Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Corpos Quadráticos e Reticulados

por

João Coelho Silva Filho

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Junho/2001

João Pessoa - Pb

Corpos Quadráticos e Reticulados

por

João Coelho Silva Filho

Dissertação apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPB, como requisito parcial para obtenção do título de Mestre em Matemática.

Área de Concentração: Álgebra

Aprovada por:

Prof. Dr. Antônio de Andrade e Silva

Prof. Dr. Lenimar Nunes de Andrade

Prof. Dr. Hélio Pires de Almeida

Universidade Federal da Paraíba
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Mestrado em Matemática

Junho/2001

Agradecimentos

1. Ao meu orientador Prof. Dr. Antônio de Andrade e Silva, pela orientação eficaz neste trabalho, pela compreensão, pelo incentivo e pela valiosa colaboração para realização deste.

2. Aos professores do DM - UFPB, pelo incentivo, conhecimento e experiência transmitido, os quais foram indispensáveis para elaboração deste.

3. A todos os colegas do Curso de Mestrado, pelo incentivo e amizade. Em especial aos que contribuiram diretamente na elaboração deste.

4. À Rosimar, Sandino, Ana Paula, João Magarefe e toda a minha família, por tudo que fizeram em meu favor. Agradeço pelo apoio e incentivos recebidos e pela compreensão do motivo de tê-los privado da minha presença por vários momentos importantes de suas vidas e por me esperarem sempre, carinhosamente, de braços abertos.

5. À UEMA e à CAPES, pela colaboração financeira.

6. À todos que diretamente ou indiretamente contribuiram na realização deste trabalho.

Dedicatória

À minha mãe
"in memoriam"
Maria dos Santos
Ao meu pai
meus filhos
minha esposa e
todos os meus familiares.

Notação

$\mathbb{Z}_K$ - Anel dos inteiros de um corpo de número K

$R[x]$ - Anel dos polinômios sobre R

B - Base

$\mathbb{N}$ - 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

$\overline{\alpha}$ - Conjugado complexo de α

$\equiv$ - Congruente

$[I]$ - Classe do ideal I

$\det A$ - Determinante de A

$D(B)$ - Discriminante de B

$|$ - Divide

$\exists$ - Existe

$\lfloor \cdot \rfloor$ - Função maior inteiro

∂f - Grau do polinômio f

$[K : \mathbb{Q}]$ - Grau de K sobre $\mathbb{Q}$

$\langle x_1, \ldots, x_n \rangle$ - Ideal gerado por $x_1, \ldots, x_n$

$(K : \mathbb{Q})$ - Índice de K em $\mathbb{Q}$

$\simeq$ - Isomorfo

$N(\alpha)$ - Norma do elemento α

$N(I)$ - Norma do ideal I

$\ker f$ - Núcleo do homomorfismo f

$\forall$ - Para todo

$f_\alpha(x)$ - Polinômio caracteristico de α

$\prod$ - Produto

Λ - Retitculado

$\approx$ - Semelhante

$\backsim$ - Similar

$\sum$ - Soma

$Tr(\alpha)$ - Traço de α

$V(\Lambda)$ - Volume da região fundamental de Λ

Sumário

Introdução

Os números têm fascinado o homem há milênios. Os pitagóricos estudaram muitas propriedades dos números Naturais e o famoso teorema de Pitágoras, através da geometria, contendo um enuciado da teoria dos números. Mas, antes os babilônios já haviam notado os tríades de Pitágoras. Um tablete de barro de 1500 A.C. mostra a sofisticada técnica dos Babilônios.

Os Gregos Antigos se concentraram no estudo da Geometria, mas, se interesaram pelos números. Em 250 D.C. Diophantus de Alexandria escreveu um significante tratado em equações polinomiais, que estudava as soluções em frações, hoje chamado de equações Diofantinas. Os Hindus acrescentaram os números negativos e o zero, com a conquista de Alexandria pelos moslem, a matemática é enxertada pelas influências Grega e Hindu. No século XVI, Cardano usa os negativos e os imaginários, formando mais tarde os números complexos.

Um grande matemático da teoria dos números foi Pierre Fermat. Ele fez pequenas publicações em correspondência com outros matemáticos. Ele lançou vários desafios na teoria dos números e deixou vários teoremas cujas provas não eram conhecidas. O fato mais famoso é a equação Diofantina

$$x^n + y^n = z^n$$

que não tem solução inteira não-trivial para x, y, z e $n \geq 3$. Como não foi conhecida a prova, o teorema foi reduzido a conjectura juntamente com outros resultados. Vários estudiosos da teoria dos números atacaram esses problemas, por exemplo Kummer. Gauss citou esse fato em um trabalho de teoria dos números, o que já tinha sido observado empiricamente por Euler. Somente em 1993, o matemático inglês Andrew Wilies completou a prova que já havia 345 anos da formulação de Fermat.

No nosso trabalho, enuciaremos alguns conceitos e resultados básicos dos grupos abelianos finitamente gerados, daremos um definição abstrata de anel comutativo com

unidade, onde serão feitos alguns exemplos, entre eles os *inteiros de Gauss*, que são números complexos da forma $a + bi$, onde a e b são inteiros. Definiremos os corpos e reticulados apresentando os principais resultados necessários para a compeensão deste trabalho.

Para desenvolver esta teoria dos corpos quadráticos, apresentaremos os resultados da teoria dos números algébricos construindo os subcorpos e subanéis de $\mathbb{C}$. Um subanel de $\mathbb{C}$ é um conjunto fechado para adição, subtração, multiplicação e contém o 1. Se um número θ é um elemento de um subanel, então θ é chamado *algébrico,* se ele é raiz de algum polinômio com coeficientes inteiros e α é chamado *transcendente* se θ não é raíz de nenhum polinômio com coeficientes inteiros. $\mathbb{Z}[\theta]$ é o menor subanel de $\mathbb{C}$ contendo θ e $\mathbb{Z}$ e é chamado o subanel gerado por θ. Para abordarmos a fatoração única de um inteiro algébrico, estudaremos as funções *norma* e *traço* de um elemento θ, além, do *discriminante* da base de um corpo de números.

Um corpo quadrático é um corpo de dimensão 2. Uma base minimal de um corpo quadrático é da forma

$$\{1, \theta\},$$

onde só existem duas possibilidades para θ:

$$\theta = \sqrt{d} \text{ ou } \theta = \frac{1+\sqrt{d}}{2},$$

onde d é livre de quadrado, logo, d não divide 4 e $d \equiv 1, 2$ ou $3 (\mathrm{mod}\, 4)$. Se $d > 0$, o anel $\mathbb{Z}[\theta]$ são simples, assim trabalharemos o anel dos inteiros $\mathbb{Z}_K$ de um corpo $K = \mathbb{Q}(\theta)$ com $d < 0$, os quais apresentam figuras interesantes. A representação geométrica de $\mathbb{Z}_K$ é uma grade retangular, triangular ou quadrática, este último é quando $d = -1$, o anel dos inteiros de Gauss $\mathbb{Z}[i]$, essas grades geométrica serão identificadas como uma representação gráfica dos reticulados que estão associados a um ideal de $\mathbb{Z}_K$.

No último e principal capítulo, procuraremos os irredutíveis em $\mathbb{Z}_K$, com o objetivo de provar a fatorização única em ideais primos e relacionar primos em $\mathbb{Z}$ com ideais primos em $\mathbb{Z}_K$. Há duas possibilidades para um ideal de $\mathbb{Z}_K$ ou ele é gerado por 2 elementos ou é principal. Fechando o trabalho, provaremos o Lema de Minkowski que garante a existência de um conjunto conveniente S de pontos não-nulos de um reticulados Λ, relacionado com a região fundamental do reticulado Λ. Conhecendo os ideais e com base no Lema de Minkowski faremos um estudo das classes de ideais de $\mathbb{Z}_K$, estas formam um

grupo abeliano e se o grupo formado pela classe de ideais de $\mathbb{Z}_K$ é trivial, então todo ideal de $\mathbb{Z}_K$ é principal. Onde $\mathbb{Z}_K$ é um domínio de fatoração única. Em geral,o grupo gerado pelas classes de ideais é cíclico, temos o caso $\mathbb{Z}_K = \mathbb{Z}\left[\sqrt{-21}\right]$, onde o grupo das classe de ideais é o Grupo de Klein. Será apresentado um algoritmo de tentativas e erros para podermos investigar o conjunto de geradores da classe de ideais, ou seja, o grupo de classe $\mathcal{C}$.

Capítulo 1

Resultados Básicos

Neste capítulo apresentaremos alguns resultados básicos da teoria dos grupos, anéis e módulos que serão necessários para os próximos capítulos, o leitor interessado em mais detalhes deve consultar [3, 5, 7]. Apresentaremos também a definição, propriedades e resultados sobre reticulados que serão necessários para o desenvolvimento deste trabalho.

1.1 Grupos

Um conjunto não vazio G munido com uma operação binária

$$\begin{aligned} * : \quad & G \times G \longrightarrow G \\ & (a, b) \longmapsto a * b \end{aligned}$$

é um *semigrupo* se a operação binária é associativa, isto é, $a * (b * c) = (a * b) * c$, para todos $a, b, c \in G$.

Um semigrupo G é um *grupo* se as seguintes condições são satisfeitas:

1. Existe $e \in G$ tal que $e * a = a$, para todo $a \in G$.

2. Para todo $a \in G$, existe $b \in G$ tal que $b * a = e$.

O grupo é *abeliano* ou *comutativo* se também vale

3. $a * b = b * a$, para todos $a, b \in G$.

Com o objetivo de simplificar a notação usaremos ab em vez de $a * b$. A *ordem* de um grupo G é a cardinalidade do conjunto G e denotaremos por $|G|$. Se G e H são dois

grupos, então o *produto direto* de G com H, denotado por $G \times H$, é o conjunto de todos os pares ordenados (g, h), onde $g \in G$ e $h \in H$, com a operação binária

$$(g, h)\,(g', h') = (gg', hh')\,.$$

É fácil mostrar que $G \times H$ é um grupo com elemento identidade (e, e) e o elemento inverso de (g, h) é (g^{-1}, h^{-1}). Assim, $G^2 = G \times G$. Generalizando, temos

$$G^n = G \times G \times \cdots \times G.$$

Sejam G um grupo e H um subconjunto de G. Dizemos que H é um *subgrupo* de G, em símbolos $H \leq G$, se as seguintes condições são satisfeitas:

1. $H \neq \emptyset$;

2. $ab^{-1} \in H$, para todos $a, b \in H$.

Note que, se G é um grupo de ordem finita, então um subconjunto não vazio H de G é um subgrupo se, e somente se, H é fechado com relação à operação de G.

Sejam G um grupo e H um subgrupo de G. Dado $a \in G$, o conjunto

$$aH = \{ah : \forall h \in H\}$$

é chamado a *classe lateral à esquerda* de H em G determinada por a. De modo semelhante, podemos definir a classe lateral à direita Ha de H em G. O conjunto de todas as classes laterais à esquerda de H em G formam uma partição de G, que denotamos por $\frac{G}{H}$.

Dados $a, b \in G$, dizemos que a *é congruente a* b *módulo* H se $a^{-1}b \in H$, que denotamos por $a \equiv b (\mathrm{mod}\, H)$. É fácil verificar que $\equiv$ é uma relação de equivalência em G e que a classe de equivalência determinada por a é igual a classe lateral à esquerda aH. O elemento a é chamado um *representante* da classe de equivalência. É também fácil verificar que existe uma correspondência biunívoca entre o conjunto das classes laterais à esquerda de H em G e o conjunto das classes laterais à direita de H em G. A cardinalidade do conjunto das classes laterais à esquerda (ou à direita) de H em G é chamado o *índice* de H em G, que denotamos por $(G : H)$.

Sejam G um grupo e H um subgrupo de G. Dizemos que H é um *subgrupo normal* de G, em símbolos $H \trianglelefteq G$, se

$$Ha = aH, \forall a \in G,$$

isto é,

$$aHa^{-1} = H, \forall a \in G.$$

Sejam G um grupo e H um subgrupo de G. Então $\frac{G}{H}$ é um grupo com operação $aHbH = abH$, para todos $a, b \in G$, se, e somente se, H é um subgrupo normal de G. Neste caso, $\frac{G}{H}$ é chamado o *grupo quociente* de G por H.

Um grupo abeliano aditivo G é *finitamente gerado* se existirem $g_1, \ldots, g_n$ em G tais que

$$g = a_1 g_1 + \cdots + a_n g_n, a_i \in \mathbb{Z}$$

para todo $g \in G$, isto é, G é finitamente gerado se $G = \langle g_1, \ldots, g_n \rangle$. Quando $G = \langle g \rangle$, para algum $g \in G$, dizemos que G é *cíclico* A ordem de um elemento $g \in G$, em símbolos $o(g)$, é definida como $o(g) = |\langle g \rangle|$. É fácil verificar que se $o(g)$ é finita, então $o(g)$ é igual ao menor inteiro positivo k tal que $g^k = e$.

Sejam G e H dois grupos. Uma função φ de G em H é um *homomorfismo de grupos* se

$$\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2),$$

para todos $g_1, g_2 \in G$. Neste caso, a *imagem* de φ é o conjunto

$$\begin{aligned} \operatorname{Im}\varphi &= \{h : h = \varphi(g) \text{ para algum } g \in G\} \\ &= \{\varphi(g) : g \in G\}. \end{aligned}$$

O *núcleo* de φ é o conjunto

$$\ker\varphi = \{g \in G : \varphi(g) = e\}.$$

É fácil verificar que $\operatorname{Im}\varphi$ é um subgrupo de H e $\ker\varphi$ é um subgrupo normal de G.

Um homomorfismo de grupos $\varphi : G \longrightarrow H$ é um *isomorfismo* se φ é bijetora. Quando existir um isomorfismo entre G e H dizemos que G e H são *isomorfos* e denotamos por $G \simeq H$. Um *endomorfismo* de um grupo G é um homomorfismo $\varphi : G \longrightarrow G$. Denotamos por

$$\operatorname{End}(G) = \{\varphi : G \longrightarrow G : \varphi \text{ é um homomorfismo}\}.$$

Um *automorfismo* de um grupo G é um isomorfismo $\varphi : G \longrightarrow G$. Denotamos por

$$\operatorname{Aut}(G) = \{\varphi : G \longrightarrow G : \varphi \text{ é um isomorfismo}\}.$$

Teorema 1.1 [5] *Sejam G, H dois grupos e $\varphi : G \longrightarrow H$ um homomorfismo de grupos. Então*

$$\frac{G}{\ker \varphi} \simeq \operatorname{Im} \varphi.$$

■

Dizemos que os elemento $g_1, \ldots, g_n$ de um grupo G são *linearmente independentes* sobre $\mathbb{Z}$ se

$$a_1 g_1 + \cdots + a_n g_n = 0 \Rightarrow a_i = 0, \forall i = 1, \ldots, n.$$

Um conjunto $\{g_1, \ldots, g_n\}$ de elementos linearmente independentes de G que gera G, é chamado uma $\mathbb{Z}$-*base* de G. É fácil verificar que se G é um grupo abeliano que possui uma $\mathbb{Z}$-base com n elementos, então

$$G \simeq \mathbb{Z}^n.$$

Um grupo abeliano que possui uma $\mathbb{Z}$-base com n elementos é chamado um *grupo abeliano livre* de posto n.

1.2 Anéis

Nesta seção apresentaremos alguns resultados clássicos da teoria de anéis que serão necessários para a compreensão desta dissertação.

Um *anel* é um conjunto não vazio R equipado com duas operações binárias adição $(x, y) \to x + y$ e multiplicação $(x, y) \to xy$ tal que as seguintes propriedades valem:

1. R é um grupo comutativo sob a adição.
2. $x(yz) = (xy)z$, para todos $x, y, z \in R$.
3. $x(y + z) = xy + xz$, $(x + y)z = xz + yz$, para todos $x, y, z \in R$.

   Se um anel R satisfaz as propriedades:

4. Existe $1 \in R$ tal que $x1 = 1x = x$, para todo $x \in R$, dizemos que R é um *anel com identidade.*
5. $xy = yx$, para quaisquer $x, y \in R$, dizemos que R é um *anel comutativo*

   Se um anel R satisfaz a propriedade:

6. Para todos $x, y \in R$, $xy = 0 \Rightarrow x = 0$ ou $y = 0$, dizemos que R é um *anel sem divisores de zero*. Caso contrário, dizemos que R é um *anel com divisores de zero*.

Dizemos que um elemento $x \in R$, $x \neq 0$, é *regular* se x não é divisor de zero.

Se R é um anel comutativo, com identidade e sem divisores de zero, dizemos que R é um *domínio*. Um elemento $x \in R$ é dito uma *unidade* de R se existir $y \in R$ tal que $xy = yx = 1$. Denotaremos por $U(R)$ o conjunto de todas as unidades de R. Se $U(R) = R^* = R - \{0\}$, dizemos que R é um *corpo*. Salvo menção explicita em contrário, todos os anéis considerados neste trabalho serão comutativos com identidade.

Um subconjunto não vazio S de um anel R é um *subanel* de R se as seguintes condições são satisfeitas:

1. para todos $x, y \in S$, tem-se $x - y \in S$;
2. para todos $x, y \in S$, tem-se $xy \in S$;
3. $1 \in S$.

Um subconjunto não vazio I de um anel R é um *ideal* de R se as seguintes condições são satisfeitas:

1. para todos $x, y \in I$, tem-se $x - y \in I$;
2. Para todo $x \in I$ e $r \in R$, tem-se $rx \in I$.

Sejam R e S dois anéis. Uma função ϕ de R em S é um *homomorfismo de anéis* se as seguintes condições são satisfeitas:

1. $\phi(x + y) = \phi(x) + \phi(y)$, para todos $x, y \in R$;
2. $\phi(xy) = \phi(x)\phi(y)$, para todos $x, y \in R$.

Um ideal I de R é dito *próprio* se $I \neq R$. Um ideal I de R é dito *finitamente gerado* se existir um subconjunto finito $S = \{x_1, x_2, \ldots, x_n\}$ de R tal que

$$\begin{aligned} I &= \langle S \rangle \\ &= Rx_1 + Rx_2 + \cdots + Rx_n \\ &= \{\sum_{i=1}^{n} r_i x_i : r_i \in R\}. \end{aligned}$$

O ideal $I = Rx = \langle x \rangle$ é chamado *ideal principal* gerado por $x \in R$. Um domínio R é um *domínio de ideais principais* se todo ideal de R é principal.

Sejam R um anel e $x, y \in R$, com $x \neq 0$. Dizemos que x *divide* y, em símbolos $x \mid y$, se existir $z \in R$ tal que $y = xz$. Se $y = xz$, com $x, z \in R - U(R)$, dizemos que x é um *divisor próprio* de y. Sejam $x, y \in R^*$, dizemos que x e y são *associados* se existir $u \in U(R)$ tal que $y = ux$.

Lema 1.1 [5] *Sejam R um domínio e $x, y \in R^*$. Então*:

1. *$x \in U(R)$ se, e somente se, $\langle x \rangle = \langle 1 \rangle = R$;*
2. *x divide y se, e somente se, $\langle y \rangle \subseteq \langle x \rangle$;*
3. *x e y são associados se, e somente se, $\langle y \rangle = \langle x \rangle$;*
4. *x é um divisor próprio de y se, e somente se, $\langle y \rangle \subset \langle x \rangle \subset \langle 1 \rangle$.* ■

Sejam I e J dois ideais de R. Então

$$I + J = \{x + y : x \in I \text{ e } y \in J\}$$

e

$$IJ = \{\sum_{i=1}^{n} x_i y_i : x_i \in I, y_i \in J \text{ e } n \in \mathbb{N}\}$$

são ideais de R. Note que, a soma e a multiplicação de ideais podem, de forma indutiva, ser generalizada para qualquer número finito de ideais.

Um ideal P de um anel R é um *ideal primo* de R se $P \neq R$ e para todos $x, y \in R$ e $xy \in P$, tem-se $x \in P$ ou $y \in P$.

Teorema 1.2 [5] *Sejam R um anel e P um ideal de R. Então as seguintes condições são equivalentes*:

1. *P é um ideal primo de R;*
2. *Se I e J são ideais de R tais que $IJ \subseteq P$, então $I \subseteq P$ ou $J \subseteq P$;*
3. *$\frac{R}{P}$ é um domínio.* ■

Um ideal não nulo M de um anel R é um *ideal maximal* de R se $M \neq R$ e se J é um ideal de R tal que $M \subseteq J \subseteq R$, então $M = J$ ou $J = R$. Dizemos que R é um *anel local* se R tem um único ideal maximal. Neste caso, $U(R) = R - M$. Um ideal M de um anel R é um *ideal minimal* de R se $M \neq R$ e J é um ideal de R tal que $\{0\} \subseteq J \subseteq M$, então $J = \{0\}$ ou $J = M$.

Proposição 1.1 *Seja I um ideal próprio de R. Então I é maximal se, e somente se, $\langle I, r\rangle = R$, para todo $r \in R - I$.* ■

Observação 1.1 *Todo ideal maximal é primo.*

Teorema 1.3 [5] *Sejam R um anel e M um ideal de R. Então M é maximal se, e somente se, $\frac{R}{M}$ é um corpo.* ■

Seja R um anel. Um elemento $p \in R^*$ é *irredutível* sobre R se as seguintes condições são satisfeitas:

1. $p \notin U(R)$;
2. Se $p = bc$, então $b \in U(R)$ ou $c \in U(R)$, isto é, p não tem divisores próprios.

Proposição 1.2 *Seja R um domínio. Então as seguintes condições são equivalentes*:

1. *Para cada $x \in R^*$, com $x \notin U(R)$, o processo de fatoração de x termina após um número finito de passos e resulta na fatoração $x = p_1 \cdots p_k$ de x em fatores irredutíveis de R;*
2. *Se $\langle x_1\rangle \subset \langle x_2\rangle \subset \cdots \subset \langle x_n\rangle \subset \cdots$ é uma seqüência estritamente crescente, então existe $n_0 \in \mathbb{N}$ tal que $\langle x_n\rangle = \langle x_{n_0}\rangle$, para todo $n \geq n_0$.*

Prova. (1. $\Rightarrow$ 2.) Suponhamos que

$$\langle x_1\rangle \subset \langle x_2\rangle \subset \cdots \subset \langle x_n\rangle \subset \cdots$$

seja uma seqüência estritamente crescente infinita. Então $\langle x_n\rangle \subset \langle 1\rangle$, para todo $n \in \mathbb{N}$, pois $\langle x_n\rangle \subset \langle x_{n+1}\rangle \subset \langle 1\rangle$. Como $\langle x_{n-1}\rangle \subset \langle x_n\rangle$ temos que x_n é um divisor próprio de x_{n-1}, digamos $x_{n-1} = x_n y_n$, com $x_n, y_n \notin U(R)$. Assim,

$$x_1 = x_2 y_2 = x_3 y_3 x_2 = x_4 y_4 y_3 x_2 = \cdots .$$

Logo, o processo de fatoração de x_1 não termina após um número finito de passos.

(2. $\Rightarrow$ 1.) Suponhamos que $x \in R^*$ e $x \notin U(R)$. Se x é irredutível, nada há para provar. Se não, existem $x_1, x_2 \in R - U(R)$ tais que $x = x_1x_2$. Se x_1 e x_2 são irredutíveis acabou. Caso contrário, pelo menos um dos dois é redutível, digamos x_1, assim, existem $x_{11}, x_{12} \in R - U(R)$ tais que $x_1 = x_{11}x_{12}$, e assim por diante. Agora, vamos verificar que este processo termina. Como $x = x_1x_2$ temos que

$$\langle x \rangle \subset \langle x_1 \rangle \subset R.$$

Pela fatoração de x_1, obtemos

$$\langle x \rangle \subset \langle x_1 \rangle \subset \langle x_{11} \rangle \subset R.$$

Assim, se este processo não terminar, obtemos uma seqüência estritamente crescente infinita

$$\langle x \rangle \subset \langle x_1 \rangle \subset \langle x_{11} \rangle \subset \cdots \subset R.$$

■

Seja R um anel. Um elemento $p \in R$ é *primo* sobre R se as seguintes condições são satisfeitas

1. $p \notin U(R)$;
2. Se p divide ab, então p divide a ou p divide b.

Observação 1.2 *Todo elemento primo não nulo é irredutível.*

Um domínio R é chamado um *domínio de fatoração única* se as seguintes condições são satisfeitas:

1. Para todo $a \in R^*$ e $a \notin U(R)$, existem elementos irredutíveis $p_i \in R$, $1 \leq i \leq n$, tais que
$$a = \prod_{i=1}^{n} p_i.$$
2. Dadas duas fatorações em irredutíveis de R,
$$\prod_{i=1}^{n} p_i = \prod_{j=1}^{m} q_j,$$
então $m = n$ e existe uma permutação σ de $\{1, \ldots, n\}$ tal que $p_i = uq_{\sigma(i)}$, onde $u \in U(R)$.

Proposição 1.3 [5] *Seja R um domínio. Suponhamos que a fatoração exista em R. Então R é um domínio de fatoração única se, e somente se, qualquer elemento irredutível é primo.* ■

Proposição 1.4 [5] *Se R é domínio de ideais principais, então R é um domínio de fatoração única.* ■

Uma *função Euclidiana* para um domínio R é uma função $\varphi : R^* \longrightarrow \mathbb{Z}$ tal que

1. Se $a, b \in R^*$ e a divide b, então $\varphi(a) \leq \varphi(b)$;

2. Se $a, b \in R$, com $b \neq 0$, então existem $q, r \in R$ tais que

$$a = bq + r, \text{ onde } r = 0 \text{ ou } \varphi(r) < \varphi(b).$$

Exemplo 1.1 *Seja*

$$R = \mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$$

o anel dos inteiros de Gauss. Então a função $\varphi : R^* \longrightarrow \mathbb{Z}$ definida por

$$\varphi(\alpha) = a^2 + b^2,$$

onde $\alpha = a + bi$, é Euclidiana. De fato, sejam $\alpha, \beta \in R^*$ e se β divide α, então existe $\gamma \in R^*$ tal que $\alpha = \beta\gamma$. Como $|\gamma|^2 \geq 1$ temos que

$$\varphi(\beta) \leq \varphi(\beta)\varphi(\gamma) = \varphi(\beta\gamma) = \varphi(\alpha).$$

Por outro lado, como podemos identificar $\mathbb{C}$ com o plano, temos que cada $\frac{\alpha}{\beta} \in \mathbb{C}$ está no interior ou na fronteira de um quadrado com diagonal de comprimento $\sqrt{2}$. Assim, existe um vértice q com distância menor que ou igual a $\frac{\sqrt{2}}{2}$ de $\frac{\alpha}{\beta}$. Logo,

$$\left|\frac{\alpha}{\beta} - q\right| \leq \frac{\sqrt{2}}{2} < 1.$$

Tomando $r = \alpha - q\beta$, obtemos que $\alpha = q\beta + r$, onde

$$|r| = |\alpha - q\beta| = |\beta| \left|\frac{\alpha}{\beta} - q\right| < |\beta|.$$

Assim, $\varphi(r) < \varphi(\beta)$. Portanto, φ é uma função Euclidiana.

Se um domínio R tem uma função Euclidiana, dizemos que R é um *domínio Euclidiano.*

Teorema 1.4 [5] *Se R é um domínio Euclidiano, então R é um domínio de ideais principais.* ■

Seja R um anel. Um *R-módulo V* é grupo comutativo aditivo munido com uma aplicação $R \times V \to V$, $(x, v) \to xv$, tal que as seguintes propriedades valem:

1. $x(yv) = (xy)v$, para todos $x, y \in R$ e $v \in V$.

2. $x(u + v) = xu + xv$, para todo $x \in R$ e $u, v \in V$.

3. $(x + y)v = xv + yv$, para todos $x, y \in R$ e $v \in V$.

4. $1v = v$, para todo $v \in V$.

Note que, se R é um corpo, então um R-módulo é um espaço vetorial sobre R.

Exemplo 1.2 *Seja G qualquer grupo abeliano aditivo. Então é fácil verificar que G é um $\mathbb{Z}$-módulo com a operação*

$$\mathbb{Z} \times G \to G, (n, g) \to ng,$$

onde

$$ng = \begin{cases} (n-1)g + g & se\ n > 0 \\ 0 & se\ n = 0 \\ (-n)(-g) & se\ n < 0. \end{cases}$$

Um subconjunto não vazio W de um R-módulo V é um *R-submódulo* de V se as seguintes condições são satisfeitas:

1. para todos $w, v \in W$, tem-se $w - v \in W$;

2. Para todo $x \in R$ e $w \in W$, tem-se $xw \in W$.

Teorema 1.5 *Sejam G e H dois grupos abelianos. Sejam $\{g_1, \ldots, g_n\}$ uma $\mathbb{Z}$-base de G e $h_1, \ldots, h_n$ elementos arbitrários de H. Então existe um único homomorfismo de grupos $\varphi : G \to H$ tal que $\varphi(g_i) = h_i$, para todo $i = 1, 2, \ldots, n$.*

Prova. Seja $g \in G$. Como $\{g_1, \ldots, g_n\}$ é uma $\mathbb{Z}$-base de G temos que existem únicos $a_i \in \mathbb{Z}$ tais que

$$g = a_1 g_1 + \cdots + a_n g_n.$$

Definimos $\varphi : G \to H$ por

$$\varphi(g) = a_1h_1 + \cdots + a_nh_n.$$

Sendo os a_i únicos, a função φ é bem definida e $\varphi(g_i) = h_i$, pois

$$g_i = 0g_1 + \cdots + 1g_i + \cdots + 0g_n, i = 1, \ldots, n.$$

Sejam $g = a_1g_1 + \cdots + a_ng_n$ e $g' = b_1g_1 + \cdots + b_ng_n$. Então

$$g + g' = (a_1 + b_1)g_1 + \cdots + (a_n + b_n)g_n.$$

Logo,

$$\begin{aligned}
\varphi(g + g') &= (a_1 + b_1)h_1 + \cdots + (a_n + b_n)h_n \\
&= a_1h_1 + b_1h_1 + \cdots + a_nh_n + b_nh_n \\
&= (a_1h_1 + \cdots + a_nh_n) + (b_1h_1 + \cdots + b_nh_n) \\
&= \varphi(g) + \varphi(g').
\end{aligned}$$

Finalmente, se $\psi : G \to H$ é um homomorfismo tal que $\psi(g_i) = h_i$, para todo $i = 1, 2, \ldots, n$, então

$$\begin{aligned}
\psi(g) &= \psi(a_1g_1 + \cdots + a_ng_n) \\
&= a_1\psi(g_1) + \cdots + a_n\psi(g_n) \\
&= a_1h_1 + \cdots + a_nh_n \\
&= \varphi(g).
\end{aligned}$$

Como $\psi(g) = \varphi(g)$, para todo $g \in G$, temos que $\psi = \varphi$. ■

Seja V um R-módulo. Uma seqüência crescente

$$W_1 \subseteq W_2 \subseteq \cdots \subseteq W_n \subseteq \cdots$$

de R-submódulos de V é uma *cadeia crescente*. Uma seqüência crescente

$$W_1 \subset W_2 \subset \cdots \subset W_n \subset \cdots$$

de R-submódulos de V é uma *cadeia estritamente crescente*. De modo inteiramente análogo, define-se uma cadeia decrescente e cadeia estritamente decrescente. Dizemos que uma cadeia crescente

$$W_1 \subseteq W_2 \subseteq \cdots \subseteq W_n \subseteq \cdots$$

de R-submódulos de V é *estacionária* se existir $n_0 \in \mathbb{N}$ tal que

$$W_n = W_{n_0}, \forall n \geq n_0.$$

Um anel R é um *anel Noetheriano* se todo ideal de R é finitamente gerado.

Proposição 1.5 *Seja R um anel. Então as seguintes condições são equivalentes*:

1. *R é anel Noetheriano*;

2. *Toda cadeia crescente de ideais de R é estacionária*;

3. *Todo conjunto não vazio de ideais de R tem um elemento maximal.*

Prova. (1. $\Rightarrow$ 2.) Seja

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

uma cadeia crescente de ideais de R. É fácil verificar que

$$I = \bigcup_{n=1}^{\infty} I_n$$

é um ideal de R. Por hipótese, existem $a_1, \ldots, a_k \in R$ tal que

$$I = \langle a_1, \ldots, a_k \rangle.$$

Como $a_1, \ldots, a_k \in I$ temos que existem $n_{i_1}, \ldots, n_{i_k} \in \mathbb{N}$ tais que $a_1 \in I_{n_{i_1}}, \ldots, a_k \in I_{n_{i_k}}$. Tomando $n_0 = \max\{n_{i_1}, \ldots, n_{i_k}\}$ temos que $a_1, \ldots, a_k \in I_{n_0}$. Logo, $I \subseteq I_{n_0}$ assim, $I = I_{n_0}$. Portanto, $I_n = I_{n_0}, \forall n \geq n_0$.

(2. $\Rightarrow$ 3.) Seja

$$\mathcal{F} = \{I : I \text{ um ideal de } R\}$$

uma família não vazia de ideais de R. Seja $I_1 \in \mathcal{F}$. Então, se I_1 é um elemento maximal, acabou, caso contrário, existe $I_2 \in \mathcal{F}$ tal que $I_1 \subset I_2$. Se I_2 é um elemento maximal, acabou, caso contrário, existe $I_3 \in \mathcal{F}$ tal que $I_1 \subset I_2 \subset I_3$. Prosseguindo assim, e pela hipótese, $\mathcal{F}$ contém um elemento maximal $M = I_k$.

(3. $\Rightarrow$ 1.) Seja I um ideal de R. Seja

$$\mathcal{F} = \{J : J \text{ é um ideal finitamente gerado de } R \text{ e } J \subseteq I\}.$$

Como $\{0\} \in \mathcal{F}$ temos que $\mathcal{F} \neq \emptyset$. Logo, pela hipótese, $\mathcal{F}$ contém um elemento maximal M.

Afirmação: $M = I$.

De fato, suponhamos, por absurdo, que $M \subsetneq I$. Então, existe $x \in I$ e $x \notin M$. Se $L = M + \langle x \rangle \subseteq I$, então $L \in \mathcal{F}$, com $M \subsetneq L$, o que é uma contradição. ■

Exemplo 1.3 *Todo anel de ideais principais é um anel Noetheriano.*

Sejam R um anel e

$$R^{seq} = \{f = (a_i)_{i \in \mathbb{Z}_+} : a_i \in R\}$$

o conjunto das *seqüências formais* sobre R tal que $a_i \neq 0$ somente para um número finito de índices. Dados $f = (a_i)_{i \in \mathbb{Z}_+}, g = (b_i)_{i \in \mathbb{Z}_+} \in R^{seq}$, dizemos que

$$f = g \Leftrightarrow a_i = b_i, \forall i \in \mathbb{Z}_+.$$

Definimos em R^{seq} duas operações binárias, adição e multiplicação, por

$$f + g = (a_0 + b_0, a_1 + b_1, \ldots) \text{ e } fg = (c_0, c_1, \ldots),$$

onde

$$c_k = \sum_{i+j=k} a_i b_j.$$

Note que, somente um número finito de termos aparece nesta soma, pois se $i + j = k$, então $0 \leq i, j \leq k$. Com estas operações R^{seq} é um anel comutativo com identidade, o qual será chamado de *anel dos polinômios* na variável x.

Seja

$$S = \{(a, 0, 0, \ldots) : a \in R\}.$$

Então, S é um subanel de R^{seq} isomorfo a R. Assim, podemos identificar $(a, 0, 0, \ldots)$ com a. Vamos denotar ax por

$$(0, a, 0, \ldots).$$

Mais geralmente, o símbolo ax^n denota

$$(0, 0, \ldots, 0, a, 0, \ldots),$$

onde a está na $(n+1)$-ésima posição. Usando esta notação cada seqüência

$$f = (a_0, a_1, \ldots, a_n, 0, \ldots)$$

pode ser escrita de modo único na forma

$$\begin{aligned} f &= (a_0, 0, 0, \ldots) + (0, a_1, 0, \ldots) + \cdots + (0, \ldots, 0, a_n, 0, \ldots) + \cdots \\ &= a_0 + a_1 x + \cdots + a_n x^n \\ &= \sum_{i=0}^{n} a_i x^i. \end{aligned}$$

Para identificar a indeterminada x vamos denotar R^{seq} por $R[x]$.

Lema 1.2 (Critério de Eisenstein) [5] *Sejam R um domínio e*

$$f = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + a_n x^n \in R[x].$$

Se existir um ideal primo P de R tal que

1. $a_n \notin P$;
2. $a_0, a_1, \ldots, a_{n-1} \in P$;
3. $a_0 \notin P^2$,

então f é irredutível sobre R. ■

Teorema 1.6 (Kronecker) [5] *Se $f \in K[x]$ é irredutível sobre o corpo K, então existe um corpo L contendo K e as raízes de f.* ■

1.3 Reticulados

A *norma quadrática* ou *peso Euclidiano* $\|\mathbf{x}\|^2$ de um vetor $\mathbf{x} \in \mathbb{R}^n$ é a soma dos quadrados de suas componentes, isto é, $\|\mathbf{x}\|^2 = (\mathbf{x}, \mathbf{x}) = \mathbf{x}\mathbf{x}^t$, onde $(\mathbf{x}, \mathbf{x})$ é o produto interno de $\mathbf{x}$ por $\mathbf{x}$. A *distância Euclidiana quadrática* entre dois vetores $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$ é a norma quadrática de sua diferença, isto é, $d^2(\mathbf{x}, \mathbf{y}) = \|\mathbf{x} - \mathbf{y}\|^2$. Isto implica que $\mathbb{R}^n$ está munido com uma medida de distância aditiva, a qual é invariante por translação.

Uma *isometria* ou um *movimento rígido* de $\mathbb{R}^n$ é uma função $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ que preserva distância, isto é,

$$\|\varphi(\mathbf{x}) - \varphi(\mathbf{y})\| = \|\mathbf{x} - \mathbf{y}\|,$$

para todos $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. O conjunto de todas as isometrias de $\mathbb{R}^n$, denotado por $\mathrm{Isom}(\mathbb{R}^n)$, é um subgrupo do grupo simétrico $S_{\mathbb{R}^n}$. Uma *translação* por um vetor $\mathbf{x}_0 \in \mathbb{R}^n$ é um

função $t_{\mathbf{x}_0} : \mathbb{R}^n \to \mathbb{R}^n$ dado por $t_{\mathbf{x}_0}(\mathbf{x}) = \mathbf{x} + \mathbf{x}_0$, para todo $\mathbf{x} \in \mathbb{R}^n$. Uma translação é completamente determinada quando sabemos seu valor na origem, isto é,

$$t_{\mathbf{x}_0}(0) = \mathbf{x}_0.$$

É claro que $t_{\mathbf{x}_0} \in \text{Isom}(\mathbb{R}^n)$, para todo $\mathbf{x}_0 \in \mathbb{R}^n$. O conjunto das translações de $\mathbb{R}^n$, denotado por $T(\mathbb{R}^n)$, é um subgrupo normal de $\text{Isom}(\mathbb{R}^n)$. Além disso, $T(\mathbb{R}^n)$ é isomorfo ao grupo aditivo dos vetores de translações $\mathbf{x}_0 \in \mathbb{R}^n$, isto é, a função $\psi : T(\mathbb{R}^n) \to (\mathbb{R}^n, +)$ definida por $\psi(t_{\mathbf{x}_0}) = \mathbf{x}_0$ é um isomorfismo.

Uma transformação linear $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ é chamada *ortogonal* se a mesma preserva o produto interno, isto é,

$$(T(\mathbf{x}), T(\mathbf{y})) = (\mathbf{x}, \mathbf{y}),$$

para todos $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$. É claro que $T \in \text{Isom}(\mathbb{R}^n)$. O conjunto das transformações ortogonais de $\mathbb{R}^n$, denotado por $O(\mathbb{R}^n)$, é um subgrupo de $\text{Isom}(\mathbb{R}^n)$. Note que, os elementos $O(\mathbb{R}^n)$ são rotações em torno da origem e/ou reflexões através do hiperplano passando pela origem (um *hiperplano* H em $\mathbb{R}^n$ é uma translação de um subespaço W de dimensão $n-1$).

Seja $B = \{e_1, \ldots, e_n\}$ a base canônica em $\mathbb{R}^n$. Então para cada $T(e_j) \in \mathbb{R}^n$ existem únicos $r_{ij} \in \mathbb{R}$ tais que

$$T(e_j) = \sum_{i=1}^{n} r_{ij} e_i. \qquad \text{(eq1)}$$

Seja $\mathbf{O}$ a transposta da matriz dos coefientes do sistema (**??**), isto é, $\mathbf{O} = (r_{ij})$. Assim,

$$\begin{aligned} \langle T(e_i), T(e_j) \rangle &= \left\langle \sum_{k=1}^{n} r_{ki} e_k, \sum_{l=1}^{n} r_{jl} e_l \right\rangle \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} r_{ki} r_{jl} \langle e_k, e_l \rangle \\ &= \sum_{k=1}^{n} r_{ik} r_{kj}, \end{aligned}$$

pois $\langle e_k, e_l \rangle = \delta_{kl}$. Como $\langle T(e_i), T(e_j) \rangle = \langle e_i, e_j \rangle$ temos que

$$\sum_{k=1}^{n} r_{ik} r_{kj} = \delta_{ij}.$$

Portanto, $\mathbf{O}\mathbf{O}^t = \mathbf{I}$. Neste caso, as colunas (linhas) de $\mathbf{O}$ formam uma base ortonormal para $\mathbb{R}^n$. Além disso, se $\det(\mathbf{O}) = 1$ dizemos que T é uma *rotação própria*; se $\det(\mathbf{O}) = -1$

dizemos que T é uma *rotação imprópria*; se $\det(\mathbf{O}) = -1$ e $\mathbf{O}^2 = I$ dizemos que T é uma *reflexão.*

Uma *esfera* em $\mathbb{R}^n$ com centro $\mathbf{c}$ e raio ρ consiste de todos os pontos $\mathbf{x} \in \mathbb{R}^n$ tais que $\|\mathbf{x} - \mathbf{c}\|^2 = \rho^2$, isto é,

$$E_\rho(\mathbf{c}) = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x} - \mathbf{c}\|^2 = \rho^2\}.$$

O *volume* de $E_\rho(\mathbf{0})$ é definido por

$$V(E_\rho(\mathbf{0})) = \frac{\pi^{\frac{n}{2}}\rho^n}{G\left(\frac{n+2}{2}\right)},$$

onde

$$G(\alpha) = \int_0^\infty e^{-x}x^{\alpha-1}dx, \alpha > 0,$$

é a função Gama. Sendo n um inteiro positivo há dois casos a serem considerados:

1. Se n é par, digamos $n = 2k$, então

$$V(E_\rho(\mathbf{0})) = \frac{\pi^k\rho^{2k}}{k!},$$

2. Se n é ímpar, digamos $n = 2k + 1$, então

$$V(E_\rho(\mathbf{0})) = \frac{2^{2k+1}k!\pi^k\rho^{(2k+1)}}{(2k+1)!}.$$

Note que, $V(E_\rho(\mathbf{c})) = V(E_\rho(\mathbf{0}))$, pois o volume é invariante por translação.

Um *empacotamento esférico* Γ em $\mathbb{R}^n$ de raio ρ consiste de uma seqüência infinita de pontos $\mathbf{c}_1, \mathbf{c}_2, \ldots$ em $\mathbb{R}^n$, tais que $\|\mathbf{c}_i - \mathbf{c}_j\|^2 \geq 4\rho^2$ para todo $i \neq j$. Os $\mathbf{c}_i$ são os centros das esferas e ρ é o *raio de empacotamento* e, neste caso,

$$d^2_{\min}(\Gamma) = 4\rho^2,$$

onde $d^2_{\min}(\Gamma)$ é a distância Euclidiana quadrática mínima entre os elementos de Γ, isto é, a distância intraconjunto de Γ.

Um subgrupo aditivo em $\mathbb{R}^n$ é *discreto* se sua interseção com qualquer subconjunto limitado em $\mathbb{R}^n$ é finita. Um *reticulado* Λ é um subgrupo aditivo discreto em $\mathbb{R}^n$ ou, equivalentemente, os centros do empacotamento esférico de Λ formam um grupo aditivo sob a adição de vetores.

Exemplo 1.4 *$\Lambda = \mathbb{Z}^n$ é um reticulado de $\mathbb{R}^n$.*

Teorema 1.7 *Seja Λ um reticulado em $\mathbb{R}^n$. Então Λ é gerado, como $\mathbb{Z}$-módulo, por m vetores linearmente independentes sobre $\mathbb{R}$, neste caso $m \leq n$.*

Prova. Seja $\{\mathbf{x}_1, \ldots, \mathbf{x}_m\}$ um subconjunto maximal de vetores linearmente independentes de Λ sobre $\mathbb{R}$. Sejam $\Gamma = \langle \mathbf{x}_1, \ldots, \mathbf{x}_m \rangle$, $\Gamma_{m-1} = \langle \mathbf{x}_1, \ldots, \mathbf{x}_{m-1} \rangle$ e $\Lambda_{m-1} = \Lambda \cap \Gamma_{m-1}$. Então é claro que Λ_{m-1} é discreto. Portanto, se $m > 1$, podemos supor, como hipótese de indução, que Λ_{m-1} é gerado, como $\mathbb{Z}$-módulo, por l vetores linearmente independentes sobre $\mathbb{R}$, digamos $\mathbf{y}_1, \ldots, \mathbf{y}_l$. Como $\mathbf{x}_1, \ldots, \mathbf{x}_{m-1} \in \Lambda_{m-1}$ temos que $l = m - 1$. Assim, podemos substituir $\mathbf{y}_1, \ldots, \mathbf{y}_{m-1}$ por $\mathbf{x}_1, \ldots, \mathbf{x}_{m-1}$. Seja

$$T = \{\mathbf{x} \in \Lambda : \mathbf{x} = t_1\mathbf{x}_1 + \cdots + t_m\mathbf{x}_m, \ 0 \leq t_i < 1 \ \text{e} \ 0 \leq t_m \leq 1\}.$$

Então é claro que T é limitado, finito e $\mathbf{x}_m \in T$, pois Λ é discreto. Assim, podemos escolher $\mathbf{y}_m \in T$, com o último coeficiente t_m o menor possível e positivo, digamos

$$\mathbf{y}_m = c_1\mathbf{x}_1 + \cdots + c_m\mathbf{x}_m, 0 < c_m \leq 1.$$

Afirmação: $\{\mathbf{x}_1, \ldots, \mathbf{x}_{m-1}, \mathbf{y}_m\}$ é uma $\mathbb{Z}$-base de Λ.

De fato. É fácil verificar que $\{\mathbf{x}_1, \ldots, \mathbf{x}_{m-1}, \mathbf{y}_m\}$ é linearmente independente sobre $\mathbb{R}$. Dado qualquer vetor $\mathbf{x} \in \Lambda$ temos que

$$\mathbf{x} = b_1\mathbf{x}_1 + \cdots + b_{m-1}\mathbf{x}_{m-1} + b_m\mathbf{y}_m, b_i \in \mathbb{R}.$$

Como para cada i, $b_i = q_i + a_i$, onde $q_i \in \mathbb{Z}$ e $0 \leq a_i < 1$, temos que $\mathbf{x} = \mathbf{z} + \mathbf{r}$, onde

$$\mathbf{z} = q_1\mathbf{x}_1 + \cdots + q_{m-1}\mathbf{x}_{m-1} + q_m\mathbf{y}_m \ \text{e} \ \mathbf{r} = a_1\mathbf{x}_1 + \cdots + a_{m-1}\mathbf{x}_{m-1} + a_m\mathbf{y}_m.$$

Sendo $\mathbf{r} \in T$ e $a_m < b_m$ temos, pela escolha de b_m, que $a_m = 0$. Portanto, $\{\mathbf{x}_1, \ldots, \mathbf{x}_{m-1}, \mathbf{y}\}$ gera Λ. ■

Sejam G, H dois grupos abelianos livres e $f : G \to H$ um isomorfismo de grupos. Se $\{h_1, \ldots, h_m\}$ é uma $\mathbb{Z}$-base de H e $f(g_i) = h_i$, $i = 1, \ldots, m$, então é fácil verificar que $\{g_1, \ldots, g_m\}$ é uma $\mathbb{Z}$-base de G.

Teorema 1.8 *Sejam G um grupo abeliano livre de posto n e H um subgrupo próprio de G. Então H tem uma $\mathbb{Z}$-base com m elementos e $m \leq n$.*

Prova. Seja $\{g_1, \ldots, g_m\}$ uma $\mathbb{Z}$-base de G. Então existe um único homomorfismo $\sigma : G \to \mathbb{R}^n$ tal que

$$\sigma(g_i) = \mathbf{e}_i, \forall i = 1, \ldots, n \text{ e } \mathbf{e}_i \in \mathbb{R}^n.$$

É fácil verificar que σ é injetor. Logo, $G \simeq \sigma(G)$. Todo vetor $\mathbf{x} \in \mathbb{R}^n$ pode ser escrito de modo único na forma

$$\mathbf{x} = t_1\mathbf{e}_1 + \cdots + t_n\mathbf{e}_n, t_i \in \mathbb{R}.$$

Definimos $\phi : \mathbb{R}^n \to \mathbb{R}^n$ por

$$\phi(\mathbf{x}) = (t_1, \ldots, t_n).$$

Então $\phi(B_r[\mathbf{0}])$ é limitado, onde $B_r[\mathbf{0}]$ é uma bola fechada de centro $\mathbf{0}$ e raio r. Assim, existe $k \in \mathbb{R}$ tal que

$$\|\phi(\mathbf{x})\| \leq k, \forall \mathbf{x} \in B_r[\mathbf{0}].$$

Agora, se $a_1\mathbf{e}_1 + \cdots + a_n\mathbf{e}_n \in B_r[\mathbf{0}]$, $a_i \in \mathbb{Z}$, então $\|(a_1, \ldots, a_n)\| \leq k$. Logo,

$$|a_i| \leq \|(a_1, \ldots, a_n)\| \leq k, \forall i = 1, \ldots, n.$$

O número de soluções inteiras desta desigualdade é finito e, assim, $\sigma(G) \cap B_r[\mathbf{0}]$ também o é. Portanto, $\sigma(G)$ é discreto. Pelo Teorema 1.7, H tem uma $\mathbb{Z}$-base com m elementos e $m \leq n$. ■

Como todo reticulado de dimensão $m \leq n$ pode ser mergulhado (imerso como um sub-reticulado) em um reticulado de dimensão n, então salvo menção explícita em contrário, todos os reticulados e sub-reticulados deste trabalho são de dimensão n

Seja $\Gamma = \langle \mathbf{x}_1, \ldots, \mathbf{x}_n \rangle$ um reticulado em $\mathbb{R}^n$ gerado por n vetores linearmente independentes $\mathbf{x}_1, \ldots, \mathbf{x}_n$ sobre $\mathbb{R}$. Se

$$\mathbf{x}_i = (x_{i1}, \ldots, x_{in}),$$

então a matriz

$$M = [\mathbf{x}_i : 1 \leq i \leq n],$$

cujas linhas são os vetores $\mathbf{x}_i$ é chamada uma *matriz geradora* do reticulado Γ, e os elementos do reticulado Γ consistem de todos os vetores $\mathbf{u}M$, onde $\mathbf{u} \in \mathbb{Z}^n$.

Seja $\{\mathbf{y}_1, \ldots, \mathbf{y}_n\}$ qualquer $\mathbb{Z}$-base de Γ. Então existem únicos $b_{ij} \in \mathbb{Z}$ tais que

$$\mathbf{y}_j = \sum_{i=1}^{n} b_{ij}\mathbf{x}_i, 1 \leq j \leq n.$$

De modo análogo, existem únicos $a_{ij} \in \mathbb{Z}$ tais que

$$\mathbf{x}_j = \sum_{i=1}^{n} a_{ij}\mathbf{y}_i, 1 \leq j \leq n.$$

Logo,

$$\begin{aligned} \mathbf{x}_j &= \sum_{i=1}^{n} a_{ij}\mathbf{y}_i \\ &= \sum_{i=1}^{n} a_{ij} \sum_{k=1}^{n} b_{ki}\mathbf{x}_k \\ &= \sum_{k=1}^{n} \left(\sum_{i=1}^{n} a_{ij}b_{ki} \right) \mathbf{x}_k. \end{aligned}$$

Assim,

$$\sum_{i=1}^{n} a_{ij}b_{ki} = \begin{cases} 1 & \text{se } j = k \\ 0 & \text{se } j \neq k. \end{cases}$$

Se $\mathbf{A} = [a_{ij}]$ é a matriz de mudança da $\mathbb{Z}$-base $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ para a $\mathbb{Z}$-base $\{\mathbf{y}_1, \ldots, \mathbf{y}_n\}$ e $\mathbf{B} = [b_{ij}]$ é a matriz de mudança da $\mathbb{Z}$-base $\{\mathbf{y}_1, \ldots, \mathbf{y}_n\}$ para a $\mathbb{Z}$-base $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$, então

$$\det(\mathbf{A}) \det(\mathbf{B}) = \det(\mathbf{AB}) = 1.$$

Portanto, $\det(\mathbf{B}) = \pm 1$. Conclusão: toda $\mathbb{Z}$-base $\{\mathbf{y}_1, \ldots, \mathbf{y}_n\}$ de Γ pode ser obtida a partir de uma dada $\mathbb{Z}$-base $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ de Γ, onde

$$\mathbf{y}_j = \sum_{i=1}^{n} b_{ij}\mathbf{x}_i, 1 \leq j \leq n,$$

com $b_{ij} \in \mathbb{Z}$ e $\det(\mathbf{B}) = \pm 1$.

O *determinante* do reticulado Γ é o valor absoluto do determinante da matriz geradora M, isto é,

$$d(\Gamma) = |\det(M)|.$$

Note, do exposto acima, que $d(\Gamma)$ é independente da $\mathbb{Z}$-base escolhida para Γ.

Sejam Γ um reticulado de $\mathbb{R}^n$ e Λ um sub-reticulado de Γ. Sejam $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ uma $\mathbb{Z}$-base de Γ e $\{\mathbf{y}_1, \ldots, \mathbf{y}_m\}$ uma $\mathbb{Z}$-base de Λ. Como $\mathbf{y}_j \in \Gamma$ temos que existem únicos $b_{ij} \in \mathbb{Z}$ tais que

$$\mathbf{y}_j = \sum_{i=1}^{n} b_{ij}\mathbf{x}_i, 1 \leq j \leq n.$$

Se $\mathbf{B} = [b_{ij}]$, então

$$d = \det(\mathbf{B}) = \frac{d(\Gamma)}{d(\Lambda)}$$

é chamado o *índice* de Λ em Γ. Note que, d depende somente de Λ e Γ, não das $\mathbb{Z}$-bases escolhidas para Λ e Γ. Pela Regra de Cramer, obtemos que

$$d\mathbf{x}_j = \sum_{i=1}^{n} a_{ij}\mathbf{y}_i, 1 \leq j \leq n,$$

onde $a_{ij} \in \mathbb{Z}$. Portanto,

$$d\Gamma \subseteq \Lambda \subseteq \Gamma,$$

onde $d\Gamma = \{d\mathbf{x} : \mathbf{x} \in \Gamma\}$ é um reticulado. Portanto, $\{d\mathbf{x}_1, \ldots, d\mathbf{x}_n\}$ é uma $\mathbb{Z}$-base de Λ.

Lema 1.3 *Sejam Γ um reticulado de $\mathbb{R}^n$ e Λ um sub-reticulado de Γ. Então*:

1. *Para cada $\mathbb{Z}$-base $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ de Γ existe uma $\mathbb{Z}$-base $\{\mathbf{y}_1, \ldots, \mathbf{y}_n\}$ de Λ tal que*

$$\mathbf{y}_i = \sum_{j=1}^{i} b_{ij}\mathbf{x}_j,$$

onde $b_{ij} \in \mathbb{Z}$, $b_{ii} \neq 0$, $1 \leq i \leq n$.

2. *Para cada $\mathbb{Z}$-base $\{\mathbf{y}_1, \ldots, \mathbf{y}_n\}$ de Λ existe uma $\mathbb{Z}$-base $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ de Γ tal que*

$$\mathbf{y}_i = \sum_{j=1}^{i} b_{ij}\mathbf{x}_j,$$

onde $b_{ij} \in \mathbb{Z}$, $b_{ii} \neq 0$, $1 \leq i \leq n$.

Prova. 1. Seja d o índice de Λ em Γ. Como $d\mathbf{x}_j \in \Lambda$ temos que existem vetores $\mathbf{y}_i \in \Lambda$ tais que

$$\mathbf{y}_i = \sum_{j=1}^{i} b_{ij}\mathbf{x}_j,$$

onde $b_{ij} \in \mathbb{Z}$, $b_{ii} \neq 0$, $1 \leq i \leq n$. Assim, para cada i, podemos escolher $\mathbf{y}_i \in \Lambda$, com o último coeficiente $|b_{ii}|$ o menor possível e $b_{ii} \neq 0$.

Afirmação. $\{\mathbf{y}_1, \ldots, \mathbf{y}_n\}$ é uma $\mathbb{Z}$-base de Λ.

De fato. É claro que $\langle \mathbf{y}_1, \ldots, \mathbf{y}_n \rangle \subseteq \Lambda$. Suponhamos, por absurdo, que exista $\mathbf{z} \in \Lambda - \langle \mathbf{y}_1, \ldots, \mathbf{y}_n \rangle$. Como $\mathbf{z} \in \Gamma$ temos que existem únicos $a_i \in \mathbb{Z}$, tais que

$$\mathbf{z} = \sum_{i=1}^{n} a_i\mathbf{x}_i.$$

Seja k, $1 \leq k \leq n$, o menor inteiro tal que

$$\mathbf{z} = \sum_{i=1}^{k} a_i\mathbf{x}_i \text{ e } a_k \neq 0.$$

Desde que $b_{kk} \neq 0$, podemos escolher $c \in \mathbb{Z}$ tal que

$$|a_k - cb_{kk}| < |b_{kk}| .$$

O vetor

$$\mathbf{z} - c\mathbf{y}_k = \sum_{i=1}^{k} (a_i - cb_{ki})\mathbf{x}_i \in \Lambda - \langle \mathbf{y}_1, \ldots, \mathbf{y}_n \rangle ,$$

pois $\mathbf{z} \in \Lambda - \langle \mathbf{y}_1, \ldots, \mathbf{y}_n \rangle$. Logo, $a_k - cb_{kk} \neq 0$, o que é uma contradição. Portanto, $\Lambda = \langle \mathbf{y}_1, \ldots, \mathbf{y}_n \rangle$.

2. Seja $\{\mathbf{y}_1, \ldots, \mathbf{y}_n\}$ uma $\mathbb{Z}$-base fixada de Λ. Como $d\Gamma$ é um sub-reticulado de Λ, onde d é o índice de Λ em Γ, temos (por 1.) que existe uma $\mathbb{Z}$-base $\{d\mathbf{x}_1, \ldots, d\mathbf{x}_n\}$ de $d\Gamma$ tal que

$$d\mathbf{x}_i = \sum_{j=1}^{i} c_{ij}\mathbf{y}_j,$$

onde $c_{ij} \in \mathbb{Z}$, $c_{ii} \neq 0$, $1 \leq i \leq n$. Logo,

$$\mathbf{y}_i = \sum_{j=1}^{i} b_{ij}\mathbf{x}_j,$$

onde $b_{ij} \in \mathbb{Q}$, $b_{ii} \neq 0$, $1 \leq i \leq n$. É claro que $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ é uma $\mathbb{Z}$-base de Γ. Como $\mathbf{y}_i \in \Gamma$ e todo $\mathbf{x} \in \Gamma$ pode ser escrito de modo único na forma

$$\mathbf{x} = x_1\mathbf{x}_1 + \cdots + x_n\mathbf{x}_n, x_i \in \mathbb{R},$$

temos que $b_{ij} \in \mathbb{Z}$. ■

Corolário 1.1 *Sejam Γ um reticulado de $\mathbb{R}^n$ e Λ um sub-reticulado de Γ. Então:*

1. *Para cada $\mathbb{Z}$-base $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ de Γ existe uma $\mathbb{Z}$-base $\{\mathbf{y}_1, \ldots, \mathbf{y}_n\}$ de Λ tal que*

$$\mathbf{y}_i = \sum_{j=1}^{i} b_{ij}\mathbf{x}_j,$$

onde $b_{ij} \in \mathbb{Z}$, $b_{ii} > 0$ e $0 \leq b_{ji} < b_{jj}$, $1 \leq i \leq n$.

2. *Para cada $\mathbb{Z}$-base $\{\mathbf{y}_1, \ldots, \mathbf{y}_n\}$ de Λ existe uma $\mathbb{Z}$-base $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ de Γ tal que*

$$\mathbf{y}_i = \sum_{j=1}^{i} b_{ij}\mathbf{x}_j,$$

onde $b_{ij} \in \mathbb{Z}$, $b_{ii} > 0$ e $0 \leq b_{ji} < b_{ii}$, $1 \leq i \leq n$.

Prova. 1. Para mostrar que $b_{ii} > 0$, basta substituir $\mathbf{x}_i$ por $-\mathbf{x}_i$ se $b_{ii} < 0$. Agora, substituimos $\mathbf{y}_i$ por

$$\mathbf{z}_i = \sum_{j=1}^{i-1} c_{ij}\mathbf{y}_j + \mathbf{y}_i,$$

onde $c_{ij} \in \mathbb{Z}$ são coeficientes a serem determinados. Note que, para qualquer escolha dos coeficientes c_{ij}, o conjunto $\{\mathbf{z}_1, \ldots, \mathbf{z}_n\}$ é uma $\mathbb{Z}$-base de Λ. Logo,

$$\mathbf{z}_i = \sum_{j=1}^{i} d_{ij}\mathbf{x}_j,$$

onde $d_{ii} = b_{ii}$. Assim, para $j < i$, temos que

$$d_{ij} = c_{ij}b_{jj} + c_{i(j+1)}b_{(j+1)j} + \cdots + c_{i(i-1)}b_{(i-1)j} + b_{ij}.$$

Portanto, para cada i, podemos escolher $c_{i1}, c_{i2}, \ldots, c_{i(i-1)}$ de modo que

$$0 \leq d_{ij} < d_{jj} = b_{jj}.$$

A prova de 2. é análoga. ■

Corolário 1.2 *Sejam Γ um reticulado de $\mathbb{R}^n$ e Λ um sub-reticulado de Γ. Então o índice de Λ em Γ é igual a $[\Gamma : \Lambda]$.*

Prova. Seja d o índice de Λ em Γ. Então, pelo Lema 1.3, temos que

$$d = \prod_{i=1}^{n} |b_{ii}|.$$

Mas pela prova do Corolário 1.1 todo $\mathbf{x} \in \Gamma$ está na mesma classe como exatamente um dos vetores

$$c_1\mathbf{x}_1 + \cdots + c_n\mathbf{x}_n, 0 \leq c_j < b_{jj}.$$

Portanto, $d = [\Gamma : \Lambda]$. ■

Observação 1.3 *Sejam G um grupo abeliano livre de posto n e H um subgrupo próprio de G. Então $[G : H]$ é finito se, e somente se, os postos de G e H são iguais.*

Seja Λ um reticulado em $\mathbb{R}^n$. Então obtemos uma partição de $\mathbb{R}^n$ em classes de equivalência módulo Λ, isto é, dados $\mathbf{x}, \mathbf{y} \in \mathbb{R}^n$, $\mathbf{x} \equiv \mathbf{y} (\mathrm{mod}\, \Lambda)$ se, e somente se, $-\mathbf{x} + \mathbf{y} \in \Lambda$. Assim, a classe de equivalência de $\mathbf{x}$ ou a translação do reticulado Λ por $\mathbf{x}$ é o conjunto

$\mathbf{x}+\Lambda=\{\mathbf{x}+\lambda:\lambda\in\Lambda\}$. Note que, $\mathbf{x}+\Lambda$ pode ser caracterizado como o conjunto de pontos em $\mathbb{R}^n$ que são gerados pelo grupo das translações por elementos de Λ

$$T(\Lambda)=\{t_\lambda:\mathbf{y}\longmapsto\mathbf{y}+\lambda:\mathbf{y}\in\mathbb{R}^n,\lambda\in\Lambda\},$$

agindo no ponto inicial $\mathbf{x}$

$$\mathbf{x}+\Lambda=\{t_\lambda(\mathbf{x}):t_\lambda\in T(\Lambda)\}.$$

Em outras palavras, $\mathbf{x}+\Lambda$ é a órbita de $\mathbf{x}$ sob o grupo $T(\Lambda)$.

Uma região em $\mathbb{R}^n$ que contém um e somente um ponto de cada classe lateral à esquerda de Λ em $\mathbb{R}^n$ é chamada de *região fundamental*. Note que região fundamental não é única, mas toda região fundamental deve ter o mesmo volume, pois o volume é invariante por translação. O *volume fundamental* de um reticulado Λ é o volume de uma região fundamental, o qual será denotado por $V(\Lambda)$.

Seja $\{\mathbf{x}_1,\ldots,\mathbf{x}_n\}$ uma $\mathbb{Z}$-base para o reticulado Λ. Então o conjunto

$$\mathbf{P}=P(\mathbf{x}_1,\ldots,\mathbf{x}_n)=\left\{\sum_{i=1}^{n}a_i\mathbf{x}_i:0\leq a_i<1\right\},$$

é uma região fundamental de Λ. De fato, dado $\mathbf{x}\in\mathbb{R}^n$, digamos $\mathbf{x}=b_1\mathbf{x}_1+\cdots+b_n\mathbf{x}_n$, $b_i\in\mathbb{R}$, como para cada i, $b_i=c_i+a_i$, onde $c_i\in\mathbb{Z}$ e $0\leq a_i<1$, temos que $\mathbf{x}=\mathbf{y}+\mathbf{r}$ com $\mathbf{y}\in\Lambda$ e $\mathbf{r}\in\mathbf{P}$. Finalmente, se $\mathbf{x}=\mathbf{y}'+\mathbf{r}'$ com $\mathbf{y}'\in\Lambda$ e $\mathbf{r}'\in\mathbf{P}$, então $\mathbf{y}+\mathbf{r}=\mathbf{y}'+\mathbf{r}'$ se, e somente se, $\mathbf{y}=\mathbf{y}'$ e $\mathbf{r}=\mathbf{r}'$, pois $0\leq|a_i-a_i'|<1$ e $c_i-c_i'\in\mathbb{Z}$. A região fundamental $\mathbf{P}$ é chamada *região fundamental básica* para Λ.

Lema 1.4 *Seja Λ um reticulado de $\mathbb{R}^n$. Então $\mathbb{R}^n=\dot{\cup}_{\lambda\in\Lambda}(\lambda+\mathbf{P})$.*

Prova. Seja $\{\mathbf{x}_1,\ldots,\mathbf{x}_n\}$ uma $\mathbb{Z}$-base para o reticulado Λ. Então $\{\mathbf{x}_1,\ldots,\mathbf{x}_n\}$ é uma base para $\mathbb{R}^n$. Assim, para cada $\mathbf{x}\in\mathbb{R}^n$, obtemos que

$$\mathbf{x}=b_1\mathbf{x}_1+\cdots+b_n\mathbf{x}_n,b_i\in\mathbb{R}.$$

Como, para cada $i=1,\ldots,n$, temos que $b_i=c_i+a_i$, onde $c_i\in\mathbb{Z}$ e $0\leq a_i<1$, segue-se que $\mathbf{x}=\mathbf{y}+\mathbf{r}$ com $\mathbf{y}\in\Lambda$ e $\mathbf{r}\in\mathbf{P}$. Portanto, $\mathbf{x}\in\dot{\cup}_{\lambda\in\Lambda}(\lambda+\mathbf{P})$. ■

Lema 1.5 *Seja Λ um reticulado em $\mathbb{R}^n$. Então $V(\Lambda)=d(\Lambda)=V(P)$.*

Prova. Seja $\{\mathbf{x}_1,\ldots,\mathbf{x}_n\}$ uma $\mathbb{Z}$-base para o reticulado Λ em $\mathbb{R}^n$. Por definição

$$V(P)=\int_P dt_1\cdots dt_n.$$

Se $\mathbf{x}_i = (x_{1i}, \ldots, x_{ni})$, então fazendo a mudança de variáveis

$$t_i = \sum_{j=1}^{n} x_{ji} t'_j,$$

onde $0 \leq t'_j < 1$, obtemos

$$V(P) = \int_0^1 |\det(x_{ji})| \, dt'_1 \cdots dt'_n = |\det(x_{ji})| \, .$$

Portanto, $V(\Lambda) = d(\Lambda) = V(P)$. ■

Seja Λ um reticulado em $\mathbb{R}^n$. A *densidade* de Λ é definida por

$$\Delta = \frac{V(E_\rho(\mathbf{0}))}{V(\Lambda)}$$

e a *densidade de centro* de Λ é definida por

$$\delta = \frac{\Delta}{V(E_1(\mathbf{0}))}.$$

Exemplo 1.5 *Seja $\Lambda = \mathbb{Z}^2$ um reticulado em $\mathbb{R}^2$. Então o conjunto $\{(1,0),(0,1)\}$ é uma $\mathbb{Z}$-base para o reticulado Λ. O raio de empacotamento $\rho = \frac{1}{2}$ e*

$$d(\Lambda) = V(\Lambda) = \det \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1.$$

Além disso, a densidade de Λ é $\Delta = \frac{\pi}{4}$ e a densidade de centro $\delta = \frac{1}{4}$.

Corolário 1.3 *Sejam Γ um reticulado de $\mathbb{R}^n$ e Λ um sub-reticulado de Γ. Então*

$$[\Gamma : \Lambda] = \frac{V(\Gamma)}{V(\Lambda)}.$$

Em particular, $[\Gamma : r\Gamma] = r^n$, para todo $r \in \mathbb{Z}$. ■

Corolário 1.4 *Sejam Γ,Λ e Π reticulados de $\mathbb{R}^n$ tais que $\Pi \subseteq \Lambda \subseteq \Gamma$. Então*

$$[\Gamma : \Pi] = [\Gamma : \Lambda][\Lambda : \Pi].$$

■

Teorema 1.9 *Sejam $\mathbf{T} = T^n$ o toro em $\mathbb{R}^n$, onde $T = E_1(\mathbf{0})$ e Λ um reticulado de $\mathbb{R}^n$. Então*

$$\frac{\mathbb{R}^n}{\Lambda} \simeq \mathbf{T}.$$

Prova. Seja $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ uma $\mathbb{Z}$-base para o reticulado Λ. Então $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ é uma base para $\mathbb{R}^n$. Assim, para cada $\mathbf{x} \in \mathbb{R}^n$, obtemos que

$$\mathbf{x} = b_1\mathbf{x}_1 + \cdots + b_n\mathbf{x}_n, b_i \in \mathbb{R}.$$

A função $\sigma : \mathbb{R}^n \to \mathbf{T}$ definida por

$$\sigma(\mathbf{x}) = (e^{2\pi b_1 i}, \ldots, e^{2\pi b_n i})$$

é claramente um homomorfismo de grupos (aditivo) sobrejetor e $\ker \sigma = \Lambda$. Portanto,

$$\frac{\mathbb{R}^n}{\Lambda} \simeq \mathbf{T}.$$

■

Observação 1.4 *É fácil verificar que* $\widehat{\sigma} = \sigma\,|_{\mathbf{P}}\colon \mathbf{P} \to \mathbf{T}$ *é bijetora. Neste caso,* $V(X) = V(\widehat{\sigma}^{-1}(X))$*, para cada subconjunto* X *de* $\mathbf{T}$ *e* $V(X)$ *existe se, e somente se,* $V(\widehat{\sigma}^{-1}(X))$ *existe em* $\mathbb{R}^n$*.*

Teorema 1.10 *Sejam* $\sigma : \mathbb{R}^n \to \mathbf{T}$ *e* X *um subconjunto limitado de* $\mathbb{R}^n$ *tal que* $V(X)$ *existe. Se* $\sigma(V(X)) \neq V(X)$*, então* $\widehat{\sigma} = \sigma\,|_X$ *é não injetora.*

Prova. Suponhamos, por absurdo, que $\widehat{\sigma} = \sigma\,|_X$ seja injetora. Como X é um subconjunto limitado de $\mathbb{R}^n$ e $\mathbb{R}^n = \dot{\cup}_{\lambda\in\Lambda}(\lambda + \mathbf{P})$ temos que X intercepta somente um número finito de classes $\lambda + \mathbf{P}$, com $\lambda \in \Lambda$. Fazendo

$$X_\lambda = X \cap (\lambda + \mathbf{P}),$$

obtemos que

$$X = X_{\lambda_1} \cup \cdots \cup X_{\lambda_n}.$$

Para cada λ_j, $j = 1, \ldots, n$, definimos

$$Y_{\lambda_j} = X_{\lambda_j} - \lambda_j,$$

de modo que $Y_{\lambda_j} \subseteq \mathbf{P}$. Como, por hipótese, $\sigma(\mathbf{x} - \lambda_j) = \sigma(\mathbf{x})$ para cada $\mathbf{x} \in \mathbb{R}^n$ temos que $Y_{\lambda_j} \cap Y_{\lambda_k} = \emptyset$, se $j \neq k$. Finalmente, desde que

$$V(X_{\lambda_j}) = V(Y_{\lambda_j}), \forall j = 1, \ldots, n \text{ e } \sigma(X_{\lambda_j}) = \widehat{\sigma}(Y_{\lambda_j}),$$

temos que

$$\begin{aligned} V(\sigma(X)) &= V\left(\sigma\left(\bigcup_{j=1}^{n} X_{\lambda_j}\right)\right) \\ &= V\left(\bigcup_{j=1}^{n} \sigma(X_{\lambda_j})\right) \\ &= V\left(\bigcup_{j=1}^{n} \widehat{\sigma}(Y_{\lambda_j})\right) \\ &= \sum_{j=1}^{n} V(Y_{\lambda_j}) \\ &= \sum_{j=1}^{n} V(X_{\lambda_j}) \\ &= V(X), \end{aligned}$$

o que é uma contradição. ■

Seja X um subconjunto de $\mathbb{R}^n$. Dizemos que X é *convexo* se

$$t\mathbf{x} + (1-t)\mathbf{y} \in X,\ \forall \mathbf{x}, \mathbf{y} \in X \text{ e } t \in [0,1].$$

Dizemos que X é *centrado simetricamente* se para todo $\mathbf{x} \in X$, tem-se $-\mathbf{x} \in X$.

Lema 1.6 (Minkowski) *Sejam Λ um reticulado de $\mathbb{R}^n$, X um subconjunto limitado, convexo e centrado simetricamente. Se*

$$V(X) > 2^n V(\Lambda),$$

então $X \cap \Lambda \neq \{\mathbf{0}\}$.

Prova. Sejam $\mathbf{P}$ a região fundamental básica de Λ e $\Gamma = 2\Lambda$. Então a região fundamental básica $\mathbf{P'} = 2\mathbf{P}$ de Γ tem volume $V(\mathbf{P'}) = 2^n V(\mathbf{P})$. Considerando o toro

$$\mathbf{T} = \frac{\mathbb{R}^n}{\Gamma}$$

temos, por definição, que

$$V(\mathbf{T}) = V(\mathbf{P'}) = 2^n V(\mathbf{P}).$$

Pelo Teorema 1.9 temos que $\sigma(X) \subseteq \mathbf{T}$ e

$$V(\sigma(X)) \leq V(\mathbf{T}) = 2^n V(\mathbf{P}) < V(X).$$

Logo, σ não preserva volume. Assim, pelo Teorema 1.10, $\sigma\ |_X$ é não injetora. Logo, existem $\mathbf{x}, \mathbf{y} \in X$, $\mathbf{x} \neq \mathbf{y}$, tal que $\sigma(\mathbf{x}) = \sigma(\mathbf{y})$ ou, equivalentemente,

$$\mathbf{x} - \mathbf{y} \in \Gamma.$$

Como X centrado simetricamente e convexo temos que $-\mathbf{y} \in X$ e

$$\frac{\mathbf{x} - \mathbf{y}}{2} \in X.$$

Portanto,

$$\mathbf{z} = \frac{\mathbf{x} - \mathbf{y}}{2} \in X \cap \Lambda,$$

com $\mathbf{z} \neq \mathbf{0}$. ■

Corolário 1.5 *Todo reticulado Λ em $\mathbb{R}^2$ possui um vetor $\mathbf{x} \neq \mathbf{0}$ tal que*

$$\|\mathbf{x}\|^2 \leq \frac{4V(\Lambda)}{\pi}.$$

Prova. Seja $X = E_\rho(\mathbf{0})$ o círculo de raio ρ e centro na origem tal que

$$V(X) > 2^2 V(\Lambda) \ \text{ ou } \ \rho^2 > \frac{2^2 V(\Lambda)}{\pi}.$$

Então, pelo Lema 1.6, existe $\mathbf{x} \in X \cap \Lambda$, com $\mathbf{x} \neq \mathbf{0}$. Logo, para todo $\epsilon > 0$, suficientemente pequeno, obtemos que

$$\|\mathbf{x}\|^2 < \frac{4V(\Lambda)}{\pi} + \epsilon.$$

Desde que $|X \cap \Lambda|$ é finita e ϵ é suficientemente pequeno, existe $\mathbf{x} \in X \cap \Lambda$, com $\mathbf{x} \neq \mathbf{0}$ tal que

$$\|\mathbf{x}\|^2 \leq \frac{4V(\Lambda)}{\pi}.$$

■

Lema 1.7 *Sejam Γ um reticulado de $\mathbb{R}^n$ e Λ um sub-reticulado de Γ. Então existem apenas um número finito de reticulados Λ' entre Λ e Γ.*

Prova. Sejam $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$ uma $\mathbb{Z}$-base para Λ e

$$\mathbf{P} = \left\{ \sum_{i=1}^{n} a_i \mathbf{x}_i : 0 \leq a_i < 1 \right\}.$$

Então existem um número finito de elementos de Λ que estão contidos em P, pois P é limitado. Assim, se Λ' é um reticulado entre Λ e Γ, então existem um número finito de possibilidades para o conjunto $\Lambda' \cap P$. Seja $\Lambda' \cap P = S$.

Afirmação. S e Λ determinam Λ'.

De fato. Seja $\mathbf{y} \in \Lambda'$. Então existe $\mathbf{x} \in \Lambda$ tal que $\mathbf{y} - \mathbf{x} \in P$. Logo, $\mathbf{y} - \mathbf{x} \in S$. Portanto, $\Lambda' = S + \Lambda$. ■

Corolário 1.6 *Sejam Λ um reticulado em $\mathbb{R}^n$ e $r \in \mathbb{Z}_+$. Então existe somente um número finito de reticulados Γ em $\mathbb{R}^n$ que contém Λ e tal que $[\Gamma : \Lambda] = r$.*

Prova. Seja Γ um reticulado em $\mathbb{R}^n$ tal que $[\Gamma : \Lambda] = r$. Então $r\Gamma \subseteq \Lambda \subseteq \Gamma$. Pelo Lema 1.7, existe somente um número finito de reticulados Γ em $\mathbb{R}^n$ que contém Λ e tal que $[\Gamma : \Lambda] = r$. ■

Capítulo 2

Corpos Quadráticos

Neste capítulo caracterizaremos o anel dos inteiros algébricos do corpo de números $\mathbb{Q}[\sqrt{d}]$, onde d é um inteiro livre de quadrados.

2.1 Inteiros Algébricos

Nesta seção apresentaremos algumas definições e resultados básicos da teoria algébrica dos números que serão necessários para a compreensão deste capítulo. O leitor interessado em mais detalhes pode consultar [7].

Sejam K um subcorpo de $\mathbb{C}$ e $\theta \in \mathbb{C}$. Denotamos por

$$K[\theta] = \{f(\theta) : f \in K[x]\}$$

o menor subdomínio de $\mathbb{C}$ contendo K e θ, e

$$K(\theta) = \{\frac{f(\theta)}{g(\theta)} : f, g \in K[x], g(\theta) \neq 0\}$$

o corpo quociente de $K[\theta]$.

Um elemento $\theta \in \mathbb{C}$ é um *número algébrico* se existir $m \in \mathbb{N}$ tal que o conjunto

$$\{1, \theta, \ldots, \theta^m\}$$

é linearmente dependente sobre $\mathbb{Q}$.

Seja L um subcorpo de K. Podemos ver K como um espaço vetorial sobre L e K é chamado uma extensão de L. Dizemos que K é uma extensão finita se K é um espaço vetorial de dimensão finita sobre L. Se K é uma extensão finita de L, indicamos por

$$[K : L]$$

a dimensão de K visto como um espaço vetorial de sobre L e $[K : L]$ é chamado o *grau* de K sobre L.

Teorema 2.1 *Seja $\theta \in \mathbb{C}$. Então θ é algébrico sobre $\mathbb{Q}$ se, e somente se, $\mathbb{Q}[\theta]$ é uma extensão finita de $\mathbb{Q}$.*

Prova. Suponhamos que $[\mathbb{Q}[\theta] : \mathbb{Q}] = n$. Então os elementos $1, \theta, \ldots, \theta^n$ são linearmente dependentes sobre $\mathbb{Q}$. Portanto, θ é algébrico sobre $\mathbb{Q}$.

Reciprocamente, seja $f = \text{irr}(\theta, \mathbb{Q})$, com $\partial f = n$.

Afirmação: $\mathbb{Q}[\theta]$ é um espaço vetorial sobre $\mathbb{Q}$ gerado por $1, \theta, \ldots, \theta^{n-1}$.

De fato, basta mostrar que $\mathbb{Q}[\theta]$ é um corpo. Para isto, é suficiente mostrar que $\theta^n \in \mathbb{Q}[\theta]$ e $\frac{1}{\beta} \in \mathbb{Q}[\theta]$, para todo $\beta \in \mathbb{Q}[\theta]^*$. Como $f(\theta) = 0$, temos que

$$a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} + \theta^n = 0,$$

isto é,

$$\theta^n = -(a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}) \in \mathbb{Q}[\theta].$$

Seja $\beta \in \mathbb{Q}[\theta]^*$ e $\beta = h(\theta)$, onde $h \in \mathbb{Q}[x]$ e $\partial h < n$. Então $\text{mdc}(f, h) = 1$. Logo, existem $g_1, g_2 \in \mathbb{Q}[x]$ tais que

$$fg_1 + hg_2 = 1.$$

Assim,

$$1 = f(\theta)g_1(\theta) + h(\theta)g_2(\theta) = h(\theta)g_2(\theta).$$

Portanto, $\frac{1}{\beta} = g_2(\theta) \in \mathbb{Q}[\theta]$. Neste caso, $\mathbb{Q}[\theta] = \mathbb{Q}(\theta)$. ■

Um elemento $\theta \in \mathbb{C}$ é um *inteiro algébrico* se existir um polinômio mônico $f(x) \in \mathbb{Z}[x]$ tal que $f(\theta) = 0$. Seja

$$\overline{\mathbb{Z}} = \{\theta \in \mathbb{C} : \theta \text{ é um inteiro algébrico}\}.$$

Então $\overline{\mathbb{Z}}$ é um subanel de $\mathbb{C}$.

Um subcorpo K de $\mathbb{C}$ é um *corpo de números* se ele é uma extensão finita de $\mathbb{Q}$, isto é, K é um espaço vetorial sobre $\mathbb{Q}$ de dimensão finita.

Teorema 2.2 *Se K é uma extensão finita de $\mathbb{Q}$, então existe um número (inteiro) algébrico $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$. Neste caso, qualquer $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$ é chamado um elemento primitivo de K.*

Prova. Vamos usar indução sobre $[K : \mathbb{Q}] = n$. Se $n = 1$, nada há para provar. Suponhamos que $n > 1$ e que o resultado seja válido para todas as extensões de $\mathbb{Q}$ com dimensão menor do que n.

Seja $\alpha_1 \in K$, com $\alpha_1 \notin \mathbb{Q}$. Se $K_1 = \mathbb{Q}(\alpha_1)$ e $K = K_1$, acabou; caso contrário, existe $\alpha_2 \in K$ tal que $\alpha_2 \notin K_1$. Seja $K_2 = K_1(\alpha_2) = \mathbb{Q}(\alpha_1, \alpha_2)$. Prosseguindo assim temos que existem $\alpha_1, \alpha_2, \ldots, \alpha_m \in K$, $m > 1$, tais que

$$K = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_m) \text{ e } \alpha_i \notin K_{i-1} = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_{i-1}).$$

Como $[K_{m-1} : \mathbb{Q}] < n$ temos, pela hipótese de indução, que existe $\alpha \in K_{m-1}$ tal que $K_{m-1} = \mathbb{Q}(\alpha)$. Mas

$$K = K_m = K_{m-1}(\alpha_m) = \mathbb{Q}(\alpha, \alpha_m).$$

Assim, fazendo $\alpha_m = \beta$, obtemos que $K = \mathbb{Q}(\alpha, \beta)$. Agora, vamos provar que existe $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$.

Sejam $p = \text{irr}(\alpha, \mathbb{Q})$ e $q = \text{irr}(\beta, \mathbb{Q})$, com $\partial(p) = r$ e $\partial(q) = s$. Como a característica de $\mathbb{Q}$ é zero temos que todas as raízes de p e q em $\mathbb{C}$ são distintas. Sejam $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ e $\beta = \beta_1, \beta_2, \ldots, \beta_s$ as raízes de p e q, respectivamente. Assim, cada equação

$$\alpha_i + \beta_j x = \alpha + \beta x, i = 1, \ldots, r, j = 2, \ldots, s,$$

tem um número finito de soluções em $\mathbb{C}$ e no máximo uma em $\mathbb{Q}$. Como $\mathbb{Q}$ é infinito temos que existe $c \in \mathbb{Q}$ tal que

$$\alpha_i + \beta_j c \neq \alpha + \beta c, i = 1, \ldots, r, j = 2, \ldots, s.$$

Seja $\theta = \alpha + c\beta \in K$. Então é claro que $\mathbb{Q}(\theta) \subseteq \mathbb{Q}(\alpha, \beta)$ e $\theta - c\beta_j \neq \alpha_i$, para todo $i = 1, \ldots, r, j = 2, \ldots, s$. Defina

$$f = p(\theta - cx) \in \mathbb{Q}(\theta)[x].$$

Logo, $f(\beta) = p(\alpha) = 0$ e $f(\beta_j) \neq 0$, para todo $j = 2, \ldots, s$, isto é, β é uma raiz de f e nenhum β_j é raiz de f, $j = 2, \ldots, s$. Seja $g = \text{irr}(\beta, \mathbb{Q}(\theta))$. Então g divide f e q. Logo, $g = x - \beta$, isto é, $\beta \in \mathbb{Q}(\theta)$ e $\alpha = \theta - c\beta \in \mathbb{Q}(\theta)$. Portanto, $\mathbb{Q}(\alpha, \beta) \subseteq \mathbb{Q}(\theta)$. ■

Teorema 2.3 *Seja $K = \mathbb{Q}(\theta)$, tal que $[K : \mathbb{Q}] = n$. Então existem exatamente n homomorfismos injetores $\sigma_i : K \to \mathbb{C}$. Além disso, $\theta_i = \sigma_i(\theta)$ são as raízes de $f = \text{irr}(\theta, \mathbb{Q})$.*

Prova. Sejam $\theta_1, \ldots, \theta_n$ as raízes distintas de f. Então cada θ_i também tem polinômio iredutível f, pois se $f_i = \text{irr}(\theta_i, \mathbb{Q})$, então f_i divide f e $f_i = f$. Assim, existe um único isomorfismo de corpos

$$\sigma_i : \mathbb{Q}(\theta) \longrightarrow \mathbb{Q}(\theta_i)$$

tal que $\sigma_i(\theta) = \theta_i$. De fato, se $\alpha \in \mathbb{Q}(\theta)$, então existe $g \in \mathbb{Q}[x]$ tal que $\alpha = g(\theta)$. Assim, pelo Algoritmo da Divisão, existem únicos $q, r \in \mathbb{Q}[x]$ tais que

$$g = fq + r, \text{ onde } 0 \leq \partial r < n.$$

Logo, $\alpha = r(\theta)$ com $\partial r < n$. Como $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ temos que $\sigma_i(\alpha) = r(\theta_i)$.

Reciprocamente, se $\sigma : K \longrightarrow \mathbb{C}$ é um homomorfismo injetor, então

$$0 = \sigma(0) = \sigma(f(\theta)) = f(\sigma(\theta)).$$

Assim, $\sigma(\theta)$ é um dos θ_i. Portanto, $\sigma = \sigma_i$, para algum $i = 1, \ldots, n$. ■

Os elementos $\theta_i = \sigma_i(\theta)$ são chamados os *conjugados* de θ. Neste caso,

$$B = \{1, \theta, \ldots, \theta^{n-1}\}$$

é uma base de K como espaço vetorial sobre $\mathbb{Q}$.

2.2 Traço e Norma

Seja $\alpha \in K$. Então a função $\phi_\alpha : K \to K$ definida por $\phi_\alpha(\beta) = \alpha\beta$ é claramente uma transformação linear sobre $\mathbb{Q}$. Denotamos por $\text{End}_\mathbb{Q} K$ o conjunto de todas as transformações lineares sobre $\mathbb{Q}$. Logo, a função $\varphi : K \to \text{End}_\mathbb{Q} K$ definida por $\varphi(\alpha) = \phi_\alpha$ é um homomorfismo de anéis injetor. Portanto, podemos identificar K com um subcorpo de $\text{End}_\mathbb{Q} K$. Se

$$B = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$$

é uma base de K como espaço vetorial sobre $\mathbb{Q}$ e

$$\phi_\alpha(\alpha_j) = \sum_{i=1}^{n-1} a_{ij}\alpha_i,$$

então

$$f_\alpha(x) = \det(x\mathbf{I} - \mathbf{A})$$

é o *polinômio característico* de α sobre $\mathbb{Q}$, onde $\mathbf{A} = (a_{ij})$ é a $n \times n$ matriz da transformação linear ϕ_α em relação à base B.

Teorema 2.4 *Sejam $K = \mathbb{Q}(\theta)$ e $\alpha \in K$. Se $p = \mathrm{irr}(\alpha, \mathbb{Q})$, então $f_\alpha = p^k$, para algum $k \in \mathbb{N}$. Além disso, $f_\alpha = p$ se, e somente se, α é um elemento primitivo de K.*

Prova. Seja

$$p = \mathrm{irr}(\alpha, \mathbb{Q}) = c_0 + c_1 x + \cdots + c_{m-1}x^{m-1} + x^m.$$

Então $\{1, \alpha, \ldots, \alpha^{m-1}\}$ é uma base de $K(\alpha)$ sobre $\mathbb{Q}$. Se $\{\beta_0, \ldots, \beta_{k-1}\}$ é uma base de K sobre $K(\alpha)$, então

$$\{\alpha^i \beta_j : 0 \leq i \leq m-1 \text{ e } 0 \leq j \leq k-1\}$$

é uma base de K sobre $\mathbb{Q}$. Logo, a matriz de ϕ_α nesta base é da forma

$$\mathbf{A} = \begin{pmatrix} \mathbf{A}_0 & \mathbf{O} & \cdots & \mathbf{O} \\ \mathbf{O} & \mathbf{A}_1 & \cdots & \mathbf{O} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{O} & \mathbf{O} & \cdots & \mathbf{A}_{k-1} \end{pmatrix},$$

onde

$$\mathbf{A}_j = \begin{pmatrix} 0 & 0 & \cdots & 0 & -c_0 \\ 1 & 0 & \cdots & 0 & -c_1 \\ 0 & 1 & \cdots & 0 & -c_2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & -c_{m-2} \\ 0 & 0 & \cdots & 1 & -c_{m-1} \end{pmatrix}.$$

Portanto,

$$\begin{aligned} f_\alpha(x) &= \det(x\mathbf{I} - \mathbf{A}) \\ &= \prod_{j=0}^{k-1} \det(x\mathbf{I} - \mathbf{A}_j) \\ &= p^k. \end{aligned}$$

Finalmente, se $f_\alpha = p$, então

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = n = [\mathbb{Q}(\theta) : \mathbb{Q}].$$

Logo, $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\theta)$ e α é um elemento primitivo de K. Por outro lado, se α é um elemento primitivo de K, então $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$. Portanto, $\partial p = n$ e $f_\alpha = p$. ■

Seja $\mathbf{A}$ a matriz da transformação linear ϕ_α em relação à alguma base. O *traço* e a *norma* de α são definidos por

$$Tr(\alpha) = Tr(\mathbf{A}) \text{ e } N(\alpha) = \det(\mathbf{A}).$$

Se $a \in \mathbb{Q}$ a matriz da transformação linear ϕ_a será a matriz diagonal $a\mathbf{I}$. Portanto,

$$Tr(a) = na \text{ e } N(a) = a^n, \forall a \in \mathbb{Q}.$$

Suponhamos que

$$f_\alpha(x) = (x - \alpha_0) \cdots (x - \alpha_{n-1})$$

em $\mathbb{C}$. Então

$$Tr(a) = \sum_{j=0}^{n-1} \alpha_j \text{ e } N(a) = \prod_{j=0}^{n-1} \alpha_j.$$

De fato, se

$$f_\alpha(x) = \det(x\mathbf{I} - \mathbf{A}) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

então

$$a_{n-1} = -Tr(\mathbf{A}) \text{ e } a_0 = (-1)^n \det(\mathbf{A}).$$

Por outro lado, é fácil verificar que

$$\sum_{j=0}^{n-1} \alpha_j = -a_{n-1} \text{ e } \prod_{j=0}^{n-1} \alpha_j = (-1)^n a_0.$$

Exemplo 2.1 *Seja θ uma raiz do polinômio irredutível $f(x) = x^3 + 6x^2 + 9x + 3 \in \mathbb{Q}[x]$. Então $K = \mathbb{Q}(\theta)$ é isomorfo ao conjunto das matrizes da forma*

$$\begin{pmatrix} a & -3c & -3b + 18c \\ b & a - 9c & -9b + 51c \\ c & b - 6c & a - 6b + 27c \end{pmatrix}, \text{ onde } a, b, c \in \mathbb{Q}.$$

De fato. É claro que $B = \{1, \theta, \theta^2\}$ é uma base de K. Logo, cada $\alpha \in K$ é da forma $\alpha = a + b\theta + c\theta^2$, com $a, b, c \in \mathbb{Q}$. Assim,

$$\begin{aligned} \phi_\alpha(1) &= \alpha \\ \phi_\alpha(\theta) &= -3c + (a - 9c)\theta + (b - 6c)\theta^2 \\ \phi_\alpha(\theta^2) &= (-3b + 18c) + (-9b + 51c)\theta + (a - 6b + 27c)\theta^2. \end{aligned}$$

Neste caso,

$$\begin{aligned} Tr(\alpha) &= 3a - 6b + 18c \\ N(\alpha) &= a^3 - 6a^2b + 18a^2c - 45acb + 45ac^2 + 9ab^2 \\ &\quad +18cb^2 - 27bc^2 - 3b^3 + 9c^3. \end{aligned}$$

A função $\psi : K \times K \to \mathbb{Q}$ definida por $\psi((\alpha, \beta)) = Tr(\alpha\beta)$ é uma forma bilinear simétrica sobre K. O determinante desta forma associado à base $B = \{1, \theta, \ldots, \theta^{n-1}\}$ de K é chamado *discriminante* de B, isto é,

$$D(B) = \det(Tr(\theta^{i+j})).$$

Se $B' = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ é uma outra base de K tal que $\alpha_i = \sum_{j=0}^{n-1} a_{ij}\theta^j$, onde $\mathbf{B} = (a_{ij})$ é a matriz mudança de base, então

$$Tr(\alpha_i\alpha_j) = \sum_{k,l=0}^{n-1} a_{il}a_{jk}Tr((\theta^{k+l})).$$

Portanto,

$$D(B') = (\det \mathbf{B})^2 D(B).$$

Exemplo 2.2 *Sejam θ uma raiz do polinômio irredutível $f(x) = x^3 + 6x^2 + 9x + 3$ e $\alpha = a + b\theta + c\theta^2 \in K = \mathbb{Q}(\theta)$. Então $Tr(\alpha) = 3a - 6b + 18c$ e*

$$\begin{aligned} D(B) &= \det \begin{pmatrix} Tr(1) & Tr(\theta) & Tr(\theta^2) \\ Tr(\theta) & Tr(\theta^2) & Tr(\theta^3) \\ Tr(\theta^2) & Tr(\theta^3) & Tr(\theta^4) \end{pmatrix} \\ &= \det \begin{pmatrix} 3 & -6 & 18 \\ -6 & 18 & -63 \\ 18 & -63 & 234 \end{pmatrix} \\ &= 81. \end{aligned}$$

Seja $\beta = \theta^{-1}$. Então $\beta = -3 - 2\theta - \frac{1}{3}\theta^2$. Assim, a transformação linear $T(1) = 1$, $T(\theta) = \theta$ e $T(\theta^2) = \beta$ tem a matriz associada

$$\mathbf{B} = \begin{pmatrix} 1 & 0 & -3 \\ 0 & 1 & -2 \\ 0 & 0 & -\frac{1}{3} \end{pmatrix},$$

com $\det(\mathbf{B}) = -\frac{1}{3}$. *Portanto,* $B' = \{1, \theta, \beta\}$ *é uma base de* K *com*

$$D(B') = (\det \mathbf{B})^2 D(B) = 9.$$

Teorema 2.5 *Seja* $K = \mathbb{Q}(\theta)$. *Então a forma bilinear* $\psi : K \times K \to \mathbb{Q}$ *definida por* $\psi((\alpha, \beta)) = Tr(\alpha\beta)$ *é não singular.*

Prova. Como $K = \mathbb{Q}(\theta)$ temos que

$$f_\theta = \text{irr}(\theta, \mathbb{Q}) = \prod_{i=1}^{n}(x - \theta_i).$$

Logo,

$$Tr(\theta) = -\sum_{i=1}^{n} \theta_i \text{ e } N(\theta) = (-1)^n \prod_{i=1}^{n} \theta_i.$$

Pelo Teorema 2.3, existem exatamente n homomorfismos injetores $\sigma_i : K \longrightarrow \mathbb{C}$ com $\sigma_i(\theta) = \theta_i$. Assim,

$$Tr(\theta) = -\sum_{i=1}^{n} \sigma_i(\theta) \text{ e } N(\theta) = (-1)^n \prod_{i=1}^{n} \sigma_i(\theta).$$

Considerando a matriz $\mathbf{A} = (\sigma_j(\theta^i))$, com $0 \leq i \leq n-1$ e $1 \leq j \leq n$ temos que o elemento da i-ésima linha e j-ésima coluna de $\mathbf{A}^t\mathbf{A}$ é dado por

$$\sum_{k=1}^{n} \sigma_k(\theta^i)\sigma_k(\theta^j) = \sum_{k=1}^{n} \sigma_k(\theta^{i+j}) = Tr(\theta^{i+j}).$$

Logo,

$$\det(\mathbf{A}^t\mathbf{A}) = (\det(\mathbf{A}))^2 = \det(Tr(\theta^{i+j})).$$

Mas, $\det(Tr(\theta^{i+j}))$ é precisamente o discriminante da base $B = \{1, \theta, \ldots, \theta^{n-1}\}$, isto é,

$$D(B) = \left[\det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \theta_1 & \theta_2 & \cdots & \theta_n \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1^{n-1} & \theta_2^{n-1} & \cdots & \theta_n^{n-1} \end{pmatrix} \right]^2.$$

Logo,

$$D(B) = \prod_{i<j} (\theta_i - \theta_j)^2 \neq 0.$$

Assim, a matriz $\mathbf{A}^2$ associada a forma bilinear ψ na base $B = \{1, \theta, \ldots, \theta^{n-1}\}$, é não singular. Portanto ψ é não singular. ■

Observação 2.1 *Decorre da prova do Teorema acima que* $D(B) = (\det(\mathbf{A}))^2$,

$$f'(\theta) = \prod_{i \neq 1}(\theta - \theta_i) \;\; e \;\; f(\sigma_i(\theta)) = \prod_{i \neq j}(\theta_j - \theta_i),$$

e

$$N(f'(\theta)) = (-1)^{\frac{n(n-1)}{2}} \prod_{i<j}(\theta_i - \theta_j)^2 = (-1)^{\frac{n(n-1)}{2}} D(B).$$

O anel $\mathbb{Z}_K = K \cap \overline{\mathbb{Z}}$ é chamado o *anel dos inteiros* de K. É fácil verificar que se $\alpha \in K$, então existe $a \in \mathbb{Z}$ tal que $a\alpha \in \mathbb{Z}_K$. Além disto, $K = \mathbb{Q}(\theta)$ para algum $\theta \in \overline{\mathbb{Z}}$.

Seja $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ uma base de K sobre $\mathbb{Q}$. Como K é o corpo de frações de $\mathbb{Z}_K$ temos que existe $\gamma \in \mathbb{Z}_K$ tal que $\alpha_i = \beta_i \gamma^{-1}$, com $\beta_i \in \mathbb{Z}_K$ e $i = 0, \ldots, n-1$. Logo,

$$B = \{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$$

é uma $\mathbb{Z}$-*base* de $\mathbb{Z}_K$. Note que $Tr(\beta_i \beta_j) \in \mathbb{Z}$ e $D(B) \in \mathbb{Z}$. Uma *base minimal* de K sobre Q é uma $\mathbb{Z}$-base B tal que $|D(B)|$ seja mínimo.

Teorema 2.6 *O anel* $\mathbb{Z}_K$ *é um* $\mathbb{Z}$*-módulo livre de posto* n *gerado por uma base minimal. Toda base do* $\mathbb{Z}$*-módulo* $\mathbb{Z}_K$ *é minimal.*

Prova. Seja $B = \{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ uma base minimal de K. Então é claro que

$$\alpha = \sum_{i=0}^{n-1} x_i \beta_i \in \mathbb{Z}_K,$$

onde $x_i \in \mathbb{Z}$. Dado $\alpha \in \mathbb{Z}_K$. Suponhamos, por absurdo, que

$$\alpha = \sum_{i=0}^{n-1} y_i \beta_i \in \mathbb{Z}_K,$$

onde $y_i \in \mathbb{Q}$. Como podemos escrever $y_1 = x_1 + r$, onde $x_1 \in \mathbb{Z}$, $r \in \mathbb{Q}$ e $0 < r < 1$, temos que o conjunto $B' = \{\alpha - x_1\beta_1, \beta_1, \ldots, \beta_{n-1}\}$ é uma $\mathbb{Z}$-base de $\mathbb{Z}_K$, pois a matriz mudança de base

$$\mathbf{B} = \begin{pmatrix} r & 0 & \cdots & 0 \\ y_2 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ y_{n-1} & 0 & \ldots & 1 \end{pmatrix}$$

tem $\det(\mathbf{B}) = r$. Logo, $D(B') = r^2 D(B)$ e $|D(B')| < |D(B)|$, o que é uma contradição. Reciprocamente, sejam $B = \{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$, $B' = \{\beta'_0, \beta'_1, \ldots, \beta'_{n-1}\}$ duas bases do

$\mathbb{Z}$-módulo $\mathbb{Z}_K$ e r, t os determinantes das matrizes mudanças de bases. Então $D(B') = r^2 D(B)$ e $D(B) = t^2 D(B')$. Logo, $(rt)^2 = 1$. Como $r, t \in \mathbb{Z}$ temos que $r^2 = 1$ e $D(B') = D(B)$. ■

Teorema 2.7 *Seja $\mathbb{Z}_K$ o anel dos inteiros de K. Então*:

1. *$\mathbb{Z}_K$ é Noetheriano.*

2. *Todo ideal primo de $\mathbb{Z}_K$ é maximal.*

Prova. 1. Seja I qualquer ideal não nulo de $\mathbb{Z}_K$. Pelo Teorema 2.6, $(\mathbb{Z}_K, +)$ é um grupo abeliano livre de posto n. Assim, pelo Teorema 1.8, $(I, +)$ é um grupo abeliano livre de posto m com $m \leq n$. Como toda $\mathbb{Z}$-base de $(I, +)$ gera I como um ideal, temos que I é finitamente gerado. Portanto, $\mathbb{Z}_K$ é Noetheriano.

2. Sejam P um ideal primo de $\mathbb{Z}_K$ e $\alpha \in P$, $\alpha \neq 0$. Então

$$N = N(\alpha) = (-1)^n \prod_{i=1}^{n} \sigma_i(\alpha) \in P,$$

pois $\sigma_1(\alpha) = \alpha \in P$. Logo, $\langle N \rangle \subseteq P$. Como $(\frac{\mathbb{Z}_K}{\langle N \rangle}, +)$ é um grupo abeliano finitamente gerado em que todo elemento tem ordem finita temos que $\frac{\mathbb{Z}_K}{\langle N \rangle}$ é finito. Pelo Teorema da Correspondência $\frac{\mathbb{Z}_K}{P}$ é um domínio finito e, assim, um corpo. Portanto, P é um ideal maximal. ■

2.3 Representação Geométrica dos Ideais de $\mathbb{Z}_K$

Seja $K = \mathbb{Q}[\theta]$. Então é fácil verificar que os conjugados $\sigma_i(\theta) = \theta_i$ de θ não necessita ser elemento de K. Assim, dizemos que σ_i é real se $\sigma_i(K) \subseteq \mathbb{R}$, caso contrário, é complexo. É claro que se σ_i é complexo, então $\overline{\sigma}_i : K \to \mathbb{C}$ definida por $\overline{\sigma}_i(\beta) = \overline{\sigma_i(\beta)}$ é um homomorfismo injetor tal que $\overline{\sigma}_i \neq \sigma_i$ e $\overline{\sigma}_i^2 = \sigma_i$. Assim, denotamos os homomorfismos injetores reais por $\sigma_1, \ldots, \sigma_k$, os complexos por $\sigma_{k+1}, \overline{\sigma}_{k+1}, \ldots, \sigma_{k+l}, \overline{\sigma}_{k+l}$ e $n = k + 2l$.

Proposição 2.1 *Seja $\varphi : K \to \mathbb{R}^n$ definida por*

$$\varphi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_k(\alpha), \mathrm{Re}(\sigma_{k+1}(\alpha)), \mathrm{Im}(\sigma_{k+1}(\alpha)), \ldots).$$

Então:

1. φ é um homomorfismo injetor;

2. $\varphi(a\alpha) = a\varphi(\alpha)$ para todo $a \in \mathbb{Q}$ e $\alpha \in K$. ■

Teorema 2.8 *Seja K um corpo de números. Se $B = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ é uma base de K sobre $\mathbb{Q}$, então $\{\varphi(\alpha_0), \varphi(\alpha_1), \ldots, \varphi(\alpha_{n-1})\}$ é linearmente independente sobre $\mathbb{R}$. Em particular, se $\{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ é uma $\mathbb{Z}$-base de K sobre $\mathbb{Q}$, então*

$$\Gamma = \varphi(\mathbb{Z}_K) = \langle \varphi(\alpha_0), \varphi(\alpha_1), \ldots, \varphi(\alpha_{n-1}) \rangle$$

é um reticulado em $\mathbb{R}^n$.

Prova. Como

$$\varphi(\alpha_j) = (\sigma_1(\alpha_j), \ldots, \sigma_k(\alpha_j), \mathrm{Re}(\sigma_{k+1}(\alpha_j)), \mathrm{Im}(\sigma_{k+1}(\alpha_j)), \ldots),$$

basta mostrar que

$$D = \det \begin{pmatrix} \sigma_1(\alpha_0) & \cdots & \sigma_k(\alpha_0) & \mathrm{Re}(\sigma_{k+1}(\alpha_0)) & \mathrm{Im}(\sigma_{k+1}(\alpha_0)) & \cdots \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\alpha_{n-1}) & \cdots & \sigma_k(\alpha_{n-1}) & \mathrm{Re}(\sigma_{k+1}(\alpha_{n-1})) & \mathrm{Im}(\sigma_{k+1}(\alpha_{n-1})) & \cdots \end{pmatrix}$$

é diferente de zero. Seja

$$E = \det \begin{pmatrix} \sigma_1(\alpha_0) & \cdots & \sigma_k(\alpha_0) & \sigma_{k+1}(\alpha_0) & \overline{\sigma}_{k+1}(\alpha_0) & \cdots \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\alpha_{n-1}) & \cdots & \sigma_k(\alpha_{n-1}) & \sigma_{k+1}(\alpha_{n-1}) & \overline{\sigma}_{k+1}(\alpha_{n-1}) & \cdots \end{pmatrix}.$$

Como

$$\sigma_{k+j}(\alpha_r) = \mathrm{Re}(\sigma_{k+j}(\alpha_r)) + i\,\mathrm{Im}(\sigma_{k+j}(\alpha_r)), j = 1, \ldots l, r = 0, \ldots, n-1,$$

temos, substituindo a $(k+j)$-ésima coluna C_{k+j} de D por $C_{k+j} + iC_{k+j+1}$, que

$$D = \det \begin{pmatrix} \sigma_1(\alpha_0) & \cdots & \sigma_k(\alpha_0) & \sigma_{k+1}(\alpha_0) & \mathrm{Im}(\sigma_{k+1}(\alpha_0)) & \cdots \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\alpha_{n-1}) & \cdots & \sigma_k(\alpha_{n-1}) & \sigma_{k+1}(\alpha_{n-1}) & \mathrm{Im}(\sigma_{k+1}(\alpha_{n-1})) & \cdots \end{pmatrix}$$

Como

$$\sigma_{k+j}(\alpha_r) - \overline{\sigma}_{k+j}(\alpha_r) = 2i\,\mathrm{Im}(\sigma_{k+j}(\alpha_r)), j = 1, \ldots l, r = 0, \ldots, n-1,$$

temos, substituindo a $(k+j+1)$-ésima coluna C_{k+j+1} de D por $C_{k+j} - 2iC_{k+j+1}$, que

$$D = \det \begin{pmatrix} \sigma_1(\alpha_0) & \cdots & \sigma_k(\alpha_0) & \sigma_{k+1}(\alpha_0) & \overline{\sigma}_{k+1}(\alpha_0) & \cdots \\ \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\alpha_{n-1}) & \cdots & \sigma_k(\alpha_{n-1}) & \sigma_{k+1}(\alpha_{n-1}) & \overline{\sigma}_{k+1}\alpha_{n-1}) & \cdots \end{pmatrix}.$$

Logo, $E = (-2i)^l D$. Pelo Teorema 2.5, $E^2 = D(B) \neq 0$. Portanto, $D \neq 0$. ■

2.4 Corpos Quadráticos

Um *corpo quadrático* é um corpo de números K de dimensão 2 sobre $\mathbb{Q}$. Portanto, $K = \mathbb{Q}(\theta)$, onde θ é um inteiro algébrico e raiz do polinômio

$$f = \mathrm{irr}(\theta, \mathbb{Q}) = x^2 + ax + b, \text{ com } a, b \in \mathbb{Z}.$$

Assim,

$$\theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2} \text{ ou } 2\theta = -a \pm \sqrt{a^2 - 4b}.$$

Seja $a^2 - 4b = c^2 d$, onde $c, d \in \mathbb{Z}$ e d livre de quadrado. Então

$$\begin{aligned} K &= \mathbb{Q}(\theta) \\ &= \mathbb{Q}(2\theta) \\ &= \mathbb{Q}(-a \pm c\sqrt{d}) \\ &= \mathbb{Q}(\sqrt{d}). \end{aligned}$$

Se d é negativo, K é chamado um *corpo quadrático imaginário* e se d é positivo, K é chamado um *corpo quadrático real*.

Seja $\theta \in K$. Então $\theta = a + b\sqrt{d}$, onde $a, b \in \mathbb{Q}$. Se $\overline{\theta} = a - b\sqrt{d}$, então

$$\begin{aligned} f &= (x - \theta)(x - \overline{\theta}) \\ &= x^2 - 2ax + (a^2 - b^2 d). \end{aligned}$$

Portanto, $\theta \in \mathbb{Z}_K$ se, e somente se, $2a \in \mathbb{Z}$ e $a^2 - b^2 d \in \mathbb{Z}$.

Teorema 2.9 *Seja $d \in \mathbb{Z}$ livre de quadrado. Então*

$$\mathbb{Z}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{se } d \equiv 2 \text{ ou } 3 (\mathrm{mod}\, 4), \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{se } d \equiv 1 (\mathrm{mod}\, 4). \end{cases}$$

Prova. Se $\theta \in \mathbb{Z}_K$, então $2a \in \mathbb{Z}$ e $a^2 - b^2 d \in \mathbb{Z}$. Como

$$4a^2 - 4b^2 d = (2a)^2 - d(2b)^2 \in 4\mathbb{Z} \subset \mathbb{Z}$$

temos que $(2b)^2 \in \mathbb{Z}$. Seja $2b = \frac{r}{s}$, onde $r, s \in \mathbb{Z}$, $s \neq 0$ e $\mathrm{mdc}(r, s) = 1$. Então

$$d(2b)^2 = \frac{dr^2}{s^2} \in \mathbb{Z}.$$

Se $s \neq \pm 1$, então existe um fator primo p de s. Assim, p^2 divide dr^2. Sendo $\text{mdc}(p^2, r^2) = 1$ temos que p^2 divide d, o que é uma contradição. Logo, $2b \in \mathbb{Z}$. Portanto, podemos assumir $a = \frac{m}{2}$ e $b = \frac{n}{2}$. Assim, há dois casos a serem considerados:

$1^{\underline{0}}$ Caso - Se n é par, então m é par, pois $m^2 - dn^2 \in 4\mathbb{Z}$. Portanto, $a, b \in \mathbb{Z}$.

$2^{\underline{0}}$ Caso - Se n é ímpar, então m é ímpar, pois $m^2 - dn^2 \in 4\mathbb{Z}$. Portanto, $a, b \in \mathbb{Z} + \frac{1}{2}$, isto é,

$$\theta = \frac{m}{2} + \frac{n}{2}\sqrt{d},$$

com m, n ímpares.

Como $m^2 \equiv dn^2 (\text{mod}\, 4)$ e d livre de quadrado temos que $d \equiv 1, 2 \text{ ou } 3 (\text{mod}\, 4)$.

Se $d \equiv 1 (\text{mod}\, 4)$, então $m^2 - n^2 \equiv 0 (\text{mod}\, 4)$. Logo, m e n têm a mesma paridade. Portanto,

$$\mathbb{Z}_K \subseteq \mathbb{Z}[\frac{1+\sqrt{d}}{2}].$$

Reciprocamente, se m e n têm a mesma paridade, então

$$\frac{m + n\sqrt{d}}{2} + \frac{m - n\sqrt{d}}{2} = m \in \mathbb{Z}$$

e

$$\left(\frac{m + n\sqrt{d}}{2}\right)\left(\frac{m - n\sqrt{d}}{2}\right) = \frac{m - dn^2}{4} \in \mathbb{Z}.$$

Portanto,

$$\frac{m}{2} + \frac{n}{2}\sqrt{d} \in \mathbb{Z}_K.$$

Neste caso,

$$\mathbb{Z}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}].$$

Se $d \equiv 2 \text{ ou } 3 (\text{mod}\, 4)$, então prova-se, de modo análogo, que $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$. ■

Uma maneira simples para escrever os inteiros algébricos com $d \equiv 1 \,\text{mod}\, 4$, é a introdução do inteiro algébrico

$$\eta = \frac{1+\sqrt{d}}{2},$$

o qual é raiz de $\text{irr}(\eta, \mathbb{Q}) = x^2 - x + \frac{1-d}{4}$. Assim, se $d \equiv 1 \,\text{mod}\, 4$, então $\mathbb{Z}_K = \mathbb{Z}[\eta]$.

Teorema 2.10 *Se $d \equiv 2$ ou $3 (\text{mod}\, 4)$, então $B = \{1, \sqrt{d}\}$ é uma base minimal de $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$. Se $d \equiv 1 (\text{mod}\, 4)$, então $B = \{1, \eta\}$ é uma base minimal de $\mathbb{Z}_K = \mathbb{Z}[\eta]$.*

Prova. Se $d \equiv 2$ ou $3 (\mathrm{mod}\, 4)$, então $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$ e $\alpha \in \mathbb{Z}_K$ é da forma $\alpha = a + b\sqrt{d}$, com $a, b \in \mathbb{Z}$, e $\mathrm{irr}(\sqrt{d}, \mathbb{Q}) = x^2 - d$ temos que

$$\begin{aligned} \phi_\alpha(1) &= \alpha \\ \phi_\alpha(\sqrt{d}) &= bd + a\sqrt{d}. \end{aligned}$$

Logo, $\mathbb{Z}_K$ é isomorfo ao conjunto das matrizes da forma

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix}, \text{ onde } a, b \in \mathbb{Z}.$$

Neste caso,

$$Tr(\alpha) = 2a \text{ e } N(\alpha) = a^2 - db^2.$$

Assim, o discriminante associado à base B é dado por

$$\begin{aligned} D(B) &= \det \begin{pmatrix} Tr(1) & Tr(\sqrt{d}) \\ Tr(\sqrt{d}) & Tr(d) \end{pmatrix} \\ &= \det \begin{pmatrix} 2 & 0 \\ 0 & 2d \end{pmatrix} \\ &= 4d. \end{aligned}$$

Como $Tr(\alpha)$ é um número inteiro par temos que o discriminante de qualquer base inteira B' de $\mathbb{Z}_K$ é um múltiplo de 4, por exemplo $D(B') = 4m$. Assim, se r é o determinante da matriz mudança de base, então $D(B) = r^2 D(B')$ ou $d = r^2 m$. Suponhamos que $|m| < |d|$. Então

$$|m| < \left|r^2 m\right| \Rightarrow |r| > 1.$$

Logo, d possui um fator quadrático, o que é uma contradição. Portanto, a base $B = \{1, \sqrt{d}\}$ é minimal.

Finalmente, como cada $\alpha \in \mathbb{Z}_K = \mathbb{Z}[\eta]$ é da forma $\alpha = a + b\eta$, com $a, b \in \mathbb{Z}$, e $\mathrm{irr}(\eta, \mathbb{Q}) = x^2 - x + \frac{1-d}{4}$ temos que

$$\begin{aligned} \phi_\alpha(1) &= \alpha \\ \phi_\alpha(\eta) &= \frac{b(d-1)}{4} + (a+b)\eta \end{aligned}$$

Logo, $\mathbb{Z}_K$ é isomorfo ao conjunto das matrizes da forma

$$\begin{pmatrix} a & \frac{b(d-1)}{4} \\ b & a+b \end{pmatrix}, \text{ onde } a, b \in \mathbb{Z}.$$

Neste caso,

$$Tr(\alpha) = 2a + b \text{ onde } N(\alpha) = a^2 + ab - \frac{b^2(d-1)}{4}.$$

Assim, o discriminante associado à base B é dado por

$$\begin{aligned} D(B) &= \det \begin{pmatrix} Tr(1) & Tr(\eta) \\ Tr(\eta) & Tr(\eta^2) \end{pmatrix} \\ &= \det \begin{pmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{pmatrix} \\ &= d. \end{aligned}$$

Como $Tr(\alpha)$ é um número inteiro temos que o discriminante de qualquer base inteira B' de $\mathbb{Z}_K$ é um inteiro, por exemplo $D(B') = m$. Assim, se r é o determinante da matriz mudança de base, então $d = r^2 m$. Suponhamos que $|m| < |d|$. Então $|r| > 1$. Logo, d possui um fator quadrático, o que é uma contradição. Portanto, a base $B = \{1, \eta\}$ é minimal. ■

Se $d < 0$ e $d \equiv 1 (\mathrm{mod}\, 4)$, então $K = \mathbb{Q}[\eta]$,

$$\mathbb{Z}_K = \{\frac{a + b\sqrt{d}}{2} : a, b \in \mathbb{Z}, \text{ com a mesma paridade}\}$$

e

$$\mathrm{irr}(\eta, \mathbb{Q}) = x^2 - x + \frac{1-d}{4}.$$

Seja $B = \{1, \eta\}$ uma base minimal para $\mathbb{Z}_K$ e $\sigma : K \to \mathbb{C}$ um homomorfismo injetor. Então dado $\alpha \in K$, digamos $\alpha = a + b\eta$ com $a, b \in \mathbb{Q}$, obtemos que

$$\sigma(\alpha) = a + b\sigma(\eta).$$

Também

$$\begin{aligned} 0 &= \sigma(0) \\ &= \sigma(\eta^2 - \eta + \frac{1-d}{4}) \\ &= \sigma(\eta)^2 - \sigma(\eta) + \frac{1-d}{4}. \end{aligned}$$

Logo, $\sigma(\eta) = \eta$ ou $\sigma(\eta) = \overline{\eta}$. Portanto,

$$\sigma(\alpha) = \alpha \text{ ou } \sigma(\alpha) = \overline{\alpha}.$$

Assim, pelo Teorema 2.3 existem dois homomorfismos injetores $\sigma, \overline{\sigma} : K \to \mathbb{C}$. Logo, $\varphi : K \to \mathbb{R}^2$ definida por

$$\varphi(\alpha) = (\mathrm{Re}(\sigma(\alpha)), \mathrm{Im}(\sigma(\alpha)))$$

é um homomorfismo injetor e $\leqslant_1 = \varphi(\mathbb{Z}_K)$ é um reticulado em $\mathbb{R}^2$ gerado por $\varphi(1)$ e $\sigma(\eta)$, isto é,

$$B' = \{(1,0), (\frac{1}{2}, \frac{\sqrt{-d}}{2})\}$$

é uma $\mathbb{Z}$-base de Γ_1 com

$$V(\Gamma_1) = \frac{\sqrt{|d|}}{2}, \Delta = \frac{\pi}{2\sqrt{|d|}} \text{ e } \delta = \frac{1}{2\sqrt{|d|}}.$$

Como $d \leq -3$ temos que o ângulo A entre os vetores da base B', dado por

$$\cos A = \frac{\frac{1}{2}}{\frac{1-d}{4}} = \frac{2}{1-d},$$

é menor que ou igual a $\frac{\pi}{3}$. Portanto, as regiões fundamentais são triângulos isósceles, pois o ângulo é invariante por isometrias. Em particular, se $d = -3$, então a região fundamental é um triângulo equilátero e $\Gamma_2 = A_2$ é o reticulado hexagonal de $\mathbb{R}^2$. Note que, $N(\alpha) = N(\varphi(\alpha))$, pois

$$\begin{aligned} N(\alpha) &= (-1)^2 \alpha \overline{\alpha} \\ &= |\sigma(\alpha)|^2 \\ &= N(\sigma(\alpha)). \end{aligned}$$

Como $|\sigma(\alpha)|^2 = |\mathrm{Re}(\sigma(\alpha))|^2 + |\mathrm{Im}(\sigma(\alpha))|^2$ temos que $N(\varphi(\alpha)) = \|\varphi(\alpha)\|^2$.

Se $d < 0$ e $d \equiv 2 \text{ ou } 3 (\mathrm{mod}\, 4)$, então $K = \mathbb{Q}[\sqrt{d}]$,

$$\mathbb{Z}_K = \{a + b\sqrt{d} : a, b \in \mathbb{Z}\}$$

e

$$\mathrm{irr}(\eta, \mathbb{Q}) = x^2 - d.$$

Seja $B = \{1, \sqrt{d}\}$ uma base minimal para $\mathbb{Z}_K$ e $\sigma : K \to \mathbb{C}$ um homomorfismo injetor. Então dado $\alpha \in K$, digamos $\alpha = a + b\sqrt{d}$ com $a, b \in \mathbb{Q}$, obtemos que

$$\sigma(\alpha) = a + b\sigma(\sqrt{d}).$$

Também

$$d = \sigma(d) = \sigma(\sqrt{d})^2$$

Logo, $\sigma(\sqrt{d}) = \sqrt{d}$ ou $\sigma(\sqrt{d}) = -\sqrt{d}$. Portanto,

$$\sigma(\alpha) = \alpha \text{ ou } \sigma(\alpha) = \overline{\alpha}.$$

Assim, pelo Teorema 2.3 existem dois homomorfismos injetores $\sigma, \overline{\sigma} : K \to \mathbb{C}$. Logo, $\varphi : K \to \mathbb{R}^2$ definida por

$$\varphi(\alpha) = (\mathrm{Re}(\sigma(\alpha)), \mathrm{Im}(\sigma(\alpha)))$$

é um homomorfismo injetor e $\leqq_2 = \varphi(\mathbb{Z}_K)$ é um reticulado em $\mathbb{R}^2$ gerado por $\varphi(1)$ e $\sigma(\sqrt{d})$, isto é,

$$B' = \{(1,0), (0, \sqrt{-d})\}$$

é uma $\mathbb{Z}$-base de $\leqq_2$ com

$$V(\Gamma_2) = \sqrt{|d|}, \Delta = \frac{\pi}{4\sqrt{|d|}} \text{ e } \delta = \frac{1}{4\sqrt{|d|}}.$$

Como os vetores da base B', são ortogonais temos que o ângulo entre eles é igual $\frac{\pi}{2}$. Portanto, as regiões fundamentais são retângulos. Em particular, se $d = -1$, então a região fundamental é um quadrado e $\leqq_2 = \mathbb{Z}^2$. Note que, $N(\alpha) = N(\varphi(\alpha))$, pois

$$\begin{aligned} N(\alpha) &= (-1)^2 \alpha\overline{\alpha} \\ &= |\sigma(\alpha)|^2 \\ &= N(\sigma(\alpha)). \end{aligned}$$

Como $|\sigma(\alpha)|^2 = |\mathrm{Re}(\sigma(\alpha))|^2 + |\mathrm{Im}(\sigma(\alpha))|^2$ temos que $N(\varphi(\alpha)) = \|\varphi(\alpha)\|^2$.

Observação 2.2 *Se $K = \mathbb{Q}(\sqrt{d})$, onde d é um inteiro livre de quadrado, então $N(\alpha) = N(\varphi(\alpha))$ para todo $\alpha \in K$.*

Capítulo 3

Fatoração em Ideais Primos

Os ideais foram introduzidos com o propósito de recuperar a unicidade da fatoração em domínios. Assim, neste capítulo estudaremos a fatoração de ideais no anel dos inteiros $\mathbb{Z}_K$ de um corpo quadrático $K = \mathbb{Q}(\sqrt{d})$ com $d < 0$, usando a teoria dos reticulados associados a $\mathbb{Z}_K$. Além disso, mostraremos que todo ideal de $\mathbb{Z}_K$ é principal ou é gerado por dois elementos.

3.1 Elementos Irredutíveis de $\mathbb{Z}_K$

Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Então sabemos que $N(\alpha) \in \mathbb{Z}_+$, para todo $\alpha \in \mathbb{Z}_K$. Além disto,

$$N(\beta\gamma) = N(\beta)\, N(\gamma), \forall \beta, \gamma \in \mathbb{Z}_K.$$

Este resultado nos fornece um critério para a análise da irredutibilidade dos elementos de $\mathbb{Z}_K$. Portanto, para estudar a fatoração de α, devemos fazer um estudo nos elementos, cuja norma divide $N(\alpha)$.

Teorema 3.1 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$.*

1. *$\alpha \in U(\mathbb{Z}_K)$ se, e somente se, $N(\alpha) = 1$;*
2. *Se $N(\alpha) = p$, onde p é um número primo, então α é um elemento irredutível de $\mathbb{Z}_K$;*
3. *Se $d = -1$, então $U(\mathbb{Z}_K) = \{\pm 1, \pm i\}$, onde $i^2 = -1$;*

4. *Se* $d = -3$, *então* $U(\mathbb{Z}_K) = \{\pm 1, \pm\omega, \pm\omega^2\}$, *onde* $\omega = \exp(\frac{2\pi i}{3})$;

5. *Se* $d \notin \{-3, -1\}$, *então* $U(\mathbb{Z}_K) = \{-1, 1\}$.

Prova. 1. Suponhamos que $\alpha \in U(\mathbb{Z}_K)$. Então existe $\beta \in \mathbb{Z}_K$ tal que $\alpha\beta = 1$. Logo,

$$N(\alpha) N(\beta) = N(1) = 1.$$

Como $N(\alpha)$ e $N(\beta)$ são inteiros positivos temos que $N(\alpha) = 1$. Reciprocamente, como $N(\alpha) = \alpha\overline{\alpha}$ temos que $\alpha\overline{\alpha} = 1$. Portanto, $\alpha \in U(\mathbb{Z}_K)$.

2. Suponhamos que $\alpha = \beta\gamma$. Então

$$p = N(\alpha) = N(\beta) N(\gamma).$$

Logo, $N(\beta) = 1$ ou $N(\gamma) = 1$. Assim, $\beta \in U(\mathbb{Z}_K)$ ou $\gamma \in U(\mathbb{Z}_K)$. Portanto, α é um elemento irredutível de $\mathbb{Z}_K$.

3. Se $d = -1$, então $\mathbb{Z}_K = \mathbb{Z}[i]$. Dado $\alpha \in U(\mathbb{Z}_K)$ existe $\beta \in \mathbb{Z}_K$ tal que $\alpha\beta = 1$. Logo,

$$N(\alpha) N(\beta) = N(1) = 1.$$

Tomando $\alpha = a + ib$ e $\beta = c + id$, obtemos que

$$(a^2 + b^2)(c^2 + d^2) = 1.$$

Logo, $a^2 + b^2 = 1$. Neste caso, as únicas soluções inteiras são $(\pm 1, 0)$ e $(0, \pm 1)$. Portanto, $U(\mathbb{Z}_K) = \{\pm 1, \pm i\}$.

4. Se $d = -3$, então $\mathbb{Z}_K = \mathbb{Z}[\eta]$, onde $\eta = \frac{1+i\sqrt{3}}{2}$. Dado $\alpha \in U(\mathbb{Z}_K)$ existe $\beta \in \mathbb{Z}_K$ tal que $\alpha\beta = 1$. Logo,

$$N(\alpha) N(\beta) = N(1) = 1.$$

Tomando

$$\alpha = a + b\frac{1 + i\sqrt{3}}{2} \text{ e } \beta = c + d\frac{1 + i\sqrt{3}}{2},$$

obtemos que

$$\left(a^2 + ab + b^2\right)\left(c^2 + cd + d^2\right) = 1.$$

Como $a^2 + ab + b^2 = 1$ temos que $|ab| \leq 1$ e $a \neq b$. Assim, se $|ab| < 1$ e $a \neq b$, temos duas possibilidade: $a = \pm 1$ e $b = 0$ ou $a = 0$ e $b = \pm 1$. Se $|ab| = 1$ e $a \neq b$, temos duas possibilidade: $a = 1$ e $b = -1$ ou $a = -1$ e $b = 1$. Logo, as únicas soluções inteiras são $(\pm 1, 0)$, $(0, \pm 1)$, $(1, -1)$ e $(-1, 1)$. Portanto, $U(\mathbb{Z}_K) = \{\pm 1, \pm\omega, \pm\omega^2\}$.

5. Se $d < -3$, então dado $\alpha \in U(\mathbb{Z}_K)$ existe $\beta \in \mathbb{Z}_K$ tal que $\alpha\beta = 1$. Logo,

$$N(\alpha)\, N(\beta) = N(1) = 1.$$

Tomando

$$\alpha = a + b\sqrt{d} \text{ e } \beta = r + s\sqrt{d},$$

obtemos que

$$\left(a^2 - db^2\right)\left(r^2 - ds^2\right) = 1.$$

Logo, $a^2 - db^2 = 1$. Neste caso, as únicas soluções inteiras são $(\pm 1, 0)$. Finalmente, se $d = -2$, então $a^2 + 2b^2 = 1$ e também, neste caso, as únicas soluções inteiras são $(\pm 1, 0)$. Portanto, $U(\mathbb{Z}_K) = \{-1, 1\}$. ■

Proposição 3.1 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Então existe uma fatoração em $\mathbb{Z}_K$.*

Prova. Suponhamos que $\alpha = \beta\gamma$ é uma fatoração em $\mathbb{Z}_K$, com $\beta, \gamma \notin U(\mathbb{Z}_K)$. Então

$$N(\alpha) = N(\beta)\, N(\gamma)$$

é uma fatoração em $\mathbb{Z}$. Portanto, pela Proposição 1.2, temos que a existência da fatoração em $\mathbb{Z}_K$ segue da existência da fatoração em $\mathbb{Z}$. ■

Proposição 3.2 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Se $d \equiv 3 (\mathrm{mod}\, 4)$, então $\mathbb{Z}_K = \mathbb{Z}[i]$ é o único domínio de fatoração única.*

Prova. Suponhamos que $d \equiv 3 \bmod 4$ e $d \neq -1$. Então

$$1 - d = 2\left(\frac{1-d}{2}\right) \text{ e } 1 - d = (1 + \sqrt{-d})(1 - \sqrt{-d})$$

são duas fatorizações de $1 - d$ em $\mathbb{Z}_K$. Vamos provar que 2 é um elemento irredutível em $\mathbb{Z}_K$. Suponhamos que $2 = \alpha\beta$. Então

$$4 = N(2) = N(\alpha)\, N(\beta).$$

Logo, $N(\alpha) = 1$, 2 ou 4. Como $d \leq -5$, obtemos que $N(\alpha) = 1$ ou 4. Assim, se $N(\alpha) = 1$, então $\alpha \in U(\mathbb{Z}_K)$ e se $N(\alpha) = 4$, então $\beta \in U(\mathbb{Z}_K)$. Portanto, 2 é um elemento irredutível de $\mathbb{Z}_K$. É claro que

$$\mathrm{mdc}(2, 1 + \sqrt{-d}) = \mathrm{mdc}(2, 1 - \sqrt{-d}) = 1,$$

pois $\frac{1\pm\sqrt{-d}}{2} \notin \mathbb{Z}_K$. ■

Já sabemos que, para cada ideal I de $\mathbb{Z}_K$ o conjunto $\varphi(I)$ é um reticulado de $\mathbb{R}^2$. Mas a recíproca é, em geral, falsa. Mas temos o seguinte resultado.

Proposição 3.3 *Sejam $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, $\mathbb{Z}_K$ o anel dos inteiros de K e Γ um reticulado de $\mathbb{R}^2$. Então*:

1. *Se $d \equiv 2$ ou $3 (\mathrm{mod}\, 4)$ e $\sqrt{d}\alpha \in I = \varphi^{-1}(\Gamma)$, para todo $\alpha \in I$, então I é um ideal de $\mathbb{Z}_K$;*

2. *Se $d \equiv 1 (\mathrm{mod}\, 4)$ e $\eta\alpha \in I$, para todo $\alpha \in I = \varphi^{-1}(\Gamma)$ e $\eta = \frac{1+\sqrt{d}}{2}$, então I é um ideal de $\mathbb{Z}_K$.*

Prova. 1. Dados $\alpha, \beta \in I$, existem $\mathbf{x}, \mathbf{y} \in \Gamma$ tais que $\mathbf{x} = \varphi(\alpha)$ e $\mathbf{y} = \varphi(\beta)$. Logo,

$$\mathbf{x} - \mathbf{y} = \varphi(\alpha) - \varphi(\beta) = \varphi(\alpha - \beta),$$

isto é, $\alpha - \beta \in I$. Como $\sqrt{d}\alpha \in I$, para todo $\alpha \in I$, temos que $(a + b\sqrt{d})\alpha \in I$, para todos $a, b \in \mathbb{Z}$. Portanto, I é um ideal de $\mathbb{Z}_K$. De modo análogo, prova-se 2. ■

3.2 Fatoração de Ideais

Nesta seção provaremos a unicidade da fatoração em ideais primos sobre $\mathbb{Z}_K$. Para isso usaremos os resultados obtidos na teoria dos reticulados.

Sejam $I = \langle\alpha\rangle$ e $J = \langle\beta\rangle$ dois ideais principais de $\mathbb{Z}_K$. Então é fácil verificar que

$$IJ = \langle\alpha\beta\rangle.$$

Mais geralmente, se $I = \langle\alpha_1, \ldots, \alpha_m\rangle$ e $J = \langle\beta_1, \ldots, \beta_n\rangle$ dois ideais não nulos de $\mathbb{Z}_K$, então

$$IJ = \langle\alpha_1\beta_1, \ldots, \alpha_1\beta_n, \ldots, \alpha_m\beta_1, \ldots, \alpha_m\beta_n\rangle.$$

Além disso, se $I = \langle\alpha\rangle$ e J é qualquer ideal de $\mathbb{Z}_K$, então

$$IJ = \alpha J = \{\alpha\beta : \beta \in J\}.$$

Sejam I e J dois ideais não nulos em $\mathbb{Z}_K$. Dizemos que I *divide* J se existir um ideal K de $\mathbb{Z}_K$ tal que

$$J = IK.$$

Exemplo 3.1 *Seja* $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-5}]$. *Então é fácil verificar que* 2, 3 *e* $1 \pm \sqrt{-5}$ *são elementos irredutíveis de* $\mathbb{Z}_K$ *e*

$$2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Portanto, $\mathbb{Z}_K$ *não é um domínio de fatoração única. Além disso, o ideal* $I_1 = \langle 2, 1+\sqrt{-5}\rangle$ *não é principal em* $\mathbb{Z}_K$. *Sejam*

$$I_2 = \langle 2, 1 - \sqrt{-5}\rangle, J_1 = \langle 3, 1 + \sqrt{-5}\rangle \ \ e \ \ J_2 = \langle 3, 1 - \sqrt{-5}\rangle,$$

três ideais de $\mathbb{Z}_K$. *Então*

$$I_1 I_2 = \langle 4, 2 + 2\sqrt{-5}, 2 - 2\sqrt{-5}, 6\rangle.$$

Logo, $I_1 I_2 \subseteq \langle 2\rangle$, *pois* 2 *divide cada um dos geradores. Por outro lado,*

$$2 = 6 - 4 \in I_1 I_2.$$

Portanto,

$$I_1 I_2 = \langle 2\rangle.$$

Agora,

$$I_1 J_1 = \langle 6, 2 + 2\sqrt{-5}, 3 + 3\sqrt{-5}, -4 + 2\sqrt{-5}\rangle.$$

Logo, $I_1 I_2 \subseteq \langle 1 + \sqrt{-5}\rangle$, *pois* $1 + \sqrt{-5}$ *divide cada um dos geradores. Por outro lado,*

$$1 + \sqrt{-5} = 3 + 3\sqrt{-5} - (2 + 2\sqrt{-5}) \in I_1 J_1.$$

Portanto,

$$I_1 J_1 = \langle 1 + \sqrt{-5}\rangle.$$

De modo análogo, prova-se que

$$I_2 J_2 = \langle 1 - \sqrt{-5}\rangle \ \ e \ \ J_1 J_2 = \langle 3\rangle.$$

Portanto,

$$\begin{aligned} \langle 6\rangle &= \langle 2\rangle\langle 3\rangle = I_1 I_2 J_1 J_2 \\ &= \langle 1 + \sqrt{-5}\rangle\langle 1 + \sqrt{-5}\rangle = I_1 J_1 I_2 J_2. \end{aligned}$$

Finalmente, $I_2 = \overline{I}_1$ *e* $J_2 = \overline{J}_1$, *onde*

$$\overline{I} = \{\overline{\alpha} : \alpha \in I\}$$

é o conjugado complexo do ideal I. *Neste caso,* $I_1 = \overline{I}_1$ *e* $J_1 \neq \overline{J}_1$, *pois*

$$1 - \sqrt{-5} = 2 - (1 + \sqrt{-5}) \in I_1.$$

Lema 3.1 *Sejam $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, $\mathbb{Z}_K$ o anel dos inteiros de K e I um ideal não nulo de $\mathbb{Z}_K$. Então $I\overline{I} = \langle n \rangle$, para algum $n \in \mathbb{Z}$.*

Prova. Seja I um ideal não nulo de $\mathbb{Z}_K$. Então $\Gamma = \varphi(I)$ é um reticulado associado a I de $\mathbb{R}^2$. Logo, existem dois vetores linearmente independentes $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{R}^2$ tais que

$$\Gamma = \langle \mathbf{x}_1, \mathbf{x}_2 \rangle.$$

Como $\mathbf{x}_1, \mathbf{x}_2 \in \Gamma$ temos que existem $\alpha, \beta \in I$ tais que $\mathbf{x}_1 = \varphi(\alpha)$ e $\mathbf{x}_2 = \varphi(\beta)$. Portanto, $B = \{\alpha, \beta\}$ é uma $\mathbb{Z}$-base de I e

$$I = \langle \alpha, \beta \rangle.$$

É claro que $\overline{I}$ é gerado por $\overline{\alpha}$ e $\overline{\beta}$. Logo,

$$I\overline{I} = \langle \overline{\alpha}\alpha, \alpha\overline{\beta}, \overline{\alpha}\beta, \beta\overline{\beta} \rangle.$$

Como $\overline{\alpha\overline{\alpha}} = \alpha\overline{\alpha}$, $\overline{\beta\overline{\beta}} = \beta\overline{\beta}$ e $\overline{\alpha\overline{\beta} + \overline{\alpha}\beta} = \alpha\overline{\beta} + \overline{\alpha}\beta$ temos que eles estão em $\mathbb{Q}$. Visto que eles são inteiros algébricos temos que $\alpha\overline{\alpha}, \beta\overline{\beta}, \alpha\overline{\beta} + \overline{\alpha}\beta \in \mathbb{Z}$. Seja

$$n = \text{mdc}\left(\alpha\overline{\alpha}, \beta\overline{\beta}, \alpha\overline{\beta} + \overline{\alpha}\beta\right).$$

Afirmação: $I\overline{I} = \langle n \rangle$.

De fato. Como $n = \text{mdc}\left(\alpha\overline{\alpha}, \beta\overline{\beta}, \alpha\overline{\beta} + \overline{\alpha}\beta\right)$ temos que existem $r, s, t \in \mathbb{Z}$ tais que

$$\begin{aligned} n &= r\alpha\overline{\alpha} + s\beta\overline{\beta} + t(\alpha\overline{\beta} + \overline{\alpha}\beta) \\ &= r\alpha\overline{\alpha} + s\beta\overline{\beta} + t\alpha\overline{\beta} + t\overline{\alpha}\beta. \end{aligned}$$

Logo, $n \in I\overline{I}$, isto é, $\langle n \rangle \subseteq I\overline{I}$. Reciprocamente, por construção existem $\gamma, \delta, \lambda \in \mathbb{Z} \subseteq \mathbb{Z}_K$ tais que $\alpha\overline{\alpha} = \gamma n$, $\beta\overline{\beta} = \delta n$ e $\alpha\overline{\beta} + \overline{\alpha}\beta = \lambda n$. Por outro lado, é fácil verificar que

$$\frac{\overline{\alpha}\beta}{n} \text{ e } \frac{\alpha\overline{\beta}}{n}$$

são raízes do polinômio $f(x) = x^2 - \lambda x + \gamma\delta \in \mathbb{Z}[x]$. Assim,

$$\frac{\overline{\alpha}\beta}{n}, \frac{\alpha\overline{\beta}}{n} \in \mathbb{Z}_K,$$

isto é, existem $\epsilon, \varepsilon \in \mathbb{Z}_K$ tais que $\overline{\alpha}\beta = \epsilon n$ e $\alpha\overline{\beta} = \varepsilon n$. Portanto, $\alpha\overline{\alpha}, \beta\overline{\beta}, \alpha\overline{\beta}, \overline{\alpha}\beta \in \langle n \rangle$ e $I\overline{I} \subseteq \langle n \rangle$. ■

Proposição 3.4 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K. Se I, J e L são ideais não nulos de $\mathbb{Z}_K$, Então*:

1. *Se $IL \subseteq IJ$, então $L \subseteq J$. Em particular, se $IJ = IL$, então $J = L$;*

2. *$J \subseteq I$ se, e somente se, I divide J;*

3. *Se P é um ideal primo de $\mathbb{Z}_K$ tal que P divide IJ, então P divide I ou P divide J.*

Prova. 1. Suponhamos que $IL \subseteq IJ$. Então, pelo Lema 3.1, temos que

$$nL = I\overline{I}L \subseteq I\overline{I}J = nJ.$$

Portanto,

$$L = n^{-1}(nL) \subseteq n^{-1}(nJ) = J.$$

2. Primeiro suponhamos que $I = \langle \alpha \rangle$ e $J \subseteq I$. Seja

$$K = \{\alpha^{-1}\beta : \beta \in J\}.$$

Então é fácil verificar que K é um ideal de $\mathbb{Z}_K$ e $\alpha K = J$. Portanto, $J = IK$. Agora, suponhamos que I é arbitrário e $J \subseteq I$. Então

$$\overline{I}J \subseteq I\overline{I} = \langle n \rangle.$$

Assim, existe um ideal K de $\mathbb{Z}_K$ tal que

$$nK = \overline{I}J \text{ e } I\overline{I}K = \overline{I}J.$$

Por 1, $IK = J$. Portanto I divide J. A recíproca é imediata.

3. Suponhamos que P divide IJ. Então $IJ \subseteq P$. Logo, $I \subseteq P$ ou $J \subseteq P$. Portanto, P divide I ou P divide J. ■

Proposição 3.5 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Então:*

1. *Se I é um ideal não nulo de $\mathbb{Z}_K$, então existe somente um número finito de ideais J entre I e $\mathbb{Z}_K$.*

2. *Todo ideal próprio de $\mathbb{Z}_K$ está contido em um ideal maximal.*

Prova. 1. Seja I um ideal não nulo de $\mathbb{Z}_K$. Então $\varphi(I)$ é um reticulado associado a I de $\mathbb{R}^2$. Logo, pelo Lema 1.7, existe apenas um número finito de reticulados Λ entre $\varphi(I)$ e $\varphi(\mathbb{Z}_K)$. Portanto, existe somente um número finito de ideais J entre I e $\mathbb{Z}_K$.

2. Seja I um ideal próprio de $\mathbb{Z}_K$. Então I está contido em apenas um número finito de ideais $\mathbb{Z}_K$. Portanto, basta procurar entre eles o que seja maximal. ■

Teorema 3.2 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Então todo ideal não nulo de $\mathbb{Z}_K$ pode ser escrito de modo único, a menos da ordem, como um produto de ideais primos.*

Prova. (Existência) Seja I ideal não nulo de $\mathbb{Z}_K$. Se I é um ideal primo, nada há para provar. Suponhamos que I não seja primo. Então I não é maximal. Assim, podemos encontrar um ideal próprio I_1 de $\mathbb{Z}_K$ tal que $I \subseteq I_1$. Logo, pela Proposição 3.4, I_1 divide I. Assim, existe um ideal J_1 de $\mathbb{Z}_K$ tal que $I = I_1 J_1$. Portanto, $I \subset J_1$, pois se $I = I_1 J_1 = J_1$, então pela Proposição 3.4, $\mathbb{Z}_K = I_1$, o que é uma contradição. De modo análogo mostra-se que $I \subset I_1$. Como existe somente um número finito de ideais entre I e $\mathbb{Z}_K$ temos que este processo termina após um número finito de passos. Quando isto ocorre todos os fatores são ideais maximais e, assim, ideais primos. Portanto, todo ideal não nulo de $\mathbb{Z}_K$ pode ser escrito como um produto de ideais primos.

(Unicidade) Suponhamos que temos dois produto de ideais primos:

$$P_1 \cdots P_r = Q_1 \cdots Q_s.$$

Vamos usar indução sobre r. Se $r = 1$, então

$$P_1 = Q_1 \cdots Q_s.$$

Após uma reordenação, se necessário, podemos supor que Q_1 divide P_1. Como P_1 é maximal temos que

$$P_1 = Q_1.$$

Assim, se $s > 1$, então pela Proposição 3.4, obtemos que

$$\mathbb{Z}_K = Q_2 \cdots Q_s$$

e $\mathbb{Z}_K = Q_j$, para algum $2 \leq j \leq s$, o que é uma contradição. Logo, $s = 1$.

Suponhamos que o resultado seja válido para $r - 1$ e

$$P_1 \cdots P_r = Q_1 \cdots Q_s.$$

Após uma reordenação, se necessário, podemos supor que P_r divide Q_s. Como Q_s é maximal temos que

$$P_r = Q_s.$$

Logo, pela Proposição 3.4, obtemos que

$$P_1 \cdots P_{r-1} = Q_1 \cdots Q_{s-1}.$$

Pela hipótese de indução segue que $r-1 = s-1$ e, assim, $r = s$. Portanto, após uma reordenação, se necessário, obtemos que $P_j = Q_j$, $j = 1, \ldots, r$. ■

Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Seja I ideal não nulo de $\mathbb{Z}_K$. Então $I = P_1 \cdots P_r$, onde P_i são ideais primos de $\mathbb{Z}_K$ com $P_i + P_j = \langle 1 \rangle$, se $i \neq j$. Logo,

$$\frac{\mathbb{Z}_K}{I} \simeq \frac{\mathbb{Z}_K}{P_1} \times \cdots \times \frac{\mathbb{Z}_K}{P_r}.$$

Como

$$\frac{\mathbb{Z}_K}{P_j}, j = 1, \ldots, r,$$

é finito temos, pela demonstração do Teorema 2.7, que

$$\frac{\mathbb{Z}_K}{I}$$

é finito. A *norma* de um ideal não nulo I de $\mathbb{Z}_K$ é definida por

$$N(I) = \left| \frac{\mathbb{Z}_K}{I} \right|.$$

Teorema 3.3 *Sejam $K = \mathbb{Q}(\theta)$ e $\mathbb{Z}_K$ o anel dos inteiros de K. Então*:

1. *Todo ideal não-nulo I de $\mathbb{Z}_K$ tem uma $\mathbb{Z}$-base $B = \{\alpha_1, \ldots, \alpha_n\}$, onde $[K : \mathbb{Q}] = n$.*

2. $$N(I) = \sqrt{\left| \frac{D(B)}{D} \right|},$$

   onde D é o discriminante de K.

Prova. 1. Como $\frac{\mathbb{Z}_K}{I}$ é finito temos, pela Observação 1.3, que $(I, +)$ é um grupo abelino livre de posto n. Portanto, I tem uma $\mathbb{Z}$-base da forma $B = \{\alpha_1, \ldots, \alpha_n\}$.

2. Seja $B' = \{\beta_1, \ldots, \beta_n\}$ uma $\mathbb{Z}$-base de $\mathbb{Z}_K$. Como $\alpha_i \in \mathbb{Z}_K$ temos que existem únicos $c_{ij} \in \mathbb{Z}$ tais que

$$\alpha_i = \sum_{j=1}^{n} c_{ij} \beta_j.$$

Assim, se $\mathbf{C} = (c_{ij})$, então

$$N(I) = \left| \frac{\mathbb{Z}_K}{I} \right| = |\det(\mathbf{C})|.$$

Como $D(B) = (\det(\mathbf{C}))^2 D(B')$ temos que

$$N(I) = \sqrt{\left|\frac{D(B)}{D}\right|},$$

onde $D = D(B')$. ■

Corolário 3.1 *Sejam $K = \mathbb{Q}(\theta)$ e $\mathbb{Z}_K$ o anel dos inteiros de K. Se $I = \langle\alpha\rangle$ é um ideal principal de $\mathbb{Z}_K$, então $N(I) = N(\alpha)$.* ■

Teorema 3.4 *Sejam $K = \mathbb{Q}(\theta)$, com grau $n = k + 2l$, e I um ideal não nulo de $\mathbb{Z}_K$. Então*

$$V(\varphi(I)) = \frac{N(I)\sqrt{|D|}}{2^l},$$

onde D é o discriminante de K.

Prova. Sejam $B' = \{\alpha_0, \alpha_1, \ldots, \alpha_{n-1}\}$ uma $\mathbb{Z}$-base de I, $\Gamma = \varphi(I) = \langle\varphi(\alpha_0), \varphi(\alpha_1), \ldots, \varphi(\alpha_{n-1})\rangle$ um reticulado em $\mathbb{R}^n$ e $M = (\varphi(\alpha_i))$ a matriz geradora de Γ. Então

$$V(\Gamma) = |\det(M)|.$$

Pelo Teorema 2.8, $\det(M) = (-2i)^{-l}E$, de modo que, $|\det(M)| = 2^{-l}|E|$. Como $D(B') = E^2$ e

$$N(I) = \left|\frac{D(B')}{D}\right|,$$

temos que

$$V(\Gamma) = \frac{N(I)\sqrt{|D|}}{2^l}.$$

■

Teorema 3.5 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Então $\mathbb{Z}_K$ é um domínio de fatoração única se, e somente se, $\mathbb{Z}_K$ é um domínio de ideais principais.*

Prova. Suponhamos que $\mathbb{Z}_K$ seja um domínio de fatoração única e P qualquer ideal primo não nulo de $\mathbb{Z}_K$. Então P contém um elemento irredutível, digamos π, pois todo $\alpha \in P$,$\alpha \neq 0$ é um produto de elementos irredutíveis. Logo, π é um elemento primo e $\langle\pi\rangle$ é um ideal primo. Como $\langle\pi\rangle$ é maximal e $\langle\pi\rangle \subseteq P$ temos que $P = \langle\pi\rangle$. Potanto, P é principal. Assim, pelo Teorema 3.2, todo ideal não nulo de $\mathbb{Z}_K$ é principal. Pela Proposição 1.4, temos a recíproca. ■

Proposição 3.6 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Se P é um ideal primo não nulo de $\mathbb{Z}_K$, então $P = \langle p \rangle$ ou $P\overline{P} = \langle p \rangle$, para algum primo $p \in \mathbb{Z}$.*

Prova. Seja P um ideal primo não nulo de $\mathbb{Z}_K$. Então $P\overline{P} = \langle n \rangle$, para algum $n \in \mathbb{Z}$. Como $\mathbb{Z}$ é um domínio de fatoração única e $n \neq 1$ temos que

$$n = \pm p_1 \cdots p_r,$$

onde os p_i são primos distintos. Logo, por hipótese, P divide um dos fatores $\langle p \rangle$ de $\langle n \rangle$, onde $p = p_j$. Como $\overline{P}$ também divide $\langle p \rangle$, pois $p = \overline{p}$, temos que $P\overline{P}$ divide $\langle p^2 \rangle$. Assim, $\langle p^2 \rangle \subseteq P\overline{P}$. Temos duas possibilidades:

$$\langle p^2 \rangle = P\overline{P} \text{ ou } \langle p^2 \rangle \subset P\overline{P}.$$

Se $\langle p^2 \rangle = P\overline{P}$ temos, pelo Teorema 3.2, que $P = \overline{P} = \langle p \rangle$. Se $\langle p^2 \rangle \subset P\overline{P}$ temos, pelo Teorema 3.2, que $P\overline{P} = \langle p \rangle$. Portanto,

$$P = \overline{P} = \langle p \rangle \text{ ou } P\overline{P} = \langle p \rangle.$$

■

Proposição 3.7 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Se $p \in \mathbb{Z}$ é um número primo, então existe um ideal primo não nulo P de $\mathbb{Z}_K$ tal que*

$$P = \langle p \rangle \text{ ou } P\overline{P} = \langle p \rangle .$$

Prova. Seja p um número primo de $\mathbb{Z}$. Então $I = \langle p \rangle$ é um ideal não nulo de $\mathbb{Z}_K$. Pelo Teorema 3.2, existe um ideal primo P de $\mathbb{Z}_K$ tal que P divide I. Como $\overline{P}$ também divide I, pois $\overline{p} = p$, temos que $P\overline{P}$ divide $\langle p^2 \rangle$. Assim, $\langle p^2 \rangle \subseteq P\overline{P}$. Temos duas possibilidades:

$$\langle p^2 \rangle = P\overline{P} \text{ ou } \langle p^2 \rangle \subset P\overline{P}.$$

Se $\langle p^2 \rangle = P\overline{P}$ temos, pelo Teorema 3.2, que $P = \overline{P} = \langle p \rangle$. Se $\langle p^2 \rangle \subset P\overline{P}$ temos, pelo Lema 3.1, que $P\overline{P} = \langle p \rangle$. Portanto,

$$P = \overline{P} = \langle p \rangle \text{ ou } P\overline{P} = \langle p \rangle.$$

■

Seja $p \in \mathbb{Z}$ um número primo. Dizemos que p *permanece primo* em $\mathbb{Z}_K$ se $P = \langle p \rangle$ é um ideal primo em $\mathbb{Z}_K$. Se $P\overline{P} = \langle p \rangle$ e $P \neq \overline{P}$, dizemos que p é *decomponível* em $\mathbb{Z}_K$. Se $P\overline{P} = \langle p \rangle$ e $P = \overline{P}$, dizemos que p é *ramificado* em $\mathbb{Z}_K$.

Exemplo 3.2 *Seja* $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-5}]$. *Então para o ideal* $P = \langle 2, 1+\sqrt{-5}\rangle$ *de* $\mathbb{Z}_K$ *temos que* $P = \overline{P}$ *e* $P\overline{P} = \langle 2\rangle$. *Portanto,* 2 *é ramificado em* $\mathbb{Z}_K$. *Para o ideal* $P = \langle 3, 1+\sqrt{-5}\rangle$ *de* $\mathbb{Z}_K$ *temos que* $P \neq \overline{P}$ *e* $P\overline{P} = \langle 3\rangle$. *Portanto,* 3 *é decomponível em* $\mathbb{Z}_K$.

Proposição 3.8 *Sejam* $K = \mathbb{Q}(\sqrt{d})$ *e* $\mathbb{Z}_K$ *o anel dos inteiros de* K, *onde* $d < 0$ *e* $p \in \mathbb{Z}$ *um primo.*

1. *Suponhamos que* $d \equiv 2$ *ou* $3(\mathrm{mod}\, 4)$. *Então* p *permanece primo em* $\mathbb{Z}_K$ *se, e somente se,* $f = x^2 - d$ *é irredutível sobre* $\mathbb{Z}_p$;

2. *Suponhamos que* $d \equiv 1(\mathrm{mod}\, 4)$. *Então* p *permanece primo em* $\mathbb{Z}_K$ *se, e somente se,*

$$f = x^2 - x + \frac{1-d}{4}$$

é irredutível sobre $\mathbb{Z}_p$.

Prova. 1. Suponhamos que $d \equiv 2$ ou $3(\mathrm{mod}\, 4)$ e $p \in \mathbb{Z}$ um número primo. Então $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$ e $f = x^2 - d$ é irredutível sobre $\mathbb{Z}$, pois d é livre de quadrados. A função

$$\rho : \mathbb{Z}_K \to \mathbb{Z}_p[\sqrt{d}]$$

definida por $\rho(a+b\sqrt{d}) = \overline{a}+\overline{b}\sqrt{d}$, onde $\overline{a}, \overline{b} \in \mathbb{Z}_p$, é um homomorfismo de anéis sobrejetor e $\ker\rho = \langle p\rangle = p\mathbb{Z}_K$. Logo,

$$\frac{\mathbb{Z}_K}{\langle p\rangle} \simeq \mathbb{Z}_p[\sqrt{d}].$$

Por outro lado, a função

$$\sigma : \mathbb{Z}_p[x] \to \mathbb{Z}_p[\sqrt{d}]$$

definida por $\sigma(g) = g(\sqrt{d})$, para todo $g \in \mathbb{Z}_p[x]$, é um homomorfismo sobrejetor de anéis e $\ker\sigma = \langle f\rangle$. Logo,

$$\frac{\mathbb{Z}_p[x]}{\langle f\rangle} \simeq \mathbb{Z}_p[\sqrt{d}].$$

Assim,

$$\frac{\mathbb{Z}_p[x]}{\langle f\rangle} \simeq \frac{\mathbb{Z}_K}{\langle p\rangle}.$$

Portanto, p permanece primo em $\mathbb{Z}_K$, isto é, $P = \langle p\rangle$ é um ideal primo maximal de $\mathbb{Z}_K$ se, e somente se, $\frac{\mathbb{Z}_K}{P}$ é um corpo se, e somente se, f é irredutível sobre $\mathbb{Z}_p$.

2. A parte (b) é análoga. ■

Exemplo 3.3 *Seja* $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-67}]$. *Então* $-67 \equiv 1(\mathrm{mod}\, 4)$. *É fácil verificar que o polinômio* $f = x^2 - x + 17$ *é irredutível sobre* $\mathbb{Z}_p$, *para* $p = 2$, 3 *ou* 5. *Portanto, os números primos* 2, 3 *e* 5 *permanecem primos em* $\mathbb{Z}_K$.

3.3 Classe de Ideais

Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Sejam I e J dois ideais não nulos de $\mathbb{Z}_K$. Dizemos que I e J são *similares* se existirem $\alpha, \beta \in \mathbb{Z}_K^*$ tais que

$$\beta J = \alpha I.$$

Vamos denotar por $I \sim J$. É fácil verificar que $\sim$ é uma relação de equivalência em $\mathbb{Z}_K$. Para cada ideal I de $\mathbb{Z}_K$, $[I]$ denota o subconjunto formado pelos ideais de $\mathbb{Z}_K$ que são similares a I, isto é,

$$[I] = \{J : J \text{ é um ideal de } \mathbb{Z}_K \text{ e } J \sim I\}.$$

Esse conjunto é chamado *a classe de ideal* determinada por I.

Observação 3.1 *Como $\gamma = \beta^{-1}\alpha \in K^*$, dizemos que I e J são* similares*, se existe $\gamma \in K^*$ tal que*

$$J = \gamma I.$$

Seja $\mathcal{I}_{\mathbb{Z}_K}$ a família de todos os ideais principais de $\mathbb{Z}_K$. Então é fácil verificar que $\mathcal{I}_{\mathbb{Z}_K}$ é um semigrupo multiplicativo com elemento identidade $\mathbb{Z}_K = \langle 1 \rangle$ e que a função $\sigma : \mathbb{Z}_K \to \mathcal{I}_{\mathbb{Z}_K}$ definida por $\sigma(\alpha) = \langle \alpha \rangle$, para todo $\alpha \in \mathbb{Z}_K$, é um homomorfismo de semigrupos. Além disso, $\mathbb{Z}_K$ é um domínio de ideais principais se, e somente se, σ é sobrejetora.

Proposição 3.9 *Sejam $K = \mathbb{Q}(\sqrt{d})$, $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$, e I um ideal não nulo de $\mathbb{Z}_K$. Então I é similar a $\mathbb{Z}_K$ se, e somente se, I é um ideal principal.*

Prova. I é similar a $\mathbb{Z}_K$ se, e somente se, existe $\gamma \in K^*$ tal que $I = \gamma \mathbb{Z}_K$. Logo, $\gamma \in I$, isto é, $\gamma \in \mathbb{Z}_K$. Portanto, $I = \langle \gamma \rangle$. ■

O *conjunto quociente* de $\mathbb{Z}_K$ pela relação de equivalência $\sim$, em símbolos $\mathcal{C}$, é o conjunto de todas as classes de ideais de $\mathbb{Z}_K$. Assim,

$$\mathcal{C} = \{[I] : I \text{ é um ideal de } \mathbb{Z}_K\}.$$

Teorema 3.6 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Então $\mathcal{C}$ com a operação*

$$[I][J] = [IJ],$$

para todos os ideais I e J de $\mathbb{Z}_K$, é um grupo abeliano.

Prova. Sejam I, I', J e J' ideais de $\mathbb{Z}_K$ tais que $[I] = [I']$ e $[J] = [J']$. Então existem $\alpha, \beta \in K^*$ tais que

$$I' = \alpha I \quad \text{e} \quad J' = \beta J.$$

Logo,

$$I'J' = \alpha\beta IJ.$$

Assim, $[IJ] = [I'J']$, isto é, a operação é bem definida. É fácil verificar que essa operação é associativa, comutativa e que $[\mathbb{Z}_K]$ é o elemento identidade. Finalmente, pelo Lema 3.1, $I\overline{I} = \langle n \rangle$, para algum $n \in \mathbb{Z}$. Como $[\langle n \rangle] = [\langle 1 \rangle]$ temos que $[I][\overline{I}] = [\mathbb{Z}_K]$, isto é, $[\overline{I}]$ é o inverso de $[I]$. ■

A ordem $|\mathcal{C}|$ do grupo de classe $\mathcal{C}$ é chamada de *número de classe*.

Corolário 3.2 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Então $\mathbb{Z}_K$ é um domínio de fatoração única se, e somente se, $|\mathcal{C}| = 1$.* ■

Lema 3.2 *Sejam $K = \mathbb{Q}(\sqrt{d})$, $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$ e I um ideal não nulo de $\mathbb{Z}_K$. Então $[\mathbb{Z}_K : nI] = n^2 [\mathbb{Z}_K : I]$, para todo $n \in \mathbb{Z}$.*

Prova. Sejam $\Gamma = \varphi(\mathbb{Z}_K)$ e $\Lambda = \varphi(I)$ os reticulados de $\mathbb{R}^2$ associados a $\mathbb{Z}_K$ e I, respectivamente. Assim, pelo Corolário 1.3, temos que $[\mathbb{Z}_K : nI] = n^2 [\mathbb{Z}_K : I]$, para todo $n \in \mathbb{Z}$. ■

Proposição 3.10 *Sejam $K = \mathbb{Q}(\sqrt{d})$, $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$ e I um ideal não nulo de $\mathbb{Z}_K$. Então*

$$N(I) = [\mathbb{Z}_K : I].$$

Prova. Se $I = \mathbb{Z}_K$ nada há para provar. Primeiro vamos supor que I é igual a um ideal primo P. Então, pela Proposição 3.6, temos que existe um número primo $p \in \mathbb{Z}$ tal que $P = \langle p \rangle$ ou $P\overline{P} = \langle p \rangle$. Se $P = \langle p \rangle$ e J qualquer ideal de $\mathbb{Z}_K$, então $N(P) = p^2$ e $JP = pJ$. Logo,

$$[\mathbb{Z}_K : JP] = p^2[\mathbb{Z}_K : J]$$

e

$$[\mathbb{Z}_K : P] = [\mathbb{Z}_K : p\mathbb{Z}_K] = p^2[\mathbb{Z}_K : \mathbb{Z}_K] = p^2.$$

Assim, $[\mathbb{Z}_K : JP] = [\mathbb{Z}_K : J][\mathbb{Z}_K : P]$ e $[\mathbb{Z}_K : P] = N(P)$. Se $P\overline{P} = \langle p \rangle$ e J qualquer ideal de $\mathbb{Z}_K$, então $N(P) = p$ e $JP\overline{P} = pJ$. Pela Proposição 3.4, temos que $JP\overline{P} \subset JP \subset J$. Logo,

$$[\mathbb{Z}_K : J] < [\mathbb{Z}_K : JP] < [\mathbb{Z}_K : JP\overline{P}] = p^2[\mathbb{Z}_K : J].$$

Como cada índice é um divisor do próximo temos que $[\mathbb{Z}_K : JP] = p[\mathbb{Z}_K : J]$. Em particular, para $J = \mathbb{Z}_K$, obtemos que $[\mathbb{Z}_K : P] = p = N(P)$. Assim, $[\mathbb{Z}_K : JP] = [\mathbb{Z}_K : J][\mathbb{Z}_K : P]$ e $[\mathbb{Z}_K : P] = N(P)$. Finalmente, se I é um ideal arbitrário de $\mathbb{Z}_K$, então pelo Teorema 3.2

$$I = P_1 \cdots P_n,$$

onde $P_1, \ldots, P_n$ são ideais primos de $\mathbb{Z}_K$. Logo, por indução sobre n, obtemos que

$$\begin{aligned} [\mathbb{Z}_K : I] &= [\mathbb{Z}_K : P_1 \cdots P_{n-1}][\mathbb{Z}_K : P_n] \\ &= N(P_1 \cdots P_{n-1}).N(P_n) \\ &= N(I). \end{aligned}$$

■

Corolário 3.3 *Sejam $K = \mathbb{Q}(\sqrt{d})$, $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$ e I, J dois ideais não nulos de $\mathbb{Z}_K$. Então $[\mathbb{Z}_K : IJ] = [\mathbb{Z}_K : I]\,[\mathbb{Z}_K : J]$.* ■

Teorema 3.7 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Então toda classe de ideais em $\mathbb{Z}_K$ contém um ideal I tal que*

$$N(I) \leq \mu,$$

onde $\mu = \dfrac{2\sqrt{|D|}}{\pi}$ e D é o discriminante de $\mathbb{Z}_K$.

Prova. Seja I um ideal qualquer de $\mathbb{Z}_K$. Devemos encontrar um ideal $L \in [I]$ tal que $N(L) \leq \mu$. Seja $\Gamma = \varphi(I)$ o reticulado de $\mathbb{R}^2$ associado a I. Então, pelo Corolário 1.5, existe $\mathbf{x} \in \Lambda^*$ tal que

$$\|\mathbf{x}\|^2 \leq \frac{4V(\Gamma)}{\pi}.$$

Como $\mathbf{x} \in \Lambda^*$ temos que existe $\alpha \in I^*$ tal que $\varphi(\alpha) = \mathbf{x}$. Assim, $\langle \alpha \rangle \subseteq I$ e, pela Proposição 3.4, existe um ideal J de $\mathbb{Z}_K$ tal que $IJ = \langle \alpha \rangle$. Logo, $N(\alpha) = N(I)N(J)$. Pela Proposição 3.3, temos que

$$V(\Gamma) = \frac{N(I)\sqrt{|D|}}{2}.$$

Como $N(\alpha) = N(\varphi(\alpha)) = \|\mathbf{x}\|^2$ temos que

$$\begin{aligned} N(I)N(J) &\leq \frac{4V(\Gamma)}{\pi} \\ &= \frac{4\frac{N(I)\sqrt{|D|}}{2}}{\pi}, \end{aligned}$$

isto é,

$$N(J) \leq \mu,$$

onde $\mu = \dfrac{2\sqrt{|D|}}{\pi}$ e D é o discriminante de $\mathbb{Z}_K$. Finalmente, como IJ é um ideal principal temos que $[J]$ é a iversa de $[I]$, isto é, $[J] = [\overline{I}]$. Assim, provamos que $[J]$ contém um ideal cuja norma satisfaz a desigualdade. A prova segue-se trocando $\overline{I}$ por I. ■

Teorema 3.8 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Então o grupo de classe* C *é finito.*

Prova. Pela Proposição 3.10 e pelo Teorema 3.7, basta provar que existe um número finito de ideais I tais que

$$[\mathbb{Z}_K : I] \leq \mu.$$

Seja $\Lambda = \varphi(I)$ o reticulado de $\mathbb{R}^2$ associado a I. Escolhendo $n \in \mathbb{Z}_+$, com $n \leq \mu$, obtemos, pelo Corolário 1.6, que existe um número finito de reticulados Γ de $\mathbb{R}^2$ contendo Λ tal que $[\Gamma : \Lambda] = n$. Como existe um número finito de possibilidades para n temos o resultado.■

Teorema 3.9 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Então o grupo de classe* C *é gerado pela classe dos ideais primos P que divide $\langle p \rangle$, com $p \leq \lfloor \mu \rfloor$, onde p é um número primo e $\lfloor \cdot \rfloor$ é a função maior inteiro.*

Prova. Pelo Teorema 3.7, todo elemento de C contém um ideal I de $\mathbb{Z}_K$ tal que $N(I) \leq \mu$. Como $N(I)$ é um número inteiro temos que

$$N(I) \leq \lfloor \mu \rfloor.$$

Suponhamos que

$$I = P_1 \cdots P_m,$$

onde $P_1, \ldots, P_m$ são ideais primos de $\mathbb{Z}_K$. Então

$$N(I) = N(P_1) \cdots N(P_m).$$

Logo,

$$N(P_j) \leq \lfloor \mu \rfloor, \forall j = 1, \ldots, m.$$

Portanto, as classes dos ideais primos P, com $N(P) \leq \lfloor \mu \rfloor$, formam um conjunto de geradores de C. ■

Podemos usar o Teorema 3.9, como um algoritmo de tentativas e erros para determinar C.

Algoritmo

1. Calcular o discriminante D de $\mathbb{Z}_K$, o valor de μ e em seguida $\lfloor \mu \rfloor$.
2. Calcular os primos p com $p \leq \lfloor \mu \rfloor$.
3. Verificar se p permanece primo em $\mathbb{Z}_K$. Se p permanece primo, então exclua $\langle p \rangle$ da classe dos fatores primos. Se não, então inclua ele na classe de um dos fatores primos.
4. Repetir o Passo 3 para todos os geradores primos de $\mathcal{C}$.
5. Calcular as relações entre os geradores primos de $\mathcal{C}$.

Exemplos 3.1 *Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Então, pelo Teorema 2.9, $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$ e $D = 4d$ se $d \equiv 2$ ou $3 (\mathrm{mod}\, 4)$, $\mathbb{Z}_K = \mathbb{Z}[\eta]$ e $D = d$ se $d \equiv 1 (\mathrm{mod}\, 4)$, onde $\eta = \frac{1+\sqrt{d}}{2}$.*

1. *Se $d = -7$, então $d \equiv 1 (\mathrm{mod}\, 4)$. Logo, $\mathbb{Z}_K = \mathbb{Z}[\eta]$ e $D = -7$. Assim,*

$$\mu = \frac{2\sqrt{|D|}}{\pi} = \frac{2\sqrt{7}}{\pi} \approx 1,7$$

   e $\lfloor \mu \rfloor = 1$. A classe de ideais primos de $\mathbb{Z}_K$ é vazia. Portanto, $\mathrm{C} = \{[0]\}$ e $\mathbb{Z}_K$ é um domínio de ideais principais.

2. *Se $d = -67$, então $d \equiv 1 (\mathrm{mod}\, 4)$. Logo, $\mathbb{Z}_K = \mathbb{Z}[\eta]$ e $D = -67$. Assim,*

$$\mu = \frac{2\sqrt{|D|}}{\pi} = \frac{2\sqrt{67}}{\pi} \approx 5,2$$

e $\lfloor \mu \rfloor = 5$. *O grupo de classe* C *é gerado pelos ideais primos de* $\mathbb{Z}_K$ *dividindo* $\langle 2 \rangle$, $\langle 3 \rangle$ *e* $\langle 5 \rangle$. *Pela Proposição 3.8, p permanece primo em* $\mathbb{Z}_K$ *se, e somente se,*

$$f = x^2 - x + 17$$

é irredutível sobre $\mathbb{Z}_p$. *É fácil verificar que isto é verdade para os primos* 2, 3 *e* 5. *Portanto,* $\mathrm{C} = \{[\mathbb{Z}_K]\}$ *e* $\mathbb{Z}_K$ *é um domínio de ideais principais.*

3. *Se* $d = -14$, *então* $d \equiv 2 (\mathrm{mod}\, 4)$. *Logo,* $\mathbb{Z}_K = \mathbb{Z}[\sqrt{d}]$ *e* $D = -56$. *Assim,*

$$\mu = \frac{2\sqrt{|D|}}{\pi} = \frac{2\sqrt{56}}{\pi} \approx 4,7$$

e $\lfloor \mu \rfloor = 4$. *O grupo de classe* C *é gerado pelos ideais primos de* $\mathbb{Z}_K$ *dividindo* $\langle 2 \rangle$ *e* $\langle 3 \rangle$. *Pela Proposição 3.8, p permanece primo em* $\mathbb{Z}_K$ *se, e somente se,*

$$f = x^2 + 14$$

é irredutível sobre $\mathbb{Z}_p$. *É fácil verificar que f é redutível para os primos* 2 *e* 3. *Note que,* $P\overline{P} = \langle 2 \rangle$ *e* $P = \overline{P}$, *onde* $P = \langle 2, \sqrt{-14} \rangle$, $Q\overline{Q} = \langle 3 \rangle$ *e* $Q \neq \overline{Q}$, *onde* $Q = \langle 3, 1 + \sqrt{-14} \rangle$. *Logo, a ordem da classe* $[P]$ *é igual a* 2 *em* C, *pois* $[P]^2 = [\langle 1 \rangle]$. *Por outro lado, para calcular a ordem da classe* $[Q]$, *podemos calcular as potências do ideal explicitamente e encontrar a menor potência cujo reticulado associado é similar ao reticulado associado a* $\mathbb{Z}_{\mathbb{K}}$, *o que não é eficiente. Assim, é melhor calcular a norma de alguns elementos de* $\mathbb{Z}_{\mathbb{K}}$, *na tentativa de encontrar uma relação entre os geradores. Os mais naturais para tentar são:* $\sqrt{-14}$ *e* $1 + \sqrt{-14}$. *Como*

$$N(\sqrt{-14}) = 14 \ \ e \ \ N(1 + \sqrt{-14}) = 15$$

temos que eles não são bons, pois envolvem os primos 5 *e* 7 *que não estão entre os fatores de nossos geradores. O elemento* $2 + \sqrt{-14}$ *é melhor, pois*

$$N(2 + \sqrt{-14}) = 18 = 2 \cdot 3 \cdot 3.$$

Logo,

$$\langle 2 + \sqrt{-14} \rangle \langle 2 - \sqrt{-14} \rangle = P\overline{P}Q\overline{Q}Q\overline{Q} = P^2Q^2\overline{Q}^2.$$

Como $\langle 2 + \sqrt{-14} \rangle \neq \langle 2 - \sqrt{-14} \rangle$ *e* $\langle 2 - \sqrt{-14} \rangle = \overline{\langle 2 + \sqrt{-14} \rangle}$ *temos que* $\langle 2 + \sqrt{-14} \rangle = PQ^2$ *ou* $\langle 2 + \sqrt{-14} \rangle = P\overline{Q}^2$. *Note que* $\langle 3 \rangle$ *é um fator tanto de* PQ^2 *quanto de* $P\overline{Q}^2$. *Assim, podemos assumir que* $\langle 2 + \sqrt{-14} \rangle = PQ^2$. *Então* $[P][Q]^2 = [\langle 1 \rangle]$, *pois* $\langle 2 + \sqrt{-14} \rangle$ *é um ideal principal. Logo,* $[Q]^2 = [P]^{-1} = [P]$ *e* $[Q]^4 = [\langle 1 \rangle]$. *Portanto,* $\mathrm{C} = \langle [Q] \rangle$ *é um grupo cíclico de ordem* 4.

d	D	$\lfloor\mu\rfloor$	$\lvert\mathcal{C}\rvert$
-2	-8	1	1
-5	-20	2	2
-13	-52	4	2
-14	-56	4	$4c$
-21	-84	5	$4k$
-23	-23	3	3
-26	-104	6	6
-47	-47	4	5
-71	-71	5	7

Tabela 3.1: Grupos de classe de ideais

4. Se $d = -23$*, então* $d \equiv 1 (\mathrm{mod}\, 4)$*. Logo,* $\mathbb{Z}_K = \mathbb{Z}[\eta]$ *e* $D = -23$*. Assim,*

$$\mu = \frac{2\sqrt{|D|}}{\pi} = \frac{2\sqrt{23}}{\pi} \approx 3,1$$

e $\lfloor\mu\rfloor = 3$*. O grupo de classe* C *é gerado pelos ideais primos de* $\mathbb{Z}_K$ *dividindo* $\langle 2\rangle$ *e* $\langle 3\rangle$*. Pela Proposição 3.8, p permanece primo em* $\mathbb{Z}_K$ *se, e somente se,*

$$f = x^2 - x + 6$$

é irredutível sobre $\mathbb{Z}_p$*. É fácil verificar que* f *é redutível para os primos* 2 *e* 3*. Note que,* $P\overline{P} = \langle 2\rangle$ *e* $P \neq \overline{P}$*, onde* $P = \langle 2, \eta\rangle$*. Vamos sopor que* $Q\overline{Q} = \langle 3\rangle$*. Como* $N(\eta) = 6$ *e* $N(1+\eta) = 8$ *temos que*

$$\langle\eta\rangle\langle\overline{\eta}\rangle = P\overline{P}Q\overline{Q} \;\; e \;\; \langle 1+\eta\rangle\langle\overline{1+\eta}\rangle = P^3\overline{P}^3.$$

Reordenando, se necessário, obtemos que $\langle\eta\rangle = PQ$ *e* $\langle 1+\eta\rangle = P^3$ *ou* $\overline{P}^3$*. Logo,* $[Q] = [P]^{-1}$ *e* $[P]^3 = [\langle 1\rangle]$*. Portanto,* $\mathrm{C} = \langle [P]\rangle$ *é um grupo cíclico de ordem* 3*. Na Tabela* 3.1*, apresentaremos alguns grupos de classe de ideais*

Sejam $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, onde $d < 0$. Pela Proposição 3.2, temos que $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-1}]$ é o único domínio de fatoração única, se $d \equiv 3 (\mathrm{mod}\, 4)$. Também temos o seguinte resultado:

Corolário 3.4 *Sejam* $K = \mathbb{Q}(\sqrt{d})$ *e* $\mathbb{Z}_K$ *o anel dos inteiros de* K*, onde* $d < 0$*. Se* $d \equiv 2 (\mathrm{mod}\, 4)$*, então* $\mathbb{Z}_K = \mathbb{Z}[\sqrt{-2}]$ *é o único domínio de fatoração única.*

Prova. Suponhamos que $d \equiv 2(\mathrm{mod}\, 4)$ e $d \neq -2$. Então $d \leq -6$. Como

$$\mu \leq \frac{2\sqrt{|4d|}}{\pi} = \frac{4\sqrt{|d|}}{\pi}$$

e $d \leq -6$ temos que $\lfloor \mu \rfloor \geq 2$. Logo, os geradores primos do grupo de classe divide ao menos $\langle 2 \rangle$. Pela Proposição 3.8, p permanece primo em $\mathbb{Z}_K$ se, e somente se,

$$f = x^2 - d$$

é irredutível sobre $\mathbb{Z}_p$. É fácil verificar que f é redutível para o primo 2, pois d é um número par. Portanto, o grupo de classe de ideais é não trivial. ■

Pode ser mostrado que: se $K = \mathbb{Q}(\sqrt{d})$ e $\mathbb{Z}_K$ o anel dos inteiros de K, com $d < 0$, então $\mathbb{Z}_K$ é um domínio de fatoração única se, e somente se,

$$d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

Referências Bibliográficas

[1] Cassels, J. W. S., *An Introdution to the Geometry of Number*. Springer, Berlin, 1959.

[2] Endler, O., *Teoria dos Números Agébricos*. IMPA, Rio de Janeiro, 1986.

[3] Garcia, A. L. e Lequain, Y., *Álgebra: Um Curso de Introdução*. IMPA, Rio de Janeiro, 1988.

[4] Herstein, I. N., *Tópicos de Álgebra*. Editora Polígono S. A. 1970.

[5] Michael, A., *Algebra*. New Jersey, 1991.

[6] Rotman, J. J., *Galois Theory*. Springer, New York, 1998.

[7] Stewart, Ian N. and Tall, D. O., *Algebraic Number Theory*. Chapman and Hall, 1986.

[8] Querré, J., *Cours d'Algèbre*. Masson Paris, 1976.

[9] Weiss, E., *Algebraic Number Theory*. New York, 1963.