# ANÉIS EUCLIDIANOS

LUIZ ANTÔNIO PERESI

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência de Computação da Universidade Estadual de Campinas como requisito parcial para obtenção do título de Mestre em Matemática.

ORIENTADOR: Prof. Dr. JOHN EDMONDS DAVID

Este trabalho foi realizado com o auxílio financeiro da Fundação de Amparo À Pesquisa do Estado de São Paulo.

-dezembro de 1977-

A meus pais e Miyako

# INTRODUÇÃO

O objetivo do presente trabalho é um estudo dos anéis euclidianos e introdução aos problemas em aberto dessa área.

Iniciamos o nosso trabalho apresentando as definições e resultados básicos dos anéis euclidianos, suas propriedades elementares e de estabilidade e os exemplos clássicos.

Em seguida, mostramos que todo anel euclidiano admite um algorítmo mínimo. Esse algorítmo mínimo pode ser construido por construção transfinita. Essa construção fornece uma condição necessária e suficiente para que um anel de integridade seja euclidiano. Apresentamos duas construções transfinitas: uma feita por T. Motzkin ((4), 1949) e a outra por P. Samuel ((10); 1971). Mostramos que a construção transfinita de Samuel nada mais é que uma generalização da construção transfinita de Motzkin. Além disso, mostramos que um anel de integridade é Motzkin-euclidiano se e somente se é Samuel euclidiano (quando o conjunto W da construção transfinita de Samuel é o anel dos inteiros). Esses dois últimos resultados são inéditos do nosso conhecimento.

Em vários casos, o algorítmo mínimo pode ser explicitamente construido, mas sua estrutura é complicada em geral. Construimos o algorítmo mínimo para o anel dos números inteiros, para o anel dos polinômios em uma variável e para um anel principal com um número finito de ideais maximais.

Seja A um domínio euclidiano, $\theta$ seu algorítmo mínimo e S um sistema multiplicativo de A com $0 \notin S$. O algorítmo $\theta$ induz um algorítmo $\theta'$ em $S^{-1}A$ (lema 1.4.6). $\theta'$ não é necessariamente o algorítmo mínimo de $S^{-1}A$. Como exemplo, construimos o algorítmo mínimo $\theta''$ de $S^{-1}A$, $A = Z$ e S o conjunto dos números inteiros primos com 6 e mostramos que esse algorítmo é diferente de $\theta'$. Nossa descrição explicita de $\theta''$

também é inédita do nosso conhecimento.

A seguir, apresentamos alguns resultados básicos sôbre domínios de Dedekind e número de classe. Em particular, apresentamos o número de classe dos inteiros algébricos de $Q[\sqrt{d}]$, para diversos d (d inteiro positivo livre de quadrados).

Classificamos todos os anéis de inteiros de $Q[\sqrt{-d}]$ e alguns anéis de $Q[\sqrt{d}]$ (d inteiro positivo livre de quadrados) e de corpos ciclotômicos, que são euclidianos.

Terminamos apresentando exemplos de anéis principais que não são euclidianos e problemas em aberto.

Quero externar aqui o meu agradecimento ao Prof. Dr. John Edmonds David pela proposição do presente trabalho, pela orientação, pelo incentivo e, principalmente, pela resolução dos problemas inéditos apresentados.

Agradeço o apoio da FAPESP através da concessão de bolsas de estudo, sem as quais este trabalho não teria sido realizado.

# ÍNDICE

# CAPÍTULO - 1

## ANÉIS EUCLIDIANOS

### 1.1 - Definições e resultados básicos

Definição 1.1.1 - Dado um anel comutativo A, um algorítmo euclidiano em A é uma aplicação $\psi: A \longrightarrow W$, onde W é um conjunto bem ordenado, tal que:

(a) $\psi(ab) \geq \psi(a)$ para todo $a, b \in A-(0)$

(b) dados $a, b \in A$, $b \neq 0$, existem $q, r \in A$, tais que

$a = bq + r$ e $\psi(r) < \psi(b)$

Definição 1.1.2 - Um anel de integridade com algorítmo euclidiano é denominado anel euclidiano.

Teorema 1.1.3 - Seja A um anel euclidiano e seja I um ideal de A. Então, existe um elemento $a_0 \in I$ tal que I consiste exatamente de todos os $a_0x$ quando x percorre A.

Demonstração:

Se I consiste exatamente do elemento 0, basta fazer $a_0 = 0$ e a conclusão do teorema vale.

Assim, podemos admitir que $I \neq (0)$; portanto, existe $a \neq 0$ em I. Tomamos um $a_0 \in I$ tal que $\psi(a_0)$ seja mínimo.

Suponhamos que $a \in I$. Pela propriedade (b) do algorítmo

em A (1.1.1), existem t, r ε A tais que $a = ta_0 + r$ onde $r = 0$ ou $\psi(r) < \psi(a_0)$. Como a e $ta_0$ estão em I, segue que $r \varepsilon I$. Da escolha de $a_0$, a única possibilidade para r é $r = 0$, e $a = ta_0$, o que demonstra o teorema.

Representamos o ideal de todos os múltipos de a por (a) ou Aa.

Definição 1.1.4 - Um anel de integridade A com elemento unidade é um anel principal se todo ideal I em A é da forma I = Aa para algum a ε I.

Corolário 1.1.5 - Um anel euclidiano possui um elemento unidade.

Demonstração:

Seja A um anel euclidiano. Como A é um ideal de A, pelo teorema 1.1.3, existe $u_0 \varepsilon A$ tal que $A = (u_0)$. Logo, $u_0 = u_0 c$ para algum $c \varepsilon A$.

Se $a \varepsilon A$, $a = xu_0$, para algum $x \varepsilon A$. Logo, $ac = (xu_0)c = x(u_0 c) = xu_0 = a$. Assim, c é o elemento unidade.

Denotamos o elemento unidade de um anel euclidiano por 1.

Em vista do teorema 1.1.3 e do seu corolário 1.1.5, pode-mos concluir que todo anel euclidiano é um anel principal.

Definição 1.1.6 - Se $a \neq 0$ e b estão em um anel comutativo A, então a divide b, se existe $c \varepsilon A$ tal que $b = ac$.

Usamos a notação a / b para representar o fato de que a divide b.

Definição 1.1.7 - Se $a,b \varepsilon A$, então $d \varepsilon A$ é dito um máximo di-

visor comum de a e b se:

(1) $d / a$ e $d / b$

(2) sempre que $c / a$ e $c / b$, então $c / d$

Usamos a notação $d = (a,b)$.

Lema 1.1.8 - Seja A um anel euclidiano. Então, dois elementos quaisquer a e b em A possuem um máximo divisor comum d. Além disso, $d = \lambda a + \mu b$ para certos $\lambda, \mu \in A$.

Demonstração :

Seja $I = \{ra + sb , r \text{ e } s \text{ percorrendo } A\}$. Afirmamos que I é um ideal de A. De fato, se x e y estão em I, então $x = r_1 a + s_1 b$ e $y = r_2 a + s_2 b$. Logo, $x - y = (r_1 - r_2)a + (s_1 - s_2)b \in I$. Se $u \in A$, $ux = u(r_1 a + s_1 b) = (ur_1)a + (us_1)b \in I$.

Como I é ideal, pelo teorema 1.1.3, existe um elemento d em I tal que $I = (d)$. Do fato de $d \in I$ e todo elemento de I ser da forma $ra + sb$, $d = \lambda a + \mu b$ para certos $\lambda, \mu \in A$.

Pelo corolário 1.1.5, A possui um elemento unidade. Assim, $a = 1a + 0b \in I$ e $b = 0a + 1b \in I$. Estando em I são ambos múltiplos de d , donde $d / a$ e $d / b$.

Suponhamos, finalmente, que $c / a$ e $c / b$; então, $c / \lambda a$ e $c / \mu b$, de modo que $c / \lambda a + \mu b = d$.

Portanto, d satisfaz todas as condições exigidas para um máximo divisor comum e o lema está demonstrado.

Definição 1.1.9 - Seja A um anel comutativo com elemento unidade 1. Um elemento $a \in A$ é uma unidade em A se existe um elemento $b \in A$ tal que $ab = 1$.

Definição 1.1.10 - Seja A um anel comutativo com elemento uni-

dade. Dois elementos a e b são ditos associados se b = ua para alguma unidade u em A.

Lema 1.1.11 - Seja A um anel euclidiano e a, b ε A. Então, para todo algorítmo $\psi$ em A, temos:

(1) Se b não é uma unidade, $\psi(a) < \psi(ab)$

(2) a é uma unidade se e somente se $\psi(a) = \psi(1)$

Demonstração :

(1) Pela condição (b) da definição de algorítmo euclidiano (1.1.1), a = abx + r onde r ε A e $\psi(r) < \psi(ab)$. Logo, r = a - abx = a(1 -bx) e r ε Aa. Como o valor que $\psi$ assume em a é o mínimo de $\psi$ para quaisquer valores de Aa e $\psi(r) < \psi(a)$, a única possibilidade é bx = 1 e b é uma unidade de A. Absurdo. b não é unidade, por hipótese.

O resultado disso é $\psi(a) < \psi(ab)$.

(2) Suponhamos que $\psi(a) = \psi(1)$. Como 1 e a são elementos de A, pela definição de anel euclidiano (1.1.2), segue que existem x, r ε A tais que 1 = ax + r, com $\psi(r) < \psi(a) = \psi(1)$. Se $r \neq 0$, então r = r.1, contrariando $\psi(r) < \psi(1)$. Logo, r = 0 e 1 = ax, donde a é uma unidade.

Se por outro lado, a é uma unidade, existe x ε A tal que ax = 1. Pela propriedade (a) da definição de algorítmo euclidiano (1.1.1), $\psi(a) \leq \psi(ax) = \psi(1)$ e também $\psi(1) \leq \psi(a.1) = \psi(a)$. Logo, $\psi(a) = \psi(1)$.

Definição 1.1.12 - No anel euclidiano A uma não unidade $0 \neq \pi$ é dito um elemento irredutível de A se sempre que $\pi = ab$ onde a e b estão em A, então a ou b é uma unidade.

Definição 1.1.13 - No anel euclidiano A, uma não unidade

$\pi$ é dito um elemento primo de A se sempre que $\pi / ab$, onde a e b estão em A, então $\pi / a$ ou $\pi / b$.

Lema 1.1.14 - Seja A um anel euclidiano, Então, todo elemento em A é uma unidade em A ou pode ser escrito como o produto de um número finito de elementos irredutíveis de A.

Demonstração :

A demonstração é feita por indução sôbre $\psi(a)$.

Se $\psi(a) = \psi(1)$, então a é uma unidade (1.1.11).

Admitimos que o lema seja verdadeiro para todos os elementos x em A tais que $\psi(x) < \psi(a)$. Se A é um elemento irredutível de A, nada há a demonstrar, Portanto, suponhamos que $a = bc$, onde b e c não são unidades em A. Pelo lema 1.1.11, $\psi(b) < \psi(bc) = \psi(a)$ e $\psi(c) < \psi(bc) = \psi(a)$. Assim, pela nossa hipótese de indução, b e c podem ser escritos como produtos de um número finito de elementos irredutíveis de A:

$b = \pi_1 \cdot \pi_2 \cdots \pi_n$ e $c = \pi'_1 \cdot \pi'_2 \cdots \pi'_m$.

Consequentemente,

$a = bc = \pi_1 \cdots \pi_n, \pi'_1 \cdots \pi'_m$ e desta forma a foi fatorado como um produto de um número finito de elementos irredutíveis. Isto completa a demonstração do teorema.

Definição 1.1.15 - No anel euclidiano A, a e b são ditos primos entre si (ou relativamente primos) se seu máximo divisor comum é uma unidade de A.

Como todo associado de um máximo divisor comum é um máximo divisor comum, e como o elemento unidade 1 é associado de qualquer unidade, se a e b são primos entre si podemos admitir que $(a,b) = 1$.

Lema 1.1.16 - Seja A um anel euclidiano. Suponhamos que para

$a, b \in A$, $a / bc$ e $(a,b) = 1$. Então, $a / c$.

Demonstração :

Do lema 1.1.8 e $(a,b) = 1$, segue que $1 = \lambda a + \mu b$. Multiplicando essa relação por c, obtemos $c = \lambda ac + \mu bc$. Ora, $a / \lambda ac$, sempre, e $a / \mu bc$ pois $a / bc$; portanto, $a / (\lambda ac + \mu bc) = c$.

Lema 1.1.17 - Se $\pi$ é um elemento irredutível no anel euclidiano A e $\pi / ab$; onde $a, b \in A$, então $\pi$ divide pelo menos a ou b.

Demonstração :

Suponhamos que $\pi$ não divide a; então $(\pi, a) = 1$; Pelo lema 1.1.16, $\pi / b$.

Corolário 1.1.18 - Se $\pi$ é um elemento irredutível no anel euclidiano A e se $\pi / a_1.a_2 \ldots a_n$ então $\pi$ divide pelo menos um dos $a_1, \ldots, a_n$.

Demonstração:

Segue do lema 1.1.17, por indução sôbre n.

Teorema 1.1.19 - (Teorema da Unicidade da fatoração)

Seja A um anel euclidiano e $a \neq 0$ uma não unidade em A. Suponhamos que $a = \pi_1.\pi_2 \ldots \pi_n = \pi'_1.\pi'_2 \ldots \pi'_m$ onde os $\pi_i$ e os $\pi'_j$ são elementos irredutíveis de A. Então, $n = m$ e cada $\pi_i$, $1 \leqslant i \leqslant n$ é associado a algum $\pi'_j$, $1 \leqslant j$, $j \leqslant m$ e, reciprocamente, cada $\pi'_k$ é associado a algum $\pi_q$.

Demonstração :

Como $a = \pi_1 \cdot \pi_2 \cdots \pi_n = \pi'_1 \cdot \pi'_2 \cdots \pi'_m$, $\pi_1$ divide $\pi_1 \cdot \pi_2 \cdots \pi_n$ e portanto $\pi_1$ divide $\pi'_1 \cdot \pi'_2 \cdots \pi'_m$. Pelo corolário 1.1.18, $\pi_1$ divide algum $\pi'_i$ ; como $\pi_1$ e $\pi'_i$ são ambos elementos irredutíveis de A, eles são associados e $\pi'_i = u_1 \cdot \pi_1$, onde $u_1$ é uma unidade de A. Assim, $\pi_1 \cdot \pi_2 \cdots \pi_n = \pi'_1 \cdot \pi'_2 \cdots \pi'_m = u_1 \cdot \pi'_1, \pi'_2, \cdots \pi'_{i-1} \cdot \pi_1 \cdot \pi'_{i+1} \cdots \pi'_m$. Cancelando $\pi_1$, ficamos com $\pi_2 \cdots \pi_n = \pi'_1 \cdots \pi'_{i-1} \cdot \pi'_{i+1} \cdots \pi'_m$. Após alguns passos, o primeiro membro torna-se o elemento unidade 1 e o segundo membro o produto de um certo número de $\pi'_j$ (o excesso de m sôbre n). Isto implica, $n \leq m$ (os $\pi'$ não são unidades).

Analogamente, $m \leq n$, de modo que $n = m$.

No processo, mostramos também que todo $\pi_i$ possui algum $\pi'_j$ como associado e reciprocamente.

Definição 1.1.20 - Um anel de integridade A, com elemento unidade, é um anel fatorial se:

(a) todo elemento não nulo em A é uma unidade ou pode ser escrito como o produto de um número finito de elementos irredutíveis de A.

(b) a decomposição na parte (a) é única a menos da ordem e de associados de elementos irredutíveis.

Combinando o lema 1.1.14 e o teorema 1.1.19, podemos concluir que todo anel euclidiano é um anel fatorial.

Definição 1.1.21 - Um anel comutativo A é um anel noetheriano se satisfaz a seguinte condição:

(acc) toda cadeia estritamente crescente de ideais de A é

finita.

Lema 1.1.22 - Todo anel principal é noetheriano.

Demonstração :

Seja A um anel principal. Seja $I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I_i$ uma cadeia estritamente crescente de ideais de A. $\cup I_i$ é um ideal de A. Como A é principal, existe $y \in \cup I_i$ tal que $\cup I_i = Ay$. Existe também um n tal que $y \in I_n$. Logo, $I_{n+k} \subseteq \cup I_i = Ay \subseteq I_n$, para todo k. Como $I_n \subseteq I_{n+k}$ para todo k, segue que $I_{n+k} = I_n$, para todo k.

Portanto, essa cadeia é finita, o que demonstra o lema.

Lema 1.1.23 - O ideal $I = (a_0)$ é um ideal maximal do anel euclidiano A se e somente se $a_0$ é um elemento irredutível de A.

Demonstração :

Demonstraremos primeiramente que se $a_0$ não for um elemento irredutível, então $I = (a_0)$ não é um ideal maximal. De fato, suponhamos que $a_0 = bc$, onde $b,c \in A$ e nem b e nem c são unidades. Seja $B = (b)$; então, certamente $a_0 \in B$ e logo $I \subset B$. Se $B = A$, então $1 \in B$ e $1 = xb$ para algum $x \in A$, implicando que b é uma unidade em A, o que é absurdo. Por outro lado, se $I = B$, então $b \in B = I$, donde $b = x.a_0$ para algum $x \in A$. Combinado com $a_0 = bc$, isto resulta em $a_0 = xca_0$, e consequentemente $xc = 1$. Mas isto implica que c é uma unidade em A, contradizendo novamente nossa hipótese. Portanto, B é diferente de I e A e, como $I \subset B$, I não pode ser um ideal maximal de A.

Reciprocamente, suponhamos que $a_0$ seja um elemento irredutí

vel de A e que U seja um ideal de A tal que $I = (a_0) \subseteq U \subseteq A$. Pelo teorema 1.1.3, $U = (u_0)$. Como $a_0 \in I \subseteq U = (u_0)$, $a_0 = xu_0$ para algum $x \in A$. Mas $a_0$ é um elemento irredutível de A, donde segue x ou $u_0$ é uma unidade em A. Se $u_0$ é uma unidade em A, $U = A$. Se, por outro lado, x é uma unidade em A, $x^{-1} \in A$ e a relação $a_0 = xu_0$ torna-se $u_0 = x^{-1}{}_0 \in I$, pois I é um ideal de A. Isto implica que $U \subseteq I$; junto com $I \subseteq U$ concluimos que $U = I$. Portanto, não existe nenhum ideal de A que esteja estritamente contido entre I e A. Isto significa que I é um ideal maximal de A.

Corolário 1.1.24 - Seja I um ideal de um anel principal A. Então, I está contido em um número finito de ideais maximais.

Demonstração:

Seja $x \in A$ tal que $I = (x)$. Sejam $M_i \supseteq I$ ideais maximais. Para todo i existem primos $p_i$ tais que $M_i = (p_i)$. Também, $M_i = M_j$ se e somente se $i = j$ e isto acontece se e somente se $p_i$ e $p_j$ são associados. Então, podemos definir

$I_i = \left(\frac{x}{p_1 \cdots p_i}\right)$. Claramente $I_i$ é um ideal de A e

$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots \subseteq I_i \subseteq \cdots$ Mas, pelo lema 1.1.21, A é noetheriano. Então, podemos concluir que essa cadeia é finita e isto é equivalente a "o ideal I está contido em um número finito de ideais maximais".

Corolário 1.1.25 - Seja A um anel principal, $p \in A$ primo e $x \in A$. Então, $p^i / x$ para no máximo um número finito de índices i.

Demonstração :

Para todo índice i tal que $p^i$ / x definimos $I_i = (\frac{x}{p^i})$. Claramente $I_i$ é um ideal de A e $I_i \subseteq I_{i+1}$ para todo índice i. Como,pelo lema 1.1.22, A é noetheriano , segue que a cadeia $I_1 \subsetneq I_2 \subsetneq \ldots$ é finita. Logo, o número de índices i para os quais $p^i$ / x é finito.

Teorema 1.1.26 - Todo anel principal A é anel fatorial.

Demonstração :

Seja x ε A. Se x é uma unidade ou um elemento primo de A, nada há a demonstrar.

Suponhamos que x não é unidade e não é primo. Pelo corolário 1.1.23, $(x) \subseteq M_1,\ldots,M_n$ onde os $M_i$ são ideais maximais de A. Como A é principal, existem $p_i,\ldots, p_n$ primos em A tais que $M_1 = (p_i),\ldots, M_n = (p_n)$. Pelo corolário 1.1.24, para i = 1,...,n existem $k_i$ tais que $p_i^1$ / x, ... , $p_i^{k_i}$ / x e $p_i^{k_i+1} \nmid x$. Também $p_i^{k_i}$ e $p_j^{k_j}$ não são iguais para $i \neq j$. Logo, $\P p_i^{k_i} / x$ e existe y ε A, tal que $x = \P p_i^{k_i}.y$. Se $(y) \neq A$, existe um ideal maximal M = (p), p primo em A, p não associado a nenhum $p_i$ (se p é associado a algum $p_i$, $p_i$ / y e $p_i^{k_i+1}$ / x, que é uma contradição ) tal que (y) = M. Isto contradiz o fato de que (x) está contido no máximo em n ideais maximais. Logo, (y) = A. O elemento 1 pertence a A; então, existe z ε A tal que yz = 1. Portanto, y é uma unidade.

Assim, demonstramos que todo elemento não unidade e não primo de A pode ser escrito como um produto de primos de A que implica A é fatorial.

## 1.2 - Propriedades elementares dos anéis euclidianos

Lema 1.2.1 - Para $b \in A$, $b \neq 0$, temos $\psi(b) > \psi(0)$. Logo, $\psi(0)$ é o menor elemento de $\psi(A)$.

Demonstração:

Pela parte (b) da definição de algorítmo euclidiano (1.1.1), $0 = bq + b_1$ com $\psi(b_1) < \psi(b)$. Por indução, definimos uma sequência $b, b_1, \ldots, b_n$ de elementos de A com a seguinte propriedade: se $b_n = 0$, a sequência já está construída; se $b_n \neq 0$ escrevemos $0 = b_n q_n + b_{n+1}$ com $\psi(b_{n+1}) < \psi(b_n)$. Como $(\psi(b_n))$ é uma sequência estritamente decrescente de elementos de um conjunto bem ordenado, deve ser finita. Logo, existe $n \geq 1$ tal que $b_n = 0$. Então, $\psi(0) = \psi(b_n) < \psi(b)$.

Lema 1.2.2 - Um elemento $b \in A$ tal que $\psi(b)$ é o menor elemento de $\psi(A) - \{\psi(0)\}$ é uma unidade em A.

Demonstração:

Por hipótese b é diferente de 0. Para todo a em A, temos $a = bq + r$ com $\psi(r) < \psi(b)$; logo $r = 0$. Então, $A = (b)$ e b é uma unidade.

Definição 1.2.3 - Uma aplicação $\psi: A \longrightarrow W$, onde A é um anel comutativo e W é um conjunto bem ordenado, satisfazendo a condição (b) da definição de algorítmo euclidiano (1.1.1), é denominado algorítmo fraco.

Um algorítmo fraco não satisfaz, necessariamente, a condição (a) da definição 1.1.1, como mostra o exemplo

Exemplo 1.2.4 - Seja $A = Z$, $\psi: A \longrightarrow N$, $\psi(n) = |n|$ para $n \neq 5$ e $\psi(5) = 13$.

Para todo $n \neq 0$ em A tal que $|n| \leq 5$ ou $|n| \geq 14$, os represen-

tantes $r = 0, 1, \ldots, |n| - 1$ de classes módulo n satisfazem $\psi(r) < \psi(n)$.

Para $6 \leq |n| \leq 13$ substituimos o representante 5 por $5 - |n|$, o qual também satisfaz $\psi(5 - |n|) < \psi(n)$. Logo, $\psi$ é um algorítimo fraco.

Mas $\psi(5) > \psi(10)$ e $\psi(5) > \psi(-5)$, contrariando a condição (a) da definição 1.1.1.

Entretanto, um anel com algorítmo fraco admite algorítmos euclidianos, como mostra o

Lema 1.2.5 - Se $\psi: A \longrightarrow W$ é um algorítmo fraco, então $\psi_1: A \longrightarrow W$, definido por $\psi_1(0) = \psi(0)$ e

$$\psi_1(a) = \min_{b \in Aa - (0)} \psi(b) \quad \text{para} \quad a \neq 0$$

é um algorítmo tal que:

a) $\psi_1(ac) = \psi_1(a)$ se e somente se $Aac = Aa$

b) $\psi_1(a) \leq \psi(a)$ para $a \in A$.

Demonstração :

Como W é bem ordenado $\psi_1$ está bem definida.

Se $b \in Aac$, então $b \in Aa$. Logo, $Aac \subset Aa$. Pela definição de $\psi_1$, $\psi_1(ac) \geq \psi_1(a)$. Isto demonstra a condição (a) da definição de algorítmo euclidiano (1.1.1).

Sejam $b \neq 0$ e $a \in A$; pela definição de $\psi_1$, $\psi_1(b) = \psi(bc)$ para um certo $c \in A$. Pela condição (b) da definição 1.1.1, $a = bcq + r$ com $\psi(r) < \psi(bc)$; logo, $\psi_1(r) \leq \psi(r) < \psi(bc) = \psi_1(b)$. Isto mostra que $\psi$ é um algorítmo.

Finalmente, como $a \in Aa - (0)$, da definição de $\psi_1$, segue que $\psi_1(a) \leq \psi(a)$ para todo $a \in A$. Isto demonstra a parte (b). Por outro lado, se $\psi_1(ac) = \psi_1(a)$, $a = acq + r$ com

$\psi_1(r) < \psi_1(a)$; como $r = a(1 - cq)$, a parte b) implica que $r = 0$. Logo, $Aac = Aa$. Assim, a parte a) do lema está demonstrada.

Em vista do lema 1.2.5, todo anel de integridade com algo-- rítmo fraco é euclidiano.

Corolário 1.2.6 - (recíproco do lema 1.2.2)

Se $\psi_1$ é como no lema 1.2.5 e se u é uma unidade de A, então $\psi_1(u)$ é o menor elemento $\beta$ de $\psi(A) - \{\psi(0)\}$.

Demonstração:

Pelo lema 1.2.2, existe uma unidade u' com valor $\psi_1(u') = \beta$. Como u é associado a u', $u' = uc$ para alguma unidade c em A. Logo, $Au' = Auc$ e pela parte a) do lema 1.2.4, $\psi_1(uc) = \psi_1(u')$. Como $\psi_1(uc) = \psi_1(u)$, segue que $\psi_1(u)$ é o menor elemento de $\psi(A) - \{\psi(0)\}$.

O corolário acima nem sempre vale para algorítmo fraco, como mostra o

Exemplo 1.2.7 - Em Z definimos: $\psi(n) = |n|$ para $n \neq 1$ e $\psi(1) = 2$. Para $n \neq 1$, usamos 0, 1, ... , $|n| - 1$ como represen tantes módulo n e para $n = 1$ usamos 0 e -1 como represen-- tante módulo 2. Assim, $\psi$ é um algorítmo fraco em Z. O elemento unidade 1 é uma unidade em A, mas $\psi(-1) = 1 < \psi(1) = 2$.

## 1.3 - Anéis de valorizações

Definição 1.3.1 - Seja A um domínio de integridade. Uma apli-- cação $V: K^* \longrightarrow G$, onde K é o corpo de frações de A, $K^* = K - \{0\} = \{\text{unidades de K}\}$ e G é um grupo abeliano totalmente or

denado, tal que $V(xy) = V(x) + V(y)$ e $V(x + y) \geq \min\{V(x), V(y)\}$ é denominada uma <u>valorização de K</u>.

O conjunto $A_V = \{x \in K^* \text{ tal que } V(x) \geq 0\} \cup \{0\}$ é um anel. De fato, se $x$ e $y \in A_V$ então $V(x) \geq 0$ e $V(y) \geq 0$. Como $V(x + y) \geq \min\{V(x), V(y)\}$, segue que $V(x + y) \geq 0$ e logo $x + y \in A_V$. Também, como $V(xy) = V(x) + V(y)$, segue que $V(xy) \geq 0$. As outras propriedades de anel seguem facilmente.

O anel $A_V$ é denominado <u>anel da valorização V</u>.

Seja A um anel principal. Vamos determinar todos os anéis das valorizações não triviais, do corpo de frações K de A, que contem A.

Seja $A_V$ o anel da valorização V de K tal que $A \subseteq A_V$. Seja p um primo em A. Definimos $V_p : K^* \longrightarrow Z$ da seguinte maneira: se $x \in K^*$, escrevemos $x = \frac{a}{b}$ com a e b em A; x pode ser escrito, também, como $x = p^t \frac{a'}{b'}$ com a' e b' em A, $(p,a') = (p,b') = 1$ e $t \in Z$; então, $V_p(x) = t$.

Por exemplo, se $A = Z$ e $p = 5$, então

$V(\frac{120}{32}) = 1$ pois $\frac{120}{32} = \frac{24}{32} \cdot 5^1$ e

$V(\frac{32}{120}) = -1$ pois $\frac{32}{120} = \frac{32}{24} \cdot 5^{-1}$

É fácil verificar que $V_p$ é uma valorização.

Vamos mostrar que $A_V = A_{V_p}$, para algum primo $p \neq 0$. Se $x \in A_V$, $x = \frac{a}{b} \cdot p^t$, $t \in Z$, $(a,p) = (b,p) = 1$ e

$0 \leq V(x) = V(\frac{a}{b}) + V(p^t) = V(a) + V(\frac{1}{b}) + V(p^t)$. Como

$0 = V(1) = V(\frac{b}{b}) = V(b \cdot \frac{1}{b}) = V(b) + V(\frac{1}{b})$,

$V(\frac{1}{b}) = - V(b)$. Logo, $0 \leq V(a) - V(b) + V(p^t)$.

Seja $M_V = \{x \in K^*$ tal que $V(x) > 0\}$. Como será mostrado no lema 1.3.7, $M_V$ é um ideal maximal de $A_V$. Também, $M_V \cap A$ é um ideal primo de A. De fato, se a e b estão em $A \subseteq A_V$ e ab está em $M_V \cap A$, então a ou b pertence $M_V$ ($M_V$ é maximal), Como a e b estão em A, a ou b pertence a $M_V \cap A$. Também, $M_V \cap A \neq (0)$. De fato, como V é não trivial, existe $0 \neq y \in M_V$. Escrevendo $x = \frac{c}{d}$, temos $0 < V(x) = V(c) - V(d)$ ou $V(d) < V(c)$. Como $A \subseteq A_V$, $0 \leq V(d)$ e, portanto, $0 < V(c)$. Logo, $c \in M_V \cap A \neq 0$. Portanto, $0 \neq M_V \cap A = A_p$ para algum primo $p \neq 0$ em A.

Como $(p,a) = 1$, $a \in A - (M_V \cap A)$ e $a \notin M_V$. Logo, $V(a) = 0$. Analogamente, $V(b) = 0$. Então, $0 < V(x) = V(p^t) = t.V(p)$. Como $V_p(p) \geq 0$, temos $t \geq 0$ e podemos concluir que $x \in A_{V_p}$.

Por outro lado, se $x \in A_{V_p}$ então $x = \frac{a}{b}.p^t$, $t \geq 0$, $1 = (a,p) = (b,p)$. Então, $V(x) = V(a) - V(b) + V(p^t) = t.V(p)$. Como $V(p) \geq 0$, $t.V(p) \geq 0$. Logo, $V(x) \geq 0$ e $x \in A_V$.

Definição 1.3.2 - Seja V uma valorização em K (corpo de frações do anel de integridade A). Seja p um primo tal que $A_V = A_{V_p}$. V é normal se $V = V_p$.

Definição 1.3.3 - Seja $V: K^* \longrightarrow G$ uma valorização. O conjunto $\Gamma_V = \{V(x)$ tal que $x \in K^*\}$ é denominado o grupo de valôres de V.

É fácil verificar que $(\Gamma_V, +)$ é um grupo abeliano totalmente

ordenado.

Definição 1.3.4 - Uma valorização $V: K^* \longrightarrow G$ é discreta (de pôsto 1) quando $\Gamma_V \simeq Z$ onde $\simeq$ significa isomorfismo de grupos abelianos totalmente ordenados.

Exemplo 1.3.5 - Seja A um domínio de integridade; $p \in A$ um primo tal que $\cap Ap^i = (0)$. Afirmamos que $V_p$ é uma valoriza-- ção discreta. De fato:

1) $V_p$ é bem definida em Z pois se $a \neq 0$ e $p^m / a$ então m é limitado; caso contrário, $a \in \cap Ap^i = (0)$ e a seria igual a 0.

2) $V_p(ab) = V_p(a) + V_p(b)$ pois se $0 \neq a = p^n a'$ e $0 \neq b = p^{n'} b'$, com $(p,a') = (p,b') = 1$, então $V_p(a) = n$, $V_p(b) = m$ e $V_p(a.b) = n + m$..

3) $V_p(a + b) \geq \min \{V_p(a), V_p(b)\}$ pois se $0 \neq a = p^n a'$ e $0 \neq b = p^m b'$, então $a + b = p^n a' + p^m b' =$

$= p^{\min\{n, m\}} . (p^{n - \min\{n, m\}} . a' + p^{m - \min\{n, m\}} . b')$

4) $\Gamma_{V_p} = Z$ pois claramente $\Gamma_V \subset Z$ e, além disso, dado $t \in Z$ existe $p^t \in A$ tal que $V_p(p^t) = t$ e logo $Z \subset \Gamma_{V_p}$.

Observe que $V_p(a)$ é o menor m tal que $p^m / a$. Observe também que $V_p$ satisfaz $V_p(\frac{a}{b}) = V_p(a) - V_p(b)$ (*). De fato, se $\frac{a}{b} = \frac{x}{y}$ então $V_p(ay) = V_p(bx)$, $V_p(a) + V_p(y) =$

$= V_p(b) + V_p(x)$, $V_p(a) - V_p(b) = V_p(x) - V_p(y)$ e (*) está bem definida; também,

$V_p(\frac{a}{b} \cdot \frac{x}{y}) = V_p(ax) - V_p(by) = V_p(a) + V_p(x) - V_p(b) - V_p(y) =$

$V_p(a) - V_p(b) + V_p(x) - V_p(y) = V_p(\frac{a}{b}) + V_p(\frac{x}{y})$. E ainda

$V_p(\frac{a}{b} + \frac{x}{y}) = V_p(ay + bx) - V_p(by) > \min\{V_p(ay), V_p(bx)\} - (V_p(b) - V_p(y)) >$

$\min\{V_p(ay) - V_p(b) - V_p(y) = V_p(a) - V_p(b) = V_p(\frac{a}{b}),$

$V_p(bx) - V_p(b) - V_p(y) = V_p(x) - V_p(y) = V_p(\frac{x}{y})\} =$

$= \min\{V_p(\frac{a}{b}), V_p(\frac{x}{y})\}$

Lema 1.3.6 - Seja $V: K^* \longrightarrow G$ uma valorização. O conjunto das unidades de $A_V$ é $U(A_V) = \{x \in K^* \text{ tal que } V(x) = 0\}$.

Demonstração:

Se $V(x) = 0$, então $V(\frac{1}{x}) = 0$. Logo, x é uma unidade em $A_V$.

Seja $x \in A_V$ e suponhamos que $V(x) = z > 0$. Como G é um grupo totalmente ordenado, -z não pode ser maior que zero (se $-z > 0$, $z - z > 0$, que é uma contradição em G); logo, $\frac{1}{x} \notin A_V$ e portanto x não é uma unidade.

Então, $x \in A_V$ é uma unidade se e somente se $V(x) = 0$.

Definição 1.3.7 - Um anel comutativo A é um anel local se possui somente um ideal maximal.

Lema 1.3.8 - Seja $V: K^* \longrightarrow G$ uma valorização. $A_V$ é um anel local e $M_V = \{x \in K^* \text{ tal que } V(x) > 0\}$ é o único ideal maximal de $A_V$.

Demonstração:

Se x e y estão em $M_V$, $V(x) > 0$ e $V(y) > 0$. Como

o grupo G é totalmente ordenado, $V(x) + V(y) > 0$. Logo, $x + y \in M_V$. Se $y \in A_V$ e $x \in M_V$, então $V(y) > 0$ e $V(x) > 0$; como G é totalmente ordenado, $V(xy) = V(x) + V(y) > 0$. Portanto, $M_V$ é um ideal de $A_V$.

Seja I um ideal de $A_V$ tal que $M_V \subset I \subset A_V$. Se $I \neq A_V$, então I não contem unidades de $A_V$. Como $A_V - U(A_V) = M_V$, segue que $I = M_V$.

Lema 1.3.9 - Se $V: K^* \longrightarrow G$ é uma valorização discreta, então $A_V$ é um anel principal. Além disso, $A_V$ possui somente dois ideais primos: (0) e $M_V$.

Demonstração:

Seja $I \neq (0)$ um ideal de $A_V$. Seja $x \in I$ tal que $V(x)$ é o mínimo dos $V(y)$, $y \in I$. Se $y \in I$, $V(\frac{y}{x}) \geq 0$. Logo, $\frac{y}{x} \in A_V$. Portanto, $y \in (x) \subseteq I$. Segue-se que $I = (x)$.

Claramente (0) é um ideal primo. Como $M_V$ é maximal, $M_V$ é primo. Seja $P = (p)$ um ideal primo de $A_V$. Como $M_V$ é o único ideal maximal de $A_V$, $P \subseteq M_V = (x)$. Logo, $p / x$. Então, x é associado a p. Logo, $M_V = P$.

O lema 1.3.9 mostra que se V é uma valorização discreta, então $A_V$ é um anel principal. Como $A_V$ é um subanel de K e K é um corpo, $A_V$ é também um domínio principal.

## 1.4 - Exemplos de anéis euclidianos

Nesta seção, veremos alguns exemplos clássicos de anéis euclidianos. No capítulo 3, veremos outros exemplos.

Definição 1.4.1 - Um conjunto bem ordenado W contém o conjunto N dos números naturais como um segmento inicial se e somente se existe $\alpha \in W$ tal que $I_\alpha = \{\beta \text{ tal que } \beta < \alpha\}$ é ordem-isomorfo a N.

Lema 1.4.2 - Suponhamos que o conjunto W contém N como um segmento inicial, que o anel A é um domínio de integridade e que $\cap Ap^i = (0)$ para todo primo p em A. Seja $(V_p)_{p\in P}$ o conjunto de todas as valorizações de A (correspondentes aos elementos primos de A).

Então, para todo algorítmo $\psi$ em A temos
$\psi(x) \geq 1 + \sum_{p\in P} V_p(x)$ para todo $x \neq 0$ em A.

Demonstração:

Podemos substituir $\psi$ por $\psi_1$ ( onde $\psi_1$ é o algorítmo definido no lema 1.2.4), já que $\psi(x) \geq \psi_1(x)$ para todo x em A. Se x' é um múltiplo estrito de x, temos $\psi_1(x') > \psi_1(x)$. Então, a nossa afirmação é demonstrada por indução, começando com o caso $\Sigma V_p(x) = 0$ para todo p. Logo, $p \nmid x$ para todo p; - esse fato implica que x é uma unidade e $\psi_1(x) \geq 1$. Então, $\psi_1(x) \geq 1 + \Sigma V_p(x)$.

Suponhamos que a nossa afirmação é válida para todo x em A tal que $\Sigma V_p(x) = n > 0$. Seja $y \in A$ tal que $\Sigma V_p(y) = n + 1$. Existe um primo $p_0$ em A tal que $p_0 \mid y$. Logo, se $z = \frac{y}{p_0}$ então $\psi_1(z) \geq 1 + \Sigma V_p(z)$. Também, como $p_0 z = y$, $\psi_1(y) > \psi_1(z)$ (1.2.4 , a). Como W é bem ordenado, temos:

$\{v' \text{ tal que } \psi_1(z) < v'\} \subseteq \{v' \text{ tal que } 1 + \Sigma V_p(z) < v'\}$; e

$\min\{v' \text{ tal que } \psi_1(z) < v'\} \geq \min\{v' \text{ tal que } 1 + \Sigma V_p(z) < v'\}$.

Como, por definição, $\psi_1(z) + 1 = \min\{v' \text{ tal que } \psi_1(z) < v'\}$ e $1 + 1 + \Sigma V_p(z) = \min\{v' \text{ tal que } 1 + \Sigma V_p(z) < v'\}$, então

$\psi_1(z)+1 \geq 2 + \Sigma V_p(z)$. Logo, $\psi_1(y) \geq \psi_1(z) + 1 \geq$ $2 + \Sigma V_p(z) = 1 + \Sigma V_p(y)$.

Lema 1.4.3 - Um domínio principal A com um número finito de ideais maximais $Ap_1, \ldots, Ap_n$ é euclidiano para o algorítmo $\psi(x) = 1 + \sum_{i=1}^{n} V_i(x)$ para $x \neq 0$ e $\psi(0) = 0$, onde $V_i$ denota a valorização normal $V_{p_i}$.

Demonstração:

Seja b um elemento não zero de A e $\overline{x'}$ um elemento de A/Ab. Temos que encontrar um representante x de $\overline{x'}$ em A tal que $\psi(x) < \psi(b)$. Para $\overline{x'}=0$ tomamos $x = 0$. Para $\overline{x'} \neq 0$, existem índices i tais que $V_i(x') < V_i(b)$ (caso contrário, x' pertenceria a Ab e $\overline{x'}= 0$). Para um índice j tal que $V_j(x') \geq V_j(b)$, como $\frac{x'}{p_j^{V_j(b)}}$ e $\frac{b}{p_j^{V_j(b)}} \in A$ e $V_j\left(\frac{b}{p_j^{V_j(b)}}\right) = 0$, existe $z_j$ tal que $\frac{x'}{p_j^{V_j(b)}} \equiv z_j \frac{b}{p_j^{V_j(b)}} \mod Ap_j$; logo, $x' \equiv z_j b \mod Ap_j^{1 + V_j(b)}$ (1), com $z_j \in A$, bem definido módulo $Ap_j$. O teorema do resto chines fornece um elemento $z \in A$ tal que $x' \equiv zb \mod Ap_j^{1 + V_j(b)}$ (2) para um tal índice j. Seja $x = b(1 - z) + x'$; de (1), (2) e $\bar{x} = \overline{x'}$ segue $x \equiv b \mod Ap_j^{1 + V_j(b)}$. Logo, $v_j(x) = V_j(b)$ para um tal índice j. Como para os outros índices i $V_i(x) = V_i(x') < V_i(b)$, $\sum_{i=1}^{n} V_i(x) < \sum_{i=1}^{n} V_i(b)$ e logo $\psi(x) < \psi(b)$.

Corolário 1.4.4 - O anel das valorizações discretas é euclidiano para o algorítmo $\psi(x)=1 + V(x)$ para $x \neq 0$ e $\psi(0) = 0$.

Demonstração:

Pela observação que segue o lema 1.3.9, $A_V$ é um domínio principal com um único ideal maximal $M_V$. Pelo lema 1.4.3, $A_V$ é euclidiano para o algorítmo $\psi$.

Observação 1.4.5 -

1) Um anel principal é um produto finito de domínios principais e de anéis principais com um único ideal maximal nilpotente Ap.

Todo elemento não nulo x de um anel principal com um único ideal maximal nilpotente pode ser escrito como $x = p^{V(x)}u$, onde u é uma unidade e V(x) é unicamente determinado por x. Logo, pelo lema 1.4.3 , 1 + V(x) é um algorítmo e o anel correspondente é euclidiano.

Portanto a questão "se um anel principal é euclidiano" se resume a domínios principais.

2) Se A é euclidiano para $\psi$, A* é finito e se n é um inteiro qualquer, então $\psi^{-1}(\{n\})$ é finito.

Vamos mostrar, inicialmente, que "se A é noetheriano, $A_0 = \{0\}$, $A_n = \{0\} \cup \{b \in A \text{ tal que } \bigcup_{i=0}^{n-1} A_i \longrightarrow A/Ab \text{ é sobrejetora}\}$, e o número de elementos de A* (denotado por $\#A^*$), onde A* é o conjunto de unidades de A, é finito então $\# A_n$ é finito para todo n".

De fato, suponhamos que $\# \bigcup_{i=0}^{n-1} A_i < \infty$. Se $I \in \{I \text{ tal que } \bigcup_{i=0}^{n-1} A_i \longrightarrow A/I \text{ é sobrejetora}\}$, então $\#A/I \leq \# \bigcup_{i=0}^{n-1} A_i < \infty$. Logo,

$\{I \text{ tal que } \bigcup_{i=0}^{n-1} A_i \longrightarrow A/I \text{ é sobrejetora}\} \subseteq \{I \text{ tal que } \neq\neq A/I \leqslant \neq\neq \bigcup_{i=0}^{n-1} A_i\}$ (1). Como

$\{I \text{ tal que } \neq\neq A/I \leqslant \neq\neq \bigcup_{i=0}^{n-1} A_i = m\} = \bigcup_{i=0}^{m} \{I \text{ tal que } \neq\neq A/I = i\}$,

$\neq\neq\{I \text{ tal que } \neq\neq A/I \leqslant \neq\neq \bigcup_{i=0}^{n-1} A_i = m\} =$

$\sum_{i=0}^{m} \neq\neq \{I \text{ tal que } \neq\neq A/I = i\} = m' < \infty$ (2).

De(1) e (2) segue $\neq\neq\{I \text{ tal que } \bigcup_{i=0}^{n-1} A_i \longrightarrow A/I \text{ é sobrejetora}\} \leqslant m' < \infty$.

Também, $\{b \in A \text{ tal que } \bigcup_{i=0}^{n-1} A_i \longrightarrow A/Ab \text{ é sobrejetora}\} =$

$\cup\{b \in A \text{ tal que } \bigcup_{i=1}^{n-1} A_i \longrightarrow A/Ab \text{ é sobrejetora, } Ab = I\}$, onde a união é discreta e é tomada sobre todos os ideais I de A tais que existe $b \in A$, $I = Ab$ e $\cup A_i \longrightarrow A/I$ é sobrejetora. Logo,

$\neq\neq \{b \in A \text{ tal que } \bigcup_{i=0}^{n-1} A_i \longrightarrow A/Ab \text{ é sobrejetora}\} =$

$\Sigma \neq\neq \{b \in A \text{ tal que } \bigcup_{i=1}^{n-1} A_i \longrightarrow A/Ab \text{ é sobrejetora, } Ab = I\}$, onde a $\Sigma$ é tomados sobre os mesmos índices da união. Como

$\{I \subset A \text{ tal que existe } b \in A,\ I = Ab, \cup_{i=1}^{n-1} A_i \longrightarrow A/I \text{ é sobrejetora}\} \subseteq$

$\{I \subset A \text{ tal que } \cup_{i=1}^{n-1} A_i \longrightarrow A/I \text{ é sobrejetora}\}$,

$\neq\neq \{I \subset A \text{ tal que existe } b \in A,\ I = Ab, \cup_{i=1}^{n-1} A_i \longrightarrow A/I \text{ é sobreje-}$

$\text{tora}\} \leqslant m'$. Portanto, $\{I \text{ tal que } \cup_{i=1}^{n-1} A_i \longrightarrow A/I \text{ é sobrejetora}\} =$

$\{I_0, I_1, \ldots, I_t\}$, $t \leqslant m'$ e $I_i$ distintos. Logo,

$\neq\neq \{b \in A \text{ tal que } \cup_{i=1}^{n-1} A_i \longrightarrow A/Ab \text{ é sobrejetora}\} \leqslant$

$\sum_{i=0}^{t} \neq\neq \{b \in A$ tal que $\bigcup_{i=1}^{n-1} A_i \longrightarrow A/Ab, Ab = I_i\}$ . Dado i,

$\{ b \in A$ tal que $\bigcup_{i=1}^{n-1} A_i \longrightarrow A/I_i$ é sobrejetora , $Ab = I_i\} =$

$\{b, u_1b, u_2b, \ldots, u_sb\}$ onde b é qualquer elemento de A, satisfazendo $A_b = I$ e $\{u_i\} = A^*$. Logo,

$\neq\neq \{b$ tal que $\bigcup_{i=1}^{n-1} A_i \longrightarrow A/I_i$ é sobrejetora, $Ab = I_i\} = \neq\neq A^*$.

Portanto, $\neq\neq \{b \in A$ tal que $\bigcup_{i=1}^{n-1} A_i \longrightarrow A/Ab$ é sobrejetora$\} =$

$\sum_{i=0}^{t} \neq\neq A^* = (t + 1) \neq\neq A^* < \infty$.

Dado n, seja $\{x \in \psi(A)$ tal que $x < n\} =$

$\{x_0 < x_1 < \ldots < x_{k-1}\}$ . Então, $\psi^{-1}(\{x_0\}) = \{0\} = A_0$,

$\psi^{-1}(\{x_1\}) \subseteq \{b \in A$ tal que $A_0 \longrightarrow A/Ab$ é sobrejetora$\} \cup \{0\} = A_1$.

Suponhamos, por hipótese de indução, que $\psi^{-1}(x_j) \subseteq A_j$ para todo $j \leq i \leq k-2$. Como,

$\psi^{-1}(\{x_{i+1}\}) \subseteq \{b \in A$ tal que $\bigcup_{j=0}^{i} \psi^{-1}(\{x_j\}) \longrightarrow A/Ab$ é sobrejetora$\} \subseteq$

$\{b \in A$ tal que $\bigcup_{j=0}^{i} A_j \longrightarrow A/Ab$ é sobrejetora$\}$, então

$\psi^{-1}(\{x_{i+1}\}) \subseteq A_{i+1}$. Logo,

$\psi^{-1}(\{n\}) \subseteq \{b \in A$ tal que $\bigcup_{i=0}^{k-1} \psi^{-1}(x_i) \longrightarrow A/Ab$ é sobrejetora$\} \subseteq$

$\{b \in A$ tal que $\bigcup_{i=1}^{k} A_i \longrightarrow A/Ab$ é sobrejetora$\} \cup \{0\} = A_{k+1}$. Podemos concluir que $\neq\neq \psi^{-1}(\{n\}) \leq \neq\neq A_{k+1} < \infty$.

Lema 1.4.6 - Sejam A um domínio euclidiano e S um sistema multiplicativo tal que $0 \notin S$. Então, $S^{-1}A$ é euclidiano.

Demonstração:

Seja $\bar{S} = S \cup \{$divisores dos elementos de $S\}$. $\bar{S}$ é um

sistema multiplicativo pois se $s_1$ e $s_2 \in \bar{S}$ existem $s_1'$ e $s_2' \in S$ tais que $s_1 s_1' = s_1''$ e $s_2 s_2' = s_2''$ com $s_1''$ e $s_2'' \in S$; logo, $s_1 s_2 / s_1' s_2'' \in S$ e $s_1 s_2 \in \bar{S}$. Também, $\bar{S}^{-1}A = S^{-1}A$ pois: como $S \subseteq \bar{S}$, temos $S^{-1}A \subseteq \bar{S}^{-1}A$; se $a/s \in \bar{S}^{-1}A$, então $ss' = s'' \in S$ e logo, $as'/s'' = a/s \in S^{-1}A$. Então, podemos supor S com as propriedades de $\bar{S}$.

Pelo lema 1.2.4, existe um algorítmo $\psi$ em A tal que $y \in Ax$, $y \neq 0$, implica $\psi(x) \leq \psi(y)$. Como A é um anel fatorial, todo elemento x de $S^{-1}A$ pode ser escrito como $x = \frac{s}{t} x'$ com $s \in \bar{S}$ e $x' \in A$ primos com todos os elementos de S; então, x' é unicamente determinado além das unidades por x. Definimos $\psi'(x) = \psi(x')$ e mostraremos que $\psi'$ é um algorítmo em $S^{-1}A$.

Primeiramente notamos que, para $s, s' \in S$ e $x \in S^{-1}A$, temos $\psi'(s) = \psi(1)$ e $\psi'(\frac{sx}{s'}) = \psi'(x)$. Consideremos $a \in A$ e $b \in S^{-1}A$ com $b \neq 0$ e escrevemos $b = \frac{s}{t} b'$ como acima.

Vamos mostrar que o homomorfismo $A/Ab' \longrightarrow S^{-1}A/S^{-1}Ab$ dado por $a + Ab' \longmapsto a + S^{-1}Ab$ é sobrejetor. Se S não tem primos, então $S^{-1}A = A$, $b' \in A$ e $Ab = Ab'$ e a afirmação segue. Suponhamos, então, que S tem primos. Para todo $p \in S$, $p \nmid b'$, e Ap é maximal. Logo, $(p,b')A = A$. Então, existem $u_p$ e $w_p$ em A tais que $1 = u_p p + w_p b'$ e logo $1 \equiv u_p p \bmod b'$. Agora, seja $s \in S$, com s não unidade de A. Como A é um anel fatorial $s = y p_1^{s_1} \ldots p_n^{s_n}$, $p_i \in S$. Logo,

$$\frac{1}{p_i} = u_{p_i} + \frac{w_{p_i}}{p_i} b' \quad , \quad \frac{1}{s} = \frac{1}{y} \frac{1}{p_1^{s_1}} \cdots \frac{1}{p_n^{s_n}} \quad ,$$

$$\frac{1}{s} = \frac{1}{y} \frac{p_1^{s_1} u_{p_1}^{s_1}}{p_1^{s_1}} \cdots \frac{p_n^{s_n} u_{p_n}^{s_n}}{p_n^{s_n}} + \frac{x}{p_1^{s_1} \ldots p_n^{s_n}} b' \quad e$$

$\frac{1}{s} = \frac{1}{y} u_{p_1}^{s_1} \ldots u_{p_n}^{s_n} + \frac{x}{p_1^{s_1} \ldots p_n^{s_n}} b'$. Como

$u_{p_1}^{s_1} \ldots u_{p_n}^{s_n} \in A$ e $\frac{x}{p_1^{s_1} \ldots p_n^{s_n}} \in S^{-1}A$, temos

$\frac{1}{s} \equiv \frac{1}{y} u_{p_1}^{s_1} \ldots u_{p_n}^{s_n} \mod S^{-1}Ab' = S^{-1}Ab$. Logo, existe

$a_s = \frac{1}{y} u_{p_1}^{s_1} \ldots u_{p_n}^{s_n} \in A$ tal que

$\frac{1}{s} \equiv a_s \mod S^{-1}Ab$ e se $\frac{g}{s} \in S^{-1}A$ então

$a_s g + S^{-1}Ab = (a_s + S^{-1}Ab)\ (g + S^{-1}Ab) =$

$(\frac{1}{s} + S^{-1}Ab)\ (g + S^{-1}Ab) = \frac{g}{s} + S^{-1}Ab$. Portanto,

$a_s g \longmapsto \frac{g}{s} + S^{-1}A$. Se s é uma unidade de A, então

$\frac{g}{s} = gs^{-1} \in A$ e $\frac{g}{s} + S^{-1}A = gs^{-1} + S^{-1}A$. Logo, $gs^{-1} \longrightarrow \frac{g}{s}$.

Como o homomorfismo $A/Ab' \longrightarrow S^{-1}A/S^{-1}Ab$ é sobrejetor, existe $c \in A$ tal que $\frac{a}{s} \equiv c \mod S^{-1}Ab$ e logo

$a \equiv sc \mod S^{-1}Ab$.

Podemos escrever $c = b'q + r$ com $q, r \in A$ e $\psi(r) < \psi(b')$. Logo, $c \equiv r \mod S^{-1}Ab$.

Portanto, $\frac{a}{s} \equiv r \mod S^{-1}Ab$ e

$\psi'(r) = \psi(r') < \psi(r) < \psi(b') = \psi'(b)$.

Lema 1.4.8 - Seja A um anel euclidiano, então $A' = A\left[\left[X\right]\right]\left[X^{-1}\right]$

é euclidiano.

Demonstração:

Seja $\psi$ um algorítmo em A. Os elementos de A' são séries de potências $\sum_{n>n_0} a_n x^n$, $a_n \in A$, com, possivelmente, um número finito de termos com expoente negativo. Para $s \in A'$, $s \neq 0$ seja a(s) o coeficiente do termo que possui o menor grau em s, $s = a(s)\, x^q + a_{q+1}\, x^{q+1} + \ldots$ Fixamos $\psi'(s) = \psi(a(s))$, $\psi'(0) = \psi(0)$ e provaremos que $\psi'$ é um algorítmo para A'. Considere $s \in A'$, $s \neq 0$ tal que $s = a(s)\, x^{\alpha} + \ldots$ com $a(s) \neq 0$. Para cada $t = a(t)\, x^{\beta} + \ldots$ em A' escrevemos $a(t) = a(s)\, b_0 + c$ com $b, c \in A$, $\psi(c) < \psi(a(s))$ e fixamos $t_1 = t - bx^{\beta_0 - \alpha} s = c\, x^{\beta} +$ (termos de maior grau). Se $c \neq 0$, paramos o processo já que $\psi'(t_1) = \psi(c) < \psi(a(s)) = \psi'(s)$. Se $c = 0$, construimos, analogamente, $t_2 = t_1 - b_1 x^{\beta_1 - \alpha} s$ onde $t_1 = a(t_1)\, x^{\beta_1} +$ (termos de menor grau). Se o processo para após um número finito de passos, digamos i-1 passos temos:

$$t_1 = t - b_0 x^{\beta_0 - \alpha} s\,, \quad t_2 = t_1 - b_1 x^{\beta_1 - \alpha} s\,, \quad \ldots\,,$$

$$t_i = t_{i-1} - b_{i-1} x^{\beta_{i-1} - \alpha} s\,.$$

Como, $t_{i-1} = a(t_{i-1}) x^{\beta_{i-1}} +$ (termos de menor grau),

$t_i = (a(t_{i-1})\, x^{\beta_{i-1}} +$ (termos de menor grau) $- b_{i-1} x^{\beta_{i-1} - \alpha} \cdot (a(s)\, x^{\alpha} +$ (termos de menor grau)) $= c_{i-1}\, x^{\beta_{i-1}} +$ (termos de menor grau).

Como $c_{i-1} \neq 0$, $\psi'(t_i) = \psi(a(t_i) = \psi(c_{i-1}) < \psi(a(s)) = \psi'(s)$.

Se $c_0 = 0$ para todo i, temos $\beta_i < \beta_{i+1}$. Logo,

$\Omega = \sum_i b_i\, x^{\beta_i} \in A$, $x^{\alpha}\Omega \in A'$, $t = x^{\alpha}\Omega s$ e $t \equiv 0 \bmod s$. Neste caso, $\psi'(0) < \psi'(s)$.

# CAPÍTULO - 2

## A CONSTRUÇÃO TRANSFINITA E O ALGORÍTMO MÍNIMO

### 2.1 - O algorítmo mínimo

Definição 2.1.1 - Dois algorítmos $\psi: A \longrightarrow W$ e $\psi': A \longrightarrow W'$ em um anel A são isomorfos se existe um ordem-isomorfismo (preserva a ordem) $h: \psi(A) \longrightarrow \psi'(A)$ tal que $\psi' = h\circ\psi$.

Ordinal é uma classe de conjuntos dados indutivamente por:
$\phi$, $\phi + 1 = \{\phi\}$, $\phi + 2 = \{\phi,\{\phi\}\}$, $\phi + 3 = \{\phi,\{\phi\}, \{\phi,\{\phi\}\}\}$...

Seja W um conjunto ordinal tal que Card W > Card A.

Seja $\psi: A \longrightarrow V$ um algorítmo euclidiano. Im $\psi$ é um conjunto bem ordenado com a ordem de V e Card Im $\psi \leq$ Card A < Card W. Então, Im $\psi$ é ordem-isomorfo a um segmento inicial $I_\psi$ de W. Existe um ordem-isomorfismo $\nu: Im\psi \longrightarrow I_\psi$. Definimos $\psi' = \nu\circ\psi: A \longrightarrow I_\psi \subseteq W$. Obviamente $\psi'$ é um algorítmo euclidiano e $\psi$ e $\psi'$ são isomorfos.

Portanto, todos os algorítmos euclidianos no anel A podem ser construidos tomando seus valores no conjunto W.

Os elementos de W são costumeiramente denotados por
0, 1, 2, 3, ... , w, w + 1, ... , 2w, ...

Lema 2.1.2 - Se $\psi_\alpha: A \longrightarrow W$ é uma família não vazia de algorítmos euclidianos em um anel euclidiano A, então $\psi = \inf_\alpha \psi_\alpha$ é também um algorítmo euclidiano em A.

Demonstração:

Considere $a, b \varepsilon A, b \neq 0$. Como W é bem ordenado, existe um índice $\alpha$ tal que $\psi(b) = \psi_\alpha(b)$. Podemos escrever $a = bq + r$ com $q, r \varepsilon A$ e $\psi_\alpha(r) < \psi_\alpha(b)$. Então $\psi(r) < \psi_\alpha(r) < \psi_\alpha(b) = \psi(b)$, mostrando que $\psi$ é um algorítmo euclidiano em A.

Também, dado a e $b \varepsilon A-\{0\}$, existe $\alpha$ tal que $\psi(ab) = \psi_\alpha(ab)$. Como, $\psi_\alpha(ab) \geq \psi_\alpha(a)$, $\psi(ab) \geq \psi_\alpha(a) \geq \psi(a)$.

O lema 2.1.2 mostra que todo anel euclidiano A admite um algorítmo mínimo $\theta$ (isto é, o ínfimo de todos os algorítmos).

O algorítmo $\theta$ goza as propriedades descritas no lema 1.2.4 e em seus corolários. Além disso, pelo lema 1.2.1 , $\theta(x) = 0$ se e somente se $x = 0$ e, pelo lema 1.2.2 e corolário 1.2.5, $\theta(x) = 1$ se e somente se x é uma unidade (observe que (A) é isomorfo a um segmento inicial de W

## 2.2 - A construção transfinita de Samuel e Motzkin

Inicialmente, veremos a construção transfinita de P. Samuel (10).

Lema 2.2.1 - Seja $\theta: A \longrightarrow W$ o algorítmo mínimo em um anel euclidiano A. Para $\alpha \varepsilon A$ seja $A_\alpha = \{x \varepsilon A$ tal que $\theta(x) \leqslant \alpha\}$ . e $A'_\alpha = \{x \varepsilon A$ tal que $\theta(x) < \alpha\}$ . Então, $A_\alpha$ é a união de (0) com o conjunto dos elementos $b \varepsilon A$ tais que a aplicação $A'_\alpha \longrightarrow A/Ab$ é sobrejetora ( isto é, representantes de classes módulo Ab podem ser achados em $A'_\alpha$).

Demonstração:

Se $b \varepsilon A_\alpha$ e se $a + Ab$ ($a \varepsilon A$) é qualquer classe módulo Ab, escrevendo $a = bq + r$, encontramos um representante r dessa classe tal que $\theta(r) < \theta(b) \leqslant \alpha$, isto é, $r \varepsilon A'_\alpha$.

Reciprocamente, considere $b \neq 0$ tal que $A'_\alpha \longrightarrow A/Ab$ é sobrejetora e suponha que $\theta(b) > \alpha$ . Agora, defina $\theta_1: A \longrightarrow W$ por $\theta_1(b) = \alpha$ e $\theta_1(x) = \theta(x)$ para $x \neq b$. Afirmamos que $\theta_1$ é um

algorítmo. De fato, para as relações $a = bq + r$ nas quais b age como um divisor, sabemos que cada classe $a + Ab$ tem um representante $r \in A'_\alpha$, isto é, um elemento r tal que $\theta_1(r) < \alpha = \theta_1(b)$; por outro lado, em uma relação $a = cq + b$, na qual b age como um resto e $c \neq b$, temos $\theta_1(b) = \alpha < \theta(b) < \theta(c) = \theta_1(c)$. Isto contradiz o fato de que $\theta$ é o menor algorítmo. Logo, $\theta(b) \leq \alpha$.

O lema 2.2.1 mostra que o algorítmo mínimo pode ser construido por indução transfinita, já que $A'_\alpha$ determina $A_\alpha$ de maneira simples.

Exemplo 2.2.2 - $\theta(x) = 2$ significa que A/Ax admite um sistema de representantes feito de 0 e unidades. Um tal x é necessariamente um elemento primo (ou seja, irredutível) de A.

A construção transfinita descrita no lema 2.2.1 pode ser feita em todo o anel. Mais precisamente:

A construção transfinita 2.2.3 - Seja A um anel e W um conjunto ordinal tal que card A < card W. Fazemos $A_0 = \{0\}$. Para $\alpha > 0$ em W, definimos $A_\alpha$ por indução transfinita como segue:

$$A'_\alpha = \bigcup_{\beta < \alpha} A_\beta \quad \text{e} \quad A_\alpha = (0) \cup \{b \in A \text{ tal que } A'_\alpha \to A/bA \text{ é sobrejetora}\}$$

Vamos mostrar que A é euclidiano se e somente se $A = \bigcup_{\alpha \in W} A_\alpha$.

Suponhamos que A é euclidiano e seja $\theta$ o algorítmo mínimo. $A_0 = \{0\} = \{x \in A \text{ tal que } \theta(x) \leq 0\}$ e $A'_0 = \phi = \{x \in A \text{ tal que } \theta(x) < 0\}$. Seja $\alpha \neq 0$ e suponhamos que para todo $\beta < \alpha$, $A'_\beta = \{x \in A \text{ tal que } \theta(x) < \beta\}$ e $A_\beta = \{x \in A \text{ tal que } \theta(x) \leq \beta\}$. Logo, $A'_\alpha = \bigcup_{\beta < \alpha} \{x \in A \text{ tal que } \theta(x) \leq \beta\} = \{x \in A \text{ tal que } \theta(x) < \alpha\}$

e, pelo lema 2.2.1, $(0) \cup \{x \in A$ tal que $\theta(x) \leq \alpha\} = \{x \in A$ tal que $A'_\alpha \to A/Ab$ é sobrejetora$\} = A_\alpha$. Se $x \in A$, $\theta(x) \in W$; logo, $x \in A_{\theta(x)} \subseteq \bigcup A_\alpha$.

Então, $A \subset \bigcup_{\alpha \in W} A_\alpha$ e como $\bigcup_{\alpha \in W} A_\alpha \subset A$, temos $A = \bigcup_{\alpha \in W} A_\alpha$.

Por outro lado, suponhamos que $\bigcup A_\alpha = A$. Seja $\theta: A \to W$ definido por $\theta(x) = \alpha$ se e somente se $x \in A_\alpha - A'_\alpha$. Se $b \in \bigcup_{\alpha \in W} A_\alpha$, seja $V = \{\beta$ tal que $b \in A_\beta\}$ e $\alpha = \min V$; então, $\theta(b) = \alpha$. Existe $r \in A'_\alpha$ tal que $r + Ab = a + Ab$. Como $r \in \bigcup_{\beta < \alpha} A_\beta$, $\theta(r) < \alpha$.

Logo, $\theta$ é um algorítmo para A e A é euclidiano. Em particular, $\theta$ é o algorítmo mínimo de A.

Veremos, agora, a construção transfinita de T. Motzkin (4).

Definição 2.2.4 - Seja A um anel de integridade. Um Motzkin - -algorítmo euclidiano é dado por uma norma $|a|$ definida em A - - $\{0\}$, com valores no conjunto N dos números naturais e tal que $|a| \geq |b|$ para b dividindo a e para b em A - $\{0\}$ e a não divisível por b existem q e r em A satisfazendo $a = qb + r$, $|r| < |b|$.

Definição 2.2.5 - Seja A um domínio de integridade. Um subconjunto de A - $\{0\}$ é chamado um ideal produto se $P(A - 0) \subseteq P$.

Definição 2.2.6 - Seja A um domínio de integridade. Para todo subconjunto $S \subset A$, o conjunto $B = \{b \in A$ tal que existe $a \in A$ com $a + bA \subseteq S\}$ é chamado o conjunto derivado total de S, e a intersecção $B \cap S$ é chamado o conjunto derivado S'.

Se S é um ideal produto, S' também o é.

A construção transfinita 2.2.7 - Para $i = 0, 1, 2, \ldots$ seja $P_i = \{b \in A$ tal que $|b| \geq i\}$. Obviamente, $P_i$ é um ideal produto.

Se $b \in P_i'$, então $b \in P_i$ e $|b \geq i$. Também, existem a tal que $a + bA \subseteq P_i$ e $r = a + bq$ com $|r| < |b|$. Como $r \in P_i$, $i \leq |r| < |b|$ e $i + 1 \leq |b|$. Logo, $b \in P_{i+1}$. Portanto, $P_i' \subseteq P_{i+1}$.

Também, $\cap P_i = \emptyset$.

Por outro lado, dada uma sequência $A = P_0 \supset A - \{0\} = P_1 \supset P_2 \supset \ldots$ de ideais produtos tal que $P_i' \subset P_{i+1}$, a norma $|b| = i$ para $b \in P_i - P_{i+1}$ satisfaz todas as condições para um Motzkin - algorítmo euclidiano. De fato:

1) Seja $b \in P_i - P_{i+1}$; $b \notin P_i' \subseteq P_{i+1}$. Logo, $a + bA \not\subset P_{i+1}$. Existe $q \in A$ tal que $a + bq \in P_i$. Então, $|a + bq| < i = |b|$.

2) Sejam $a \neq 0$ e $b \neq 0$ elementos de A e suponhamos que $a \in P_i$. Como $b \neq 0$, $ab \in P_i$. Logo, $|ab| \geq i = |a|$.

Portanto, existe uma correspondência biunívoca entre sequências desse tipo e algorítmos euclidianos.

Definição 2.2.8 - Se para outro Motzkin-algorítmo, com a sequência $\overline{P}_i$, sempre $P_i \subseteq \overline{P}_i$, dizemos que o primeiro Motzkin-algorítmo é mais rápido.

Se existe um Motzkin-algorítmo euclidiano em A, então existe o Motzkin-algorítmo euclidiano mais rápido, definido pela $P_0, P_1, P_2, \ldots$ onde $P_0 = A$, $P_1 = A - \{0\}$ e $P_i = P_i'$.

Logo, A é Motzkin-euclidiano se e somente $\cap P_i = \emptyset$.

Lema 2.2.9 - Com a notação das construções de Motzkin e Samuel, e supondo que o conjunto W da construção transfinita de Samuel é o conjunto N dos números naturais, para todo $i \geq 0$, $P_{i+1} = A - A_i$.

Demonstração:

Como $P_1 = A - \{0\}$ e $A_0 = \{0\}$, $P_1 = A - A_0$.

Sabemos que $A_1 = \{\text{unidades de A}\} \cup \{0\}$. $B_2 = \{b \in A$ tal que existe $a \in A$ com $a + bA \subseteq P_1\}$ e $P_2 = B_2 \cap P_1$. Claramente, $\{\text{unidades de A}\} \cap B_2 = \emptyset$ e $0 \notin B_2$. Também, se $b \neq 0$ não é unidade de A, $0 \notin 1 + bA \subseteq P_1$ e logo, $b \in B_2$. Portanto, $P_2 = A - A_1$.

Suponhamos, como hipótese de indução, que $P_{r+1} = A - A_r$ para todo $r + 1 \leq n$.

Como $B_{n+2} = \{b \in A$ tal que existe $a \in A$ com $a + bA \subseteq P_{n+1} = A - A_n\}$, $P_{n+2} = B_{n+2} \cap P_{n+1} = B_{n+2} \cap (A - A_n)$. Devemos mostrar que $B_{n+2} \cap (A - A_n) = A - A_{n+1}$.

De fato, seja $b \in B_{n+2} \cap (A - A_n)$. Suponhamos que $b \in A_{n+1}$; então, $A'_{n+1} \longrightarrow A/Ab$ é sobrejetora. Como $A'_{n+1} = \bigcup_{i<n+1} A_i = A_n$, $A_n \longrightarrow A/Ab$ é sobrejetora. Como, $b \in B_{n+1}$, existe $a \in A$ tal que $a + bA \subseteq A - A_n$. Também, existe $c \in A_n$ tal que $c - a \in bA$ e existe $r \in A$ tal que $c - a = br$ ou $c = a + br$. Então $a + br \in a + bA \subseteq A - A_n$ e $a + br = c \in A_n$, que é uma contradição.

Portanto, $B_{n+2} \cap (A - A_n) \subseteq A - A_{n+1}$.

Por outro lado, como $A_n \subseteq A_{n+1}$, se $x \in A - A_n$ então $x \in A - A_{n+1}$. Logo $x \notin \{b$ tal que $A_n \to A/Ab$ é sobrejetora$\}$ e existe um $a \in A$ tal que $a + bA$ não é alcançado por qualquer elemento de $A_n$, isto é, $(a + xA) \cap A_n = \phi$. Portanto, $a + xA \subseteq A - A_n$ e $x \in B_{n+2}$. Logo, $A - A_{n+1} \subseteq B_{n+2} \cap (A - A_n)$.

Corolário 2.2.10 - $\cap P_n = \emptyset$ se e somente se $A = \cup A_n$. Então, A é Motzkin-euclidiano se e somente se A é Samuel-euclidiano para N.

Também $P_i - P_{i+1} = A_i - A_{i-1}$ para todo $i \geq 0$ e $A_0 = \emptyset$. Logo, a construção transfinita de Motzkin é igual a construção transfinita de Samuel para N.

Demonstração:

Imediata do lema.

## 2.3 - Aplicação à definição de anel euclidiano.

Para que um anel de integridade seja euclidiano é necessário apenas mostrar que ele possui um algorítmo com valores em um conjunto parcialmente ordenado com a condição da cadeia descendente, como mostra o

Lema 2.3.1 -Seja A um anel de integridade, T um conjunto parcialmente ordenado com a condição da cadeia descendente e $\psi: A \to T$ uma aplicação tal que, dados a e $b \neq 0$ em A, existem q, $r \in A$ tais que $a = bq + r$ e $\psi(r) < \psi(b)$. Então, A é euclidiano.

Demonstração:

Seja $(A_\alpha)$ a construção transfinita em A e $A' = \bigcup_\alpha A_\alpha$.

Se $A' \neq A$, escolha $b \in A - A'$ tal que $\psi(b)$ seja minimal. Então, $\psi(r) < \psi(b)$ implica $r \in A'$; logo, $A' \to A/Ab$ é sobrejetiva. Mas isto implica $b \in A'$, que é uma contradição. Portanto, $A = A'$ e $A$ é euclidiano.

## 2.4 - Exemplos de algorítmo mínimo.

Exemplo 2.4.1 - Para $A = Z$ (anel dos inteiros) temos $A_2' = A_1' = \{-1, 0, +1\}$ e esse conjunto contém três inteiros consecutivos. Isto fornece representantes para as classes mod 2 e mod 3, de tal maneira que $A_3' = \{-3, -2, -1, 0, 1, 2, 3\}$. Aqui temos sete inteiros consecutivos e $A_4' = A_3$ é o intervalo $[-7, +7]$, formado por 15 inteiros consecutivos.

Observe:

$A_1 = \{-(2 - 1), 0, (2 - 1)\}$

$A_2 = \{-(2^2 - 1), \ldots, 0, \ldots, (2^2 - 1)\}$

$A_3 = \{-(2^3 - 1), \ldots, 0, \ldots, (2^3 - 1)\}$

Suponhamos, como hipótese de indução, que

$A_i = \{-(2^i - 1), \ldots, 0, \ldots, (2^i - 1)\}$.

Sabemos que $A_{i+1} = \{b \in A$ tal que $A_i \to A/Ab$ é sobrejetora$\}$ e $|A_i| = 2(2^i - 1) + 1 = 2^{i+1} - 1$. Logo, $|A/Ab| \leq 2^{i+1} - 1$. Mas para $|b| \leq 2^{i+1} - 1$, $\{-(2^i - 1), \ldots, \overline{0}, \ldots, \overline{2^i - 1}\} = A/Ab$. Realmente, se $0 \leq x < 2^{i+1} - 1$, então $x \leq 2^{i+1}$; logo, $x \leq 2^i - 1$ ou $2^i - 1 < x$; nestes casos $-(2^i - 1) \leq x - 2^{i+1} + 1 < 0$; então, $x - 2^{i+1} + 1 \in A_i$ e $x - 2^{i+1} + 1 \equiv x \bmod 2^{i+1} - 1$. Portanto, $A_{i+1} = \{b \in A$ tal que $|b| \leq 2^{i+1} - 1\} =$

$= \{-(2^{i+1} - 1), \ldots, 0, \ldots, 2^{i+1} - 1\}$.

Portanto, se $x \in A_i - A_{i-1}$, $x = 2^{i-1} + c_2\, 2^{i-2} + \ldots + c_{i-1} 2 + c_i$. onde $c_i \in \{0,1\}$. Logo, o número de dígitos binários

de $|x|$ é $\|x\| = i$ e o algorítmo mínimo $\theta$ em A é $\theta(x) = i = \|x\|$.

Exemplo 2.4.2 - Seja K um corpo e A o anel polinomial em uma variável $A = K[x]$. Como $A^* = K^*$ temos $A_2' = A_1 = K$. Então, os elementos de $A_2$ são 0 e os polinômios p tais que $K[x]/(p)$ é um espaço vetorial de dimensão $\leq 1$ sôbre K; esses são os polinômios de grau $\leq 1$ e formam um espaço bidimensional sobre K.

Suponhamos, como hipótese de indução, que $A'_{n+1} = A_n$ onde $A_n$ é o espaço vetorial n-dimensional dos polinômios de grau $\leq n-1$.

$A_{n+1} = (0) \cup \{b \in A$ tal que $A_n \xrightarrow{\psi} A/Ab$ é sobrejetora$\}$. $\psi$ é uma transformação linear sobrejetora; então, $\dim \psi(A_n) \leq n \leq |A/Ab|$. Como $\psi(A_n) = A/Ab$, $\dim A/Ab \leq n$; logo, $\delta b = $ grau de $b \leq n + 1$. Por outro lado, se $\delta f \leq n + 1$, $f \neq 0$, então a aplicação $A_n \xrightarrow{\psi} A/Af$ é sobrejetora. Uma base para A/Af é $\{\bar{1}, \bar{x}, \ldots, \bar{x}^{\delta f - 1}\}$. Então, dado $\bar{y} \in A/Af$, $\bar{y} =$ polinômio de grau $\leq \delta f - 1 < n$ e existe $z \in A_n$ tal que $\bar{y} = \bar{z}$. Logo, $A_{n+1}$ é o espaço vetorial dos polinômios de grau $\leq n$.

Logo, o algorítmo mínimo $\theta$ em A é dado por $\theta(f) = \delta(f) + 1$.

Exemplo 2.4.3 - Seja A um domínio principal com um número finito de ideais maximais $Ap_i$, $i = 1, \ldots, n$, e seja $V_i$ a valorização normalizada $V_{p_i}$ de A. Segue do lema 1.4.3 e 1.4.4 que o algorítmo mínimo $\theta$ em A é dado por $\theta(x) =$

$$= 1 + \sum_{i=1}^{n} V_i(x) \text{ para } x \neq 0 \text{ e } \theta(0) = 0.$$

Exemplo 2.4.4 - Seja A o anel dos inteiros em um corpo numérico quadrático imaginário (3.3.3). Se $A^*$ é finito, os conjuntos $A_n$ da construção transfinita (2,2,3) são finitos (1.1.46; (2)) e podem ser determinados uns após os outros.

P. Samuel (10) calculou para $A = Z[\sqrt{-1}]$ e $A = Z[\sqrt{-2}]$ e esses conjuntos pareciam ser bastante irregulares; para $Z[\sqrt{-2}]$ essas cardinalidades são 1,3,9,21,35,61,99,153,227, 327.

Como exemplo, vamos calcular para $A = Z[\sqrt{-2}]$ até a cardinalidade 9.

A é integralmente fechado e o conjunto das suas unidades é $\{-1,1\}$ (12).

Com a notação da construção transfinita temos: $A_0 = \{0\}$, $A_0' = \{0\}$ e $A_1 = (0) \cup \{b \in A$ tal que $\{0\} \to A/bA$ é sobrejetora$\}$. Como $\{0\} \to A/bA$ é sobrejetora se e somente se $|A/bA| = 1$ e isto acontece se e somente se $b \in \{-1, 1\}$, $A_1 = \{0, \pm 1\}$.

$A_2 = \{b \in Z[\sqrt{-2}]$ tal que $\{0,\pm 1\} \to A/Ab$ é sobrejetora$\} \cup (0)$. Logo, $b \neq 0 \in A_2$ se e somente se $|A/Ab| \leq 3$. Temos três casos:

1) $|A/Ab| = 1$. Neste caso, $bA = A$ e $b \in \{\pm 1\}$.

2) $|A/Ab| = 2$. Neste caso, $1 \notin bA$, $Z/bA\cap Z \neq (0)$ e $|Z/bA\cap Z| \geq 2$. Como $|A/bA| = 2$, $A/bA = Z/bA\cap Z = Z_2$ e $bA\cap Z = 2Z$.

Suponhamos que $b = x + \sqrt{2}\,iy$ e $\bar{b}$ é o conjugado de b; então, $b.\bar{b} = x^2 + 2y^2$.

Seja $a \in Z\cap bA$, $a = bb'$, $b' \in A$, então $a = \bar{a} = \bar{b}\bar{b}'$. Logo, $a^2 = bb'(\bar{b}'\bar{b}')$.

Se $a = 2$ então $4 = (\bar{b}b).(b'\bar{b}')$ e $x^2 + 2y^2 = bb' = 2$ (se $x^2 + 2y^2 = 4$ então $2/x^2$, $2/y^2$ e $4 = x^2 + 8y'$ que é uma contra-

dição já que $x^2 + 8y' > 4$).

Se $y = 0$ então $x = 2$. Logo, $|A/bA| = 4$ que é uma contradição. Logo, $y \neq 0$.

Então, a única possibilidade é $x = 0$ e $y = \pm 1$.

Logo, $\pm\sqrt{-2} \in \{b \in A$ tal que $\{0, \pm 1\} \longrightarrow A/bA$ é sobrejetora$\}$.

Como $\pm\sqrt{-2}$ não é unidade de A e como 2Z é maximal, $2Z = \pm\sqrt{-2}A \cap Z$. O homomorfismo canônico $Z \longrightarrow A/\sqrt{-2}A$ é sobrejetor e $\text{Ker}\ \psi = \sqrt{-2}A \cap Z$. Logo, $Z/2Z \cong A/\sqrt{-2}A$. Portanto, $\{b \in A$ tal que $\{0, \pm 1\} \longrightarrow A/bA$ é sobrejetora$\} = \{\pm\sqrt{-2}$ .

(3) $|A/bA| = 3$. Neste caso, $1 \notin bA$, $Z/bA \cap Z \neq (0)$, $|Z/bA \cap Z| \leq 3$ e $Z/bA \cap Z \subset A/bA = Z_3$. Então, $Z/bA \cap Z = A/bA = Z_3$.

Se $a = 3$ então $x^2 + 2y^2 / 9 = a^2$. Então, temos três possibilidades:

a) $x^2 + 2y^2 = 1$. Neste caso, $bb' = 1$ e b é uma unidade. Contradição.

b) $x^2 + 2y^2 = 3$. Então, $x = \pm 1$ e $y = \pm 1$.

c) $x^2 + 2y^2 = 9$. As possibilidades para este caso são $x = \pm 1$, $y = \pm 2$, $x = 3$ e $y = 0$. Em todos eles, $3 \notin bA \cap Z$. Contradição.

Então, a única possibilidade é $x = \pm 1$ e $y = \pm 1$.

Logo, $\pm 1 \pm \sqrt{-2} \in \{b \in A$ tal que $\{0, \pm 1\} \longrightarrow A/bA\}$.

Como $\pm 1 \pm \sqrt{-2}$ não é unidade de A e como 3Z é maximal, $3Z = (\pm 1 \pm \sqrt{-2})A \cap Z$. O homomorfismo canônico $Z \xrightarrow{\psi} A/(\pm 1 \pm \sqrt{-2})A$ é sobrejetor e $\text{Ker}\ \psi = (\pm 1 \pm \sqrt{-2})A \cap Z$. Logo, $Z/3Z \cong A/(\pm 1 \pm \sqrt{-2})A$. Portanto, $\{b \in A$ tal que $\{0, \pm 1\} \longrightarrow A/bA$ é sobrejetora $= \{\pm 1 \pm \sqrt{-2}\}$.

Portanto, $A_2 = \{0, \pm 1, \pm\sqrt{-2}, \pm 1 \pm \sqrt{-2}\}$.

## 2.5 - Um caso especial de algorítmo mínimo

Seja A um domínio euclidiano, $\theta$ seu algorítmo mínimo e S um subconjunto multiplicativo de A com $0 \notin S$. O algorítmo $\theta'$ em $S^{-1}A$ deduzido de $\theta$ como no lema 1.4.6 não é necessariamente o algorítmo mínimo em $S^{-1}A$.

Por exemplo, sejam $A = Z$ e S o conjunto dos inteiros primos com 6. Seja $\theta(n)$ = número de dígitos binários de $|n|$ (exemplo 2.4.1). Como $4 = \frac{1}{1}\,4$ e 4 é primo com todos os elementos de S, $\theta'(4) = \theta(4) = 3$; como $9 = \frac{1}{1}\,9$ e 9 é primo com todos elementos de S, $\theta'(9) = \theta(9) = 4$.

Vamos mostrar que para o algorítmo mínimo $\psi$ em $S^{-1}A$ temos $\psi(4) = \psi(9) = 3$.

Se $a_1, a_2 \in A$, $s_1$ e $s_2 \in S$ e $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = 1$, então $a_1.a_2 = s_1.s_2 \in S$. Logo, o conjunto das unidades de $S^{-1}A$ é $\frac{S}{S}$.

Seja $b \in S^{-1}A$; podemos escrever $b = \frac{s}{t}\,b'$, $s, t \in S$, $b' \in A$ e $(b',s) = 1$ para todo $s \in S$. Seja $S^{-1}A \xrightarrow{\psi} S^{-1}A/S^{-1}Ab$ o homomorfismo $x \longmapsto x + S^{-1}Ab$ homomorfismo canônico. Seja,

$\nu: A \to S^{-1}A/S^{-1}Ab$ a restrição de $\psi$ a A. Claramente, $x \to x + S^{-1}Ab$

$\operatorname{Ker}\nu = (b\,S^{-1}A) \cap A$. Como $\frac{s}{t}\,b' = b$ e $\frac{s}{t}$ é uma unidade de $S^{-1}A$, $S^{-1}Ab' = S^{-1}Ab$; logo $b'A \subseteq (bS^{-1}A) \cap A$.

Seja $x \in (S^{-1}Ab') \cap A$; $x = b'\frac{y}{t}$, $y \in A$, $t \in S$; e, $tx = b'y$. Se p é primo em A e $p^n/t$, então $p^n/y$; logo, $t/y$ e $y = y^*t$, $y^* \in A$. Então, $x = b'y^* \in b'A$ e podemos concluir que $(S^{-1}Ab) \cap A \subseteq Ab'$. Portanto, $\operatorname{Ker}\nu = (S^{-1}Ab) \cap A = Ab'$.

Por um teorema de isomorfismo $A/Ab' \cong \nu(A) \subseteq S^{-1}A/S^{-1}Ab$. Como a aplicação canônica $A/Ab' \to S^{-1}Ab$ é sobrejetora (demonstração do lema 1.4.6), $A/Ab' \cong S^{-1}A/S^{-1}Ab$.

Sejam $A/Ab' \xrightarrow{\nu_b} S^{-1}A/S^{-1}Ab$ e

$x+Ab' \longmapsto x + S^{-1}Ab$

$S^{-1}A \xrightarrow{\pi_b} S^{-1}A/S^{-1}Ab$

$\alpha \longmapsto \alpha + S^{-1}Ab.$

Seja $\alpha \in S^{-1}A$; então, $\alpha = \frac{x}{t}$, $x \in A$ e $t \in s$.

Afirmamos que $\alpha + S^{-1}Ab = xa + S^{-1}Ab$, onde $at - 1 \in S^{-1}Ab$; então, $\frac{1}{t} \in S^{-1}A$. Logo, $\frac{1}{t}(at - 1) \in S^{-1}Ab$ e $a - \frac{1}{t} \in S^{-1}Ab$. Portanto, $\alpha = \frac{x}{t} = x\frac{1}{t} \equiv x \cdot a \bmod S^{-1}Ab$ e, logo, $\alpha + S^{-1}Ab = xa + S^{-1}Ab$.

Uma consequência imediata de $\alpha + S^{-1}Ab = xa + S^{-1}Ab$ com $at - 1 \in S^{-1}Ab$ é $\nu_b(xa + Ab') = xa + S^{-1}Ab = \alpha + S^{-1}Ab$.

Seja $T \subseteq S^{-1}A$. Vamos resolver o seguinte problema: "quando a aplicação $\pi_b(T) \to S^{-1}A/S^{-1}Ab$ é sobrejetora?"

Definimos $T'(b) = \nu_b^{-1}(\pi_b(T))$. Então,

$T'(b) = \{ xa + Ab'$ tal que existe $\alpha \in T$ com $\alpha = \frac{x}{t}$ e $at - 1 \in Ab'\}$.

Obviamente, $\pi_b(T) = S^{-1}A/S^{-1}Ab$ se e somente se $T'(b) = A/Ab'$.

Se $T = \{0\}$, então $T'(b) = \{xa + Ab'$ tal que $0 = \frac{x}{t}$, $at-1 \varepsilon Ab'$, $a \varepsilon A\} = \{0 + Ab'\}$. Logo, $T'(b) = \{Ab'\} = A/Ab'$ se e somente se $b' \varepsilon \cup(A)$. Logo, o conjunto $(S^{-1}A)_1$ da construção transfinita (2.2.3) é igual a $\{0\} \cup \frac{S}{S}$.

Se $T = \{0\} \cup \frac{S}{S}$, então $T'(b) = \{xa + Ab'$ tal que $0 = \frac{x}{t}$ ou $\frac{s}{s'} = \frac{x}{t}$, com $at - 1 \varepsilon Ab'$, $a \varepsilon A\} = \{Ab'$, $xa + Ab'$ tal que $\frac{s}{s'} = \frac{x}{t}$ e $at - 1 \varepsilon Ab'$, $a \varepsilon A\} = \{Ab'$, $sa + Ab'$ tal que $s, t \varepsilon S$, $at - 1 \varepsilon Ab'$, $a \varepsilon A\}$. Logo, $T'(b) = A/Ab'$ se e somente se $\{Ab'$, $sa + Ab'$ tal que $s, t \varepsilon S$, $at - 1 \varepsilon Ab'$, $a \varepsilon A\} = A/Ab'$. temos:

1) Se $b' \varepsilon \frac{S}{S}$, então $\{Ab'\} = A/Ab'$

2) Se $b' = 2$, então $A/Ab' = \{Ab', 1 + Ab'\} \cong Z_2$. Para $s = 5$, $t = 1$ e $a = 1$, $sa + Ab' = 5 + Ab' = 1 + Ab'$. Logo, $\pi_b(T) = S^{-1}A/S^{-1}Ab$.

3) Se $b' = 3$, então $A/Ab' = \{Ab', 1 + Ab', 2 + Ab'\} \cong Z_3$. Para $s = 7$, $t = 1$ e $a = 1$, $sa + Ab' = 1 + Ab'$ e para $s = 5$, $t=1$ e $a = 1$, $sa + Ab' = 2 + Ab'$. Logo, $\pi_b(T) = S^{-1}A/S^{-1}Ab$.

4) Para $b' = 2^i.3^j$, $i + j \geq 2$, temos dois casos:

   a) se $i \geq 1$, então $\overline{2} \neq \overline{0}$, $sa - 2 \varepsilon Ab'$ e $2/sa$; logo, $2/at$ implica $2/-1$, que é uma contradição.

b) se $j \geq 1$, então $\bar{3} \neq \bar{0}$, $sa - 3 \in Ab'$ e $3/sa$; logo $3/at$ que implica $3/-1$, que é uma contradição.

Portanto, o conjunto $(S^{-1}A)_2$ da construção transfinita (2.2.3) é $\{0\} \cup \frac{S}{S} \cup \frac{S2}{S} \cup \frac{S3}{S}$.

Para $T = \{0\} \cup \frac{S}{S} \cup \frac{S2}{S} \cup \frac{S3}{S}$, $T'(b) = \{Ab', sa + Ab', 2sa + Ab', 3sa + Ab', s \in A$, tal que existe $t$ com $at - 1 \in Ab'\}$.

Se $b' = 4$ então $A/Ab' = \{Ab', 1 + Ab', 2 + Ab', 3 + Ab'\}$. Para $s = 5$, $a = 1$, $t = 1$, $sa + Ab' = 1 + Ab'$; para $s = 1$, $a = 1$, $t = 1$, $2sa + Ab' = 2 + Ab'$; e, para $s = 11$, $a = 1$, $t = 1$, $sa + Ab' = 3 + Ab'$.

Se $b' = 9$, então $A/Ab' = \{Ab', 1 + Ab', 2 + Ab', 3 + Ab', 4 + Ab', 5 + Ab', 6 + Ab', 7 + Ab', 8 + Ab'\}$. Para $s = 5$, $a = 1$, $t = 1$, $2sa + Ab' = 1 + Ab'$; para $s = a = t = 1$, $2sa + Ab' = 2 + Ab'$; para $s = a = t = 1$, $3sa + Ab' = 3 + Ab'$; para $s = 13$, $a = t = 1$, $sa + Ab' = 4 + Ab'$; para $s = 5$, $a = t = 1$, $sa + Ab' = 5 + Ab'$; para $s = 5$, $a = t = 1$, $3sa + Ab' = 6 + Ab'$; para $s = 7$, $a = t = 1$, $sa + Ab' = 7 + Ab'$; e, para $s = 17$, $a = t = 1$, $sa + Ab' = 8 + Ab'$.

Portanto, $4$ e $9 \in (S^{-1}A)_3 - (S^{-1}A)_2$ e $\psi(4) = \psi(9) = 3$.

Para resolver o nosso problema, foi suficiente encontrar $A_2$ e mostrar que $4$ e $9 \in (S^{-1}A)_3 - (S^{-1}A)_2$. Mas é possível mostrar que $(S^{-1}A)_n = \{0\} \cup \frac{S2^i3^j}{S}$, para todo $n$, $i + j \leq n - 1$.

# CAPÍTULO - 3

# ANÉIS DE INTEIROS

## 3.1 - Anéis de Dedekind

Definição 3.1.1 - Seja A um domínio de integridade e K seu corpo de frações. Um A - módulo $M \neq 0$, contido em K, é um ideal fracionário de A quando existe um elemento $a \in A$, $a \neq 0$, tal que $aM \subset A$.

Todo ideal de A é também um ideal fracionário (tomando a = 1) e se necessário o chamaremos ideal integral.

Entretanto, K não é um ideal fracionário de A (a não ser quando A = K).

O conjunto dos ideais fracionários de A é munido de uma operação de multiplicação: $MM' = \{ \sum_{i=1}^{n} x_i x_i' \text{ tal que } n \geq 1, x_i \in M, x_i' \in M' \}$

É fácil verificar que MM' é um ideal fracionário. Além disso, se M e M são ideais integrais, MM' também o é.

Essa operação é comutativa, asssociativa e tem um elemento unidade, que é o ideal A: MA = A.

Dizemos que um ideal fracionário M é inversível quando existe um ideal fracionário M' tal que MM' = A.

Lema 3.1.2 - Se M é um ideal fracionário e existe $x \in K$ tal que $M = Ax$, então M é inversível. Além disso, um domínio de integridade A é principal se e somente se todo ideal fracionário de A é um ideal principal de A.

Demonstração:

Se $M = Ax$, existe $M' = Ax^{-1}$ tal que $MM' = A$.

Se A é principal e M é um ideal fracionário de A, existe $x \in K$ tal que $xM \subseteq A$. Então, xM é um ideal de A e $xM = yA$. Logo $M = yx^{-1}A$.

Por outro lado, suponhamos que todo ideal fracionário de A é um ideal principal de A. Seja I um ideal de A. Existe $x \in K$ tal que $I = xA$. Como $1 \in A$, $x \in I \subseteq A$. Logo, $I = Ax$.

Teorema 3.1.3 - Seja A um domínio de integridade. As seguintes propriedades são equivalentes:

(1) A é noetheriano, integralmente fechado e todo ideal primo de A é maximal.

(2) Todo ideal (integral) de A é expresso, de maneira única, como produto de ideais primos.

(3) Todo ideal (integral) de A é produto de ideais primos.

(4) O conjunto dos ideais fracionários de A é um grupo multiplicativo.

Demonstração:

(12), pag 104, teorema 1.

Definição 3.1.4 - Um domínio de integridade A é um domínio de Dedekind quando satisfaz as propriedades equivalentes (1), (2), (3) e (4) do teorema 3.1.3.

Corolário 3.1.5 - Todo domínio de integridade principal A é um domínio de Dedekind.

Demonstração:

Seja I um ideal (integral) de A. Como A é principal, $I = (a)$, $a \in A$. Pelo corolário 1.1.25, $a = p_1^{s_1} \ldots p_k^{s_k}$, $p_i \in A$, primo.

Portanto, $I = (p_1^{s_1} \ldots p_k^{s_k}) = (p_1)^{s_1} \ldots (p_k)^{s_k}$. Como $p_i$ é primo, o ideal $(p_i)$ é primo e I é um produto de ideais primos.

Corolário 3.1.6 - Seja A um domínio de Dedekind e K seu corpo de frações. Seja L uma extensão separável de K de grau n e seja B o fecho integral de A em L. Então, B é um domínio de Dedekind.

Demonstração:

B é integralmente fechado por definição. B é um submódulo de um A - módulo livre M de posto n((12), pag 87, (A)). Como A é um anel noetheriano, M é um A - módulo noetheriano ((12), pag 91, (G)) e B também é um A - módulo noetheriano, isto é, um anel noetheriano.

Se Q é um ideal primo não-nulo de B, $Q \cap A = P$ é um ideal primo de A e $Q \cap A \neq 0$ ((12),pag 72, (B)). Então, P é um ideal maximal de A e Q é um ideal maximal de B ((12), pag 74, (G)).

Pelo teorema 3.1.3, B é um domínio de Dedekind.

Teorema 3.1.7 - Seja A um domínio de Dedekind. A é fatorial se e somente se A é principal.

Demonstração:

Pelo teorema 1.1.26, se A é principal então A é fatorial.

Suponhamos que A é fatorial. Seja I um ideal de A. Como A é um domínio de Dedekind, $I = P_1^{\ell_1} \ldots P_t^{\ell_t}$, onde os $P_i$ são ideais primos de A.

Seja $a \in P_i$. Como A é fatorial, $a = p_1^{s_1} \ldots p_k^{s_k}$. Como $P_i$ é primo, um dos $p_1, \ldots p_k$ está em $P_i$, digamos $p_{i_0}$. Então, $(0) \subsetneq (p_{i_0}) \subseteq P_i \subsetneq A$ e, pelo teorema 3.1.3 (1), $P_i$ é maximal e $P_i = (p_{i_0})$.

Portanto, $I = P_1^{\ell_1} \ldots P_t^{\ell_t} = (p_{1_0})^{\ell_1} \ldots (p_{t_0})^{\ell_t} = (p_{1_0}^{\ell_1} \ldots p_{t_0}^{\ell_t})$.

Logo, A é principal.

## 3.2 - Número de classe.

Lema 3.2.1 - Sejam A um domínio de Dedekind, G o grupo dos ideais fracionários de A e H o conjunto dos ideais fracionários principais de A. Então, H é um subgrupo normal de G.

Demonstração:

Como G é um grupo abeliano, é suficiente mostrar que H é um subgrupo de G.

De fato, se $M_1, M_2 \in H$, $M_1 = Ax_1$ e $M_2 = Ax_2$, $x_1$ e $x_2 \in K$, então $M_1 M_2 = A x_1 x_2 \in H$. Também, se $M \in H$, $M = Ax$ e $(Ax^{-1})M = M(Ax^{-1}) = A$.

Definição 3.2.2 - O grupo quociente CA = G/H é denominado classe dos divisores.

Lema 3.2.4 - Sejam $M_1$, $M_2$ $\varepsilon$ G. Então, $M_1 + H = M_2 + H$ se e somente se existe $x \varepsilon K-\{0\}$ tal que $M_1 = M_2 x$.

Demonstração :

$M_1 + H = M_2 + H$ se e somente se $M_1 M_2^{-1} \varepsilon H$.

$M_1 M_2^{-1} \varepsilon H$ se e somente se existe $x \varepsilon K-\{0\}$ tal que $M_1 M_2^{-1} = Ax$. $M_1 M_2^{-1} = Ax$ se e somente se $M_1 = M_2 Ax$. Finalmente, $M_1 = M_2 Ax$ se e somente se $M_1 = M_2 x$.

Teorema 3.2.4 - CA = {1} se e somente se A é principal.

Demonstração:

Se CA = {1} então H = G. Logo, dado um ideal $I \neq (0)$ (integral) de A, existe $x \varepsilon K-\{0\}$ tal que $I = Ax$. Portanto, A é principal.

Suponhamos que A é principal. Seja M um ideal fracionário de A. Existe $x \varepsilon A$ tal $xM \subseteq A$, isto é, xM é um ideal de A. Logo, existe $y \neq 0 \varepsilon A$ tal que $xM = Ay$. Portanto, $M = A(y/x)$ e $M \varepsilon H$. Então, H = G.

Definição 3.2.5 - O inteiro $n_A = |CA|$ é denominado o número de classe de A.

Corolário 3.2.6 - $n_A = 1$ se e somente se A é principal.

Demonstração:

Imediata do teorema 3.2.4.

## 3.3 - O número de classe do anel dos inteiros algébricos de $Q[\sqrt{d}]$.

Definição 3.3.1 - Seja K uma extensão de F. Um elemento $x \in K$ é algébrico sôbre F se existem elementos $\alpha_0, \ldots \alpha_n$ em F, não todos nulos, tais que $\alpha_0 x^n + \ldots + \alpha_n = 0$.

Definição 3.3.2 - Dizemos que um número complexo x é um número algébrico se é algébrico sôbre o corpo Q dos números racionais.

Definição 3.3.3 - Um número algébrico que é uma raiz de um polinômio mônico com coeficientes em Z é chamado um inteiro algébrico.

Seja K uma extensão quadrática de Q, isto é, $[K:Q] = 2$. $K = Q[\sqrt{d}]$ onde d é um inteiro livre de quadrados ((12), pag 60).

Seja A o anel de todos os inteiros algébricos de $Q[\sqrt{d}]$.

Para $2 \leq d \leq 499$, d livre de quadrados, temos:

142 A com $n_A = 1$

109 A com $n_A = 2$

12 A com $n_A = 3$

25 A com $n_A = 4$ ((8), pag 422, 423 e 424)

3 A com $n_A = 5$

3 A com $n_A = 6$

3 A com $n_A = 8$

Os únicos inteiros a, $a = -d$, $1 \leq a < 500$, livres de quadrados para os quais $n_A = 1$ são: 1, 2, 3, 7, 11, 43, 67 e

167 ((8), pag 425 e 426).

## 3.4 - Anéis dos inteiros de extensões quadráticas e ciclotômicas.

Vimos na seção anterior que existem muitos aneís dos inteiros algébricos de $Q[\sqrt{d}]$ que são principais.

O problema consiste em saber quais desses anéis são euclidianos.

Já foi mostrado que existem exatamente cinco corpos quadráticos imaginários $Q[\sqrt{d}]$ , d = -1, -2, -3, -7, -11 e dezesseis corpos quadráticos reais, d = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73, para os quais o anei dos inteiros algébricos é euclidiano (em todos eles o algorítmo euclidiano é a norma) (7)

Vamos mostrar que os únicos corpos quadráticos imaginários $Q[\sqrt{d}]$ para os quais o anel dos inteiros algébricos é euclidiano são aqueles para os quais d = -1, -2, -3, -7, -11.

Lema 3.4.1 - Seja A o anel de todos os inteiros algébricos de $Q[\sqrt{d}]$ , d livre de quadrados. $a + b\sqrt{d} \in A$ se e somente $2a = u \in Z$, $2b = v \in Z$ e $u^2 - dv^2 \equiv 0 \pmod 4$.

Demonstração:

Se $x = a + b\sqrt{d} \in A$, então seu conjugado $x' = a - b\sqrt{d}$ é também um inteiro algébrico. Logo,
$x + x' = 2a \in A \cap Q = Z$, $xx' = a^2 - b^2 d \in Z$

Segue que $(2a)^2 - (2b)^2 \in 4Z$ e, como $(2a)^2 \in Z$, também $(2b)^2 \in Z$; mas d é um inteiro livre de quadrados, então 2b

tem denominador igual a 1, isto é, $2b = v \in Z$.

Por outro lado, essas condições implicam $a^2 - b^2 d \in Z$ e, como x é uma raiz de $X^2 - 2ax + (a^2 - b^2 d)$, x é um inteiro algébrico.

Lema 3.4.2 - Sejam $K = Q[\sqrt{d}]$, onde d é um inteiro livre de quadrados e A o anel de todos os inteiros algébricos de K.

Se $d \equiv 1 \pmod 4$ então $A = \{u/2 + v/2\sqrt{d}$, u e v $\in Z$, u e v com a mesma paridade$\}$. Se $d \equiv 2$ ou $3 \pmod 4$, então, $A = \{ a + b\sqrt{d}$ com a, b $\in Z\}$.

Demonstração:

Examinaremos todos os casos possíveis.

Se $d \equiv 2 \pmod 4$

| u | par | par | impar | impar | |
|---|---|---|---|---|---|
| v | par | impar | par | impar | |
| $u^2 - dv^2 \equiv$ | 0 | 2 | 1 | 3 | mod 4 |

Se $d \equiv 3 \pmod 4$

| u | par | par | impar | impar | |
|---|---|---|---|---|---|
| v | par | impar | par | impar | |
| $u^2 - dv^2 \equiv$ | 0 | 1 | 1 | 2 | mod 4 |

Se $d \equiv 1 \pmod 4$

| u | par | par | impar | impar | |
|---|---|---|---|---|---|
| v | par | impar | par | impar | |
| $u^2 - dv^2 \equiv$ | 0 | 3 | 1 | 0 | mod 4 |

Agora, o resultado segue do lema 3.4.1.

Lema 3.4.3 - Os únicos corpos quadráticos imaginários

$Q[\sqrt{-d}]$ para os quais o anel A dos inteiros algébricos é euclidiano são aqueles cujo d = 1, 2, 3, 7, 11.

Demonstração:

Exceto para d = 1 e d = 3, as únicas unidades em em A são $\pm 1$. ((12), pag 131,(D)). Excluido esses dois casos, usamos a construção transfinita (2.2.3). Então, $A_1 = \{-1, 0, +1$ (com a notação dessa construção). $A_2 - A_1$ consiste de todos os elementos de norma 2 ou 3. Para $-d \equiv 2$ ou 3 (mod 4), temos $A = Z + Z\sqrt{-d}$ (lema 3.4.2) e a norma de $x = a + b\sqrt{-d}$ $(a, b \in Z)$ é $a^2 + b^2 d$; a equação $a^2 + b^2 d = 2$ ou 3 tem solução somente se $d \leq 3$. Para $d \equiv 1$ (mod 4), $A = \{a/2 + b/2\sqrt{-d}$, a, b $\in Z$, a e b com a mesma paridade$\}$, a equação a ser resolvida é $a^2 + b^2 d = 8$ ou 12 e tem solução somente se $d \leq 12$, isto é, somente se d = 7 ou 11.

Portanto, se A é euclidiano, $A_2 - A_1 \neq \emptyset$ e os únicos possíveis valôres para d são 2, 7, 11 (também 1 e 3). Mas, em cada um desses cinco casos, sabe-se que A é euclidiano.

Lema 3.3.4 - $X^n - 1$ tem n zeros distintos em corpo decomponível $Z_n$ sôbre o corpo Q dos números racionais.

Demonstração:

Existe um corpo decomponível para $x^n - 1$ ((20, pag. 206, teorema 2), onde $x^n - 1$ tem no máximo n zeros distintos. Como Mdc $(x^n - 1, nx^{n-1}) = 1$, $x^n - 1$ tem exatamente n zeros distintos.

Lema 3.4.5 - Os zeros de $x^n-1$ formam um grupo multiplicativo $T_n$ de ordem n em Z. Este grupo tem $\psi(n)$ geradores ($\psi$ = função de Euler).

Demonstração:

É fácil verificar que os n zeros de $x^n-1$ formam um grupo multiplicativo em $Z_n$. Como $T_n$ é um grupo abeliano finito existe um $m \leq n$ tal que $\zeta^m = 1$ para todo $\zeta \in T_n$ e $T_n$ tem um elemento de ordem m. Se $m < n$, então $x^m-1$ teria n zeros que é uma contradição. Portanto , $m = n$ e existe um elemento $\zeta$ de ordem n em $T_n$.

Definição 3.4.6 - Os geradores de $T_n$ são chamados as n-ésimas raízes primitivas da unidade.

Lema 3.4.7 - $Z_n = Q(\zeta)$ onde $\zeta$ é uma n-ésima raiz primitiva da unidade.

Demonstração:

$x^n-1$ tem todos os zeros em $Q(\zeta)$ porque eles são todos potências de $\zeta$.

No que segue, seja m um inteiro positivo e $\zeta_m$ uma raiz m-ésima primitiva da unidade. O anel dos inteiros de Z em $Q(\zeta_m)$ é $Z[\zeta_m]$ ((12), pag 269, 4B).

Como $Z[\zeta_m] = Z[\zeta_{2m}]$ para m impar, temos onze anéis euclidianos não isomorfos correspondentes a m = 1, 3, 4, 5, 7,8,9 11, 12, 15 e 20. Os casos m = 1, 3, 4, 5, 8, 12 são mais ou menos clássicos ((1), pag 117 - 118 e 391 - 393; (2),

(3), pag 228-231); (7), capitulos 12, 14 e 15; (13); e (15)). Os outros cincos casos são aparentemente novos.

Para m par, o anel $Z[\zeta_m]$ tem número de classe 1 se e somente se $\psi(m) \leq 20$ ou $m = 70$, 84 ou 90, (14). Logo, existem exatamente trinta anéis $Z[\zeta_m]$ não isomorfos que são principais.

Para $\psi(m) \leq 10$, $m \neq 16$, $m \neq 24$, $Z[\zeta_m]$ é euclidiano para a norma (22).

## 3.5 - Exemplos de anéis principais não euclidianos.

Em 1949, T. Motzkin (4) mostrou que o anel dos inteiros de $Q[\sqrt{-19}]$ não é euclidiano.

Em 1971, P. Samuel (10) mostrou que o anel dos inteiros de $Q[\sqrt{-19}]$, $Q[\sqrt{-67}]$, $Q[\sqrt{-163}]$ não são euclidianos (imediata do lema 3.4.3).

Em 1973, J.C. Wilson (16) mostrou, baseado no trabalho de T. Motzkin (4), que o anel dos inteiros de $Q[\sqrt{-19}]$ não é euclidiano, usando uma linguagem mais acessível aos estudantes não graduados em algebra.

Em 1975, K.W. Kenneth (21) deu tratamento ainda mais simples ao trabalho de J.C. Wilson (16) e também mostrou que o anel dos inteiros de $Q[\sqrt{-19}]$, $Q[\sqrt{-43}]$, $Q[\sqrt{-67}]$ e $Q[\sqrt{-163}]$ não são euclidianos.

Em 1971, R.E. MacRae (11) mostrou que $A=Z_3[x,y]/(y^2-x^3+x+1)$ é principal mas não é euclidiano.

Em 1973, C.Queen (19) mostrou que $M^{-1}A$ é euclidiano, onde $M = \{(x + 2)^i \cdot (x + 1)^j\}$.

Em 1974, R. Markanda (19) mostrou que $M^{-1}A$ não é euclidiano pela norma.

## 3.6 - Um problema em aberto.

Quanto aos corpos quadráticos reais, aqueles para os quais o anel dos inteiros é euclidiano não são conhecidos. Nem mesmo se sabe se existe um corpo para o qual o anel dos inteiros é euclidiano sem ser euclidiano pela norma (isto é, um corpo fora da lista dos dezesseis da seção anterior).

P.Samuel (10) acredita que $Z[\sqrt{14}]$ pode ser um provável candidato.

## Bibliografia


(1) C.F. Gauss, Werke, Zweiter Band (Gottinger, 1876)

(2) J. Ouspensky, Note sur les nombres entier dépendant d'une racine cinquième de l'unité, Math, Ann., 66, (1909), 109-112.

(3) E. Landau, Vorlesungen über Zahlentheorie, Band 3, (Leipzig, 1927)

(4) T. Motzkin, On the Euclidean Algorithm, Bulletin of Americ. Math. Soc, vol 55, (1949), 1142-1149

(5) O. Zariski, P.Samuel, Comutative Algebra, Van Nostrand, (NY, 1958)

(6) I. Herstein, Topics in Algebra, Blaisdell, (NY, 1964)

(7) G.H. Hardy, E.M. Wright, An Introduction to The Theory of Numbers, Oxford Un. Press, (London, 1965)

(8) Z.I. Borevich, I.R.Shafarevich, Number Theory, Academic Press, (NY, 1966)

(9) J.W.S. Cassels, On a conjecture of R.M. Robinson about sums of roots on unity, J. Reine Angew Math, 238, (1969), 112-131

(10) P.Samuel, About Euclidean Rings, Journal of Algebra, vol 19, (1971), 282-301

(11) R.E.MacRae, On Unique Factorization in Certain Rings of Algebraic Functions, Journal of Algebra, vol 17, (1971), 243-261

(12) P.Ribenboim, Algebraic Numbers, Wiley-Interscience, (NY, 1972)

(13) R.B.Lakein, Euclid's Algorithm in Complex Fields, Acta Arith, 20, (1972), 393-400

(14) J.M.Masley, On the Class Number of Ciclotomic Fields, (thesis, Princepton Universitary), (1972)

(15) On Ciclotomic Fields Euclidean for The Norm Map, Notices Americ. Math. Soc., 19,(1972), A-813 (abstract- 700-A 3)

(16) J.C. Wilson, A Principal Ideal Ring That Is Not Euclidean, Mathematic Magazine, Jan-Feb, (1973)

(17) P.J. Weinberger, On Euclidean Rings of Algebraic Integers, Proc. Symp. Pne Math., 24 (Analytic Number Theory), 321-332, Americ. Math. Soc., (1973)

(18) C.Queen, Euclid's Algorithm in Global Fields, Bull. Americ. Math. Soc., vol 79, (1973), 1229-1231

(19) R.Markanda, Un Exemple d'Anneaux Eucliden, Contes Rendus Acad. Sc. Paris, vol 279, (1974), (A), 125-126

(20) R.A. Dean, Elementos de Álgebra Abstrata, Livros Técnicos e Científicos Editora S.A., (Rio de Janeiro, 1974)

(21) S.W. Kenneth, Note on Non-Euclidean Principal Ideal Domains, Mathematics Magazine, may-june, (1975).

(22) H.W.Lenstra, Euclid's Algorithm in Ciclotomic Fields, Journal London Math. Soc. (2), 10, (1975), 457-465