Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

ANÉIS EUCLIDIANOS E ALGUMAS DE SUAS PROPRIEDADES

por

ROSVITA FUELBER FRANKE

Porto Alegre, julho de 2001

Dissertação submetida por ROSVITA FUELBER FRANKE* como requisito parcial para a obtenção do grau de Mestre em Matemática pelo Programa de Pós-Graduação em Matemática do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.

Professor Orientador:
Dra. Cydara Cavedon Ripoll

Banca Examinadora:
Dra. Ada Maria de Souza Doering
Dra. Luisa Rodriguez Doering
Dr. Yves Albert Emile Lequain

Data de Defesa: 13 de julho de 2001.

---

* Bolsista da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES

Agradecimentos

À Universidade Federal do Rio Grande do Sul pela oportunidade oferecida;

Aos professores do Programa de Pós Graduação, pelo incentivo e amizade;

À professora Cydara pela orientação segura, apoio, incentivo e compreensão recebidos durante todo o transcorrer do trabalho e curso;

Aos amigos e colegas, pela palavra de estímulo que sempre veio na hora certa;

À Deus que sempre esteve presente;

Ao meu querido marido Frederico, agradeço e dedico este trabalho, pela paciência, carinho, amizade, atenção, amor, incentivo e por compartilhar comigo desta etapa tão importante de minha vida.

Abstract

In this work we will see some aspects of the euclidean rings such as: the generalization to rings of the usual concept of eucideans domains, their elementary properties, the smallest algorithm and its construction.

We will show some examples and discuss in which cases the norm will give us an euclidean funcion for the case of quadratic fields for which the ring of integers is euclidean.

Resumo

Neste trabalho estudamos alguns aspectos dos anéis euclidianos, tais como: a generalização para anéis do conceito usual de domínio euclidiano; suas propriedades básicas; o menor algoritmo e sua construção.

Apresentamos também exemplos e discutimos em que casos a norma dá origem a uma função euclidiana no caso de anéis de inteiros quadráticos.

Sumário

INTRODUÇÃO

Neste trabalho estudamos alguns aspectos dos anéis euclidianos, tais como: a generalização para anéis do conceito usual de domínio euclidiano, levando em conta a necessidade de ampliarmos o contra-domínio da função euclidiana para um conjunto bem ordenado e o desejo de manter a propriedade de ser principal; suas propriedades básicas; definimos o que chamamos de menor algoritmo e discutimos sua construção.

Apresentamos também exemplos e discutimos em que casos a norma dá origem a uma função euclidiana no caso de anéis de inteiros quadráticos.

A referência básica para este trabalho é [S_2]. No entanto gostaríamos de salientar que no artigo citado o autor ainda aborda a situação em que o anel é um anel de coordenadas de uma curva algébrica afim de genus zero, situação esta que não será tratada aqui.

Sobre teoria básica de álgebra relembramos aqui a seguinte definição e as seguintes proposições:

*Definição*1: Dois ideais $\mathcal{J}, \mathcal{I}$ de um anel A são ditos **comaximais** se $\mathcal{I} + \mathcal{J} = A$.

É claro que quaisquer dois ideais maximais distintos são comaximais. Ainda:

Proposição 0.1: *Sejam A um anel e $\mathcal{U}_1,...,\mathcal{U}_n$ ideais de A. Se $\mathcal{U}_i,\mathcal{U}_j$ forem comaximais sempre que $i \neq j$, então*

$$\bigcap_{i=1}^{n} \mathcal{U}_i = \prod_{i=1}^{n} \mathcal{U}_i.$$

Proposição 0.2: *Sejam A um anel e $\mathcal{U}_1,...,\mathcal{U}_n$ ideais quaisquer de A. Com relação ao homomorfismo*

$$\phi : A \to \prod_{i=1}^{n} \frac{A}{\mathcal{U}_i}$$

dado por $\phi(x) = (x + \mathcal{U}_1, ..., x + \mathcal{U}_n)$, temos:

i) ϕ *é sobrejetora* $\Leftrightarrow$ $\mathcal{U}_i, \mathcal{U}_j$ *forem comaximais sempre que* $i \neq j$;

ii) ϕ *é injetora* $\Leftrightarrow \bigcap_{i=1}^{n} \mathcal{U}_i = (0)$.

Como conseqüência destas proposições temos o seguinte corolário:

Teorema 0.3: **Teorema Chinês de Restos**: *Sejam* $A_1, \ldots, A_n$ *ideais dois a dois comaximais em um anel R. Então, dados* $b_1, \ldots, b_n \in R$, *sempre existe* $b \in R$ *tal que*

$$b \equiv b_i (\mathrm{mod} A_i) \qquad (i = 1, 2, n).$$

Além disso b é unicamente determinado a menos de congruências módulo o ideal

$$\bigcap_{i=1}^{n} A_i = \prod_{i=1}^{n} A_i.$$

Durante o texto nos referiremos a estes resultados como proposição 0.1, proposição 0.2 e teorema 0.3.

Para a prova dos resultados citados acima veja a proposição 1.10 de [A-M].

A seguir, listamos algumas **convenções** que serão consideradas ao longo deste trabalho:

1) A menos que especificado o contrário, todo anel será comutativo com unidade;

2) Por **domínio** consideramos um anel comutativo com unidade e sem divisores de zero;

3) Os módulos são todos unitários, isto é, $1m = m$, para todo m pertencente ao módulo.

E também estabelecemos as seguintes **notações**:

1) $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$;

2) $B^* = B - \{0\}$;

3) $U(A)$ = invertíveis do anel A;

4) $\langle x \rangle$ = ideal gerado pelo elemento x;

5) $cf(D)$ = corpo de frações do domínio D.

Capítulo 1

PRÉ-REQUISITOS

1.1 Conjuntos Bem Ordenados

Definição 1.1.1: Uma **ordem parcial** (ou algumas vezes simplesmente chamada uma **ordem**) em um conjunto X é uma relação reflexiva, anti-simétrica e transitiva em X; e neste caso X é dito um conjunto **parcialmente ordenado**.

Definição 1.1.2: Se uma ordem parcial $\leqslant$ num conjunto X satisfaz ainda a propriedade que para todo x e y em X, $x \leqslant y$ ou $y \leqslant x$, então $\leqslant$ é chamada uma **ordem total**, e X é dito um conjunto **totalmente ordenado**.

Definição 1.1.3: Um conjunto A parcialmente ordenado é dito **bem ordenado** (e sua ordem é chamada uma **boa ordenação**), se todo subconjunto não vazio de A possui menor elemento.

Propriedades básicas de um conjunto bem ordenado:

i) Todo conjunto bem ordenado é totalmente ordenado (e portanto todo subconjunto de um conjunto bem ordenado possui **o** menor elemento).

ii) Todo subconjunto de um conjunto bem ordenado é também bem ordenado.

A demonstração destas propriedades, bem como maiores detalhes sobre toda esta seção podem ser encontrados em [Ha].

Definição 1.1.4: Sejam A e B conjuntos totalmente ordenados. Considere o

conjunto $A \times B$. A relação

$$(a_1, b_1) \leqslant (a_2, b_2) \Leftrightarrow a_1 < a_2 \text{ ou } (a_1 = a_2 \text{ e } b_1 \leqslant b_2)$$

define uma relação de ordem em $A \times B$ chamada de **ordem lexicográfica**.

Exemplos:

a) O conjunto $\mathbb{N}$ é um conjunto bem ordenado;

b) Se A e B são conjuntos bem ordenados tem-se que $A \times B$ com a ordem lexicográfica é também bem ordenado.

De fato: Seja H um subconjunto de $A \times B$.

Consideremos o seguinte conjunto:

$$H_A = \{a \in A | \exists b \in B,\ (a,b) \in H\} \subset A.$$

Como o conjunto A é bem ordenado por hipótese, temos que existe um elemento

$$a_0 \in H_A \text{ tal que } a_0 \leqslant a, \forall a \in H_A.$$

Consideramos agora o conjunto

$$H_B = \{b \in B | (a_0, b) \in H\} \subset B.$$

Usando que o conjunto B é um conjunto bem ordenado, temos que

$$\exists\ b_0 \in H_B \text{ tal que } b_0 \leqslant y, \forall y \in H_B.$$

Afirmamos que o elemento (a_0, b_0) é o menor elemento do conjunto H.

Tomemos $(a,b) \in H$. Então $a \in H_A$ e portanto $a_0 \leqslant a$.

Se $a_0 < a$ então está pronto; caso $a_0 = a$ então $b \in H_B$ e portanto $b_0 \leqslant b$ pela construção de b_0.

Assim, temos que $(a_0, b_0) \leqslant (a,b)$.

■

Definição 1.1.5: Se X é um conjunto parcialmente ordenado, e se $a \in X$, o conjunto $\{x \in X \mid x < a\}$ é chamado o **segmento inicial** determinado por a. Um subconjunto Y de um conjunto parcialmente ordenado X é dito um **segmento inicial de** X se existe em X um elemento a tal que Y é o segmento inicial determinado por a.

Aqui, como exemplo, temos que o segmento inicial determinado por $(1,n) \in \mathbb{N} \times \mathbb{N}$, com a ordem lexicográfica, é o conjunto $\{0\} \times \mathbb{N}$.

Definição 1.1.6: Sejam A e W conjuntos bem ordenados. Dizemos que uma bijeção $\xi : A \to W$ **preserva ordem** ou é um **ordem-isomorfismo** se a seguinte condição é

verificada:

$$\forall a,b \in A, a \leqslant b \Rightarrow \xi(a) \leqslant \xi(b).$$

Assim, se tivermos conjuntos bem ordenados W_1, W_2 com $\#W_1 < \#W_2$ temos que sempre podemos encontrar um segmento inicial de W_2 que é ordem-isomorfo a W_1.

Definição 1.1.7: Dados dois conjuntos E e F disjuntos e bem ordenados, podemos definir uma boa ordem em $E \cup F$ de modo que pares de elementos em E e também pares de elementos em F retenham a ordem que tinham, e de modo que cada elemento de E preceda cada elemento de F. Com uma tal ordem, o conjunto bem ordenado $E \cup F$ é chamado **soma ordinal** dos conjuntos bem ordenados E e F.

Para efetuarmos a soma ordinal de um conjunto bem ordenado W com o próprio conjunto W, podemos considerar os conjuntos $W_1 = \{(x,0) | x \in W\}$ e $W_2 = \{(x,1) | x \in W\}$ que, naturalmente, são ordem-isomorfos a W mas agora com a vantagem de serem disjuntos. Daí, considerando em $W_1 \cup W_2$ a soma ordinal de W_1 e W_2 teremos $W_1 \cup W_2$ um conjunto bem ordenado com a ordem lexicográfica.

Outro fato importante sobre conjuntos bem ordenados é que podemos obter resultados sobre seus elementos por um processo análogo ao de indução matemática. Mais precisamente: suponhamos que S seja um subconjunto de um conjunto bem ordenado X, e suponhamos que a condição "$x \in X$ e o segmento inicial determinado por x está totalmente contido em S" implique $x \in S$. Nestas condições, o **Princípio de Indução Transfinita** afirma que devemos ter $S = X$. Equivalentemente: se a presença, em S, de um conjunto de todos os predecessores estritos de um elemento de X implica a presença do próprio elemento em S, então S contém todo X ou seja, $S = X$.

1.2 Domínios Fatoriais, Principais, Noetherianos e Artinianos

Mencionamos inicialmente alguns resultados gerais de anéis comutativos que serão utilizados aqui mesmo neste parágrafo. Salientamos que as demontrações não apresentadas, salvo menção em contrário, podem ser encontradas em [A-M].

Lema 1.2.1: *Sejam A um anel e $\mathcal{M}_1, \mathcal{M}_2$ dois ideais maximais distintos de A. Então, para qualquer $t \in \mathbb{N}^*$, $\mathcal{M}_1^t$ e $\mathcal{M}_2^t$ são ideais comaximais.*

Prova: Por contraposição suponhamos que $\mathcal{M}_1^t + \mathcal{M}_2^t \neq A$. Teremos então

que existe $\mathcal{M}$ ideal maximal de A tal que $\mathcal{M}_1' + \mathcal{M}_2' \subseteq \mathcal{M}$. Mas então $\mathcal{M}_1' \subseteq \mathcal{M}$ e, como $\mathcal{M}$ é primo tem-se que $\mathcal{M}_1 \subseteq \mathcal{M}$, e portanto, como ambos são maximais teremos $\mathcal{M}_1 = \mathcal{M}$.

Fazendo o mesmo raciocínio para a outra parcela teremos $\mathcal{M}_2 = \mathcal{M}$, donde $\mathcal{M}_1 = \mathcal{M}_2$.

■

Definição 1.2.2: Um elemento $p \neq 0$ e não invertível de um anel A é dito um **elemento primo** se para todo $a, b \in A$, temos

$$p|ab \Rightarrow p|a \text{ ou } p|b,$$

onde por $x|y$ estamos significando divisibilidade em A, ou seja, que existe $z \in A$ tal que $y = zx$.

Definição 1.2.3: Um elemento $x \neq 0$ e não invertível de um anel A é dito **irredutível** em A se não possui fatoração não-trivial em A, isto é, se $a, b \in A$ são tais que $ab = x$, então a ou b é invertível em A.

Lema 1.2.4: *Em um domínio, todo elemento primo é irredutível.*

Salientamos que a volta desta afirmação não é sempre verdadeira: prova-se que em $\mathbb{Z}[\sqrt{-5}]$ o elemento 3 é irredutível mas não é primo.

No entanto existe uma situação particular onde esta recíproca é válida, como mostramos a seguir.

Definição 1.2.5: Seja A um anel. Um ideal $\mathcal{I}$ de A é dito um **ideal principal** se existe $x \in A$ tal que $\mathcal{I}=\langle x \rangle$. Um anel (respectivamente um domínio) no qual todo ideal é principal é chamado de **anel a ideais principais** (respectivamente **domínio a ideais principais -DIP**).

Proposição 1.2.6: *Num anel a ideais principais A todo elemento irredutível é primo. (Com isto, temos que em um domínio a ideais principais {primos} = {irredutíveis}).*

Definição 1.2.7: Um ideal $\mathcal{I}$ de um anel A é dito **ideal nilpotente** se $\mathcal{I}^n = (0)$ para algum inteiro $n > 0$.

Em [Z-S] (Th.IV.15.33) encontramos um interessante teorema sobre a estrutura dos anéis a ideais principais:

Teorema 1.2.8: *A soma direta de anéis a ideais principais é ainda um anel a ideais principais. Cada anel a ideais principais é a soma direta de domínios a ideais*

principais e de anéis a ideais principais com um único e nilpotente ideal primo. Ainda, num anel a ideais principais com um único e nilpotente ideal primo $\langle p \rangle$ todo elemento não nulo x é da forma $x = p^{v(x)}u$, onde u é invertível e $v(x)$ é univocamente determinado por x.

Definição 1.2.9: Um domínio D é dito um **domínio de fatoração única -DFU**, se todo elemento não nulo e não invertível de D se escreve como produto de irredutíveis de D e tal fatoração é única, a menos de ordem e de associados.

Proposição 1.2.10: *Em um domínio de fatoração única, um ideal é maximal se e somente se é gerado por um elemento irredutível.*

Queremos agora mostrar que todo domínio a ideais principais é um domínio de fatoração única; para tanto, precisamos de algumas definições importantes:

Definição 1.2.11: Uma **cadeia ascendente** de ideais de um anel A é uma seqüência $(\mathcal{I}_j)_{j\in\mathbb{N}}$ de ideais de A tais que

$$\mathcal{I}_0 \subseteq \mathcal{I}_1 \subseteq \ldots \subseteq \mathcal{I}_n \subseteq \ldots$$

De maneira análoga define-se **cadeia descendente**.

Uma cadeia é dita **estacionária** se existe n tal que $\mathcal{I}_0 \subseteq \mathcal{I}_1 \subseteq \ldots \subseteq \mathcal{I}_n = \mathcal{I}_{n+1} = \ldots.$

O **comprimento** de uma cadeia ascendente é o número de inclusões estritas. Uma **cadeia maximal** de A é aquela em que nenhum ideal extra pode ser inserido através de inclusões próprias, o que é equivalente a dizer que cada quociente $\frac{\mathcal{I}_j}{\mathcal{I}_{j-1}}$ é um anel simples, ou seja, não possui ideais além dos triviais.

Proposição 1.2.12: *Suponha que o anel A tem uma cadeia maximal de comprimento n. Então cada cadeia maximal de A tem comprimento n, e cada cadeia em A pode ser estendida a uma cadeia maximal.*

Definição 1.2.13: Um anel A é chamado de **noetheriano** se satisfaz uma das três condições equivalentes:

i) Todo conjunto não vazio de ideais de A tem um elemento maximal;

ii) Toda cadeia ascendente de ideais de A é estacionária;

iii) Todo ideal em A é finitamente gerado.

Resaltamos que o tipo mais simples de anéis noetherianos são os anéis a ideais

principais.

Podemos agora mostrar que:

Proposição 1.2.14: *Todo domínio a ideais principais é um domínio de fatoração única.*

Prova: Para a prova da existência da fatoração, começamos considerando $a \in A$ não invertível e não irredutível. Temos que $\langle a \rangle \subset \mathcal{M} = \langle m_1 \rangle$, para algum irredutível m_1. Portanto $a = m_1 a_1$, para algum $a_1 \in A$, não invertível.

Se a_1 for irredutível ou invertível está pronto. Caso contrário temos $\langle a_1 \rangle \subseteq \langle m_2 \rangle$ para algum irredutível $m_2 \in A$ e, como anteriormente, teremos $a_1 = m_2 a_2$ com a_2 não invertível e portanto $a = m_1 m_2 a_2$.

Se a_2 for irredutível está pronto, caso contrário continuamos o processo. Garantimos que este processo de fatoração em irredutíveis é finito, uma vez que a cadeia

$$\langle a \rangle \subseteq \langle a_1 \rangle \subseteq \langle a_2 \rangle \subseteq \ldots$$

tem de ser estacionária, já que o anel é noetheriano.

Para a unicidade, tomemos um elemento $a \in A$ não invertível e não irredutível e suponhamos

$$a = m_1 m_2 \ldots\ldots m_n \quad \text{e} \quad a = p_1 p_2 \ldots\ldots p_s$$

com p_i e m_j todos irredutíveis em A.

Temos que $m_1 m_2 \ldots\ldots m_n = p_1 p_2 \ldots\ldots p_s$. Suponhamos que $n \leqslant s$. Como $m_1 | a$ temos que

$$\begin{aligned} & m_1 | p_1 p_2 \ldots\ldots p_s \\ \Rightarrow\ & \exists j, m_1 | p_j \\ \Rightarrow\ & p_j = m_1 t_1 \\ \Rightarrow\ & t_1 \in U(A), \end{aligned}$$

sendo esta última implicação válida por que m_1 e p_1 são ambos irredutíveis.

Após reordenar o produto $p_1 p_2 \ldots\ldots p_s$ de modo a termos $j = 1$, obtemos

$$m_1 m_2 \ldots\ldots m_n = t_1 m_1 p_2 \ldots\ldots p_s.$$

Como estamos em um domínio podemos então considerar que

$$m_2 \ldots\ldots m_n = t_1 p_2 \ldots\ldots p_s.$$

Seguindo este raciocínio para $m_2, m_3, \ldots m_n$ e reordenando a cada vez que for necessário chegamos a

$$m_n = t_1 t_2 \ldots t_{n-1} p_n \ldots p_s \text{ com } t_1, t_2, \ldots, t_{n-1} \in U(A).$$

Como m_n é irredutível, por hipótese, conclui-se que $n = s$ e m_n e p_n são associados.

■

Salientamos que a recíproca desta proposição não é válida pois $K[X, Y]$ é DFU mas não é DIP.

Proposição 1.2.15: *Se D é um domínio noetheriano e $\mathcal{M}$ é um ideal maximal de D tal que $\frac{D}{\mathcal{M}}$ é finito então $\frac{D}{\mathcal{M}^t}$ é um anel finito, para todo $t \in \mathbb{N}^*$.*

Prova: Afirmamos inicialmente que para todo $r \in \mathbb{N}$, $\frac{\mathcal{M}^r}{\mathcal{M}^{r+1}}$ é um $\frac{D}{\mathcal{M}}$ –espaço vetorial de dimensão finita; daí, por hipótese, temos que $\frac{D}{\mathcal{M}}$ é finito, o que significa que $\frac{\mathcal{M}^r}{\mathcal{M}^{r+1}}$ é um conjunto finito, para todo $r \in \mathbb{N}^*$.

De fato, se D é um anel noetheriano então $\frac{D}{\mathcal{M}^{r+1}}$ é também noetheriano, e portanto $\frac{\mathcal{M}^r}{\mathcal{M}^{r+1}}$ é um ideal finitamente gerado de $\frac{D}{\mathcal{M}^{r+1}}$, digamos, $\frac{\mathcal{M}^r}{\mathcal{M}^{r+1}} = \langle \overline{m_1}, ..., \overline{m_t} \rangle$. Afirmamos que tais elementos são também geradores do $\frac{D}{\mathcal{M}^{r+1}}$ –espaço vetorial $\frac{\mathcal{M}^r}{\mathcal{M}^{r+1}}$, pois

$$\overline{m} \in \frac{\mathcal{M}^r}{\mathcal{M}^{r+1}} \Rightarrow \overline{m} = \sum_{finita} a_{i_1 \ldots i_t} \overline{m_1}^{i_1} \ldots \overline{m_t}^{i_t} \in \frac{D}{\mathcal{M}^{r+1}} \overline{m_1} + \ldots + \frac{D}{\mathcal{M}^{r+1}} \overline{m_t}.$$

Note agora ainda que existe um isomorfismo de anéis entre

$$\frac{D}{\mathcal{M}^r} \text{ e } \frac{\frac{D}{\mathcal{M}^{r+1}}}{\frac{\mathcal{M}^r}{\mathcal{M}^{r+1}}}.$$

Daí afirmamos que, para todo $r \in \mathbb{N}^*$, $\frac{D}{\mathcal{M}^r}$ é também finito. A prova é por indução sobre r : para $r = 1$ temos que se $\frac{D}{\mathcal{M}}$ é finito por hipótese; seja $r \geqslant 1$ e suponhamos que $\frac{D}{\mathcal{M}^r}$ é finito. Então, pelo isomorfismo de anéis acima, temos que $\frac{D}{\mathcal{M}^{r+1}}$ é finito.

■

Proposição 1.2.16: *Se D é um domínio a ideais principais e $\{\mathcal{M}_\alpha\}_{\alpha \in I}$ denota a família de todos os seus ideais maximais, então*

$$\bigcap_{\alpha \in I} D_{\mathcal{M}_\alpha} = D,$$

onde $D_{\mathcal{M}_\alpha}$ denota o domínio D localizado em $\mathcal{M}_\alpha$ para $\alpha \in I$.

Prova: ($\subseteq$) Inicialmente observemos que, quando tomamos um elemento $x \in \bigcap_{\alpha \in I} D_{\mathcal{M}_\alpha} \subset cf(D)$, podemos considerar que $x = \frac{a}{b}$, com $a, b \in D$ sem fatores irredutíveis em comum, uma vez que, por ser domínio principal, D é um DFU. Afirmamos que $b \notin \mathcal{M}_\alpha$, para todo $\alpha \in I$.

De fato, por definição de localização, podemos considerar que, para cada $\alpha \in I$, existem $w_\alpha \in D$ e $y_\alpha \notin \mathcal{M}_\alpha$ tais que

$$\frac{a}{b} = \frac{w_\alpha}{y_\alpha}.$$

Suponhamos por absurdo que $b \in \mathcal{M}_\alpha$ para algum α. Neste caso, usando novamente que D é um DFU, podemos considerar

$$ay_\alpha = bw_\alpha \in \mathcal{M}_\alpha$$
$$\Rightarrow a \in \mathcal{M}_\alpha, \text{ pois } y_\alpha \notin \mathcal{M}_\alpha.$$

Daí, supondo $\mathcal{M}_\alpha = \langle m_\alpha \rangle$ teremos m_α irredutível e

$$b = m_\alpha s \quad \text{e} \quad a = m_\alpha t,$$

para algum $s, t \in A$, absurdo.

Assim, ao tomarmos $x = \frac{a}{b} \in \bigcap_{\alpha \in I} D_{\mathcal{M}\alpha}$ teremos que $a \in D$ mas $b \notin \bigcup_{\alpha \in I} \mathcal{M}_\alpha$; mas então, $b \in U(D)$, e portanto $\frac{a}{b} = ab^{-1} \in D$.

($\supseteq$) Tomemos $x \in D$, então $\frac{x}{1} \in D$ e, como $1 \notin \bigcup_{\alpha \in I} \mathcal{M}_\alpha$, temos que $\frac{x}{1} \in \bigcap_{\alpha \in I} D_{\mathcal{M}_\alpha}$.

■

Definição 1.2.17: Dado um ideal $\mathcal{I}$ de um anel A o conjunto $r(\mathcal{I}) = \{x \in A \mid \exists n > 0; x^n \in \mathcal{I}\}$ é dito o **radical** de $\mathcal{I}$.

Definição 1.2.18: Um ideal $\mathcal{I}$ de um anel A é dito **primário** se $\mathcal{I} \neq A$ e se, para todo $x, y \in A$,

$$xy \in \mathcal{I} \Rightarrow \text{ou } x \in \mathcal{I} \text{ ou } y^n \in \mathcal{I} \text{ para algum } n > 0.$$

Uma propriedade dos ideais primários é a de que se $\mathcal{I}$ é um ideal primário então $r(\mathcal{I})$ é o menor ideal primo que contém $\mathcal{I}$.

*Definição*1.2.19: Uma **decomposição primária** de um ideal $\mathcal{U}$ de A é uma expressão de $\mathcal{U}$ como uma intersecção finita de ideais primários, digamos $\mathcal{U} = \bigcap_{i=1}^{n} \mathcal{I}_i$.

Proposição 1.2.20: *Em um anel noetheriano A todo ideal possui uma decomposição primária.*

Definição 1.2.21: A intersecção de todos os ideais primos de um anel é um

ideal, que chamamos **nilradical**.

Proposição 1.2.22: *Em um anel noetheriano o nilradical é um ideal nilpotente e é igual a* $r(0)$.

Definição 1.2.23: Um anel A é dito **artiniano** se satisfaz uma das seguintes condições equivalentes:

i) Cada conjunto não vazio de ideais em A tem elemento minimal;

ii) (condição de cadeia descendente - **ccd**): Cada cadeia descendente de ideais em A é estacionária.

Salientamos que, como exemplo de conjunto que satisfaz **ccd**, podemos citar os conjuntos bem ordenados, ou seja, todo conjunto bem ordenado satisfaz a condição de cadeia descendente. No entanto não vale a recíproca, isto é um conjunto que satisfaz **ccd** pode ser apenas parcialmente ordenado, enquanto que todo conjunto bem ordenado é necessariamente totalmente ordenado. E de fato: $\mathbb{N} \times \mathbb{N}$ com a **ordem cardinal**

$$(a_1, a_2) \leqslant (b_1, b_2) \Leftrightarrow a_1 \leqslant b_1 \text{ e } a_2 \leqslant b_2$$

é parcialmente ordenado, satisfaz **ccd** e não é totalmente ordenado pois $(1,2)$ e $(2,1)$ são incomparáveis.

Proposição 1.2.24: *Um anel artiniano tem apenas um número finito de ideais maximais.*

Proposição 1.2.25: *Um anel A admite uma cadeia maximal de ideais se somente se é artiniano e noetheriano.*

Note que um anel artiniano e noetheriano tem cadeia maximal de comprimento finito, pois satisfaz as condições de cadeia descendente e ascendente.

Proposição 1.2.26: *Seja A um anel em que o ideal nulo é um produto* $(0) = \mathcal{M}_1 \ldots \mathcal{M}_n$ *de ideais maximais (não necessariamente distintos). Então A é noetheriano se e somente se A é artiniano.*

Definição 1.2.27: Dizemos que a **dimensão (de Krull)** de um anel A é o supremo dos comprimentos de todas as cadeias de ideais primos do anel A.

Proposição 1.2.28: *Um anel A é artiniano se e somente se é noetheriano e tem*

dimensão nula, ou seja, todo ideal primo é maximal.

Proposição 1.2.29: *A é um anel artiniano em que todos os seus corpos de restos são finitos se e somente se A é um anel de cardinalidade finita.*

Prova: Suponhamos que A é um anel artiniano com corpos de restos finitos. Pela proposição 1.2.24, A tem um número finito de ideais maximais, digamos $\mathcal{M}_1,...,\mathcal{M}_r$.

Como todo anel artiniano tem dimensão de Krull zero, temos que $\mathcal{M}_1,...,\mathcal{M}_r$ são todos os ideais primos de A. Portanto, pela proposição 0.1,

$$r(0) = \bigcap_{\mathcal{P}\text{ primo de }A} \mathcal{P} = \bigcap_{i=1}^{r} \mathcal{M}_i = \prod_{i=1}^{r} \mathcal{M}_i.$$

Como todo anel artiniano é noetheriano, temos que o nilradical de A é nilpotente, pela proposição 1.2.22. Ou seja, existe $s \in \mathbb{N}$, tal que

$$\mathcal{M}_1^s.....\mathcal{M}_r^s = (\mathcal{M}_1.....\mathcal{M}_r)^s = r(0)^s = 0.$$

Portanto o homomorfismo natural de anéis:

$$\omega : A \to \frac{A}{\mathcal{M}_1^s} \times ... \times \frac{A}{\mathcal{M}_r^s} \qquad (*)$$

pela proposição 0.1, tem núcleo

$$\mathcal{M}_1^s \cap ... \cap \mathcal{M}_r^s = \mathcal{M}_1^s.....\mathcal{M}_r^s = 0$$

e portanto, pelos lema 1.2.1 e proposição 0.2, é um isomorfismo.

Mas A é um anel noetheriano com corpos de restos finitos. Então $\frac{A}{\mathcal{M}_i^s}$ tem cardinalidade finita para cada i. Portanto, por $(*)$, A tem cardinalidade finita.

A recíproca é clara.

■

Proposição 1.2.30: *Seja D um domínio noetheriano de dimensão um com corpos de restos finitos. Então, para todo ideal não nulo $\mathcal{U}$ de D, o anel quociente $\frac{D}{\mathcal{U}}$ tem cardinalidade finita.*

Prova: Seja $\mathcal{U}$ um ideal não nulo de D; para mostrar que $\frac{D}{\mathcal{U}}$ é finito vamos mostrar que

$$\frac{D}{\mathcal{U}} \simeq \frac{\frac{D}{\mathcal{U}}}{\frac{\mathcal{M}_1^t}{\mathcal{U}}} \times ... \times \frac{\frac{D}{\mathcal{U}}}{\frac{\mathcal{M}_s^t}{\mathcal{U}}}$$

onde $\mathcal{M}_1,...,\mathcal{M}_s$ são alguns ideais maximais de D e $t \in \mathbb{N}^*$, pois daí, como $\frac{\frac{D}{\mathcal{U}}}{\frac{\mathcal{M}_i^t}{\mathcal{U}}} \simeq \frac{D}{\mathcal{M}_i^t}$, teremos que $\frac{D}{\mathcal{U}}$ é finito, pois mostraremos que cada $\frac{D}{\mathcal{M}_i^t}$ é também finito.

Observemos primeiramente que se D é noetheriano e $\mathcal{U} \neq 0$ então $\mathcal{U}$ admite uma decomposição primária, digamos, $\mathcal{U} = \bigcap_{i=1}^{s} \mathcal{I}_i$ com $r(\mathcal{I}_i) = \mathcal{P}_i$. Então, como D tem dimensão um, temos que cada ideal primo $\mathcal{P}_i$ já é maximal. Fazemos então $\mathcal{P}_i = \mathcal{M}_i$, para todo i.

Afirmamos agora que $\mathcal{M}_1, ..., \mathcal{M}_s$ são todos os ideais primos de D que contêm $\mathcal{U}$. De fato, pois se existir $\mathcal{P}$ tal que $\mathcal{P} \supseteq \mathcal{U} = \bigcap_{i=1}^{s} \mathcal{I}_i$ então, sendo $\mathcal{P}$ primo, temos que $\exists i$ tal que $\mathcal{I}_i \subseteq \mathcal{P}$. Mas então $\mathcal{P} = r(\mathcal{P}) \supseteq r(\mathcal{I}_i) = \mathcal{M}_i$, donde $\mathcal{P} = \mathcal{M}_i$, uma vez que $\mathcal{M}_i$ é maximal.

Como sabemos que existe uma bijeção entre os conjuntos

{ ideais primos de $\frac{D}{\mathcal{U}}$ } e { ideais primos de D que contêm $\mathcal{U}$ },

temos que os ideais $\frac{\mathcal{M}_1}{\mathcal{U}}, ..., \frac{\mathcal{M}_s}{\mathcal{U}}$ são todos os ideais primos (e também maximais) de $\frac{D}{\mathcal{U}}$, o que implica que, em $\frac{D}{\mathcal{U}}$, temos

$$r(0) = \bigcap_{\mathcal{P} \text{ primo de } \frac{D}{\mathcal{U}}} \mathcal{P} = \bigcap_{i=1}^{s} \frac{\mathcal{M}_i}{\mathcal{U}} = \prod_{i=1}^{s} \frac{\mathcal{M}_i}{\mathcal{U}},$$

sendo esta última igualdade válida pela proposição 0.1. Ainda, como $\frac{D}{\mathcal{U}}$ é noetheriano, temos pela proposição 1.2.22 que $r(0)$ é nilpotente. Portanto $\exists t \in \mathbb{N}^*$ tal que $\left(\prod_{i=1}^{s} \frac{\mathcal{M}_i}{\mathcal{U}} \right)^t = (0)$, ou seja, $(\frac{\mathcal{M}_i}{\mathcal{U}})^t ..... (\frac{\mathcal{M}_s}{\mathcal{U}})^t = (0)$, ou ainda, $\frac{\mathcal{M}_i^t}{\mathcal{U}} ..... \frac{\mathcal{M}_s^t}{\mathcal{U}} = (0)$.

Agora, pelo lema 1.2.1 os ideais $\frac{\mathcal{M}_i^t}{\mathcal{U}}$ e $\frac{\mathcal{M}_j^t}{\mathcal{U}}$ são também comaximais quando $i \neq j$. Logo, pela proposição 0.2 temos que a aplicação

$$\varphi : \frac{D}{\mathcal{U}} \to \frac{\frac{D}{\mathcal{U}}}{\frac{\mathcal{M}_1^t}{\mathcal{U}}} \times ... \times \frac{\frac{D}{\mathcal{U}}}{\frac{\mathcal{M}_s^t}{\mathcal{U}}}$$

é sobrejetora e injetora, já que

$$\ker \varphi = \bigcap_{i=1}^{s} \frac{\mathcal{M}_i^t}{\mathcal{U}} = \prod_{i=1}^{s} \frac{\mathcal{M}_i^t}{\mathcal{U}} = (0).$$

Resta-nos portanto mostrar que $\frac{D}{\mathcal{M}_i^t}$ é finito, para cada $i \in \{1, ..., s\}$.

Como D é noetheriano, temos que $\frac{D}{\mathcal{M}_i^t}$ também é noetheriano e, como D tem dimensão um, temos que o único ideal primo (e maximal) de $\frac{D}{\mathcal{M}_i^t}$ é $\frac{\mathcal{M}_i}{\mathcal{M}_i^t}$ e portanto $\dim \frac{D}{\mathcal{M}_i^t} = 0$. Assim, $\frac{D}{\mathcal{M}_i^t}$ é também artiniano, pela proposição 1.2.28.

Afirmamos que $\frac{D}{\mathcal{M}_i^t}$ tem corpos de restos finitos. De fato, $\frac{D}{\mathcal{M}_i^t}$ tem um

único ideal maximal que é $\frac{\mathcal{M}_i}{\mathcal{M}_i^t}$. Portanto

$$\frac{\frac{D}{\mathcal{M}_i^t}}{\frac{\mathcal{M}_i}{\mathcal{M}_i^t}} \simeq \frac{D}{\mathcal{M}_i},$$

logo é finito pois por hipótese D tem corpos de restos finitos. Portanto pela proposição anterior temos que $\frac{D}{\mathcal{M}_i^t}$ é finito.

■

Definição 1.2.31: Definimos **norma** de um ideal $\mathcal{U}$ de um anel A como sendo o número $\#(\frac{A}{\mathcal{U}})$; a norma de um elemento $b \in A$ é definido por $\#\left(\frac{A}{\langle b\rangle}\right)$.

Notação: $n(\mathcal{U})$ para a norma do ideal $\mathcal{U}$ e $n(b)$ para a norma do elemento b.

O que a Proposição 1.2.30 nos diz então é que num domínio noetheriano de dimensão 1 com corpos de restos finitos todo ideal não nulo tem norma finita.

Proposição 1.2.32: Sejam A um anel e $b \in A$ não divisor de zero. Então para cada $a \in A$ a função $\sigma : \frac{A}{\langle a\rangle} \to \frac{\langle b\rangle}{\langle ab\rangle}$ é um isomorfismo de grupos, e $n(ab) = n(a).n(b)$.

Prova: Inicialmente observemos que $\langle ab\rangle \subseteq \langle b\rangle$ e portanto o quociente $\frac{\langle a\rangle}{\langle ab\rangle}$ faz sentido. Ainda, sabemos que os grupos $\frac{A}{\langle b\rangle}$ e $\frac{\frac{A}{\langle ab\rangle}}{\frac{\langle b\rangle}{\langle ab\rangle}}$ são isomorfos. Daí obtemos: $n(b)\#\frac{\langle b\rangle}{\langle ab\rangle} = n(ab)$.

Portanto se mostrarmos o isomorfismo entre $\frac{A}{\langle a\rangle}$ e $\frac{\langle b\rangle}{\langle ab\rangle}$, teremos $\#\frac{\langle b\rangle}{\langle ab\rangle} = n(a)$, e portanto $n(b).n(a) = n(ab)$.

Consideremos a aplicação:

$$\sigma : \frac{A}{\langle a\rangle} \to \frac{\langle b\rangle}{\langle ab\rangle}, \text{ definida por } \sigma(\bar{x}) = \overline{\overline{xb}}.$$

Afirmamos que σ está bem definida; de fato, dados $x, x' \in A$,

$$\bar{x} = \bar{x'} \Rightarrow x - x' \in \langle a\rangle \Rightarrow (x - x')b \in \langle ab\rangle \Rightarrow \overline{\overline{xb}} = \overline{\overline{x'b}}.$$

Ainda, como b não é divisor de zero temos que vale também a recíproca das afirmações acima, ou seja

$$\overline{\overline{xb}} = \overline{\overline{x'b}} \Rightarrow (x - x')b \in \langle ab\rangle \Rightarrow x - x' \in \langle a\rangle \Rightarrow \bar{x} = \bar{x'}.$$

Assim, σ é injetora. O resto da prova é fácil de ser feita.

■

Teorema 1.2.33: *Em um anel noetheriano A, o número de ideais com uma dada norma finita é finito.*

Prova: Seja $n \in \mathbb{N}^*$ fixado.

Como o número de anéis com n elementos não isomorfos entre si é finito, basta-nos mostrar que, fixado um anel R com n elementos, o conjunto de ideais de A, que denotaremos por $\{\mathcal{U}_\alpha\}_{\alpha \in I}$ para os quais $\frac{A}{\mathcal{U}_\alpha} \simeq R$ é finito, ou seja, que o conjunto I é finito.

Seja $\mathcal{U} = \bigcap_{\alpha \in I} \mathcal{U}_\alpha$. A mostrar: o número de ideais de A que contêm $\mathcal{U}$ é finito, pois daí teremos em particular que o número de ideais $\mathcal{U}_\alpha$ é finito.

Para tal consideramos o anel $B = \frac{A}{\mathcal{U}}$.

Pretendemos mostrar que o anel B é finito (pois daí tem um número finito de ideais e portanto o número de ideais de A que contêm $\mathcal{U}$ é finito).

Note que se o ideal $\mathcal{U}$ for maximal então está pronto pois $\mathcal{U}=\mathcal{U}_\alpha$ para todo $\alpha \in I$ e portanto I tem um único elemento.

Vamos então considerar o caso em que $\mathcal{U}$ não é maximal.

Para concluirmos que B é um anel finito, vamos utilizar a proposição 1.2.30, mostrando que B é artiniano e que todos os seus corpos de restos são finitos.

Observe que B é noetheriano pois $B = \frac{A}{\mathcal{U}}$ é quociente de anel noetheriano. Então, pela proposição 1.2.29, para mostrarmos que B é artiniano basta mostrar que $\dim B = 0$, ou seja, que todo ideal primo de B é maximal.

Resta-nos mostrar então que B tem dimensão de Krull zero e corpos de restos finitos.

Seja $\mathcal{P}$ um ideal primo de B. Afirmamos que $\frac{B}{\mathcal{P}}$ é um domínio finito (pois daí, como todo domínio finito é corpo, temos que $\mathcal{P}$ é um ideal maximal), e também que os corpos de restos são finitos.

Para mostrarmos que $\frac{B}{\mathcal{P}}$ é finito, consideremos inicialmente o homomorfismo de anéis:

$$\psi : B = \frac{A}{\mathcal{U}} \to \prod_{\alpha \in I} \frac{A}{\mathcal{U}_\alpha} \simeq \prod_{\alpha \in I} R \text{ dado por } \psi(u + \mathcal{U}) = (u + \mathcal{U}_\alpha)_{\alpha \in I}.$$

Tal homomorfismo está bem definido e é injetor, pois $\mathcal{U} \subseteq \mathcal{U}_\alpha$ para todo α e

$$\psi(u + \mathcal{U}) = 0 \Leftrightarrow \forall \alpha \in I,\ u \in \mathcal{U}_\alpha$$
$$\Leftrightarrow u \in \bigcap_{\alpha \in I} \mathcal{U}_\alpha = \mathcal{U} \Leftrightarrow u + \mathcal{U} = 0 + \mathcal{U}.$$

Agora, como R é finito, temos que R tem um número finito de ideais maximais, digamos, $\mathcal{M}_1, \ldots, \mathcal{M}_r$, e também que R é artiniano. Assim, pela Proposição 1.2.29,

temos que R é noetheriano e $\dim R = 0$ e $\mathcal{M}_1, ..., \mathcal{M}_r$ são também todos os ideais primos de R. Portanto, sendo $r(0)$ o nilradical de R, temos:

$$r(0) = \bigcap_{\mathcal{P} \text{ primos de } R} \mathcal{P} = \bigcap_{i=1}^{r} \mathcal{M}_i = \mathcal{M}_1 ..... \mathcal{M}_r.$$

Sendo R noetheriano, pela proposição 1.2.23 tal ideal é nilpotente, ou seja, existe s tal que

$$(0) = (\mathcal{M}_1, ..., \mathcal{M}_r)^s = \mathcal{M}_1^s, ..., \mathcal{M}_r^s.$$

Afirmamos agora que existe um polinômio mônico $p(X) \in \mathbb{Z}[X]$ que se anula em todos os elementos de R.

De fato, sendo R um anel finito, o anel $\frac{R}{\mathcal{M}_j}$ é também finito, digamos, com q_j elementos. Então:

$$\forall r \in R,\ r^{q_j} \equiv r \bmod(\mathcal{M}_j), \text{ ou seja, } \forall r \in R,\ r^{q_j} - r \in \mathcal{M}_j$$

e, portanto

$$\forall r \in R,\ \prod_{j=1}^{r} (r^{q_j} - r)^s \in \mathcal{M}_1^s ..... \mathcal{M}_r^s = (0).$$

Assim o polinômio mônico $p(X) = \prod_{j=1}^{r} (X^{q_j} - X)$ satisfaz $p(r) = 0$, para todo $r \in R$.

Segue daí que obtemos um polinômio $p(X) \in R[X]$ tal que, para todo $r \in \prod_{i \in I} R$, temos $p(r) = 0$.

Em particular, temos que para todo $b \in B$, $p(\psi(b)) = \psi(p(b)) = 0$ e, como ψ é injetora, concluimos que $p(b) = 0$ para todo $b \in B$. Portanto para todo ideal primo $\mathcal{P}$ de B temos que $\frac{B}{\mathcal{P}}$ é domínio, e ainda, $p(a + \mathcal{P}) = 0$ para todo $a + \mathcal{P} \in \frac{B}{\mathcal{P}}$.

Podemos então concluir que $\frac{B}{\mathcal{P}}$ é finito, logo um corpo, e portanto $\mathcal{P}$ é maximal.

Ainda, com a demonstração acima fica também demonstrado que todos os corpos de restos de B são finitos, o que completa a prova.

■

No capítulo 3 deste trabalho estaremos calculando a norma em vários tipos de anéis.

1.3 Valorizações

Definição 1.3.1: Dados um corpo K e um grupo abeliano totalmente ordenado $(\Gamma,+)$, uma aplicação $v : K^* \to \Gamma$ é dita uma **valorização** sobre K se, para todo $x,y \in K^*$ vale:

i) $v(xy) = v(x) + v(y)$;

ii) $v(x+y) \geqslant \min\{v(x), v(y)\}$.

Exemplo 1: Fazendo $K = \mathbb{Q}$, tomamos um elemento $p \in \mathbb{Z}$ primo; então cada elemento $x = \frac{b}{d} \in \mathbb{Q}^*$ pode ser escrito unicamente da forma $x = \frac{b}{d} = p^a \frac{y}{z}$, onde $a \in \mathbb{Z}$ e $mdc(y,p) = 1 = mdc(z,p)$. Definimos então a valorização $v_p : \mathbb{Q} \to \mathbb{Z}$ por $v_p(x) = a$, que é chamada **valorização p–ádica**.

Listamos a seguir vários resultados sobre valorizações, alguns sem demonstração. Maiores detalhes sobre o assunto podem ser encontrados em [R_1].

Proposição 1.3.2: *Dados um corpo K e uma valorização v sobre K, tem-se*:

i) $v(1) = 0$;

ii) $v(-x) = v(x)$;

iii) se $v(x) \neq v(y)$ *então* $v(x+y) = \min\{v(x), v(y)\}$;

iv) $v(x^{-1}) = -v(x)$.

Definição 1.3.3: Seja B um domínio, e K seu corpo de frações. Dizemos que B é um **anel de valorização** de K, se para cada $x \in K^*$, $x \in B$ ou $x^{-1} \in B$.

Proposição 1.3.4: *Um anel de valorização é um anel local, ou seja, possui um único ideal maximal.*

Lema 1.3.5: *Dados um corpo K e uma valorização v sobre o corpo K, o anel*

$$A_v = \{x \in K^* \mid v(x) \geqslant 0\} \cup \{0\}$$

é um anel de valorização do corpo K. O ideal maximal de A_v é dado por

$$M_v = \{x \in K^* \mid v(x) > 0\} \cup \{0\}$$

e portanto

$$U(A_v) = \{x \in K | v(x) = 0\}.$$

Definição 1.3.6: O anel A_v definido no lema acima é denominado **anel de valorização associado a** v.

Sejam Γ um grupo totalmente ordenado, D um domínio e $K = cf(D)$ o corpo de frações de D. Se $v : D^* \to \Gamma$ é uma função que satisfaz as condições (i) e (ii) da definição 1.3.1 pode-se estender v a $K^* = (cf(D))^*$ definindo $v(\frac{a}{b}) = v(a) - v(b)$ e daí teremos v uma valorização sobre K.

Exemplo 2: Fazendo $F = K(X) = cf(K[X])$ e fazendo uso da proposição 1.2.6, tome um polinômio irredutível $f \in K[X]$ e defina v_f como no exemplo 1.

Em geral,

Proposição 1.3.7: *Sejam D um DFU e $p \in D$ um elemento irredutível de D. Então a aplicação*

$$v_p : D^* \to \mathbb{N} \text{ dada por:}$$

$v_p(x) = s$, onde s é o expoente do elemento irredutível p que aparece na fatoração de x, satisfaz as condições (i) e (ii) da definição 1.3.1 *e portanto induz uma valorização sobre o corpo de frações de D.*

Prova: Se considerarmos $x,y \in D^*$ não invertíveis e tais que $x = ap^s$ e $y = bp^t$ com $p \nmid a$ e $p \nmid b$, então $v_p(x) = s$ e $v_p(y) = t$; daí

$$xy = ap^s bp^t \Rightarrow xy = abp^{s+t} \text{ e } p \nmid ab \Rightarrow v_p(xy) = s + t = v_p(x) + v_p(y).$$

E, se considerarmos, sem perda de generalidade, $t \leqslant s$, temos:

$$x + y = ap^s + bp^t \Rightarrow x + y = p^t(ap^{s-t} + b) \Rightarrow v_p(x + y) \geqslant t = \min\{v_p(x), v_p(y)\}.$$

■

Definição 1.3.8: *Seja D* um domínio de fatoração única. A valorização definida na proposição acima é chamada de **valorização** $p-ádica$ **de** D, ou **sobre o corpo de frações de** D.

Temos também que se D é um DFU vale:

Proposição 1.3.9: *Seja D um domínio de fatoração única e seja $\mathcal{M} = \langle p \rangle$ um ideal maximal de D. Então o anel de valorização associado a v_p é igual ao anel $D_{\mathcal{M}}$, anel de localização em $\mathcal{M}$.*

Prova: Temos que $D_{v_p} = \{x \in (cf(D))^* | v(x) \geqslant 0\} \cup \{0\}$, enquanto que

$D_{\mathcal{M}} = \{\frac{a}{b} | a \in D, b \in D \backslash \mathcal{M}\}$.

Tomemos $x \in D_{v_p}$, não nulo, da forma $x = \frac{a}{b}$ com $a, b \in D$ e $mdc(a,b) = 1$. Daí:

$$v_p(x) \geqslant 0 \Rightarrow v_p\left(\frac{a}{b}\right) \geqslant 0$$
$$\Rightarrow v_p(a) - v_p(b) \geqslant 0$$
$$\Rightarrow v_p(a) \geqslant v_p(b).$$

Daí, como estamos supondo $mdc(a,b) = 1$, temos necessariamente $v_p(b) = 0$; logo $b \notin \mathcal{M}$ e portanto $x \in D_{\mathcal{M}}$. Assim, $D_{v_p} \subseteq D_{\mathcal{M}}$.

Reciprocamente, se $x \in D_{\mathcal{M}} - \{0\}$ então temos que x se escreve como $x = \frac{a}{b}$ com $a \in D^*$ (pois $x \neq 0$) e $b \notin D \backslash \mathcal{M}$ e portanto $v_p(b) = 0$, enquanto que $v_p(a) \geqslant 0$. Daí $v_p(x) = v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b) = v_p(a) \geqslant 0$.

Assim, $D_{\mathcal{M}} \subseteq D_{v_p}$.

■

Reenunciamos portanto a proposição 1.2.16:

Corolário 1.3.10: *Se D é um domínio a ideais principais e $\{\mathcal{M}_\alpha\}_{\alpha \in I}$ denota a família de ideais maximais de D, digamos, $\mathcal{M}_\alpha = \langle p_\alpha \rangle$, com p_α irredutível em D para todo $\alpha \in I$, então:*

$$\bigcap_{\alpha \in I} D_{v_{p_\alpha}} = \bigcap_{\alpha \in I} D_{\mathcal{M}_\alpha} = D.$$

Definição 1.3.11: Uma valorização é dita uma **valorização discreta (de posto 1)** se o conjunto imagem da valorização for o conjunto $\mathbb{Z}$.

Um domínio D é um **anel de valorização discreta** se existe uma valorização discreta definida em $K = cf(D)$ cujo anel de valorização associado é D.

Se A é um anel de valorização associado a uma valorização discreta v então, dado $x \in A$ satisfazendo $x \neq 0$ e $v(x) = k$, temos, para $y \in A$,

$$v(y) \geqslant k = v(x) \Rightarrow$$
$$v(\tfrac{y}{x}) = v(y) - v(x) \geqslant 0 \Rightarrow$$
$$\tfrac{y}{x} \in A \Rightarrow$$
$$y = \tfrac{y}{x} x \in \langle x \rangle.$$

Daí, dado um ideal $\mathcal{U} \neq (0)$ de A, tomando $x \in \mathcal{U}$ tal que $x \neq 0$ e $v(x)$ é o menor

elemento de $v(\mathcal{U}) \subseteq \mathbb{N}$, teremos $\mathcal{U} = \langle x \rangle$, pois

$$y \in \mathcal{U} \Rightarrow v(y) \geqslant v(x) \Rightarrow y \in \langle x \rangle.$$

Portanto A é um domínio principal e portanto noetheriano.

Afirmamos também que A tem dimensão de Krull igual a um. De fato, seja $\mathcal{P}$ um ideal primo não nulo de A, digamos, $\mathcal{P} = \langle x \rangle$. Seja $\mathcal{M} = \langle y \rangle$ um ideal maximal de A que contém $\mathcal{P}$. Então

$$x \in \mathcal{P} \subseteq \mathcal{M} = \langle y \rangle \Rightarrow x = ya \in \mathcal{P},$$

para algum $a \in A$. Daí, como $\mathcal{P}$ é ideal primo temos que $y \in \mathcal{P}$ ou $a \in \mathcal{P}$.

Se $a \in \mathcal{P} = \langle x \rangle$ um simples cálculo nos permite concluir que $y \in U(A)$, absurdo pois y é irredutível.

Logo $y \in \mathcal{P}$ e portanto $\mathcal{P} = \mathcal{M}$.

Provamos assim que todo anel de valorização associado a uma valorização discreta é noetheriano (até principal) e tem dimensão de Krull igual a um.

1.4 Anel de Inteiros Algébricos

Neste parágrafo faremos algumas considerações sobre extensões algébricas e definiremos a norma de um elemento algébrico e provaremos que ela coincide com a norma definida em 1.2.32.

Sejam K, L corpos com L uma extensão finita de K, digamos, $[L : K] = n$, e dado um $K-$ operador linear P sobre L, podemos cosiderar a matriz de P em relação a alguma base de L. Denotando tal matriz por, $(a_{ij})_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant n}}$, define-se **a norma** de P como sendo

$$N(P) = \det(a_{ij}),$$

e o **traço** de P como

$$TrP = \sum_{i=1}^{n} a_{ii}$$

e, ainda, o **polinômio característico** de P como

$$p(X) = \det(X.I_L - P),$$

onde por I_L denotamos o operador identidade sobre L.

Mostra-se que

$$\det(X.I_L - P) = X^n - (TrP)X^{n-1} + ... + (-1)^n N(P).$$

Definição 1.4.1: Seja $L|K$ uma extensão finita e separável de corpos, e seja $\widetilde{K}$ um fecho algébrico de K que contém L. Dado $x \in L$ definimos **a norma de** x (respectivamente o **polinômio característico de** x) **com respeito à extensão** $L|K$ como sendo a norma (respectivamente o polinômio característico) do operador linear "multiplicação por x sobre L", que denotaremos por P_x.

Notação: $N_{L|K}(x)$ para a norma de x.

Pode-se mostrar que a norma possui as seguintes propriedades:

i) $x \in K \Rightarrow N_{L|K}(x) = x^{[L:K]}$;

ii) a norma é multiplicativa: $N_{L|K}(xy) = N_{L|K}(x)N_{L|K}(y)$.

Definição 1.4.2: Sejam K,L corpos com L extensão de K e seja $\alpha \in L$. Consideremos o homomorfismo de anéis dado por:

$$\Psi : K[X] \to L \text{ e definido por: } \Psi(f(X)) = f(\alpha).$$

Se α é algébrico sobre K então o ideal $Ker(\Psi)$ é um ideal principal gerado por um polinômio não nulo e irredutível $p(X)$ que podemos supor mônico. Portanto para todo polinômio $g(X) \in K[X]$ tal que $g(\alpha) = 0$ teremos que $p(X)|g(X)$ em $K[X]$. Este polinômio $p(X)$ é chamado de **polinômio minimal de** α e, será denotado por $p_{\alpha|K}(X)$;

Proposição 1.4.3: *Sejam K um corpo de característica zero, L uma extensão algébrica de grau n sobre K, α um elemento de L, e $x_1, x_2, ..., x_n$ as raizes distintas do polinômio minimal de α sobre K. Então*

$$N_{L|K}(\alpha) = x_1 x_2 .... x_n.$$

Prova: Veja [S$_1$] página 44.

Proposição 1.4.4: *Sejam K um corpo de característica zero, L uma extensão algébrica de grau n sobre K, $\alpha \in L$. Então o polinômio característico de α com respeito à extensão $[L : K]$ é a potência $[L : K[\alpha]]$ do polinômio minimal de α sobre K.*

Prova: Veja também [S$_1$] página 44.

Definição 1.4.5: Um corpo K é dito um **corpo de números algébricos** se for uma extensão finita de $\mathbb{Q}$. Neste caso, todo elemento de K é dito um **número algébrico**.

Definição 1.4.6: Seja $K|\mathbb{Q}$ uma extensão finita (e portanto algébrica de $\mathbb{Q}$), e seja I_K o fecho inteiro de $\mathbb{Z}$ em K, isto é,

$$I_K = \{\alpha \in K \mid \alpha \text{ é raiz de algum polinômio mônico } f(X) \in \mathbb{Z}[X]\}$$

O conjunto I_K é chamado de **anel dos inteiros algébricos de** K e $\alpha \in I_K$ é dito um **inteiro algébrico**.

É claro que todo elemento inteiro é um número algébrico.

Observação: Como $\mathbb{Z}$ é inteiramente fechado, é claro que $I_K \cap \mathbb{Q} = \mathbb{Z}$.

Relembramos agora alguns fatos sobre anéis de inteiros algébricos que nos serão úteis no capítulo 3.

Em todo o restante desta seção K denotará uma extensão finita de $\mathbb{Q}$, e denotaremos $N_{K|\mathbb{Q}}(\alpha)$ por $N(\alpha)$.

Lema 1.4.7: *Para todo* $\alpha \in K$ *existe* $m \in \mathbb{Z}^*$ *tal que* $m\alpha \in I_K$.

Prova: Consideremos o polinômio minimal $p_{\alpha|\mathbb{Q}}(X) \in \mathbb{Q}[X]$:

$$p_{\alpha|\mathbb{Q}}(X) = \frac{a_0}{b_0} + \frac{a_1}{b_1}X + \frac{a_2}{b_2}X^2 + \frac{a_3}{b_3}X^3 + \ldots + \frac{a_{n-1}}{b_{n-1}}X^{n-1} + X^n.$$

Consideramos $m = b_0 b_1 b_2 \ldots b_{n-1}$; então para todo i, $\frac{m}{b_i} \in \mathbb{Z}$. Daí

$$m^n p_{\alpha|\mathbb{Q}}(X) = a_0 b_0^{n-1} b_1^n b_2^n \ldots b_{n-1}^n + a_1 b_0^n b_1^{n-1} b_2^n \ldots b_{n-1}^n X + \ldots + a_{n-1} b_0^n b_1^n b_2^n \ldots b_{n-1}^{n-1} X^{n-1} + m^n X^n.$$

Considerando agora $c_i = \frac{m}{b_i} a_i m^{n-i-1} \in \mathbb{Z}$ para $1 \leqslant i \leqslant n-1$, temos

$$m^n p_{\alpha|\mathbb{Q}}(X) = c_0 m^0 + c_1(mX) + c_2(mX)^2 + c_3(mX)^3 + \ldots + c_{n-1}(mX)^{n-1} + (mX)^n$$

com $c_i \in \mathbb{Z}$.

Daí, como α é raiz do polinômio minimal, temos que:

$$0 = m^n p_{\alpha|\mathbb{Q}}(\alpha) = c_0 m^0 + c_1(m\alpha) + c_2(m\alpha)^2 + c_3(m\alpha)^3 + \ldots + c_{n-1}(m\alpha)^{n-1} + (m\alpha)^n.$$

Assim, temos que $m\alpha \in K$ é raiz do polinômio mônico

$$c_0 m^0 + c_1 X + c_2 X^2 + c_3 X^3 + \ldots + c_{n-1} X^{n-1} + X^n \in \mathbb{Z}[X]$$

e portanto $m\alpha \in I_K$.

■

Proposição 1.4.8: *Se* $\alpha \in I_K$ *então o polinômio minimal de* α *sobre* $\mathbb{Q}$ *(que denotamos por* $p_{\alpha|\mathbb{Q}}(X)$*) já tem coeficientes inteiros.*

Prova: Se $\alpha \in I_K$ então, por definição, existe $g(X) \in \mathbb{Z}[X]$ mônico e tal que $g(\alpha) = 0$; mas α é também algébrico. Assim, como $\mathbb{Z}[X] \subset \mathbb{Q}[X]$ temos que existe

$f(X) \in \mathbb{Q}[X]$ tal que

$$g(X) = p_{\alpha|\mathbb{Q}}(X)f(X).$$

Seja $p_{\alpha|\mathbb{Q}}(X) = \prod_{i=1}^{n}(X - x_i)$ a decomposição de $p_{\alpha|\mathbb{Q}}(X)$ em $\widetilde{K}[X]$ e seja $L = K(x_1,...,x_n)$. Temos então que

$$g(X) = \prod_{i=1}^{n}(X - x_i)f(X).$$

Como $x_1,...,x_n$ são raízes do polinômio $g(X) \in \mathbb{Z}[X]$ temos que $x_1,...,x_n \in I_L$. Ora, os coeficientes de $p_{\alpha|\mathbb{Q}}(X)$ são somas de produtos de suas raízes, logo são elementos também de I_L. Logo

$$p_{\alpha|\mathbb{Q}}(X) \in I_L[X] \cap \mathbb{Q}[X] = (I_L \cap \mathbb{Q})[X] = \mathbb{Z}[X].$$

Análogo resultado serve para $f(X)$.

■

Corolário 1.4.9: *Se $\alpha \in I_K$ então $N(\alpha) \in \mathbb{Z}$.*

Prova: Sabemos que $\pm N(\alpha)$ é o termo independente do polinômio característico de α, que por sua vez, é uma potência do polinômio minimal de α. (Proposição 1.4.4). Portanto, pela proposição acima, é um número inteiro.

■

Corolário 1.4.10: *Se $\alpha \in I_K$ então $\alpha \in U(I_K) = \{$inversíveis de $I_K\}$ se e só se* $N(\alpha) = \pm 1$.

Prova: Se $\alpha \in U(I_K)$ então existe $\beta \in I_K$ tal que $\alpha\beta = 1$; então $N(\alpha\beta) = 1$ e, como a norma é multiplicativa, temos que $N(\alpha)N(\beta) = 1$. Agora, como $N(\alpha), N(\beta) \in \mathbb{Z}$ temos que $N(\alpha) = \pm 1$.

Reciprocamente, suponhamos que $N(\alpha) = \pm 1$. Sabemos que o polinômio característico de α é dado por $X^n - (Tr\alpha)X^{n-1} + ... + (-1)^n N(\alpha)$ e é uma potência do polinômio minimal de α, o qual, pela proposição 1.4.8, tem coeficientes em $\mathbb{Z}$, digamos

$$X^n + b_{n-1}X^{n-1} + ... + b_1X \pm 1 = 0, \text{ com } b_i \in \mathbb{Z}.$$

Portanto, temos

$$\alpha^n + b_{n-1}\alpha^{n-1} + ... + b_1\alpha \pm 1 = 0$$

donde

$$(\alpha^{n-1} + b_{n-1}\alpha^{n-2} + ... + b_1)\alpha = \pm 1$$

e portanto $\pm(\alpha^{n-1} + b_{n-1}\alpha^{n-2} + ... + b_1)$ é o inverso de α, e é um elemento de I_K. Logo $\alpha \in U(I_K)$.

■

Teorema 1.4.11: *Se $K|\mathbb{Q}$ é uma extensão finita de grau n então I_K é um $\mathbb{Z}$-módulo livre de posto n, e também todo $\mathbb{Z}$-submódulo de I_K é livre e de posto menor ou igual a n. Ainda, fixado um $\mathbb{Z}$-submódulo de I_K de posto q existe uma base $\{e_1, ..., e_n\}$ de I_K e existem inteiros não nulos $c_1, ..., c_q$ tais que*

$$\{c_1e_1, ..., c_qe_q\}$$

é uma base para tal submódulo.

Prova: Veja Teorema 1 página 47 em [S_1], seu corolário e Teorema 1 página 26 em [S_1].

Definição 1.4.12: Se $K|\mathbb{Q}$ é uma extensão finita de grau 2 então dizemos que K é uma **extensão quadrática de** $\mathbb{Q}$ ou um **corpo quadrático**.

Definição 1.4.13: Um inteiro $d \neq 1$ é dito **sem fatores quadráticos** ou **livre de quadrados** se não existe um primo p tal que $p^2|d$

Exemplo 1.4.14: Se $d \in \mathbb{Z}$ não é um quadrado perfeito (por exemplo, d livre de quadrados), então $K = \mathbb{Q}(\sqrt{d})$ é uma extensão quadrática de $\mathbb{Q}$. De fato, $\sqrt{d}$ é raiz do polinômio $X^2 - d \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$, e como d não é um quadrado perfeito temos que $X^2 - d$ é irredutível sobre que, sendo portanto o polinômio minimal de $\sqrt{d}$ sobre $\mathbb{Q}$.

Teorema 1.4.15: *Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$, onde d é um inteiro sem fatores quadráticos.*

Prova: Se K é um corpo quadrático, todo elemento α de $K - \mathbb{Q}$ é de grau 2 sobre $\mathbb{Q}$, e é portanto um elemento primitivo de K (isto é $K = \mathbb{Q}(\alpha)$ e $\{1, \alpha\}$ é uma base de K sobre $\mathbb{Q}$). Seja $f(X) = X^2 + bX + c$ ($b, c \in \mathbb{Q}$) o polinômio minimal de um tal elemento α. A resolução da equação de segundo grau $\alpha^2 + b\alpha + c = 0$ nos dá $2\alpha = -b \pm \sqrt{b^2 - 4c}$. Desta forma temos que $K = \mathbb{Q}[\sqrt{b^2 - 4c}]$.

Reciprocamente, se d é livre de quadrados então, pelo exemplo acima, $\mathbb{Q}(\sqrt{d})$ é uma extensão quadrática de $\mathbb{Q}$.

■

Definição 1.4.16: Dado um corpo quadrático $K = \mathbb{Q}(\sqrt{d})$ dizemos que K é:

- **um corpo quadrático real** se $d > 0$;

- **um corpo quadrático imaginário** se $d < 0$.

Teorema 1.4.17: *Seja* $d \in \mathbb{Z}$ livre de quadrados e seja $K = \mathbb{Q}(\sqrt{d})$. *Então*:

i) $Aut_{\mathbb{Q}}(K)$ *só possui dois elementos*: id_K *e* σ, *onde* σ *é o automorfismo conjugação (em relação à irracionalidade quadrática* $\sqrt{d}$), ou seja:

$$\forall r,s \in \mathbb{Q},\ \sigma(r+s\sqrt{d}) = r - s\sqrt{d};$$

ii) se $\alpha = r+s\sqrt{d}$ *com* $r,s \in \mathbb{Q}$ *e* $s \neq 0$ *então*

$$p_{\alpha|\mathbb{Q}}(X) = X^2 - 2rX + (r^2 - ds^2)$$

e portanto, temos $N(\alpha) = r^2 - ds^2$;

iii) $\alpha = r+s\sqrt{d} \in I_K$ *se e só se*

$$2r \in \mathbb{Z} \quad \text{e} \quad r^2 - ds^2 \in \mathbb{Z};$$

iv) se d é congruente a 2 *ou* 3 *módulo* 4 *então*

$$I_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$$

e, se d é congruente a 1 *módulo* 4 *então*

$$I_K = \{\tfrac{z_1}{2} + \tfrac{z_2}{2}\sqrt{d} \mid z_1,z_2 \in \mathbb{Z} \text{ e são de mesma paridade}\}$$
$$= \mathbb{Z} + \mathbb{Z}\tfrac{1+\sqrt{d}}{2};$$

v) I_K *é um* $\mathbb{Z}$*-módulo livre, de base*

$$\{1, \sqrt{d}\},\ \text{se } d \equiv 2 \text{ ou } 3 (\mathrm{mod}\, 4)$$
$$\text{e } \{1, \tfrac{1+\sqrt{d}}{2}\},\ \text{se } d \equiv 1 (\mathrm{mod}\, 4).$$

Prova: Para provar o item (*i*) observamos que o elemento $\sqrt{d}$ é raiz do polinômio irredutível $X^2 - d$ e admite um conjugado em K, a saber: $-\sqrt{d}$. Existe, então além da identidade, apenas mais um automorfismo σ de K, a saber, o que aplica $\sqrt{d}$ em $-\sqrt{d}$, ou seja,

$$\sigma(r+s\sqrt{d}) = r - s\sqrt{d}.$$

Para a prova do item (*ii*) vemos que α é claramente raiz do polinômio

$$(X-\alpha)(X-\sigma(\alpha)) = X^2 - 2rX + (r^2 - ds^2) \in \mathbb{Q}[X],$$

e como $(X-\alpha) \notin \mathbb{Q}[X]$ pois $s \neq 0$, podemos concluir que

$$p_{\alpha|\mathbb{Q}}(X) = X^2 - 2rX + (r^2 - ds^2).$$

O item (*iii*) é conseqüência de (*ii*) e da proposição 1.4.8.

Provemos agora o item (*iv*). É claro que $\mathbb{Z} + \mathbb{Z}\sqrt{d} \subseteq I_K$ pois cada $r + s\sqrt{d}$ com $r,s \in \mathbb{Z}$ é raiz do polinômio mônico $X^2 - 2rX + r^2 - ds^2 \in \mathbb{Z}[X]$. Inicialmente observe que por (*iii*) temos

$$\begin{aligned} \alpha = r + s\sqrt{d} \in I_K &\Rightarrow 2r \in \mathbb{Z} \quad \text{e} \quad r^2 - ds^2 \in \mathbb{Z} \\ &\Rightarrow (2r)^2 - 4(r^2 - ds^2) \in \mathbb{Z} \\ &\Rightarrow (2s)^2 d \in \mathbb{Z}. \end{aligned}$$

Como d é livre de quadrados, não há como ser simplificado o denominador de s, caso ele não seja ± 1. Concluimos assim que $2s \in \mathbb{Z}$, e portanto

$$\begin{aligned} &\alpha = r + s\sqrt{d} \in I_K \\ \Rightarrow u = 2r \in \mathbb{Z} \quad &\text{e} \quad v = 2s \in \mathbb{Z} \quad \text{e} \quad r^2 - ds^2 \in \mathbb{Z}, \end{aligned}$$

ou seja:

$$\alpha \in I_K \Rightarrow \alpha = \tfrac{u}{2} + \tfrac{v}{2}\sqrt{d},$$

onde $u, v \in \mathbb{Z}$ são tais que $u^2 - dv^2 \in 4\mathbb{Z}$, isto é, $u^2 \equiv dv^2 (\mathrm{mod}\, 4)$.

Como d é livre de quadrados, temos que nunca ocorre $d \equiv 0(\mathrm{mod}\, 4)$. Ainda, como $u^2 \equiv 0$ ou $1(\mathrm{mod}\, 4)$, temos

$$\begin{aligned} &u^2 \equiv 1(\mathrm{mod}\, 4) \\ \Leftrightarrow\ &v^2 \text{ não é congruente a } 0(\mathrm{mod}\, 4) \\ \Leftrightarrow\ &v^2 \equiv 1(\mathrm{mod}\, 4). \end{aligned}$$

Assim

$$u^2 \equiv 0(\mathrm{mod}\, 4) \Leftrightarrow v^2 \equiv 0(\mathrm{mod}\, 4)$$

ou seja, u e v são de mesma paridade. Portanto, provamos que

$$\begin{aligned} I_K &\subseteq \{\tfrac{z_1}{2} + \tfrac{z_2}{2}\sqrt{d} \mid z_1, z_2 \in \mathbb{Z} \text{ e são de mesma paridade}\} \\ &= \mathbb{Z} + \mathbb{Z}\tfrac{1+\sqrt{d}}{2} \end{aligned}$$

Afirmamos que se $d \equiv 1(\mathrm{mod}\, 4)$ então a inclusão acima é até uma igualdade. De fato, se $\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d}$ com $m,n \in \mathbb{Z}$ de mesma paridade então:

$$\begin{aligned} &2\alpha = m + n\sqrt{d} \\ \Rightarrow\ &2\alpha - m = n\sqrt{d} \\ \Rightarrow\ &4\alpha^2 - 4\alpha m + m^2 = dn^2 \\ \Rightarrow\ &\alpha^2 - \alpha m + \tfrac{m^2 - dn^2}{4} = 0. \qquad (*) \end{aligned}$$

Daí como m e n têm mesma paridade, temos:

-m,n pares, digamos, $m = 2u$ e $n = 2v$,

$$m^2 - dn^2 = 4u^2 - 4dv^2 \in 4\mathbb{Z}$$
$$\Rightarrow \frac{m^2-dn^2}{4} \in \mathbb{Z}$$

e portanto, por $(*)$, α é raiz de um polinômio mônico de grau 2 com coeficientes inteiros, ou seja, $\alpha \in I_K$.

-m,n ímpares, digamos, $m = 2u + 1$ e $n = 2v + 1$,

$$m^2 - dn^2 = 4u^2 + 4u + 1 - d(4v^2 + 4v + 1)$$
$$= 4(u^2 - dv^2 + u - dv) + 1 - d$$

e como $d \equiv 1(\mathrm{mod}4)$, temos $1 - d \in 4\mathbb{Z}$, e portanto novamente

$$\frac{m^2-dn^2}{4} \in \mathbb{Z},$$

donde por $(*)$ temos $\alpha \in I_K$.

Note agora que:

-$d \equiv 2(\mathrm{mod}4) \Rightarrow dv^2$ é par $\Rightarrow u^2$ é par $\Rightarrow u$ é par e v é par

$$\Rightarrow \alpha = \frac{u}{2} + \frac{v}{2}\sqrt{d} \in \mathbb{Z} + \mathbb{Z}[\sqrt{d}].$$

-$d \equiv 3(\mathrm{mod}4)$ e v é ímpar $\Rightarrow d \equiv 3(\mathrm{mod}4)$ e

$$v^2 \equiv 1(\mathrm{mod}4) \Rightarrow u^2 \equiv dv^2 \equiv 3(\mathrm{mod}4),$$

absurdo.

Assim, concluimos que se $d \equiv 3(\mathrm{mod}4)$ então necessariamente v (e portanto também u) são pares.

Daí novamente $\alpha = \frac{u}{2} + \frac{v}{2}\sqrt{d} \in \mathbb{Z} + \mathbb{Z}[\sqrt{d}]$, comprovando que nos casos $d \equiv 2(\mathrm{mod}4)$ e $d \equiv 3(\mathrm{mod}4)$ temos

$$I_K = \mathbb{Z} + \mathbb{Z}[\sqrt{d}]$$

A prova do item (v) é clara.

■

Teorema 1.4.18: *Seja $K = \mathbb{Q}(\sqrt{d})$ com $d < 0$ e livre de quadrados. Então:*

a) Para $d = -1$, temos $U(I_K) = \{\pm 1, \pm i\}$;

b) Para $d = -3$, $U(I_K) = \{\pm 1, \xi, \xi^2, \xi^4, \xi^5\}$ onde ξ é a raiz sexta complexa da unidade $\xi = \frac{1+\sqrt{-3}}{2}$;

c) Para $d \neq \{-1, -3\}$ temos $U(I_K) = \{\pm 1\}$.

Prova: Notamos inicialmente que pela proposição anterior, para

$\alpha = r + s\sqrt{d} \in K$ temos $N(\alpha) = r^2 - ds^2 = r^2 + |d|s^2 \geqslant 0$.

Consideremos primeiro o caso em que $d \equiv 2(\mathrm{mod}\,4)$ ou $d \equiv 3(\mathrm{mod}\,4)$. Por (iv) da proposição anterior temos que todo elemento $\alpha \in I_K$ é da forma $m + n\sqrt{d}$, com $m, n \in \mathbb{Z}$, e por 1.4.10, teremos que

$$\alpha \in U(I_K) \Leftrightarrow m^2 + n^2|d| = 1. \qquad (*)$$

Quando $d = -1$, $(*)$ ocorrerá se e somente se

$$(m,n) \in \{(1,0),(0,1),(-1,0),(0,-1)\} \Leftrightarrow \alpha \in \{1, i, -1, -i\}.$$

Isto prova o item (a).

Quando $d \neq -1$, $(*)$ ocorrerá se e somente se

$$(m,n) \in \{(1,0),(-1,0)\} \Leftrightarrow \alpha \in \{1,-1\}.$$

No caso em que $d \equiv 1(\mathrm{mod}\,4)$, os elementos $\alpha \in I_K$ são da forma $\frac{m}{2} + \frac{n}{2}\sqrt{d}$, com $m, n \in \mathbb{Z}$, satisfazendo, $m \equiv n(\mathrm{mod}\,2)$. Novamente usando 1.4.10 temos que

$$\alpha \in U(I_K) \Leftrightarrow \frac{m^2}{4} + \frac{n^2}{4}|d| = 1,$$

ou seja,

$$m^2 + n^2|d| = 4. \qquad (**)$$

Quando $d \neq -3$, $(**)$ ocorrerá se e somente se

$$(m,n) \in \{(2,0),(-2,0)\} \Leftrightarrow \alpha \in \{1,-1\}.$$

Quando $d = -3$ $(**)$ ocorrerá se e somente se

$$(m,n) \in \{(2,0),(1,1),(-1,1),(-2,0),(-1,-1),(1,-1)\} \Leftrightarrow$$

$$\Leftrightarrow \alpha \in \left\{1, \frac{1+\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, -1, \frac{-1-\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}\right\}.$$

Note que estes elementos são as potências da raiz sexta complexa da unidade $\xi = \frac{1+\sqrt{-3}}{2}$.

■

A proposição a seguir nos mostra que a norma definida nesta seção coincide com a norma definida na seção 2 (veja definição 1.2.32).

Proposição 1.4.19: *Seja K um corpo de números algébricos e suponhamos $[K : \mathbb{Q}] = n$. Se α é um elemento não nulo de I_K, tem-se que $|N(\alpha)| = \#\left(\frac{I_K}{\langle\alpha\rangle}\right)$.*

Prova: Notemos inicialmente que, pelo corolário 1.4.9, temos $N(\alpha) \in \mathbb{Z}$, e portanto faz sentido tentar provar que $|N(\alpha)| = \#\left(\frac{I_K}{\langle\alpha\rangle}\right)$.

Pelo teorema 1.4.11, sabemos que I_K é um $\mathbb{Z}$-módulo livre de posto n. Dado $\alpha \in I_K$, temos que a aplicação multiplicação por α é um isomorfismo entre I_K e $\langle\alpha\rangle$. Assim, o

submódulo $\langle\alpha\rangle$ é também um $\mathbb{Z}$-módulo livre de posto n. Então, novamente pelo teorema 1.4.11, temos que existe uma base $\{e_1,...,e_n\}$ de I_K e existem inteiros não nulos $c_1,...,c_n$ tais que $\{c_1e_1,c_2e_2,...,c_ne_n\}$ é uma base de $\langle\alpha\rangle$. Ou seja,

$$\langle\alpha\rangle = \mathbb{Z}c_1e_1 \oplus ... \oplus \mathbb{Z}c_ne_n.$$

Suponhamos sem perda de generalidade, que $c_1,...,c_n \in \mathbb{N}^*$. É fácil ver que a alicação

$$\varphi : I_K \to \frac{\mathbb{Z}}{\langle c_1\rangle} \times ... \times \frac{\mathbb{Z}}{\langle c_n\rangle}$$

$$r_1e_1 + ... + r_ne_n \mapsto (r_1 + c_1\mathbb{Z},...,r_n + c_n\mathbb{Z})$$

é um homomorfismo de $\mathbb{Z}$-módulos sobrejetor e cujo núcleo é precisamente $\mathbb{Z}c_1e_1 \oplus ... \oplus \mathbb{Z}c_ne_n = \langle\alpha\rangle$. Assim, existe um isomorfismo de $\mathbb{Z}$-módulos entre $\frac{I_K}{\langle\alpha\rangle}$ e $\prod_{i=1}^{n} \frac{\mathbb{Z}}{\langle c_i\rangle}$. Daí:

$$\#\left(\frac{I_K}{\langle\alpha\rangle}\right) = \#\left(\prod_{i=1}^{n} \frac{\mathbb{Z}}{\langle c_i\rangle}\right) = c_1.c_2.....c_n.$$

Queremos agora calcular $N(\alpha)$, ou seja, o determinante da matriz do operador m_α, multiplicação por α. Observe inicialmente que:

(*i*) $\{\alpha e_1,...,\alpha e_n\}$ é também uma base de $\langle\alpha\rangle$. De fato:

$$\langle\alpha\rangle \text{ é ideal de } I_K \quad \text{e} \quad e_1,...,e_n \in I_K$$

$$\Rightarrow \mathbb{Z}\alpha e_1 + ... + \mathbb{Z}\alpha e_n \subseteq \langle\alpha\rangle.$$

Ainda, para $i \in \{1,...,n\}$,

$$c_ie_i \in \langle\alpha\rangle$$

$$\Rightarrow c_ie_i = \alpha u, \text{ com } u \in I_K = \mathbb{Z}e_1 + ... + \mathbb{Z}e_n$$

$$\Rightarrow c_ie_i \in \alpha(\mathbb{Z}e_1 + ... + \mathbb{Z}e_n) = \mathbb{Z}\alpha e_1 + ... + \mathbb{Z}\alpha e_n$$

Daí temos um automorfismo linear $\nu : \langle\alpha\rangle \to \langle\alpha\rangle$ induzido por $\nu(c_ie_i) = \alpha e_i$;

(*ii*) o operador linear $\mu : I_K \to I_K$ induzido por $\mu(e_i) = c_ie_i$, $i = 1,...,n$, tem imagem $\langle\alpha\rangle$;

(*iii*) o operador $m_\alpha : I_K \to I_K$ "multiplicação por α" satisfaz $m_\alpha = \nu \circ \mu$.

Logo, $N(\alpha) = \det(m_\alpha) = \det(\nu).\det(\mu)$.

Mas, observamos agora que $\det(\nu)$ é um número inteiro invertível e, portanto $\det(\nu) = \pm 1$. Temos também que $\det(\mu) = c_1.....c_n$ e, assim, obtemos

$$N(\alpha) = \pm 1c_1.....c_n.$$

Assim, temos que de fato $|N(\alpha)| = \#\left(\frac{I_K}{\langle\alpha\rangle}\right)$.

■

Para obter maiores informações sobre esta seção indicamos [S_1], [S-T], [E] e [H-W].

Capítulo 2

ANÉIS EUCLIDIANOS E SUAS PROPRIEDADES ELEMENTARES

2.1 Definição usual de domínio euclidiano e comentários

Definição 2.1.1: A definição usual de um domínio Euclidiano é a de que D é um domínio com uma aplicação $\varphi : D \to \mathbb{N}$ tal que:

(1) $\forall\, a,b \in D^*$, $\varphi(ab) \geq \varphi(a)$;

(2) dados $a,b \in D$, com $b \neq 0$, existem q e r em D tais que $a = bq + r$ e $\varphi(r) < \varphi(b)$.

Façamos inicialmente alguns comentários a este respeito:

a) Alguns autores (por exemplo [G-L]) definem domínio euclidiano exigindo apenas que exista $\sigma : D^* \to \mathbb{N}$ que satisfaça (1) e (2).

Note que, definindo $\varphi' : D \to \mathbb{N}$ por

$$\varphi'(d) = \begin{cases} 0, \text{ se } d = 0 \\ \varphi(d) + 1, \text{ se } d \neq 0, \end{cases}$$

teremos que φ' satisfaz (1) e (2), de modo que as duas definições são equivalentes.

b) A condição anel "com unidade" é dispensável na definição, mas acaba sendo necessária. De fato, em [H] não se trabalha apenas com anéis com unidade, e define-se anel euclidiano como sendo um anel comutativo R sem divisores de zero para o qual existe $\psi : R \to \mathbb{N}$ que satisfaz (1) e

(2') $\forall a,b \in R^*$, existem $q,r \in R$ tais que $a = bq + r$ com $r = 0$ ou $\psi(r) < \psi(b)$.

Inicialmente note que o caso $a = 0$ poderia muito bem ter sido incluido nesta condição, pois basta-nos tomar $q = r = 0$. Além disso, em [H] prova-se que todo anel euclidiano tem unidade, de modo que temos afinal que anel euclidiano em [H] é um domínio que satisfaz (1) e (2'), ou seja, em [H] a definição poderia ter sido desde o início a mesma que em [G-L].

c) Por que exige-se ainda em (2) que b seja diferente de zero?

Para consistência da própria condição: note que se a queremos válida mas incluimos a possibilidade $b = 0$ então, se tomássemos $b = 0$ e $a \neq 0$ com $\varphi(a) > \varphi(0)$ então teríamos $a = bq + r$ se e só se $r = a$, mas aí $\varphi(r) = \varphi(a) > \varphi(0) = \varphi(b)$, absurdo.

d) Com a definição 2.1.1, afirmamos que o anel de polinômios $K[X]$ com coeficientes sobre um corpo K não é um domínio euclidiano com a função grau. De fato, dados $a \in K^*$ e $p(X) \in K[X]$ teríamos que, se $K[X]$ fosse euclidiano para ∂, existiriam $q(X), r(X) \in K[X]$ tais que $p(X) = q(X)a + r(X)$ com $\partial(r(X)) < \partial(a) = 0$ um absurdo, pois ∂ tem imagem $\mathbb{N}$.

No entanto, se definirmos $\varphi : K[X] \to \mathbb{N}$ por

$$\varphi(p(X)) = \begin{cases} 0, & \text{se } p(X) = 0 \\ \partial(p(X)) + 1, & \text{se } p(X) \neq 0 \end{cases}$$

então teremos $K[X]$ euclidiano com a função φ.

2.2 A definição de anel euclidiano

Definição 2.2.1: Dado um anel (comutativo com unidade A), denominamos **algoritmo euclidiano** (ou simplesmente um algoritmo) em A uma aplicação $\varphi : A \to W$, onde W é um conjunto bem ordenado, que satisfaz a condição:

$$\forall a, b \in A,\ b \neq 0,\ \exists\ q, r \in A \text{ tais que } a = bq + r \text{ e } \varphi(r) < \varphi(b). \qquad (*)$$

Dizemos que A é **euclidiano** se admite um algoritmo euclidiano em A, e quando quisermos especificar o algoritmo, diremos que A é **euclidiano para** φ e usaremos a notação (A, φ).

É claro então que todo domínio euclidiano da definição 2.1.1 é um domínio

euclidiano na definição acima também. Mostraremos adiante que a condição (1) que é incluida na definição 2.1.1 de domínio euclidiano não é essencial, no sentido que um algoritmo como em 2.2.1 sempre dá origem a um outro algoritmo que satisfaz também a condição (1) em 2.1.1.

Convenção: Em todo o restante deste trabalho a definição adotada para anel euclidiano (incluindo o caso domínio) será a apresentada em 2.2.1.

2.3 Propriedades elementares dos anéis euclidianos e exemplos

Proposição 2.3.1: *φ é um algoritmo para um anel A se e só se, para qualquer elemento não nulo b fixado, todo elemento $a \in A$ admite um representante r em A para a classe de a em $\frac{A}{<b>}$ com $\varphi(r) < \varphi(b)$.*

Prova: Sejam φ um algoritmo para um anel A e $b \in A$ um elemento não nulo. Então, dado $a \in A$, sabemos que existe $r \in A$ tal que $a = bq + r$ com $\varphi(r) < \varphi(b)$. Daí

$$a - r = bq \Rightarrow a - r \in \langle b \rangle \Rightarrow \bar{a} = \bar{r} \text{ em } \frac{A}{\langle b \rangle},$$

e portanto r é o representante procurado.

Reciprocamente, seja $b \neq 0$ um elemento do anel A. Queremos mostrar que para cada $a \in A$ existem elementos $q, r \in A$ tais que $a = bq + r$ com $\varphi(r) < \varphi(b)$. Por hipótese, para cada $a \in A$ existe x em A tal que $\bar{x} = \bar{a}$ em $\frac{A}{\langle b \rangle}$ com $\varphi(x) < \varphi(b)$. Daí

$$\bar{x} = \bar{a} \Rightarrow a - x \in \langle b \rangle \Rightarrow$$

$$\exists\, q_1 \in A \text{ tal que } a - x = bq_1 \Rightarrow a = bq_1 + x;$$

basta então tomar $r = x$ e $q = q_1$ que teremos φ um algoritmo para A.

■

Proposição 2.3.2: *Seja (A, φ) um anel euclidiano. Então, para todo $b \in A$, $b \neq 0$, temos $\varphi(b) > \varphi(0)$, ou seja, $\varphi(0)$ é o menor elemento de $\varphi(A)$.*

Prova: Fazendo $a = 0$ em 2.2.1 temos que, por $(*)$, existem $q_1, b_1 \in A$ tais que $0 = bq_1 + b_1$ e $\varphi(b_1) < \varphi(b)$. Definimos então indutivamente uma seqüência $b_1, b_2, \ldots, b_n, \ldots$ de elementos de A pela seguinte regra: se $b_n = 0$ paramos; se $b_n \neq 0$ novamente utilizamos $(*)$ e escrevemos $0 = b_n q_{n+1} + b_{n+1}$ com $\varphi(b_{n+1}) < \varphi(b_n)$, gerando assim o elemento b_{n+1}. Como $(\varphi(b_n))$ é uma seqüência estritamente decrescente de elementos

de um conjunto bem ordenado, temos que o conjunto $\{\varphi(b_n) \mid n \in \mathbb{N}^*\}$ tem menor elemento, digamos, $\varphi(b_m)$. Afirmamos que $b_m = 0$. De fato, caso contrário se dividirmos 0 por b_m teremos $0 = b_m q_m + b_{m+1}$ com $\varphi(b_{m+1}) < \varphi(b_m)$ o que é absurdo pois $\varphi(b_m)$ é o menor elemento de $\{\varphi(b_n) \mid n \in \mathbb{N}^*\}$. Em qualquer caso, provamos então que

$$\varphi(b) > \varphi(b_1) > \ldots > \varphi(b_m) = \varphi(0).$$

■

Proposição 2.3.3: *Se um elemento b de um anel euclidiano (A, φ) é tal que $\varphi(b)$ é o menor elemento de $\varphi(A) - \varphi(0)$ então b é um invertível em A.*

Prova: Da hipótese temos $b \neq 0$. Então, para todo $a \in A$, existem $q, r \in A$ tais que $a = bq + r$ satisfazendo $\varphi(r) < \varphi(b)$. Mas então, pelo caráter minimal de b, $\varphi(r) = \varphi(0)$, donde $r = 0$, pela proposição anterior.

Portanto $A = \langle b \rangle$, ou seja, b é invertível.

■

Notemos que a recíproca da proposição acima não é válida. De fato, a aplicação $\varphi : \mathbb{Z} \to \mathbb{N}$ dada por

$$\varphi(n) = \begin{cases} |n| \text{ para } n \neq 1 \\ 2 \text{ para } n = 1 \end{cases}$$

é um algoritmo para $\mathbb{Z}$, pois, para todo $n \neq 0$ em $\mathbb{Z}$ tal que $|n| \leq 1$ ou $|n| \geq 3$, os representantes $r = 0, 1, \ldots, |n| - 1$ das classes $\bmod n$ satisfazem $\varphi(r) < \varphi(n)$. Para $|n| = 2$ trocamos o representante 1 por $1 - 2 = -1$, que satisfaz $\varphi(-1) < \varphi(n) = 2$ (por exemplo escrevemos $7 = 4.2 - 1$ ao invés de $7 = 3.2 + 1$). Portanto por 2.2.1 φ é um algoritmo.

No entanto $\varphi(-1) = 1 < 2 = \varphi(1)$ com 1 sendo um invertível em $\mathbb{Z}$.

Veremos adiante uma condição sobre o anel A que vai nos garantir a validade desta recíproca.

Proposição 2.3.4: *Todo anel euclidiano (A, φ) é um anel a ideais principais.*

Prova: Seja I um ideal não nulo de A. Tomamos então, entre os elementos não nulos de I, um elemento b com o menor valor para φ. Note que tal elemento existe, uma vez que $\varphi(I - \{0\})$ é subconjunto de um conjunto bem ordenado. Afirmamos que $I = \langle b \rangle$. De fato, para todo $a \in I$, escrevemos $a = bq + r$ com $\varphi(r) < \varphi(b)$. Como $r = a - bq \in I$, temos necessariamente $r = 0$.

■

Corolário 2.3.5: *Todo domínio euclidiano é um domínio fatorial.*

Prova: Basta aplicar 2.3.4 e 1.2.14.

■

A recíproca do corolário 2.3.5 não é válida. De fato, $\mathbb{Z}[X]$ ou $K[X,Y]$, com K corpo, são domínios fatoriais que não são euclidianos pois não são principais.

Mostraremos adiante (corolário 4.1.10) que também não é válida a recíproca da proposição 2.3.4. No entanto provaremos na proposição 2.3.16 que todo domínio principal com um número finito de ideais maximais é sempre euclidiano.

Considerando a definição 2.2.1 listamos agora alguns exemplos de anéis euclidianos:

Exemplo 2.3.6: É fácil verificar que o anel dos números inteiros $\mathbb{Z}$ é euclidiano para o algoritmo φ dado pelo algoritmo de Euclides.

Exemplo 2.3.7: É fácil verificar que o anel dos números inteiros $\mathbb{Z}$ é euclidiano para o algoritmo $\varphi(n) = |n|$.

Exemplo 2.3.8: Perguntamo-nos se com esta definição de anel euclidiano a "função" grau ∂ tem chances de ser um algoritmo para o anel de polinômios $K[X]$, com coeficientes sobre um corpo K. Observe que pela proposição 2.3.2 demonstrada acima deveremos ter $\partial(0) < 0$. Assim, se não exigirmos que $\mathbb{N}$ seja um segmento inicial de W, podemos tomar $W = \{-\infty\} \cup \mathbb{N}$ com $-\infty < n$ para todo $n \in \mathbb{N}$ e definir $\partial(0) = -\infty$. Agora sim a função $\partial : K[X] \to W$ é um algoritmo para $K[X]$.

Também a função $\varphi : K[X] \to \mathbb{N}$ definida por

$$\varphi(p(X)) = \begin{cases} 0, \text{ se } p(X) = 0 \\ 1 + \partial(p(X)), \text{ se } p(X) \neq 0 \end{cases}$$

é um algoritmo para $K[X]$, pois como vimos no comentário (d) anteriormente, esta função serve na definição 2.1.1 e portanto também na definição 2.2.1.

Exemplo 2.3.9: Afirmamos que o anel $\mathbb{Z}[\sqrt{p}]$, com p primo positivo, é euclidiano com a função $\varphi : \mathbb{Z}[\sqrt{p}] \to \mathbb{N}$ dada por

$$\varphi(a + b\sqrt{p}) = \left|N(a + b\sqrt{p})\right| = |a^2 - pb^2|$$

(veja 1.4.17 (*iii*)).

De fato, sejam $\alpha, \beta \in \mathbb{Z}[\sqrt{p}]$ com $\beta \neq 0$; procuramos $r, q \in \mathbb{Z}[\sqrt{p}]$ tais que $\alpha = q\beta + r$ com $\varphi(r) < \varphi(\beta)$, ou seja, procuramos q tal que $\varphi(r) = \varphi(\alpha - q\beta) < \varphi(\beta)$. Como

a norma é multiplicativa temos

$$\varphi(r) = \varphi(\alpha - q\beta) = |N(\alpha - q\beta)| = \left|N(\beta)N(\tfrac{\alpha}{\beta} - q)\right| = |N(\beta)||N(\tfrac{\alpha}{\beta} - q)| = \varphi(\beta)\left|N(\tfrac{\alpha}{\beta} - q)\right|,$$

e portanto procuramos $q \in \mathbb{Z}[\sqrt{p}]$ tal que $|N(\frac{\alpha}{\beta} - q)| < 1$.

Escrevendo $\alpha = a + b\sqrt{p}$ e $\beta = c + d\sqrt{p}$ temos

$$\frac{\alpha}{\beta} = \frac{a+b\sqrt{p}}{c+d\sqrt{p}} = \left(\frac{ac-pbd}{c^2-pd^2}\right) + \left(\frac{bc-ad}{c^2-pd^2}\right)\sqrt{p} \in \mathbb{Q}[\sqrt{p}].$$

Denotemos $\frac{\alpha}{\beta}$ por $x + y\sqrt{p}$. Daí, se escolhermos $e \in \mathbb{Z}$ e $f \in \mathbb{Z}$ tais que $|x - e| \leqslant 1$ e $|y - f| \geqslant \frac{1}{p}$ e tomarmos $q = e + f\sqrt{p} \in \mathbb{Z}[\sqrt{p}]$ teremos então

$$\left|N(\tfrac{\alpha}{\beta} - q)\right| = \left|N((x + y\sqrt{p}) - (e + f\sqrt{p}))\right| = \left|N((x - e) - (y - f)\sqrt{p})\right| =$$

$$= |(x - e)^2 - p(y - f)^2| \leqslant 1 - \tfrac{1}{p} < 1$$

e portanto, para tal q, temos $\varphi(\alpha - q\beta) < \varphi(\beta)$.

■

Exemplo 2.3.10: O anel $\mathbb{Z}[i]$ dos inteiros de Gauss é euclidiano para a função norma $n : \mathbb{Z}[i] \to \mathbb{N}$ que é dada por

$$n(a + bi) = a^2 + b^2,$$

como é fácil verificar, de maneira análoga à do exemplo acima, onde aqui escolhemos e e f satisfazendo $|x - e| \leqslant \frac{1}{2}$ e $|y - f| \leqslant \frac{1}{2}$.

Exemplo 2.3.11: Apresentamos agora um exemplo de algoritmo euclidiano envolvendo um conjunto bem ordenado W "muito maior" que $\mathbb{N}$. Consideremos a aplicação $\varphi : \mathbb{Z} \to W$, onde $\mathbb{N} \subset W$, definida por:

$$\begin{cases} \varphi(0) = 0 \\ \varphi(k) = \varphi(|k|) = \varphi(2^j(2n + 1)) \ = j\varpi + n + 1, \ \textit{para } n \geqslant 0, \end{cases}$$

onde ϖ denota o primeiro ordinal transfinito e $j = v_2(k)$ onde v_2 denota a valorização 2 *–ádica.*

Sejam $A, B \in \mathbb{Z}$ com $B \neq 0$; procuramos $Q, R \in \mathbb{Z}$ tais que $A = BQ + R$, com $\varphi(R) < \varphi(B)$.

Inicialmente note que basta-nos considerar $A \geqslant 0$ e $B > 0$, pois se encontrarmos $Q, R \in \mathbb{Z}$ tais que $A = BQ + R$ com $\varphi(R) < \varphi(B)$ como $\varphi(-B) = \varphi(B)$ e $\varphi(-R) = \varphi(R)$ poderemos escrever:

a) $A = (-B)(-Q) + R$ e ainda temos $\varphi(R) < \varphi(B) = \varphi(-B)$;

b) $-A = B(-Q) + (-R)$ e ainda temos $\varphi(-R) = \varphi(R) < \varphi(B)$;

c) $-A = (-B)Q + (-R)$ e ainda temos $\varphi(-R) = \varphi(R) < \varphi(B) = \varphi(-B)$.

Ainda, se $A = 0$ e $B > 0$ então $A = B.0 + 0$ e $\varphi(0) = 0 < \varphi(B)$. Assim, resta-nos provar o resultado para o caso $A > 0$ e $B > 0$.

Consideramos então $A = 2^j(2n+1)$ e $B = 2^s(2d+1)$ com $n \geqslant 0$ e $d \geqslant 0$. Como $A, B \in \mathbb{N}^*$ sabemos que o algoritmo da divisão nos dá elementos $q, r \in \mathbb{Z}$ tais que

$$A = Bq + r \text{ com } 0 \leqslant r < |B| = B.$$

Se $r = 0$ está pronto: $\varphi(0) = 0 < \varphi(B)$.

Suponhamos que $r = 2^t(2k+1)$ com $k \geqslant 0$. Assim temos:

$$A = Bq + r \text{ com } 0 \leqslant r < B \Leftrightarrow$$

$$2^j(2n+1) = 2^s(2d+1)q + 2^t(2k+1) \text{ com } 0 < 2^t(2k+1) < 2^s(2d+1). \qquad (*)$$

Consideramos agora duas possibilidades:

1° Caso: $t \leqslant s$.

Neste caso, temos que se tomarmos $Q = q$ e $R = r$ teremos:

$$A = BQ + R, \text{ com } \varphi(R) = \varphi(r) = t\varpi + k + 1 < s\varpi + d + 1 = \varphi(B).$$

2° Caso: $t > s$, digamos $t = s + i$.

Aqui temos:

$$2^j(2n+1) = 2^s(2d+1)q + 2^t(2k+1) \text{ com } 0 < 2^{s+i}(2k+1) < 2^s(2d+1).$$

Daí

$$\begin{aligned} 2^j(2n+1) &= 2^s(2d+1)q + 2^t(2k+1) \\ &= 2^s(2d+1)q + 2^t(2k+1) + 2^s(2d+1) - 2^s(2d+1) \\ &= 2^s(2d+1)[q+1] + 2^t(2k+1) - 2^s(2d+1) \\ &= B(q+1) + 2^t(2k+1) - 2^s(2d+1). \end{aligned}$$

Olhamos agora o termo

$$\begin{aligned} R &= 2^t(2k+1) - 2^s(2d+1) \\ &= 2^{s+i}(2k+1) - 2^s(2d+1) \\ &= 2^s[2(2^ik + 2^{i-1} - d) - 1] \end{aligned}$$

e observamos que $R < 0$, por $(*)$. Considerando

$$\lambda = 2^ik + 2^{i-1} - d = 2^{i-1}(2k+1) - d$$

temos $2^s(2\lambda - 1) = R < 0$, donde $\lambda < 0$.

Portanto $-R = 2^s[2(-\lambda) + 1]$ e ainda $-\lambda \geqslant 0$.

Então:

$$\varphi(R) = \varphi(-R) = s\varpi + (-\lambda) + 1 = s\varpi - 2^{i-1}(2k+1) + d + 1 < s\varpi + d + 1 = \varphi(B).$$

Assim, se considerarmos $Q = q + 1$ e $R = 2^s[2(2^ik + 2^{i-1} - d) - 1)]$

teremos

$$A = BQ + R, \text{ com } \varphi(R) < \varphi(B).$$

■

OBS: Pode-se provar que q e r dados na definição 2.2.1 são únicos nos exemplos 2.3.6 e 2.3.8 acima. Mas esta propriedade não vale em geral. De fato, já para o exemplo 2.3.7 isto não ocorre: $3 = 2.1 + 1 = 2.2 - 1$ com $\varphi(1) = \varphi(-1) < \varphi(2)$.

Um algoritmo para um anel A nem sempre satisfaz a condição (1) da definição 2.1.1. Por exemplo:

Exemplo 2.3.12: Retomemos o anel euclidiano $(\mathbb{Z}, \varphi)$ onde φ é dada por

$$\varphi(n) = \begin{cases} |n| \text{ para } n \neq 1 \\ 2 \text{ para } n = 1 \end{cases}$$

Note que $\varphi(-1.1) = \varphi(-1) < \varphi(1)$, e portanto φ não satisfaz (1) de 2.1.1.

No entanto afirmamos que tal condição não é essencial, no sentido de que um algoritmo euclidiano sempre pode gerar um algoritmo que satisfaça também (1). Mais precisamente:

Proposição 2.3.13: *Se $\varphi : A \to W$ é um algoritmo para um anel A, então a aplicação $\varphi_1 : A \to W$ definida por*

$$\varphi_1(a) = \begin{cases} \varphi(0), \text{ se } a = 0 \\ \min_{b \in \langle a \rangle - \{0\}} \{\varphi(b)\} \text{ se } a \neq 0 \end{cases}$$

é também um algoritmo e satisfaz ainda, para todo $a, c \in A$,

i) $\varphi_1(a) \leqslant \varphi(a)$;

ii) $\varphi_1(ac) \geq \varphi_1(a)$ *se* $ac \neq 0$.

Prova: Inicialmente observemos que φ_1 está bem definida já que estamos considerando W bem ordenado; além disso, é claro que $\varphi_1(a) \leq \varphi(a)$ para todo $a \in A$.

Para provarmos que φ_1 é um algoritmo, vamos considerar $a, b \in A$, com $b \neq 0$. Por definição temos que $\varphi_1(b) = \varphi(bc)$ para algum c conveniente em A. Sendo φ um algoritmo, existem $q, r \in A$ tais que $a = bcq + r$ com $\varphi(r) < \varphi(bc)$. Portanto temos $\bar{a} = \bar{r}$ em $\frac{A}{\langle b \rangle}$ e $\varphi_1(r) \leq \varphi(r) < \varphi(bc) = \varphi_1(b)$.

A propriedade (*ii*) decorre da definição de $\varphi_1(a)$, já que

$$ac \in \langle a \rangle \Rightarrow \langle ac \rangle \subseteq \langle a \rangle \Rightarrow \varphi_1(ac) \geq \varphi_1(a).$$

■

Proposição 2.3.14: *Se $\varphi : A \to W$ é um algoritmo que satisfaz a condição* (1) *da definição* 2.1.1, *isto é*

$$\varphi(ac) \geqslant \varphi(a) \text{ se } a, c \in A \text{ são tais que } ac \neq 0$$

então φ satisfaz também

$$\varphi(ac) = \varphi(a) \text{ se e somente se } \langle ac \rangle = \langle a \rangle.$$

Em particular, se A for um domínio

$$\varphi(ac) = \varphi(a) \text{ se e somente se } c \text{ é invertível.}$$

Prova: Sejam $a, c \in A$ tais que $ac \neq 0$. Se $\langle ac \rangle = \langle a \rangle$ então, $a = acd$ e portanto por hipótese temos que $\varphi(a) = \varphi(acd) \geqslant \varphi(ac)$; por outro lado temos que $\varphi(ac) \geqslant \varphi(a)$. Assim, temos de fato $\varphi(ac) = \varphi(a)$.

Reciprocamente, se $\varphi(ac) = \varphi(a)$ então, como φ é algoritmo, temos que existem $q, r \in A$ tais que $a = acq + r$ com $\varphi(r) < \varphi(ac) = \varphi(a)$. Temos então $r = a(1 - cq)$, o que implica $r \in \langle a \rangle$. Daí, se $r \neq 0$, podemos escrever, utilizando:

$$\varphi(r) = \varphi(a(1 - cq)) \geqslant \varphi(a) = \varphi(ac) > \varphi(r),$$

um absurdo. Logo, temos de fato $r = 0$, ou seja, $a = acq$, e assim temos $\langle a \rangle = \langle acq \rangle \subseteq \langle ac \rangle \subseteq \langle a \rangle$ e portanto $\langle a \rangle = \langle ac \rangle$.

■

Corolário 2.3.15: *Se $\varphi : A \to W$ é um algoritmo que satisfaz*

$$\forall\, a, c \in A \text{ tais que } ac \neq 0,\ \varphi(ac) \geqslant \varphi(a)$$

(*como por exemplo o algoritmo φ_1 construído na proposição* 2.3.13), *então vale a recíproca da proposição* 2.3.3, *ou seja, se u é um invertível de A, então $\varphi(u)$ é o menor elemento β de $\varphi(A) - \varphi(0)$. Em particular,*

$$u \in U(A) \Leftrightarrow \varphi(u) = \varphi(1).$$

Prova: Note que

$$u \in U(A) \Rightarrow \exists\, u' \in U(A),\ uu' = 1$$
$$\Rightarrow \varphi(1) = \varphi(uu') \geqslant \varphi(u) = \varphi(u.1) \geqslant \varphi(1).$$

Logo,

$$\forall\, u \in U(A),\ \varphi(u) = \varphi(1).$$

Agora, pela proposição 2.3.3, se $u \in A$ é tal que $\varphi(u) = \beta$ então u é

invertível, o que completa a prova.

■

Corolário 2.3.16: *Sejam W um conjunto bem ordenado que contém $\mathbb{N}$ como segmento inicial e A um anel euclidiano que é um domínio. Sejam $P = \{p \in A \mid p$ é irredutível$\}$ e $V = \{v_p \mid p \in P\}$ o conjunto de todas as valorizações $p-$ádicas sobre $cf(A)$. Então, para qualquer algoritmo φ em A temos*

$$\varphi(x) \geqslant 1 + \sum_{p \in P} v_p(x),$$

para qualquer $x \neq 0$ em A.

Prova: Inicialmente observamos que se φ_1 é um algoritmo construído a partir de φ como em 2.3.13, então basta-nos mostrar que a desigualdade é válida para φ_1, pois daí, pelo ítem (i) de 2.3.13 temos que, para todo $x \in A$,

$$\varphi(x) \geqslant \varphi_1(x)$$

e portanto, para todo $x \neq 0$ em A,

$$\varphi(x) \geqslant \varphi_1(x) \geqslant 1 + \sum_{p \in P} v_p(x).$$

Para os $x \in A$ para os quais $\varphi_1(x) > n$ para todo $n \in \mathbb{N}$ a desigualdade é clara.

Vamos então considerar $x \in A$ tal que $\varphi_1(x) = n \in \mathbb{N}^*$.

Inicialmente observe que se $x = up_1^{r_1}.....p_t^{r_t}$ com $u \in U(A)$ e $p_1,...,p_t$ irredutíveis distintos então, pela proposição 2.3.14 temos

$$\varphi_1(x) = \varphi_1(p_1^{r_1}.....p_t^{r_t}),$$

e como $\langle p_1^{r_1}.....p_t^{r_t}\rangle \subsetneq \langle p_1^{r_1-1}.....p_t^{r_t}\rangle$ temos, por (ii) de 2.3.13 e pela proposição 2.3.14

$$\varphi_1(p_1^{r_1}.....p_t^{r_t}) > \varphi_1(p_1^{r_1-1}.....p_t^{r_t}).$$

Como $\varphi_1(x) \in \mathbb{N}^*$ e $\mathbb{N}$ é o segmento inicial de W, temos

$$\varphi_1(p_1^{r_1}.....p_t^{r_t}) \geqslant 1 + \varphi_1(p_1^{r_1-1}.....p_t^{r_t}).$$

Fazendo o mesmo raciocínio agora com o elemento $p_1^{r_1-1}.....p_t^{r_t}$ ao invés de $p_1^{r_1}.....p_t^{r_t}$, não é difícil convencer-se que

$$\varphi_1(x) \geqslant r_1 + \varphi_1(p_2^{r_2}.....p_t^{r_t}) \geqslant r_1 + r_2 + \varphi_1(p_3^{r_3}.....p_t^{r_t}) \geqslant$$
$$\geqslant ... \geqslant r_1 + r_2 + ... + r_{t-1} + (r_t - 1) + \varphi_1(p_t).$$

Agora note que como p_t é irredutível e $\mathbb{N}$ é um segmento inicial de W, temos $\varphi_1(p_t) \geqslant 2$ pois, pelo corolário 2.3.15, $\varphi_1(u) = 1$ se e somente se u é invertível, e

portanto

$$\varphi_1(x) \geqslant r_1 + r_2 + ... + r_t + 1,$$

ou seja,

$$\varphi_1(x) \geqslant 1 + \sum_{p \in P} v_p(x).$$

■

Já salientamos anteriormente que nem todo domínio principal é euclidiano; no entanto temos válida a seguinte proposição:

Proposição 2.3.17: *Um domínio A a ideais principais com um número finito de ideais maximais, digamos,* $Ap_1 = \mathcal{M}_1, ..., Ap_n = \mathcal{M}_n$, *é euclidiano com algoritmo dado pela aplicação* $\varphi : A \to \mathbb{N}$ *tal que*

$$\varphi(x) = \begin{cases} 0, \text{ se } x = 0 \\ 1 + \sum_{i=1}^{n} v_i(x), \text{ se } x \neq 0 \end{cases},$$

onde v_i *denota a valorização* p_i *– ádica de A.*

Prova: Inicialmente observe que se $b \in U(A)$ então $v_i(b) = 0$ para todo i e portanto $\varphi(b) = 1$. E se $b \notin U(A)$ e $b \neq 0$ então existe $j \in \{1,2,...,n\}$ tal que $b \in \mathcal{M}_j$ e portanto $v_j(b) > 0$, donde, como $b \neq 0$, temos $\varphi(b) = 1 + \sum_{i=1}^{n} v_i(b) > 1$. De qualquer modo, temos

$$b \neq 0 \Rightarrow \varphi(b) \geqslant 1.$$

Sejam $a, b \in A$ com $b \neq 0$. Pela proposição 2.3.1 basta encontrarmos $r \in A$ tal que $\bar{r} = \bar{a}$ em $\frac{A}{\langle b \rangle}$ e $\varphi(r) < \varphi(b)$ para termos que φ é um algoritmo.

Se $a \in \langle b \rangle$, digamos, $a = bq$, tomamos $r = 0$ e $a = bq + 0$, e teremos de fato $\varphi(r) = \varphi(0) = 0 < 1 \leqslant \varphi(b)$.

Suponhamos agora $a \notin \langle b \rangle$, e seja r' um representante qualquer de $\bar{a}$ em $\frac{A}{\langle b \rangle}$.

Afirmamos que $v_i(r') < v_i(b)$ para algum índice $i \in \{1,2,3,...,n\}$.

De fato, caso contrário teríamos $v_i(r') \geqslant v_i(b)$ para todo i, ou seja, em $K = cf(A)$ teríamos $v_i(\frac{r'}{b}) \geqslant 0$ para todo i, e portanto, pela proposição 1.3.9 e seu corolário,

$$\frac{r'}{b} \in \bigcap_{i=1}^{n} A_{v_i} = \bigcap_{i=1}^{n} A_{\mathcal{M}_i} = A.$$

Assim $r' \in \langle b \rangle$, o que contradiz a hipótese $\overline{r'} = \overline{a} \neq \overline{0}$ em $\frac{A}{\langle b \rangle}$.

Afirmamos agora que, para os indices i tais que $v_i(r') < v_i(b)$, temos necessariamente que $v_i(r') = v_i(r)$ para todo $r \in \overline{a}$, e portanto, para os índices i tais que $v_i(r') < v_i(b)$ o elemento r' na classe de a pode ser substituido por qualquer outro desta mesma classe, sem que seja alterado o valor de $\varphi(r')$. De fato: se $r' = bq + r$ para algum $q \in A$ então

$$v_i(b) > v_i(r') = v_i(bq + r) \geqslant \min\{v_i(bq), v_i(r)\}.$$

Note agora que se $v_i(bq) \leqslant v_i(r)$ então teríamos

$$v_i(b) > v_i(r') \geqslant v_i(bq) = v_i(b) + v_i(q) \geqslant v_i(b),$$

um absurdo. Assim, temos $v_i(bq) > v_i(r)$ e, pela proposição 1.3.2 (iv), temos

$$v_i(r') = \min\{v_i(bq), v_i(r)\} = v_i(r).$$

Devemos agora verificar o que ocorre quando $v_j(r') \geqslant v_j(b)$, para algum $j \in \{1,2,3...,n\}$. Queremos substituir r' por um representante conveniente da classe de a que satisfaça $v_j(r) = v_j(b)$ para todos os j tais que $v_j(r') \geqslant v_j(b)$.

Inicialmente observe que, como A é domínio de fatoração única e $x \in A$ temos que, se um elemento irredutível $p \in A$ é tal que $p \nmid x$, então $x \notin \langle p \rangle$, e portanto $\langle x \rangle + \langle p \rangle = A$, uma vez que $\langle p \rangle$ é maximal, e isto nos possibilita dizer que existem $y, s \in A$ tais que $yp + sx = 1$. Então para todo $w \in A$, temos $wyp + wsx = w$, ou ainda,

$$\forall\, w \in A\ \exists\, z \in A \text{ tal que } w \equiv zx \pmod{p} \text{ (a saber } z = sw). \qquad (1)$$

Para os índices j tais que $v_j(r') \geqslant v_j(b)$ temos, pondo $v_j(b) = n$ e $v_j(r') = n + t$ com $t \in \mathbb{N}$,

$$r' = cp_j^{n+t} \text{ com } p_j \nmid c \qquad (2)$$

$$b = fp_j^n \text{ com } p_j \nmid f. \qquad (3)$$

Assim, de (2) e (3) teremos

$$fr' = fcp_j^{n+t} = cbp_j^t.$$

Agora, se tomarmos $x = f$ e $w = c$ em (1) acima, teremos que existe $z' \in A$ tal que $c \equiv z'f \pmod{p_j}$; ou seja, existem $z', \lambda \in A$ tais que

$$c = z'f + p_j\lambda. \qquad (4)$$

Fazendo então $z_j = z'p_j^t$ temos, por (2), (4) e (3) que

$$r' = cp_j^{n+t} = (z'f + p_j\lambda)p_j^{n+t} =$$

$$= z'fp_j^{n+t} + \lambda p_j^{n+t+1} = z_jfp_j^n + \lambda p_j^{n+t+1} =$$

$$= z_j b + \lambda p_j^{n+t+1} \Rightarrow r' \equiv z_j b \,(\mathrm{mod}\langle p_j^{n+1}\rangle).$$

Assim, podemos dizer agora que para os índices j tais que $v_j(r') \geqslant v_j(b)$ existe um elemento bem definido z_j módulo $\mathcal{M}_j$ tal que $r' \equiv z_j b \,(\mathrm{mod}\langle p_j^{v_j(b)+1}\rangle)$.

Usando agora o Teorema Chinês de Restos para o sistema de congruências

$$X \equiv 1 - z_j (\mathrm{mod}\,\mathcal{M}_j) \text{ para } j \in \{1,2,3,...n\} \text{ tal que } v_j(r') \geqslant v_j(b)$$

temos que existe $z \in A$ tal que $z \equiv (1 - z_j)(\mathrm{mod}\,\mathcal{M}_j)$ para todo j tal que $v_j(r') \geqslant v_j(b)$.

Afirmamos que $r = r' + bz$ é um representante para $\bar{a}$ em A que satisfaz $v_j(r) = v_j(b)$, para todo j tal que $v_j(r') \geqslant v_j(b)$.

De fato, para tais j temos

$$r' - z_j b \in \mathcal{M}_j^{n+1},$$

uma vez que $v_j(b) = n$.

Além disso,

$$z \equiv (1 - z_j)(\mathrm{mod}\,\mathcal{M}_j) \Leftrightarrow z - 1 = m_j - z_j$$

para algum $m_j \in \mathcal{M}_j$.

Daí $r = r' + bz$ satisfaz:

$$r - b = r' + bz - b = r' + (z-1)b = r' + (m_j - z_j)b =$$
$$= r' - z_j b + m_j b \in \mathcal{M}_j^{n+1} + \mathcal{M}_j^{n+1} = \mathcal{M}_j^{n+1}.$$

Portanto $v_j(r-b) \geqslant n+1 = v_j(b) + 1 > v_j(b)$ e portanto temos

$$v_j(r) = v_j(b),$$

pela proposição 1.3.2 (*iv*).

Sendo assim, concluimos que

$$v_j(r) = v_j(b) \text{ se } v_j(r') \geqslant v_j(b)$$

e

$$v_j(r) < v_j(b) \text{ se } v_j(r') < v_j(b)$$

e portanto

$$\sum_{i=1}^{n} v_i(r) < \sum_{i=1}^{n} v_i(b) \Rightarrow 1 + \sum_{i=1}^{n} v_i(r) < 1 + \sum_{i=1}^{n} v_i(b) \Rightarrow \varphi(r) < \varphi(b).$$

■

Corolário 2.3.18: *O anel de valorização associado a uma valorização discreta v é euclidiano para a função*

$$\varphi(x) = \begin{cases} 0, \text{ se } x = 0 \\ 1 + v(x) \text{ se } x \neq 0 \end{cases}$$

Prova: Para esta prova, basta observarmos que o anel de valorização discreta é um domínio a ideais principais com um só ideal maximal.

■

Proposição 2.3.19: *Sejam $A_1,...,A_n$ anéis e $A = A_1 \times A_2 \times ... \times A_n$ Se (A,φ) é anel euclidiano então, para cada $i \in \{1,...,n\}$, o anel A_i é também euclidiano.*

Prova: Vamos provar apenas, para $n = 2$. É facil convencer-se, por indução sobre n, que a afirmação é também válida para $n > 2$.

Existe um algoritmo $\varphi : A \to W$ e, então dados $(a_1,a_2),(b_1,b_2) \in A$ com $(b_1,b_2) \neq (0,0)$ existem $(q_1,q_2),(r_1,r_2) \in A$ tais que $(a_1,a_2) = (q_1,q_2)(b_1,b_2) + (r_1,r_2)$ com

$$\varphi((r_1,r_2)) < \varphi((b_1,b_2))$$

Definimos então:

$$\varphi_1 : A_1 \to W \text{ como } \varphi_1(x) = \varphi((x,0)) \ \forall\, x \in A_1 \text{ e}$$

$$\varphi_2 : A_2 \to W \text{ como } \varphi_2(y) = \varphi((0,y)) \ \forall\, y \in A_2.$$

Afirmamos que φ_1 é um algoritmo em A_1. De fato, dados $a,b \in A_1$ com $b \neq 0$, consideramos os pares $(a,0),(b,0) \in A_1 \times A_2$; como $A_1 \times A_2$ é euclidiano, existem $(q_1,q_2),(r_1,r_2) \in A_1 \times A_2$ tais que:

$$(a,0) = (b,0)(q_1,q_2) + (r_1,r_2) \text{ com } \varphi((r_1,r_2)) < \varphi((b,0))$$

ou seja:

$$(a,0) = (bq_1 + r_1, 0q_2 + r_2),$$

o que significa que

$$a = bq_1 + r_1 \text{ e } 0 = r_2.$$

Assim, temos

$$\varphi_1(r_1) = \varphi((r_1,0)) = \varphi((r_1,r_2)) < \varphi((b,0)) = \varphi_1(b).$$

De forma análoga prova-se que φ_2 é algoritmo para A_2.

■

Veremos agora que a recíproca desta proposição não é tão trivial:

Proposição 2.3.20: *O produto cartesiano de um número finito de anéis euclidianos é um anel euclidiano.*

Prova: Novamente provaremos apenas o caso em que $A = A_1 \times A_2$. Para mais do que dois anéis euclidianos é fácil convencer-se de que a afirmação acima é válida utilizando indução sobre o número de anéis considerados.

Suponhamos A_1, A_2 euclidianos para $\varphi_i : A_i \to W_i$ com $i \in \{1,2\}$. Consideramos $W' = W_1 \times W_2$ ordenado pela ordem lexicográfica, que sabemos ser ainda um conjunto bem ordenado (veja exemplo b após definção 1.1.4), consideramos a soma ordinal de duas cópias de W' que denotaremos por W (veja definição 1.1.7), e sejam $h' : W' \to W$ e $h'' : W' \to W$ aplicações injetivas que preservam ordem, e tais que $h'(\lambda) < h''(\mu)$ para todos $\lambda, \mu \in W'$.

Dados $x_1 \in A_1$ e $x_2 \in A_2$ definimos $\varphi : A_1 \times A_2 \to W$ como segue:

(i) Se x_1, x_2 forem ambos nulos ou nenhum deles for nulo, definimos

$$\varphi(x_1, x_2) = h'((\varphi_1(x_1), \varphi_2(x_2))),$$

(ii) Se somente um deles for nulo, então definimos

$$\varphi(x_1, x_2) = h''((\varphi_1(x_1), \varphi_2(x_2))).$$

Note que desta maneira estamos fazendo com que $\varphi(0,0)$ seja o menor elemento de W, pois $\varphi(0,0) = h'(\varphi_1(0), \varphi_2(0))$ e h' preserva a ordem e $h'(x,y) < h''(a,b)$ para todo (x,y), $(a,b) \in A_1 \times A_2$.

Afirmamos que φ definida acima é um algoritmo euclidiano para $A_1 \times A_2$. De fato, sejam $a = (a_1, a_2)$, $b = (b_1, b_2) \in A_1 \times A_2$ com b não nulo. Vamos encontrar $r, q \in A_1 \times A_2$ tais que $a = bq + r$ com $\varphi(r) < \varphi(b)$.

1° Caso: suponhamos que b_1, b_2 são ambos não nulos. Neste caso, como A_1 e A_2 são euclidianos, existem $q_i, r_i \in A_i$ para $i \in \{1,2\}$ tais que $a_i = b_i q_i + r_i$ com $\varphi_i(r_i) < \varphi_i(b_i)$.

Se r_1, r_2 forem ambos nulos ou nenhum deles for nulo, temos:

$$\varphi(r_1, r_2) = h'((\varphi_1(r_1), \varphi_2(r_2))) < h'((\varphi_1(b_1), \varphi_2(b_2))) = \varphi(b_1, b_2) = \varphi(b).$$

Assim, podemos tomar $q = (q_1, q_2)$ e $r = (r_1, r_2)$ e teremos $a = bq + r$ com $\varphi(r) < \varphi(b)$.

Agora, se algum dos elementos r_1, r_2 for nulo, digamos, sem perda de generalidade $r_1 = 0 \neq r_2$ escrevemos:

$$a_1 = b_1(q_1 - 1) + b_1, \; a_2 = b_2 q_2 + r_2.$$

e tomando $r = (b_1, r_2)$, $q = (q_1 - 1, q_2)$, teremos

$$\varphi(r) = \varphi(b_1, r_2) = h'((\varphi_1(b_1), \varphi_2(r_2))) < h'((\varphi_1(b_1), \varphi_2(b_2))) = \varphi(b_1, b_2) = \varphi(b),$$

ou seja, podemos tomar $r = (b_1, r_2)$ e $q = (q_1 - 1, q_2)$ e teremos $\varphi(r) < \varphi(b)$.

2° Caso: se exatamente um entre b_1 e b_2 é nulo, digamos, sem perda de generalidade, $b_1 = 0 \neq b_2$.

Se $a_1 = 0$ então $a_1 = 0.b_1 + 0$, e como φ_2 é um algoritmo, temos que existem $q_2, r_2 \in A_2$ tais que

$$a_2 = b_2 q_2 + r_2, \text{ com } \varphi_2(r_2) < \varphi_2(b_2),$$

donde concluimos que, tomando $q = (0, q_2)$ e $r = (0, r_2)$ obtemos $a = bq + r$, com

$$\varphi(r) = \varphi(0, r_2) = \begin{cases} \varphi(0,0) < \varphi(b_1, b_2), \text{ se } r_2 = 0 \\ h''(\varphi_1(0), \varphi_2(r_2)) < h''(\varphi_1(0), \varphi_2(b_2)) = \varphi(0, b_2) = \varphi(b_1, b_2) \text{ se } r_2 \neq 0. \end{cases}$$

Se $a_1 \neq 0$ então escrevemos $a_1 = 0.q_1 + a_1$ e $a_2 = b_2 q_2 + r_2$ com $r_2 \in A_2$ não nulo (isto sempre é possível se $A_2 \neq \{0\}$. Note que se $A_2 = \{0\}$ então $A_1 \times A_2 \simeq A_1$ e não temos nada a mostrar neste caso).

Então $(a_1, a_2) = (q_1, q_2)(0, b_2) + (a_1, r_2)$ e, como $a_1 \neq 0 \neq r_2$ temos

$$\varphi(a_1, r_2) = h'(\varphi_1(a_1), \varphi_2(r_2)) < h''(\varphi_1(0), \varphi_2(b_2)) = \varphi(0, b_2) = \varphi(b_1, b_2).$$

■

Exemplo 2.3.21: Com esta proposição podemos agora construir exemplos de anéis euclidianos que não são domínios, como por exemplo $\mathbb{Z} \times \mathbb{Z}$.

Observação 1: O algoritmo φ construido na demonstração da proposição acima é chamado por Samuel [SP$_2$] de "algoritmo transfinito". Afirmamos que em alguns casos tais algoritmos são inevitáveis, como no caso $\mathbb{Z} \times \mathbb{Z}$. De fato, inicialmente provamos:

Proposição 2.3.22: *Dado um anel euclidiano (A, φ) tal que $U(A)$ é finito então, fixado um número inteiro qualquer n, o conjunto $A_n = \varphi^{-1}(\{n\})$ é também finito.*

Prova: Inicialmente observamos que como A é euclidiano temos que A é um anel a ideais principais. Então, pela proposição 1.2.8, temos que A é a soma direta de domínios a ideais principais e de anéis a ideais principais com um único e nilpotente ideal primo, digamos,

$$A = B_1 \times \ldots \times B_m \times \ldots \times B_s,$$

onde $B_1, \ldots, B_m$ são domínios e $B_{m+1}, \ldots, B_s$ são anéis a ideais principais com um único e nilpotente ideal primo.

Ainda, como $U(A)$ é finito, temos necessariamente que $U(B_i)$ é finito para todo $i \in \{1, \ldots, s\}$.

Afirmamos que todo ideal $\mathcal{I}$ de A tem apenas um número finito de

geradores, ou seja, fixado $b = (b_1, ..., b_s) \in A$, existe apenas um número finito de possibilidades para $c = (c_1, ..., c_s)$ tais que $Ab = Ac$. De fato se $Ab = Ac$, existem $d = (d_1, ..., d_s)$ e $e = (e_1, ..., e_s)$ tais que $c = bd$ e $b = ec$. Mas então, para todo $i \in \{1, ..., s\}$,

$$c_i = b_i d_i \text{ e } b_i = e_i c_i.$$

Daí, se $i \leqslant m$ podemos concluir que $d_i, e_i \in U(B_i)$, ou seja, b_i e c_i são associados pois B_i é um domínio.

Se $i > m$ então, pela proposição 1.2.8 sabemos que b_i é da forma

$$b_i = p_i^{v(b_i)} u_b,$$

onde u_b é invertível e $v(b_i) \geqslant 0$ é univocamente determinado por b_i; da mesma forma escrevemos

$$c_i = p_i^{v(c_i)} u_c, d_i = p_i^{v(d_i)} u_d, e_i = p_i^{v(e_i)} u_e,$$

onde $B_i p_i$ é o único ideal maximal nilpotente de B_i.

Daí:

$$c_i = b_i d_i \text{ e } b_i = e_i c_i \Rightarrow p_i^{v(c_i)} u_c = p_i^{v(b_i)} u_b p_i^{v(d_i)} u_d \text{ e } p_i^{v(b_i)} u_b = p_i^{v(e_i)} u_e p_i^{v(c_i)} u_c \Rightarrow$$

$$p_i^{v(c_i)} u_c = p_i^{v(b_i)+v(d_i)} u_b u_d \text{ e } p_i^{v(b_i)} u_b = p_i^{v(e_i)+v(c_i)} u_e u_c,$$

donde pela unicidade de representação,

$$v(c_i) = v(b_i) + v(d_i) \text{ e } v(b_i) = v(e_i) + v(c_i) \Rightarrow v(d_i) = v(e_i) = 0.$$

E portanto $c_i = b_i u_d$, ou seja, também neste caso c_i é associado de b_i.

Como cada $U(B_i)$ é finito concluimos que existe um número finito de possibilidades para o elemento $c = (c_1, ..., c_s)$.

Daí, por indução sobre n, temos que se $A'_n = A_0 \cup A_1 \cup ... \cup A_{n-1}$ é finito e $\varphi(b) = n$ então $A'_n \to \frac{A}{\langle b \rangle}$ é sobrejetora pela proposição 2.3.1, e então $\frac{A}{\langle b \rangle}$ é finito; portanto $\langle b \rangle$ tem norma finita e, como euclidiano é noetheriano, pela proposição 1.2.33, existe apenas um número finito de possibilidades para $\langle b \rangle$. Por outro lado, pela observação inicial, existe apenas um número finito de possibilidades para b. Logo $A_n = \varphi^{-1}(\{n\})$ é finito.

■

Provemos agora que não existe algoritmo para $\mathbb{Z} \times \mathbb{Z}$ da forma $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$. De fato, caso contrário teríamos $\varphi((1,0)) = n$ para algum $n \in \mathbb{N}$ e, utilizando a demonstração da proposição acima, com a mesma notação empregada lá, teríamos $A'_n = A_0 \cup A_1 \cup ... \cup A_{n-1}$ finito e $A'_n \to \frac{(\mathbb{Z}\times\mathbb{Z})}{\langle (1,0) \rangle}$ sobrejetora, e portanto o anel $\frac{(\mathbb{Z}\times\mathbb{Z})}{\langle (1,0) \rangle}$ é também finito, absurdo.

Observação 2: Samuel em [SP_2] salienta que ainda é um problema em aberto responder se existe algum domínio D que é euclidiano e que não admite nenhum algoritmo tomando apenas valores naturais.

Proposição 2.3.23: *Seja A um domínio euclidiano, e $S \subset A$ um subconjunto multiplicativamente fechado (tal que $0 \notin S$). Então A_S é euclidiano.*

Prova: Inicialmente observamos que basta provarmos para S um sistema multiplicativo saturado, pois se S' é a saturação de S, então $A_{S'} = A_S$.

Vamos considerar S saturado; então S é gerado por alguns elementos irredutíveis de A e pelos invertíveis. Então para cada $x \in A_S$ temos que existe $x' \in A$ tal que $x = (\frac{s}{t})x'$ com $s,t \in S$ e x' primo com todos os irredutíveis de S , e portanto também primo com todos os elementos de S. Afirmamos que para cada $x \in A_S$ tal x' é único, a menos de invertíveis. De fato,

$$\frac{a}{s} = \frac{b}{t} \text{ em } A_S \Leftrightarrow ta = sb.$$

Daí, fatorando a e b obteremos alguns fatores irredutíveis pertencentes a S e outros não pertencentes a S. Mas como $s, t \in S$, pela fatoração única os fatores irredutíveis não pertencentes a S serão os mesmos, a menos de invertíveis. Desta forma podemos escrever:

$$a = a'x_1...x_r \text{ e } b = b'x_1,...,x_r,$$

onde $a', b' \in S$ e $x_1...x_r$ são os irredutíveis não pertencentes a S. Daí

$$\frac{a}{s} = \frac{a'}{s}x_1...x_r \text{ e } \frac{b}{t} = \frac{b'}{t}x_1...x_r.$$

Definimos agora $\varphi_S : A_S \to \varphi(A)$ pondo $\varphi_S(x) = \varphi(x')$ onde φ é um algoritmo em A que satisfaz as condições das proposições 2.3.13 e 2.3.14. Temos que φ_S está bem definida, pois se $u \in U(A)$ então $\varphi(ux') = \varphi(x')$, uma vez que φ satisfaz 2.3.14.

Afirmamos agora que φ_S é um algoritmo para A_S.

Sejam $a,b \in A_S$, com $b \neq 0$, digamos, $a = \left(\frac{s_1}{t_1}\right)a'$ e $b = \left(\frac{s_2}{t_2}\right)b'$ com $s_1,s_2,t_1,t_2 \in S$ e a', b' primos com qualquer elemento de S. Note que

$$b \neq 0 \Rightarrow s_2 \neq 0 \neq b'.$$

Como (A,φ) é um domínio euclidiano, temos que existem $q_1,r_1 \in A$ tais que

$$a' = q_1b' + r_1, \text{ com } \varphi(r_1) < \varphi(b').$$

Daí:

$$a = \left(\frac{s_1}{t_1}\right)a' = \left(\frac{s_1}{t_1}\right)q_1b' + \left(\frac{s_1}{t_1}\right)r_1 =$$
$$= \left(\frac{s_1}{t_1}\right)\left(\frac{t_2}{s_2}\right)q_1\left(\frac{s_2}{t_2}\right)b' + \left(\frac{s_1}{t_1}\right)r_1 =$$

$$= \left(\frac{s_1}{t_1}\right)\left(\frac{t_2}{s_2}\right)q_1 b + \left(\frac{s_1}{t_1}\right)r_1.$$

Afirmamos que

$$\varphi_S\left(\frac{s_1}{t_1}r_1\right) < \varphi_S(b).$$

De fato, escreva agora $r_1 = l_1 ... l_r r'$ com $l_i \in S$ e r' primo com qualquer elemento de S. Então, como $r \in \langle r' \rangle$ e $qb' \in \langle b' \rangle$ temos:

$$\varphi_S\left(\frac{s_1}{t_1}r_1\right) = \varphi(r') \leqslant \varphi(r_1) < \varphi(b') = \varphi_S(b),$$

sendo a primeira desigualdade válida por (*ii*) da proposição 2.3.13.

Portanto, tomando $q = \left(\frac{s_1 t_2}{t_1 s_2}\right)q_1$ e $r = \left(\frac{s_1}{t_1}\right)r_1$ teremos:

$$a = qb + r \text{ com } \varphi_S(r) < \varphi_S(b).$$

■

Proposição 2.3.24: *Se A é um anel euclidiano, então o anel $A' = A[[X]][X^{-1}]$ de polinômios em X^{-1} com coeficientes séries formais em X é euclidiano.*

Prova: Seja φ um algoritmo para o anel A.

Observemos inicialmente que os elementos de A' podem ser expressos com séries de potências $\sum_{n \geqslant n_0} a_n X^n$ com $a_n \in A$ e $n_0 \in \mathbb{Z}$.

Desta forma, sem perda de generalidade, todo elemento não nulo $s \in A'$, pode ser escrito na forma

$$s = a(s)X^{\alpha} + \sum_{n \geqslant 1} a_n X^{\alpha+n} \qquad (*)$$

com $a_n \in A$ para todo $n \in \mathbb{N}^*$ e $a(s) \in A$, $a(s) \neq 0$ e $\alpha \in \mathbb{Z}$.

Definimos agora

$$\varphi'(s) = \begin{cases} \varphi(0), \text{ se } s = 0 \\ \varphi(a(s)), \text{ se } s \neq 0. \end{cases}$$

Fixado $s \in A'$ não nulo como em $(*)$ temos:

$$0 = 0.s + 0 \text{ com } \varphi'(0) = \varphi(0) < \varphi(a(s)) = \varphi'(s)$$

e, para $t \in A$, $t \neq 0$, digamos,

$$t = a(t)X^{\beta} + \sum_{m \geqslant 1} b_m X^{\beta+m}$$

com $b_m \in A$ para todo $m \in \mathbb{N}^*$, $a(t) \in A$, $a(t) \neq 0$ e $\beta \in \mathbb{Z}$, escrevemos:

$$a(t) = ba(s) + c \text{ com } \varphi(c) < \varphi(a(s)).$$

Daí, afirmamos que

$$t = (bX^{\beta-\alpha})s + cX^{\beta} + \sum_{m\geqslant 1}(b_m - ba_m)X^{\beta+m}.$$

De fato:

$$t = a(t)X^{\beta} + \sum_{m\geqslant 1} b_m X^{\beta+m} =$$

$$= (ba(s) + c)X^{\beta} + \sum_{m\geqslant 1} b_m X^{\beta+m} =$$

$$= ba(s)X^{\beta} + cX^{\beta} + \sum_{m\geqslant 1} b_m X^{\beta+m} =$$

$$= (bX^{\beta-\alpha})(a(s)X^{\alpha}) + cX^{\beta} + \sum_{m\geqslant 1} b_m X^{\beta+m} =$$

$$= (bX^{\beta-\alpha})s - (bX^{\beta-\alpha})\left[\sum_{n\geqslant 1} a_n X^{\alpha+n}\right] + cX^{\beta} + \sum_{m\geqslant 1} b_m X^{\beta+m} =$$

$$= (bX^{\beta-\alpha})s - \sum_{n\geqslant 1} ba_n X^{\beta+n} + cX^{\beta} + \sum_{m\geqslant 1} b_m X^{\beta+m} =$$

$$= (bX^{\beta-\alpha})s + cX^{\beta} + \sum_{m\geqslant 1}(b_m - ba_m)X^{\beta+m}.$$

Daí, denominando $q = bX^{\beta-\alpha}$ e $r = cX^{\beta} + \sum_{m\geqslant 1}(b_m - ba_m)X^{\beta+m}$ temos que se $c \neq 0$ então $\varphi'(r) = \varphi(c) < \varphi(a(s)) = \varphi'(s)$.

No caso em que $c = 0$ ainda não sabemos quanto vale $\varphi'(r)$; neste caso, considerando que $r \in A'$, escrevemos $r = a(r)X^{\beta'} + \sum_{j\geqslant 1} p_j X^{\beta'+j}$ onde $\beta' > \beta$ e, "dividindo" $a(r)$ por $a(s)$ encontramos b', $r' \in A$ tais que $a(r) = a(s)b' + c'$ com $\varphi(c') < \varphi(a(s))$; analogamente ao processo anterior teremos que considerar duas possibilidades: Se $c' \neq 0$ então $\varphi'(r') = \varphi(c') < \varphi(a(s)) = \varphi'(s)$; Se $c' = 0$ então ainda não sabemos quanto vale $\varphi'(r')$, e portanto repetimos o processo.

Se o processo parar após um número finito de passos nós encontramos

$$r^{(n)} \equiv t (\mathrm{mod}\langle s\rangle) \text{ tal que } \varphi'(r^{(n)}) < \varphi'(s).$$

Caso contrário a soma infinita $u = bX^{\beta-\alpha} + b'X^{\beta'-\alpha} + \ldots + b^{(n)}X^{\beta^{(n)}-\alpha} + \ldots$ faz sentido, considerando que a seqüência $(\beta^{(n)})$ é estritamente crescente, e nós temos $t = us + 0$, onde evidentemente $\varphi'(0) < \varphi'(s)$.

■

Proposição 2.3.25: *Sejam W e W' conjuntos bem ordenados. Se $h : W \to W'$ é uma bijeção que preserva ordem e $\varphi : A \to W$ é um algoritmo então $h \circ \varphi : A \to W'$ é também um algoritmo.*

Prova: Sejam $a, b \in A$ tais que $b \neq 0$. Como φ é um algoritmo em A temos que existem $q, r \in A$ tais que $a = bq + r$ com $\varphi(r) < \varphi(b)$ em W e, portanto, aplicando h, teremos $h(\varphi(r)) < h(\varphi(b))$ em W' pois h preserva ordem. Sendo assim a aplicação $h \circ \varphi$ também será um algoritmo em A.

■

Definição 2.3.26: Dois algoritmos $\varphi : A \to W$ e $\varphi' : A \to W'$ são ditos **isomorfos** se existe uma bijeção, $h : \varphi(A) \to \varphi'(A)$, que preserva ordem tal que $\varphi' = h \circ \varphi$.

Observamos que se φ e φ' são algoritmos isomorfos, então $\varphi(a) < \varphi(b)$ se e somente se $\varphi'(a) < \varphi'(b)$.

Capítulo 3

A NORMA COMO ALGORITMO

Dado um domínio euclidiano D com corpos de restos finitos e corpo de frações K, podemos nos perguntar se a norma é um algoritmo em D, uma vez que vale o teorema 1.2.31. Relembramos que por 1.4.19, temos às vezes duas formas distintas de calculá-la. Analisamos aqui algumas situações:

i) Se $D = \mathbb{Z}$ então, para $x \in \mathbb{Z}, x \neq 0$, temos que

$$n(x) = \#\left(\frac{\mathbb{Z}}{\langle x \rangle}\right) = |x|$$

ou seja, a norma coincide com o algoritmo usual em $\mathbb{Z}$ visto no exemplo 2.3.7.

ii) Se $D = K$ e K é um corpo finito, digamos, com q elementos, então, para todo polinômio não nulo $b \in K[X]$, temos que, como $\frac{K[X]}{\langle b \rangle}$ tem por representantes os polinômios com grau menor que $\partial(b)$ podemos dizer então que

$$n(b) = \#\left(\frac{K[X]}{\langle b \rangle}\right) = q^{\partial(b)}$$

de modo que $n = h \circ \varphi$ onde:

$$\varphi : K[X] \to \mathbb{N},$$

$$\varphi(p(x)) = \begin{cases} 0, \text{ se } p(x) = 0 \\ 1 + \partial(p(x)), \text{ se } p(x) \neq 0, \end{cases}$$

$$n : K[X] \to \mathbb{N},$$

$$n(p(x)) = \begin{cases} 0, \text{ se } p(x) = 0 \\ q^{\partial(p(x))}, \text{ se } p(x) \neq 0, \end{cases}$$

e

$$h : \mathbb{N} \to \mathbb{N},$$

$$h(a) = \begin{cases} 0, \text{ se } a = 0 \\ q^{a-1}, \text{ se } a \neq 0, \end{cases}$$

é uma função injetora que preserva ordem. Portanto, pela definição 2.3.26, os algoritmos φ (algoritmo usual em $K[X]$) e n (norma) são algoritmos isomorfos.

iii) Se D é um domínio a ideais principais com um número finito de ideais maximais, digamos $\mathcal{M}_1, ..., \mathcal{M}_r$ tais que cada corpo de restos $\frac{D}{\mathcal{M}_i}$ possui q_i elementos então, se observarmos que D é um DFU e que cada $\mathcal{M}_i$ é gerado por um elemento irredutível p_i de D, temos que todo $x \in D$ se fatora em potências dos p_i's, a menos de invertíveis:

$$x = up_1^{n_1} ... p_r^{n_r}$$

com $n_1, ..., n_r \in \mathbb{N}$ e $u \in U(D)$, donde

$$< x >=< p_1^{n_1} ... p_r^{n_r} >= \prod_{i=1}^{r} < p_i^{n_i} > .$$

E então, pela proposição 0.2 e pelo lema 1.2.1, $\frac{D}{<x>} \to \prod_{i=1}^{r} \frac{D}{<p_i^{n_i}>}$ é um isomorfismo de anéis. Assim, $n(x) = \prod_{i=1}^{r} n(p_i^{n_i})$.

Mas $\frac{D}{<p_i^{n_i}>}$ é um $\frac{D}{<p_i>}$ – espaço vetorial de dimensão n_i, donde $n(p_i^{n_i}) = q_i^{n_i}$ e portanto

$$n(x) = \prod_{i=1}^{r} n(p_i^{n_i}) = \prod_{i=1}^{r} q_i^{n_i}.$$

Agora basta ver que, da fatoração de x em irredutíveis dada acima, temos

$$n_i = v_{p_i}(x), \text{ para todo } i \in \{1, ..., r\}$$

onde v_{p_i} denota a valorização p_i – *ádica* de D e portanto

$$n(x) = \prod_{i=1}^{r} q_i^{v_i(x)} (x \in D, x \neq 0).$$

iv) Se D um domínio euclidiano com corpos de restos finitos para o qual a norma é um algoritmo. Então, se S é um subconjunto multiplicativamente fechado de D, temos que, pela proposição 2.3.23 D_S é também euclidiano. Utilizando a norma como algoritmo de D, aquela proposição nos diz que, se considerarmos $x \in D_S$, $x \neq 0$ escrito na forma $x = \frac{s}{t}x'$ com $s,t \in S$ e $x' \in D$ primo com todos elementos de S, então a aplicação n' definida por $n'(x) = n(x')$ é um algoritmo em D_S. Da teoria de localização sabemos que $\frac{D}{\langle x' \rangle} \to \frac{D_S}{\langle x \rangle}$ é um isomorfismo, e portanto temos que o algoritmo n' é de fato a norma em D_S.

v) Perguntamo-nos agora para que valores de d uma extensão quadrática $\mathbb{Q}(\sqrt{d})$ (onde sempre está definida a norma) admite a norma como algoritmo.

Vamos mostrar aqui que os únicos anéis de inteiros algébricos associados a corpos quadráticos imaginários que admitem a norma como algoritmo são apenas os anéis associados a $\mathbb{Q}(\sqrt{-d})$ com $d \in \{1,2,3,7,11\}$.

Seja $K = \mathbb{Q}(\sqrt{-d})$ com d inteiro e livre de quadrados. Inicialmente observe que, neste caso, pela proposição 1.4.17 temos $|N_{K|\mathbb{Q}}(\alpha)| = N_{K|\mathbb{Q}}(\alpha)$ para todo $\alpha \in K$.

Usaremos no que segue simplesmente $N(\alpha)$ para representar $N_{K|\mathbb{Q}}(\alpha)$.

Lema 3.1: *Em $K = \mathbb{Q}(\sqrt{d})$ com $d \in \mathbb{Z}$ livre de quadrados e negativo, são equivalentes*:

(*i*) K é euclidiano para a função norma, isto é,

$\forall\, \alpha, \beta \in I_K$ *não nulos*, $\exists \gamma, \delta \in I_K$ *tais que* $\alpha = \beta\gamma + \delta$ *com* $\delta = 0$ *ou* $N(\delta) < N(\beta)$.

(*ii*) *para todo* $k \in K$, *existe* $\varepsilon \in I_K$ *tal que* $|N(k - \epsilon)| < 1$, *isto é, todo elemento de K está "próximo" de um inteiro algébrico.*

Prova: Provemos inicialmente que (*i*) implica (*ii*).

Dado $k \in K$, sabemos, pelo lema 1.4.7 que existe algum elemento $c \in \mathbb{Z}^*$ tal que $ck \in I_K$. Agora, tomando $\alpha = ck$, $\beta = c$ por (*i*) temos que existem $\gamma, \delta \in I_K$ tais que $\alpha = \beta\gamma + \delta$ com $\delta = 0$ ou $N(\delta) < N(\beta)$. Daí:

- se $\delta = 0$ então $ck = c\gamma$ para $\gamma \in I_K$, donde $k = \gamma$ e portanto, pondo $\varepsilon = \gamma$, temos

$$|N(k - \varepsilon)| = N(0) = 0 < 1;$$

- se $\delta \neq 0$ então $ck = c\gamma + \delta$ com $|N(\delta)| < |N(c)|$. Agora, como $c \neq 0$ e a norma é multiplicativa, temos que

$$|N(\delta)|\frac{1}{|N(c)|} = |N(\tfrac{\delta}{c})| < 1.$$

Mas $\frac{\delta}{c} = k - \gamma$; portanto, se tomarmos $\varepsilon = \gamma$, temos

$$|N(k-\gamma)| < 1.$$

Para provar que (*ii*) implica (*i*) basta tomarmos, para $\alpha, \beta \in I_K$ não nulos, $k = \frac{\alpha}{\beta}$ em (*ii*) e definir $\delta = \alpha - \beta\varepsilon$.

■

Teorema 3.2: *Quando d é negativo e livre de quadrados e* $K = \mathbb{Q}(\sqrt{d})$, *temos que* I_K *é euclidiano para a função norma se* $d \in \{-1,-2,-3,-7,-11\}$.

Prova: Para provar este teorema consideremos dois casos:

1°caso: $d \equiv 2$ ou $3 \pmod 4$; neste caso temos que $d \in \{-1,-2\}$ e $I_K = \mathbb{Z} + \mathbb{Z}\sqrt{d}$, pela proposição 1.4.17.

Seja $k = r + s\sqrt{d}$ com $r,s \in \mathbb{Q}$. Pelo lema anterior devemos encontrar um elemento $\varepsilon = x + y\sqrt{d}$ com $x,y \in \mathbb{Z}$ tal que

$$(r-x)^2 - d(s-y)^2 < 1$$

Como $d \in \{-1,-2\}$, tomamos x e y de forma que tenhamos $|r-x| \leqslant \frac{1}{2}$ e $|s-y| \leqslant \frac{1}{2}$ para tais elementos temos:

a) para $d = -1$: $(r-x)^2 - d(s-y)^2 \leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1$.

b) para $d = -2$: $(r-x)^2 - d(s-y)^2 \leqslant \left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2 = \frac{3}{4} < 1$, como queríamos.

2°caso: $d \equiv 1 \pmod 4$, neste caso temos que $d \in \{-3,-7,-11\}$ $I_K = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$.

Neste caso devemos encontrar $k = x + y\left(\frac{1+\sqrt{d}}{2}\right)$ com $x,y \in \mathbb{Z}$, tal que

$$(r - x - \tfrac{1}{2}y)^2 - d(s - \tfrac{1}{2}y)^2 < 1.$$

Certamente podemos encontrar um inteiro y tal que $|2s-y| \leqslant \frac{1}{2}$; e podemos encontrar um inteiro $x \in \mathbb{Z}$ tal que $|r - x - \frac{1}{2}y| \leqslant \frac{1}{2}$, para tais elementos temos:

a) para $d = -3$: $(r - x - \frac{1}{2}y)^2 - d(s - \frac{1}{2}y)^2 \leqslant \left(\frac{1}{2}\right)^2 + 3\left(\frac{1}{4}\right)^2 = \frac{7}{16} < 1$;

b) para $d = -7$: $(r - x - \frac{1}{2}y)^2 - d(s - \frac{1}{2}y)^2 \leqslant \left(\frac{1}{2}\right)^2 + 7\left(\frac{1}{4}\right)^2 = \frac{11}{16} < 1$;

c) para $d = -11$: $(r - x - \frac{1}{2}y)^2 - d(s - \frac{1}{2}y)^2 \leqslant \left(\frac{1}{2}\right)^2 + 11\left(\frac{1}{4}\right)^2 = \frac{15}{16} < 1$.

Desta forma o teorema está provado.

■

Para corpos quadráticos reais, temos que a norma serve de algoritmo apenas no caso em que

$$d \in \{2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73\}.$$

Para uma demonstração deste fato, indicamos [H-W] e [S-T] para provas parciais e [C-D] para uma prova completa.

Capítulo 4

O MENOR ALGORITMO E A CONSTRUÇÃO TRANSFINITA

4.1 O menor algoritmo

Neste capítulo vamos considerar a seguinte

Convenção: A é um anel euclidiano, e W é um conjunto bem ordenado tal que $\#W > \#A$. Então, para todo algoritmo φ de A, $\varphi(A)$ é um conjunto bem ordenado com $\#\varphi(A) \leq \#A < \#W$, e portanto, pelo que foi citado no capítulo 1 (após definição 1.1.6) sobre conjuntos bem ordenados e pela proposição 2.3.25, podemos supor que todos os algoritmos de A têm imagem no conjunto W. Vamos também supor que $\mathbb{N}$ é um segmento inicial de W. Ou seja, podemos denotar os elementos de W por $0, 1, 2, ..., \omega, \omega + 1, ..., 2\omega, ...$

Salientamos que nas condições acima, temos garantida a existência de um algoritmo $\varphi : A \to W$ satisfazendo $\varphi(0) = 0$, isto é , $0 \in \varphi(A)$. De fato, se $\varphi : A \to W$ é um algoritmo que satisfaz $\varphi(0) = s > 0$ então definimos $\varphi' : A \to W$ da seguinte forma:

$$\forall\ x \in A,\ \varphi'(x) = \varphi(x) - s.$$

Afirmamos que φ' é também um algoritmo e obviamente satisfaz $\varphi'(0) = 0$. De fato, dados $a, b \in A,\ b \neq 0$, existem $q, r \in A$ tais que

$$a = bq + r \text{ com } \varphi(r) < \varphi(b),$$

e portanto

$$\varphi'(r) = \varphi(r) - s < \varphi(b) - s = \varphi'(b).$$

Ainda, note que, pela proposição 2.3.2, temos, para todo $x \in A$, $\varphi(x) \geqslant \varphi(0) = s$ e portanto

$$\varphi'(x) = \varphi(x) - s \geqslant 0,$$

donde $\varphi'(x) \in W$ para todo $x \in A$.

Proposição 4.1.1: *Se* $\{\varphi_\alpha : A \to W\}_{\alpha \in I}$, *é uma família não vazia de algoritmos em um anel euclidiano* A, *então a função* $\theta : A \to W$ *dada por*

$$\forall a \in A,\ \theta(a) = \min_\alpha\{\varphi_\alpha(a)\}$$

é também um algoritmo em A.

Prova: Inicialmente, note que como W é bem ordenado, fixado $a \in A$ sempre existe o menor elemento do conjunto $\{\varphi_\beta(a) \mid \beta \in I\}$, e portanto θ está bem definida.

Consideremos agora $a, b \in A$, com $b \neq 0$, e seja $\alpha \in I$ tal que $\theta(b) = \varphi_\alpha(b)$. Então, em relação ao algoritmo φ_α, existem $q, r \in A$ tais que $a = bq + r$ com $\varphi_\alpha(r) < \varphi_\alpha(b)$. Daí:

$$\theta(r) \leqslant \varphi_\alpha(r) < \varphi_\alpha(b) = \theta(b),$$

provando que θ é um algoritmo em A.

■

Definição 4.1.2: O algoritmo construido na proposição acima é denominado **o menor algoritmo do anel euclidiano** A se considerarmos $\{\varphi_\alpha : A \to W\}_{\alpha \in I}$ a família de todos os algoritmos em A.

Proposição 4.1.3: (*Propriedades do menor algoritmo*): *Seja* A *um anel euclidiano com menor algoritmo* θ. *Então*:

i) $\theta = \theta_1$, *onde* θ_1 *é o algoritmo construido na proposição* 2.3.13 *a partir de* θ;

ii) $\theta(x) = 0$ *se e só se* $x = 0$;

iii) $\theta(1) = 1$;

iv) $\theta(x) = 1$ *se e só se* x *é um inversível.*

Prova: Da proposição 2.3.12 temos;

$\theta_1(0) = \theta(0) = 0$ e $\forall a \in A, a \neq 0$ temos $\theta_1(a) = \min_{b \in \langle a \rangle - \{0\}}\{\theta(b)\}$

Portanto

$$\forall a \in A,\ \theta_1(a) \leqslant \theta(a) = \min\{\varphi_\alpha(a) \mid \alpha \in I\}.$$

Como $\{\varphi_\alpha\}_{\alpha \in I}$ denota a família de todos os algoritmos com valores em W, temos $\theta_1(a) \in \{\varphi_\alpha(a) \mid \alpha \in I\}$. Portanto:

$$\forall a \in A,\ \theta_1(a) \leqslant \theta(a) = \min\{\varphi_\alpha(a) \mid \alpha \in I\} \leqslant \theta_1(a),$$

ou seja, $\theta_1 = \theta$, o que prova (*i*).

Para provar (*ii*), inicialmente observe que, pela observação feita antes da

proposição 4.1.1, é claro que $\theta(0) = 0$. Para a recíproca, basta aplicar a proposição 2.3.2.

E para provar (*iii*), inicialmente observe que $\theta(1) \geqslant 1$, uma vez que $\mathbb{N}$ é um segmento inicial de mW. Além disso,por (*i*) e pelo corolário 2.3.15, temos que

$$\theta(y) = \theta(1) \Leftrightarrow y \in U(A),$$

e portanto pela proposição 2.3.3, $\theta(1)$ é o menor elemento de $\theta(A) - \{\theta(0)\}$.

Suponhamos agora que $\theta(1) = s > 1$. Então, para todo $x \in A$, $x \neq 0$, temos

$$\theta(x) \geqslant \theta(1) = s > 1$$

e portanto,

$$\theta(x) - s \geqslant 0.$$

Daí consideramos a função $\theta' : A \to W$ dada por

$$\theta'(x) = \begin{cases} 0, \text{ se } x = 0 \\ \theta(x) - s + 1, \text{ se } x \neq 0. \end{cases}$$

Afirmamos que θ' é um algoritmo.

De fato, para todo $a, b \in A$, $b \neq 0$, temos que

$$a = bq + r, \text{ com } \theta(r) < \theta(b).$$

Se $r = 0$ então

$$\theta'(r) = 0 < 1 \leqslant \theta(b) - s + 1 = \theta'(b).$$

Se $r \neq 0$ então

$$\theta'(r) = \theta(r) - s + 1 < \theta(b) - s + 1 = \theta'(b).$$

Note agora que

$$\theta'(1) = \theta(1) - s + 1 = 1 < s = \theta(1),$$

o que é absurdo pois θ é o menor algoritmo.

Finalmente, note que (*iv*) é conseqüência da demonstração de (*iii*).

■

A proposição a seguir nos ajuda a construir o menor algoritmo:

Proposição 4.1.4: *Seja $\theta : A \to W$ o menor algoritmo em um anel euclidiano A. Para $\alpha \in W$ consideremos os conjuntos*:

$$A_\alpha = \{x \in A \mid \theta(x) \leqslant \alpha\} \quad \text{e} \quad A'_\alpha = \{x \in A \mid \theta(x) < \alpha\}.$$

Então A_α é a união de $\{0\}$ com o conjunto de todos os elementos $b \in A$ tais que a aplicação canônica $A'_\alpha \to \frac{A}{\langle b \rangle}$ é sobrejetora (isto é, representantes de todas as classes

mod$\langle b\rangle$ *podem ser encontrados em* A'_α).

Prova: Dado $b \in A_\alpha$, se $a + \langle b\rangle$ com $a \in A$, é uma classe qualquer mod$\langle b\rangle$, então, escrevendo $a = bq + r$, com $\theta(r) < \theta(b)$, encontramos um representante r desta classe tal que $\theta(r) < \theta(b) \leqslant \alpha$, e portanto, $r \in A'_\alpha$.

Reciprocamente, suponhamos agora que $b \neq 0$ é tal que $A'_\alpha \to \frac{A}{\langle b\rangle}$ é sobrejetora, e suponha que $\theta(b) > \alpha$. Chegaremos a um absurdo definindo $\sigma : A \to W$ por

$$\sigma(x) = \begin{cases} \alpha, \ se\ x = b \\ \theta(x), \ se\ x \neq b \end{cases}$$

e mostrando que σ é um algoritmo, pois daí $\sigma(b) = \alpha < \theta(b)$ contradiz o fato de que θ é o menor algoritmo. E, de fato, σ seria neste caso um algoritmo, pois:

(*i*) para as relações $a = cq + r$ com $\theta(r) < \theta(c)$ que não envolvem b, temos

$$\sigma(r) = \theta(r) < \theta(c) = \sigma(c);$$

(*ii*) para as relações em que b atua como divisor, sabemos que toda classe $\bar{a} \in \frac{A}{\langle b\rangle}$ tem um representante $r \in A'_\alpha$, isto é, $\theta(r) < \alpha < \theta(b)$, e portanto existem $q, r \in A$ tais que $a = bq + r$ com $\theta(r) < \theta(b)$;

(*iii*) para as relações $a = cq + b$ com $\theta(b) < \theta(c)$ em que b atua como resto, temos $c \neq b$ e portanto

$$\sigma(b) = \alpha < \theta(b) < \theta(c) = \sigma(c)$$

(*iv*) para as relações $b = aq + r$ com $\theta(r) < \theta(a)$ em que b atua como dividendo e não atua nem como resto nem como divisor, temos

$$\sigma(r) = \theta(r) < \theta(a) = \sigma(a);$$

e portanto σ é um algoritmo.

Logo $\theta(b) \leqslant \alpha$, ou seja, $b \in A_\alpha$.

■

Note que se A é um anel euclidiano e θ denota seu menor algoritmo então da proposição acima obtemos que

$$\theta(b) = \alpha \Leftrightarrow b \in A_\alpha - A'_\alpha.$$

Assim a proposição acima mostra que o menor algoritmo para um anel euclidiano pode ser construido por indução transfinita, uma vez que o conjunto A'_α determina A_α.

Exemplo 4.1.5: Pela proposição 4.1.3, já sabemos que $A_0 = \{0\}$ e

$A_2' = A_1 = \{0\} \cup U(A)$. Assim, $\theta(x) = 2$ significa que $\frac{A}{\langle x \rangle}$ admite um sistema de representantes constituído de zero e dos elementos invertíveis, de forma que x é necessariamente um elemento irredutível de A, pois se todo elemento não nulo de $\frac{A}{\langle x \rangle}$ é invertível então $\frac{A}{\langle x \rangle}$ é um corpo.

Salientamos três questões que são originadas com o exemplo acima:

a) pode ocorrer $A_2 - A_2' = \emptyset$ ou seja, não existir $x \in A$ tal que $\theta(x) = 2$, o que equivale a dizer que A pode não conter irredutíveis. De fato, este é o caso quando A é um corpo, e portanto um anel euclidiano. Veremos adiante em 4.1.11 um exemplo de anel não euclidiano onde também ocorre $A_2 - A_2' = \emptyset$. Na proposição 4.1.7 voltaremos a discutir a situação $A_\alpha = A_\alpha'$ para algum $\alpha \in W$.

b) a segunda observação é que a conclusão do exemplo acima não vale necessariamente para um algoritmo qualquer. De fato, se considerarmos o anel $A = \mathbb{Z}$, com o algoritmo definido em 2.3.12 temos que $\varphi(1) = 2$ e 1 não é irredutível.

c) temos também que não é válida a recíproca do exemplo acima, isto é, θ(irredutível)=2: mostraremos adiante, calculando o menor algoritmo em várias situações, que o menor algoritmo para $\mathbb{Z}$ é o dado pelo módulo. E lá $|5| = 5$ e 5 é irredutível.

Mostramos agora que a construção dos conjuntos $\{A_\alpha\}_{\alpha \in W}$ da proposição anterior serve também para detectar se um anel é ou não euclidiano.

A construção transfinita associada a um anel A. Seja A um anel, e W um conjunto bem ordenado como convencionado no início deste capítulo. Consideremos $A_0 = \{0\}$. Para $\alpha > 0$ em W, definimos A_α a partir dos conjuntos A_β com $\beta < \alpha$ por indução transfinita como segue: consideramos $A_\alpha' = \bigcup_{\beta<\alpha} A_\beta$ e definimos A_α como a união de $\{0\}$ e o conjunto de todos os elementos $b \in A$ tais que $A_\alpha' \to \frac{A}{\langle b \rangle}$ é sobrejetiva.

É claro que a seqüência $(A_\alpha)_{\alpha \in W}$ é crescente.

Teorema 4.1.6: *O anel A é euclidiano se e somente se a seqüência* $(A_\alpha)_{\alpha \in W}$ *exaure A.*

Prova: A proposição 4.1.4 nos mostra que se A for euclidiano então seu menor algoritmo gera tal seqüencia $(A_\alpha)_{\alpha \in W}$ e obviamente $\bigcup_{\alpha \in W} A_\alpha = A$.

Recíprocamente, se os conjuntos A_α construídos acima satisfazem $\bigcup_{\alpha \in W} A_\alpha = A$ então definimos a função $\theta : A \to W$ por

$$\theta(x) = \begin{cases} 0, \text{ se } x = 0 \\ \alpha \text{ se } x \neq 0 \text{ e } x \in A_\alpha - A'_\alpha \end{cases}$$

Afirmamos que θ é um algoritmo para A e, mais até, é o menor algoritmo de A.

Fixados $a, b \in A$ com $b \neq 0$, temos que $b \notin A_0$. No entanto, como $\bigcup_{\alpha \in W} A_\alpha = A$, existe $\alpha > 0$ tal que $b \in A_\alpha$. Tomando α o menor elemento de W satisfazendo esta propriedade temos que $b \notin \bigcup_{\beta < \alpha} A_\beta = A'_\alpha$, ou seja, $b \in A_\alpha - A'_\alpha$.

Mas da construção de A_α temos então que a aplicação $A'_\alpha \to \frac{A}{\langle b \rangle}$ é sobrejetora; em particular, existe $r \in A'_\alpha$ e $q \in A$ tais que $a = qb + r$.

Agora, $A'_\alpha = \bigcup_{\beta < \alpha} A_\beta$ e portanto $r \in A_\beta$ para algum $\beta < \alpha$, de modo que

$$\theta(r) \leqslant \beta < \alpha = \theta(\beta).$$

Assim, θ é um algoritmo, ou seja, A é de fato euclidiano.

■

A proposição a seguir nos mostra que a imagem do menor algoritmo em W não tem buracos:

Proposição 4.1.7: *Sejam A um anel euclidiano e θ seu menor algoritmo. Então cada $\alpha \in \theta(A)$ satisfaz a condição*

$$\forall \beta \in W, \ \beta \leqslant \alpha \Rightarrow \beta \in \theta(A).$$

Prova: Suponhamos que $A_\alpha = A'_\alpha$. Afirmamos que para todo $\beta \geqslant \alpha$, temos $A_\alpha = A'_\alpha$.

A prova é por indução transfinita, e como base de indução temos:

$$\begin{aligned} A_{\alpha+1} &= \{0\} \cup \{b \in A \mid A'_{\alpha+1} \to \tfrac{A}{\langle b \rangle} \text{ é sobrejetora}\} \\ &= \{0\} \cup \{b \in A \mid A'_\alpha \to \tfrac{A}{\langle b \rangle} \text{ é sobrejetora}\} \\ &= A_\alpha = A'_\alpha. \end{aligned}$$

Suponhamos agora que $\lambda > \alpha$ e que para todo $\alpha \leqslant \beta < \lambda$, $A_\beta = A'_\alpha$.

Daí:

$$A'_\lambda = \bigcup_{\beta < \alpha} A_\beta = \bigcup_{\beta < \alpha} A_\beta \cup \bigcup_{\alpha \leqslant \beta < \lambda} A_\beta = A'_\alpha \cup A'_\alpha = A'_\alpha$$

e portanto

$$A_\lambda = \{0\} \cup \{b \in A \mid A'_\lambda \to \tfrac{A}{\langle b\rangle} \text{ é sobrejetora}\}$$
$$= \{0\} \cup \{b \in A \mid A'_\lambda \to \tfrac{A}{\langle b\rangle} \text{ é sobrejetora}\}$$
$$= A_\alpha = A'_\alpha.$$

■

Corolário 4.1.8: *Sejam A um anel euclidiano e W um conjunto bem ordenado como convencionado no início deste capítulo. Então se existe* $\alpha \in W$ *tal que* $A_\alpha = A'_\alpha$ *então*

$$A \text{ é euclidiano} \Leftrightarrow A = \bigcup_{\beta \leq \alpha} A_\beta.$$

Apresentamos agora duas aplicações da construção transfinita:

Quando matemáticos começaram a estudar anéis de inteiros algébricos, perguntaram-se se tais anéis seriam euclidianos, mas sempre se referiam à norma como algoritmo. Aqui vamos responder a esta questão de modo geral, para o caso de anéis de inteiros algébricos associados a corpos quadráticos imáginários:

Proposição 4.1.9: *Os únicos corpos quadráticos imaginários cujo anel de inteiros algébricos A é euclidiano são os corpos* $\mathbb{Q}(\sqrt{-d})$ *com* $d \in \{1,2,3,7,11\}$.

Prova: Pela proposição 1.4.15, basta-nos considerar d livre de quadrados, de modo que $d \equiv 1,2$ ou $3(\mathrm{mod}4)$. Sabemos também pela proposição 1.4.18 que, exceto para os casos em que $d = 1$ e $d = 3$, os invertíveis em A são $U(A) = \{+1,-1\}$.

Vamos excluir da prova os casos em que $d = 1$ e $d = 3$, pois já mostramos no teorema 3.2 que a norma serve de algoritmo para estes casos.

Vamos considerar a construção transfinita para A, conservando a mesma notação citada anteriormente

$$A_0 = \{0\};$$
$$A_1 = \{0,+1,-1\} = \{0\} \cup U(A);$$

e então temos

$$A_2 - A_1 = \{b \in A \mid b \notin A_1 \text{ e } A_1 \to \tfrac{A}{\langle b\rangle} \text{ é sobrejetora}\}$$
$$= \{b \in A \mid b \notin A_1 \text{ e a aplicação } \{0,+1,-1\} \to \tfrac{A}{\langle b\rangle} \text{ é sobrejetora}\}$$

assim, podemos dizer

$$b \in A_2 - A_1 \Rightarrow n(b) = 2 \text{ ou } n(b) = 3.$$

Agora, considerando $-d \equiv 2 \pmod 4$ ou $-d \equiv 3 \pmod 4$ temos que pelo teorema 1.4.17 $A = \mathbb{Z} + \mathbb{Z}\sqrt{-d}$ e, para

$$b = a + c\sqrt{-d} \ (a, c \in \mathbb{Z})$$

$$n(b) = a^2 + c^2 d = 2 \text{ ou } n(b) = a^2 + c^2 d = 3.$$

É fácil ver que as equações acima têm solução apenas quando $d \leqslant 3$. Ou seja: se $-d \equiv 2$ ou $3 \pmod 4$ então $A_2 - A_1 \neq \emptyset$ apenas para $d \leqslant 3$, o que implica $d = 2$.

Ou seja, se $-d \equiv 2$ ou $3 \pmod 4$ então o anel de inteiros algébricos associado a $\mathbb{Q}\left(\sqrt{-d}\right)$ só tem chances de ser euclidiano para $d = 1$ ou $d = 2$. E, de fato $\mathbb{Q}\left(\sqrt{-1}\right)$ e $\mathbb{Q}\left(\sqrt{-2}\right)$ são euclidianos (para a norma), como mostramos no teorema 3.2.

Agora, se consideramos $-d \equiv 1 \pmod 4$ temos pelo teorema 1.4.17,

$$A = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{-d}}{2}\right).$$

Neste caso, se $b \in A$ é da forma

$$a + c\left(\frac{1+\sqrt{-d}}{2}\right) = \frac{2a+c}{2} + \frac{c}{2}\sqrt{-d},$$

com $a, c \in \mathbb{Z}$, então

$$n(b) = \left(\frac{2a+c}{2}\right)^2 + d\left(\frac{c}{2}\right)^2$$

e portanto

$$b \in A_2 - A_1 \Leftrightarrow n(b) = 2 \text{ ou } 3 \Leftrightarrow (2a + c)^2 + dc^2 = 8 \text{ ou } 12.$$

Novamente podemos dizer que as equações têm solução somente quando $d \leqslant 12$ e, portanto como $-d \equiv 1 \pmod 4$, temos que $d = 7$ ou $d = 11$ (lembre que $d \neq 3$). Assim, se $-d \equiv 1 \pmod 4$ então o anel de inteiros algébricos associado a $\mathbb{Q}\left(\sqrt{-d}\right)$ só tem chances de ser euclidiano para $d = 3, 7$ ou 11. E, de fato $\mathbb{Q}\left(\sqrt{-3}\right)$, $\mathbb{Q}\left(\sqrt{-7}\right)$ e $\mathbb{Q}\left(\sqrt{-11}\right)$ são euclidianos (para a norma), como mostramos no teorema 3.2.

■

Juntando os resultados obtidos com o teorema 3.2 e a proposição 4.1.9 podemos portanto afirmar:

Corolário 4.1.10: *Os únicos corpos quadráticos imaginários cujo anel de inteiros algébricos A é euclidiano são os corpos* $\mathbb{Q}(\sqrt{-d})$ *com* $d \in \{1, 2, 3, 7, 11\}$ *e, neste caso, tais anéis são até euclidianos para a função norma.*

Aqui surge-nos uma pergunta natural: nos casos mencionados no corolário

acima é a norma o menor algoritmo? Veremos adiante (após exemplo 4.1.90) que não.

Em [H-W], §14.7, é mencionado que o anel de inteiros algébricos associado a $\mathbb{Q}(\sqrt{-d})$ é um domínio fatorial para $d \in \{1,2,3,7,11,19,43,67,163\}$, e sabemos também que Stark[1] em 1967 provou que tais anéis são também principais.

Com o corolário acima concluimos:

Corolário 4.1.11: *O anel de inteiros algébricos associado a* $\mathbb{Q}(\sqrt{-d})$ *para* $d \in \{19,43,67,163\}$ *é um anel principal, fatorial mas não é euclidiano.*

Exemplo 4.1.12: Da proposição acima já conhecemos então vários exemplos de anéis (até domínios) que não são euclidianos. De fato, o que a demonstração acima nos diz é que se A é o anel de inteiros algébricos associados a $K = \mathbb{Q}\left(\sqrt{-5}\right)$ então, como $-5 \notin \{-1,-2,-3,-7,-11\}$, temos que, pela proposição 4.1.9, A não é euclidiano.

Como outra aplicação da construção transfinita podemos também agora mostrar que se generalizarmos a definição de anel euclidiano exigindo que W seja apenas um conjunto parcialmente ordenado com condição de cadeia descendente então não vamos aumentar a família de anéis euclidianos.

Proposição 4.1.13: *Seja A um anel, T um conjunto parcialmente ordenado com condição de cadeia descendente e $\varphi : A \to T$ uma aplicação tal que, dados quaisquer $a,b \in A$, com $b \neq 0$, existem $q,r \in A$ tais que $a = bq + r$ e $\varphi(r) < \varphi(b)$. Então A é euclidiano.*

Prova: Seja (A_α) a construção transfinita em A e $A' = \bigcup_{\alpha \in W} A_\alpha$, onde W é um conjunto bem ordenado que satisfaz $\#W > \#A$.

Se $A' \neq A$, escolhemos $b \in A - A'$ tal que $\varphi(b)$ é minimal (tal b de fato existe pois se T satisfaz a condição de cadeia descendente então todo subconjunto de T tem elemento minimal). Então, para todo $r \in A$,

$$\varphi(r) < \varphi(b) \Rightarrow r \in A',$$

e portanto da hipótese obtemos que

$$A' \to \frac{A}{\langle b \rangle} \text{ é sobrejetiva.}$$

Mas isto implica $b \in A'$, uma contradição.

Portanto, temos que $A' = A$ donde, pelo teorema 4.1.6, concluimos que A é euclidiano.

■

4.2. Exemplos de construção do menor algoritmo

Passamos agora a apresentar exemplos onde podemos identificar o menor algoritmo.

Exemplo 4.2.1: Consideremos $A = \mathbb{Z}$. Inicialmente observe que, como $(\mathbb{Z},|\ |)$ tem $W = \mathbb{N}$, então o menor algoritmo em $\mathbb{Z}$ vai ter $W = \mathbb{N}$. Como $U(\mathbb{Z}) = \{\pm 1\}$ é finito, já sabemos pela proposição 2.3.22 que cada A_n é uma união finita de conjuntos finitos, portanto também é finito. Afirmamos que para todo $n \in \mathbb{N}$, $A_n = \{r \in \mathbb{Z} | -2^n < r < 2^n\}$ (e portanto $x \in A_n$ se e só se o nº de dígitos de x na base 2 é n).

De fato, por indução sobre n temos:

para $n = 0$, temos:

$$A_0 = \{0\};$$

e para $n = 1$, temos:

$$A_1 = \{0\} \cup U(A) = \{0,+1,-1\} = \{r \in \mathbb{Z} | -2^1 < r < 2^1\}.$$

Seja $n \geqslant 1$ e suponhamos que

$$A_n = \{r \in \mathbb{Z} | -2^n < r < 2^n\}.$$

Então A_n tem $2(2^n - 1) + 1 = 2^{n+1} - 1$ elementos.

Agora, observe que

$$b \in A_{n+1} \text{ e } b \neq 0 \Rightarrow$$

$$\text{a aplicação } A_n \to \frac{\mathbb{Z}}{\langle b \rangle} \text{ é sobrejetora} \Rightarrow$$

$$\frac{\mathbb{Z}}{\langle b \rangle} \text{ tem } 2^{n+1} - 1 \text{ elementos ou menos} \Rightarrow$$

$$|b| < 2^{n+1} \Rightarrow$$

$$-2^{n+1} < b < 2^{n+1}.$$

A recíproca é clara. Assim,

$$A_{n+1} = \{r \in \mathbb{Z} | -2^{n+1} < r < 2^{n+1}\}.$$

Sendo assim, como o menor algoritmo em $\mathbb{Z}$ tem imagem $\mathbb{N}$, temos

$$\theta(r) = n \Leftrightarrow r \in A_n - A_{n-1} = \{r \in \mathbb{Z} | 2^{n-1} < |r| < 2^n\}$$

$\Leftrightarrow$ r envolve exatamente n dígitos na sua representação em base 2.

■

Exemplo 4.2.2: Tomemos $A = K[X]$, com K =corpo. Como $U(A) = U(K)$ temos que

$$A_0 = \{0\};$$
$$A_1 = K.$$

Daí:

$$A_2 = \{0\} \cup \{p(X) \in K[X] \mid A_1 \to \frac{K[X]}{\langle p(X)\rangle} \text{ é sobrejetora}\}.$$

Mas $K \to \frac{K[X]}{\langle p(X)\rangle}$ é sobrejetora se e somente se $\partial(p(X)) = 1$, e então:

$$A_2 = \{0\} \cup \{p(X) \in K[X] \mid \partial(p(X)) < 2\}.$$

Afirmamos que $A_n = \{0\} \cup \{p(X) \in K[X] \mid \partial(p(X)) < n\}$.

Por indução temos que:

$$A_{n+1} = \{0\} \cup \{p(X) \in K[X] \mid A_n \to \frac{K[X]}{\langle p(X)\rangle} \text{ é sobrejetora}\},$$

onde

$$A_n = \{0\} \cup \{p(X) \in K[X] \mid \partial(p(X)) < n\}.$$

Mas $\frac{K[X]}{\langle q(X)\rangle}$ tem para representantes polinômios de grau menor que $\partial(q(X))$. Daí,

$$q(X) \in A_{n+1},\ q(X) \neq 0 \Leftrightarrow \partial(q(X)) \leqslant n$$

e, portanto temos que

$$A_{n+1} = \{0\} \cup \{q(X) \in K[X] \mid \partial(q(X)) \leqslant n\}$$
$$A_{n+1} = \{0\} \cup \{q(X) \in K[X] \mid \partial(q(x)) < n+1\}.$$

Ou seja:

$$\theta(q(X)) = s \Leftrightarrow q(X) \in A_s - A_{s-1} \Leftrightarrow \partial(q(X)) = s-1 \Leftrightarrow s = \partial(q(X)) + 1.$$

Temos então que o menor algoritmo em $K[X]$ é o algoritmo dado por

$$\theta(p(X)) = \begin{cases} 1 + \partial(p(X)), \text{ se } p(X) \neq 0 \\ 0 \text{ se } p(X) = 0. \end{cases}$$

que é precisamente o algoritmo do exemplo 2.3.8, que, como vimos no início do capítulo 3, é um algoritmo isomorfo a norma.

Exemplo 4.2.3: Seja A um domínio principal com um número finito de ideais maximais $\langle p_i\rangle (i = 1,2,...,n)$, e seja v_i a valorização p_i-ádica de A. De acordo com a

proposição 2.3.17 e com o corolário 2.3.16 temos que o menor algoritmo θ em A é dado por

$$\theta(x) = \begin{cases} 1 + \sum_{i=1}^{n} v_i(x) \text{ se } x \neq 0 \\ 0 \text{ se } x = 0. \end{cases}$$

Exemplo 4.2.4: Sejam (D, φ) um domínio euclidiano, S um sistema multiplicativo em D com $0 \notin S$. Na proposição 2.3.23 vimos que φ dá origem a um algoritmo φ' para D_S. A questão é: quando $\varphi = \theta$ (o menor algoritmo para D), será que θ' é o menor algoritmo para D_S? A resposta é não.

Tomemos $D = \mathbb{Z}$ e para sistema multiplicativo S de $\mathbb{Z}$ o conjunto dos números primos com 6. Daí

$$\mathbb{Z}_S = \left\{ \tfrac{s_1}{s_2} 2^a 3^b \,|\, s_1, s_2 \in S \text{ e } a, b \in \mathbb{N} \right\}.$$

Denotemos por θ_S o menor algoritmo de $\mathbb{Z}_S$.

Pelo exemplo 4.2.1,

$$\theta(4) = \theta(0.2^0 + 0.2^1 + 1.2^2) = 3$$
$$\theta(9) = \theta(1.2^0 + 0.2^1 + 0.2^2 + 1.2^3) = 4.$$

Portanto, pela proposição 2.3.23,

$$\theta'(4) = \theta(4) = 3 \quad \text{e} \quad \theta'(9) = \theta(9) = 4.$$

Afirmamos que no entanto

$$\theta_S(4) = 3 = \theta_S(9),$$

e portanto θ' não é o menor algoritmo de $\mathbb{Z}_S$.

De fato, a construção transfinita nos dá:

$$A_0 = \{0\}$$
$$A_1 = \{0\} \cup U(\mathbb{Z}_S) = \{0\} \cup \{ \tfrac{s_1}{s_2} \,|\, s_i \in S \}$$

e também

$$\tfrac{b}{s} \in A_2 \text{ com } \tfrac{b}{s} \notin A_1 \Leftrightarrow \text{se a aplicação } A_1 \to \tfrac{\mathbb{Z}_S}{\langle \frac{b}{s} \rangle} \text{ é sobrejetora,}$$

ou seja,

$$\tfrac{b}{s} = \tfrac{s_1}{s_2} 2^m 3^n, \text{ com } m, \ n \text{ ambos não nulos e } s_1 \neq 0 \text{ está em } A_2 \Leftrightarrow$$
$$A_1 \to \tfrac{\mathbb{Z}_S}{\langle \frac{b}{s} \rangle} \text{ é sobrejetora.}$$

Note agora que

$$\tfrac{\mathbb{Z}_S}{\langle \frac{b}{s} \rangle} = \left\{ \overline{2^u 3^v} \,|\, 0 \leqslant u < m \text{ e } 0 \leqslant v < n \right\}.$$

Logo, temos

$$A_1 \to \frac{\mathbb{Z}_S}{\langle \frac{b}{s} \rangle} \text{ é sobrejetora} \Leftrightarrow$$

a aplicação $\{0\} \cup \{\frac{s_1}{s_2} | s_i \in S\} \to \left\{\overline{2^u 3^v} | \ 0 \leqslant u < m \text{ e } 0 \leqslant v < n\right\}$ é sobrejetora,

o que só é possível para $m = n = 1$.

Concluimos assim que

$$\frac{2s_1}{s}, \frac{3s_1}{s} \in A_2 \text{ e ainda } \theta_S(2^2) \geqslant 3 \text{ e } \theta_S(3^2) \geqslant 3.$$

Temos também que

$$\frac{b}{s} \in A_2 - A_1 \Leftrightarrow \frac{b}{s} = \frac{s_1}{s} 2^m 3^n$$

com $(m,n) = (1,0)$ ou $(m,n) = (0,1)$, e portanto

$$A_2 = A_1 \cup \left\{\frac{2s_1}{s}, \frac{3s_1}{s} | s, s_1 \in S\right\}$$

e portanto

$$\theta_S(2) = \theta_S(3) = 2.$$

Agora, note que a aplicação $A_2 \to \frac{\mathbb{Z}_S}{\langle \frac{b}{s} \rangle}$ é sobrejetora se $b = 2^2$ ou $b = 3^2$,

de modo que

$$2^2, 3^2 \in A_3.$$

Em particular,

$$\theta_S(4) = \theta_S(9) = 3.$$

■

Exemplo 4.2.5: O menor algoritmo, apesar de muitas vezes computável, tem em geral uma "estrutura" bastante complicada, como por exemplo, no caso em que A é anel de inteiros em um corpo quadrático imaginário. Aqui, por termos $U(A)$ sempre finito, (veja teorema 1.4.18), temos que, por 2.3.22, cada A_n é também finito. No entanto, o autor Samuel comenta que parece não haver uma regularidade em tais conjuntos, por exemplo para $\mathbb{Z} + \mathbb{Z}[\sqrt{-2}]$ ele informa que as cardinalidades dos conjuntos $A_0, A_1, A_2, ..., A_9$ são respectivamente $1, 3, 9, 21, 35, 61, 9, 153, 227, 327$.

Note que neste caso a norma não é o menor algoritmo para $\mathbb{Z} + \mathbb{Z}[\sqrt{-2}]$. De fato: em $K = \mathbb{Q}[\sqrt{-2}]$ temos que $-2 \equiv 2 (\text{mod } 4)$ e então $I_K = \mathbb{Z} + \mathbb{Z}[\sqrt{-2}]$. Sabendo que se N é a função norma, $N(a + b\sqrt{-2}) = a^2 + 2b^2$ para todo $(a + b\sqrt{-2}) \in I_K$; daí:

$$A_0 = \{0\};$$

$$A_1 = \{0\} \cup U(I_K) = \{0\} \cup \{\pm 1\} \Rightarrow \#A_1 = 3;$$

$A_2 = \{\beta \in I_K \mid N(\beta) \leqslant 2\} = \{a + b\sqrt{-2} \mid a^2 + 2b^2 \leqslant 2\} = \{0, \pm 1, \pm\sqrt{-2}\} \Rightarrow \#A_2 = 5.$

Mas segundo as contas de Samuel, $\#A_2 = 9$. Logo, N não é o menor algoritmo neste caso.

Finalmente, gostaríamos de salientar que não sabemos ainda se a troca de $\mathbb{N}$ por um conjunto W bem ordenado qualquer na definição de algoritmos euclidianos aumenta o número de domínios euclidianos. Como alguns anéis euclidianos interessantes admitem algoritmos em conjuntos bem ordenados de estrutura diferente de $\mathbb{N}$, (veja o exemplo 2.3.11), deveríamos nos perguntar se: "Dado um domínio euclidiano, o seu menor algoritmo é um algoritmo cujo contradomínio é $\mathbb{N}$?" Esta pergunta ainda não foi respondida para o caso geral; no entanto:

Proposição 4.2.6: *Em um domínio euclidiano D, de dimensão um e com corpos de restos finitos, o menor algoritmo θ é um algoritmo cujo contradomínio é $\mathbb{N}$.*

Prova: Por absurdo, suponhamos que existe um elemento $b \in D$ tal que $\theta(b) = \varpi$, onde ϖ denota o primeiro ordinal transfinito do contradomínio de θ. Como D tem corpos de restos finitos, temos, pela proposição 1.2.30, que $\frac{D}{\langle b \rangle}$ é finito, digamos, $\{c_1 + \langle b \rangle, \ldots, c_s + \langle b \rangle\}$. Cada classe $c_i + \langle b \rangle$ admite um representante r_i com $\theta(r_i) < \varpi = \theta(b)$, isto é, $\theta(r_i) \in \mathbb{N}$; portanto, $n = 1 + \max_{1 \leqslant i \leqslant s} \{\theta(r_i)\}$ é um número natural. Assim, $A_{n-1} \to \frac{D}{\langle b \rangle}$ é sobrejetora, nos indicando que $b \in A_n$ $\theta(b) = n$.

■

BIBLIOGRAFIA

[**A-M**]: ATIYAH, M; MAC DONALD, I. *Introduction to Commutative Algebra*. Addison-Wesley Publisching Company, Massachusetts, 1969.

[**C-D**]: *Euclid's Algorithm in Real Quadratic Fields*. Canadian Journal of Math 2, 289-296 (1950).

[**E**]: ENDLER, O. *Teoria dos Números Algébricos*. IMPA, Rio de Janeiro, 1986.

[**G-L**]: GARCIA, A; LEQUAIN, Y.*Álgebra*: *Um Curso de Introdução*. IMPA, Rio de Janeiro, 1988.

[**Ha**]: HALMOS, P. *Teoria Ingênua dos Conjuntos*. Ed. Polígono, São Paulo, 1973

[**H-W**]: HARDY, G; WRIGHT, E. *An Introduction to the Theory of Numbers*. Oxford University Press, London, 1954.

[**H**]: HERSTEIN, I.N., *Tópicos de Álgebra*. Editora da Universidade e Polígono. São Paulo, 1970.

[$\mathbf{R}_1$]: RIBENBOIM, P. *Théorie des Valuations*. Université de Montreal, Montreal, 1964.

[$\mathbf{R}_2$]: RIBENBOIM, P. *Algebraic Numbers*. John Witey & Sons, Inc., New York, 1972.

[$\mathbf{S}_1$]: SAMUEL, P. *Teoría Algebraica de Números*. Ediciones Omega, Barcelona, 1972.

[$\mathbf{S}_2$]: SAMUEL, P. *About Euclidean Rings*. Journal of Algebra 19, 282-301 (1971).

[**St**]: STEWART, I. *Galois Theory*. Chapman and Hall Ltd, London, 1973.

[**S-T**]: STEWART, I.; TALL, D. *Algebraic Number Theory*. Chapman and Hall Ltd, London, 1979.

[**Z-S**]: ZARINSKI, O.; SAMUEL, P. *Commutative Algebra, Vol I,II*. D. Van Nostrand Company, New Jersey, 1958.