \in K[X]$, com algum F_i não nulo. Como $\mathbb{A}^n - \mathcal{V}(F_i)$ é infinito para $n \geq 1$, então existem infinitos pontos $P \in \mathbb{A}^1$ tais que $F_i(P) \neq 0$. Daí,

$$F(P, Y) = \sum_{i=0}^{m} F_i(P) Y^i = F_0(P) + F_1(P)Y + \ldots + F_m(P)Y^m$$

e como K, é algebricamente fechado, existe $Q \in K$, tal que $F(P, Q) = 0$. Com existe infinitas possibilidades para P, então existem infinitos pares $P, Q \in K$, e $\mathcal{V}(F)$ é infinito para $n = 2$.

Suponha que $\mathcal{V}(F)$ seja infinito para todo inteiro $2 \leq t \leq n$. Vejamos para $n + 1$. Analogamente, escrevemos $F \in K[X_1, \ldots, X_{n+1}]$ como $F = \sum_{i=0}^{m} F_i X_{n+1}^i$, com $F_i \in K[X_1, \ldots, X_{n+1}]$, e algum F_i não nulo. Pela hipótese de indução, existem infinitos pontos $P = (P_1, \ldots, P_n) \in \mathbb{A}^n$ tais que $F_i(P) \neq 0$. Fazendo $F(P, X_{n+1}) = \sum_{i=0}^{m} F_i(P) X_{n+1}^i$, obtemos um ponto P_{n+1} tal que $F(P, P_{n+1}) = 0$. Logo, existem infinitos pontos $P = (P_1, \ldots, P_n, P_{n+1})$ em $\mathcal{V}(F)$. ■

6.6 Subconjuntos Algébricos do Plano

Nesta seção nos dedicamos ao estudo do plano afim $\mathbb{A}^2(K)$, com o objetivo de determinar seus subconjuntos algébricos. Para tal, segundo o Teorema 6.26, é suficiente deteminarmos os conjuntos algébricos irredutíveis.

Proposição 6.28. *Sejam F e G polinômios em $K[X, Y]$ sem fatores em comum. Então $\mathcal{V}(F, G) = \mathcal{V}(F) \cap \mathcal{V}(G)$ é um conjunto finito de pontos.*

Demonstração: Se F e G não tem nenhum fator comum em $K[X][Y]$, também não têm nenhum fator comun em $K(X)[Y]$ (Lema 3.25). Uma vez que $K(X)[Y]$

é um domínio principal, $(F,G) = (1)$ em $K(X)[Y]$, e assim $RF + SG = 1$ para algum $R, S \in K(X)[Y]$. Daí, existe $D \in K[X]$ não nulo, tal que $DR = A, DS = B \in K[X,Y]$ e, portanto, $AF + BG = D$.

Tomando $(a,b) \in \mathcal{V}(F,G)$, temos $D(a) = A(a)F(a) + B(a)G(a) = 0$. Mas D tem apenas um número finito de zeros, já que $D \in K[X]$. Isto mostra que somente um número finito de X-coordenadas aparecem entre os pontos de $\mathcal{V}(F,G)$. O mesmo raiocínio se aplica às Y-coordenadas. Portanto, existe apenas um número finito de pontos $(a,b) \in \mathcal{V}(F,G)$. ■

Corolário 6.29. *Se F é um polinômio irredutível em $K[X,Y]$ tal que $\mathcal{V}(F)$ é infinito, então $\mathcal{I}(\mathcal{V}(F)) = (F)$ e $\mathcal{V}(F)$ é irredutível.*

Demonstração: É claro que $(F) \subset \mathcal{I}(\mathcal{V}(F))$. Agora, se $G \in \mathcal{I}(\mathcal{V}(F))$, então $\mathcal{V}(F,G)$ é infinito. De fato, como $(G) \subset \mathcal{I}(\mathcal{V}(F))$, então $\mathcal{V}(G) \supset \mathcal{V}(\mathcal{I}(\mathcal{V}(F))) = \mathcal{V}(F)$. Assim, $\mathcal{V}(F,G) = \mathcal{V}(F) \cap \mathcal{V}(G) = \mathcal{V}(F)$, que é infinito. Com isso, a Proposiçao 6.28 garante que F divide G, isto é, $G \in (F)$. Portanto $\mathcal{I}(\mathcal{V}(F)) \subset (F)$. Por fim, como F é irredutível, então $(F) = \mathcal{I}(\mathcal{V}(F))$ é primo (Proposição 3.16-(ii)) e, pela Proposição 6.23, $\mathcal{V}(F)$ é irredutível. ■

Corolário 6.30. *Suponha K infinito. Então os subconjuntos algébricos irredutíveis de $\mathbb{A}^2(K)$ são: $\mathbb{A}^2(K)$, $\emptyset$, pontos, e as curvas planas irredutíveis $\mathcal{V}(F)$, onde F é um polinômio irredutível e $\mathcal{V}(F)$ é infinito.*

Demonstração: Seja V um conjunto algébrico irredutível em $\mathbb{A}^2(K)$. Se V é finito, então $V = \emptyset$ ou $V = \{P\}$ pois, se $V = \{P_1, P_2\}$, $V = \mathcal{V}(P_1) \cup \mathcal{V}(P_2)$, isto é, V seria redutível. Se $\mathcal{I}(V) = (0)$, então $V = \mathbb{A}^2(K)$, pela Proposição 6.28.

Caso contrário, $\mathcal{I}(V)$ contém um polinômio não contante F. Uma vez que $\mathcal{I}(V)$ é primo, pois V é irredutível. Se $F = F_1^{r_1} \cdot \ldots \cdot F_s^{r_s}$ é a decomposição de F em fatores irredutíveis, então algum $F_i \in \mathcal{I}(V)$, pois $\mathcal{I}(V)$ é primo. Assim, podemos supor F irredutível. Dessa forma, $\mathcal{I}(V) = (F)$. De fato, $(F) \subset \mathcal{I}(V)$ e, se $G \in \mathcal{I}(V)$, $G \notin (F)$, então

$$G \in \mathcal{I}(V) \Rightarrow (G) \subset \mathcal{I}(V) \Rightarrow \mathcal{V}(G) \supset \mathcal{V}(\mathcal{I}(V)) = V$$

e

$$F \in \mathcal{I}(V) \Rightarrow (F) \subset \mathcal{I}(V) \Rightarrow \mathcal{V}(F) \supset \mathcal{V}(\mathcal{I}(V)) = V.$$

Logo $V \subset \mathcal{V}(F) \cap \mathcal{V}(G) = \mathcal{V}(F,G)$, e $\mathcal{V}(F,G)$ é finito, pois F e G não tem fatores em comum (Proposição 6.28). ■

Corolário 6.31. *Assuma que K é algebricamente fechado, F um polinômio não constante em $K[X,Y]$. Seja $F = F_1^{n_1} \ldots F_r^{n_r}$ a decomposição de F em fatores*

irredutíveis. Então $\mathcal{V}(F) = \mathcal{V}(F_1) \cup \ldots \cup \mathcal{V}(F_r)$ *é a decomposição de* $\mathcal{V}(F)$ *em componentes irredutíveis, e* $\mathcal{I}(\mathcal{V}(F)) = (F_1 \cdot \ldots \cdot F_r)$.

Demonstração: Primeiramente, mostremos que cada $\mathcal{V}(F_i)$ é irredutível. Como $\mathcal{V}(F_i)$ é infinito, pela Proposição6.27, temos que $\mathcal{I}(\mathcal{V}(F_i)) = (F_i)$, onde F_i é irredutível. Logo, pelo Corolário 6.29, $\mathcal{V}(F_i)$ é irredutível.

Além disso, não há relações de inclusão entre os conjuntos $\mathcal{V}(F_i)$. De fato, supondo que $\mathcal{V}(F_i) \subset \mathcal{V}(F_j)$, teríamos $(F_i) = \mathcal{I}(\mathcal{V}(F_i)) \supset \mathcal{I}(\mathcal{V}(F_j)) = (F_j)$; mas nenhum F_i divide F_j, para todo j.

Por fim, temos que $\mathcal{I}(\cup_i \mathcal{V}(F_i)) = \cap_i \mathcal{I}(\mathcal{V}(F_i)) = \cap_i (F_i)$. Como todo polinômio divisível por cada F_i é também divisível por $F_1 \ldots F_r$, então $\cap_i (F_i) = (F_1 \ldots F_r)$. Portanto, $\mathcal{I}(\mathcal{V}(F)) = (F_1 \cdot \ldots \cdot F_r)$. ■

6.7 Elementos Inteiros

Recordemos que um módulo é finitamente gerado quando todo elemento se espressa como combinação linear de um número finito de geradores. Considerando R um subanel de um anel S, podemos ter S um R-módulo, um anel, ou um corpo. Nesta situação, temos:

- S é *módulo finito* sobre R se é finitamente gerado como um R-módulo.
- Sejam $v_1, \ldots, v_n \in S$, $\varphi : R[X_1, \ldots, X_n] \to S$ o homomorfismo de anéis que leva X_i em v_i. A imagem de φ é denotada por $R[v_1, \ldots, v_n]$, e é (o menor) subanel de S contendo R e $v_1, \ldots, v_n$. Assim $R[v_1, \ldots, v_n] = \left\{\sum a_{(i)} v_1^{i_1} \ldots v_n^{i_n} : a_{(i)} \in R\right\}$. S é *anel finito* sobre R se $S = R[v_1, \ldots, v_n]$ para certos $v_i \in S$.
- Suponha $R = K, S = L$ corpos. Se $v_1, \ldots, v_n \in L$, $K(v_1, \ldots, v_n)$ é o corpo de frações de $K[v_1, \ldots, v_n]$, e é um subcorpo de L. Na verdade, é o menor subcorpo de L contendo K e $v_1, \ldots, v_n$. Dizemos que L é uma *extensão finitamente gerada* de K se $L = K(v_1, \ldots, v_n)$ para certos $v_1, \ldots, v_n \in L$.

Proposição 6.32. $L = K(X)$ *é extensão finitamente gerada de* K*, mas* L *não é anel finito sobre* K.

Demonstração: Como $K[X]$ é anel finito sobre K, então $K(X)$ é extensão finitamente gerada de K. Agora, suponhamos $L = K(X)$ anel finito sobre K. Então todo $z \in L$ se escreve como $\sum a_{(i)} v_1^{i_1} \ldots v_n^{i_n}$, para certos $v_1, \ldots, v_n \in L = K(X)$ e $a_{(i)} \in K$. Dessa forma, existiria um elemento $b \in K[X]$ tal que para todo $z \in L$,

$b^n z \in K[X]$ para certo n. Entretanto, pela Proposição 6.7, existe um número infinito de polinômios irredutíveis em $K[X]$. Assim, podemos tomar $z = 1/c$, com $c \nmid b$. ■

Proposição 6.33. *Seja R subanel de S, S subanel de T.*

(i) *Se $S = \sum Av_i$ e $T = \sum Bw_j$, então $T = \sum Av_i w_j$.*

(ii) *Se $S = R[v_1, \ldots, v_n]$ e $T = S[w_1, \ldots, w_m]$, então $T = R[v_1, \ldots, v_n, w_1, \ldots, w_m]$.*

(iii) *Se R, S, T são corpos, e $S = A(v_1, \ldots, v_n)$, $T = B(w_1, \ldots, w_m)$, então $T = A(v_1, \ldots, v_n, w_1, \ldots, w_m)$.*

Demonstração:(i) É óbvia.

(ii) Pela hipótese, existem homomorfismos $\varphi : R[X_1, \ldots, X_n] \to S$ tal que $X_i \overset{\varphi}{\mapsto} v_i$, e $\psi : S[X_1, \ldots, X_m] \to T$, tal que $X_j \overset{\psi}{\mapsto} w_j$. Além disso, $S = \{\sum a_{(i)} v_1^{i_1} \cdots v_n^{i_n} : a_{(i)} \in R\}$, e $T = \{\sum b_{(j)} w_1^{j_1} \cdots w_m^{j_m} : b_{(j)} \in S\}$.

Basta considerar o homomorfismo $\Phi : R[X_1, \ldots, X_{m+n}] \to T$, tal que $X_i \overset{\varphi}{\mapsto} v_i$ para $i = 1, \ldots, n$, e $X_j \overset{\psi}{\mapsto} w_j$, para $j = n+1, \ldots, m$. É claro que $T = \left\{\sum c_{(k)} v_1^{i_1} \cdots v_n^{i_n} w_1^{j_1} \cdots w_m^{j_m} : c_{(k)} \in R\right\}$.

(iii) Análogo ao anterior, apenas considerando os elementos nos respectivos corpos de frações. ■

O resultado acima mostra que as "relações" módulo finito, anel finito e extensão finitamente gerada, são transitivas.

Definição 6.34 (Elemento Inteiro)**.** *Seja R um subanel de um anel S. Dizemos que um elemento $v \in S$ é inteiro sobre R se existe um polinômio mônico $F = X^n + a_1 X^{n-1} + \ldots + a_n \in R[X]$ tal que $F(v) = 0$. Se R e S são corpos, dizemos que v é algébrico sobre R se v é inteiro sobre R.*

Proposição 6.35. *Seja R um subanel de um domínio S, $v \in S$. Então as seguintes afirmações são equivalentes:*

(i) *v é inteiro sobre R.*

(ii) *$R[v]$ é módulo-finito sobre R.*

(iii) *Existe um subanel R' de R contendo $R[v]$ que é módulo-finito sobre R.*

Demonstração: (i) $\Rightarrow$ (ii): Se $v^n + a_1 v^{n-1} + \ldots + a_n = 0$, então $v^n \in \sum_{i=0}^{n-1} Rv^i$. É claro que $\sum_{i=0}^{n-1} Rv^i \subset R[v]$. Note que, se provarmos que $v^m \in \sum_{i=0}^{n-1} Rv^i$ para

todo m, teremos que $R[v] = \sum_{i=0}^{n-1} Rv^i$, pois todo elemento $z \in R[v]$ é da forma $\sum b_j v^j$, $b_j \in R$.

Mostremos que $v^m \in \sum_{i=0}^{n-1} Rv^i$ para todo m. Para $0 \leq m \leq n$, temos que $v^m \in \sum_{i=0}^{n} Bv^i$. Se $m = n+1$, temos

$$\begin{aligned} v^{n+1} &= v^n v = (a_1 v^{n-1} + \ldots + a_n)v \\ &= a_1 v^n + \ldots + a_n v \\ &= a_1(a_1 v^{n-1} + \ldots + a_0) + \ldots + a_n v \end{aligned}$$

que é uma combinação linear de v^i, $i = 0, \ldots, n-1$. Usando este mesmo raciocínio, obtemos que $v^m \in \sum_{i=0}^{n-1} Rv^i$ para todo m.

(ii) $\Rightarrow$ (iii): Basta tomar $R' = R[v]$.

(iii) $\Rightarrow$ (i): Se $R' = \sum_{i=1}^{n} Rw_i$, então $vw_i = \sum_{j=1}^{n} a_{ij} w_j$ para algum $a_{ij} \in R$. Então $\sum_{j=1}^{n} (\delta_{ij} v - a_{ij}) w_j = 0$ para todo i, onde $\delta_{ij} = 0$ se $i \neq j$, e $\delta_{ii} = 1$. Se considerarmos estas equações no corpo de frações de S, veremos que $(w_1, \ldots, w_n)$ é uma solução não trivial, e assim $\det(\delta_{ij} v - a_{ij}) = 0$. Uma vez que v aparece somente na diagonal da matriz, o determinante tem a forma $v^n + a_1 v^{n-1} + \ldots + a_n$, $a_i \in B$. Assim v é inteiro sobre R. ■

Corolário 6.36. *Se R é subanel de S e S é módulo finito sobre R, então S é inteiro sobre R.*

Demonstração: Para todo $v \in S$, seja $S = R'$ em (iii). Então v é inteiro sobre R pelo item (i). ■

Corolário 6.37. *O conjunto de elementos de S que são inteiros sobre R é um subanel de S que contém R.*

Demonstração: Tomemos a, b inteiros sobre S. Como $B \subset S[a]$, então b é, em particular, inteiro sobre $S[a]$. Além disso, sendo $S[a] \subset S[a, b]$, pela Proposição 6.33 - (i), temos $S[a, b]$ é módulo-finito sobre S. Como $a \pm b, ab \in R[a, b]$, pela proposição anterior, são inteiros sobre R. ■

Dizemos que S é inteiro sobre R se todo elemento de A é inteiro sobre R. Se R e S são corpos, dizemos que S é uma *extensão algébrica* de R se S é inteiro sobre R.

Proposição 6.38. *Seja L um corpo, K subcorpo algebricamente fechado de L.*

(i) *Qualquer elemento de L que é algébrico sobre K está em K.*

(ii) *Um corpo algebricamente fechado não possui extensão módulo finita, exceto si próprio.*

Demonstração: (i) Se $z \in L$ é algébrico sobre K, então z é raiz de algum polinômio mônico de grau n, com coeficientes em K. Entretanto, como K é algebricamente fechado, todas as n raízes de um polinômio de grau n em K estão em K. Logo, $z \in K$.

(ii) Seja $L^{'}$ uma extensão módulo finita sobre K. Obviamente, $K \subset L^{'}$. Agora, como todo elemento de $L^{'}$ é algébrico sobre K, pela Proposição 6.35, temos $L^{'} \subset K$. Portanto, $L^{'} = K$. ■

Proposição 6.39. *Seja K um corpo, $L = K(X)$ o corpo das funções racionais de uma variável sobre K.*

(i) *Qualquer elemento de L que é inteiro sobre $K[X]$ está em $K[X]$.*

(ii) *Não existe elemento não nulo $F \in K[X]$ tal que para todo $z \in L$, $F^n z$ é inteiro sobre $K[X]$ para algum $n > 0$.*

Demonstração: (i) Tomemos $z \in K(X)$ inteiro sobre $K[X]$, isto é, z satisfaz $z^n + a_{n-1}z^{n-1} + \ldots, +a_0 = 0$, para $a_i \in K[X]$. Como $z \in K(X)$, existem $F, G \in K[X]$ primos entre si, tais que $z = F/G$. Substituindo na expressão anterior e multiplicando por G^n temos

$$F^n + a_{n-1}F^{n-1}G + \ldots + a_0G^n = 0 \Rightarrow G \mid F^n.$$

Como G e F são produtos de fatores irredutíveis, e em $K[X]$, todo elemento irredutível é primo, concluímos que $G \mid F$. Assim, $z \in K[X]$.

(ii) Suponha que existe tal $F \in K[X]$. Então

$$(F^n z)^m + a_{m-1}(F^n z)^{m-1} + \ldots + a_0 = 0$$

para certos $a_i \in K[X]$. Em particular, tomemos $z = 1/G$, onde G é um polinômio irredutível que não divide F. Substituindo na expressão anterior e multiplicando por G^m, temos

$$F^n + a_{m-1}F^nG + \ldots + G^m a_0 = 0 \Rightarrow G \mid F^n.$$

Como G é primo, então $G \mid F$. Esta contradição garante a não existência de tal F. ■

Teorema 6.40. *Se R é um subanel de S, e $v_1, \ldots, v_n \in S$ são inteiros sobre R, então $R[v_1, \ldots, v_n]$ é módulo finito sobre R e inteiro sobre R.*

Demonstração: Temos que

$$R \subset R[v_1] \subset R[v_1, v_2] \subset \cdots \subset R[v_1, \ldots, v_n].$$

Para cada i, v_i é inteiro sobre R, e então, é inteiro sobre $R[v_1, \ldots, v_{i-1}]$. Como $R[v_1, \ldots, v_i] = R[v_1, \ldots, v_{i-1}][v_i]$, temos que $R[v_1, \ldots, v_i]$ é módulo finito sobre $R[v_1, \ldots, v_{i-1}]$, pela Proposição 6.35. Aplicações sucessivas do item (i) da Proposição 6.33, garante que $R[v_1, \ldots, v_n]$ é módulo finito sobre R. Assim, pelo Corolário 6.36, $R[v_1, \ldots, v_n]$ é inteiro sobre R. ■

Capítulo 7

Teorema dos Zeros de Hilbert

Neste capítulo apresentamos as duas versões equivalentes do *Teorema da Base de Hilbert*, também conhecido como *Nullstellensatz*. Apesar da existência de demonstrações distintas, estudamos a demonstração devida a Zariski. Além disso, para complementar a discussão sobre elementos inteiros, dedicamos uma seção ao *Lema da Normalização de Noether*.

7.1 Extensões de Corpos

Suponha K um subcorpo de um corpo L, e suponha $L = K(v)$ para algum $v \in L$. Seja $\varphi : K[X] \to L$ o homomorfismo levando X em v e $\ker(\varphi) = (F)$, $F \in K[X]$, já que $K[X]$ é um domínio principal. Pelo Teorema do Isomorfismo, $K[X]/(F)$ é isomorfo a $K[v]$, e então (F) é primo (Proposição 1.30-(i)). Temos duas possibilidades para F:

- Se $F = 0$, então $K[v]$ é isomorfo a $K[X]$, e $K(v) = L$ é isomorfo a $K(X)$. Neste caso, L não é anel finito (ou módulo finito) sobre K, de acordo com Proprosição 6.32.

- Caso $F \neq 0$, podemos assumir F mônico. Como (F) é primo, então F é irredutível e (F) é maximal (Proposição 3.16); logo $K[v]$ é um corpo e $K[v] = K(v)$. Como $0 = \varphi(F) = v^n + b_{n-1}V^{n-1} + \ldots + b_0 = F(v)$, para certos $b_i \in K$, concluímos que v é algébrico sobre K. Portanto, $L = K[v]$ é móulo finito sobre K, pela Proposição 6.35.

Para a demonstração de uma das versões do Teorema dos Zeros de Hilbert, é necessário mostrar que se L é anel finito sobre K, um corpo algebricamente fechado, então $L = K$. Entretanto, considerando a Proposição 6.38, é suficiente mostrar que L é módulo-finito sobre K. Pela discussão acima,

temos que um anel finito também é módulo finito. O lema a seguir mostra que esta afirmação é sempre verdadeira:

Lema 7.1 (Zariski). *Se um corpo L é anel finito sobre um subcorpo K, então L é módulo finito (e, portanto, algébrico) sobre K.*

Demonstração: Como L é anel finito sobre K, temos $L = K[v_1, \ldots, v_n]$ para certos $v_i \in L$. A demonstração será feita por indução sobre n. O caso $n = 1$ é tratado na discussão acima, então assumimos o resultado válido para todas as extensões geradas por $n-1$ elementos. Seja $K_1 = K(v_1)$. Por indução, $L = K_1[v_2, \ldots, v_n]$ é módulo finito sobre K_1. Se v_1 for algébrico sobre K, então $K[v_1]$ é módulo finito sobre K. Logo $K[v_1] = K(v_1)$ e, pelo item (ii) da Proposição 6.33, temos $L = K[v_1, \ldots, v_n]$.

Suponhamos então que $L = K[v_1, \ldots, v_n]$ com v_1 não algébrico sobre K. Para $i = 2, \ldots, n$, cada v_i satisfaz uma equação $v_i^{n_i} + a_{i1}v_i^{n_i-1} + \ldots + a_{in_i} = 0$, com $a_{ij} \in K_1$, pois $v_2, \ldots, v_n$ são algébricos sobre K_1 pela hipótese de indução. Se tomarmos $a \in K[v_1]$ múltiplo de todos os denominadores de a_{ij}, e multiplicarmos por a^{n_i} cada uma das equações, obteremos $(av_i)^{n_i} + aa_{i1}(av_i)^{n_i-1} + \ldots = 0$, para cada $i = 2, \ldots, n$. Assim, av_i é algébrico sobre $K[v_1]$ para $i = 2, \ldots, n$. Segue do Corolário 6.37 que para qualquer $z \in L = K[v_1, \ldots, v_n]$, existe N tal que $a^N z$ é inteiro sobre $K[v_1]$. Como v_1 não é algébrico sobre K, então $K[v_1] \subsetneq K(v_1)$ e, em particular, a afirmação vale para $z \in K(v_1) \setminus K[v_1]$. Mas como $K(v_1)$ é isomorfo a um corpo de funções racionais de uma variável sobre K, isto é absurdo, pela Proposição 6.39. Portanto, v_1 é algébrico sobre K, e $L = K[v_1, \ldots, v_n]$. ■

7.2 Lema da Normalização de Noether

Seja L uma extensão de K, e B um subconjunto de L. B é *algebricamente independente* sobre K se para algum inteiro positivo n existe um polinômio não nulo $F \in K[X_1, \ldots, X_n]$ tal que $F(b_1, \ldots, b_n) = 0$ para distintos $b_1, \ldots, b_n \in B$. Caso contrário, B é *algebricamente dependente* sobre K.

Se tal subconjunto B é maximal (com respeito a inclusão) na coleção de subconjuntos algebricamente independentes de L, dizemos que B é *base de transcendência* de L sobre K, com *grau de transcendência* $|B|$.

Lema 7.2 (Normalização de Noether). *Seja R um domínio de integridade anel finito sobre um corpo K, e seja r o grau de transcendência de K sobre L, o*

corpo de frações de R. Então existe um conjunto algebricamente independente $\{t_1, \ldots, t_r\}$ de R tal que R é inteiro sobre $K[t_1, \ldots, t_r]$.

Demonstração: Seja $R = K[u_1, \ldots, u_n]$; então $L = K(u_1, \ldots, u_n)$. Se $\{u_1, \ldots, u_n\}$ é algebricamente independente sobre K, então $\{u_1, \ldots, u_n\}$ é uma base de transcendência de L sobre K. Assim, teremos $r = n$ e o teorema é verdadeiro.

Se $\{u_1, \ldots, u_n\}$ é algebricamente dependente sobre K, então $r \leq n-1$ e

$$\sum_{(i_1,\ldots,i_n)\in\Lambda} = a_{i_1\ldots i_n} u_1^{i_1} \cdots u_n^{i_n} = 0,$$

onde Λ é um conjunto finito de n-uplas distintas de inteiros não negativos, e $a_{i_1\ldots i_n}$ é um elemento não nulo de K para cada $(i_1, \ldots, i_n) \in \Lambda$. Tomemos c um inteiro positivo maior que qualquer compontente i_s de todo elemento $(i_1, \ldots, i_n) \in \Lambda$. Se $(i_1, \ldots, i_n), (j_1, \ldots, j_n) \in \Lambda$ são tais que

$$i_1 + ci_2 + c^2 i_3 + \ldots + c^{n-1} i_n = j_1 + cj_2 + c^2 j_3 + \ldots + c^{n-1} j_n,$$

então $c \mid i_1 - j_1$, o que é impossível, a menos que $i_1 = j_1$, pois $c > i_1 \geq 0$ e $c > j_1 \geq 0$. Daí, $i_2 + ci_3 + \ldots + c^{n-2} i_n = j_2 + cj_3 + \ldots + c^{n-2} j_n$, e $c \mid i_2 - j_2 \to i_2 = j_2$. Repetindo este processo, obtemos $(i_1, \ldots, i_n) = (j_1, \ldots, j_n)$. Dessa forma, o conjunto

$$\{i_1 + ci_2 + c^2 i_3 + \ldots + c^{n-1} i_n : (i_1, \ldots, i_n) \in \Lambda\}$$

consiste de $|\Lambda|$ inteiros não negativos distintos e, em particular, admite um único elemento maximal $j_1 + cj_2 + \ldots + c^{n-1} j_n$ para algum $(j_1, \ldots, j_n) \in \Lambda$.

Agora, definimos

$$v_2 = u_2 - u_1^c,\ v_3 = u_3 - u_1^{c^2},\ \ldots, v_n = u_n - u_1^{c^{n-1}}.$$

Substituindo cada u_i por $v_i + u_1^{c^{i-1}}$, $2 \leq i \leq n$, no somatório acima e expandirmos as expressão, obtemos

$$a_{j_1\ldots j_n} u_1^{j_1 + cj_2 + c^2 j_3 + \ldots + c^{n-1} j_n} + F(u_1, v_2, \ldots, v_n) = 0,$$

onde o grau de $F \in K[X_1, \ldots, X_n]$ em X_1 é estritamente menor que $j_1 + cj_2 + \ldots + c^{n-1} j_n$. Logo u_1 é raiz do polinômio mônico

$$X^{j_1 + cj_2 + c^2 j_3 + \ldots + c^{n-1} j_n} + a_{j_1\ldots j_n}^{-1} F(X, u_2, \ldots, u_n) \in K[v_2, \ldots, v_n][X].$$

Consequentemente, u_1 é inteiro sobre $K[v_2, \ldots, v_n]$. Pelo Teorema 6.40, $K[u_1, v_2, \ldots, v_n] = K[v_2, \ldots, v_n][u_1]$ é inteiro sobre $K[v_2, \ldots, v_n]$. Como cada u_i, para $i = 2, \ldots, n$ é inteiro sobre $K[u_1, v_2, \ldots, v_n]$, temos que $R =$

$K[u_1, \ldots, u_n]$ é inteiro sobre $K[v_2, \ldots, v_n]$. Se$\{v_2, \ldots, v_n\}$ é algebricamente independente, então $r = n - 1$ e o teorema está provado. Caso contrário, o mesmo argumento para $K[v_2, \ldots, v_n]$ no lugar de K mostra que para certos $w_3, \ldots, w_n \in A$, $K[v_2, \ldots, v_n]$ é inteiro sobre $K[w_3, \ldots, w_n]$. Daí, por transitividade, R é inteiro sobre $K[w_3, \ldots, w_n]$. Se $\{w_3, \ldots, w_n\}$ é algebricamente independente, terminamos a prova. Se não for, o processo pode ser repetido até obtermos um subconjunto algebricamente independente $\{z_{n-r+1}, \ldots, z_n\}$ de r elementos de R tais que R é inteiro sobre $K[z_{r-n+1}, \ldots, z_n]$. ■

7.3 Teorema dos Zeros de Hilbert

Até o momento, vimos vários resultados e definições a respeito de conjuntos algébricos. Em particular, a Proposição 6.23 nos fornece um critério para que um dado conjunto algébrico V seja irredutível, que exige o conhecimento do conjunto de polinômios que o geram. O Teorema dos Zeros de Hilbert explicita a relação existente entre ideais e conjuntos algébricos.

Nesta seção, assumimos que K é algebricamente fechado.

Teorema 7.3 (Nullstellensatz, Forma Fraca)**.** *Se I é um ideal próprio em $K[X_1, \ldots, X_n]$, então $\mathcal{V}(I) \neq \emptyset$.*

Demonstração: Podemos assumir que I é um ideal maximal, pois para qualquer ideal maximal J que contém I, teremos $\mathcal{V}(J) \subset \mathcal{V}(I)$. Assim, $L = K[X_1, \ldots, X_n]/I$ é um corpo e, obviamente, K pode ser considerado como um subcorpo de L. Então existe homomorfismo natural de $K[X_1, \ldots, X_n]$ em L, que leva cada X_i em $X_i + I$, garantindo que L é anel finito sobre K. Pelo Lema de Zariski, L é módulo finito sobre K. Considerando que K é corpo algebricamente fechado, obtemos $K = L$, pelo item (ii) da Proposição 6.38. Logo, para cada i existe $a_i \in K$ tal que o I-resíduo de X_i é a_i, ou melhor $X_i - a_i \in I$. Mas $(X_1 - a_1, \ldots, X_n - a_n)$ é um ideal maximal em $K[X_1, \ldots, X_n]$, pela Proposição 6.16. Como $(X_1 - a_1, \ldots, X_n - a_n) \subset I$, e ambos são maximais, então $I = (X_1 - a_1, \ldots, X_n - a_n)$. Portanto, $\mathcal{V}(I) = \{(a_1, \ldots, a_n)\} \neq \emptyset$. ■

Teorema 7.4 (Nullstellensatz, Forma Forte)**.** *Seja I um ideal em $K[X_1, \ldots, X_n]$. Então $\mathcal{I}(\mathcal{V}(I)) = \mathrm{Rad}(I)$.*

De maneira geral, o resultado acima garante que se $F_1, \ldots, F_r, G \in K[X_1, \ldots, X_n]$ e G se anula sempre que $F_1, \ldots, F_r$ se anulam, então existe uma equação $G^N = A_1F_1 + \ldots + A_rF_r$, para algum $N > 0$ e certos $A_i \in K[X_1, \ldots, X_n]$.

Demonstração: A Proposição 6.18 garante que $\mathrm{Rad}(I) \subset \mathcal{I}(\mathcal{V}(I))$. Para mostrar a inclusão inversa, tomemos $G \in \mathcal{I}(\mathcal{V}(F_1, \ldots, F_r))$, com $F_i \in K[X_1, \ldots, X_n]$, e definimos $J = (F_1, \ldots, F_r, X_{n+1} \cdot G - 1) \subset K[X_1, \ldots, X_n, X_{n+1}]$. Então $\mathcal{V}(J) \subset \mathbb{A}^{n+1}(K)$ é vazio, uma vez que G se anula sempre que todos os F_i são zero. De fato, se $(a_1, \ldots, a_{n+1}) \in \mathcal{V}(J)$, então $F_i(a_1, \ldots, a_n) = 0$ e $(a_1, \ldots, a_n) \in \mathcal{V}(I)$. Porém,

$$0 = (X_{n+1} \cdot G - 1)(a_1, \ldots, a_{n+1}) = a_{n+1} \cdot G(a_1, \ldots, a_n) - 1 = -1$$

pois $G(a_1, \ldots, a_n) = 0$. Assim $\mathcal{V}(J) = \emptyset$ e, aplicando a Forma Fraca do Nullstellensatz em J, temos que $J = K[X_1, \ldots, X_{n+1}]$. Decorre desta condição que $1 \in J$, e então existe uma equação

$$1 = \sum (A_i(X_1, \ldots, X_{n+1})F_i) + B(X_1, \ldots, X_{n+1}) \cdot (X_{n+1} \cdot G - 1).$$

Tomando $Y = 1/X_{n+1}$, multiplicamos a equação acima por uma potência grande o suficiente de Y, de tal forma que $Y^N = \sum C_i(X_1, \ldots, X_n, Y)F_i + D(X_1, \ldots, X_n, Y)(G - Y)$ em $K[X_1, \ldots, X_n, Y]$. Substituindo G por Y, obtemos $G^N = \sum E_i(X_1, \ldots, X_n, G)F_i$, isto é, G^N é uma combinação linear de F_i com coeficientes em $K[X_1, \ldots, X_n]$. Logo $G^N \in I$ e $G \in \mathrm{Rad}(I)$. ■

A demonstração acima é devida a Rabinovich. Notemos que a Forma Fraca implica a Forma Forte. Na verdade, as duas formas do Teorema dos Zeros de Hilbert são equivalentes. Com efeito, suponhamos válido o Teorema 7.4, isto é, para $I \in K[X_1, \ldots, X_n]$, temos $\mathcal{I}(\mathcal{V}(I)) = \mathrm{Rad}(I)$. Se $\mathcal{V}(I) = \emptyset$, então $\mathrm{Rad}(I) = \mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\emptyset) = (1)$. Logo $(1) \subset \mathrm{Rad}(I)$, $1 \in I$ e $I = K[X_1, \ldots, X_n]$.

Como consequências do Teorema 7.4, temos os seguintes corolários.

Corolário 7.5. *Se I é um ideal radical em $K[X_1, \ldots, X_n]$, então $\mathcal{I}(\mathcal{V}(I)) = I$. Então existe uma correspondência um a um entre os ideais radicais e os conjuntos algébricos.*

Demonstração: Decorre diretamente do teorema, já que I é ideal radical, isto é, $I = \mathrm{Rad}(I)$. ■

Corolário 7.6. *Se I é um ideal primo, então $\mathcal{V}(I)$ é irredutível. Então existe uma correspondência um a um entre ideais primos e conjuntos algébricos irredutíveis. Os ideais maximais correspondem a pontos.*

Demonstração: Como I é primo, temos $\mathrm{Rad}(I) = I$ (Proposição 1.45-(k)). Daí, $\mathcal{I}(\mathcal{V}(I)) = \mathrm{Rad}(I) = I$ é primo e, pela Proposição 6.23, $\mathcal{V}(I)$ é irredutível. ■

Corolário 7.7. *Seja $F \in K[X_1, \ldots, X_n]$, e $F = F_1^{n_1} \ldots F_r^{n_r}$ a decomposição de F em fatores irredutíveis. Então $\mathcal{V}(F) = \mathcal{V}(F_1) \cup \ldots \cup \mathcal{V}(F_r)$ é a decomposição de $\mathcal{V}(F)$ em componentes irredutíveis, e $\mathcal{I}(\mathcal{V}(F)) = (F_1 \ldots F_r)$. Existe uma correspondência um a um entre polinômios irredutíveis $F \in K[X_1, \ldots, X_n]$ (a menos de multiplicação por elementos não nulos de K) e hipersuperfícies irredutíveis em $\mathbb{A}^n(K)$.*

Corolário 7.8. *Seja I um ideal em $K[X_1, \ldots, X_n]$. Então $\mathcal{V}(I)$ é um conjunto finito se, e somente se, $K[X_1, \ldots, X_n]/I$ é um espaço vetorial de dimensão finita sobre K. Se tal fato ocorrer, o número de pontos em $\mathcal{V}(I)$ é menor que ou igual a dimensão de $K[X_1, \ldots X_n]/I$ como espaço vetorial sobre K.*

Demonstração: Sejam $P_1, \ldots P_r \in \mathcal{V}(I)$. Escolhemos polinômios $F_1, \ldots, F_r \in K[X_1, \ldots, X_n]$ tais que $F_i(P_j) = 0$ se $i \neq j$ e $F_i(P_i) = 1$ (Proposição 6.20). Seja $\overline{F}_i$ o I-resíduo de F_i. Se $\sum \lambda_i \overline{F}_i = 0$, $\lambda_i \in K$, então $\sum \lambda i F_i \in I$, e $\lambda_j = (\sum \lambda_i F_i)(P_j) = 0$. Então os $\overline{F}_i$ são linearmente independentes sobre K, e portanto, r é menor que ou igual a dimensão de $K[X_1, \ldots, X_n]/I$ como espaço vetorial sobre K.

Por outro lado, se $\mathcal{V}(I) = \{P_1, \ldots, P_r\}$ é finito, seja $P_i = (a_{i1}, \ldots, a_{in})$ e $F_j = \prod_{i=1}^{r}(X_j - a_{ij})$, $j = 1, \ldots, n$. Então $F_j \in \mathcal{I}(\mathcal{V}(I))$ e $F_j^N \in I$ para algum $N > 0$. Tomando os I-resíduos, $\overline{F}_j^N = 0$, e então $\overline{X}_j^{rN}$ é uma combinação K-linear de $1, \overline{X}_j, \ldots, \overline{X}_j^{rN-1}$. Segue, por indução análoga a feita no item (ii) da Proposição 6.35, que $\overline{X}_j^s$ é uma combinação K-linear de $\overline{1}, \ldots, \overline{X}_j^{rN-1}$ para todo s, e daí que $\{\overline{X}_1^{m_1} \cdot \ldots \cdot \overline{X}_n^{m_n} : m_i < rN\}$ gera $K[X_1, \ldots, X_n]/I$ como um espaço vetorial sobre K. ■

Capítulo 8

Variedades Afins

Neste capítulo, assumimos que o corpo K é algebricamente fechado e que os conjuntos algébricos afins estarão em $\mathbb{A}^n = \mathbb{A}^n(K)$ para algum n. Além disso, todos os anéis e corpos contém K como subanel e, por homomorfismo $\varphi : A \to B$ de tais anéis, consideraremos um homomorfismo de anéis tal que $\varphi(\lambda) = \lambda$ para todo $\lambda \in K$.

Um conjunto algébrico afim irredutível é chamado de *variedade algébrica*. Ao longo deste texto, utilizaremos apenas o termo "variedades" para nos referirmos a tais conjuntos algébricos.

8.1 Anéis de Coordenadas

Seja $V \subset \mathbb{A}^n$ uma variedade não vazia. Então $\mathcal{I}(V)$ é um ideal primo em $K[X_1, \ldots, X_n]$, assim $K[X_1, \ldots, X_n]/\mathcal{I}(V)$ é um domínio.

Definição 8.1 (Anel de Coordenadas)**.** *O domínio* $\Gamma(V) = K[X_1, \ldots, X_n]/\mathcal{I}(V)$ *é o* anel de coordenadas *de* V*.*

Para todo conjunto algébrico V não vazio, denotamos por $\mathcal{F}(V, K)$ o conjunto de todas as funções de V em K. É claro que $\mathcal{F}(V, K)$, munido das operações

$$(f + g)(x) = f(x) + g(x)$$

e

$$(fg)(x) = f(x)g(x),$$

para todo $x \in V$, $f, g \in \mathcal{F}(V, K)$, é um anel. O corpo K é considerado um subanel de $\mathcal{F}(V, K)$, associado ao conjunto de todas as funções constantes.

Dizemos que uma função $f \in \mathcal{F}(V, K)$ é *função polinomial* se existe um polinômio $F \in K[X_1, \ldots, X_n]$ tal que $f(a_1, \ldots, a_n) = F(a_1, \ldots, a_n)$ para todo

$(a_1, \ldots, a_n) \in V$. Claramente, o conjunto de todas as funções polinomiais é um subanel de $\mathcal{F}(V, K)$ que contém K.

Dois polinômios F, G determinam a mesma função polinomial se, e somente se, $(F - G)(a_1, \ldots, a_n) = 0$ para todo $(a_1, \ldots, a_n) \in V$, isto é, $F - G \in \mathcal{I}(V)$. Com efeito, se $f(a_1, \ldots, a_n) = F(a_1, \ldots, a_n) = G(a_1, \ldots, a_n)$, então $(F - G)(a_1, \ldots, a_n) = 0$. Por outro lado, se $(F - G)(a_1, \ldots, a_n) = 0$, temos $F(a_1, \ldots, a_n) - G(a_1, \ldots, a_n) = 0$, e assim, $F(a_1, \ldots, a_n) = G(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)$.

A aplicação

$$\begin{aligned} \psi : K[X_1, \ldots, X_n] &\longrightarrow \mathcal{F}(V, K) \\ F &\longmapsto f = F|_V \end{aligned}$$

que associa a cada polinômio $F \in K[X_1, \ldots, X_n]$ uma função polinômial $f \in \mathcal{F}(V, K)$ é claramente um homormorfismo, cujo núcleo é $\mathcal{I}(V)$. De fato, se $F \in \ker \psi$, então $f \equiv 0$ e para qualquer $a \in V$, $0 = f(a) = F(a)$, ou seja, $F \in \mathcal{I}(V)$. Reciprocamente, para $F \in \mathcal{I}(V)$, temos que $F(a) = 0$ para todo $a \in V$. Logo $\psi(F) = f = 0$ e $F \in \ker \psi$.

Dessa forma, podemos identificar $\Gamma(V)$ com o subanel de $\mathcal{F}(V, K)$, formado por todas as funções polinomiais de V em K. Portanto, temos duas importantes maneiras de considerar um elemento de $\Gamma(V)$: como uma função em V, ou como uma classe de equivalência de polinômios.

8.2 Aplicações Polinomiais

Sejam $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ variedades. Uma função $\varphi : V \to W$ é uma *aplicação polinomial* se existirem polinômios $T_1, \ldots, T_m \in K[X_1, \ldots, X_n]$ tais que $\varphi(a_1, \ldots, a_n) = (T_1(a_1, \ldots a_n), \ldots, T_m(a_1, \ldots, a_n))$ para todo $(a_1, \ldots, a_n) \in V$.

Qualquer função $\varphi : V \to W$ induz um homomorfismo

$$\begin{aligned} \widetilde{\varphi} : \mathcal{F}(W, K) &\longrightarrow \mathcal{F}(V, K) \\ f &\longmapsto \widetilde{\varphi}(f) = f \circ \varphi \end{aligned}$$

explicitado no diagrama

$$V \xrightarrow{\varphi} W \xrightarrow{f} K, \qquad V \xrightarrow[f \circ \varphi]{} K$$

Em particular, se φ é uma aplicação polinomial, então $\widetilde{\varphi}(\Gamma(W)) \subset \Gamma(V)$. Vejamos:

Se φ é polinomial, então existem polinômios $T_1, \ldots, T_m \in K[X_1, \ldots, X_n]$ tais que, para qualquer $P \in V$, $\varphi(P) = (T_1(P), \ldots, T_m(P))$. Para $f \in \Gamma(W)$, existe $F \in K[X_1, \ldots, X_m]$ tal que $F(Q) = f(Q)$ para todo $Q \in W$. Então, para qualquer $P \in V$, temos que $f \circ \varphi(P) = f(T_1(P), \ldots, T_m(P)) = F(T_1(P), \ldots, T_m(P)) = F \circ (T_1, \ldots, T_m)(P)$. Assim, $f \circ \varphi = \widetilde{\varphi}(f)$ é um polinômio definido em V, e portanto, $\widetilde{\varphi}(f) \in \Gamma(V)$.

A restrição de $\widetilde{\varphi}$ a $\Gamma(W)$, é o homomorfismo $\widetilde{\varphi}$ de $\Gamma(W)$ em $\Gamma(V)$ tal que, se $f \in \Gamma(W)$ é o $\mathcal{I}(W)$-resíduo de um polinômio F, então $\widetilde{\varphi}(f) = f \circ \varphi$ é o $\mathcal{I}(V)$-resíduo do polinômio $F(T_1, \ldots, T_m)$. Mais explicitamente, temos:

$$f \in \Gamma(W) \Rightarrow f = F + \mathcal{I}(W)$$

e então

$$\widetilde{\varphi}(f) = \widetilde{\varphi}(f) + \mathcal{I}(V) = f \circ \varphi + \mathcal{I}(V),$$

onde $f \circ \varphi = F(T_1, \ldots, T_m)$.

Se $V = \mathbb{A}^n$, $W = \mathbb{A}^m$ e $T_1, \ldots, T_m \in K[X_1, \ldots, X_n]$ determinam uma aplicação polinomial $T : \mathbb{A}^n \to \mathbb{A}^m$, então os T_i são unicamente determinados por T e, assim, escrevemos $T = (T_1, \ldots, T_m)$. De fato, se $T(P) = (T_1(P), \ldots, T_m(P)) = (F_1(P), \ldots, F_m(P))$, então $T_i(P) - F_i(P) = (T_i - F_i)(P) = 0$ para todo i. Como K é infinito, a Proposição 6.6 garante que $T_i - F_i \equiv 0$, isto é, $F_i = T_i$.

Vejamos que cada aplicação polinomial de V em W está associada a um homomorfismo do anel de coordenadas $\Gamma(W)$ em $\Gamma(V)$.

Proposição 8.2. *Sejam $V \subset \mathbb{A}^n$, $W \subset \mathbb{A}^m$ variedades afins. Existe uma correspondência um a um entre as aplicações polinomiais $\varphi : V \to W$ e os homomorfismos $\widetilde{\varphi} : \Gamma(W) \to \Gamma(V)$. Qualquer tal $\widetilde{\varphi}$ é a restrição de uma aplicação polinomial de $\mathbb{A}^n$ em $\mathbb{A}^m$.*

Demonstração: Seja $\psi : \Gamma(W) \to \Gamma(V)$ um homomorfismo, e escolhemos $T_i \in K[X_1, \ldots, X_n]$ tais que $\psi(X_i + \mathcal{I}(W)) = T_i + \mathcal{I}(V)$, $i = 1, \ldots, m$. Então $T = (T_1, \ldots, T_m)$ é uma aplicação polinomial de $\mathbb{A}^n$ em $\mathbb{A}^m$, e induz $\widetilde{T} : \Gamma(\mathbb{A}^n) = K[X_1, \ldots, X_m] \to \Gamma(\mathbb{A}^m) = K[X_1, \ldots, X_n]$.

Afirmamos que $T(V) \subset W$. De fato, tomando $F \in \mathcal{I}(W)$, para todo $a \in V$ temos

$$\widetilde{T}(F)(a) = F \circ T(a) = F(T_1, \ldots, T_m)(a).$$

Como $F(T_1, \ldots, T_m) \in \mathcal{I}(W)(a) = \overline{F(T_1, \ldots, T_m)}(a)$ se $a \in V$, então

$$F \circ T(a) = \overline{F}(\overline{T}_1, \ldots, \overline{T}_m)(a) = \psi(F(X_1, \ldots, X_m)(a) = \psi(0_{\Gamma(W)})(a),$$

pois $F \in \mathcal{I}(W)$. Uma vez que ψ é homomorfismo, $\psi(0_{\Gamma(W)})(a) = 0_{\Gamma(V)}(a) = 0$. Com isto, obtemos $T(a) \in \mathcal{V}(\mathcal{I}(W))$. Mas W é algébrico, garantindo que $\mathcal{V}(\mathcal{I}(W)) = W$; e assim, $T(V) \subset W$. Logo, a restrição $\varphi = T|_V : V \to W$ é polinomial.

A discussão feita no início desta seção garante que, a partir da aplicação polinomial φ, obtemos um homomorfismo $\widetilde{\varphi} : \Gamma(W) \to \Gamma(V)$, tal que $\widetilde{\varphi}(F + \mathcal{I}(W)) = F(T_1, \ldots, T_m) + \mathcal{I}(V)$. Portanto, $\widetilde{\varphi} = \psi$. Portanto, dado um homomorfismo entre os anéis de coordenadas, construímos uma aplicação polinomial entre as variedades. E, pela discussão mencionada, dada uma aplicação polinomial entre variedades, construímos um homomorfismo entre anéis de coordenadas. ■

Um aplicação polinomial $\varphi : V \to W$ é um *isomorfismo* se existe uma aplicação polinomial $\psi : W \to V$ tal que $\psi \circ \varphi = \iota_V$, a identidade em V; e $\varphi \circ \psi = \iota_W$, a identidade em W. Segundo o resultado anterior, duas variedades afins são isomorfas se, e somente se, seus respectivos anéis de coordenadas são isomorfos.

8.3 Mudança de Coordenadas

Se $T = (T_1, \ldots, T_m)$ é uma aplicação polinomial de $\mathbb{A}^n$ em $\mathbb{A}^m$, e $F \in K[X_1, \ldots, X_m]$, denotamos $F^T = \widetilde{T}(F) = F(T_1, \ldots, T_m)$. Para ideais I e conjuntos algébricos V em $\mathbb{A}^m$, I^T denota o ideal em $K[X_1, \ldots, X_n]$ gerado por $\{F^T : F \in I\}$; e V^T denota o conjunto algébrico $T^{-1}(V) = \mathcal{V}(I^T)$, onde $I = \mathcal{I}(V)$.

Uma *mudança afim de coordenadas* em $\mathbb{A}^n$ é uma aplicação polinomial $T = (T_1, \ldots, T_n) : \mathbb{A}^n \to \mathbb{A}^n$ tal que cada T_i é um polinômio de grau 1, e tal que T é bijetora. Escrevendo $T_i = \sum a_{ij}X_j + a_{i0}$, então $T = T'' \circ T'$, onde T' é uma aplicação linear e T'' é uma translação. Explicitamente, $T'_1 = \sum a_{ij}X_j$ e $T''_i = X_i + a_{i0}$. Como qualquer translação tem inversa, segue que T será bijetora se, e somente se, T' é invertível. É fácil ver que, se T e U são mudanças afins de coordenadas em $\mathbb{A}^n$, então $T \circ U$ e T^{-1} também o são. Além disso, T é um automorfismo da variedade algébrica $\mathbb{A}^n$.

8.4 Funções Racionais e Anéis Locais

Seja V uma variedade em $\mathbb{A}^n$, $\Gamma(V)$ seu anel de coordenadas. Como $\Gamma(V)$ é um domínio, podemos considerar seu corpo de frações. Este corpo é

chamado de *corpo das funções racionais* em V, e denotado por $K(V)$. Um elemento de $K(V)$ é uma *função racional* em V.

Se f é uma função racional em V, e $P \in V$, dizemos que f está *definida* em P se algum par $a, b \in \Gamma(V)$, tal que $f = a/b$, temos $b(P) \neq 0$. Como pode existir várias maneiras diferentes de escrever f como um quociente de funções polinomiais, f está definida em P se é possível obter um denominador para f que não se anule em P. Entretanto, se $\Gamma(V)$ é um domínio de fatoração única, pela Proposição 3.29 existe essencialmente uma única representação $f = a/b$, com a e b sem fatores em comum. Então f está definida em P se, e somente se, $b(P) \neq 0$.

Para cada $P \in V$, definimos $\mathcal{O}_P(V)$ como o conjunto das funções racionais em V definidas em P. Com as operações definidas no corpo de frações, é claro que $\mathcal{O}_P(V)$ é um subanel de $K(V)$. Além disso, temos que $K \subset \Gamma(V) \subset \mathcal{O}_P(V) \subset K(V)$. O anel $\mathcal{O}_P(V)$ é chamado de *anel local de V em P*.

O conjunto de pontos $P \in V$ onde uma função racional f não está definida é chamado de *conjunto de polos* de f. Para $f \in \mathcal{O}_P(V)$, se $f = a/b$, $a, b \in \Gamma(V)$, $b(P) \neq 0$, definimos o *valor de f em P* como $f(P) = a(P)/b(P)$, denotado por $f(P)$.

Proposição 8.3. (i) *O conjunto de polos de uma função racional em V é um subconjunto algébrico de V.*

(ii) $\Gamma(V) = \cap_{P \in V} \mathcal{O}_P(V)$.

Demonstração: Suponha $V \subset \mathbb{A}^n$. Para $G \in K[X_1, \ldots, X_n]$, denotemos o resíduo de G em $\Gamma(V)$ por $\overline{G}$. Tomemos $f \in K(V)$.

Definimos $J_f = \left\{G \in K[X_1, \ldots, X_n] : \overline{G} \cdot f \in \Gamma(V)\right\}$. Vejamos que J_f é um ideal em $K[X_1, \ldots, X_n]$ contendo $\mathcal{I}(V)$:

- $0 \in J_f$, pois $\overline{0} = \mathcal{I}(V)$ e então $\overline{0} \cdot f \in \Gamma(V)$.
- Se $F, G \in J_F$, então $(\overline{F+G}) \cdot f = (\overline{F} + \overline{G}) \cdot f = \overline{F} \cdot f + \overline{G} \cdot f \in \Gamma(V)$. Logo, $F + G \in J_f$.
- Para $G \in J_f$, então $(\overline{-G}) \cdot f = -\overline{G} \cdot f$, que pertence a $\Gamma(V)$. Assim, $-G \in J_f$.
- Tomando $F \in K[X_1, \ldots, X_n]$ e $G \in J_f$, temos $(\overline{F \cdot G}) \cdot f = \overline{F} \cdot \overline{G} \cdot f \in \Gamma(V)$, pois $\Gamma(V)$ é anel. Logo $F \cdot G \in J_f$.

Por fim, para todo elemento $G \in \mathcal{I}(V)$, temos $\overline{G} = \overline{0} \in J_f$. Para finalizar a demonstração do item (i), provaremos que os pontos de $\mathcal{V}(J_f)$ são

exatamentes os pontos onde f não está definida, isto é, $\mathcal{V}(J_f)$ é o conjunto dos polos de f.

Tomemos $Q \in V \setminus \mathcal{V}(J_f)$. Então existe $G \in J_f$ tal que $G(Q) \neq 0$, e $\overline{G} \cdot f = \overline{H} \in \Gamma(V)$. Daí $f(Q) = \overline{H}(Q)/\overline{G}(Q)$, com $\overline{G}(Q) \neq 0$; e assim f está definida em Q. Por outro lado, seja $P \in V$ tal que f está definida em P. Dessa forma, existem $\overline{F}, \overline{G} \in \Gamma(V)$ tais que $f(P) = \overline{F}(P)/\overline{G}(P)$ com $\overline{G}(P) \neq 0$. Assim, $\overline{G}(P) \cdot f(P) = \overline{F}(P) \in \Gamma(V)$ implica em $G \in J_f$, com $G(P) \neq 0$. Portando $P \in V \setminus \mathcal{V}(J_f)$.

Para o item (ii), basta mostrar que $\cap \mathcal{O}_P \subset \Gamma(V)$, uma vez que os elementos em $\Gamma(V)$ são polinômios definidos em todo $P \in V$. Se $f \in \bigcap_{P \in V} \mathcal{O}_P(V)$, isto é, f não tem polos; o item anterior garante que $\mathcal{V}(J_f) = \emptyset$. Então, utilizando o Teorema 7.3, concluímos $1 \in J_f$, e assim, $1 \cdot f = f \in \Gamma(V)$. ■

É claro que existem funções definidas em P, com valor zero em P. Estas funções constituem o ideal $M_P(V) = \{f \in \mathcal{O}_P(V) : f(P) = 0\}$, chamado de *ideal maximal de V em P*. Obviamente, tal ideal é o núcleo do homomorfismo de valorização $f \to f(P)$ de $\mathcal{O}_P(V)$ em K. Logo, $\mathcal{O}_P(V)/M_P(V)$ é isomorfo a K.

Um elemento $f \in \mathcal{O}_P(V)$ é unidade em $\mathcal{O}_P(V)$ se, e somente se, $f(P) \neq 0$. De fato, para $f \in \mathcal{O}_P(V)$ unidade, existe $g \in \mathcal{O}_P(V)$ tal que $f \cdot g = 1$, e então $f(P) \cdot g(P) = 1$ e $f(P) \neq 0$. Agora, se $f(P) = a(P)/b(P) \neq 0$, então $g = b(P)/a(P) \in \mathcal{O}_P(V)$ e $f \cdot g = 1$. Dessa forma, podemos considerar $M_P(V) = \{\text{não unidades de } \mathcal{O}_P(V)\}$.

Pelo Corolários 1.33 e 1.34, temos que o ideal formado por todas as unidades é o único ideal maximal de $\mathcal{O})P(V)$. Assim, $\mathcal{O}_P(V)$ é um anel local e $M_P(V)$ é seu único ideal maximal.

Proposição 8.4. *$\mathcal{O}_P(V)$ é um domínio Noetheriano local.*

Demonstração: Devemos mostrar que qualquer ideal I em $\mathcal{O}_P(V)$ é finitamente gerado. Como $\Gamma(V)$ é Noetheriano, pela Proposição 4.9, sejam $f_1, \ldots, f_r$ os geradores do ideal $I \cap \Gamma(V)$. Afirmamos que $f_1, \ldots, f_r$ geram I como ideal em $\mathcal{O}_P(V)$. Com efeito, se $f \in I \subset \mathcal{O}_P(V)$, então existe $b \in \Gamma(V)$ com $b(P) \neq 0$ e $bf \in \Gamma(V)$. Daí $bf \in \Gamma(V) \cap I$, e assim $bf = \sum a_i f_i$, $a_i \in \Gamma(V)$. Fazendo $f = \sum (a_i/b) f_i$, obtemos que I é gerado por $f_1, \ldots, f_r$, como desejado. ■

8.5 Anéis de Valorização Discreta

Um anel R é chamado de *anel de valorização discreta* quando satisfaz as condições explicitadas no resultado abaixo.

Proposição 8.5. *Seja R um domínio, mas não corpo. Então as afirmações são equivalentes:*

(i) *R é Noetheriano e local, e seu ideal maximal é principal.*

(ii) *Existe um elemento irredutível $t \in A$ tal que todo elemento não nulo $z \in A$ é escrito de maneira única na forma $z = ut^n$, u unidade em R, e n inteiro não negativo.*

Demonstração: (i) $\Rightarrow$(ii): Seja M o ideal maximal, t um gerador de M. Suponha $ut^n = vt^m$, u, v unidades, $n \geq m$. Então $ut^{n-m} = v$ é unidade, o que só é possível com $n = m$, e daí $u = v$. Assim, dado $z \in R$, a expressão $z = ut^n$ é única. Para mostrar que todo z se escreve de tal forma, assumimos que z não é unidade pois, caso contrário, $z = zt^0$. Como z não é unidade, $z \in M$ e então $z = z_1 t$ para algum $z_1 \in R$. Se z_1 é unidade, terminamos a demonstração. Senão, $z_1 \in M$ e $z_1 = z_2 t$. Continuando com este raciocínio, obtemos uma sequência infinita $z_1, z_2, \ldots$ com $z_i = z_{i+1}t$. Como R é Noetheriano, a cadeia de ideais $(z_1) \subset (z_2) \subset \ldots$ tem um elemento maximal, e daí, $(z_n) = (z_{n+1})$ para algum n. Assim, se $z_{n+1} = vz_n$ para algum $v \in A$, temos $z_n = vtz_n$ e $vt = 1$, mas t não é unidade. Logo, a sequência de z_i é finita, e todo elemento z se escreve como $z = ut^n$.

(ii) $\Rightarrow$ (i): $M = (t)$ é claramente o conjunto das não unidades. Todos os ideais em R são principais, da forma (t^n), $n \geq 0$, e então R é domínio principal. ■

Um elemento t como no item (ii) é chamado de *parâmetro uniformizante* de R, e se $\bar{t}$ é um outro parâmetro, então $\bar{t} = vt$, com v unidade R. De fato, se $t, \bar{t}$ são parâmetros uniformizantes de R temos, em particular, $t = u\bar{t}^n$ e $\bar{T} = vt^m$, u, v unidades. Daí $t = uv^n t^{mn}$, e $1 = uv^n t^{mn-1}$. Logo $mn = 1$, com m, n inteiros, implica que $m = n = 1$; e assim $\bar{t} = vt$.

O expoente n é chamado de *ordem* de z, e denotado $n = \mathrm{ord}(z)$. Por definição, $\mathrm{ord}(0) = \infty$. Este conceito de ordem nos permite escrever $R = \{z \in K : \mathrm{ord}(z) \geq 0\}$ e $M = \{z \in K : \mathrm{ord}(z) > 0\}$, o ideal maximal em R.

A representação de qualquer elemento de R com em (ii) se estende para K, o corpo de frações de R: todo elemento não nulo $z \in K$ tem uma única expressão $z = ut^n$, u unidade em R e $n \in \mathbb{Z}$.

8.6 Ideais com um Número Finito de Zeros

Finalmente, nesta seção apresentamos um resultado que relaciona anéis de coordenadas de $K[X_1, \ldots, X_n]$ com os conjuntos de funções racionais em

$\mathbb{A}^n$.

Proposição 8.6. *Seja I um ideal em $K[X_1, \ldots, X_n]$, e suponha $\mathcal{V}(I) = \{P_1, \ldots, P_m\}$ finito. Seja $\mathcal{O}_i = \mathcal{O}_{P_i}(\mathbb{A}^n)$. Então existe um isomorfismo natural de $K[X_1, \ldots, X_n]/I$ em $\prod_{i=1}^m \mathcal{O}_i/I\mathcal{O}_i$.*

Demonstração: Seja $I_i = \mathcal{I}(\{P_i\}) \subset K[X_1, \ldots, X_n]$ os ideais maximais distintos que contêm I (Proposição 6.16). Denotemos $R = K[X_1, \ldots, X_n]/I$ e $R_i = \mathcal{O}_i/I\mathcal{O}_i$. Os homomorfismos naturais de φ_i de R em R_i, induzem um homomorfismo φ de R em $\prod_{i=1}^m R_i$.

Pelo Teorema dos Zeros de Hilbert (Forma Forte), $\mathrm{Rad}(I) = \mathcal{I}(\{P_1, \ldots, P_m\}) = \bigcap_{i=1}^m I_i$, e então $(\bigcap I_i)^d \subset I$ para algum d. Como $\mathcal{V}(\bigcap I_j) \bigcap \mathcal{V}(I_i) = \emptyset$ para $i \neq j$, obtemos que $\bigcap_{j \neq i} I_j$ e I_i são comaximais. Segue da Proposição 1.41 que $\bigcap(I_j^d) = (I_1 \cdot \ldots \cdot I_m)^d = (\bigcap I_j)^d \subset I$.

Agora escolhemos $F_i \in K[X_1, \ldots, X_n]$ tal que $F_i(P_j) = 0$ se $i \neq j$, $F_i(P_i) = 1$. Seja $E_i = 1 - (1 - F_i^d)^d$. Note que $E_i = F_i^d D_i$ para algum D_i. Então $E_i \in I_j^d$ se $i \neq j$, pois

$$F_i \in I_j \Rightarrow F_i^d \in I_j^d$$

e I_j^d é ideal; e também $1 - \sum_i E_i = (1 - E_j) - \sum_{i \neq j} E_i \in \cap I_j^d \subset I$, já que

$$\left((1 - E_j) - \sum_{i \neq j} E_j\right)(P_i) = 0$$

e

$$\left((1 - E_j) - \sum_{i \neq j} E_j\right)(P_j) = 0.$$

Se tomarmos e_i o resíduo de E_i em R, obtemos:

- $e_i^2 = e_i$. Temos que $e_i^2 = E_i^2 + I$, onde

$$\begin{aligned} E_i^2 &= (1 - (1 - F_i^d)^d) \cdot (1 - (1 - F_i^d)^d) \\ &= \underbrace{1 - (1 - F_i^d)^d}_{E_i} - \underbrace{(1 - F_i^d)^d + (1 - F_i^d)^{2d}}_{G} \end{aligned}$$

  Como $G(P_i) = 0$ e $G(P_j) = 0$, $G \in I$ e, assim, $e_i^2 = e_i$.

- $e_i e_j = 0$. Basta notar que

$$E_i E_j = 1 - (1 - F_j^d)^d - (1 - F_i^d)^d + 1 - F_i^d)^d 1 - F_j^d)^d$$

  se anula em qualquer P_j, mesmo com $i = j$. Logo $E_i E_j \in I$ e $I = \overline{0}$.

- $\sum e_i = 1$. Com efeito, considerando que $1 - \sum_i E_i \in \mathcal{I}$, e $I = \overline{0}$, então $\sum_i e_i = 1$.

Afirmamos que se $G \in K[X_1, \ldots, X_n]$ em $G(P_i) \neq 0$, então existe $t \in R$ tal que $tg = e_i$, onde g é o I-resíduo de G. De fato, assumindo que $G(P_i) = 1$, tomemos $H = 1 - G$, e então $(1 - H)(E_i + HE_i + \ldots + H^{d-1}E_i) = E_i - H^dE_i$. Como $H \in I_i$, temos $H^dE_i \in I$. Logo $g(e_i + he_i + \ldots + h^{d-1}e_i) = e_i$, como desejado.

Utilizando esta afirmação, mostremos que φ é um isomorfismo.

Seja f o I-resíduo de F, com $\varphi(f) = 0$, isto é, $\varphi_i(f) = \overline{0}_i = I\mathcal{O}_i$. Então, para todo i existem $H_i, G_i \in K[X_1, \ldots, X_n]$, tais que $H_i \in I$, $G_i(P_i) \neq 0$ e $F = H_i/G_i$. Assim, $F \cdot G_i = H_i \in I$, e $f \cdot g_i = 0$. Pela afirmação, tomemos $t_ig_i = e_i$. Então $f = \sum e_if = \sum t_ig_if = 0$. Logo, φ é injetor.

Como $E_i(P_i) = 1$, $\varphi_i(e_i)$ é uma unidade em R_i. Assim, como $\varphi_i(e_i)\varphi_i(e_j) = \varphi_i(e_ie_j) = 0$ se $i \neq j$, temos $\varphi_i(e_j) = 0$ para $i \neq j$. Então $\varphi_i(e_i) = \varphi_i(\sum e_j) = \varphi_i(1) = 1$. Suponhamos $z = (a_1/s_1, \ldots, a_m/s_m) \in \prod_{i=1}^m R_i$. Pela afirmação, temos $t_is_i = e_i$, então $a_i/s_i = a_it_i$ em R_i. Logo $\varphi_i(\sum t_ja_je_j) = \varphi(t_ia_i) = a_i/s_i$ e $\varphi(\sum t_ja_je_j) = z$.

■

O colorário a seguir segue diretamente desta demonstração.

Corolário 8.7. *Se $\mathcal{V}(I) = \{P\}$, então $K[X_1, \ldots, X_n]/I$ é isomorfo a $\mathcal{O}_P(\mathbb{A}^n)/I\mathcal{O}_P(\mathbb{A}^n)$.*

Considerações Finais

A principal motivação para este trabalho consiste no interesse da aluna em direcionar sua formação acadêmica e estudos posteriores para Álgebra. Durante o Trabalho de Conclusão de Curso A foram abordados conceitos básicos de Álgebra Comutativa, como anéis, módulos, sequências exatas, corpos de frações, anéis Noetherianos e o importante *Teorema da Base de Hilbert*; objetivando o domínio de resultados fundamentais desta teoria. Esta etapa, além de complementar as disciplinas de álgebra cursadas durante toda a graduação, foi essencial para o estudo desenvolvido no Trabalho de Conclusão de Curso B.

Nesta segunda etapa, estudamos os objetos centrais da Geometria Algébrica, como espaços afins, conjuntos algébricos e variedades; e alguns resultados clássicos, como o *Lema da Normalização de Noether* e o *Teorema dos Zeros de Hilbert*. O grau de complexidade de tais conceitos evidencia o avanço atingido pela aluna, com respeito ao domínio dos conteúdos e do raciocínio formal.

De maneira geral, este Trabalho de Conclusão de Curso permitiu um estudo detalhado a respeito do tema escolhido, além de proporcionar uma experiência bastante significativa no campo da pesquisa científica; enriquecendo a formação da estudante e preparando-a para as próximas etapas de sua vida acadêmica.

Referências Bibliográficas

[1] ATIYAH, M.F.; MACDONALD, I.G. *Introduction to Commutative Algebra.* Massachussetts: Addison-Wesley Publishing Company, 1969.

[2] CHATTERS,A.W.; HAJARNAVIS,C.R. *An Introductory Course in Commutative Algebra.* Nova York: Oxford University Press, 1998.

[3] DOMINGUES,H.; IEZZI, G. *Álgebra Moderna.* São Paulo: Atual, 1982.

[4] FULTON,W. *Algebraic Curves: An Introduction to Algebraic Geometry.* Massachussetts: The Benjamim/Cummings Publishing Company, 1969.

[5] GARCIA, A; LEQUAIN, Y. *Álgebra: um curso de introdução.* Rio de Janeiro: IMPA, 1988.

[6] HUNGERFORD, T.W. *Algebra.* Nova York: Springer-Verlag, 1974.

[7] JACOBSON, N.*Basic Algebra I.* W. H. Nova York: Freeman and Company, 1985.