Universidade Federal de Pernambuco

Centro de Ciências Exatas e da Natureza

Programa de Pós-Graduação em Matemática

Charlene Tereza da Silva Dias Leite

Cotas para o número de ordens cúbicas C_3 com discriminante limitado

Recife

2014

Charlene Tereza da Silva Dias Leite

Cotas para o número de ordens cúbicas C_3 com discriminante limitado

Este trabalho foi apresentado à Pós-Graduação em Matemática do Centro de Ciências Exatas e da Natureza da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre em Matemática.

Orientador: Prof. Dr. Jorge Nicolás Caro Montoya

Recife

2014

Catalogação na fonte
Bibliotecária Monick Raquel Silvestre da S. Portes, CRB4-1217

L533c Leite, Charlene Tereza da Silva Dias
Cotas para o número de ordens cúbicas C_3 com discriminante limitado / Charlene Tereza da Silva Dias Leite. – 2014.
54 f.

Orientador: Jorge Nicolás Caro Montoya.
Dissertação (Mestrado) – Universidade Federal de Pernambuco. CCEN, Matemática, Recife, 2014.
Inclui referências e apêndice.

1. Matemática. 2. Ordens cúbicas. I. Montoya, Jorge Nicolás Caro (orientador). II. Título.

510 CDD (23. ed.) UFPE- MEI 2017-217

Charlene Tereza da Silva Dias Leite

Cotas para o número de ordens cúbicas C_3 com discriminante limitado

Este trabalho foi apresentado à Pós-Graduação em Matemática do Centro de Ciências Exatas e da Natureza da Universidade Federal de Pernambuco como requisito parcial para obtenção do grau de Mestre em Matemática.

Aprovado em: 15/12/2014.

BANCA EXAMINADORA

Prof. Dr. Jorge Nicolás Caro Montoya
(Orientador)
Universidade Federal de Pernambuco

Prof. Dr. Eduardo Shirlippe Goes Leandro
(Examinador Interno)
Universidade Federal de Pernambuco

Profª. Dra. Bárbara Costa da Silva
(Examinadora Externa)
Universidade Federal Rural de Pernambuco

Ao meu amigo, meu herói, meu pai.

AGRADECIMENTOS

Ao Grande Matemático, que originou esses intrigantes conceitos, nosso Criador, Jeová Deus, por ter me dado a vida, discernimento e sabedoria.

Ao meu orientador, Professor Jorge Nicolás Caro Montoya, por ter tido a coragem de continuar um trabalho que não faz parte de sua linha de pesquisa, por ter gastado tantas horas a me orientar e por ter sido tão paciente ao lidar com minhas limitações matemáticas. Agradeço todos os "puxões de orelha".

Ao Professor Antonio Carlos Rodrigues Monteiro, por ter se iniciado a minha orientação nesse trabalho. Obrigado por tanto conhecimento a mim transmitido.

Ao meu amado marido Daniel, por sempre ser tão companheiro e compreensivo, por me receber de braços abertos a cada meu retorno à casa, por aguentar o meu mau humor quando nada parecia dar certo.

Ao meu pai, por acreditar que eu conseguiria, mesmo que eu não tivesse a mesma certeza. Por ter sido um maravilhoso motorista em tantos trajetos à rodoviária.

À minha amada mãe, por ter sido tão hospitaleira e cuidadosa. Por ter se dedicado tanto a mim, em todos esses anos.

A meus irmãos, por serem parceiros tão presentes na minha vida.

A todos os colegas do DMat que de alguma forma contribuíram com minha formação. Aos parceiros de sala, àqueles com quem cursei disciplinas, aos que estudei junto, aos que me deram carona e aos colegas de cafezinho, meus sinceros agradecimentos. Não citarei nomes para não correr o risco de esquecer alguém.

Aos professores que contribuíram com a minha formação.

Agradeço ao Professor William Charles Jagy, do fórum *Math Stack Exchange*, por responder as minhas perguntas no forúm e me "salvar" algumas vezes.

Agradeço ao Professor Manjul Bhargava por responder os meus e-mails carregados de dúvidas.

Meus agradecimentos a minha chefia no IF-Sertão, Campus Salgueiro, por me dar a flexibilidade necessária no trabalho para eu pudesse estar semanalmente em Recife.

Às amigas Giselle, Lillyane, Xênia e Priscila, por entenderem que mesmo eu estando perto, estava longe, que apesar de muito ausente, eu continuo as amando.

Como dois e dois são quatro
sei que a vida vale a pena
embora o pão seja caro
e a liberdade pequena
Como teus olhos são claros
e a tua pele, morena
como é azul o oceano
e a lagoa, serena
como um tempo de alegria
por trás do terror me acena
e a noite carrega o dia
no seu colo de açucena
sei que dois e dois são quatro
sei que a vida vale a pena
mesmo que o pão seja caro
e a liberdade, pequena.
(Ferreira Gullar)

RESUMO

O objetivo principal deste trabalho é demonstrar a veracidade da versão moderna da fórmula para contagem de ordens cúbicas com grupo de automorfismo cíclico de ordem 3 e discriminante limitado (apresentada por Manjul Bhargava), tendo como base a fórmula clássica de Harold Davenport. Para isso, são introduzidas algumas noções básicas da teoria algébrica dos números (discriminante, reticulados, norma de ideais, homomorfismo de Minkowski). Ainda, são apresentadas as noções de hessiana e *shape*, a fim de demonstrar a correspondência de Delone-Faddeev para relacionar anéis cúbicos com formas binárias cúbicas. Por fim, apresentamos a noção de forma binária quadrática reduzida, e a estudamos no caso particular da hessiana de uma forma binária cúbica munida de um automorfismo de ordem 3. Este estudo é aplicado na contagem assintótica das ordens cúbicas com grupo de automorfismo cíclico de ordem 3. No Apêndice é apresentado o trabalho computacional a fim de detalhar o isomorfismo (nada óbvio) entre anéis cúbicos e formas binárias cúbicas.

Palavras-chave: Ordens cúbicas. Discriminante. Correspondência de Delone-Faddeev. Formas cúbicas binárias.

ABSTRACT

The main purpose of this work is to demonstrate the veracity of the modern version of the formula for counting cubic orders with automorphism group cyclic of order 3 and bounded discriminant (after Manjul Bhargava), having as basis the classic formula from Harold Davenport. For this purpose are introduced some basic notions from algebraic number theory (discriminant, lattices, norm of ideals, Minkowski homomorphism). Moreover, the notions of Hessian and shape are introduced, in order to demonstrate the Delone-Faddeev correspondence, in order to relate cubic rings with cubic binary forms. Finally, we introduce the notion of reduced binary quadratic form, which is studied in the particular case of the Hessian of a binary cubic form endowed with an automorphism of order 3. This study is applied to the asymptotic counting of the cubic orders with automorphism group cyclic of order 3. On the Appendix we include all the computational work in order to detail the (not obvious at all) isomorphism between cubic rings and cubic binary forms.

Keywords: Cubic orders. Discriminant. Delone-Faddeev correspondence. Cubic binary forms.

SUMÁRIO

1 NOÇÕES PRELIMINARES

1.1 Introdução

Os primeiros resultados sobre formas binárias cúbicas com coeficientes inteiros, análogos aos resultados sobre formas quadráticas, foram demonstrados por Ferdinand Eisenstein por volta de 1844 (DICKSON, 1966). Segundo ele, considerando-se a forma cúbica

$$f(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$$

com a, b, c e d inteiros, definimos o *discriminante* de f por

$$D = B^2 - 4AC,$$

onde

$$A = b^2 - ac, B = bc - ad, C = c^2 - bd\,.$$

A forma quadrática $H_f(x, y) = Ax^2 + Bxy + Cy^2$ é a *hessiana* de f.

Algumas décadas depois, Arthur Cayley buscou melhorar a teoria de Eisenstein, simplificando e estendendo para qualquer discriminante negativo.

Por volta de 1852, Ernst Arndt, contemporâneo de Cayley, já acreditava que o número de corpos cúbicos com um discriminante dado é finito. Em 1858 ele já havia tabelado as formas cúbicas binárias reduzidas f e seus corpos para discriminantes negativos $-D$, com $D \leq 2000$. (A forma f é dita *reduzida* se $|B| \leq \frac{1}{2}|A|$ e $|C| \geq |A|$.) Esta tabela foi remodelada por Cayley, em 1871.

No século 20 houve grandes contribuições. A correspondência de Delone-Faddeev (GAN; GROSS; SAVIN, 2002) mostra uma forma de relacionar as formas binárias cúbicas com anéis cúbicos (vide o Teorema 2.4). Por outro lado, no início do século passado, os estudos de Harold Davenport e Hans Heilbronn (DAVENPORT, 1951a) forneceram uma fórmula assintótica para o número de corpos cúbicos com discriminante limitado.

Teorema 1.1 (Davenport-Heilbronn (DAVENPORT, 1951b))**.** *Seja $N_3(\xi, \eta)$ o número de corpos cúbicos K, a menos de isomorfismos, satisfazendo $\xi < \mathrm{Disc}(K) < \eta$ (sendo $\mathrm{Disc}(K)$ o discriminante do corpo K, e ζ a função Zeta de Riemann). Então*

$$N_3(0, X) = \frac{1}{12\zeta(3)}\, X + o(X);$$
$$N_3(-X, 0) = \frac{1}{4\zeta(3)}\, X + o(X)^{\S}\,.$$

§ Se $g(x)$ é uma função não nula, dizemos que $f(x) = o\big(g(x)\big)$ quando $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$.

Subsequente a este resultado, surgiu um grande interesse em verificar numericamente o teorema de Davenport-Heilbronn. Foram calculados discriminantes tão grandes quanto 10^7 e notou-se que os valores obtidos não se harmonizavam com o teorema. Isto levou a perguntas sobre o termo do erro e como determinar precisamente a ordem de um segundo termo de erro.

Em 1997, Karim Belabas procurou desenvolver um método para enumerar os corpos cúbicos, o que lhe permitiu fazer tabelas de corpos cúbicos até o discriminante absoluto 10^{11}. Como esses cálculos não concordavam muito com o teorema de Davenport-Heilbronn, Belabas passou a imaginar a existência de um termo de erro menor que $O\big(X(\log X)^a\big)$ para qualquer a. No entanto, Belabas só conseguiu obter um termo do erro exponencial da forma $O\Big(X\exp\big(-\sqrt{\log X\log(\log X)}\big)\Big)$ [†].

Em 2000, David Roberts realizou um notável estudo destes últimos cálculos em conjunto com certas considerações teóricas, o que levou à conjectura de um segundo termo de erro no teorema de Davenport-Heilbronn. Os cálculos posteriores realizados nos últimos anos têm mostrado que a conjectura de Roberts concorda bem com os dados.

Na atualidade, Manjul Bhargava vem realizando pesquisas relacionadas à teoria do discriminante. Em 2010 ele apresentou uma nova abordagem para provar o teorema de Davenport-Heilbronn original. Segundo ele (BHARGAVA; SHANKAR; TSIMERMAN, 2013),

Teorema 1.2. *Seja $N(\xi,\eta)$ o número de corpos $GL_2(\mathbb{Z})$-equivalentes de formas binárias cúbicas f, com coeficientes inteiros, satisfazendo $\xi < \mathrm{Disc}(f) < \eta$, e seja Γ a função gama. Então para todo $\epsilon > 0$ valem*

$$N(0,X) = \frac{\pi^2}{72}X + \frac{\sqrt{3}\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{15\Gamma(2/3)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon});$$
$$N(-X,0) = \frac{\pi^2}{24}X + \frac{\zeta(2/3)\Gamma(1/3)(2\pi)^{1/3}}{5\Gamma(2/3)}X^{5/6} + O_\epsilon(X^{3/4+\epsilon}).$$

O objetivo do nosso trabalho é demonstrar uma versão do teorema de Davenport para o caso particular de ordens cúbicas, levando em conta todos os refinamentos no decorrer dos anos e tendo como base o que foi produzido nestes quase dois séculos de pesquisa. Especificamente, mostraremos neste trabalho o seguinte resultado:

Teorema 1.3 ((BHARGAVA; SHNIDMAN, 2014), Theorem 1)**.** *O número de ordens cúbicas com grupo de automorfismo cíclico de ordem 3, e discriminante menor que X, é dado por*

$$\frac{\pi}{6\sqrt{3}}X^{1/2} + O(X^{1/4}).$$

[†] Dizemos que $f(x) = O\big(g(x)\big)$ se, e somente se, existe um número real positivo M e um número real x_0 tal que $|f(x)| \leq M|g(x)|$ para todo $x \geq x_0$.

Para chegarmos ao nosso objetivo, neste Capítulo 1 apresentamos noções preliminares da teoria algébrica dos números, a saber: norma, traço, discriminante e reticulado. Além disso, usamos a noção de prolongamento canônico para mostrar que o grupo de classes de ideais é finito.

No Capítulo 2, usamos a correspondência de Delone-Faddeev para relacionar anéis cúbicos com formas binárias cúbicas. Ainda, obtemos uma relação entre hessianas e *shapes*, que nos ajuda no cálculo do discriminante do anel cúbico associado a tais objetos.

No Capítulo 3, trabalhamos com formas binárias quadráticas reduzidas para demonstrar que a hessiana de uma forma binária cúbica com automorfismo de ordem 3 é equivalente a um múltiplo inteiro da forma binária quadrática $Q(x, y) = x^2 + xy + y^2$. Esse conceito é fundamental para facilitar os cálculos na contagem das ordens cúbicas, e finalmente demonstrar o teorema principal em estudo.

1.2 Generalidades

Neste capítulo apresentaremos alguns conceitos básicos de estruturas algébricas e reticulados necessários para o desenvolvimento deste trabalho. Para os casos omissos, vide (SAMUEL, 1970). Todos os anéis citados neste trabalho são anéis comutativos e com unidade.

Definição 1.4. Chamaremos de *corpo de números* toda extensão de grau finita (e consequentemente algébrica) de $\mathbb{Q}$.

Sejam A e B anéis tais que B é um A-módulo de posto n. Então, existem $b_1, \ldots, b_n \in B$ tais que $B = Ab_1 \oplus \cdots \oplus Ab_n$. O conjunto $\mathcal{B} = \{b_1, \ldots, b_n\}$ é dito uma *A-base* de B. A ordem dos elementos de uma A-base é importante; no entanto, às vezes utilizaremos a notação de conjuntos ao invés da notação de tuplas.

Dado $\mathfrak{b} \in B$, a aplicação $M_\mathfrak{b} : B \longrightarrow B$ dada por $M_\mathfrak{b}(x) = x \cdot \mathfrak{b}$, é A-linear. A matriz associada a $M_\mathfrak{b}$ segundo $\mathcal{B}$ é a matriz $[M_\mathfrak{b}] = (\alpha_{ij})_{i,j=1}^n$, onde $M_\mathfrak{b}(b_j) = \sum_{i=1}^n \alpha_{ij} b_i$ para $j = 1, \ldots, n$. Sabe-se que o traço $\mathrm{Tr}[M_\mathfrak{b}]$ e o determinante $\det[M_\mathfrak{b}]$ da matriz $[M_\mathfrak{b}]$ independem da escolha de $\mathcal{B}$.

Definição 1.5. Com as notações anteriores, definimos o *traço* e a *norma* de $\mathfrak{b}$ na extensão B/A por

$$N_{B/A}(\mathfrak{b}) = \det[M_\mathfrak{b}]\,;\ \mathrm{Tr}_{B/A}(\mathfrak{b}) = \mathrm{Tr}\,[M_\mathfrak{b}]\ .$$

Exemplo 1.6. Considere o elemento $\mathfrak{b} = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ da extensão $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$. Como

$\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ é uma $\mathbb{Q}$-base, temos

$$\begin{aligned}
\mathfrak{b} \cdot 1 &= a + b\sqrt[3]{2} + c\sqrt[3]{4}\,; \\
\mathfrak{b} \cdot \sqrt[3]{2} &= 2c + a\sqrt[3]{2} + b\sqrt[3]{4}\,; \\
\mathfrak{b} \cdot \sqrt[3]{4} &= 2b + 2c\sqrt[3]{2} + a\sqrt[3]{4}\,,
\end{aligned}$$

e assim

$$[M_{\mathfrak{b}}] = \begin{bmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{bmatrix}.$$

Portanto teremos

$$N_{\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}}(\mathfrak{b}) = \det[M_x] = a^3 + 2b^3 + 4c^3 - 6abc\,;\ \mathrm{Tr}_{\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}}(\mathfrak{b}) = \mathrm{Tr}\,[M_x] = 3a\,.$$

O *polinômio característico* de $\mathfrak{b} \in B$ é o polinômio mônico, de grau n com coeficientes em A dado por $p_{\mathfrak{b}}(x) = \det\big(xI - [M_{\mathfrak{b}}]\big)$. É fácil mostrar que $p_{\mathfrak{b}}$ independe de $[M_{\mathfrak{b}}]$ e que o coeficiente de x^{n-1} é $-\mathrm{Tr}[M_{\mathfrak{b}}] = -\mathrm{Tr}_{B/A}(\mathfrak{b})$ e o coeficiente constante será $(-1)^n \det[M_{\mathfrak{b}}]$. Vale ainda o teorema de Cayley-Hamilton: $p_{\mathfrak{b}}(\mathfrak{b}) = 0$; vide (ATIYAH; MACDONALD, 1969, Proposition 2.4).

Exemplo 1.7. Sejam $L = \mathbb{Q}[\sqrt[3]{2}]$ e $\mathfrak{b} = 1 - \sqrt[3]{2} \in \mathbb{Q}[\sqrt[3]{2}]$. O polinômio característico de $\mathfrak{b}$ sobre K é $p_{\mathfrak{b}} = x^3 - 3x^2 + 3x + 1$. Logo, $\mathrm{Tr}_{\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}}(\mathfrak{b}) = 3$ e $N_{\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}}(\mathfrak{b}) = -1$.

Seja L/K uma extensão de corpos e $\mathfrak{b} \in L/K$. O polinômio mínimo de $\mathfrak{b}$ sobre K, denotado por $m_{\mathfrak{b}}(x)$, é o polinômio mônico com coeficientes em K de menor grau que possui $\mathfrak{b}$ como raiz. No caso em que $L = K[\mathfrak{b}]$, então vale $p_{\mathfrak{b}}(x) = m_{\mathfrak{b}}(x)$, pois, pelo teorema de Cayley-Hamilton, vale $p_{\mathfrak{b}}(\mathfrak{b}) = 0$ e $\deg p_{\mathfrak{b}}(x) = [K[\mathfrak{b}] : K] = \deg m_{\mathfrak{b}}(x)$.

Teorema 1.8. *Seja L/K uma extensão de corpos de grau n. Seja $\mathfrak{b} \in L$. Então $p_{\mathfrak{b}}(x) = m_{\mathfrak{b}}(x)^{[L:K[\mathfrak{b}]]}$, onde $m_{\mathfrak{b}}(x)$ é o polinômio mínimo de $\mathfrak{b}$.*

Demonstração. Seja $C = \{\alpha_1, \ldots, \alpha_r\}$ uma base de $K[\mathfrak{b}]$ sobre K e $\{\beta_1, \ldots, \beta_m\}$ uma base de L sobre $K[\mathfrak{b}]$. É fácil verificar que $\{\alpha_1\beta_1, \ldots, \alpha_1\beta_m, \alpha_2\beta_1, \ldots, \alpha_r\beta_m\}$ é uma base de L sobre K.

Seja $M_{\mathfrak{b}} = (a_{ij})$ a matriz da multiplicação por $\mathfrak{b}$ em $K[\mathfrak{b}]$ em relação à base C. Então $\mathfrak{b} \cdot \alpha_j = \sum_{j=1}^{r} a_{ij}\alpha_j$, e assim

$$\mathfrak{b} \cdot (\alpha_j\beta_i) = \left(\sum_{j=1}^{r} a_{ij}\alpha_j\right)\beta_i = \sum_{j=1}^{r} a_{ij}\,(\alpha_j\beta_i)\,.$$

Escrevendo o elemento acima na base C de L em K concluímos que

$$\mathfrak{b}\cdot(\alpha_j\beta_i) = 0\cdot\alpha_1\beta_1 + \cdots + 0\cdot\alpha_r\beta_1 + \cdots + a_{i1}\alpha_1\beta_j + \cdots + a_{rj}\alpha_r\beta_j + \cdots + 0\cdot\alpha_1\beta_m + \cdots + 0\cdot\alpha_r\beta_m\,.$$

Portanto, na base C de L sobre K a matriz $M_{\mathfrak{b}}^*$ da multiplicação por $\mathfrak{b}$ é da forma

$$M_{\mathfrak{b}}^* = \begin{bmatrix} M_{\mathfrak{b}} & & 0 \\ & \ddots & \\ 0 & & M_{\mathfrak{b}} \end{bmatrix},$$

ou seja, $M_{\mathfrak{b}}$ se repete m vezes na diagonal principal como blocos diagonais na matriz $M_{\mathfrak{b}}^*$, e assim

$$xI_q - M_{\mathfrak{b}}^* = \begin{bmatrix} xI_r - M_{\mathfrak{b}} & & 0 \\ & \ddots & \\ 0 & & xI_r - M_{\mathfrak{b}} \end{bmatrix};$$

em particular $\det\left(xI_q - M_{\mathfrak{b}}^*\right) = \det\left(xI_r - M_{\mathfrak{b}}\right)^m$. Como $\det\left(xI_q - M_{\mathfrak{b}}^*\right)$ é o polinômio característico de $\mathfrak{b}$ sobre K e $\det\left(xI_r - M_{\mathfrak{b}}\right)$ é o polinômio mínimo de $\mathfrak{b}$ sobre K, segue que $p_{\mathfrak{b}}(x) = m_{\mathfrak{b}}(x)^{[L:K[\mathfrak{b}]]}$. □

Definição 1.9. Um *anel cúbico* é um $\mathbb{Z}$-módulo livre de posto 3. Se adicionalmente for um domínio, o anel será chamado de *ordem cúbica*.

Definição 1.10. Sejam A e B anéis com $A \subseteq B$. Um elemento $b \in B$ é dito *A-inteiro* se b é raiz de um polinômio **mônico** com coeficientes em A. O conjunto dos elementos A-inteiros em B forma uma subanel de B contendo A. Esse anel é denotado por $O_B(A)$ e é chamado de *anel dos inteiros* de A em B.

Se $O_B(A) = B$, dizemos que B é *A-inteiro*. Se $O_B(A) = A$, dizemos que A é *integralmente fechado* em B. Se A é domínio, dizemos que A é *integralmente fechado* se o for no seu corpo de frações. (por exemplo, se A for fatorial então A é integralmente fechado; vide (RIBENBOIM, 1972, pp. 71,72).)

Definição 1.11. Se K é um corpo de números, denotaremos o anel de inteiros $O_K(\mathbb{Z})$ de K sobre $\mathbb{Z}$ por O_K, e o chamaremos de *anel dos inteiros de K*.

Definição 1.12. Seja A um anel e $K \subseteq A$ um corpo. Dizemos que um elemento $a \in A$ é *K-algébrico* se a é raiz de um polinômio não constante com coeficientes em K.

Proposição 1.13. *Sejam A um domínio com corpo de frações K e L uma extensão finita de K. Se $\alpha \in O_L(A)$, então os coeficientes do polinômio característico $p_\alpha(x)$ são inteiros sobre A. Em particular, $\mathrm{Tr}_{L/K}$ e $N_{L/K}$ são A-inteiros.*

Demonstração. Se $m_\alpha(x) \in O_L(A)$, então teremos os coeficientes de $p_\alpha(x)$ em $O_L(A)$, pois pelo teorema 1.8 $p_\alpha(x)$ é potência de $m_\alpha(x)$. Mostraremos que esse é o caso.

Sejam $x_1, \ldots, x_n$ as raízes de $m_\alpha(x)$ (com multiplicidade). Como os coeficientes de $m_\alpha(x)$ são, a menos de sinal, somas de produtos dos elementos x_i, basta mostrar que

tais x_i são inteiros sobre A, já que a soma, diferença e produto de inteiros sobre A são inteiros sobre A.

Recorrendo à teoria de Galois, temos que cada x_i é um conjugado de α sobre K, e assim, existe um K-isomorfismo $\varphi_i : K[\alpha] \to K[x_i]$ tal que $\varphi_i(\alpha) = x_i$, para todo $i = 1, \ldots, n$. Como α é inteiro sobre A, segue que $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$, onde $a_i \in A$ e $a_i \neq 0$ para algum i. Aplicando a φ_i, obtemos

$$\varphi_i(\alpha)^n + a_{n-1}\varphi_i(\alpha)^{n-1} + \ldots + a_0 = 0\,,$$

e assim

$$x_i^n + a_{n-1}x_i^{n-1} + \ldots + a_0 = 0\,.$$

Portanto x_i é inteiro sobre A, para qualquer $i = 1, \ldots, n$ e, consequentemente, os coeficientes de $m_\alpha(x)$ são inteiros sobre A. □

Corolário 1.14. *Seja A um domínio. Então os coeficientes do polinômio característico $p_\alpha(x)$ são elementos de A. Em particular, $\mathrm{Tr}_{L/K}$ e $N_{L/K}$ são elementos de A.*

Demonstração. Na Proposição anterior vimos que os coeficientes do polinômio característico $p_\alpha(x)$ são elementos de K e são inteiros sobre A. Logo, os coeficientes de $p_\alpha(x)$ pertencem a A, pois A é integralmente fechado. E, consequentemente, $\mathrm{Tr}_{L/K}$ e $N_{L/K}$ são elementos de A. □

1.3 Discriminante

Nesta seção, apresentaremos os conceitos básicos de discriminante e resultados de homomorfismos de grupos que ajudam no cálculo do discriminante numa extensão de corpos.

Definição 1.15. Seja B um anel e A um subanel de B tal que B seja A-módulo livre de posto finito n. Para cada $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in B^n$ definimos o *discriminante* de $\mathbf{x}$ como o elemento de A dado por

$$\mathcal{D}(\mathbf{x}) = \det\big(\mathrm{Tr}_{B/A}(x_i x_j)\big)_{1\leq i,j\leq n}\,.$$

Se $\{x_1, x_2, \ldots, x_n\}$ é uma $\mathbb{Z}$-base do anel de inteiros $\mathcal{O}_K$, dizemos que o discriminante $\mathcal{D}(x_1, x_2, \ldots, x_n)$ é o *discriminante absoluto* do corpo de números K, e o denotamos por $\mathcal{D}_K$.

Exemplo 1.16. Seja $K = \mathbb{Q}[\sqrt[3]{2}]$. Então

$$\begin{aligned}\mathcal{D}(1,\sqrt[3]{2},\sqrt[3]{4}) &= \det\begin{bmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(1\cdot 1) & \mathrm{Tr}_{K/\mathbb{Q}}(1\cdot\sqrt[3]{2}) & \mathrm{Tr}_{K/\mathbb{Q}}(1\cdot\sqrt[3]{4}) \\ \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{2}\cdot 1) & \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{2}\cdot\sqrt[3]{2}) & \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{2}\cdot\sqrt[3]{4}) \\ \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{4}\cdot 1) & \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{4}\cdot\sqrt[3]{2}) & \mathrm{Tr}_{K/\mathbb{Q}}(\sqrt[3]{4}\cdot\sqrt[3]{4}) \end{bmatrix} \\ &= \det\begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{bmatrix} \\ &= -108\,.\end{aligned}$$

Lema 1.17 (Lema de Dedekind)**.** *Sejam G um grupo, K um corpo e $\sigma_1,\dots,\sigma_n$ homomorfismos distintos de G sobre o grupo multiplicativo de K^*. Então $\{\sigma_1,\dots,\sigma_n\}$ é um conjunto K-linearmente independente.*

Demonstração. Suponha, por absurdo, que os elementos σ_i são K-linearmente dependentes, ou seja, existem $a_1,\dots,a_n \in K$, não todos nulos, tal que $\sum_{i=1}^{n} a_i\sigma_i = 0$.

Seja r o menor número possível de tais $a_i \neq 0$. Obviamente, $r \geq 2$, pois cada $\sigma_i \neq 0$. Reordenando os índices i, podemos supor que vale

$$a_1\sigma_1(g) + a_2\sigma_2(g) + \cdots + a_r\sigma_r(g) = 0\,, \tag{1.1}$$

com $a_i \neq 0$ para todos $i = 1,\dots,r$ e $g \in G$. Assim, tomando $g,h \in G$ e aplicando a igualdade 1.1 ao elemento $gh \in G$, temos

$$a_1\sigma_1(gh) + a_2\sigma_2(gh) + \cdots + a_r\sigma_r(gh) = 0, \tag{1.2}$$

ou seja,

$$a_1\sigma_1(g)\sigma_1(h) + a_2\sigma_2(g)\sigma_2(h) + \cdots + a_r\sigma_r(g)\sigma_r(h) = 0\,. \tag{1.3}$$

Subtraindo a igualdade 1.3 com o produto de $\sigma_1(h)$ pela igualdade 1.1 obtemos

$$a_2\sigma_2(g)\big(\sigma_2(h)-\sigma_1(h)\big) + \cdots + a_r\sigma_r(g)\big(\sigma_r(h)-\sigma_1(h)\big) = 0. \tag{1.4}$$

Como a igualdade 1.4 é válida para todo g e r é mínimo, segue que para algum $i = 2,\dots,r$ vale $a_i\sigma_i(g)\big(\sigma_i(h)-\sigma_1(h)\big) = 0$; mas $a_i \neq 0$, e portanto $\sigma_i(h) = \sigma_1(h)$, contrariando a hipótese que os σ_i são distintos. □

Teorema 1.18. *Sejam L/K uma extensão de corpos de grau n (com K finito ou de característica 0) e $\sigma_1,\dots,\sigma_n$ os K-isomorfismos distintos de L em um corpo algebricamente fechado contendo K. Se $\mathbf{x} = (x_1,\dots,x_n)$ é uma base de L sobre K, temos*

$$\mathcal{D}(\mathbf{x}) = \det\big(\sigma_j(x_j)\big)^2 \neq 0\,.$$

Demonstração. Por definição, $\mathcal{D}(\mathbf{x}) = \det\big(\mathrm{Tr}_{L/K}(x_i x_j)\big)$. Como o traço de $x_i x_j$ é a soma das raízes do seu polinômio mínimo, segue que

$$\mathcal{D}(\mathbf{x}) = \det\big(\mathrm{Tr}_{L/K}(x_i x_j)\big) = \det\left(\sum_{k=1}^{n} \sigma_k(x_i x_j)\right).$$

Mas

$$\begin{bmatrix} \sigma_1(x_1) & \sigma_2(x_1) & \cdots & \sigma_n(x_1) \\ \sigma_1(x_2) & \sigma_2(x_2) & \cdots & \sigma_n(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(x_n) & \sigma_2(x_n) & \cdots & \sigma_n(x_n) \end{bmatrix} \cdot \begin{bmatrix} \sigma_1(x_1) & \sigma_2(x_1) & \cdots & \sigma_n(x_1) \\ \sigma_1(x_2) & \sigma_2(x_2) & \cdots & \sigma_n(x_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(x_n) & \sigma_2(x_n) & \cdots & \sigma_n(x_n) \end{bmatrix}^t = \left(\sum_{k=1}^{n} \sigma_k(x_i x_j)\right),$$

e portanto $\det\Big(\sum_{k=1}^{n} \sigma_k(x_i x_j)\Big) = \det\big(\sigma_i(x_j)\big)^2$, logo $\mathcal{D}(\mathbf{x}) = \det\big(\sigma_i(x_j)\big)^2$.

Agora suponha que $\det(\sigma_i(x_j)) = 0$. Então existem $a_1, \ldots, a_n \in K$ não todos nulos, tais que $\sum_{i=1}^{n} a_i \sigma_i(x_j) = 0$ para $j = 1, \ldots, n$. Pela linearidade concluímos que $\sum_{i=1}^{n} a_i \sigma_i(x) = 0$, para todo $x \in L$, o que é um absurdo, pois pelo lema 1.17 os σ_i são K-linearmente independentes. □

Observação 1.19. Com as condições do Teorema 1.18, a relação $\mathcal{D}(x_1, \ldots, x_n) \neq 0$ exprime que a forma binária $(x, y) \mapsto \mathrm{Tr}(xy)$ é não degenerada, ou seja, se $\mathrm{Tr}(xy) = 0$ para todo $x \in L$ implica $y = 0$. Assim, $s_x : y \mapsto \mathrm{Tr}(xy)$ é uma aplicação injetiva K-linear de L sobre o dual $\mathrm{Hom}_K(L, K)$ (pela estrutura de espaço vetorial sobre K). Como $\dim_K L = \dim_K \mathrm{Hom}_K(L, K) = n$, segue que $x \mapsto s_x$ é uma bijeção. A existência de *bases duais* sobre um espaço vetorial garante que, que para toda base $(x_1, \ldots, x_n)$ de L/K, existe outra base $(y_1, \ldots, y_n)$ tal que

$$\mathrm{Tr}(x_i y_j) = \delta_{ij}, \text{ para todos } 1 \leq i, j \leq n\,. \tag{1.5}$$

Teorema 1.20. *Seja A um anel integralmente fechado, K seu corpo de frações, L/K uma extensão finita de grau n e $\mathcal{O}_L(A)$ o anel dos A-inteiros de L. Suponha que K tem característica 0. Então $\mathcal{O}_L(A)$ é um A-submódulo de um A-módulo livre de posto n. Se $A = \mathbb{Z}$ (e, consequentemente, $K = \mathbb{Q}$), então $\mathcal{O}_L(A) = \mathcal{O}_L$ será um $\mathbb{Z}$-módulo livre de posto igual a n.*

Demonstração. Seja $(x_1, \ldots, x_n)$ uma K-base de L. Para cada x_i, temos que os elementos x_i^r, $0 \leq r \leq n$ são K-linearmente dependentes, pois o grau da extensão é n. Logo existem $a_0, \ldots, a_j \in K$, $1 \leq j \leq n$ e $a_j \neq 0$, tais que

$$a_j x_i^j + a_{j-1} x_i^{j-1} + \cdots + a_1 x_i + a_0 = 0\,. \tag{1.6}$$

Dividindo a igualdade 1.6 por a_j, podemos supor $a_j = 1$ Como cada coeficiente a_k é um quociente de elementos em A, podemos tomar $b_i \in A$, $b_i \neq 0$, um denominador comum de $a_0, \ldots, a_{j-1}$. Agora, multiplicando a equação 1.6 por b_i^j obtemos

$$(b_i x_i)^j + a_{j-1} b_i (b_i x_i)^{j-1} + a_{j-2} b_i^2 (b_i x_i)^{j-2} + \cdots + a_0 b_i^j = 0\,,$$

logo cada $b_i x_i$ é A-inteiro. Como $b \in A - \{0\} \subseteq K^*$, então $(b_1 x_1, \ldots, b_n x_n)$ continua sendo uma K-base de L, contida em $\mathcal{O}_L(A)$. Pela observação 1.19 existe uma outra K-base $(y_1, \ldots, y_n)$ tal que $\mathrm{Tr}(x_i' y_j) = \delta_{ij}$, onde $x_i' = b_i x_i$. Assim, cada elemento $z \in \mathcal{O}_L(A)$ pode ser escrito como $z = \sum_{i=1}^{n} b_j y_j$, com $b_j \in A$. Mas para cada i vale $x_i' z \in \mathcal{O}_L(A)$ (pois $x_i' \in \mathcal{O}_L(A)$), onde $\mathrm{Tr}(x_i z) \in A$ (vide Proposição 1.13). Assim,

$$\mathrm{Tr}(x_i' z) = \mathrm{Tr}\left(\sum_{j=1}^{n} b_j x_i' y_j\right) = \sum_{j=1}^{n} b_j \,\mathrm{Tr}(x_i' y_j) = \sum_{j=1}^{n} b_j \delta_{ij} = b_i.$$

Portanto $b_i \in A$ para todo i, o que mostra que $\mathcal{O}_L(A)$ está contido no A-módulo livre $\sum_{j=1}^{n} A y_j$.

Se $A = \mathbb{Z}$, teremos

$$\sum_{i=1}^{n} \mathbb{Z} b_i x_i \subseteq \mathcal{O}_L \subseteq \sum_{i=j}^{n} \mathbb{Z} y_j \,,$$

e portanto

$$n = \text{posto de } \sum_{i=1}^{n} \mathbb{Z} b_i x_i \leq \text{posto de } \mathcal{O}_L \leq \text{posto de } \sum_{i=j}^{n} \mathbb{Z} y_j \leq n \,. \qquad \square$$

1.4 Reticulados

Nesta seção definiremos subgrupo discreto, reticulado e região fundamental de um reticulado. Além disso apresentaremos resultados importantes para o cálculo do volume de um reticulado.

Definição 1.21. Um subgrupo aditivo H de $\mathbb{R}^n$ é dito *discreto* se, para todo compacto $K \subseteq \mathbb{R}^n$, a intersecção $H \cap K$ é finita.

Exemplo 1.22. $\mathbb{Z}^n$ é um subgrupo discreto de $\mathbb{R}^n$.

Dado $x \in \mathbb{R}$, definimos a sua *parte inteira*, denotada por $\lfloor x \rfloor$, como o maior número inteiro menor ou igual a x.

Teorema 1.23. *Seja F um grupo abeliano livre de posto finito $n \in \mathbb{Z}^+$ e seja G um subgrupo de não nulo de F. Então existe uma $\mathbb{Z}$-base $\{x_1, \ldots, x_n\}$ de F, com $1 \leq r \leq n$ e inteiros positivos $d_1 \mid d_2 \mid \cdots \mid d_r$, tais que $\{d_1 x_1, \ldots, d_r x_r\}$ é uma $\mathbb{Z}$-base de G. Em particular, G é livre de posto $\leq n$.*

Demonstração. Usaremos indução em n. Para $n = 1$, tome $x_1 \in F$ e considere o isomorfismo $\varphi : \mathbb{Z} \longrightarrow F$ tal que $\varphi(1) = x_1$. Como todos os subgrupos de $\mathbb{Z}$ são da forma $d\mathbb{Z}$, com $d \in \mathbb{Z}^+$, temos que $G = \varphi^{-1}(d\mathbb{Z})$, ou seja, $G = \langle dx_1 \rangle$.

Agora suponha que a hipótese do teorema vale para todo grupo abeliano livre com posto $< n$. Seja F um grupo abeliano livre de posto n, com base $\{x_1, \ldots, x_n\}$, e seja $G < F$, $G \neq 0$. Considere o conjunto

$$S = \{s \in \mathbb{Z} : \text{existe uma } \mathbb{Z}\text{-base } \{y_1, \ldots, y_n\} \text{ de } F \\ \text{e existem } k_2, \ldots, k_n \in \mathbb{Z}, \text{ tais que } s y_1 + k_2 y_2 + \cdots + k_n y_n \in G\} .$$

Dados $\{y_1, \ldots, y_n\}$ e os k_i como na definição acima, então $k_2, \ldots, k_n$ também pertencem ao conjunto S, pois se $j > 1$, então $\{y_j, y_1, y_2, \ldots, \widehat{y_j}, \ldots, y_n\}$ é uma $\mathbb{Z}$-base, e teremos $k_j y_j + s y_1 + k_2 y_2 + \cdots + \widehat{k_j y_j} + \cdots + k_n y_n \in G$.

Seja $g \in G \setminus 0$. Então $g \in F$, logo $g = \alpha_1 z_1 + \cdots + \alpha_n z_n$, onde $\{z_1, \ldots, z_n\}$ é base de F, e algum $\alpha_i \neq 0$. Como $\alpha_i \in S$, segue que S contem inteiro não nulo. Obviamente, S é fechado para múltiplos inteiros.

Seja d_1 o menor elemento de $S \cap \mathbb{Z}^+ \neq \emptyset$, e sejam $\{y_1, \ldots, y_n\}$ e $k_2, \ldots k_n \in \mathbb{Z}$ tais que $v := d_1 y_1 + k_2 y_2 + \cdots + k_n y_n \in G$. Pelo princípio de Euclides, $k_i = q_i d_1 + r_i$, com $0 \leq r_i < d_1$, logo $v = d_1(y_1 + q_2 y_2 + \cdots + q_n y_n) + r_2 y_2 + \cdots + r_n y_n \in G$. Seja $x_1 = y_1 + q_2 y_2 + \cdots + q_n y_n$.

Note que $\{x_1, y_2, \ldots, y_n\}$ é $\mathbb{Z}$-base de F (basta observar que a nova base foi construída por operações elementares). Como $v \in G$, segue que $d_1, r_2, \ldots, r_n \in S$. Pela minimalidade de d_1 obtemos $r_2 = \cdots = r_n = 0$. Assim, $d_1 x_1 = v \in G$.

Seja $H = \mathbb{Z}y_2 + \cdots + \mathbb{Z}y_n$. Então H tem posto $n - 1$ e temos $F = \mathbb{Z}x_1 \oplus H$. Afirmamos que vale $G = \mathbb{Z}v \oplus (G \cap H)$. Com efeito: como $v \in G$ segue que $\mathbb{Z} \subseteq G$, e portanto $G \supseteq \mathbb{Z}v \oplus (G \cap H)$. Seja $u = t_1 x_1 + t_2 y_2 + \cdots + t_n y_n$, com $t_i \in \mathbb{Z}$, e suponha que $u \in G$. Temos $t_1 = q_1' d_1 + r_1'$, com $0 \leq r_1 \leq d_1$, e assim

$$\begin{aligned} u - q_1' v &= t_1 x_1 + t_2 y_2 + \cdots + t_n y_n \\ &\quad - q_1' d_1 x_1 - q_1' r_2 y_2 - \cdots - q_1' r_n y_n \\ &= r_1' x_1 + (t_2 - q_1' r_2) y_2 + \cdots + (t_n - q_1' r_n) y_n \in G. \end{aligned}$$

Portanto $r_1' \in S$, logo pela minimalidade de d_1 segue que $r_1' = 0$, o que implica

$$\begin{aligned} u &= q_1'(d_1 x_1) + (t_2 y_2 + \cdots + t_n y_n) \\ &= q_1' v + t_2 y_2 + \cdots + t_n y_n . \end{aligned}$$

Isto mostra que $u - q_1' v \in G \cap (\mathbb{Z}y_2 \oplus \cdots \oplus \mathbb{Z}y_n) = G \cap H$ e, consequentemente, $u \in \mathbb{Z}v \oplus (G \cap H)$.

Se $G \cap H = 0$ o teorema está demonstrado; se $G \cap H \neq 0$, temos que $G \cap H$ é subgrupo não trivial de H, e H tem posto $n-1$. Pela hipótese de indução, existe uma $\mathbb{Z}$-base $\{x_2, \ldots, x_n\}$ de H, e existem $r \in \mathbb{Z}$ com $1 \leq r \leq n$ e inteiros positivos $d_2 \mid d_3 \mid \cdots \mid d_r$ tais que $G \cap H = \mathbb{Z}d_2x_2 \oplus \mathbb{Z}d_3x_3 \oplus \cdots \oplus \mathbb{Z}d_rx_r$.

Ora, $F = \mathbb{Z}x_1 \oplus H = \mathbb{Z}x_1 \oplus (\mathbb{Z}d_2x_2 \oplus \mathbb{Z}d_3x_3 \oplus \cdots \oplus \mathbb{Z}d_nx_n)$ e $G = (\mathbb{Z}d_1x_1) \oplus (\mathbb{Z}d_2x_2) \oplus (\mathbb{Z}d_3x_3) \oplus \cdots \oplus (\mathbb{Z}d_rx_r)$. Assim, $\{x_1, \ldots x_n\}$ é uma $\mathbb{Z}$-base de F e $\{d_1x_1, \ldots, d_rx_r\}$ é uma $\mathbb{Z}$-base de G.

Finalmente, vale $d_2 = q_1d_1 + r_0$, com $0 \leq r_0 \leq d_1$. Além disso, $\{x_2, x_1 + qx_2, x_3, \ldots, x_n\}$ é uma $\mathbb{Z}$-base e $d_1x_1 + d_2x_2 = w \in G$. Mas, $w = r_0x_2 + d_1(x_1 + qx_2) + 0 \cdot x_3 + \cdots + 0 \cdot x_n$, e consequentemente, $r_0 \in S$. Pela minimalidade de d_1, segue que $r_0 = 0$ e portanto, $d_1 \mid d_2$. □

Teorema 1.24. *Seja H um subgrupo discreto de $\mathbb{R}^n$. Então H é gerado (como $\mathbb{Z}$-módulo) por k vetores $\mathbb{R}$-linearmente independentes, com $k \leq n$.*

Demonstração. Seja $\beta = \{v_1, \ldots, v_k\}$ um conjunto de vetores de H linearmente independentes sobre $\mathbb{R}$, com k máximo e seja $P = \left\{ \sum_{j=1}^{k} \alpha_j v_j : 0 \leq \alpha_j \leq 1 \right\} \subseteq \mathbb{R}^n$. Como P é imagem do cubo unitário $[0,1]^k$ através da função contínua $(\alpha_1, \ldots, \alpha_k) \longmapsto \sum_{j=1}^{k} \alpha_j v_j$, segue-se que P é compacto; como H é discreto, segue que $P \cap H$ é finito. Agora, pela maximalidade de k, para qualquer $x \in H$ temos que $\{x, v_1, \ldots, v_k\}$ é $\mathbb{R}$-linearmente dependente, logo existem $\lambda_i \in \mathbb{R}$, com $i = 1, \ldots, k$, tais que $x = \sum_{i=1}^{k} \lambda_i v_i$. Para cada $j \in \mathbb{Z}^+$, consideremos

$$x_j = jx - \sum_{i=1}^{k} \lfloor j\lambda_i \rfloor v_i \in H. \tag{1.7}$$

Então $x_j = j\sum_{i=1}^{k} \lambda_i v_i - \sum_{i=1}^{k} \lfloor j\lambda_i \rfloor v_i = \sum_{i=1}^{k} \big(j\lambda_i - \lfloor j\lambda_i \rfloor\big) v_i \in P$. Ainda, $x = x_1 + \sum_{i=1}^{k} \lfloor \lambda_i \rfloor v_i$, o que mostra que H é finitamente gerado como um $\mathbb{Z}$-módulo, a saber, pelos elementos de $(P \cap H) \cup \{v_1, \ldots, v_k\} = P \cap H$ (pois $v_i \in P \cap H$ para cada i).

Por outro lado, como $P \cap H$ é finito, existem inteiros l e m distintos tais que $x_l = x_m$, logo por 1.7 teremos $(l-m) \sum_{i=1}^{k} \lambda_i v_i = \sum_{i=1}^{k} \big(\lfloor l\lambda_i \rfloor - \lfloor m\lambda_i \rfloor\big) v_i$, e assim pela $\mathbb{R}$-independência linear dos v_i segue que $\lambda_i = \frac{\lfloor l\lambda_i \rfloor - \lfloor m\lambda_i \rfloor}{l-m} \in \mathbb{Q}$.

Lembrando que $x = \sum_{i=1}^{k} \lambda_i v_i$, concluímos que H está contido no $\mathbb{Q}$-subespaço gerado por $v_1, \ldots, v_k$; em particular cada elemento do conjunto finito $P \cap H$ pode ser escrito como combinação $\mathbb{Q}$-linear dos v_i. Se $d \neq 0$ é um denominador comum de todos os escalares racionais envolvidos na escrita dos elementos de $P \cap H$, então teremos $dH \subseteq \sum_{i=1}^{k} \mathbb{Z}v_i$ pois temos $H = \sum_{w \in P \cap H} \mathbb{Z}w$, e para cada $w \in P \cap H$ teremos $dw \in \sum \mathbb{Z}v_i$.

Daí, pelo Teorema 1.23, segue que existe uma base $\{f_1, \ldots, f_k\}$ do $\mathbb{Z}$-módulo $\sum_{i=1}^{k} \mathbb{Z}v_i$ e inteiros α_i, tal que $\{\alpha_1 f_1, \ldots, \alpha_k f_k\}$ gera dH como $\mathbb{Z}$-módulo, e posto$(dH) = \#\{i : \alpha_i \neq 0\} \leq k$. Evidentemente, H e dH são isomorfos como $\mathbb{Z}$-módulos, logo posto(dH) =posto(H), e como $H \supseteq \sum \mathbb{Z}v_i$, novamente pelo Teorema 1.23 teremos posto(H) $\geq$posto$\sum_{i=1}^{k} \mathbb{Z}v_i$, sendo este último igual a k, pois os v_i são $\mathbb{R}$-linearmente independentes, logo também são $\mathbb{Z}$-linearmente independentes. Assim, posto$(dH) = k$, o que implica que $\alpha_i \neq 0$, para todo i, e assim H é gerado como $\mathbb{Z}$-módulo pelos vetores $\frac{\alpha_i}{d} f_i$, com $i = 1, \ldots, k$.

Afirmamos finalmente que $\{f_1, \ldots, f_k\}$ é $\mathbb{R}$-linearmente independente, logo o conjunto $\{\frac{\alpha_1}{d} f_1, \ldots, \frac{\alpha_k}{d} f_k\}$ também será $\mathbb{R}$-linearmente independente. De fato, como $\{f_1, \ldots, f_k\}$ é uma $\mathbb{Z}$-base de $\sum \mathbb{Z}v_i$, então existe $A = (a_{ij}) \in \mathrm{GL}_k(\mathbb{Z})$ tal que $(f_1, \ldots, f_k) = (v_1, \ldots, v_k)A$; assim se $c_1, \ldots, c_k \in \mathbb{R}$ satisfazem $(f_1, \ldots, f_k)(c_1, \ldots, c_k)^t = 0$, então $(v_1, \ldots, v_k)[A(c_1, \ldots, c_k)^t] = 0$. Como $\{v_1, \ldots, v_k\}$ é $\mathbb{R}$-linearmente independente segue que $A(c_1, \ldots, c_k)^t = 0$, logo $(c_1, \ldots, c_k)^t = 0$. □

Definição 1.25. Um subgrupo discreto de $\mathbb{R}^n$ de posto n é um dito um *reticulado* de $\mathbb{R}^n$. Um subconjunto $\mathbf{v} = \{v_1, \ldots, v_n\}$ $\mathbb{R}$-linearmente independente que gera H como $\mathbb{Z}$-módulo é chamado de *base* do reticulado H ♠. Um vetor $u = a_1 v_1 + a_2 v_2 + \cdots + a_k v_k$ de H é dito *primitivo* em relação a base $\mathbf{v} = \{v_1, \ldots, v_n\}$ se MDC$(a_1, \cdots, a_k) = 1$.

Definição 1.26. Seja $\mathbf{v} = (v_1, \ldots, v_k)$ uma $\mathbb{Z}$-base de um reticulado $H \subseteq \mathbb{R}^n$. Definimos como *região fundamental* de H em relação a $\mathbf{v}$ o conjunto

$$P_{\mathbf{v}} = \left\{ \sum_{j=1}^{k} \alpha_j v_j : 0 \leq \alpha_j < 1 \right\}.$$

Definição 1.27. Seja μ a medida de Lebesgue no $\mathbb{R}^n$. Se $S \subseteq \mathbb{R}^n$ é um conjunto Lebesgue-mensurável com $\mu(S) < \infty$, dizemos que S é *integrável* com *volume* $\mu(S)$.

Lema 1.28. *Seja H um reticulado de $\mathbb{R}^n$. Então o volume $\mu(P_{\mathbf{v}})$ é positivo e independe da base $\mathbf{v}$ escolhida para H.*

Demonstração. Seja $\mathbf{v} = \{v_1, \ldots, v_n\}$ uma $\mathbb{Z}$-base de um reticulado $H \subseteq \mathbb{R}^n$. Então $\mu(P_{\mathbf{v}}) = \left|\det[v_1 \cdots v_n]\right| > 0$, e se $\mathbf{f} = \{f_1, \ldots, f_n\}$ é uma outra base de H, então $f_i = \sum_{j=1}^{n} \alpha_{ij} v_j$, com $(\alpha_{ij}) \in \mathrm{GL}_n(\mathbb{Z})$, logo $\det(\alpha_{ij}) = \pm 1$. Assim, $\mu(P_{\mathbf{f}}) = \left|\det(\alpha_{ij})\right| \mu(P_{\mathbf{v}}) = \mu(P_{\mathbf{v}})$. □

Teorema 1.29 (Minkowski)**.** *Sejam H um reticulado de $\mathbb{R}^n$ e S um subconjunto mensurável de $\mathbb{R}^n$ tal que $\mu(S) > \mu(H)$. Então existem dois elementos $x, y \in S$, com $x \neq y$ tais que $x - y \in H$.*

♠ Tal subconjunto existe pelo Teorema 1.24.

Demonstração. Sejam $\mathbf{v} = \{v_1, \ldots, v_n\}$ uma base do reticulado H e $P_\mathbf{v}$ a região fundamental de H. Então S pode ser escrito como

$$S = \bigcup_{h \in H} [(h + P_\mathbf{v}) \cap S] .$$

Com efeito: obviamente $S \supseteq \bigcup_{h\in H} [(h + P_\mathbf{v}) \cap S]$. Para provar a inclusão oposta, dado $s \in S$, basta mostrar que existe $h \in P_\mathbf{v}$ tais que $s - h \in H$. Como os v_i são $\mathbb{R}$-linearmente independentes (pois formam uma base do reticulado H), temos que $s = \sum s_i v_i$, com $s_i \in \mathbb{R}$. Se $h = \sum \lfloor s_i \rfloor v_i \in H$, então $s - h = \sum \big(s_i - \lfloor s_i \rfloor\big) v_i \in P_\mathbf{v}$, pois $s_i - \lfloor s_i \rfloor \in [0, 1)$. Portanto

$$\mu(S) = \mu\left(\bigcup_{h\in H} \big(S \cap (h + P_\mathbf{v})\big)\right) = \sum_{h\in H} \mu\big(S \cap (h + P_\mathbf{v})\big) ,$$

pois $\big(S \cap (h_1 + P_\mathbf{v})\big) \cap \big(S \cap (h_2 + P_\mathbf{v})\big) = \emptyset$ se $h_1 \neq h_2$ [¶], e porque H é enumerável [♣].

Como μ é invariante por translação, temos $\mu\big(S \cap (h + P_\mathbf{v})\big) = \mu\big((-h + S) \cap P_\mathbf{v}\big)$. Se os conjuntos $(-h + S) \cap P_\mathbf{v}$, com $h \in H$, fossem dois a dois disjuntos, teríamos $\mu(P_\mathbf{v}) \geq \sum_{h\in H} \mu\big(P_\mathbf{v} \cap (-h + S)\big) = \mu(S)$, contrariando a hipótese. Assim, existem dois elementos distintos $h_1, h_2 \in H$, com $h_1 \neq h_2$ tais que

$$\big(P_\mathbf{v} \cap (-h_1 + S)\big) \cap \big(P_\mathbf{v} \cap (-h_2 + S)\big) = P_\mathbf{v} \cap (-h_1 + S) \cap (-h_2 + S) \neq \emptyset .$$

Portanto, existem dois elementos $x, y \in S$ tais que $-h_1 + x = -h_2 + y$, logo $x - y = h_1 - h_2 \in H - \{0\}$. □

Corolário 1.30. *Sejam H um reticulado de $\mathbb{R}^n$ e S um subconjunto convexo de $\mathbb{R}^n$ [‖] e simétrico em relação a origem (isto é, $x \in S$ se e somente se $x \in -S$). Suponha que vale uma das seguintes condições:*

- $\mu(S) > 2^n \mu(H)$, *ou*
- $\mu(S) \geq 2^n \mu(H)$ *e S é compacto.*

Então $S \cap H - \{0\} \neq \emptyset$.

Demonstração. Suponha que vale a primeira condição. Então o conjunto $S^* = \frac{1}{2}S$ satisfaz $\mu(S^*) = \frac{1}{2^n}\mu(S) > \mu(H)$, logo pelo Teorema 1.30 existem $y, z \in S^*$, $z \neq y$ tais que

[¶] Tome $s_1 = h_1 + t_1 \in S \cap (h_1 + P_\mathbf{v})$ e $s_2 = h_2 + t_2 \in S \cap (h_2 + P_\mathbf{v})$. Se $s_1 = s_2$ então $h_1 - h_2 = t_2 - t_1 \in H$. Como $t_1 = \sum_{i=1}^{n} \theta_i v_i$ e $t_2 = \sum_{i=1}^{n} \delta_i v_i$, com $\delta_i, \theta_i \in [0, 1)$, segue que $t_2 - t_1 = \sum_{i=1}^{n} (\delta_i - \theta_i) v_i$, com $\delta_i - \theta_i \in (-1, 1)$. Mas $t_2 - t_1 \in H$, logo $\delta_i - \theta_i \in \mathbb{Z}$, portanto, $\delta_i - \theta_i = 0$, resultando em $h_1 = h_2$.

[♣] De fato, H é a união enumerável da sequência crescente de conjuntos $H \cap [-j, j]^n$, com $j \geq 1$, cada um destes sendo finito pela hipótese sobre H.

[‖] Todo subconjunto convexo de $\mathbb{R}^n$ é Lebesgue-mensurável; vide http://math.stackexchange.com/207609/the-measurability-of-convex-sets.

$y - z \in H$. Como S é simétrico em relação à origem, segue que $y - z = \frac{1}{2}\left(2y + (-2z)\right) \in S$, pois $2y, 2z \in S$.

Por outro lado, se vale a segunda condição, então para todo $m \in \mathbb{Z}^+$ temos $\mu\Big(\big(1 + \frac{1}{m}\big)S\Big) > 2^n \mu(H^*)$, e assim os conjuntos $\big(1 + \frac{1}{m}\big)S$ satisfazem a primeira condição. Seja $x_m \in H^* \cap \big(1 + \frac{1}{m}\big)S$, digamos $x_m = \big(1 + \frac{1}{m}\big)y_m$, com $y_m \in S$. Como S é compacto, existe uma subsequência convergente (y_{m_j}) de (y_m), digamos $y_{n_j} \to y \in S$ quando $j \to \infty$. Então, quando $j \to \infty$, teremos $x_{n_j} \to y \in S$. Finalmente, como H^* é discreto, logo fechado, e cada $x_{n_j} \in H^*$, concluímos que $y \in H^*$. □

1.5 Norma de um ideal

Nesta seção apresentaremos o conceito de norma de um ideal do anel dos inteiros de um corpo de números e suas principais propriedades que serão úteis para provar que o grupo de classes de ideais é finito.

Definição 1.31. Seja $\mathcal{I}$ um ideal não nulo do anel de inteiros $\mathcal{O}_K$. A *norma* do ideal $\mathcal{I}$ é definida como sendo a cardinalidade do anel quociente $\mathcal{O}_K/\mathcal{I}$, ou seja,

$$N(\mathcal{I}) = \#\frac{\mathcal{O}_K}{\mathcal{I}}.$$

Proposição 1.32. *Seja K um corpo de números e x um elemento não não nulo de $\mathcal{O}_K$. Então*

$$|N(x)| = \#\frac{\mathcal{O}_K}{\mathcal{O}_K \cdot x}$$

Demonstração. Pelo Teorema 1.20, $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto n e como $\mathcal{O}_K$ e $\mathcal{O}_K \cdot x$ são isomorfos, segue que $\mathcal{O}_K \cdot x$ também é um $\mathbb{Z}$-módulo livre de posto n.

Agora, recorrendo ao Teorema 1.23, existe uma $\mathbb{Z}$-base $\{x_1, \ldots, x_n\}$ de $\mathcal{O}_K$ e $d_1, \ldots, d_n \in \mathbb{Z}$ tais que $\{d_1x_1, \ldots, d_nx_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_K \cdot x$. Tomando o homomorfismo sobrejetor $\varphi : \mathcal{O}_K \to \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{d_n\mathbb{Z}}$ definido por $\varphi\big(\sum_{i=1}^n a_i x_i\big) = (\overline{a_1}, \ldots, \overline{a_n})$, temos que $\ker(\varphi) = \mathcal{O}_K \cdot x$, pois $y = \sum_{i=1}^n a_i x_i \in \ker(\varphi)$ se, e somente se, $\varphi(y) = \bar{0}$, ou seja, $\bar{a_i} = 0$, para $i = 1, \ldots, n$, portanto $a_i \in d_i\mathbb{Z}$, para $i = 1, \ldots, n$, ou seja, $d_i \mid a_i$, para $i = 1, \ldots, n$ e assim, $y = \sum_{i=1}^{n} a_i x_i = \sum_{i=1}^{n} b_i d_i x_i$. Como $b_i \in \mathbb{Z}$, para $i = 1, \ldots, n$, segue que $y \in \mathcal{O}_K \cdot x$.

Assim, pelo teorema do isomorfismo temos

$$\frac{\mathcal{O}_K}{\mathcal{O}_K \cdot x} \simeq \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{d_n\mathbb{Z}},$$

logo $\#\frac{\mathcal{O}_K}{\mathcal{O}_K \cdot x} = d_1 \cdots d_n$.

Agora, tome a aplicação $\mathbb{Z}$-linear $\psi : O_K \longrightarrow O_K \cdot x$ definida por $\psi(x_i) = d_i x_i$, para $i = 1, \ldots, n$. Logo, $\psi(x_1) = d_1 x_1 + 0 \cdot x_2 + \cdots + 0 \cdot x_n, \ldots, \psi(x_n) = 0 \cdot x_1 + \cdots + 0 \cdot x_{n-1} + d_n \cdot x_n$ e $\det(\psi) = d_1 \cdots d_n$.

Por outro lado, considerando as $\mathbb{Z}$-bases $B = \{d_1 x_1, \ldots, d_n x_n\}$ e $C = \{x \cdot x_1, \ldots, x \cdot x_n\}$ de $O_K \cdot x$, e definindo o automorfismo $\mathbb{Z}$-linear $\phi : O_K \cdot x \longrightarrow O_K \cdot x$ tal que $\phi(d_1 x_i) = x \cdot x_i$ para $i = 1, \ldots, n$, segue que $\det(\phi) = \pm 1$. Ainda, $(\phi \circ \psi)(x_i) = \phi(\psi(x_i)) = \phi(d_i x_i) = y \cdot x_i$ para $i = 1, \ldots, n$, logo $(\phi \circ \psi)(y) = y \cdot x$. Finalmente, $N(x) = \det(\psi \circ \phi) = \det(\psi) \cdot \det(\phi) = \pm d_1 d_2 \cdots d_n = \pm \#\frac{O_K}{O_K \cdot x}$, e portanto $|N(x)| = \#\frac{O_K}{O_K \cdot x}$. □

Observação 1.33. Se $\mathcal{I}$ é um ideal, então $N(\mathcal{I})$ é finita. Com efeito, se x é um elemento não nulo de $\mathcal{I}$, então $O_K \cdot x \subseteq \mathcal{I}$ e podemos escrever $O_K/\mathcal{I}$ como um quociente de $O_K/O_K \cdot x$. Assim,

$$\#\frac{O_K}{O_K \cdot x} = \#\frac{O_K}{\mathcal{I}} \cdot \#\frac{\mathcal{I}}{O_K \cdot x},$$

e como $\frac{O_K}{O_K \cdot x}$ é finito (pela Proposição 1.32), segue que $\frac{O_K}{\mathcal{I}}$ também é finito.

1.6 Prolongamento canônico

Seja K um corpo de números de grau n. Então, existem n $\mathbb{Q}$-monomorfismos distintos $\sigma_j : K \to \mathbb{C}$. Para cada $j = 1, \ldots, n$ existe um k com $1 \leq k \leq n$ tal que $\overline{\sigma_j} = \sigma_k$, onde a barra indica conjugação complexa. Além disso, $\overline{\sigma_j} = \sigma_j$ se, e somente se, $\sigma_j(K) \subseteq \mathbb{R}$.

Assim, usando r para denotar o número de índices tal que $\sigma_j(K) \subseteq \mathbb{R}$, ordenamos os $\mathbb{Q}$-monomorfismos $\sigma_1, \ldots, \sigma_n$ da seguinte maneira:

- $\sigma_1, \ldots, \sigma_r$ são $\mathbb{Q}$-monomorfismos reais, ou seja, $\sigma_j(K) \subseteq \mathbb{R}$ para $1 \leq j \leq r$;
- $\sigma_{r+1}, \ldots, \sigma_{r+s}$ são $\mathbb{Q}$-monomorfismos não reais;
- Os $\mathbb{Q}$-monomorfismos restantes são precisamente $\overline{\sigma_{r+1}}, \ldots, \overline{\sigma_{r+s}}$.

Temos então $n = r + 2s$, e os primeiros $r + s$ $\mathbb{Q}$-monomorfismos determinam os restantes. Considere a aplicação

$$\begin{aligned} \sigma : K &\to \mathbb{R}^r \times \mathbb{C}^s \\ x &\mapsto \big(\sigma_1(x), \ldots, \sigma_{r+s}(x)\big). \end{aligned}$$

Definição 1.34. O homomorfismo de anéis σ com as condições acima será chamado de *prolongamento canônico de K* (em $\mathbb{R}^r \times \mathbb{C}^s$) ou *homomorfismo de Minkowski*.

Identificando $\mathbb{R}^r \times \mathbb{C}^s$ com $\mathbb{R}^n$, o homomorfismo σ também pode ser escrito como

$$\sigma(x) = \big(\sigma_1(x), \ldots, \sigma_r(x), \operatorname{Re}\sigma_{r+1}(x), \operatorname{Im}\sigma_{r+1}(x), \ldots, \operatorname{Re}\sigma_{r+s}(x), \operatorname{Im}\sigma_{r+s}(x)\big),$$

onde $\mathrm{Re}\,(z)$ e $\mathrm{Im}\,(z)$ denotam, respectivamente, a parte real e imaginária do número complexo z.

Exemplo 1.35. Sejam $K = \mathbb{Q}(\sqrt[3]{2})$, e $\{\sigma_1, \sigma_2, \sigma_3\}$ o grupo de $\mathbb{Q}$-monomorfismos de K em $\mathbb{C}$, onde

$$\begin{aligned}
\sigma_1(a + b\sqrt[3]{2}) &= a + b\sqrt[3]{2}\,, \\
\sigma_2(a + b\sqrt[3]{2}) &= a - \frac{\sqrt[3]{2}}{2}b + \frac{\sqrt[3]{2}\cdot\sqrt{3}}{2}\,i\,, \\
\sigma_3(a + b\sqrt[3]{2}) &= a - \frac{\sqrt[3]{2}}{2}b - \frac{\sqrt[3]{2}\cdot\sqrt{3}}{2}\,i\,,
\end{aligned}$$

para $a, b \in \mathbb{Q}$. Neste caso temos $r = s = 1$. Assim, para cada $a + b\sqrt[3]{2} \in K$, com $a, b \in \mathbb{Q}$, temos

$$\sigma(a + b\sqrt[3]{2}) = \left(a + b\sqrt[3]{2}, a - \frac{\sqrt[3]{2}}{2}b + \frac{\sqrt[3]{2}\cdot\sqrt{3}}{2}\,i, a - \frac{\sqrt[3]{2}}{2}b - \frac{\sqrt[3]{2}\cdot\sqrt{3}}{2}\,i\right).$$

Proposição 1.36. *Seja K um corpo de números de grau n e $M \subseteq K$ um $\mathbb{Z}$-módulo livre de posto n com $\mathbb{Z}$-base $(x_i)_{1\le i\le n}$. Então $\sigma(M)$ é um reticulado de $\mathbb{R}^n$ e seu volume é dado por*

$$\mu\big(\sigma(M)\big) = 2^{-s}\left|\det_{1\le i,j\le n}\big(\sigma_i(x_j)\big)\right|.$$

Demonstração. O determinante da matriz $\left[\sigma_i(x_j)\right]_{i,j=1}^{n}$ é dado por

$$d = \det\begin{bmatrix}
\sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\sigma_r(x_1) & \dots & \sigma_r(x_j) & \dots & \sigma_r(x_n) \\
\mathrm{Re}\,\sigma_{r+1}(x_1) & \dots & \mathrm{Re}\,\sigma_{r+1}(x_j) & \dots & \mathrm{Re}\,\sigma_{r+1}(x_n) \\
\mathrm{Im}\,\sigma_{r+1}(x_1) & \dots & \mathrm{Im}\,\sigma_{r+1}(x_j) & \dots & \mathrm{Im}\,\sigma_{r+1}(x_n) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\mathrm{Re}\,\sigma_{r+s}(x_1) & \dots & \mathrm{Re}\,\sigma_{r+s}(x_j) & \dots & \mathrm{Re}\,\sigma_{r+s}(x_n) \\
\mathrm{Im}\,\sigma_{r+s}(x_1) & \dots & \mathrm{Im}\,\sigma_{r+s}(x_j) & \dots & \mathrm{Im}\,\sigma_{r+s}(x_n)
\end{bmatrix}.$$

Lembrando que $\mathrm{Re}\,(z) = \frac{1}{2}(z + \overline{z})$ e $\mathrm{Im}\,(z) = \frac{1}{2i}(z - \overline{z})$, para cada $z \in \mathbb{C}$, temos

$$d = \det\begin{bmatrix}
\sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\sigma_r(x_1) & \dots & \sigma_r(x_j) & \dots & \sigma_r(x_n) \\
\frac{1}{2}(\sigma + \overline{\sigma})_{r+1}(x_1) & \dots & \frac{1}{2}(\sigma + \overline{\sigma})_{r+1}(x_j) & \dots & \frac{1}{2}(\sigma + \overline{\sigma})_{r+1}(x_n) \\
\frac{1}{2i}(\sigma - \overline{\sigma})_{r+1}(x_1) & \dots & \frac{1}{2i}(\sigma - \overline{\sigma})_{r+1}(x_j) & \dots & \frac{1}{2i}(\sigma - \overline{\sigma})_{r+1}(x_n) \\
\vdots & \ddots & \vdots & \ddots & \vdots \\
\frac{1}{2}(\sigma + \overline{\sigma})_{r+s}(x_1) & \dots & \frac{1}{2}(\sigma + \overline{\sigma})_{r+s}(x_j) & \dots & \frac{1}{2}(\sigma + \overline{\sigma})_{r+s}(x_n) \\
\frac{1}{2i}(\sigma - \overline{\sigma})_{r+s}(x_1) & \dots & \frac{1}{2i}(\sigma - \overline{\sigma})_{r+s}(x_j) & \dots & \frac{1}{2i}(\sigma - \overline{\sigma})_{r+s}(x_n)
\end{bmatrix},$$

e fazendo operações elementares segue que

$$d = \left(\frac{1}{2}\right)^s \left(\frac{1}{2i}\right)^s \det \begin{bmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_r(x_1) & \dots & \sigma_r(x_j) & \dots & \sigma_r(x_n) \\ (\sigma+\overline{\sigma})_{r+1}(x_1) & \dots & (\sigma+\overline{\sigma})_{r+1}(x_j) & \dots & (\sigma+\overline{\sigma})_{r+1}(x_n) \\ (\sigma-\overline{\sigma})_{r+1}(x_1) & \dots & (\sigma-\overline{\sigma})_{r+1}(x_j) & \dots & (\sigma-\overline{\sigma})_{r+1}(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ (\sigma+\overline{\sigma})_{r+s}(x_1) & \dots & (\sigma+\overline{\sigma})_{r+s}(x_j) & \dots & (\sigma+\overline{\sigma})_{r+s}(x_n) \\ (\sigma-\overline{\sigma})_{r+s}(x_1) & \dots & (\sigma-\overline{\sigma})_{r+s}(x_j) & \dots & (\sigma-\overline{\sigma})_{r+s}(x_n) \end{bmatrix}$$

$$= \left(\frac{1}{2}\right)^s \left(\frac{1}{2i}\right)^s \det \begin{bmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_r(x_1) & \dots & \sigma_r(x_j) & \dots & \sigma_r(x_n) \\ 2\sigma_{r+1}(x_1) & \dots & 2\sigma_{r+1}(x_j) & \dots & 2\sigma_{r+1}(x_n) \\ (\sigma-\overline{\sigma})_{r+1}(x_1) & \dots & (\sigma-\overline{\sigma})_{r+1}(x_j) & \dots & (\sigma-\overline{\sigma})_{r+1}(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ 2\sigma_{r+s}(x_1) & \dots & 2\sigma_{r+s}(x_j) & \dots & 2\sigma_{r+s}(x_n) \\ (\sigma-\overline{\sigma})_{r+s}(x_1) & \dots & (\sigma-\overline{\sigma})_{r+s}(x_j) & \dots & (\sigma-\overline{\sigma})_{r+s}(x_n) \end{bmatrix}$$

$$= (-1)^s (2i)^{-s} \det \begin{bmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_r(x_1) & \dots & \sigma_r(x_j) & \dots & \sigma_r(x_n) \\ \sigma_{r+1}(x_1) & \dots & \sigma_{r+1}(x_j) & \dots & \sigma_{r+1}(x_n) \\ \overline{\sigma_{r+1}}(x_1) & \dots & \overline{\sigma_{r+1}}(x_j) & \dots & \overline{\sigma_{r+1}}(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r+s}(x_1) & \dots & \sigma_{r+s}(x_j) & \dots & \sigma_{r+s}(x_n) \\ \overline{\sigma_{r+s}}(x_1) & \dots & \overline{\sigma_{r+s}}(x_j) & \dots & \overline{\sigma_{r+s}}(x_n) \end{bmatrix},$$

e como $\overline{\sigma_{r+k}} = \sigma_{r+s+k}$, segue que

$$d = (-1)^s (2i)^{-s} \det \begin{bmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_r(x_1) & \dots & \sigma_r(x_j) & \dots & \sigma_r(x_n) \\ \sigma_{r+1}(x_1) & \dots & \sigma_{r+1}(x_j) & \dots & \sigma_{r+1}(x_n) \\ \sigma_{r+s+1}(x_1) & \dots & \sigma_{r+s+1}(x_j) & \dots & \sigma_{r+s+1}(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r+s}(x_1) & \dots & \sigma_{r+s}(x_j) & \dots & \sigma_{r+s}(x_n) \\ \sigma_{r+2s}(x_1) & \dots & \sigma_{r+2s}(x_j) & \dots & \sigma_{r+2s}(x_n) \end{bmatrix},$$

logo

$$|d| = (2)^{-s} \det \begin{bmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_j) & \dots & \sigma_1(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_r(x_1) & \dots & \sigma_r(x_j) & \dots & \sigma_r(x_n) \\ \sigma_{r+1}(x_1) & \dots & \sigma_{r+1}(x_j) & \dots & \sigma_{r+1}(x_n) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \sigma_{r+2s}(x_1) & \dots & \sigma_{r+2s}(x_j) & \dots & \sigma_{r+2s}(x_n) \end{bmatrix},$$

ou seja, $|d| = (2)^{-s} \det\big(\sigma_i(x_j)\big)$. Como os x_i formam uma base de K em $\mathbb{Q}$, do Teorema 1.18 segue que $\det\big(\sigma_i(x_j)\big) \neq 0$ e, consequentemente, $\mathcal{D}(x_1, \dots, x_n) \neq 0$. Além disso, pelo lema de Dedekind (Lema 1.17) os vetores $\sigma(x_i)$ são linearmente independentes em $\mathbb{R}^n$, logo o $\mathbb{Z}$-módulo gerado por eles é um reticulado de $\mathbb{R}^n$, a saber

$$\begin{aligned}
&\sum_{i=1}^{n} \mathbb{Z}\, \sigma(x_i) \\
&= \sum_{i=1}^{n} \mathbb{Z} \left(\sigma_1(x_i), \dots, \sigma_r(x_i), \operatorname{Re} \sigma_{r+1}(x_i), \operatorname{Im} \sigma_{r+1}, \dots, \operatorname{Re} \sigma_{r+s}(x_i), \operatorname{Im} \sigma_{r+s}(x_i)\right) \\
&= \left(\sigma_1\left(\sum_{i=1}^{n} \mathbb{Z}x_i\right), \dots, \sigma_r\left(\sum_{i=1}^{n} \mathbb{Z}x_i\right),\right. \\
&\quad \left. \operatorname{Re} \sigma_{r+1}\left(\sum_{i=1}^{n} \mathbb{Z}x_i\right), \operatorname{Im} \sigma_{r+1}\left(\sum_{i=1}^{n} \mathbb{Z}x_i\right), \dots, \operatorname{Re} \sigma_{r+s}\left(\sum_{i=1}^{n} \mathbb{Z}x_i\right), \operatorname{Im} \sigma_{r+s}\left(\sum_{i=1}^{n} \mathbb{Z}x_i\right)\right) \\
&= \big(\sigma_1(M), \dots, \sigma_r(M), \operatorname{Re} \sigma_{r+1}(M), \operatorname{Im} \sigma_{r+1}(M), \dots, \operatorname{Re} \sigma_{r+s}(M), \operatorname{Im} \sigma_{r+s}(M)\big) \\
&= \sigma(M)\,,
\end{aligned}$$

e seu volume será dado por $\mu(\sigma(M)) = |d| = (2)^{-s} \det\left(\sigma_i(x_j)\right)$. □

Proposição 1.37. *Seja K um corpo de números com discriminante absoluto $\mathcal{D}_K$. Sejam $\mathcal{O}_K$ seu anel de inteiros e $\mathcal{I}$ um ideal não nulo de $\mathcal{O}_K$. Então $\sigma(\mathcal{O}_K)$ e $\sigma(\mathcal{I})$ são reticulados e valem $\mu\left(\sigma(\mathcal{O}_K)\right) = 2^{-s} \left|\mathcal{D}_K\right|^{1/2}$ e $\mu\left(\sigma(\mathcal{I})\right) = 2^{-s} \left|\mathcal{D}_K\right|^{1/2} N(\mathcal{I})$.*

Demonstração. Seja $x \in \mathcal{I}$ não nulo. Então $\mathcal{O}_K \cdot x \subseteq \mathcal{I} \subseteq \mathcal{O}_K$. Pelo Teorema 1.20 $\mathcal{O}_K$ é $\mathbb{Z}$-módulo livre de posto n, portanto, $\mathcal{I}$ e $\mathcal{O}_K \cdot x$ também são $\mathbb{Z}$-módulos livres. Como $\mathcal{O}_K \cdot x$ e $\mathcal{O}_K$ são isomorfos, segue que posto de $\mathcal{O}_K \cdot x =$ posto de $\mathcal{O}_K = n$. Ainda, o mesmo resultado implica as desigualdades

$$n = \text{ posto de } \mathcal{O}_K \cdot x \leq \text{ posto de } \mathcal{I} \leq \text{ posto de } \mathcal{O}_K = n\,,$$

e portanto $\mathcal{I}$ é $\mathbb{Z}$-módulo livre de posto n. Aplicando a Proposição 1.36 segue que $\sigma(\mathcal{O}_K)$ e $\sigma(\mathcal{I})$ são reticulados de $\mathbb{R}^n$.

Por outro lado, se $\{x_1, \dots, x_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{O}_K$, já vimos na Proposição 1.18 que $\mathcal{D}_K = \det\big(\sigma_i(x_j)\big)^2$. Comparando com o resultado da Proposição anterior, obtemos

$\mu\left(\sigma(\mathcal{O}_K)\right) = 2^{-s}\left|\mathcal{D}_K\right|^{1/2}$. Ora, como $\mathcal{I}$ também tem posto n como $\mathbb{Z}$-módulo, então existem inteiros positivos $d_1 \mid d_2 \mid \cdots \mid d_n$ tais que $\{d_1x_1, \ldots, d_nx_n\}$ é uma $\mathbb{Z}$-base de $\mathcal{I}$. Imitando o argumento da Proposição 1.32 (com $\mathcal{I}$ no lugar de $\mathcal{O}_K \cdot x$), concluímos que vale $N(\mathcal{I}) = d_1 \cdots d_n$. O raciocínio da Proposição 1.36 mostra neste caso que $\sigma(\mathcal{I})$ é o $\mathbb{Z}$-módulo gerado pelos vetores $\sigma(d_ix_i) = d_i\sigma(x_i)$, logo o volume de $\sigma(\mathcal{I})$ será igual a $2^{-s}\det\big(d_j\sigma_i(x_j)\big) = d_1 \cdots d_n\mu\big(\sigma(\mathcal{O}_K)\big) = N(\mathcal{I})\mu\big(\sigma(\mathcal{O}_K)\big)$. □

1.7 Finitude do grupo de classes de ideais

Proposição 1.38. *Para $t \geq 0$, seja*

$$B_t = \left\{(y_1, \ldots, y_r, z_1, \ldots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : \sum_{i=1}^{r} |y_i| + 2\sum_{j=1}^{s} |z_j| \leq t\right\},$$

onde r e s são inteiros positivos e $n = r + 2s$. Então vale

$$\mu(B_t) = 2^r\left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}. \tag{1.8}$$

Demonstração. Denotaremos $\mu(B_t) = V(r, s, t)$ e usaremos indução dupla em r e s.

Note que $V(1, 0, t) = 2t$ (pois neste caso B_t é o segmento de reta $[-t, t]$) e $V(0, 1, t) = \frac{\pi t^2}{4}$ (neste caso B_t é o disco de raio $\frac{t}{2}$ centrado na origem de $\mathbb{C}$).

Seja s tal que (1.8) vale para certo valor r. Provaremos então que também vale para os valores $r + 1$ e s.

O conjunto $B_t \subseteq \mathbb{R} \times \mathbb{R}^r \times \mathbb{C}^s$ correspondente a $r + 1$ e s é definido por

$$|y| + \sum_{i=1}^{r} |y_i| + 2\sum_{j=1}^{s} |z_j| \leq t \qquad (y \in \mathbb{R}).$$

Fazendo integração iterada temos

$$V(r + 1, s, t) = \int_{\mathbb{R}} V\big(r, s, t - |y|\big)\, dy = \int_{-t}^{t} V\big(r, s, t - |y|\big)\, dy.$$

Utilizando a hipótese de indução, segue que

$$V(r + 1, s, t) = 2\int_0^t 2^r\left(\frac{\pi}{2}\right)^s \frac{(t - y)^n}{n!} dy = 2^{r+1}\left(\frac{\pi}{2}\right)^s \frac{t^{n+1}}{(n + 1)!},$$

que satisfaz o item 1.8.

Similarmente, suponha que a igualdade 1.8 vale para certos valores r e s; provaremos então que a igualdade também vale para os valores r e $s + 1$.

O conjunto $B_t \subseteq \mathbb{R}^r \times \mathbb{C}^s \times \mathbb{C}$ correspondente a r e $s+1$ é definido por

$$\sum_{i=1}^{r} |y_i| + 2\sum_{j=1}^{s} |z_j| + 2|z| \leq t \qquad (z \in \mathbb{C})\,.$$

Novamente efetuando integração iterada obtemos

$$V(r, s+1, t) = \int_{\mathbb{C}} V\big(r, s, t - 2|z|\,\big)\, d\mu(z) = \int_{|z| \leq \frac{t}{2}} V\big(r, s, t - 2|z|\,\big)\, d\mu(z)\,,$$

onde $d\mu(z)$ denota a medida de Lebesgue em $\mathbb{C}$. Fazendo $z = \rho e^{i\theta}$ (com $\rho > 0$ e $0 \leq \theta \leq 2\pi$) temos $d\mu(z) = \rho d\rho d\theta$, e utilizando a hipótese de indução segue que

$$\begin{aligned} V(r, s+1, t) &= \int_0^{\frac{t}{2}} \int_0^{2\pi} 2^r \left(\frac{\pi}{2}\right)^2 \frac{(t-2\rho)^n}{n!} \rho d\rho d\theta = 2\pi \frac{2^r}{n!} \left(\frac{\pi}{2}\right)^s \int_0^{\frac{t}{2}} (t-2\rho)^n \rho d\rho \\ &= \frac{2^r}{(n+2)!} \left(\frac{\pi}{2}\right)^{s+1} t^{n+2}, \end{aligned}$$

o que mostra que vale (1.8), pois $r + 2(s+1) = n+2$. □

Proposição 1.39. *Seja K um corpo de números de grau n com discriminante absoluto $\mathcal{D}_K$ e $\mathcal{I}$ um ideal inteiro não nulo de $\mathcal{O}_K$. Sejam r e s como na Definição 1.34. Então existe $x \in \mathcal{I}$, x não nulo, tal que*

$$\left|N_{\mathbb{K}/\mathbb{Q}}(x)\right| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n} |\mathcal{D}_K|^{1/2} N(\mathcal{I})\,.$$

Demonstração. Seja σ o prolongamento canônico de K em $\mathbb{R}^r \times \mathbb{C}^s$. Para cada $t > 0$, seja B_t o conjunto definido na Proposição 1.38. Então B_t é compacto, convexo e simétrico em relação a origem, e pela Proposição 1.38 vale $\mu(B_t) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!}$. Como $\mu(B_t)$ é contínua como função de t, com imagem $[0, \infty)$, pelo teorema do valor intermediário existe um valor t de modo que $\mu(B_t) = 2^n \mu(\sigma(\mathcal{I}))$, e assim pelo Corolário 1.30 existirá $x \in \mathcal{I} - \{0\}$ tal que $\sigma(x) \in B_t$. Por outro lado, pela Proposição 1.37 teremos $\mu\big(\sigma(\mathcal{I})\big) = 2^{-s} |\mathcal{D}_K|^{1/2} N(I)$, e assim

$$2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!} = 2^{n-s} |\mathcal{D}_K|^{1/2} N(\mathcal{I})\,,$$

isto é,

$$t^n = 2^{n-r} \pi^{-s} n! |\mathcal{D}_K|^{1/2} N(\mathcal{I}) = \left(\frac{4}{\pi}\right)^s n! |\mathcal{D}_K|^{1/2} N(\mathcal{I}).$$

Agora, avaliando a norma, temos

$$\left|N(x)_{\mathbb{K}/\mathbb{Q}}\right| = \prod_{i=1}^{r} |\sigma_i(x)| \prod_{j=r+1}^{r+s} |\sigma_j(x)| \prod_{j=r+1}^{r+s} |\sigma_j(x)|\,.$$

Aplicando a desigualdade da média aritmética e média geométrica, e usando que $x \in B_t$, obtemos

$$\begin{aligned}\left|N(x)_{\mathbb{K}/\mathbb{Q}}\right| &\leq \left[\frac{\sum_{i=1}^{r}|\sigma_i(x)| + \sum_{j=r+1}^{r+s}\left(|\sigma_j(x)| + |\overline{\sigma_j(x)}|\right)}{n}\right]^n \\ &= \left[\frac{\sum_{i=1}^{r}|\sigma_i(x)| + \sum_{j=r+1}^{r+s}2|\sigma_j(x)|}{n}\right]^n \\ &\leq \frac{t^n}{n^n} \\ &= \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\,|\mathcal{D}_K|^{1/2}N(\mathcal{I})\,. \qquad \square\end{aligned}$$

Corolário 1.40. *Seja K um corpo de números de grau n e discriminante absoluto $\mathcal{D}_K$. Então, $|\mathcal{D}_K| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$. Ainda o valor $\frac{n}{\log|\mathcal{D}_K|}$ é majorado por uma constante independente de K.*

Demonstração. Tomando $\mathcal{I} = \mathcal{O}_K$ na proposição 1.39, obtemos $x \in \mathcal{O}_K$, x não nulo, tal que

$$1 \leq |N(x)| = \left|N_{\mathbb{K}/\mathbb{Q}}(x)\right| \leq \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}|\mathcal{D}_K|^{1/2}\,,$$

logo $|\mathcal{D}_K|^{1/2} \geq \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!}$. Como $\frac{\pi}{4} < 1$ e $2s \leq n$, segue que

$$|\mathcal{D}_K| \geq \left(\frac{\pi}{4}\right)^{2s} \frac{n^{2n}}{n!^2} \geq \left(\frac{\pi}{4}\right)^{n} \frac{n^{2n}}{n!^2}.$$

Definindo $a_n := \left(\frac{\pi}{4}\right)^s \frac{n^n}{n!}$ temos, consequentemente, $|\mathcal{D}_K| \geq (a_n)^2$. Ora, $a_2 = \frac{\pi^2}{4}$ e

$$\begin{aligned}\frac{a_{n+1}}{a_n} &= \frac{\pi}{4}\frac{(n+1)^{2n+2}}{[(n+1)!]^2}\frac{(n!)^2}{n^{2n}} = \frac{\pi}{4}\frac{(n+1)^{2n}}{n^{2n}} = \frac{\pi}{4}\left(1+\frac{1}{n}\right)^{2n} \\ &= \frac{\pi}{4}\left[\binom{2n}{0}1^{2n}\left(\frac{1}{n}\right)^0 + \binom{2n}{1}1^{2n-1}\left(\frac{1}{n}\right)^1 + \epsilon\right],\end{aligned}$$

com $\epsilon \geq 0$, isto é, $\frac{a_{n+1}}{a_n} \geq \frac{\pi}{4}(1+2) = \frac{3\pi}{4}$, que combinado com $|\mathcal{D}_K| \geq a_n$ implica, para $n \geq 2$,

$$a_n = a_2\prod_{k=2}^{n-1}\frac{a_{k+1}}{a_k} \geq a_2\prod_{k=2}^{n-1}\left(\frac{3\pi}{4}\right) = \frac{\pi^2}{4}\left(\frac{3\pi}{4}\right)^{n-2}.$$

Assim, $|\mathcal{D}_K| \geq \frac{\pi^2(3\pi)^{n-2}}{4^{n-1}} = \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1}$. Finalmente, temos

$$\frac{\log|\mathcal{D}_K|}{n} \geq \frac{n-1}{n}\left[\log\frac{\pi}{3} + \log\left(\frac{3\pi}{4}\right)\right] \geq \frac{1}{2}\left[\log\frac{\pi}{3} + \log\left(\frac{3\pi}{4}\right)\right],$$

pois $n \geq 2$, e portanto $\frac{n}{\log|\mathcal{D}_K|} \leq \frac{2}{\log\left(\frac{\pi}{3}\right)+\log\left(\frac{3\pi}{4}\right)}$, a qual é uma constante independente do corpo de números K. $\square$

Corolário 1.41 (Hermite-Minkowski)**.** *Para todo corpo de números $K \neq \mathbb{Q}$, o discriminante absoluto $\mathcal{D}_K$ de K é $\neq \pm 1$.*

Demonstração. Pelo Corolário anterior temos $|\mathcal{D}_K| \geq \frac{\pi}{3}\left(\frac{3\pi}{4}\right)^{n-1} > 1$, pois $n \neq 1$. □

Lema 1.42. *Se $x \in O_K$, então o polinômio mínimo de x sobre $\mathbb{Q}$ tem coeficientes em $\mathbb{Z}[x]$.*

Demonstração. Se $x^r + a_1 x_{r-1} + \cdots + a_r = 0$, com $a_i \in \mathbb{Z}$, então aplicando os $\mathbb{Q}$-monomorfismos $\sigma : K \longrightarrow \mathbb{C}$ obtemos $\sigma(x)^r + a_1\sigma(x)^{r-1} + \cdots + a_r = 0$, logo cada $\sigma(x) \in O_K$, e assim as somas e produtos deles também pertencem a O_K. Em particular, os coeficientes do polinômio mínimo de x sobre $\mathbb{Q}$ serão elementos de O_K e por definição de polinômio mínimo, estão em $\mathbb{Q}$, e assim estão em $O_K \cap \mathbb{Q} = \mathbb{Z}$. □

Teorema 1.43 (Hermite)**.** *Em $\mathbb{C}$, existe um número finito de corpos de números com um discriminante $\mathcal{D}_K$ dado.*

Demonstração. Vimos no Corolário 1.40 que o grau n de um corpo de números K é majorado de forma que $n \leq C \log|\mathcal{D}_K|$, onde C é constante real. Sejam r e s como em 1.6, e definamos, em $\mathbb{R}^r \times \mathbb{C}^s$, o seguinte conjunto B:

1. Se $r > 0$, definimos

$$B = \Big\{ (y_1, \cdots, y_r, z_1, \cdots, z_s) \in \mathbb{R}^r \times \mathbb{C}^s : |y_1| \leq 2^{n-1}\left(\frac{\pi}{2}\right)^{-s} |\mathcal{D}_K|^{1/2}; \\ |y_i|, |z_j| \leq \frac{1}{2} \text{ para } i = 2, \cdots, r,\ j = 1, \cdots, s \Big\}.$$

2. Se $r = 0$, definimos

$$B = \Big\{ (z_1, \cdots, z_s \in \mathbb{C}^s : |z_1 - \overline{z_1}| = 2\,|\mathrm{Im}\,(z_1)| \leq 2^n \left(\frac{\pi}{2}\right)^{1-s} |\mathcal{D}_K|^{1/2}, \\ |z_1 + \overline{z_1}| = 2\,|\mathrm{Re}\,(z_1)| \leq \frac{1}{2};\ |z_j| \leq \frac{1}{2} \text{ para } j = 2, \cdots, s \Big\}.$$

Então B é um conjunto compacto, convexo e simétrico em relação a origem, com volume dado por [**]

$$\mu(B) = 2^{n-s}|\mathcal{D}_K|^{1/2}. \tag{1.9}$$

Se σ é o prolongamento canônico de K, a Proposição 1.37 e o Corolário 1.30 mostram que existe um elemento $x \neq 0$ de O_K tal que $\sigma(x) \in B$. Afirmamos que x é um elemento primitivo de K em $\mathbb{Q}$. Com efeito: No caso 1 a definição do conjunto B implica $|\sigma_i(x)| \leq \frac{1}{2}$

[**] No caso 1 o volume será um produto de volumes de intervalos e discos, a saber $\mu(B) = \left[2 \cdot 2^{n-1}\left(\frac{\pi}{2}\right)^{-s}|\mathcal{D}_K|^{1/2}\right] \cdot \left[2 \cdot \frac{1}{2}\right]^{r-1} \cdot \left[\pi\left(\frac{1}{2}\right)^2\right]^s = 2^{n-s}|\mathcal{D}_K|^{1/2}$. Já no caso 2, o volume será determinado por um retângulo e por discos, a saber $\mu(B) = \left[2^n\left(\frac{\pi}{2}\right)^{1-s}|\mathcal{D}_K|^{\frac{1}{2}}\right] \cdot \frac{1}{2} \cdot \left[\pi\left(\frac{1}{2}\right)^2\right]^{s-1} = 2^{n-s}|\mathcal{D}_K|^{1/2}$.

para todo $i \neq 1$. Como $|N(x)| = \prod_{i=1}^{n} |\sigma_i(x)|$ é um inteiro não nulo, necessariamente temos $|\sigma_1(x)| \geq 1$, e em particular $\sigma_1(x) \neq \sigma_i(x)$ para cada $i \neq 1$. Se $\ell = [K : \mathbb{Q}(x)]$, então o homomorfismo σ_1, quando restrito ao subcorpo $K(x)$, admite ℓ extensões a um $\mathbb{Q}$-homomorfismo de K em $\mathbb{C}$ (isto pois na nossa situação todas as extensões de corpo são automaticamente separáveis). Portanto estas extensões τ devem ser algumas das extensões σ_i; como $\tau(x) = \sigma_1(x) \neq \sigma_i(1)$ para todo $i \neq 1$, concluímos que necessariamente vale $\tau = \sigma_1$, o que prova que vale $\ell = 1$, isto é, $K = \mathbb{Q}(x)$.

No caso 2, o mesmo raciocínio sobre $|N(x)|$ usado acima, junto com a definição do conjunto B neste caso, implicam que vale necessariamente $|\sigma_1(x)|\,|\overline{\sigma_1(x)}| = |\sigma_1(x)|^2 \geq 1$, logo $|\sigma_1(x)| = |\overline{\sigma_1(x)}| \geq 1$, e em particular $\sigma_1(x) \neq \sigma_j(x)$ quando σ_j é distinto de σ_1 e $\overline{\sigma_1}$. Como $|\mathrm{Re}\,\sigma_1(x)| \leq \frac{1}{4}$, então necessariamente $\sigma_1(x) \notin \mathbb{R}$, logo também vale $\sigma_1(x) \neq \overline{\sigma_1(x)}$. Raciocinando como no caso 1, concluímos de novo que x é primitivo.

Finalmente, notemos que o conjunto B é limitado (B estará contido num cubo centrado na origem, com lado dependendo de r, s e $\mathcal{D}_K$). Portanto existe uma constante $C > 0$ tal que $|\sigma_i(x)| \leq C$ para cada i. Se s_k denota a k-ésima função simétrica elementar, a saber $s_k(t_1, \ldots, t_n) = \sum_{1 \leq i_1 < \cdots < i_k \leq n} t_{i_1} \cdots t_{i_k}$, então os coeficientes do polinômio minimal de x sobre $\mathbb{Q}$ são precisamente os valores $s_k\big(\sigma_1(x), \ldots, \sigma_n(x)\big)$, cada um destes satisfazendo $\big|s_k\big(\sigma_1(x), \ldots, \sigma_n(x)\big)\big| \leq s_k(C, \ldots, C) = \binom{n}{k} C^k$. Assim, os coeficientes do polinômio minimal de x sobre Q são limitados. Já que tais coeficientes são inteiros pelo Lema 1.42, concluímos que existe apenas um número finito de polinômios mínimos possíveis para x, e consequentemente, apenas um número finito de valores possíveis de x em $\mathbb{C}$. Como $K = \mathbb{Q}(x)$, haverá então apenas um número finito de possibilidades para o corpo K. □

2 CORRESPONDÊNCIA ENTRE ANÉIS CÚBICOS E FORMAS CÚBICAS BINÁRIAS

O objetivo desse capítulo é relacionar anéis cúbicos com formas binárias cúbicas. Para isso, usaremos a correspondência de Delone-Faddeev.

2.1 Correspondência de Delone-Faddeev

Considere a ação de $\mathrm{GL}_2(\mathbb{Z})$ em formas cúbicas binárias, ou seja, a ação de um elemento $\gamma = \left[\begin{smallmatrix} E & F \\ G & H \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{Z})$ no polinômio $p(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ (com $a,b,c,d \in \mathbb{Z}$), dada por

$$(\gamma \cdot p)(x,y) = \frac{1}{\det(\gamma)}\, p(Ex + Gy, Fx + Hy). \tag{2.1}$$

Definição 2.1. Seja $(A,+,\cdot)$ um anel comutativo com unidade. Dizemos que A é um *anel cúbico* se $(A,+)$ é um $\mathbb{Z}$-módulo livre de posto 3.

Afirmação 2.2. Podemos supor que 1 faz parte de uma $\mathbb{Z}$-base de $(A,+)$.

Demonstração. Seja (x,y,z) uma $\mathbb{Z}$-base de A. Dado o subgrupo $\mathbb{Z}\cdot 1$ de $(A,+)$, existe, pelo Teorema 1.23, um inteiro positivo d tal que dx é uma $\mathbb{Z}$-base de $\mathbb{Z}\cdot 1$. Em particular existe $n \in \mathbb{Z}$ tal que $ndx = 1$, isto é, $(nd\cdot 1)x = 1$. Assim, $x \in A^*$, logo $A = A\cdot x^{-1} = (\mathbb{Z}\cdot x \oplus \mathbb{Z}\cdot y \oplus \mathbb{Z}\cdot z)\cdot x^{-1} = \mathbb{Z}\cdot 1 \oplus \mathbb{Z}\cdot(yx^{-1}) \oplus \mathbb{Z}\cdot(zx^{-1})$. Assim, os elementos $1, yx^{-1}, zx^{-1}$ formam uma $\mathbb{Z}$-base de A. □

Seja $(1,\alpha,\beta)$ uma $\mathbb{Z}$-base de A. Então para quaisquer $m,n \in \mathbb{Z}$ temos que $(1,\alpha+m,\beta+n)$ é também uma $\mathbb{Z}$-base de A. Se $\alpha\beta = t_1\cdot 1 + t_2\cdot\alpha + t_3\cdot\beta$, com $t_1,t_2,t_3 \in \mathbb{Z}$, então $(\alpha+m)(\beta+n) = \alpha\beta + n\alpha + m\beta + nm\cdot 1 = (t_1+mn)\cdot 1 + (t_2+n)\alpha + (t_3+m)\beta$. Tomando $m = -t_3, n = -t_2$ obtemos $(\alpha+m)(\beta+n) \in \mathbb{Z}$. Assim, podemos supor que a nossa $\mathbb{Z}$-base $\mathcal{B} = (1,\alpha,\beta)$ satisfaz $\alpha\beta \in \mathbb{Z}$. Chamaremos tal $\mathbb{Z}$-base de *boa*.

Seja A um anel cúbico com $\mathbb{Z}$-base boa $\mathcal{B} = (1,\alpha,\beta)$. Então existem inteiros l,m,n,p,q,r,s tais que

$$\alpha\beta = n\cdot 1 = \beta\alpha\,, \tag{2.2}$$

$$\alpha^2 = m\cdot 1 + p\alpha + q\beta\,, \tag{2.3}$$

$$\beta^2 = l\cdot 1 + r\alpha + s\beta\,. \tag{2.4}$$

Temos $\alpha^2\cdot\beta = m\beta + p\alpha\beta + q\beta^2 = (np+ql)\cdot 1 + qr\alpha + (m+qs)\beta$, enquanto $\alpha\cdot(\alpha\cdot\beta) = n\alpha = 0\cdot 1 + n\alpha + 0\cdot\beta$. Como $\alpha^2\cdot\beta = \alpha\cdot(\alpha\cdot\beta)$, concluímos que valem $n = qr$ e

$m = -qs$; similarmente, as igualdades acima junto com a igualdade $\alpha \cdot \beta^2 = (\alpha \cdot \beta) \cdot \beta$ implicam $l = -pr$. Portanto, a cada par $(A, \mathcal{B})$, sendo A um anel cúbico com uma $\mathbb{Z}$-base boa $\mathcal{B} = (1, \alpha, \beta)$, associamos a única quádrupla $\mathcal{N}(A, \mathcal{B}) = (p, q, r, s)$ de inteiros satisfazendo

$$\left.\begin{aligned} \alpha\beta &= qr \cdot 1\,; \\ \alpha^2 &= -qs \cdot 1 + p\alpha + q\beta\,; \\ \beta^2 &= -pr \cdot 1 + r\alpha + s\beta\,. \end{aligned}\right\} \tag{2.5}$$

Observação 2.3. Dada qualquer quádrupla (p, q, r, s) de inteiros, existe um anel A com uma base boa $\mathcal{B} = (1, \alpha, \beta)$ tal que $(p, q, r, s) = \mathcal{N}(A, \mathcal{B})$. Com efeito: basta considerar o $\mathbb{Z}$-módulo livre com base $\mathcal{B} = (1, \alpha, \beta)$, e definir os produtos desta base segundo as regras $1 \cdot 1 = 1, 1 \cdot \alpha = \alpha, 1 \cdot \beta = \beta$, os valores $\alpha\beta, \alpha^2, \beta^2$ através de (2.5), e estender esta multiplicação por comutatividade e distributividade.

O seguinte resultado mostra como podemos relacionar as formas binárias cúbicas com os anéis cúbicos.

Teorema 2.4. *Existe uma bijeção natural entre o conjunto de classes de* $\mathrm{GL}_2\,\mathbb{Z}$*-equivalência de formas cúbicas não nulas e o conjunto de classes de isomorfismos de anéis cúbicos.*

Demonstração. Sejam A, A' anéis cúbicos, com $\mathbb{Z}$-bases boas $\mathcal{B} = (1, \alpha, \beta)$ e $\mathcal{B}' = (1, \alpha', \beta')$, respectivamente. Ainda, sejam $(p, q, r, s) = \mathcal{N}(A, \mathcal{B})$ e $(p', q', r', s') = \mathcal{N}(A', \mathcal{B}')$. Uma aplicação $T : A' \to A$ será um isomorfismo de anéis com unidade precisamente quando se cumpram as seguintes condições:

i) $T(1) = 1$;

ii) T é homomorfismo de grupos; isto é, T é uma transformação $\mathbb{Z}$-linear;

iii) T é uma bijeção;

iv) T respeita produtos.

As condições i) e ii) equivalem a termos

$$\begin{aligned} T(1) &= 1 \cdot 1 + 0 \cdot \alpha + 0 \cdot \beta\,; \\ T(\alpha') &= u \cdot 1 + E \cdot \alpha + F \cdot \beta\,; \\ T(\beta') &= v \cdot 1 + G \cdot \alpha + H \cdot \beta\,, \end{aligned}$$

para alguns $u, v, E, F, G, H \in \mathbb{Z}$. Seja $[T]$ a matriz associada à transformação $\mathbb{Z}$-linear T com respeito das $\mathbb{Z}$-bases $\mathcal{B}'$ e $\mathcal{B}$, isto é,

$$[T] = \begin{bmatrix} 1 & u & v \\ 0 & E & G \\ 0 & F & H \end{bmatrix}.$$

Em presença das condições i) e ii), a condição iii) equivale a termos $[T] \in \mathrm{GL}_3(\mathbb{Z})$, ou seja, $\det[T] = \pm 1$. Mas $\det[T] = \det(\gamma)$, onde $\gamma = \left[\begin{smallmatrix} E & F \\ G & H \end{smallmatrix}\right]$. Finalmente, em presença das condições i)-iii), para termos iv) é necessário e suficiente que valham

$$\left.\begin{aligned} T(\alpha')T(\beta') = T(\alpha'\beta') = T(-a'd') = -a'd' \cdot 1\,; \\ T(\alpha'^2) = T(\alpha')^2\,; \\ T(\beta'^2) = T(\beta')^2\,. \end{aligned}\right\} \tag{2.6}$$

As igualdades (2.6), junto com a definição das tuplas $(p,q,r,s) = \mathcal{N}(A,\mathcal{B})$ e $(p',q',r',s') = \mathcal{N}(A',\mathcal{B}')$ baseadas nas igualdades (2.5), implicam a igualdade matricial $(p',q',r',s')^t = \det(\gamma)\, W_\gamma\, (p,q,r,s)^t$, sendo W_γ a matriz dada pela fórmula (A.10) no Apêndice A.

Por outro lado, toda forma cúbica $p(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ corresponde a uma única quádrupla (a,b,c,d) de inteiros. Se $\theta = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{Z})$ e $(\gamma \cdot p)(x,y) = a'x^3 + b'x^2y + c'xy^2 + d'y^3$, então vale a igualdade matricial $(a',b',c',d')^t = \det(\theta)\, Z_\theta\, (a,b,c,d)^t$, sendo Z_θ a matriz dada pela fórmula (A.12) no Apêndice A. Fazemos a identificação direta da forma cúbica com sua quádrupla de coeficientes.

Finalmente, consideremos a classe de isomorfismo de um anel cúbico A. Fixada uma base boa $\mathcal{B}$ de A, o natural seria atribuir, à classe de equivalência de A, a classe de equivalência da forma cúbica $(p,q,r,s) = \mathcal{N}(A,\mathcal{B})$. No entanto, esta atribuição **não** é a correspondência desejada, pois se A' é um anel cúbico isomorfo ao anel A, com base boa $\mathcal{B}'$, **não** é necessariamente verdadeiro que a forma cúbica $(p',q',r',s') = \mathcal{N}(A',\mathcal{B}')$ seja $\mathrm{GL}_2(\mathbb{Z})$-equivalente à forma cúbica (p,q,r,s).

Seja $\phi(a,b,c,d) = (-b,a,-d,c)$. Atribuímos, à classe de equivalência de A, a classe de equivalência da forma cúbica $(a,b,c,d) = \phi^{-1}(p,q,r,s) = (\phi^{-1} \circ \mathcal{N})(A,\mathcal{B})$. Se A' é um anel cúbico isomorfo ao anel A, com base boa $\mathcal{B}'$, então pelo anterior existe uma única matriz $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ tal que $(p',q',r',s')^t = W_\gamma\, (p,q,r,s)^t$. Se $(a',b',c',d') = \phi^{-1}(p',q',r',s') = (\phi^{-1} \circ \mathcal{N})(A',\mathcal{B}')$, verifica-se que vale $(a',b',c',d')^t = Z_\gamma\, (a,b,c,d)^t$ (vide o Apêndice A para as contas detalhadas), o que mostra que $(\phi^{-1} \circ \mathcal{N})(A',\mathcal{B}')$ é uma forma cúbica $\mathrm{GL}_2(\mathbb{Z})$-equivalente à forma cúbica $(\phi^{-1} \circ \mathcal{N})(A,\mathcal{B})$. □

Corolário 2.5. *Existe um isomorfismo natural entre o grupo de automorfismos do anel A e o estabilizador em $\mathrm{GL}_2(\mathbb{Z})$ de alguma forma cúbica f associada ao anel A pela correspondência de Delone-Fadeev.*

Demonstração. Com as notações da prova do Teorema anterior, sejam A, A', A'' anéis cúbicos com bases boas $\mathcal{B} = (1,\alpha,\beta)$, $\mathcal{B}' = (1,\alpha',\beta')$, $\mathcal{B}'' = (1,\alpha'',\beta'')$, respectivamente. Se $Q : A'' \to A'$ e $T : A' \to A$ são isomorfismos de anéis com unidade, então as matrizes associadas $[Q]$, $[T]$ destas transformações $\mathbb{Z}$-lineares (com respeito das bases mencionadas) são da forma

$$[T] = \begin{bmatrix} 1 & u & v \\ 0 & & \\ 0 & & \gamma^t \end{bmatrix};\ [Q] = \begin{bmatrix} 1 & \hat{u} & \hat{v} \\ 0 & & \\ 0 & & \delta^t \end{bmatrix},$$

com $\gamma, \delta \in \mathrm{GL}_2(\mathbb{Z})$. Portanto a matriz associada a $TQ : A'' \to A$ (nas bases correspondentes) será

$$[T][Q] = \begin{bmatrix} 1 & \tilde{u} & \tilde{v} \\ 0 & & \\ 0 & & \gamma^t \delta^t \end{bmatrix} = \begin{bmatrix} 1 & \tilde{u} & \tilde{v} \\ 0 & & \\ 0 & & (\delta\gamma)^t \end{bmatrix}.$$

Sejam $(p, q, r, s) = \mathcal{N}(A, \mathcal{B}), (p', q', r', s') = \mathcal{N}(A', \mathcal{B}'), (p'', q'', r'', s'') = \mathcal{N}(A'', \mathcal{B}'')$, sendo $\mathcal{N}$ dado pela fórmula (2.5). Então temos $(p'', q'', r'', s'')^t = \det(\delta\gamma) W_{\delta\gamma}(p, q, r, s)^t$; por outro lado, vale

$$\begin{aligned} (p'', q'', r'', s'')^t &= \det(\delta) W_\delta (p', q', r', s')^t \\ &= \det(\delta) W_\delta \left[\det(\gamma) W_\gamma (p, q, r, s)^t \right]. \end{aligned}$$

Comparando estas duas igualdades obtemos $W_{\delta\gamma}(p, q, r, s)^t = W_\delta W_\gamma (p, q, r, s)^t$. Já que (p, q, r, s) é arbitrário (vide a Observação 2.3), concluímos a igualdade matricial $W_{\delta\gamma} = W_\delta W_\gamma$, para quaisquer $\gamma, \delta \in \mathrm{GL}_2(\mathbb{Z})$; como $W_I = I$, então em particular para qualquer $\theta \in \mathrm{GL}_2(\mathbb{Z})$ vale $(W_\theta)^{-1} = W_{\theta^{-1}}$.

Tomemos agora $A'' = A' = A$ e $\mathcal{B}'' = \mathcal{B}' = \mathcal{B}$. A cada automorfismo T do anel A atribuímos a matriz $\Gamma(T) = \gamma^{-1}$, onde $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ é a única matriz tal que $[T] = \begin{bmatrix} 1 & u & v \\ 0 & & \\ 0 & & \gamma^t \end{bmatrix}$ (na base $\mathcal{B}$). Se Q é outro automorfismo de A e $[Q] = \begin{bmatrix} 1 & u & v \\ 0 & & \\ 0 & & \gamma^t \end{bmatrix}$, então $\Gamma(TQ) = (\delta\gamma)^{-1} = \gamma^{-1}\delta^{-1} = \Gamma(T)\Gamma(Q)$. Isto mostra que γ é um homomorfismo do grupo de automorfismos de A em $\mathrm{GL}_2(\mathbb{Z})$. Se $\Gamma(T) = I$ então $[T] = \left[\begin{smallmatrix} 1 & u & v \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{smallmatrix}\right]$; as fórmulas (A.7) e (A.8) mostram que neste caso (a saber, $E = H = 1, F = G = 0$) teremos $u = v = 0$, logo $[T] = I$, o que mostra que T é neste caso o automorfismo identidade de A, e assim Γ é um homomorfismo injetivo.

Finalmente, seja (a, b, c, d) a forma cúbica associada ao par $(A, \mathcal{B})$ pela correspondência de Delone-Fadeev. Então temos $(a, b, c, d)^t = (M_\phi)^{-1}(p, q, r, s)^t$, onde $M_\phi = \left[\begin{smallmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{smallmatrix}\right]$ (vide o final do Apêndice A). Um elemento $\theta \in \mathrm{GL}_2(\mathbb{Z})$ está no estabilizador da forma cúbica (a, b, c, d) precisamente quando vale $(a, b, c, d)^t = \det(\theta) Z_\theta (a, b, c, d)^t$. Usando a igualdade $M_\phi Z_\theta = W_\theta M_\phi$, a condição anterior equivale a termos $(p, q, r, s)^t = \det(\theta) W_\theta (p, q, r, s)^t$, ou ainda, $(p, q, r, s)^t = \det(\theta^{-1}) W_{\theta^{-1}} (p, q, r, s)^t$. Esta última condição equivale a termos $\theta = \Gamma(T)$, para algum automorfismo T do anel A (a saber, a transformação $\mathbb{Z}$-linear $T : A \to A$ com matriz associada $[T] = \begin{bmatrix} 1 & u & v \\ 0 & & \\ 0 & & (\theta^{-1})^t \end{bmatrix}$). □

Lema 2.6. *Se A é domínio e M é um A-módulo livre, então M não possui torção, ou seja, se $r \in A - \{0\}$ e $m \in M - \{0\}$, então $rm \neq 0$.*

Demonstração. Seja $\{v_i\}_{i \in I}$ uma A-base de M. Se $m \in M - \{0\}$, então $m = \sum_{i \in I} r_i v_i$, com $r_i \in A$ e $r_j \neq 0$ para algum j. Se $r \in A - \{0\}$, então $rm = \sum_{i \in I} (r r_i) v_i$ e $r r_j \neq 0$ pois A é domínio, logo $rm \neq 0$. □

Corolário 2.7. *Um anel cúbico é um domínio (ou seja, uma ordem cúbica) se, e somente se, a forma cúbica correspondente é irredutível sobre* $\mathbb{Q}$.

Demonstração. Se $p(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$ for redutível sobre $\mathbb{Q}$, então possui um fator linear homogêneo $a_1x + b_1y$, o qual após uma mudança de variáveis em $\mathrm{GL}_2(\mathbb{Z})$ podemos converter no fator y [§]. Assim, podemos supor $a = 0$, e com as notações do Teorema 2.4 teremos $(p,q,r,s) = \phi(0,b,c,d) = (-b,0,-d,c)$, logo $q = 0$, e isto implica $\alpha\beta = qr = 0$ por (2.5), portanto A não é um domínio.

Reciprocamente, sejam ω, θ elementos não nulos de A com $\omega\theta = 0$. Pelo teorema de Cayley-Hamilton (vide (ATIYAH; MACDONALD, 1969), Proposition 2.4) existem $b_1, b_2, b_3 \in \mathbb{Z}$ tais que $\omega^3 + b_1\omega^2 + b_2\omega + b_3 = 0$. Multiplicando por θ obtemos $b_3\omega = 0$, logo $b_3 = 0$ pelo Lema 2.6, de modo que $\omega D = 0$, sendo $D = \omega^2 + b_1\omega + b_2$. Se $D = 0$, então da igualdade $\theta D = 0$ obtemos $b_2 = 0$, e assim $\omega^2 = -b_1\omega$; se $D \neq 0$ então $D(D - b_2) = D(\omega^2 + b_1\omega) = \omega D(\omega + b_1) = 0$, logo $D^2 = b_2 D$. Tudo isto mostra que existem $\alpha, \beta \in A$ não nulos tais que $\alpha\beta = 0$ e $\alpha^2 = d\alpha$, com $d \in \mathbb{Z}$.

Afirmamos que 1 e α são $\mathbb{Z}$-linearmente independentes. Com efeito, sejam $r, s \in \mathbb{Z}$ tais que $r \cdot 1 + s\alpha = 0$. Multiplicando por β obtemos $r\beta = 0$, logo $r = 0$ pelo Lema 2.6. Assim $s\alpha = 0$, logo $s = 0$ pelo Lema 2.6.

Seja $(1, \theta_2, \theta_3)$ uma $\mathbb{Z}$-base de A. Se $\alpha = c_1 \cdot 1 + c_2\theta_2 + c_3\theta_3$, com $c_1, c_2, c_3 \in \mathbb{Z}$, sejam $\alpha_1 = c_2\theta_2 + c_3\theta_3$ e $c = \mathrm{MDC}(c_2, c_3)$. Se $c_2 = cc_2'$, $c_3 = cc_3'$ então $\mathrm{MDC}(c_2', c_3') = 1$, logo existem $p, q \in \mathbb{Z}$ tais que $pc_1' + qc_2' = 1$. Portanto os elementos $\alpha_2 = c_2'\theta_2 + c_3'\theta_3$ e $\theta = -q\theta_2 + p\theta_3$ satisfazem

$$\begin{bmatrix} 1 \\ \alpha_2 \\ \theta \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & c_2' & c_3' \\ 0 & -q & p \end{bmatrix} \begin{bmatrix} 1 \\ \theta_2 \\ \theta_3 \end{bmatrix},$$

e como $\det \begin{bmatrix} 1 & 0 & 0 \\ 0 & c_2' & c_3' \\ 0 & -q & p \end{bmatrix} = 1$, segue que $(1, \alpha_2, \theta)$ é uma $\mathbb{Z}$-base de A. Se $\alpha_2\theta = p \cdot 1 + q\alpha_2 + r\theta$, então $\alpha_3 = \alpha_2 - r \cdot 1$ e $\mu = \theta - q \cdot 1$ satisfazem

$$\alpha_3\mu = p + rq = n \in \mathbb{Z}, \tag{2.7}$$

logo $\mathcal{B}' = (1, \alpha_3, \mu)$ é $\mathbb{Z}$-base boa. Ora, temos $\alpha = c_1 \cdot 1 + \alpha_1 = c_1 \cdot 1 + c\alpha_2 = c\alpha_3 + k \cdot 1$, onde $k = cr + c_1$. De $\alpha^2 = d\alpha$ segue $(c\alpha_3 + k \cdot 1)^2 = d(c\alpha_3 + k \cdot 1)$, ou seja

$$c^2\alpha_3^2 + k_1\alpha_3 + k_2 \cdot 1 = 0, \tag{2.8}$$

onde $k_1 = c(2k - d)$ e $k_2 = k^2 - dk$. Multiplicando 2.8 por μ e usando 2.7 obtemos $0 = c^2 n\alpha_3 + k_1 n \cdot 1 + k_2\mu$. Como $(1, \alpha_3, \mu)$ é uma $\mathbb{Z}$-base, segue que $k_1 n = c^2 n = k_2 = 0$.

§ De fato, multiplicando por uma constante adequada podemos supor $\mathrm{MDC}(a_1, b_1) = 1$, $\log 0\, pa_1 + qb_1 = 1$ para alguns $p, q \in \mathbb{Z}$. Se $\theta = \begin{bmatrix} q & a_1 \\ -p & b_1 \end{bmatrix}$ então $\det(\theta) = 1$ e $\theta\binom{0}{1} = \binom{a_1}{b_1}$, logo $\gamma = (\theta^t)^{-1}$ satisfaz $\gamma \in \mathrm{GL}_2(\mathbb{Z})$ e $(0,1) = (a_1, b_1)\gamma$, como desejado.

Como $c \neq 0$ então necessariamente $n = 0$, isto é, $\alpha_3 \mu = 0$. Finalmente, se $(p', q', r', s') = \mathcal{N}(A, \mathcal{B}')$, então por 2.5 temos $q'r' = 0$. A forma binária cúbica (a', b', c', d') associada ao par $(A, \mathcal{B}')$ é $\phi^{-1}(p', q', r', s') = -\phi(p', q', r', s') = (q', -p', s', -r')$, logo $a' = 0$ ou $d' = 0$. Assim, a forma cúbica $a'x^3 + b'x^2y + c'xy^2 + d'$ será múltiplo de x ou y, e portanto redutível. □

Proposição 2.8. *O discriminante $\Delta(p)$ de uma forma binária cúbica $p(x, y)$ é igual ao discriminante $\mathcal{D}_A$ do anel cúbico correspondente A.*

Demonstração. Sejam $\mathrm{Tr} : A \to \mathbb{Z}$ a forma do traço e $\mathcal{B} = (1, \alpha, \beta)$ uma $\mathbb{Z}$-base boa de A. Então temos

$$\mathcal{D}_A = \det \begin{bmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\alpha) & \mathrm{Tr}(\beta) \\ \mathrm{Tr}(\alpha) & \mathrm{Tr}(\alpha^2) & \mathrm{Tr}(\alpha\beta) \\ \mathrm{Tr}(\beta) & \mathrm{Tr}(\alpha\beta) & \mathrm{Tr}(\beta^2) \end{bmatrix}. \tag{2.9}$$

Se $(p, q, r, s) = \mathcal{N}(A, \mathcal{B})$, então $(a, b, c, d) = \phi^{-1}(p, q, r, s) = (q, -p, s, -r)$. Das fórmulas (2.5) segue $\alpha \cdot 1 = 0 \cdot 1 + 1 \cdot \alpha + 0 \cdot \beta$, $\alpha \cdot \alpha = -qs \cdot 1 + p \cdot \alpha + q \cdot \beta$, $\alpha \cdot \beta = qr \cdot 1 + 0 \cdot \alpha + 0 \cdot \beta$, e portanto $\mathrm{Tr}(\alpha) = \mathrm{Tr} \begin{bmatrix} 0 & -qs & qr \\ 1 & p & 0 \\ 0 & q & 0 \end{bmatrix} = p = -b$; similarmente obtemos $\mathrm{Tr}(\beta) = \mathrm{Tr} \begin{bmatrix} 0 & qr & -pr \\ 0 & 0 & r \\ 1 & 0 & s \end{bmatrix} = s = c$. Ainda, obviamente teremos $\mathrm{Tr}(1) = 3 \cdot 1 = 3$ e $\mathrm{Tr}(\alpha\beta) = 3 \cdot \alpha\beta = 3qr = -3ad$. Finalmente, usando estes valores e aproveitando a $\mathbb{Z}$-linearidade do traço, obtemos $\mathrm{Tr}(\alpha^2) = -qs\,\mathrm{Tr}(1) + p\,\mathrm{Tr}(\alpha) + q\,\mathrm{Tr}(\beta) = -3qs - bp + cq = -3ac + b^2 + ac = b^2 - 2ac$, e similarmente $\mathrm{Tr}(\beta^2) = c^2 - 2bd$. Portanto

$$\mathcal{D}_A = \det \begin{bmatrix} 3 & -b & c \\ -b & b^2 - 2ac & -3ad \\ c & -3ad & c^2 - 2bd \end{bmatrix}.$$

Por outro lado, o discriminante Δ da forma cúbica $p(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ é dado por

$$\Delta = b^2c^2 + 18abcd - 4ac^3 - 4b^3d - 27a^2d^2\,.$$

Como $\mathcal{D}_A = \Delta$, o resultado segue. □

2.2 Hessianas e *Shapes*

Seja $p(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ uma forma binária cúbica inteira. Denominamos *hessiana de p* à forma binária quadrática integral

$$H_p(x, y) = -\frac{1}{4} \det \begin{bmatrix} \dfrac{\partial p(x,y)}{\partial x^2} & \dfrac{\partial p(x,y)}{\partial x \partial y} \\ \dfrac{\partial p(x,y)}{\partial y \partial x} & \dfrac{\partial p(x,y)}{\partial y^2} \end{bmatrix}.$$

A hessiana goza das seguintes propriedades:

Proposição 2.9. *Se duas formas binárias cúbicas f e g são equivalentes por um elemento de* $\mathrm{GL}_2(\mathbb{Z})$*, então as hessianas H_f e H_g correspondentes são equivalentes pelo mesmo elemento, sem o fator do determinante. Para uma forma binária cúbica f temos $\Delta(H_f) = -3 \cdot \Delta(f)$.*

Demonstração. Seja $g(x,y) = \frac{1}{\det(\gamma)} \cdot f\big((x,y)\cdot\gamma\big)$, onde $\gamma = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right]$. Fazendo $u = Ax + Cy$ e $v = Bx + Dy$ podemos escrever $g(x,y) = f(u,v)$, e usando a regra da cadeia obtemos

- $\dfrac{\partial^2 g}{\partial x^2} = \dfrac{1}{\det\gamma}\left(A^2\,\dfrac{\partial^2 f}{\partial u^2} + 2AB\,\dfrac{\partial^2 f}{\partial u\partial v} + B^2\,\dfrac{\partial^2 f}{\partial v^2}\right)$;
- $\dfrac{\partial^2 g}{\partial x\partial y} = \dfrac{1}{\det\gamma}\left(AC\,\dfrac{\partial^2 f}{\partial u^2} + (AD+BC)\,\dfrac{\partial^2 f}{\partial u\partial v} + BD\,\dfrac{\partial^2 f}{\partial v^2}\right)$;
- $\dfrac{\partial^2 g}{\partial y^2} = \dfrac{1}{\det\gamma}\left(C^2\,\dfrac{\partial^2 f}{\partial u^2} + 2CD\,\dfrac{\partial^2 f}{\partial u\partial v} + D^2\,\dfrac{\partial^2 f}{\partial v^2}\right)$.

Usando estas igualdades, junto com a igualdade $\det(\gamma)^2 = 1$, obtemos

$$\begin{aligned}
H_g(x,y) &= -\frac{1}{4}\cdot\left[\frac{\partial^2 g}{\partial x^2}\cdot\frac{\partial^2 g}{\partial y^2} - \left(\frac{\partial^2 g}{\partial x\partial y}\right)^2\right] \\
&= -\frac{1}{4}\left(A^2\,\frac{\partial^2 f}{\partial u^2} + 2AB\,\frac{\partial^2 f}{\partial u\partial v} + B^2\,\frac{\partial^2 f}{\partial v^2}\right)\cdot\left(C^2\,\frac{\partial^2 f}{\partial u^2} + 2CD\,\frac{\partial^2 f}{\partial u\partial v} + D^2\,\frac{\partial^2 f}{\partial v^2}\right) \\
&\quad + \frac{1}{4}\left(AC\,\frac{\partial^2 f}{\partial u^2} + (AD+BC)\,\frac{\partial^2 f}{\partial u\partial v} + BD\,\frac{\partial^2 f}{\partial v^2}\right)^2 \\
&= -\frac{1}{4}\left[(AD-BC)^2\,\frac{\partial^2 f}{\partial u^2}\cdot\frac{\partial^2 f}{\partial v^2} - \big[(AD)^2 + 2ABCD + (BC)^2 - 4ABCD\big]\frac{\partial^2 f}{\partial u\partial v}\right] \\
&= -\frac{1}{4}\left(\frac{\partial^2 f}{\partial u^2}\cdot\frac{\partial^2 f}{\partial v^2} - \frac{\partial^2 f}{\partial u\partial v}\right) \\
&= H_f(u,v) \\
&= H_f\big((x,y)\cdot\gamma\big)\,.
\end{aligned}$$

Por outro lado, se $f(x,y) = ax^3 + bx^2y + cxy^2 + dy^3$, então

$$\begin{aligned}
H_f &= -\frac{1}{4}\det\begin{bmatrix} 6ax + 2bx & 2bx + 2cy \\ 2bx + 2cy & 2cx + 6dy \end{bmatrix} \\
&= (b^2 - 3ac)x^2 + (bc - 9ad)xy + (c^2 - 3bd)y^2\,. \qquad (2.10)
\end{aligned}$$

Fazendo $P = b^2 - 3ac$, $Q = bc - 9ad$ e $R = c^2 - 3bd$ temos, por definição de discriminante de formas binárias quadráticas, $\Delta(H_f) = Q^2 - 4PR$, e portanto

$$\begin{aligned}
\Delta(H_f) &= (bc - 9ad)^2 - 4(b^2 - 3ac)(c^2 - 3bd) \\
&= -3(b^2c^2 + 18abcd - 4ac^3 - 4db^3 - 27a^2d^2) = -3\Delta(f)\,. \qquad \square
\end{aligned}$$

Definição 2.10. Definimos o *shape* $Q(x, y)$ do anel A como a classe de $\mathrm{GL}_2(\mathbb{Z})$-equivalência da parte primitiva da forma binária quadrática inteira $\mathrm{Tr}(z^2)$, onde $z \in \mathbb{Z}+3A$ e $\mathrm{Tr}(z) = 0$ [†].

Proposição 2.11. *Seja A um anel correspondente à forma binária cúbica $p(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ através da correspondência de Delone-Fadeev. Então a classe de $\mathrm{GL}_2(\mathbb{Z})$-equivalência da parte primitiva da hessiana $H_p(x, y)$ corresponde ao* shape *de A.*

Demonstração. Considere o conjunto $S = \{z \in \mathbb{Z} + 3A : \mathrm{Tr}(z) = 0\}$. Afirmamos que vale $S = \{3r - \mathrm{Tr}(r) : r \in A\}$. Com efeito, temos $S = \{n + 3r : n \in \mathbb{Z},\ r \in A, 3n + 3\,\mathrm{Tr}(r) = 0\} \subseteq \{3r - \mathrm{Tr}(r) : r \in A\}$. Reciprocamente, se $r \in A$ e $t = -\mathrm{Tr}(r) + 3r \in \mathbb{Z} + 3A$, então $\mathrm{Tr}(t) = \mathrm{Tr}\big(-\mathrm{Tr}(r)\big) + 3\,\mathrm{Tr}(r) = -3\,\mathrm{Tr}(r) + 3\,\mathrm{Tr}(r) = 0$.

Assim, tomando uma $\mathbb{Z}$-base boa $(1, \alpha, \beta)$ de A e $z \in S$, existem $p, x, y \in \mathbb{Z}$ tais que $z = 3(p \cdot 1 + x \cdot \alpha + y \cdot \beta) - \mathrm{Tr}(p \cdot 1 + x \cdot \alpha + y \cdot \beta) = 3x\alpha + 3y\beta - x\mathrm{Tr}(\alpha) - y\mathrm{Tr}(\beta)$, logo $z = x\big(3\alpha - \mathrm{Tr}(\alpha)\big) + y\big(3\beta - \mathrm{Tr}(\beta)\big) = x(3\alpha + b) + y(3\beta - c)$. Elevando ao quadrado obtemos

$$\begin{aligned} z^2 &= (3\alpha + b)^2x^2 + 2(3\alpha + b)(3\beta - c)xy + (3\beta - c)^2y^2 \\ &= (9\alpha^2 + 6b\alpha + b^2)x^2 + 2(9\alpha\beta - 3c\alpha + 3b\beta - bc)xy + (9\beta^2 - 6c\beta + c^2)y^2\,. \end{aligned}$$

Usando os cálculos feitos na prova da Proposição 2.8, referentes ao traço dos elementos, obtemos

$$\begin{aligned} \mathrm{Tr}(z^2) &= \big(9\,\mathrm{Tr}(\alpha^2) + 6b\,\mathrm{Tr}(\alpha) + 3b^2\big)x^2 + 2\big(9\,\mathrm{Tr}(\alpha\beta) - 3c\,\mathrm{Tr}(\alpha) + 3b\,\mathrm{Tr}(\beta) - 3bc\big)xy \\ &\quad + \big(9\,\mathrm{Tr}(\beta^2) - 6c\,\mathrm{Tr}(\beta) + 3c^2\big)y^2 \\ &= \big(9(b^2 - 2ac) - 3b^2\big)x^2 + 2(-27ad + 3bc)xy + \big(9(c^2 - 2bd) - 3c^2\big)y^2 \\ &= 6(b^2 - 3ac)x^2 + 6(bc - 9ad)xy + 6(c^2 - 3bd)y^2 \\ &= 6H_p(x, y)\,. \end{aligned}$$

Portanto $\mathrm{Tr}(z^2)$ e $H_p(x, y)$ possuem a mesma parte primitiva. □

[†] Uma forma inteira é dita *primitiva* quando seus coeficientes são primos relativos. Desta forma, se $\mathrm{Tr}(z^2) = ax^2 + bxy + cy^2$ e $\mathrm{MDC}(a, b, c) = d$, então sua parte primitiva será $Q(x, y) = \frac{a}{d}x^2 + \frac{b}{d}xy + \frac{c}{d}y^2$.

3 ORDENS CÚBICAS COM GRUPO DE AUTOMORFISMO C_3

Neste capítulo será provado o resultado principal do trabalho. A prova requer certos preliminares algébricos adicionais, os quais serão apresentados nas seções a seguir.

3.1 Formas quadráticas binárias reduzidas

Nesta seção introduzimos a noção de forma binária quadrática reduzida, e a utilizamos para demonstrar que a hessiana de uma forma binária cúbica com automorfismo de ordem 3 é equivalente a um múltiplo inteiro da forma binária quadrática $Q(x, y) = x^2 + xy + y^2$.

Definição 3.1. Uma forma binária quadrática $f(x, y) = Px^2 + Qxy + Ry^2$ é dita *reduzida* se $|Q| \leq |P| \leq |R|$.

Dizemos que duas formas binárias quadráticas $f(x, y) = Px^2 + Qxy + Ry^2$ e $f'(x, y) = P'x^2 + Q'xy + R'y^2$ são $\mathrm{GL}_2(\mathbb{Z})$-*equivalentes (resp.* $\mathrm{SL}_2(\mathbb{Z})$-*equivalentes)*, quando existe $\left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{Z})$ (resp. $\mathrm{SL}_2(\mathbb{Z})$) tal que $f'(x, y) = f\big((x, y) \cdot \gamma\big) = f(Ax + Cy, Bx + Dy)$, ou seja,

$$\left.\begin{aligned} P' &= PA^2 + QAB + RB^2\,; \\ Q' &= 2PAC + Q(AD + BC) + 2RBD\,; \\ R' &= PC^2 + QCD + RD^2\,. \end{aligned}\right\} \tag{3.1}$$

Dada $f(x, y) = Px^2 + Qxy + Ry^2$ definimos a matriz auxiliar $N_f = \left[\begin{smallmatrix} 2P & Q \\ Q & 2R \end{smallmatrix}\right]$. Note que as igualdades que determinam a equivalência das formas f e f' são equivalentes à igualdade matricial $N_{f'} = \gamma N_f \gamma^t$. Por outro lado, lembramos que o discriminante da forma quadrática f é definido como o valor $\Delta(f) = Q^2 - 4PQ$, ou seja, $\Delta(f) = -\det(N_f)$. Portanto $\Delta(f') = -\det(N_{f'}) = -\det(N_f)\det(\gamma)\det(\gamma^t) = -\det(N_f)$, o que mostra que o discriminante é invariante por $\mathrm{GL}_2(\mathbb{Z})$-equivalência.

Teorema 3.2. *Toda forma binária quadrática de discriminante negativo é* $\mathrm{SL}_2(\mathbb{Z})$*-equivalente a uma forma reduzida de mesmo discriminante.*

Demonstração. Seja $f(x, y) = Px^2 + Qxy + Ry^2$ uma forma binária quadrática com discriminante negativo, ou seja $Q^2 - 4PR < 0$. Como $0 \leq Q^2 < 4PR$, concluímos que P e R possuem mesmo sinal. Se f não é reduzida, seja $\delta \in \mathbb{Z}$ tal que $|\delta - \frac{Q}{2R}| \leq \frac{1}{2}$, logo vale $|-Q + 2R\delta| \leq |R|$. Tomando $\gamma = \left[\begin{smallmatrix} 0 & 1 \\ -1 & \delta \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$ e usando as equações 3.1, temos que f

é equivalente à forma $f'(x,y) = P'x^2 + Q'xy + R'y^2$, onde $P' = R$, $Q' = -Q + 2\delta R$, $R' = P - Q\delta + R\delta^2$; note que $|Q'| \leq |R| = |P'|$. Assim, podemos supor $|Q| \leq |P|$, e procedemos agora por indução em $|P|$: obviamente $|P| \leq |R|$ se $|P| = 0$. Seja $k \geq 1$ tal que toda forma quadrática f com $|P| < k$ é equivalente a uma forma quadrática reduzida. Se uma forma f satisfaz $|P| > |R|$, então aplicando o processo anterior encontraremos uma forma f' equivalente a f tal que $|P'| = |R'| < |P|$, logo pela hipótese de indução f' será equivalente a uma forma reduzida, e assim o será f. □

Teorema 3.3. *Uma forma quadrática binária $f(x,y) = Px^2 + Qxy + Ry^2$ é fixada por uma matriz $\tau \in \mathrm{SL}_2(\mathbb{Z})$ de ordem 3 se, e somente se, existe $n \in \mathbb{Z}$ tal que f é $\mathrm{SL}_2(\mathbb{Z})$-equivalente à forma $\ell(x,y) = nx^2 + nxy + ny^2$.*

Demonstração. Seja $S = \left[\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbb{Z})$. Então $S^{-1} = \left[\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right]$, e S, S^{-1} têm ordem 3 em $\mathrm{SL}_2(\mathbb{Z})$. Suponha que f é $\mathrm{GL}_2(\mathbb{Z})$-equivalente a $\ell(x,y) = nx^2 + nxy + ny^2$, com $n \in \mathbb{Z}$, digamos $N_\ell = \gamma N_f \gamma^t$, com $\gamma \in \mathrm{GL}_2(\mathbb{Z})$. É fácil ver que S fixa ℓ, isto é, $N_\ell = SN_\ell S^t$, e assim $N_f = (\gamma^{-1}S\gamma)N_f(\gamma^{-1}S\gamma)^t$, logo f é fixada por $\gamma^{-1}S\gamma \in \mathrm{SL}_2(\mathbb{Z})$, a qual, por ser conjugada a S, também terá ordem 3.

Reciprocamente, suponha que f é fixada por $\tau \in \mathrm{SL}_2(\mathbb{Z})$ de ordem 3, digamos $\tau = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right]$. Se $a = \mathrm{Tr}(\tau) = A + D$, então o polinômio característico de τ será $p(x) = x^2 - ax + 1$. Ora, temos $x^3 - 1 = p(x)(x + a) + (a + 1)\big((a-1)x - 1\big)$. Avaliando em τ e lembrando que τ tem ordem 3 concluímos que $(a+1)\big((a-1)\tau - I\big) = 0$; se fosse $(a-1)\tau = I$, após elevar ao cubo obteríamos $(a-1)^3 I = I$, logo $(a-1)^3 = 1$. Portanto $a = 2$, e assim $I = (a-1)\tau = \tau$, o que contradiz o fato de τ ter ordem 3. Isto mostra que vale necessariamente $a = A + D = -1$. Isto será usado na prova do fato a seguir, que será deixada para o final do argumento.

Afirmação 3.4. Existe $g \in \mathrm{SL}_2(\mathbb{Z})$ tal que $\tau = gTg^{-1}$, onde $T \in \{S, S^{-1}\}$.

Da igualdade $N_f = \tau N_f \tau^t$ junto com o resultado da Afirmação acima obtemos $(gTg^{-1})N_f(gTg^{-1})^t = N_f$. Se $f'(x,y) = f\big((x,y)\cdot g^{-1}\big)$, então $N_{f'} = g^{-1}N_f(g^{-1})^t = \left[\begin{smallmatrix} 2P' & Q' \\ Q' & 2R' \end{smallmatrix}\right]$, e a igualdade anterior se converte em $TN_{f'}T^t = N_{f'}$; em particular também vale $T^{-1}N_{f'}(T^{-1})^t = T^{-1}\big[TN_{f'}T^t\big](T^{-1})^t = N_{f'}$. Como $T = S$ ou $T^{-1} = S$, concluímos que vale incondicionalmente $SN_{f'}S^t = N_{f'}$, isto é,

$$\begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 2P' & Q' \\ Q' & 2R' \end{bmatrix}\begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix} = \begin{bmatrix} 2P' & Q' \\ Q' & 2R' \end{bmatrix},$$

que resulta em

$$\begin{bmatrix} 2R' & 2R' - Q' \\ 2R' - Q' & 2P' - 2Q' + 2R' \end{bmatrix} = \begin{bmatrix} 2P' & Q' \\ Q' & 2R' \end{bmatrix},$$

do qual claramente segue $P' = Q' = R' = n$, e assim $f\big((x,y)\cdot g^{-1}\big) = nx^2 + nxy + ny^2$.

Prova da Afirmação 3.4. A equação a resolver é $\tau g = gT$. Fazendo $g = \left[\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right]$ e tomando $T = S$, a equação fica

$$\begin{bmatrix} Ax + Bz & Ay + Bw \\ Cx + Dz & Cy + Dw \end{bmatrix} = \begin{bmatrix} y & -x - y \\ w & -z - w \end{bmatrix},$$

de onde obtemos $x = -(A+1)y - Bw, z = -Cy - (D+1)w$, e assim

$$1 = xw - yz = Cy^2 + (D - A)yw - Bw^2. \tag{3.2}$$

Reciprocamente, suponha que existem $y, w \in \mathbb{Z}$ satisfazendo (3.2), e sejam $x = -(A+1)y - Bw, z = -Cy - (D+1)w$. Lembrando que valem $AD - BC = 1$ e $A + D = -1$, obtemos

$$\begin{aligned} Ax + Bz &= -A(A+1)y - ABw - BCy - B(D+1)w \\ &= \big[-A(A+1) - BC\big]y - B(A + D + 1)w \\ &= \big[-A(A+1) + 1 - AD\big]y \\ &= \big[-A(A+1) + 1 - A(-1 - A)\big]y \\ &= y, \end{aligned}$$

e similarmente obtemos $Cx + Dz = w$, o que mostra que g é solução de $\tau g = gS$. De maneira análoga, tomando $T = S^{-1}$, a equação $\tau g = gT$ fica

$$\begin{bmatrix} Ax + Bz & Ay + Bw \\ Cx + Dz & Cy + Dw \end{bmatrix} = \begin{bmatrix} -x - y & x \\ -z - w & z \end{bmatrix},$$

de onde obtemos $x = Ay + Bw, z = Cy + Dw$, e assim

$$-1 = yz - xw = Cy^2 + (D - A)yw - Bw^2. \tag{3.3}$$

Como no caso anterior, se y, w satisfazem (3.3) e definimos $x = Ay + Bw, z = Cy + Dw$, então g satisfará $\tau g = gS^{-1}$. Isto mostra que o nosso problema equivale a mostrar que uma das equações (3.2) ou (3.3) possui uma solução com entradas inteiras.

Ora, o discriminante da forma binária quadrática $h(y, w) = Cy^2 + (D-A)yw - Bw^2$ é dado por $\Delta(h) = (D-A)^2 + 4BC = (D+A)^2 - 4AD + 4BC$. Lembrando que vale $A + D = -1$ e $AD - BC = 1$, concluímos que vale $\Delta(h) = -3$, logo pelo Teorema 3.2 a forma $h(y, w)$ será $\mathrm{SL}_2(\mathbb{Z})$-equivalente a uma forma reduzida, digamos $ay^2 + byw + cw^2$, a qual também terá discriminante -3, ou seja $4ac = b^2 + 3$, logo $ac = |ac|$, e como a forma é reduzida, isto é, $|b| \leq |a| \leq |c|$, segue que $b^2 \leq |ac|$. Daí $4b^2 \leq 4|ac| = b^2 + 3$, logo $3b^2 \leq 3$, e portanto $b = \pm 1$ (não podemos ter $b = 0$, pois isto implicaria $4ac = 3$), o que por sua vez implica $ac = 1$, e em particular, $a = \pm 1$. Evidentemente, duas formas equivalentes tomam os mesmos valores. Avaliando $ay^2 + byw + cw^2$ no ponto $(1, 0)$ concluímos que $ay^2 + byw + cw^2$ assume o valor 1 ou -1, e consequentemente h assume o valor 1 ou -1, como queríamos demonstrar. □

3.2 A ação de $\mathrm{SO}_Q(\mathbb{C})$ em $\mathbb{C}^2$

Seja $Q(x,y) = x^2 + xy + y^2$, e seja $\mathrm{SO}_Q(\mathbb{C})$ o subgrupo de elementos de $\mathrm{SL}_2(\mathbb{C})$ que preservam a forma quadrática $Q(x,y)$ pela ação natural em formas quadráticas, ou seja,

$$\mathrm{SO}_Q(\mathbb{C}) = \left\{\gamma \in \mathrm{SL}_2(\mathbb{C}) : Q(x,y) = Q\big((x,y)\cdot\gamma\big)\right\}.$$

Definimos a *ação cúbica* de $\mathrm{SO}_Q(\mathbb{C})$ em $\mathbb{C}^2$ por $\gamma \cdot v = \gamma^3 v$, onde o vetor coluna $v = (b,c)^t \in \mathbb{C}^2$, e definimos a *forma quadrática adjunta associada a* $Q(x,y)$ por $Q'(b,c) := b^2 - bc + c^2$. Finalmente, definimos $\mathrm{SO}_Q(\mathbb{C}) = \mathrm{SL}_2(\mathbb{Z}) \cap \mathrm{SO}_Q(\mathbb{C})$ e $L \subseteq \mathbb{C}^2$ o reticulado $\left\{(b,c)^t : b,c \in \mathbb{Z}^2, b \equiv c \pmod 3\right\}$.

Lema 3.5. *O grupo* $\mathrm{SO}_Q(\mathbb{Z})$ *é cíclico de ordem* 6*, gerado pela matriz* $\delta = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right]$.

Demonstração. Seja $\gamma = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right] \in \mathrm{SO}_Q(\mathbb{Z})$. As igualdades (3.1) junto com a condição $\det(\gamma) = 1$ se convertem, neste caso, nas igualdades

$$1 = A^2 + AB + B^2\,; \tag{3.4}$$
$$1 = C^2 + CD + D^2\,; \tag{3.5}$$
$$1 = 2AC + AD + BC + 2BD\,; \tag{3.6}$$
$$1 = AD - BC\,. \tag{3.7}$$

Substituindo (3.7) em (3.6) e simplificando obtemos

$$AC + BC + BD = 0\,, \tag{3.8}$$

ou, equivalentemente,

$$(A+B)(C+D) = AD\,. \tag{3.9}$$

Finalmente, as igualdades (3.4) e (3.5) podem são equivalentes a

$$(A+B)^2 = 1 + AB\,; \tag{3.10}$$
$$(C+D)^2 = 1 + CD\,; \tag{3.11}$$
$$(A+B+1)(A+B-1) = AB\,; \tag{3.12}$$
$$(C+D+1)(C+D-1) = CD\,. \tag{3.13}$$

Afirmamos que vale $ABCD = 0$. Com efeito: se $AB = 0$, acabou; note que também vale $-\gamma \in \mathrm{SO}_Q(\mathbb{Z})$, logo todas as igualdades anteriores são mantidas ao mudarmos os sinais dos valores A, B, C, D simultaneamente. Se fosse $AB > 0$, então por conta da observação anterior poderíamos supor $A, B \geq 1$; mas então teríamos $A + B + 1 \geq A + 1$ e $A + B - 1 \geq B$, logo por (3.12) teríamos $AB \geq (A+1)B > AB$, o que é um absurdo. Portanto $AB < 0$, logo por (3.10) teremos $0 \leq (A+B)^2 = 1 + AB \leq 0$. Assim $A + B = 0$,

logo por (3.9) teremos $AD = 0$, logo $D = 0$. Similarmente prova-se que $CD \leq 0$, e que $CD < 0$ implica $A = 0$.

Se $A = 0$ então (3.4) implica $B = \pm 1$, (3.7) implica $C = -B$, e (3.9) implica $D = -C = B$ logo $\gamma = \pm\left[\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right]$. Se $B = 0$ então (3.4) implica $A = \pm 1$, o que junto com (3.8) implica $C = 0$, e (3.7) implica $D = A$, logo $\gamma = \pm I$. Se $C = 0$ então (3.5) implica $D = \pm 1$, o que junto com (3.8) implica $B = 0$, e (3.7) implica $A = D$, logo $\gamma = \pm I$. Finalmente, se $D = 0$ então (3.5) implica $C = \pm 1$, (3.7) implica $B = -C$, e (3.9) implica $A = -B = C$, logo $\gamma = \pm\left[\begin{smallmatrix} 1 & -1 \\ 1 & 0 \end{smallmatrix}\right]$. Isto prova que $\mathrm{SO}_Q(\mathbb{Z})$ é um grupo de ordem 6. Ainda, o elemento $\delta = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right]$ satisfaz $\delta^2 - \delta + I = 0$ (pelo teorema de Cayley-Hamilton), isto é, $\delta^2 = \delta - I \neq I$, logo $\delta^3 = \delta^2 - \delta = -I$, e isto mostra que δ tem ordem 6 em $\mathrm{SO}_Q(\mathbb{Z})$. □

Teorema 3.6. *Existe uma bijeção natural entre o conjunto das $\mathrm{SO}_Q(\mathbb{Z})$-órbitas de vetores não nulos $(b, c)^t \in L$ e os anéis A que são C_3-cúbicos orientados. Sob esta bijeção vale $\mathcal{D}(A) = Q'(b, c)^2$.*

Demonstração. Seja A um anel C_3-cúbico, com automorfismo T de ordem 3. Seja $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ uma forma binária cúbica correspondente a A pela correspondência de Delone-Faddeev, digamos a forma cúbica associada ao par $(A, \mathcal{B})$, sendo $\mathcal{B}$ uma base boa fixada de A. Então a matriz associada a T segundo esta base é da forma $[T] = \begin{bmatrix} 1 & u & v \\ 0 & & \\ 0 & & \gamma^t \end{bmatrix}$, para algum $\gamma \in \mathrm{GL}_2(\mathbb{Z})$. Como a ordem de γ também será igual a 3, então de fato vale $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Pelo Corolário 2.5 temos que γ fixa f, logo γ também fixa H_f, pela Proposição 2.9. Portanto, pelo Teorema 3.3 temos que H_f é $\mathrm{SL}_2(\mathbb{Z})$-equivalente à forma binária quadrática nQ, para algum inteiro não nulo n.

Assim, após uma mudança de base, podemos assumir $H_f = nQ$, e portanto $n = b^2 - 3ac = bc - 9ad = c^2 - 3bd$ pela fórmula (2.10). Se $bc \neq 0$, então $a = \frac{b^2 - n}{3c}$ e $d = \frac{c^2 - n}{3b}$, logo $n = bc - 9ad = bc - \frac{(b^2 - n)(c^2 - n)}{bc}$. Assim, teremos $nbc = (bc)^2 - (b^2 - n)(c^2 - n)$, a qual se reduz a $b^2 - bc + c^2 = Q'(b, c) = n$. Usando esta igualdade nas igualdades originais obtemos $a = \frac{b^2 - n}{3c} = \frac{bc - c^2}{3c} = \frac{b - c}{3}$, e similarmente $d = \frac{c - b}{3}$.

Ora, se $b = 0$, então a igualdade $H_f = nQ$ vira $n = -3ac = -9ad = c^2$, logo $a = -\frac{c}{3} = \frac{b - c}{3}$ e $d = \frac{c}{3} = \frac{c - b}{3}$, e as mesmas igualdades sobre a e d valem quando $c = 0$. Finalmente, temos $a = \frac{b - c}{3} \in \mathbb{Z}$, logo $(b, c) \in L$.

Reciprocamente, se $(b, c)^t \in L$ é não nulo, então definindo $a = \frac{b - c}{3}$, $d = \frac{c - b}{3}$ e $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, então os cálculos na prova da implicação anterior mostram que vale $H_f = nQ$, onde $n = Q'(b, c)$. Se $\theta = \left[\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right]$, então $\theta \in \mathrm{SL}_2(\mathbb{Z})$ tem ordem 3. A matriz Z_θ da fórmula (A.12) será igual a $\left[\begin{smallmatrix} -1 & 1 & -1 & 1 \\ -3 & 2 & -1 & 0 \\ -3 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{smallmatrix}\right]$, e é fácil verificar que vale $Z_\theta(a, b, c, d)^t = (a, b, c, d)^t$, logo pela igualdade (A.11) concluímos que a forma cúbica f é fixada por θ, e assim o anel A possuirá um automorfismo de ordem 3, pela correspondência de Delone-Fadeev.

Agora suponha que as formas f e f' correspondem, respectivamente, a $(b,c)^t$ e $(b',c')^t \in L$. Pelo anterior temos $H_f(x,y) = mQ(x,y)$ e $H_{f'}(x,y) = nQ(x,y)$, onde $m = Q'(b,c), n = Q'(b',c')$. Se f e f' são $\mathrm{SL}_2(\mathbb{Z})$-equivalentes, digamos $f'(x,y) = f\big((x,y)\cdot\gamma\big)$, com $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, então pela Proposição 2.9 temos $H_{f'}(x,y) = H_f\big((x,y)\cdot\gamma\big)$, isto é, $nQ(x,y) = mQ\big((x,y)\cdot\gamma\big)$. Como Q é definida positiva (ou seja, $Q(r,s) > 0$ para quaisquer inteiros r,s com $r \neq 0$ ou $s \neq 0$), segue que m e n possuem o mesmo sinal; também, como a forma Q assume o valor 1, então valem $m \mid n$ e $n \mid m$. Isto prova que vale $m = n$, logo $Q(x,y) = Q\big((x,y)\cdot\gamma\big)$, o que prova que vale $\gamma \in \mathrm{SO}_Q(\mathbb{Z})$. O recíproco é óbvio, pois $\mathrm{SO}_Q(\mathbb{Z}) \subseteq \mathrm{SL}_2(\mathbb{Z})$ por definição.

Lembramos que valem $a = -d = (b-c)/3$. Seja $f\big((x,y)\cdot\gamma\big) = a'x^3 + b'x^2y + c'xy^2 + d'y^3$, com $\gamma \in \mathrm{SO}_Q(\mathbb{Z})$. Se $\delta = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right]$, então pelo Lema 3.5 (e sua prova) temos $\delta^3 = -I$ e $\gamma = \delta^k$ para algum $k \geq 0$, logo $\gamma^3 = (\delta^3)^k = (-I)^k = (-1)^k I$, e assim $\gamma^3(b,c)^t = (-1)^k(b,c)^t$. Por outro lado, a matriz Z_δ da fórmula (A.12) será igual a $\left[\begin{smallmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 3 \\ 0 & 1 & -2 & 3 \\ -1 & 1 & -1 & 1 \end{smallmatrix}\right]$, e verifica-se que vale $Z_\delta(a,b,c,d)^t = -(a,b,c,d)^t$, logo

$$\begin{aligned}(a',b',c',d')^t &= Z_\gamma(a,b,c,d)^t \\ &= Z_{\delta^k}(a,b,c,d)^t \\ &= Z_\delta^k(a,b,c,d)^t \\ &= (-1)^k(a,b,c,d)^t\,,\end{aligned}$$

o que implica $(b',c')^t = (-1)^k(b,c)^t = \gamma^3(b,c)^t$. Fica provado então que f e f' são $\mathrm{SO}_Q(\mathbb{Z})$-equivalentes precisamente quando $(b,c)^t$ e $(b',c')^t$ são $\mathrm{SO}_Q(\mathbb{Z})$ sob a ação cúbica. Finalmente, pelas Proposições 2.8, 2.9 e 2.11 temos $\mathcal{D}_A = \Delta(f) = -\frac{1}{3}\Delta(H_f)$. Como $H_f(x,y) = rx^2 + sxy + ty^2$, sendo $r = s = t = n = Q'(b,c)$, segue que $\Delta(H_f) = s^2 - 4rt = -3n^2$. □

3.3 O número de ordens cúbicas C_3 com discriminante limitado

Nesta seção provaremos o teorema principal em estudo. Primeiro mostraremos que o número de formas redutíveis $f(x,y)$ que corresponde a anéis C_3 é desprezível.

Lema 3.7. *O número de classes de* $\mathrm{SL}_2(\mathbb{Z})$*-equivalência de formas binárias cúbicas redutíveis com hessiana múltipla de* $Q(x,y) = x^2 + xy + y^2$*, e discriminante menor que* X*, é* $O(X^{1/4})$.

Demonstração. Daremos uma estimativa superior do número de classes de $\mathrm{SL}_2(\mathbb{Z})$-equivalência de formas redutíveis f de discriminante menor que X com hessiana múltipla de Q. Basta primeiro contar as formas primitivas f, e depois somar sobre todos os conteúdos positivos possíveis para f. Qualquer forma primitiva redutível f com

hessiana nQ tem um fator linear $gx + hy$ como g e h inteiros primos entre si. Além disso, devido o automorfismo de ordem 3 dado pela matriz $\theta = \left[\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right]$ (vide a prova do Teorema 3.6), obtemos que f tem 3 fatores lineares primitivos, a saber, os obtidos através da aplicação sucessiva de θ ao fator $gx + hy$. Como $(x, y) \cdot \theta = (-x - y, x)$ e $(x, y) \cdot \theta^2 = (y, -x - y)$, segue que

$$f(x, y) = (gx + hy)\big((h - g)x - gy\big)\big(-hx + (g - h)y\big)\,,$$

ou seja,

$$f(x, y) = gh(g - h)x^3 + (-g^3 + 3g^2h - h^3)x^2y + (-g^3 + 3gh^2 - h^3)xy^2 - gh(g - h)y^3.$$

Computando o discriminante de f encontramos

$$\Delta(f) = (g^2 - gh + h^2)^6 = Q'(g, h)^6.$$

Assim, se $\Delta(f) < X$, então $Q'(g, h) < X^{1/6}$, e portanto o número total de valores para o par (g, h), e consequentemente para f, é no máximo $O(X^{1/6})$.

A fim de contar o número total de formas f, não apenas as primitivas, somamos sobre todos os possíveis conteúdos c de f. Uma vez que $\Delta(f/c) = \Delta(f)/c^4$, temos

$$\begin{aligned}
\frac{1}{X^{1/4}}\left|\sum_{c=1}^{X^{1/4}} O\big((X/c^4)^{1/6}\big)\right| &= \left|\sum_{c=1}^{X^{1/4}} \frac{O(X^{1/6}/c^{2/3})}{X^{1/4}}\right| \\
&= \left|\sum_{c=1}^{X^{1/4}} \frac{O(X^{1/6}/c^{2/3})}{X^{1/6}/c^{2/3}}\,\frac{X^{1/6}/c^{2/3}}{X^{1/4}}\right| \\
&\leq \sum_{c=1}^{X^{1/4}} \frac{A_c}{c^{2/3}X^{1/12}}\,,
\end{aligned}$$

onde A satisfaz $O(X^{1/6}/c^{2/3}) \leq AX^{1/6}/c^{2/3}$. Escrevendo $y = X^{1/12}$, a última soma se reescreve como $\sum_{c=1}^{y^3} \frac{A}{c^{2/3}y}$. Aplicando o teste da integral concluímos que esta soma é comparável com o valor da integral $\int_1^{y^3} \frac{A}{c^{2/3}y}\,dc = 3\frac{A}{y}c^{1/3}\Big|_{c=1}^{c=y^3} = 3A - \frac{3A}{y} \leq 3A$, o que mostra que a soma inicial é limitada. Assim, temos

$$\sum_{c=1}^{X^{1/4}} O\big((X/c^4)^{1/6}\big) = O(X^{1/4})\,. \qquad \square$$

E finalmente temos as ferramentas para provar o teorema principal em estudo:

Teorema 3.8. *O número de ordens cúbicas com grupo de automorfismo isomorfo a um grupo cíclico de ordem 3, e discriminante menor que X, é*

$$\frac{\pi}{6\sqrt{3}}X^{1/2} + O(X^{1/4})\,.$$

Demonstração. Usando os resultados do Teorema 3.6 e do Lema 3.7, basta contar o número de elementos $(b, c)^t \in L$, a menos de $\mathrm{SO}_2(\mathbb{Z})$-equivalência, acrescentando a condição $Q'(b, c)^2 = (b^2 - bc + c^2)^2 < X$. O número de pontos inteiros interiores à região elíptica definida pela última desigualdade é aproximadamente igual a sua área, a saber $(2\pi/\sqrt{3})X^{1/2}$, com erro de no máximo $O(X^{1/4})$ (vide (COHN, 1980), p. 161). Sabe-se que $\mathrm{SO}_Q(\mathbb{Z})$ é isomorfo a C_6, o grupo cíclico de ordem 6. Uma vez que essa ação é cúbica, o subgrupo cíclico $C_3 \subseteq \mathrm{SO}_Q(\mathbb{Z})$ de ordem 3 age trivialmente. A menos de equivalência, obtemos

$$\frac{2\pi}{2\sqrt{3}}X^{1/2} + O(X^{1/4})$$

pontos interiores à elipse. Portanto, o número de escolhas dos pontos com $b \equiv c \pmod 3$ será

$$\frac{\pi}{3\sqrt{3}}X^{1/2} + O(X^{1/4}).$$

Este é o número de anéis C_3-cúbicos orientados com discriminante limitado por X. Pelo Lema 3.7, os anéis C_3-cúbicos que não são ordens serão absorvidos pelo termo do erro. Já que até agora foram contados apenas os anéis cúbicos orientados, dividimos por 2 e obtemos o resultado para anéis cúbicos. □

REFERÊNCIAS

ATIYAH, M. F.; MACDONALD, I. G. *Introduction to commutative algebra*. [S.l.]: Addison-Wesley Publishing Co., Reading, Mass.-London-Don Mills, Ont., 1969. ix+128 p. Citado 2 vezes nas páginas 13 e 37.

BHARGAVA, M.; SHANKAR, A.; TSIMERMAN, J. On the Davenport-Heilbronn theorems and second order terms. *Inventiones Mathematicae*, v. 193, n. 2, p. 439–499, 2013. ISSN 0020-9910. Citado na página 11.

BHARGAVA, M.; SHNIDMAN, A. On the number of cubic orders of bounded discriminant having automorphism group C_3, and related problems. *Algebra & Number Theory*, v. 8, n. 1, p. 53–88, 2014. ISSN 1937-0652. Citado na página 11.

COHN, H. *Advanced number theory*. [S.l.]: Dover Publications, Inc., New York, 1980. xi+276 p. Reprint of ıt A second course in number theory, 1962, Dover Books on Advanced Mathematics. ISBN 0-486-64023-X. Citado na página 48.

DAVENPORT, H. On the class-number of binary cubic forms. I. *Journal of the London Mathematical Society. Second Series*, v. 26, p. 183–192, 1951. ISSN 0024-6107. Citado na página 10.

DAVENPORT, H. On the class-number of binary cubic forms. II. *Journal of the London Mathematical Society. Second Series*, v. 26, p. 192–198, 1951. ISSN 0024-6107. Citado na página 10.

DICKSON, L. E. *History of the theory of numbers. Vol. III: Quadratic and higher forms*. [S.l.]: Chelsea Publishing Co., New York, 1966. v+313 p. (With a chapter on the class number by G. H. Cresse). Citado na página 10.

GAN, W. T.; GROSS, B.; SAVIN, G. Fourier coefficients of modular forms on G_2. *Duke Mathematical Journal*, v. 115, n. 1, p. 105–169, 2002. ISSN 0012-7094. Citado 2 vezes nas páginas 10 e 50.

RIBENBOIM, P. *Algebraic numbers*. [S.l.]: Wiley-Interscience [A Division of John Wiley & Sons, Inc.], New York-London-Sydney, 1972. x+300 p. Pure and Applied Mathematics, Vol. 27. Citado na página 14.

SAMUEL, P. *Algebraic theory of numbers*. [S.l.]: Houghton Mifflin Co., Boston, Mass., 1970. 109 p. (Translated from the French by Allan J. Silberger). Citado na página 12.

APÊNDICE A – PROVA DA CORRESPONDÊNCIA DE DELONE-FADEEV

Durante o desenvolvimento deste trabalho, nos deparamos com um "pequeno grande problema": na demonstração do teorema 2.4, Gordan Savin na referência (GAN; GROSS; SAVIN, 2002) afirmava que o anel cúbico A com $\mathbb{Z}$-base boa $(1, \alpha, \beta)$ que seria isomorfo a uma forma cúbica, preservando discriminante, deveria ter os produtos definidos como

$$\begin{aligned} \alpha\beta &= -ad\,; \\ \alpha^2 &= -ac + b\alpha - a\beta\,; \\ \beta^2 &= -bd + d\alpha - c\beta\,, \end{aligned}$$

onde a, b, c, d são inteiros. No entanto, depois de cálculos extensos concluímos que havia algo de errado nessa definição dos produtos. Isto nos fez questionar: De onde veio essa escolha dos produtos? Depois de mais cálculos extensos chegamos à definição correta. O objetivo desse Apêndice é expor nosso trabalho computacional, o qual constitui o complemento da demonstração do Teorema 2.4 (naquela demonstração são feitas as contas mais simples, as quais serão omitidas nesta apresentação).

Lembramos que a cada par $(A, \mathcal{B})$, sendo A um anel cúbico com uma $\mathbb{Z}$-base boa $\mathcal{B} = (1, \alpha, \beta)$, associamos a única quádrupla $\mathcal{N}(A, \mathcal{B}) = (p, q, r, s)$ de inteiros satisfazendo as igualdades

$$\left.\begin{aligned} \alpha\beta &= qr\,; \\ \alpha^2 &= -qs + p\alpha + q\beta\,; \\ \beta^2 &= -pr + r\alpha + s\beta\,. \end{aligned}\right\} \tag{A.1}$$

Dado outro anel cúbico A' com $\mathbb{Z}$-base boa $\mathcal{B}' = (1, \alpha', \beta')$, seja $(p', q', r', s') = \mathcal{N}(A', \mathcal{B}')$; em particular valem

$$\left.\begin{aligned} \alpha'\beta' &= q'r'\,; \\ \alpha'^2 &= -q's' + p'\alpha' + q'\beta'\,; \\ \beta'^2 &= -p'r' + r'\alpha' + s'\beta'\,. \end{aligned}\right\} \tag{A.2}$$

Se $T : A' \to A$ é um isomorfismo de anéis com unidade, então existem $u, v \in \mathbb{Z}$ e $\gamma = \left[\begin{smallmatrix} E & F \\ G & H \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{Z})$ tais que

$$\left.\begin{aligned} T(1) &= 1 \cdot 1 + 0 \cdot \alpha + 0 \cdot \beta\,; \\ T(\alpha') &= u \cdot 1 + E \cdot \alpha + F \cdot \beta\,; \\ T(\beta') &= v \cdot 1 + G \cdot \alpha + H \cdot \beta\,, \end{aligned}\right\} \tag{A.3}$$

Como T respeita produtos, então valem as igualdades

$$T(\alpha'\beta') = T(\alpha')T(\beta')\,; \tag{A.4}$$
$$T(\alpha'^2) = T(\alpha')^2\,; \tag{A.5}$$
$$T(\beta'^2) = T(\beta')^2\,; \tag{A.6}$$

Substituindo as igualdades (A.2) e (A.3) em (A.4) obtemos $q'r' = (u + E\alpha + F\beta)(v + G\alpha + H\beta)$. Expandindo e usando (A.1) obtemos

$$\begin{aligned} q'r' = {} & uv - qsEG + qrEH + qrFG - prFH \\ & + (Gu + Ev + pEG + rFH)\alpha \\ & + (Hu + qEG + Fv + sFH)\beta\,. \end{aligned}$$

Pela unicidade da escrita dos elementos do anel na $\mathbb{Z}$-base $(1, \alpha, \beta)$, seguem as igualdades

$$\begin{aligned} 0 &= Gu + Ev + pEG + rFH\,; \\ 0 &= Hu + qEG + Fv + sFH\,. \end{aligned}$$

Resolvendo o sistema acima obtemos

$$u = \frac{pEFG + rF^2H - qE^2G - sEFH}{EH - FG}\,; \tag{A.7}$$
$$v = \frac{qEG^2 + sFGH - pEGH - rFH^2}{EH - FG}\,. \tag{A.8}$$

Ora, substituindo as igualdades (A.2) e (A.3) em (A.5) obtemos $T(-q's' + p'\alpha' + q'\beta') = (u + E\alpha + F\beta)^2$. Expandindo e usando (A.1), junto com a unicidade da escrita na $\mathbb{Z}$-base $(1, \alpha, \beta)$, obtemos

$$\begin{aligned} p'E + q'G &= pE^2 + rF^2 + 2uE\,; \\ p'F + q'H &= qE^2 + sF^2 + 2uF\,. \end{aligned}$$

Substituindo o valor de u dado por (A.7) e resolvendo o sistema chegamos a

$$\begin{aligned} p' &= \frac{E(EH + 2FG)p - 3E^2Gq + 3F^2Hr - F(FG + 2EH)s}{EH - FG}\,; \\ q' &= \frac{-E^2Fp + E^3q - F^3r + EF^2s}{EH - FG}\,. \end{aligned}$$

Finalmente, substituindo as igualdades (A.2) e (A.3) em (A.6) obtemos $T(-p'r' + r'\alpha' + s'\beta') = (v + G\alpha + H\beta)^2$. Expandindo e usando (A.1), junto com a unicidade da escrita na $\mathbb{Z}$-base $(1, \alpha, \beta)$, obtemos

$$\begin{aligned} r'E + s'G &= pG^2 + rH^2 + 2vG\,; \\ r'F + s'H &= qG^2 + sH^2 + 2vH\,. \end{aligned}$$

Substituindo o valor de v dado por (A.8) e resolvendo o sistema chegamos a

$$r' = \frac{G^2Hp - G^3q + H^3r - GH^2s}{EH - FG};$$
$$s' = \frac{-G(FG + 2EH)p + 3EG^2q - 3FH^2r + H(EH + 2FG)s}{EH - FG}.$$

As igualdades obtidas podem ser escritas na forma matricial

$$\begin{pmatrix} p' \\ q' \\ r' \\ s' \end{pmatrix} = \frac{1}{\det(\gamma)} W_\gamma \begin{pmatrix} p \\ q \\ r \\ s \end{pmatrix} = \det(\gamma)\, W_\gamma \begin{pmatrix} p \\ q \\ r \\ s \end{pmatrix}. \tag{A.9}$$

onde

$$W_\gamma = \begin{bmatrix} E(2FG + EH) & -3E^2G & 3F^2H & -F(FG + 2EH) \\ -E^2F & E^3 & -F^3 & EF^2 \\ G^2H & -G^3 & H^3 & -GH^2 \\ -G(FG + 2EH) & 3EG^2 & -3FH^2 & H(2FG + EH) \end{bmatrix}. \tag{A.10}$$

Por outro lado, lembramos que a ação de $\theta = \left[\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right] \in \mathrm{GL}_2(\mathbb{Z})$ na forma cúbica $f(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$ é dada por

$$(\theta \cdot f)(x, y) = \frac{1}{\det(\theta)} f(Ax + Cy, Bx + Dy) = \det(\theta)\, f(Ax + Cy, Bx + Dy).$$

Se $(\theta \cdot f)(x, y) = a'x^3 + b'x^2y + c'xy^2 + d'y^3$, então vale a igualdade matricial

$$\begin{pmatrix} a' \\ b' \\ c' \\ d' \end{pmatrix} = \det(\theta)\, Z_\theta \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}, \tag{A.11}$$

onde

$$Z_\theta = \begin{bmatrix} A^3 & A^2B & AB^2 & B^3 \\ 3A^2C & A(AD + 2BC) & B(BC + 2AD) & 3B^2D \\ 3AC^2 & C(BC + 2AD) & D(AD + 2BC) & 3BD^2 \\ C^3 & C^2D & CD^2 & D^3 \end{bmatrix}. \tag{A.12}$$

Queremos encontrar uma transformação linear ϕ que satisfaça

$$\phi(a, b, c, d) = (p, q, r, s) \tag{A.13}$$
$$\phi(a', b', c', d') = (p', q', r', s') \tag{A.14}$$

Seja M_ϕ a matriz associada a transformação linear ϕ. Usando as igualdades A.9 e A.11 obtemos

$$\det(\theta)\, M_\phi\, Z_\theta \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \det(\gamma)\, W_\gamma\, M_\phi \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix},$$

ou seja $\det(\theta)\, M_\phi\, Z_\theta = \det(\gamma)\, W_\gamma\, M_\phi$. Portanto W_γ e Z_θ são matrizes semelhantes quando $\det(\gamma) = \det(\theta)$.

Para facilitar o trabalho computacional, observamos a forma das matrizes:

$$W_\gamma = \begin{bmatrix} E(2FG+EH) & -3E^2G & 3F^2H & -F(FG+2EH) \\ -E^2F & E^3 & -F^3 & EF^2 \\ G^2H & -G^3 & H^3 & -GH^2 \\ -G(FG+2EH) & 3EG^2 & -3FH^2 & H(2FG+EH) \end{bmatrix};$$

$$Z_\theta = \begin{bmatrix} A^3 & A^2B & AB^2 & B^3 \\ 3A^2C & A(AD+2BC) & B(BC+2AD) & 3B^2D \\ 3AC^2 & C(BC+2AD) & D(AD+2BC) & 3BD^2 \\ C^3 & C^2D & CD^2 & D^3 \end{bmatrix}.$$

Vemos que tomando $\theta = \gamma$, as matrizes W_γ e Z_θ parecem ser equivalentes, ou seja, existem P e Q matrizes não singulares tais que $W_\gamma = PZ_\gamma Q$. Assim, nosso novo par de matrizes será

$$W_\gamma = \begin{bmatrix} E(2FG+EH) & -3E^2G & 3F^2H & -F(FG+2EH) \\ -E^2F & E^3 & -F^3 & EF^2 \\ G^2H & -G^3 & H^3 & -GH^2 \\ -G(FG+2EH) & 3EG^2 & -3FH^2 & H(2FG+EH) \end{bmatrix};$$

$$Z_\gamma = \begin{bmatrix} E^3 & E^2F & EF^2 & F^3 \\ 3E^2G & E(EH+2FG) & F(FG+2EH) & 3F^2H \\ 3EG^2 & G(FG+2EH) & H(EH+2FG) & 3FH^2 \\ G^3 & G^2H & GH^2 & H^3 \end{bmatrix},$$

e nosso objetivo é encontrar P e Q. Seguiremos as seguintes etapas:

- Trocamos as posições da primeira e segunda coluna de W_γ, multiplicando-a à direita por $Q_1 = \left[\begin{smallmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{smallmatrix}\right]$, resultando em

$$W_\gamma Q_1 = \begin{bmatrix} -3E^2G & E(2FG+EH) & 3F^2H & -F(FG+2EH) \\ E^3 & -E^2F & -F^3 & EF^2 \\ -G^3 & G^2H & H^3 & -GH^2 \\ 3EG^2 & -G(2EH+FG) & -3FH^2 & H(2FG+EH) \end{bmatrix}.$$

- Para trocar em $W_\gamma Q_1$ as posições das primeira e segunda linhas, a multiplicamos à esquerda por Q_1, resultando em

$$Q_1 W_\gamma Q_1 = \begin{bmatrix} E^3 & -E^2F & -F^3 & EF^2 \\ -3E^2G & E(2FG+EH) & 3F^2H & -F(FG+2EH) \\ -G^3 & G^2H & H^3 & -GH^2 \\ 3EG^2 & -G(2EH+FG) & -3FH^2 & H(2FG+EH) \end{bmatrix}.$$

- Agora, para trocar as posições da terceira e da quarta coluna na matriz anterior a multiplicamos à direita por $Q_2 = \left[\begin{smallmatrix} 1&0&0&0\\ 0&1&0&0\\ 0&0&0&1\\ 0&0&1&0 \end{smallmatrix}\right]$, resultando em

$$Q_1 W_\gamma Q_1 Q_2 = \begin{bmatrix} E^3 & -E^2F & EF^2 & -F^3 \\ -3E^2G & E(2FG+EH) & -F(FG+2EH) & 3F^2H \\ -G^3 & G^2H & -GH^2 & H^3 \\ 3EG^2 & -G(2EH+FG) & H(2FG+EH) & -3FH^2 \end{bmatrix}.$$

- Para trocar as posições das terceira e quarta linhas na matriz acima a multiplicamos à esquerda por Q_2, resultando em

$$Q_2 Q_1 W_\gamma Q_1 Q_2 = \begin{bmatrix} E^3 & -E^2F & EF^2 & -F^3 \\ -3E^2G & E(2FG+EH) & -F(FG+2EH) & 3F^2H \\ 3EG^2 & -G(2EH+FG) & H(2FG+EH) & -3FH^2 \\ -G^3 & G^2H & -GH^2 & H^3 \end{bmatrix}.$$

- Para ajustar os sinais, basta multiplicar as segunda e quarta linhas e as segunda e quarta colunas por -1, ou seja, multiplicar a matriz anterior à direita e à esquerda por $Q_3 = \left[\begin{smallmatrix} 1&0&0&0\\ 0&-1&0&0\\ 0&0&1&0\\ 0&0&0&-1 \end{smallmatrix}\right]$, resultando em

$$Q_3 Q_2 Q_1 W_\gamma Q_1 Q_2 Q_3 = Z_\gamma .$$

Seja $P = Q_1 Q_2 Q_3 = \left[\begin{smallmatrix} 0&-1&0&0\\ 1&0&0&0\\ 0&0&0&-1\\ 0&0&1&0 \end{smallmatrix}\right]$. Como $Q_i^{-1} = Q_i$ para $i = 1, 2, 3$, segue que $Z_\gamma = P^{-1} W_\gamma P$. Finalmente, tomamos ϕ dada por $M_\phi = P$, isto é, $\phi(a, b, c, d) = (-b, a, -d, c)$.