UNIVERSIDADE FEDERAL DO PARÁ

INSTITUTO DE CIÊNCIAS EXATAS E NATURAIS
FACULDADE DE MATEMÁTICA

FELIPE BAIA MACEDO

CORPOS QUADRÁTICOS: UMA INTRODUÇÃO À TEORIA DOS NÚMEROS ALGÉBRICOS

Belém

2023

CERTIFICADO DE AVALIAÇÃO

FELIPE BAIA MACEDO

CORPOS QUADRÁTICOS: UMA INTRODUÇÃO À TEORIA DOS NÚMEROS ALGÉBRICOS

Trabalho de Conclusão de Curso apresentado para a obtenção do grau de Licenciado em Matemática da Faculdade de Matemática da Universidade Federal do Pará e avaliado pela seguinte banca examinadora:

Prof. Dr. Jean Carlos de Aguiar Lelis (Orientador)
Faculdade de Matemática, UFPA

Profª. Dra. Juliana Silva Canella (Membro)
Faculdade de Matemática, UFPA

Prof. Dr. Marcel Vinhas Bertolini (Membro)
Faculdade de Matemática, UFPA

DATA DA DEFESA: ____ /____ /____

Conceito: _____

DEDICATÓRIA

Dedico primeiramente a Deus, por me conceder forças e trazer alegria para a minha vida. Dedico especialmente aos meus pais, Fabio Mendes Macedo e Maria do Livramento de Souza Baia.

AGRADECIMENTOS

A Deus por abençoar cada passo dado nessa jornada, por me fortalecer em dias difíceis e pelo seu infinito amor transbordado em minha vida.

À minha família pelo seu amor incondicional, por sempre acreditarem no meu potencial e estarem presente nos momentos felizes e tristes, cuidando e me incentivando a conquistar meus sonhos.

À Universidade Federal do Pará pela oportunidade de formação, pelo acolhimento e todas as atividades de ensino e pesquisa proporcionadas. Gostaria de agradecer também à Superintendência de Assistência Estudantil por prestar apoio financeiro durante uma grande parte da graduação.

Ao meu orientador Profº Dr. Jean Carlos de Aguiar Lelis por me apresentar a Teoria dos Números Algébricos e auxiliar nesse estudo bastante prazeroso, suas contribuições foram fundamentais para a conclusão deste trabalho. Sua dedicação, compreensão e paciência são admiráveis. Sou imensamente grato por ele compartilhar seu vasto conhecimento comigo, o responsável por despertar-me o desejo de seguir para a pós-graduação em Matemática.

A todos os professores que contribuíram para a minha formação. Excepcionalmente, aos professores(as) Marcel Bertolini, Tania Valdivia, Ulisses Canto e Valter Junior.

Aos meus valiosos amigos que caminharam comigo nessa trajetória. Em especial, a Sarah Sarmento, Fabiola Sodré e Jennyfer Neves, elas me encorajaram, ajudaram e demonstraram o valor de uma grande amizade, sem a presença delas a caminhada teria sido mais árdua. Agradeço particularmente aos meus companheiros de classe, Augusto Ramos que esteve comigo desde o ensino fundamental, Wallace Junior pela ajuda acadêmica, Ronaldo Machado pelos conselhos e a Larissa Paulo por todo incentivo.

Muito obrigado a todos!

A álgebra é generosa: frequentemente ela dá mais do que se lhe pediu.

(Jean Le Rond d'Alembert)

RESUMO

Este trabalho tem a finalidade de apresentar os Corpos Quadráticos. Para isso, será necessário realizarmos uma introdução à Teoria dos Números Algébricos. Destacamos que o principal objetivo é conseguir apresentar os assuntos de maneira didática sem perder o rigor matemático, por esse motivo, destacamos as definições, proposições, lemas e teoremas com suas respectivas cores e diversos exemplos para facilitar a ideia da teoria. Para tal propósito, apresentaremos alguns conceitos e resultados que complementam assuntos vistos em Álgebra Abstrata nos cursos de graduação, a fim que o leitor construa uma base necessária para compreender o conteúdo principal desta pesquisa. Serão apresentados os conceitos de corpos quadráticos e anéis de inteiros quadráticos, assim como, suas características. No decorrer, vamos abordar os anéis quadráticos complexos e os anéis quadráticos reais. Por fim, demonstramos que $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ é um anel principal que não é euclidiano e discutimos se existem outros com a mesma estrutura.

Palavras-chave: Corpos Quadráticos. Anel de Inteiros Algébricos. Números Algébricos. Extensões de Corpos.

LISTA DE SÍMBOLOS

$\mathbb{N}$	Conjunto dos Números Naturais.
$\mathbb{Z}$	Conjunto dos Números Inteiros.
$\mathbb{Q}$	Conjunto dos Números Racionais.
$\mathbb{R}$	Conjunto dos Números Reais.
$\mathbb{C}$	Conjunto dos Números Complexos.
$\subsetneq$	Contido mas não é igual.
$Ker(\phi)$	Núcleo de (ϕ).
$Im(\phi)$	Imagem de (ϕ).
$\partial(f(x))$	Grau do polinômio $f(x)$.
$\mathfrak{N}$	Anel Noetheriano.
$\mathcal{O}_K$	Anel de Inteiros Algébricos do corpo de números K.
$\mathcal{N}_K(\alpha)$	Norma de α.
$\mathcal{T}_K(\alpha)$	Traço de α.

$K(\alpha)$	Corpo K adjunto α.
$p_\alpha(x)$	Polinômio minimal de α.
$p(x_1, \ldots, x_n)$	Polinômios simétricos.
$\overline{\mathbb{Q}}$	Conjunto dos Números Algébricos.
$F\|K$	Extensão de Corpos.
$[F : K]$	Grau da Extensão de Corpos.
$\Delta[\alpha_1, \ldots, \alpha_n]$	Discriminante de uma base.
$det(A)$	Determinante de A.
(a_{ij})	Matriz.
$\mathbb{Q}(\sqrt{m})$	Corpos Quadráticos.
$\mathbb{Z}[\theta]$	Anel Quadrático.

SUMÁRIO

1 PRELIMINARES **14**

1.1 Grupos 15

1.2 Anéis e Domínios 17

1.3 Anéis de Polinômios 25

1.4 Espaços Vetoriais 30

1.5 Extensões de Corpos 35

1.6 Polinômios simétricos 39

1.7 Módulos 41

1.8 Grupos abelianos livres 42

2 Números Algébricos **45**

2.1 Números Algébricos 45

2.2 Conjugados e Discriminantes 47

2.3 Inteiros Algébricos 49

2.4 Bases integrais 51

2.5 Normas e Traços 52

3 Corpos Quadráticos **55**

3.1 Corpos Quadráticos 55

3.2 Inteiros Quadráticos que são Domínios Euclidianos 60

3.3 Anéis Principais que não são Euclidianos 65

Referências Bibliográficas. **72**

INTRODUÇÃO

Para investigar como a *Teoria dos Números Algébricos* surge, precisamos retomar ao ano de 1637, quando um famoso problema é conjecturado pelo matemático francês Pierre de Fermat, conhecido como o *Último Teorema de Fermat* onde afirma que não há solução para a equação

$$x^n + y^n = z^n, \tag{1}$$

se $n \geq 3$ e (x, y, z) são inteiros positivos. Refere-se de uma generalização do famoso teorema de Pitágoras, apesar do seu enunciado ser de fácil compreensão, diversas tentativas de demonstrações falharam e isso perdurou por bastante tempo. Este teorema trará motivação para os primeiros conceitos necessários para o estudo da Teoria dos Números Algébricos. O matemático Gabriel Lamé $(1795 - 1870)$, utilizou um método para solucionar o problema, ele supôs que a equação está situada no conjunto dos complexos e utilizou a raiz $p-$ésima primitiva da unidade $\zeta_p \neq 1$, para fatorar a equação (1) em termos lineares

$$x^p + y^p = (x + y) \cdot (x + \zeta_p y) \cdot \ldots \cdot (x + \zeta_p^{p-1} y).$$

Porém, está demonstração não estava correta, Joseph Liouville $(1809 - 1882)$ analisou que precisava de uma fatoração única no conjunto dos números inteiros ciclotômicos

$$\alpha_0 + \alpha_1 \zeta_p + \alpha_2 \zeta_p^2 + \ldots + \alpha_{p-1} \zeta_p^{p-1},$$

com $\alpha_i \in \mathbb{Z}$. Agora o problema centrava na unicidade de fatoração, e nesse contexto, Ernst Kummer (1810–1893) provou que dependendo do caso, a unicidade de fatoração nem sempre é possível, por exemplo, para $n = 23$. Kummer escreve uma carta para Liouville informando sobre: "a fatoração única em domínios de inteiros ciclotômicos "pode ser salva" com a introdução de um novo tipo de número complexo, os quais tenho chamado de números complexos ideais" (Kleiner, 2007). A partir de então, ele introduziu o *número ideal* e o *fator primo ideal*. Como a fatoração única em elementos irredutíveis algumas vezes falha em $\mathbb{Z}[\zeta_p]$, notou que certa propriedade sempre é válida para p quando o domínio $\mathbb{Z}[\zeta_p]$ é fatorial, cada ideal fatora unicamente em produto de *ideais primos*. Tal descoberta foi essencial para o desenvolvimento da Teoria dos Números Algébricos.

O estudo algébrico do anel $\mathbb{Z}[\sqrt{m}] = \{a + b\sqrt{m} \,|\, a, b, m \in \mathbb{Z}\}$, em que m é positivo livre de quadrados, auxiliou na obtenção de soluções inteiras na equação de Pell

$$x^2 - my^2 = (x - \sqrt{m}y)(x + \sqrt{m}y) = 1,$$

pela fatoração de números algébricos do anel $\mathbb{Z}[\sqrt{m}]$, temos que, as soluções inteiras (a, b) da equação de Pell, são representados pelos elementos invertíveis da forma $a + b\sqrt{m}$. Esse exemplo nos permite observar a suma importância no estudo algébrico do anel $\mathbb{Z}[\sqrt{m}]$ para a Teoria dos Números.

Embora a Teoria dos Números Algébricos tenha surgido como ferramenta, ela se tornou uma teoria independente, com forte aplicabilidade na *geometria aritmética, equações diofantinas* e na *construção de reticulados*. Sua noção principal está centrada no *anel dos inteiros algébricos* $\mathcal{O}_K$ de um *corpo de números* K. Estamos interessados em extensões de corpos que são gerados a partir da adjunção de uma raiz quadrada, são as chamadas extensões quadráticas, e o corpo gerado é dito *corpo quadrático*. Como são extensões de grau 2, veremos que toda extensão finita é algébrica.

No capítulo 1, abordamos os conceitos preliminares que envolvem tópicos da teoria dos anéis com foco especial nos anéis comutativos com unidade e ideais, a fatoração de polinômios com coeficientes em um corpo e aos resultados das extensões de corpos e dos polinômios simétricos, serão essenciais para compreendermos determinadas estruturas algébricas.

No capítulo 2, tratamos sobre os conceitos e resultados importantes para realizarmos uma introdução à Teoria dos Números Algébricos. Apresentamos noções fundamentais, que

incluem, os números algébricos, o conjunto dos números algébricos, corpos de números, conjugados, discriminantes, inteiros algébricos, bases integrais, normas, traços e o anel de inteiros algébricos.

No capítulo 3, realizamos um estudo sobre os Corpos Quadráticos $\mathbb{Q}(\sqrt{m})$, onde vamos caracterizar os seus anéis de inteiros algébricos, base integral, discriminante, norma e traço. Verificaremos quando os anéis de inteiros quadráticos $\mathbb{Z}[\theta]$ são euclidianos com a norma absoluta. Particularizamos um caso especial de anel, como exemplo, o anel $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ e demonstraremos que ele é principal e não euclidiano, para isso, vamos primeiramente provar que todo anel quase euclidiano é principal e identificar os elementos invertíveis e irredutíveis do respectivo anel.

CAPÍTULO

1

PRELIMINARES

A teoria dos anéis é um ramo da Matemática Pura que estuda e caracteriza as estruturas algébricas dos anéis, seus conceitos e resultados contribuiriam para o estudo de domínios euclidianos e domínios de ideias principais, sendo ambos objeto de estudo deste trabalho, inicialmente os estudos da teoria de anéis originou-se dos polinômios sobre corpos e a Teoria dos Números Algébricos. O conceito de grupo foi um passo fundamental para o surgimento das ideias abstratas, diversos matemáticos como Richard Dedekind (1831–1916), Leopold Kronecker (1823–1891) e Ernst Eduard Kummer (1810–1893) e o jovem matemático Évariste Galois ($1811 - 1832$) realizaram contribuições para o campo da Álgebra abstrata. Antes da fundamentação axiomática da Álgebra, o que tínhamos eram diversos resultados e problemas que agrupados adquiriam um tema em comum que servia de pontapé para outros resultados serem colecionados e assim unificar em um conjunto comum de conceitos.

1.1 Grupos

A origem da estrutura algébrica conhecida como *grupo* está relacionada ao estudo de equações polinomiais por Évariste Galois como podemos ver em [4]. O conceito de grupo é a noção central para Álgebra abstrata, pois outras estruturas algébricas que conheceremos em seções posteriores como, anéis, corpos e espaços vetoriais podem ser vistos como grupos munidos de operações e axiomas.

Definição 1.1: Grupos

Um conjunto não vazio G munido com uma operação $*$

$$\begin{aligned} *: \ G \times G \ &\to \ G \\ (a,b) \ &\mapsto a * b \end{aligned}$$

é um grupo se as condições seguintes são satisfeitas:

i) Fechamento

$$\forall\, a, b \in G, \ \ a * b \in G.$$

ii) A operação é associativa

$$\forall\, a, b, c \in G, \ \ a * (b * c) = (a * b) * c.$$

iii) Existe um elemento neutro

$$\forall\, a \in G, \ \exists\, e \in G \ \textit{tal que} \ \ a * e = e * a.$$

iv) Todo elemento possui um elemento inverso

$$\forall\, a \in A, \ \exists\, b \in G, \ \ \textit{tal que}\ a * b = b * a = e.$$

Um grupo $(G, *)$ é chamado de *grupo abeliano* ou comutativo se a operação $*$ for comutativa, ou seja,

$$\forall\, a, b \in G, \ \ a * b = b * a.$$

Os grupos abelianos receberam esse nome em honra ao matemático Niels Henrik Abel $(1802 - 1829)$. Para simplificar notações, escreveremos G em vez de $(G, *)$, para deno-

tar um grupo e utilizaremos ab no lugar de $a * b$.

Seja G um grupo e S um subconjunto não-vazio de G. É dito que S é um *subgrupo* de G quando o conjunto S é um grupo com a operação de G. A próxima proposição fornece as condições necessárias e suficientes para que S seja um subgrupo de G.

Proposição 1.1

Seja G um grupo e S um subconjunto de G. As seguintes condições são equivalentes:

(a) S é um subgrupo de G.

(b) (i) $e \in S$,

(ii) $\forall\, a, b \in S$, temos que $ab \in S$,

(iii) $\forall\, a \in S$, temos que $a^{-1} \in S$.

(c) $S \neq \varnothing$ e $\forall\, a, b \in S$, temos que $ab^{-1} \in S$.

Demonstração. Veja em [8], páginas 126 e 127. □

Seja α um elemento do grupo $(G, \cdot)$. O subgrupo gerado por a é o conjunto de todas as potências de expoente inteiro de a e denotamos por (a), isto é

$$(a) := \{a^n \,|\, n \in \mathbb{Z}\} = \{\ldots, a^{n-1}, a^{-1}, 0, a, a^2, a^{n+1}, \ldots\}.$$

Caso o grupo aditivo $(G, +)$ e $b \in G$, então b é o conjunto de todos os múltiplos de b

$$(b) := \{nb \,|\, n \in \mathbb{Z}\} = \{\ldots, -2b, -b, e, b, 2b, \ldots\}.$$

Um grupo é chamado *cíclico* se existir $g \in G$ tal que $(g) = G$. Então, todos os elementos de G são potências ou múltiplos de g, neste caso dizemos que g é *gerador* de G. Também podemos obter um *subgrupo cíclico*, note que o conjunto dos inteiros pares, $2\mathbb{Z} = \{2k \,|\, k \in \mathbb{Z}\}$, é um subgrupo de $(\mathbb{Z}, +)$, então $2\mathbb{Z}$ é um subgrupo cíclico de $\mathbb{Z}$ gerado pelo elemento 2. Porém, um grupo cíclico pode ter mais de um gerador. Por exemplo, o grupo $(\mathbb{Z}, +)$ é um grupo cíclico com os geradores ± 1, porque todo inteiro é múltiplo de ± 1.

Proposição 1.2

Todo subgrupo de um grupo cíclico é também cíclico.

Demonstração. Veja em [4], páginas 178 e 179. □

1.2 Anéis e Domínios

Neste trabalho iremos nos restringir aos *anéis comutativos com unidade.*

Definição 1.2: Anel Comutativo com Unidade

Um *anel* ou *anel comutativo* $(A, +, \cdot)$ é um conjunto A com pelo menos dois elementos, munido de duas operações denotadas por $+$ (adição) e por $\cdot$ (multiplicação) que satisfazem as seguintes propriedades:

i) Associatividade da adição

$$\forall\ a, b, c \in A,\ (a + b) + c = a + (b + c).$$

ii) Existe um elemento neutro em relação à adição

$$\exists\ 0 \in A, \text{ isto é, } \forall x \in A,\ 0 + a = a \quad \text{e} \quad a + 0 = a.$$

iii) Inverso aditivo

$$\forall\ a \in A, \exists\ (-a) \in A, \quad \text{tal que} \quad a + (-a) = 0 \quad \text{e} \quad (-a) + a = 0.$$

iv) Comutatividade da adição

$$\forall\ a, b \in A,\ a + b = b + a.$$

v) Associatividade da multiplicação

$$\forall\ a, b, c \in A,\ (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

vi) Existe um elemento neutro em relação à multiplicação

$$\exists\ 1 \in A, \text{ isto é, } \forall\ a \in A,\ 1 \cdot a = a \quad \text{e} \quad a \cdot 1 = a.$$

vii) Comutatividade da multiplicação

$$\forall\ a, b \in A,\ a \cdot b = b \cdot a.$$

viii) Adição é distributiva relativamente à multiplicação

$$\forall\ a, b, c \in A,\ a \cdot (b + c) = a \cdot b + a \cdot c.$$

Em um anel $(B, +, \cdot)$, diz-se *divisor de zero* um elemento não-nulo $a \in B$, se existe um elemento não-nulo $b \in B$ tal que $ab = 0$. Por exemplo, o anel $(\frac{\mathbb{Z}}{6\mathbb{Z}}, +, \cdot)$, possui elementos que são divisores de zero, pois $\bar{2} \neq 0$ e $\bar{3} \neq 0$, note que, $\bar{2} \cdot \bar{3} = \bar{0}$. Assim, o anel $\frac{\mathbb{Z}}{6\mathbb{Z}}$ possui divisores de zero.

Sejam A um anel e S um subconjunto não vazio de A. Suponhamos que S seja fechado para as operações de adição e multiplicação de A. Se S for um anel com as operações de A, é dito que S é um *subanel* de A.

Proposição 1.3

Um subconjunto não-vazio S de um anel A é um subanel de A se, e somente se, satisfazem as seguintes condições:

(i) $0_A \in S$;

(ii) $\forall\, a, b \in S \Rightarrow a - b = a + (-b) \in S$;

(iii) $\forall\, a, b \in S \Rightarrow ab \in S$.

Demonstração. Veja em [8], página 43. □

Vamos denotar por $S \leq A$ para indicar que S é um subanel de A. Segue alguns exemplos de subanéis, $\mathbb{Z} \leq \mathbb{Z}[\sqrt{p}] \leq \mathbb{Q}[\sqrt{p}] \leq \mathbb{R} \leq \mathbb{C}$, onde p é um número primo ≥ 2.

Definição 1.3: Domínio e Corpo

(a) Um anel $(D, +, \cdot)$ é chamado de *domínio* se o produto de quaisquer dois elementos não-nulos de D é um elemento não-nulo, ou seja, para todo $a, b \in D\backslash\{0\}$, temos que, $ab \neq 0$. O domínio também é conhecido como *domínio de integridade* ou *domínio integral*.

(b) Um anel $(C, +, \cdot)$ é chamado de *corpo* se todo elemento não-nulo de C é invertível, ou seja,

$$\forall\ a \in C \setminus \{0\},\ \exists\ b \in C,\ tal\ que,\ \ a \cdot b = 1.$$

Sejam F e K corpos com $F \subset K$. Dizemos que F é subcorpo de C se, e somente se, F é um corpo com as operações de K. Por exemplo, sendo $\mathbb{R}$ subcorpo de $\mathbb{C}$ e $\mathbb{Q}$ subcorpo de $\mathbb{R}$, isto implica que, $\mathbb{Q}$ subcorpo de $\mathbb{C}$.

Proposição 1.4

Sejam K um corpo e F um subconjunto não vazio de K. Para que F seja um subcorpo de K é necessário e suficiente que:

(i) $0, 1 \in F$;

(ii) Se $a, b \in F$, então $a - b \in F$;

(iii) Se $a, b \in F$, $b \neq 0$ então $ab^{-1} \in F$.

Demonstração. Veja em [4], páginas 225 e 226. □

Consideremos $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ um subconjunto de $\mathbb{R}$.

(i) $0 = 0 + 0\sqrt{2}$ e $1 = 1 + 0\sqrt{2} \Rightarrow 0, 1 \in \mathbb{Q}[\sqrt{2}]$;

(ii) Se $\alpha, \beta \in \mathbb{Q}[\sqrt{2}]$. Sendo $\alpha = (a + b\sqrt{2})$ e $\beta = (c + d\sqrt{2})$ com $a, b, c, d \in \mathbb{Q}$. Então,

$$\alpha - \beta = (a - c) + (b - d)\sqrt{2}.$$

Note que, tanto $(a - c)$ como $(b - d)$ pertencem ao corpo dos racionais. Portanto, concluímos que $\alpha - \beta \in \mathbb{Q}[\sqrt{2}]$;

(iii) Se $\alpha, \beta \in \mathbb{Q}[\sqrt{2}]$, $\beta \neq 0$. Sendo $\alpha = (a + b\sqrt{2})$ e $\beta = (c + d\sqrt{2})$ com $a, b, c, d \in \mathbb{Q}$ e c, d ambos não nulos. Logo, temos que:

$$\alpha\beta^{-1} = a + b\sqrt{2} \cdot \frac{1}{c + d\sqrt{2}} = \frac{(a + b\sqrt{2})(c - d\sqrt{2})}{(c + d\sqrt{2})(c - d\sqrt{2})} = \frac{ac - 2bd}{c^2 - 2d^2} + \frac{bc - ad}{c^2 - 2d^2}\sqrt{2}.$$

Segue que, $c^2 - 2d^2 \neq 0$, porque $\frac{c}{d} \neq \sqrt{2}$. Então, $\frac{ac-2bd}{c^2-2d^2}$, $\frac{bc-ad}{c^2-2d^2} \in \mathbb{Q}$. Portanto, $\alpha\beta^{-1} \in \mathbb{Q}[\sqrt{2}]$. Podemos concluir que $\mathbb{Q}[\sqrt{2}]$ é um subcorpo de $\mathbb{R}$.

Exemplo 1.1

Nos itens (a) e (b) são apresentados alguns corpos, enquanto no (c) são expostos anéis que não são corpos.

(a) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, são corpos.

(b) $(\mathbb{Z}_p, +, \cdot)$, é um corpo se, e somente se, p é primo.

(c) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}[i], +, \cdot)$, $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ são domínios.

Definição 1.4: Ideal

Seja um anel $(A, +, \cdot)$ e seja I um subconjunto não-vazio de A. Dizemos que I é um *ideal* de A se satisfazem as seguintes condições:

(a) $a - b \in I, \forall\, a, b \in I$.

(b) $xa \in I, \forall a \in I \ \ e \ \ \forall\, x \in A$.

Existem alguns casos especiais de ideais, segue alguns deles. São ditos *ideais triviais* de A, os ideais $J = \{0\}$ e $J = A$. Um ideal I é dito *ideal próprio* se este não contém a unidade de A. Por exemplo, o conjunto dos inteiros pares $2\mathbb{Z}$ é um ideal de $\mathbb{Z}$ que não contém a unidade de $\mathbb{Z}$. Portanto, $2\mathbb{Z}$ é um ideal próprio de $\mathbb{Z}$.

Definição 1.5: Ideais

Seja A um anel comutativo com unidade.

(a) Um ideal I em A é dito *ideal principal* se ele é gerado por um elemento em A, ou seja, $a \in A$ tal que $I = (a)$.

(b) Um ideal I em A é dito *finitamente gerado* se existem $n \in \mathbb{N}$ e $a_1, \ldots, a_n \in A$ tais que $I = (a_1, a_2, \ldots, a_n)$.

(c) Dizemos que P é um *ideal primo* se $P \subsetneqq A$ e, para quaisquer $a, b \in A$, $ab \in P \Rightarrow a \in P$ ou $b \in P$.

(d) Dizemos que M é um *ideal maximal* se $M \subsetneqq A$ e se os únicos ideais em A que contém M são os próprios A e M.

Segundo [4], os ideais foram definidos primeiramente por Richard Dedekind, sendo estes uma generalização do que Ernst Kummer chamou de números ideais. Desenvolvida mais tarde, pela Emmy Noether.

Definição 1.6: Domínio de Ideais Principais

Um domínio D é dito *domínio de ideais principais* se todo ideal em D é principal.

O anel dos inteiros possui a propriedade de todo ideal ser um ideal principal. Mais ainda, conheceremos um teorema na seção de anéis de polinômios, que fornece como resultado que

os anéis de polinômios com coeficientes em um corpo são domínios de ideais principais.

Definição 1.7

Um anel no qual todo ideal é finitamente gerado é dito *noetheriano*.

O termo Noetheriano é uma homenagem à matemática Emmy Noether, que contribuiu fortemente para a teoria dos anéis comutativos, esse anel será importante para nosso estudo, pois satisfazem a condição de cadeia ascendente para ideais.

Seja $\mathfrak{N}$ um anel e considere $\{I_i\}_{i\in\mathbb{N}}$ uma família de ideais para $\mathfrak{N}$. Dada uma cadeia ascendente de ideais de um anel

$$I_1 \subseteq I_2 \subseteq I_3 \cdots I_x \subseteq I_{x+1} \subseteq \ldots$$

dizemos que a cadeia acima é estacionária se existe $x \in \mathbb{N}$ tal que $I_y = I_x$ para $y \geq x$.

Teorema 1.1

Seja um anel $\mathfrak{N}$. Então $\mathfrak{N}$ é dito noetheriano se, e somente se, toda cadeia ascendente de ideais de $\mathfrak{N}$ é estacionária.

Demonstração. Veja em [7], página 36. □

Por exemplo, temos que $\mathbb{Z}$ e qualquer corpo K, são exemplos de anéis noetherianos.

Proposição 1.5

Seja $\mathfrak{N} \to \mathfrak{M}$ um homomorfismo sobrejetor de anéis. Se $\mathfrak{N}$ é noetheriano, então $\mathfrak{M}$ também é noetheriano.

Demonstração. Veja em [1], página 87. □

Proposição 1.6

Seja $\mathfrak{N}$ um anel noetheriano e I um ideal de A. Então I contém um produto finito de ideais primos.

Demonstração. Veja em [1], páginas 90 e 91. □

Definição 1.8: Domínio Euclidiano

Um *domínio euclidiano* $(D, +, \cdot, \phi)$ é um domínio D com uma função

$$\phi : D\backslash\{0\} \to \mathbb{N}$$

que satisfazem as seguintes propriedades:

(i) $\forall\, a, b \in D, b \neq 0$, existem $q, r \in D$ tais que $a = bq + r$ com $r = 0$ ou $\phi(r) < \phi(b)$.

(ii) $\forall\, a, b \in D$ temos que $\phi(a) \leq \phi(ab)$.

No capítulo 3, apresentaremos alguns exemplos de domínios que não são euclidianos.

Teorema 1.2

Todo domínio euclidiano é um domínio de ideais principais.

Demonstração. Veja em [17], página 92. □

Vejamos alguns domínios euclidianos com suas respectivas aplicações.

(i) O anel dos inteiros com a função valor absoluto é um domínio euclidiano.

$$\begin{aligned} \phi : \ \mathbb{Z}\backslash\{0\} &\to \mathbb{N} \\ \phi(n) &\mapsto |n|. \end{aligned}$$

(ii) O anel dos inteiros Gaussianos $\mathbb{Z}[i] = \{a + bi \,|\, a, b \in \mathbb{Z}\}$ é um domínio euclidiano com a função norma. (Conheceremos a norma com mais detalhes na seção de normas e traços).

$$\begin{aligned} \mathcal{N} : \ \mathbb{Z}\backslash\{0\} &\to \mathbb{N} \\ \mathcal{N}(a + bi) &\mapsto a^2 + b^2. \end{aligned}$$

(iii) Seja K um corpo, o anel de polinômios numa variável sobre K é representado por $K[x]$ é um domínio euclidiano com a função grau.

$$\begin{aligned} \delta : \ K[x]\backslash\{0\} &\to \mathbb{N} \\ \delta(f(x)) &\mapsto \partial(f(x)). \end{aligned}$$

Definição 1.9

(a) Seja $a \in A$. Um elemento $b \in A$ é dito divisor de a em A se existe $c \in A$ tal que $a = bc$. É dito que a é múltiplo de b, ou que b divide a, e denotamos $b \,|\, a$.

(b) Um elemento $a \in A$ é dito invertível em A se existe $b \in A$ tal que $ab = 1$. Vamos denotar o conjunto dos elementos invertíveis por A^*.

(c) Dois elementos $a, b \in A$ são associados em A se existe $u \in A$, u invertível em A, tal que $a = ub$.

(d) Um elemento não-invertível $a \in A\backslash\{0\}$ é irredutível em A se a possui apenas fatorações triviais em D, ou seja, $\forall\, a, b \in A$ tais que $a = bc \Rightarrow b$ ou c é invertível em A. Vale ressaltar que os únicos divisores de um elemento irredutível a são os elementos associados de a em A e os elementos invertíveis.

(e) Um elemento não-invertível $p \in A$ é chamado primo se para quaisquer $a, b \in A$,

$$p|ab \;\Rightarrow\; p|a \;\; ou \;\; p|b.$$

Por exemplo, os invertíveis de $\mathbb{Z}$ são $\{\pm 1\}$ e seus elementos irredutíveis são $\{\pm p\}$ tal que p é um número primo, enquanto os invertíveis de $\mathbb{Z}[i]$ são $\{\pm 1, \pm i\}$ e seus elementos irredutíveis são determinados pela norma que será definida na seção normas e traços.

Definição 1.10: Domínio de fatoração única

Seja D um domínio. É dito *domínio de fatoração única* ou *domínio fatorial* se todo elemento não-nulo e não-invertível de D pode ser escrito unicamente como produto de elementos irredutíveis de D, em outras palavras:

(a) Todo elemento não-nulo e não-invertível de D é produto finito de fatores irredutíveis.

(b) Se $\{p_m\}_{1 \leq m \leq x}$ e $\{q_n\}_{1 \leq n \leq y}$ são famílias finitas de elementos irredutíveis de D tais que $p_1 \dots p_x = p_1 \dots p_y$, então, $x = y$ e a menos de ordenação, temos uma bijeção σ de $\{1, \dots, x\}$ sobre $\{1, \dots, x\}$ tal que p_m é associado a $q_{\sigma(m)}, \forall\, m = (1, \dots, x)$.

Todo corpo K é um domínio fatorial.

Exemplo 1.2

(a) $\mathbb{Z}$, $\mathbb{Z}[i]$ são domínios fatoriais.

(b) $\mathbb{Z}[\sqrt{-3}]$, $\mathbb{Z}[\sqrt{-11}]$ não são domínios fatoriais.

Os contraexemplos do item (b) são demonstrados nas páginas 65 e 66.

Proposição 1.7

Seja D um domínio. Então são equivalentes:

(a) D é um domínio fatorial.

(b) Todo elemento irredutível de D é primo.

Demonstração. Veja em [7], página 35. □

Teorema 1.3

Seja um anel $\mathfrak{N}$. então

(a) Se $\mathfrak{N}$ é domínio noetheriano, então todo elemento não-invertível de $\mathfrak{N}\backslash\{0\}$ é escrito como produto finito de irredutíveis.

(b) $\mathfrak{N}$ é domínio principal se, e somente se, $\mathfrak{N}$ é um domínio fatorial com a seguinte propriedade:

$$\forall\, a, b \in \mathfrak{N}\backslash\{0\}, \exists\, c, d \in \mathfrak{N} \; tais\, que \; MDC\,\{a, b\} = ac + bd.$$

Demonstração. Veja em [7], páginas 36 até 38. □

Observamos anteriormente que $\mathbb{Z}[i]$ com a função norma é um domínio euclidiano, e agora foi dado o exemplo que ele também é domínio fatorial, é natural questionarmos se, todo domínio euclidiano é um domínio de fatoração única.

Teorema 1.4

Todo domínio de ideais principais é um domínio de fatoração única.

Demonstração. Veja em [17], página 92 e 93. □

Teorema 1.5

Todo domínio euclidiano é um domínio de fatoração única.

Demonstração. Pelo teorema 1.2 temos que todo domínio euclidiano é um domínio de ideais principais e pelo teorema 1.4 todo domínio de ideais principais é um domínio de fatoração única. Portanto, todo domínio euclidiano é um domínio de fatoração única. □

Domínio Euclidiano $\subseteq$ Domínio de ideais principais $\subseteq$ Domínio de fatoração única.

Nesta seção, vimos que um domínio euclidiano também é um domínio de ideais principais que, por sua vez, é um domínio de fatoração única. Porém, a recíproca não é verdadeira, um domínio de fatoração única não necessariamente é um domínio de ideais principais.

1.3 Anéis de Polinômios

Seja A um anel, vamos denotar por $A[x]$ e chamá-lo de *anel de polinômios* numa variável sobre A. Um polinômio $p(x)$ com coeficientes em A é expresso da seguinte forma

$$p(x) = a_0 + a_1x + \cdots + a_nx^n = \sum_j^n a_jx^j,$$

para $n \in \mathbb{N} \cup \{0\}$, $a_j \in A$, para $0 \leq j \leq n$. O coeficiente a_0 chamamos de *termo constante.* Denotamos por $A[x]$ o conjunto de todos os polinômios com coeficientes em A.

$$A[x] = \{a_0 + a_1x + \cdots + a_nx^n = \sum_j^n a_jx^j \,|\, a_j \in A,\, 0 \leq j \leq n, n \in \mathbb{N}\}.$$

Denotamos como, $p(x) = 0$ um *polinômio nulo* e $p(x) = a_0$ sendo um *polinômio constante.* Se $p(x) \neq 0$, então existe algum coeficiente diferente de zero, logo, há um maior índice n tal que $a_n \neq 0$. Definimos o *grau* de $p(x)$ por n e o denotamos por $\partial(p(x))$. O coeficiente líder de $p(x)$ é denotado por a_n. Os polinômios de grau n com coeficiente líder $a_n = 1$ são chamados de *polinômios mônicos* e não definimos o grau do polinômio nulo. No conjunto $A[x]$ está definido as operações de adição e multiplicação de polinômios, a cerca das operações de A. A definição de adição de polinômios $f(x) = \sum_{j=0}^n a_jx^j$ e $p(x) = \sum_{j=0}^n b_jx^j$ em $A[x]$ como segue

$$f(x) + p(x) = \sum_{j=0}^n c_jx^j,$$

onde $c_j = a_j + b_j$, para $0 \leq j \leq n$.

A definição de multiplicação de polinômios

$$f(x) = \sum_{j=0}^{n} a_j x^j \qquad e \qquad p(x) = \sum_{j=0}^{m} b_j x^j$$

em $A[x]$ é dado por

$$f(x) \cdot p(x) = \sum_{j=0}^{n+m} c_j x^j,$$

onde

$$\begin{aligned} c_0 &= a_0 \cdot b_0 \\ c_1 &= a_0 \cdot b_1 + a_1 \cdot b_0 \\ &\vdots \\ c_j &= a_0 \cdot b_j + a_1 \cdot b_{j-1} + \cdots + a_j \cdot b_0 \\ &\vdots \\ c_{n+m} &= c_n \cdot c_m. \end{aligned}$$

Por exemplo, sejam $f(x) = 2x^2 + x + 1$, $g(x) = x - 1$ em $\mathbb{Z}[x]$. Então,

$$f(x) + g(x) = (2+0)x^2 + (1+1)x + (1-1) = 2x^2 + 2x.$$

Vamos calcular $f(x) \cdot g(x)$. Usando a propriedade distributiva de polinômios, temos

$$\begin{aligned} f(x) \cdot g(x) &= (2x^2 + x + 1) \cdot (x - 1) \\ &= 2x^2 \cdot (x-1) + x \cdot (x-1) + 1 \cdot (x-1) \\ &= (2x^3 - 2x^2) + (x^2 - x) + (x - 1) \\ &= 2x^3 + (-2+1)x^2 + (-1+1)x + (-1) \\ &= 2x^3 - x^2 - 1. \end{aligned}$$

O resultado da adição de dois polinômios é chamado de *soma*, e da multiplicação de *produto*.

Se $f(x)$ e $p(x)$ são polinômios não-nulos, então $f(x) \cdot p(x)$ em $A[x]$ é não-nulo, segue que, $A[x]$ é um domínio. Além do mais, possui a propriedade multiplicativa do grau.

$$\partial(f(x) \cdot p(x)) = \partial(f(x)) + \partial(p(x))$$

Observação: Caso A não seja um domínio, se um dos coeficientes líderes de $f(x)$ ou $p(x)$ for invertível, então a propriedade multiplicativa do grau continua valendo. O próximo resultado surge como consequência da propriedade multiplicativa do grau.

Proposição 1.8

Sejam $f(x), p(x) \in A[x]\backslash\{0\}$. Se $p(x)$ tem coeficiente líder invertível e divide $f(x)$, então $\partial(p(x)) \leq \partial(f(x))$.

Demonstração. Ver em [10], páginas 112. □

Teorema 1.6: Teorema de Gauss

Seja D um domínio fatorial. Então $D[x]$ é um domínio fatorial.

Demonstração. Veja em [7], páginas 48 e 49. □

Por exemplo, $\mathbb{Z}[x]$ é um domínio fatorial, (porém não é domínio de ideais principais). Entretanto, se K é um corpo, então o anel de polinômios com coeficientes em K é um domínio euclidiano, que por sua vez, é um domínio de ideais principais, segundo a seção anterior. Um método prático para dividir polinômios é utilizando a *divisão euclidiana,* que é semelhante ao algoritmo de Euclides utilizado na divisão de números inteiros. Vamos chamar $f(x)$ de dividendo, $p(x)$ de divisor, $q(x)$ de quociente e $r(x)$ de resto.

Proposição 1.9: Divisão Euclidiana

Sejam $f(x), p(x) \in A[x]$, com $p(x) \neq 0$ e coeficiente líder invertível em A. Então, existem $q(x), r(x) \in A[x]$, unicamente determinados, tais que

$$f(x) = p(x)q(x) + r(x)$$

onde $r(x) = 0$ ou $\partial(r(x)) < \partial(p(x))$.

Demonstração. Ver em [10], páginas 113 e 114. □

Mais resultados e exemplos envolvendo a divisão euclidiana em $A[x]$, são encontrados na seção 3.5 e 3.6 do livro [10]. Também apresenta um método eficiente para determinar o quociente e o resto da divisão euclidiana em $A[x]$ utilizando o *algoritmo de Briot-Ruffini.*

Seja $f(x)$ um polinômio sobre o anel A. Um elemento $\alpha \in A$ é chamado *raiz* de $f(x)$ se $f(\alpha) = 0$. Tendo como exemplo, o polinômio $f(x) = x^2 + 1$ tal que $f(x) \in \mathbb{C}[x]$, os números complexos i e $-i$ são raízes do polinômio $f(x)$, pois $f(i) = f(-i) = 0$.

Proposição 1.10: Teste da raiz

Seja $f(x)$ em $A[x]\backslash\{0\}$. Então, $\alpha \in A$ é uma raiz de $f(x)$ se, e somente se, $x - \alpha$ divide $f(x)$.

Demonstração. Ver em [10], páginas 118. □

Proposição 1.11

Seja A um domínio e $f(x)$ um polinômio em $A[x]\backslash\{0\}$. Se $f(x)$ tem grau n, então $f(x)$ tem no máximo n raízes em A.

Demonstração. Ver em [10], página 130. □

Seja $\alpha \in A[x]$ é uma raiz de $f(x) \in A[x]$. Dizemos que α é uma *raiz de multiplicidade* m quando $(x - \alpha)^m$ divide $f(x)$ mas $(x - \alpha)^{m+1}$ não divide $f(x)$ em $A[x]$. Então, existe $q(x) \in A[x]$ tal que

$$f(x) = (x - \alpha)^m q(x),$$

com $q(\alpha) \neq 0$, ou seja, significa que α não é raiz de $q(x)$ e garante que a multiplicidade da raiz α não é maior que m.

Seja K um subcorpo de $\mathbb{C}$, tal que $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$. A derivada de $f(x)$ é o polinômio definido da seguinte maneira

$$f'(x) = D(f(x)) = \sum_{j=1}^{n} j a_j x^{j-1} = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}.$$

Sendo $f' = f^{(1)}$, definimos as derivadas sucessivas por

$$f^{(j+1)}(x) = D(f^{(j)}(x)),$$

para cada $j \in \mathbb{N}$.

Sejam K um corpo e $f(x) \in K[x]\backslash\{0\}$. É dito que $f(x)$ é um *polinômio irredutível* em $K[x]$ se $f(x) = p(x) \cdot h(x)$, com $p(x), h(x) \in K[x]$, então $f(x)$ ou $p(x)$ é um polinômio

constante não-nulo. Quando não, dizemos que o polinômio $f(x)$ é *redutível* em $K[x]$, se e somente se, existirem polinômios $p(x)$ e $h(x)$ em $K[x]$ tais que $f(x) = p(x) \cdot h(x)$, com $0 < \partial(p(x)) < \partial(f(x))$ e $0 < \partial(h(x)) < \partial(f(x))$.

Exemplo 1.3

Observe que $x^2 - 2$ não é irredutível em $\mathbb{R}[x]$, pois $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ em $\mathbb{R}[x]$. Porém, $x^2 - 2$ é irredutível em $\mathbb{Q}[x]$, visto que não tem raiz em $\mathbb{Q}$.

Geralmente, quando temos polinômios com coeficientes inteiros, consideramos a fatoração de polinômios sobre $\mathbb{Q}$. Dessa forma, conseguimos estabelecer uma condição para soluções racionais.

Lema 1.1: Lema de Gauss

Seja $f(x) \in \mathbb{Z}[x]$ e suponha que $f(x) = p(x)q(x)$, onde $p(x), q(x) \in \mathbb{Q}[x]$. Então existe $\tau \in \mathbb{Q}^*$, tal que $\tau p, \tau^{-1} q \in \mathbb{Z}[x]$.

Demonstração. Ver [17], páginas 19 e 20. □

Então, podemos associar todo polinômio com coeficientes racionais em um polinômio com coeficientes inteiros, basta multiplicarmos pelo mínimo múltiplo comum dos denominadores. O próximo teorema permite que obtemos uma condição suficiente para que um polinômio com coeficientes inteiros seja irredutível em $\mathbb{Q}[x]$.

Teorema 1.7: Critério de Eisenstein

Seja $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ um polinômio em $\mathbb{Z}[x]$. Suponha que exista um número primo p tal que $p \nmid a_n$, $p | a_0, \cdots, p | a_{n-1}$ e $p^2 \nmid a_0$. Então, $f(x)$ é irredutível em $\mathbb{Q}[x]$.

Demonstração. Ver [17], páginas 20 e 21. □

Exemplo 1.4

Seja o polinômio $f(x) = 8x^3 + 28x^2 + 49x + 77 \in \mathbb{Z}[x]$ é irredutível em $\mathbb{Q}[x]$, uma vez que, se $p = 7$, temos, $7 \nmid 8$, $7|28$, $7|49$, $7|77$ *e* $7^2 \nmid 77$.

1.4 Espaços Vetoriais

O objetivo principal desta seção é introduzir o conceito de *espaço vetorial*. Além deste, outros objetos de estudos da Álgebra Linear vão ser abordados no intuito de consolidar uma base necessária para compreender algumas definições do próximo capítulo. Elementos de um espaço qualquer são chamados de *vetores* e os elementos do corpo de *escalares*.

Definição 1.11: Espaço vetorial

Um conjunto não vazio V é um espaço vetorial sobre um corpo K, munido de duas operações

$$\begin{array}{rcl} + : V \times V & \to & V \\ (a,b) & \mapsto & a+b \end{array} \qquad e \qquad \begin{array}{rcl} \cdot : K \times V & \to & V \\ (\alpha,a) & \mapsto & \alpha a \end{array}$$

chamadas de adição e multiplicação por escalar que satisfazem as seguintes condições:

1) para quaisquer $a, b, c \in V$, existe a adição, com as seguintes propriedades:

   (i) $a + b = b + a$ (comutatividade);

   (ii) $a + (b + c) = (a + b) + c$ (associatividade);

   (iii) $\exists\, 0 \in V$ tal que $a + 0 = a$ (existência do elemento neutro);

   (iv) $\exists\, (-a) \in V$ tal que $a + (-a) = 0$ (existência do elemento oposto).

2) para quaisquer $a, b \in V$ e $\alpha, \beta \in K$, existe a multiplicação, com as seguintes propriedades:

   (i) $1a = a$ (existência do elemento neutro);

   (ii) $\alpha(\beta a) = (\alpha\beta)a$ (associatividade);

   (iii) $a(\alpha + \beta) = a\alpha + a\beta$ (distributividade do vetor em relação aos escalares);

   (iv) $\alpha(a + b) = \alpha a + \alpha b$ (distributividade do escalar em relação aos vetores).

É habitual na Álgebra Linear, a terminologia espaço vetorial também ser chamada de *espaço linear*. O corpo $\mathbb{C}$ é um espaço vetorial sobre $\mathbb{Q}$ com as operações de adição e multiplicação de $\mathbb{C}$, entretanto, $\mathbb{Q}$ não é um espaço vetorial sobre $\mathbb{C}$. Todo corpo K é um

espaço vetorial sobre o próprio corpo K com as operações usuais de adição e multiplicação de K. Portanto, $\mathbb{C}$ é um espaço vetorial sobre $\mathbb{C}$.

Definição 1.12: Subespaço vetorial

Seja um espaço vetorial V sobre um corpo K. Um subespaço vetorial (ou subespaço) de V é um subconjunto $S \subset V$ com as seguintes propriedades:

(i) $0 \in S$;

(ii) $\forall\, a, b \in V$, $a + b \in S$;

(iii) $\forall\, \alpha \in K$ e $\forall\, a \in V$, $\alpha a \in S$.

Se S é um subespaço vetorial de V, então S também é um espaço vetorial sobre K. Por exemplo, se $\mathbb{C}$ é um espaço vetorial sobre $\mathbb{Q}$, então $\mathbb{R}$ é um subespaço vetorial de $\mathbb{C}$. Inclusive, $\mathbb{R}$ é um espaço vetorial sobre $\mathbb{Q}$.

Definição 1.13

Sejam um espaço vetorial V sobre um corpo K, e $S = \{x_1, \ldots, x_n\}$ um subconjunto finito de V. O subconjunto X de todos os elementos $x \in V$ que podem ser escritos como combinação linear dos elementos de S é um subespaço vetorial denominado *Subespaço gerado* por S.

$$X = \{x = \alpha_1 x_1, \ldots, \alpha_n x_n \,|\, \alpha_i \in K, x \in V\}.$$

Dizemos que S é um *conjunto de geradores* para X, e que S gera o subespaço de X.

Seja um espaço vetorial V sobre o corpo K. Dizemos que um conjunto $L = \{a_1, \ldots, a_n\} \subset V$ é *linearmente independente* (abreviadamente, L.I) se, e somente, se a combinação linear

$$\alpha_1 a_1, \ldots, \alpha_n a_n = 0 \tag{1.1}$$

com $\alpha_i \in K$, somente for possível quando $\alpha_1 = \ldots = \alpha_n = 0$. Caso contrário, se L não é L.I, isto é, for possível uma igualdade do tipo (1.1) sem que os escalares α_i sejam todos iguais a zero. Então, L é dito linearmente dependente (abreviadamente, L.D). Uma *base* de um espaço vetorial V é um conjunto finito $B \subset V$ linearmente independente que gera V. A *dimensão* de um espaço vetorial V é o número de vetores de qualquer uma das bases para

V e denotamos por $dim\,(V)$. Dizemos que um espaço vetorial é de *dimensão finita* se existe uma base finita para V, quando não, é dito que a dimensão de V é infinita.

Proposição 1.12

Todo espaço finitamente gerado admite uma base

Demonstração. Veja em [2], página 77 e 78. □

Se V é um espaço finitamente gerado, então V é um espaço de dimensão finita. Por exemplo, $B = \{(1,0,0),(0,1,0),(0,0,1)\}$ é uma base para o espaço $\mathbb{R}^3$, conhecida como *base canônica* de $\mathbb{R}^3$ com $dim\,(\mathbb{R}^3) = 3$.

Corolário 1.1

Se o espaço vetorial V admite uma base $B = \{b_1, \ldots, b_n\}$ com n elementos, qualquer outra base de V também possui n elementos.

Demonstração. Veja em [12], página 29. □

Teorema 1.8

Seja V um espaço vetorial de dimensão finita n. Então:

a) Todo conjunto X de geradores de V contém uma base.

b) Todo conjunto linearmente independente $\{a_1, \ldots, a_n\} \subset V$ está contido numa base.

c) Todo subespaço vetorial $S \subset V$ tem dimensão finita, a qual é menor ou igual a n.

d) Se a dimensão do subespaço $S \subset V$ é igual a n, então $S = V$.

Demonstração. Veja em [12], página 30. □

Definição 1.14: Transformação linear

Sejam V e W espaços vetoriais sobre um corpo K. Uma função $T : V \to W$ é uma *transformação linear* se as seguintes condições são satisfeitas:

(i) $\forall\, u, v \in V,\ T(u+v) = T(u) + T(v)$;

(ii) $\alpha \in K$ e $\forall\, u \in V,\ T(\alpha u) = \alpha T(u)$.

Uma transformação linear é uma função que preserva as operações dos espaços vetoriais. Caso, $V = W$, uma transformação linear $T : V \to V$, dizemos que T é um *operador linear* sobre V. Os exemplos mais simples de transformações lineares são, a função nula $0 : V \to W$, definida por $0 \cdot v = 0$ e a função identidade $Id : V \to V$, definida por $Id(v) = v$, para $v \in V$, sendo esta última um operador linear, conhecido como *operador identidade*.

Teorema 1.9

Sejam V e W espaços vetoriais sobre um corpo K. Se $B = \{b_1, \ldots, b_n\}$ for uma base de V e se o conjunto $\{v_1, \ldots, v_n\} \subseteq W$, então existe uma única transformação linear $T : V \to W$ tal que $T(b_i) = v_i$, para cada $i = 1, \ldots, n$.

Demonstração. Veja em [3], página 82. □

Teorema 1.10: Teorema do Núcleo e da Imagem

Sejam V e W espaços vetoriais de dimensão finita sobre um corpo K e $T : V \to V$ uma transformação linear, então

$$dim(V) = dim(Ker(T)) + dim(Im(T))$$

Demonstração. Veja em [3], página 87 e 88. □

Na página 85, da referência [3], é provado que o $Ker(T)$ é um subespaço vetorial de V e a $Im(T)$ é um subespaço vetorial de W. Se assumirmos que V tem dimensão finita, podemos definir o *posto* de T sendo a dimensão da $Im(T)$.

Chamamos de *matriz* um conjunto de números complexos, organizados em linhas e colunas, seguindo uma estrutura disposta em tabela, respeitando certa ordem. Representamos a matriz M com (m linhas e n colunas) por $M_{m\times n}$. Denotaremos o conjunto das matrizes de ordem $m \times n$ com entradas em R por $M_{m\times n}(R)$. Cada elemento $(a_{ij}) \in M_{m\times n}$ onde os índices indicam a posição da $i-$ésima linha e $j-$ésima coluna à qual pertence o elemento. Caso $m = n$, chamamos a matriz $M_{n\times n}$ de matriz quadrada de ordem n.

Se A é uma matriz quadrada de ordem 2, dada por

$$A_{2\times 2} = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

O *determinante* de uma matriz é um número real associado a matriz quadrada. Indicado por

$$det(A) = a_{11}a_{22} - a_{12}a_{21}.$$

Portanto, para calcular o determinante de uma matriz 2×2, basta efetuar o produto da diagonal principal e subtrair este resultado do produto da diagonal secundária. Por exemplo, a matriz de ordem 2.

$$M_{2\times 2} = \begin{bmatrix} 4 & -5 \\ 2 & -2 \end{bmatrix}$$

seu determinante é dado por

$$det(M) = 4 \cdot (-2) - (-5) \cdot 2 = 2.$$

De maneira geral, dada uma matriz de ordem $n \times n$ representada por

$$A_{n\times n} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & \cdots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \cdots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \cdots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & a_{n3} & \cdots & a_{nn} \end{bmatrix}.$$

Podemos calcular o determinante utilizando determinantes de matrizes de ordem $n-1$, ou seja, a partir dos determinantes de ordem 2, conseguimos calcular os de ordem 3 e com os de ordem 3 calcular os de ordem 4, e assim sucessivamente.

Definição 1.15

Seja A uma matriz $n \times n$. A matriz M_{ij} é a submatriz $(n-1) \times (n-1)$ obtida pela eliminação da i-ésima linha e da j-ésima coluna de A. O determinante de M_{ij} recebe o nome de *determinante menor* do elemento a_{ij} ou, mais resumidamente, *menor de* a_{ij}. O cofator A_{ij} de a_{ij} é definido por

$$A_{ij} = (-1)^{i+j} det(M_{ij}).$$

Intuitivamente, o determinante de uma matriz $n \times n$, é o escalar definido recursivamente por

$$det(A) = \begin{cases} a_{11}, & se \quad n = 1, \\ a_{11}A_{11} + \cdots + a_{1n}A_{1n}, & se \quad n > 1, \end{cases}$$

sendo A_{1j} o cofator de a_{1j}, para $j = 1, \ldots, n$.

1.5 Extensões de Corpos

Nesta seção apresentaremos algumas noções de *extensões de corpos* e alguns resultados importantes e necessários como o teorema da torre que terá grande aplicação para compreendermos as extensões algébricas.

Definição 1.16: Extensão de Corpos

Uma extensão de corpos é uma inclusão $K \subset F$ de um subcorpo K de um corpo F.

Notação: Dizemos que F é uma extensão de K e denotamos por $F \,|\, K$.
Usaremos a expressão K-*espaço vetorial* para indicar um espaço vetorial sobre K. Então, F pode ser visto como um K-espaço vetorial. Pois, K é um corpo, logo, a adição em K é comutativa, associativa, possui o elemento neutro e todo elemento possui simétrico. Além disso, se $a, b \in F$ e $c, d \in K$, temos que:

(i) $(a+b)c = ac + bc$,

(ii) $(c+d)a = ac + ad$,

(iii) $a(bc) = (ab)c$,

(iv) $1c = c$.

Exemplo 1.5

Vejamos alguns exemplos de extensões de corpos:

(a) $\mathbb{C} \,|\, \mathbb{R}$, $\mathbb{R} \,|\, \mathbb{Q}$, $\mathbb{C} \,|\, \mathbb{Q}$.

Definição 1.17: Extensão finita

A dimensão do espaço vetorial F sobre K será chamada de *grau da extensão* e será denotada por

$$[F : K] = dim_K F.$$

Uma extensão $F \,|\, K$ será dita *finita*, se F como espaço vetorial sobre K for finito, isto é, se

$$[F : K] = n < \infty.$$

A próxima definição é importante para obtermos corpos intermediários em uma extensão entre os corpos K e F.

Definição 1.18: Adjunção

Dada uma extensão $F \,|\, K$ e um elemento $\alpha \in F$. Definimos a adjunção de α a K como sendo o menor subcorpo de F contendo $K \cup \{\alpha\}$ e o denotamos por $K(\alpha)$. Portanto, $\alpha \in K(\alpha)$ e $K \subset K(\alpha) \subset F$.

Essa definição permite construirmos corpos intermediários $\mathbb{Q}(\alpha)$ tais que $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{C}$. Se adjuntarmos a unidade imaginária ao corpo dos racionais, obtemos o corpo dos números Gaussianos $\mathbb{Q}(i) = \{a + bi \,|\, a, b \in \mathbb{Q}\}$ que é o menor subcorpo de $\mathbb{C}$ contendo $\mathbb{Q} \cup \{\sqrt{i}\}$.

Exemplo 1.6

Vamos expor dois exemplos distintos, uma com dimensão finita e outro com dimensão infinita.

(a) Seja $F = \{a + bi \,|\, a, b \in \mathbb{Q}\}$. Temos que, a extensão $F \,|\, \mathbb{Q}$ é finita, pois F é um espaço vetorial sobre $\mathbb{Q}$ gerado por 1 e i.

(b) Seja α uma indeterminada sobre $\mathbb{Q}$. Então, a extensão $\mathbb{Q}(\alpha) \,|\, \mathbb{Q}$ não é finita, pois $\{1, \alpha, \alpha^2, \dots\}$ é linearmente independente sobre $\mathbb{Q}$.

Definição 1.19

Seja uma extensão $F \,|\, K$ e um elemento $\alpha \in F$. Dizemos que α é algébrico sobre um corpo F, se α é raiz de um polinômio não-nulo em $K[x]$.

Caso α não seja algébrico sobre K, então dizemos que α é transcendente sobre K. Por exemplo, a extensão $\mathbb{R} \,|\, \mathbb{Q}$ não é algébrica, pois π é transcendente sobre $\mathbb{Q}$.

Definição 1.20: Polinômio mínimo

Dada uma extensão $F \,|\, K$ e um elemento $\alpha \in F$ algébrico sobre K, definimos o polinômio mínimo de α sobre K, como o polinômio mônico de menor grau com coeficientes em K que satisfaz $p(\alpha) = 0$.

Teorema 1.11

Sejam os corpos K e F. Dada uma extensão $F \mid K$ e um elemento $\alpha \in F$. Seja $p(x)$ um polinômio mônico com coeficientes em K, tal que $p(\alpha) = 0$. Temos que as seguintes condições são equivalentes:

(a) $p(x)$ é o polinômio mínimo de α;

(b) Se $q(x) \in K[x]$ tal que $q(\alpha) = 0$, então $p(x)$ divide $q(x)$;

(c) $p(x)$ é irredutível.

Demonstração. Veja em [10], páginas 216 e 217. □

Teorema 1.12

Dada uma extensão $F \mid K$ e um elemento $\alpha \in F$ algébrico sobre K. Se n é o grau do polinômio mínimo de α sobre K, então $[K(\alpha) : K] = n$ e $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ é uma base de $K(\alpha)$ sobre K.

Demonstração. Veja em [10], páginas 217 e 218. □

Exemplo 1.7

Temos que, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$ e $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$. Os números $\sqrt{2}$ e $\sqrt[4]{2}$ são algébricos sobre $\mathbb{Q}$, com polinômios mínimos $x^2 - 2$ e $x^4 - 2$.

O próximo teorema nos permite calcular o grau de uma extensão mais complicada se conhecermos os graus de algumas outras extensões mais simples.

Teorema 1.13: Teorema da torre

Sejam K, L, F subcorpos de $\mathbb{C}$, tais que $K \subseteq L \subseteq F$ e $[F : K]$ é finita. Então, $[F : K] = [F : L][L : K]$.

Demonstração. Veja em [10], páginas 218 e 219. □

Se $[F : L] = \infty$ ou $[L : K] = \infty$, então $[F : K] = \infty$. Além disto, se $[F : K] = \infty$, então $[F : L] = \infty$ ou $[L : K] = \infty$. Note que, $[F : K] = 1$ se, e somente se, $F = K$.

Definição 1.21: Extensão algébrica

Uma extensão $F \mid K$ é algébrica, se todo $\alpha \in F$ é algébrico sobre K.

As extensões algébricas finitamente geradas são espaços vetoriais de dimensão finita. A noção de extensão algébrica é transitiva, ou seja, $K \subseteq L \subseteq F$

Teorema 1.14

Toda extensão finita é algébrica.

Demonstração. Veja em [10], páginas 222. □

Exemplo 1.8

Vamos verificar se a extensão $\mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}$ é algébrica.
O anel é definido como $\mathbb{Q}(\sqrt{2}) = \{a + b\,(\sqrt{2}) \mid a, b \in \mathbb{Q}\}$, seja $\alpha \in \mathbb{Q}(\sqrt{2})$. Então,

$$\alpha = a + b\,(\sqrt{2}) \Rightarrow (\alpha - a)^2 = (b\,(\sqrt{2}))^2 \Rightarrow \alpha^2 - 2a\alpha + a^2 - 2b^2 = 0.$$

Daí, α é raiz do polinômio $p(x) = x^2 - 2xa + a^2 - 2b^2 \in \mathbb{Q}[x]$, concluímos que α é algébrico sobre $\mathbb{Q}$. Portanto, $\mathbb{Q}(\sqrt{2}) \mid \mathbb{Q}$ é algébrica.

Corolário 1.2

Seja $F \mid K$ uma extensão finita. Então, existem $\alpha_1, \ldots, \alpha_n$ em F algébricos sobre K, tais que $F = K(\alpha_1, \ldots, \alpha_n)$.

Demonstração. Veja em [10], páginas 222. □

Teorema 1.15

Se $F|K$ é um corpo de extensão e $\alpha \in F$. Então, α é algébrico sobre K se, e somente se, $K(\alpha)$ é uma extensão finita de K. Neste caso, $[K(\alpha) : K] = \partial(p(x))$ onde $p(x)$ é o polinômio mínimo de α sobre K e $K(\alpha) = K[\alpha]$.

Demonstração. Veja [17], páginas 23 e 24. □

As extensões algébricas finitamente geradas possuem a estrutura algébrica que são espaços vetoriais de dimensão finita. Adiante, vai interessar para nosso estudo as extensões algébricas de grau 2.

1.6 Polinômios simétricos

Seja $A[x_1, \ldots, x_n]$ denota o anel dos polinômios em $x_1, \ldots, x_n$ indeterminadas com coeficientes num anel A. Seja S_n o grupo simétrico de permutações de índices em $\{1, 2, \ldots, n\} \mapsto \{1, 2, \ldots, n\}$.

Definição 1.22: Polinômio simétrico

Seja A um anel e seja $p(x_1, \ldots, x_n)$ um polinômio em $A[x_1, \ldots, x_n]$. Dizemos que $p(x_1, \ldots, x_n)$ é um *polinômio simétrico* se ele é invariante por permutações das indeterminadas $x_1, \ldots, x_n$, ou seja, se

$$p(x_1, \ldots, x_n) = p(x_{\sigma(1)}, \ldots, x_{\sigma(2)}),$$

para todas as bijeções $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$.

Em geral, temos os *polinômios simétricos elementares* nas variáveis $x_1, \ldots, x_n$.

$$s_r(x_1, \ldots, x_n)$$

onde $1 \leq r \leq n$. Definido como sendo a soma de todos os produtos distintos possíveis de x_i's. Então

$$\begin{aligned}
s_1(x_1, \ldots, x_n) &= \sum_{i=1}^{n} x_i = x_1 + \cdots + x_n \\
s_2(x_1, \ldots, x_n) &= \sum_{1 \leq i_1 < i_2 \leq n} x_{i_1} x_{i_2} = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n \\
&\vdots \\
s_j(x_1, \ldots, x_n) &= \sum_{1 \leq i_1 < i_2 < \cdots < i_j \leq n} x_{i_1} x_{i_2} \ldots x_{i_j} \\
&\vdots \\
s_n(x_1, \ldots, x_n) &= \prod_{i=1}^{n} x_i.
\end{aligned}$$

Por exemplo, seja $p(x_1, x_2)$ um polinômio em $\mathbb{Z}[x_1, x_2]$. É dito que $p(x_1, x_2)$ é um polinômio simétrico quando, $p(x_1, x_2) = x_1 + x_2 = x_2 + x_1 = p(x_2, x_1)$, ou seja, quando permutamos as variáveis, o polinômio permanece o mesmo. Com um contraexemplo simples, temos que o polinômio $p(x_1, x_2) = x_1 - x_2$ não é simétrico. Pois, se permutarmos as variáveis, o

polinômio $p(x_2, x_1) = x_2 - x_1 \neq p(x_1, x_2)$. Eles são bastante úteis para resolver problemas algébricos de fatoração de polinômios.

Um polinômio simétrico em $x_1, \ldots, x_n$ variáveis, também pode ser reescrito como um polinômio simétrico elementar em $s_1, \ldots, s_n$.

Teorema 1.16

Seja A um anel. Então, todo polinômio simétrico em $A[x_1, \ldots, x_n]$ é escrito como um polinômio com coeficientes em A nos polinômios simétricos elementares $s_1, \ldots, s_n$.

Demonstração. Veja em [17], páginas 25 e 26. □

De acordo, com o teorema anterior. Sejam A um anel e $p(x_1, x_2)$ um polinômio simétrico em $A[x_1, x_2]$. Vamos escrever $p(x_1, x_2) = 3x_1^2x_2 - x_1^2x_2^2 + 3x_1x_2^2$ em termos de $s_1 = x_1 + x_2$ e $s_2 = x_1x_2$.

$$\begin{aligned} p(x_1, x_2) = \; & 3x_1^2x_2 - x_1^2x_2^2 + 3x_1x_2^2 \\ & = 3x_1^2x_2 + 3x_1x_2^2 - x_1^2x_2^2 \\ & = 3x_1x_2(x_1 + x_2) - (x_1x_2)^2 \\ & = 3s_2(s_1) - (s_2)^2. \end{aligned}$$

Corolário 1.3

Suponha que F é uma extensão de um corpo K, $p(x) \in K[x]$, $\partial p(x) = n$ e as raízes de $p(x)$ são $\theta_1, \ldots, \theta_n \in F$. Se $h(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ é simétrico, então $h(\theta_1, \ldots, \theta_n) \in K$.

Demonstração. Veja em [17], página 26. □

Teorema 1.17: Teorema de Newton

Seja A um anel e $p(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$, um polinômio simétrico. Então, existe um único polinômio $h(x_1, \ldots, x_n) \in A[x_1, \ldots, x_n]$, efetivamente calculável, tal que $p(x_1, \ldots, x_n) = h(s_1, \ldots, s_n)$.

Demonstração. Veja em [7], páginas 76 até 78. □

Segue que, os polinômios simétricos são gerados pelos polinômios simétricos elementares.

1.7 Módulos

Os módulos são uma generalização de espaço vetorial, onde o corpo é substituído por um anel, no qual temos esse anel como o conjunto dos escalares. Também apresentaremos as definições de submódulos, módulo quociente, módulo livre.

Definição 1.23: A-módulo

Sejam A um anel e um grupo abeliano aditivo $(M, +)$ munido de uma multiplicação escalar

$$\begin{aligned} \cdot : \ A \times M \ &\to \quad M \\ (a, m) \ &\mapsto a \cdot m \end{aligned}$$

é dito um $A-$módulo se satisfaz os seguintes axiomas, para quaisquer $a, b \in A$ e $m, n \in M$, temos:

(i) $(a + b)m = am + bm$;

(ii) $a(m + n) = am + an$;

(iii) $a(bm) = (ab)m$;

(iv) $1m = m$.

A função $\cdot$ é chamada de A-ação em M. Temos que, o próprio anel A é um A-módulo. Um espaço vetorial V sobre um corpo K é um K-módulo. Neste ponto de vista, podemos ver A-módulo como uma generalização de um espaço vetorial. Em particular, definimos um *A-submódulo* de M como sendo um subgrupo N de M com as operações herdadas de M tal que se $n \in N$ e $a \in A$, então $an \in N$, os submódulos de A são exatamente os ideais A. Podemos também definir o *módulo quociente* M/N como o grupo quociente, com A-ação

$$\begin{aligned} \cdot : \ A \times M/N \ &\to \quad M/N \\ (a, m + N) \ &\mapsto a \cdot (m + N) = am + N \end{aligned}$$

com $a \in A$ e $m \in M$.

Um A-módulo de M será chamado *finitamente gerado* se existirem $m_1, \ldots, m_n \in M$ tais que $M = A \cdot m_1 + \cdots + A \cdot m_n$, é dito que $m_1, \ldots, m_n$ formam um *conjunto de geradores* de

M. Dizemos que os elementos $b_1, \ldots, b_n$ de M são linearmente independentes sobre A se, para quaisquer $a_1, \ldots, a_n \in A$, a igualdade

$$\sum_{i=1}^{n} a_i b_i = 0$$

implicar que $a_1 = \ldots = a_n = 0$. Além disto, se $b_1, \ldots, b_n$ formarem um conjunto de geradores de M, então $b_1, \ldots, b_n$ será uma *base* de M. Vale frisar, que nem todo módulo finitamente gerado possui uma base. Um A-módulo que possua uma base é chamado *livre*. Todo espaço vetorial não-nulo de dimensão finita é um *módulo livre*. Definimos o *posto* de um módulo livre G sendo o número de elementos da base de G. Um ideal I de A será um A-módulo livre se, e somente se, I for um ideal principal, gerado por um elemento que não seja divisor de zero de A, então esse elemento forma uma base de I.

Um $\mathbb{Z}-$*módulo* é um grupo abeliano $(G, +)$ (e inversamente, todo grupo abeliano é um $\mathbb{Z}-$módulo), podemos transformá-lo num $\mathbb{Z}-$módulo, definindo para quaisquer $m \in G$ e $n \in \mathbb{Z}$ positivo, temos

(i) $0m = 0 \qquad$ e $\qquad 1m = m$;

(ii) $(n+1)m = nm + m$;

(iii) $(-n)m = -nm$.

1.8 Grupos abelianos livres

Seja V um espaço vetorial sobre um corpo K. O conjunto V munido com a operação de soma de vetores é um grupo abeliano. Se G é finitamente gerado como $\mathbb{Z}$-módulo, então existem $g_1, \ldots, g_n \in G$ tais que quaisquer $g \in G$ é escrito como uma soma do tipo

$$g = m_1 g_1 + \ldots + m_n g_n \tag{1.2}$$

com $m_1 + \ldots + m_n \in \mathbb{Z}$. Então G é um grupo abeliano finitamente gerado.

Generalizando a noção de independência linear num espaço vetorial, dizemos que os elementos $g_1, \ldots, g_n \in G$ são linearmente independentes sobre $\mathbb{Z}$ se qualquer equação

$$0 = m_1 g_1 + \ldots + m_n g_n,$$

para $m_i \in \mathbb{Z}$ tais que $m_1 = \ldots = m_n = 0$. Uma base para G é um conjunto que gera G e denotamos por $\mathbb{Z}-$base. Se $\{g_1, \ldots, g_n\}$ é uma base, cada $g \in G$ é representada de maneira única por (1.2). Um grupo abeliano com uma base de n elementos é chamado de *grupo abeliano livre de posto n*. Se G é um grupo abeliano livre de posto n e sejam $\{x_1 + \ldots + x_n\}$, $\{y_1 + \ldots + y_n\}$ ambas bases de G, então existem inteiros a_{ij} e b_{ij} tais que

$$x_i = \sum_j b_{ij} y_j \qquad e \qquad y_i = \sum_j a_{ij} x_j.$$

Se considerarmos as matrizes

$$A = (a_{ij}) \qquad e \qquad B = (b_{ij}).$$

Então, o produto das matrizes resulta na matriz identidade. Portanto, $det(A)det(B) = 1$, como $det(A)$ e $det(B)$ são inteiros, isto implica que $det(A) = det(B) = \pm 1$. Uma matriz quadrada sobre $\mathbb{Z}$ com determinante igual a ± 1 é dita *unimodular*.

Lema 1.2

Seja G um grupo abeliano livre de posto n com base $\{x_1, \ldots, x_n\}$. Suponha que (a_{ij}) é uma matriz quadrada com entrada de números inteiros. Então, os elementos

$$y_i = \sum_j a_{ij} x_j$$

formam uma base de G se, e somente se, (a_{ij}) é unimodular.

Demonstração. Veja em [17], página 29. □

Teorema 1.18

Seja G um grupo abeliano livre de posto n. Todo subgrupo H de G é livre de grau $m \leq n$. Além disso, existe uma base $\{x_1, \ldots, x_n\}$ para G e números inteiros positivos $\alpha_1, \ldots, \alpha_m$ tais que $\{\alpha_1 x_1, \ldots, \alpha_m x_m\}$ é uma base para H.

Demonstração. Veja em [17] páginas 30 e 31. □

Cada subgrupo de um grupo abeliano livre, é também um grupo abeliano livre.

Teorema 1.19

Seja G um grupo abeliano livre de posto n, e H um subgrupo de G. Então $G\,/\,H$ é finito se, e somente se, os postos de G e H forem iguais. Se esse for o caso, e se G e H tiverem $\mathbb{Z}$-bases $\{x_1, \ldots, x_n\}$ e $\{y_1, \ldots, y_n\}$ com $y_i = \sum_j \alpha_{ij} x_j$, então

$$|G\,/\,H| = |det(\alpha_{ij})|.$$

Demonstração. Veja em [17] páginas 31 e 32. □

Por exemplo, seja G um grupo abeliano livre de posto 3 e $\mathbb{Z}$-base x, y, z, e se H tem $\mathbb{Z}$-base $4x, 6y, 14z$. Por consequência do Teorema 1.19 temos

$$|G\,/\,H| = |det(\alpha_{ij})| = \left| \begin{bmatrix} 4 & 0 & 0 \\ 0 & 6 & 0 \\ 0 & 0 & 14 \end{bmatrix} \right| = |4 \cdot 6 \cdot 14| = 336$$

.

Proposição 1.13

Todo grupo abeliano finitamente gerado com n geradores é o produto direto de um grupo abeliano finito e de um grupo livre com k geradores onde $k \leq n$.

Demonstração. Veja em [17], página 32. □

Proposição 1.14

Um subgrupo de um grupo finitamente gerado é finitamente gerado.

Demonstração. Veja em [17], página 33. □

Este capítulo inicial apresentou assuntos com grande relevância para o decorrer do nosso trabalho, como conceitos e resultados fundamentais para adiante compreendermos os próximos tópicos. Adiante vamos realizar uma introdução à teoria dos números algébricos.

CAPÍTULO

2

NÚMEROS ALGÉBRICOS

Neste capítulo, realizaremos o estudo dos números algébricos, inteiros algébricos e seus respectivos conjuntos. Apresentaremos noções fundamentais para o estudo introdutório da Teoria dos Números Algébricos. A meta principal é compreender o anel dos inteiros algébricos. A motivação para esse estudo surge das equações diofantinas, quando o matemático alemão Gauss, generalizou a noção de número inteiro para um número inteiro algébrico como será abordado, ele utilizou o anel de inteiros quadráticos, conhecido como o *anel de inteiros gaussianos*, representado por $\mathbb{Z}[i]$. Note que, mesmo a unidade imaginária não sendo um número inteiro racional. veremos que i é um inteiro algébrico, pois satisfaz a equação $x^2 + 1 = 0$.

2.1 Números Algébricos

Um número complexo α é dito algébrico se é algébrico sobre $\mathbb{Q}$, ou seja, se é raiz de um polinômio não-nulo com coeficientes em $\mathbb{Q}$. Caso contrário, ele é dito transcendente.

Denotamos por $\overline{\mathbb{Q}}$ o conjunto dos números algébricos. ainda mais, $\overline{\mathbb{Q}}$ é um corpo.

Teorema 2.1

O conjunto dos números algébricos $\overline{\mathbb{Q}}$ é um subcorpo do corpo $\mathbb{C}$.

Demonstração. Utilizando o teorema 1.15 que afirma, se α é algébrico se, e somente se, $[\mathbb{Q}(\alpha) : \mathbb{Q}] < +\infty$. Suponhamos que $\alpha, \beta \in \overline{\mathbb{Q}}$. Pelo teorema da torre, temos que

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}],$$

como β é algébrico sobre $\mathbb{Q}$, implica que β também é algébrico sobre $\mathbb{Q}(\alpha)$, logo, o fator a direita $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ é finito e o fator a esquerda $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)]$ também é finito. Portanto, $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}]$ é finito. Como, $\alpha + \beta, \alpha - \beta, \alpha\beta$ e α/β se $\beta \neq 0$, pertencem a $\mathbb{Q}(\alpha, \beta)$, temos que, todos eles são algébricos. Portanto, $\overline{\mathbb{Q}}$ é um subcorpo de $\mathbb{C}$. □

Todo o corpo $\overline{\mathbb{Q}}$ não é interessante para o nosso estudo, pois $[\,\overline{\mathbb{Q}} : \mathbb{Q}\,] = +\infty$. Então, iremos nos restringir ao estudo dos subcorpos K de $\overline{\mathbb{Q}}$ tais que $[K : \mathbb{Q}] < +\infty$. Isto implica, que todo elemento de K é algébrico. Portanto, $K \subseteq \overline{\mathbb{Q}}$.

Um subcorpo $K \subseteq \mathbb{C}$ é chamado de *corpo de números* se $[K : \mathbb{Q}] < +\infty$. O grau de K é o grau da extensão de corpos $[K : \mathbb{Q}]$, isto é, a dimensão de K como um $\mathbb{Q}$-espaço vetorial. Se K é um corpo de números, então $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ para um número finito de números algébricos $\alpha_1, \ldots, \alpha_n$. O corpo dos racionais $\mathbb{Q}$ é o menor corpo de números, ou seja, todo corpo de números contém $\mathbb{Q}$.

Exemplo 2.1

Os itens mostram um corpo de números (a) e um contraexemplo (b).

(a) Seja $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \,|\, a, b \in \mathbb{Q}\}$ um corpo de números, de fato, todo elemento desse corpo é combinação linear dos elementos 1 e $\sqrt{2}$. Portanto $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 < +\infty$.

(b) Dizemos que $\mathbb{Q}(\pi)$ não é um corpo de números, pois, π é um número transcendente e não é raiz de nenhuma equação polinomial sobre $\mathbb{Q}$. Portanto $[\mathbb{Q}(\pi) : \mathbb{Q}] = +\infty$.

Podemos mostrar que todo corpo de números é da forma $K = \mathbb{Q}(\theta)$, para algum θ algébrico.

Proposição 2.1

Se K é um corpo de números, então $K = \mathbb{Q}(\theta)$ para algum θ algébrico.

Demonstração. Ver em [17], página 39. □

2.2 Conjugados e Discriminantes

Nesta seção introduzimos os *conjugados* de um número algébrico e o *discriminante* de uma base para $\mathbb{Q}(\theta)$ sobre $\mathbb{Q}$, usando os conjugados de θ para mostrar que o discriminante é sempre um número racional diferente de zero.

Definição 2.1

Definimos os monomorfismos e os conjugados como:

(a) (Monomorfismos). Seja K um corpo de números, um monomorfismo é um homomorfismo injetor $\sigma : K \to \mathbb{C}$.

(b) (Conjugados). Sejam $K = \mathbb{Q}(\theta)$ um corpo de números de grau n, $\alpha \in K$, e sejam σ_i todos os monomorfismos de K em $\mathbb{C}$. Os elementos $\sigma_i(\alpha)$ para $i = 1, \ldots, n$ são chamados de $K-$ conjugados de α.

Se $K = \mathbb{Q}(\theta)$ é um corpo de números, existem, em geral, vários monomorfismos distintos $\sigma : K \to \mathbb{C}$. Por exemplo, se $K = \mathbb{Q}(i)$, sendo i a unidade imaginária, então as possibilidades são:

$$\sigma_1(x + iy) = x + iy,$$

$$\sigma_2(x + iy) = x - iy,$$

para $x, y \in \mathbb{Q}$.

Teorema 2.2

Seja $K = \mathbb{Q}(\theta)$ um corpo de números de grau n sobre $\mathbb{Q}$. Então existem exatamente n monomorfismos distintos $\sigma_i : K \to \mathbb{C}$ $(i = 1, \ldots, n)$. Os elementos $\sigma_i(\theta) = \theta_i$ são as raízes distintas em $\mathbb{C}$ do polinômio minimal de θ sobre $\mathbb{Q}$.

Demonstração. Veja em [17], páginas 40 e 41. □

Um observação importante, nem todos os conjugados de um elemento θ estão necessariamente no seu corpo K.

Exemplo 2.2

Seja o corpo $\mathbb{Q}(\sqrt[3]{2})$. Pelo teorema 2.2, temos que existem 3 monomorfismos distintos $\sigma : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{C}$, pois $x^3 - 2$ é o polinômio mínimo de $\sqrt[3]{2}$ sobre $\mathbb{Q}$. Todos os elementos de $\mathbb{Q}(\sqrt[3]{2})$ são números reais. Porém, os conjugados de $\sqrt[3]{2}$ são as raízes complexas distintas, $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$, $\omega^2\sqrt[3]{2}$, onde $\omega = e^{\frac{2\pi i}{3}} \in \mathbb{C}$.

Para cada $\alpha \in K = \mathbb{Q}(\theta)$, o polinômio de α sobre o corpo K é definido por

$$f_\alpha(x) = \prod_{i=1}^{n}(x - \sigma_i(\alpha))$$

Teorema 2.3

Os coeficientes do polinômio de α sobre um corpo de números K são racionais, isto é, $f_\alpha(x) \in \mathbb{Q}[x]$.

Demonstração. Temos que, $\alpha = r(\theta)$ para algum elemento $r \in \mathbb{Q}[x], \partial(r) < n$. Logo, o polinômio de α sobre um corpo de números é da forma:

$$f_\alpha(x) = \prod_{i}(x - \sigma_i(\alpha))$$

$$f_\alpha(x) = \prod_{i}(x - r(\sigma_i)),$$

onde os σ_i são as raízes distintas do polinômio minimal $p(x) \in \mathbb{Q}[x]$ de θ. Logo, os coeficientes de $f_\alpha(x)$ são da forma

$$h(\theta_1, \ldots, \theta_n),$$

onde $h(x_1, \ldots, x_n)$ é um polinômio simétrico em $\mathbb{Q}[x_1, \ldots, x_n]$, pelo teorema de Newton para funções simétricas $h(x_1, \ldots, x_n)$ pode ser escrito como um polinômio

$$h(s_1, \ldots, s_n),$$

onde $s_1, \ldots, s_n$ são os polinômios simétricos elementares em $\mathbb{Q}[x_1, \ldots, x_n]$. Então pelo corolário 1.3, concluímos que $h(\theta_1, \ldots, \theta_n) \in \mathbb{Q}$. □

Teorema 2.4

Com a notação anterior:

(a) O polinômio f_α é uma potência do polinômio minimal p_α.

(b) Os K-conjugados de α são zeros do polinômio p_α em $\mathbb{C}$, cada um repetindo n/m vezes, onde $m = \partial p_\alpha$ é um divisor de n.

(c) O elemento $\alpha \in \mathbb{Q}$ se, e somente se, todos os seus $K-$ conjugados são iguais.

(d) $\mathbb{Q}(\alpha) = \mathbb{Q}(\theta)$ se, e somente se, todos os $K-$ conjugados de α são distintos.

Demonstração. Ver em [17], página 42. □

Seja $K = \mathbb{Q}(\theta)$ de grau n e seja $\{\alpha_1, \ldots, \alpha_n\}$ uma base de K como $\mathbb{Q}-$espaço vetorial. Definimos o *discriminante* dessa base como sendo

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

Se considerarmos uma outra base $\beta_1, \ldots, \beta_n$, então

$$\beta_k = \sum_{i=1}^{n} c_{ik}\alpha_i, \qquad (c_{ik} \in \mathbb{Q}).$$

Para, $k = 1, \ldots, n$. Com $det(c_{ik}) \neq 0$. Isto implica que,

$$\Delta[\beta_1, \ldots, \beta_n] = [det(c_{ik})]^2 \Delta[\alpha_1, \ldots, \alpha_n].$$

Teorema 2.5

O discriminante de qualquer base para $K = \mathbb{Q}(\theta)$ é racional e não-nulo. Se todos os K-conjugados de θ são reais, então o discriminante de qualquer base é positivo.

Demonstração. Veja [17], página 43. □

2.3 Inteiros Algébricos

Um número complexo θ é um *inteiro algébrico* se é raiz de um polinômio mônico $p(x)$ com coeficientes inteiros. Em outras palavras,

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

onde $a_i \in \mathbb{Z}$, para todo, $0 \leq i \leq n-1$.

Observação: Na teoria algébrica dos números, um inteiro algébrico é muitas vezes chamado apenas de inteiro, enquanto os inteiros ordinários (os elementos do conjunto dos inteiros $\mathbb{Z}$) são chamados de inteiros racionais. Por exemplo, a unidade imaginária i é um inteiro algébrico, pois satisfaz a equação $x^2 + 1 = 0$.
Observe o contraexemplo, $\theta = \frac{\sqrt[3]{2}}{2}$ anula o polinômio $8x^3 - 2 = 0$. Mas, θ não é um inteiro algébrico pois o polinômio não é mônico. Um inteiro $m \neq 1$ é chamado livre de quadrados se não existe um primo p tal que $p^2|m$.

Lema 2.1

Um número complexo θ é um inteiro algébrico se, e somente se, o grupo aditivo gerado por todas as potências $1, \theta, \theta^2, \ldots$ é finitamente gerado.

Demonstração. Ver em [17] páginas 44 e 45. □

Denotamos por $\mathbb{B}$ o conjunto dos inteiros algébricos.

Teorema 2.6

O conjunto inteiros algébricos $\mathbb{B}$ formam um subanel do corpo dos números algébricos.

Demonstração. Veja em [17], página 45. □

Lema 2.2

Um número algébrico α é um inteiro algébrico se, e somente se, seu polinômio minimal sobre $\mathbb{Q}$ tem coeficientes em $\mathbb{Z}$.

Demonstração. Ver em [17], página 47. □

Uma extensão desta técnica permite-nos provar um teorema que será bastante útil:

Teorema 2.7

Seja θ um número complexo que é raiz de um polinômio mônico $p(x)$ cujos coeficientes são inteiros algébricos. Então, θ é um inteiro algébrico.

Demonstração. Ver em [17] página 45. □

Pelo teorema 2.6 e 2.7, podemos construir novos inteiros algébricos a partir de outros conhecidos. Por exemplo, $\sqrt[3]{5}$ e $\sqrt{2}$ são raízes de $x^3 - 5$ e $x^2 - 2$, respectivamente. Segue que, $\sqrt[3]{5} + \sqrt{2}$ é raiz de $x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17$. Portanto, $\sqrt[3]{5} + \sqrt{2}$ é um inteiro algébrico.

2.4 Bases integrais

Seja K um corpo de números de grau n sobre $\mathbb{Q}$. Uma $\mathbb{Q}-$base de K é uma base para K como um espaço vetorial sobre $\mathbb{Q}$. Pela proposição 2.1, temos que $K = \mathbb{Q}(\theta)$ onde θ é um inteiro algébrico, segue que o polinômio minimal $p(x)$ de θ tem grau n e $\{1, \theta, \ldots, \theta^{n-1}\}$ é uma base para K formada por inteiros algébricos.

O anel dos inteiros $\mathcal{O}_K$ com a adição é um grupo abeliano livre finitamente gerado com posto igual ao grau de K. Dizemos que uma $\mathbb{Z} - base$ para $(\mathcal{O}_K, +)$ como grupo abeliano livre é uma *base integral* para K. Ou seja, uma $\mathbb{Q}$-base para K que é uma $\mathbb{Z}$-base para $(\mathcal{O}_K, +)$. Portanto, $\{\alpha_1, \ldots, \alpha_n\}$ é uma base integral se, e somente se, todos os elementos $\alpha_i \in \mathcal{O}_K$ e qualquer elemento $\alpha \in \mathcal{O}_K$ é escrito de maneira única como

$$\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n,$$

para inteiros racionais $a_1, \ldots, a_n$.

Lema 2.3

Se $\{\alpha_1, \ldots, \alpha_n\}$ é uma base de K consistindo de inteiros, então o discriminante $\Delta[\alpha_1, \ldots, \alpha_n]$ é um inteiro racional, diferente de zero.

Demonstração. Ver em [17], página 48. □

Teorema 2.8

Cada corpo de número K possui uma base integral, e o grupo aditivo de $\mathcal{O}_K$ é abeliano livre de posto n igual ao grau de K.

Demonstração. Ver em [17], páginas 48 e 49. □

O lema 1.2 é necessário para provarmos um resultado importante sobre base integral para o corpo de números K.

Teorema 2.9

Seja $\{\alpha_1, \ldots, \alpha_n\}$ uma $\mathbb{Q} - base$ para K tal que $\alpha_1, \ldots, \alpha_n \in \mathcal{O}_K$. Se $\Delta[\alpha_1, \ldots, \alpha_n]$ é livre de quadrados, então $\{\alpha_1, \ldots, \alpha_n\}$ é uma base integral para K.

Demonstração. Seja $\{\beta_1, \ldots, \beta_n\}$ uma base integral. Então, existem inteiros racionais c_{ij} tal que $\alpha_i = \sum c_{ij}\beta_j$, temos

$$\Delta[\alpha_1, \ldots, \alpha_n] = (det\, c_{ij})^2 \Delta[\beta_1, \ldots, \beta_n].$$

Como $det\, c_{ij}$ é um quadrado e $\Delta[\beta_1, \ldots, \beta_n]$ é um inteiro racional, segue que $\Delta[\alpha_1, \ldots, \alpha_n]$ é livre de quadrados, então $det\, c_{ij} = \pm 1$, isto implica que c_{ij} é unimodular. Pelo lema 1.2, $\{\alpha_1, \ldots, \alpha_n\}$ é uma $\mathbb{Z} - base$ para $\mathcal{O}_K$, ou seja, uma base integral para K. □

Observação: A recíproca não é verdadeira, isto é, existem bases integrais que podem ter discriminantes que não sejam livre de quadrados.

Para duas bases integrais $\{\alpha_1, \ldots, \alpha_n\}$, $\{\beta_1, \ldots, \beta_n\}$ de um corpo de números K, temos

$$\Delta[\alpha_1, \ldots, \alpha_n] = (\pm 1)^2 \Delta[\beta_1, \ldots, \beta_n] = \Delta[\beta_1, \ldots, \beta_n],$$

como a matriz correspondente à mudança de base é unimodular, então o *discriminante* de uma base integral é independente da base integral que escolhemos.

2.5 Normas e Traços

A *norma* e o *traço* são conceitos importantes que permitem transformar um problema sobre inteiros algébricos em um problema sobre inteiros racionais. Seja $K = \mathbb{Q}(\theta)$ um corpo de números de grau n e seja $\sigma_1, \ldots, \sigma_n$ os monomorfismos de $K \to \mathbb{C}$. O polinômio f_α é uma potência do polinômio minimal p_α pelo item (a) do teorema 2.4, pelo lema 2.2 e o lema de Gauss 1.1. Temos que $\alpha \in K$ é um número inteiro se, e somente se, os polinômios tiverem coeficientes inteiros racionais, para qualquer $\alpha \in K$.

Definimos a norma de α por

$$\mathcal{N}_K(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha),$$

em outras palavras, a norma é o produto de todos os conjugados de α.

E o traço de α por

$$\mathcal{T}_K(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha),$$

ou seja, a norma é a soma de todos os conjugados de α.

Como o polinômio minimal é

$$f_\alpha(x) = \prod_{i=1}^{n} (x - \sigma_i(\alpha)).$$

A observação acima implica que se α é um número inteiro, então a norma e o traço de α são inteiros racionais. Como os σ_i são monomorfismos, é claro que

Proposição 2.2

A norma é multiplicativa e o traço é $\mathbb{Q} - linear$, isto é, para qualquer $\alpha, \beta \in K$ e $a, b \in \mathbb{Q}$, temos

$$\mathcal{N}_K(\alpha\beta) = (\mathcal{N}_K(\alpha))(\mathcal{N}_K(\beta)),$$

e

$$\mathcal{T}_K(a\,\alpha + b\,\beta) = a\mathcal{T}_K(\,\alpha) + b\mathcal{T}_K(\,\beta).$$

Demonstração. Decorre da definição de norma e traço e das propriedades dos monomorfismos que

$$\mathcal{N}_K(\alpha\beta) = \prod \sigma_i(\alpha\beta) = \prod \sigma_i(\alpha)\sigma_i(\beta) = \mathcal{N}_K(\alpha)\mathcal{N}_K(\beta),$$

e

$$\begin{aligned}
\mathcal{T}_K(a\,\alpha + b\,\beta) &= \sum \sigma_i(a\,\alpha + b\,\beta) \\
&= \sum (\sigma_i(a)\sigma_i(\alpha) + \sigma_i(b)\sigma_i(\beta)) \\
&= \sum (a\sigma_i(\alpha) + b\sigma_i(\beta)) \\
&= a\mathcal{T}_K(\,\alpha) + b\mathcal{T}_K(\,\beta).
\end{aligned}$$

□

A norma depende do corpo K. Entretanto, se o corpo estiver claro no contexto, podemos simplificar linguagem abreviando a norma e o traço de α por $\mathcal{N}(\alpha)$ e $\mathcal{T}(\alpha)$ respectivamente.

Proposição 2.3

Seja $K = \mathbb{Q}(\theta)$ um corpo de números onde θ possui polinômio minimal $p(x)$ de grau n. Então, a $\mathbb{Q} - base$ $\{1, \theta, \ldots, \theta^{n-1}\}$ possui o discriminante

$$\Delta[1, \theta, \ldots, \theta^{n-1}] = (-1)^{\frac{1}{2}n(n-1)}\mathcal{N}(Dp(\theta)),$$

onde $Dp(\theta)$ é a derivada de $p(x)$ em θ.

Demonstração. Ver [17], página 52. □

A seguinte proposição traz um resultado que envolve o discriminante e o traço:

Proposição 2.4

Se $\{\alpha_1, \ldots, \alpha_n\}$ é uma $\mathbb{Q} - base$ de K, então

$$\Delta[\alpha_1, \ldots, \alpha_n] = det(\mathcal{T}_K(\alpha_i\alpha_j)) \in \mathbb{Q}.$$

Com $1 \leq i, j \leq n$.

Demonstração. Segue pelas propriedades do determinante que

$$\mathcal{T}_K(\alpha_i\alpha_j) = \sum_{m=1}^{n} \sigma_m(\alpha_i\alpha_j) = \sum_{m=1}^{n} \sigma_m(\alpha_i)\sigma_m(\alpha_j).$$

Portanto,

$$\begin{aligned}
\Delta[\alpha_1, \ldots, \alpha_n] &= (det\,(\sigma_i(\alpha_j)))^2 \\
&= (det\ (\sigma_j(\alpha_i)))(det\,(\sigma_i(\alpha_j))) \\
&= det\left(\sum_{m=1}^{n} \sigma_m(\alpha_i)\sigma_m(\alpha_j)\right) \\
&= det(\mathcal{T}_K(\alpha_i\alpha_j)).
\end{aligned}$$

□

CAPÍTULO

3

CORPOS QUADRÁTICOS

3.1 Corpos Quadráticos

Um corpo $K \subseteq \mathbb{C}$ é dito quadrático se, e somente se K é extensão do corpo dos racionais $\mathbb{Q}$ tal que $[K : \mathbb{Q}] = 2$. Também podemos dizer que K é uma extensão quadrática de $\mathbb{Q}$. Então, $K = \mathbb{Q}(\theta)$ onde θ é um inteiro algébrico e também é raiz de um polinômio quadrático com coeficientes inteiros.

Definição 3.1: Corpo Quadrático

Um corpo quadrático é um corpo de números K de grau 2 sobre $\mathbb{Q}$.

Seja $p(x) = x^2 + bx + c = 0$ um polinômio com coeficientes em $\mathbb{Z}$. Resolver

$$x^2 + bx + c$$

equivale a encontrar θ, que pode ser tomado por

$$\theta = \frac{-b \pm \sqrt{(b^2 - 4c)}}{2}.$$

Seja $\Delta = b^2 - 4c = n^2 m$ onde $n, m \in \mathbb{Z}$ e m é livre de quadrados. Segue que

$$\theta = \frac{-b \pm n\sqrt{m}}{2}.$$

Portanto, $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{m})$.

Proposição 3.1

Os corpos quadráticos são da forma $\mathbb{Q}(\sqrt{m})$ para m inteiro livre de quadrados.

Demonstração. Seja $K = \mathbb{Q}(\theta)$ um corpo quadrático e θ um inteiro algébrico, por definição $[K : \mathbb{Q}] = 2$, então o polinômio mínimo de θ sobre $\mathbb{Q}$ é de grau 2. Temos que o polinômio $x^2 + bx + c$, com $b, c \in \mathbb{Z}$ e seu discriminante é dado por $\Delta = b^2 - 4c$ e a raiz tomado como

$$\theta = \frac{-b \pm \sqrt{\Delta}}{2}.$$

Para mostrar que $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{\Delta})$, temos que $\sqrt{\Delta} = \pm(2\theta + b)$, logo $\mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{Q}(\theta)$, e consequentemente $\theta = \frac{-b \pm \sqrt{\Delta}}{2}$. Assim, $\mathbb{Q}(\theta) \subset \mathbb{Q}(\sqrt{\Delta})$. Portanto, se θ for livre de quadrados, está demonstrado. Caso contrário, podemos escrever $\Delta = n^2 m$ onde $n, m \in \mathbb{Z}$ e m é livre de quadrados, então $\sqrt{\Delta} = n\sqrt{m}$. Segue que $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{m})$ porque $\sqrt{\Delta} = n\sqrt{m}$, então $\mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{Q}(\sqrt{m})$ por outro lado $\sqrt{m} = \frac{\sqrt{\Delta}}{n}$, concluí-se que $\mathbb{Q}(\sqrt{m}) \subset \mathbb{Q}(\sqrt{\Delta})$. □

Definição 3.2: Anel de Inteiros Algébricos

Seja K um corpo de números. O anel de inteiros de K, denotado por $\mathcal{O}_K$, é o conjunto de todos os inteiros algébricos de K, ou seja, $\mathcal{O}_K = K \cap \mathbb{B}$.

Denotamos por $\mathcal{O}_{\mathbb{Q}(\sqrt{m})}$ o anel dos inteiros algébricos de $\mathbb{Q}(\sqrt{m})$. Temos que o anel $\mathcal{O}_K$ herda as operações do corpo de números K.

Nesse momento o nosso objetivo é caracterizar os anéis de inteiros algébricos de $\mathbb{Q}(\sqrt{m})$, como m é um inteiro livre de quadrados, então $m \equiv 1, 2, 3 \, (mod\, 4)$.

Teorema 3.1

Seja $m \neq 1$ um inteiro livre de quadrados. Então, o anel dos inteiros algébricos de $\mathbb{Q}(\sqrt{m})$ são:

$$\theta = \begin{cases} \frac{1+\sqrt{m}}{2} & se \quad m \equiv 1 \, (mod\ 4), \\ \sqrt{m} & se \quad m \equiv 2 \ ou \ 3 \, (mod\ 4). \end{cases}$$

Demonstração. Seja um elemento $\alpha \in \mathbb{Q}(\sqrt{m})$ tem a forma $\alpha = r + s\sqrt{m}$ para $r, s \in \mathbb{Q}$. Então

$$\alpha = \frac{a + b\sqrt{m}}{c}$$

onde $a, b, c \in \mathbb{Z}$, $c > 0$ e são primos entre si. Temos que α é um inteiro se e somente se, os coeficientes do polinômio mínimo são inteiros

$$\left(x - \left(\frac{a + b\sqrt{m}}{c}\right)\right)\left(x - \left(\frac{a - b\sqrt{m}}{c}\right)\right).$$

Temos que

$$\frac{a^2 - b^2 m}{c^2} \in \mathbb{Z}, \tag{3.1}$$

$$\frac{2a}{c} \in \mathbb{Z}. \tag{3.2}$$

Se a e c possuem um fator p primo em comum, então (3.1) implica que p divide b (sendo m livre de quadrados) mas isso contradiz a nossa suposição anterior. Logo, por (3.2) temos duas possibilidades, $c = 1$ ou $c = 2$. Se $c = 1$, então α é um inteiro de K, em qualquer caso, podemos analisar o caso se $c = 2$. Segue que a e b devem ser ambos ímpares, e $\frac{a^2 - b^2 m}{4} \in \mathbb{Z}$, então $a^2 - b^2 m \equiv 0 (mod\ 4)$. Seja $2k + 1$ um número ímpar, seu quadrado é $4k^2 + 4k + 1 \equiv 1 (mod\ 4)$, logo, $a^2 \equiv 1 \equiv b^2 (mod\ 4)$, isto implica, que $m \equiv 1 (mod\ 4)$. Consequentemente, se $m \equiv 1 (mod\ 4)$, segue que a e b são ímpares. Portanto, α é um inteiro pois (3.1) e (3.2) são verdadeiros.

Se $m \not\equiv 1 (mod\ 4)$, então $c = 1$, e os inteiros de $\mathbb{Q}(\sqrt{m})$ são os elementos de $\mathbb{Z}[\sqrt{m}]$. Note que, se c = 1, então

$$a + b\sqrt{m} = a - b + 2b\left(\frac{1 + \sqrt{m}}{2}\right) = a - b + 2b\theta \in \mathbb{Z}[\theta].$$

Se $m \equiv 1 (mod\ 4)$, temos $c = 2$, sendo a e b ambos ímpares e portanto, os inteiros de $\mathbb{Q}(\sqrt{m})$ são os elementos de $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. Como, $c = 2$, então a e b são ímpares e temos que

$$\frac{a + b\sqrt{m}}{2} = \frac{a - b}{2} + \frac{b + b\sqrt{m}}{2} = \frac{a - b}{2} + b\theta \in \mathbb{Z}[\theta].$$

Temos que a ou b devem ser ímpares. Se b é par, então a é ímpar. Desde que $a^2 - mb^2 \equiv 0 (mod\ 4)$ e $b = 2k$, onde $k \in \mathbb{Z}$. Daí temos, $0 \equiv a^2 - m(2k)^2 \equiv a^2 - 4k^2 m \equiv a^2 (mod\ 4)$. Mas, se a é ímpar, então $a = 2k' + 1$ onde $k \in \mathbb{Z}$. Logo, $a^2 = 4k'^2 + 4k + 1 \equiv 1 (mod\ 4)$, chegamos há uma contradição, portanto b é ímpar. Se a fosse mesmo par, então $a = 2k$ e

$a^2 = 4k^2 \equiv 0(mod\ 4)$, ou seja, $b^2m \equiv 0(mod\ 4)$, mas b é ímpar, logo $b^2 \equiv 1(mod\ 4)$, então $0 \equiv b^2m \equiv m(mod\ 4)$, podemos escrever $m = 4q$ onde $q \in \mathbb{Z}$ com m é livre de quadrados. Portanto, uma contradição, segue que a e b devem ser ambos ímpares. □

$\mathbb{Z}[\theta]$ é o anel quadrático formado pelos inteiros de $\mathbb{Q}(\sqrt{m})$.

1. Para o caso, $m = -1$, como $m \not\equiv 1\,(mod\ 4)$, o anel de inteiros de $\mathbb{Q}(i)$ é o anel $\mathbb{Z}[i]$, chamado de Inteiros Gaussianos.

2. Para o caso, $m = -3$, como $m \equiv 1\,(mod\ 4)$, o anel de inteiros de $\mathbb{Q}(\sqrt{-3})$ é o anel $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ chamado Inteiros de Eisenstein.

Os homomorfismos de $\mathbb{Q}(\sqrt{m}) \to \mathbb{C}$ são:

$$\sigma_1(a + b\sqrt{m}) = a + b\sqrt{m},$$

$$\sigma_2(a + b\sqrt{m}) = a - b\sqrt{m}.$$

Conhecer os conjugados são necessários para calcular os discriminantes de um corpo quadrático.

Teorema 3.2

Seja $\mathbb{Q}(\sqrt{m})$ o corpo quadrático onde m é um inteiro livre de quadrados:

(a) Se $m \not\equiv 1\,(mod\ 4)$. Então, $\mathbb{Q}(\sqrt{m})$ tem uma base integral da forma $\{1, \sqrt{m}\}$ e o discriminante é igual a $4m$.

(b) Se $m \equiv 1\,(mod\ 4)$. Então, $\mathbb{Q}(\sqrt{m})$ tem uma base integral da forma $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$ e o discriminante é igual a m.

Demonstração. As afirmações sobre as bases, seguem do teorema anterior. Como o corpo quadrático é um corpo de dimensão 2. Uma base minimal de um corpo quadrático é da forma $\{1, \theta\}$, onde as possibilidades para θ são

$$\theta = \sqrt{m} \qquad ou \qquad \theta = \frac{1 + \sqrt{m}}{2}.$$

Para m livre de quadrados, onde m não divide 4, então $m \equiv 1, 2, 3\,(mod\,4)$. Para o caso $m \not\equiv 1\,(mod\ 4)$ temos que $\{1, \sqrt{m}\}$ é a base integral para o corpo quadrático $\mathbb{Q}(\sqrt{m})$.

Calculando o discriminante temos

$$\Delta[\mathbb{Q}(\sqrt{m})] = \Delta[1, \sqrt{m}] = \begin{bmatrix} 1 & \sqrt{m} \\ 1 & -\sqrt{m} \end{bmatrix}^2 = (-2\sqrt{m})^2 = 4m,$$

analogamente, se $m \equiv 1\,(mod\ 4)$, então $\left\{1, \frac{1+\sqrt{m}}{2}\right\}$ é a base integral para o corpo quadrático $\mathbb{Q}(\sqrt{m})$. Logo, o discriminante é dado por

$$\Delta[\mathbb{Q}(\sqrt{m})] = \Delta\left[1, \frac{1+\sqrt{m}}{2}\right] = \begin{bmatrix} 1 & \frac{1+\sqrt{m}}{2} \\ 1 & \frac{1-\sqrt{m}}{2} \end{bmatrix}^2 = (-\sqrt{m})^2 = m.$$

Como queríamos demonstrar. □

Exemplo 3.1

Determine a base integral e o discriminante dos anéis $\mathbb{Q}(\sqrt{11})$ e $\mathbb{Q}(\sqrt{-11})$.

(a) Seja $m = 11 \not\equiv 1\,(mod\ 4)$, então $\mathbb{Q}(\sqrt{11})$ possui uma base integral da forma $\{1, \sqrt{11}\}$ e o discriminante é igual a $4m = 4 \cdot 11 = 44$.

(b) Seja $m = -11 \equiv 1\,(mod\ 4)$, então $\mathbb{Q}(\sqrt{-11})$ possui uma base integral da forma $\left\{1, \frac{1+\sqrt{-11}}{2}\right\}$ e o discriminante é igual a $m = -11$.

Na próxima proposição, apresentaremos como funciona a norma e o traço para elementos de um corpo quadrático.

Proposição 3.2: Norma e Traço

Seja $\mathbb{Q}(\sqrt{m})$ o corpo quadrático (onde m é um inteiro livre de quadrados). Seja $\alpha = r + s\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ onde $r, s \in \mathbb{Q}$. Então,

$$\mathcal{N}(\alpha) = r^2 - ms^2 \quad e \quad \mathcal{T}(\alpha) = 2r.$$

Demonstração. O polinômio mínimo de $\sqrt{m}$ sobre $\mathbb{Q}$ é $x^2 - m = (x - \sqrt{m})(x + \sqrt{m})$. Então, os monomorfismos de $\sqrt{m}$ são

$$\sigma_1 : \sqrt{m} \to \sqrt{m},$$
$$\sigma_2 : \sqrt{m} \to -\sqrt{m}.$$

Pela definição de norma e traço, temos

$$\mathcal{N}(r+s\sqrt{m}) = \sigma_1(r+s\sqrt{m})\sigma_2(r+s\sqrt{m}) = (r+s\sqrt{m})(r-s\sqrt{m}) = r^2 - ms^2,$$
$$\mathcal{T}(r+s\sqrt{m}) = \sigma_1(r+s\sqrt{m}) + \sigma_2(r+s\sqrt{m}) = (r+s\sqrt{m}) + (r-s\sqrt{m}) = 2r.$$

□

Conhecer a norma de um elemento de $\mathbb{Z}[\theta]$ é necessário para que anéis quadráticos sejam euclidianos.

Lema 3.1

Para todo $\alpha, \beta \in \mathbb{Q}(\sqrt{m})$ a norma goza das seguintes propriedades:

1) $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha)\mathcal{N}(\beta)$.

2) Se $\alpha \in \mathbb{Z}[\theta]$, então $\mathcal{N}(\alpha) \in \mathbb{Z}$.

3) Se $m > 0$, então $|\mathcal{N}(a+b\sqrt{m})| = |a^2 - mb^2| \leq max\{a^2, mb^2\}$.

4) Se $\alpha \in \mathbb{Z}[\theta]$, então α é inversível se e somente se $\mathcal{N}(\alpha) = \pm 1$.

5) Se $\alpha \in \mathbb{Z}[\theta]$ e $\mathcal{N}(\alpha) = p$ com p número primo, então α é irredutível.

Demonstração. Ver [1], página 5. □

3.2 Inteiros Quadráticos que são Domínios Euclidianos

Segundo [17], página 95. O matemático estadunidense Leonard Eugene Dickson provou que $\mathbb{Q}(\sqrt{m})$ é euclidiano para $m = 2, 3, 5, 13$ e afirmou equivocadamente que não existiam outros valores para m, tal que $\mathbb{Q}(\sqrt{m})$ seja Euclidiano. Sucessivamente, o alemão Oskar Perron demonstrou que para $m = 6, 7, 11, 17, 21, 29$ também satisfaziam a condição Euclidiana. Continuamente os matemáticos Oppenheimer, Robert Remak e László Redei adicionaram os valores para $m = 19, 33, 37, 41, 55$ *e* 73. Erroneamente, László Rédei também defendeu que para $\mathbb{Q}(\sqrt{97})$ o anel quadrático seria euclidiano, mas isso foi refutado por Eric Barnes e Peter Swinnerton-Dyer. Hans Heilbronn provou em 1934 que a lista de valores para m é finita, e o problema foi finalizado por Harold Chatland e Harold Davenport.

Teorema 3.3

Se $m > 0$, existe um algoritmo da divisão em $\mathbb{Z}[\theta]$, isto significa, que $\mathbb{Z}[\theta]$ é um anel euclidiano, quando $m \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$.

A demonstração é diferente para determinados valores de m, portanto não temos como generalizar e demonstrar para todos os casos de uma mesma maneira, faremos a demonstração para $m = 2, 3, 5, 13$ e indicaremos onde encontrar a prova para outros valores.

Teorema 3.4

Existe um algoritmo da divisão em $\mathbb{Z}[\theta]$, quando $m = 2, 3, 5, 13$.

Demonstração. Utilizaremos a propriedade 3) do lema 3.1

Queremos mostrar que se $\lambda \in \mathbb{Q}(\sqrt{m})$, existe $q \in \mathbb{Z}[\theta]$ tal que $\mathcal{N}(\lambda - q) < 1$.
No caso de $m \not\equiv 1\,(mod\ 4)$, ou seja, quando $m = 2, 3$, se $\lambda = a + b\sqrt{m}$ com $a, b \in \mathbb{Q}$, tomamos $x, y \in \mathbb{Z}$ tais que $|a - x| \leq \frac{1}{2}$ e $|b - y| \leq \frac{1}{2}$. Então, se $q = x + y\sqrt{m}$, temos

$$\mathcal{N}(\lambda - q) = \mathcal{N}(a - x + (b - y)\sqrt{m}) = |(a - x)^2 + m(b - y)^2| \leq max\left\{\frac{1}{4}, \frac{m}{4}\right\} < 1.$$

Quando $m \equiv 1\,(mod\ 4)$, ou seja, no caso em que $m = 5, 13$, como acima, $\lambda = a + b\sqrt{m}$, com $a, b \in \mathbb{Q}$, tomamos $y = \frac{v}{2}$ com $v \in \mathbb{Z}$ tal que $|b - y| \leq \frac{1}{4}$ e seja $x = \frac{u}{2}$ com $u \in \mathbb{Z}$, logo $u \equiv v\,(mod\ 2)$, tal que $|a - x| \leq \frac{1}{2}$. De acordo com a construção dos anéis quadráticos, quando $m \equiv 1\,(mod\ 4)$, os elementos u e v têm que ter a mesma paridade. Logo, se $q = x + y\sqrt{m}$, então

$$\mathcal{N}(\lambda - q) = \mathcal{N}(a - x + (b - y)\sqrt{m}) = |(a - x)^2 - m(b - y)^2| \leq max\left\{\frac{1}{4}, \frac{m}{16}\right\} < 1.$$

Portanto, o teorema está demonstrado. □

Teorema 3.5

Existe um algoritmo da divisão em $\mathbb{Z}[\theta]$ quando $m = 6, 7, 17, 21, 29$.

Demonstração. Ver [1], páginas 10, 11 *e* 12. □

Teorema 3.6

Se $m < 0$, existe um algoritmo da divisão em $\mathbb{Z}[\theta]$, isto é, que $\mathbb{Z}[\theta]$ é um anel euclidiano, quando $m \in \{-1, -2, -3, -7, -11\}$.

Demonstração. Dados $\alpha, \beta \in \mathbb{Z}[\theta]$ e $\beta \neq 0$, queremos descobrir um quociente e um resto pertencente ao anel de inteiros algébricos, ou seja, $q, r \in \mathbb{Z}[\theta]$ tais que $\alpha = \beta q + r$ com $\mathcal{N}(r) < \mathcal{N}(\beta)$. Assim,

$$\mathcal{N}(r) = \mathcal{N}(\alpha - \beta q) = \mathcal{N}\left(\beta\left(\frac{\alpha}{\beta} - q\right)\right) = \mathcal{N}(\beta)\mathcal{N}\left(\frac{\alpha}{\beta} - q\right).$$

Resta mostrar que se $\lambda \in \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{m})$, o corpo das frações de $\mathbb{Z}[\theta]$ tal que $1 > \mathcal{N}(\lambda - q)$. No caso de $m \not\equiv 1\,(mod\ 4)$, isto é, quando $m = -1, -2$. Seja $\lambda = a + b\sqrt{m}$ com $a, b \in \mathbb{Q}$, considerando $x, y \in \mathbb{Z}$ tais que

$$|a - x| \leq \frac{1}{2} \ \ e \ \ |b - y| \leq \frac{1}{2}.$$

Segue-se que tomando $\lambda = x + y\sqrt{m}$, temos

$$\mathcal{N}(\lambda - q) = \mathcal{N}(a - x + (b - y)\sqrt{m}) \leq (a - x)^2 - m(b - y)^2 \leq \frac{1}{4} + |m|\frac{1}{4} < 1.$$

Quando $m \equiv 1\,(mod\ 4)$, ou seja, no caso em que $m = -3, -7, -11$, como acima, $\lambda = a + b\sqrt{m}$, tomamos $y = \frac{v}{2}$ com $v \in \mathbb{Z}$ tal que $|b - y| \leq \frac{1}{4}$ e seja $x = \frac{u}{2}$ com $u \in \mathbb{Z}$, logo $u \equiv v\,(mod\ 2)$, tal que $|a - x| \leq \frac{1}{2}$. Lembrando, assim como vimos na construção dos anéis quadráticos, quando $m \equiv 1\,(mod\ 4)$, os elementos u e v têm que ter a mesma paridade. Então, seja $q = x + y\sqrt{m}$, logo

$$\mathcal{N}(\lambda - q) = \mathcal{N}(a - x + (b - y)\sqrt{m}) \leq (a - x)^2 - m(b - y)^2 \leq \frac{1}{4} + |m|\frac{1}{16} < 1.$$

□

Esses são os únicos valores para m que faça o anel de inteiros ser euclidiano.

Teorema 3.7

O anel de inteiros de $\mathbb{Q}(\sqrt{m})$ não é euclidiano para $m < -11$ livre de quadrados.

Demonstração. Ver em [17], página 95. □

O funcionamento do algoritmo da divisão no anel de inteiros Gaussianos $\mathbb{Z}[i]$. De acordo com o teorema 3.6.

Exemplo 3.2

Sejam $m = -1$, $\alpha = 7 - 6i$, $\beta = 2 + i$. Verificaremos a divisão euclidiana.

Demonstração. Temos, $-1 \equiv 3\,(mod\ 4)$ vamos encontrar $q = x + y\sqrt{m}$, $r = s + t\sqrt{m} \in \mathbb{Z}[\sqrt{-1}]$ tais que $\alpha = q\beta + r$ com $\mathcal{N}(r) < \mathcal{N}(b)$. Seja $\frac{\alpha}{\beta} = a + b\sqrt{-1} = \frac{8}{5} - \frac{19}{5}i$, temos $a = \frac{8}{5}$ e $b = -\frac{19}{5}$.

Tomamos x e $y \in \mathbb{Z}$ tais que $|a - x| \leq \frac{1}{2}$ e $|b - y| \leq \frac{1}{2}$.

Seja $x = 2$. Então

$$|a - x| = \left|\frac{8}{5} - 2\right| = \left|-\frac{2}{5}\right| = \frac{2}{5} \leq \frac{1}{2}.$$

Tomando $y = -4$.

$$|b - y| = \left|-\tfrac{19}{5} + 4\right| = \left|\tfrac{1}{2}\right| = \tfrac{1}{2} \leq \tfrac{1}{2}.$$

Desse modo, temos $q = x + y\sqrt{m} = 2 - 4\sqrt{-1}$, temos

$$r = \alpha - q\beta = 7 - 6i - (2 - 4i)(2 + i) = -1.$$

Portanto,

$$\mathcal{N}(r) = \mathcal{N}(-1) = 1 < 5 = \mathcal{N}(2 + i) = \mathcal{N}(\beta).$$

□

O anel de inteiros Gaussianos $\mathbb{Z}[i]$ é um domínio de fatoração única, porém, vejamos alguns casos de inteiros algébricos complexos que não são domínios de fatoração única.

Exemplo 3.3

$\mathbb{Z}[\sqrt{-11}]$ não é um anel fatorial.

Demonstração. Seja $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ o anel de inteiros algébricos de $\mathbb{Q}(\sqrt{-11})$. Queremos mostrar que o subanel $\mathbb{Z}[\sqrt{-11}]$ de $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$, não é um anel fatorial. Pelo teorema 3.6 temos que $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ é um anel euclidiano. Considere

$$12 = 2 \cdot 2 \cdot 3 = (1 + \sqrt{-11})(1 - \sqrt{-11}).$$

Temos

$$\mathcal{N}(2) = 4, \mathcal{N}(3) = 9 \ \ e \ \ \mathcal{N}(1 + \sqrt{-11}) = \mathcal{N}(1 - \sqrt{-11}) = 12.$$

Em $\mathbb{Z}[\sqrt{-11}]$ não existem elementos com norma 2, os elementos 2, 3, $1 + \sqrt{-11}$, $1 - \sqrt{-11}$ são irredutíveis, pela propriedade 5) do lema 3.1. Logo, 12 é escrito de duas maneiras

distintas como produto de elementos irredutíveis e assim $\mathbb{Z}[\sqrt{-11}]$ não é um anel fatorial. Então,

$$\mathcal{N}\left(\frac{1 \pm \sqrt{-11}}{2}\right) = 3,$$

como

$$\left(\frac{1+\sqrt{-11}}{2}\right) \cdot \left(\frac{1-\sqrt{-11}}{2}\right) = 3.$$

Mas, 2, $\left(\frac{1+\sqrt{-11}}{2}\right)$ e $\left(\frac{1-\sqrt{-11}}{2}\right)$ são elementos irredutíveis em $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$. Portanto, a única maneira de escrever 12 como produto de elementos irredutíveis em $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ é dado por

$$12 = 2 \cdot 2 \cdot \left(\frac{1+\sqrt{-11}}{2}\right) \cdot \left(\frac{1-\sqrt{-11}}{2}\right).$$

□

Exemplo 3.4

$\mathbb{Z}[\sqrt{-3}]$ não é um anel fatorial.

Demonstração. Seja $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ o anel de inteiros algébricos de $\mathbb{Q}(\sqrt{-3})$. Queremos mostrar que o subanel $\mathbb{Z}[\sqrt{-3}]$ de $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, não é um anel fatorial. Pelo teorema 3.6, temos que $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$ é um anel euclidiano. Considere

$$4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3}).$$

Temos

$$\mathcal{N}(2) = \mathcal{N}(1+\sqrt{-3}) = \mathcal{N}(1-\sqrt{-3}) = 4.$$

Em $\mathbb{Z}[\sqrt{-11}]$ não existem elementos com norma 2, note que os elementos 2, $1+\sqrt{-3}$, $1+\sqrt{-3}$ são irredutíveis, pela propriedade 5) do lema 3.1. Como os elementos inversíveis de $\mathbb{Z}[\sqrt{-3}]$ são ± 1, temos que 2, $1+\sqrt{-3}$, $1+\sqrt{-3}$ não são associados. Logo, 4 é escrito de duas maneiras distintas como produto de elementos irredutíveis e assim $\mathbb{Z}[\sqrt{-3}]$ não é um anel fatorial. No entanto, em $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, os elementos 2, $1+\sqrt{-3}$, $1+\sqrt{-3}$ são associados. Portanto, a menos de elementos irredutíveis, as duas decomposições,

$$4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3}),$$

são iguais. □

3.3 Anéis Principais que não são Euclidianos

Todo Domínio Euclidiano é um Domínio de Ideal Principal, mas a recíproca não é verdadeira. Nesta seção apresentaremos o anel principal $\mathbb{Z}[\omega]$, onde $\omega = \frac{1+\sqrt{-19}}{2}$ e veremos que ele não satisfaz a condição euclidiana.

Lema 3.2

No anel $\mathbb{Z}[\omega]$, a norma possui as seguintes propriedades:

(a) $\mathcal{N}(\alpha) \geq 0$, $\forall\, \alpha \in \mathbb{Z}[\omega]$.

(b) $\mathcal{N}(a + b\omega) = a^2 + ab + 5b^2 = n$.

(c) $\mathcal{N}(a + b\omega) = (a + b)^2 - ab + 4b^2 = n$.

Demonstração. Ver [1], página 20. □

Lema 3.3

Os elementos invertíveis de $\mathbb{Z}[\omega]$ são 1 e -1.

Demonstração. Seja um elemento $\alpha \in \mathbb{Z}[\omega]$, como $m \equiv 1\,(mod\ 4)$, pelo teorema 3.6, temos que α é da forma $\frac{a+b\sqrt{-19}}{2}$, sendo $a, b \in \mathbb{Z}$, $a \equiv b\,(mod\ 2)$. Então, pela norma, α é um elemento inversível se e somente se,

$$\mathcal{N}\left(\frac{a + b\sqrt{-19}}{2}\right) = \left(\frac{a + b\sqrt{-19}}{2}\right) \cdot \left(\frac{a - b\sqrt{-19}}{2}\right) = \frac{a^2 + 19b^2}{4} = 1.$$

Basta encontrarmos as soluções da equação $a^2 + 19b^2 = 4$, quando $b = 0$ e $a = \pm 2$, resulta que $\alpha = \pm 1$. Portanto o lema está demonstrado. □

Lema 3.4

Os elementos ω, $\omega - 1$, $\omega + 1$, 2 *e* 3 são irredutíveis em $\mathbb{Z}[\omega]$.

Demonstração. Pela definição de norma, temos que

$$\mathcal{N}(\omega) = \omega\overline{\omega} = \left(\frac{1 + \sqrt{-19}}{2}\right) \cdot \left(\frac{1 - \sqrt{-19}}{2}\right) = \frac{1 + 19}{4} = 5.$$

De maneira análoga, obtemos que $\mathcal{N}(\omega - 1) = 5$ e $\mathcal{N}(\omega + 1) = 7$. Como 5 e 7 são números primos, pela propriedade 5) do lema 3.1 obtemos que $\omega, \omega - 1$ e $\omega + 1$ são irredutíveis.

Analisando os casos em que 2 e 3 são irredutíveis, veja que, $\mathcal{N}(2) = 4$ e $\mathcal{N}(3) = 9$, faremos uso das propriedades 1) e 4) do lema 3.1 e iremos mostrar que não existem elementos em $\mathbb{Z}[\omega]$ com norma 2 ou 3. Para isso, seja $n = 2$ ou $n = 3$ e vamos supor que existe $a+b\omega \in \mathbb{Z}[\omega]$ tal que $\mathcal{N}(a + b\omega) = n$. Suponha que $ab \geq 0$ e pela propriedade 2) do lema 3.2, temos

$$\mathcal{N}(a + b\omega) = a^2 + ab + 5b^2 = n.$$

Como $n \leq 3$, isto implica, que $b = 0$ e $a = \pm\sqrt{n}$. Analogamente, suponhamos que $ab \leq 0$. Pela propriedade 4) do lema 3.2, observamos

$$\mathcal{N}(a + b\omega) = (a + b)^2 - ab + 4b^2 = n.$$

De mesmo modo, como $n \leq 3$, temos $b = 0$ e $a = \pm\sqrt{n}$. Daí $\sqrt{n} \notin \mathbb{Z}$, logo não existem elementos em $\mathbb{Z}[\omega]$ com norma igual a 2 ou 3. Portanto, concluímos que 2 e 3 são irredutíveis. □

Definição 3.3: Anel Quase Euclidiano

Dizemos que A é um *anel quase euclidiano* se existe uma aplicação $\varphi : A\backslash\{0\} \to \mathbb{N}$ satisfazendo a seguinte condição:
Para todo $\alpha, \beta \in A\backslash\{0\}$ tais que $\varphi(\alpha) \geq \varphi(\beta)$, temos que $\beta|\alpha$ ou existem $\eta, \kappa \in A$ tal que $0 < \varphi(\underbrace{\eta\alpha - \kappa\beta}_{\neq 0}) < \varphi(\beta)$.

Com essa definição conseguimos provar que todo anel quase euclidiano é principal e servirá de ferramenta para mostrar que o anel $\mathbb{Z}[\omega]$ é um anel principal.

Teorema 3.8

Todo anel quase euclidiano é principal.

Demonstração. Seja A um anel quase euclidiano e I um ideal não nulo de A. Determinamos $\beta \in I$ sendo um elemento não nulo tal que $\varphi(\beta)$ seja mínimo, como o contradomínio é o conjunto dos naturais, podemos escolher um elemento tal que ele seja mínimo entre todos os elementos não nulos pertencentes ao ideal I, ou seja, qualquer $\lambda \in I\backslash\{0\}$, temos que $\varphi(\lambda) \geq \varphi(\beta)$. Queremos provar que $I = (\beta)$, para isso, seja $\alpha \in I$ e suponhamos que $\alpha \notin (\beta)$. Pelo fato de $\alpha \in I$, temos que $\varphi(\alpha) \geq \varphi(\beta)$. Consequentemente, como $\alpha \notin (\beta)$,

logo $\beta \nmid \alpha$. Sabemos que o anel A é quase euclidiano, então existem $\eta, \kappa \in A$ tais que

$$0 < \varphi(\eta\alpha - \kappa\beta) < \varphi(\beta).$$

Note que, $\eta\alpha - \kappa\beta \in I$, pelo fato de $\eta\alpha - \kappa\beta \neq 0$ e I ser um ideal, mas esse fato contradiz a minimalidade de $\varphi(\beta)$. Desse modo, $I \subset (\beta)$ e como $\beta \in I$, também temos que $(\beta) \subset I$. Concluímos que $I = (\beta)$, ou seja, β gera o ideal I. Portanto, A é um anel quase euclidiano. □

Agora, podemos demonstrar que o anel $\mathbb{Z}[\omega]$ não é euclidiano.

Teorema 3.9

$\mathbb{Z}[\omega]$ não é um anel euclidiano.

Demonstração. Suponhamos que $\mathbb{Z}[\omega]$ seja um anel euclidiano com a aplicação φ. Como o contradomínio é o conjunto dos naturais, buscamos um elemento que não seja inversível em $\mathbb{Z}[\omega]\backslash\{0\}$, então seja $s \in \mathbb{Z}[\omega]\backslash\{-1, 0, 1\}$ tal que $\varphi(s)$ seja mínimo entre os elementos do domínio. Pelo algoritmo da divisão, existe um quociente e um resto, dados por $q, r \in \mathbb{Z}[\omega]$ tais que

$$2 = sq + r$$

com $r = 0$ ou $\varphi(r) < \varphi(s)$. Mas, a escolha de s influência nos valores capazes de r admitir, que são -1, 0 ou 1. Note que, se $r = 1$, teríamos $1 = sq$, ou seja, s seria inversível, contrariando o fato de s não ser inversível. Logo, se $r = 0$ temos $sq = 2$ ou se $r = -1$ temos $sq = 3$, isto implica, que $s|2$ ou $s|3$, pelo lema 3.4, os elementos 2 e 3 são irredutíveis em $\mathbb{Z}[\omega]$, segue-se então que os possíveis valores de s são $s = \pm 2$ ou $s = \pm 3$. De mesmo modo, aplicando o algoritmo da divisão, existem $q', r' \in \mathbb{Z}[\omega]$ tais que

$$\omega = sq' + r'$$

com $r' = 0$ ou $\varphi(r') < \varphi(s)$. Analogamente, a escolha de s determina os possíveis valores de r', que podem ser -1, 0 ou 1. Para cada valor de r' sucessivamente, temos $sq' = \omega + 1$, $sq' = \omega$ ou $sq' = \omega - 1$. Seja λ um dos valores: $\omega + 1, \omega, \omega - 1$. Então

$$\lambda = sq'.$$

Pelo lema 3.4, os elementos $\omega + 1, \omega, \omega - 1$ são irredutíveis em $\mathbb{Z}[\omega]$, logo λ é irredutível. Assim, q' é inversível ou s é inversível. Mas, s não é inversível pelo fato de s ser irredutível,

isto implica, que q' é inversível. Portanto, $\mathcal{N}(q') = 1$ e $\mathcal{N}(\lambda) = \mathcal{N}(s)$. Porém, temos pelo lema 3.4, que $\mathcal{N}(\lambda) = \mathcal{N}(\lambda - 1) = 5$ ou $\mathcal{N}(\lambda) = \mathcal{N}(\lambda + 1) = 7$, entretanto $\mathcal{N}(s) = 4$ ou $\mathcal{N}(s) = 9$. Com essa contradição, concluímos a demonstração que $\mathbb{Z}[\omega]$ não é um anel euclidiano. □

Para mostrar que $\mathbb{Z}[\omega]$ é um anel principal, basta verificar que ele é um anel quase euclidiano e pelo teorema 3.8, implicará que é principal.

Teorema 3.10

$\mathbb{Z}[\omega]$ é um anel principal.

Demonstração. Queremos mostrar que $\mathbb{Z}[\omega]$ é um anel quase euclidiano com a função norma usual. Sejam dados $\alpha, \beta \in \mathbb{Z}[\omega]\backslash\{0\}$ tais que $\mathcal{N}(\alpha) \geq \mathcal{N}(\beta)$, se $\beta|\alpha$ está demonstrado. Então, vamos supor que $\beta \nmid \alpha$, pela definição de anel quase euclidiano devemos encontrar $\eta, \kappa \in \mathbb{Z}[\omega]$ tais que

$$0 < \mathcal{N}(\eta\alpha - \kappa\beta) < \mathcal{N}(\beta).$$

Isso é equivalente a mostrar que existem $\eta, \kappa \in \mathbb{Z}[\omega]$ tais que

$$0 < \mathcal{N}\left(\eta\frac{\alpha}{\beta} - \kappa\right) < \mathcal{N}(1).$$

Segue-se que $\frac{\alpha}{\beta} \in \mathbb{Q}(\sqrt{-19})$, o corpo de frações de $\mathbb{Z}[\omega]$ e também $\frac{\alpha}{\beta} \notin \mathbb{Z}[\omega]$. Com $a, b \in \mathbb{Z}$ e $c > 0$ sendo a, b, c primos entre si, isto é, $(a, b, c) = 1$. Conseguimos escrever esse elemento de tal maneira

$$\frac{\alpha}{\beta} = \frac{a + b\sqrt{-19}}{c}$$

Note que, se $c = 1$, temos $\frac{\alpha}{\beta} \in \mathbb{Z}[\omega]$, logo $\beta|\alpha$. Então, supondo que $c > 1$. Vamos analisar as possibilidades distintas para quando c for igual a $2, 3, 4$ ou maior e igual a 5.

(i) Seja $c = 2$. Como $\frac{\alpha}{\beta} \notin \mathbb{Z}[\omega]$, sabemos que a e b têm paridade distintas. Assim, escolhendo $\eta = 1$ e $\kappa = \frac{a-1+b\sqrt{-19}}{2}$ em $\mathbb{Z}[\omega]$, então

$$\eta\frac{\alpha}{\beta} - \kappa = \frac{a + b\sqrt{-19}}{2} - \frac{a - 1 + b\sqrt{-19}}{2} = \frac{1}{2} \neq 0.$$

Aplicando a norma, temos

$$0 < \mathcal{N}\left(\eta\frac{\alpha}{\beta} - \kappa\right) = \mathcal{N}\left(\frac{1}{2}\right) = \frac{1}{4} < 1.$$

(ii) Seja $c = 3$. Como $(a, b, c) = 1$, temos que a e b não podem ser ambos divisíveis por 3. Daí, $a^2 + b^2 \equiv 1\,(mod\ 3)$ ou $a^2 + b^2 \equiv 2\,(mod\ 3)$, logo

$$a^2 + 19b^2 \equiv a^2 + b^2 \not\equiv 0\,(mod\ 3).$$

Então, existem $q, r \in \mathbb{Z}$ tais que $a^2 + 19b^2 = 3q + r$ com $0 < r < 3$. Assim, escolhendo $\eta = a - b\sqrt{-19}$ e $\kappa = q$, temos

$$\begin{aligned}
\eta\frac{\alpha}{\beta} - \kappa &= (a - b\sqrt{-19})\left(\frac{a + b\sqrt{-19}}{3}\right) - q \\
&= \frac{a^2 + 19b^2}{3} - q \\
&= \frac{a^2 + 19b^2 - 3q}{3} \\
&= \frac{3q + r - 3q}{3} \\
&= \frac{r}{3} \neq 0.
\end{aligned}$$

Sabemos que $r \leq 2$. Aplicando a norma, obtemos

$$0 < \mathcal{N}\left(\eta\frac{\alpha}{\beta} - \kappa\right) = \mathcal{N}\left(\frac{r}{3}\right) \leq \frac{4}{9} < 1.$$

(iii) Seja $c = 4$. Como $(a, b, c) = 1$, temos que a e b não podem ser ambos pares, isto implica, que ambos são ímpares ou possuem paridades distintas. Primeiramente, vamos supor que a e b possuem paridades distintas. Então, $a^2+19b^2 \equiv a^2-b^2 \not\equiv 0\,(mod\ 4)$, segue-se que existem $q, r \in \mathbb{Z}$ tais que $a^2 + 19b^2 = 4q + r$ com $0 < r < 4$, porém, como a e b têm paridades diferentes, o caso $r = 2$ é descartado, então os possíveis valores para r são 1 ou 3. Desse modo, tomando $\eta = a - b\sqrt{-19}$ e $\kappa = q$ em $\mathbb{Z}[\omega]$, temos

$$\begin{aligned}
\eta\frac{\alpha}{\beta} - \kappa &= (a - b\sqrt{-19})\left(\frac{a + b\sqrt{-19}}{4}\right) - q \\
&= \frac{a^2 + 19b^2}{4} - q \\
&= \frac{a^2 + 19b^2 - 4q}{4} \\
&= \frac{4q + r - 4q}{4} \\
&= \frac{r}{4} \neq 0.
\end{aligned}$$

Sabemos que $r \leq 3$. Aplicando a norma, obtemos

$$0 < \mathcal{N}\left(\eta\frac{\alpha}{\beta} - \kappa\right) = \mathcal{N}\left(\frac{r}{4}\right) \leq \frac{9}{16} < 1.$$

Suponhamos que a e b sejam ambos ímpares. Então, $a = 2m + 1$ e $b = 2n + 1$, com $m, n \in \mathbb{Z}$, tais que

$$a^2 + 19b^2 \equiv a^2 + 3b^2 \equiv 4m^2 + 4m + 1 + 3(4n^2 + 4n + 1) \equiv 1 + 3 \cdot 1 \equiv 4\,(mod\ 8).$$

Consequentemente, existe $q \in \mathbb{Z}$ tal que $a^2+19b^2 = 8q+4$. Assim, tomando $\eta = \frac{a-b\sqrt{-19}}{2}$ e $\kappa = q$ em $\mathbb{Z}[\omega]$, temos

$$\begin{aligned}
\eta\frac{\alpha}{\beta} - \kappa &= \left(\frac{a - b\sqrt{-19}}{2}\right)\cdot\left(\frac{a + b\sqrt{-19}}{8}\right) - q \\
&= \frac{a^2 + 19b^2}{8} - q \\
&= \frac{8q + 4 - 8q}{8} \\
&= \frac{4}{8} \\
&= \frac{1}{2} \neq 0.
\end{aligned}$$

Aplicando a função norma, obtemos

$$0 < \mathcal{N}\left(\eta\frac{\alpha}{\beta} - \kappa\right) = \mathcal{N}\left(\frac{1}{2}\right) \leq \frac{1}{4} < 1.$$

(iv) Seja $c \geq 5$. Como $(a, b, c) = 1$, logo existem $d, e, f \in \mathbb{Z}$ tais que $ad + be + ef = 1$. Assim, $\frac{ae-19bd}{c}$, daí existem $q, r \in \mathbb{Z}$ temos $ae-19bd = qc+r$ com $|r| \leq \frac{c}{2}$. Desse modo, podemos tomar $\eta = e + d\sqrt{-19}$ e $\kappa = q - f\sqrt{-19}$ em $\mathbb{Z}[\omega]$, temos

$$\begin{aligned}
\eta\frac{\alpha}{\beta} - \kappa &= (e + d\sqrt{-19})\left(\frac{a + b\sqrt{-19}}{c}\right) - (q - f\sqrt{-19}) \\
&= \frac{ae - 19bd + (ad + be)\sqrt{-19}}{c} - (q - f\sqrt{-19}) \\
&= \frac{ae - 19bd - qc + (ad + be + cf)\sqrt{-19}}{c} \\
&= \frac{qc + r - qc + (ad + be + cf)\sqrt{-19}}{c} \\
&= \frac{r + (ad + be + cf)\sqrt{-19}}{c} \\
&= \frac{r + \sqrt{-19}}{c}.
\end{aligned}$$

Mas, $c, r \in \mathbb{Z}$, então $\frac{r+\sqrt{-19}}{c} \in \mathbb{Z}[\omega]$. Aplicando a norma, obtemos

$$0 < \mathcal{N}\left(\eta\frac{\alpha}{\beta} - \kappa\right).$$

Basta mostrar que

$$1 > \mathcal{N}\left(\eta\frac{\alpha}{\beta} - \kappa\right).$$

Note que, se $c = 5$, então

$$\mathcal{N}\left(\eta\frac{\alpha}{\beta} - \kappa\right) = \mathcal{N}\left(\frac{r+\sqrt{-19}}{5}\right) \leq \frac{4+19}{25} = \frac{23}{25} < 1.$$

Se $c \geq 6$, então $|r| \leq \frac{c}{2}$, temos

$$\mathcal{N}\left(\eta\frac{\alpha}{\beta} - \kappa\right) = \mathcal{N}\left(\frac{r+\sqrt{-19}}{6}\right) \leq \frac{1}{4} + \frac{19}{6^2} = \frac{1}{4} + \frac{19}{36} = \frac{7}{9} < 1.$$

Portanto, está demonstrado que $\mathbb{Z}[\omega]$ é um anel principal.

□

Para $m \in \{-19, -43, -67, -163\}$ os corpos quadráticos complexos $\mathbb{Q}(\sqrt{m})$ também são Domínios de Ideias Principais que não são Domínios Euclidianos, demonstrado pelo matemático estadunidense Harold Mead Stark em [9], páginas 1 até 27. E uma solução em português para o caso $m = -43$ em [1], páginas 26 até 30.

Considerações Finais

Conclui-se que este trabalho ao longo de seu desenvolvimento, abordou diversos tópicos que geralmente não são encontrados nos livros básicos de Álgebra, então construímos uma base complementar aos cursos obrigatórios oferecidos durante a graduação e a partir daí, foi permitido introduzir conceitos e resultados importantes da Teoria dos Números Algébricos, conhecemos propriedades que colaboraram para a compreensão da estrutura algébrica dos corpos quadráticos.

Foi visto e demonstrado para quais valores de $m < 0$ o anel quadrático é euclidiano, em seguida, foram expostos dois exemplos de anéis quadráticos complexos que não são anéis fatoriais e indicamos referências para encontrar a demonstração para os casos $m > 0$, em que o anel quadrático real é euclidiano.

O trabalho serve de incentivo para se aprofundar ao estudo dos corpos ciclotômicos, reticulados, geometria algébrica, equações diofantinas entre outros.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] ANDRADE, .J.F. **Tópicos especiais em álgebra**, SBM 2013.

[2] CALLIOLI. C.A; DOMINGUES. H.H; COSTA. R.C.F. **Álgebra Linear e Aplicações**, 6º edição. São Paulo: ATUAL, 2003.

[3] COELHO. F.U; LOURENÇO. M.L **Um curso de Álgebra Linear**, 2º edição. São Paulo: EDUSP, 2010.

[4] DOMINGUES. H.H; IEZZI. G. **Álgebra moderna**, 4º edição. São Paulo, Atual, 2003.

[5] ENDLER, .O. **Teoria dos números algébricos**, IMPA, 2014.

[6] FRÖHLICH. A; TAYLOR. M.J. **Algebraic number theory**, Cambridge University Press, 1993.

[7] GARCIA. A; LEQUAIN. Y. **Elementos de álgebra**, 7ª edição. Rio de Janeiro, IMPA, 2022.

[8] GONÇALVES, .A. **Introdução à álgebra**, 5º edição. Rio de Janeiro, IMPA, 2011.

[9] HAROLD, M. **A complete Determination of the Complex Quadratic Fields of Class**, Michigan Math, 1967.

[10] HEFEZ. A; Villela. M.L.T. **Polinômios e equações algébricas**, SBM, 2012.

[11] JARVIS, P. **Algebraic Number Theory**, Springer, 2014.

[12] LIMA. E.L. **Álgebra Linear**, 1º edição. Rio de Janeiro, IMPA, 2014.

[13] MARTINEZ. F.B; MOREIRA. C.G; SALDANHA. N; TENGAN. E. **Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro**, Projeto Euclides, IMPA, 2013.

[14] NEUKIRCH. J. **Algebraic number theory, Springer**, 1992.

[15] OPPENHEIM, .A. **Quadratic fields with and without Euclid's algorithm**, Mathematische Annalen, vol. 109, p. 349–352, 1934.

[16] SHAFAREVICH. I.R; BOREVICH. Z.I. **Number theory**, Academic Press, 1986.

[17] STEWART. I; TALL. D. **Algebraic number theory and Fermat's last theorem**, 4rd edition. CRC Press, 2016.