UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
DEPARTAMENTO DE MATEMÁTICA
CURSO DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Maria de Fátima Cruz Tavares

RETICULADOS OBTIDOS POR COLAGEM

FORTALEZA
2011

Maria de Fátima Cruz Tavares

RETICULADOS OBTIDOS POR COLAGEM

Dissertacão submetida à Coordenação do Curso de Pós-Graduação em Matemática, da Universidade Federal do Ceará, para a obtenção do grau de Mestre em Matemática.

Área de concentracão: Matemática

Orientador: Prof. Dr. José Othon Dantas Lopes

Fortaleza

2011

Tavares, Maria de Fátima Cruz

T231r Reticulados obtidos por colagem / Maria de Fátima Cruz Tavares. – Fortaleza, 2011.

82f. :il.

Orientador: Prof. Dr. José Othon Dantas Lopes

Área de concentração: Matemática

Dissertação (Mestrado) - Universidade Federal do Ceará, Centro de Ciências, Depto de Matemática, 2011.

1 - Álgebra I. Lopes, José Othon Dantas (Orient.)

CDD 512

Aos meus pais, irmãos e sobrinhos amados,
dedico.

Agradecimentos

À minha família pelo apoio e compreensão nos momentos de ausência.

Ao meu orientador querido, José Othon Dantas Lopes, pela amizade sincera, paciência, dedicação, incentivo e por depositar em mim sua confiança diante desse trabalho.

Aos meus professores do Departamento de Matemática da UFC, pela excelente formação. Aos professores José Valter Lopes Nunes e José Afonso de Oliveira, pelo acompanhamento mais de perto do desenvolvimento desse trabalho.

Aos meus professores de graduação, Mário de Assis, Fernando Luiz, Zelálber Gondim, Marcos Antônio e José Alves, em especial ao querido professor Juscelino P. Silva, pela amizade sincera, incentivo e confiança depositada em mim, que foi motivo maior para realização deste sonho.

Aos meus colegas do curso de Pós - Graduação, pela amizade e pelo agradável convívio.

As minhas amigas queridas, Wanderlândia, Jardênia, Priscila, Raquel, Lília, Heloísa, Kiara, Selene e Elaine, por compartilhar as alegrias, tristezas e dificuldades durante essa caminhada que agora se completa.

À Andréa Costa Dantas, pelo carinho e toda sua atenção.

Aos membros da banca: Prof. Dr. Trajano Pires da Nobrega Neto e Prof. Dr. José Alberto Duarte Maia.

À FUNCAP pelo suporte financeiro.

À todos que direta ou indiretamente contribuíram para a realização deste sonho, em especial ao meu amigo Gladeston, pela ajuda com o latex.

E acima de Tudo a Deus. Não enumero os motivos pela simples razão de não caberem em nenhum livro.

Resumo

O objetivo principal desse trabalho é a obtenção de novos reticulados através de uma técnica elementar por colagem. Para reticulados quaisquer $\mathscr{A}$ e $\mathscr{B}$ de dimensões n e m respectivamente, esta técnica nos permite a obtenção de um outro reticulado $(n+m-1)$ - dimensional. Dado dois reticulados $\mathscr{A}$ e $\mathscr{B}$ de dimensões $n \geq 2$ e $m \geq 2$ respectivamente, contendo o reticulado Λ_2, nos permite a obtenção de um novo reticulado $(n+m-2)$ - dimensional. Em particular, dado um reticulado n - dimensional $\mathscr{H}$, com densidade de centro δ, nos permite explicitamente a obtenção de um novo reticulado $(n+1)$ - dimensional $\mathscr{H}'$, com densidade de centro $\delta/\sqrt{3}$. Através deste método, novos reticulados são encontrados e analisaremos alguns de seus parâmetros principais, como o volume, a distância mínima, a quantidade de vetores de comprimento mínimo e a densidade de centro.

Palavras-Chaves: reticulados, técnica, colagem, dimensões, densidade de centro.

Abstract

The main objective of this work is to obtain new lattices through an elementary technique of collage. For any lattices $\mathscr{A}$ and $\mathscr{B}$ of dimension n and m respectively, this technique allows us to obtain a other lattice $(n+m-1)$ - dimensional. Given two lattices $\mathscr{A}$ and $\mathscr{B}$ of dimension $n \geq 2$ and $m \geq 2$ respectively, with an a lattice Λ_2, this technique allows us to obtain a new lattice $(n+m-2)$ - dimensional. In particular, given one lattice n - dimensional $\mathscr{H}$, with center density δ, this technique allows us to explicitly obtain a new lattice $(n+1)$ - dimensional $\mathscr{H}'$, with center density $\delta/\sqrt{3}$. Through this method, new lattices are found and will review some of its key parameters such as volume, the minimum distance, the number of vectors of minimum length and center the density.

Keywords: lattices, technique, collage, dimension, center density.

Sumário

Lista de Figuras

Lista de Siglas

$\mathbb{N}$: conjunto dos números naturais

$\mathbb{Z}$: conjunto dos números inteiros

$\mathbb{Q}$: conjunto dos números racionais

$\mathbb{R}$: conjunto dos números reais

$\mathbb{C}$: conjunto dos números complexos

$\mathbb{K}, \mathbb{L}$: corpos

$\mathfrak{a}, \mathfrak{b}, \mathfrak{p}, \mathfrak{q}$: ideais

$F(X), G(X), P(X), Q(X)$: polinômios

$\mathbb{L}/\mathbb{K}$: $\mathbb{L}$ é uma extensão de $\mathbb{K}$

$A[x]$: anel dos polinômios sobre A em x

$\ker(\sigma)$: núcleo do homomorfismo σ

$a|b$: a divide b

$\varphi(n)$: φ-função de Euler para o inteiro n

$[\mathbb{L} : \mathbb{K}]$: grau de $\mathbb{L}$ sobre $\mathbb{K}$

$\mathscr{N}_{\mathbb{L}/\mathbb{K}}$: norma em relação à extensão $\mathbb{L}/\mathbb{K}$

$\mathscr{N}(\mathfrak{p})$: norma de um ideal $\mathfrak{p}$

$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}$: traço em relação à extensão $\mathbb{L}/\mathbb{K}$

(A_{ij}): matriz

$\det(A_{ij})$: determinante da matriz (A_{ij})

$D(x_1,\ldots,x_n)$: discriminante de uma n-upla

$\zeta_n = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$: raiz n-ésima da unidade

ζ: raiz p-ésima primitiva da unidade

$\sum$: somatório

$\prod$: produtório

$\mathrm{card}(X)$: cardinalidade de um conjunto X

$\mathscr{A},\mathscr{B},\mathscr{C},\mathscr{H}$: reticulados

$Vol(\mathscr{H})$: volume do reticulado $\mathscr{H}$

$\dim\mathscr{H}$: dimensão do reticulado $\mathscr{H}$

$\mathrm{Dist}_{\min}(\mathscr{H})$: distância mínima do reticulado $\mathscr{H}$

$\mathrm{Kiss}(\mathscr{H})$: números de vetores de comprimento mínimo do reticulado $\mathscr{H}$

$\delta(\mathscr{H})$: densidade de centro do reticulado $\mathscr{H}$

$\Delta(\mathscr{H})$: densidade de empacotamento do reticulado $\mathscr{H}$

$[x]$: inteiro mais próximo de x

$\overline{x}$: conjugado complexo do elemento x

$\overline{\alpha}$: conjugação complexa $(\overline{\alpha}(x) = \overline{\alpha(x)})$

$\frac{a}{b}$: quociente de a por b

Introdução

Encontrar reticulados com maior densidade de empacotamento em cada dimensão é um problema clássico em teoria dos números e este parte do 18º problema de Hilbert proposto em 1900, que consistia em saber como dispor esferas no espaço, de modo que elas ocupem a maior fração desse espaço, ou seja, que esta distribuição tenha maior densidade. Dentre uma lista de questões este problema teve destaque no desenvolvimento da ciência e têm sido um grande desafio para vários matemáticos. Entendemos por empacotamente esférico a disposição de esferas de mesmo raio no espaço euclidiano n - dimensional de tal modo que a intersecção de duas delas tenha no máximo um ponto. Dentre os empacotamentos esféricos, aqueles cujo conjunto de centros das esferas constituía um subgrupo discreto do $\mathbb{R}^n$, despertaram particular interesse e passaram a se chamar empacotamentos reticulados. Em 1948 com a publicação do artigo de Claude E. Shannon, ficou estabelecido que o problema de encontrar empacotamentos esféricos densos em um dado espaço é equivalente a encontrar códigos corretores de erros eficientes. A partir daí, passaram-se a associar o estudo dos códigos ao dos reticulados. Com isso, o interesse pelo 18° problema de David Hilbert aumentou consideravelmente, surgiram várias famílias de reticulados, cada uma delas visando dar uma melhor contribuição no que diz respeito à densidade de empacotamento.

Um código baseado em reticulados pode ser avaliado primeiramente pela sua densidade, em que o melhor código possui o maior valor de densidade de empacotamento de esferas. Uma segunda categoria de avaliação é o "kissing number", em que o melhor código é o que possui o menor "kissing number"(menor número de vizinhos), pois um número maior de vizinhos incrementa a probabilidade de erro na transmissão. No empacotamento reticulado, o "kissing number"é o mesmo para qualquer esfera. Em empacotamentos arbitrários, o "kissing number"pode variar de uma esfera para outra. No espaço tridimensional, o problema do "kissing number"apareceu em uma famosa discussão entre Isaac Newton e David Gregory, em 1694. Este problema pergunta quantas esféras idênticas podem ser arranjadas de forma que todas elas

toquem uma outra esféra idêntica central. No espaço n - dimensional o problema do "kissing number"pode ser considerado análogo ao problema do empacotamento esférico, tratando-se do "empacotamento"de pontos distribuídos na superfície de uma esfera. Se enunciarmos o problema do "kissing number"perguntando quantos pontos podem ser colocados na superfície de uma esfera n - dimensional tal que a separação angular entre quaisquer dois pontos seja ao menos igual a 60^o, vemos que o problema do "kissing number"tem relação estreita com códigos esféricos.

Afim de encontrar reticulados com ótimas densidades, nesse trabalho apresentaremos uma técnica elementar por colagem para obtenção de novos reticulados e analisaremos alguns de seus parâmetros principais, como o volume, a distância mínima, a quantidade de vetores de comprimento mínimo, ou seja, o "kissing number"e a densidade de centro. Para reticulados quaisquer $\mathscr{A}$ e $\mathscr{B}$ com dimensões n e m respectivamente, esta técinca nos permite a obtenção de um novo reticulado $(n+m-1)$ - dimensional. Dados dois reticulados $\mathscr{A}$ e $\mathscr{B}$ de dimensões $n \geq 2$ e $m \geq 2$ respectivamente, contendo o reticulado Λ_2, nos permite a obtenção de um outro reticulado $(n+m-2)$ - dimensional. Em particular, dado um reticulado n - dimensional $\mathscr{H}$, com densidade de centro δ, nos permite explicitamente a obtenção de um outro reticulado $(n+1)$ - dimensional $\mathscr{H}'$, chamado de reticulado estendido, com densidade de centro $\delta/\sqrt{3}$. A construção exige uma matriz geradora para $\mathscr{H}$ e um vetor de comprimento mínimo em $\mathscr{H}$, que produzirá uma matriz geradora para $\mathscr{H}'$.

No primeiro capítulo apresentamos aos leitores com menos conhecimentos em teoria algébrica dos números. Sendo assim, introduzimos os conceitos de divisibilidade em anéis de ideais principais, módulos sobre anéis de ideais principais, raízes da unidade, corpos finitos, elementos inteiros sobre anéis e algébricos sobre um corpo, elementos conjugados, corpos conjugados, inteiros em corpos quadráticos, norma, traço, discriminante, corpos numéricos e ciclotômicos, módulos Noetherianos, anel de Dedekind, norma de um ideal e outros conceitos indispensáveis ao desenvolvimento dos demais capítulos.

No segundo capítulo apresentamos a teoria de reticulados, dando ênfase à sua relação com o problema do empacotamento esférico. Introduzimos também alguns exemplos de reticulados e suas propriedades.

No terceiro capítulo, fornecendo os pré-requisitos específicos, detalhamos as demonstrações dos resultados usados na construção dos novos reticulados obtidos por colagem. Em seguida, faremos a calagem de reticulados em um ponto, que tem dimensão zero, depois a calagem em dimensão 1 e finalizaremos com a calagem em dimensão 2. Para concluir o trabalho, faremos algumas aplicações de um caso particular dessa última colagem.

Capítulo 1

Preliminares

Conteúdo

As demonstrações feitas nesse capítulo foram baseadas em [Samuel 2008]

1.1 Divisibilidade em anéis de ideais principais e φ-função de Euler

Definição 1.1 *Sejam A um domínio de integridade, $\mathbb{K} = \left\{ \frac{a}{b} \mid a,b \in A,\ b \neq 0 \right\}$ seu corpo de frações e x,y elementos de $\mathbb{K}$. Dizemos que x divide y se existe $a \in A$ tal que $y = ax$. Equivalentemente, dizemos que x é um divisor de y, ou que y é múltiplo de x.*

Definição 1.2 *Dado $x \in \mathbb{K}$, chamamos Ax o conjunto dos múltiplos de x. Assim, podemos dizer que $y \in Ax$, em vez de $x|y$, ou ainda $Ay \subset Ax$.*

Observação 1.1 *O conjunto Ax é chamado um ideal principal fracionário de $\mathbb{K}$, com respeito a A. Se $x \in A$, então Ax é o ideal principal (ordinário) de A gerado por x.*

A relação de divisibilidade possui as seguintes propriedades:

i. $x|x$

ii. Se $x|y$ e $y|z$ então $x|z$

Em geral, não podemos concluir que se $x|y$ e $y|x$ então $x = y$. Podemos apenas dizer que $Ax = Ay$, o que significa $(\text{se } y \neq 0)$ que o quociente xy^{-1} é um elemento invertível de A. Neste caso, x e y são chamados de associados.

Observação 1.2 *Os elementos de $\mathbb{K}$ que são associados de 1_A, identidade de A, são os elementos invertíveis em A. Eles são chamados as unidades de A. Estes elementos formam um grupo com a multiplicação e denotamos este grupo por A^*.*

Exemplo 1.1 *Se A é um corpo, então $A^* = A - (0)$. Se $A = \mathbb{Z}$, então $A^* = \{1,-1\}$*

Definição 1.3 *Um anel A é chamado anel de ideais principais, se o mesmo é um domínio de integridade e se todo ideal dele for principal.*

Exemplo 1.2 *$\mathbb{Z}$ é um anel de ideais principais.*

Exemplo 1.3 *Se $\mathbb{K}$ é um corpo, o anel de polinômios em uma variável sobre $\mathbb{K}$, $\mathbb{K}[x]$, é um anel de ideais principais.*

Vejamos algumas propriedades de divisibilidade em um corpo de frações $\mathbb{K}$ de um anel de ideais principais A.

i. Dois elementos arbitrários u e v de $\mathbb{K}$ possuem um máximo divisor comum (mdc), isto é, um elemento $d \in \mathbb{K}$ para o qual vale a seguinte relação:

$$x|u \qquad \text{e} \qquad x|v \qquad \Leftrightarrow \qquad x|d \tag{1.1}$$

ii. (Identidade de Bezout): Existem elementos $a, b \in A$ tal que o mdc de u e v pode ser escrito da forma:

$$d = au + bv \tag{1.2}$$

iii. Dois elementos arbitrários u, v de $\mathbb{K}$, possuem um mínimo múltiplo comum (mmc), isto é, existe um elemento $m \in \mathbb{K}$, para o qual é válida a relação:

$$u|x \qquad \text{e} \qquad v|x \qquad \Leftrightarrow \qquad m|x \tag{1.3}$$

iv. Vale a seguinte relação entre o mdc e o mmc:

$$\text{mdc}(u,v).\ \text{mmc}(u,v) = u.v \tag{1.4}$$

Definição 1.4 *Dois elementos a, b de A são chamados relativamente primos se $mdc(a,b) = 1$*

Lema 1.1 (Euclides) *Sejam a, b elementos de um anel de ideais principais A. Se a divide bc e a é relativamente primo com b então, a divide c.*

Prova: Pela identidade de Bezout, existem $a', b' \in A$ tais que:

$$1 = a'a + b'b \Rightarrow\ c = a'ac + b'bc$$

Como a divide bc, então a divide $b'bc$. Por outro lado, a divide $a'ac$. Logo, a divide $a'ac + b'bc$ e daí a divide c.

O teorema a seguir mostra que existe uma única fatoração em produtos de primos.

Teorema 1.1 *Seja A um anel de ideais principais e $\mathbb{K}$ seu corpo de frações. Então existe um subconjunto $P \subset A$ tal que todo $x \in \mathbb{K}$ pode ser expresso unicamente da forma*

$$x = u \prod_{p \in P} p^{v_p(x)}$$

onde u é uma unidade em A e os expoentes $v_p(x)$ são elementos de $\mathbb{Z}$, todos nulos, exceto para um subconjunto finito deles.

(Veja a demonstração do Teorema 1.1 em [Mollin 1999])

Definição 1.5 *Seja $n \geq 1$, definimos $\varphi(n)$ como sendo o número de inteiro q, com $0 \leq q \leq n$, tal que q e n são relativamente primos. Como 0 e n são divisíveis por n, basta considerarmos $1 \leq q \leq n-1$, $\forall\, n > 1$ e definimos $\varphi(1) = 1$. A função φ assim definida é chamada φ-função de Euler.*

Observação 1.3 *Se p é primo, então claramente temos:*

$$\varphi(p) = p - 1$$

pois, como p é primo, todos os elementos q, com $1 \leq q \leq p-1$, são relativamente primos com p.

Observação 1.4 *Se $n = p^s$, uma potência de um primo, então os inteiros relativamente primos com n são todos inteiros q, com $1 \leq q \leq n-1$, os quais não são múltiplos de p.*

Proposição 1.1 *Seja $n \geq 1$ um número natural. O valor $\varphi(n)$ da φ-função de Euler é igual ao número de elementos de $\mathbb{Z}/n\mathbb{Z}$ que geram este grupo. Também é igual ao número de unidades do anel $\mathbb{Z}/n\mathbb{Z}$.*

Prova: Sabemos que cada classe de congruência módulo $n\mathbb{Z}$, contém um único inteiro q tal que $0 \leq q \leq n-1$. Para cada inteiro q, denote $\overline{q}$ sua classe residual módulo $n\mathbb{Z}$. Para demonstrarmos esta proposição vamos mostrar as seguintes implicações:
(I) q relativamente primo com $n \Rightarrow \overline{q}$ uma unidade do anel $\mathbb{Z}/n\mathbb{Z}$.

De fato, suponha que q é relativamente primo com n. Assim, pela identidade de Bezout, existem inteiros x, y tais que $qx + ny = 1$. Daí, $\overline{qx+ny} = \overline{1} \Rightarrow \overline{qx} + \overline{ny} = \overline{1} \Rightarrow \overline{qx} = \overline{1} \Rightarrow \overline{q}\,\overline{x} = \overline{1}$. Logo, $\overline{q}$ é uma unidade em $\mathbb{Z}/n\mathbb{Z}$.
(II) $\overline{q}$ uma unidade do anel $\mathbb{Z}/n\mathbb{Z} \Rightarrow \overline{q}$ gera o grupo aditivo $\mathbb{Z}/n\mathbb{Z}$.

Se $\overline{q}$ é uma unidade em $\mathbb{Z}/n\mathbb{Z}$ então existe um inteiros x tal que $\overline{q}\,\overline{x} = \overline{1}$. Daí, $\overline{a}\,\overline{q}\,\overline{x} = \overline{a}$ (no anel $\mathbb{Z}/n\mathbb{Z}$) onde $\overline{a}$ é um elemento arbitrário de $\mathbb{Z}/n\mathbb{Z}$, com $0 \leq a < n$. Segue-se que $\overline{a} = \overline{a}\,\overline{x}\,\overline{q} = (ax)\overline{q}$ (no grupo aditivo $\mathbb{Z}/n\mathbb{Z}$). Logo, $\overline{q}$ gera o grupo $\mathbb{Z}/n\mathbb{Z}$.
(III) $\overline{q}$ gera o grupo aditivo $\mathbb{Z}/n\mathbb{Z} \Rightarrow q$ relativamente primo com n.

Se $\overline{q}$ gera o grupo $\mathbb{Z}/n\mathbb{Z}$, então existe um inteiro x tal que $x\overline{q} = \overline{1}$. Assim, $xq \equiv 1 \mod n$. Daí, existe um inteiro y tal que $xq - 1 = yn \Rightarrow 1 = xq - yn$. Seja $d = \text{mdc}(q,n)$ então $d|q$ e $d|n$. Assim, $d|(xq - yn)$. Logo, $d|1$. Portanto, $\text{mdc}(q,n) = 1$.

Lema 1.2 *Sejam A um anel, $\mathfrak{a}$ e $\mathfrak{b}$ ideais de A tal que $\mathfrak{a} + \mathfrak{b} = A$. Então $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$ e o homomorfismo canônico $\sigma : A \to A/\mathfrak{a} \times A/\mathfrak{b}$ induz um isomorfismo $\theta : A/\mathfrak{ab} \to A/\mathfrak{a} \times A/\mathfrak{b}$. Lembre-se que o homomorfismo σ leva cada $x \in A$ no par, consistindo das classes de x módulo $\mathfrak{a}$ e das classes de x módulo $\mathfrak{b}$.*

Prova: Sabemos que, em geral $\mathfrak{ab} \subset \mathfrak{a}$ e $\mathfrak{ab} \subset \mathfrak{b}$, então $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$. Seja $x \in \mathfrak{a} \cap \mathfrak{b}$, como $\mathfrak{a} + \mathfrak{b} = A$, então existem elementos $x_1 \in \mathfrak{a}$ e $x_2 \in \mathfrak{b}$ tais que $x_1 + x_2 = 1_A$. Daí, $x = x_1x + x_2x = x_1x + xx_2$, pois A é comutativo. Como $x_1x \in \mathfrak{ab}$ e $xx_2 \in \mathfrak{ab}$ então $x_1x + xx_2 \in \mathfrak{ab}$. Logo, $x \in \mathfrak{ab}$ e assim, $\mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{ab}$. Portanto, $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$.

Mostraremos agora que o homomorfismo σ induz o isomorfismo θ. De fato, $\ker\sigma = \{x \in A;\ \sigma(x) = 0_{A/\mathfrak{a}\times A/\mathfrak{b}}\}$. Seja $x \in \ker\sigma$, daí $\sigma(x) = 0$ implica $(x + \mathfrak{a}, x + \mathfrak{b}) = (0 + \mathfrak{a}, 0 + \mathfrak{b}) \Rightarrow x + \mathfrak{a} = 0 + \mathfrak{b}$ e $x + \mathfrak{a} = 0 + \mathfrak{b}$, assim $x \in \mathfrak{a}$ e $x \in \mathfrak{b}$. Daí, $x \in \mathfrak{a} \cap \mathfrak{b} = \mathfrak{ab}$. Logo, $\ker\sigma = \mathfrak{ab}$. Para provarmos que σ é sobrejetiva mostraremos que para todo par $(y + \mathfrak{a}, z + \mathfrak{b}) \in A/\mathfrak{a} \times A/\mathfrak{b}$ existe $x \in A$ tal que $(x + \mathfrak{a}, x + \mathfrak{b}) = (y + \mathfrak{a}, z \times \mathfrak{b})$, ou seja, para cada par $(y,z) \in A$ existe um elemento $x \in A$ tal que $x + \mathfrak{a} = y + \mathfrak{a}$ e $x + \mathfrak{b} = z + \mathfrak{b}$. Considere $x_1 \in \mathfrak{a}$ e $x_2 \in \mathfrak{b}$ tal que $x_1 + x_2 = 1_A$ e tome $x = x_1z + x_2y$. Assim, $x + \mathfrak{a} = (x_1z + x_2y) + \mathfrak{a} = x_2y + \mathfrak{a} = (1_A - x_1)y + \mathfrak{a}$, pois $x_1z \in \mathfrak{a}$ e $x_1 + x_2 = 1_A \Rightarrow x_2 = 1_A - x_1$. Logo, $x + \mathfrak{a} = (y - x_1y) + \mathfrak{a} = y + \mathfrak{a}$, de outra forma, dizemos que $x \equiv y \mod \mathfrak{a}$. Temos também que $x + \mathfrak{b} = (x_1z + x_2y) + \mathfrak{b} = x_1z + \mathfrak{b} = (1_A - x_2)z + \mathfrak{b} = z - x_2z + \mathfrak{b} = z + \mathfrak{b}$, de outra forma, dizemos que $x \equiv z \mod \mathfrak{b}$. Portanto, φ é sobrejetiva. Logo, pelo teorema dos isomorfismos de anéis temos que $A/\ker\sigma \cong A/\mathfrak{a} \times A/\mathfrak{b}$, ou seja, $A/\mathfrak{ab} \cong A/\mathfrak{a} \times A/\mathfrak{b}$. Portanto, σ induz o isomorfismo $\theta : A/\mathfrak{ab} \to A/\mathfrak{a} \times A/\mathfrak{b}$.

Lema 1.3 *Sejam A um anel e $\{\mathfrak{a}_i\}_{1\leq i\leq r}$, um conjunto finito de ideais de A tal que $\mathfrak{a}_i + \mathfrak{a}_j = A$, $\forall\, i \neq j$. Então existe um isomorfismo canônico de $A/\mathfrak{a}_1 \cdots \mathfrak{a}_r$ sobre $\prod_{i=1}^{r} A/\mathfrak{a}_i$.*

Prova: Para o caso $r = 2$, fica provado pelo Lema 1.2. Vamos usar indução sobre r. Ponha $\mathfrak{b} = \mathfrak{a}_2 \cdots \mathfrak{a}_r$. Mostraremos que $\mathfrak{a}_1 + \mathfrak{b} = A$, para $i \geq 2$ temos $\mathfrak{a}_1 + \mathfrak{a}_i = A$, pois por hipótese $\mathfrak{a}_i + \mathfrak{a}_j = A$, $\forall\, i \neq j$. Daí, existem elementos $x_i \in \mathfrak{a}_1$ e $y_i \in \mathfrak{a}_i$ tal que $x_i + y_i = 1_A$ e $1_A = \prod_{i-2}^{r}(x_i + y_i) = c + y_2 \cdots y_r$, onde c é a soma dos termos, cada um dos quais contém um menor x_i como fator. Temos que $c \in \mathfrak{a}_1$ e como $y_2 \cdots y_r \in \mathfrak{b}$ então $c + y_2 \cdots y_r \in \mathfrak{a}_1 + \mathfrak{b}$. Assim, $1_A \in \mathfrak{a}_1 + \mathfrak{b}$ e daí $\mathfrak{a}_1 + \mathfrak{b} = A$. Pelo Lema 1.2, segue-se que $A/\mathfrak{a}_1\mathfrak{b}$ é isomorfo a $A/\mathfrak{a}_1 \times A/\mathfrak{b}$. Pela hipótese

de indução, temos que $A/\mathfrak{b} = A/\mathfrak{a}_2 \cdots \mathfrak{a}_r$ é isomorfo a $A/\mathfrak{a}_2 \times \cdots \times A/\mathfrak{a}_r$. Logo, $A/\mathfrak{a}_1 \cdots \mathfrak{a}_r$ é isormorfo a $A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_r$.

Proposição 1.2 *Sejam n e n' inteiros relativamente primos. Então o anel $\mathbb{Z}/nn'\mathbb{Z}$ é isomorfo ao anel produto $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$.*

Prova: Como n e n' são inteiros relativamente primos, então existem inteiros x e y tais que $nx + n'y = 1$. Daí, como $nx + n'y \in n\mathbb{Z} + n'\mathbb{Z}$ temos que $1 \in n\mathbb{Z} + n'\mathbb{Z}$. Logo, $n\mathbb{Z} + n'\mathbb{Z} = \mathbb{Z}$ e portanto o resultado segue-se do Lema 1.2.

1.2 Módulos sobre anéis de ideais principais, raízes da unidade e corpos finitos

Definição 1.6 *Um A-módulo M é um grupo (a operação é adição) provido da aplicação $A \times M \to M$ tal que*

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

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

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

$$1x = x$$

com $a, b \in A$ e $x, y \in M$.

Definição 1.7 *Sejam A um anel comutativo e I um conjunto. Denotamos $A^{(I)}$ o conjunto das sequências $(a_i)_{i \in I}$ indexadas por I, de elementos de A tais que $a_i = 0$, exceto para um número finito de índices $i \in I$.*

Definição 1.8 *Um A-módulo M e dito ser um A-módulo livre quando existe uma família $(a_i)_{i \in I}$ de elementos de M, satisfazendo as seguintes condicões:*
a) A família $(a_i)_{i \in I}$ é linearmente independente;
b) Todo elemento $a \in M$ é escrito como combinacão linear da família $(a_i)_{i \in I}$.

Observação 1.5 *Uma família $(a_i)_{i \in I}$ satisfazendo as condicões da Definicão 1.8 é chamada uma base do A-módulo livre, onde o número de elementos da base é chamado o posto de M. Se I é um conjunto finito, dizemos que o A-módulo M é finitamente gerado ou do tipo finito.*

Definição 1.9 *Um A-módulo M é dito do tipo finito se contém um conjunto finito de geradores.*

Teorema 1.2 *Sejam A um anel e M um A-módulo. As seguintes condições são equivalentes:*
(a) Toda família não vazia de submódulos de M contém um elemento maximal (com a relação de inclusão);
(b) Toda sequência crescente $(M_n)_{n\geq 0}$ (ainda para a relação de inclusão) de submódulos de M é estacionária, isto é, existe n_0 tal que $M_n = M_{n_0}$, $\forall\, n \geq n_0$;
(c) Todo submódulo de M é do tipo finito.

Prova: Primeiro vamos mostrar que $(a) \Rightarrow (c)$ Seja E um submódulo de M e Φ a coleção consistindo de todos submódulos do tipo finito de E. Temos que Φ não é vazia, pois $0 \in \Phi$. Por (a), segue-se que Φ contém um elemento maximal F. Para $x \in E$, $F + Ax$ é um submódulo do tipo finito de E, pois Ax é um módulo gerado por x e F é um submódulo do tipo finito de E. Temos que $F + Ax$ é gerado pela união de x e qualquer conjunto finito de geradores de F. Como $F \subset F + Ax$ e F é maximal, então $F + Ax = F$. Portanto, $x \in F$, $E \subset F$ e assim $E = F$. Logo, E é do tipo finito.

Agora vamos mostrar que $(c) \Rightarrow (b)$ Seja $(M_n)_{n\geq 0}$ uma sequência crescente de submódulos de M. Então $E = \bigcup_{n\geq 0} M_n$ é um submódulo de M. Por (c) este submódulo E contém um conjunto finito de geradores $\{x_1, \ldots, x_q\}$. Temos que, para todo i, existe um índice $n(i)$. Então $x_i \in M_{n_0}$, onde $n_0 \geq \max\{n(i)\}\ \forall\, i$, pois $(M_n)_{n\geq n_0}$ é crescente. Daí, $E \subset M_{n_0}$ assim temos $E = M_{n_0}$, pois $M_{n_0} \subset E$. Para $n \geq n_0$, as relações de inclusão $M_{n_0} \subset M_n \subset E$ e a igualdade $E = M_{n_0}$ implica que $M_n = M_{n_0}$. Logo, a sequência $(M_n)_{n\geq 0}$ é estacionária a partir de n_0.

A equivalência de (a) em (b) é um caso particular do Lema 1.4 sobre conjunto parcialmente ordenados.

Lema 1.4 *Seja T um conjunto parcialmente ordenado. As seguintes afirmações são equivalentes:*
(a) Todo subconjunto não vazio de T contém um elemento maximal;
(b) Toda sequência crescente $(t_n)_{n\geq 0}$ de elementos de T é estacionária.

Prova: $(a) \Rightarrow (b)$ Por (a) temos que a sequência $(t_n)_{n\geq 0}$ contém um elemento maximal. Seja t_q o elemento maximal da sequência crescente $(t_n)_{n\geq 0}$. Como a sequência $(t_n)_{n\geq 0}$ é crescente, para $n \geq q$ temos $t_n \geq t_q$. Sendo t_q maximal, segue-se que $t_n = t_q$, $\forall\, n \geq q$. Logo, toda sequência $(t_n)_{n\geq 0}$ de elementos de T é estacionária.

$(b) \Rightarrow (a)$ Suponha que exista um subconjunto S de T que não contém um elemento maximal. Então, para todo $x \in S$, o conjunto dos elementos de S que são maiores do que x é não

vazio. Daí, pelo axioma da escolha, existe uma aplicação $f : S \to S$ tal que $f(x) > x \; \forall \; x \in S$. Como S é não vazio, podemos escolher $t_0 \in S$ e definir por indução a sequência $(t_n)_{n\geq 0}$ da forma $t_{n+1} = f(t_n)$. Esta sequência é estritamente crescente e não estacionária, o que é uma contradição. Logo, todo subconjunto não vazio de T contém um elemento maximal.

Corolário 1.1 *Em um anel de ideal principal A toda família não vazia de ideais contém um elemento maximal.*

Prova: Se considerarmos A como um módulo sobre si mesmo, seus submódulos são ideais, como todos os ideais são principais, eles são A-submódulos gerados por um único elemento, assim do tipo finito. Logo, o resultado segue-se pela implicação de (c) em (a) do Teorema 1.2.

Sejam A um domínio de integridade e $\mathbb{K}$ seu corpo de frações. Um A-módulo livre pode ser mergulhado em um espaço vetorial sobre $\mathbb{K}$. Segue-se que o mesmo é verdade para qualquer submódulo M de um A-módulo livre.

Definição 1.10 *A dimensão do subspaço gerado por M é chamado posto de M. Se M é livre e admite uma base possuindo n elementos, então o posto de M é n.*

Teorema 1.3 *Seja A anel de ideais principais, M um A-módulo livre de posto n, e M' um submódulo de M. Então:*
(a) M' é livre de posto q, com $0 \leq q \leq n$;
(b) Se $M' \neq (0)$, então existem uma base $\{e_1, \ldots, e_n\}$ de M e elementos não nulos $a_1, \ldots, a_q \in A$, onde $\{a_1e_1, \ldots, a_qe_q\}$ é uma base de M' tal que $a_i | a_{i+1}$, $1 \leq i \leq q-1$.

Prova: Seja $L(M,A)$ o conjunto das formas lineares em M. Para $u \in L(M,A)$, $u(M')$ é um submódulo de A, um ideal de A. Podemos escrever $u(M') = A_{a_u}$ com $a_u \in A$, pois os ideais de A são principais. Seja $u \in L(M,A)$ tal que A_{a_u} é maximal entre A_{a_v}, onde $v \in L(M,A)$, isto pelo Corolário 1.1. Agora tomemos uma base $\{x_1, \ldots, x_n\}$ de M, o qual identifica M com A^n. Seja $p_{r_i} : M \to A$ a projeção da i-ésima cordenada, isto é, $p_{r_i}(x_j) = \delta_{ij}$. Daí, se $M' \neq (0)$, para pelo menos um i, com $1 \leq i \leq n$, temos $p_{r_i}(M') \neq (0)$. Daí, $a_u \neq 0$ e por construção, existe $e' \in M'$ tal que $u(e') = a_u$. Vamos mostrar que, para todo $v \in L(M,A)$, $a_u | v(e')$. De fato, se $d = mdc(a_u, v(e'))$ então $d = a_u b + v(e')c$ com $b, c \in A$. Daí, $d = (ub + cv)(e')$. Como $bu + cv$ é uma forma linear em M temos que $A_{a_u} \subset A_d \subset u(M')$. Daí, a maximalidade de A_{a_u} implica que $A_d = A_{a_u}$. Logo, $a_u | v(e')$, pois $a_u | d$ e $d | v(e')$. Em particular, $a_u | p_{r_i}(e')$, daí $p_{r_i}(e') = a_u b_i$ com

$b_i \in A$. Ponha $e = \sum_{i=1}^{n} b_i x_i$, então $e' = a_u e$. Logo, como $u(e') = a_u = a_u u(e)$ temos que $u(e) = 1$ (note que $a_u \neq 0$). Mostraremos que:

$$M = \ker(u) + Ae \tag{1.5}$$

De fato, como já temos que $\ker(u) + Ae \subset M$, resta mostrar que $M \subset \ker(u) + Ae$. Dado $x \in M$, $x = u(x)e + [x - u(x)e]$. Vemos que:

$$u[x - u(x)e] = u(x) - u(x)u(e) = u(x) - u(x)1 = 0,$$

pois $u(e) = 1$. Daí, $x - u(x)e \in \ker(u)$. Assim, $x = u(x)e + x - u(x)e \in \ker(u + Ae)$, pois $u(x)e \in Ae$ e $x - u(x)e \in \ker(u)$. Logo, $M = \ker(u) + Ae$

Agora mostraremos que:

$$M' = M' \cap \ker(u) + Ae' \tag{1.6}$$

onde $e' = a_u e$ (as somas sendo direta).

De fato, como $[M' \cap \ker(u) + Ae'] \subset M'$, basta mostrar que $M' \subset [M' \cap \ker(u) + Ae']$. Dado $y \in M'$, $u(y) = ba_u$ com $b \in A$, temos que:

$$y = ba_u e + y - ba_u e = be' + y - u(y)e,$$

novamente temos que $y - u(y)e = y - ba_u e = y - be' \in M'$. Daí, $y - u(y)e \in \ker(u) \cap M'$ e como $be' \in Ae'$ temos que $y = be' + y - u(y)e \in [Ae' + \ker(u) \cap M']$. Logo, $M' = M' \cap \ker(u) + Ae'$.

Agora vamos mostrar (a) por indução no posto q de M'. Se $q = 0$ então $M' = (0)$ e não há o que provar. Se $q > 0$ então $M' \cap \ker(u)$ tem posto $q - 1$, pela equação 1.6, e portanto é livre pela hipótese de indução. Como na equação 1.6 a soma é direta, obtemos uma base para M' adicionando e' a uma base para $M' \cap \ker(u)$. Logo, M' é livre.

Para provar (b) usaremos indução no posto n de M. No caso $n = 0$, não temos o que mostrar. Agora se $n > 0$, pelo item (a) o $\ker(u)$ é livre de posto $n - 1$, pois na equação 1.5 a soma é direta. Aplicamos a hipótese de indução no módulo livre $\ker(u)$ e no seu submódulo $M' \cap \ker(u)$. Se $M' \cap \ker(u) \neq (0)$ existem $q \leq n$, uma base $\{e_1, \ldots, e_n\}$ do $\ker(u)$, uma base $\{e_1, \ldots, e_n\}$ do $\ker(u)$ e elementos não nulos $a_2, \ldots, a_q$ de A tais que $\{a_2 e_2, \ldots, a_q e_q\}$ é uma base para $M' \cap \ker(u)$ e tais que $a_i | a_{i+1}$, onde $2 \leq i \leq q - 1$. Fixemos $a_1 = a_u$ e $e_1 = e$. Daí, $\{e_1, \ldots, e_n\}$ é uma base para M pela equação 1.5 e $\{a_1 e_1, \ldots, a_q e_q\}$ é uma base para M' pela equação 1.6 e pelo fato de $e' = a_1 e_1$.

Resta provar que $a_1 | a_2$. De fato, seja $v \in L(M, A)$ definida pela relação $v(e_1) = v(e_2) = 1$

e $v(e_i) = 0$, para $i \geq 3$. Assim, $a_1 = a_u = v(a_u e_1) = v(e') \in v(M')$, daí $Aa_u \subset v(M')$ pela maximalidade de Aa_u. Concluímos que $v(M') = Aa_u = Aa_1$, como $a_2 = a_2 v(e_2) = v(a_2 e_2) \in v(M') = Aa_1$ temos que $a_2 \in Aa_1$, isto é, $a_1 | a_2$.

Observação 1.6 *Os ideais Aa_i no Teorema 1.3 são chamados fatores invariantes de M' e M.*

Corolário 1.2 *Sejam A um anel de ideais principais e E um A-módulo do tipo finito. Então, E é isomorfo ao produto $(A/\mathfrak{a}_1) \times \cdots \times (A/\mathfrak{a}_n)$ onde os $\mathfrak{a}_i$'s são ideais de A tais que $\mathfrak{a}_1 \supset \cdots \supset \mathfrak{a}_n$.*

Prova: Sendo E um A-módulo do tipo finito, considere $\{x_1, \ldots, x_n\}$ um conjunto finito de geradores de E. Sabemos que existe homomorfismo sobrejetivo, $\sigma : A^n \to E$ e que pelo teorema dos homomorfismo sobrejetivos, $A^n/\ker\sigma$ é isomorfo a E. Temos, pelo Teorema 1.2, que existem uma base $\{e_1, \ldots, e_n\} \in A^n$, um inteiro $q < n$ e elementos não nulos $\mathfrak{a}_1, \ldots, \mathfrak{a}_q \in A$ tais que $\mathfrak{a}_1 | \mathfrak{a}_{i+1}$, $\forall\, i$, onde $1 \leq i \leq q-1$. Ponhamos $\mathfrak{a}_p = 0$ para $q+1 \leq p \leq n$. Então, $A^n/\ker\sigma$ é isomorfo ao produto dos $A_{e_i}/A_{\mathfrak{a}_i e_i}$, para $1 \leq i \leq n$. Temos ainda que $A_{e_i}/A_{\mathfrak{a}_i e_i}$ é isomorfo a $A/A_{\mathfrak{a}_i}$. Daí, $A^n/\ker\sigma$ é isomorfo ao produto dos $A/A_{\mathfrak{a}_i}$. Pondo $\mathfrak{a}_i = A_{\mathfrak{a}_i}$, temos que $A^n/\ker\sigma$ é isomorfo ao produto dos $A/\mathfrak{a}_i$. Logo, como $A^n/\ker\sigma$ é isomorfo a E podemos concluir que E é isomorfo a $(A/\mathfrak{a}_1) \times \cdots \times (A/\mathfrak{a}_n)$.

Definição 1.11 *Dizemos que um módulo E sobre um domínio de integridade A é livre de torção se a relação $ax = 0$, com $a \in A$ e $x \in E$, implica $a = 0$ ou $x = 0$.*

Corolário 1.3 *Sobre um anel de ideais principais A, todo módulo do tipo finito E, que é livre de torção, é livre.*

Prova: Temos que, pelo Corolário 1.2, E é isomorfo a $A/\mathfrak{a}_1 \times \cdots \times A/\mathfrak{a}_n$. Suprimindo os fatores que são zero, podemos supor que $\mathfrak{a}_i \neq A$, $\forall\, i$. Suponha que $\mathfrak{a}_1 \neq (0)$ e sejam $a \in \mathfrak{a}_1$, diferente de zero, e $x_1 \in A/\mathfrak{a}_1$, também diferente de zero. Se $x = (x_1, 0, \ldots, 0) \in E$, então a relação $ax = 0$ não implica $a = 0$ ou $x = 0$, pois x e a são não nulos. Daí, isto contraria a hipótese de E ser livre de torção. Logo, $\mathfrak{a}_1 = (0)$ e portanto $\mathfrak{a}_i = (0)$, $\forall\, i$, pois $\mathfrak{a}_i \subset \mathfrak{a}_1$. Daí, E é isomorfo a A^n e como A^n é livre, temos que E é livre.

Corolário 1.4 *Sobre um anel de ideais principais A, todo módulo E do tipo finito é isomorfo a um produto finito de módulos M_i's, onde cada M_i é igual a A ou a um quociente A/A_{p^s}, com p primo.*

Prova: Decompondo cada fator A/Aa, com $a \neq 0$, temos pelo Lema 1.3, que se $a = up_1^{s_1} \cdots p_n^{s_n}$ é uma fatoração de primos, A/Aa é isomorfo ao produto dos $A/A_{p_i^{s_i}}$'s. Daí, E é isomorfo a A/A_{p^s}, com p primo, pois E é isomorfo a A/Aa pelo Corolário 1.2 e ainda, se $a = 0$ então E isomorfo a A^n, já que pelo Corolário 1.2, temos que E é isomorfo a $A/a_1 \times \cdots \times A/a_n$. Logo, E é isomorfo a um produto finito de módulos $M_i's$, onde cada M_i é igual a A ou a um quociente A/A_{p^s}, com p primo.

Corolário 1.5 *Seja G um grupo comutativo finito, então existe $x \in G$, cuja ordem é o mínimo múltiplo comum das ordens dos elementos de G.*

Prova: Um grupo comutativo é um $\mathbb{Z}$-módulo (a operação sendo adição). Temos, pelo Corolário 1.2, que G é isomorfo a $\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z}$, onde $a_1|a_2 \cdots a_{n-1}|a_n$. Assim, temos $a_i \neq 0$, $\forall\, i$, pois caso contrário G seria infinito. Escrevemos y para classe de resíduos de 1 em $\mathbb{Z}/a_n\mathbb{Z}$ e ponhamos $x = (0, \ldots, 0, y)$. Daí, a ordem de x é obviamente a_n. Assim, dado $z = (z_1, \ldots, z_n) \in G$, temos que $za_n = 0$, pois $a_i|a_n$, $\forall\, i$. Logo, a_n é um múltiplo da ordem de z e portanto x é o elemento procurado.

Teorema 1.4 *Seja $\mathbb{K}$ um corpo. Todo subgrupo finito G do grupo multiplicativo $\mathbb{K}^*$ consiste de raízes da unidade e é cíclico.*

Prova: Temos, pelo Corolário 1.5, que existe um elemento $z \in G$, cuja ordem n é o mínimo múltiplo comum das ordens dos elementos de G. Logo, $y^n = 1$, $\forall\, y \in G$. Como um polinômio de grau n sobre um corpo tem no máximo n raízes no corpo, temos que G possui no máximo n elementos (estamos olhando o polinômio como $y^n - 1$). Por outro lado, tendo z ordem n, temos que G contém os n elementos: $z, z^2, \ldots, z^n = 1$, os quais são todos distintos. Logo, G é constituído das raízes n-ésimas da unidade e é cíclico gerado por z.

Observação 1.7 *Seja $\mathbb{K}$ um corpo. Existe um único homomorfismo de anéis $\sigma : \mathbb{Z} \to \mathbb{K}$, definida por $\sigma(n) = \underbrace{1+1+\cdots+1}_{n \text{ vezes}}$, para $n \geq 0$ e $\sigma(-n) = -\sigma(n)$ se $n < 0$. Se σ é injetiva, ela identifica $\mathbb{Z}$ com um subanel de $\mathbb{K}$, então $\mathbb{K}$ também contém o corpo de frações $\mathbb{Q}$ de $\mathbb{Z}$. Neste caso, dizemos que $\mathbb{K}$ é de caracteristica zero. Se σ não é injetiva, o $\ker\sigma$ é um ideal de $\mathbb{Z}$, então $\ker\sigma = p\mathbb{Z}$, $p > 0$, pois todo ideal de $\mathbb{Z}$ é principal. Assim, $\mathbb{Z}/p\mathbb{Z}$ é identificado com um subanel de $\mathbb{K}$. Daí, $\mathbb{Z}/p\mathbb{Z}$ é um corpo e então $p\mathbb{Z}$ é um ideal primo. Logo, p é um número primo. Dizemos neste caso, que $\mathbb{K}$ é de característica p. Agora escrevemos F_p para designar $\mathbb{Z}/p\mathbb{Z}$. O subcorpo $\mathbb{Q}$ ou F_p, de $\mathbb{K}$ é o menor subcorpo de $\mathbb{K}$ e é chamado o subcorpo primo de $\mathbb{K}$. Temos que, para todo número primo p, existem corpos de caracteristica p, ou seja, F_p.*

Proposição 1.3 *Se $\mathbb{K}$ é um corpo de característica $p \neq 0$, então $px = 0$, $\forall\, x \in \mathbb{K}$ e $(x+y)^p = x^p + y^p$, $\forall\, x, y \in \mathbb{K}$.*

Prova: Como a característica de $\mathbb{K}$ é $p \neq 0$, então para todo $x \in \mathbb{K}$ temos $px = (p1)x = 0x = 0$. Por outro lado, pela fórmula binominal, temos que:

$$(x+y)^p = \sum_{j=0}^{p} \binom{p}{j} x^j y^{p-j} = \binom{p}{0} x^0 y^p + \sum_{j=1}^{p-j} \binom{p}{j} x^j y^{p-j} + \binom{p}{p} x^p y^0,$$

isto é,

$$(x+y)^p = x^p + y^p + \sum_{j=1}^{p-1} \binom{p}{j} x^j y^{p-1}$$

O coeficiente binominal $\binom{p}{j}$ é um inteiro e seu valor é $\dfrac{p!}{j!(p-j)!}$. Como o número primo p aparece no numerador, mas não no denominador, então $\binom{p}{j}$ é um múltiplo de p, $\forall\, 1 \leq j \leq p-1$. Logo, $\binom{p}{j} x^j y^{p-j} = 0$, $\forall\, 1 \leq j \leq p-1$. Daí, $\sum_{j=1}^{p-1} \binom{p}{j} x^j y^{p-j} = 0$. Portanto, $(x+y)^p = x^p + y^p$.

Teorema 1.5 *Seja $\mathbb{K}$ um corpo finito. Se $q = card(\mathbb{K})$, então:*
(a) A característica de $\mathbb{K}$ é um primo p, $\mathbb{K}$ é um espaço vetorial de dimensão finita s sobre F_p e $q = p^s$;
(b) O grupo multiplicativo $\mathbb{K}^*$ é cíclico de ordem $q-1$;
(c) $x^{q-1} = 1$, $\forall\, x \in \mathbb{K}^*$ e $x^q = x$, $\forall\, x \in \mathbb{K}$.

Prova: (a) Como $\mathbb{Z}$ é infinito e $\mathbb{K}$ é finito, então $\varphi : \mathbb{Z} \to \mathbb{K}$ não é injetiva. Daí, $\mathbb{K}$ não pode ter característica zero. Logo, $\mathbb{K}$ contém F_p, com p primo e sua característica é p. Temos que, $\mathbb{K}$ é um espaço vetorial sobre F_p, cuja dimensão s deve ser finita, pois caso contrário, $\mathbb{K}$ seria um corpo infinito. Seja $\{e_1, \ldots, e_s\}$ uma base de $\mathbb{K}$ sobre F_p. Assim, qualquer $x \in \mathbb{K}$ pode ser escrito de maneira única como $x = x_1 e_1 + \cdots + x_s e_s$, onde $x_i \in F_p$, com $i = 1, \ldots, s$. Cada x_i na expressão pode ser escolhido de p maneiras, pois o número de elementos de F_p é igual a p. Logo, o número de elementos de $\mathbb{K}$ é p^s e daí teremos $q = p^s$ como queríamos.

(b) O resultado segue-se diretamente do Teorema 1.4, pois os elementos nulo de $\mathbb{K}$ não podem pertencer a $\mathbb{K}^*$.

(c) Como a ordem de $\mathbb{K}^*$ é $q-1$ pelo item (b), então temos $x^{q-1} = x$, $\forall\, x \in \mathbb{K}^*$ e $x^q = x$, $\forall\, x \in \mathbb{K}$.

Observação 1.8 *(a) e (c) implicam que um corpo finito $\mathbb{K}$ com q elementos é o conjunto de raízes do polinômio $P(x) = x^q - x$, que possui exatamente q raízes. Escrevemos F_q para um corpo com q elementos, pois dois corpos finitos com q elementos são isomorfos.*

Teorema 1.6 (Chevalley) *Sejam $\mathbb{K}$ um corpo finito e $F(X_1,\ldots,X_n)$ um polinômio homogêneo de grau d sobre $\mathbb{K}$ ("lembrando que, um polinômio é dito homogêneo de grau d, quando todos seus monômios tem grau d"). Suponha $d < n$, então existe um ponto $(x_1,\ldots,x_n) \in \mathbb{K}^n$ diferente da origem tal que $F(x_1,\ldots,x_n) = 0$.*

Prova: Considere $q = \text{card}(\mathbb{K})$ e p a característica de $\mathbb{K}$, então $q = p^s$, pelo Teorema 1.5. Seja $V \subset \mathbb{K}^n$ o conjunto dos zeros de F, isto é, o conjunto dos pontos $(x_1,\ldots,x_n) \in \mathbb{K}^n$. Temos, pelo Teorema 1.5, que $F(x)^{q-1} = 1$, $\forall\, x \in \mathbb{K}^n - V$. Assim, o polinômio $G(x) = F(x)^{q-1} = 1$, $\forall\, x \in \mathbb{K}^n - V$, com valores em F_p. O número módulo p de pontos de $\mathbb{K}^n - V$ será então dado pela soma $\sum_{x\in\mathbb{K}^n} G(x)$.

Vamos agora calcular esta soma e mostrar que ela vale zero módulo p, isto é, $\sum_{x\in\mathbb{K}^n} G(x) \equiv 0 \mod p$. Se isso ocorrer, então teremos que a $\text{card}(\mathbb{K}^n - V)$ é um múltiplo de p. Como $\text{card}(\mathbb{K}^n) = q^n = (p^s)^n = p^{ns}$ é também um múltiplo de p, então a $\text{card}(V)$ é também um múltiplo de p. Temos que V já contém a origem, então se para $\text{card}(V)$, necessariamente V contém outros pontos, pois $p \geq 2$. Para provar esse teorema é suficiente mostrar que $\sum_{x\in\mathbb{K}^n} G(x) = 0 \in F_p$. Para calcular $\sum_{x\in\mathbb{K}^n} G(x)$, observe que o polinômio G é uma combinação linear dos monômios $M_\alpha(x) = x_1^{\alpha_1}\cdots x_n^{\alpha_n}$. Para determinar $\sum_{x\in\mathbb{K}^n} G(x)$ é suficiente calcular

$$\sum_{x\in\mathbb{K}^n} M_\alpha(x) = \sum_{x\in\mathbb{K}^n} x_1^{\alpha_1}\cdots x_n^{\alpha_n} = \left(\sum_{x_1\in\mathbb{K}^n} x_1^{\alpha_1}\right)\cdots\left(\sum_{x_n\in\mathbb{K}^n} x_n^{\alpha_n}\right)$$

Daí, o problema reduz-se ao cálculo de somas da forma $\sum_{y\in\mathbb{K}} y^\beta$, com $\beta \in \mathbb{N}$.

I) Para $\beta = 0$ temos $y^\beta = 1$, $\forall\, y \in \mathbb{K}$, consequentemente, $\sum_{y\in\mathbb{K}} y^\beta = \sum_{y\in\mathbb{K}} 1 = q \equiv 0 \mod p$.

II) Para $\beta > 0$, o termo 0^β é o zero, assim a soma reduz a $\sum_{y\in\mathbb{K}^*} y^\beta$. Como $\mathbb{K}^*$ é um grupo cíclico de ordem $q-1$, pelo item (b) do Teorema 1.5. Seja w gerador de $\mathbb{K}^*$. Daí, $\sum_{y\in\mathbb{K}^*} y^\beta = \sum_{j=0}^{q-2} w^{\beta j}$, que é a soma de uma progressão geométrica.

Assim, consideremos dois casos:

III) Se $w^\beta \neq 1$, isto é, se β não é múltiplo de $q-1$, então $\sum_{j=0}^{q-2} w^{\beta j} = \dfrac{w^{\beta(q-1)} - 1}{w^\beta - 1} = 0$, pois

$w^{q-1} = 1$.

IV) Se $w^{\beta} = 1$, isto é, se β é um múltiplo de $q-1$. Então,

$$\sum_{j=0}^{q-2} w^{\beta j} = \underbrace{1+1+\cdots+1}_{(q-1)\text{ vezes}} = q-1$$

Segue por I), III) e IV) que $\sum_{x\in\mathbb{K}^n} x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ desaparece, a menos que todos os α_i's são não nulos e múltiplos de $q-1$. Neste caso, o grau $\alpha_1+\cdots+\alpha_n$ do monômio é no mínimo $(q-1)n$. Mas, como $G = F^{q-1}$, G possui grau $(q-1)d$ e $(q-1)d < (q-1)n$, pois $d < n$, não podemos ter os α_i's não nulos e múltiplos de $q-1$. Portanto, $\sum_{x\in\mathbb{K}^n} M_\alpha(x) = 0$, para todo monômio $M_\alpha(x)$ que aparece em G com coeficientes não nulos. Logo, $\sum_{x\in\mathbb{K}^n} G(x) = 0$.

1.3 Elementos inteiros sobre anéis e algébricos sobre um corpo

Definição 1.12 *Os números complexos que satisfazem uma equação da forma* $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$*, onde os coeficientes* a_i*'s, com* $i = 0,\cdots,n-1$*, são racionais, são chamados números algébricos. Quando* $a_i \in \mathbb{Z}$*,* $i = 0,\cdots,n-1$*, o número algébrico x chama-se inteiro algébrico.*

1.3.1 Elementos inteiros sobre um anel

Teorema 1.7 *Sejam R um anel, A um subanel de R e x um elemento de R. As seguintes condições são equivalentes:*

(a) Existem $a_0,\ldots,a_{n-1} \in A$ *tal que* $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_o = 0$*, isto é, x é raiz de um polinômio mônico com coeficientes em A;*

(b) O anel $A[x]$ *é um A-módulo do tipo finito;*

(c) Existe um subanel B de R que contém A e x, o qual é um A-módulo do tipo finito.

Prova: Primeiro vamos mostrar que $(a) \Rightarrow (b)$. Temos por hipótese que existem $a_0,\ldots,a_{n-1} \in A$ tal que

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 + a_0 = 0 \tag{1.7}$$

Seja M um A-submódulo de R gerado por $1, x, \ldots, x^{n-1}$. Pela hipótese acima temos que $x^n \in M$. Daí, multiplicando a equação 1.7 por x^j, obtemos:

$$x^{n+j} = -a_{n-1}x^{n+j-1} - \cdots - a_1x^{j+1} - a_ox^j.$$

Fazendo indução sobre j, temos que $x^{n+j} \in M$, $\forall\ j \geq 0$. Como $A[x]$ é um A-módulo gerado por x^k, com $k \geq 0$, temos que $A[x] = M$. Sendo M um A-submódulo do tipo finito temos que $A[x]$ é um A-módulo do tipo finito.

$(b) \Rightarrow (c)$ Temos por hipótese que o anel $A[x]$ é um A-módulo do tipo finito. Daí, basta tomar $B = A[x]$. Logo, existe um subanel B de R que contém A e x, o qual é um A-módulo do tipo finito.

$(c) \Rightarrow (a)$ Temos por hipótese, que existe um subanel B de R que contém A e x, o qual é um A-módulo do tipo finito. Daí, B possui um conjunto finito de geradores. Seja $\{y_1, \ldots, y_n\}$ um conjunto finito de geradores para B como um módulo sobre A, isto é,

$$B = Ay_1 + \cdots + Ay_n$$

Assim, dado $x \in B$ e sendo B um subanel de R, segue-se que $xy_i \in B$, $\forall\ i = 1, \ldots, n$. Logo, $xy_i = \sum_{j=1}^{n} a_{ij} y_j$, para qualquer $i = 1, \ldots, n$ e $a_{ij} \in A$, com $i \leq 1$ e $j \leq n$. Isto significa que $\sum_{j=1}^{n} (\delta_{ij} x - a_{ij}) y_j = 0$, com $i = 1, \ldots, n$, onde $\delta_{ij} = 0$ se $i \neq j$ e $\delta_{ij} = 1$ se $i = j$. Considere o sistema de n equações lineares homogêneas em $\{y_1, \ldots, y_n\}$. Escreva d para o determinante, $\det(\delta_{ij} x - a_{ij})$. Fazendo o cálculo usando a regra de cramer, obtem-se $dy_i = 0, \forall i = 1, \ldots, n$. Daí, $db = 0$, $\forall\ b \neq 0$. Mas, d é um polinômio mônico em x, pois o termo de ordem superior aparece na expressão do produto $\prod_{i=1}^{n} (x - a_{ii})$, entre os termos da diagonal principal. Daí, sendo $d = 0$, obtemos o que queríamos.

Definição 1.13 *Sejam R um anel e A um subanel de R. Um elemento x de R é dito inteiro sobre A se este satisfaz as condições de equivalência:*
(a) Existem $a_0, \ldots, a_{n-1} \in A$ *tal que* $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_o = 0$*, isto é, x é raiz de um polinômio mônico com coeficientes em A;*
(b) O anel $A[x]$ *é um A-módulo do tipo finito;*
(c) Existe um subanel B de R que contém A e x, o qual é um A-módulo do tipo finito.

Observação 1.9 *Seja* $P \in A[x]$ *um polinômio mônico tal que* $P(x) = 0$*, esta relacão é chamada uma equação de dependência inteira de x sobre A.*

Exemplo 1.4 *O elemento* $x = \sqrt{2}$ *de R é inteiro sobre* $\mathbb{Z}$*. A relação* $x^2 - 2 = 0$ *é uma equação de dependência inteira.*

Proposição 1.4 *Sejam R um anel, A um subanel de R e $\{x_1,\ldots,x_n\}$ um conjunto finito de elementos de R. Se para todo i, x_i é inteiro sobre $A[x_1,\ldots,x_{i-1}]$, em particular se todos os x_i's são inteiros sobre A, então $A[x_1,\ldots,x_n]$ é um A-módulo do tipo finito.*

Prova: Agiremos por indução em n. Para $n=1$, temos pelo o item (b) do Teorema 1.7, que $A[x_1,\ldots,x_n]$ é um A-módulo do tipo finito. Assumiremos que $B=A[x_1,\ldots,x_{n-1}]$ é um A-módulo do tipo finito. Então, $B=\sum_{j=1}^{p} Ab_j$. Temos que, o caso $n=1$, implica que $A[x_1,\ldots,x_{n-1}]=B[x_n]$ é um B-módulo do tipo finito. Daí, escrevemos $B[x_n]=\sum_{k=1}^{q} Bc_k$. Então, $A[x_1,\ldots,x_n]=\sum_{k=1}^{q}\left(\sum_{j=1}^{p} Ab_j\right)c_k=\sum_{k,j}^{q,p} Ab_jc_k$. Assim, $\{b_1c_1,\ldots,b_pc_q\}$ é um conjunto finito de geradores para $A[x_1,\ldots,x_n]$, como um módulo sobre A. Logo, $A[x_1,\ldots,x_n]$ é um A-módulo do tipo finito.

Corolário 1.6 *Sejam R um anel, A um subanel de R, x e y elementos de R, os quais são inteiros sobre A, então $x+y$, $x-y$, xy são inteiros sobre A.*

Prova: Como $x+y$, $x-y$ e xy pertencem a $A[x,y]$, pela Proposição 1.3, $A[x,y]$ é um A-módulo do tipo finito. Daí, pelo item (c) do Teorema 1.7, temos que $x+y$, $x-y$ e xy são inteiros sobre A.

Corolário 1.7 *Sejam R um anel e A um subanel de R. O conjunto A' de elementos de R os quais são inteiros sobre A é um subanel de R que contém A.*

Prova: Pelo Corolário 1.2, A' é um subanel de R. Temos ainda que $A\subset A'$, pois se $a\in A$, a é raiz do polinômio mônico $P(x)=x-a$ que tem coeficientes em A. Então a é inteiro sobre A, isto é, $a\in A'$

Definição 1.14 *Sejam R um anel, A um subanel de R. O anel A' de elementos de R os quais são inteiros sobre A é chamado o fecho inteiro de A em R. Seja A um domínio de integridade e $\mathbb{K}$ seu corpo de frações. O fecho inteiro de A em $\mathbb{K}$ é chamado fecho inteiro de A. Seja B um anel e A um subanel de B. Dizemos que B é inteiro sobre A se todo elemento de B é inteiro sobre A, isto é, se o fecho inteiro de A em B é o próprio B.*

Proposição 1.5 (Transitividade) *Sejam C um anel, B um subanel de C e A um subanel de B. Se B é inteiro sobre A e se C é inteiro sobre B. Então, C é inteiro sobre A.*

Prova: Dado $x \in C$, como C é inteiro sobre B, temos que x é inteiro sobre B, daí existe uma equação de dependência inteira $x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$, com os $b_i \in B$, onde $i = 0, \ldots, n-1$. Ponha $B' = A[b_0, \ldots, b_{n-1}]$, então x é inteiro sobre B'. Como B é inteiro sobre A, os b_i's são inteiros sobre A. Daí, pela Proposição 1.4, temos que $B'[x] = A[b_0, \ldots, b_{n-1}, x]$ é um A-módulo do tipo finito. Assim, pelo o item (c) do Teorema 1.7, x é inteiro sobre A. Logo, C é inteiro sobre A.

Proposição 1.6 *Sejam B um domínio de integridade e A um subanel de B tal que B é inteiro sobre A. Para que B seja um corpo é necessário e suficiente que A seja um corpo.*

Prova: Suponha que A seja um corpo e seja $b \in B$, onde $b \neq 0$. Então $A[b]$ é um espaço vetorial de dimensão finita sobre A, isto pelo o item (b) do Teorema 1.7. Por outro lado a aplicação $y \mapsto by$ é uma A-transformação linear de $A[b]$. Esta transformação é injetiva, pois seu núcleo é zero, ja que $A[b]$ é um domínio de integridade e $b \neq 0$. Daí, segue-se do teorema do núcleo e da imagem que essa transformação é sobrejativa. Logo, existe $b' \in A[b]$ tal que $bb' = 1$, isto é, para qualquer $b \in B - (0)$, b é invertível em B. Portanto, B é um corpo.

Reciprocamente, suponha que B é um corpo. Dado $a \in A - (0)$ temos que a possui um inverso $a^{-1} \in B$, o qual satisfaz a equação de dependência inteira $a^{-n} + a_{n-1}a^{-n+1} + \cdots + a_1a^{-1} + a_0 = 0$, onde $a_i \in A$. Multiplicando por a^{n-1}, obtemos $a^{-1} = -(a_{n-1} + \cdots + a_1a^{n-2} + a_0a^{n-1})$, isto é, $a^{-1} \in A$. Logo, A é um corpo.

Definição 1.15 *Um anel A é dito integralmente fechado se for um domínio de integridade e se for seu próprio fecho inteiro. Em outras palavras, todo elemento x do corpo de frações $\mathbb{K}$ de A, que é inteiro sobre A, pertence a A.*

Exemplo 1.5 *Sejam A um domínio de integridade e $\mathbb{K}$ seu corpo de frações. Então o fecho inteiro A' de A, isto é, o fecho inteiro de A em $\mathbb{K}$, é integralmente fechado.*

Exemplo 1.6 *Todo anel de ideais principais é integralmente fechado. De fato, por definição um anel de ideais principais é um domínio de integridade. Seja x um elmento de um corpo de frações $\mathbb{K}$ de A, que é inteiro sobre A. Seja $x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$, com $a_i \in A$, uma equação de dependência inteira de x sobre A. Escreva $x = \frac{a}{b}$, com $a, b \in A$ e o mdc de a e b igual a 1. Substituíndo $\frac{b}{a}$ na equação de dependência inteira e multiplicando-a por b^n, obtemos $a^n + b(a_{n-1}a^{n-1} + \cdots + a_1b^{n-2} + a_0b^{n-1}) = 0$. Assim, $b|a^n$ com $mdc(a,b) = 1$. Logo, pelo o lema de Euclides temos que $b|a$. Portanto, b é uma unidade de A. Daí, $x = \frac{a}{b}$ é um elemento de A. Logo, A é integralmente fechado.*

1.3.2 Elementos algébricos sobre um corpo

Definição 1.16 *Sejam R um anel e $\mathbb{K}$ um subcorpo de R. Um elemento $x \in R$ é chamado algébrico sobre $\mathbb{K}$ se existem elementos $a_0, a_1, \ldots, a_n \in K$ nem todos nulos tal que*

$$a_n x^n + \cdots + a_1 x + a_0 = 0 \tag{1.8}$$

equivalentemente, os monômios $(x^j)_{j\in\mathbb{N}}$ são linearmente dependentes sobre $\mathbb{K}$. Um elemento de R que não é algébrico é chamado transedental sobre $\mathbb{K}$. Isto é, x é transedental sobre $\mathbb{K}$ se e somente se os monômios $(x^j)_{j\in\mathbb{N}}$, são linearmente independentes sobre $\mathbb{K}$.

Observação 1.10 *Na definição anterior, podemos assumir que $a_n \neq 0$. Neste caso, $a_n^{-1} \in \mathbb{K}$, multiplicando a equação 1.8 por a_n^{-1}, obtemos uma equação de dependência inteira. Portanto, sobre um corpo algébrico equivale também sobre um corpo inteiro. Se $\mathbb{K} \subset R$ e $x \in R$ temos que x é algébrico sobre $\mathbb{K}$ se e somente se $[\mathbb{K}[x] : \mathbb{K}]$ é finito.*

Definição 1.17 *Dizemos que um anel R, contendo um corpo $\mathbb{K}$, é algébrico sobre $\mathbb{K}$, se todo elemento de R é algébrico sobre $\mathbb{K}$. Se R é um corpo, então R é chamado uma extensão algébrica de $\mathbb{K}$.*

Definição 1.18 *Dado um corpo $\mathbb{L}$ e um subcorpo $\mathbb{K}$ de $\mathbb{L}$, chamamos a dimensão $[\mathbb{L} : \mathbb{K}]$, o grau de $\mathbb{L}$ sobre $\mathbb{K}$. Toda extensão de grau finito de $\mathbb{Q}$ é chamado um corpo numérico algébrico (ou simplesmente um corpo numérico).*

Observação 1.11 *Pelo item (c) do Teorema 1.7 temos que, se o grau de $\mathbb{L}$ sobre $\mathbb{K}$ é finito, então $\mathbb{L}$ é uma extensão algébrica de $\mathbb{K}$.*

Proposição 1.7 *Sejam $\mathbb{K}$ um corpo, $\mathbb{L}$ uma extensão algébrica de $\mathbb{K}$ e $\mathbb{M}$ uma extensão algébrica de $\mathbb{L}$. Então $\mathbb{M}$ é uma extensão algébrica de $\mathbb{K}$. Além disso,*

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}].$$

Prova: Pela Proposição 1.5, segue que $\mathbb{M}$ é uma extensão algébrica sobre $\mathbb{K}$. Resta mostrar que $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$. Seja $\{x_i\}_{i\in I}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$ e $\{y_j\}_{j\in J}$ uma base de $\mathbb{M}$ sobre $\mathbb{L}$. Vamos mostrar que $\{x_i y_j\}_{(i,j)\in I\times J}$ é uma base de $\mathbb{M}$ sobre $\mathbb{K}$. Daí, a relação $\sum a_{ij} x_i y_j = 0$, com $a_{ij} \in \mathbb{K}$, implica $\sum \left(\sum a_{ij} x_i\right) y_j = 0$. Como $\{y_j\}_{j\in J}$ é L.I, pois $\{y_j\}_{j\in J}$ é uma base $\forall\ j$. Consequentimente, $a_{ij} = 0$, $\forall\ (i,j) \in I \times J$, pois $\{x_i\}_{i\in I}$ é uma base para $\mathbb{M}$ sobre $\mathbb{K}$. Portanto, $[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}]$.

Proposição 1.8 *Sejam R um anel e $\mathbb{K}$ um subcorpo de R. Então:*
(a) O conjunto $\mathbb{K}'$ de elementos de R, algébricos sobre $\mathbb{K}$, é um subanel de R contendo $\mathbb{K}$;
(b) Se R é um domínio de integridade, então $\mathbb{K}'$ é um subcorpo de R.

Prova: (a) Como $\mathbb{K}$ é um subcorpo de R, então os elementos de R que são algébricos sobre $\mathbb{K}$ são elementos inteiros sobre $\mathbb{K}$. Logo, pelo Corolário 1.7, o conjunto formado pelos elementos de R, que são inteiros sobre $\mathbb{K}$, é um subanel de R que contém $\mathbb{K}$.
(b) Como R é um domínio de integridade e $\mathbb{K}' \subset R$ é um subanel de R, então $\mathbb{K}$ é um domínio de integridade. Além disso, $\mathbb{K}$ é um subanel de $\mathbb{K}'$ e $\mathbb{K}'$ é algébrico sobre $\mathbb{K}$. Assim, pela Proposição 1.6, temos que $\mathbb{K}'$ é um corpo se e somente se $\mathbb{K}$ é um corpo. Como $\mathbb{K}$ é um subcorpo de R, então $\mathbb{K}'$ é um subcorpo de R.

Proposição 1.9 *Sejam $\mathbb{K}$ um corpo e $P(X) \in \mathbb{K}[X]$ um polinômio não constante. Então existe uma extensão algébrica $\mathbb{K}'$ de $\mathbb{K}$ de grau finito tal que $P(X)$ fatora $\mathbb{K}'[X]$ em um produto de polinômios de grau* 1 *(polinômios lineares).*

Prova: Usaremos indução sobre o grau d de $P(X)$. Se $d = 1$, então o resultado segue, pois $P(X)$ é um polinômio de grau 1. Seja $F(X)$ um fator irredutível de $P(X)$. Temos que existe uma extensão $\mathbb{K}''$ de grau finito sobre $\mathbb{K}$ (isto é, $\mathbb{K}[x]$) contendo um elemento x tal que $X - x$ divide $F(X) \in \mathbb{K}''[X]$. Daí, $\varphi(F(X)) = \varphi(G(X))\varphi(Q(X))$ implica que:

$$0 = (a_n x^n + \cdots + a_1 x + a_0)(b_m x^m + \cdots + b_1 x + b_0).$$

Como $\mathbb{K}[X]$ é D.I. então $a_n x^n + \cdots + a_1 x + a_0 = 0$ ou $b_m x^m + \cdots + b_1 x + b_0 = 0$. Suponha que $a_n x^n + \cdots + a_1 x + a_0 = 0$, então $G(X) \in \ker\varphi$. Logo, $F(X)$ divide $G(X)$ e daí o grau de G é maior e igual que o grau de F. Como o grau de G é menor e igual que o grau de F temos que o grau de F é igual ao grau de G e daí $F(X)$ é irredutível. Reciprocamente, suponha que $F(X)$ é irredutível, então $(F(X))$ é ideal primo. Daí, $\mathbb{K}[X]/(F(X))$ é D.I. Como $\mathbb{K}[X] \cong \mathbb{K}[X]/(F(X))$ então $\mathbb{K}[X]$ é D.I. daí, $X - x$ divide $F(X)$ em $\mathbb{K}''[X]$. Assim, $X - x$ também divide $P(X)$. Portanto, $P(X) = (X - x)P_1(X)$ com $P_1(X) \in \mathbb{K}''[X]$. Como $P_1(X)$ possui grau $d - 1$, então pela hipótese de indução $P_1(X)$ fatora em produto de polinômios lineares em uma extensão $\mathbb{K}'$ de grau finito $\mathbb{K}''$. Pela Proposição 1.4 $\mathbb{K}'$ é de grau finito sobre $\mathbb{K}$. Logo, $P(X) = (X - x)P_2(X)$ onde $P_2(X)$ é a fatoração de $P_1(X)$ em produto de polinômios lineares em uma extensão $\mathbb{K}'$ de $\mathbb{K}$.

Definição 1.19 (Corpos Algebricamente Fechados) *Um corpo $\mathbb{K}$ é chamado algebricamente fechado se todo polinômio não constante $P(X) \in \mathbb{K}[X]$ pode ser expresso como um produto de fatores lineares, todos em $\mathbb{K}[X]$.*

1.4 Elementos conjugados, corpos conjugados e inteiros em corpos quadráticos

Definição 1.20 *Dados dois corpos $\mathbb{L}$ e $\mathbb{L}'$ ambos contendo um corpo $\mathbb{K}$, chamamos todo isomorfismo $\varphi : \mathbb{L} \to \mathbb{L}'$ tal que $\varphi(a) = a$ para todo $a \in \mathbb{K}$ um $\mathbb{K}$-isomorfismo de $\mathbb{L}$ em $\mathbb{L}'$. Neste caso, dizemos que $\mathbb{L}$ e $\mathbb{L}'$ são $\mathbb{K}$-isomorfos, se eles são algébricos sobre $\mathbb{K}$ dizemos que eles são conjugados sobre $\mathbb{K}$.*

Definição 1.21 *Dados duas extensões $\mathbb{L}$ e $\mathbb{L}'$ de $\mathbb{K}$, dizemos que dois elementos $x \in \mathbb{L}$ e $x' \in \mathbb{L}'$ são conjugados sobre $\mathbb{K}$ se existe um $\mathbb{K}$-isomorfismo, $\varphi : \mathbb{K}(x) \to \mathbb{K}(x')$ tal que $\varphi(x) = x'$. Tal φ é única.*

Observação 1.12 *A existência de φ significa que x e x' são ambos transendentais sobre $\mathbb{K}$ ou são ambos algébricos sobre $\mathbb{K}$ com o mesmo polinômio minimal.*

Exemplo 1.7 *Sejam $F(X)$ um polinômio irredutível de grau n sobre $\mathbb{K}$ e $x_1, \ldots, x_n$ suas raízes na extensão $\mathbb{K}'$ de $\mathbb{K}$. Então os x_i's são dois a dois conjugados sobre $\mathbb{K}$.*

Lema 1.5 *Sejam $\mathbb{K}$ um corpo de característica zero ou um corpo finito e $F(X) \in \mathbb{K}[X]$ um polinômio mônico irredutível. Considere $F(X) = \prod_{i=1}^{n} (X - x_i)$ sua decomposição em produto de fatores lineares na extensão $\mathbb{K}'$ de $\mathbb{K}$. Então as n raízes $x_1, \ldots, x_n$ de $F(X)$ são distintas.*

Prova: Suponha por absurdo, que as n raízes de $F(X)$ não são todos distintas. Assim, $F(X)$ possui uma raiz múltipla. Daí, $F(X)$ possui uma raiz comum com seu, derivado $F'(X)$. Pois, se a é uma raiz de $F(X)$ de multiplicidade k então $F(X) = (X-a)^k G(X)$ e daí $F'(X) = k(X-a)^{k-1}G(X) + (X-a)^k G'(X)$. Logo, a é também raiz de $F'(X)$ de multiplicidade pelo menos $k-1$ se $k > 1$. Logo, $F(X)$ divide $F'(X)$. Como o grau de F' é menor e igual que o grau de F e F divide F' então $F'(X)$ é o polinômio zero. Daí, $F'(X) = nX^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + a_1 = 0$. Isto significa que $n.1 = 0$ e $j.a_j = 0$ para todo $j = 1, \ldots, n-1$. Mas, isso não pode ocorrer em um corpo $\mathbb{K}$ de característica zero. Se $\mathbb{K}$ tem característica $p \neq 0$, então a relação $n.1 = 0$ e $j.a_j = 0$ para $j = 1, \ldots, n-1$, significa que p divide n e que $a_j = 0$, $\forall\ j$ que não é múltiplo de p. Logo, $F(X)$ é da forma:

$$F(X) = X^{qp} + b_{q-1}X^{(q-1)p} + \cdots + b_1 X^p + b_0$$

com $b_i \in K$, pois, os termos a_j que não são zero, são os termos em que j é da forma: $qp - p, qp - 2p, \ldots, qp - qp$. Se cada um dos b_i's é uma p-ésima potência, isto é, $b_i = c_i^p$ com

$c_i \in \mathbb{K}$ então $F(X) = (X^q + C_{q-1}X^{q-1} + \cdots + C_0)^p$ isto pela Proposição 1.8. Logo, $F(X)$ não é irredutivel o que é absurdo. Podemos supor sempre que os b_i's são p-ésima potências, pois se $\mathbb{K}$ é um corpo finito com característica $p \neq 0$, então a aplicação $f : \mathbb{K} \to \mathbb{K}$, dada por $f(x) = x^p$, é injetiva, pois $x^p = y^p \Rightarrow x^p - y^p = 0 \Rightarrow (x-y)^p = 0 \Rightarrow x - y = 0 \Rightarrow x = y$. Como $\mathbb{K}$ é finito e f é injetiva, então f é sobrejetiva. Assim, para todo $y \in \mathbb{K}$ existe $x \in \mathbb{K}$ tal que $f(x) = y$, ou seja, $x^p = y$. Portanto, as n raízes $x_1, \ldots, x_n$ de $F(X)$ são distintas.

Observação 1.13 *Os corpos $\mathbb{K}$ de característica $p \neq 0$ para os quais $x \mapsto x^p$ é sobrejetiva (isto é, para os quais todo elemento de $\mathbb{K}$ é uma p-ésima potência) são chamados corpos perfeitos. Pelo que vimos anteriormente, os corpos finitos são perfeitos. Por convenção, corpos de característica zero são também considerados perfeitos. O Lema 1.5 é verdadeiro para todo corpo perfeito $\mathbb{K}$.*

Teorema 1.8 *Seja $\mathbb{K}$ um corpo de característica zero ou um corpo finito. Considere $\mathbb{K}'$ uma extensão de $\mathbb{K}$ de grau finito n e $\mathbb{B}$ um corpo algebricamente fechado contendo $\mathbb{K}$. Então existe n $\mathbb{K}$-isomorfismos distintos de $\mathbb{K}'$ em $\mathbb{B}$.*

Prova: Se o corpo extensão $\mathbb{K}'$ de $\mathbb{K}$ é da forma $\mathbb{K}' = \mathbb{K}[x]$, com $x \in \mathbb{K}'$ então o polinômio minimal $F(X)$ de x sobre $\mathbb{K}$ é da grau n. Ele possui n raízes $x_1, \ldots, x_n \in C$, todas distintas, pelo Lema 1.5. Pelo o Exemplo 1.7 os x_i's são dois a dois conjugados sobre $\mathbb{K}$ e daí para cada $i = 1, \ldots, n$ temos um $\mathbb{K}$-isomorfismo, $\sigma_i : \mathbb{K}[X] \to \mathbb{B}$ tal que $\sigma_i(x) = x_i$. Neste caso, o teorema fica provado. Continuaremos por indução sobre o grau n de $\mathbb{K}'$. Seja $x \in \mathbb{K}'$ e considere os corpos $\mathbb{K} \subset \mathbb{K}[x] \subset \mathbb{K}'$ e ponha $q = [\mathbb{K}[x] : \mathbb{K}]$. Podemos assumir $q > 1$, pois $\mathbb{K} \neq \mathbb{K}[x])$. Pelo que vimos anteriormente, existem q $\mathbb{K}$-isomorfismo distintos $\sigma_1, \ldots, \sigma_q$ de $K[x]$ em $\mathbb{B}$. Como $\mathbb{K}[x_i] = \mathbb{K}[\sigma_i(x)]$ e $\mathbb{K}[x]$ são isomorfos, pois x e x_i são conjugados e $\mathbb{K}[x] \subset \mathbb{K}'$, então é possível construir uma extensão $\mathbb{K}'_i$ de $\mathbb{K}[\sigma_i(x)]$ e um isomorfismo $\tau : \mathbb{K}' \to \mathbb{K}'_i$ que extende σ_i, (isto é válido pelo resultado encontrado em [Endler 2007]). Temos que $\mathbb{K}[\sigma_i(x)]$ é um corpo de característica zero ou um corpo finito, pois $\mathbb{K}[\sigma_i(x)]$ é uma extensão finita de k e $\mathbb{K}$ é de característica zero ou corpo finito. Como $\mathbb{K}_i : \mathbb{K}[\sigma_i(x)] = [\mathbb{K}' : \mathbb{K}[x]] = \frac{n}{q} < n$, pois $\mathbb{K}'_i \simeq \mathbb{K}'$ e $\mathbb{K}[\sigma_i(x)] \simeq \mathbb{K}[x]$, então pela hipótese de indução temos que existem $\frac{n}{q}$ $\mathbb{K}[\sigma_i(x)]$-isomorfismo distintos ϑ_{ij} de $\mathbb{K}'_i$ em $\mathbb{B}$. "Estamos supondo que o teorema é válido para o caso em que $[\mathbb{K}' : \mathbb{K}] = h < n$, que é a hipótese de indução. Neste caso estamos considerando no teorema $\mathbb{K}' = \mathbb{K}'_i$ e $\mathbb{K} = \mathbb{K}[\sigma_i(x)]$". Logo, as n aplicações compostas $\vartheta_{ij} \circ \tau_i$ resulta $q\frac{n}{q} = n$ $\mathbb{K}$-isomorfismos de $\mathbb{K}'$ em $\mathbb{B}$. Eles são distintos, pois para $i \neq i'$ temos que $\vartheta_{ij} \circ \tau_i$ e $\vartheta_{i'j'} \circ \tau'_i$ diferem em $\mathbb{K}[x]$ e para $i = i'$, mas $j \neq j'$ temos que ϑ_{ij} e $\vartheta_{ij'}$ diferem em $\mathbb{K}'_i$. Portanto, o teorema está provado.

Corolário 1.8 (Teorema do Elemento Primitivo) *Seja $\mathbb{K}$ um corpo finito ou um corpo de*

característica zero. Seja $\mathbb{K}'$ uma extensão de $\mathbb{K}$ de grau finito n. Então, existe um elemento x de $\mathbb{K}'$ (chamado um elemento primitivo) tal que $\mathbb{K}' = \mathbb{K}[x]$.

Prova: Se $\mathbb{K}$ é finito, então $\mathbb{K}'$ é finito, pois $\mathbb{K}'$ é uma extensão finita de $\mathbb{K}$ e seu grupo multiplicativo $\mathbb{K}'^*$ é formado de potências de um elemento x, pelo item (b) do Teorema 1.5. Logo, $\mathbb{K}' = \mathbb{K}[x]$. Suponha que $\mathbb{K}$ é de característica zero e assim $\mathbb{K}$ é um corpo infinito. Pelo Teorema 1.8 existem n $\mathbb{K}$-isomorfismos distintos σ_i de $\mathbb{K}'$ em um corpo algebricamente fechado $\mathbb{F}$, contendo $\mathbb{K}$. Para $i \neq j$, a equação $\sigma_i(y) = \sigma_j(y)$, com $y \in \mathbb{K}'$, define um subconjunto V_{ij} de $\mathbb{K}'$ que é um $\mathbb{K}$-subespaço do espaço vetorial $\mathbb{K}'$. De fato, sejam $y, y' \in V_{ij}$ e $k \in \mathbb{K}$, então para $i \neq j$ temos que $\sigma_i(y) = \sigma_j(y)$ e $\sigma_i(y') = \sigma_j(y')$. Daí, $\sigma_i(y+y') = \sigma_i(y) + \sigma_i(y') = \sigma_j(y') + \sigma_j(y') = \sigma_j(y+y')$, e ainda $\sigma_i(ky') = \sigma_i(k)\sigma_i(y') = k\sigma_j(y') = \sigma_j(y') = \sigma_i(k)\sigma_j(y')$. Logo, $y - y' \in V_{ij}$ e $ky' \in V_{ij}$. Assim, V_{ij} é subespaço vetorial de $\mathbb{K}'$. Temos que V_{ij} é distintos de $\mathbb{K}'$ quando $\sigma_i \neq \sigma_j$. Como $\mathbb{K}$ é infinito, a álgebra linear mostra que a união dos V_{ij} não é todo $\mathbb{K}'$. Tome x fora dessa união, então os $\sigma_i(x)$ são dois a dois disjuntos. Logo, o polinômio mínimo $P(X)$ de x sobre $\mathbb{K}$ possui no mínimo n raízes que são os $\sigma_i(x)$ em C. Assim, grau$P \geq n$, ou seja, $[\mathbb{K}[x] : \mathbb{K}] \geq n$. Como $\mathbb{K}[x] \subset \mathbb{K}'$ e $[\mathbb{K}' : \mathbb{K}] = n$, então $[\mathbb{K}[x] : \mathbb{K}] = n$, portanto $[\mathbb{K}' : \mathbb{K}[x]] = 1$. Logo, $\mathbb{K}' = \mathbb{K}[x]$.

Definição 1.22 *Qualquer extensão de grau dois sobre o corpo $\mathbb{Q}$ dos números racionais é chamado um corpo quadrático.*

Proposição 1.10 *Todo corpo quadrático é da forma $\mathbb{Q}(\sqrt{d})$ onde d é um inteiro livre de quadrado, ou seja, d não é divisível por quadrados diferentes de 1, mais precisamente $d = -1$ ou d é igual a mais ou menos o produto de primos distintos.*

Prova: Seja $\mathbb{K}$ um corpo quadrático, qualquer elemento $x \in \mathbb{K} - \mathbb{Q}$ é de grau 2 sobre $\mathbb{Q}$ assim é um elemento primitivo de $\mathbb{K}$, isto é, $\mathbb{K} = \mathbb{Q}[x]$ e $(1, x)$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Seja $F(X) = X^2 + bX + c$, onde $b, c \in \mathbb{Q}$, o polinômio minimal de tal elemento $x \in \mathbb{K}$. Resolvendo a equação quadrática $x^2 + bx + c = 0$ obtemos, $x = \frac{-b}{2} \pm \frac{1}{2}\sqrt{b^2 - 4c}$, como $\frac{-b}{2}$ e $\frac{1}{2}$ já pertencem a $\mathbb{Q}$, temos que $\mathbb{K} = \mathbb{Q}(\sqrt{b^2 - 4c})$. Agora, $b^2 - 4c$ é um número racional $\frac{u}{v} = \frac{uv}{v^2}$ com u e $v \in \mathbb{Z}$. Daí, como $\frac{1}{v^2}$ está em $\mathbb{Q}$ temos que $\mathbb{K} = \mathbb{Q}(\sqrt{uv})$. Com efeito é possível escrever $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ onde d é um inteiro livre de quadrado, isto é, d é mais ou menos o produto de primos distintos.

Observação 1.14 *O elemento $\sqrt{d}$ é uma raiz do polinômio irredutível $X^2 - d$. Esse elemento $\sqrt{d}$ possui um conjugado em $\mathbb{K}$, e este será denotado por $-\sqrt{d}$.*

Observação 1.15 *Existe um automorfismo σ de $\mathbb{K}$ que leva $\sqrt{d}$ em $-\sqrt{d}$. Daí, para qualquer elemento de $\mathbb{K}$ da forma $a+b\sqrt{d}$ com $a,b \in \mathbb{Q}$, temos*

$$\sigma(a+b\sqrt{d}) = a-b\sqrt{d} \tag{1.9}$$

Lema 1.6 *Seja A um domínio integralmente fechado, $\mathbb{K}$ seu corpo de frações e $\mathbb{L}$ uma extensão algébrica de $\mathbb{K}$. Se B é o fecho inteiro de A em $\mathbb{L}$ então $B \cap \mathbb{K} = A$.*

Prova: Seja $x \in \mathbb{L}$ inteiro sobre A e seja $F(X) \in \mathbb{K}[x]$ o polinômio minimal de x sobre $\mathbb{K}$. Seja $\mathbb{L}'$ o corpo de raizes de F sobre $\mathbb{K}$, isto é, o corpo gerado sobre $\mathbb{K}$ pelas raízes de F. Seja A' o fecho inteiro de A em $\mathbb{L}'$ então $A' \cap \mathbb{K} = A$, pois $A' \cap \mathbb{K}$ é inteiro sobre A. Daí, o lema segue do fato de que A é integralmente fechado, isto é, $B = A'$.

Teorema 1.9 *Seja $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ um corpo quadrático com $d \in \mathbb{Z}$ livre de quadrados, portanto não congruente a zero módulo* 4.
(a) Se $d \equiv 2 \mod 4$ ou $d \equiv 3 \mod 4$, o anel A dos inteiros de $\mathbb{K}$ consiste de todo elemento da forma $a+b\sqrt{d}$ com $a,b \in \mathbb{Z}$.
(b) Se $d \equiv 1 \mod 4$, A consiste de todo elemento da forma $\frac{1}{2}(u+v\sqrt{d})$, com $u,v \in \mathbb{Z}$ de mesma paridade.

Prova: Vimos anteriormente que existe um automorfismo σ de $\mathbb{K}$ que leva $\sqrt{d}$ em $\sqrt{d}$. Se $x \in A$ então existem $a_i \in \mathbb{Z}$, $i = o, \ldots, n-1$ tais que $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, portanto $\sigma(x)^n + a_{n-1}\sigma(x)^{n-1} + \cdots + a_1\sigma(x) + a_0 = 0$, isto é, $\sigma(x) \in A$. Como A é um anel $x + \sigma(x) \in A$ e $x\sigma(x) \in A$. Mas, se $x = a + b\sqrt{d}$, com $a,b \in \mathbb{Q}$ então por 1.9 temos

$$x + \sigma x = a + b\sqrt{d} + \sigma(a+b\sqrt{d}) = a + b\sqrt{d} + a - b\sqrt{d} = 2a$$

$$x\sigma(x) = (a+b\sqrt{d})(a-b\sqrt{d}) = a^2 - db^2 \in \mathbb{Q}$$

Como $\mathbb{Z}$ é um domínio integralmente fechado pelo Exemplo 1.6, segue-se do Lema 1.6 que

$$2a \in A \cap \mathbb{Q} = \mathbb{Z} \tag{1.10}$$

e

$$a^2 - db^2 \in A \cap \mathbb{Q} = \mathbb{Z} \tag{1.11}$$

As condições 1.10 e 1.11 são necessária para que $x = a + b\sqrt{d}$ seja inteiro sobre $\mathbb{Z}$. E são suficiente, pois x é raiz de $x^2 - 2ax + a^2 - db^2 = 0$ que pertence a $\mathbb{Z}[x]$. Ainda pela essas condições podemos observar que $a^2 - db^2 \in \mathbb{Z}$ (consequentemente $2a^2 \in \mathbb{Z}$), temos também que

$d(2b)^2 \in \mathbb{Z}$. Por outro lado, d é livre de quadrados, assim, se $2b$ não fosse inteiro, o denominador não teria um fator primo p. Esse fator primo teria de aparecer como p^2 no denominador de $(2b)^2$. Multiplicação por d não valeria $(2b)^2$ em $\mathbb{Z}$, pois $p^2 \nmid d$. Logo, podemos concluir que $2b$ é um número inteiro. Resumindo podemos tomar $a = \frac{u}{2}$ e $b = \frac{v}{2}$ com $u, v \in \mathbb{Z}$. Daí, pelas condições 1.10 e 1.11 temos

$$u^2 - dv^2 \in 4\mathbb{Z} \tag{1.12}$$

Se v é par então u também é par, pois, $v = 2k$ temos que $u^2 - d(2k)^2 = 4t \Rightarrow u^2 = 4t - 4dk^2 = 4(t - dk^2) \Rightarrow u^2 \equiv 0 \mod 4$. Logo, $a, b \in \mathbb{Z}$, já que $a = \frac{u}{2}$ e $b = \frac{v}{2}$. Assim, os elementos de A são da forma $a + b\sqrt{d}$, onde $a, b \in \mathbb{Z}$. Isto prova (a) e parte de (b). Se v é ímpar então $v^2 \equiv 1 \mod 4$. As possibilidades $\mod 4$ para u^2 são 0 e 1, já que u^2 é quadrado. Como d é livre de quadrados, d não é múltiplo de 4. Necessariamente por 1.12 $u^2 \equiv 1 (\mod 4)$ e $d \equiv 1 \mod 4$ já que $v^2 \equiv 1 \mod 4 \Rightarrow u^2 \equiv d \mod 4$. Logo os elementos de A são da forma $\frac{u}{2} + \frac{v}{2}\sqrt{d}$ onde u e v saõ de mesma paridade e isto conclui o item (b).

Observação 1.16 *No caso que $d \equiv 2 \mod 4$ ou $d \equiv 3 \mod 4$, $(1, \sqrt{d})$ é uma base para A como $\mathbb{Z}$-módulo. Se $d \equiv 1 (\mod 4)$, $(1, \frac{1}{2}(1 + \sqrt{d}))$ é uma base para o $\mathbb{Z}$-módulo A. De fato, por (b) 1, $\frac{1}{2}(1 + \sqrt{d})$ pertencem a A. Reciprocamente, para mostrar que $\frac{1}{2}(u + v\sqrt{d})$ (com $u, v \in \mathbb{Z}$ de mesma paridade) é expresso como uma combinação $\mathbb{Z}$-linear de 1 e $\frac{1}{2}(1 + \sqrt{d})$, por subtração de $\frac{1}{2}(1 + \sqrt{d})$, reduzir o problema no caso onde u e v são pares, neste caso $\frac{1}{2}(u + v\sqrt{d}) = \frac{u}{2} + \frac{v}{2}\sqrt{d} + \frac{v}{2} - \frac{v}{2} = \left(\frac{u}{2} - \frac{v}{2}\right)1 + v\frac{1}{2}(1 + \sqrt{d})$. Logo, $\frac{1}{2}(u + v\sqrt{d})$ é escrito como combinação linear de 1 e $\frac{1}{2}(1 + \sqrt{d})$.*

Observação 1.17 *Se $d > 0$, $\mathbb{Q}(\sqrt{d})$ é chamado um corpo quadrático real. Existe um subcorpo de conjugado para $\mathbb{Q}(\sqrt{d})$ sobre $\mathbb{Q}$. Se $d < 0$ então $\mathbb{Q}(\sqrt{d})$ é chamado um corpo quadrático imaginário.*

1.5 Norma, traço e discriminante

Seja A um anel, E um A-módulo livre de posto finito e seja u um endomorfismo de E, isto é, um homomorfismo $u : E \to E$. Na álgebra linear definimos o traço, o determinante e o polinômio característico de u da seguinte forma: se $\{e_i\}$ é uma base de E e se (A_{ij}) é uma matriz de u com respeito a essa base, então o traço, o determinante e o polinômio característico de u são respectivamente:

$$\mathrm{T}r(u) = \sum_{i=1}^{n} a_{ii},\ \det u = \det(A_{ij}) \tag{1.13}$$

e

$$\det(XI_E - u) = \det(X\delta_{ij} - A_{ij}), \tag{1.14}$$

onde $j \neq i \Rightarrow \delta_{ij} = 0$ e $j = i \Rightarrow \delta_{ij} = 1$

Observação 1.18 *Esses valores independem da escolha da base. As fórmulas 1.13 e 1.14 implicam:*

$$\mathrm{T}r(u+u') = \sum_{i=1}^{n} a_{ii} + a'_{ii} = \sum_{i=1}^{n} a_{ii} + \sum_{i=1}^{n} a'_{ii} = \mathrm{T}_r(u) + \mathrm{T}r(u') \tag{1.15}$$

$$\det(uu') = \det(A_{ij}A'_{ij}) = \det(A_{ij}).\det(A'_{ij}) = \det(u)\det(u') \tag{1.16}$$

$$\det(XI_E - u) = X^n - \mathrm{T}r(u)X^{n-1} + \cdots + (-1)^n \det(u) \tag{1.17}$$

Para $n = 2$ temos:

$$\det(XI_E - u) = \det\left[X\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\right] = \det\begin{pmatrix} X - a_{11} & -a_{12} \\ -a_{21} & X - a_{22} \end{pmatrix}$$

$$= (X - a_{11})(X - a_{22}) - a_{12}a_{21} = X^2 - Xa_{22} - Xa_{11} + a_{11}a_{22} - a_{12}a_{21}$$

$$= X^2 - (a_{22} + a_{11}X + \det A_{ij}) = X^2 - \mathrm{T}r(u)X + (-1)^2\det(u)$$

Seja B um anel e A um subanel de B tal que B é um A-módulo livre de posto finito n, por exemplo, A pode ser um corpo e B uma extensão finita de A com grau n. Para $x \in B$, a multiplicação m_x por x, isto é, $y \mapsto xy$ com $y \in A$, é um endomorfismo do A-módulo B, isto é, um homomorfismo $m_x : B \to B$.

Definição 1.23 *Chamaremos traço (resp. norma, polinômio característico) de $x \in B$, relativo a B e A, o traço (resp. determinante, polinômio característico) do endomorfismo m_x da multiplicação por x.*

Observação 1.19 *O traço (resp. a norma) de x é denotado por $\mathrm{T}r_{B/A}(x)$ (resp. $\mathcal{N}_{B/A}(x)$) ou $\mathrm{T}r(x)$ (resp. $\mathcal{N}(x)$) quando não houver confusão. Estes são elementos de A.*

Para $x, x' \in B$ e $a \in A$ temos $m_x + m'_x = m_{x+x'}$ e $m_x \circ m'_x = m_{xx'}$ e $m_{ax} = am_x$. Além disso, a matriz de m_a com respeito a qualquer base de B sobre A, é a matriz diagonal cujas entradas são

a. Das fórmulas 1.13, 1.14, 1.15, 1.16 e 1.17 obtemos:

$$\mathrm{T}r(x+x') = \mathrm{T}r(m_{x+x'}) = \mathrm{T}r(m_x + m'_x) = \mathrm{T}r(m_x) + \mathrm{T}r(m'_x) = \mathrm{T}r(x) + \mathrm{T}r(x')$$

$$\mathrm{T}r(ax) = \mathrm{T}r(m_{ax}) = \mathrm{T}r(am_x) = a\mathrm{T}r(m_x) = a\mathrm{T}r(x)$$

$$\mathrm{T}r(a) = \mathrm{T}r(m_a) = \underbrace{a+a+\cdots+a}_{n \text{ vezes}} = na$$

$$\mathscr{N}(xx') = d(xx') = d(x)d(x') = \mathscr{N}(x)\mathscr{N}(x')$$

$$\mathscr{N}(a) = \det(a) = \det(m_a) = \underbrace{a\cdots a}_{n \text{ vezes}} = a^n$$

$$\mathscr{N}(ax) = \det(ax) = \det(a)\det(x) = a^n\mathscr{N}(x)$$

Proposição 1.11 *Seja* $\mathbb{K}$ *um corpo de característica zero ou um corpo finito,* $\mathbb{L}$ *uma extensão algébrica de* $\mathbb{K}$ *com grau n, x um elemento de* $\mathbb{L}$*, e as raízes* $x_1,\ldots,x_n$*. O polinômio minimal* $F(X) \in \mathbb{K}[X]$ *de x sobre* $\mathbb{K}$ *(em alguma extensão conveniente de* $\mathbb{K}$*), cada uma repetida* $[\mathbb{L} : \mathbb{K}[X]]$ *vezes. Então* $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x) = x_1 + \cdots + x_n$*,* $\mathscr{N}_{\mathbb{L}/\mathbb{K}}(x) = x_1 \cdots x_n$*. O polinômio característico de x, relativo as extensões* $\mathbb{L}$ *e* $\mathbb{K}$ *é igual a* $(X - x_1)\cdots(X - x_n)$*.*

Prova: Vamos primeiro considerar o caso onde x é um elemento primitivo de $\mathbb{L}$ sobre $\mathbb{K}$. Seja $F(X)$ o polinômio minimal de x sobre $\mathbb{K}$. Então $\mathbb{L}$ é um $\mathbb{K}$-isomorfismo para $\mathbb{K}(X)/F(X)$ e $\{1, x, \ldots, x^{n-1}\}$ é uma base para $\mathbb{L}$ sobre $\mathbb{K}$. Ponhamos $F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. A matriz do endomorfismo m_x com respeito a esta base é:

$$M = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & -a_{n-1} \end{bmatrix}$$

O determinante de $XI_L - m_x$ é portanto o determinante da matriz

$$XI_n - M = \det\left[\begin{pmatrix} X & 0 & \dots & 0 \\ 0 & X & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & X \end{pmatrix} - \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}\right] =$$

$$\det\begin{bmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & X & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & -1 & X-a_{n-1} \end{bmatrix}$$

Expandindo esse determinante como um polinômio em X, obtemos o polinômio característico de x, isto é, $\det(XI_n - M) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = F(X)$. Daí, pelas equações 1.15, 1.16, 1.17 temos que $\mathrm{T}r(x) = -a_{n-1}$ e $\mathscr{N}(x) = (-1)^n a_0$. Como x é um elemento primitivo de $\mathbb{L}$ sobre $\mathbb{K}$, temos $F(X) = (X - x_1)\cdots(X - x_n)$, pois F possui exatamente n raízes. Igualando os coeficentes vemos que $\mathrm{T}r(x) = x_1 + \cdots + x_n$ e $\mathscr{N}(x) = x_1 \cdots x_n$.

Consideremos agora o caso geral. Ponha $r = [\mathbb{L} : \mathbb{K}[X]]$. É suficiente mostrar que o polinômio característico $P(X)$ de x, com respeito a $\mathbb{L}$ e $\mathbb{K}$, é igual a r-ésima potência do polinômio minimal de x sobre $\mathbb{K}$, isto é, $F(X)^n = P(X)$. Seja $\{y_i\}_{i=1,\dots,q}$ uma base para $\mathbb{K}[X]$ sobre $\mathbb{K}$ e $\{z_j\}_{j=1,\dots,r}$ uma base para $\mathbb{L}$ sobre $\mathbb{K}[X]$ e $\{y_i z_j\}_{i=1,\dots,q,\, j=1,\dots,r}$ uma base para $\mathbb{L}$ sobre $\mathbb{K}$ e $n = qr$ pela Proposição 1.7. Seja $M = (A_{ih})$ a matriz para a multiplicação por x em $\mathbb{K}[X]$, com respeito a base $\{y_i\}_{i=1,\dots,q}$. Assim, $xy_i = \sum_h a_{ih} y_h$. Daí, obtemos então $x(y_i z_j) = \sum_h (a_{ih} y_h) z_j = \sum_h a_{ih}(y_h z_j)$, para $i = 1, \dots, q$ e $j = 1, \dots, r$. Logo, a matriz M_1 de $m_x : \mathbb{L} \to \mathbb{L}$, com respeito a base do $\mathbb{K}$-espaço vetorial $\mathbb{L}$, considerada acima, é a matriz de blocos diagonais da forma:

$$M_1 = \begin{pmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M \end{pmatrix}$$

Como M_1 é $n \times n$ e M é $q \times q$ temos que M deve aparecer r vezes em M_1, como blocos diagonais em M_1, já que $n = qr$. Daí, a matriz $XI_n - M_1$ consiste de r blocos diagonais cada um da forma $XI_q - M$. Consequentimente, $\det(XI_n - M_1) = \det(XI_n - M)^r$. O lado esquerdo da equação é $P(X)$, enquanto $\det(XI_q - M)$ é o polinômio minimal de x sobre $\mathbb{K}$, de acordo com a primeira parte da prova. Logo, o polinômio característico $P(X)$ de x, com respeito a $\mathbb{L}$ e a $\mathbb{K}$, é igual a r-ésima potência do polinômio minimal de x sobre $\mathbb{K}$.

Proposição 1.12 *Seja A um domínio de integridade, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão de $\mathbb{K}$ com grau finito e $x \in \mathbb{L}$ inteiro sobre A. Assuma que $\mathbb{K}$ tem característica zero. Então os coeficentes do polinômio característico $P(X)$ de x relativa a $\mathbb{L}$ e $\mathbb{K}$, em particular $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x)$ e $\mathcal{N}_{\mathbb{L}/\mathbb{K}}(x)$ são inteiros sobre A.*

Prova: Pela Proposição 1.11, $P(X) = (X - x_1)\cdots(X - x_n)$; assim os coeficientes de $P(X)$ são, a menos de sinal, somas de produto dos x_i's. Daí, é suficiente mostrar que os x_i's são inteiros sobre A pelo Corolário 1.6. Como cada x_i é um conjugado de x sobre $\mathbb{K}$, pois os x_i's são dois a dois conjugados e $\mathbb{K}[x]/P(X) \simeq \mathbb{K}[x_i]$ e existe um $\mathbb{K}$-isomorfismo $\sigma_i : \mathbb{K}[x] \to \mathbb{K}[x_i]$ tal que $\sigma_i(x) = x_i$. Sendo x inteiro sobre A existem $a_i \in A$, $i = 0, \cdots, n-1$ tais que $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$. Assim, $\sigma_i(x)^n + \cdots + \sigma_i(a_0) = 0$. Logo, $x_i^n + a_{n-1}x_i^{n-1} + \cdots + a_0 = 0$ e isso prova que x_i é inteiro sobre A $\forall i$.

Corolário 1.9 *Suponha, além disso, que A é integralmente fechado. Então os coeficientes do polinômio característico de x, em particular $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x)$ e $\mathcal{N}_{\mathbb{L}/\mathbb{K}}(x)$, são elementos de A.*

Prova: Por definição os coeficientes são elementos de $\mathbb{K}$. Pela Proposição 1.12, eles são inteiros sobre A, sendo A integralmente fechado, eles pertencem a A.

Definição 1.24 *Seja B um anel e A um subanel de B tal que B é um A-módulo livre de posto finito n. Para $\{x_1, \ldots, x_n\} \subset B^n$, chamamos o discriminante do conjunto $\{x_1, \ldots, x_n\}$ o elemento de A definido pela relação: $D(x_1, \ldots, x_n) = \det(\mathrm{Tr}_{B/A}(x_i x_j))$, isto é, o determinante da matriz da forma:*

$$\begin{pmatrix} \mathrm{Tr}_{B/A}(x_1x_1) & \mathrm{Tr}_{B/A}(x_1x_2) & \ldots & \mathrm{Tr}_{B/A}(x_1x_n) \\ \mathrm{Tr}_{B/A}(x_2x_1) & \mathrm{Tr}_{B/A}(x_2x_2) & \ldots & \mathrm{Tr}_{B/A}(x_2x_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}_{B/A}(x_nx_1) & \mathrm{Tr}_{B/A}(x_nx_2) & \ldots & \mathrm{Tr}_{B/A}(x_nx_n) \end{pmatrix}$$

Os discriminantes de diferentes n-uplas estão relacionadas da seguinte maneira:

Proposição 1.13 *Se* $\{y_1,\cdots,y_n\}\subset B^n$ *é o conjunto dos elementos de B tal que* $y_i=\sum_{j=1}^{n}a_{ij}x_j$, *com* $A_{ij}\in A$. *Então,* $D(y_1,\ldots,y_n)=[\det(A_{ij})][\det(x_1,\ldots,x_n)]$.

Prova: Veja que:

$$\mathrm{T}r(y_py_q)=\mathrm{T}r\left[\left(\sum_{i=1}^{n}a_{pi}x_i\right)\left(\sum_{j=1}^{n}a_{qj}x_j\right)\right]=\mathrm{T}r\left(\sum_{i,j}a_{pi}a_{qj}x_ix_j\right)=\sum_{i,j}a_{pi}a_{qj}(\mathrm{T}r(x_ix_j))$$

Daí, temos a equação matricial

$$\mathrm{T}r(y_py_q)=(A_{pi})(\mathrm{T}r(x_ix_j))(A_{qj}^t)$$

onde (A_{qj}^t) é a transposta de (A_{qj}). Calculando o determinante das matrizes acima, obtemos:

$$\det(\mathrm{T}r(y_py_q))=\det(A_{pi})\det(\mathrm{T}r(x_ix_j))\det(A_{qj}^t)$$

$$D(y_1,\ldots,y_n)=\det(A_{pi})\det(\mathrm{T}r(x_ix_j))\det(A_{qj}^t)$$

$$D(y_1,\ldots,y_n)=(\det(A_{ij}))^2\det(\mathrm{T}r(x_ix_j))$$

$$D(y_1,\ldots,y_n)=(\det(A_{ij}))^2D(x_1,\ldots,x_n)$$

Observação 1.20 *A Proposição 1.13 implica que o discriminante de bases para B sobre A são associados em A. Isto significa que a matriz* (A_{ij}) *que expressa uma base em termos da outra possui uma inversa com entradas em A. Assim,* $(A_{ij})(A_{ij})^{-1}=I$ *e daí* $\det(A_{ij})\det(A_{ij})^{-1}=1$. *Logo,* $\det(A_{ij})$ *e* $\det(A_{ij})^{-1}$ *são unidades em A.*

Definição 1.25 *Seja B um anel e A um subanel de B tal que B é um A-módulo livre de posto n. Assim, o ideal principal de A gerado pelo discriminante de qualquer base de B sobre A é chamado o discriminante de B sobre A. Dentamos este ideal por* $D_{B/A}$.

Proposição 1.14 *Suponha que* $D_{B/A}$ *contém um elemento que não é um divisor de zero. Então, para que o conjunto* $\{x_1,\ldots,x_n\}\subset B^n$ *seja uma base de B sobre A, é necessário e suficiente que* $D(x_1,\ldots,x_n)$ *gere* $D_{B/A}$.

Prova: $\Rightarrow$) É imediato da Definição 1.25.

$\Leftarrow$) Suponha que $d=D(x_1,...,x_n)$ gera $D_{B/A}$. Seja $\{e_1,\cdots,e_n\}$ uma base de B sobre A. Ponha $d'=D(e_1,\ldots,e_n)$ e $x_i=\sum_{j=1}^{n}a_{ij}e_j$ com $a_{ij}\in A$, $1\leq i\leq n$. Assim, pela Proposição 1.13

temos que $D(x_1,\ldots,x_n) = \det(A_{ij})^2 D(e_1,\ldots,e_n)$, ou seja,

$$d = \det(A_{ij})^2 d' \tag{1.18}$$

Por hipótese, temos que $Ad = D_{B/A}$. Daí, $Ad = D_{B/A} = Ad(A_{ij})^2 d' = Ad'$. Logo, existe $b \in A$ tal que tal que $d' = bd$ daí, $d = \det(A_{ij})^2 d' \Rightarrow d = \det(A_{ij})^2 bd \Rightarrow d - \det(A_{ij})^2 bd = 0 \Rightarrow d(1 - b\det(A_{ij})^2) = 0$. Temos que d não é divisor de zero, pois caso contrário todo elemento de $D_{B/A}$ seria um divisor de zero (o que não pode ocorrer, já que $D_{B/A}$ possui um elemento que não é divisor de zero). Logo, $1 - b\det(A_{ij})^2 = 0$. Isto significa que $\det(A_{ij}) \neq 0$. Assim, a matriz (A_{ij}) é invertível. Portanto, $\{x_1,\ldots,x_n\}$ é uma base de B sobre A. Pois, como (A_{ij}) é invertível, então a transformação linear $u : B \to B$ é um isomorfismo, pois (A_{ij}) é a matriz de u, daí u leva base em base. Sendo $\{e_1,\ldots,e_n\}$ base, então $(A_{ij})(e_1,\ldots,e_n) = \{x_1,\ldots,x_n\}$ é base.

Proposição 1.15 *Seja $\mathbb{K}$ um corpo que é finito ou de característica zero e $\mathbb{L}$ uma extensão de $\mathbb{K}$ de grau finito n. Considere $\sigma_1,\ldots,\sigma_n$ os n $\mathbb{K}$-isomorfismos distintos de $\mathbb{L}$ em um corpo algebricamente fechado C contendo $\mathbb{K}$. Então, se $\{x_1,\ldots,x_n\}$ é uma base para $\mathbb{L}$ sobre $\mathbb{K}$, temos que $D(x_1,\ldots,x_n) = \det(\sigma_i(x_j))^2 \neq 0$.*

Prova: Vamos mostrar inicialmente que $D(x_1,\ldots,x_n) = \det(\sigma_i(x_j))^2$. De fato, $D(x_1,\ldots,x_n) = \det(\mathrm{T}r(x_i x_j)) = \det(\sigma_1(x_i x_j) + \cdots + \sigma_n(x_i x_j)) = \det\left(\sum_{k=1}^{n} \sigma_k(x_i x_j)\right) = \det(\sigma_k(x_i)\sigma_k(x_j)) = \det(\sigma_k(x_i))\det(\sigma_k(x_j)) = \det(\sigma_i(x_j))^2$. Agora vamos mostrar que $\det(\sigma_i(x_j)) \neq 0$. Suponha, por obsurdo, que $\det(\sigma_i(x_j)) = 0$ então existem $u_1,\cdots,u_n \in C$ nem todos nulos, tais que $\sum_{i=1}^{n} u_i\sigma_i(x_j) = 0$, $\forall\ j$, por linearidade, concluímos que $\sum_{i=1}^{n} u_i\sigma_i(x) = 0$ para todo $x \in \mathbb{L}$, mas isso contradiz o lema abaixo.

Lema 1.7 (Dedekind) *Seja G um grupo, C um corpo e $\sigma_1,\ldots,\sigma_n$ homomorfismos distintos de G no grupo multiplicativo C^*. Então os σ_i's são linearmente independentes sobre C, isto é, $\sum_{i=1}^{n} u_i\sigma_i(g) = 0$, $\forall\ g \in G$ implica que os u_i's são zero.*

Prova: Suponha, por absurdo, que os σ_i's são linearmente dependente. Considere a relação não trivial $\sum_{i=1}^{n} u_i\sigma_i = 0$ $(u_i \in C)$ tal que o número q de u_i's que são não nulos é mínimo. Após a reenumeração podemos supor que:

$$u_1\sigma_1(g) + \cdots + u_q\sigma_q(g) = 0,\ \forall\ g \in G \tag{1.19}$$

Temos $q \geq 2$, pois os σ_i's são não nulos. Para g e h arbitrários em G, temos que:

$$u_1\sigma_1(hg) + \cdots + u_q\sigma_q(hg) = u_1\sigma_1(h)\sigma_1(g) + \cdots + u_q\sigma_q(h)\sigma_q(g) = 0$$

pois, $hg \in G$ e como $u_1\sigma_1(g)+\cdots+u_q\sigma_q(g)=0$, $\forall\, g \in G$, então $u_1\sigma_1(hg)+\cdots+u_q\sigma_q(hg)=0$. Se multiplicarmos 1.19 por $\sigma_1(h)$ temos:

$$u_1\sigma_1(h)\sigma_1(g)+\cdots+u_q\sigma_q(h)\sigma_q(g)=0$$

Daí,

$$u_1\sigma_1(h)\sigma_1(g)+\cdots+u_q\sigma_1(h)\sigma_q(g)-u_1\sigma_1(h)\sigma_1(g)-\cdots-u_q\sigma_q(h)\sigma_q(g)=o$$

Assim,

$$u_1(\sigma_1(h)-\sigma_2(h))\sigma_2(g)+\cdots+u_q(\sigma_1(h)-\sigma_q(h))\sigma_q(g)=0,$$

como esta igualdade é verdade para todo $g \in G$ e q foi escolhido tão pequeno quanto possível, segue que $u_2(\sigma_1(h)-\sigma_2(h))=0$. Daí, $\sigma_1(h)=\sigma_2(h)$, $\forall\, h \in G$, pois $u_2 \neq 0$, o que é obsurdo, pois por hipótese os σ_i's são distintos.

Observação 1.21 *Como as condições da proposição 1.15, a relação $D(x_1,\ldots,x_n) \neq 0$ mostra que a forma bilinear $(x,y) \mapsto \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(xy)$ é não degenerada, isto é, $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(xy)=0$, $\forall\, y \in \mathbb{L}$ implica que $x=0$. Assim, a aplicação $\mathbb{K}$-linear que associa a cada $x \in \mathbb{L}$ a forma $\mathbb{K}$-linear $s_x : y \mapsto \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(xy)$ é uma injeção de $\mathbb{L}$ em seu dual $\hom_{\mathbb{K}}(\mathbb{L},\mathbb{K})$. Como $\mathbb{L}$ e $\hom_{\mathbb{K}}(\mathbb{L},\mathbb{K})$ são da mesma dimensão finita n sobre $\mathbb{K}$, segue que $x \mapsto s_x$ é uma bijeção. A existência de "bases duais"de um espaço vetorial e seu dual implica que, para toda base $\{x_1,\ldots,x_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$, existe uma base $\{y_1,\ldots,y_n\}$ tal que $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(x_iy_j)=\delta_{ij}$ $(1 \leq i,j \leq n)$.*

Teorema 1.10 *Seja A um anel integralmente fechado, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$, uma extensão de $\mathbb{K}$ de grau finito n e A' o fecho integral de A em $\mathbb{L}$. Suponha que $\mathbb{K}$ é de característica zero. Então A' é um A-submódulo de um A-módulo livre de posto n.*

Prova: Seja $\{x_1,\ldots,x_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Cada x_i é algébrico sobre $\mathbb{K}$ e daí para todo i, temos uma equação da forma,

$$a_nx_i^n+a_{n-1}x_i^{n-1}+\cdots+a_0=0,$$

com $a_j \in A$ $\forall j=0,\ldots,n$, pois $\mathbb{L}$ é extensão algébrica de $\mathbb{K}$, já que $[\mathbb{L}:\mathbb{K}]$ é finito. Podemos assumir que $a_n \neq 0$. Multiplicando a equações acima a_n^{n-1}, obetemos

$$a_n^{n-1}a_nx_i^n+a_n^{n-1}a_{n-1}x_i^{n-1}+\cdots+a_n^{n-1}a_0=0$$

$$a_n^nx_i^n+a_n^{n-1}a_{n-1}x_i^{n-1}+\cdots+a_n^{n-1}a_0=0$$

$$(a_nx_i)^n+a_{n-1}(a_nx_i)^{n-1}+\cdots+a_n^{n-1}a_0=0.$$

Logo, $a_n x_i$ é inteiro sobre A. Pondo $x_i' = a_n x_i$, então $\{x_1', \cdots, x_n'\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Contido em A', pois $a_n x_i$ é inteiro sobre A. Pela Observação 1.21, existe uma base $\{y_1, \ldots, y_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$ tal que $\mathrm{Tr}(x_i' y_j) = \delta_{ij}$. Seja $z \in A'$. Como $\{y_1, \ldots, y_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, podemos escrever $z = \sum_{j=1}^{n} b_j y_j$, com $b_j \in \mathbb{K}$, pois $z' \in A' \Rightarrow z \in \mathbb{L}$ ser inteiro sobre A e como $\{y_1, \ldots, y_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ então de fato temos $z = \sum_{j=1}^{n} (b_j y_j)$. Para todo i, temos que $x_i' z \in A'$, pois $x_i' \in A'$ e $z \in A$. Logo, $\mathrm{Tr}(x_i' z) \in A$, pelo Corolário 1.9. Assim, $\mathrm{Tr}(x_i' z) = \mathrm{Tr}(x_i' \sum_{j=1}^{n} b_j y_j) = \mathrm{Tr}(\sum_{j=1}^{n} b_j x_i' y_j) = \sum_{j=1}^{n} b_j \mathrm{Tr}(x_i' y_j)$, pois $b_j \in \mathbb{K}$.

$$\mathrm{Tr}(x_1' z) = \sum_{j=1}^{n} b_j \delta_{ij} = b_1 \delta_{i1} + \cdots + b_i \delta_{ij} = b_i$$

Podemos concluir que $b_i \in A$, $\forall\, i$, pois $\mathrm{Tr}(x_i' z) \in A$. Isto implica que A' é um submódulo do A-módulo livre $\sum_{j=1}^{n} a_{yj}$, pois $x' z \in A'$, $\forall\, z \in \sum_{j=1}^{n} a_{yj}$ e $\forall\, x_i' \in A'$.

Corolário 1.10 *Com as hipóteses do Teorema 1.10 e supondo que A é principal, temos que A' é um A-módulo livre de posto n.*

Prova: Como A' é um submódulo de um A-módulo livre e A é principal, então pelo item (a) do Teorema 1.3, se A é um anel de ideais principais, M é A-módulo livre de posto n e M' é um submódulo de M então M' é livre de posto $\leq n$. Daí, temos que A' é livre de posto $\leq n$. Por outro lado, temos pela prova do Teorema 1.10 que A' contém uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Assim, A' possui uma base com n elementos. Portanto, A' é de posto n.

1.6 A terminologia dos corpos numéricos e corpos ciclotômicos

Definição 1.26 *Qualquer extensão finita (e portanto algébrica) de $\mathbb{Q}$ é chamada um corpo de números algébricos ou corpo numérico.*

Definição 1.27 *Um corpo numérico de grau 2 (resp. 3) é chamado corpo quadrático (rep. cúbico). Para um corpo numérico $\mathbb{K}$, $[\mathbb{K} : \mathbb{Q}]$ denota o grau de $\mathbb{K}$.*

Observação 1.22 *Um corpo numérico sempre possui característica zero, pois contém $\mathbb{Q}$ e consequentemente $\mathbb{Z}$. Os elementos de um corpo numérico $\mathbb{K}$ que são inteiros sobre $\mathbb{Z}$ são*

chamados, os inteiros de $\mathbb{K}$. Eles formam um subanel A de $\mathbb{K}$ pelo Corolário 1.7. Esse anel A é um $\mathbb{Z}$-módulo livre de posto $[\mathbb{K}:\mathbb{Q}]$ pelo Corolário 1.10.

Os discriminantes das bases do $\mathbb{Z}$-módulo A diferem por uma unidade em $\mathbb{Z}$ pela Definição 1.25, uma unidade que é exatamente um quadrado em $\mathbb{Z}$ pela Proposição 1.13. Esta unidade só pode ser $+1$, isto é, o discriminante do $\mathbb{Z}$-módulo A é um elemento bem definido de $\mathbb{Z}$. Ele é chamado o discriminante absoluto ou discriminante de $\mathbb{K}$. Frequentemente, por abuso de linguagem atribuímos a $\mathbb{K}$ noções que são definidas relativas a A. Assim, quando falamos de ideais (ou unidades) de $\mathbb{K}$, queremos dizer ideais (ou unidades) de A.

Definição 1.28 *Seja $\mathbb{K}$ um corpo. Um elemento $\zeta \in \mathbb{K}$ tal que $\zeta^p = 1$ é chamado uma raiz p-ésima da unidade. Dizemos que ζ é uma raiz p-ésima primitiva da unidade se $\zeta^p = 1$ e $\zeta^m \neq 1$ para $1 < m < p$.*

Definição 1.29 *Um corpo ciclotômico é qualquer corpo gerado sobre $\mathbb{Q}$ pelas raízes da unidade.*

Observação 1.23 *Dado um número primo p, escrevemos ζ para p-ésima raiz primitiva da unidade em ($\mathbb{C}$ por exemplo). Estudaremos os corpos ciclotômicos $\mathbb{Q}[\zeta]$. O número ζ é uma raiz do polinômio $X^p - 1$. Como $\zeta \neq 1$, temos que ζ é uma raiz do polinômio $\dfrac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + X + 1$, o qual é chamado polinômio ciclotômico. Para mostrarmos que este é irredutível sobre $\mathbb{Q}$ precisaremos do seguinte lema.*

Lema 1.8 (Lema de Gauss) *Seja A um anel de ideais principais, p um elemento primo de A e $F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 \in A[X]$ tal que $p|a_i$ $(0 \leq i \leq n-1)$ e $p \nmid a_0$. Então, $F(X)$ é irredutível sobre $\mathbb{K}$ o corpo de frações de A.*

Prova: Suponha que $F = GH$ com $G, H \in \mathbb{K}[X]$ e ambos polinômios mônicos. As raízes de F são inteiras sobre A. Qualquer raiz de G ou H é uma raiz de F, portanto inteiro sobre A. Os coeficientes de G (respe. H) são somas de produtos de raízes de G (respe. H), eles são portanto inteiros sobre A, pelo Corolário 1.6. Como A é um anel de ideais principais, temos que A é integralmente fechado pelo Exemplo 1.6. Logo, $G, H \in A[X]$. Agora considere $\overline{F}, \overline{G}$ e $\overline{H}$ como sendo as imagens de F, G e H respectivamente em $(A/A_p)[x]$, então $\overline{F} = \overline{GH}$. Como por hipótese $p|a_i$, $0 \leq i \leq n-1$, temos que $\overline{F} = X^n$, pois $F[x] = \sum d_i x' \mapsto \overline{F(x)} = \sum \overline{d}_i x_i$. Como A/A_p é domínio de integridade, a fatoração $X^n = \overline{GH}$ é necessariamente da forma $X^n = X^q X^{n-q}$ (pois, $\overline{G}$ e $\overline{H}$ são mônicos), assim $\overline{G} = X^q$ e $\overline{H} = X^{n-q}$. Se G e H são ambos não constantes, então p divide os termos constantes de G e H. Logo, p^2 divide os termos constantes a_0 de F, mas isso contraria a hipótese. Logo, ou G ou H é constante e F é irredutível.

Exemplo 1.8 *O polinômio $X^3 - 2X + 6$ é irredutível sobre $\mathbb{Q}$. Basta tomar $p = 2$ e $A = \mathbb{Z}$ no Lema de Gauss.*

Teorema 1.11 *Para qualquer número primo p o polinômio ciclotômico*

$$X^{p-1} + X^{p-2} + \cdots + X + 1$$

é irredutível em $\mathbb{Q}[x]$.

Prova: Ponha $X = Y + 1$. Então, $X^{p-1} + X^{p-2} + \cdots + X + 1 = \dfrac{X^p - 1}{X - 1} = \dfrac{(Y+1)^p - 1}{Y} = Y^{p-1} + \displaystyle\sum_{j=p-1}^{1} \binom{p}{j} Y^{j-1} = F_1(Y)$. Se $F_1(Y)$ é irredutível, então também o é um polinômio ciclotômico. Observando que p divide cada um dos coeficientes binominais $\binom{p}{j}$ e p^2 não divide o termo constante $\binom{p}{j} = p$, concluímos do Critério de Eisenstein que $F_1(Y)$ é irredutível.

Observação 1.24 *O teorema acima implica que $\mathbb{Q}[\zeta]$ é de grau $p - 1$, portanto $\{1, \zeta, \cdots, \zeta^{p-1}\}$ é uma base para $\mathbb{Q}[\zeta]$ sobre $\mathbb{Q}$. Passaremos a estudar o anel dos inteiros de $\mathbb{Q}[\zeta]$ e mostrar que o mesmo é $\mathbb{Z}[\zeta]$. Para isso, precisamos calcular alguns traços e normas (escrevemos $\mathrm{Tr}(x)$ e $\mathscr{N}(x)$ no lugar de $\mathrm{Tr}_{\mathbb{Q}[\zeta]/\mathbb{Q}}(x)$ e $\mathscr{N}_{\mathbb{Q}[\zeta]/\mathbb{Q}}(x)$). Notemos que o conjugado de ζ sobre $\mathbb{Q}$ são os ζ^j, $j = 1, \ldots, p-1$.*

Observação 1.25 *A irredutibilidade do polinômio ciclotômico implica imediatamente:*

$$\mathrm{Tr}(\zeta) = -1, \quad \mathrm{Tr}(1) = (p-1)1 = p - 1$$

pois, o $\mathrm{Tr}(\zeta) = -a_{p-2}$ e polinômio característico de ζ relativo a $\mathbb{Q}[\zeta]$ e $\mathbb{Q}$ é o polinômio ciclotômico $F(X) = X^{p-1} + X^{p-2} + \cdots + X + 1$. Portanto, $\mathrm{Tr}(\zeta^j) = -1$ para $j = 1, \ldots, p-1$ e assim,

$$\mathrm{Tr}(1 - \zeta) = \mathrm{Tr}(1) + \mathrm{Tr}(-\zeta) = \mathrm{Tr}(1) - \mathrm{Tr}(\zeta) = \mathrm{Tr}(1 - \zeta^1) = \cdots = \mathrm{Tr}(1 - \zeta^{p-1}) = p$$

Por outro lado, pelo Teorema 1.11 temos que o polinômio ciclotômico é $F_1(Y) = Y^{p-1} + pY^{p-2} + p$, onde $Y = X - 1$. Como esse é o polinômio minimal de ζ sobre $\mathbb{Q}$ temos que $\mathscr{N}(Y) = \mathscr{N}(\zeta - 1) = (-1)^{p-1} p$ a partir daí segue-se que $\mathscr{N}(1 - \zeta) = p$, pois $\mathscr{N}(1 - \zeta) = \mathscr{N}[-1(\zeta - 1)] = \mathscr{N}(-1)\mathscr{N}(\zeta - 1) = (-1)^{p-1}\mathscr{N}(1 - \zeta) = (-1)^{p-1}(-1)^{p-1} p = (-1)^{2(p-1)} p = p$.
Como a norma de $1 - \zeta$ é o produto dos conjugados de $1 - \zeta$, temos que:

$$p = (1 - \zeta)(1 - \zeta^2) \cdots (1 - \zeta^{p-1}) \tag{1.20}$$

Escrevendo A para o anel dos inteiros em $\mathbb{Q}[\zeta]$. *Evidentimente A contém* ζ *e suas potências. Provaremos agora que:*

$$A(1-\zeta)\cap\mathbb{Z} = p\mathbb{Z} \tag{1.21}$$

Sabemos que $p \in A$, *pela fórmula 1.20. Daí,* $A(1-\zeta)\cap\mathbb{Z} \supset p\mathbb{Z}$. *Sendo* $p\mathbb{Z}$ *ideal maximal de* $\mathbb{Z}$, *se* $A(1-\zeta)\cap\mathbb{Z} \neq p\mathbb{Z}$ *é porque* $A(1-\zeta)\cap\mathbb{Z} = \mathbb{Z}$, *isto é,* $1-\zeta$ *é uma unidade em A. Mas, neste caso os conjugados* $(1-\zeta^j)$ *de* $(1-\zeta)$ *também são unidades, segue-se da fómula 1.20 que p deve ser uma unidade em* $A\cap\mathbb{Z}$, *e assim* $p^{-1} \in \mathbb{Z}$, *o que é absurdo, pelo Exemplo 1.6. Logo,* $A(1-\zeta)\cap\mathbb{Z} = p\mathbb{Z}$. *Vamos agora mostrar que, para qualquer* $y \in A$,

$$\mathrm{Tr}(y(1-\zeta)) \in p\mathbb{Z} \tag{1.22}$$

Cada conjugado $y_j(1-\zeta^j)$ *de* $y(1-\zeta)$ *é um múltiplo em A de* $1-\zeta^j$, *o que é ele próprio um múltiplo de* $1-\zeta$, *pois* $1-\zeta^j = (1-\zeta)(1+\zeta+\cdots+\zeta^{j-1})$. *Como o traço é a soma dos conjugados, temos* $\mathrm{Tr}(y(1-\zeta)) \in A(1-\zeta)$. *Daí, a equação 1.22 segue imediatamente da equação 1.21, pois o traço de um inteiro pertence a* $\mathbb{Z}$, *pelo Corolário 1.9.*

Agora vamos determinar o anel dos inteiros em $\mathbb{Q}[\zeta]$.

Teorema 1.12 *Seja p um número primo e* ζ *uma raiz p-ésima primitiva da unidade em* $\mathbb{C}$. *Então o anel A dos inteiros do corpo ciclotômico* $\mathbb{Q}[\zeta]$ *é* $\mathbb{Z}[\zeta]$ *e* $(1,\zeta,\cdots,\zeta^{p-2})$ *é uma base do* $\mathbb{Z}$*-módulo A.*

Prova: Como $\mathbb{Z} \subset A$ e $\zeta \in A$ temos que $\mathbb{Z}[\zeta] \subseteq A$. Seja $x = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$, com $a_i \in \mathbb{Q}$, um elemento de A. Então,

$$x(1-\zeta) = a_0(1-\zeta) + a_1(\zeta-\zeta^2) + \cdots + a_{p-2}(\zeta^{p-2}-\zeta^{p-1})$$

Daí,

$$\begin{aligned}
\mathrm{Tr}[x(1-\zeta)] &= \mathrm{Tr}[a_0(1-\zeta) + a_1(\zeta-\zeta^2) + \cdots + a_{p-2}(\zeta^{p-2}-\zeta^{p-1})] \\
&= \mathrm{Tr}[a_0(1-\zeta)] + \mathrm{Tr}[a_1(\zeta-\zeta^2)] + \cdots + \mathrm{Tr}[a_{p-2}(\zeta^{p-2}-\zeta^{p-1})] \\
&= \mathrm{Tr}(a_0)\mathrm{Tr}(1-\zeta) + \mathrm{Tr}(a_1)\mathrm{Tr}(\zeta-\zeta^2) + \cdots + \mathrm{Tr}(a_{p-2})\mathrm{T}(\zeta^{p-2}-\zeta^{p-1}) \\
&= pa_0
\end{aligned}$$

Pela equação 1.22, $pa_0 \in p\mathbb{Z}$, assim $a_0 \in \mathbb{Z}$. Como $\zeta^p = 1$, temos temos $\zeta^p = \zeta\zeta^{-1}$, ou seja, $\zeta^{-1} = \zeta^{p-1}$, daí $\zeta^{-1} \in A$. Portanto, $(x-a_0)\zeta^{-1} \in A$. Logo,

$$(x-a_0)\zeta^{-1} = (a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} - a_0)\zeta^{-1} = a_1 + a_2\zeta + \cdots + a_{p-2}\zeta^{p-2} \in A$$

Usando o mesmo argumento de antes, mostra-se que $a_1 \in \mathbb{Z}$. Aplicando o mesmo argumento sucessivamente concluímos que cada $a_i \in \mathbb{Z}$, com $i = 0, \ldots, p-2$. Logo, $x \in \mathbb{Z}[\zeta]$.

Observação 1.26 *Os resultados dessa seção extende-se facilmente ao caso de corpos ciclotômicos $\mathbb{Q}[t]$ onde t é uma raiz p^r-ésima primitiva da unidade, com p primo. Um tal corpo é de grau $p^{r-1}(p-1)$ e seu anel de inteiros é $\mathbb{Z}[t]$. O polinômio minimal de t sobre $\mathbb{Q}$ é:* $X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1 = \dfrac{X^{p^r} - 1}{X^{p^{r-1}} - 1}$.

1.7 Módulos Noetherianos e alguns preliminares sobre ideais

Definição 1.30 *Um A-módulo M é chamado Noetheriano se o mesmo satisfaz as seguintes condições de equivalência:*
(a) Toda coleção não vazia de submódulos de M contém um elemento maximal;
(b) Toda sequência crescente de submódulos de M é estacionária;
(c) Todo submódulo de M é do tipo finito.
Um anel A é Noetheriano se, considerado como um A-módulo, for um módulo Noetheriano.

Observação 1.27 *Quando consideramos um anel como um A-módulo sobre si mesmo, seus submódulos são seus ideais, com isso e em virtude da condição (c), dizemos que um anel A é Noetheriano quando os seus ideais são gerados por um número finito de elementos.*

Exemplo 1.9 *Todo anel de ideais principais é Noetheriano, pelo Corolário 1.1.*

Proposição 1.16 *Seja A um anel, E um A-módulo e E' um submódulo de E. Para que E seja Noetheriano é necessário e suficiente que E' e E/E' sejam Noetherianos.*

Prova: Suponha que E seja Noetheriano. Temos que toda sequência crescente de submódulos de E' é também uma sequência crescente de submódulos de E. Sendo E Noetheriano, toda sequência crescente de submódulos de E é estacionária. Daí, toda sequência crescente de submódulos de E' é estacionária. Logo, E' é Noetheriano. Considerando o homomorfismo canônico $\sigma : E \to E/E'$, o mesmo define uma correspondêcia biunívoca que preserva a inclusão entre os submódulos de E que contém E' e os submódulos de E/E'. Logo, toda sequência crescente de submódulos de E/E', corresponde através de σ a uma sequência crescente de submódulos de E. Como toda sequência crescente de submódulos de E é estacionária, temos que toda sequência crescente de submódulos de E/E' também

é estacionária. Logo, E/E' é Noetheriano. Reciprocamente, suponha que E' e E/E' são Noetherianos. Seja $(F_n)_{n\geq 0}$ uma sequência crescente de submódulos de E. Como E' é Noetheriano, existe um inteiro n_0 tal que $F_n \cap E' = F_{n+1} \cap E'$ para todo $n \geq n_0$, pois $F_n \cap E'$ é uma sequência crescente de submódulos de E'. Como E/E' é Noetheriano, existe um inteiro n_1 tal que $(F_n + E')/E' = (F_{n+1} + E')/E'$ para todo $n \geq n_1$, pois $(F_n + E')/E'$ é uma sequência crescente de submódulos de E/E'. Logo, $F_n + E' = F_{n+1} + E'$ para todo $n \geq n_1$. Tome $n \geq \sup(n_0, n_1)$. Mostraremos que $F_n = F_{n+1}$, para isto, é suficiente mostrar que $F_{n+1} \subset F_n$, pois $F_n \subset F_{n+1}$, já que $(F_n)_{n\geq 0}$ é crescente. De fato, seja $x \in F_{n+1}$, como $F_n + E' = F_{n+1} + E'$ temos que existem $y \in F_n$ e $y', y'' \in E'$ tais que $x + y' = y + y''$. Assim, $x - y = y'' - y' \in F_{n+1} \cap E' = F_n \cap E'$, pois $y'' - y' \in E'$ e como $x - y \in F_{n+1}$. Como $x - y$ e y pertencem a F_n temos que $(x-y)+y \in F_n$, isto é, $x \in F_n$. Logo, $F_{n+1} \subset F_n$. Portanto, $F_n = F_{n+1}$ para todo $n \geq \sup(n_0, n_1)$. Logo, E é Noetheriano.

Corolário 1.11 *Seja A um anel e sejam $E_1, \ldots, E_n$ A-módulos Noetherianos. Então o A-módulo produto $\prod_{i=1}^{n} E_i$ é Noetheriano.*

Prova: Faremos indução sobre n. Para $n = 1$ a afirmação é verdadeira, pois E_1 é Noetheriano. Suponha que a afirmação é verdadeira para $n-1$, com $n \geq 2$. Temos que $(E_1 \times \cdots \times E_n)/E_n$ é isomorfo a $E_1 \times \cdots \times E_{n-1}$ que é Noetheriano por hipótese. Logo, pela Proposição 1.16 temos que $E_1 \times \cdots \times E_n$ é Noetheriano.

Corolário 1.12 *Sejam A um anel Noetheriano e E um A-módulo do tipo finito. Então E é um módulo Noetheriano e portanto todos os seus submódulos são do tipo finito.*

Prova: Seja $E = Ax_1 + \cdots + Ax_n$ e $\varphi : A^n \to E$ um homomorfismo dado por $\varphi(a_1, \ldots, a_n) = \sum_{i=1}^{n} a_i x_i$. Assim, $A^n/\ker\varphi$ é isomorfo a E. Como A é Noetheriano, pelo Corolário 1.11 temos que $A^n = A \times \cdots \times A$ é Noetheriano. Assim, pela Proposição 1.16 temos que $A^n/\ker\varphi$ é Noetheriano. Logo, E é Noetheriano.

Definição 1.31 *Um ideal $\mathfrak{p}$ de um anel A é chamado primo se o quociente $A/\mathfrak{p}$ for um domínio de integridade. Equivalentemente, se $x, y \in A - \mathfrak{p}$ então $xy \in A - \mathfrak{p}$, isto é, $A - \mathfrak{p}$ é fechado para a multiplicação.*

Definição 1.32 *Um ideal $\mathfrak{q}$ de um anel A é chamado maximal se o quociente $A/\mathfrak{q}$ for um corpo. Equivalentemente, se para todo ideal $\mathfrak{p}$ de A tal que $\mathfrak{q} \subseteq \mathfrak{p} \subseteq A$ implicar que $\mathfrak{q} = \mathfrak{p}$ ou $\mathfrak{p} = A$.*

Observação 1.28 *Todo ideal maximal é primo. A recíproca é falsa, pois o ideal* (0) *de* $\mathbb{Z}$ *é primo, mas não é maximal.*

Lema 1.9 *Seja A um anel,* $\mathfrak{p}$ *um ideal primo de A e* A' *um subanel de A. Então* $\mathfrak{p} \cap A'$ *é um ideal primo de* A'.

Prova: Seja $\varphi : A' \to A$ a aplicação de inclusão e $\sigma : A \to A/\mathfrak{p}$ o homomorfismo canônico. Assim, a composta $\phi = \sigma \circ \varphi : A' \to A/\mathfrak{p}$ é um homomorfismo tal que $\ker = \{a' \in A' \mid \phi(a') = 0\} = \{a' \in A' \mid a' + \mathfrak{p} = 0 + \mathfrak{p}\} = \{a' \in A' \mid a' \in \mathfrak{p}\}$. Assim, $\ker\phi = A' \cap \mathfrak{p}$. Pelo teorema dos homomorfismos de anéis temos que $A'/A' \cap \mathfrak{p} \simeq \mathrm{Im}\phi$. Logo, $A'/A' \cap \mathfrak{p}$ é um subanel de $A/\mathfrak{p}$. Como $\mathfrak{p}$ é um ideal primo então $A/\mathfrak{p}$ é um D.I. Como um subanel de um D.I. é também um D.I. temos que $A'/A' \cap \mathfrak{p}$ é um D.I. e daí $A' \cap \mathfrak{p}$ é um ideal primo.

Definição 1.33 *Dados dois ideais* $\mathfrak{a}$ *e* $\mathfrak{b}$ *de um anel A, definimos o produto de* $\mathfrak{a}$ *e* $\mathfrak{b}$ *como o conjunto de todas as somas finitas* $\sum_{i=1}^{n} a_i b_i$ *de produtos de elementos de* $\mathfrak{a}$ *por elementos de* $\mathfrak{b}$, *isto é,* $\mathfrak{ab} = \left\{ \sum_{i=1}^{n} a_i b_i \mid n > 0,\ a_i \in \mathfrak{a} \ \ e \ \ b_i \in \mathfrak{b} \right\}$.

Observação 1.29 *É claro que* $\mathfrak{ab}$ *é um ideal de A. Além disso,* $\mathfrak{ab} \subset \mathfrak{a}$ *e* $\mathfrak{ab} \subset \mathfrak{b}$ *e daí* $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$, *mas nem sempre* $\mathfrak{ab} = \mathfrak{a} \cap \mathfrak{b}$, *para que ocorra a igualdade é necessário que* $\mathfrak{a} + \mathfrak{b} = A$.

Observação 1.30 *A multiplicação de ideais é associativa e comutativa. De fato, se* $\mathfrak{p}_1, \mathfrak{p}_2$ *e* $\mathfrak{p}_3$ *são ideais de um anel A, então*

$$\begin{aligned}
(\mathfrak{p}_1\mathfrak{p}_2)\mathfrak{p}_3 &= \left\{ \sum_{i=1}^{n} (a_i b_i) c_i \mid n > 0,\ a_i \in \mathfrak{p}_1, b_i \in \mathfrak{p}_2, c_i \in \mathfrak{p}_3 \right\} \\
(\mathfrak{p}_1\mathfrak{p}_2)\mathfrak{p}_3 &= \left\{ \sum_{i=1}^{n} a_i (b_i c_i) \mid n > 0,\ a_i \in \mathfrak{p}_1, b_i \in \mathfrak{p}_2, c_i \in \mathfrak{p}_3 \right\} \\
(\mathfrak{p}_1\mathfrak{p}_2)\mathfrak{p}_3 &= \mathfrak{p}_1(\mathfrak{p}_2\mathfrak{p}_3)
\end{aligned}$$

e

$$\begin{aligned}
\mathfrak{p}_1\mathfrak{p}_2 &= \left\{ \sum_{i=1}^{n} a_i b_i \mid n > 0,\ a_i \in \mathfrak{p}_1, b_i \in \mathfrak{p}_2 \right\} \\
\mathfrak{p}_1\mathfrak{p}_2 &= \left\{ \sum_{i=1}^{n} b_i a_i \mid n > 0,\ b_i \in \mathfrak{p}_2, a_i \in \mathfrak{p}_1 \right\} \\
\mathfrak{p}_1\mathfrak{p}_2 &= \mathfrak{p}_2\mathfrak{p}_1
\end{aligned}$$

Dado um A-módulo E, um submódulo F e um ideal $\mathfrak{p}$ *de A, definimos analogamente o produto de* $\mathfrak{p}F$. *Este é um submódulo de E.*

Lema 1.10 *Se um ideal primo* $\mathfrak{p}$ *de um anel A contém um produto* $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ *de ideais, então* $\mathfrak{p}$ *contém pelo menos um dos ideais* $\mathfrak{a}_i$.

Prova: Suponha por absurdo que $\mathfrak{a}_i \nsubseteq \mathfrak{p}$ para todo i. Assim, existe $x_i \in \mathfrak{a}_i - \mathfrak{p}$ para todo i. Logo, $x_1 x_2 \cdots x_n \notin \mathfrak{p}$, pois $\mathfrak{p}$ é primo. Mas, $x_1 x_2 \ldots x_n \in \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_n \subset \mathfrak{p}$ o que é absurdo. Portanto, $\mathfrak{p}$ contém pelo menos um dos ideais $\mathfrak{a}_i$.

Lema 1.11 *Em um anel Noetheriano todo ideal contém um produto de ideais primos. Em um domínio de integridade Noetheriano A todo ideal não nulo contém um produto de ideais primos não nulos.*

Prova: Suponha por absurdo que a família ϕ dos ideais não nulos de A que não contém um produto de ideais primos não nulos é não vazia. Como A é Noetheriano, ϕ contém um elemento maximal $\mathfrak{q}$. O ideal $\mathfrak{q}$ não pode ser primo, pois caso contrário $\mathfrak{q}$ não pertenceria a ϕ. Assim, existem $x, y \in A - \mathfrak{q}$ tais que $xy \in \mathfrak{q}$. Os ideais $\mathfrak{q} + Ax$ e $\mathfrak{q} + Ay$ contém $\mathfrak{q}$ como um subconjunto próprio, pois $x \in \mathfrak{q} + Ax$ e $x \notin \mathfrak{q}$, $y \in \mathfrak{q} + Ay$ e $y \notin \mathfrak{q}$. Como $\mathfrak{q}$ é um elemento maximal da família ϕ, temos que os ideais $\mathfrak{q} + Ax$ e $\mathfrak{q} + Ay$ não pertencem a ϕ. Logo, estes ideais contém produto de ideais primos não nulos $\mathfrak{p}_1 \cdots \mathfrak{p}_n \subset \mathfrak{q} + Ax$ e $\mathfrak{p}'_1 \cdots \mathfrak{p}'_n \subset \mathfrak{q} + Ay$ como $xy \in \mathfrak{q}$, então $(\mathfrak{q} + Ax)(\mathfrak{q} + Ay) \subset \mathfrak{q}$. Logo, $\mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{p}'_1 \cdots \mathfrak{p}'_n \subset \mathfrak{q}$ o que é absurdo, pois $\mathfrak{q} \in \phi$. Portanto, ϕ é vazia. Agora seja A um domínio de integridade e $\mathbb{K}$ seu corpo de frações. Chamamos qualquer A-submódulo $\mathfrak{a}$ de $\mathbb{K}$ para o qual existe $d \in A - (0)$ tal que $d\mathfrak{a} \subset A$, um ideal fracionário de A ou de $\mathbb{K}$ com respeito a A. Isso significa que os elementos de $\mathfrak{a}$ tem um denominador comum $d \in A$. Os ideais ordinários de A são ideais fracionários com $d = 1$. As vezes os chamamos de ideais inteiros para distingui-los dos ideais fracionários. Qualquer A-submódulo $\mathfrak{a}$ do tipo finito contido em $\mathbb{K}$ é um ideal fracionário. Isto segue do fato que se $\{x_1, \ldots, x_n\}$ é um conjunto de geradores de $\mathfrak{a}$, os x_i's tem um denominador comum d (o produto dos denominadores d_i's onde $x_i = a_i d_i^{-1}$ com $a_i, d_i \in A$) e d é um denominador comum para $\mathfrak{a}$. Reciprocamente, se A é Noetheriano, todo ideal fracionário $\mathfrak{a}$ é um A-módulo do tipo finito, pois $\mathfrak{a} \subset d^{-1}A$ e $d^{-1}A$ é um A-módulo isomorfo a A. Como A é Noetheriano, todo submódulo de A é do tipo finito. Logo, $\mathfrak{a}$ é do tipo finito.

Definição 1.34 *Definimos o produto* $\mathfrak{p}\mathfrak{p}'$ *de dois ideais fracionários* $\mathfrak{p}$ *e* $\mathfrak{p}'$ *como o conjunto das somas finitas* $\sum x_i y_i$ *onde* $x_i \in \mathfrak{p}$ *e* $y_i \in \mathfrak{p}'$.

Observação 1.31 *Se* $\mathfrak{p}$ *e* $\mathfrak{p}'$ *são ideais fracionários com denominadores comum d e* d' *respectivamente, então os conjuntos* $\mathfrak{p} \cap \mathfrak{p}', \mathfrak{p} + \mathfrak{p}'$ *e* $\mathfrak{p}\mathfrak{p}'$ *são todos ideais fracionários. Eles*

são claramente A-submódulos de $\mathbb{K}$ e tem como denominador comum d ou d', $d+d'$ e dd' respectivamente. Os ideais fracionários não nulos de A constituem um monoíde comutativo sobre a multiplicação, isto é, um semigrupo comutativo com unidade.

1.8 Anéis de Dedekind e norma de um ideal

Definição 1.35 *Um domínio de integridade A é chamado um anel de Dedekind se o mesmo é Noetheriano e integralmente fechado, e se todo ideal primo não nulo de A for maximal.*

Exemplo 1.10 *Qualquer anel de ideais principais é um anel de Dedekind, pois o mesmo é Noetheriano, integralmente fechado e todos ideal primo não nulo seu é maximal.*

Teorema 1.13 *Seja A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$, e A' o fecho inteiro de A em $\mathbb{L}$. Assuma que $\mathbb{K}$ tem característica zero. Então A' é um anel de Dedekind e um A-módulo do tipo finito.*

Prova: O anel A' é integralmente fechado por construção, é Notheriano e um A-módulo do tipo finito pela Proposição 1.16. Resta mostrar que todo ideal primo $\mathfrak{p}' \neq (0)$ de A' é maximal. Para isso escolha um elemento $x \in \mathfrak{p}' - (0)$ e considere uma equação de dependência inteira de x sobre A, que possui menor grau possível.

$$X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0 = 0, \text{ com } a_i \in A \tag{1.23}$$

Assim, $a_0 \neq 0$, caso contrário x satisfaz uma equação de dependência inteira de grau menor que n. Pela equação 1.23 temos que $a_0 \in A'x \cap A \subset \mathfrak{p}' \cap A$, pois $a_0 = -x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)$. Portanto, $\mathfrak{p}' \cap A \neq (0)$. Como $\mathfrak{p}' \cap A$ é um ideal primo de A pelo Lema 1.9, temos que $\mathfrak{p}' \cap A$ é um ideal maximal de A, pois A é de Dedekind. Portanto, $A/\mathfrak{p}' \cap A$ é um corpo. Mas, $A/\mathfrak{p}' \cap A$ pode ser indentificado como um subanel de $A'/\mathfrak{p}'$ e este é inteiro sobre $A/\mathfrak{p}' \cap A$, pois A' é inteiro sobre A. Assim, $A'/\mathfrak{p}'$ é um corpo pela Proposição 1.6. Logo, $\mathfrak{p}'$ é maximal.

Teorema 1.14 *Seja A um anel de Dedekind que não é um corpo. Todo ideal maximal de A é invertível no monoíde de ideais fracionários de A, isto é, se $\mathfrak{a}$ é um ideal maximal de A existe um ideal fracionário $\mathfrak{a}'$ de A tal que $\mathfrak{a}'\mathfrak{a} = A$*

Prova: Seja $\mathfrak{a}$ um ideal maximal de A. Então $\mathfrak{a} \neq (0)$, pois A não é um corpo. Ponha

$$\mathfrak{a}' = \{x \in \mathbb{K} \mid x\mathfrak{a} \subset A\} \tag{1.24}$$

Claramente, $\mathfrak{a}'$ é um A-submódulo de $\mathbb{K}$, qualquer elemento não nulo de $\mathfrak{a}$ serve como um denominador comum para os elementos de M'. Assim, $\mathfrak{a}'$ é um ideal fracionário de A. É suficiente mostrar que $\mathfrak{a}'\mathfrak{a} = A$. Pela equação 1.24 temos que $\mathfrak{a}'\mathfrak{a} \subset A$, por outro lado, $A \subset \mathfrak{a}'$, pois sendo $\mathfrak{a}$ um ideal maximal de A, dado $a \in A$, $a\mathfrak{a} \subset \mathfrak{a} \subset A \Rightarrow a \in \mathfrak{a}'$. Assim, $\mathfrak{a} = A\mathfrak{a} \subset \mathfrak{a}'\mathfrak{a}$. Como $\mathfrak{a}$ é maximal e $\mathfrak{a} \subset \mathfrak{a}'\mathfrak{a} \subset A$ então $\mathfrak{a} = \mathfrak{a}'\mathfrak{a}$ ou $\mathfrak{a}'\mathfrak{a} = A$. Daí, resta mostrar que $\mathfrak{a} = \mathfrak{a}'\mathfrak{a}$ não pode ocorrer. Se $\mathfrak{a}'\mathfrak{a} = \mathfrak{a}$ e $x \in \mathfrak{a}'$ então $x\mathfrak{a} \subset \mathfrak{a}$, $x^2\mathfrak{a} \subset x\mathfrak{a} \subset \mathfrak{a}$ e $x^n\mathfrak{a} \subset \mathfrak{a}$ para qualquer $n \in \mathbb{N}$, por indução. Assim, qualquer elemento não nulo $d \in \mathfrak{a}$ é um denominador cumum para todas as potências x^n de x, $n \in \mathbb{N}$. Segue-se que $A[x]$ é um ideal fracionário de A. Como A é Noetheriano, $A[x]$ é um A-módulo do tipo finito, assim x é inteiro sobre A pelo Teorema 1.7. Mas, A é integralmente fechado, portanto $x \in A$ e consequentemente $\mathfrak{a}'\mathfrak{a} = \mathfrak{a}$ implica $\mathfrak{a}' = A$. Daí, resta mostrar que $\mathfrak{a}' = A$ não pode ocorrer, para isso, tome um elemento não nulo $a \in \mathfrak{a}$. O ideal Aa contém um produto de ideais primos não nulos $\mathfrak{p}_1 \cdots \mathfrak{p}_n$ pelo Lema 1.11. Podemos tomar n como o menor possível. Daí, temos $\mathfrak{a} \supset Aa \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n$ isto significa que $\mathfrak{a} \supset \mathfrak{p}_1$ para algum i pelo Lema 1.10, digamos $i = 1$. Como $\mathfrak{p}_1$ é maximal, pois A é de Dedekind, temos que $\mathfrak{a} = \mathfrak{p}_1$. Ponha $\mathfrak{q} = \mathfrak{p}_2 \cdots \mathfrak{p}_n$, daí $Aa \supset \mathfrak{a}\mathfrak{q}$ e $Aa \not\supseteq \mathfrak{q}$, pois n é o menor possível. Assim, existe $b \in \mathfrak{q}$ tal que $b \notin Aa$. Como $\mathfrak{a}\mathfrak{q} \subset Aa$ temos que $\mathfrak{a}b \subset Aa$ e consequentemente $\mathfrak{a}ba^{-1} \subset A$. De acordo com a definição de $\mathfrak{a}'$, isso significa que $ba^{-1} \in \mathfrak{a}'$. Mas, como $b \notin Aa$ temos que $ba^{-1} \notin A$. Assim, $\mathfrak{a}' \neq A$ e consequentemente $\mathfrak{a}'\mathfrak{a} \neq \mathfrak{a}$. Logo, $\mathfrak{a}'\mathfrak{a} = A$ como queríamos provar.

Teorema 1.15 *Seja A um anel de Dedekind e* P *um conjunto de ideais primos não nulos de A. Então:*
(a) Todo ideal fracionário não nulo $\mathfrak{q}$ de A, pode ser unicamente expresso na forma:

$$\mathfrak{q} = \prod_{\mathfrak{a} \in \mathrm{P}} \mathfrak{a}^{n_p(\mathfrak{q})}$$

onde, para qualquer $\mathfrak{a} \in$ P, $n_p(\mathfrak{q}) \in \mathbb{Z}$ e para quase todo $\mathfrak{a} \in$ P, $n_p(\mathfrak{q}) = 0$
(b) O monoíde dos ideais fracionários não nulos de A é um grupo.

Prova: Primeiro provaremos a existência de (a), isto é, que qualquer ideal fracionário $\mathfrak{q}$ é um produto de potências (≥ 0 ou ≤ 0) de ideais primos. Existe $d \in A - (0)$ tal que $d\mathfrak{q} \subset A$, isto é, tal que $d\mathfrak{q}$ é um inteiro de A, $\mathfrak{q} = (d\mathfrak{q})(Ad)^{-1}$. Sem perda de generalidade, podemos provar (a) para ideais inteiros. Prosseguindo como no Lema 1.11, considere a coleção ϕ dos ideais não nulos em A que não são produto de ideais primos. Suponha que ϕ não é vazia. Como A é Noetheriano, ϕ possui um elemento maximal $\mathfrak{p}$. Então $\mathfrak{p} \neq A$, pois A é produto da coleção vazia de ideais primos. Assim, $\mathfrak{p}$ está contido em um ideal maximal $\mathfrak{a}$, que é um elemento maximal na coleção de ideais não triviais de A que contém $\mathfrak{p}$. Seja $\mathfrak{a}'$ o ideal fracionário inverso de $\mathfrak{a}$. Como $\mathfrak{p} \subset \mathfrak{a}$ temos que $\mathfrak{p}\mathfrak{a}' \subset \mathfrak{a}\mathfrak{a}' = A$. Como $\mathfrak{a}' \supset A$ temos que $\mathfrak{p}\mathfrak{a}' \supset \mathfrak{p}$. De fato, $\mathfrak{p}\mathfrak{a}' \neq \mathfrak{p}$, pois se $\mathfrak{p}\mathfrak{a}' = \mathfrak{p}$

e $x \in \mathfrak{a}'$ então $x\mathfrak{p} \subset \mathfrak{p}$, $x^n \subset \mathfrak{p}$ para todo n, x é inteiro sobre A e $x \in A$. Mas, isso é impossível, pois $\mathfrak{a}' \neq A$, caso contrário teríamos $\mathfrak{a}' = A$ e $\mathfrak{a}\mathfrak{a}' = \mathfrak{a}$. Pela maximalidade de $\mathfrak{p}$ em ϕ, temos que $\mathfrak{p}\mathfrak{a}' \notin \phi$, assim $\mathfrak{p}\mathfrak{a}' = \mathfrak{a}_1 \cdots \mathfrak{a}_n$. Multiplicando por $\mathfrak{a}$ temos que $\mathfrak{p} = \mathfrak{a}\mathfrak{a}_1 \cdots \mathfrak{a}_n$ o que é absurdo, pois $\mathfrak{p} \in \phi$. Logo, todo ideal inteiro de A é produto de ideais primos. Provaremos agora a unicidade em (a). Suponha que $\prod_{\mathfrak{a}\in \mathrm{P}} \mathfrak{a}^{n(\mathfrak{p})} = \prod_{\mathfrak{a}\in \mathrm{P}} \mathfrak{a}^{\mathrm{m}(\mathfrak{p})}$, isto é, $\prod_{\mathfrak{p}\in \mathrm{P}} \mathfrak{a}^{n(p)-m(p)} = A$. Se $n(p) - m(p) \neq 0$ para algum ideal primo $\mathfrak{a} \in \mathrm{P}$, podemos separar os expoentes positivos e negativos e escrever

$$\mathfrak{a}_1^{\alpha_1} \cdots \mathfrak{a}_r^{\alpha_r} = \mathfrak{a}'^{s_1}_1 \cdots \mathfrak{a}'^{s_k}_k$$

onde $\mathfrak{a}_i, \mathfrak{a}'_j \in \mathrm{P}$, $\alpha_i > 0$ e $\beta_j > 0$, $\mathfrak{a}_i \neq \mathfrak{a}'_j$ para todo i e j. Assim, $\mathfrak{a}_1$ contém $\mathfrak{a}'^{\beta_1}_1 \cdots \mathfrak{a}'^{\beta_k}_k$ pelo Lema 1.11, daí $\mathfrak{a}_1 \supset \mathfrak{a}'_j$, digamos $\mathfrak{a}_1 \supset \mathfrak{a}'_1$. Mas, $\mathfrak{a}_1$ e $\mathfrak{a}'_1$ são ambos maximais, o que implica que $\mathfrak{a}_1 = \mathfrak{a}'_1$, o que é uma contradição, pois $\mathfrak{a}_i \neq \mathfrak{a}'_j$ para todo i e j. Finalmente, temos que $\prod_{\mathfrak{a}\in \mathrm{P}} \mathfrak{a}^{-n_p(\mathfrak{q})}$ é o inverso de $\prod_{\mathfrak{a}\in \mathrm{P}} \mathfrak{a}^{n_p(\mathfrak{q})}$ e isto prova (b).

Observação 1.32 *Temos abaixo algumas fórmulas as quais $n_p(\mathfrak{q})$ denota o expoente de $\mathfrak{a}$ na fatoração de $\mathfrak{q}$ em um produto de ideais primos. Veja:*

$$\begin{gathered}
n_p(\mathfrak{p}\mathfrak{q}) = n_p(\mathfrak{p}) + n_p(\mathfrak{q}) \\
\mathfrak{q} \subset A \Leftrightarrow n_p(\mathfrak{p}) \geq n_p(\mathfrak{q}), \ \forall \ \mathfrak{a} \in \mathrm{P} \\
\mathfrak{p} \subset \mathfrak{q} \Leftrightarrow n_p(\mathfrak{p}) \geq n_p(\mathfrak{q}), \ \forall \ \mathfrak{a} \in \mathrm{P} \\
n_p(\mathfrak{p} + \mathfrak{q}) = \inf\{n_p(\mathfrak{p}), n_p(\mathfrak{q})\} \\
n_p(\mathfrak{p} \cap \mathfrak{q} = \sup\{n_p(\mathfrak{p}), n_p(\mathfrak{q})\}
\end{gathered} \tag{1.25}$$

Observação 1.33 *As vezes escrevemos $\mathscr{N}(x)$ no lugar de $\mathscr{N}_{\mathbb{K}/\mathbb{Q}}(x)$.*

Proposição 1.17 *Seja $\mathbb{K}$ um corpo numérico, n seu grau e A o anel dos inteiros de $\mathbb{K}$. Se x é um elemento não nulo de A, então $|\mathscr{N}(x)| = card(A/Ax)$.*

Prova: Sabemos que A é um $\mathbb{Z}$-módulo livre de posto n e Ax é um $\mathbb{Z}$-submódulo de A, também de posto n, pois a multiplicação por x implica A em Ax isomorficamente. Pelo Teorema 1.3 existe uma base $\{e_1, \ldots, e_n\}$ do $\mathbb{Z}$-módulo A e elementos c_i de $\mathbb{N}$ tais que $\{c_1e_1, \ldots, c_ne_n\}$ é uma base de Ax. Além disso, o grupo abeliano A/Ax é isomorfo ao grupo abeliano finito $\prod_{i=1}^{n} \mathbb{Z}/c_i\mathbb{Z}$, cuja ordem é $c_1 \cdots c_n$. Escreva u para a aplicação $\mathbb{Z}$-linear de A em Ax definida por $u(e_i) = c_ie_i$ para $i = 1, \ldots, n$. Temos que $\det(u) = c_1 \cdots c_n$, por outro lado, $\{xe_1, \ldots, xe_n\}$ é também uma base para Ax. Existe assim um automorfismo ν do $\mathbb{Z}$-módulo Ax tal que $\nu(c_ie_i) =$

xe_i. Então $\det(v)$ é invertível em $\mathbb{Z}$, portanto $\det(v) = \pm 1$. Mas, vu é uma multiplicação por x, e seu determinante é, por definição, $\mathscr{N}(x)$. Como $\det(vu) = \det(v)\det(u)$ podemos concluir que $\mathscr{N}(x) = \pm c_1 \cdots c_n = \pm \text{card}(A/Ax)$.

Definição 1.36 *Dado um ideal inteiro não nulo $\mathfrak{p}$ de A, chamamos o número card$(A/\mathfrak{p})$ a norma de $\mathfrak{p}$ é denotada por $\mathscr{N}(\mathfrak{p})$.*

Observação 1.34 *Note que $\mathscr{N}(\mathfrak{p})$ é finita. De fato, se x é um elemento não nulo de $\mathfrak{p}$ então $Ax \subset \mathfrak{p}$ e $A/\mathfrak{p}$ pode ser identificado com um quociente de A/Ax. Assim, card$(A/\mathfrak{p}) \leq$ card(A/Ax), que é finita pela Proposição 1.17. Por outro lado, vemos que para um ideal principal Ay temos $\mathscr{N}(Ay) = |\mathscr{N}(y)|$.*

Proposição 1.18 *Seja $\mathbb{K}$ um corpo numérico, n seu grau e A o anel dos inteiros de $\mathbb{K}$. Se $\mathfrak{p}$ e $\mathfrak{q}$ são ieais inteiros não nulos de A, então $\mathscr{N}(\mathfrak{pq}) = \mathscr{N}(\mathfrak{p})\mathscr{N}(\mathfrak{q})$.*

Prova: O ideal $\mathfrak{q}$ se fatora em um produto de ideais maximais pelo Teorema 1.15, daí é suficiente mostrar que $\mathscr{N}(\mathfrak{pb}) = \mathscr{N}(\mathfrak{p})\mathscr{N}(\mathfrak{b})$ para $\mathfrak{b}$ maximal. Como $\mathfrak{pb} \subset \mathfrak{p}$ temos $\text{card}(\mathfrak{p}/\mathfrak{pb}) = \text{card}(A/\mathfrak{b})$. Agora $\mathfrak{p}/\mathfrak{pb}$ pode ser considerado como um espaço vetorial sobre $A/\mathfrak{b}$. Seus subespaços são seus A-submódulos, eles são da forma $\mathfrak{a}'/\mathfrak{pb}$ onde $\mathfrak{a}'$ é um ideal tal que $\mathfrak{pb} \subset \mathfrak{a}' \subset \mathfrak{p}$. Mas, a fórmula 1.25 implica que não existem ideais entre $\mathfrak{pb}$ e $\mathfrak{p}$. Portanto, o espaço vetorial $\mathfrak{p}/\mathfrak{pb}$ é de dimensão 1 sobre $A/\mathfrak{b}$. Logo, temos que $\text{card}(\mathfrak{p}/\mathfrak{pb}) = \text{card}(A/\mathfrak{b})$.

Capítulo 2

Reticulados

Conteúdo

2.1 Subgrupos discretos do $\mathbb{R}^n$

As demonstrações feitas nesta seção foram baseadas em [Samuel 2008]

Definição 2.1 *Um subgrupo $\mathscr{H}$ de $\mathbb{R}^n$ é discreto se, e somente se, para todo subconjunto compacto K de $\mathbb{R}^n$, a interseção $\mathscr{H} \cap K$ é um conjunto finito.*

Exemplo 2.1 *$\mathbb{Z}^n$ é um subgrupo discreto de $\mathbb{R}^n$.*

Teorema 2.1 *Seja $\mathscr{H}$ um subgrupo discreto de $\mathbb{R}^n$, então $\mathscr{H}$ é gerado, como um $\mathbb{Z}$-módulo, por r vetores linearmente independentes sobre $\mathbb{R}$, com $r \leq n$.*

Prova: Seja $\{e_1,\ldots,e_r\}$ o conjunto dos elementos de $\mathscr{H}$ que são linearmente independentes sobre $\mathbb{R}$, onde r é o maior possível $(r \leq n)$. Considere

$$\mathscr{P} = \left\{ x \in \mathbb{R}^n \mid x = \sum_{i=1}^{r} \alpha_i e_i,\ 0 \leq \alpha_i \leq 1 \right\} \tag{2.1}$$

o paralelepípedo construído com esses vetores. Temos que $\mathscr{P}$ é compacto. Assim, $\mathscr{P} \cap \mathscr{H}$ é finito, pois $\mathscr{H}$ é discreto. Tome $x \in \mathscr{H}$. Pela maximalidade do conjunto $\{e_1,\ldots,e_r\}$, segue que:

$$x = \sum_{i=1}^{r} \lambda_i e_i$$

Pois, se x não fosse combinação linear dos vetores e_i's então $\{e_1,\ldots,e_r,x\}$ seriam L.I., o que contraria a maximalidade de r. Para $j \in \mathbb{Z}$, defina:

$$x_j = jx - \sum_{i=1}^{r} [j\lambda_i] e_i, \tag{2.2}$$

onde $[\mu]$ denota o maior inteiro menor ou igual a $\mu \in \mathbb{R}$. Assim,

$$\begin{aligned} x_j &= j\left(\sum_{i=1}^{r} \lambda_i e_i\right) - \sum_{i=1}^{r} [j\lambda_i] e_i \\ x_j &= \sum_{i=1}^{r} j\lambda_i e_i - \sum_{i=1}^{r} [j\lambda_i] e_i \end{aligned}$$

Logo,

$$x_j = \sum_{i=1}^{r} \left(j\lambda_i - [j\lambda_i]\right) e_i \tag{2.3}$$

Como

i. $j\lambda_i \geq [j\lambda_i] \Rightarrow j\lambda_i - [j\lambda_i] \geq 0$

ii. $j\lambda_i < [j\lambda_i] + 1 \Rightarrow j\lambda_i - [j\lambda_i] < 1$

segue que $x_j \in \mathscr{P}$. Por outro lado, pela equação 2.2, temos que $x_j \in \mathscr{H}$. Daí, $x_j \in \mathscr{P} \cap \mathscr{H}$. Fazendo $j = 1$ em 2.2, temos que:

$$x_1 = x - \sum_{i=1}^{r} [\lambda_i] e_i \Rightarrow x = x_1 + \sum_{i=1}^{r} [\lambda_i] e_i$$

Assim, o $\mathbb{Z}$-módulo $\mathscr{H}$ é gerado por $\mathscr{P} \cap \mathscr{H}$ e daí é do tipo finito. Por outro lado, como $x_j \in \mathscr{P} \cap \mathscr{H}$, $\mathscr{P} \cap \mathscr{H}$ é finito e $\mathbb{Z}$ é infinito, então existem inteiros distintos j e k tais que

$x_j = x_k$. Logo, pela equação 2.3, temos:

$$\begin{aligned}\sum_{i=1}^{r}(j\lambda_i - [j\lambda_i])e_i &= \sum_{i=1}^{r}(k\lambda_i - [k\lambda_i])e_i \\ \sum_{i=1}^{r}(j\lambda_i - k\lambda_i)e_i &= \sum_{i=1}^{r}([j\lambda_i] - [k\lambda_i])e_i\end{aligned}$$

Assim,

$$\sum_{i=1}^{r}(j\lambda_i - k\lambda_i - [j\lambda_i] + [k\lambda_i])e_i = 0$$

Sendo os e_i's linearmente independentes, temos:

$$j\lambda_i - k\lambda_i - [j\lambda_i] + [k\lambda_i] = 0$$

isto é,

$$(j-k)\lambda_i = [j\lambda_i] - [k\lambda_i]$$

Dessa forma, os λ_i's são racionais. Logo, o $\mathbb{Z}$-módulo $\mathscr{H}$ é gerado por um número finito de elementos, que são combinações lineares de e_i's com coeficientes racionais. Seja $d \in \mathbb{Z} - (0)$ o denominador comum desses coeficientes. É válido que:

$$d\mathscr{H} \subset \sum_{i=1}^{r}\mathbb{Z}e_i$$

De fato, se $a \in d\mathscr{H}$, então existem $\mu_1, \ldots, \mu_r \in \mathbb{Q}$, tais que:

$$a = d(\mu_1 e_1 + \cdots + \mu_r e_r)$$

Daí, existem $a_i, b_i \in \mathbb{Z}$, com $i = 1, \ldots, r$ de modo que:

$$a = d\left(\frac{a_1}{b_1}e_1 + \cdots + \frac{a_r}{b_r}e_r\right)$$

Como d é o denominador comum, temos que $d = b_1 \ldots b_r$
Desta Forma,

$$\begin{aligned}a &= b_1 \ldots b_r\left(\frac{a_1}{b_1}e_1 + \cdots + \frac{a_r}{b_r}e_r\right) \\ a &= b_2 \cdots_r a_1 e_1 + b_1 b_3 \cdots_r a_2 e_2 + \cdots + b_1 b_2 \cdots_{r-1} a_r e_r\end{aligned}$$

Logo,

$$a \in \sum_{i=1}^{r} \mathbb{Z}e_i$$

Concluímos que existe uma base $\{f_i\}_{i=1,\ldots,r}$ do $\mathbb{Z}$-módulo $\sum_{i=1}^{r} \mathbb{Z}e_i$ e inteiros α_i, com $i = 1,\ldots,r$, tal que $\{\alpha_1 f_1,\ldots,\alpha_r f_r\}$ gera $d\mathscr{H}$, pelo Teorema 1.3. Como o $\mathbb{Z}$-módulo $d\mathscr{H}$ possui o mesmo posto que $\mathscr{H}$ e além disso $\mathscr{H} \supset \sum_{i=1}^{r} \mathbb{Z}e_i$, então o posto de $d\mathscr{H}$ é maior ou igual a r. Pela maximalidade de r decorre que o posto de $d\mathscr{H}$ é r e os α_i's são não-nulo, pois caso contrário $d\mathscr{H}$ não teria posto. Daí, os f_i's são linearmente independentes sobre $\mathbb{R}$. Portanto, o módulo $d\mathscr{H}$ e consequentemente $\mathscr{H}$, é gerado, sobre $\mathbb{Z}$, pelos r vetores linearmente independentes sobre $\mathbb{R}$.

Definição 2.2 *Um subgrupo discreto de $\mathbb{R}^n$, de posto n, é chamado um reticulado em $\mathbb{R}^n$.*

Observação 2.1 *Pelo Teorema 2.1, um reticulado é gerado sobre $\mathbb{Z}$ por uma base de $\mathbb{R}^n$, que é então uma $\mathbb{Z}$-base para o dado reticulado. Para cada $\mathbb{Z}$-base $\alpha = \{e_1,\ldots,e_r\}$ de um reticulado $\mathscr{H}$ escrevemos $\mathscr{P}_\alpha$ para o paralelepípedo semi-aberto*

$$\mathscr{P}_\alpha = \left\{ x \in \mathbb{R}^n; x = \sum_{i=1}^{r} \alpha_i e_i, 0 \leq \alpha_i \leq 1 \right\}.$$

Vamos denotar por μ a medida de Lebesgue em $\mathbb{R}^n$, isto é, se S é um subconjunto mensurável de $\mathbb{R}^n$, $\mu(S)$ é a sua medida, que também pode ser chamado seu volume.

Definição 2.3 *Seja $\mathscr{H} \subset \mathbb{R}^n$ um reticulado, com $\mathbb{Z}$-base $\alpha = \{e_1,\ldots,e_r\}$. O conjunto*

$$\mathscr{P}_\alpha = \left\{ x \in \mathbb{R}^n; x = \sum_{i=1}^{r} \alpha_i e_i, 0 \leq \alpha_i \leq 1 \right\}$$

é chamado de região fundamental de $\mathscr{H}$, com relação a base $\alpha = \{e_1,\ldots,e_r\}$.

Definição 2.4 *Sejam $\mathscr{H} \subset \mathbb{R}^n$ um reticulado e $v = \{v_1,\ldots,v_n\}$ uma base de $\mathscr{H}$. Se $v_i = (v_{i1},\ldots,v_{in})$ para $i = 1,\ldots,n$, chamamos de matriz geradora do reticulado $\mathscr{H}$ a matriz*

$$(A_{ij}) = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix}$$

A matriz $(B_{ij}) = (A_{ij})(A_{ij})^t$, onde t denota a transposta, é chamada de matriz de Gram do reticulado.

Exemplo 2.2 *$\mathscr{H} = \mathbb{Z}^2$ é um reticulado gerado pelos vetores $e_1 = (1,0)$ e $e_2 = (0,1)$, com região fundamental descrita na figura abaixo.*

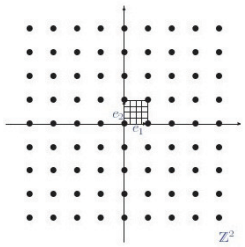


Figura 1: Região fundamental de $\mathbb{Z}^2$

Exemplo 2.3 *$\mathscr{H} = \mathbb{Z}^3$ é um reticulado gerado pelos vetores $e_1 = (1,0,0)$, $e_2 = (0,1,0)$ e $e_3 = (0,0,1)$, com região fundamental descrita pela figura abaixo.*

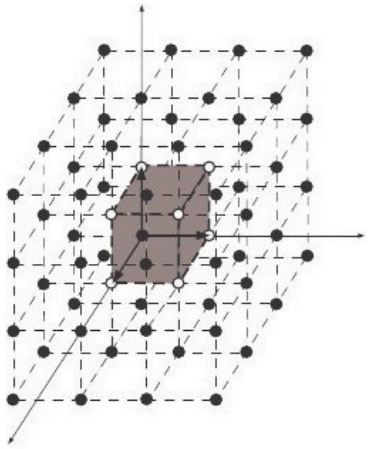


Figura 2: Região fundamental de $\mathbb{Z}^3$

Lema 2.1 *O volume $\mu(\mathscr{P}_e)$ é independente da base $e = \{e_1, \ldots, e_n\}$ escolhida para $\mathscr{H}$.*

Prova: Seja $f = \{f_1, \ldots, f_n\}$ uma base para $\mathscr{H}$. Então $f_i = \sum_{i=1}^{n} \alpha_{ij} e_j$, com $\alpha_{ij} \in \mathbb{Z}$. Assim, $\mu(\mathscr{P}_f) = |\det(\alpha_{ij})| \mu(\mathscr{P}_e)$ (resultado do cálculo de volume em análise). A matriz (α_{ij}), sendo associada a uma mudança de base, é invertível (resultado de álgebra linear). Logo, $\det(\alpha_{ij})$ é também invertível. Como (α_{ij}) é uma matriz inteira, então seu determinante é um número inteiro. Logo, $\det(\alpha_{ij}) = \pm 1$, pois os únicos inteiros inversíveis são 1 e -1. Portanto, $\mu(\mathscr{P}_f) = 1.\mu(\mathscr{P}_e)$, isto é, $\mu(\mathscr{P}_f) = \mu(\mathscr{P}_e)$.

Observação 2.2 *O volume do paralelepípedo $\mathscr{P}_e$ associado à base e de $\mathscr{H}$ é chamado o volume do reticulado $\mathscr{H}$ e é denotado por $Vol(\mathscr{H})$.*

Teorema 2.2 (Minkowski) *Seja $\mathscr{H}$ um reticulado em $\mathbb{R}^n$ e seja S um subconjunto mensurável de $\mathbb{R}^n$ tal que $\mu(S) > Vol(\mathscr{H})$. Então, existem dois pontos distintos x, $y \in S$ tal que $x - y \in \mathscr{H}$*

Prova: Seja $e = \{e_1, \ldots, e_n\}$ uma $\mathbb{Z}$-base de $\mathscr{H}$ e $\mathscr{P}_e$ o paralelepípedo associado a e. Como $\mathscr{P}_e$ é um domínio fundamental para $\mathscr{H}$, ou seja, todo ponto de $\mathbb{R}^n$ é congruente $\mod \mathscr{H}$ a um e somente um ponto de $\mathscr{P}_e$, então

$$\mathbb{R}^n = \bigcup_{h \in \mathscr{H}} (h + \mathscr{P}_e)$$

Como

$$S = S \cap \mathbb{R}^n = S \cap \left(\bigcup_{h \in \mathscr{H}} (h + \mathscr{P}_e) \right) = \bigcup_{h \in \mathscr{H}} S[\cap (h + \mathscr{P}_e)]$$

Daí,

$$\mu(s) = \mu \left(\bigcup_{h \in \mathscr{H}} S[\cap (h + \mathscr{P}_e)] \right) = \sum_{h \in \mathscr{H}} \mu[S \cap (h + \mathscr{P}_e)] \tag{2.4}$$

Como μ é translação invariante,

$$\mu[S \cap (h + \mathscr{P}_e)] = \mu[(-h + S) \cap \mathscr{P}_e]$$

Os conjuntos $(-h + S) \cap \mathscr{P}_e$, com $h \in \mathscr{H}$, não pode ser dois a dois disjuntos, caso contrário $\mu(\mathscr{P}_e) \geq \sum_{h \in \mathscr{H}} \mu(-h + S) \cap \mathscr{P}_e$ o que contraria a equação 2.4 e a hipótese $\mu(\mathscr{P}_e) = Vol(\mathscr{H}) < \mu(S)$. Consequentemente, exite dois elementos distintos h e h' de $\mathscr{H}$ tal que $-h + x = -h' + y$. Então, $x - y = h - h' \in \mathscr{H}$ e $x \neq y$, assim $h \neq h'$.

Corolário 2.1 *Seja $\mathscr{H}$ um reticulado em $\mathbb{R}^n$ e S um subconjunto mensurável de $\mathbb{R}^n$ que é simétrico em relação a origem e convexo. Assuma que S satisfaz as seguintes condições:*
(a) $\mu(S) > 2^n Vol(\mathscr{H})$
(b) $\mu(S) \geq 2^n Vol(\mathscr{H})$ e S é compacto.
Então, $S \cap (\mathscr{H} - \{0\}) \neq \emptyset$.

Prova: No caso (a) apliquemos o Teorema 2.2 para o conjunto $S' = \frac{1}{2}S$ onde $\mu(S') = 2^{-n}\mu(S) > Vol(\mathscr{H})$. Seja y e z pontos distintos de S', tal que $(y - z) \in \mathscr{H}$. Então $y - z$ também pertence a S, $y - z = \frac{1}{2}[2y + (-2z)]$ e S é simétrico em relação a origem e convexo. Portanto, $(y - z) \in S \cap (\mathscr{H} - \{0\})$.

Para provar o caso (b) usaremos o caso (a) para $(1+\varepsilon)S$ para $\varepsilon > 0$. Então, $(\mathscr{H} - \{0\}) \cap (1+\varepsilon)S$ é um conjunto não vazio compacto, isto é, finito, pois é compacto e discreto. Além disso, $\bigcap_{\varepsilon>0} [(\mathscr{H} - \{0\}) \cap (1+\varepsilon)S] \neq \emptyset$. Como essa interseção é não vazia, temos que os conjuntos compactos alinhados nunca se anulam. Isto siginifica que existe um ponto de $\mathscr{H} - \{0\}$ que pertencem a $(1+\varepsilon)S$ para todo $\varepsilon > 0$. Logo, como S é compacto, o ponto de $\mathscr{H} - \{0\}$ pertencem a S também.

2.2 A imersão canônica de um corpo numérico

As demonstrações feitas nessa seção foram baseadas em [Samuel 2008]

Seja $\mathbb{K}$ um corpo numérico de grau n (corpo extensão de $\mathbb{Q}$ de grau n). Vimos na seção 1.4 pelo Teorema 1.8 que existem exatamente n isomorfismos distintos $\sigma_i : \mathbb{K} \to \mathbb{C}$. Seja $\alpha : \mathbb{C} \to \mathbb{C}$ a conjugação complexa. Então, para cada $i = 1, \ldots, n$, temos que $\alpha \circ \sigma_i = \sigma_j$, $1 \leq j \leq n$ e $\sigma_i = \sigma_j$ se e somente se $\sigma_i(\mathbb{K}) \subset \mathbb{R}$.

Veja que:

$$\alpha \circ \sigma_i = \overline{\sigma_i} \Rightarrow \alpha(\alpha \circ \sigma_i) = \alpha(\overline{\sigma_i}) \Rightarrow \overline{\alpha \circ \sigma_i} = \overline{\overline{\sigma_i}} \Rightarrow \overline{\alpha \circ \sigma_i} = \sigma_i$$

Assim, os monomorfismos complexos ocorrem em pares complexos conjugados. Escreva r_1 para o número de índices tal que $\sigma_i(\mathbb{K}) \subset \mathbb{R}$. Então, $n - r_1$ é um número par. Logo, podemos escrever:

$$n - r_1 = 2r_2 \Rightarrow r_1 + 2r_2 = n$$

Vamos reenumerar os σ_i' s de modo que $\sigma_i(\mathbb{K}) \subset \mathbb{R}$, para $1 \leq i \leq r_1$ e tal que $\sigma_{j+r_2}(x) = \overline{\sigma_j(x)}$, para $r_1 + 1 \leq j \leq r_1 + r_2$. Assim, os primeiros $r_1 + r_2$ isomorfismos determinam os últimos r_2. Para $x \in \mathbb{K}$, defina:

$$\sigma(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_{r_1+r_2}(x))$$

Chamamos σ a imersão canônica de $\mathbb{K}$ em $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, isto é um homomorfismo injetivo de anéis, e vamos identificar $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ com $\mathbb{R}^n$.

Proposição 2.1 *Se M é um $\mathbb{Z}$-submódulo livre de $\mathbb{K}$ de posto n e se $(x_i)_{1\leq i\leq n}$ é uma $\mathbb{Z}$-base de M, então $\sigma(M)$ é um reticulado em $\mathbb{R}^n$, cujo volume é*

$$Vol(\sigma(M)) = 2^{-r_2} |\det_{1\leq j,i\leq n} (\sigma_j(x_i))|$$

Prova: Para i fixado, as coordenadas de $\sigma_i(x_i)$ com respeito a base canônica de $\mathbb{R}^n$ são:

$$\sigma_1(x_i),\ldots,\sigma_{r_1}(x_i),R(\sigma_{r_1+1}(x_i)),I(\sigma_{r_1+1}(x_i)),\ldots,R(\sigma_{r_1+r_2}(x_i)),I(\sigma_{r_1+r_2}(x_i)), \tag{2.5}$$

onde R e I denota respectivamente o número real e imaginário. Vamos calcular o determinante D da matriz cuja i-ésima coluna é dada por 2.5.

$$D=\begin{vmatrix}
\sigma_1(x_1) & \cdots & \sigma_1(x_i) & \cdots & \sigma_1(x_n)\\
\sigma_2(x_1) & \cdots & \sigma_2(x_i) & \cdots & \sigma_2(x_n)\\
\vdots & \ddots & \vdots & \ddots & \vdots\\
\sigma_{r_1}(x_1) & \cdots & \sigma_{r_1}(x_i) & \cdots & \sigma_{r_1}(x_n)\\
R(\sigma_{r_1+1}(x_1)) & \cdots & R(\sigma_{r_1+1}(x_i)) & \cdots & R(\sigma_{r_1+1}(x_n))\\
I(\sigma_{r_1+1}(x_1)) & \cdots & I(\sigma_{r_1+1}(x_i)) & \cdots & I(\sigma_{r_1+1}(x_n))\\
\vdots & \ddots & \vdots & \ddots & \vdots\\
R(\sigma_{r_1+r_2}(x_1)) & \cdots & R(\sigma_{r_1+r_2}(x_i)) & \cdots & R(\sigma_{r_1+r_2}(x_n))\\
I(\sigma_{r_1+r_2}(x_1)) & \cdots & I(\sigma_{r_1+r_2}(x_i)) & \cdots & I(\sigma_{r_1+r_2}(x_n))
\end{vmatrix}$$

Usando as fórmulas $R(z)=\dfrac{1}{2}(z+\overline{z})$ e $I(z)=\dfrac{1}{2i}(z-\overline{z})$, $z\in\mathbb{C}$, temos:

$$D=\begin{vmatrix}
\sigma_1(x_1) & \cdots & \sigma_1(x_i) & \cdots & \sigma_1(x_n)\\
\sigma_2(x_1) & \cdots & \sigma_2(x_i) & \cdots & \sigma_2(x_n)\\
\vdots & \ddots & \vdots & \ddots & \vdots\\
\sigma_{r_1}(x_1) & \cdots & \sigma_{r_1}(x_i) & \cdots & \sigma_{r_1}(x_n)\\
\frac{1}{2}(\sigma_{r_1+1}(x_1)+\overline{\sigma_{r_1+1}(x_1)}) & \cdots & \frac{1}{2}(\sigma_{r_1+1}(x_i)+\overline{\sigma_{r_1+1}(x_i)}) & \cdots & \frac{1}{2}(\sigma_{r_1+1}(x_n)+\overline{\sigma_{r_1+1}(x_n)})\\
\frac{1}{2i}(\sigma_{r_1+1}(x_1)-\overline{\sigma_{r_1+1}(x_1)}) & \cdots & \frac{1}{2i}(\sigma_{r_1+1}(x_i)-\overline{\sigma_{r_1+1}(x_i)}) & \cdots & \frac{1}{2i}(\sigma_{r_1+1}(x_n)-\overline{\sigma_{r_1+1}(x_n)})\\
\vdots & \ddots & \vdots & \ddots & \vdots\\
\frac{1}{2}(\sigma_{r_1+r_2}(x_1)+\overline{\sigma_{r_1+r_2}(x_1)}) & \cdots & \frac{1}{2}(\sigma_{r_1+r_2}(x_i)+\overline{\sigma_{r_1+r_2}(x_i)}) & \cdots & \frac{1}{2}(\sigma_{r_1+r_2}(x_n)+\overline{\sigma_{r_1+r_2}(x_n)})\\
\frac{1}{2i}(\sigma_{r_1+r_2}(x_1)-\overline{\sigma_{r_1+r_2}(x_1)}) & \cdots & \frac{1}{2i}(\sigma_{r_1+r_2}(x_i)-\overline{\sigma_{r_1+r_2}(x_i)}) & \cdots & \frac{1}{2i}(\sigma_{r_1+r_2}(x_n)-\overline{\sigma_{r_1+r_2}(x_n)})
\end{vmatrix}$$

$$D = \left(\frac{1}{2}\right)^{r_2}\left(\frac{1}{2i}\right)^{r_2}\begin{vmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_i) & \cdots & \sigma_1(x_n) \\ \sigma_2(x_1) & \cdots & \sigma_2(x_i) & \cdots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \cdots & \sigma_{r_1}(x_i) & \cdots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1)+\overline{\sigma_{r_1+1}(x_1)} & \cdots & \sigma_{r_1+1}(x_i)+\overline{\sigma_{r_1+1}(x_i)} & \cdots & \sigma_{r_1+1}(x_n)+\overline{\sigma_{r_1+1}(x_n)} \\ \sigma_{r_1+1}(x_1)-\overline{\sigma_{r_1+1}(x_1)} & \cdots & \sigma_{r_1+1}(x_i)-\overline{\sigma_{r_1+1}(x_i)} & \cdots & \sigma_{r_1+1}(x_n)-\overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1)+\overline{\sigma_{r_1+r_2}(x_1)} & \cdots & \sigma_{r_1+r_2}(x_i)+\overline{\sigma_{r_1+r_2}(x_i)} & \cdots & \sigma_{r_1+r_2}(x_n)+\overline{\sigma_{r_1+r_2}(x_n)} \\ \sigma_{r_1+r_2}(x_1)-\overline{\sigma_{r_1+r_2}(x_1)} & \cdots & \sigma_{r_1+r_2}(x_i)-\overline{\sigma_{r_1+r_2}(x_i)} & \cdots & \sigma_{r_1+r_2}(x_n)-\overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}$$

$$D = \left(\frac{1}{2}\right)^{r_2}\left(\frac{1}{2i}\right)^{r_2}\begin{vmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_i) & \cdots & \sigma_1(x_n) \\ \sigma_2(x_1) & \cdots & \sigma_2(x_i) & \cdots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \cdots & \sigma_{r_1}(x_i) & \cdots & \sigma_{r_1}(x_n) \\ 2\sigma_{r_1+1}(x_1) & \cdots & 2\sigma_{r_1+1}(x_i) & \cdots & 2\sigma_{r_1+1}(x_n) \\ \sigma_{r_1+1}(x_1)-\overline{\sigma_{r_1+1}(x_1)} & \cdots & \sigma_{r_1+1}(x_i)-\overline{\sigma_{r_1+1}(x_i)} & \cdots & \sigma_{r_1+1}(x_n)-\overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 2\sigma_{r_1+r_2}(x_1) & \cdots & 2\sigma_{r_1+r_2}(x_i) & \cdots & 2\sigma_{r_1+r_2}(x_n) \\ \sigma_{r_1+r_2}(x_1)-\overline{\sigma_{r_1+r_2}(x_1)} & \cdots & \sigma_{r_1+r_2}(x_i)-\overline{\sigma_{r_1+r_2}(x_i)} & \cdots & \sigma_{r_1+r_2}(x_n)-\overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}$$

$$D = \frac{1}{2^{r_2}}\frac{1}{(2i)^{r_2}}2^{r_2} = (2i)^{-r_2}\begin{vmatrix} \sigma_1(x_1) & \cdots & \sigma_1(x_i) & \cdots & \sigma_1(x_n) \\ \sigma_2(x_1) & \cdots & \sigma_2(x_i) & \cdots & \sigma_2(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1}(x_1) & \cdots & \sigma_{r_1}(x_i) & \cdots & \sigma_{r_1}(x_n) \\ \sigma_{r_1+1}(x_1) & \cdots & \sigma_{r_1+1}(x_i) & \cdots & \sigma_{r_1+1}(x_n) \\ \overline{\sigma_{r_1+1}(x_1)} & \cdots & \overline{\sigma_{r_1+1}(x_i)} & \cdots & \overline{\sigma_{r_1+1}(x_n)} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r_1+r_2}(x_1) & \cdots & \sigma_{r_1+r_2}(x_i) & \cdots & \sigma_{r_1+r_2}(x_n) \\ \overline{\sigma_{r_1+r_2}(x_1)} & \cdots & \overline{\sigma_{r_1+r_2}(x_i)} & \cdots & \overline{\sigma_{r_1+r_2}(x_n)} \end{vmatrix}$$

Assim, obtemos $D = (2i)^{-r_2} \det_{1\leq j,i\leq n}(\sigma_j(x_i))$. Como os x_i's formam uma base para $\mathbb{K}$ sobre $\mathbb{Q}$, pela Proposição 1.15 temos que $\det(\sigma_j(x_i)) \neq 0$ e portanto $D \neq 0$. Daí, os vetores $\sigma(x_i)$ são linearmente independentes em $\mathbb{R}^n$ e geram $\sigma(M)$, ou seja, $\sigma(M)$ é um reticulado do $\mathbb{R}^n$. Do fato de $(x_1,\ldots,x_n)$ ser uma $\mathbb{Z}$-base de M, temos $m = \sum_{i=1}^{n} a_i x_i$, com $a_i \in \mathbb{Z}$, para todo $m \in M$. Assim, $\sigma(M) = \sum_{i=1}^{n} \sigma(a_i x_i) = \sum_{i=1}^{n} a_i \sigma(x_i)$, com $a_i \in \mathbb{Z}$, ou seja, $\sigma(M) = \left\{ \sum_{i=1}^{n} a_i \sigma(x_i) \mid a_i \in \mathbb{Z} \right\}$. Daí,

$$Vol(\sigma(M)) = |D| = |(2i)^{-r_2} \det_{1\leq j,i\leq n} \sigma_j(x_i)| = 2^{-r_2} |\det_{1\leq j,i\leq n} \sigma_j(x_i)|.$$

Logo, $Vol(\sigma(M)) = 2^{-r_2} |\det_{1\leq j,i\leq n} \sigma_j(x_i)|$.

Proposição 2.2 *Seja d o discriminante absoluto de $\mathbb{K}$, A o anel dos inteiros de $\mathbb{K}$ e $\mathfrak{p}$ o ideal inteiro não nulo de A. Então, $\sigma(A)$ e $\sigma(\mathfrak{p})$ são reticulados, com respectivos volumes,*

$$Vol(\sigma(A)) = 2^{-r_2}|d|^{\frac{1}{2}},\ Vol(\sigma(\mathfrak{p})) = 2^{-r_2}|d|^{\frac{1}{2}}\mathcal{N}(\mathfrak{p}).$$

Prova: Sabemos que A e $\mathfrak{p}$ são $\mathbb{Z}$-módulos livres de posto n. Assim, pela proposição 2.1 temos que $\sigma(\mathfrak{p})$ e $\sigma(A)$ são reticulados do $\mathbb{R}^n$ e que $Vol(\sigma(A)) = 2^{-r_2}|\det \sigma_i(x_j)|_{1\leq i,j\leq n}$, onde $\{x_1,\ldots,x_n\}$ é uma $\mathbb{Z}$-base de A. Pela Proposição 1.15, $d = \det(\sigma_i(x_j))^2$ e daí $|d|^{\frac{1}{2}} = |\det \sigma_i(x_j)|$, portanto $Vol(\sigma(A)) = 2^{-r_2}|d|^{\frac{1}{2}}$. Para a segunda fórmula, temos que $\sigma(\mathfrak{p})$ é um subgrupo de $\sigma(A)$ de índice $\mathcal{N}(\mathfrak{p})$ (pela definição 1 da seção 5 do capítulo 3), uma vez que $A/\mathfrak{p}$ é isomorfo a $\sigma(A)/\sigma(\mathfrak{p})$. Além disso, como um domínio fundamental de $\sigma(\mathfrak{p})$ é a união disjunta de $\mathcal{N}(\mathfrak{p})$ cópias de um domínio fundamental de $\sigma(A)$, segue-se que $Vol(\sigma(\mathfrak{p})) = 2^{-r_2}|d|^{\frac{1}{2}}\mathcal{N}(\mathfrak{p})$. Logo,

$$Vol(\sigma(A)) = 2^{-r_2}|d|^{\frac{1}{2}} \text{ e } Vol(\sigma(\mathfrak{p})) = 2^{-r_2}|d|^{\frac{1}{2}}\mathcal{N}(\mathfrak{p}).$$

Exemplo 2.4 *Se $\mathbb{K} = \mathbb{Q}(\zeta_5)$, onde $\zeta_5 = e^{\frac{2\pi i}{5}}$, então seu anel dos inteiros é $\mathbb{Z}[\zeta_5]$ e $\{1,\zeta_5\}$ é uma $\mathbb{Z}$-base. Como $\mathbb{K}$ é totalmente imaginário, segue que $r_2 = 1$, e assim*

$$\begin{aligned} Vol(\sigma_{\mathbb{K}}(\mathbb{Z}[\zeta_5])) &= \frac{1}{2}\left|\det\begin{pmatrix} \sigma_1(1) & \sigma_1(\zeta_5) \\ \sigma_2(1) & \sigma_2(\zeta_5) \end{pmatrix}\right| \\ &= \frac{1}{2}\left|\begin{pmatrix} 1 & \zeta_5 \\ 1 & \overline{\zeta_5} \end{pmatrix}\right| = \frac{1}{2}\left|-\frac{1}{2} - \frac{i\sqrt{5}}{2} - \left(-\frac{1}{2} + \frac{i\sqrt{5}}{2}\right)\right| = \frac{1}{2}\sqrt{5} \end{aligned}$$

Portanto, a imagem do homomorfismo canônico $\sigma_{\mathbb{K}}(\mathbb{Z}[\sqrt{5}])$ é um reticulado de posto 4, cujo volume é $\dfrac{\sqrt{5}}{2}$.

Os exemplos das seções a seguir foram baseados em [Ferrari 2008. 105f], [Alves 2005. 125f] e [Naves 2009. 88f]

2.3 Empacotamento esférico

O problema clássico de empacotamento esférico consiste em encontrar um arranjo de esferas idênticas no espaço Euclidiano n - dimensional de forma que a fração do espaço coberto por essas esferas seja a maior possível. Ao estudar a densidade de empacotamento, um dos principais problemas é a obtenção de reticulados com alta densidade e que sejam ao mesmo tempo manipuláveis. Para que possamos prosseguir no estudo de reticulados, precisamos da noção de volume.

O volume no $\mathbb{R}^n$ é bem conhecido e pode ser facilmente transferido para o $\mathbb{R}$ - espaço V n - dimensional através do isomorfismo natural entre $\mathbb{R}^n$ e V , e definido por meio de uma base $\{v_1,\ldots,v_n\}$. Além disso, é possível restringir a subconjuntos C de V que são reuniões finitas da região fundamental, usando apenas as seguintes propriedades de volume:
(a) $Vol(x+C) = Vol(C),\ \forall\ x \in V$
(b) $Vol(yC) = y^n Vol(C),\ \forall\ y \in \mathbb{R},\ y > 0$
(c) Se $C \cap C' = \emptyset$ então $Vol(C \cup C') = Vol(C) + Vol(C')$, onde C' também é um subconjunto de V.

Definição 2.5 *Sejam $\mathscr{H} \subseteq \mathbb{R}^n$ um reticulado, $\alpha = \{v_1,\ldots,v_n\}$ uma base de $\mathscr{H}$ e $\mathscr{P}_\alpha$ a região fundamental. Se $v_i = (v_{i1},\ldots,v_{in})$ para $i = 1,\ldots,n$, definimos o volume da região fundamental $\mathscr{P}_\alpha$, como o módulo do determinante da matriz*

$$\begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix}$$

Definição 2.6 *Sejam $\mathscr{H} \subseteq \mathbb{R}^n$ um reticulado e $v = \{v_1,\ldots,v_n\}$ uma base de $\mathscr{H}$, onde $v_i = \{v_{i1},\ldots,v_{in}\}$ para $i = 1,\ldots,n$. Definimos o discriminante do reticulado $\mathscr{H}$ por $Disc(\mathscr{H}) =$*

$(\det B_{ij})^2$, *onde*

$$B_{ij} = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{n1} & v_{n2} & \cdots & v_{nn} \end{pmatrix}$$

Exemplo 2.5 *Seja* $\mathscr{H} \subseteq \mathbb{R}^3$ *um reticulado,* $\beta = \{(1,1,2),(0,3,1),(-1,3,2)\}$ *uma base de* $\mathscr{H}$ *e* $\mathscr{P}_\beta$ *a região fundamental. Assim,*

$$Vol(\mathscr{P}_\beta) = \begin{vmatrix} 1 & 1 & 2 \\ 0 & 3 & 1 \\ -1 & 3 & 2 \end{vmatrix} = |-4| = 4$$

Definição 2.7 *Seja* $\mathscr{H} \subseteq \mathbb{R}^n$ *um reticulado com base* $\alpha = \{v_1, \ldots, v_n\}$. *Definimos o volume do reticulado* $\mathscr{H}$ *como sendo o volume da região fundamental* $\mathscr{P}_\alpha$, *isto é,* $Vol(\mathscr{H}) = Vol(\mathscr{P}_\alpha)$

Definição 2.8 *Um empacotamento esférico, ou simplesmente um empacotamento no* $\mathbb{R}^n$, *é uma distribuição de esferas de mesmo raio no* $\mathbb{R}^n$ *de forma que a intersecção de quaisquer duas esferas tenha no máximo um ponto. Pode-se descrever um empacotamento indicando apenas o conjunto dos centros das esferas e o raio.*

Definição 2.9 *Um empacotamento reticulado é um empacotamento em que o conjunto dos centros das esferas formam um reticulado* $\mathscr{H}$ *de* $\mathbb{R}^n$.

Exemplo 2.6 $\mathscr{H} = \mathbb{Z}^2$ *é um reticulado gerado pelos vetores* $e_1 = (1,0)$ *e* $e_2 = (0,1)$, *com região fundamental P e uma translação* $P + l$ *descrita na figura abaixo.*

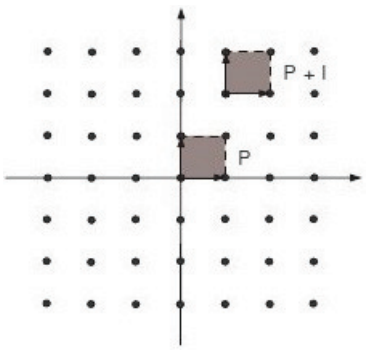


Figura 3: Uma translação de $\mathbb{Z}^2$

Definição 2.10 *Dado um empacotamento no $\mathbb{R}^n$, associado a um reticulado $\mathscr{H}$ com $v = \{v_1, \ldots, v_n\}$ uma $\mathbb{Z}$-base, definimos a sua densidade de empacotamento como sendo a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas.*

Exemplo 2.7 *Empacotamento do reticulado $\mathscr{H} = \mathbb{Z}^2$.*
Veja:

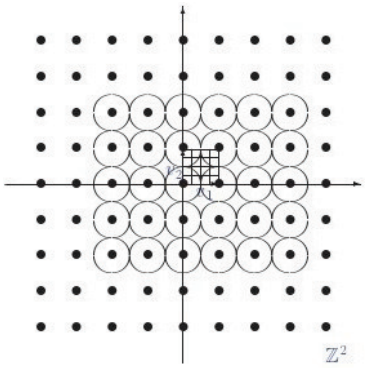


Figura 4: Empacotamento de $\mathbb{Z}^2$

Observação 2.3 *No empacotamento associado a um reticulado $\mathscr{H}$ em que as esferas tenham raio máximo. Para determinação deste raio, observamos que, fixado $k > 0$, a intersecção do conjunto compacto $\{x \in \mathbb{R}^n \mid |x| \leq k\}$, como o reticulado $\mathscr{H}$ é um conjunto finito, de onde segue que o número $Dist_{\min}(\mathscr{H}) = \min\{|\lambda| \mid \lambda \in \mathscr{H},\ \lambda \neq 0\}$ está bem definido e $(Dist_{\min}(\mathscr{H}))^2$ é chamado de norma mínima. Observamos que $\rho = Dist_{\min}(\mathscr{H})/2$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de $\mathscr{H}$ e obter um empacotamento, assim ρ é chamado raio de empacotamento do reticulado. Dessa forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados. Denotando por $\mathscr{B}(\rho)$ a esfera com centro na origem e raio ρ, temos que a densidade de empacotamento de $\mathscr{H}$ é igual a*

$$\Delta(\mathscr{H}) = \frac{\textit{Volume de uma esfera de raio } \rho}{\textit{Volume do reticulado}} = \frac{Vol(\mathscr{B}(\rho))}{Vol(\mathscr{H})} = \frac{Vol(\mathscr{B}(1))\rho^n}{Vol(\mathscr{H})}$$

pois, sendo $\mathscr{B}(\rho)$ uma esfera em $\mathbb{R}^n$ com centro na origem e raio ρ, sabemos que seu volume é dado por $Vol(\mathscr{B}(\rho)) = Vol(\mathscr{B}(1))\rho^n$. Portanto, o problema se reduz ao estudo de um outro parâmetro, chamado de densidade de centro, que é dado por

$$\delta(\mathscr{H}) = \frac{\rho^n}{Vol(\mathscr{H})}$$

Logo, temos a seguinte relação

$$\Delta(\mathscr{H}) = Vol(\mathscr{B}(1))\delta(\mathscr{H})$$

ou seja, a densidade de empacotamente de $\mathscr{H}$ é igual ao produto entre o volume da esfera com centro na origem e raio 1 e a densidade de centro $\delta(\mathscr{H})$.

Exemplo 2.8 *Se $\mathscr{H} = \mathbb{Z}^2$, com base $\beta = \{(2,0),(1,1)\}$, então $\rho = \sqrt{2}/2$, $Vol(\mathscr{B}(1)) = \pi$ e o volume do reticulado é dado por*

$$Vol(\mathscr{H}) = \begin{vmatrix} 2 & 0 \\ 1 & 1 \end{vmatrix} = 2$$

e a densidade de centro é $\delta(\mathscr{H}) = \frac{1}{4}$. Logo, a densidade de empacotamento é dada por

$$\Delta(\mathscr{H}) = \frac{\pi}{4}.$$

Exemplo 2.9 *Se $\mathscr{H} \subset \mathbb{Z}^3$, com base $\beta = \{(4,0,0),(0,3,0),(0,2,1)\}$, então $\rho = \sqrt{5}/2$, $Vol(\mathscr{B}(1)) = \frac{4\pi}{3}$ e o volume do reticulado é dado por*

$$Vol(\mathscr{H}) = \begin{vmatrix} 4 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 2 & 1 \end{vmatrix} = 12$$

e a densidade de centro é $\delta(\mathscr{H}) = \frac{5\sqrt{5}}{96}$. Logo, a densidade de empacotamento é dada por

$$\Delta(\mathscr{H}) = \frac{5\pi\sqrt{5}}{72}.$$

2.4 Alguns reticulados e suas propriedades

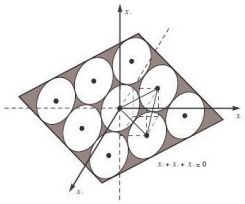
Nesta seção apresentamos as definições de reticulados conhecidos na literatura e que possuem densidade de centro boas. Além disso, é provado que essas densidades são as melhores até a dimensão 8. Em dimensões maiores que 8, existem reticulados com densidades de centro ótimas (K_{12} e Λ_{24}), e existem reticulados com densidades de centro recordes, mas não se sabe se essas densidades são boas.

Definição 2.11 (Reticulado n - dimensional A_n) *Para todo $n \geq 1$, temos que $A_n = \{(x_0,\ldots,x_n) \in \mathbb{Z}^{n+1} \mid x_0 + \cdots + x_n = 0\}$ é um reticulado. Assim, por definição, A_n está contido no hiperplano $\sum_{i=0}^{n} x_i = 0$ e possui uma matriz geradora M, dada por*

$$\begin{pmatrix} -1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & -1 & 1 & \cdots & 0 & 0 \\ 0 & 0 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & 1 \end{pmatrix}$$

onde, o raio de empacotamento é dado por $\rho = \sqrt{2}/2$ *e a densidade de centro é* $\delta = 2^{-n/2}(n+1)^{-1/2}$.

Exemplo 2.10 *Reticulado* 2 *- dimensional* A_2. *O reticulado* A_2 *é formado por todos os pontos* (x_0, x_1, x_2) *de* $\mathbb{Z}^3$ *que pertencem ao plano* $x_0 + x_1 + x_2 = 0$, *contido em* R^3. *A figura mostra a*



disposição dos pontos do reticulado no espaço tridimensional, assim como o empacotamento associado. O raio de empacotamento é dado por $\rho = \sqrt{2}/2$ *e a densidade de centro é* $\delta = 1/2\sqrt{3} = 0,28868$, *que é a densidade de centro máxima para dimensão* 2.

Definição 2.12 (Reticulado n **- dimensional** D_n**)** *Para todo* $n \geq 3$, *temos que* $D_n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n \mid x_1 + \cdots + x_n \text{ é par}\}$ *é um reticulado. Possui uma matriz geradora M, dada por*

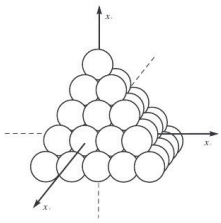
$$\begin{pmatrix} -1 & -1 & 0 & \cdots & 0 & 0 \\ 1 & -1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & -1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & -1 \end{pmatrix}$$

onde, o raio de empacotamento é dado por $\rho = \sqrt{2}/2$ *e a densidade de centro é* $\delta = 2^{-(n+2)/2}$.

Exemplo 2.11 *Reticulado* 3 *- dimensional* D_3. *O reticulado* D_3 *é formado por todos os pontos* $(x_1, x_2, x_3) \in \mathbb{Z}^3$ *tal que* $x_1 + x_2 + x_3$ *é um número par. Uma matriz geradora para* D_3 *é dada por*

$$\begin{pmatrix} -1 & -1 & 0 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix}$$

A figura abaixo mostra o arranjo das esferas do empacotamento associado a D_3.



O raio de empacotamento é dado por $\rho = \sqrt{2}/2$ *e a densidade de centro máxima para dimensão* 3 *é* $\delta = 1/4\sqrt{3} = 0,17678$.

Exemplo 2.12 *Reticulado* 4 *- dimensional* D_4. *O reticulado* D_4 *é formado por todos os pontos* $(x_1,x_2,x_3,x_4) \in \mathbb{Z}^4$ *tal que* $x_1+x_2+x_3+x_4$ *é um número par. Uma matriz geradora para* D_4 *é dada por*

$$\begin{pmatrix} -1 & -1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & -1 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

O raio de empacotamento é dado por $\rho = \sqrt{2}/2$ *e a densidade de centro é* $\delta = 1/8 = 0,125$, *que é a densidade de centro máxima para dimensão* 4.

Exemplo 2.13 *Reticulado* 5 *- dimensional* D_5. *O reticulado* D_5 *é formado por todos os pontos* $(x_1,x_2,x_3,x_4,x_5) \in \mathbb{Z}^5$ *tal que* $x_1+x_2+x_3+x_4+x_5$ *é um número par. Uma matriz geradora para* D_5 *é dada por*

$$\begin{pmatrix} -1 & -1 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 & 0 \\ 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

O raio de empacotamento é dado por $\rho = \sqrt{2}/2$ *e a densidade de centro é* $\delta = 1/8\sqrt{2} = 0,8839$*, que é a densidade de centro máxima para dimensão* 5.

Definição 2.13 (Reticulado 8 **- dimensional** E_8**)** *O reticulado* E_8 *é definido por*

$$E_8 = \left\{ (x_0, \ldots, x_8) \in \mathbb{R}^8 \mid \forall\, x_i \in \mathbb{Z} \text{ ou } x_i \in \mathbb{Z} + \frac{1}{2}, \sum x_i \equiv 0 \mod 2 \right\}$$

Uma matriz geradora para este reticulado é dada por

$$\begin{pmatrix} 2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 & 1/2 \end{pmatrix}$$

O raio de empacotamento é dado por $\rho = \sqrt{2}/2$ *e a densidade de centro é* $\delta = 1/16 = 0,06250$*, que é a densidade de centro máxima para dimensão* 8.

Definição 2.14 (Reticulado 7 **- dimensional** E_7**)** *O reticulado* E_7 *é definido por* $E_7 = \{x \in E_8 \mid xv = 0,$ *para algum vetor minimal* $v \in E_8\}$*. Uma matriz geradora para este reticulado é dada por*

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1/2 & 1/2 & 1/2 & 0 & 1/2 & 0 & 0 \\ 0 & 1/2 & 1/2 & 1/2 & 0 & 1/2 & 0 \\ 0 & 0 & 1/2 & 1/2 & 1/2 & 0 & 1/2 \end{pmatrix}$$

O raio de empacotamento é dado por $\rho = \sqrt{2}/2$ *e a densidade de centro é* $\delta = 1/16 = 0,06250$*, que é a densidade de centro máxima para dimensão* 7*.*

Definição 2.15 (Reticulado 6 **- dimensional** E_6**)** *O reticulado* E_6 *é definido por* $E_6 = \{x \in E_8 \mid xv = 0,\ \forall\ x \in V\}$*, onde* V *é um* A_2 *- subreticulado em* E_8*. Uma matriz geradora para este reticulado é dada por*

$$\begin{pmatrix} 0 & -1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 1 & 0 \\ 1/2 & 1/2 & 1/2 & 1/2 & -1/2 & -1/2 & -1/2 & -1/2 \end{pmatrix}$$

O raio de empacotamento é dado por $\rho = \sqrt{2}/2$ *e a densidade de centro é* $\delta = 1/8\sqrt{3} = 0,07217$*, que é a densidade de centro máxima para dimensão* 6*.*

Definição 2.16 (Reticulado laminado Λ_n**)** *Seja* $\Lambda_0 = \{A\}$*, onde* A *é um ponto do* $\mathbb{R}^n$*. Para* $n \geq 1$*, tomemos todos os reticulados n - dimensionais com norma mínima igual a* 4*, que tenham no mínimo um subreticulado* Λ_{n-1} *e selecione aqueles com discriminante mínimo. Este reticulado é chamado de reticulado laminado* Λ_n*.*

Observação 2.4 *Até a dimensão* 8*, para as famílias de reticulados definida acima, temos as seguintes equivalências:* $\Lambda_1 \cong \mathbb{Z} \cong A_1$*,* $\Lambda_3 \cong A_3 \cong D_3$*,* $\Lambda_5 \cong D_5$*,* $\Lambda_7 \cong E_7$*,* $\Lambda_2 \cong A_2$*,* $\Lambda_4 \cong D_4$*,* $\Lambda_6 \cong E_6$ *e* $\Lambda_8 \cong E_8$*.*

Capítulo 3

Colagem de Reticulados

Conteúdo

As demonstrações feitas neste capítulo foram baseadas em [Flores, Interlando & NOBREGA NETO A ser publicado]

3.1 Preliminares

Sabemos que um reticulado n - dimensional é um subgrupo discreto de $\mathbb{R}^n$ de posto n e este pode ser descrito como um conjunto $\mathscr{H} = \left\{ \sum_{i=1}^{n} a_i u_i \mid a_i \in \mathbb{Z} \right\}$ onde cada u_i, $i = 1, \ldots, n$, é uma matriz $1 \times n$ com entradas em $\mathbb{R}$, e o conjunto $\{u_1, \ldots, u_n\}$ é linearmente independente sobre $\mathbb{R}$.

Definição 3.1 *Seja $\mathscr{H}$ um reticulado n - dimensional. O raio de empacotamento de $\mathscr{H}$,*

denotado por ρ, é definido por

$$\rho = \frac{1}{2} min\{d(x,y)\ ;\ x,y \in \mathscr{H},\ x \neq y\},$$

onde $d(x,y)$ é a distância euclidiana em $\mathbb{R}^n$. Em palavras, o raio de empacotamento é a metade da distância mínima entre os pontos do reticulado.

Definição 3.2 *O volume de $\mathscr{H}$, denotado por $Vol(\mathscr{H})$, é definido como o volor absoluto do determinante da matriz geradora do reticulado $\mathscr{H}$.*

Definição 3.3 *A densidade de centro do reticulado $\mathscr{H}$, denotado por $\delta(\mathscr{H})$, é definido por*

$$\delta(\mathscr{H}) = \frac{\rho^n}{Vol(\mathscr{H})}$$

Definição 3.4 *O "kissing number"do reticulado $\mathscr{H}$, denotado por $Kiss(\mathscr{H})$, é definido como o número de vetores de comprimento mínimo do reticulado $\mathscr{H}$.*

Lema 3.1 *Dados números inteiros $a_1,\ldots,a_n$ relativamente primos, então existe uma matriz, com entradas inteiras,*

$$A_{n\times n} = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$$

tal que $A_{n\times n}$ é invertível.

Corolário 3.1 *Dados um reticulado $\mathscr{H}$ de $\mathbb{R}^n$, com $\mathbb{Z}$-base $\{u_1,\ldots,u_n\}$ e $w = b_1u_1+\cdots+b_nu_n$ um vetor de $\mathscr{H}$ então w faz parte de alguma $\mathbb{Z}$-base de $\mathscr{H}$ se, e somente se $b_1,\ldots,b_n$ são relativamente primos.*

Prova: $\Rightarrow$) Suponha que $b_1,\ldots,b_n$ não são relativamente primos, então existe $r \in \mathbb{Z}$, $r \neq \pm 1$, tal que $r|b_i$, para $i = 1,\ldots,n$. Assim, podemos escrever $w = r\left(\frac{b_1}{r}u_1+\cdots+\frac{b_n}{r}u_n\right)$. Seja $w' = \frac{b_1}{r}u_1+\cdots+\frac{b_n}{r}u_n$ e suponha que w faz parte de uma $\mathbb{Z}$-base de $\mathscr{H}$, ou seja, que existe uma $\mathbb{Z}$-base de $\mathscr{H}$ da forma $\{w,v_2,\ldots,v_n\}$. Daí, como $w' \in \mathscr{H}$, podemos escrever $w' = a_1w + a_2v_2\cdots+a_nv_n$, com $a_i \in \mathbb{Z}$. Logo, temos $a_1w+a_2v_2\cdots+a_nv_n = \frac{b_1}{r}u_1+\cdots+\frac{b_n}{r}u_n \Rightarrow r(a_1w + a_2v_2\cdots+a_nv_n) - b_1u_1+\cdots+b_nu_n = 0$, daí $ra_1w+ra_2v_2\cdots+ra_nv_n - w = 0 \Rightarrow (ra_1-1)w + ra_2v_2+\cdots+ra_nv_n = 0$, como os vetores $w,v_2\ldots,v_n$ são linearmente independentes, temos ra_1-

$1 = 0 \Rightarrow ra_1 = 1 \Rightarrow a_1 = \dfrac{1}{r} \notin \mathbb{Z}$, já que $r \neq \pm 1$, mas isso é absurdo, pois $a_1 \in \mathbb{Z}$. Logo, temos que se w faz parte de uma $\mathbb{Z}$-base de $\mathscr{H}$ então os b_i's são relativamente primos.

$\Leftarrow$) Se os b_i's são relativamente primos, então pelo Lema 3.1 temos que w faz parte de alguma $\mathbb{Z}$-base de $\mathscr{H}$.

Corolário 3.2 *Dados um reticulado $\mathscr{H}$ de $\mathbb{R}^n$ e v_1 um vetor de comprimento mínimo de $\mathscr{H}$ então v_1 faz parte de uma $\mathbb{Z}$-base de $\mathscr{H}$.*

Prova: Seja $\{u_1, \ldots, u_n\}$ uma $\mathbb{Z}$-base de $\mathscr{H}$, como $v_1 \in \mathscr{H}$, podemos escrever $v_1 = a_1u_1 + \cdots + a_nu_n$, com $a_i \in \mathbb{Z}$. Temos que os a_i's são relativamente primos, pois se não fosse existiria $r \in \mathbb{Z}$, $r \neq \pm 1$ tal que $v_1 = r\left(\dfrac{a_1}{r}u_1 + \cdots + \dfrac{a_n}{r}u_n\right)$, daí teríamos um vetor $w = \left(\dfrac{a_1}{r}u_1 + \cdots + \dfrac{a_n}{r}u_n\right) \in \mathscr{H}$ de comprimento menor do que o comprimento de v_1, o que não pode ocorrer, já que v_1 é um vetor não nulo de comprimento mínimo de $\mathscr{H}$. Logo, os a_i's são relativamente primos e portanto pelo Lema 3.1 temos que v_1 faz parte de uma $\mathbb{Z}$-base de $\mathscr{H}$.

Lema 3.2 *Dados um reticulado $\mathscr{H}$ de $\mathbb{R}^n$, v_1 um vetor de comprimento mínimo de $\mathscr{H}$ e $\{v_1, u_2, \ldots, u_n\}$ uma $\mathbb{Z}$-base de $\mathscr{H}$, seja v_2 um vetor de $\mathscr{H}$ tal que v_2 seja linearmente independente com v_1 e que tenha comprimento mínimo dentre os vetores linearmente independentes com v_1. Podemos supor $v_2 = a_1 \cdot v_1 + t \cdot u$, onde $u \in \mathscr{H}$ e $a_1, t \in \mathbb{Z}$, com $t > 0$. Nestas condições teremos $t = 1$.*

Prova: Podemos supor, sem perda de generalidade, que $|v_1| = 1$ e que o ângulo θ formado pelos vetores v_1 e v_2 satisfaz $\dfrac{\pi}{3} \leq \theta \leq \dfrac{\pi}{2}$, daí como $v_2 = a_1v_1 + tu$, temos que

$$\begin{aligned}
|v_2|^2 &= |a_1v_1 + tu|^2 \\
&= a_1^2|v_1|^2 + 2a_1t(v_1.u) + t^2|u|^2 \\
&= a_1^2|v_1|^2 + 2a_1t|u||v_1|\cos\theta + t^2|u|^2 \\
&= a_1^2 + 2a_1t|u|\cos\theta + t^2|u|^2 \\
&= a_1^2 + 2a_1t|u|\cos\theta + t^2|u|^2(\cos^2\theta + \sin^2\theta) \\
&= a_1^2 + 2a_1t|u|\cos\theta + t^2|u|^2\cos^2\theta + t^2|u|^2\sin^2\theta \\
&= (a_1 + t|u|\cos\theta)^2 + t^2|u|^2\sin^2\theta
\end{aligned}$$

Se $a_1 + t|u|\cos\theta \notin \left[-\frac{1}{2}, \frac{1}{2}\right]$, então tomamos $v_2' = bv_1 + tu$, onde $b = a_1 + 1$ ou $b = a_1 - 1$ de tal modo que $(b + t|u|\cos\theta)^2 < (a_1 + t|u|\cos\theta)^2$ e daí teremos $b^2 + 2bt|u|\cos\theta + t^2|u|^2\cos^2\theta <$

$a_1^2+2a_1t|u|\cos\theta+t^2|u|^2\cos^2\theta$, daí $b^2|v_1|^2+2bt(u.v_1)+t^2|u|^2<a_1^2|v_1|^2+2a_1t(u.v_1)+t^2|u|^2$, assim $|bv_1+tu|^2<|a_1v_1+tu|^2$, logo $|bv_1+tu|<|a_1v_1+tu|$, isto é, $|v_2'|<|v_2|$ contrariando a minimalidade de $|v_2|$. Assim, podemos supor que $a_1+t|u|\cos\theta\in\left[-\frac{1}{2},\frac{1}{2}\right]$. Tomando $v_2'=a_1v_1+(t-1)u$, temos

$$\begin{aligned}
|v_2'|^2 &= |a_1v_1+(t-1)u|^2\\
&= a_1^2|v_1|^2+2a_1(v_1.u)(t-1)+(t-1)^2|u|^2\\
&= a_1^2+2a_1t(v_1.u)-2a_1(v_1.u)+u^2t^2-2tu^2+u^2\\
&= |v_2|^2-2a_1|v_1||u|\cos\theta-|u|^2(2t-1)\\
&= |v_2|^2-2a_1|u|\cos\theta-|u|^2(\cos^2\theta+\sin^2\theta)(2t-1)\\
&= |v_2|^2-2a_1|u|\cos\theta-(|u|^2\cos^2\theta)(2t-1)-(|u|^2\sin^2\theta)(2t-1)\\
&= |v_2|^2-2a_1|u|\cos\theta-2t|u|^2\cos^2\theta+|u|^2\cos^2\theta-|u|^2\sin^2\theta)(2t-1)\\
&= |v_2|^2-2(a_1+t|u|\cos\theta)|u|\cos\theta+|u|^2\cos^2\theta-|u|^2\sin^2\theta(2t-1)\\
&= |v_2|^2-2(a_1+t|u|\cos\theta)|u|\cos\theta+|u|^2(\cos^2\theta-2t\sin^2\theta+\sin^2\theta)\\
&= |v_2|^2-2(a_1+t|u|\cos\theta)|u|\cos\theta+|u|^2(1-2t\sin^2\theta)
\end{aligned}$$

Sabendo que $-\dfrac{1}{2}\leq a_1+t|u|\cos\theta\leq\dfrac{1}{2}$, que $\dfrac{\pi}{3}\leq\theta\leq\dfrac{\pi}{2}$ e supondo $t\geq 2$, concluímos novamente que, $|v_2'|<|v_2|$, contrariando a hipótese de minimalidade de $|v_2|$. Portanto, temos que $t=1$.

Corolário 3.3 *Sejam $\mathscr{H}$ um reticulado de $\mathbb{R}^n$, v_1 um vetor de comprimento mínimo de $\mathscr{H}$ e v_2 um vetor linearmente independente com v_1 e que dentre os vetores linearmente independentes com v_1 tenha comprimento mínimo. Então existem $v_3,\ldots,v_n$ vetores de $\mathscr{H}$ tais que $\{v_1,v_2,v_3,\ldots,v_n\}$ é uma $\mathbb{Z}$-base de $\mathscr{H}$.*

Prova: Pelo Corolário 3.2, sejam $u_2,\ldots,u_n\in\mathscr{H}$ tais que $\{v_1,u_2,\ldots,u_n\}$ seja uma $\mathbb{Z}$-base de $\mathscr{H}$. Podemos tomar $v_2=a_1v_1+a_2u_2+\cdots+a_nu_n$. Pelo Lema 3.2 temos que $a_1,a_2,\ldots,a_n$ são relativamente primos e pelo Lema 3.1 existe uma matriz

$$B=\begin{pmatrix} a_2 & a_3 & \cdots & a_n\\ b_{32} & b_{33} & \cdots & b_{3n}\\ \vdots & \vdots & \ddots & \vdots\\ b_{n2} & b_{n3} & \cdots & b_{nn}\end{pmatrix}$$

com entradas inteiras, cujo determinante é 1. Tomando $v_i = b_{i2}u_2 + \ldots + b_{in}u_n$, para $i = 3, \ldots, n$, e como a matriz

$$B' = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ a_1 & a_2 & a_3 & \cdots & a_n \\ 0 & b_{32} & b_{33} & \cdots & b_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & b_{n2} & b_{n3} & \cdots & b_{nn} \end{pmatrix}$$

invertível, pois a matriz B é invertível. Daí, temos que $\{v_1, \ldots v_n\}$ é uma $\mathbb{Z}$-base de $\mathscr{H}$, onde $v_1 = (1, 0, \ldots, 0)$, $v_2 = (a_1, a_2, \ldots, a_n)$ e $v_i = (0, b_{i2}, \ldots, b_{in})$, para $i = 3, \ldots, n$.

Lema 3.3 *Seja $\mathscr{H}$ um reticulado em $\mathbb{R}^n$, cujos vetores de comprimento mínimo têm comprimento 1, com $\mathbb{Z}$-base $\{u_1, \ldots, u_n\}$. Sem perda de generalidade podemos supor que $u_i = (a_{i1}, \ldots, a_{in})$, para $i = 1, \ldots, n-1$, que $u_n = (0, \ldots, 0, 1)$ e que $|a_{in}| \leq \frac{1}{2}$. Tomando $\mathscr{H}'$ como sendo o reticulado gerado por u_i' com $i = 1, \ldots, n-1$, onde $u_i' = (a_{i1}, \ldots, a_{in-1})$, a distância mínima de $\mathscr{H}'$ é pelo menos $\dfrac{\sqrt{3}}{2}$.*

Prova: De fato, seja $u' = \lambda_1 u_1' + \cdots + \lambda_{n-1} u_{n-1}'$ um vetor de $\mathscr{H}'$. Considere o vetor $u = \lambda_1 u_1 + \cdots + \lambda_{n-1} u_{n-1}$, t' a n-ésima coordenada de u e t o inteiro mais próximo de t'. Daí, temos

$$\begin{aligned} u &= \lambda_1(a_{11}, \ldots, a_{1n-1}, a_{1n}) + \lambda_2(a_{21}, \ldots, a_{2n-1}, a_{2n}) + \cdots \\ &\quad + \lambda_{n-1}(a_{n-11}, \ldots, a_{n-1n-1}, a_{n-1n}) \\ &= (\lambda_1 a_{11}, \ldots, \lambda_1 a_{1n-1}, \lambda_1 a_{1n}) + (\lambda_2 a_{21}, \ldots, \lambda_2 a_{2n-1}, \lambda_2 a_{2n}) + \cdots \\ &\quad + (\lambda_{n-1} a_{n-11}, \ldots, \lambda_{n-1} a_{n-1n-1}, \lambda_{n-1} a_{n-1n}) \\ &= (\lambda_1 a_{11} + \lambda_2 a_{21} + \cdots + \lambda_{n-1} a_{n-11}, \ldots, \lambda_1 a_{1n-1} + \lambda_2 a_{2n-1} + \cdots + \\ &\quad \lambda_{n-1} a_{n-1n-1}, \lambda_1 a_{1n} + \lambda_2 a_{2n} + \cdots + \lambda_{n-1} a_{n-1n}) \end{aligned}$$

onde $t' = \lambda_1 a_{1n} + \lambda_2 a_{2n} + \cdots + \lambda_{n-1} a_{n-1n}$.
Veja que:

$$\begin{aligned} u' &= \lambda_1(a_{11}, \ldots, a_{1n-2}, a_{1n-1}) + \lambda_2(a_{21}, \ldots, a_{2n-2}, a_{2n-1}) + \cdots \\ &\quad + \lambda_{n-1}(a_{n-1,1}, \ldots, a_{n-1n-2}, a_{n-1n-1}) \\ &= (\lambda_1 a_{11}, \ldots, \lambda_1 a_{1n-2}, \lambda_1 a_{1n-1}) + (\lambda_2 a_{21}, \ldots, \lambda_2 a_{2n-2}, \lambda_2 a_{2n-1}) + \cdots \\ &\quad + (\lambda_{n-1} a_{n-11}, \ldots, \lambda_{n-1} a_{n-1n-2}, \lambda_{n-1} a_{n-1n-1}) \\ &= (\lambda_1 a_{11} + \lambda_2 a_{21} + \cdots + \lambda_{n-1} a_{n-11}, \ldots, \lambda_1 a_{1n-2} + \lambda_2 a_{2n-2} + \cdots + \lambda_{n-1} a_{n-1n-2}, \\ &\quad \lambda_1 a_{1n-1} + \lambda_2 a_{2n-1} + \cdots + \lambda_{n-1} a_{n-1n-1}) \end{aligned}$$

e

$$\begin{aligned} u - tu_n &= (\lambda_1 a_{11} + \lambda_2 a_{21} + \cdots + \lambda_{n-1} a_{n-11}, \ldots, \lambda_1 a_{1n-1} + \lambda_2 a_{2n-1} + \cdots + \\ &\quad \lambda_{n-1} a_{n-1n-1}, \lambda_1 a_{1n} + \lambda_2 a_{2n} + \cdots + \lambda_{n-1} a_{n-1n}) - t(0, \ldots, 0, 1) \\ &= (\lambda_1 a_{11} + \lambda_2 a_{21} + \cdots + \lambda_{n-1} a_{n-11}, \ldots, \lambda_1 a_{1n-1} + \lambda_2 a_{2n-1} + \cdots + \\ &\quad \lambda_{n-1} a_{n-1n-1}, \lambda_1 a_{1n} + \lambda_2 a_{2n} + \cdots + \lambda_{n-1} a_{n-1n} - t) \\ &= (\lambda_1 a_{11} + \lambda_2 a_{21} + \cdots + \lambda_{n-1} a_{n-11}, \ldots, \lambda_1 a_{1n-1} + \lambda_2 a_{2n-1} + \cdots + \\ &\quad \lambda_{n-1} a_{n-1n-1}, t' - t) \end{aligned}$$

Assim, o vetor $u - tu_n$ tem as $n-1$ coordenadas iguais as do vetor u' e a n-ésima coordenada, $t' - t$, entre $-\frac{1}{2}$ e $\frac{1}{2}$. Tendo em vista que o vetor $u - tu_n$ é não nulo e portanto tem norma maior ou igual a 1, temos que $1 \leq |u - tu_n|^2 = |u'|^2 + (t' - t)^2 \leq |u'|^2 + \left(\frac{1}{2}\right)^2 = |u'|^2 + \frac{1}{4} \Rightarrow 1 \leq |u'|^2 + \frac{1}{4} \Rightarrow |u'|^2 \geq 1 - \frac{1}{4} = \frac{3}{4} \Rightarrow |u'|^2 \geq \frac{3}{4}$, isto é, $|u'| \geq \frac{\sqrt{3}}{2}$. Logo, a distância mínima de $\mathscr{H}'$ é pelo menos $\frac{\sqrt{3}}{2}$.

Lema 3.4 *Sejam $\mathscr{H}$ um reticulado de posto maior ou igual que 2 e $\beta = \{v_1, \ldots, v_n\}$ uma base de $\mathscr{H}$. Sem perda de generalidade podemos supor que $|v_1| = 1$, v_2 é um vetor de comprimento mínimo dentre os vetores que são linearmente independentes com v_1 e ainda que $v_1 = (0, \ldots, 0, 1)$. Suponhamos que $v_2 = (0, \ldots, 0, \frac{\sqrt{3}}{2}, \frac{1}{2})$ e $v_i = (a_{i1}, \ldots, a_{in})$, com $i = 1, \ldots, n-2$. Sejam $v_i' = (a_{i1}, \ldots, a_{in-2})$, $i = 1, \ldots, n-2$ e $\mathscr{H}'$ o reticulado gerado por $\{v_1', \ldots, v_{n-2}'\}$. Então a distância mínima de $\mathscr{H}'$ é pelo menos $\frac{3}{4}$.*

Prova: De fato, seja $v' = \lambda_1 v_1' + \cdots + \lambda_{n-2} v_{n-2}'$ um vetor não nulo de $\mathscr{H}'$. Tomando $v = \lambda_1 v_1 + \cdots + \lambda_{n-2} v_{n-2} + \lambda_{n-1} v_{n-1} + \lambda_n v_n \in \mathscr{H}$ é possível encontrar λ_{n-1} e λ_n números inteiros tais que $v'' = v - \lambda_{n-1} v_{n-1} - \lambda_n v_n \in \mathscr{H}$ tem a última coordenada entre $-\frac{1}{2}$ e $\frac{1}{2}$ e a penúltima coordenada entre $-\frac{\sqrt{3}}{4}$ e $\frac{\sqrt{3}}{4}$. Assim,

$$\begin{aligned} |v''|^2 &= |\lambda_1 v_1 + \cdots + \lambda_{n-2} v_{n-2}|^2 \\ &= |\lambda_1 (a_{11}, \ldots, a_{1n-2}, a_{1n-1}, a_{1n}) + \cdots \\ &\quad + \lambda_{n-2} (a_{n-21}, \ldots, a_{n-2n-2}, a_{n-2n-2}, a_{n-2n-1}, a_{n-2n})|^2 \\ &= (\lambda_1 a_{11} + \cdots + \lambda_{n-2} a_{n-21})^2 + \cdots + (\lambda_1 a_{1n-2} + \cdots + \lambda_{n-2} a_{n-2n-2})^2 \\ &\quad + (\lambda_1 a_{1n-1} + \cdots + \lambda_{n-2} a_{n-2n-1})^2 + (\lambda_1 a_{1n} + \cdots + \lambda_{n-2} a_{n-2n})^2 \\ &= |v'|^2 + (\lambda_1 a_{1n-1} + \cdots + \lambda_{n-2} a_{n-2n-1})^2 + (\lambda_1 a_{1n} + \cdots + \lambda_{n-2} a_{n-2n})^2 \\ &= |v'|^2 + r^2 + s^2 \end{aligned}$$

onde $r = \lambda_1 a_{1n-1} + \cdots + \lambda_{n-2} a_{n-2n-1}$ e $s = \lambda_1 a_{1n} + \cdots + \lambda_{n-2} a_{n-2n}$. Como v'' tem a última coordenada entre $-\frac{1}{2}$ e $\frac{1}{2}$ e a penúltima entre $-\frac{\sqrt{3}}{4}$ e $\frac{\sqrt{3}}{4}$ temos que $0 \leq r^2 \leq \frac{3}{16}$ e $0 \leq s^2 \leq \frac{1}{4}$. Visto que $|v''|^2 \geq 1$, pois $v'' \in \mathscr{H}$, temos $1 \leq |v''|^2 = |v'|^2 + r^2 + s^2 \leq |v''|^2 + \frac{3}{16} + \frac{1}{4} \Rightarrow 1 \leq |v'|^2 + \frac{7}{16} \Rightarrow |v'|^2 \geq 1 - \frac{7}{16} = \frac{9}{16} \Rightarrow |v'| \geq \frac{3}{4}$. Logo, a distância mínima de $\mathscr{H}'$ é pelo menos $\frac{3}{4}$.

3.2 Colagem de reticulados em dimensão 0

Teorema 3.1 *Sejam $\mathscr{A}$ um reticulado de dimensão n e $\mathscr{B}$ um reticulado de dimensão m, ambos com distância mínima 1. Suponhamos $\{u_i\}_{i=1,\ldots,n}$ uma base de $\mathscr{A}$, onde $u_i = (a_{i1}, \ldots, a_{in})$ com $i = 1, \ldots, n$ e $\{v_i\}_{i=1,\ldots,m}$ uma base de $\mathscr{B}$, onde $v_i = (b_{i1}, \ldots, b_{im})$ com $i = 1, \ldots, m$. Seja $\mathscr{C}$ o reticulado com matriz geradora dada por:*

$$C = \begin{pmatrix} a_{11} & \ldots & a_{1n} & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} & 0 & \ldots & 0 \\ 0 & \ldots & 0 & b_{11} & \ldots & b_{1m} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & b_{m1} & \ldots & b_{mm} \end{pmatrix}$$

Então temos:

1. $\dim(\mathscr{C}) = \dim(\mathscr{A}) + \dim(\mathscr{B})$
2. $Vol(\mathscr{C}) = Vol(\mathscr{A})Vol(\mathscr{B})$
3. $Dist_{\min}(\mathscr{C}) = 1$
4. $Kiss(\mathscr{C}) = Kiss(\mathscr{A}) + Kiss(\mathscr{B})$
5. $\delta(\mathscr{C}) = \delta(\mathscr{A})\delta(\mathscr{B})$

Prova: 1. Sabemos que a dimensão do reticulado $\mathscr{A}$ é n e que a dimensão do reticulado $\mathscr{B}$ é m. Assim, temos que a dimensão do reticulado $\mathscr{C}$ é igual a somas das dimensões de $\mathscr{A}$ e $\mathscr{B}$. Logo, $\dim(\mathscr{C}) = n + m$, isto é, $\dim(\mathscr{C}) = \dim(\mathscr{A}) + \dim(\mathscr{B})$.

2. Sabemos que, por definição, o volume do reticulado $\mathscr{A}$ é o valor absoluto do determinante da matriz

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \dots & a_{nn} \end{pmatrix}$$

e o volume de $\mathscr{B}$ é o valor absoluto do determinante da matriz

$$B = \begin{pmatrix} b_{11} & \dots & b_{1m} \\ \vdots & \ddots & \vdots \\ b_{m1} & \dots & b_{mm} \end{pmatrix}$$

Daí, temos que $|\det C| = |\det A||\det B|$. Logo, como $Vol(\mathscr{A}) = |\det A|$, $Vol(\mathscr{B}) = |\det B|$ e $Vol(\mathscr{C}) = |\det C|$ temos que $Vol(\mathscr{C}) = Vol(\mathscr{A})Vol(\mathscr{B})$.

3. Mostraremos que distância mínima do reticulado $\mathscr{C}$ é igual a 1, isto é, dado qualquer vetor não nulo em $\mathscr{C}$ seu comprimento é sempre maior ou igual a 1. Com efeito, temos por hipótese que o reticulado $\mathscr{A}$ e o reticulado $\mathscr{B}$ têm distância mínima igual a 1, isto é, dado qualquer vetor não nulo em $\mathscr{A}$ e em $\mathscr{B}$ seu comprimento é sempre maior ou igual a 1. Daí, como $\mathscr{C}$ possui matriz geradora C, qualquer vetor de $\mathscr{C}$ tem mesmo comprimento que um vetor de $\mathscr{A}$ ou de $\mathscr{B}$. Assim, dado qualquer vetor não nulo em $\mathscr{C}$ seu comprimento é sempre maior ou igual a 1. Logo, $\text{Dist}_{\min}(\mathscr{C}) = 1$.

4. De fato, como o reticulado $\mathscr{C}$ possui matriz geradora C a quantidade de vetores de comprimento mínimo de $\mathscr{C}$ é igual a quantidade de vetores de comprimento mínimo de $\mathscr{A}$ mais a quantidade de vetores de comprimento mínimo de $\mathscr{B}$. Logo, $\text{Kiss}(\mathscr{C}) = \text{Kiss}(\mathscr{A}) + \text{Kiss}(\mathscr{B})$.

5. Como a distância mínima do reticulado $\mathscr{C}$ é igual a 1, temos que o raio de empacotamento deste é $\frac{1}{2}$. Daí, temos por definição que $\delta(\mathscr{C}) = \frac{(\frac{1}{2})^{n+m}}{Vol(\mathscr{C})}$. Como os reticulados $\mathscr{A}$ e $\mathscr{B}$ têm distância mínima igual a 1, os raios de empacotamentos destes também são iguais a $\frac{1}{2}$. Assim, temos $\delta(\mathscr{A}) = \frac{(\frac{1}{2})^{n}}{Vol(\mathscr{A})}$ e $\delta(\mathscr{B}) = \frac{(\frac{1}{2})^{m}}{Vol(\mathscr{B})}$. Sabemos que $Vol(\mathscr{C}) = Vol(\mathscr{A})Vol(\mathscr{B})$, por outro lado, $Vol(\mathscr{C}) = \frac{(\frac{1}{2})^{n+m}}{\delta(\mathscr{C})}$. Logo, temos

$$\frac{(\frac{1}{2})^{n+m}}{\delta(\mathscr{C})} = Vol(\mathscr{A})Vol(\mathscr{B})$$

$$\Rightarrow \delta(\mathscr{C}) = \frac{(\frac{1}{2})^{n+m}}{Vol(\mathscr{A})Vol(\mathscr{B})} = \frac{(\frac{1}{2})^{n+m}}{\frac{(\frac{1}{2})^n}{\delta(\mathscr{A})}\frac{(\frac{1}{2})^m}{\delta(\mathscr{B})}}$$

$$\Rightarrow \delta(\mathscr{C}) = \frac{2^{-n-m}}{\frac{2^{-n-m}}{\delta(\mathscr{A})\delta(\mathscr{B})}} = 2^{-n-m}\frac{\delta(\mathscr{A})\delta(\mathscr{B})}{2^{-n-m}} = \delta(\mathscr{A})\delta(\mathscr{B})$$

Logo, $\delta(\mathscr{C}) = \delta(\mathscr{A})\delta(\mathscr{B})$.

3.3 Colagem de reticulados em dimensão 1

Teorema 3.2 *Sejam $\mathscr{A}$ um reticulado de dimensão n e $\mathscr{B}$ um reticulado de dimensão m, ambos com distância mínima 1. Suponhamos $\{u_i\}$, $i = 1,\ldots,n$ uma base de $\mathscr{A}$, com $u_i = (a_{i1},\ldots,a_{in})$, $i = 1,\ldots,n-1$ e $u_n = (0,\ldots,0,1)$ e $\{v_i\}_{i=1,\ldots,m}$ uma base de $\mathscr{B}$ com $v_i = (b_{i1},\ldots,b_{im})$ $i = 2,\ldots,m$ e $v_1 = (1,0,\ldots,0)$. Seja $\mathscr{C}$ o reticulado com matriz geradora dada por:*

$$C = \begin{pmatrix} a_{11} & \ldots & a_{1n-1} & a_{1n} & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & 0 & \ddots & 0 \\ a_{n-11} & \ldots & a_{n-1n-1} & a_{n-1n} & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 1 & 0 & \ldots & 0 \\ 0 & \ldots & 0 & b_{21} & b_{22} & \ldots & b_{2m} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & b_{m1} & b_{m2} & \ldots & b_{mm} \end{pmatrix}$$

Então temos:

1. $\dim(\mathscr{C}) = \dim(\mathscr{A}) + \dim(\mathscr{B}) - 1$

2. $Vol(\mathscr{C}) = Vol(\mathscr{A})Vol(\mathscr{B})$

3. $Dist_{\min}(\mathscr{C}) = 1$

4. $Kiss(\mathscr{C}) = Kiss(\mathscr{A}) + Kiss(\mathscr{B}) - 2$

5. $\delta(\mathscr{C}) = 2\delta(\mathscr{A})\delta(\mathscr{B})$

Prova: 1. Sabemos que a dimensão do reticulado $\mathscr{A}$ é n e que a dimensão do reticulado $\mathscr{B}$ é m. Assim, temos que a dimensão do reticulado $\mathscr{C}$ é igual a somas das dimensões de $\mathscr{A}$ e $\mathscr{B}$ menos 1, pois temos um vetor na interseção das bases desses reticulados. Logo, $\dim(\mathscr{C}) = n+m-1$, isto é, $\dim(\mathscr{C}) = \dim(\mathscr{A}) + \dim(\mathscr{B}) - 1$.

2. Sabemos que, por definição, o volume do reticulado $\mathscr{A}$ é o valor absoluto do determinante da matriz

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n-1} & a_{1n} \\ \vdots & \ddots & \vdots & \vdots \\ a_{n-11} & \dots & a_{n-1n-1} & a_{n-1n} \\ 0 & \dots & 0 & 1 \end{pmatrix}$$

e o volume de $\mathscr{B}$ é o valor absoluto do determinante da matriz

$$B = \begin{pmatrix} 1 & 0 & \dots & 0 \\ b_{21} & b_{22} & \dots & b_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & \dots & b_{mm} \end{pmatrix}$$

Considere a matriz

$$A' = \begin{pmatrix} a_{11} & \dots & a_{1n-1} \\ \vdots & \ddots & \vdots \\ a_{n-11} & \dots & a_{n-1n-1} \end{pmatrix}$$

Daí, $|\det A| = 1|\det A'|$ e $|\det C| = |\det A'||\det B|$, isto é, $|\det C| = |\det A|\det B|$. Logo, como $Vol(\mathscr{A}) = |\det A|$, $Vol(\mathscr{B}) = |\det B|$ e $Vol(\mathscr{C}) = |\det C|$ temos que $Vol(\mathscr{C}) = Vol(\mathscr{A})Vol(\mathscr{B})$.

3. Mostraremos agora que a distância mínima do reticulado $\mathscr{C}$ é igual a 1, isto é, dado qualquer vetor não nulo em $\mathscr{C}$ seu comprimento é sempre maior ou igual a 1. De fato, sabemos que o reticulado $\mathscr{A}$ possui matriz geradora A, isto é, $\{u_1,\dots,u_n\}$ é uma base de $\mathscr{A}$, onde $u_n = (0,\dots,0,1)$ e $u_i = (a_{i1},\dots,a_{in})$, com $i = 1,\dots,n-1$. Seja $\mathscr{A}'$ um reticulado que possui matriz geradora A', isto é, $\{u'_1,\dots,u'_{n-1}\}$ é uma base de $\mathscr{A}'$, onde $u'_i = (a_{i1},\dots,a_{in-1})$, com $i = 1,\dots,n-1$. Pelo Lema 3.3 temos que $\mathscr{A}'$ tem distância mínima pelo menos $\frac{\sqrt{3}}{2}$. Por outro lado, sabemos que o reticulado $\mathscr{B}$ possui matriz geradora B, isto é, $\{v_1,\dots,v_m\}$ é uma base de $\mathscr{B}$, onde $v_1 = (1,0\dots,0)$ e $v_i = (b_{i1},\dots,b_{im})$ com $i = 2,\dots,m$. Seja $\mathscr{B}'$ um reticulado que possui matriz geradora igual a

$$B' = \begin{pmatrix} b_{22} & \dots & b_{2m} \\ \vdots & \ddots & \vdots \\ b_{m2} & \dots & b_{mm} \end{pmatrix}$$

isto é, $\{v'_2,\ldots,v'_m\}$ é uma base de $\mathscr{B}'$, onde $v'_i=(b_{i2},\ldots,b_{im})$, com $i=2,\ldots,m$. Pelo Lema 3.3, podemos concluir que a distância mínima de $\mathscr{B}'$ é também pelo menos $\frac{\sqrt{3}}{2}$. Daí, seja $w=w_1+w_2+w_3\in\mathscr{C}$ um vetor não nulo, com $w_1=\sum_{i=1}^{n-1}a_iu''_i$, $w_2=\lambda u''_n=\lambda v''_1$ e $w_3=\sum_{i=2}^{m}b_iv''_i$, onde $u''_i=(a_{i1},\ldots,a_{in-1},a_{in},0,\ldots,0)$, com $i=1,\ldots,n-1$, $u''_n=(0,\ldots,0,1,0,\ldots,0)=v''_1$ e $v''_i=(0,\ldots,0,b_{i1},b_{i2},\ldots,b_{im})$, com $i=2,\ldots,m$. Daí, temos

$$\begin{aligned}|w|^2 &= \left(\sum_{i=1}^{n-1}a_ia_{i1}\right)^2+\cdots+\left(\sum_{i=1}^{n-1}a_ia_{in-1}\right)^2\\ &+ \left(\sum_{i=1}^{n-1}a_ia_{in}+\lambda+\sum_{i=2}^{m}b_ib_{i1}\right)^2\\ &+ \left(\sum_{i=2}^{m}b_ib_{i2}\right)^2+\cdots+\left(\sum_{i=2}^{m}b_ib_{im}\right)^2\\ &= |w'_1|^2+s+|w'_2|^2\end{aligned}$$

onde w'_1 é um vetor não nulo pertencente a $\mathscr{A}'$, w'_2 é um vetor não nulo pertencente a $\mathscr{B}'$ e $s=\left(\sum_{i=1}^{n-1}a_ia_{in}+\lambda+\sum_{i=2}^{m}b_ib_{i1}\right)^2$. Como qualquer vetor não nulo de $\mathscr{A}'$ e $\mathscr{B}'$ tem comprimento maior ou igual a $\frac{\sqrt{3}}{2}$ temos $|w|^2=|w'_1|^2+s+|w'_2|^2\geq|w'_1|^2+|w'_2|^2\geq\frac{3}{4}+\frac{3}{4}=\frac{6}{4}>1$, isto é, $|w|\geq 1$ ou seja, w tem comprimento mínimo igual a 1. Logo, $\mathrm{Dist}_{\min}(\mathscr{C})=1$.

4. Contar os vetores de $\mathscr{C}$ de comprimento 1, significa contar quantos vetores da forma $w=w_1+w_2+w_3$ tem comprimento 1, onde $w_1=\sum_{i=1}^{n-2}a_iu''_i$, $w_2=\lambda u''_n=\lambda v''_1$ e $w_3=\sum_{i=3}^{m}b_iv''_i$, isto é, contar os vetores w de $\mathscr{C}$ tais que $|w|=|w'_1|^2+s+|w'_2|^2=1$. Daí, o número de vetores dessa forma de comprimento 1 do reticulado $\mathscr{C}$, tais que $w'_1=0$ é $\mathrm{Kiss}(\mathscr{B})$ e o número de vetores dessa forma de comprimento 1 do reticulado $\mathscr{C}$, tais que $w'_2=0$ é $\mathrm{Kiss}(\mathscr{A})$. Temos pelo item anterior que, se $w'_1\neq 0$ e $w'_2\neq 0$, w terá comprimento maior que 1. Logo, podemos concluir que $\mathrm{Kiss}(\mathscr{C})=\mathrm{Kiss}(\mathscr{A})+\mathrm{Kiss}(\mathscr{B})-2$.

5. Como a distância mínima do reticulado $\mathscr{C}$ é igual a 1, temos que o raio de empacotamento deste é $\frac{1}{2}$, daí, por definição, temos $\delta(\mathscr{C})=\frac{(\frac{1}{2})^{n+m-1}}{Vol(\mathscr{C})}$. Como os reticulados $\mathscr{A}$ e $\mathscr{B}$ têm distância mínima igual a 1, os raios de empacotamentos destes também são iguais a $\frac{1}{2}$. Assim, temos $\delta(\mathscr{A})=\frac{(\frac{1}{2})^{n}}{Vol(\mathscr{A})}$ e $\delta(\mathscr{B})=\frac{(\frac{1}{2})^{m}}{Vol(\mathscr{B})}$. Sabemos que $Vol(\mathscr{C})=Vol(\mathscr{A})Vol(\mathscr{B})$, por outro

lado, $Vol(\mathscr{C}) = \frac{(\frac{1}{2})^{n+m-1}}{\delta(\mathscr{C})}$. Logo, temos

$$\frac{(\frac{1}{2})^{n+m-1}}{\delta(\mathscr{C})} = Vol(\mathscr{A})Vol(\mathscr{B})$$

$$\Rightarrow \delta(\mathscr{C}) = \frac{(\frac{1}{2})^{n+m-1}}{Vol(\mathscr{A})Vol(\mathscr{B})} = \frac{(\frac{1}{2})^{n+m-1}}{\frac{(\frac{1}{2})^{n}}{\delta(\mathscr{A})}\frac{(\frac{1}{2})^{m}}{\delta(\mathscr{B})}} = \frac{2^{-n-m+1}}{\frac{2^{-n-m}}{\delta(\mathscr{A})\delta(\mathscr{B})}}$$

$$\Rightarrow \delta(\mathscr{C}) = \frac{2^{-n-m}2}{\frac{2^{-n-m}}{\delta(\mathscr{A})\delta(\mathscr{B})}} = 2^{-n-m}2\frac{\delta(\mathscr{A})\delta(\mathscr{B})}{2^{-n-m}} = 2\delta(\mathscr{A})\delta(\mathscr{B})$$

Logo, $\delta(\mathscr{C}) = 2\delta(\mathscr{A})\delta(\mathscr{B})$.

3.4 Colagem de reticulados em dimensão 2

Teorema 3.3 *Sejam $\mathscr{A}$ e $\mathscr{B}$ reticulados de dimensão $n \geq 2$ e $m \geq 2$, respectivamente, ambos com distância mínima 1 e contendo Λ_2. Suponhamos $\{u_i, i = 1,\ldots,n\}$ uma base de $\mathscr{A}$ com $u_i = (a_{i1},\ldots,a_{in})$, $i = 1,\ldots,n-2$, $u_{n-1} = (0,\ldots,0,\frac{\sqrt{3}}{2},\frac{1}{2})$ e $u_n = (0,\ldots,1)$ e $\{v_i, i = 1,\ldots,m\}$ uma base de $\mathscr{B}$, com $v_i = (b_{i1},\ldots,b_{im})$ $i = 3,\ldots,m$, $v_1 = (1,0,\ldots,0)$ e $v_2 = (\frac{\sqrt{3}}{2},\frac{1}{2},0,\ldots,0)$. Seja $\mathscr{C}$ o reticulado com matriz geradora dada por:*

$$C = \begin{pmatrix} a_{11} & \ldots & a_{1n-2} & a_{1n-1} & a_{1n} & 0 & \ldots & 0 \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-21} & \ldots & a_{n-2n-2} & a_{n-2n-1} & a_{n-2n} & 0 & \ldots & 0 \\ 0 & \ldots & 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} & 0 & \ldots & 0 \\ 0 & \ldots & 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & \cdots & 0 & b_{31} & b_{32} & b_{33} & \ldots & b_{3m} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \ldots & 0 & b_{m1} & b_{m2} & b_{m3} & \ldots & b_{mm} \end{pmatrix}$$

Então temos:

1. $\dim(\mathscr{C}) = \dim(\mathscr{A}) + \dim(\mathscr{B}) - \dim(\Lambda_2)$
2. $Vol(\mathscr{C}) = \dfrac{Vol(\mathscr{A})Vol(\mathscr{B})}{Vol(\Lambda_2)}$
3. $Dist_{\min}(\mathscr{C}) = 1$
4. $Kiss(\mathscr{C}) = Kiss(\mathscr{A}) + Kiss(\mathscr{B}) - Kiss(\Lambda_2)$

5. $\delta(\mathscr{C}) = \dfrac{\delta(\mathscr{A})\delta(\mathscr{B})}{\delta(\Lambda_2)}$.

Prova: 1. Sabemos que a dimensão do reticulado $\mathscr{A}$ é $n \geq 2$ e a dimensão do reticulado $\mathscr{B}$ é $m \geq 2$. Assim, temos que a dimensão do reticulado $\mathscr{C}$ é igual a somas das dimensões de $\mathscr{A}$ e $\mathscr{B}$ menos 2, pois temos dois vetores na interseção das bases desses reticulados. Portanto, como a dimensão do reticulado Λ_2 é dois, temos que $\dim\mathscr{C} = \dim\mathscr{A} + \dim\mathscr{B} - \dim\Lambda_2$.

2. Sabemos que, por definição, o volume do reticulado $\mathscr{A}$ é o valor absoluto do determinante da matriz

$$A = \begin{pmatrix} a_{11} & \dots & a_{1n-2} & a_{1n-1} & a_{1n} \\ \vdots & \ddots & \vdots & \vdots & \vdots \\ a_{n-21} & \dots & a_{n-2n-2} & a_{n-2n-1} & a_{n-2n} \\ 0 & \dots & 0 & \frac{\sqrt{3}}{2} & \frac{1}{2} \\ 0 & \dots & 0 & 0 & 1 \end{pmatrix}$$

Considere a matriz

$$A' = \begin{pmatrix} a_{11} & \dots & a_{1n-2} \\ \vdots & \ddots & \vdots \\ a_{n-21} & \dots & a_{n-2n-2} \end{pmatrix}$$

Temos que $Vol(\mathscr{A}) = |\det A| = |\det A'| Vol(\Lambda_2)$, isto é, $|\det A'| = \dfrac{Vol(\mathscr{A})}{Vol(\Lambda_2)}$. Por outro lado, como $\mathscr{B}$ possui matriz geradora igual a

$$B = \begin{pmatrix} \frac{\sqrt{3}}{2} & \frac{1}{2} & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ b_{31} & b_{32} & b_{33} & \dots & b_{3m} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{m1} & b_{m2} & b_{m3} & \dots & b_{mm} \end{pmatrix}$$

Assim, temos que $Vol(\mathscr{C}) = |\det C| = |\det A'||\det B| = |\det A'| Vol(\mathscr{B})$, isto é,

$$|\det A'| = \frac{Vol(\mathscr{C})}{Vol(\mathscr{B})}$$

Daí, temos

$$\frac{Vol(\mathscr{C})}{Vol(\mathscr{B})} = |\det A'| = \frac{Vol(\mathscr{A})}{Vol(\Lambda_2)}$$

Logo,

$$Vol(\mathscr{C}) = \frac{Vol(\mathscr{A})Vol(\mathscr{B})}{Vol(\Lambda_2)}.$$

3. Mostraremos agora que a distância mínima do reticulado $\mathscr{C}$ é igual a 1, isto é, dado qualquer vetor não nulo em $\mathscr{C}$ seu comprimento é sempre maior ou igual a 1. De fato, sabemos que o reticulado $\mathscr{A}$ possui matriz geradora A, isto é, $\{u_1,\ldots,u_n\}$ é uma base de $\mathscr{A}$, onde $u_{n-1} = (0,\ldots,0,\frac{\sqrt{3}}{2},\frac{1}{2})$, $u_n = (0,\ldots,0,1)$ e $u_i = (a_{i1},\ldots,a_{in})$, com $i = 1,\ldots,n-2$. Seja $\mathscr{A}'$ um reticulado que possui matriz geradora A', isto é, $\{u'_1,\ldots,u'_{n-2}\}$ é uma base de $\mathscr{A}'$, onde $u'_i = (a_{i1},\ldots,a_{in-2})$, com $i = 1,\ldots,n-2$. Pelo Lema 3.4 temos que $\mathscr{A}'$ tem distância mínima pelo menos $\frac{3}{4}$. Por outro lado, sabemos que o reticulado $\mathscr{B}$ possui matriz geradora B, isto é, $\{v_1,\ldots,v_m\}$ é uma base de $\mathscr{B}$, onde $v_1 = (\frac{\sqrt{3}}{2},\frac{1}{2},0,\ldots,0)$, $v_2 = (0,1,0\ldots,0)$ e $v_i = (b_{i1},\ldots,b_{im})$, com $i = 3,\ldots,m$. Seja $\mathscr{B}'$ um reticulado que possui matriz geradora igual a

$$B' = \begin{pmatrix} b_{33} & \ldots & b_{3m} \\ \vdots & \ddots & \vdots \\ b_{m3} & \ldots & b_{mm} \end{pmatrix}$$

isto é, $\{v'_3,\ldots,v'_m\}$ é uma base de $\mathscr{B}'$, onde $v'_i = (b_{i3},\ldots,b_{im})$, com $i = 3,\ldots,m$. Novamente pelo Lema 3.4, temos que $\mathscr{B}'$ possui distância mínima pelo menos $\frac{3}{4}$. Daí, seja $w = w_1+w_2+w_3 \in \mathscr{C}$ um vetor não nulo, com $w_1 = \sum_{i=1}^{n-2} a_i u''_i$, $w_2 = \lambda_1 u''_{n-1} + \lambda_2 u''_n = \lambda_1 v''_1 + \lambda_2 v''_2$ e $w_3 = \sum_{i=3}^{m} b_i v''_i$, onde $u''_i = (a_{i1},\ldots,a_{in-1},a_{in},0,\ldots,0)$, com $i = 1,\ldots,n-2$, $u''_{n-1} = (0,\ldots,0,\frac{\sqrt{3}}{2},\frac{1}{2},0,\ldots,0) = v''_1$, $u''_n = (0,\ldots,0,1,0,\ldots,0) = v''_2$ e $v''_i = (0,\ldots,0,b_{i1},b_{i2},\ldots,b_{im})$, com $i = 3,\ldots,m$. Daí, temos

$$\begin{aligned}
|w|^2 &= \left(\sum_{i=1}^{n-2} a_i a_{i1}\right)^2 + \cdots + \left(\sum_{i=1}^{n-2} a_i a_{in-2}\right)^2 \\
&+ \left(\sum_{i=1}^{n-2} a_i a_{in-1} + \frac{\lambda_1\sqrt{3}}{2} + \sum_{i=3}^{m} b_i b_{i1}\right)^2 \\
&+ \left(\sum_{i=1}^{n-2} a_i a_{in} + \frac{\lambda_1 + 2\lambda_2}{2} + \sum_{i=3}^{m} b_i b_{i2}\right)^2 \\
&+ \left(\sum_{i=3}^{m} b_i b_{i3}\right)^2 + \cdots + \left(\sum_{i=3}^{m} b_i b_{im}\right)^2 \\
&= |w'_1|^2 + s + |w'_2|^2
\end{aligned}$$

onde w'_1 é um vetor não nulo pertencente a $\mathscr{A}'$, w'_2 é um vetor não nulo pertencente a $\mathscr{B}'$ e $s = \left(\sum_{i=1}^{n-2} a_i a_{in-1} + \frac{\lambda_1\sqrt{3}}{2} + \sum_{i=3}^{m} b_i b_{i1}\right)^2 + \left(\sum_{i=1}^{n-2} a_i a_{in} + \frac{\lambda_1 + 2\lambda_2}{2} + \sum_{i=3}^{m} b_i b_{i2}\right)^2$. Como qualquer vetor não nulo de $\mathscr{A}'$ e $\mathscr{B}'$ tem comprimento maior ou igual a $\frac{3}{4}$ e temos $|w|^2 = |w'_1|^2 + s + |w'_2|^2$, podemos concluir que $|w|^2 \geq \frac{9}{16} + \frac{9}{16} = \frac{18}{16} > 1$, isto é, $|w| \geq 1$, ou seja, w tem comprimento mínimo igual a 1. Logo, $\text{Dist}_{\min}(\mathscr{C}) = 1$.

4. Contar os vetores de $\mathscr{C}$ de comprimento 1, significa contar quantos vetores da forma $w = w_1 + w_2 + w_3$ tem comprimento 1, onde $w_1 = \sum_{i=1}^{n-2} a_i u''_i$, $w_2 = \lambda_1 u''_{n-1} + \lambda_2 u''_n = \lambda_1 v''_1 + \lambda_2 v''_2$ e $w_3 = \sum_{i=3}^{m} b_i v''_i$, isto é, contar os vetores $w \in \mathscr{C}$, tais que $|w|^2 = |w'_1|^2 + s + |w'_2|^2 =$. Daí, o número de vetores de comprimento 1, dessa forma, do reticulado $\mathscr{C}$, tais que $w_1 = 0$ é $\text{Kiss}(\mathscr{B})$ e o número de vetores de comprimento 1, dessa forma, do reticulado $\mathscr{C}$, tais que $w_3 = 0$ é $\text{Kiss}(\mathscr{A})$. Temos pelo item anterior que, se $w'_1 \neq 0$ e $w'_2 \neq 0$, então w terá comprimento maior que 1. Daí, segue que $\text{Kiss}(\mathscr{C}) = \text{Kiss}(\mathscr{A}) + \text{Kiss}(\mathscr{B}) - 6$. Como o reticulado Λ_2 tem 6 vetores de comprimento 1, temos que $\text{Kiss}(\Lambda_2) = 6$. Logo, podemos concluir que $\text{Kiss}(\mathscr{C}) = \text{Kiss}(\mathscr{A}) + \text{Kiss}(\mathscr{B}) - \text{Kiss}(\Lambda_2)$.

5. Como a distância mínima do reticulado $\mathscr{C}$ é igual a 1, temos que o raio de empacotamento deste é $\frac{1}{2}$, daí, por definição, temos que $\delta(\mathscr{C}) = \frac{(\frac{1}{2})^{n+m-2}}{Vol(\mathscr{C})}$. Como os reticulados $\mathscr{A}$, $\mathscr{B}$ e Λ_2 têm distância mínima igual a 1, os raios de empacotamentos destes também são iguais a $\frac{1}{2}$. Assim, temos $\delta(\mathscr{A}) = \frac{(\frac{1}{2})^n}{Vol(\mathscr{A})}$, $\delta(\mathscr{B}) = \frac{(\frac{1}{2})^m}{Vol(\mathscr{B})}$ e $\delta(\Lambda_2) = \frac{(\frac{1}{2})^2}{Vol(\Lambda_2)}$. Sabemos que $Vol(\mathscr{C}) = \frac{Vol(\mathscr{A})Vol(\mathscr{B})}{Vol(\Lambda_2)}$, por outro lado, $Vol(\mathscr{C}) = \frac{(\frac{1}{2})^{n+m-2}}{\delta(\mathscr{C})}$. Assim,

$$\frac{Vol(\mathscr{A})Vol(\mathscr{B})}{Vol(\Lambda_2)} = \frac{(\frac{1}{2})^{n+m-2}}{\delta(\mathscr{C})} \Rightarrow \frac{\frac{(\frac{1}{2})^n}{\delta(\mathscr{A})}\frac{(\frac{1}{2})^m}{\delta(\mathscr{B})}}{\frac{(\frac{1}{2^2})}{\delta(\Lambda_2)}} = \frac{2^{-n-m+2}}{\delta(\mathscr{C})}$$

$$\Rightarrow \frac{\delta(\mathscr{C})(\frac{1}{2^n})(\frac{1}{2^m})}{\delta(\mathscr{A})\delta(\mathscr{B})} = 2^{-n-m+2}\frac{2^{-2}}{\delta(\Lambda_2)} \Rightarrow \frac{\delta(\mathscr{C})2^{-n-m}}{\delta(\mathscr{A})\delta(\mathscr{B})} = 2^{-n-m+2}\frac{2^{-2}}{\delta(\Lambda_2)}$$

$$\Rightarrow \frac{\delta(\mathscr{C})}{\delta(\mathscr{A})\delta(\mathscr{B})} = \frac{2^{-n-m}2^2 2^{-2}}{2^{-n-m}\delta(\Lambda_2)} \Rightarrow \frac{\delta(\mathscr{C})}{\delta(\mathscr{A})\delta(\mathscr{B})} = \frac{1}{\delta(\Lambda_2)}$$

Logo,

$$\Rightarrow \delta(\mathscr{C}) = \frac{\delta(\mathscr{A})\delta(\mathscr{B})}{\delta(\Lambda_2)}.$$

3.4.1 Um caso particular da colagem em dimensão 2

Seja $\mathscr{H}$ um reticulado de $\mathbb{R}^n$, com base $\{u_1,\ldots,u_n\}$. Sem perda de generalidade, podemos assumir que seu raio de empacotamento é igual a $\frac{1}{2}$, isto é, a distância mínima de $\mathscr{H}$ é igual a 1. Seja $u_i=(a_{i1},...,a_{in})$, com $i=1,\ldots,n$ e $w=(c_1,\ldots,c_n)\in\mathscr{H}$ um vetor de comprimento 1. Podemos escrever $w=b_1u_1+\cdots+b_nu_n$ para certos $b_i\in\mathbb{Z}$, com $i=1,\ldots,n$. Defina $v_i=(a_{i1},\ldots,a_{in},0)$, com $i=1,\ldots,n$ e $v_{n+1}=(\frac{c_1}{2},\ldots,\frac{c_n}{2},\frac{\sqrt{3}}{2})$. Como $\sum_{i=1}^{n}c_i^2=|w|^2=1$ temos que $|v_{n+1}|^2=\sum_{i=1}^{n}\left(\frac{c_i}{2}\right)^2+\left(\frac{\sqrt{3}}{2}\right)^2=\frac{1}{4}\sum_{i=1}^{n}c_i^2+\frac{3}{4}=\frac{1}{4}+\frac{3}{4}=1$, isto é, $|v_{n+1}|=1$. Dizemos que o reticulado $\mathscr{H}$ possui matriz geradora igual a

$$A=\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$$

Considere agora a matriz

$$A'=\begin{pmatrix} a_{11} & \ldots & a_{1n} & 0 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n1} & \ldots & a_{nn} & 0 \\ \frac{c_1}{2} & \cdots & \frac{c_n}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$$

Daí, temos que a matriz A' é invertível, já que a matriz A é invertível. Logo, definimos o reticulado estendido $\mathscr{H}'\subset\mathbb{R}^{n+1}$, como sendo um reticulado de posto $n+1$ com matriz geradora A'.

Lema 3.5 *Com a notação acima, podemos garantir que o comprimento mínimo de qualquer vetor não nulo do reticulado estendido $\mathscr{H}'$ é igual a 1. Equivalentemente, o raio de empacotamento de $\mathscr{H}'$ é igual a $\frac{1}{2}$.*

Prova: De fato, seja $v=d_1v_1+\cdots+d_nv_n+d_{n+1}v_{n+1}$ um vetor não nulo de $\mathscr{H}'$, onde $v_i=(a_{i1},\ldots,a_{in},0)$, com $i=1,\ldots,n$ e $v_{n+1}=(\frac{c_1}{2},\ldots,\frac{c_n}{2},\frac{\sqrt{3}}{2})$. Seja $u'=(c'_1,\ldots,c'_n)\in\mathscr{H}$ dado

por $u' = d_1u_1 + \cdots + d_nu_n$. Se $d_{n+1} = 0$, então temos

$$\begin{aligned}
|v|^2 &= |d_1v_1 + \cdots + d_nv_n|^2 = |d_1(a_{11}, \ldots, a_{1n}, 0) + \cdots + d_n(a_{n1}, \ldots, a_{nn}, 0)|^2 \\
&= |(d_1a_{11}, \ldots, d_1a_{1n}, 0) + (d_2a_{21}, \ldots, d_2a_{2n}, 0) + \cdots + (d_na_{n1}, \ldots, d_na_{nn}, 0)|^2 \\
&= |(d_1a_{11} + d_2a_{21} + \cdots + d_na_{n1}, \ldots, d_1a_{1n} + d_2a_{2n} + \cdots + d_na_{nn}, 0)|^2 \\
&= (d_1a_{11} + d_2a_{21} + \cdots + d_na_{n1})^2 + \cdots + (d_1a_{1n} + d_2a_{2n} + \cdots + d_na_{nn})^2 + 0^2 \\
&= (d_1a_{11} + d_2a_{21} + \cdots + d_na_{n1})^2 + \cdots + (d_1a_{1n} + d_2a_{2n} + \cdots + d_na_{nn})^2 \\
&= |(d_1a_{11} + d_2a_{21} + \cdots + d_na_{n1}, \ldots, d_1a_{1n} + d_2a_{2n} + \cdots + d_na_{nn})|^2 \\
&= |(d_1a_{11}, \ldots, d_1a_{1n}) + (d_2a_{21}, \ldots, d_2a_{2n}) + \cdots + (d_na_{n1}, \ldots, d_na_{nn})|^2 \\
&= |d_1(a_{11}, \ldots, a_{1n}) + \cdots + d_n(a_{n1}, \ldots, a_{nn})|^2 \\
&= |d_1u_1 + \cdots + d_nu_n|^2 = |u'|^2 \geq 1
\end{aligned}$$

pois, $u' \in \mathscr{H}$. Se $|d_{n+1}| \geq 1$, sem perda de generalidade, podemos assumir que $d_{n+1} = -1$, pois $d_{n+1} \in \mathbb{Z}$. Seja $w = (c_1, \ldots, c_n) \in \mathscr{H}$ um vetor de comprimento 1, com $w = b_1u_1 + \cdots + b_nu_n$, onde os $b_i \in \mathbb{Z}$. Seja $u = (2d_1 - b_1)u_1 + \cdots + (2d_n - b_n)u_n$. Se $u \neq 0$ então $|u| \geq 1$, pois $u \in \mathscr{H}$. Veja que:

$$\begin{aligned}
|u|^2 &= |(2d_1 - b_1)u_1 + \cdots + (2d_n - b_n)u_n|^2 \\
&= |(2d_1u_1 - b_1u_1) + \cdots + (2d_nu_n - b_nu_n)|^2 \\
&= |2d_1u_1 + \cdots + 2d_nu_n - (b_1u_1 + \cdots + b_nu_n)|^2 \\
&= |2(d_1u_1 + \cdots + d_nu_n) - (b_1u_1 + \cdots + b_nu_n)|^2 \\
&= |2u' - w|^2 \\
&= |2(c'_1, \ldots, c'_n) - (c_1, \ldots, c_n)|^2 \\
&= |(2c'_1, \ldots, 2c'_n) - (c_1, \ldots, c_n)|^2 \\
&= |(2c'_1 - c_1, \ldots, 2c'_n - c_n)|^2 \\
&= (2c'_1 - c_1)^2 + \cdots + (2c'_n - c_n)^2
\end{aligned}$$

e

$$\begin{aligned}
|v|^2 &= |d_1v_1+\cdots+d_nv_n-v_{n+1}|^2 \\
&= |(c'_1,\ldots,c'_n,0)-(c_1/2,\ldots,c_n/2,\sqrt{3}/2)|^2 \\
&= |(c'_1-c_1/2,\ldots,c'_n-c_n/2,0-\sqrt{3}/2|^2 \\
&= (c'_1-c_1/2)^2+\cdots+(c'_n-c_n/2)^2+(0-\sqrt{3}/2)^2 \\
&= \left(\frac{2c'_1-c_1}{2}\right)^2+\cdots+\left(\frac{2c'_n-c_n}{2}\right)^2+\frac{3}{4} \\
&= \frac{1}{4}\left((2c'_1-c_1)^2+\cdots+(2c'_n-c_n)^2\right)+\frac{3}{4} \\
&= \frac{1}{4}|u|^2+\frac{1}{4}\geq\frac{1}{4}1+\frac{3}{4}=1
\end{aligned}$$

pois, temos que $|u|^2\geq 1$. Logo, $|v|\geq 1$. Se $u=0$ então sendo $u=2u'-w$ temos que $w=2u'\Rightarrow |w|=2|u'|\geq 2.1=2$, isto é, $|w|\geq 2$ que contradiz o fato de $|w|=1$. Portanto, se $|d_{n+1}|\geq 1$ então temos que $|v|\geq 1$. Logo, o comprimento mínimo de qualquer vetor não nulo do reticulado estendido $\mathscr{H}'$ é igual a 1.

Lema 3.6 *Seja $\mathscr{H}$ um reticulado de $\mathbb{R}^n$ com base $\{u_1,\ldots,u_n\}$, onde $u_i=(a_{i1},...,a_{in})$, $i=1,\ldots,n$ e seja $\mathscr{H}'\subset\mathbb{R}^{n+1}$ o reticulado estendido. Então, $Vol(\mathscr{H}')=\frac{\sqrt{3}}{2}Vol(\mathscr{H})$.*

Prova: Temos que o reticulado $\mathscr{H}$ possui matriz geradora igual a

$$A=\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$$

e o reticulado estendido $\mathscr{H}'$ possui matriz geradora igual a

$$A'=\begin{pmatrix} a_{11} & \ldots & a_{1n} & 0 \\ \vdots & \ddots & \vdots & \vdots \\ a_{n1} & \ldots & a_{nn} & 0 \\ \frac{c_1}{2} & \ldots & \frac{c_n}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$$

Daí, por definição $Vol(\mathscr{H})=|\det A|$ e $Vol(\mathscr{H}')=|\det A'|$. Assim, como $|\det A'|=\frac{\sqrt{3}}{2}|\det A|$ temos que $Vol(\mathscr{H}')=\frac{\sqrt{3}}{2}Vol(\mathscr{H})$.

Teorema 3.4 *Se $\mathscr{H} \subset \mathbb{R}^n$ é um reticulado de posto n de densidade de centro δ, então $\mathscr{H}' \subset \mathbb{R}^{n+1}$ é um reticulado de posto $n+1$ de densidade de centro igual a $\delta/\sqrt{3}$.*

Prova: Sabemos que, por definição, $\delta(\mathscr{H}) = \dfrac{\rho^n}{Vol(\mathscr{H})}$, onde ρ é o raio de empacotamento de $\mathscr{H}$. Como $\mathscr{H}$ tem distância mínima igual a 1, temos que seu raio de empacotamento é igual a $\dfrac{1}{2}$, daí $\delta(\mathscr{H}) = \dfrac{(\frac{1}{2})^n}{Vol(\mathscr{H})}$. Pelo Lema 3.5 o raio de empacotamento de $\mathscr{H}'$ é igual a $\dfrac{1}{2}$, daí $\delta(\mathscr{H}') = \dfrac{(\frac{1}{2})^{n+1}}{Vol(\mathscr{H}')}$. Temos que $Vol(\mathscr{H}') = \frac{\sqrt{3}}{2}Vol(\mathscr{H})$ pelo Lema 3.6. Assim,

$$\delta(\mathscr{H}') = \frac{(\frac{1}{2})^{n+1}}{\frac{\sqrt{3}}{2}Vol(\mathscr{H})} \Rightarrow \delta(\mathscr{H}') = \frac{(\frac{1}{2})^n(\frac{1}{2})}{\frac{\sqrt{3}}{2}Vol(\mathscr{H})} \Rightarrow \delta(\mathscr{H}') = \frac{(\frac{1}{2})^n(\frac{1}{2})}{(\frac{1}{2})\sqrt{3}Vol(\mathscr{H})}$$

$$\Rightarrow \delta(\mathscr{H}') = \frac{(\frac{1}{2})^n}{\sqrt{3}Vol(\mathscr{H})} = \frac{\delta(\mathscr{H})}{\sqrt{3}}$$

Logo, $\delta(\mathscr{H}') = \delta/\sqrt{3}$.

3.4.2 Aplicações do Teorema 3.4

Agora vamos discutir um pouco aplicações do Teorema 3.4. Além de preencher lacunas na tabela de reticulados, este pode ser usado para criar novos reticulados com densidades récordes. Para evitar números grandes que naturalmente surgem em maiores dimensões, costuma-se listar $\log_2 \delta$ em vez de δ, onde δ denota densidade de centro. Com isto em mente, segue do Teorema 3.4 que começando com um reticulado n - dimensional de densidade de centro δ e estendendo este k-vezes sucessivas, a densidade de centro $\delta^{(k)}$ resultando de um reticulado $(n+k)$ - dimensional satisfaz $\log_2 \delta^{(k)} = \log_2 \delta - k\log_2 \sqrt{3}$.

As aplicações foram baseadas em [Conway & Sloane 1999]

1. Em dimensões 64, a densidade de centro do reticulado satisfaz $\log_2 \delta = 25,36$. Estendendo o reticulado correspondente 4 vezes sucessivas, obtemos um reticulado de dimensão 68 tal que $\log_2 \delta = 22,19$. O récorde atual, até então conhecido, em dimensão 68 satisfaz $\log_2 \delta = 19,88$.

2. Em dimensão 80, o récorde atual satisfaz $\log_2 \delta = 40,14$. Estendendo o reticulado correspondente 6 vezes sucessivas, obtemos um reticulado em dimensão 86 tal que $\log_2 \delta = 35,38$. O récorde atual, até então conhecido, em dimensão 86 é atingido pelo reticulado de Shimada$_{86}$, para o qual $\log_2 \delta = 34,20$.

3. Em dimensões 240, o récorde atual satisfaz $\log_2 \delta = 245$. Estendendo o reticulado correspondente 8 vezes sucessivas, obtemos um reticulado em dimensão 248 tal que $\log_2 \delta = 238,66$. O récorde atual, até então conhecido, em dimensão 248 é atingido pelo reticulado de Thompson-Smith, para o qual $\log_2 \delta \leq 196,53$.

4. Em dimensão 512, o récorde atual satisfaz $\log_2 \delta = 797,12$. Estendendo o reticulado correspondente 8 vezes sucessivas, obtemos um reticulado em dimensão 520 tal que $\log_2 \delta = 790,78$. O récorde atual, até então conhecido, em dimensão 520 é atingido pelo reticulado de Craig A_{520}^{42}, para o qual $\log_2 \delta = 767,46$.

5. Em dimensão 4096, o récorde atual satisfaz $\log_2 \delta = 11527$. Estendendo o reticulado correspondente 2 vezes sucessivas, obtemos um reticulado em dimensão 4098 tal que $\log_2 \delta = 11525,41$. O récorde atual, até então conhecido, em dimensão 4098 é atingido pelo reticulado de Craig A_{4098}^{246}, para o qual $\log_2 \delta = 11344$.

Referências Bibliográficas

ALVES, C. **Reticulados via corpos ciclotômicos**. 2005. 125f. Dissertação (Mestrado em Matemática) — Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São Paulo.

CONWAY, J. H.; SLOANE, N. J. A. **Sphere Packings, Lattices and Groups**. 3. ed. New York: Springer Verlag, 1999.

ENDLER, O. **Teoria dos corpos**. Rio de Janeiro: IMPA, 2007.

FERRARI, A. J. **Reticulados algébricos via corpos abelianos**. 2008. 105f. Dissertação (Mestrado em Matemática) — Instituto de Biociências, Letras e Ciências Exatas, Universidade Estadual Paulista, São Paulo.

FLORES, A. L.; INTERLANDO, J. C.; NOBREGA NETO, T. P. da. Uma técnica para construção de novos reticulados. A ser publicado.

MOLLIN, R. A. **Algebraic number theory**. Boca Raton: Chapman & Hall, 1999.

NAVES, L. R. B. **A densidade de empacotamentos esféricos em reticulados**. 2009. 88f. Dissertação (Mestrado profissional) — Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas, São Paulo.

SAMUEL, P. **Algebraic theory of numbers**. New York: Dover, 2008.