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

Construção de STBCs de Ordem Maximal em Álgebras Centrais Simples

por

Josenildo Brandão Santos

sob orientação do

Prof. Dr. Antônio de Andrade e Silva

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

Setembro/2012

João Pessoa - PB

S237c Santos, Josenildo Brandão.

Construção de STBCs de ordem maximal em álgebras centrais simples / Josenildo Brandão Santos.- João Pessoa, 2013. 96f.

Orientador: Antônio de Andrade e Silva.

Dissertação (Mestrado) - UFPB/CCEN.

1. Matemática. 2. Álgebras. 3. Códigos. 4. Corpo de números. 5. Ordem maximal. 6. Reticulados.

UFPB/BC CDU: 51(043)

Construção de STBCs de Ordem Maximal em Álgebras centrais Simples

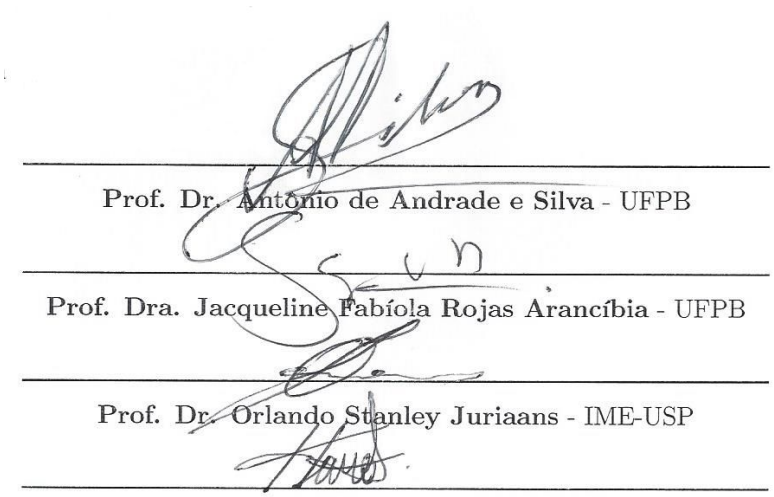
por

Josenildo Brandão Santos

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

Área de Concentração: Álgebra

Aprovada por:



Prof. Dr. Antônio de Andrade e Silva - UFPB

Prof. Dra. Jacqueline Fabíola Rojas Arancíbia - UFPB

Prof. Dr. Orlando Stanley Juriaans - IME-USP

Prof. Dr. Napoleón Caro Tuesta - UFPB

Universidade Federal da Paraíba

Centro de Ciências Exatas e da Natureza

Programa de Pós-Graduação em Matemática

Curso de Mestrado em Matemática

Setembro/2012

Agradecimentos

Nesta caminhada, convivi com muitas pessoas que de forma direta ou indireta contribuíram para que esse projeto se concretizasse. Assim, gostaria de deixar aqui registrado os meus sinceros agradecimentos.

- A Deus porque sem Ele nada sou e nada posso fazer.

- A minha família e em especial à minha mãe Maria de Lourdes Brandão Santos e ao meu pai José Carlos dos Santos (*in memoriam*), pelo apoio, incentivo e crença em mim.

- Ao Professor Dr. *Antônio de Andrade e Silva*, que foi muito mais um amigo do que um orientador e, aliás, a palavra orientador não consegue descrever a pessoa incrível que ele representa.

- Aos amigos Guilherme, Yane, Nívea e Reginaldo por serem minha família neste período do mestrado e por me acolherem, aconselharem e apoiarem em todos os momentos.

- Aos professores Elisandra Gloss, Napoleon Tuesta, Daniel Pelegrino e Everaldo Medeiros que muito contribuiram para a minha formação acadêmica, profissional e pessoal.

- Aos colegas do curso de mestrado, em especial aos amigos que sempre tiveram presentes nos momentos de maior dificuldade do curso: Pâmela, Rainelly, Pedro, Gilson, Wanderson, Gustavo, Nacib, Bruna, Ana Karine e Ivaldo.

- Aos amigos Lenita (Nita), Cristiane Gomes (Binha), Elaine (Lay), Edson, Célia Nunes, Naldeci (Nal), Andrea (Dea) e Maria São Pedro (Peu) por ouvirem com paciência os meus desabafos e por me acalmarem nos momentos de angústia.

- A Graça, pela atenção e presteza no atendimento de secretaria.

- Aos colegas do Centro Integrado Oscar Marinho Falcão.

- Aos colegas do Colegiado de Matemática no DEDC - UNEB - Campus de Teixeira de Freitas.

Dedicatória

A meu pai José Carlos dos Santos
(*in memoriam*).

Resumo

Nesta dissertação, será apresentada uma maneira para construir STBCs denso com diversidade completa, de ordem maximal em álgebras centrais simples. Construiremos um código reticulado ST com determinante não nulo para uma aplicação de quatro antenas de transmissão MISO. Apresentaremos também, um algoritmo geral para testar a maximalidade de uma ordem dada, uma vez que com o uso de uma ordem maximal em vez de apenas o anel dos inteiros algébricos, conseguimos um aumento na capacidade do código sem perda no determinante mínimo. Além disso, utilizando o ideal de uma ordem maximal melhoramos ainda mais o código, à medida que aumentamos o determinante mínimo.

Palavras Chave: Álgebras, Códigos, Corpo de Números, Ordem Maximal, Reticulados.

Abstract

In this dissertation, a way to build dense STBCs with full diversity of maximal order in central simple algebra will be presented. We constructed a retriculated ST code with a nonzero determinant for a quad antenna MISO transmission. Also, we will present a general algorithm to test the limit of a given order, since by the use of a maximum order instead of just the algebraic integer ring, we can increase the capacity of the code without a loss in the minimum determinant. Furthermore, by using the ideal of a maximum order we can further improve the code, as we increase the minimum determinant.

Key words: Algebras, Codes, Numbers Field, Maximal Orders, Lattice.

Notação

R - Anel

$R[x]$ - Anel dos polinômios sobre R

$U_n(R)$ - Conjunto das raízes n-ésimas das unidades de R

$P_n(R)$ - Conjunto das raízes n-ésimas primitivas da unidade

$\mathcal{O}_K$ - Anel dos inteiros em K

$\mathbb{Z}[i]$ - Anel dos inteiros Gaussianos

$\frac{\mathbb{Z}}{n\mathbb{Z}} = \mathbb{Z}_n$ - Anel dos inteiros módulo n

$\mathbb{Z}_p[x]$ - Conjunto dos polinômios na variável x com coeficientes em $\mathbb{Z}_p$

$\mathbb{Z}$ - Conjunto dos números inteiros

$\mathbb{Q}$ - Conjunto dos números racionais

$\mathbb{R}$ - Conjunto dos números reais

$\mathbb{C}$ - Conjunto dos números complexos

$\mathbb{H}$ - Álgebra dos quatérnios de Hamilton

$\mathrm{End}_{\mathbb{Q}}(K)$ - Conjunto dos operadores lineares sobre $\mathbb{Q}$

$\mathrm{Aut}_{\mathbb{Q}}(K)$ - Conjunto dos isomorfismos em K

$[x]$ - Ideal principal gerado por x

$[a_1, a_2, \ldots, a_n]$ - ideal gerado por $\{a_1, a_2, \ldots, a_n\}$

$\mathrm{mdc}(a, b)$ - Máximo dividor comum de a e b

$\frac{R}{I}$ - Anel quociente de R sobre I

$\mathrm{Gal}(f, \mathbb{Q})$ - Corpo de decomposição de um polinômio f

$\mathrm{Gal}(F/K)$ - Grupo de Galois de F sobre K

F/K - Extensão de um corpo F sobre um corpo K

$\partial(f)$ - Grau do polinômio f

$\overline{\alpha}$ - Conjugado de α

$E_\rho(\mathbf{0})$ - Esfera de raio ρ e centro $\mathbf{0}$

$[F : K]$ - Grau de F sobre K

Φ_n - n-ésimo polinômio ciclotômico

f_α - Polinômio caracteristico de α

ξ_n - Raiz n-ésima da unidade

$\mathrm{irr}(\theta, K)$ - Polinômio irredutível de θ sobre K

$\mathcal{A}$ - K-álgebra

$\mathcal{U}(\mathcal{A})$ - Conjunto dos elementos invertíveis de $\mathcal{A}$

$\mathcal{Z}(\mathcal{A})$ - Centro da K-álgebra

$\ker \phi$ - Núcleo da função ϕ

$\mathrm{Im}\, \phi$ - Imagem da função ϕ

$|X|$ - Cardinalidade do conjunto X

$\oplus$ - Soma direta

$\otimes$ - Produto tensorial

$\equiv$ - Congruente

$|$ - Divide

$\simeq$ - Isomorfo

$\forall$ - Para todo

$\sum$ - Soma

$\prod$ - Produto

$M_n(K)$ - Conjunto das matrizes de ordem $n \times n$ com entradas em K

$\mathbf{A}_f$ - Representação matricial de f

$\det \mathbf{A}$ - determinante da matriz $\mathbf{A}$

$\mathrm{sgn}(\sigma)$ - sinal de σ

$\mathrm{tr}(\alpha)$ - Traço reduzido de α

$\mathrm{nr}(\alpha)$ - Norma reduzida de α

$N(\alpha)$ - Norma absoluta de α

$\mathrm{Tr}(\alpha)$ - Traço absoluto de α

$K(\alpha_1, \ldots, \alpha_n)$ - menor subcorpo contendo $\alpha_1, \ldots, \alpha_n$ e K

$\Delta[\alpha_1, \ldots, \alpha_n]$ - discriminante de $\{\alpha_1, \ldots, \alpha_n\}$

$d(\mathcal{O})$ - discriminante ideal de $\mathcal{O}$

Γ - Reticulado

$\mathcal{O}$ - Ordem

$\mathcal{L}$ - Anel de Lipschitz

$\mathcal{H}$ - Anel de Hurwitz

$\mathcal{C}$ - Código

$\mathbf{G}$ - Matriz geradora de um reticulado

$\mathrm{div}(\alpha, \beta)$ - distância de Hamming entre α e β

Sumário

Introdução **x**

1 Preliminares **1**

1.1 Corpo de Números 1

1.2 Inteiros Algébricos 9

1.3 Corpos Quadráticos e Ciclotômicos 12

1.4 Ordens 16

2 Álgebras com Divisão Cíclicas **27**

2.1 Álgebras 27

2.2 Álgebras dos Quatérnios 35

2.3 Álgebras Cíclicas 46

3 Reticulados e Ordens dos Quatérnios **52**

3.1 Reticulados 52

3.2 Ordens 60

4 Reticulados Algébricos e Códigos **65**

4.1 Reticulados Algébricos 65

4.2 Códigos 67

4.3 Algoritmo 74

Referências Bibliográficas **82**

Introdução

Histórico

A álgebra tem desempenhado um papel significativo no desenvolvimento da chamada teoria da codificação. A partir de um problema sobre a confiabilidade na comunicação em um canal com ruído, surge uma teoria com o objetivo de detectar e corrigir erros na transmissão de informações. Ao transmitirmos dados, podem ocorrer problemas tais como interferências eletromagnéticas ou mesmo erros humanos (erros de digitação, por exemplo) que chamamos ruído fazendo com que a mensagem recebida seja diferente daquela que foi enviada. Assim, da necessidade de recuperar e corrigir a mensagem enviada é que surge a teoria dos códigos corretores de erros. Em 1948, Shannon dá início a esta teoria através de um trabalho onde mostra que, usando códigos corretores de erros, é possível projetar sistemas de comunicação digital com probabilidade de erro tão pequena quanto se deseje. Desde então, apareceram inúmeras pesquisas em busca de códigos bons, capazes de melhorar o desempenho de sistemas de comunicação digital, ressaltando-se em particular, os códigos sobre álgebras.

Os códigos corretores de erros surgem, por exemplo, quando fazemos o uso de informações digitalizadas, tais como na comunicação sem fio, nos aparelhos de armazenamento de dados, no processamento de imagens digitais, na internet, no rádio, etc. Um código corretor de erros é, basicamente, uma forma organizada de acrescentar algum dado a cada informação que precise ser transmitida ou armazenada, de modo que permita, ao recuperá-la, detectar e corrigir os erros no processo de transmissão desta informação.

Da teoria clássica da codificação um *código "linear"* sobre um corpo finito $\mathbb{F}$ é um subespaço de $\mathbb{F}^n$, em que n é o comprimento do código. O *posto* do código é a sua dimensão e as *palavras código* são os vetores em $\mathbb{F}^n$. Se todas as palavras código tem o mesmo comprimento, diremos que o código está na forma de *bloco*. A *distância mínima* de um

código, que é um parâmetro de desempenho deste, é a menor *distância de Hamming* entre duas palavras código distintas, em que a distância de Hamming conta o número de símbolos em que as duas palavras código diferem. Esta teoria clássica, tinha sua fundamentação matemática na teoria elementar dos números, em que corpos finitos eram a ferramenta central no desenvolvimento de códigos binários e, graças aos avanços tecnológicos e ao aumento na potência de processamento, disponível em receptores digitais, mudou-se o foco da atenção para a busca de códigos de sinais no espaço no quadro de sistemas de modulação codificadas. É aí que a teoria dos reticulados Euclidianos se torna útil na concepção de constelações de sinais densos, ou seja, qualquer subconjunto finito de $\mathbb{R}^n$. No entanto, com o advento da comunicação sem fio, os teóricos da codificação foram "forçados"a lidar com canais de desvanecimento. Embora a investigação matemática tenha progredido na compreensão de questões levantadas na teoria da codificação clássica, pesquisas em engenharia apontavam para novos problemas de codificação que apareciam na comunicação sem fio. Assim, é que, para criar códigos, novos critérios tiveram que ser considerados a fim de melhorar o desempenho pobre dos sistemas de transmissão sem fio.

Assim sendo, o projeto dos códigos corretores de erros foi substituído pelo chamado *código espaço temporal* (ST). Neste contexto, um código linear é um subgrupo aditivo de $M_n(F)$, em que F é um subcorpo de $\mathbb{C}$ e $M_n(F)$ denota o conjunto de todas as matrizes $n \times n$ com entradas em F. Uma palavra código é, agora, uma matriz deste subgrupo e a distância mínima é substituída pelo "*determinante mínimo*" como parâmetro. O determinante mínimo é definido como o módulo do menor determinante da diferença de duas palavras código distintas. O objetivo é maximizar o determinante mínimo, para em particular se certificar que ele é não nulo, sempre que duas matrizes no código são distintas. No caso em que o determinante mínimo é não nulo dizemos que o código é de *diversidade completa*. Este último requisito atrai, de forma natural, a atenção para as *álgebras com divisão* uma vez que supondo, por exemplo, que o código é um subanel de $M_n(F)$ de diversidade completa, então ele é um anel com divisão que é uma álgebra com divisão sobre o seu centro.

Com o intuito de transmitir de maneira eficiente muita informação em curtos intervalos de tempo, a utilização de múltiplas antenas se tornou uma proposta bastante interessante. Essa ideia já vinha sendo explorada no sistema de comunicação móvel há vários anos com múltiplas antenas instaladas no receptor. Tal sistema, conhecido como $MIMO$ (*Multiple*

Input-Multiple Output) está representado na figura abaixo:

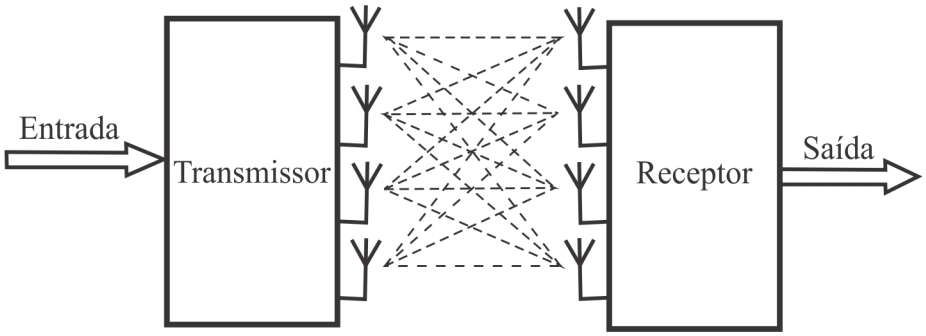


Figura 1: Modelo de um Canal MIMO

Em 1998, Alamouti propôs a construção de um código simples para comunicação sem fio com duas antenas transmissoras e (opcionalmente) múltiplas antenas receptoras. Esta construção consistia em considerar $z, w \in \mathbb{C}$ os símbolos da informação a ser enviada e

$$\mathcal{C} = \left\{ \begin{bmatrix} z & -\overline{w} \\ w & \overline{z} \end{bmatrix} : z, w \in \mathbb{C} \right\}$$

um *livro de códigos* (*codebook*) ou o *espaço de palavras*. A fim de obter um código eficiente, Alamouti projetou seu código para ser de diversidade completa. Formalmente, se $\mathbf{X}_1$ e $\mathbf{X}_2$ são duas palavras código em $\mathcal{C}$ então

$$\det(\mathbf{X}_1 - \mathbf{X}_2) = |z_1 - z_2|^2 + |w_1 - w_2|^2 \geq 0.$$

Note que a igualdade acontece se, e somente se, $z_1 = z_2$ e $w_1 = w_2$. Boa performance combinada com simplicidade fez o código de Alamouti muito atrativo. Por isso, tentativas de compreendê-lo melhor foram feitas com o objetivo de generalizá-lo. Daí que, em 1999, Tarokh et al. generalizaram o código de Alamouti para o caso de múltiplas antenas no transmissor e chamaram essa nova classe de códigos como *códigos espaço temporais de bloco-STBC* (*Space-Time Block Codes*) que eram associados basicamente a matrizes ortogonais. Em 2002, Sethuraman et al. perceberam que as palavras código do código de Alamouti podiam ser vistas como multiplicação à esquerda de matrizes por elementos da álgebra dos quatérnios de Hamilton e, é por isso, que nesta dissertação esta álgebra será amplamente considerada.

Nesta dissertação utilizaremos um caso particular do sistema $MIMO$, ou melhor, um sistema onde temos multiplas entradas e apenas uma saída. Neste sistema, conhecido

como $MISO$ (*Multiple Input-Single Output*), o sinal recebido $\mathbf{y} \in \mathbb{C}^n$ é dado por

$$\mathbf{y} = \mathbf{hX} + \mathbf{n},$$

em que $\mathbf{X}$ é uma palavra transmitida do código $\mathcal{C}$, $\mathbf{h}$ é a resposta do canal de desvanecimento Rayleigh e as componentes do vetor ruído $\mathbf{n}$ são variáveis complexas gaussianas aleatórias (independentes e identicamente distribuídas).

Descrição do trabalho

Em [**?**] Hollanti e Lahtonen propõem a construção de $STBCs$ denso, de ordem maximal em álgebras centrais simples, para um sistema $MISO$ com quatro antenas no transmissor e, com base neste trabalho, esta dissertação foi desenvolvida. Este desenvolvimento se deu em quatro capítulos nos quais foram apresentados as ferramentas necessárias para compreensão da construção descrita anteriormente.

No Capítulo 1 apresentamos noções básicas sobre a teoria algébrica dos números, no que diz respeito aos inteiros algébricos, corpo de números, corpos quadráticos e ciclotômicos além de alguns resultados sobre ordens de um corpo quadrático.

Os códigos serão construídos sobre uma álgebra e, por isso, no capítulo 2, fazemos um estudo de álgebras evidenciando as álgebras centrais simples, as álgebras cíclicas e as álgebras dos quatérnios.

No capítulo 3, abordamos um pouco da teoria dos reticulados e ordens sobre álgebras dos quatérnios.

Finalizamos esta dissertação, apresentando no capítulo 4, um método para determinar reticulados algébricos via imersão de Minkowiski e códigos sobre álgebras, além de um algoritmo que permite testar a maximalidade de uma ordem em uma álgebra central simples.

Capítulo 1

Preliminares

Neste capítulo apresentaremos algumas definições e resultados básicos da teoria algébrica dos números que serão necessários para a compreensão desta dissertação. O leitor interessado em mais detalhes pode consultar [**?**, **?**, **?**].

1.1 Corpo de Números

Salvo menção explícita em contrário, todos os corpos considerados nesta dissertação são subcorpos dos números complexos $\mathbb{C}$.

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

$$\begin{aligned} K[\theta] &= \left\{ \sum_{i=0}^{n} a_i \theta^i : n \in \mathbb{Z}_+ \text{ e } a_0, a_1, \ldots, a_n \in K \right\} \\ &= \{ f(\theta) : f \in K[x] \} \end{aligned}$$

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

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

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

Um elemento $\theta \in \mathbb{C}$ chama-se *algébrico* sobre K se existir $m \in \mathbb{N}$ tal que o conjunto

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

é linearmente dependente sobre K ou, equivalentemente, se existir um polinômio não constante

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \text{ onde } a_0, a_1, \ldots, a_{n-1}, a_n \in K,$$

tal que $f(\theta) = 0$. Em particular, se θ é algébrico sobre $\mathbb{Q}$ diremos que θ é um número algébrico. Note que $f(\theta) = 0$ implica que

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

e como f é não constante temos que $a_n \neq 0$. Assim, pondo $a_n^{-1} \cdot f(\theta) = 0$, obtemos

$$\theta^n + (a_n^{-1}a_{n-1})\theta^{n-1} + \cdots + \left(a_n^{-1}a_1\right)\theta + a_n^{-1}a_0 = 0.$$

Portanto, podemos supor, sem perda de generalidade, que o polinômio f é mônico.

Proposição 1.1 *Sejam α um elemento de $\mathbb{C}$ e K um subcorpo de $\mathbb{C}$. Então a função $\phi : K[x] \to \mathbb{C}$ definida como $\phi(f) = f(\alpha)$ é um homomorfismo de aneis tal que*:

1. $\operatorname{Im}\phi = K[\alpha]$ *e* $K \subseteq K[\alpha] \subseteq \mathbb{C}$.

2. α *é algébrico sobre* K *se, e somente se,* $\ker\phi \neq \{0\}$.

3. $\frac{K[x]}{\ker\phi} \simeq K[\alpha]$.

Seja $\theta \in \mathbb{C}$ algébrico sobre K. Então $K(\theta) = K[\theta]$, pois

$$\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_1\theta + a_0 = 0 \Rightarrow \theta(-a_0^{-1}(a_{n-1}\theta^{n-2} + \cdots + a_1)) = 1.$$

Teorema 1.1 *Seja $\theta \in \mathbb{C}$ algébrico sobre K. Então*:

1. *Existe um único polinômio mônico $p \in K[x]$ de menor grau tal que $p(\theta) = 0$.*

2. *p é um polinômio irredutível sobre K.*

3. *Se $f \in K[x]$ é tal que $f(\theta) = 0$, então p divide f.*

O polinômio p do Teorema **??** chama-se o *polinômio minimal* de θ e será denotado por $p = \operatorname{irr}(\theta, K)$.

Seja F um subcorpo de K. Podemos ver K como um espaço vetorial sobre F e K chama-se *extensão* de F. Diremos que K é uma *extensão finita* se K é um espaço vetorial de dimensão finita sobre F. Se K é uma extensão finita de F, denotaremos por

$$[K : F]$$

a dimensão de K visto como um espaço vetorial de sobre F e $[K : F]$ chama-se o *grau* de K sobre F.

Sejam $\alpha, \beta \in \mathbb{C}$. Diremos que α é *conjugado* a β sobre K se α e β são raízes do mesmo polinômio irredutível sobre K. É importante observar que o conceito de conjugado é o mesmo conceito clássico do conjugado de um número complexo, pois se $a, b \in \mathbb{R}$, com $b \neq 0$, então o conjugado de $\alpha = a + bi$ é $\beta = a - bi$ e ambos são raízes do polinômio

$$f = x^2 - 2ax + a^2 + b^2 \in \mathbb{R}[x],$$

o qual é irredutível sobre $\mathbb{R}$.

Exemplo 1.1 *Seja K uma extensão de $\mathbb{Q}$. Então $[K : \mathbb{Q}] = 2$ se, e somente se, existe $d \in \mathbb{Q}$ tal que $K = \mathbb{Q}(\sqrt{d})$.*

Solução. Sendo K um espaço vetorial de dimensão 2 sobre $\mathbb{Q}$, podemos estender a base $\{1\}$ de $\mathbb{Q}$, para uma base de K sobre $\mathbb{Q}$, digamos $\{1, \alpha\}$, onde $\alpha \in K - \mathbb{Q}$. Logo,

$$K = \mathbb{Q} \oplus \alpha\mathbb{Q} = \{a + b\alpha : a, b \in \mathbb{Q}\}.$$

Como K é um corpo temos que $\alpha^2 \in K$. Assim, existem $a, b \in \mathbb{Q}$ tais que $\alpha^2 = a + b\alpha$. Logo,

$$\left(\alpha - \frac{b}{2}\right)^2 = a + \frac{b^2}{4} \in \mathbb{Q}.$$

Pondo

$$\beta = \alpha - \frac{b}{2} \in K,$$

temos que $\{1, \beta\}$ é também uma base de K sobre $\mathbb{Q}$ tal que $K = \mathbb{Q}(\beta)$, onde

$$\beta^2 = a + \frac{b^2}{4} = d \in \mathbb{Q}.$$

Portanto,

$$K = \mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}.$$

Reciprocamente, é facil verificar que K com a adição

$$(a_1 + b_1\sqrt{d}) + (a_2 + b_2\sqrt{d}) = (a_1 + a_2) + (b_1 + b_2)\sqrt{d}$$

e a multiplicação

$$(a_1 + b_1\sqrt{d}) \cdot (a_2 + b_2\sqrt{d}) = (a_1a_2 + b_1b_2d) + (a_1b_2 + a_2b_1)\sqrt{d}$$

é um corpo, com uma base $\{1, \sqrt{d}\}$. Portanto, $[K : \mathbb{Q}] = 2$. ■

Observação 1.1 *Como $d \in \mathbb{Q}$ temos que d pode ser escrito de modo único sob a forma*

$$d = \frac{m}{n} = \frac{mn}{n^2},$$

onde $m, n \in \mathbb{Z}$ e $\text{mdc}(m, n) = 1$. Logo, $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}(\sqrt{mn})$, onde $\sqrt{mn} \in K - \mathbb{Q}$. Portanto, podemos supor, sem perda de generalidade, que d é um número inteiro livre de quadrados.

Proposição 1.2 (Teorema da Conjugação) *Sejam $\alpha, \beta \in \mathbb{C}$ algébricos sobre K, com $[K(\alpha) : K] = n$. Então a função $\varphi : K(\alpha) \to K(\beta)$ definida como $\varphi(\alpha) = \beta$ e $\varphi(a) = a$, para todo $a \in K$, é um isomorfismo se, e somente se, α e β são conjugados sobre K.*

Sejam K uma extensão finita de $\mathbb{Q}$ e $\alpha \in K^*$. Então a função $L_\alpha : K \to K$ definida como $L_\alpha(\beta) = \alpha\beta$ é claramente uma transformação linear injetora sobre $\mathbb{Q}$. Denotaremos por $\text{End}_\mathbb{Q}(K)$ o conjunto de todos os operadores lineares sobre $\mathbb{Q}$. Logo, a função $L : K \to \text{End}_\mathbb{Q}(K)$ definida como $L(\alpha) = L_\alpha$ é um homomorfismo de aneis injetor. Portanto, podemos identificar K com um subcorpo de $\text{End}_\mathbb{Q}(K)$. Se

$$B = \{\alpha_1, \ldots, \alpha_n\}$$

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

$$\{L_{\alpha_1}, \ldots, L_{\alpha_n}\}$$

é uma base de $\text{End}_\mathbb{Q}(K)$ e

$$L_\alpha(\alpha_j) = \sum_{i=1}^{n} a_{ij}\alpha_i, \;\; j = 1, \ldots, n$$

então

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

é o *polinômio característico* de α sobre $\mathbb{Q}$, em que $\mathbf{A}_\alpha = [a_{ij}]$ é a matriz $n \times n$ de L_α em relação à base B. O *traço absoluto* e a *norma absoluta* de α são definidos por

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

Portanto, para determinarmos $\text{Tr}(\alpha)$ e $N(\alpha)$, escolhemos uma base

$$B = \{\alpha_1, \ldots, \alpha_n\}$$

para K e

$$L_\alpha(\alpha_j) = \sum_{i=1}^{n} a_{ij}\alpha_i, \;\; j = 1, \ldots, n$$

Suponhamos que

$$f_\alpha(x) = (x - \alpha_1) \cdots (x - \alpha_n) \in \mathbb{C}[x].$$

Então

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

Finalmente, a função $T : K \to \mathbb{Q}$ definida como $T(\alpha) = \mathrm{Tr}(\alpha)$ é um funcional linear.

Exemplo 1.2 *Sejam $K = \mathbb{Q}(\sqrt{d})$, com d livre de quadrados e $\theta \in K$. Então $f_\theta = x^2 - 2ax + a^2 - db^2$, $\mathrm{Tr}(\theta) = 2a$ e $N(\theta) = a^2 - db^2$, onde $a, b \in \mathbb{Q}$.*

Solução. Como $\{1, \sqrt{d}\}$ é uma base K sobre $\mathbb{Q}$ temos que $\theta = a + b\sqrt{d}$, onde $a, b \in \mathbb{Q}$. Assim,

$$\begin{aligned} L_\theta(1) &= (a + b\sqrt{d}) \cdot 1 = a + b\sqrt{d} \\ L_\theta(\sqrt{d}) &= (a + b\sqrt{d}) \cdot \sqrt{d} = bd + a\sqrt{d} \end{aligned}$$

Portanto,

$$\mathbf{A}_\theta = \begin{bmatrix} a & bd \\ b & a \end{bmatrix}.$$

Neste caso, $\mathrm{Tr}(\theta) = 2a$, $N(\theta) = a^2 - db^2$ e $f_\theta = x^2 - 2ax + a^2 - db^2 \in \mathbb{Q}[x]$. ■

Observação 1.2 *Seja $K = \mathbb{Q}(\sqrt{d})$, com d livre de quadrados. Então K é isomorfo ao corpo de matrizes*

$$\mathcal{L}_K = \left\{ \begin{bmatrix} a & bd \\ b & a \end{bmatrix} : a, b \in \mathbb{Q} \right\} \subseteq M_2(\mathbb{Q}).$$

Explicitamente, a função $L : K \to \mathcal{L}_K \subseteq M_2(\mathbb{Q})$ definida como

$$L(a + b\sqrt{d}) = a\mathbf{I} + b\mathbf{A},$$

em que

$$\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \mathbf{A} = \begin{bmatrix} 0 & d \\ 1 & 0 \end{bmatrix} \in M_2(\mathbb{Q}) \;\; e \;\; \mathbf{A}^2 = \begin{bmatrix} d & 0 \\ 0 & d \end{bmatrix} = d\mathbf{I},$$

é um isomorfismo.

Seja K uma extensão de $\mathbb{Q}$. Uma $\mathbb{Q}$-*imersão* (ou simplesmente uma imersão) de K em $\mathbb{C}$ é qualquer homomorfismo de corpos não nulo $\sigma : K \to \mathbb{C}$ tal que $\sigma(a) = a$, para todo $a \in \mathbb{Q}$, isto é, $\sigma|_{\mathbb{Q}} = I$. Neste caso, diremos que $\mathbb{Q}$ é o *corpo fixo* de σ. Um *isomorfismo* de K sobre L é qualquer isomorfismo de corpos $\sigma : K \to L$ tal que $\sigma(a) = a$, para todo $a \in \mathbb{Q}$, e será denotado por

$$\mathrm{Aut}_{\mathbb{Q}}(K) = \{\sigma : K \to K : \sigma \text{ é um isomorfismo}\}.$$

Note que qualquer $\mathbb{Q}$-imersão σ de K em $\mathbb{C}$ é uma transformação linear sobre $\mathbb{Q}$.

Teorema 1.2 *Seja K uma extensão de $\mathbb{Q}$ de grau n. Então*:

1. *Existe $\theta \in K$ tal que $K = \mathbb{Q}(\theta)$. (O elemento θ chama-se* elemento primitivo)

2. *Existem exatamente n imersões $\sigma_i : K \to \mathbb{C}$, onde $\sigma_i(\theta) = \theta_i$ são as raízes em $\mathbb{C}$ de* $\mathrm{irr}(\theta, \mathbb{Q})$. *As imagens $K_i = \sigma_i(K) = \mathbb{Q}(\theta_i)$ em $\mathbb{C}$ chamam-se* corpos conjugados *de K, e os K_i são isomorfos a K.*

3. *Para cada i, todos os elementos de K_i são números algébricos e seus graus dividem n.*

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

Sejam K/F uma extensão e $f \in F[x]$. Diremos que f *decompõe-se* sobre K se

$$f = a(x - \alpha_1) \cdots (x - \alpha_n),$$

onde $\alpha_1, \ldots, \alpha_n \in K$ e $a \in F$. Note que os α_i não são necessariamente distintos e

$$f = a(x - \alpha_1) \cdots (x - \alpha_n) \in K[x].$$

Sejam F um corpo e $f \in F[x]$. Um *corpo de decomposição* de f sobre F é uma extensão K/F tal que as seguintes condições são satisfeitas:

1. f decompõe-se sobre K.

2. K é minimal com respeito à condição (1), isto é, se f decompõe sobre L, sendo $F \subseteq L \subseteq K$, então $K = L$.

Vamos denotar o corpo de decomposição de um polinômio $f \in \mathbb{Q}[x]$ por $K = \mathrm{Gal}(f, \mathbb{Q})$.

Seja K uma extensão finita de $\mathbb{Q}$. Diremos que $K/\mathbb{Q}$ é uma *extensão Galoisiana* se K é igual aos seus corpos de conjugações ou, equivalentemente, K é um corpo de decomposição de algum polinômio $f \in \mathbb{Q}[x]$.

Teorema 1.3 *Seja $K/\mathbb{Q}$ uma extensão Galoisiana. Então*

$$|\mathrm{Aut}_{\mathbb{Q}}(K)| = [K : \mathbb{Q}].$$

Além disso, se $\alpha \in K$ e $\alpha \notin \mathbb{Q}$, então existe $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(K)$ tal que $\sigma(\alpha) \neq \alpha$.

Seja $K/\mathbb{Q}$ uma extensão qualquer. O subgrupo $\mathrm{Aut}_{\mathbb{Q}}(K)$ do grupo $\mathrm{Aut}(K)$ chama-se *grupo de Galois* de $K/\mathbb{Q}$ e será denotado por

$$\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(K),$$

pois se $\sigma, \varphi \in \mathrm{Gal}(K/\mathbb{Q})$, então

$$(\varphi\sigma)(a) = \varphi(\sigma(a)) = \varphi(a) = a \Rightarrow \varphi\sigma \in \mathrm{Gal}(K/\mathbb{Q}).$$

Diremos que $K/\mathbb{Q}$ é uma *extensão abeliana* (*cíclica*) se ela é Galoisiana e seu grupo de Galois $\mathrm{Gal}(K/\mathbb{Q})$ é abeliano (cíclico).

Note que se $\alpha \in \mathbb{C}$ é algébrico sobre K e $p = \mathrm{irr}(\alpha, K) \in K[x]$, então

$$|\mathrm{Gal}(K(\alpha)/K)| = \text{ número de raízes de } p.$$

Portanto, $K(\alpha)/K$ é uma extensão Galoisiana se, e somente se, p possui n raízes distintas em $K(\alpha)$, com $n = \partial(p)$.

Exemplo 1.3 *Sejam $K = \mathbb{Q}(\sqrt{d})$, com d livre de quadrados. Então* $\mathrm{Gal}(K/\mathbb{Q}) \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$.

Solução. Para qualquer $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ e $\alpha = a + b\sqrt{d} \in K$, onde $a, b \in \mathbb{Q}$, obtemos

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

Assim, σ é completamente determinado pelo valor $\sigma(\sqrt{d})$. Como

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

temos que $\sigma(\sqrt{d})$ é uma raiz do polinômio $\mathrm{irr}(\sqrt{d}, \mathbb{Q}) \in \mathbb{Q}[x]$. Logo,

$$\sigma(\sqrt{d}) = \sqrt{d} \text{ ou } \sigma(\sqrt{d}) = -\sqrt{d}.$$

Portanto, $\sigma = I$ ou $\sigma = \sigma_1$, com $\sigma_1(\alpha) = a - b\sqrt{d}$ o conjugado de α. Neste caso,

$$\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma_1\} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}}$$

e $K/\mathbb{Q}$ é uma extensão cíclica. ■

Sejam $f \in \mathbb{Q}[x]$ um polinômio qualquer e $K = \mathrm{Gal}(f, \mathbb{Q})$. Então o *grupo de Galois* de f sobre $\mathbb{Q}$ é o grupo $\mathrm{Gal}(K/\mathbb{Q})$. Neste caso, se

$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$$

e $\alpha \in K$ é uma raiz de f, então para cada $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ fixado, obtemos

$$\begin{aligned} f(\sigma(\alpha)) &= a_n\sigma(\alpha)^n + \cdots + a_1\sigma(\alpha) + a_0 \\ &= \sigma(a_n)\sigma(\alpha^n) + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) \\ &= \sigma(a_n\alpha^n + \cdots + a_1\alpha + a_0) \\ &= \sigma(0) = 0. \end{aligned}$$

Portanto, $\sigma(\alpha) \in K$ é uma raiz de f, ou seja, as raízes de f são permutadas por qualquer $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. Mais geralmente, temos o seguinte resultado:

Teorema 1.4 *Seja $K/\mathbb{Q}$ uma extensão Galoisiana, com $[K : \mathbb{Q}] = n$. Então $\mathrm{Gal}(K/\mathbb{Q})$ é isomorfo a um subgrupo de S_n. Em particular, $|\mathrm{Gal}(K/\mathbb{Q})|$ divide $n!$.*

Sejam K um corpo qualquer e G um subconjunto de $\mathrm{Aut}(K)$. Então o conjunto

$$K^G = \{\alpha \in K : \sigma(\alpha) = \alpha, \ \forall \ \sigma \in G\}$$

é um subcorpo de K. O subcorpo K^G chama-se *corpo fixo* de G.

Sejam $K/\mathbb{Q}$ uma extensão e $G = \mathrm{Gal}(K/\mathbb{Q})$. Vamos denotar por $\mathrm{Int}(K/\mathbb{Q})$ o conjunto de todos os corpos intermediários de $K/\mathbb{Q}$ e por $\mathrm{Sub}(G)$ o conjunto de todos os subgrupos de G.

Teorema 1.5 (Teorema Fundamental da Teoria de Galois) *Sejam $K/\mathbb{Q}$ uma extensão Galoisiana e $G = \mathrm{Gal}(K/\mathbb{Q})$. Então:*

1. *A função $\gamma : \mathrm{Sub}(G) \to \mathrm{Int}(K/\mathbb{Q})$ definida como $\gamma(H) = K^H$ é uma bijeção invertendo ordem, com inversa $\delta : \mathrm{Int}(K/\mathbb{Q}) \to \mathrm{Sub}(G)$ definida por $\delta(F) = \mathrm{Gal}(K/F)$.*

2. *Para qualquer $F \in \mathrm{Int}(K/\mathbb{Q})$, $F/\mathbb{Q}$ é uma extensão Galoisiana se, e somente se, $\mathrm{Gal}(K/F)$ é um subgrupo normal em G. Em particular,*

$$\frac{G}{\mathrm{Gal}(K/F)} \simeq \mathrm{Gal}(F/\mathbb{Q}).$$

1.2 Inteiros Algébricos

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

Teorema 1.6 *Seja $\theta \in \mathbb{C}$ número algébrico. Então as seguintes condições são equivalentes*:

1. *θ é um inteiro algébrico.*

2. *O anel $\mathbb{Z}[\theta]$ é um $\mathbb{Z}$-módulo finitamente gerado.*

3. *Existe um subanel $\mathcal{O}$ de $\mathbb{C}$ que é um $\mathbb{Z}$-módulo finitamente gerado e tal que $\theta \in \mathcal{O}$.*

4. *Existe um $\mathbb{Z}$-módulo finitamente gerado não nulo $\mathcal{M}$ de $\mathbb{C}$ tal que $\theta\mathcal{M} \subseteq \mathcal{M}$.*

Seja

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

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

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

$$\mathcal{O}_K = \mathbb{B} \cap K$$

chama-se *anel dos inteiros* em K. Observe que, $\mathcal{O}_K$ possui todas as operações de K, exceto a inversão. Note que se um subanel $\mathcal{O}$ de $\mathbb{C}$ é um $\mathbb{Z}$-módulo finitamente gerado, então pelo item (3) do Teorema **??** $\mathcal{O} \subseteq \mathcal{O}_K$.

Sejam R um subanel de $\mathbb{C}$ e $K = Q(R)$ seu corpo quociente. Diremos que R é *integralmente fechado* em K se $\mathcal{O}_K = R$.

Proposição 1.3 *Seja K um corpo de números. Se $\alpha \in K$, então existe $b \in \mathbb{Z}^*$ tal que $b\alpha \in \mathcal{O}_K$. Portanto, qualquer número algébrico é da forma $\alpha = a^{-1}\beta$, onde $a \in \mathbb{Z}^*$ e $\beta \in \mathcal{O}_K$. Neste caso, $K = \mathbb{Q}\mathcal{O}_K$.*

Uma base de K sobre $\mathbb{Q}$

$$\{\alpha_1, \ldots, \alpha_n\}$$

chama-se uma *base integral* ($\mathbb{Z}$-*base*) para K se $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ e cada $\beta \in \mathcal{O}_K$ pode ser escrito de modo único sob a forma

$$\beta = b_1\alpha_1 + \cdots + b_n\alpha_n,$$

onde $b_i \in \mathbb{Z}$, ou seja,

$$\mathcal{O}_K = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n.$$

Teorema 1.7 *Seja K um corpo de números de grau n. Então existe $\theta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\theta)$. Neste caso, $\partial(\mathrm{irr}(\theta, \mathbb{Q})) = n$.*

Sejam $K = \mathbb{Q}(\theta)$ e $\theta_i = \sigma_i(\theta),\ i = 1, \ldots, n$, os conjugados de θ. Então

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \ldots, \sigma_n\}.$$

Como

$$p = \mathrm{irr}(\theta, \mathbb{Q}) = (x - \theta_1) \cdots (x - \theta_n) \in K[x]$$

temos que

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

Se

$$p = \mathrm{irr}\,(\theta, \mathbb{Q}) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0,$$

então $\mathrm{Tr}(\theta) = -a_{n-1} \in \mathbb{Q}$ e $N(\theta) = (-1)^n a_0 \in \mathbb{Q}$. Em particular, se $\theta \in \mathcal{O}_K$, então $\mathrm{Tr}(\theta), N(\theta) \in \mathbb{Z}$.

Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base de K sobre $\mathbb{Q}$. Definimos o *discriminante* desta base como

$$\Delta[\alpha_1, \ldots, \alpha_n] = \det[\mathrm{Tr}(\alpha_i\alpha_j)] = \{\det[\sigma_i(\alpha_j)]\}^2.$$

Sendo $K = \mathbb{Q}(\theta)$ e $\partial(p) = n$ temos que $\{1, \theta, \ldots, \theta^{n-1}\}$ é uma base de K. Assim,

$$\alpha_j = \sum_{i=1}^{n} c_{ij}\theta^{i-1}, \ \ (j = 1, \ldots, n) \ \text{ onde } \ c_{ij} \in \mathbb{Q},$$

e $m = \det[c_{ij}] \neq 0$. Portanto,

$$\Delta[\alpha_1, \ldots, \alpha_n] = m^2\Delta[1, \theta, \ldots, \theta^{n-1}].$$

Note que $\sigma_i(\theta^j) = \theta_i^j$. Então

$$d(p) = \Delta[1, \theta, \ldots, \theta^{n-1}] = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j)^2$$

é o *discriminante* de p. Assim,

$$d(p) = (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\theta_i - \theta_j) = (-1)^{\frac{n(n-1)}{2}} N(p'(\theta)),$$

em que p' é a derivada formal de p e $d(p) \in \mathbb{Q}$ Portanto, o discriminante de qualquer base de K é racional e não nulo.

Teorema 1.8 *Sejam K um corpo de número de grau n e $\mathcal{O}_K$ o seu anel de inteiros. Então*:

1. *$\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto n.*

2. *Qualquer ideal não nulo J em $\mathcal{O}_K$ é um $\mathbb{Z}$-módulo livre de posto n.*

Corolário 1.1 *Seja K um corpo de números de grau n. Então K possui pelo menos uma base integral.*

O discriminante de qualquer base integral de K chama-se o *discriminante do corpo K* e será denotado por δ_K. Assim, $\delta_K \neq 0$ e $\delta_K \in \mathbb{Z}$. Portanto, se $K = \mathbb{Q}(\theta)$, onde $\theta \in \mathcal{O}_K$, então

$$d(p) = m^2 \delta_K.$$

Neste caso,

$$\begin{aligned} m &= \left| \frac{\mathcal{O}_K}{\mathbb{Z} \oplus \mathbb{Z}\theta \oplus \cdots \oplus \mathbb{Z}\theta^{n-1}} \right| \\ &= [\mathcal{O}_K : \mathbb{Z} \oplus \mathbb{Z}\theta \oplus \cdots \oplus \mathbb{Z}\theta^{n-1}]. \end{aligned}$$

Em particular, $d(p)$ é um múltiplo quadrático de δ_K e

$$\delta_K \equiv 0 \text{ ou } 1 \pmod 4.$$

Uma *base minimal* para K é uma base integral com $|\delta_K|$ mínimo.

Proposição 1.4 *Sejam $K = \mathbb{Q}(\theta)$ um corpo de números de grau n, onde $\theta \in \mathcal{O}_K$, e $p = \text{irr}(\theta, \mathbb{Q})$. Então* $\text{Gal}(K/\mathbb{Q})$ *é um subgrupo de A_n se, e somente se, $d(p)$ é um quadrado em $\mathbb{Z}$.*

Prova. Sejam $\theta_i = \sigma_i(\theta),\ i = 1, \ldots, n$, os conjugados de θ e

$$D = \prod_{1 \leq i < j \leq n} (\theta_i - \theta_j).$$

Então é claro que $D \in \mathcal{O}_K$ e

$$\sigma(D) = \operatorname{sgn}(\sigma) D,\ \forall\ \sigma \in S_n.$$

Assim, $\sigma(D) = D$, para todo $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$. Portanto, $D \in \mathbb{Z}$ e $d(p)$ é um quadrado em $\mathbb{Z}$.

Reciprocamente, se $D \in \mathbb{Z}$, então $D \neq 0$, pois todas as raízes de p são distintas. Logo, $\operatorname{sgn}(\sigma) = 1$, para todo $\sigma \in \operatorname{Gal}(E/\mathbb{Q})$, pois $\sigma(D) = D$. Portanto, $\operatorname{Gal}(E/\mathbb{Q})$ é um subgrupo de A_n. Note que como A_n é um subgrupo normal de S_n temos que qualquer subgrupo de A_n depende somente de suas classes de conjugações. ■

1.3 Corpos Quadráticos e Ciclotômicos

Um *corpo quadrático* K sobre $\mathbb{Q}$ é um corpo de números de grau 2. Então, pelo Exemplo **??**, $K = \mathbb{Q}(\sqrt{d})$, com d livre de quadrados é um corpo quadrático. Note que se $\beta \in K$, então

$$\beta = \frac{a + b\sqrt{d}}{c},\ \text{ onde } a, b, c \in \mathbb{Z},\ \text{ e } \operatorname{mdc} c(a, b, c) = 1.$$

Assim, pelo Exemplo **??**,

$$\operatorname{Tr}(\beta) = \beta + \sigma_1(\beta) = \frac{2a}{c} \text{ e } N(\beta) = \beta\sigma_1(\beta) = \frac{a^2 - db^2}{c^2}.$$

Além disso,

$$\beta^2 = \operatorname{Tr}(\beta)\beta - N(\beta) \Leftrightarrow \beta^2 - \operatorname{Tr}(\beta)\beta + N(\beta) = 0.$$

Portanto, $\beta \in \mathcal{O}_K$ se, e somente se, $\operatorname{Tr}(\beta), N(\beta) \in \mathbb{Z}$, ou seja,

$$\begin{cases} \operatorname{Tr}(\beta) \equiv 0 \pmod{c} \\ N(\beta) \equiv 0 \pmod{c^2} \end{cases}$$

Teorema 1.9 *Sejam $K = \mathbb{Q}(\sqrt{d})$, d livre de quadrados, e $\mathcal{O}_K$ o anel dos inteiros. Então*:

1. $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ *se* $d \equiv 2$ *ou* $3 \pmod 4$. *Neste caso,* $\delta_K = 4d$ *e*

$$\left\{1, \sqrt{d}\right\}$$

é uma base integral para K.

2. $\mathcal{O}_K = \mathbb{Z}[\frac{1}{2}(1+\sqrt{d})]$ *se* $d \equiv 1 \pmod 4$. *Neste caso,* $\delta_K = d$ *e*

$$\left\{1, \frac{1+\sqrt{d}}{2}\right\}$$

é uma base integral para K.

Corolário 1.2 *Se* $d \equiv 1 \pmod 4$, *então qualquer elemento de* $\mathcal{O}_K$ *pode ser escrito sob a forma*

$$\frac{a+b\sqrt{d}}{2}, \ \ com \ a \equiv b \pmod 2.$$

Prova. Como

$$\left\{1, \frac{1+\sqrt{d}}{2}\right\}$$

é uma base integral para K temos que cada $\beta \in \mathcal{O}_K$ pode ser escrito de modo único so a forma

$$\beta = x + y\left(\frac{1+\sqrt{d}}{2}\right) = \frac{2x+y+y\sqrt{d}}{2}.$$

Pondo $a = 2x + y$ e $b = y$, obtemos

$$\beta = \frac{a+b\sqrt{d}}{2}, \ \text{com} \ a \equiv b \pmod 2.$$

Reciprocamente, se

$$\beta = \frac{a+b\sqrt{d}}{2}, \ \text{com} \ a \equiv b \pmod 2,$$

então

$$\beta = \frac{a+b\sqrt{d}}{2} = \frac{b+2x+b\sqrt{d}}{2} = x + b\left(\frac{1+\sqrt{d}}{2}\right).$$

Portanto, $\beta \in \mathcal{O}_K$. ■

Seja K uma extensão de $\mathbb{Q}$. Diremos que $\xi \in K$ é uma *raiz n-ésima da unidade* se ξ é uma raiz do polinômio

$$f = x^n - 1 \in \mathbb{Q}[x].$$

O conjunto

$$U_n(K) = \{\xi \in K : \xi^n = 1\},$$

chama-se o *conjunto das raízes n-ésimas das unidades* de K e é um subgrupo cíclico de K^* de ordem no máximo n. Se $\xi^n = 1$, mas $\xi^k \neq 1$, para $1 \leq k \leq n-1$, diremos que ξ é uma *raiz n-ésima primitiva da unidade* e denotaremos por $P_n(K)$ o conjunto de todas as raízes n-ésimas primitivas da unidade.

Exemplo 1.4 *Construir um corpo de decomposição sobre* $\mathbb{Q}$ *para o polinômio* $f = x^n - 1 \in \mathbb{Q}[x]$.

Solução. Seja $\xi = \xi_n = e^{\frac{2\pi}{n}i} \in \mathbb{C}$. Então, pela Fórmula De Moivre, ξ é uma raiz de f, pois

$$\xi^n = \left(\cos\frac{2\pi}{n} + i\,\mathrm{sen}\,\frac{2\pi}{n}\right)^n = \cos 2\pi + i\,\mathrm{sen}\,2\pi = 1.$$

Como $f' = nx^{n-1}$ temos que $\mathrm{mdc}(f, f') = 1$. Portanto, as raízes $1, \xi, \ldots, \xi^{n-1}$ são distintas. Assim, $K = \mathrm{Gal}(f, \mathbb{Q}) = \mathbb{Q}(\xi)$ é um corpo de decomposição de f sobre $\mathbb{Q}$. Neste caso,

$$f = x^n - 1 = \prod_{j=0}^{n-1}(x - \xi^j) \in K[x]$$

e K chama-se a *n-ésima extensão ciclotômica* de $\mathbb{Q}$. ■

Seja $K = \mathbb{Q}(\xi)$ a n-ésima extensão ciclotômica de $\mathbb{Q}$. O polinômio

$$\Phi_n = \prod_{\xi \in P_n(K)} (x - \xi) = \prod_{k \in U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)} (x - \xi^k)$$

chama-se o *n-ésimo polinômio ciclotômico* sobre K. Note que

$$x^n - 1 = \prod_{d|n} \Phi_d$$

e $\Phi_n \in \mathbb{Z}[x]$, para todo $n \in \mathbb{N}$, pois

$$x^n - 1 = \Phi_n \prod_{d|n, d \neq n} \Phi_d = \Phi_n g,$$

com g um polinômio mônico de grau menor do que n, e o resultado segue do Lema de Gauss. Por exemplo, $\Phi_1 = x - 1$, $\Phi_2 = x + 1$, $\Phi_4 = x^2 + 1$ e

$$x^8 - 1 = \Phi_1\Phi_2\Phi_4\Phi_8.$$

Portanto, $\Phi_8 = x^4 + 1$.

Teorema 1.10 *Seja* $K = \mathbb{Q}(\xi)$ *a n-ésima extensão ciclotômica de* $\mathbb{Q}$.

1. *Qualquer polinômio ciclotômico sobre* $\mathbb{Z}$ *é irredutível.*

2. *$K/\mathbb{Q}$ é uma extensão Galoisiana e*

$$\mathrm{Gal}\,(K/\mathbb{Q}) = \{\sigma_k : \mathrm{mdc}(n,k) = 1, \textit{onde } \sigma_k(\xi) = \xi^k\} \simeq U\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right).$$

Neste caso, $|\mathrm{Gal}\,(K/\mathbb{Q})| = \phi(n)$, onde ϕ é a função de Euler, e $K/\mathbb{Q}$ é uma extensão abeliana.

3. *O anel dos inteiros de K é $\mathcal{O}_K = \mathbb{Z}[\xi]$ e*

$$\left\{1, \xi, \xi^2, \ldots, \xi^{\phi(n)-1}\right\}$$

é uma base integral de K sobre $\mathbb{Q}$. Neste caso,

$$\delta_K = (-1)^{\frac{\phi(n)}{2}\cdot s} \cdot \frac{n^{\phi(n)}}{\prod\limits_{p|n} p^{\frac{\phi(n)}{p-1}}},$$

em que s é o número de primos distintos na fatoração de n.

4. *O anel dos inteiros de $F = \mathbb{Q}(\xi + \xi^{-1}) \subset K$ é $\mathcal{O}_K = \mathbb{Z}[\xi + \xi^{-1}]$ e*

$$\left\{1, \xi + \xi^{-1}, \xi^2 + \xi^{-2}, \ldots, \xi^{\frac{\phi(n)}{2}-1} + \xi^{-\frac{\phi(n)}{2}+1}\right\}$$

é uma base integral de F sobre $\mathbb{Q}$.

Exemplo 1.5 *Sejam*

$$\xi = e^{\frac{2\pi}{9}i} \in \mathbb{C}$$

a raiz nona da unidade e $F = \mathbb{Q}(\alpha)$, onde $\alpha = \xi + \xi^{-1} = 2\cos\left(\frac{2\pi}{9}\right) \in \mathbb{R}$. Então $\mathrm{Gal}(F/\mathbb{Q}) \simeq \frac{\mathbb{Z}}{3\mathbb{Z}}$.

Solução. Note que

$$\begin{aligned} f &= (x - (\xi + \xi^{-1}))(x - (\xi^2 + \xi^{-2}))(x - (\xi^4 + \xi^{-4})) \\ &= 1 - 3x + x^3 \in \mathbb{Q}[x], \end{aligned}$$

pois $\xi^9 = 1$. É claro que f é irredutível sobre $\mathbb{Q}$ e que F é o corpo de decomposição de f, pois se $\alpha_1 = \alpha$, $\alpha_2 = \xi^2 + \xi^{-2}$ e $\alpha_3 = \xi^4 + \xi^{-4}$, então

$$\alpha_1^2 = \alpha_2 + 2, \;\; \alpha_2^2 = \alpha_3 + 2 \;\text{ e }\; \alpha_3^2 = \alpha_1 + 2.$$

Já vimos que cada elemento $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$ é completamente determinado por $\sigma(\alpha_1)$, digamos $\sigma_i(\alpha_1) = \alpha_i$, $i = 1, 2, 3$. É claro que $\sigma_1 = I$. Se $\sigma_2(\alpha_1) = \alpha_2$, então

$$\sigma_2(\alpha_2) = \sigma_2(\alpha_1^2 - 2) = \alpha_2^2 - 2 = \alpha_3$$

e de modo inteiramente análogo, obtemos $\sigma_2(\alpha_3) = \alpha_1$, $\sigma_2^2 = \sigma_3$ e $\sigma_2^3 = \sigma_1$. Portanto,

$$\mathrm{Gal}(F/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3\} = \langle \sigma_2 \rangle \simeq A_3 \simeq \frac{\mathbb{Z}}{3\mathbb{Z}},$$

que é o resultado desejado. ■

Teorema 1.11 *Sejam F um corpo contendo uma raiz n-ésima da unidade e $f = x^n - c \in F[x]$. Se $K = \mathrm{Gal}(f, F)$, então existe um homomorfismo de grupos injetor*

$$\varphi : \mathrm{Gal}(K/F) \to \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

Além disso, f é irredutível se, e somente se, φ é sobrejetora. Neste caso, $[K : F] = n$ e K/F é uma extensão abeliana.

Prova. É claro que $\alpha = \sqrt[n]{c} \in \mathbb{C}$ é uma raiz de f. Seja $\beta \in \mathbb{C}$ uma raiz qualquer de f. Então

$$\left(\frac{\beta}{\alpha}\right)^n = \frac{\beta^n}{\alpha^n} = \frac{c}{c} = 1.$$

Logo, $\beta = \alpha\xi$, em que ξ é uma raiz do polinômio $g = x^n - 1 \in \mathbb{Q}[x]$. Assim, as raízes distintas de f são

$$\alpha, \alpha\xi, \ldots, \alpha\xi^{n-1}.$$

Portanto, $K = \mathrm{Gal}(f, F) = F(\alpha)$ é um corpo de decomposição de f.

Agora, se $\sigma \in \mathrm{Gal}(K/F)$, então σ é completamente determinada pelo valor k, onde $\sigma(\alpha) = \alpha\xi^k$. É fácil verificar que a função

$$\varphi : \mathrm{Gal}(K/F) \to \frac{\mathbb{Z}}{n\mathbb{Z}}$$

definida como $\varphi(\sigma) = k + n\mathbb{Z}$ é um homomorfismo de grupos injetor. ■

1.4 Ordens

O objetivo principal desta seção é classificar todas as "ordens" de um corpo quadrático.

Seja K um corpo de números de grau n. Um subconjunto $\mathcal{O}$ de K é uma *ordem* em K se as seguintes condições são satisfeitas:

1. $\mathcal{O}$ é um subanel de K, com a mesma unidade de K.

2. $\mathcal{O}$ é um $\mathbb{Z}$-módulo finitamente gerado.

3. O posto de $\mathcal{O}$ é máximo n.

Note que a condição (3) afirma que $\mathcal{O}$ contém uma base de K sobre $\mathbb{Q}$. Neste caso, $K = \mathbb{Q}\mathcal{O}$.

Sejam $K = \mathbb{Q}(\sqrt{d})$, d livre de quadrados, e $\mathcal{O}_K$ seu anel dos inteiros. Com o objetivo de simplificar a notação vamos por

$$k = \begin{cases} 1, & \text{se } d \not\equiv 1 \pmod 4 \\ 2, & \text{se } d \equiv 1 \pmod 4 \end{cases}$$

e definir

$$\eta = \frac{k - 1 + \sqrt{d}}{k}.$$

Assim, $\beta \in \mathcal{O}_K$ se, e somente se, existem $x, y \in \mathbb{Z}$ tais que

$$\beta = x + y\eta.$$

Sejam $\mathcal{O}$ uma ordem em K e $\{\alpha_1, \alpha_2\}$ uma base para $\mathcal{O}$. Então, pelo Exemplo **??**,

$$\begin{aligned} \Delta(\alpha_1, \alpha_2) &= \{\det[\sigma_i(\alpha_j)]\}^2 = \begin{bmatrix} \alpha_1 & \alpha_2 \\ \sigma_1(\alpha_1) & \sigma_1(\alpha_2) \end{bmatrix}^2 \\ &= (\alpha_1\sigma_1(\alpha_2) - \alpha_2\sigma_1(\alpha_1))^2 . \end{aligned}$$

Em particular,

$$\delta_K = \Delta(1, \eta) = (\sigma_1(\eta) - \eta)^2 = \left(\frac{2}{k}\right)^2 d.$$

Teorema 1.12 *Com as notações acima, temos que qualquer ordem de $K = \mathbb{Q}(\eta)$ é da forma $\mathbb{Z}[m\eta]$, para algum $m \in \mathbb{N}$. Além disso, se $m > 1$, então $\mathbb{Z}[m\eta]$ não é um ideal em $\mathcal{O}_K = \mathbb{Z}[\eta]$.*

Prova. É claro que $\mathbb{Z}[m\eta]$ é uma ordem de K, para todo $m \in \mathbb{N}$, pois

$$\mathbb{Z}[m\eta] = \{a + bm\eta : a, b \in \mathbb{Z}\}$$

Por outro lado, seja $\{\alpha_1, \alpha_2\}$ uma base para $\mathcal{O}$. Como $1 \in \mathcal{O}$ temos que existem $x, y \in \mathbb{Z}$ tais que

$$1 = x\alpha_1 + y\alpha_2.$$

Pondo $D = \text{mdc}(x, y)$, existem $r, s \in \mathbb{Z}$ tais que

$$rx - sy = D \Leftrightarrow r\left(\frac{x}{D}\right) - s\left(\frac{y}{D}\right) = 1.$$

Sendo

$$\begin{bmatrix} \frac{1}{D} \\ \beta \end{bmatrix} = \begin{bmatrix} \frac{x}{D} & \frac{y}{D} \\ s & r \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \end{bmatrix},$$

em que $\beta = s\alpha_1 + r\alpha_2$, teremos uma nova base

$$\left\{\frac{1}{D}, \beta\right\}$$

para $\mathcal{O}$, pois

$$\det\left(\begin{bmatrix} \frac{x}{D} & \frac{y}{D} \\ s & r \end{bmatrix}\right) = r\left(\frac{x}{D}\right) - s\left(\frac{y}{D}\right) = 1.$$

Afirmação. $D = 1$.

De fato, se $D > 1$, então

$$\frac{1}{D^2} \in \mathcal{O}, \text{ pois } \frac{1}{D} \in \mathcal{O}.$$

Assim, existem $u, v \in \mathbb{Z}$ tais que

$$\frac{1}{D^2} = \frac{u}{D} + v\beta \Rightarrow \beta = \frac{1}{vD^2} - \frac{u}{vD} \in \mathbb{Q},$$

o que é um absurdo. Portanto, $\{1, \beta\}$ é uma base para $\mathcal{O}$.

Finalmente, como $\beta^2 \in \mathcal{O}$ temos que existem $b, c \in \mathbb{Z}$ tais que

$$\beta^2 = c + b\beta \Leftrightarrow \beta^2 - b\beta - c = 0,$$

ou seja, $\beta \in \mathcal{O}_K$. Logo, existem $f, m \in \mathbb{Z}$, com $m > 0$, tais que

$$\beta = f + m\eta$$

Portanto, $\mathcal{O} \subseteq \mathcal{O}_K$ e

$$\begin{aligned} \mathcal{O} &= \{a + b\beta : a, b \in \mathbb{Z}\} \\ &= \{a + b(f + m\eta) : a, b \in \mathbb{Z}\} \\ &= \{(a + bf) + b(m\eta) : a, b \in \mathbb{Z}\}, \end{aligned}$$

ou seja, $\mathcal{O} = \mathbb{Z}[m\eta]$, para algum $m \in \mathbb{N}$. ■

Observação 1.3 *Como $\{1, m\eta\}$ é uma base para $\mathcal{O}$ temos que*

$$\begin{aligned} \Delta(1, m\eta) &= (\sigma_1(m\eta) - m\eta)^2 = m^2(\sigma_1(\eta) - \eta)^2 = m^2\delta_K \\ &= \left(\frac{2m}{k}\right)^2 d. \end{aligned}$$

Teorema 1.13 *Seja K um corpo de número de grau n. Então as seguintes condições são equivalentes*:

1. *A função $T : K \to \mathbb{Q}$ definida como $T(\alpha) = \mathrm{Tr}(\alpha)$ é linear sobre $\mathbb{Q}$ e sobrejetora.*

2. *A função T não é identicamente nula.*

3. *A forma bilinear $b : K \times K \to \mathbb{Q}$ definida por $b(\alpha, \beta) = \mathrm{Tr}(\alpha\beta)$ é não degenerada.*

Prova. $(1 \Rightarrow 2)$ É claro. Para provar que $(2 \Rightarrow 1)$, suponhamos que $T \neq 0$. Então existe $\alpha \in K$, com $T(\alpha) = b \neq 0$. Logo,

$$T(cb^{-1}\alpha) = cb^{-1}T(\alpha) = cb^{-1}b = c, \ \ \forall \ c \in \mathbb{Q}.$$

Portanto, T é sobrejetora.

$(1 \Rightarrow 3)$ Suponhamos que T seja sobrejetora. Então existe $\alpha \in K^*$ tal que $T(\alpha) \neq 0$. Dado $\beta \in K^*$, existe $\alpha\beta^{-1} \in K$ tal que

$$b(\alpha\beta^{-1}, \beta) = T(\alpha\beta^{-1}\beta) = T(\alpha) \neq 0.$$

Portanto, b é não degenerada.

$(3 \Rightarrow 1)$ Segue da definição. ■

Teorema 1.14 *Sejam K um corpo de números de grau n e $\varphi : K \to \mathbb{Q}$ uma função linear sobre $\mathbb{Q}$. Então existe um único $\alpha \in K$ tal que $\varphi(\beta) = \mathrm{Tr}(\alpha\beta)$, para todo $\beta \in K$.*

Prova. Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base para K. Então, pelo item (3) Teorema **??**, o sistema de equações lineares

$$\sum_{i=1}^{n} \mathrm{Tr}(\alpha_i\alpha_j)x_i = \varphi(\alpha_j), \ \ j = 1, \ldots, n,$$

possui uma única solução $c_1, \ldots, c_n \in \mathbb{Q}$. Portanto, existe um único

$$\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n \in K$$

tal que $\varphi(\beta) = \mathrm{Tr}(\alpha\beta)$. ■

Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base para K. Então para qualquer $\alpha \in K$ existem únicos $c_1(\alpha), \ldots, c_n(\alpha) \in \mathbb{Q}$ tais que

$$\alpha = c_1(\alpha)\alpha_1 + \cdots + c_n(\alpha)\alpha_n \in K.$$

Assim, as funções $f_j : K \to \mathbb{Q}$ definidas como $f_j(\alpha) = c_j(\alpha)$, $j = 1, \ldots, n$, são claramente lineares sobre $\mathbb{Q}$. Logo, pelo Teorema **??**, existem únicos $\beta_j \in K$ tais que $f_j(\alpha) = \mathrm{Tr}(\beta_j \alpha)$, para todo $\alpha \in K$. Pondo $\alpha = \alpha_i$, $i = 1, \ldots, n$, obtemos

$$\mathrm{Tr}(\beta_j \alpha_i) = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases}$$

Além disso, $\{\beta_1, \ldots, \beta_n\}$ é uma nova base para K, pois se

$$b_1\beta_1 + \cdots + b_n\beta_n = 0,$$

então

$$0 = \mathrm{Tr}(0\alpha_i) = \mathrm{Tr}(b_1\beta_1\alpha_i + \cdots + b_n\beta_n\alpha_i) = b_i, \;\; i = 1, \ldots, n.$$

Portanto, para qualquer base $\{\alpha_1, \ldots, \alpha_n\}$ para K existe uma única base $\{\beta_1, \ldots, \beta_n\}$ para K tal que

$$\mathrm{Tr}(\beta_j \alpha_i) = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases}$$

e, para todo $\alpha \in K$, teremos

$$\alpha = \mathrm{Tr}(\alpha_1\alpha)\beta_1 + \cdots + \mathrm{Tr}(\alpha_n\alpha)\beta_n,$$

pois

$$\alpha = d_1\beta_1 + \cdots + d_n\beta_n \Rightarrow \mathrm{Tr}(\alpha_i\alpha) = d_i, \;\; i = 1, \ldots, n.$$

A base $\{\beta_1, \ldots, \beta_n\}$ chama-se a *base dual* da base $\{\alpha_1, \ldots, \alpha_n\}$. Consequentemente, $\{\alpha_1, \ldots, \alpha_n\}$ é uma base dual de $\{\beta_1, \ldots, \beta_n\}$ e, para todo $\alpha \in K$, teremos

$$\alpha = \mathrm{Tr}(\beta_1\alpha)\alpha_1 + \cdots + \mathrm{Tr}(\beta_n\alpha)\alpha_n.$$

Corolário 1.3 *Com os dados do Teorema* **??**, *a função* $T : K \to \mathcal{L}(K, \mathbb{Q})$ *definida como* $T(\alpha) = \varphi$ *é um isomorfismo sobre* $\mathbb{Q}$, *em que* $\varphi(\beta) = \mathrm{Tr}(\alpha\beta)$.

Proposição 1.5 *Sejam* K *um corpo de números de grau* n *e* $\mathcal{O}_K$ *seu anel dos inteiros. Sejam* $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$ *uma base de* K *e* $\{\beta_1, \ldots, \beta_n\}$ *a sua base dual. Então*

$$\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n \subseteq \mathcal{O}_K \subseteq \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n.$$

Prova. Dado $\alpha \in \mathcal{O}_K$,

$$\alpha = \mathrm{Tr}(\alpha_1\alpha)\beta_1 + \cdots + \mathrm{Tr}(\alpha_n\alpha)\beta_n.$$

Como $\mathrm{Tr}(\alpha_i\alpha) \in \mathbb{Z}$ temos que

$$\alpha \in \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n.$$

Portanto,

$$\mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n \subseteq \mathcal{O}_K \subseteq \mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n.$$

Observe que

$$\mathbb{Z}\beta_1 \oplus \cdots \oplus \mathbb{Z}\beta_n = \{\beta \in K : \mathrm{Tr}(\alpha\beta) \in \mathbb{Z},\ \forall\ \alpha \in \mathcal{O}\},$$

onde $\mathcal{O} = \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n$. ■

Note que se $\mathbf{M} = [\sigma_i(\alpha_j)]$, então

$$\mathbf{M}^{-1} = \frac{1}{\det \mathbf{M}} \mathrm{adj}(\mathbf{M}) \text{ e } \delta_K\mathcal{O}_K \subseteq \mathbb{Z}\alpha_1 \oplus \cdots \oplus \mathbb{Z}\alpha_n.$$

Teorema 1.15 *Sejam K um corpo de números de grau n e $\mathcal{O}$ uma ordem qualquer em K. Se $\alpha_1, \ldots, \alpha_r \in \mathcal{O}_K$, então $\mathcal{O}[\alpha_1, \ldots, \alpha_r]$ é uma ordem em K.*

Prova. Como $\mathcal{O} \subseteq \mathcal{O}[\alpha]$ temos que $\mathcal{O}[\alpha]$ contém n elementos linearmente independentes sobre $\mathbb{Z}$. Assim, resta provar que $\mathcal{O}[\alpha]$ é um $\mathbb{Z}$-módulo. Seja $\{\beta_1, \ldots, \beta_n\}$ uma base qualquer para $\mathcal{O}$. Sendo

$$\alpha^k = b_0 + b_1\alpha + \cdots + b_{m-1}\alpha^{m-1},\ \forall\ k \in \mathbb{N},$$

com $m = \partial(\mathrm{irr}(\alpha, \mathbb{Z}))$, teremos que qualquer $\beta \in \mathcal{O}[\alpha]$ pode ser escrito sob a forma

$$\beta = \sum_{j=1}^{m-1}\sum_{i=1}^{n} c_{ij}\beta_i\alpha^j.$$

Portanto, $\mathcal{O}[\alpha]$ é um $\mathbb{Z}$-módulo finitamente gerado. O resto da prova segue por indução sobre r. ■

Teorema 1.16 *Seja K um corpo de números de grau n. Então $\mathcal{O}_K$ é a ordem maximal em K.*

Prova. Seja $\mathcal{O}$ qualquer ordem em K. Então, pelo Teorema **??**, $\mathcal{O} \subseteq \mathcal{O}_K$. Seja $\{\beta_1, \ldots, \beta_n\}$ uma base qualquer para $\mathcal{O}$ e $\{\gamma_1, \ldots, \gamma_n\}$ a base dual. Então, pela prova da Proposição **??**,

$$\mathcal{O}_K \subseteq \mathbb{Z}\gamma_1 \oplus \cdots \oplus \mathbb{Z}\gamma_n.$$

Portanto, $\mathcal{O}_K$ é a ordem maximal em K. ■

Sejam K um corpo de número de grau n e $\mathcal{O}$ uma ordem qualquer em K. O *discriminante ideal* de $\mathcal{O}$ sobre $\mathbb{Z}$, denotado por $d(\mathcal{O})$, é igual a "raiz quadrada" do ideal $\mathcal{I}_K$ em $\mathbb{Z}$ gerado pelo conjunto

$$T = \{\det(\mathrm{Tr}(\alpha_i\alpha_j)) : 0 \leq i, j \leq n\},$$

onde $\alpha_i \in \mathcal{O}$, ou seja,

$$\mathcal{I}_K = \{a_1x_1 + \cdots + a_kx_k : k \in \mathbb{N},\ a_i \in \mathbb{Z} \text{ e } x_i \in T\}$$

Note que $d(\mathcal{O}) \neq \{0\}$, pois a forma bilinear associada a Tr é não degenerada. Portanto, se J é ideal não nulo em $\mathcal{O}$, então J é um $\mathbb{Z}$-módulo livre de posto n.

Teorema 1.17 *Sejam K um corpo de número de grau n e $\mathcal{O}$ uma ordem qualquer em K (em $\mathcal{O}_K$). Para todas as bases $\{\alpha_1, \ldots, \alpha_n\}$ de $\mathcal{O}$ os discriminantes $\Delta(\alpha_1, \ldots, \alpha_n)$ coincidem. Em particular, os discriminantes de todas as bases integrais de $\mathcal{O}_K$ coincidem.*

Teorema 1.18 *Sejam K um corpo de número de grau n e $\theta \in \mathcal{O}_K$. Então as seguintes condições são equivalentes*:

1. $\mathcal{O}_K = \mathbb{Z}[\theta]$.
2. $\{1, \theta, \ldots, \theta^{n-1}\}$ *é uma base integral para* $\mathcal{O}_K$.
3. $\delta_K = \Delta(1, \theta, \ldots, \theta^{n-1})$.

Vamos finalizar esta seção com um estudo detalhado do corpo $K = \mathrm{Gal}(f, \mathbb{Q})$, onde

$$f = x^3 - 3x + 1 \in \mathbb{Z}[x].$$

É claro que f é irredutível sobre $\mathbb{Q}$. Seja $\theta \in \mathbb{C}$ uma raiz de f. Então, pelo Exemplo **??**, $K = \mathbb{Q}(\theta)$, onde $\theta \in \mathcal{O}_K$ e $\{1, \theta, \theta^2\}$ é uma base de K sobre $\mathbb{Q}$. Logo, cada $\alpha \in K$

pode ser escrito de modo único sob a forma $\alpha = a + b\theta + c\theta^2$, onde $a, b, c \in \mathbb{Q}$. Assim,

$$\begin{aligned} L_\alpha(1) &= \alpha \cdot 1 = a + b\theta + c\theta^2 \\ L_\alpha(\theta) &= \alpha \cdot \theta = -c + (a + 3c)\theta + b\theta^2 \\ L_\alpha(\theta^2) &= \alpha \cdot \theta^2 = -b + (3b - c)\theta + (a + 3c)\theta^2 \end{aligned}$$

pois $\theta^3 = 3\theta - 1$ e $\theta^4 = 3\theta^2 - \theta$. Portanto, $K = \mathbb{Q}(\theta)$ é isomorfo ao conjunto das matrizes da forma

$$\mathbf{A}_\alpha = \begin{bmatrix} a & -c & -b \\ b & a + 3c & 3b - c \\ c & b & a + 3c \end{bmatrix}, \text{ onde } a, b, c \in \mathbb{Q}.$$

Neste caso,

$$\begin{aligned} f_\alpha(x) &= \det(x\mathbf{I} - \mathbf{A}_\alpha) \\ &= x^3 + b_1 x^2 + b_2 x + b_3 \end{aligned}$$

em que

$$\begin{aligned} b_1 &= -\operatorname{Tr}(\alpha) = -(3a + 6c), \\ b_2 &= 3a^2 + 12ac - 3b^2 + 3bc + 9c^2 \\ b_3 &= -N(\alpha) = -(a^3 + 6a^2c - 3ab^2 + 3abc + 9ac^2 - b^3 + 3bc^2 + c^3). \end{aligned}$$

Portanto,

$$\begin{aligned} d(f) &= \det \begin{bmatrix} \operatorname{Tr}(1) & \operatorname{Tr}(\theta) & \operatorname{Tr}(\theta^2) \\ \operatorname{Tr}(\theta) & \operatorname{Tr}(\theta^2) & \operatorname{Tr}(\theta^3) \\ \operatorname{Tr}(\theta^2) & \operatorname{Tr}(\theta^3) & \operatorname{Tr}(\theta^4) \end{bmatrix} \\ &= \det \begin{bmatrix} 3 & 0 & 6 \\ 0 & 6 & -3 \\ 6 & -3 & 18 \end{bmatrix} \\ &= 81. \end{aligned}$$

Poderíamos também obter o discriminante de f da seguinte maneira: como

$$f'(\theta) = 3\theta^2 - 3 = -3 + 3\theta^2$$

temos que

$$\begin{aligned} d(f) &= (-1)^{\frac{3(3-1)}{2}} N(f'(\theta)) \\ &= -[(-3)^3 + 6(-3)^2 3 + 9(-3)3^2 + 3^3] \\ &= 81. \end{aligned}$$

Note que $d(f) = 9^2$ é um quadrado em $\mathbb{Z}$ e $\mathrm{Gal}(K/\mathbb{Q}) = \langle\sigma\rangle = \{I, \sigma, \sigma^2\}$, com $\sigma(\theta) = \alpha_2$, $\sigma^2(\theta) = \alpha_3$; $\alpha_1 = \theta$, α_2 e α_3 são as raízes de f.

Agora, vamos determinar uma base integral para K. Primeiro note que

$$m = \left|\frac{\mathcal{O}_K}{\mathbb{Z} \oplus \mathbb{Z}\theta \oplus \mathbb{Z}\theta^2}\right| = \left|\frac{\mathcal{O}_K}{\mathbb{Z}[\theta]}\right| \geq 1.$$

É fácil verificar que qualquer $\beta \in K$ pode ser escrito sob a forma

$$\beta = \frac{1}{D}(u + v\theta + w\theta^2),$$

onde $u, v, w, D \in \mathbb{Z}$ e $\mathrm{mdc}(u, v, w, D) = 1$. Como $[K : \mathbb{Q}] = 3$ temos que o polinômio minimal de β é da forma

$$\begin{aligned} p &= (x - \beta)(x - \sigma(\beta))(x - \sigma^2(\beta)) \\ &= \prod_{i=1}^{3} \left(x - \frac{u}{D} - \frac{v}{D}\alpha_i - \frac{w}{D}\alpha_i^2\right) \\ &= x^3 - \frac{\mathrm{Tr}(\beta)}{D}x^2 + \frac{b_2}{D^2}x - \frac{N(\beta)}{D^3} \end{aligned}$$

onde

$$\begin{aligned} \mathrm{Tr}(\beta) &= 3(u + 2w) \\ b_2 &= 3(u^2 + 4uv - v^2 + vw + 3w^2) \\ N(\beta) &= u^3 + 6u^2w - 3uv^2 + 3uvw + 9uw^2 - v^3 + 3vw^2 + w^3 \end{aligned}$$

Assim, $\beta \in \mathcal{O}_K$ se, e somente se,

$$\begin{cases} \mathrm{Tr}(\beta) \equiv 0 \pmod{D} \\ b_2 \equiv 0 \pmod{D^2} \\ N(\beta) \equiv 0 \pmod{D^3}. \end{cases}$$

Se existisse um número primo p tal que p divide D, u e w, então, por b_2, p^2 divide $v(4u - v + w)$. Logo, p divide v, o que é impossível. Portanto, $\mathrm{mdc}(D, u, w) = 1$.

Afirmação. $D = 1$.

De fato, se $D > 1$, então $D = 3$ e $\text{mdc}(3, u) = \text{mdc}(3, w) = 1$. Logo, $\text{mdc}(3, v) = 1$ e por $N(\beta)$

$$u - v + w \equiv 0 \,(\text{mod}\, 3).$$

Assim, existem apenas duas possibilidades: $u \equiv w \equiv 1 \,(\text{mod}\, 3)$, $v \equiv -1 \,(\text{mod}\, 3)$ ou $u \equiv w \equiv -1 \,(\text{mod}\, 3)$, $v \equiv 1 \,(\text{mod}\, 3)$. Se $u \equiv w \equiv 1 \,(\text{mod}\, 3)$, $v \equiv -1 \,(\text{mod}\, 3)$, digamos $u = 3r + 1$, $w = 3s + 1$ e $v = 3t - 1$, então

$$\begin{aligned} N(\beta) &= 27r^3 + 162r^2s + 81r^2 + 243rs^2 + 81rst + 243rs - 81rt^2 + 81rt \\ &\quad +54r + 27s^3 + 81s^2t + 81s^2 + 81st + 54s - 27t^3 + 27t + 9. \end{aligned}$$

Assim,

$$9 \equiv 0 \,(\text{mod}\, 27),$$

o que é impossível. Se $u \equiv w \equiv -1 \,(\text{mod}\, 3)$, $v \equiv 1 \,(\text{mod}\, 3)$, obtemos de modo análogo

$$-9 \equiv 0 \,(\text{mod}\, 27).$$

Portanto, $D = 1$ e $\beta \in \mathbb{Z}[\theta]$. Consequentemente, $\mathcal{O}_K = \mathbb{Z}[\theta]$ e $\{1, \theta, \theta^2\}$ é uma base integral para K.

Finalmente, vamos determinar a base dual de $\{1, \theta, \theta^2\}$. Seja $\{\beta_1, \beta_2, \beta_3\}$ a base dual de $\{1, \theta, \theta^2\}$. Então

$$\text{Tr}(\beta_j \theta^{i-1}) = \begin{cases} 1, & \text{se } i = j \\ 0, & \text{se } i \neq j \end{cases}$$

Como

$$\beta_j = a_{1j} + a_{2j}\theta + a_{3j}\theta^2, \;\; j = 1, 2, 3,$$

temos que

$$\begin{cases} \text{Tr}(\beta_1) = 1 \\ \text{Tr}(\beta_1\theta) = 0 \\ \text{Tr}(\beta_1\theta^2) = 0 \end{cases} \Leftrightarrow \begin{cases} 3a_{11} + 0a_{21} + 6a_{31} = 1 \\ 0a_{11} + 6a_{21} - 3a_{31} = 0 \\ 6a_{11} - 3a_{21} + 18a_{31} = 0 \end{cases}$$

Logo,

$$a_{11} = \frac{11}{9}, \;\; a_{21} = -\frac{2}{9} \text{ e } a_{31} = -\frac{4}{9}$$

e

$$\beta_1 = \frac{1}{9}(11 - 2\theta - 4\theta^2).$$

De modo análogo, obtemos

$$\beta_2 = \frac{1}{9}(-2 + 2\theta + \theta^2) \text{ e } \beta_3 = \frac{1}{9}(-4 + \theta + 2\theta^2).$$

Portanto, pelo Teorema **??**, teremos

$$\mathcal{O}_K \subseteq \mathbb{Z}\beta_1 \oplus \mathbb{Z}\beta_2 \oplus \mathbb{Z}\beta_3.$$

Se

$$\mathbf{C} = \frac{1}{9}\begin{bmatrix} 11 & -2 & -4 \\ -2 & 2 & 1 \\ -4 & 1 & 2 \end{bmatrix}$$

então

$$\Delta(\beta_1, \beta_2, \beta_3) = (\det \mathbf{C})^2 \Delta(\{1, \theta, \theta^2\}) = \frac{1}{81} \notin \mathbb{Z}.$$

Consequentemente, $\{\beta_1, \beta_2, \beta_3\}$ não é uma base integral para K. Mas

$$\delta_K \left(\mathbb{Z}\beta_1 \oplus \mathbb{Z}\beta_2 \oplus \mathbb{Z}\beta_3\right) \subseteq \mathcal{O}_K.$$

Capítulo 2

Álgebras com Divisão Cíclicas

Neste capítulo apresentaremos as principais definições e resultados básicos sobre álgebras, que serão necessários para os capítulos subsequentes. O leitor interessado em mais detalhes pode consultar [**?**, **?**, **?**].

2.1 Álgebras

Salvo menção explícita em contrário, a palavra anel nesta dissertação significa anel com unidade.

Já vimos que se K é um corpo de números de grau n, então existe $\theta \in \mathcal{O}_K$ tal que $K = \mathbb{Q}(\theta)$ e $\partial(\text{irr}(\theta, \mathbb{Q})) = n$. Além disso, K é um espaço vetorial sobre $\mathbb{Q}$, pois essas operações já existem de modo natural no corpo K. Note que a condição

$$c(\alpha\beta) = (c\alpha)\beta = \alpha(c\beta), \ \ \forall \ c \in \mathbb{Q} \ \text{ e } \ \alpha, \beta \in K,$$

é claramente satisfeita em K, de modo que a multiplicação sobre K é bilinear sobre $\mathbb{Q}$. Isto motiva a seguinte definição:

Seja K um corpo. Uma *álgebra* sobre K ou uma K-*álgebra* é um anel $\mathcal{A}$ tal que $V = (\mathcal{A}, +)$ é um espaço vetorial sobre K e o seguinte axioma é satisfeito

$$c(\alpha\beta) = (c\alpha)\beta = \alpha(c\beta), \ \ \forall \ c \in K \ \text{ e } \ \alpha, \beta \in \mathcal{A},$$

de modo que a multiplicação sobre $\mathcal{A}$ é bilinear. O *posto* e uma *base* de uma álgebra $\mathcal{A}$ significa o posto e uma base, respectivamente, do espaço vetorial V sobre K.

Seja $\mathcal{A}$ uma álgebra sobre K. Diremos que $\mathcal{A}$ é uma *álgebra com divisão* se qualquer elemento não nulo α em $\mathcal{A}$ possui um inverso em $\mathcal{A}$, isto é,

$$\mathcal{U}(\mathcal{A}) = \mathcal{A} - \{0\} = \mathcal{A}^*.$$

Proposição 2.1 *Seja $\mathcal{A}$ uma álgebra de dimensão n sobre K. Então as seguintes condições são equivalentes*:

1. *$\mathcal{A}$ é uma álgebra com divisão.*

2. *$\mathcal{A}$ não possui divisores de zero.*

Sejam K um corpo, V um espaço vetorial de dimensão n sobre K e $\mathcal{A} = \mathrm{End}_K(V)$ o conjunto de todas as transformações lineares de V em V. Então $\mathcal{A}$ munido com as operações de adição $\phi + \varphi$ definida como

$$(\phi + \varphi)(\alpha) = \phi(\alpha) + \varphi(\alpha), \ \ \forall \ \alpha \in V,$$

e composição externa $c\phi$ definida como

$$(c\phi)(\alpha) = c\phi(\alpha), \ \ \forall \ c \in K \ \text{ e } \ \alpha \in V,$$

é um espaço vetorial de dimensão n^2 sobre K, com uma base ordenada lexicograficamente

$$B = \{f_{ij} : i, j = 1, \ldots, n\},$$

isto é,

$$f_{11}, \ldots, f_{1n}, f_{21}, \ldots, f_{2n}, \ldots, f_{n1}, \ldots, f_{nn},$$

em que

$$f_{ij}(\alpha_k) = \delta_{jk}\alpha_i = \begin{cases} \alpha_i, & \text{se } \ j = k \\ 0, & \text{se } \ j \neq k. \end{cases}$$

O produto dos elementos básicos em $\mathcal{A}$ é dado por

$$f_{ij}f_{kl} = \delta_{jk}f_{il} = \begin{cases} f_{il}, & \text{se } \ j = k \\ 0, & \text{se } \ j \neq k \end{cases} \quad \text{e } \ 0f_{ij} = f_{ij}0 = 0.$$

Assim, cada $\phi \in \mathcal{A}$ pode ser escrito de modo único sob a forma

$$\phi = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}f_{ij}.$$

Finalmente, $\mathcal{A}$ munido com a operação de composição de funções $\phi\varphi$ definida como

$$(\phi\varphi)(\alpha) = \phi(\varphi(\alpha)), \ \ \forall \ \alpha \in V,$$

é um anel não comutativo com identidade, chamado de *endomorfismo de aneis*. Portanto, $\mathcal{A} = \mathrm{End}_K(V)$ é uma álgebra sobre K, pois

$$c(\phi\varphi) = (c\phi)\varphi = \phi(c\varphi), \ \ \forall \ c \in K \ \text{ e } \ \phi, \varphi \in \mathcal{A}.$$

Note que a função $f : K \to \mathcal{A} = \mathrm{End}_K(V)$ definida como $f(a) = aI$ é um monomorfismo de aneis. Logo, podemos identificar K com o subcorpo

$$\{aI : a \in K\}$$

de $\mathcal{A}$ que está contido no centro $\mathcal{Z}(\mathcal{A})$ da álgebra $\mathcal{A}$. Por outro lado, dado $\phi \in \mathcal{Z}(\mathcal{A})$, temos que

$$\phi\varphi = \varphi\phi, \ \ \forall \ \varphi \in \mathcal{A}.$$

Em particular,

$$\phi f_{ij} = f_{ij}\phi, \ \ i, j = 1, \ldots, n.$$

Fixando $i \neq j$, obtemos

$$\begin{aligned} \phi f_{ij} &= \left(\sum_{k=1}^{n} \sum_{l=1}^{n} a_{kl} f_{kl} \right) f_{ij} = \sum_{k=1}^{n} \sum_{l=1}^{n} a_{kl} f_{kl} f_{ij} \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} a_{kl} \delta_{li} f_{kj} = \sum_{k=1}^{n} a_{ki} f_{kj} \end{aligned}$$

e

$$\begin{aligned} f_{ij}\phi &= f_{ij} \left(\sum_{k=1}^{n} \sum_{l=1}^{n} a_{kl} f_{kl} \right) = \sum_{k=1}^{n} \sum_{l=1}^{n} a_{kl} f_{ij} f_{kl} \\ &= \sum_{k=1}^{n} \sum_{l=1}^{n} a_{kl} \delta_{jk} f_{il} = \sum_{l=1}^{n} a_{jl} f_{il}. \end{aligned}$$

Logo,

$$\sum_{k=1}^{n} a_{ki} f_{kj} = \sum_{l=1}^{n} a_{jl} f_{il}.$$

Comparando os coeficientes, temos que $a_{ki} = 0$ quando $i \neq k$ e $a_{ii} = a_{jj} = a$. Portanto, $\varphi = aI$ e, consequentemente,

$$K = \mathcal{Z}(\mathcal{A}).$$

Seja $\mathcal{A}$ uma álgebra sobre K. Diremos que $\mathcal{A}$ é uma *álgebra central* se $K = \mathcal{Z}(\mathcal{A})$. Portanto, se V um espaço vetorial de dimensão n sobre K, então $\mathcal{A} = \mathrm{End}_K(V)$ é uma álgebra central, mas não é uma álgebra com divisão, pois se $j \neq k$, então

$$f_{ij} f_{kl} = 0,$$

com $f_{ij} \neq 0$ e $f_{kl} \neq 0$.

As definições de subálgebras, álgebras geradas, homomorfismos de álgebras, ideais, etc. são análogos aos já vistos, por isto, vamos omití-los nesta dissertação. Por exemplo, um subconjunto não vazio J de uma álgebra $\mathcal{A}$ sobre K é um *ideal* de $\mathcal{A}$ se as seguintes condições são satisfeitas:

1. Se $\alpha, \beta \in J$, então $\alpha - \beta \in J$.

2. Se $c \in K$ e $\alpha \in J$, então $c\alpha \in J$.

3. Se $\lambda \in \mathcal{A}$ e $\alpha \in J$, então $\lambda\alpha \in J$ e $\alpha\lambda \in J$.

Note que se $\mathcal{A}$ é uma álgebra com identidade $1_{\mathcal{A}}$, então qualquer ideal J do anel $\mathcal{A}$ é um ideal da álgebra $\mathcal{A}$, pois

$$c\alpha = c(1_{\mathcal{A}}\alpha) = (c1_{\mathcal{A}})\alpha \in J.$$

Sejam $\mathcal{A}$ e $\mathcal{B}$ duas álgebras sobre K e $f : \mathcal{A} \to \mathcal{B}$ um homomorfismo de álgebras. A *imagem* de f é o conjunto

$$\mathrm{Im}\, f = \{\beta \in \mathcal{B} : \beta = f(\alpha), \text{para algum } \alpha \in \mathcal{A}\} = \{f(\alpha) : \alpha \in \mathcal{A}\} = f(\mathcal{A}).$$

O *núcleo* de f é o conjunto

$$\ker f = \{\alpha \in \mathcal{A} : f(\alpha) = 0\} = f^{-1}(0).$$

Observação 2.1 $\ker f$ *é um ideal em* $\mathcal{A}$ *e* $\mathrm{Im}\, f$ *é uma subálgebra de* $\mathcal{B}$.

Seja $\mathcal{A}$ uma álgebra sobre K. Diremos que $\mathcal{A}$ é uma *álgebra simples* se $\mathcal{A}^2 \neq \{0\}$ e os únicos ideais de $\mathcal{A}$ são $\{0\}$ e $\mathcal{A}$. Note que se $\mathcal{A}$ é uma álgebra com identidade, então a condição $\mathcal{A}^2 \neq \{0\}$ é sempre verdadeira.

Exemplo 2.1 *Qualquer álgebra com divisão é uma álgebra simples.*

Solução. Sejam $\mathcal{A}$ uma álgebra com divisão sobre K e J um ideal de $\mathcal{A}$. Suponhamos que $J \neq \{0\}$. Então J contém um elemento não nulo $a \in \mathcal{A}$. Logo, dado $\beta \in \mathcal{A}$, obtemos

$$\beta = \beta 1_{\mathcal{A}} = (\beta a^{-1})a \in J.$$

Portanto, $J = \mathcal{A}$. ■

Sejam $\mathcal{A}$ uma álgebra de posto n sobre K, $V = (\mathcal{A}, +)$ o espaço vetorial sobre K e

$$B_1 = \{\alpha_1, \ldots, \alpha_n\} \text{ e } B_2 = \{\beta_1, \ldots, \beta_n\}$$

bases de $\mathcal{A}$. Seja $f : V \to V$ uma transformação linear qualquer. Então

$$f(\alpha_1), \ldots, f(\alpha_n) \in V.$$

Como B_2 é uma base de V temos que existem únicos $a_{ij} \in K$ tais que

$$f(\alpha_j) = \sum_{i=1}^{n} a_{ij}\beta_i, \;\; j = 1, \ldots, n,$$

isto é, f é completamente determinada pelos os escalares a_{ij}. A transposta da matriz dos coeficientes deste sistema será chamada a *representação matricial* de f em relação às bases B_1 e B_2 e será denotada por

$$\mathbf{A}_f = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}.$$

Reciprocamente, dados $\mathbf{A} = [a_{ij}] \in M_n(K)$,

$$\alpha = b_1\alpha_1 + \cdots + b_n\alpha_n \in V, \text{ onde } b_i \in K.$$

Então existe uma única transformação linear $f : V \to V$ definido como

$$f(\alpha) = \left(\sum_{i=1}^{n} b_i a_{1i}\right)\beta_1 + \cdots + \left(\sum_{i=1}^{n} b_i a_{ni}\right)\beta_m$$

tal que $\mathbf{A} = \mathbf{A}_f$. Assim, a função

$$\varphi : \mathrm{End}_K(V) \to M_n(K)$$

definida como $\varphi(f) = \mathbf{A}_f$ é um isomorfismo de álgebras. Portanto, as álgebras $M_n(K)$ e $\mathrm{End}_K(V)$ são equivalentes e vamos nos referir a estas álgebras indistintamente.

Observação 2.2 *Note que esse isomorfismo induz as operações usuais de matrizes*

$$\mathbf{A}_{f+g} = \mathbf{A}_f + \mathbf{A}_g, \ \ \mathbf{A}_{cf} = c\mathbf{A}_f \ \ e \ \ \mathbf{A}_{g\circ f} = \mathbf{A}_g\mathbf{A}_f,$$

para todos $f, g \in \mathrm{End}(V)$ *e* $c \in K$*, pois*

$$\begin{aligned}(g\circ f)(\alpha_j) &= g(f(\alpha_j)) = g\left(\sum_{k=1}^{n} a_{kj}\alpha_k\right)\\ &= \sum_{k=1}^{n} a_{kj}g(\alpha_k) = \sum_{k=1}^{n} a_{kj}\left(\sum_{i=1}^{n} b_{ik}\alpha_i\right)\\ &= \sum_{i=1}^{n} c_{ij}\alpha_i, \ \ j = 1\ldots, n,\end{aligned}$$

com

$$c_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj}, \ \ i, j = 1\ldots, n.$$

Teorema 2.1 *Sejam* K *um corpo e* $\mathcal{A} = M_n(K)$*. Então* $\mathcal{A}$ *é uma álgebra central simples.*

Prova. Resta provar que $\mathcal{A}$ é simples. Seja J um ideal em $\mathcal{A}$. Suponhamos que $J \neq \{0\}$. Então J contém uma matriz não nula

$$\mathbf{A} = [a_{ij}] \in \mathcal{A},$$

com $a_{kl} \neq 0$, para algum $k, l = 1, \ldots, n$. Como

$$\begin{aligned}\mathbf{E}_{ik}\mathbf{A}\mathbf{E}_{lj} &= \mathbf{E}_{ik}\left(\sum_{p=1}^{n}\sum_{q=1}^{n} a_{pq}\mathbf{E}_{pq}\right)\mathbf{E}_{lj} = \sum_{p=1}^{n}\sum_{q=1}^{n} a_{pq}\left(\mathbf{E}_{ik}\mathbf{E}_{pq}\right)\mathbf{E}_{lj}\\ &= \sum_{p=1}^{n}\sum_{q=1}^{n} a_{pq}\delta_{kp}\mathbf{E}_{iq}\mathbf{E}_{lj} = \sum_{q=1}^{n} a_{kq}\mathbf{E}_{iq}\mathbf{E}_{lj} = \sum_{q=1}^{n} a_{kq}\delta_{ql}\mathbf{E}_{ij}\\ &= a_{kl}\mathbf{E}_{ij}\end{aligned}$$

temos que

$$\mathbf{E}_{ij} = \left(a_{kl}^{-1}\mathbf{E}_{ik}\right)\mathbf{A}\mathbf{E}_{lj} \in I.$$

Em particular,

$$\mathbf{I}_n = \mathbf{E}_{11} + \cdots + \mathbf{E}_{nn} \in I.$$

Portanto, $I = \mathcal{A}$. ■

Sejam V um espaço vetorial de dimensão n sobre K,

$$B_1 = \{\alpha_1, \ldots, \alpha_n\} \ \text{e} \ B_2 = \{\beta_1, \ldots, \beta_n\}.$$

duas bases de V. Então sabemos que existem únicos $p, q \in \mathrm{End}_K(V)$ tais que

$$p(\alpha_i) = \beta_i, \;\; i = 1, \ldots, n, \;\; \text{e} \;\; q(\beta_j) = \alpha_j, \;\; j = 1, \ldots, n.$$

Afirmação. p é uma bijeção com inversa q.

De fato.

$$(pq)(\beta_j) = p(q(\beta_j)) = p(\alpha_j) = \beta_j, \;\; j = 1, \ldots, n,$$

e

$$(qp)(\alpha_i) = q(p(\alpha_i)) = q(\beta_i) = \alpha_i, \;\; i = 1, \ldots, n.$$

Seja $g = p^{-1}fp$, para cada $f \in \mathrm{End}_K(V)$ Então

$$\mathbf{B}_f = \mathbf{A}_g = \mathbf{A}_{p^{-1}fp} = \mathbf{A}_{p^{-1}}\mathbf{A}_f\mathbf{A}_p.$$

Pondo $\mathbf{P} = \mathbf{A}_p$, obtemos

$$\mathbf{B}_f = \mathbf{P}^{-1}\mathbf{A}_f\mathbf{P}.$$

Portanto, as matrizes $\mathbf{A}_f$ e $\mathbf{B}_f$ são *semelhantes* ou *conjugadas*. Além disso, provamos o seguinte teorema:

Teorema 2.2 *Sejam $\mathcal{A}$ uma álgebra de posto n sobre K e $V = (\mathcal{A}, +)$ o espaço vetorial sobre K. Então a função $\varphi : \mathrm{End}_K(V) \to \mathrm{End}_K(V)$ definida como*

$$\varphi(f) = p^{-1}fp,$$

para algum $p \in \mathrm{Aut}_K(V)$ é um isomorfismo. Em particular, qualquer elemento de $\mathrm{Aut}_K(V)$ é um automorfismo interno. Note que $\mathrm{Aut}_K(V) \simeq \mathrm{GL}_n(F)$ o grupo linear geral de grau n.

Observação 2.3 *Pode ser provado, com auxílio do Teorema acima, que se $\mathcal{A}$ é uma álgebra central simples de posto n sobre K, então qualquer elemento $\varphi \in \mathrm{Aut}_K(\mathcal{A})$ é interno, ou seja, $\varphi(x) = \alpha^{-1}x\alpha$, para todo $x \in \mathcal{A}$ e $\alpha \in \mathcal{A}^*$.*

Sejam $\mathcal{A}$ uma álgebra de posto n sobre K, $V = (\mathcal{A}, +)$ o espaço vetorial sobre K e $\alpha \in \mathcal{A}$. Então a função $L_\alpha : V \to V$ definida como $L_\alpha(x) = \alpha x$ é claramente linear sobre K (observe que se $\mathcal{A}$ é uma álgebra com divisão, então L_α é bijetora). Logo, a função

$L : \mathcal{A} \to \mathrm{End}_K V \simeq M_n(K)$ definida como $L(\alpha) = L_\alpha$ é um homomorfismo de álgebras injetor, pois $L_{\alpha+\beta} = L_\alpha + L_\beta$, $L_{c\alpha} = cL_\alpha$,

$$\begin{aligned} L_{\alpha\beta}(x) &= (\alpha\beta)x = \alpha(x\beta) = L_\alpha(x\beta) \\ &= L_\alpha(L_\beta(x)) = (L_\alpha L_\beta)(x), \ \forall \ x \in \mathcal{A}, \end{aligned}$$

e se $\alpha \neq \beta$, então

$$L_\alpha(1_\mathcal{A}) = \alpha \neq \beta = L_\beta(1_\mathcal{A}).$$

Portanto, podemos identificar $\mathcal{A}$ com uma subálgebra

$$A_L = \{L_\alpha : \alpha \in \mathcal{A}\}$$

de $M_n(K)$. De modo análogo, temos que a função $R_\alpha : V \to V$ definida como $R_\alpha(x) = x\alpha$ é claramente linear sobre K. Logo, a função $R : \mathcal{A} \to \mathrm{End}_K V \simeq M_n(K)$ definida como $R(\alpha) = R_\alpha$ é um *anti-homomorfismo* de álgebras injetor

$$\begin{aligned} R_{\alpha\beta}(x) &= x(\alpha\beta) = (x\alpha)\beta = R_\beta(x\alpha) \\ &= R_\beta(R_\alpha(x)) = (R_\beta R_\alpha)(x), \ \forall \ x \in \mathcal{A}, \end{aligned}$$

Observe que $L_\alpha R_\alpha = R_\alpha L_\alpha$, para todo $\alpha \in \mathcal{A}$. Neste caso, as álgebras A_L e A_R são *álgebras opostas* ou *recíprocas*. Agora, se

$$B = \{\alpha_1, \ldots, \alpha_n\}$$

é uma base de V,

$$\{L_{\alpha_1}, \ldots, L_{\alpha_n}\}$$

é uma base de A_L e

$$L_\alpha(\alpha_j) = \sum_{i=1}^{n} b_{ij}\alpha_i, \ \ j = 1, \ldots, n,$$

então

$$f_\alpha(x) = \det(x\mathbf{I} - \mathbf{A}_\alpha) \in K[x]$$

é o *polinômio característico* de α sobre K, com $\mathbf{A}_\alpha = [b_{ij}]$ a matriz $n \times n$ de L_α em relação à base B. O *traço absoluto* e a *norma absoluta* de α são definidos por

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

Consequentemente, qualquer $\alpha \in \mathcal{A}$ é algébrico sobre K. Note que se $f \in K[x]$, então

$$f(L_\alpha) = L_{f(\alpha)}.$$

Portanto, α é uma raiz de f se, e somente se, L_α também o é.

Teorema 2.3 *Sejam $\mathcal{A}$ uma álgebra de posto n sobre K, $\alpha \in \mathcal{A}$ e $p = \mathrm{irr}(\alpha, K) \in K[x]$. Então*:

1. *p é o único polinômio mônico de menor grau tal que $p(\alpha) = 0$.*
2. *Se $f \in K[x]$ é tal que $f(\alpha) = 0$, então p divide f.*
3. *Os polinômios f_α e p possuem os mesmos fatores irredutíveis, a menos de multiplicidades.*

Os conceitos e resultados sobre inteiros algébricos, vistos no Capítulo 1, podem ser estendidos, com alguns ajustes, para uma álgebra $\mathcal{A}$ de posto n sobre K, por exemplo, se

$$\alpha = \begin{bmatrix} 0 & \frac{1}{2} \\ 0 & 0 \end{bmatrix}, \beta = \begin{bmatrix} 0 & 0 \\ \frac{1}{2} & 0 \end{bmatrix} \in M_2(\mathbb{Q})$$

então α e β são inteiros, pois ambos são raízes do polinômio $f = x^2 \in \mathbb{Z}[x]$, mas $\alpha + \beta$ e $\alpha\beta$ não são inteiros, pois eles são raízes dos polinômios

$$f = x^2 - \frac{1}{4} \in \mathbb{Q}[x] \text{ e } g = x^2 - \frac{1}{4}x \in \mathbb{Q}[x],$$

respectivamente. Isto ocorre porque $\alpha\beta \neq \beta\alpha$.

2.2 Álgebras dos Quatérnios

Vamos iniciar esta seção fazendo algumas observações sobre o corpo dos números complexos $\mathbb{C}$ e a álgebra dos quatérnios de Hamilton $\mathbb{H}$.

Já vimos que $\mathbb{C}$ é uma álgebra (comutativa) sobre $\mathbb{R}$, com uma base $\{1, i\}$. Além disso, é fácil verificar que $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{1, \sigma\}$, onde

$$\sigma(z) = \overline{z}.$$

Para um $\alpha = a + bi \in \mathbb{C}$ fixado, a função $L_\alpha : \mathbb{C} \to \mathbb{C}$ definida como $L_\alpha(z) = \alpha z$ é linear sobre $\mathbb{R}$ e

$$L_\alpha(1) = a + bi \text{ e } L_\alpha(i) = -b + ai.$$

Assim, a função $L : \mathbb{C} \to \mathrm{End}_{\mathbb{R}}\,\mathbb{C} \simeq M_2(\mathbb{R})$ definida como

$$L(a + bi) = L_\alpha \leftrightarrow \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

é um homomorfismo de álgebras injetor sobre $\mathbb{R}$. Portanto, podemos identificar $\mathbb{C}$ com o conjunto das matrizes

$$\left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R}).$$

Note que

$$N(a) = \alpha\sigma(\alpha) = a^2 + b^2 = |\alpha| \text{ e } \operatorname{Tr}(\alpha) = \alpha + \sigma(\alpha) = 2a = \operatorname{Re}(\alpha + \overline{\alpha}).$$

Como $|\alpha z| = |\alpha|\,|z|$, para todo $z \in \mathbb{C}$, temos que L_α é uma rotação se, e somente se, $|\alpha| = 1$.

Sejam

$$1 = (1,0,0,0),\ \ i = (0,1,0,0),\ \ j = (0,0,1,0) \text{ e } k = (0,0,0,1)$$

a base canônica de $\mathbb{R}^4$. Então é fácil verificar que o subconjunto

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\} \subseteq \mathbb{R}^4,$$

com a soma e multiplicação por escalar é um subespaço vetorial de $\mathbb{R}^4$, e com a operação de multiplicação sobre $\mathbb{H}$ obtida por meio da tábua de multiplicação

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

e estendida por linearidade para todo $\mathbb{H}$, é uma álgebra sobre $\mathbb{R}$ não comutativa, chamada de *álgebra dos quatérnios de Hamilton*. A palavra *quatérnio* significa o elemento de qualquer conjunto com quatro pessoas ou objetos.

Dado $\alpha = a + bi + cj + dk \in \mathbb{H}$, obtemos

$$\alpha = (a + bi) + j(c - di) = z + jw, \text{ onde } z, w \in \mathbb{C}.$$

Assim, $\mathbb{H}$ é um espaço vetorial sobre $\mathbb{C}$, com a multiplicação por escalar $\mathbb{H} \times \mathbb{C} \to \mathbb{H}$, e $\{1, j\}$ é uma base de $\mathbb{H}$ sobre $\mathbb{C}$. Para um $\alpha \in \mathbb{H}$ fixado, a função $L_\alpha : \mathbb{H} \to \mathbb{H}$ definida como $L_\alpha(x) = \alpha x$ é linear sobre $\mathbb{C}$. Logo, a função $L : \mathbb{H} \to \operatorname{End}_{\mathbb{C}} \mathbb{H} \simeq M_2(\mathbb{C})$ definida como

$$L(\alpha) = L_\alpha \leftrightarrow \begin{bmatrix} z & -\overline{w} \\ w & \overline{z} \end{bmatrix}$$

é um homomorfismo de álgebras injetor sobre $\mathbb{C}$. Portanto, podemos identificar $\mathbb{H}$ com o conjunto das matrizes

$$\mathbb{H}_L = \left\{ \begin{bmatrix} z & -\overline{w} \\ w & \overline{z} \end{bmatrix} : z, w \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C}).$$

Então $\mathbb{H}_L$ é uma álgebra sobre $\mathbb{C}$. Note que se $\mathbf{A} \in \mathbb{H}_L$, com $\mathbf{A} \neq \mathbf{O}$, então

$$\mathbf{A}^{-1} = (|z|^2 + |w|^2)^{-1} \begin{bmatrix} \overline{z} & \overline{w} \\ -w & z \end{bmatrix} \in \mathbb{H}_L.$$

Portanto, $\mathbb{H}_L$ é uma álgebra com divisão. É claro que as matrizes

$$\begin{aligned} \mathbf{1} &= L_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \ \mathbf{I} = L_i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \\ \mathbf{J} &= L_j = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \text{ e } \mathbf{K} = L_k = \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}, \end{aligned}$$

formam uma base para $\mathbb{H}_L$.

Agora, dado

$$\mathbf{A} = \begin{bmatrix} z & -\overline{w} \\ w & \overline{z} \end{bmatrix} \in \mathcal{Z}(\mathbb{H}_L),$$

obtemos

$$\begin{bmatrix} z & -\overline{w} \\ w & \overline{z} \end{bmatrix} \begin{bmatrix} 0 & -\overline{u} \\ u & 0 \end{bmatrix} = \begin{bmatrix} 0 & -\overline{u} \\ u & 0 \end{bmatrix} \begin{bmatrix} z & -\overline{w} \\ w & \overline{z} \end{bmatrix}, \ \forall \ u \in \mathbb{C}.$$

Logo,

$$uz = u\overline{z} \text{ e } \overline{u}w = u\overline{w}, \ \forall \ u \in \mathbb{C}.$$

Assim, $z \in \mathbb{R}$ e $w = 0$. Portanto,

$$\mathbb{R} \leftrightarrow \{a\mathbf{I} : a \in \mathbb{R}\} = \mathcal{Z}(\mathbb{H})$$

e $\mathbb{H}$ é uma álgebra central simples. Observe que se $\alpha = a + bi + cj + dk \in \mathbb{H}$, então

$$L_\alpha \leftrightarrow \mathbf{A}_\alpha = \begin{bmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix}.$$

Neste caso,

$$\mathrm{Tr}(\alpha) = 4a = 2(z + \overline{z}) \text{ e } N(\alpha) = (a^2 + b^2 + c^2 + d^2)^2 = (|z|^2 + |w|^2)^2.$$

Finalmente, para um $z \in \mathbb{C}$ fixado, a função $R_z : \mathbb{H} \to \mathbb{H}$ definida como $R_z(x) = xz$ é linear sobre $\mathbb{C}$. Assim, a função $R : \mathbb{C} \to \mathrm{End}_{\mathbb{C}}\,\mathbb{H} \simeq M_2(\mathbb{C})$ definida como

$$R(z) = R_z \leftrightarrow \begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix}$$

é um anti-homomorfismo de álgebras injetor. Portanto, podemos identificar $\mathbb{C}$ com o conjunto das matrizes

$$\mathcal{F} = \left\{ \begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix} : z \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C}).$$

Portanto, provamos o seguinte teorema.

Teorema 2.4 *Com as notações acima, obtemos*:

1. *A álgebra $M_2(\mathbb{C})$ é igual a álgebra*

$$[\mathbb{H}_L, \mathcal{F}] = \left\{ \sum_{r=1}^{n} L_{\alpha_r} R_{\beta_r} : n \in \mathbb{N} \text{ e } \alpha_r, \beta_r \in \mathbb{H} \right\}.$$

2. $\dim M_2(\mathbb{C}) = (\dim \mathbb{H}_L) \cdot (\dim \mathcal{F})$.

3. $\mathbf{AB} = \mathbf{BA}$, *para qualquer* $\mathbf{A} \in \mathbb{H}_L$ *e* $\mathbf{B} \in \mathcal{F}$.

Em particular, $M_2(\mathbb{C}) \simeq \mathbb{H} \otimes_{\mathbb{R}} \mathbb{C}$.

Agora, vamos generalizar a definição de álgebra dos quatérnios de Hamilton para um corpo qualquer K contendo $\mathbb{Q}$.

Lema 2.1 *Sejam K um corpo e $\mathcal{A}$ uma álgebra com divisão não comutativa de dimensão 4 sobre K. Então o polinômio minimal de qualquer elemento de $\mathcal{A}$ é quadrático.*

Prova. Já vimos que qualquer elemento de $\mathcal{A}$ satisfaz um polinômio de grau menor do que ou igual a 4, com coeficientes em K. Se para algum $\alpha \in \mathcal{A}$ o polinômio minimal de α é de grau 4, então 1, α, α^2 e α^3 são linearmente independentes sobre K. Assim, eles formam uma base de $\mathcal{A}$ sobre K. Como as potências de α comutam entre si temos

que $\mathcal{A}$ seria comutativa, o que é impossível. Logo, qualquer elemento em $\mathcal{A}$ satisfaz um polinômio de grau menor do que ou igual a 3, com coeficientes em K. Suponhamos que, para algum $a \in \mathcal{A}$, o polinômio minimal é de grau 3. Então 1, α e α^2 são linearmente independentes sobre K e, além disso, existe $\beta \in \mathcal{A}$ tal que $\beta \notin K(\alpha)$. Assim, 1, α, α^2 e β formam uma base de $\mathcal{A}$ sobre K. Em particular,

$$\alpha\beta = c_0 + c_1\alpha + c_2\alpha^2 + c_3\beta, \text{ onde } c_i \in K, i = 0, 1, 2, 3,$$

ou, equivalentemente,

$$(\alpha - c_3)\,\beta = c_0 + c_1\alpha + c_2\alpha^2.$$

Como $\alpha \notin K$ temos que $\alpha - c_3 \neq 0$. Logo,

$$\beta = (\alpha - c_3)^{-1}\left(c_0 + c_1\alpha + c_2\alpha^2\right) \in K(\alpha),$$

o que é uma contradição. Portanto, se $\alpha \in \mathcal{A}$ e $\alpha \notin K$, o polinômio minimal de α sobre K é quadrático. ■

Teorema 2.5 *Sejam K um corpo e $\mathcal{A}$ uma álgebra com divisão não comutativa de dimensão 4 sobre K. Então podemos escolher uma base 1, i, j e k para $\mathcal{A}$ satisfazendo*

$$i^2 = a, \;\; j^2 = b \;\; e \;\; k = ij = -ji,$$

onde $a, b \in K - \{0\}$. Neste caso, é usual dar-se a operação de multiplicação da álgebra $\mathcal{A}$ por meio de uma tábua de multiplicação

$\bullet$	1	i	j	k
1	1	i	j	k
i	i	a	k	aj
j	j	$-k$	b	$-bi$
k	k	$-aj$	bi	$-ab$

e estender isto por linearidade para uma multiplicação sobre $\mathcal{A}$.

Prova. Seja $\alpha \in \mathcal{A}$, $\alpha \notin K$. Então, pelo Lema **??**, 1 e α formam uma base de $K(\alpha)$ sobre K. Seja $\beta \in \mathcal{A}$ tal que $\beta \notin K(\alpha)$.

Afirmação. 1, α, β e $\alpha\beta$ são linearmente independentes sobre K.

De fato, suponhamos que

$$c_0 + c_1\alpha + c_2\beta + c_3\alpha\beta = 0, \text{ onde } c_r \in K, r = 0, 1, 2, 3.$$

Então

$$(c_2 + c_3\alpha)\,\beta = -c_0 - c_1\alpha.$$

Se $c_2 + c_3\alpha = 0$, então $c_2 = c_3 = 0$, pois 1 e α são linearmente independentes e, consequentemente, $c_0 = c_1 = 0$. Se $c_2 + c_3\alpha \neq 0$, então

$$\beta = (c_2 + c_3\alpha)^{-1}\,(-c_0 - c_1\alpha) \in K(\alpha)$$

o que contradiz a escolha de β. Portanto, 1, α, β e $\alpha\beta$ formam uma base de $\mathcal{A}$ sobre K.

Agora, construiremos a partir desta base a base desejada. Já vimos que o polinômio de β sobre K é quadrático, então podemos escrever este polinômio sob a forma

$$x^2 + 2cx + d, \;\; c, d \in K.$$

Seja $j = \beta + c$. Então $j \notin K(\alpha)$, pois $\beta \notin K(\alpha)$. Assim, 1, α, j e αj formam uma base de $\mathcal{A}$ sobre K. Além disso,

$$j^2 = (\beta + c)^2 = \beta^2 + 2c\beta + c^2 = b,$$

onde $b = -d + c^2 \in K$. Seja $j_0 = \alpha^{-1} j \alpha$. Então $j_0 \neq j$, pois $\mathcal{A}$ é não comutativa, e

$$j_0^2 = \alpha^{-1} j^2 \alpha = \alpha^{-1} b \alpha = j^2.$$

Logo, para $y = j - j_0$, teremos

$$y \neq 0 \;\text{ e }\; yj + j_0 y = 0.$$

Portanto,

$$-j = y^{-1} j_0 y = (\alpha y)^{-1} j (\alpha y).$$

Ponha $i = \alpha y$. Se $i \in K$ ou j é um polinômio em i, então j comuta com i e, consequentemente, $-j = j$, o que é impossível. Assim, $i \notin K$, $j \notin K(i)$ e 1, i, j e $k = ij$ formam uma base de $\mathcal{A}$ sobre K.

Agora, como $-j = i^{-1} j i$ temos que $-i = j^{-1} i j$. Portanto, i e i^{-1} possuem o mesmo polinômio minimal e o polinômio minimal de i é quadrático, donde concluímos que $i^2 = a \in K$. ■

A álgebra $\mathcal{A}$ será denotada por

$$\mathcal{A} = \left(\frac{a, b}{K}\right) \;\text{ ou }\; \mathcal{A} = (a, b)_K = K[i, j],$$

ou simplesmente $\mathcal{Q}$, a qual será chamada de *álgebra dos quatérnios generalizada* ou simplesmente *álgebra dos quatérnios* sobre K e a base $\{1, i, j, k\}$ é chamada de *base de definição* da álgebra.

Lema 2.2 *Seja K um corpo. Então as álgebras $(a, b)_K$ e $(ax^2, by^2)_K$ são isomorfas, para todos $a, b, x, y \in K^*$. Em particular, $(a, b)_K$ e $(b, a)_K$ são isomorfas.*

Prova. Sejam $\mathcal{A} = (a, b)_K$ e $\mathcal{B} = (ax^2, by^2)_K$. Então, pelo Teorema **??**, existem bases $\{1, i, j, k\}$ e $\{1, e, f, ef\}$ de $\mathcal{A}$ e $\mathcal{B}$, respectivamente, tais que

$$i^2 = a, \;\; j^2 = b \text{ e } e^2 = ax^2, \;\; f^2 = by^2.$$

Assim, é fácil verificar que a função $\varphi : \mathcal{B} \to \mathcal{A}$ definida como

$$\varphi(c_0 + c_1 e + c_2 f + c_3 ef) = c_0 + c_1 xi + c_2 yj + c_3 xyk,$$

é um isomorfismo de álgebras. Por exemplo, $(xi)^2 = ax^2$.

Finalmente, com $i \leftrightarrow abi$ e $j \leftrightarrow abj$, obtemos

$$(a, b)_K \simeq (a^2 b^3, a^3 b^2)_K \simeq (b, a)_K,$$

ou seja, $(a, b)_K$ e $(b, a)_K$ são isomorfas. ■

Seja $\alpha \in \mathcal{A}$, digamos

$$\alpha = c_0 + c_1 i + c_2 j + c_3 k, \;\; c_0, c_1, c_2, c_3 \in K.$$

Então

$$\overline{\alpha} = c_0 - c_1 i - c_2 j - c_3 k$$

chama-se o *conjugado* de α. Além disso, para quaisquer $\alpha, \beta \in \mathcal{A}$ e $c \in K$, valem as seguintes propriedades:

$$\overline{c\alpha} = c\overline{\alpha}, \;\; \overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}, \;\; \overline{\alpha\beta} = \overline{\beta}\overline{\alpha} \text{ e } \overline{\overline{\alpha}} = \alpha,$$

ou seja, a função $\overline{} : \mathcal{A} \to \mathcal{A}$ é um antiautomorfismo de álgebras e $\mathcal{A}^0 = \overline{\mathcal{A}}$ é a álgebra oposta de $\mathcal{A}$. A *norma reduzida* de α e o *traço reduzido* de α, em símbolos $\mathrm{nr}(\alpha)$ e $\mathrm{tr}(\alpha)$, são definidos como

$$\mathrm{nr}(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha = c_0^2 - ac_1^2 - bc_2^2 + abc_3^2 \text{ e } \mathrm{tr}(\alpha) = \alpha + \overline{\alpha} = 2c_0.$$

Portanto, sobre a álgebra das matrizes a norma e o traço absoluto coincidem com a norma e o traço reduzido. Como

$$\alpha = (c_0 + c_1 i) + j(c_2 - c_3 i) = z + jw, \;\; c_0, c_1, c_2, c_3 \in K,$$

temos que

$$\mathrm{nr}(\alpha) = (z + jw)(\overline{z} - j\overline{w}) = z\overline{z} - bw\overline{w}.$$

Observe, não é para toda escolha de a e b em K, que o Teorema **??** determina uma álgebra com divisão sobre K, com uma base $\{1, i, j, k\}$ satisfazendo

$$i^2 = a, \;\; j^2 = b \;\text{ e }\; k = ij = -ji,$$

onde a, $b \in K - \{0\}$. Se a ou b é um quadrado em K uma tal álgebra é isomorfa a álgebra $M_2(K)$. Por exemplo,

$$(1, b)_K \simeq M_2(K), \;\; i \leftrightarrow \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \;\text{ e }\; j \leftrightarrow \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}.$$

Mas temos a seguinte caracterização:

Proposição 2.2 *Seja $\mathcal{A}$ uma álgebra dos quatérnios sobre K tal que $\mathcal{A} = (a, b)_K$. Então as seguintes condições são equivalentes*:

1. *$\mathcal{A}$ é uma álgebra com divisão*;
2. *$\mathrm{nr}(\alpha) \neq 0$, para todo $\alpha \in \mathcal{A}^*$, ou seja, $\mathrm{nr} : \mathcal{A} \to K$ é uma forma quadrática não degenerada*;
3. *A única solução da equação $x^2 = ay^2 + bz^2$ em K é a trivial.*

Prova. $(1 \Rightarrow 2)$ Se $\alpha \in \mathcal{A}^*$, então $\alpha^{-1} \in \mathcal{A}$. Logo,

$$\alpha^{-1}\,\mathrm{nr}(\alpha) = \alpha^{-1}(\alpha\overline{\alpha}) = \overline{\alpha} \neq 0.$$

Portanto, $\mathrm{nr}(\alpha) \neq 0$, para todo $\alpha \in \mathcal{A}^*$.

$(2 \Rightarrow 3)$ Suponhamos, por absurdo, que a equação possua pelo menos uma solução não trivial em K, digamos $x_0, y_0, z_0 \in K$. Então $\alpha = x_0 + y_0 i + z_0 j \in \mathcal{A}^*$, com

$$\mathrm{nr}(\alpha) = x_0^2 - ay_0^2 - bz_0^2 = 0,$$

o que é uma contradição.

(3 $\Rightarrow$ 1) Se $\alpha \in \mathcal{A}^*$, então

$$\alpha = c_0 + c_1 i + c_2 j + c_3 k = c_0 + c_1 i + j(c_3 - c_4 i), \;\; c_0, c_1, c_2, c_3 \in K.$$

Assim, devemos provar que α é invertível. Se $c_3 - c_4 i = 0$, então $\alpha = c_0 + c_1 i \neq 0$ é invertível em $K(i) = K(\sqrt{a})$ e portanto, em $\mathcal{A}$. Se $c_3 - c_4 i \neq 0$, então $c_3 - c_4 i$ é invertível em $K(i)$ e

$$\alpha(c_3 - c_4 i)^{-1} = (c_0 + c_1 i)(c_3 - c_4 i)^{-1} + j.$$

Logo, para provar que α é invertível basta mostrar que todo elemento da forma

$$x + yi + zj$$

é invertível, com pelo menos um escalar não nulo. Note que

$$(x + yi + zj)(x - yi - j) = x^2 - ay^2 - bz^2 \in K^*,$$

pois

$$x^2 - ay^2 - bz^2 = 0 \Rightarrow x^2 = ay^2 + bz^2,$$

o que é impossível. Portanto,

$$(x + yi + zj)^{-1} = \frac{x - yi - zj}{x^2 - ay^2 - bz^2}.$$

Consequentemente, α é invertível. ■

Lema 2.3 *Seja $\mathcal{A}$ uma álgebra dos quatérnios sobre K.*

1. *A norma reduzida* nr *induz um endomorfismo de grupos* $\mathrm{nr} : \mathcal{U}(\mathcal{A}) \to \mathcal{U}(\mathcal{A})$.

2. *O traço reduzido* tr *induz um funcional linear sobrejetor* $\mathrm{tr} : \mathcal{A} \to K$.

3. *A função $b : \mathcal{A} \times \mathcal{A} \to K$ definida como $b(\alpha, \beta) = \mathrm{tr}(\alpha\beta)$ é bilinear e não degenerada.*

Proposição 2.3 *Seja $\mathcal{A}$ uma álgebra de dimensão 4 sobre K. Então $\mathcal{A}$ é uma álgebra dos quatérnios se, e somente se, $\mathcal{A}$ é uma álgebra central simples.*

Prova. Suponhamos que $\mathcal{A}$ seja uma álgebra dos quatérnios. Seja

$$\alpha = c_0 + c_1 i + c_2 j + c_3 k \in \mathcal{Z}(\mathcal{A}), \;\; c_0, c_1, c_2, c_3 \in K,$$

Então,

$$0 = \alpha k - k\alpha = 2(c_1 i + c_2 j)k \Rightarrow c_1 = c_2 = 0.$$

De modo análogo, prova-se que $c_3 = 0$. Portanto, $\mathcal{Z}(\mathcal{A}) = K$.

Finalmente, sejam J um ideal em $\mathcal{A}$ e

$$\alpha = c_0 + c_1 i + c_2 j + c_3 k \in J - \{0\}, \;\; c_0, c_1, c_2, c_3 \in K.$$

Se $c_1 = c_2 = c_3 = 0$, então $\alpha = c_0 \in K^*$ e $1 = \alpha\alpha^{-1} = \alpha^{-1}\alpha \in J$, ou seja, $J = \mathcal{A}$. Se $c_l \neq 0$, para algum $l = 1, 2, 3$, então

$$\alpha k - k\alpha = 2(c_1 i + c_2 j)k \in J.$$

Logo,

$$\beta = c_1 i + c_2 j \in J.$$

Assim,

$$\beta j + j\beta = 2c_2 b \in J.$$

Como $2c_2 b \in K$ temos que $J = \mathcal{A}$. Portanto, $\mathcal{A} = (a, b)_K$ é uma álgebra central simples.

A recíproca segue do Teorema **??**. ■

Observe que para cada $\alpha \in \mathcal{A}$, α é *puro* ($\alpha \in \mathcal{A} - K$) se, e somente se, $\overline{\alpha} = -\alpha$ e α é *escalar* ($\alpha \in K$) se, e somente se, $\overline{\alpha} = \alpha$.

Note que se

$$\alpha = c_0 + c_1 i + c_2 j + c_3 k \in \mathcal{A}, \;\; c_0, c_1, c_2, c_3 \in K,$$

então

$$\begin{aligned} \alpha^2 &= c_0^2 + ac_1^2 + bc_2^2 - abc_3^2 + 2c_0(c_1 i + + c_2 j + c_3 k) \\ &= -c_0^2 + ac_1^2 + bc_2^2 - abc_3^2 + 2c_0(c_0 + c_1 i + + c_2 j + c_3 k) \\ &= -\operatorname{nr}(\alpha) + \operatorname{tr}(\alpha)\alpha. \end{aligned}$$

Portanto, α é uma raiz do polinômio (irredutível se $\alpha \notin K$)

$$p = x^2 - \operatorname{tr}(\alpha)x + \operatorname{nr}(\alpha) \in K[x].$$

Em particular,

$$\alpha^2 = \begin{cases} -\operatorname{nr}(\alpha), & \text{se } \alpha \text{ é puro} \\ \operatorname{nr}(\alpha), & \text{se } \alpha \text{ é escalar} \end{cases}$$

ou seja, $\alpha^2 \in K$ se, e somente se, α é puro ou é escalar. Portanto, se $\alpha \in \mathcal{A} - K$, então $[L : K] = 2$, onde $L = K(\alpha)$.

Teorema 2.6 *Sejam $\mathcal{A}$ uma álgebra dos quatérnios sobre K e $\alpha \in \mathcal{A}$. Então α é um inteiro algébrico sobre $\mathcal{A}$ ($\alpha \in \mathcal{O}_K$) se, e somente se, $p = \mathrm{irr}(\alpha, K) \in \mathbb{Z}[x]$ ou, equivalentemente, $\mathrm{tr}(\alpha), \mathrm{nr}(\alpha) \in \mathbb{Z}$.*

Prova. Suponhamos que α seja um inteiro algébrico sobre $\mathcal{A}$. Então existe $g \in \mathbb{Z}[x]$ tal que $g(\alpha) = 0$. Assim, pelo item (2) do Teorema **??**, existe um polinômuio mônico $h \in K[x]$ tal que $g = ph$. Portanto, pelo Lema de Gauss, $p \in \mathbb{Z}[x]$.

A recíproca segue da definição. ■

Suponhamos que a não seja um quadrado em K, isto é, $\sqrt{a} \notin K$. Então, dado $\alpha = c_0 + c_1 i + c_2 j + c_3 k \in \mathcal{A}$, obtemos

$$\alpha = (c_0 + c_1\sqrt{a}) + j(c_2 - c_3\sqrt{a}) = z + jw \in \mathcal{A}, \;\; z, w \in F = K(\sqrt{a}).$$

Assim, $\mathcal{A}$ é um espaço vetorial sobre F e $\{1, j\}$ é uma base de $\mathcal{A}$ sobre F. Para um $\alpha \in \mathcal{A}$ fixado, a função $L_\alpha : \mathcal{A} \to \mathcal{A}$ definida como $L_\alpha(x) = \alpha x$ é linear sobre F. Logo, a função $L : \mathcal{A} \to \mathrm{End}_F\, \mathcal{A} \simeq M_2(F)$ definida como

$$L(\alpha) = L_\alpha \leftrightarrow \begin{bmatrix} z & b\sigma(w) \\ w & \sigma(z) \end{bmatrix},$$

onde $\sigma \in \mathrm{Aut}_K(F)$, é um homomorfismo de álgebras injetor sobre F. Portanto, podemos identificar $\mathcal{A}$ com o conjunto das matrizes

$$\mathcal{A}_L = \left\{ \begin{bmatrix} z & b\sigma(w) \\ w & \sigma(z) \end{bmatrix} : z, w \in F \right\} \subseteq M_2(F).$$

É claro que as matrizes

$$\begin{aligned} \mathbf{1} &= L_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \; \mathbf{I} = L_i = \begin{bmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{bmatrix}, \\ \mathbf{J} &= L_j = \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix} \text{ e } \mathbf{K} = L_k = \begin{bmatrix} 0 & b\sqrt{a} \\ -\sqrt{a} & 0 \end{bmatrix}, \end{aligned}$$

formam uma base para $\mathcal{A}_L$. Observe que

$$L_\alpha \leftrightarrow \mathbf{A}_\alpha = \begin{bmatrix} c_0 & ac_1 & bc_2 & -abc_3 \\ c_1 & c_0 & bc_3 & -bc_2 \\ c_2 & -ac_3 & c_0 & ac_1 \\ c_3 & -c_2 & c_1 & c_0 \end{bmatrix}.$$

Neste caso,

$$\mathrm{Tr}(\alpha) = 4c_0 = 2\,\mathrm{tr}(\alpha) \text{ e } N(\alpha) = (c_0^2 - ac_1^2 - bc_2^2 + abc_3^2)^2 = \mathrm{nr}(\alpha)^2.$$

A imersão

$$L : \mathcal{A} \to \mathcal{A}_L \subseteq M_2(F)$$

chama-se de *imersão de Cayley*.

Finalmente, para um $z \in F$ fixado, a função $R_z : \mathcal{A} \to \mathcal{A}$ definida como $R_z(x) = xz$ é linear sobre F. Assim, a função $R : F \to \mathrm{End}_F\,\mathcal{A} \simeq M_2(F)$ definida como

$$R(z) = R_z \leftrightarrow \begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix}$$

é um anti-homomorfismo de álgebras injetor. Portanto, podemos identificar F com o conjunto das matrizes

$$\mathcal{F}_L = \left\{ \begin{bmatrix} z & 0 \\ 0 & z \end{bmatrix} : z \in F \right\} \subseteq M_2(F).$$

Portanto, provamos o seguinte teorema.

Teorema 2.7 *Com as notações acima, obtemos*:

1. *A álgebra $M_2(F)$ é igual a álgebra*

$$[\mathcal{A}_L, \mathcal{F}_R] = \left\{ \sum_{r=1}^{n} L_{\alpha_r} R_{\beta_r} : n \in \mathbb{N} \text{ e } \alpha_r, \beta_r \in \mathcal{A} \right\}.$$

2. $\dim M_2(F) = (\dim \mathcal{A}_L) \cdot (\dim \mathcal{F}_L)$.

3. $\mathbf{AB} = \mathbf{BA}$, *para qualquer* $\mathbf{A} \in \mathcal{A}_L$ *e* $\mathbf{B} \in \mathcal{F}_R$.

Em particular, $M_2(F) \simeq \mathcal{A} \otimes_K F$.

2.3 Álgebras Cíclicas

Sejam K um corpo contendo $\mathbb{Q}$ e F uma extensão quadrática de K. Então, de modo análogo ao Exemplo **??**, existe $a \in K$ tal que $F = K(\sqrt{a})$. Assim, pelo Exemplo **??**,

$$\mathrm{Gal}(F/K) = \{1, \sigma\} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}},$$

onde $\sigma(z) = x - y\sqrt{a} \in F$ é o conjugado de $z = x + y\sqrt{a} \in F$, e F/K é uma extensão cíclica. Pelo exposto acima, se $\mathcal{A}$ é uma álgebra dos quatérnios sobre K e $\alpha = c_0 + c_1 i + c_2 j + c_3 k \in \mathcal{A}$, então

$$\alpha = (c_0 + c_1\sqrt{a}) + j(c_2 - c_3\sqrt{a}) = z + j\sigma(w) \in \mathcal{A}, \;\; z, w \in F.$$

Neste caso,

$$j^2 = b \;\text{ e }\; zj = j\sigma(z), \;\; \forall \;\; z \in F.$$

Portanto, esta formulação da álgebra dos quatérnios $\mathcal{A}$ depende de uma extensão quadrática F de K e de um automorfismo $\sigma \in \mathrm{Gal}(F/K)$, em outras palavras, $\mathcal{A}$ depende da equação (cíclica)

$$x^2 - a \in K[x]$$

e de um grupo cíclico $\mathrm{Gal}(F/K)$. Isto motiva a seguinte definição:

Sejam F/K uma extensão cíclica de grau n, com $\mathrm{Gal}\,(F/K) = \langle\sigma\rangle$, e $b \in K^*$ fixado. Diremos que o terno $\mathcal{A} = (F/K, \sigma, b)$ é uma *álgebra cíclica* sobre K se

$$\begin{aligned} \mathcal{A} &= F \oplus \beta F \oplus \cdots \oplus \beta^{n-1} F \\ &= \{c_0 + \beta c_1 + \cdots + \beta^{n-1} c_{n-1} : c_m \in F\} \end{aligned}$$

e a multiplicação é dada pelas equações

$$\beta^n = b \;\text{ e }\; \alpha\beta = \beta\sigma(\alpha), \;\; \forall \;\; \alpha \in F,$$

onde $f = x^n - b \in K[x]$ é irredutível sobre K e $\beta \in \mathbb{C}$ uma raiz de f.

Note que se $F = K(\theta)$ e

$$p = \mathrm{irr}(\theta, K) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in K[x],$$

então

$$\theta, \sigma(\theta), \ldots, \sigma^{n-1}(\theta)$$

são as raízes (distintas) de p em F. Como $\{1, \theta, \ldots, \theta^{n-1}\}$ é uma base F sobre K temos que cada $\gamma \in F$ pode ser escrito de modo único sob a forma

$$\gamma = a_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1}, \;\; \text{onde} \;\; a_0, a_1, \ldots, a_{n-1} \in K.$$

Assim,

$$\sigma = g \in K[x] \;\text{ e }\; \sigma^n(\theta) = \theta.$$

Sendo $\beta \in \mathbb{C}$ uma raiz de f, teremos que $\{1, \beta, \ldots, \beta^{n-1}\}$ é uma base $\mathcal{A}$ sobre F e

$$\begin{aligned} \mathcal{A} &= F \oplus \beta F \oplus \cdots \oplus \beta^{n-1} F \\ &= \left\{ \sum_{i=1}^{n-1} \sum_{j=1}^{n-1} a_{ij} \beta^i \theta^j : a_{ij} \in K \right\} \end{aligned}$$

é uma álgebra de posto n^2 sobre K, com relações

$$\theta\beta = \beta\sigma(\theta), \theta^2\beta = \theta\beta\sigma(\theta) = \beta\sigma(\theta)^2, \ldots, \theta^m\beta = \beta\sigma(\theta)^m, \ldots$$

Portanto, para qualquer $h \in K[x]$, obtemos

$$h(\theta)\beta = \beta h(\sigma(\theta))$$

e, indutivamente,

$$h(\theta)\beta^m = \beta^m h(\sigma^m(\theta)), \ \forall \ m \in \mathbb{Z}_+.$$

Para um

$$\alpha = c_0 + \beta c_1 + \cdots + \beta^{n-1} c_{n-1}\beta \in \mathcal{A}, \ \text{onde} \ c_0, c_1, \ldots, c_{n-1} \in F,$$

fixado, a função $L_\alpha : \mathcal{A} \to \mathcal{A}$ definida como $L_\alpha(x) = \alpha x$ é linear sobre F. Então

$$\begin{aligned} L_\alpha(1) &= \alpha \cdot 1 = c_0 + \beta c_1 + \cdots + \beta^{n-1} c_{n-1} \\ L_\alpha(\beta) &= \alpha \cdot \beta = b\sigma(c_{n-1}) + \beta\sigma(c_0) + \cdots + \beta^{n-1}\sigma(c_{n-2}) \\ L_\alpha(\beta^2) &= \alpha \cdot \beta^2 = b\sigma^2(c_{n-2}) + \beta b\sigma^2(c_{n-1}) + \cdots + \beta^{n-1}\sigma^2(c_{n-3}) \\ &\vdots \\ L_\alpha(\beta^{n-1}) &= \alpha \cdot \beta^{n-1} = b\sigma(c_{n-1}) + \beta\sigma(c_0) + \cdots + \beta^{n-1}\sigma(c_{n-2}) \end{aligned}$$

Logo, a função $L : \mathcal{A} \to \mathrm{End}_F \mathcal{A} \simeq M_n(F)$ definida como

$$L(\alpha) = L_\alpha \leftrightarrow \begin{bmatrix} c_0 & b\sigma(c_{n-1}) & b\sigma^2(c_{n-2}) & \cdots & b\sigma^{n-1}(c_1) \\ c_1 & \sigma(c_0) & b\sigma^2(c_{n-1}) & \cdots & b\sigma^{n-1}(c_2) \\ c_2 & \sigma(c_1) & \sigma^2(c_0) & \cdots & b\sigma^{n-1}(c_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & \sigma(c_{n-2}) & \sigma^2(c_{n-3}) & \cdots & \sigma^{n-1}(c_0) \end{bmatrix}$$

é um homomorfismo de algebras injetor sobre F. Portanto, podemos identificar $\mathcal{A}$ com o conjunto das matrizes

$$\mathcal{A}_L = \left\{ \begin{bmatrix} c_0 & b\sigma(c_{n-1}) & b\sigma^2(c_{n-2}) & \cdots & b\sigma^{n-1}(c_1) \\ c_1 & \sigma(c_0) & b\sigma^2(c_{n-1}) & \cdots & b\sigma^{n-1}(c_2) \\ c_2 & \sigma(c_1) & \sigma^2(c_0) & \cdots & b\sigma^{n-1}(c_3) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & \sigma(c_{n-2}) & \sigma^2(c_{n-3}) & \cdots & \sigma^{n-1}(c_0) \end{bmatrix} : c_m \in F \right\} \subseteq M_n(F).$$

Finalmente, para um $\gamma \in F$ fixado, a função $R_\gamma : \mathcal{A} \to \mathcal{A}$ definida como $R_\gamma(x) = x\gamma$ é linear sobre F. Assim, a função $R : F \to \mathrm{End}_F\, \mathcal{A} \simeq M_n(F)$ definida como

$$R(\gamma) = R_\gamma \leftrightarrow \begin{bmatrix} \gamma & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \gamma \end{bmatrix}$$

é um anti-homomorfismo de algebras injetor. Portanto, podemos identificar F com o conjunto das matrizes

$$\mathcal{F}_L = \left\{ \begin{bmatrix} \gamma & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \gamma \end{bmatrix} : \gamma \in F \right\} \subseteq M_n(F).$$

E assim, provamos o seguinte teorema.

Teorema 2.8 *Com as notações acima, obtemos*:

1. *A álgebra $M_n(F)$ é igual a álgebra*

$$[\mathcal{A}_L, \mathcal{F}_R] = \left\{ \sum_{r=1}^{m} L_{\alpha_r} R_{\gamma_r} : m \in \mathbb{N} \ \ e \ \ \alpha_r, \gamma_r \in \mathcal{A} \right\}.$$

2. $\dim M_n(F) = (\dim \mathcal{A}_L) \cdot (\dim \mathcal{F}_L)$.

3. $\mathbf{AB} = \mathbf{BA}$, *para qualquer* $\mathbf{A} \in \mathcal{A}_L$ *e* $\mathbf{B} \in \mathcal{F}_R$.

Em particular, $M_n(F) \simeq \mathcal{A} \otimes_K F$.

Teorema 2.9 *Sejam $F = K(\theta)$ uma extensão cíclica de grau n, com* $\mathrm{Gal}\,(F/K) = \langle\sigma\rangle$, *e $b \in K^*$ fixado. Se nenhuma potência de b menor do que a n-ésima é a norma de um polinômio em θ, com coeficitentes em K, então $\mathcal{A} = (F/K, \sigma, b)$ é uma álgebra com divisão sobre K.*

Prova. Confira [**?**, page, 221-226]. ■

Vamos finalizar esta seção com dois exemplos concretos de álgebras cíclicas:

Pondo $K = \mathbb{Q}(i)$ e $F = \mathbb{Q}(\xi)$, com

$$\xi = \xi_8 = e^{\frac{\pi}{4}i} = \frac{1}{\sqrt{2}}(1+i) \in \mathbb{C},$$

temos que F é o corpo de decomposição do polinômio

$$p = x^2 - i \in K[x],$$

o qual é irredutível sobre K. Assim, F é uma extensão cíclica de grau 2 sobre K, com o grupo de Galois

$$\mathrm{Gal}(F/K) = \{1, \sigma\} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}},$$

onde $\sigma(\xi) = \xi^5 \in F$. Seja $b \in F^*$ tal que

$$\begin{aligned} b &\neq N(x+\xi y) = (x+\xi y)\sigma(x+\sigma(\xi)y) = (x+\xi y)(x+\xi^5 y) \\ &= x^2 - iy^2, \ \forall \ x, y \in K. \end{aligned}$$

Então $f = t^2 - b \in F[t]$ é irredutível sobre F. Se $\beta = j \in \mathbb{C}$ é uma raiz de f, então

$$\begin{aligned} \mathbf{H} &= F \oplus \beta F \\ &= \{z + \beta w : z, w \in F\} \end{aligned}$$

é uma álgebra cíclica de posto 4, com relações

$$\xi^4 + 1 = 0, \ \ \beta^2 = b \ \text{ e } \ \xi\beta = \beta\xi^5.$$

Portanto,

$$\mathbf{H} \leftrightarrow \mathcal{A}_L = \left\{ \begin{bmatrix} z & b\sigma(w) \\ w & \sigma(z) \end{bmatrix} : z, w \in F \right\} \subseteq M_2(F).$$

Note que F é um espaço vetorial sobre K, com uma base $\{1, \xi\}$ e $\{1, \xi, j, \xi j\}$ é uma base de $\mathbf{H}$ sobre K.

Agora, sejam

$$\xi = \xi_9 = e^{\frac{2\pi}{9}i} \in \mathbb{C}$$

a raiz nona da unidade $K = \mathbb{Q}$ e $F = \mathbb{Q}(\theta)$, onde

$$\theta = \xi + \xi^{-1} = 2\cos\left(\frac{2\pi}{9}\right) \in \mathbb{R}.$$

Então, pelo Exemplo **??**,

$$\mathrm{Gal}(F/\mathbb{Q}) = \langle\sigma\rangle \simeq \frac{\mathbb{Z}}{3\mathbb{Z}},$$

com $\sigma(\theta) = \alpha_2$, $\sigma^2(\theta) = \alpha_3$, onde $\alpha_1 = \theta, \alpha_2, \alpha_3 \in \mathbb{R}$ são as raízes de

$$p = \mathrm{irr}(\theta, \mathbb{Q}) = 1 - 3x + x^3 \in \mathbb{Z}[x].$$

Note que $\sigma(\theta) = \theta^2 - 2$, $\sigma^2(\theta) = 2 + \theta - \theta^2$ e F é uma extensão cíclica de grau 3 sobre K.

Seja $b \in K^*$, com

$$b \neq N(\gamma) = \gamma\sigma(\gamma)\sigma^2(\gamma), \ \ \forall \ \gamma \in F.$$

Então $f = x^3 - b \in \mathbb{Q}[x]$ é irredutível sobre $\mathbb{Q}$. Se $\beta \in \mathbb{C}$ é uma raiz de f, então

$$\begin{aligned} \mathcal{A} &= F \oplus \beta F \oplus \beta^2 F \\ &= \{c_0 + \beta c_1 + \beta^2 c_2 : c_0, c_1, c_2 \in F\} \end{aligned}$$

é uma álgebra cíclica de posto 9, com relações

$$\theta^3 - 3\theta + 1 = 0, \ \ \beta^3 = b \ \text{ e } \ \theta\beta = \beta(\theta^2 - 2).$$

Portanto,

$$\mathcal{A} \leftrightarrow \mathcal{A}_L = \left\{ \begin{bmatrix} c_0 & b\sigma(c_2) & b\sigma^2(c_1) \\ c_1 & \sigma(c_0) & b\sigma^2(c_2) \\ c_2 & \sigma(c_1) & \sigma^2(c_0) \end{bmatrix} : c_m \in F \right\} \subseteq M_3(F).$$

Capítulo 3

Reticulados e Ordens dos Quatérnios

Neste capítulo apresentaremos alguns conceitos e resultados sobre reticulados e ordens sobre álgebras dos quatérnios $\mathcal{A}$, necessários para o desenvolvimento desta dissertação. O leitor interessado em mais detalhes pode consultar [**?**, **?**, **?**, **?**].

3.1 Reticulados

Nesta seção vamos generalizar alguns conceitos e resultados vistos no Capítulo 1, para um espaço vetorial qualquer.

Sejam K um corpo de números, $\mathcal{O}_K$ seu anel dos inteiros e V um espaço vetorial de dimensão finita sobre K. Se Γ é um $\mathcal{O}_K$-módulo de V, definimos

$$K\Gamma = \{c\alpha : c \in K \text{ e } \alpha \in \Gamma\}.$$

Assim, pela Proposição **??**, obtemos

$$K\Gamma = \{\alpha^{-1}\beta : \alpha \in \mathcal{O}_K, \ \alpha \neq 0, \text{ e } \beta \in \Gamma\}.$$

Portanto, $K\Gamma$ é um subespaço de V, ou seja,

$$K\Gamma = [\Gamma] = \left\{ \sum_{i=1}^{m} c_i\alpha_i : m \in \mathbb{N}, \ c_i \in K \text{ e } \alpha_i \in \Gamma \right\}.$$

Um $\mathcal{O}_K$-módulo Γ chama-se um *reticulado* em V se existir uma base

$$\{\alpha_1, \ldots, \alpha_n\}$$

para V tal que

$$\Gamma \subseteq \mathcal{O}_K\alpha_1 + \cdots + \mathcal{O}_K\alpha_n.$$

Diremos que Γ é um *reticulado completo* em V se, além disso,

$$K\Gamma = V.$$

Em particular,

$$\mathcal{O}_K\alpha_1 + \cdots + \mathcal{O}_K\alpha_n$$

é um reticulado completo em V.

Seja J um subconjunto de K, com $J \neq \{0\}$. Diremos que J é um *ideal fracionário* de K se as seguintes condições são satisfeitas:

1. J é um $\mathcal{O}_K$-módulo.

2. Existe $b \in \mathcal{O}_K$ tal que $bJ \subseteq \mathcal{O}_K$, ou seja, bJ é um ideal de $\mathcal{O}_K$.

Note que isto é equivalente a: J é um reticulado completo em K tal que $\mathbb{Q}J = K$. Portanto, qualquer ideal de $\mathcal{O}_K$ é necessariamente um ideal fracionário de K, pois é possível provar que $\mathcal{O}_K$ é um anel Noetheriano.

Lema 3.1 *Sejam V um espaço vetorial de dimensão finita e Γ um reticulado completo em V. Então um $\mathcal{O}_K$-módulo Λ em V é um reticulado em V se, e somente se, existir $b \in \mathcal{O}_K$ tal que $b\Lambda \subseteq \Gamma$.*

Prova. Suponhamos que Λ seja um $\mathcal{O}_K$-módulo em V. Então existe uma base

$$\beta = \{\alpha_1, \ldots, \alpha_n\}$$

de V tal que

$$\Lambda \subseteq \mathcal{O}_K\alpha_1 + \cdots + \mathcal{O}_K\alpha_n.$$

Como Γ é um reticulado completo em V temos que Γ contém uma base

$$\gamma = \{\gamma_1, \ldots, \gamma_n\}$$

de V. Logo, existem únicos $r_{ij} \in K$ tais que

$$\alpha_j = \sum_{i=1}^{n} r_{ij}\gamma_i, \;\; j = 1, \ldots, n.$$

Pondo

$$r_{ij} = \frac{a_{ij}}{b_{ij}} \text{ e } b_j = b_{1j}b_{2j}\cdots b_{nj} \in \mathcal{O}_K,$$

obtemos $b_j r_{ij} \in \mathcal{O}_K$, para todo i e j. (Neste caso, o conjunto gerado pelos r_{ii} é um ideal fracionário de K). Assim, existe $b = b_1 b_2 \cdots b_n \in \mathcal{O}_K$ tal que

$$b\alpha_j \subseteq \mathcal{O}_K\gamma_1 + \cdots + \mathcal{O}_K\gamma_n \subseteq \Gamma.$$

Portanto, existe $b \in \mathcal{O}_K$ tal que $b\Lambda \subseteq \Gamma$.

Reciprocamente, suponhamos que existe $b \in \mathcal{O}_K$ tal que $b\Lambda \subseteq \Gamma$. Como Γ é um reticulado completo em V temos que Γ contém uma base

$$\beta = \{\beta_1, \ldots, \beta_n\}$$

de V tal que

$$\Gamma \subseteq \mathcal{O}_K\beta_1 + \cdots + \mathcal{O}_K\beta_n.$$

Então

$$\Lambda \subseteq b^{-1}\Gamma \subseteq \mathcal{O}_K(b^{-1}\beta_1) + \cdots + \mathcal{O}_K(b^{-1}\beta_n).$$

Portanto, Λ é um reticulado em V. ■

Corolário 3.1 *Sejam V um espaço vetorial de dimensão finita sobre K e U um subespaço de V, com $\Gamma \subseteq U \subseteq V$. Então Γ é um reticulado em V se, e somente se, Γ é um reticulado em U.*

Prova. Como U é um subespaço de V temos que U contém uma base

$$\alpha = \{\alpha_1, \ldots, \alpha_k\}$$

que é parte de uma base

$$\beta = \{\alpha_1, \ldots \alpha_k, \alpha_{k+1}, \ldots, \alpha_n\}$$

de V. Definimos

$$\Lambda_1 = \mathcal{O}_K\alpha_1 + \cdots + \mathcal{O}_K\alpha_k \text{ e } \Lambda = \mathcal{O}_K\alpha_1 + \cdots + \mathcal{O}_K\alpha_n.$$

Se Γ é um reticulado em U, então existe $b \in \mathcal{O}_K$ tal que $b\Gamma \subseteq \Lambda_1 \subseteq \Lambda$. Portanto, Γ é um reticulado em V.

Reciprocamente, suponhamos que Γ seja um reticulado em V. Então existe $b \in \mathcal{O}_K$ tal que $b\Gamma \subseteq \Lambda$. Logo,

$$b\Gamma \subseteq \Lambda \cap U = \Lambda_1,$$

pois $\Gamma \subseteq U$. Portanto, Γ é um reticulado em U. ■

Observação 3.1 *Sejam V um espaço vetorial sobre K de dimensão finita.*

1. *Qualquer $\mathcal{O}_K$-submódulo de um reticulado Γ em V é um reticulado.*

2. *Se Γ e Λ são reticulados em V, então $\Gamma \cap \Lambda$ é um reticulado em V. Além disso, $c\Gamma$, $J\Gamma$ e $\Gamma + \Lambda$ são reticulados, para todo $c \in K$ e todo ideal fracionário J de K, onde*

$$J\Gamma = \left\{ \sum_{i=1}^{m} c_i \alpha_i : m \in \mathbb{N},\ c_i \in J \ \text{ e } \ \alpha_i \in \Gamma \right\}.$$

3. *É claro que $\mathcal{O}_K c$ e $c\mathcal{O}_K$ são reticulados em V, para todo $c \in K$. Portanto,*

$$J_1\gamma_1 + \cdots + J_k\gamma_k$$

é um reticulado em V, para todo ideal fracionário J_i de K e $\gamma_i \in K$. Em particular, qualquer $\mathcal{O}_K$-módulo finitamente gerado em V é um reticulado em V.

Agora, vamos considerar o corpo K como sendo o corpo dos números reais $\mathbb{R}$ e $V = \mathbb{R}^n$. Dados $\alpha_1, \ldots, \alpha_m \in \mathbb{R}^n$ com $m \leq n$, consideremos o conjunto

$$\Gamma = \mathbb{Z}\alpha_1 + \cdots + \mathbb{Z}\alpha.$$

Diremos que um subconjunto C de $\mathbb{R}^n$ é *compacto* se C é limitado e fechado. Diremos que subgrupo aditivo em $\mathbb{R}^n$ é *discreto* se a sua interseção com qualquer subconjunto limitado (compacto) em $\mathbb{R}^n$ é finita.

O próximo resultado nos permitirá concluir quando um dado subconjunto Γ de $\mathbb{R}^n$ é um reticulado, sem a necessidade de conhecermos uma base deste.

Proposição 3.1 *Um subconjunto Γ de $\mathbb{R}^n$ é um reticulado de $\mathbb{R}^n$ se, e somente se, Γ é um subgrupo aditivo e discreto em $\mathbb{R}^n$.*

Prova. Suponhamos que Γ seja um reticulado de $\mathbb{R}^n$. Então é fácil verificar que Γ é um subgrupo aditivo. Suponhamos que $\alpha_1, \ldots, \alpha_m$ seja uma base de Γ, então

$$m \leq n$$

e existem $\alpha_{m+1}, \ldots, \alpha_n \in \mathbb{R}^n$ tais que $\alpha_1, \ldots, \alpha_n$ seja uma base para $\mathbb{R}^n$. Portanto,

$$\Lambda = [\alpha_1, \ldots, \alpha_n]$$

é um reticulado contendo Γ. Assim, para provar que Γ é discreto, basta provar que Λ o é. Seja $\{\beta_1, \ldots, \beta_n\}$ a base dual de $\{\alpha_1, \ldots, \alpha_n\}$, isto é,

$$(\alpha_i, \beta_j) = \delta_{ij} \;\; i, j = 1, \ldots, n.$$

Então, para todo $\alpha = c_1\alpha_1 + \cdots + c_n\alpha_n \in \Lambda$, teremos que

$$(\alpha, \beta_j) = c_j, \;\; j = 1, \ldots, n.$$

Para todo $r > 0$ e todo $\alpha \in \Lambda \cap B_r$, com

$$B_r = \{\alpha \in \mathbb{R}^n : \|\alpha\| \leq r\},$$

temos que

$$|c_j| = \left|(\alpha, \beta_j)\right| \leq \|\alpha\| \left\|\beta_j\right\| \leq r \left\|\beta_j\right\|, \;\; j = 1, \ldots, n.$$

Logo, $\Lambda \cap B_r$ é finito. Portanto, Λ é discreto.

Reciprocamente, seja Γ um grupo aditivo e discreto em $\mathbb{R}^n$. Suponhamos que os elementos $\gamma_1, \ldots, \gamma_m$ formem um sistema maximal de elementos de Γ linearmente independentes sobre $\mathbb{R}$. Então $\gamma_1, \ldots, \gamma_m$ formam uma base do reticulado

$$\Gamma_0 = \mathbb{Z}\gamma_1 + \cdots + \mathbb{Z}\gamma_m.$$

Seja

$$T_\gamma = \left\{ \sum_{i=1}^{m} r_i\gamma_i : 0 \leq r_i < 1, \;\; i = 1, \ldots, m \right\}$$

a *região fundamental básica* de Γ. Então

$$(\Gamma \cap T_\gamma) + \Gamma_0 \subseteq \Gamma,$$

e como todo $\delta \in \Gamma$ é linearmente dependente (sobre $\mathbb{R}$) de $\gamma_1, \ldots, \gamma_m$ temos que

$$(\Gamma \cap T_\gamma) + \Gamma_0 = \Gamma.$$

Logo,

$$\delta = \sum_{i=1}^{m} c_i\gamma_i + \sum_{i=1}^{m} r_i\gamma_i \;\text{ com }\; c_i \in \mathbb{Z} \;\text{ e }\; 0 \leq r_i < 1, \;\; i = 1, \ldots, m.$$

Assim,

$$\sum_{i=1}^{m} r_i\gamma_i = \left(\delta - \sum_{i=1}^{m} c_i\gamma_i \right) \in \Gamma \cap T_\gamma.$$

Agora, considerando o homomorfismo canônico

$$\pi : \Gamma \to \frac{\Gamma}{\Gamma_0},$$

temos que $\frac{\Gamma}{\Gamma_0}$ é finito, pois Γ discreto e T_γ limitado implicam que $\Gamma \cap T_\gamma$ é finito. Seja d a ordem de $\frac{\Gamma}{\Gamma_0}$. Então

$$\Gamma \subseteq d^{-1}\Gamma_0 = \mathbb{Z}\delta_1 + \cdots + \mathbb{Z}\delta_m, \text{ onde } \delta_i = d^{-1}\gamma_i, \ i = 1, \ldots, m.$$

Portanto, Γ é um $\mathbb{Z}$-módulo livre, de um posto $k \leq m$. Logo, possui uma base

$$\{\alpha_1, \ldots, \alpha_k\}.$$

Como

$$\Gamma_0 \subseteq \Gamma \subseteq d^{-1}\Gamma_0$$

temos que

$$\mathbb{R}\gamma_1 + \cdots + \mathbb{R}\gamma_m = \mathbb{R}\alpha_1 + \cdots + \mathbb{R}\alpha_k,$$

ou seja, $\alpha_1, \ldots, \alpha_k$ são linearmente independentes sobre $\mathbb{R}$. Portanto, Γ é um reticulado de $\mathbb{R}^n$. ■

Sejam Γ um reticulado completo em $\mathbb{R}^n$, $\{\alpha_1, \ldots, \alpha_n\}$ uma base de Γ e

$$\alpha_i = (a_{i1}, \ldots, a_{in}) \in \mathbb{R}^n.$$

Então a matriz

$$\begin{aligned} \mathbf{G} &= [\alpha_i : 1 \leq i \leq n] \\ &= \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \end{aligned}$$

cujas linhas são determinadas pelas coordenadas dos vetores α_i, chama-se uma *matriz geradora* do reticulado Γ e os elementos de Γ são os vetores $\mathbf{uG}$, onde $\mathbf{u} \in \mathbb{Z}^n$.

Seja $\{\beta_1, \ldots, \beta_n\}$ outra base de Γ. Então existem únicos $b_{ij} \in \mathbb{Z}$ tais que

$$\beta_j = \sum_{i=1}^{n} b_{ij}\alpha_i, \ 1 \leq j \leq n.$$

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

$$\alpha_j = \sum_{i=1}^{n} a_{ij}\beta_i, \;\; 1 \leq j \leq n.$$

Logo,

$$\alpha_j = \sum_{i=1}^{n} a_{ij}\beta_i = \sum_{i=1}^{n} \left(a_{ij} \sum_{k=1}^{n} b_{ki}\alpha_k \right) = \sum_{k=1}^{n} \left(\sum_{i=1}^{n} a_{ij}b_{ki} \right) \alpha_k.$$

Assim,

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

Se $\mathbf{A} = [a_{ij}]$ é a matriz de mudança da base $\{\beta_1, \ldots, \beta_n\}$ para a base $\{\alpha_1, \ldots, \alpha_n\}$ e $\mathbf{B} = [b_{ij}]$ é a matriz de mudança da base $\{\alpha_1, \ldots, \alpha_n\}$ para a base $\{\beta_1, \ldots, \beta_n\}$, então

$$\mathbf{AB} = \mathbf{I}_n,$$

em que $\mathbf{I}_n$ é a matriz identidade de ordem n. Donde,

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

Portanto,

$$\det \mathbf{A} = \det \mathbf{B} = \pm 1.$$

Conclusão. Qualquer base $\{\beta_1, \ldots, \beta_n\}$ de Γ pode ser obtida a partir de uma dada base $\{\alpha_1, \ldots, \alpha_n\}$ de Γ, com

$$\beta_j = \sum_{i=1}^{n} b_{ij}\alpha_i, \;\; 1 \leq j \leq n,$$

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

O *determinante* do reticulado Γ é o quadrado do determinante de uma matriz geradora $\mathbf{G}$, isto é,

$$\det \Gamma = |\det \mathbf{G}|^2 .$$

É importante lembrar que se $\mathbf{G}$ não é uma matriz quadrada, então

$$\det \Gamma = \det(\mathbf{G}\mathbf{G}^t),$$

em que $\mathbf{G}\mathbf{G}^t$ é a *matriz de Gram* de Γ. Note, do exposto acima, que $\det \Gamma$ é independente da base escolhida para Γ.

Sejam Γ um reticulado em $\mathbb{R}^n$, Λ um sub-reticulado de Γ, $\{\alpha_1, \ldots, \alpha_n\}$ uma base de Γ e $\{\beta_1, \ldots, \beta_n\}$ uma base de Λ. Como $\beta_j \in \Gamma$ temos que existem únicos $b_{ij} \in \mathbb{Z}$ tais que

$$\beta_j = \sum_{i=1}^{n} b_{ij}\alpha_i, \;\; 1 \leq j \leq n.$$

Se $\mathbf{B} = [b_{ij}]$, então

$$N = |\det \mathbf{B}| = \frac{\det \Gamma}{\det \Lambda}$$

é chamado de *índice* de Γ em Λ. Note que N depende somente de Λ e Γ, não das bases escolhidas para Λ e Γ. Pela Regra de Cramer, obtemos

$$N\alpha_j = \sum_{i=1}^{n} a_{ij}\beta_i, \;\; 1 \leq j \leq n,$$

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

$$N\Gamma \subseteq \Gamma \subseteq \Lambda,$$

em que $N\Gamma = \{N\alpha : \alpha \in \Gamma\}$ é um reticulado. Portanto, $\{N\alpha_1, \ldots, N\alpha_n\}$ é uma base de $N\Gamma$. O *volume fundamental* de um reticulado Γ é o volume de uma região fundamental (básica), o qual será denotado por $V(\Gamma)$. Pode ser provado que (confira [**?**])

$$V(\Gamma) = V(\mathbf{F}),$$

em que

$$\mathbf{F} = \left\{ \sum_{i=1}^{n} r_i\alpha_i : 0 \leq r_i < 1, \;\; i = 1, \ldots, n \right\}$$

A *densidade* de Γ é definida como

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

e a *densidade de centro* de Γ é definida como

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

em que

$$E_\rho(\mathbf{0}) = \{\alpha \in \mathbb{R}^n : \|\alpha\| = \rho\}$$

é a esfera de centro $\mathbf{0}$, raio ρ e $\|\alpha_i - \alpha_j\|^2 \geq 4\rho^2$, para todo $i \neq j$. Neste caso,

$$\rho = \frac{1}{2}\min\{\|\alpha\| : \alpha \in \Gamma\}$$

é chamado o *raio de empacotamento* de Γ.

Finalmente, sejam $\alpha = (a_1, \ldots, a_n)$ e $\beta = (b_1, \ldots, b_n)$ vetores de $\mathbb{R}^n$. A *diversidade* ou *distância de Hamming* de α e β é definida como

$$\operatorname{div}(\alpha, \beta) = |\{i : a_i \neq b_i, \ \forall \ i = 1, \ldots, n\}|,$$

isto é, o número de componentes em que α e β diferem. Seja S um subconjunto de $\mathbb{R}^n$. A *diversidade* ou *distância minima de Hamming* de S é definida como

$$\operatorname{div} S = \min\{\operatorname{div}(\alpha, \beta) : \alpha, \beta \in S, \ \text{com} \ \alpha \neq \beta\}.$$

Em particular, se Γ é um reticulado em $\mathbb{R}^n$, então

$$\operatorname{div} \Gamma = \min\{\operatorname{div}(\mathbf{0}, \alpha) : \alpha \in \Gamma\}.$$

3.2 Ordens

Nesta seção vamos estender os conceitos e resultados sobre ordens, dado no Capítulo 1, para uma álgebra dos quatérnios. Embora esses resultados continuam válidos para qualquer domínio de Dedekind.

Seja $\mathcal{A}$ uma álgebra dos quatérnios sobre K. Um subconjunto $\mathcal{O}$ de $\mathcal{A}$ é uma *ordem* em $\mathcal{A}$ se as seguintes condições são satisfeitas:

1. $\mathcal{O}$ é um subanel de $\mathcal{A}$, com a mesma unidade de $\mathcal{A}$.

2. $\mathcal{O}$ é um $\mathcal{O}_K$-módulo finitamente gerado.

3. O posto de $\mathcal{O}$ é máximo r, isto é, $\mathcal{A} = K\mathcal{O}$.

Note que esta definição é equivalente a: $\mathcal{O}$ é um reticulado completo em $\mathcal{A}$. Além disso, $\alpha\beta \in \mathcal{O}$, para todos $\alpha, \beta \in \mathcal{O}$, e qualquer elemento $\alpha \in \mathcal{O}$ é inteiro sobre $\mathcal{O}_K$, pois $\mathcal{O}_K[\alpha] \subseteq \mathcal{O}$ é um $\mathcal{O}_K$-módulo finitamente gerado. Portanto,

$$\operatorname{nr}(\alpha), \operatorname{tr}(\alpha) \in \mathcal{O}_K, \ \forall \ \alpha \in \mathcal{O}.$$

Observação 3.2 *Seja*

$$\Gamma = \mathcal{O}_K\alpha_0 + \mathcal{O}_K\alpha_1 + \mathcal{O}_K\alpha_2 + \mathcal{O}_K\alpha_3.$$

Então Γ é um reticulado em $\mathcal{A}$. Assim, os conjuntos

$$\mathcal{O}_L(\Gamma) = \{\alpha \in \mathcal{A} : \alpha\Gamma \subset \Gamma\} \ \ e \ \ \mathcal{O}_R(\Gamma) = \{\alpha \in \mathcal{A} : \Gamma\alpha \subset \Gamma\}$$

são ordens em $\mathcal{A}$, pois são subaneis de $\mathcal{A}$ e $\mathcal{O}_K$-submódulos de Γ.

Exemplo 3.1 *Sejam*

$$\xi = e^{\frac{\pi}{4}i} = \frac{1}{\sqrt{2}}(1+i) \in \mathbb{C}$$

a raiz oitava da unidade, $K = \mathbb{Q}(i)$ *e*

$$\mathbf{H} = \mathbb{Q}(\xi) \oplus j\mathbb{Q}(\xi)$$

uma subálgebra da álgebra dos quatérnios de Hamilton sobre K*, com uma base* $\{1, \xi, j, j\xi\}$ *sobre* K*, com* $\mathbb{Q}(\xi) = K(\xi) = \mathbb{Q}(i, \sqrt{2})$*. É fácil verificar que*

$$\mathcal{L} = \{c_0 + \xi c_1 + jc_2 + j\xi c_3 : \ \ ou \ c_i \in \mathcal{G}\}.$$

é uma ordem de $\mathbf{H}$*, chamada de* anel de Lipschitz*, onde* $\mathcal{G} = \mathbb{Z}[i]$ *é o anel dos inteiros de Gauss. Note que*

$$\mathcal{O} = \mathcal{L} + \alpha\mathbb{Z} = [1, \xi, j, \alpha],$$

em que

$$\alpha = \frac{1 + \xi + j + j\xi}{2},$$

é uma ordem de $\mathbf{H}$ *contendo* $\mathcal{L}$*.*

Sejam $\mathcal{A}$ uma álgebra sobre K e $\mathcal{O}$ uma ordem em $\mathcal{A}$. Diremos que $\mathcal{O}$ é uma *ordem maximal* em $\mathcal{A}$ se $\mathcal{O} \neq \mathcal{A}$ e se $\mathcal{O}_1$ é uma ordem em $\mathcal{A}$ tal que $\mathcal{O} \subseteq \mathcal{O}_1 \subseteq \mathcal{A}$, então $\mathcal{O} = \mathcal{O}_1$ ou $\mathcal{O}_1 = \mathcal{A}$.

Exemplo 3.2 *Seja* K *um corpo de números e* $\mathcal{A} = M_2(K)$*. Então* $\mathcal{O} = M_2(\mathcal{O}_K)$ *é uma ordem maximal em* $\mathcal{A}$*.*

Solução. Sejam $\mathcal{O}_1$ uma ordem em $\mathcal{A}$ tal que $\mathcal{O} \subseteq \mathcal{O}_1 \subseteq \mathcal{A}$ e consideremos o conjunto

$$R = \{c \in K : c \text{ é uma entrada de alguma matriz de } \mathcal{O}_1\}.$$

Então é fácil verificar que R é um subanel de K contendo $\mathcal{O}_K$ tal que $\mathbb{Q}R = K$. Assim, R é uma ordem em K. Logo, pelo Teorema **??**, $\mathcal{O}_K = R$ ou $R = K$. Portanto, $\mathcal{O} = \mathcal{O}_1$ ou $\mathcal{O}_1 = \mathcal{A}$. ■

Sejam $\mathcal{A}$ uma álgebra dos quatérnios sobre K e $\mathcal{O}$ uma $\mathcal{O}_K$-ordem em $\mathcal{A}$. O *discriminante ideal* de $\mathcal{O}$, denotado por $d(\mathcal{O})$, é igual a raiz quadrada do ideal $\mathcal{I}_K$ em $\mathcal{O}_K$ gerado pelo conjunto

$$T = \{\det(\mathrm{tr}(\alpha_i\alpha_j)) : 0 \leq i, j \leq 2\},$$

onde $\alpha_i \in \mathcal{O}$, ou seja,

$$\mathcal{I}_K = \{a_1x_1 + \cdots + a_kx_k : k \in \mathbb{N},\ \ a_i \in \mathcal{O}_K \ \text{ e } \ x_i \in T\}.$$

Note que $d(\mathcal{O}) \neq \{0\}$, pois a forma bilinear associada a tr é não degenerada.

Proposição 3.2 *Sejam $\mathcal{A}$ uma álgebra dos quatérnios sobre K e $\mathcal{O}$ uma $\mathcal{O}_K$-ordem em $\mathcal{A}$. Se $\mathcal{O}$ possui uma base $\{e_1, e_2, e_3, e_4\}$ e $d = \det(\mathrm{tr}(e_ie_j))$, então $d\mathcal{O}_K \subseteq d(\mathcal{O})$ e*

$$d(\mathcal{O}) = (d\mathcal{O}_K)^{\frac{1}{2}} = \{d\beta : \beta \in \mathcal{O}_K\}^{\frac{1}{2}}.$$

Além disso, se Γ é qualquer $\mathcal{O}_K$-ordem de $\mathcal{A}$ contendo $\mathcal{O}$, então

$$d\Gamma \subseteq \mathcal{O}_K[e_1, e_2, e_3, e_4] \subseteq \mathcal{O}.$$

Prova. É fácil verificar que

$$(d\mathcal{O}_K)^{\frac{1}{2}} \subseteq d(\mathcal{O}).$$

Por outro lado, sejam $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathcal{O}$, de modo que

$$\alpha_i = \sum_{k=1}^{4} a_{ik}e_k,$$

onde $a_{ik} \in \mathcal{O}_K$. Então

$$\begin{aligned} \det(\mathrm{tr}(\alpha_i\alpha_j)) &= \det(\mathbf{A})d\det(\mathbf{A}^t) \in d\mathcal{O}_K \\ &\Rightarrow \ d(\mathcal{O}) \subseteq (d\mathcal{O}_K)^{\frac{1}{2}}, \end{aligned}$$

onde $\mathbf{A} = [a_{ik}]$ e $\det(\mathbf{A}) \in \mathcal{O}_K$. Portanto, $d(\mathcal{O}) = (d\mathcal{O}_K)^{\frac{1}{2}}$. ■

Corolário 3.2 *Sejam $\mathcal{A}$ uma álgebra dos quatérnios sobre K e $\mathcal{O}$, $\mathcal{O}_0$ duas $\mathcal{O}_K$-ordem em $\mathcal{A}$. Se $\mathcal{O} \subseteq \mathcal{O}_0$, então $d(\mathcal{O}_0)$ divide $d(\mathcal{O})$ e $d(\mathcal{O}) = d(\mathcal{O}_0)$ implica que $\mathcal{O} = \mathcal{O}_0$.* ■

Exemplo 3.3 *Sejam $\mathcal{A} = (a, b)_K$, onde $a, b \in \mathcal{O}_K$. Então*

$$\mathcal{O} = (a, b)_{\mathcal{O}_K} = \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k : \alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathcal{O}_K\}$$

é uma ordem em $\mathcal{A}$. Como $\{e_1, e_2, e_3, e_4\} = \{1, i, j, k\}$ é a base definindo $\mathcal{O}$ temos que $(\mathrm{tr}(e_ie_j))$ é a seguinte matriz diagonal:

$$[\mathrm{tr}(e_ie_j)] = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -2a & 0 & 0 \\ 0 & 0 & -2b & 0 \\ 0 & 0 & 0 & 2ab \end{pmatrix}.$$

Portanto,

$$d(\mathcal{O}) = 4ab = 4\mathcal{O}_K = \{4\beta : \beta \in \mathcal{O}_K\}.$$

Em particular, se $K = \mathbb{Q}$, $a = b = -1$ *e*

$$\{e_1, e_2, e_3, e_4\} = \left\{1, i, j, \frac{1+i+j+k}{2}\right\},$$

então $d(\mathcal{O}) = 2\mathbb{Z}$.

Observação 3.3 *Sejam*

$$\mathcal{A} = (\sqrt{2}, -1)_K$$

uma álgebra dos quatérnios sobre $K = \mathbb{Q}(\sqrt{2})$ *e* $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$. *Então*

$$\mathcal{A} = (\sqrt{2}, -1)_K \simeq (-\sqrt{2}, -1)_K = \mathcal{A}_1 \ \text{ e } \ d(\mathcal{A}) = d(\mathcal{A}_1) = \sqrt{2}\mathbb{Z}.$$

Teorema 3.1 *Sejam* $\mathcal{A}$ *uma álgebra dos quatérnios sobre* K *e* R *um subanel de* $\mathcal{A}$ *contendo* $\mathcal{O}_K$ *tal que* $KR = \mathcal{A}$. *Se cada* $a \in R$ *é inteiro sobre* $\mathcal{O}_K$, *então* R *é uma* $\mathcal{O}_K$*-ordem em* $\mathcal{A}$. *Reciprocamente, qualquer* $\mathcal{O}_K$*-ordem em* $\mathcal{A}$ *possui estas propriedades.*

Prova. Suponhamos que R seja um subanel de $\mathcal{A}$ contendo $\mathcal{O}_K$ tal que $KR = \mathcal{A}$. Então

$$\mathcal{A} = \sum_{i=1}^{4} Ke_i,$$

onde $e_i \in R$. Assim,

$$d = \det\left(\operatorname{tr}(e_i e_j)\right) \in \mathcal{O}_K,$$

pois os e_i são inteiros sobre $\mathcal{O}_K$.

Afirmação.

$$R \subseteq d^{-1} \sum_{i=1}^{4} \mathcal{O}_K e_i.$$

De fato, seja $\alpha \in R$, de modo que

$$\alpha = \sum_{i=1}^{4} r_i e_i \in K.$$

Então

$$\operatorname{tr}(\alpha e_j) = \sum_{i=1}^{4} r_i \operatorname{tr}(e_i e_j), \ \ 1 \leq j \leq 4.$$

Como $\alpha e_j \in R$ temos que $\operatorname{tr}(\alpha e_j) \in \mathcal{O}_K$. Logo, pela Regra de Cramer,

$$r_i = \frac{b_i}{d}, \ \ 1 \leq i \leq 4,$$

onde $b_i \in \mathcal{O}_K$. Assim,

$$R \subseteq d^{-1} \sum_{i=1}^{4} \mathcal{O}_K e_i.$$

Portanto, R é um reticulado em $\mathcal{A}$. ■

Teorema 3.2 *Qualquer álgebra $\mathcal{A}$ sobre um corpo K contém pelo menos uma ordem maximal em $\mathcal{A}$.*

Prova. Confira [**?**, page, 127]. ■

Proposição 3.3 *Sejam $\mathcal{A}$ uma álgebra central simples sobre K e $\mathcal{M}$ uma $\mathcal{O}_K$-ordem de $\mathcal{A}$. Então existe $\alpha \in \mathcal{O}_K$, com $\alpha \neq 0$, tal que $\alpha \cdot 1 \in \mathcal{O}_K$. Além disso,*

$$\mathcal{O}_L(\mathcal{M}) = \{b \in \alpha^{-1}\mathcal{M} : b\mathcal{M} \subseteq \mathcal{M}\} \subseteq \alpha^{-1}\mathcal{M}.$$

Teorema 3.3 *Sejam $\mathcal{A}$ uma álgebra dos quatérnios sobre K e $\mathcal{O}$ uma $\mathcal{O}_K$-ordem em $\mathcal{A}$. Então existe uma base $\{e_1, e_2, e_3, e_4\}$ de $\mathcal{A}$ e um ideal fracionário J de K tal que*

$$\mathcal{O} = \{a_1e_1 + x_2e_2 + x_3e_3 + x_4x_4 : a_1 \in J,\ \ x_i \in \mathcal{O}_K\}.$$

Prova. Confira [**?**, page, 212]. ■

Exemplo 3.4 *Sejam*

$$\mathcal{A} = (\sqrt{2}, -1)_K$$

uma álgebra dos quatérnios sobre $K = \mathbb{Q}(\sqrt{2})$ e $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$, com uma base $\{1, e, f, ef\}$ satisfazendo

$$e^2 = \sqrt{2},\ \ f^2 = -1$$

e $\mathcal{O} = (\sqrt{2}, -1)_R$, em que

$$R = \left\{ \frac{x}{2^n} : x \in \mathcal{O}_K \ \ e \ \ n \in \mathbb{N} \right\}.$$

Então $d(\mathcal{O}) = \sqrt{2}\mathbb{Z}$. Além disso, como observado em **??**,

$$\mathcal{A} \simeq \mathcal{A}_1 = (-\sqrt{2}, -1)_K \ \ e \ \ d(\mathcal{A}) = \sqrt{2}\mathbb{Z}.$$

Desta forma, $\mathcal{O}$ é uma R-ordem maximal em $\mathcal{A}$.

Capítulo 4

Reticulados Algébricos e Códigos

Neste capítulo apresentaremos um método para determinar reticulados algébricos em R^n via a imersão de Minkowiski e códigos baseados em álgebras. Além disso, apresentaremos um algoritmo para determinar uma ordem maximal em uma álgebra central simples.

4.1 Reticulados Algébricos

Sejam K um corpo de números e $\mathcal{O}_K$ o seu anel dos inteiros. Então $K = \mathbb{Q}(\theta)$, onde $\theta \in \mathcal{O}_K$. Sejam $\sigma_1 = 1, \ldots, \sigma_n$ o conjunto de todas as imersões de K em $\mathbb{C}$, isto é,

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1 = 1, \ldots, \sigma_n\}.$$

A *assinatura* de K é um par (r, s), onde r é o número de imersões de K cuja imagem está em $\mathbb{R}$, e $2s$ é o número de imersões não reais, de modo que $r + 2s = n$. Note que o número de imersões não reais sempre ocorrem aos pares, pois se σ é uma imersão não real, então $\overline{\sigma}$ também o é. Vamos ordenar os σ_i, de modo que, para todo $\alpha \in K$, $\sigma_i(\alpha) \in \mathbb{R}$, $1 \leq i \leq r$, e $\sigma_{j+s}(\alpha)$ é a conjugação de $\sigma_j(\alpha)$, para $r + 1 \leq j \leq r + s$.

O homomorfismo $\varphi : K \to \mathbb{R}^r \times \mathbb{C}^s$ definido como

$$\varphi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \sigma_{r+1}(\alpha), \ldots, \sigma_{r+s}(\alpha))$$

chama-se de *imersão canônica* ou *imersão de Minkowiski*. Assim, podemos definir $\varphi : K \to \mathbb{R}^n$ como

$$\varphi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_r(\alpha), \mathrm{Re}\,\sigma_{r+1}(\alpha), \mathrm{Im}\,\sigma_{r+1}(\alpha), \ldots, \mathrm{Re}\,\sigma_{r+s}(\alpha), \mathrm{Im}\,\sigma_{r+s}(\alpha)),$$

onde Re e Im denotam, respectivamente, a parte real e imaginária de α.

Teorema 4.1 *Seja $\varphi : K \to \mathbb{R}^n$ definido acima. Então*:

1. *φ é um homomorfismo injetor.*

2. *$\varphi(c\alpha) = c\varphi(\alpha)$, para todo $c \in \mathbb{Q}$ e $\alpha \in K$.*

3. *Se $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de K sobre $\mathbb{Q}$, então $\{\varphi(\alpha_1), \varphi(\alpha_2), \ldots, \varphi(\alpha_n)\}$ é linearmente independente sobre $\mathbb{R}$.*

4. *Seja $\mathcal{O}$ um $\mathbb{Z}$-módulo livre de $\mathcal{O}_K$, com $\{\alpha_1, \ldots, \alpha_n\}$ uma base integral para K. Então a imagem de $\mathcal{O}$*

$$\Gamma = \varphi(\mathcal{O}) = [\varphi(\alpha_1), \ldots, \varphi(\alpha_n)]$$

via φ em $\mathbb{R}^n$ é um reticulado, com geradores $\varphi(\alpha_1), \ldots, \varphi(\alpha_n)$, o qual é chamado de reticulado algébrico.

Corolário 4.1 *Seja $\varphi : K \to \mathbb{R}^n$ a imersão canônica. Então $\varphi(J)$ é um reticulado algébrico em $\mathbb{R}^n$, para todo ideal não nulo em $\mathcal{O}_K$.*

Note que se $\{\alpha_1, \ldots, \alpha_n\}$ uma base integral para K, então a matriz geradora do reticulado Γ é dada por

$$\mathbf{G} = \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \operatorname{Re}\sigma_{r+1}(\alpha_1) & \operatorname{Im}\sigma_{r+1}(\alpha_1) & \cdots & \operatorname{Re}\sigma_{r+s}(\alpha_1) & \operatorname{Im}\sigma_{r+s}(\alpha_1) \\ \sigma_1(\alpha_2) & \cdots & \sigma_r(\alpha_2) & \operatorname{Re}\sigma_{r+1}(\alpha_2) & \operatorname{Im}\sigma_{r+1}(\alpha_2) & \cdots & \operatorname{Re}\sigma_{r+s}(\alpha_2) & \operatorname{Im}\sigma_{r+s}(\alpha_2) \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \operatorname{Re}\sigma_{r+1}(\alpha_n) & \operatorname{Im}\sigma_{r+1}(\alpha_n) & \cdots & \operatorname{Re}\sigma_{r+s}(\alpha_n) & \operatorname{Im}\sigma_{r+s}(\alpha_n) \end{bmatrix}$$

Exemplo 4.1 *Se $K = \mathbb{Q}(\eta)$, em que $d \equiv 1 \pmod 4$,*

$$\eta = \frac{1+\sqrt{d}}{2} \;\; e \;\; d < 0,$$

então $\leqslant\!\!\!\!\!\!= \varphi(\mathcal{O}_K)$ é um reticulado em $\mathbb{R}^2$.

Solução. Pelo Teorema **??**, $\{1, \eta\}$ é uma base integral de K. Seja $\sigma : K \to \mathbb{C}$ uma imersão. Então dado $\alpha \in K$, digamos $\alpha = a + b\eta$, onde $a, b \in \mathbb{Q}$, obtemos

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

Como $\sigma(\eta)$ é também uma raiz de

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

temos que $\sigma(\eta) = \eta$ ou $\sigma(\eta) = \overline{\eta}$. Portanto, $\sigma(\alpha) = \alpha$ e $\sigma(\alpha) = \overline{\alpha}$. Assim, existem exatamente duas imersões $\sigma_1, \sigma_2 : K \to \mathbb{C}$, com $\sigma_2 = \overline{\sigma}_1$. Neste caso, $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1 = 1, \sigma_2\}$. Logo, a função $\varphi : K \to \mathbb{R}^2$ definida como

$$\varphi(\alpha) = (\mathrm{Re}\,\sigma_1(\alpha), \mathrm{Im}\,\sigma_1(\alpha))$$

é uma imersão canônica e $\Gamma = \varphi(\mathcal{O}_K)$ é um reticulado em $\mathbb{R}^2$ gerado por $\varphi(1)$ e $\varphi(\eta)$, isto é, o conjunto

$$\left\{(1,0), \left(\frac{1}{2}, \frac{\sqrt{-d}}{2}\right)\right\}$$

é uma $\mathbb{Z}$-base de Γ. Portanto,

$$\mathbf{G} = \begin{bmatrix} \mathrm{Re}\,\sigma_1(1) & \mathrm{Im}\,\sigma_1(1) \\ \mathrm{Re}\,\sigma_1(\eta) & \mathrm{Im}\,\sigma_1(\eta) \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ \frac{1}{2} & \frac{\sqrt{-d}}{2} \end{bmatrix}$$

é uma matriz geradora de Γ. ■

4.2 Códigos

Quando falamos de codificação de espaços temporais descrevemos o problema de codificação que estamos interessados para transmitir n antenas em termos da construção de subgrupos aditivos G de $M_n(F)$, onde todas as matrizes não nulas de G são invertíveis e $F \subseteq \mathbb{C}$ é um subcorpo. Portanto, subconjuntos $\mathcal{C}$ de G produzem livros de códigos de diversidade completa.

Sejam $\mathcal{A}$ uma álgebra dos quatérnios (ou uma álgebra qualquer) sobre K e F um subcorpo (maximal) de A contendo K. Para cada $\alpha \in \mathcal{A}$ fixado, a função $L_\alpha : \mathcal{A} \to \mathcal{A}$ definida como $L_\alpha(x) = \alpha x$ é linear sobre F. Logo, a função $L : \mathcal{A} \to M_2(F)$ definida como

$$L(\alpha) = \mathbf{M}_\alpha = \begin{bmatrix} z & b\sigma(w) \\ w & \sigma(z) \end{bmatrix},$$

onde $\sigma \in \mathrm{Aut}_K(F)$ e $2 = \dim_F(\mathcal{A})$, é um homomorfismo de algebras injetor sobre F. Portanto, podemos identificar $\mathcal{A}$ com o conjunto das matrizes

$$\mathcal{A}_L = \left\{ \begin{bmatrix} z & b\sigma(w) \\ w & \sigma(z) \end{bmatrix} : z, w \in F \right\} \subseteq M_2(F) \subseteq M_2(\mathbb{C}).$$

Um *código baseado na álgebra* $\mathcal{A}$ ou simplesmente um *código* sobre $\mathcal{A}$ é um subconjunto (finito) $\mathcal{C}$ de $M_2(\mathbb{C})$ definido como

$$\mathcal{C} = \{\mathbf{X} = \mathbf{M}_\alpha : \alpha \in \mathcal{B}\},$$

onde $\mathcal{B}$ é um subconjunto de $\mathcal{A}$.

Proposição 4.1 *Se $\mathcal{A}$ é uma álgebra com divisão sobre K, então $\mathcal{C}$ é um código de diversidade completa.*

Prova. Dados $\mathbf{X}_1, \mathbf{X}_2 \in \mathcal{C}$, com $\mathbf{X}_1 \neq \mathbf{X}_2$. Então existem $\alpha, \beta \in \mathcal{B}$, com $\alpha \neq \beta$, tais que $L(\alpha) = \mathbf{M}_\alpha$ e $L(\beta) = \mathbf{M}_\alpha$. Assim.

$$L(\alpha - \beta) = \mathbf{M}_{\alpha-\beta}$$

é uma matriz invertível em $M_2(F)$, pois L é um homomorfismo de aneis e $\alpha - \beta$ é uma unidade em $\mathcal{A}$. Portanto,

$$\det(\mathbf{X}_1 - \mathbf{X}_2) \neq 0$$

e $\mathcal{C}$ é um código de diversidade completa. ■

Seja F um corpo de número de grau n. Então $F = \mathbb{Q}(\theta)$, com θ uma raiz do polinômio

$$p = \text{irr}(\theta, \mathbb{Q}) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + x^n \in \mathbb{Q}[x],$$

e a função $L : F \to M_n(\mathbb{Q})$, definida como $L(\alpha) = \mathbf{M}_\alpha$, é um homomorfismo de aneis injetor. Como $\{1, \theta, \ldots, \theta^{n-1}\}$ é uma base F sobre $\mathbb{Q}$ temos que cada $\alpha \in F$ pode ser escrito de modo único sob a forma

$$\alpha = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}, \text{ onde } c_0, c_1, \ldots, c_{n-1} \in \mathbb{Q}.$$

Assim,

$$\begin{aligned} L_\alpha(1) &= c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1} \\ L_\alpha(\theta) &= -ac_{n-1} + (c_0 - a_1c_{n-1})\theta + \cdots + (c_{n-2} - a_{n-1}c_{n-1})\theta^{n-1} \\ &\vdots \end{aligned}$$

Portanto,

$$\begin{aligned} \mathbf{M}_\alpha &= \begin{bmatrix} c_0 & -a_0c_{n-1} & \cdots & \cdots \\ c_1 & c_0 - a_1c_{n-1} & \cdots & \cdots \\ \vdots & \vdots & \vdots & \vdots \\ c_{n-1} & c_{n-2} - a_{n-1}c_{n-1} & \cdots & \cdots \end{bmatrix} \\ &= c_0\mathbf{I}_n + c_1\mathbf{M}_\theta + \cdots + c_{n-1}\mathbf{M}_\theta^{n-1}, \end{aligned}$$

em que

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

é a matriz companheira de p. Consequentemente, o código

$$\mathcal{C} = \{\mathbf{X} = \mathbf{M}_\alpha : \alpha \in F\},$$

é de diversidade completa, pois $\mathcal{A} = F$ é uma álgebra (um corpo) sobre $K = \mathbb{Q}$ ou

$$\det \mathbf{X} = N(\alpha) = (-1)^n a_0 \neq 0.$$

Em particular, se

$$p = \text{irr}(\theta, \mathbb{Q}) = x^n - a \in \mathbb{Q}[x],$$

com $a \neq 0$, então

$$\mathbf{M}_\alpha = \begin{bmatrix} c_0 & ac_{n-1} & ac_{n-2} & \cdots & ac_1 \\ c_1 & c_0 & ac_{n-1} & \cdots & ac_2 \\ c_2 & c_1 & c_0 & \cdots & ac_3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ c_{n-1} & c_{n-2} & c_{n-3} & \cdots & c_0 \end{bmatrix}$$

e o código

$$\mathcal{C} = \{\mathbf{X} = \mathbf{M}_\alpha : \alpha \in F\},$$

é de diversidade completa. Note que

$$\mathcal{S} = \{c_0, c_1, \ldots, c_{n-1}\}$$

é o conjunto de sinais, os elementos de $\mathcal{S}$ são os símbolos de informações e os outros são símbolos de verificação de paridade ou símbolos de detecção para ser enviado sobre o canal. Portanto, o código $\mathcal{C}$ é sobre $\mathcal{S}$ e as entradas das matrizes palavras código estão no conjunto $\mathcal{S} \cup a\mathcal{S}$. Além disso, esse código é possível se existir n antenas de transmissão na saída do transmissor. É importante observar que $\mathcal{C}$ é um código finito quando limitamos os símbolos de informações c_i.

A *taxa de informação* R do código $\mathcal{C}$ é definida como a razão entre os símbolos de informações e os coeficientes enviados. No código acima

$$R = \frac{n}{n^2} = \frac{1}{n}.$$

Agora, vamos considerar a álgebra dos quatênios de Hamilton

$$\mathbb{H} = (-1,-1)_{\mathbb{R}} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}.$$

Seja

$$\xi = \xi_8 = e^{\frac{\pi}{4}i} = \frac{1}{\sqrt{2}}(1+i) \in \mathbb{C}$$

a raiz oitava da unidade. Então, pelo Exemplo **??**,

$$\begin{aligned} \mathbf{H} &= \mathbb{Q}(\xi) \oplus j\mathbb{Q}(\xi) \\ &= \{c_0 + \xi c_1 + jc_2 + j\xi c_3 : c_0, c_1, c_2, c_3 \in \mathbb{Q}(i)\} \end{aligned}$$

é uma álgebra de posto 4 sobre $K = \mathbb{Q}(i)$, a qual é uma subálgebra de $\mathbb{H}$. Neste caso,

$$\mathcal{C} = \left\{ \begin{bmatrix} c_0 & ic_1 & -c_2 & -\overline{c}_3 \\ c_1 & c_0 & i\overline{c}_3 & -\overline{c}_2 \\ c_2 & ic_3 & \overline{c}_0 & \overline{c}_1 \\ c_3 & c_2 & -i\overline{c}_1 & \overline{c}_0 \end{bmatrix} : c_0, c_1, c_2, c_3 \in \mathbb{Q}(i) \right\}$$

é um código de diversidade completa. Observe que

$$R = \frac{4}{4^2} = \frac{1}{4}.$$

Finalmente, vamos considerar a álgebra dos quatérnios (cíclica) $\mathcal{A} = (a,b)_K$, com

$$i^2 = a, \;\; j^2 = b \;\text{ e }\; k = ij = -ji,$$

onde $a, b \in K - \{0\}$. Sejam $i \notin K$ e $F = K(i)$. Então F é o corpo de decomposição do polinômio $p = x^2 - a \in K[x]$, o qual é irredutível sobre K. Assim, F é uma extensão cíclica de grau 2 de K, com o grupo de Galois

$$\mathrm{Gal}(F/K) = \{1, \sigma\} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}},$$

em que $\sigma(x + y\sqrt{a}) = x - y\sqrt{a} \in F$. Portanto,

$$\mathcal{C}_{\mathcal{A}} = \left\{ \begin{bmatrix} x + y\sqrt{a} & b(z - w\sqrt{a}) \\ z + w\sqrt{a} & x - y\sqrt{a} \end{bmatrix} : x, y, z, w \in K \right\}$$

é um código de diversidade completa sobre $\mathcal{A} = (a,b)_K = (F/K, \sigma, b)$. Neste caso, os símbolos de informações do código $\mathcal{C}_\mathcal{A}$ são x, y, z e w.

Já vimos que

$$\mathbf{H} = \mathbb{Q}(\xi) \oplus j\mathbb{Q}(\xi)$$

é uma álgebra com divisão de posto 4 sobre $K = \mathbb{Q}(i)$, contida na álgebra dos quatérnios de Hamilton $\mathbb{H} = (-1,-1)_\mathbb{R}$, e que o conjunto

$$\mathcal{L} = \{c_0 + \xi c_1 + jc_2 + j\xi c_3 : c_0, c_1, c_2, c_3 \in \mathcal{G}\}$$

é o anel de Lipschitz. Note que $\mathcal{L}$ não é uma $\mathcal{G}$-ordem maximal em $\mathbf{H}$, pois

$$\mathcal{H} = \mathcal{G}[\rho, \rho\xi, j, j\xi],$$

com $\mathcal{G} = \mathbb{Z}[i]$ e

$$\rho = \frac{1+i+j+k}{2},$$

é um subanel de $\mathbf{H}$ contendo $\mathcal{L}$. O anel $\mathcal{H}$ chama-se o *anel de Hurwitz* em $\mathbf{H}$. Observe que $q = c_0 + \xi c_1 + jc_2 + j\xi c_3 \in \mathcal{H}$ se, e somente se, existem $a_0, a_1, a_2, a_3 \in \mathcal{G}$ tais que

$$c_0 + \xi c_1 + jc_2 + j\xi c_3 = \rho a_0 + \rho\xi a_1 + ja_2 + j\xi a_3.$$

se, e somente se, $(1+i)c_t \in \mathcal{G}$, $t = 0,1,2,3$, e $c_0+c_2, c_1+c_3 \in \mathcal{G}$. Neste caso, se $I = \mathcal{G}[1+i]$, então $[\mathcal{G} : I] = 2$ e $[\mathcal{H} : \mathcal{L}] = 4$. Como $N(a+bi) = a^2+b^2 \geq 1$ temos o seguinte resultado:

Proposição 4.2 *Sejam $\mathcal{L}$, $\mathcal{H}$ o anel de Lipschitz e Hurwitz, respectivamente, em $\mathbf{H}$ e*

$$\alpha = c_0 + \xi c_1 + jc_2 + j\xi c_3 \in \mathbf{H}.$$

Então

$$\Gamma_\mathcal{L} = \{\mathbf{M}_\alpha : c_0, c_1, c_2, c_3 \in \mathcal{G}\}$$

e

$$\Gamma_\mathcal{H} = \left\{\mathbf{M}_\alpha : c_0, c_1, c_2, c_3 \in \frac{1+i}{2}\mathcal{G}, c_0 + c_2 \in \mathcal{G}, c_1 + c_3 \in \mathcal{G}\right\}$$

são STBC-reticulados de determinante mínimo igual a 1.

Observe que pondo $K = \mathbb{Q}(\sqrt{2})$ e $F = \mathbb{Q}(\xi)$, com

$$\xi = \xi_8 = e^{\frac{\pi}{4}i} = \frac{1}{\sqrt{2}}(1+i) \in \mathbb{C},$$

temos que F é o corpo de decomposição do polinômio

$$p = (x - \xi)(x - \xi^{-1}) = x^2 - \sqrt{2}x + 1 \in K[x],$$

o qual é irredutível sobre K. Assim, F é uma extensão cíclica de grau 2 sobre K, com o grupo de Galois

$$\mathrm{Gal}(F/K) = \{1, \sigma\} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}},$$

onde $\sigma(\xi) = \xi^{-1} \in F$. Portanto,

$$\mathbf{H} = \mathbb{Q}(\xi) \oplus j\mathbb{Q}(\xi) \simeq (F/K, \sigma, -1),$$

com $j^2 = -1$.

Proposição 4.3 *O anel Hurwitz*

$$\mathcal{H} = \{c_0 + \xi c_1 + jc_2 + j\xi c_3 : c_i \in K, (1+i)c_t \in \mathcal{G},\ \forall\ t,\ \ e\ \ c_0 + c_2, c_1 + c_3 \in \mathcal{G}\}$$

é uma $\mathbb{Z}$-ordem maximal em $\mathbf{H}$.

Prova. É fácil verificar que $\mathcal{H}$ é um subanel de $\mathbf{H}$ e que $\mathbf{H} = \mathbb{Q}\mathcal{H}$. Seja $\mathcal{O}$ qualquer $\mathbb{Z}$-ordem em $\mathbf{H}$. Então, pelo Teorema **??**, $\mathcal{O}[\sqrt{2}] = \mathcal{O}\mathbb{Z}[\sqrt{2}]$ também é uma $\mathbb{Z}[\sqrt{2}]$-ordem em $\mathbf{H}$. Assim, basta provar que $\mathcal{H}$ é uma $\mathbb{Z}[\sqrt{2}]$-ordem maximal. Suponhamos, por absurdo, que $\mathcal{H}$ não seja $\mathbb{Z}[\sqrt{2}]$-ordem maximal. Então existe uma $\mathbb{Z}[\sqrt{2}]$-ordem $\mathcal{O} = \mathcal{H}[q]$ contendo propriamente $\mathcal{H}$, com $q = a_1 + a_2 j$ e

$$a_t = c_{t0} + \xi c_{t1} + \xi^2 c_{t2} + \xi^3 c_{t3} \in F,\ \ t = 1, 2.$$

Logo,

$$\mathrm{tr}(q) = 2c_{10} + (c_{11} - c_{13})\sqrt{2} \in \mathbb{Z}[\sqrt{2}],$$

de modo que

$$\text{ou}\ \ c_{10} \in \mathbb{Z}\ \ \text{ou}\ \ c_{10} \in \mathbb{Z} + \frac{1}{2}$$

e $c_{11} - c_{13} \in \mathbb{Z}$. De modo análogo,

$$\mathrm{tr}(q\xi) = -2c_{13} + (c_{10} - c_{12})\sqrt{2} \in \mathbb{Z}[\sqrt{2}],$$

de modo que

$$\text{ou}\ \ c_{1l} \in \mathbb{Z}\ \ \text{ou}\ \ c_{1l} \in \mathbb{Z} + \frac{1}{2},\ \ l = 0, 1, 2, 3$$

e os pares

$$\text{ou } (c_{10}, c_{12}), (c_{11}, c_{13}) \in \mathbb{Z}^2 \text{ ou } (c_{10}, c_{12}), (c_{11}, c_{13}) \in \mathbb{Z}^2 + \frac{1}{2}.$$

Agora, usando $\mathrm{tr}(q\xi)$ e $\mathrm{tr}(qj\xi)$, obtemos

$$\text{ou } c_{2l} \in \mathbb{Z} \text{ ou } c_{2l} \in \mathbb{Z} + \frac{1}{2}, \ \ l = 0, 1, 2, 3$$

e os pares

$$\text{ou } (c_{20}, c_{22}), (c_{21}, c_{23}) \in \mathbb{Z}^2 \text{ ou } (c_{20}, c_{22}), (c_{21}, c_{23}) \in \mathbb{Z}^2 + \frac{1}{2}.$$

Podemos supor, sem perda de generalidade, que

$$c_{1l}, c_{2l} \in \left\{0, \frac{1}{2}\right\}, \ \ l = 0, 1, 2, 3,$$

pois substituindo q por $q - \omega_1$ ou $q - \omega_2 j$, onde $\omega_1, \omega_2 \in \mathbb{Z}[\xi]$, não muda a $\mathbb{Z}[\sqrt{2}]$-ordem $\mathcal{O} = \mathcal{H}[q]$, uma vez que $\mathbb{Z}[\xi] \subseteq \mathcal{H}$. Além disso, se substituirmos q por $q-\rho$ ou $q-\rho\xi$, então ainda podemos restringir ao caso em que $c_{2l} = 0$, $l = 0, 1, 2, 3$. Assim, é fácil verificar que a norma de qualquer um dos elementos

$$q = \frac{1}{2}(1+i), \frac{1}{2}(1+i)\xi, \frac{1}{2}(1+i)(1+\xi)$$

não está em $\mathbb{Z}[\sqrt{2}]$, o que é uma contradição. ■

Em tudo que segue I representa uma ideal não nulo em $\mathcal{O}_K$ (ou em um domínio Noetheriano). Consideremos o reticulado

$$E_8 = \frac{1}{1+i}\left\{(c_0, c_1, c_2, c_3) \in \mathcal{G}^4 : c_0 + I = c_t + I, \ \ t = 1, 2, 3, \ \ \sum_{t=0}^{3} c_t \in 2\mathcal{G}\right\}.$$

O leitor interessado em outras construções desse reticulado pode consultar [**?**]. Com a identificação entre os elementos (c_0, c_1, c_2, c_3) de $\mathcal{G}^4$e os elementos de $\mathbf{H}$, é fácil verificar que $\Gamma = (1+i)\, E_8$ possui o conjunto

$$\{2, (1+i) + (1+i)\,\xi, (1+i)\,\xi + (1+i)\,j, 1 + \xi + j + j\xi\} \subseteq \mathcal{L}$$

como uma $\mathcal{G}$-base, enquanto o conjunto

$$\{1+i, 1+\xi, \xi+j, \rho+\rho\xi\} \subseteq \mathcal{H}$$

é uma $\mathcal{G}$-base para E_8. Neste caso, $E_8 = \mathcal{H}[1+\xi]$, isto é, E_8 é um ideal não nulo do anel de Hurwitz $\mathcal{H}$ gerado por $1+\xi$ e, pela Proposição **??**, o reticulado Γ_{E_8} a seguir é ótimo dentro de $\mathbf{H}$.

Proposição 4.4 *Sejam $\mathcal{L}$ o anel de Lipschhitz em $\mathbf{H}$ e*

$$\alpha = c_0 + \xi c_1 + jc_2 + j\xi c_3 \in \mathbf{H}.$$

Então

$$\Gamma_{E_8} = \left\{ \mathbf{M}_\alpha : c_0 + I = c_t + I,\ \ t = 1, 2, 3,\ \ \sum_{t=0}^{3} c_t \in 2\mathcal{G} \right\}$$

é um sub-reticulado de $\Gamma_{\mathcal{L}}$, com $[\Gamma_{\mathcal{L}} : \Gamma_{E_8}] = 16$. Além disso, o determinante mínimo de Γ_{E_8} é igual a 64.

Prova. Seja $\mathbf{M}_I = \mathbf{M}_\alpha$, com $\alpha = 1 + \xi$. Então

$$\det(\mathbf{M}_I \overline{\mathbf{M}_I}^t) = 4.$$

Pelo exposto acima, qualquer matriz de Γ_{E_8} pode ser escrita sob a forma

$$\mathbf{A} = \mathbf{M}\mathbf{M}_I(1 + i),$$

onde $\mathbf{M}$ é uma matriz em $\Gamma_{\mathcal{H}}$. Assim,

$$\det(\mathbf{A}\overline{\mathbf{A}}^t) = 16 \det(\mathbf{M}_I \overline{\mathbf{M}_I}^t) \det(\mathbf{M}\overline{\mathbf{M}}^t).$$

Note que c_0 pode ser escolhido arbitrariamente em $\mathcal{G}$, enquanto c_1 e c_2 devem estar na classe $c_0 + I$ e c_3 deve ser escolhido de maneira que

$$c_0 + c_1 + c_2 + c_3 \in 2\mathcal{G} = I^2.$$

Como $I = [1 + i]$ é um ideal em $\mathcal{G}$ de índice 2 temos que o índice de Γ_{E_8} em $\Gamma_{\mathcal{L}}$ é 16.

Finalmente, pela Proposição **??**, o determinante mínimo Γ_{E_8} é igual a 64. ■

4.3 Algoritmo

Antes de apresentarmos o algoritmo daremos mais algumas observações e definições.

Sejam A um anel comutativo com identidade e $S \subseteq A$. Diremos que S é um *sistema multiplicativo* de A se as seguintes condições são satisfeitas:

1. $1 \in S$.

2. $st \in S$, $\forall s, t \in S$.

Dados $(a,s),(b,t) \in A \times S$, definimos

$$(a,s) \sim (b,t) \Leftrightarrow \exists\ u \in S \text{ tal que } (at-bs)\,u = 0.$$

Então é fácil verifica que $\sim$ é uma relação de equivalência sobre $A \times S$. Além disso,

$$S^{-1}A = \frac{A \times S}{\sim} = \left\{ \frac{a}{s} : a \in A \text{ e } s \in S \right\}$$

é uma partição de $A \times S$, em que $\frac{a}{s}$ denota a classe $\overline{(a,s)}$.

Teorema 4.2 *O conjunto $S^{-1}A$ munido com as operações binárias*

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st} \quad e \quad \frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$$

é um anel comutativo com identidade. Em particular, se A é um domínio de integridade e $S = A - \{0\}$, então $S^{-1}A$ é um corpo, chamado o corpo de frações *de A.*

Consideremos um ideal I em A. Então

$$S^{-1}I = \left\{ \frac{x}{s} : x \in I \text{ e } s \in S \right\}$$

é um ideal em $S^{-1}A$. Reciprocamente, se J é um ideal em $S^{-1}A$, então

$$I = \left\{ a \in A : \frac{a}{1} \in J \right\}$$

é um ideal em A. Portanto, as funções

$$\varphi: \begin{array}{ccc} I(A) & \to & I(S^{-1}A) \\ I & \mapsto & S^{-1}I \end{array} \quad \text{e} \quad \psi: \begin{array}{ccc} I(S^{-1}A) & \to & I(A) \\ J & \longmapsto & \psi(J) \end{array}$$

em que

$$\psi(J) = \left\{ a \in A : \frac{a}{1} \in J \right\}$$

estão bem definidas e satisfazem $(\varphi \circ \psi)(J) = J$ e $(\psi \circ \varphi)(I) \neq I$. Mas temos o seguinte resultado:

Teorema 4.3 *Existe uma correspondência biunívoca entre os ideais primos P de A que são disjuntos com S e os ideais primos Q de $S^{-1}A$.*

Proposição 4.5 *Sejam A um anel comutativo com identidade e P um ideal em A. Então*:

1. *$S = A - P$ é um sistema multiplicativo de A se, e somente se, P é um ideal primo.*

2. O conjunto

$$M = \left\{ \frac{a}{s} : a \in P \ \ e \ \ s \notin P \right\}$$

é o único ideal maximal em $S^{-1}A = A_P$*, chamado de localização de* A *em* P*.*

Agora, vamos obter um caso particular da Proposição acima. Seja p um número primo. Então $P = [p] = p\mathbb{Z}$ é um ideal primo (maximal) de $\mathbb{Z}$. Consideremos o conjunto

$$\mathbb{Z}_P = \left\{ \frac{a}{s} \in \mathbb{Q} : a, s \in \mathbb{Z}, \ \text{com} \ \ s \notin P \right\}.$$

Então $\mathbb{Z}_P$ é um domínio de ideais principais, pois se J é um ideal de $\mathbb{Z}_P$, então é fácil verificar que o conjunto

$$I = \left\{ a \in \mathbb{Z} : \frac{a}{s} \in J, \ \text{para algum} \ \ s \notin P \right\}$$

é um ideal em $\mathbb{Z}$. Assim, existe um menor inteiro positivo d tal que

$$I = d\mathbb{Z} = \{dn : n \in \mathbb{Z}\}.$$

Afirmação. $J = \frac{d}{x}\mathbb{Z}_P$, para algum $x \notin P$.
De fato, dado $u \in J$, digamos $u = \frac{a}{s}$, onde $a, s \in \mathbb{Z}$ e $s \notin P$. Então, pelo Algoritmo da Divisão, existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = qd + r, \ \ \text{com} \ \ 0 \leq r < d.$$

Logo, $r = 0$, pois se $r > 0$, então

$$\frac{r}{s} = u - q\frac{d}{s} \in J,$$

o que contradiz a minimalidade de d. Assim,

$$u = \frac{a}{s} = \frac{d}{x}\left(\frac{qx}{s}\right) \in \left[\frac{d}{x}\right] = \frac{d}{x}\mathbb{Z}_P.$$

Agora, vamos provar que o conjunto

$$M_P = \left\{ \frac{a}{s} : a \in P \ \text{e} \ \ s \notin P \right\} = p\mathbb{Z}_P$$

é o único ideal maximal em $\mathbb{Z}_P$. Dados $\frac{a}{s}, \frac{b}{t} \in M_P$ e $\frac{x}{u} \in \mathbb{Z}_P$, obtemos

$$\frac{a}{s} - \frac{b}{t} = \frac{at - bs}{st} \in M_P,$$

pois $at - bs \in P$ e $st \notin S$,

$$\frac{a}{s} \cdot \frac{x}{u} = \frac{ax}{su} \in M_P,$$

pois $ax \in P$ e $su \notin P$. Logo, M_P é um ideal em $\mathbb{Z}_P$.

Finalmente, se $\frac{y}{b} \in \mathbb{Z}_P - M_P$, então $y \notin P$. Assim,

$$\frac{b}{y} \in \mathbb{Z}_P \text{ e } \frac{y}{b} \in \mathcal{U}(\mathbb{Z}_P).$$

Portanto, se I é um ideal qualquer em $\mathbb{Z}_P$ tal que $I \not\subset M_P$, então $I \subseteq \mathcal{U}(R_P)$, ou seja, $I = A_P$. Assim, M_P é o único ideal maximal em $\mathbb{Z}_P$. Neste caso, diremos que $\mathbb{Z}_P$ é um domínio local. Além disso, se $\mathcal{O}$ é uma $\mathbb{Z}$-ordem em $\mathbb{Z}_P$, usaremos a notação

$$\mathcal{O}_P = \mathbb{Z}_P\mathcal{O}.$$

Seja R um anel comutativo com identidade. O conjunto

$$\text{Rad}(R) = \{x \in A : xM = \{0\}\},$$

em que M é um R-módulo simples, chama-se o *Radical de Jacobson* de R ou, equivalentemente, $\text{Rad}(R)$ é igual a interseção de todos os ideais maximais em R. Por exemplo,

$$\text{Rad}(\mathbb{Z}_P) = p\mathbb{Z}_P.$$

Proposição 4.6 *Seja R um anel comutativo com identidade. Então $x \in \text{Rad}\,(R)$ se, e somente se, $1 - xy$ é uma unidade em R, para todo $y \in R$.*

Proposição 4.7 *Sejam $\mathcal{A}$ uma álgebra central simples de posto n sobre K e $\mathcal{O}$ uma R-ordem maximal de $\mathcal{A}$ (R um anel de Dedekind). Então os ideais primos $\mathcal{P}$ em $\mathcal{O}$ estão em correspondência biunívoca com os ideais primos P em R via $P = \mathcal{P} \cap R$ e $P\mathcal{O} \subseteq \mathcal{P}$.*

1. *Qualquer ideal $\mathcal{J}$ em $\mathcal{O}$ pode ser escrito sob a forma*

   $$\mathcal{J} = \mathcal{P}_1 \cdots \mathcal{P}_m,$$

   onde $\mathcal{P}_1, \ldots, \mathcal{P}_m$ são ideais primos em $\mathcal{O}$.

2. *Para um ideal primo P em R existe um único número natural n_P tal que $P\mathcal{O} = \mathcal{P}^{n_P}$. Os números n_P são divisores de n e $n_P = 1$, exceto para uma quantidade finita de ideais primos P em R.*

3. *$d(\mathcal{O})$ é idependente da R-ordem maximal $\mathcal{O}$. Além disso, se $n_P > 1$, então $\mathcal{P}$ divide $d(\mathcal{O}) \in \mathcal{O}$, ou seja, $\mathcal{P}$ divide $[d(\mathcal{O})]$*

Prova. Confira [**?**, Chapter 6]. ■

Proposição 4.8 *Sejam $\mathcal{A}$ uma álgebra central simples de posto n sobre K e P um ideal primo em R. Se $\mathcal{O}$ é uma R-ordem de $\mathcal{A}$ tal que $\mathcal{O}_P$ não é uma R_P-ordem maximal, então existe um ideal $P\mathcal{O} \subseteq \mathcal{I}$ em $\mathcal{O}$, para o qual $\mathcal{O} \subset \mathcal{O}_L(\mathcal{I})$.*

Podemos usar as Proposições **??** e **??**, como um algoritmo para determinarmos a maximalidade de uma R-ordem em uma algebra central simples sobre um corpo K. Sejam $\mathcal{O}$ uma $\mathcal{O}_K$-ordem em $\mathcal{A}$ e k um múltiplo de $d(\mathcal{O})$. Então o algoritmo trabalha como segue:

Na entrada do algoritmo requeremos duas listas:

1. Consiste dos ideais primos P de $\mathcal{O}_K$ que dividem k.

2. Os ideais primos $\mathcal{P}$ em $\mathcal{O}$ que contêm $P\mathcal{O}$.

Note, pelas Proposições **??** e **??**, que se P não está contido na primeira lista, então $\mathcal{O}_P$ é uma $(\mathcal{O}_K)_P$-ordem maximal. Assim, devemos verificar a maximalidade local nos ideais primos P da primeira lista. Portanto, pelas Proposições **??** e **??**, basta aplicar o algoritmo a seguir em cada P.

Algoritmo

1.^{0} **Passo**. Existe um único um ideal primo $\mathcal{P}$ de $\mathcal{O}$ na segunda lista tal que $P\mathcal{O} \subseteq \mathcal{P}$? Se não pare e $\mathcal{O}$ não é uma $(\mathcal{O}_K)_P$-ordem maximal. Caso contrário, vá para o Passo 2.

2.^{0} **Passo**. Existe um inteiro t, com $1 \leq t \leq n$, tal que $P\mathcal{O} = \mathcal{P}^t$? Se não pare e $\mathcal{O}$ não é uma $(\mathcal{O}_K)_P$-ordem maximal. Caso contrário, vá para o Passo 3.

3.^{0} **Passo**. A igualdade

$$\{J : P\mathcal{O} \subseteq J \text{ ideal de } \mathcal{O}\} = \{\mathcal{P}^i : 0 \leq i \leq t\}$$

vale? Se não pare e $\mathcal{O}$ não é uma $(\mathcal{O}_K)_P$-ordem maximal. Caso contrário, vá para o Passo 4.

4.^{0} **Passo**. É a $\mathcal{O}_K$-ordem $\mathcal{O}_E(\mathcal{P}^i) = \mathcal{O}$, para todo ideal $\mathcal{P}^i$ em $\mathcal{O}$, com $0 \leq i \leq t$? Sim, então $\mathcal{O}$ é uma $(\mathcal{O}_K)_P$-ordem maximal. Caso contrário, $\mathcal{O}$ não é uma $(\mathcal{O}_K)_P$-ordem maximal.

Como uma aplicação deste algoritmo apresentamos o seguinte exemplo:

Exemplo 4.2 *Se $\mathcal{A}$ é uma álgebra dos quatérnios sobre $K = \mathbb{Q}(i)$, então*

$$\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}, i\right]$$

é uma ordem maximal de $\mathcal{A}$.

Solução. Seja $F = K(\sqrt{5}) = \mathbb{Q}(\sqrt{5}, i)$. Então F é o corpo de decomposição do polinômio

$$p = x^2 - x - 1 \in K[x],$$

o qual é irredutível sobre K, com

$$\theta = \frac{1+\sqrt{5}}{2} \text{ e } \overline{\theta} = 1 - \theta = \frac{1-\sqrt{5}}{2}$$

raízes. Assim, F é uma extensão cíclica de grau 2 sobre K, com o grupo de Galois

$$\mathrm{Gal}(F/K) = \{1, \sigma\} \simeq \frac{\mathbb{Z}}{2\mathbb{Z}},$$

onde $\sigma(x + \theta y) = x + \overline{\theta} y \in F$. Como

$$i \neq N(x + \theta y) = x^2 + xy - y^2, \ \forall \ x, y \in K,$$

temos que $f = t^2 - i \in K[t]$ é irredutível sobre K. Se $\beta \in \mathbb{C}$ é uma raiz de f, então

$$\begin{aligned} \mathbf{E} &= F \oplus \beta F \\ &= \{z + \beta w : z, w \in F\} \end{aligned}$$

é uma álgebra cíclica de posto 4, com uma base $\{1, \theta, \beta, \beta\theta\}$. Note que $\mathcal{O}_K = \mathbb{Z}[i]$ é o anel dos inteiros de Gauss. Assim, $\mathcal{O} = \mathcal{O}_K[\theta]$ é a $\mathbb{Z}[i]$-ordem maximal de $\mathbf{E}$, com discriminante $d = 5^2$. Logo, a primeira lista é formada pelos primos $P = [2 + i]$ e $P = [2 - i]$. Logo, aplicaremos o algoritmo apenas para o ideal $P = [2 + i]$.

Primeiro note que como $\beta^2 = -2$ em $\frac{\mathcal{O}}{P\mathcal{O}}$ temos que β define um corpo $\mathbb{F}_{25}$. Assim, qualquer ideal não trivial $I \subset \frac{\mathcal{O}}{P\mathcal{O}}$ é um espaço vetorial sobre $\mathbb{F}_{25}$ e

$$I \cap \mathbb{F}_{25} = \{0\}.$$

É possível verificar que o ideal $J = \mathbb{F}_{25}[\theta + 2]$ é nilpotente. Como

$$\dim_{\mathbb{F}_5} \left(\frac{\mathcal{O}}{P\mathcal{O}} \right) = 4$$

J é o único ideal maximal não trivial em $\frac{\mathcal{O}}{P\mathcal{O}}$. Então

$$J = \text{Rad} \left(\frac{\mathcal{O}}{P\mathcal{O}} \right) = \mathbb{F}_5[\theta + 2] \oplus \mathbb{F}_5[\beta\,(\theta + 2)].$$

Portanto, a segunda lista é:

$$\left\{ P\mathcal{O}, \mathcal{P} = \left\langle \sqrt{5}, P\mathcal{O} \right\rangle, \mathcal{O} \right\},$$

com $\mathcal{P}$ o único ideal primo e $\sqrt{5} = 2\theta - 1$. O algoritmo agora é feito como se segue:

1.^{0} **Passo**. Já vimos que $\mathcal{P}$ é o único ideal primo na segunda lista

2.^{0} **Passo.** Se $t = 2$, então $\mathcal{P}^t = P\mathcal{O}$.

De fato, a inclusão $\mathcal{P}^2 \subseteq P\mathcal{O}$ é imediata. Então basta provar que $P\mathcal{O} \subseteq \mathcal{P}^2$, isto é, que $P \in \mathcal{P}^2$. Note que

$$(2 + i)^2, \left(\sqrt{5} \right)^2 \in \mathcal{P}^2.$$

Como $\mathcal{G}$ é um domínio Euclidiano temos que existem $a, b \in \mathcal{G}$ tais que

$$a\,(2 + i)^2 + b5 = 2 + i.$$

Logo, $P = (2 + i) \in \mathcal{P}^2$.

3.^{0} **Passo**. Sendo $\mathcal{P}^0 = \mathcal{O}$, $\mathcal{P}^1 = \mathcal{P}$ e $\mathcal{P}^2 = P\mathcal{O}$, obtemos

$$\{J : P\mathcal{O} \subseteq J \text{ ideal de } \mathcal{O}\} = \{\mathcal{P}^i : 0 \leq i \leq 2\}.$$

4.^{0} **Passo**. Devemos provar que $\mathcal{O}_E\,(\mathcal{M}) = \mathcal{O}$, para todo

$$\mathcal{M} \in \left\{ P\mathcal{O}, \mathcal{P} = \left\langle \sqrt{5}, P\mathcal{O} \right\rangle, \mathcal{O} \right\}.$$

Note que

$$\mathcal{O} \subseteq \mathcal{O}_E\left(\mathcal{P}^i\right), \;\; 1 \leq i \leq t.$$

Pela Proposição **??**, $\mathcal{O}_E\,(\mathcal{M}) \subseteq 1^{-1}\mathcal{O}$, com $1 \in \mathcal{O}$ e

$$\mathcal{O}_E\,(\mathcal{M}) \subseteq (2 + i)^{-1}\,\mathcal{O}.$$

Observe que $2+i \in \mathcal{M}$, para todo $\mathcal{M}$. No caso $\mathcal{M} = P\mathcal{O}$, é claro que $\mathcal{O}_E(\mathcal{M}) \subseteq \mathcal{O}$ e também no caso $\mathcal{M} = \mathcal{P}$. Assim, resta provar se

$$x = p + r\beta + s\sqrt{5} + t\beta\sqrt{5} \in \mathcal{O}_E(M), \text{ onde } p, r, s, t \in \mathbb{Q}(i),$$

então $2 + i$ não divide os denominadores de p, r, s e t. Considerando os elementos $x\sqrt{5}, x(2+i) \in \mathcal{P}$ temos que isto é verdade e, consequentemente, $\mathcal{O}$ é maximal em P. ■

Referências Bibliográficas

[1] Conway, J. H. and Sloane, N. J. A., *Sphere Packing, Lattices and Groups.* Springer-Verlag, 1993.

[2] Dickson, L.E. Algebras and Their Arithmetics. The University of Chicago Press, 1923.

[3] Endler, O. *Teoria dos Números Algébricos.* IMPA, Rio de Janeiro, 1985.

[4] Felzenszwalb, B. *Álgebras de Dimensão Finita.* IMPA, Rio de Janeiro, 1979.

[5] Garcia, A. L. e Lequain, Y., *Álgebra: Um Curso de Introdução.* IMPA, Rio de Janeiro, 1988.

[6] Gonçalves, A. *Introdução à Álgebra.* IMPA, Rio de Janeiro, 1979.

[7] Hiltunen, J,; Hollanti, C. and Lahtonen, J. "Dense Full-Diversity Matrix Lattices for Four Transmit Antenna MISO Channel," *TUCS Technical Report*, $N.^0$ 664, 2005.

[8] Hollanti, C. and Lahtonen, J. "A New Tool: Constructing SBTCs from Maximal Orders in Central Simple Algebras," *Information Theory Workshop*, 2006, Punta Del Este, $322 - 226$.

[9] Maclachlan, C. e Reider, A. W. *The Arithmetic of Hyperbolic* 3*-Manifolds.* Spring-Verlag, Berlim-Heidelberg-New York, 2003.

[10] MacLane, S. and Birkhoff, G. *Algebra.* Macmillan Company, 1968.

[11] O'Meara, O. T. *Introduction to Quadratic Forms.* Spring-Verlag, Berlim-Heidelberg-New York, 1973.

[12] Reiner, I. *Maximal Orders.* Academic Press, London, 1975.

[13] Ribenboin, P. *Algebraic Numbers*. New York, Wiley-Interscience, 1972.

[14] Samuel, P., *Algebraic Theory of Numbers.* Hermann, Paris 1970..

[15] Stewart, I.N. e Tall, D.O. *Algebraic Number Theory*. Chapman and Hall, 1996.

[16] Vignéras, M. F. *Aritmétique des Algébres de Quaternions*. Spring-Verlag, Berlim-Heidelberg-New York, 1980.

[17] Weiss, E., *Algebraic Number Theory*, Dover, 1998.