**Universidade Estadual de Mato Grosso do Sul**

**Unidade Universitária de Nova Andradina**
**Curso de Matemática Licenciatura**

# Teoria dos Números Algébricos

**Pedro Henrique Justo Dos Santos**

Nova Andradina- MS

2017

# Teoria dos Números Algébricos

**Pedro Henrique Justo dos Santos**

Trabalho de Conclusão de Curso, do curso de Matemática - Licenciatura, no período noturno, como parte dos requisitos para a obtenção do grau de Licenciado em Matemática pela Universidade Estadual de Mato Grosso do Sul, sob a orientação do prof. Dr. Fábio Rodrigues Lucas.

Nova Andradina- MS
2017

# Teoria dos Números Algébricos

**Pedro Henrique Justo dos Santos**

Aprovado em 08/08/2017

---

Prof. Dr. Fábio Rodrigues Lucas - UEMS (Orientador)

---

Prof. Ms. Luiz Oreste Cauz - UEMS (Titular)

---

Prof. Dr. Oyran Silva Rayzaro - UEMS (Titular)

*"O talento desenvolve-se na solidão,*

*mas o caráter desenvolve-se*

*na agitação do mundo."*

(GOETHE)

# Dedicatória

*A Deus.*

*Aos meus pais.*

*Ao meu irmão, que venceu*

*a luta contra o crack.*

*Aos meus amigos.*

*A minha família.*

*A UEMS.*

*A minha psicóloga Débora.*

*A minha psiquiatra Mariana.*

*A mim mesmo.*

# Agradecimentos

Eu agradeço a Deus, a minha família e os meus amigos por incentivarem-me a realizar a graduação de Matemática e este trabalho.

Eu agradeço ao professor Fábio por ter aceitado esta proposta do trabalho, por ter me auxiliado a desenvolvê-lo e pela sua paciência para corrigí-lo.

Eu agradeço aos professores Luiz e Oyran por terem sugerido algumas referências e sugestões para o texto.

Finalmente, agradeço a todos aqueles que contribuíram para a elaboração deste trabalho.

# Resumo

Este trabalho tem por objetivo um estudo introdutório sobre a teoria dos números algébricos. Ele possui o intuito de investigar e estudar de que forma as propriedades algébricas simples, como anéis, corpos e ideais, são estendidas para estruturas algébricas mais gerais, como corpos de números e anéis dos inteiros. Assim, este trabalho tem por finalidade em explorar e compreender as noções de inteiros algébricos, traço e norma, norma de um ideal, discriminante, anéis de Dedekind e ideais fracionários. Para isto, o trabalho apresentará preliminarmente os resultados de estruturas algébricas básicas, módulos e módulos noetherianos.

Palavras-chave: Álgebra. Módulo. Elemento algébrico. Elemento inteiro. Norma. Traço. Discriminante. Anéis de Dedekind.

# Abstract

This paper has the objective to an introductory study about the algebriac numbers theory. It's intended to investigate and study in what way the simple algebraic properties, such as rings, fields and ideals, are extended to more general algebraic structures, such as number fields and rings of integers. Thus, this work aims to explore and understand the notions of algebraic integers, trace and norm, norm of an ideal, discriminant, Dedekind rings and fractional ideals. For this, the work will show preliminarily the results of basic algebraic structures, modules and Noetherian modules.

Key words: Algebra. Module. Algebraic element. Integer element. Trace. Norm. Discriminant. Dedekind Rings.

# Sumário

# Introdução

A álgebra, no início do século XIX, era vista basicamente como a aritmética simbólica. Trabalhava-se com letras da mesma forma como se faz com os números na aritmética, da mesma forma com as propriedades básicas de comutatividade da adição e multiplicação, associatividade e a distributiva da multiplicação em relação à adição. Essas propriedades que vieram da teoria dos números inteiros puderam ser generalizadas para outros conjuntos, e inclusive em estender para outras operações que seguissem a mesma lógica dessas propriedades. Como exemplos, tivemos por William Rowan Hamilton a teoria dos números quatérnios de números reais. Tivemos por Hermann Günther Grassmann conjuntos ordenados de n reais, chamados de hipercomplexos. Tivemos por Arthur Cayley a álgebra das matrizes. Em todos esses casos, a lei da comutatividade da multiplicação não é válida. Esses exemplos marcaram o início do desenvolvimento de álgebras com leis estruturais diferentes das usuais.

A humanidade é fascinada pelos números desde os milênios. Os pitagóricos estudaram os números naturais e suas propriedades, inclusive o Teorema de Pitágoras, apesar de ter origem geométrica, contribuiu a teoria dos números. Os helênicos ainda estudaram equações polinomiais que as soluções eram números fracionários, em particular, as chamadas de equações diofantinas que apresentavam soluções com números naturais. Os hindus desenvolveram trabalhos que abordavam os números negativos e com o zero. Os hindus ainda contribuiram com o desenvolvimento dos algarismos e suas notações. Os islâmicos no século VII, ao conquistarem Alexandria, bem como o norte da África e na Espanha, trouxeram enriquecimento matemático, que inclusive a palavra "álgebra" tem origem árabe. O italiano Girolamo Cardano no século XVI usou no seu livro *Ars Magna*[1] soluções negativas e imaginárias, usados da mesma maneira que os números complexos posteriormente.

[1] Arte Maior em latim

Já Pierre de Fermat no século XVII contribuiu na fundamentação da teoria dos números moderna. Muito dos seus teoremas enunciados foram mostrados como verdadeiros posteriormente. Um de seus teoremas, o mais famoso é conhecido como Último Teorema de Fermat, o qual afirma que não existem inteiros positivos $x, y, z$ tais que $x^n + y^n = z^n$, para todo $n$ inteiro positivo maior ou igual a 3. No livro que Fermat enunciou o teorema, afirma de ter encontrado uma demonstração admirável para este fato, mas que ele ainda afirmava que "margem do rio era tão pequena"que não dava para caber a demonstração. Muitos matemáticos se prontificaram a demonstrá-lo sem sucesso, exceto em casos particulares. Ainda, a busca da demonstração foi incentivada depois de Paul Wolfskehl ter legado em 1908 uma quantia significativa para a Academia de Ciências de Göttingen para que fosse premiado para a primeira pessoa que demonstrasse completamente o Último Teorema de Fermat.

A repercussão da busca pela demonstração do Último Teorema de Fermat impulsionou outros estudos matemáticos. O Último Teorema de Fermat teve origem na área de teoria dos números inteiros e a prova da conjectura partiu para outro ramo de estudo, que é a teoria dos números algébricos. No século XIX o desenvolvimento da teoria da álgebra amadureceu de tal forma que se tornou aplicável a teoria dos números. Por este motivo que os estudiosos da teoria dos números não se interessaram no Último Teorema de Fermat.

Matemáticos como Ernst Eduard Kummer, Carl Friedrich Gauss e Leonard Euler apresentaram números particulares dos números complexos que são as raízes de um polinômio de coeficientes inteiros. Esses números eram ditos algébricos, em particular, se o polinômio tem coeficiente dominante ou principal igual a 1 é dito inteiro algébrico ou simplesmente inteiro. Gabriel Lamé, Joseph Liouville tentaram demonstrar o Último Teorema de Fermat.

Podemos salientar que grande parte da teoria dos números inteiros pode ser expressa em termos dos números inteiros algébricos. David Hilbert deu grandes contribuições para a teoria dos números. Assim, a teoria dos números algébricos atualmente é um ramo próspero e importante da matemática, com métodos elaborados e intuitivos, que não tem aplicações somente na teoria dos números, mas também na teoria dos grupos, na geometria algébrica, na topologia e na análise. Foram essas relações importantes que levaram à prova final do Último Teorema de Fermat, que foi estabelecida definitivamente como um teorema e não uma mera conjectura. A demonstração do Último Teorema de Fermat foi possível pela utilização

de vários conceitos desenvolvidos através dos tempos, muitos desses posteriores a Fermat, o que leva a crença de que, na verdade, quando Fermat pensou em ter vislumbrado a prova, ele provavelmente cometera algum erro, engano ou equívoco em seu raciocínio, ou, caso contrário, ele haveria realmente tido um insight impressionante que não foi concebido por nenhum outro matemático nos 350 anos seguintes.

No Capítulo 1 iremos apresentar as estruturas algébricas básicas e suas propriedades, para prosseguir com módulos e suas propriedades. No Capítulo 2 iremos expor alguns resultados da teoria de Galois, com uma apresentação breve sem focar muito nas suas demonstrações. No Capítulo 3 iremos tratar da teoria dos números algébricos, bem como as suas propriedades. Iremos tratar das noções de inteiros algébricos, traço, norma, norma de um ideal, discriminante, anéis de Dedekind e ideais fracionários.

# Capítulo 1

# Estruturas Algébricas e Módulos

Nesta seção apresentaremos as definições de grupos, anéis, corpos, ideais, módulos e módulos noetherianos e, algumas de suas principais propriedades. Veremos também alguns resultados clássicos da álgebra.

## 1.1 Anéis e Corpos

**Definição 1.1.** *Um conjunto não vazio $G$ e uma operação $*$ sobre $G$ é chamado de* ***grupo*** *se, e somente se essa operação satisfaz as seguintes propriedades:*

1. *$(a * b) * c = a * (b * c)$ para todo $a, b, c \in G$ (associativa);*
2. *Para todo $a \in G$, existe $e \in G$ tal que $a * e = e * a = a$ (existência do elemento neutro);*
3. *Para todo $a \in G$, existe $a' \in G$ tal que $a * a' = a' * a = e$ (existência dos elementos simétricos).*

**Observação 1.1.** *Se, além disso a operação $*$ for comutativa, isto é, $a * b = b * a$, para todo $a, b \in G$ o grupo é chamado de* ***comutativo*** *ou* ***abeliano****.*

**Definição 1.2.** *Um conjunto $A$ não vazio e um par de operações $+$ (adição) e $\cdot$ (multiplicação) sobre $A$ é chamado de* ***anel*** *se $A$ é um grupo abeliano em relação à operação $+$ e se a operação $\cdot$ satisfaz:*

1. *$(ab)c = a(bc)$, para todo $a, b, c \in A$ (associativa);*

2. $a(b+c) = ab + bc$ *e* $(a+b)c = ac + bc$*, para todo* $a, b, c \in A$ *(distributiva).*

*Nas condições acima, admitimos que* $0$ *seja o elemento neutro da operação* $+$*.*

**Definição 1.3.** *Nas condições da Definição (1.2) ainda temos que:*

1. *Quando a multiplicação do anel* $A$ *satisfaz* $ab = ba$ *para todo* $a, b \in A$*, dizemos que* $A$ *é um* ***anel comutativo****;*

2. *A multiplicação pode admitir um elemento neutro, isto é, existe* $1_A \in A$*,* $1_A \neq 0_A$ *tal que* $a1_A = 1_A a = a$*, para todo* $a \in A$*. Neste caso, dizemos que* $A$ *é um* ***anel com unidade****;*

3. *Um anel cuja multiplicação é comutativa e que possui unidade é chamado de* ***anel comutativo com unidade****.*

**Definição 1.4.** *Um subconjunto não vazio* $B$ *de um anel* $A$ *é um* ***subanel*** *de* $A$ *se* $B$ *é um anel com as mesmas operações de* $A$ *porém restritas aos elementos de* $B$*.*

**Definição 1.5.** *Seja* $A$ *um anel comutativo com unidade:*

1. *Dizemos que um elemento não nulo* $a \in A$ *é um* ***divisor próprio de zero*** *se existe um elemento não nulo* $b \in A$ *tal que* $ab = ba = 0_A$*.*

2. *Quando* $A$ *não possui divisores próprios de zero dizemos que* $A$ *é um* ***anel de integridade*** *ou* ***domínio de integridade*** *ou simplesmente de* ***domínio****.*

**Definição 1.6.** *Seja* $A$ *um anel. Consideremos o subconjunto de* $\mathbb{N}^*$*:*

$$S = \{n \in \mathbb{N}^* \mid na = 0_A, \textit{para todo } a \in A\}.$$

*Como* $S \subset \mathbb{N}^*$*, há apenas duas possibilidades:*

1. *Se* $S = \varnothing$*, então dizemos que o anel* $A$ *tem* ***característica zero****;*

2. *Se* $S \neq \varnothing$*, então existe o mínimo de* $S$*, o número* $\min\{S\}$ *pelo Princípio do Menor Número Inteiro. Logo, dizemos que o anel* $A$ *tem* ***característica*** $\min\{S\}$*.*

**Definição 1.7.** *Dizemos que um anel comutativo com unidade $\mathbb{K}$ é um* ***corpo*** *se todo elemento não nulo de $\mathbb{K}$ possui inverso em relação à multiplicação, isto é, para todo $a \in \mathbb{K} - 0$, existe $b \in \mathbb{K}$ tal que $ab = 1$.*

**Definição 1.8.** *Um subconjunto não vazio $\mathbb{L} \subset \mathbb{K}$ é chamado de* ***subcorpo*** *de $\mathbb{K}$ se $\mathbb{L}$ é um corpo com as operações de $\mathbb{K}$ restritas a $\mathbb{L}$.*

**Definição 1.9.** *Seja $A$ um anel de integridade. O corpo $\mathbb{K}$ é chamado de* ***corpo de frações*** *do anel de integridade de $A$ quando ele pode ser definido da seguinte forma:*

$$\mathbb{K} = \left\{ \frac{a}{b} \;\middle|\; (a, b) \in \mathbb{A} \times \mathbb{A}^* \right\}$$

**Definição 1.10.** *Seja $A$ um anel comutativo. Um subconjunto $\mathfrak{a} \subset A$, $\mathfrak{a} \neq \varnothing$ é chamado de* ***ideal*** *em $A$ se, para quaisquer $x, y \in \mathfrak{a}$ e para qualquer $a \in A$, as seguintes condições são satisfeitas:*

1. *$x - y \in \mathfrak{a}$;*
2. *$ax \in \mathfrak{a}$.*

**Definição 1.11.** *Seja $A$ um anel comutativo.*

1. *Tomemos $a_1, a_2, \ldots, a_n \in A$. O subconjunto $\langle a_1, a_2, \ldots, a_n \rangle$ de $A$ da forma*

$$\langle a_1, a_2, \ldots, a_n \rangle = \{x_1 a_1 + x_2 a_2 + \ldots + x_n a_n \mid x_1, x_2, \ldots, x_n \in A\}$$

   *que é um ideal, é chamado de* ***ideal gerado*** *por $a_1, a_2, \ldots, a_n$.*

2. *Um ideal $\mathfrak{a}$ gerado por um só elemento $a \in A$, isto é, $\mathfrak{a} = \langle a \rangle = \{ax \mid x \in A\}$, é chamado de* ***ideal principal*** *gerado por $a$.*

3. *Se para todo ideal do anel $A$ é principal, então dizemos que $A$ é um* ***anel principal****.*

4. *Em particular, se $A$ é um domínio de integridade onde todo ideal é principal, dizemos que $A$ é um* ***domínio principal****.*

**Definição 1.12.** *Seja $A$ um anel:*

1. *Dizemos que um ideal* $\mathfrak{p}$ *de* $A$ *é um* ***ideal primo*** *se* $\mathfrak{p} \neq A$ *e se para todo* $a, b \in A$ *tal que* $ab \in \mathfrak{p}$*, então* $a \in \mathfrak{p}$ *ou* $b \in \mathfrak{p}$*;*

2. *Dizemos que um ideal* $\mathfrak{m}$ *é um* ***ideal maximal*** *se* $\mathfrak{m} \neq A$ *e se os únicos ideais em* $A$ *que contém* $\mathfrak{m}$ *são o próprio* $\mathfrak{m}$ *e* $A$*.*

**Definição 1.13.** *Sejam* $A$ *um anel e* $\mathfrak{a}$ *um ideal de* $A$*:*

1. *Chamamos de* ***classe de equivalência*** *do elemento* $a \in A$ *em relação ao ideal* $\mathfrak{a}$ *o subconjunto* $\overline{a} = a + \mathfrak{a} = \{a + x \mid x \in \mathfrak{a}\}$*.*

2. *Dados* $a, b \in A$*, dizemos que* $a$ *é* ***côngruo*** $a$ $b$ *módulo* $\mathfrak{a}$ *se* $a - b \in \mathfrak{a}$*, e denotamos por* $a \equiv b (\mathrm{mod} \mathfrak{a})$*.*

**Definição 1.14.** *Sejam* $A$ *um anel e* $\mathfrak{a}$ *um ideal. Considerando* $A/\mathfrak{a}$ *o conjunto das classes de equivalência dos elementos de* $A$*, definimos as seguintes operações de soma e produto entre os seus elementos:*

$$\overline{a} + \overline{b} = \overline{a + b}, \text{ isto é, } (a + \mathfrak{a}) + (b + \mathfrak{a}) = (a + b) + \mathfrak{a};$$

$$\overline{a}\overline{b} = \overline{ab}, \text{ isto é, } (a + \mathfrak{a})(b + \mathfrak{a}) = (ab) + \mathfrak{a}.$$

**Definição 1.15.** *Sejam* $A$ *um anel e* $\mathfrak{a}$ *um ideal. O conjunto* $A/\mathfrak{a}$ *munido das duas operações definidas acima é um anel chamado de* ***anel quociente*** *de* $A$ *pelo ideal* $\mathfrak{a}$*. Os ideais de* $A/\mathfrak{a}$ *são da forma* $\mathfrak{a}'/\mathfrak{a}$*, onde* $\mathfrak{a}'$ *pertence ao conjunto dos ideais de* $A$ *que contém* $\mathfrak{a}$*.*

**Teorema 1.1** ([2], p.169)**.** *Seja* $A$ *um anel comutativo com unidade e* $\mathfrak{p}$ *um ideal de* $A$*. Então* $\mathfrak{p}$ *é um ideal primo se, e somente se* $A/\mathfrak{p}$ *é um domínio;*

*Demonstração.* ($\Rightarrow$) Seja $\mathfrak{p}$ um ideal primo. Suponhamos que $(a + \mathfrak{p})(b + \mathfrak{p}) = 0 + \mathfrak{p}$ para $a, b \in A$. Como $(a + \mathfrak{p})(b + \mathfrak{p}) = ab + \mathfrak{p} = 0 + \mathfrak{p}$, segue que $ab \in \mathfrak{p}$. Como $\mathfrak{p}$ é um ideal primo, segue que $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$. Logo, $a + \mathfrak{p} = 0 + \mathfrak{p}$ ou $b + \mathfrak{p} = 0 + \mathfrak{p}$. Portanto, $A/\mathfrak{p}$ é um domínio.

($\Leftarrow$) Sejam $A/\mathfrak{p}$ um domínio e $a, b \in A$ tais que $ab \in \mathfrak{p}$. Temos que $(a + \mathfrak{p})(b + \mathfrak{p}) = ab + \mathfrak{p} = 0 + \mathfrak{p}$ pois $ab \in \mathfrak{p}$. Como $A/\mathfrak{p}$ é um domínio, segue que $a + \mathfrak{p} = 0 + \mathfrak{p}$ ou $b + \mathfrak{p} = 0 + \mathfrak{p}$. Logo, $x \in \mathfrak{p}$ ou $y \in \mathfrak{p}$. Portanto, $\mathfrak{p}$ é um ideal primo. □

**Teorema 1.2** ([2], p.169)**.** *Sejam $A$ um anel comutativo com unidade e $\mathfrak{m}$ um ideal de $A$. Então $\mathfrak{m}$ é um ideal maximal se, e somente se $A/\mathfrak{m}$ é um corpo.*

*Demonstração.* ($\Rightarrow$) Seja $\mathfrak{m}$ um ideal maximal. Temos que $A/\mathfrak{m}$ é um domínio. Falta mostrar que todo elemento não nulo de $A/\mathfrak{m}$ é inversível.

Seja $a \in A$ tal que $a+\mathfrak{m} \neq 0+\mathfrak{m}$. Logo, temos que $a \notin \mathfrak{m}$. Assim, $\mathfrak{m} \subsetneq \mathfrak{m}+\langle a \rangle = A$ pois $\mathfrak{m}$ é um ideal maximal. Logo, $1 = m + ax$ com $m \in \mathfrak{m}$ e $x \in A - \mathfrak{m}, x \neq 0$. Desta forma, como $1-ax = m \in \mathfrak{m}$, segue que $1+\mathfrak{m} = ax+\mathfrak{m} = (a+\mathfrak{m})(x+\mathfrak{m})$. Portanto, $a+\mathfrak{m}$ é inversível e, desta forma, $A/\mathfrak{m}$ é um corpo.

($\Leftarrow$) Seja $A/\mathfrak{m}$ um corpo. Suponhamos que existe um ideal $\mathfrak{a} \subset A$ tal que $\mathfrak{m} \subset \mathfrak{a} \subset A$. Seja $a \in \mathfrak{a} - \mathfrak{m}$. Como $a \notin \mathfrak{m}$, segue que $a + \mathfrak{m} \neq 0 + \mathfrak{m}$.

Como $A/\mathfrak{m}$ é um corpo e $a+\mathfrak{m} \neq 0+\mathfrak{m}$, então existe $b \in A-\mathfrak{m}$ tal que $(a+\mathfrak{m})(b+\mathfrak{m}) = 1 + \mathfrak{m}$. Logo, $(a + \mathfrak{m})(b + \mathfrak{m}) = ab + \mathfrak{m} = 1 + \mathfrak{m}$. Desta forma, $ab - 1 \in \mathfrak{m}$.

Como $a \in \mathfrak{a}$, segue que $ab \in \mathfrak{a}$ e assim $1 \in \mathfrak{a}$. Portanto, $\mathfrak{a} = A$, o que implica que $\mathfrak{m}$ é maximal. □

**Definição 1.16.** *Sejam $A$ e $B$ dois anéis. Uma aplicação $\phi : A \to B$ é um* ***homomorfismo*** *de anéis de $A$ em $B$ se satizfaz as seguintes condições:*

1. *$\phi(x + y) = \phi(x) + \phi(y)$, para todo $x, y \in A$;*
2. *$\phi(xy) = \phi(x)\phi(y)$, para todo $x, y \in A$.*

**Definição 1.17.**

1. *Chamamos de* ***monomorfismo*** *um homomorfismo injetor,* ***epimorfismo*** *um homomorfismo sobrejetor e* ***isomorfismo*** *um homomorfismo bijetor. Quando um homomorfismo de um anel $A$ nele próprio é chamado de* ***endomorfismo****. Já um isomorfismo de um anel $A$ sobre si próprio é chamado de* ***automorfismo****.*
2. *O* ***núcleo do homomorfismo*** *$\phi : A \to B$, denotado por $\mathrm{Ker}(\phi)$, é o subconjunto $\mathrm{Ker}(\phi) \subset A$ definido como $\mathrm{Ker}(\phi) = \{x \in A \mid \phi(x) = 0_B\}$.*

**Teorema 1.3** ([2], pp.147-148,157,166)**.** *Se $A$ e $B$ são anéis, $x$ e $y$ são elementos de $A$ e $\phi : A \to B$ um homomorfismo, então:*

1. *$\phi(0_A) = 0_B$, $\phi(-x) = -\phi(x)$ e $\phi(x - y) = \phi(x) - \phi(y)$;*

2. $\phi$ *é um monomorfismo, e somente se* $\mathrm{Ker}(\phi) = \{0\}$*;*

3. *Se* $\phi$ *é um epimorfismo e* $A$ *possui unidade, então* $B$ *também possui unidade e* $\phi(1_A) = 1_B$*;*

4. *Se* $\phi$ *é um epimorfismo, existe unidade em* $A$ *e* $x$ *é inversível, então* $\phi(x)$ *também é inversível e* $\phi(x^{-1}) = \big(\phi(x)\big)^{-1}$*;*

5. $\mathrm{Im}(\phi)$ *é um subanel de* $B$*;*

6. $\mathrm{Ker}(\phi)$ *é um ideal de* $A$*;*

7. *Os anéis* $A/\mathrm{Ker}(\phi)$ *e* $\mathrm{Im}(\phi)$ *são isomorfos* (Teorema do Isomorfismo de Anéis).

## 1.2 Módulos

**Definição 1.18.** *Seja* $A$ *um anel. Um conjunto não vazio* $M$ *é chamado de* $A$-***módulo*** *se* $M$ *é um grupo abeliano com relação à operação* $+$ *e munido de uma aplicação* $\phi : A \times M \to M$*, definida por* $\phi(a, m) = am$*, que satisfaz para todo* $a, b \in A$ *e para todo* $m, n \in M$*:*

1. $a(m + n) = am + an$*;*

2. $(a + b)m = am + bm$*;*

3. $(ab)m = a(bm)$*;*

4. $1m = m$*.*

**Definição 1.19.** *Sejam* $A$ *um anel comutativo com unidade e* $M$ *um* $A$*-módulo. Um subconjunto* $N \subset M$ *não vazio é um* $A$-***submódulo*** *de* $M$ *se, com as operações herdadas de* $M$*,* $N$ *é também um* $A$*-módulo.*

**Definição 1.20.** *Dado um* $A$*-módulo* $M$ *e um* $A$*-submódulo* $N$ *podemos definir o* ***módulo quociente*** $M/N$ *da mesma forma como o anel quociente, onde* $a(m+N) = am+N$ *para todo* $a \in A$ *e para todo* $m \in M$*.*

**Definição 1.21.** *Um* $A$*-módulo* $M$ *é chamado de* ***finitamente gerado*** *se existirem elementos* $x_1, x_2, \ldots, x_n \in M$ *tais que todo* $m \in M$ *é da forma* $m = \sum_{i=1}^{n} a_i x_i$*, com* $a_i \in A$*, para todo* $i = 1, 2, \ldots, n$*. Neste caso, dizemos que* $x_1, x_2, \ldots, x_n$ *formam um sistema de geradores de* $M$*.*

**Definição 1.22.** *Sejam $A$ um anel, $M$ um $A$-módulo e $x_1, x_2, \ldots, x_n \in M$. Dizemos que $\{x_1, x_2, \ldots, x_n\}$ é uma* ***base*** *de $M$ se $x_1, x_2, \ldots, x_n$ formam um sistema de geradores de $M$ e se forem linearmente independentes* (LI)*, ou seja, se existirem $a_1, a_2, \ldots, a_n \in A$ tais que $m = \sum_{i=1}^{n} a_i x_i = 0$, então $a_i = 0$, para todo $i = 1, 2, \ldots, n$. Em particular, se o anel $A$ é o anel $\mathbb{Z}$, então dizemos que $\{x_1, x_2, \ldots, x_n\}$ é uma $\mathbb{Z}$-**base**.*

**Definição 1.23.** *Um $A$-módulo que possui uma base é chamado de $A$-**módulo livre**.*

**Definição 1.24.** *Seja $M$ um $A$-módulo livre. O* ***posto*** *de $M$ é a quantidade $n$ de elementos que formam sua base.*

**Teorema 1.4** ([5], p.21)**.** *Sejam $A$ um anel principal, $M$ um $A$-módulo livre de posto $n$ e $N \neq 0$ um submódulo de $M$. Então:*

1. *$N$ é livre de posto $q$, $0 \leq q \leq n$;*
2. *Existe uma base $\{e_1, e_2, \ldots, e_n\}$ de $M$ e elementos não nulos $a_1$, $a_2$, ..., $a_n \in A$ tais que $\{a_1 e_1, a_2 e_2, \ldots, a_q e_q\}$ é uma base de $N$ e tal que $a_i | a_{i+1}$, onde $1 \leq i \leq q-1$.*

**Definição 1.25.** *Sejam $A$ um anel e $M$, $N$ dois $A$-módulos. Dizemos que uma aplicação $f : M \to N$ é um* ***homomorfismo de $A$-módulos*** *se, para todo $x, y \in M$ e $a \in A$, satisfazem as seguintes condições:*

1. *$f(x + y) = f(x) + f(y)$;*
2. *$f(ax) = af(x)$,*

*Se além disso, a aplicação $f$ for injetiva, dizemos que $f$ é um* ***monomorfismo*** *de $A$-módulos; $f$ sobrejetiva é um* ***epimorfismo*** *de $A$-módulos; $f$ bijetiva é um* ***isomorfismo*** *de $A$-módulos. Quando a aplicação $f$ leva de $M$ a si mesmo é chamado de* ***endomorfismo*** *de $A$-módulos. Ainda, se a aplicação $f$ leva de $M$ a si mesmo for bijetiva, dizemos que $f$ é um* ***automorfismo*** *de $A$-módulos.*

*O* ***núcleo*** *do homomorfismo $f$ de $A$-módulos, denotado por* $\mathrm{Ker}(f)$ *é o subconjunto* $\mathrm{Ker}(f) \subset M$ *definido como* $\mathrm{Ker}(f) = \{x \in M \mid f(x) = 0_N\}$.

**Proposição 1.1** ([4], p.21)**.** *Sejam $A$ um anel, $M, N$ dois $A$-módulos e $f : M \to N$ um homomorfismo. Então:*

1. $\mathrm{Im}(f)$ *é um submódulo de* $N$*;*

2. $\mathrm{Ker}(f)$ *é um submódulo de* $M$*;*

3. $f$ *é injetiva se, e somente se* $\mathrm{Ker}(f) = \{0_N\}$.

**Teorema 1.5** ([4], p.21)**.** (Teorema do Isomorfismo de Módulos). *Se $A$ é um anel, $M$, $N$ são dois $A$-módulos e $f : M \to N$ um homomorfismo de $A$-módulos, então os módulos $M/\mathrm{Ker}(f)$ e $\mathrm{Im}(f)$ são isomorfos.*

## 1.3 Módulos Noetherianos

**Definição 1.26.** *Sejam $M$ um $A$-módulo e $I_1 \subset I_2 \subset \ldots \subset I_n \subset \ldots$ uma sequência crescente de $A$-submódulos de $M$. Dizemos que esta é uma* ***sequência crescente estacionária*** *se existir $n_0 \in \mathbb{N}$ tal que $I_n = I_{n_0}$, para todo $n \geq n_0$.*

**Observação 1.2.** *A definição é análoga para* ***sequência decrescente estacionária****.*

**Definição 1.27.** *Sejam $A$ um anel e $M$ um $A$-módulo. Dizemos que $M$ é um $A$-****módulo noetheriano*** *se satisfaz pelo menos uma das seguintes condições:*

1. *Todo conjunto não vazio de $A$-submódulos de $M$ contém um elemento maximal;*

2. *Toda sequência crescente de $A$-submódulos de $M$ é estacionária;*

3. *Todo $A$-submódulo de $M$ é finitamente gerado.*

*Dizemos que $A$ é um* ***anel noetheriano*** *se $A$ for um $A$-módulo noetheriano.*

**Proposição 1.2** ([5], pp.20, 46)**.** *Todo anel principal $A$ é noetheriano.*

*Demonstração.* Consideramos uma sequência crescente de $A$-submódulos de $M$,

$$I_1 \subset I_2 \subset I_3 \subset \ldots \subset I_n \subset \ldots \ .$$

Como $A$ é um anel principal segue que todos os ideais de $A$ são principais e como os submódulos de $A$ são exatamente os ideais de $A$, segue que os submódulos de $A$ são principais. Seja $I = \bigcup_{n\in\mathbb{N}} I_n$. Temos que $I$ é um ideal de $A$ pois $I_j$ são ideais de $A$ para todo $j \in \mathbb{N}$, onde esses ideais são subconjuntos sequentes. Agora, notemos que $I_n \subset I = \langle a\rangle$, para todo $n \in \mathbb{N}$ e $a \in I_{n_0}$, para algum $n_0 \in \mathbb{N}$, pois $a \in \langle a\rangle = I = \bigcup_{n\in\mathbb{N}} I_n$. Como $a \in I_{n_0}$ e $a \in \langle a\rangle$, segue que $I = \langle a\rangle \subset I_{n_0}$. Portanto, $I = I_{n_0}$. Assim, existe $n_0 \in \mathbb{N}$ tal que $I_n = I_{n_0}$, para todo $n \geq n_0$.

□

**Proposição 1.3** ([5], p.46)**.** *Se $A$ é um anel, $M$ é um $A$-módulo e $N$ um submódulo de $M$, então as seguintes proposições são equivalentes:*

1. *$M$ é um $A$-módulo noetheriano;*

2. *$N$ e $M/N$ são $A$-módulos noetherianos.*

*Demonstração.* Suponhamos que $M$ é noetheriano. Seja $(M_n)_{n\geq 0}$ uma sequência crescente de $A$-submódulos de $N$. Assim, $(M_n)_{n\geq 0}$ também é uma sequência crescente de $A$-submódulos de $M$. Como $M$ é noetheriano, segue que $(M_n)_{n\geq 0}$ é estacionária. Portanto $N$ é noetheriano.

Para mostrar que $M/N$ é noetheriano, consideremos os conjuntos

$$S = \{\text{submódulos de } M \text{ que contém } N\} \text{ e } T = \{\text{submódulos de } M/N\}$$

Temos que a aplicação $\varphi : S \to T$ definida por $\varphi(L) = L/N$ com $L \in S$, é uma bijeção de $S$ em $T$, pois:

1. Para todo $L_1, L_2 \in S$ temos $\varphi(L_1) = \varphi(L_2) \Rightarrow L_1/N = L_2/N \Rightarrow a(L_1 + N) = a(L_2 + N) \Rightarrow L_1 + N = L_2 + N \Rightarrow L_1 = L_2$, ou seja, $\varphi$ é injetiva;

2. Como $L \in S$, então $L$ é um $A$-submódulo de $M$ que contém $N$ e daí para todo $y = L/N \in T$, existe $x = L \in S \mid \varphi(x) = y \Rightarrow \varphi(L) = L/N$, ou seja, $\varphi$ é sobrejetiva.

Assim, se $(M_n)_{n\geq 0}$ é uma sequência crescente de $A$-submódulos de $M/N$, então $\left(\varphi^{-1}(M_n)\right)_{n\geq 0}$ também é uma sequência crescente de $A$-submódulos de $M$. Como $M$ é noetheriano, segue que $\left(\varphi^{-1}(M_n)\right)_{n\geq 0}$ é estacionária e, portanto $(M_n)_{n\geq 0}$ é estacionária. Assim, $M/N$ é noetheriano.

Agora, suponhamos pela recíproca que $M/N$ e $N$ são noetherianos. Seja $(M_n)_{n\geq 0}$ uma sequência crescente de $A$-submódulos de $M$. Assim, $(N\cap M_n)_{n\geq 0}$ é uma sequência crescente de $A$-submódulos de $N$. Como $N$ é noetheriano, segue que $(N\cap M_n)_{n\geq 0}$ é estacionária, ou seja, existe $k\in\mathbb{L}$ tal que $M_n\cap N = M_{n+1}\cap N$ e $M_n/N = M_{n+1}/N$, para todo $n\geq k$.

Sabemos que $M_n\subseteq M_{n+1}$, para todo $n\geq k$. Se $x\in M_{n+1}$, então existe $y\in M_n$ tal que $x+M_1 = y+N$. Assim, $x-y\in N\cap M_{n+1} = N\cap M_n$. Logo, $x-y\in M_n$ e como $y\in M_n$ segue que $x\in M_n$. Portanto, $M_n = M_{n+1}$, para todo $n\geq k$ e assim $M$ é noetheriano.

□

**Corolário 1.1** ([5], p.47)**.** *Se $M_1, M_2, \ldots, M_n$ são $A$-módulos noetherianos, então o produto $\prod_{i=1}^{n} M_i$ é um $A$-módulo noetheriano.*

*Demonstração.* Vamos fazer a prova por indução sobre $n$.

**(i)** Para $n=2$, identificamos $M_1\simeq M_1\times\{0\}\subseteq M_1\times M_2$ e definimos a função $\varphi: M_1\times M_2\to M_2$ tal que $\varphi(0,y) = y$. Como $\varphi$ é um epimorfismo e pelo Teorema (1.4)$queKer(\varphi)$ é um $A$-submódulo de $M_1\times M_2$, segue pelo Teorema (1.5) que $\dfrac{M_1\times M_2}{\mathrm{Ker}(\varphi)}\simeq M_2$, onde $\mathrm{Ker}(\varphi) = M_1\times\{0\}$. Como $M_2$ é noetheriano, segue pela Proposição (1.3) que $\dfrac{M_1\times M_2}{M_1\times\{0\}}$ é noetheriano e pela Proposição (1.3), segue que $M_1\times M_2$ também é noetheriano.

**(ii)** Suponhamos que o produto $\prod_{i=1}^{n-1} M_i$ é noetheriano para $n-1\geq 2$. Então, como $M_n$ é noetheriano, segue do caso **(i)** que $M_n\times\prod_{i=1}^{n-1} M_i = \prod_{i=1}^{n} M_i$ é um $A$-módulo noetheriano.

□

**Observação 1.3.** *Do Corolário (1.1) concluímos que para qualquer anel noetheriano $A$, o $A$-módulo $\prod_{i=1}^{n} A = A^n$ é noetheriano.*

**Corolário 1.2** ([5], p.47)**.** *Se $A$ é um anel noetheriano e $M$ é um $A$-módulo finitamente gerado, então $M$ é um $A$-módulo noetheriano.*

*Demonstração.* Seja $\{e_1, e_2, \ldots, e_n\}$ um conjunto de geradores do $A$-módulo $M$. Temos que a aplicação $\varphi: A^n\to M$ definida por $\varphi(a_1, a_2, \ldots, a_n) = \sum_{i=1}^{n} a_i e_i$ é um epimorfismo, pois:

1. Para todo $(a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n) \in A^n$, para $i = 1, 2, \ldots, n$, temos

$$\begin{aligned}
\varphi\big((a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n)\big) &= \varphi(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \\
&= \sum_{i=1}^{n} (a_i + b_i)e_i \\
&= \sum_{i=1}^{n} (a_i e_i + b_i e_i) \\
&= \sum_{i=1}^{n} a_i e_i + \sum_{i=1}^{n} b_i e_i \\
&= \varphi(a_1, a_2, \ldots, a_n) + \varphi(b_1, b_2, \ldots, b_n);
\end{aligned}$$

2. Para todo $x \in A$ e $(a_1, a_2, \ldots, a_n) \in A^n$, para $i = 1, 2, \ldots, n$, temos

$$\begin{aligned}
\varphi\big(x(a_1, a_2, \ldots, a_n)\big) &= \varphi(xa_1, xa_2, \ldots, xa_n) \\
&= \sum_{i=1}^{n} (xa_i)e_i \\
&= \sum_{i=1}^{n} x(a_i e_i) \\
&= x \sum_{i=1}^{n} a_i e_i \\
&= x\varphi(a_1, a_2, \ldots, a_n);
\end{aligned}$$

3. É imediato que $\varphi$ é sobrejetiva.

Assim, pelos Teoremas (1.4) e (1.5) (Teorema do Isomorfismo de Módulos), temos que $\dfrac{A^n}{\mathrm{Ker}(\varphi)} \simeq M$. Como $A$ é noetheriano, pelo Corolário (1.1) segue que $A^n$ é noetheriano. Pela Proposição (1.3) segue que $M$ é um $A$-módulo noetheriano. □

**Observação 1.4.** *Vimos no Corolário (1.2) que se $A$ for um anel noetheriano, então todo submódulo de qualquer $A$-módulo finitamente gerado também o será. Porém, quando $A$ não for noetheriano, isso não ocorre. De fato, considerando o próprio $A$ como $A$-módulo temos que $A$ possui submódulos (ideais) não finitamente gerados.*

**Proposição 1.4** ([5], p.47)**.** *Se $A$ é um anel, $B$ é um subanel de $A$ e $\mathfrak{p}$ é um ideal primo de $A$, então $\mathfrak{p} \cap B$ é um ideal primo de $B$*

*Demonstração.* Consideremos a aplicação $\varphi : B \xrightarrow{i} A \xrightarrow{\pi} A/\mathfrak{p}$, onde $i$ é a inclusão e $\pi$ é a projeção. A função $\varphi = \pi \circ i$ é um homomorfismo, pois $\pi$ e $i$ são homomorfos. Além disso, $\text{Ker}(\varphi) = \mathfrak{p} \cap B$, já que $\varphi(x) = (\pi \circ i)(x) = \pi(x) = x + \mathfrak{p}$ e $\varphi(x) = \bar{0}$ se, e somente se $x \in \mathfrak{p} \cap B$. Portanto, pelo Teorema (1.3) (Teorema do Isomorfismo de Anéis), temos $B/\mathfrak{p} \cap B \simeq \text{Im}(\varphi) \subset a/\mathfrak{p}$. Como $A/\mathfrak{p}$ é um domínio, segue que $B/\mathfrak{p} \cap B$ é um domínio. Portanto, pelo Teorema (**??**) $\mathfrak{p} \cap B$ é um ideal primo de $B$.

□

**Proposição 1.5** ([5], p. 48)**.** *Se um ideal primo $\mathfrak{p}$ de um anel $A$ contém um produto $\prod_{i=1}^{n} \mathfrak{a}_i$ de ideais, então $\mathfrak{p}$ contém pelo menos um dos ideais $\mathfrak{a}_i$, para $1 \leq i \leq n$.*

*Demonstração.* Suponhamos por absurdo que $\mathfrak{a}_i \nsubseteq \mathfrak{p}$, para todo $1 \leq i \leq n$. Então existe $\alpha_i \in \mathfrak{a}_i$ e $\alpha_i \notin \mathfrak{p}$. Como $\mathfrak{p}$ é primo, segue que $\prod_{i=1}^{n} \alpha_i \notin \mathfrak{p}$. Mas, isto acarreta em $\prod_{i=1}^{n} \alpha_i \in \prod_{i=1}^{n} \mathfrak{a}_i \subset \mathfrak{p}$, o que é um absurdo. Portanto, $\mathfrak{p}$ contém $\mathfrak{a}_i$, para algum $1 \leq i \leq n$. □

**Proposição 1.6** ([5], p.48)**.** *Em um anel noetheriano $A$ todo ideal de $A$ contém um produto de ideais primos de $A$. Em particular, em um domínio noetheriano, todo ideal não nulo contém um produto de ideais primos não nulos.*

*Demonstração.* Suponhamos por absurdo que $A$ é um anel noetheriano e $F$ é o conjunto dos ideais de $A$ que não contém um produto de ideais primos. Suponhamos ainda que $F \neq \varnothing$. Como $A$ é noetheriano, segue que $F$ tem um elemento maximal $\mathfrak{m}$. Temos que $\mathfrak{m}$ não é um ideal maximal, pois caso contrário, $\mathfrak{m}$ seria primo e assim $\mathfrak{m} \notin F$. Assim, existem $x, y \in A - \mathfrak{m}$ tal que $xy \in \mathfrak{m}$. Notemos que $\mathfrak{m} \subsetneq \langle x \rangle + \mathfrak{m}$ e $\mathfrak{m} \subsetneq \langle y \rangle + \mathfrak{m}$. Logo, $\langle x \rangle + \mathfrak{m}$ e $\langle y \rangle + \mathfrak{m}$ não pertencem a $F$. Assim,

$$\prod_{i=1}^{n} \mathfrak{p}_i \subseteq \langle x \rangle + \mathfrak{m} \text{ e } \prod_{i=1}^{n} \mathfrak{q}_i \subseteq \langle y \rangle + \mathfrak{m}$$

onde $\mathfrak{p}_i$ e $\mathfrak{q}_j$ são ideais de $A$ e

$$\left(\prod_{i=1}^{n} \mathfrak{p}_i\right)\left(\prod_{i=1}^{n} \mathfrak{p}_i\right) \subseteq \big(\langle x \rangle + \mathfrak{m}\big)\big(\langle x \rangle + \mathfrak{m}\big) \subseteq \mathfrak{m}$$

o que é um absurdo. Logo, $F = \varnothing$.

No caso do domínio noetheriano, a demonstração é análoga. □

# Capítulo 2

# Teoria dos Números Algébricos

Neste capítulo serão apresentados os conceitos que são a base da teoria dos números algébricos. Definiremos e mostraremos as propriedades e os principais resultados dos inteiros algébricos, traço, norma, discriminante, anéis de Dedekind e ideais fracionários.

## 2.1 Inteiros Algébricos

**Definição 2.1.** *Sejam* $\mathbb{K}$ *e* $\mathbb{L}$ *corpos. Dizemos que* $\mathbb{K}$ *é uma* ***extensão*** *de* $\mathbb{L}$ *se* $\mathbb{L} \subset \mathbb{K}$ *e denotaremos por* $\mathbb{K}/\mathbb{L}$.

**Definição 2.2.** *Seja* $\mathbb{K}/\mathbb{L}$ *uma extensão de corpos. O* ***grau*** *de* $\mathbb{K}$ *sobre* $\mathbb{L}$ *é a dimensão de* $\mathbb{K}$ *como espaço vetorial sobre* $\mathbb{L}$*, ou seja,* $\dim_{\mathbb{L}}(\mathbb{K})$. *Indicaremos o grau de* $\mathbb{K}/\mathbb{L}$ *por* $[\mathbb{K} : \mathbb{L}]$.

**Observação 2.1.** *No caso em que* $[\mathbb{K} : \mathbb{L}]$ *é finito, dizemos que* $\mathbb{K}$ *é uma* ***extensão finita*** *de* $\mathbb{L}$.

**Definição 2.3.** *Sejam* $\mathbb{L} \subseteq \mathbb{K}$ *corpos e um elemento* $\alpha \in \mathbb{K}$. *Pode existir ou não um polinômio* $p \in \mathbb{L}[x] - \{0\}$ *tal que* $p(\alpha) = 0$. *Se existir, então dizemos que o elemento* $\alpha$ *é* ***algébrico*** *sobre* $\mathbb{L}$. *Caso contrário, dizemos que* $\alpha$ *é* ***transcedente*** *ou* ***transcendental*** *sobre* $\mathbb{L}$.

**Observação 2.2.** *Temos que se* $\alpha \in \mathbb{K}$ *é algébrico sobre* $\mathbb{L}$*, então existe um único polinômio mônico*[1] $q$ *de grau minímo tal que* $q(\alpha) = 0$*, chamamos de* ***polinômio minimal*** *de* $\alpha$ *sobre* $\mathbb{L}$. *O polinômio minimal de* $\alpha$ *é irredutível sobre* $\mathbb{L}$.

[1] É o polinômio de coeficiente principal ou dominante igual a 1, isto é, $a_n = 1$

**Definição 2.4.** *Sejam $\mathbb{L} \subseteq \mathbb{K}$ corpos. Se $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}$, então definimos que o conjunto $\mathbb{L}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ como o menor subcorpo de $\mathbb{K}$ que contém $\mathbb{L}$ e os elementos $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{K}$.*

**Definição 2.5.** *Sejam $B \subseteq A$ anéis. Se $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$, então definimos que o conjunto $B[\alpha_1, \alpha_2, \ldots, \alpha_n]$ como o menor subanel de $A$ que contém $B$ e os elementos $\alpha_1, \alpha_2, \ldots, \alpha_n \in A$.*

**Observação 2.3.** *Nas condições da definição (2.5), temos que $B[\alpha_1, \alpha_2, \ldots, \alpha_n]$ é o conjunto de todos os polinômios em $\alpha_1, \alpha_2, \ldots, \alpha_n$ com coeficientes em $B$.*

**Definição 2.6.** *Sejam $\mathbb{L}$ um corpo finito ou um corpo de característica zero e $\mathbb{K}$ uma extensão de $\mathbb{L}$ de grau finito $n$. Um elemento $\alpha \in \mathbb{K}$ é chamado de **primitivo** se $\mathbb{K} = \mathbb{L}[\alpha]$.*

**Definição 2.7.** *Um **corpo de números** $\mathbb{K}$ é uma extensão finita do corpo $\mathbb{Q}$ dos números racionais. Se $\dim_{\mathbb{Q}}(\mathbb{K}) = n$, diz-se que $\mathbb{K}$ é um corpo de números de grau $n$.*

**Teorema 2.1** ([6], p.40)**.** *Se $\mathbb{K}$ é um corpo de números, então $\mathbb{K} = \mathbb{Q}(\alpha)$ para algum número algébrico $\alpha$.*

**Definição 2.8.** *Sejam $A \subseteq B$ anéis. Dizemos que um elemento $\alpha \in B$ é **inteiro** sobre $A$ se existe um polinômio mônico não nulo $f$ com coeficientes em $A$ tal que $f(\alpha) = 0$.*

**Teorema 2.2** ([5], p.27)**.** *Se $A$ é um anel, $B \subset A$ um subanel e $x \in A$, então são equivalentes as seguintes afirmações:*

1. *$x$ é inteiro sobre $B$;*
2. *O anel $B[x] = \left\{ \sum_{i=0}^{n} b_i x^i \;\middle|\; b_i \in B, \text{para } i = 0, 1, 2, \ldots, n \right\}$ é um $B$-módulo finitamente gerado;*
3. *Existe um subanel $C$ de $A$ tal que $C$ é um $B$-módulo finitamente gerado que contém $B$ e $x$.*

*Demonstração.* **1) $\Rightarrow$ 2)** Temos por hipótese que $x$ é inteiro sobre $B$, ou seja, existem $b_1$, $b_2$, ..., $b_{n-1} \in B$ não nulos tais que

$$x^n + \sum_{i=0}^{n-1} b_i x^i = 0.$$

Assim, podemos escrever

$$x^n = -\sum_{i=0}^{n-1} b_i x^i.$$

Seja $M = \langle 1, x, x^2, \ldots, x^{n-1} \rangle$ um $A$-módulo finitamente gerado. Temos que $x^n \in M$ pois $x^n$ é uma combinação de $1, x, x^2, \ldots, x^{n-1}$.

Agora, devemos mostrar que $B[x] = M$. Temos de imediato que $M \subset B[x]$. Agora, falta mostrar que $B[x] \subset M$. Para isto, devemos provar por indução sobre $k$ que $x^k \in M$, para todo $k \in \mathbb{N}^*$.

1. Temos que para $k \leq n$ o resultado se verifica.

2. Suponhamos por hipótese de indução que $x^k \in M$, isto é, existe $a_0, a_1, a_2, \ldots, a_{n-1} \in B$ tais que

$$x^k = \sum_{i=0}^{n-1} a_i x^i.$$

Devemos mostrar que $x^{k+1} \in M$. De fato:

$$\begin{aligned}
x^{k+1} &= x^k x \\
&= \left( \sum_{i=0}^{n-1} a_i x^i \right) x \\
&= \sum_{i=0}^{n-1} a_i x^{i+1} \\
&= a_{n-1} x^n + \sum_{i=0}^{n-2} a_i x^{i+1} \\
&= a_{n-1} \left( -\sum_{i=0}^{n-1} b_i x^i \right) + \sum_{i=0}^{n-2} a_i x^{i+1} \\
&= -a_{n-1} b_0 - a_{n-1} \sum_{i=1}^{n-1} b_i x^i + \sum_{i=0}^{n-2} a_i x^{i+1} \\
&= -a_{n-1} b_0 - a_{n-1} \sum_{i=0}^{n-2} b_{i+1} x^{i+1} + \sum_{i=0}^{n-2} a_i x^{i+1} \\
&= -a_{n-1} b_0 + \sum_{i=0}^{n-2} \big( -a_{n-1} b_{i+1} x^{i+1} + a_i x^{i+1} \big) \\
&= -a_{n-1} b_0 + \sum_{i=0}^{n-2} \big( a_i - a_{n-1} b_{i+1} \big) x^{i+1} \Longrightarrow x^{k+1} \in M.
\end{aligned}$$

Com isto, temos $B[x] \subset M$. Logo, $B[x] = M$, o que mostra que $B[x]$ é um $B$-módulo finitamente gerado.

**2) $\Rightarrow$ 3)** Basta tomarmos $C = B[x]$ por causa $B \subset B[x]$ e $x \in B[x]$.

**3) $\Rightarrow$ 1)** Suponhamos que $C = \langle y_1, y_2, \ldots, y_n \rangle$ seja um $B$-módulo finitamente gerado, ou seja, $C = \sum_{i=1}^{n} b_i y_i$. Por hipótese, temos que se $x \in C$, então $xy_i \in C$, para todo $1 \leq i \leq n$. Assim, temos que

$$xy_i = \sum_{j=1}^{n} a_{ij} y_j, 1 \leq i \leq n, a_{ij} \in A, j \leq n$$

é um sistema linear homogêneo nas variáveis $y_1, y_2, \ldots, y_n$, ou seja

$$\sum_{j=1}^{n} (\delta_{ij} x - a_{ij}) y_j = 0, 1 \leq i \leq n, \text{ onde } \delta_{ij} = \begin{cases} 1 & \text{se} \quad i = j \\ 0 & \text{se} \quad i \neq j \end{cases}.$$

Seja $d = \det(\delta_{ij} x - a_{ij})$. Pela Regra de Cramer temos que $dy_i = 0$, para todo $i = 1, 2, \ldots, n$. Consequentemente, $db = 0$, para todo $b \in B$, em particular para $b = 1$ temos $d = 0$. Mas, $d$ é um polinômio mônico na indeterminada $x$ da forma $d = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$, onde $a_i \in A$. Portanto, $x$ é inteiro sobre $A$.

□

**Proposição 2.1** ([5], p.28)**.** *Sejam $A$ um anel, $B \subset A$ um subanel e $x_1, x_2, \ldots, x_n \in A$. Se $x_1, x_2, \ldots, x_i$ são inteiros sobre $B[x_1, x_2, \ldots, x_i]$, para $i = 1, 2, \ldots, n$, então $B[x_1, x_2, \ldots, x_n]$ é um $B$-módulo finitamente gerado.*

*Demonstração.* Pelo Teorema (2.2) temos que se $x_1$ é inteiro sobre $B$, então $B[x_1]$ é um $B$-módulo finitamente gerado. Suponhamos por indução que $C = B[x_1, x_2, \ldots, x_i]$ seja um $B$-módulo finitamente gerado, ou seja, $C = \sum_{i=1}^{p} Bc_i$, onde $c_1, c_2, \ldots, c_p \in C$. Pelo Teorema (2.2) temos que $B[x_1, x_2, \ldots, x_n] = C[x_n]$ é um $C$-módulo finitamente gerado. Então

$$C[x_n] = \sum_{k=1}^{q} Cw_k = \sum_{k=1}^{q} \Big( \sum_{j=1}^{p} Bc_j \Big) w_k = \sum_{j,k} Bc_j w_k$$

onde $w_k \in C[x_n]$. Logo, $B[x_1, x_2, \ldots, x_n]$ é um $B$-módulo finitamente gerado por $\{c_j w_k\}$ com $1 \leq j \leq p$ e $1 \leq k \leq q$ e portanto $B[x_1, x_2, \ldots, x_n]$ é um $B$-módulo finitamente gerado. □

**Corolário 2.1** ([5], p.29)**.** *Sejam $A$ um anel, $B \subset A$ um subanel e $x, y \in A$. Se $x$ e $y$ são inteiros sobre $B$, então $x+y$, $x-y$ e $xy$ também são inteiros sobre $B$.*

*Demonstração.* Temos que $x+y$, $x-y$ e $xy$ pertencem a $B[x,y]$ é um $B$-módulo finitamente gerado. Logo, pelo Teorema (2.2) temos que $x+y$, $x-y$ e $xy$ são inteiros sobre $B$. □

**Definição 2.9.** *Sejam $B \subset A$ anéis. Dizemos que $A$ é inteiro sobre $B$ se todo elemento de $A$ é inteiro sobre $B$.*

**Proposição 2.2** ([5], p.29)**.** *Sejam $C \subseteq B \subseteq A$ anéis. Assim, $A$ é inteiro sobre $C$ se, e somente se $A$ é inteiro sobre $B$ e $B$ é inteiro sobre $C$.*

*Demonstração.* ($\Rightarrow$) Suponhamos que $A$ é inteiro sobre $C$. Se $\alpha \in A$, então existem $a_0, a_1, \ldots, a_{n-1} \in C$, todos não nulos tais que

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

Como $C \subset B$, segue que $a_i \in B$ para $i = 0, 1, 2, \ldots, n-1$, ou seja, $\alpha$ é inteiro sobre $B$. Portanto, $A$ é inteiro sobre $B$. Agora, seja $\alpha \in B$. Como $B \subset A$, segue que $\alpha \in A$ e, pela hipótese, $\alpha$ é inteiro sobre $C$. Portanto, $B$ é inteiro sobre $C$.

($\Leftarrow$) Agora, seja $x \in A$. Por hipótese, temos que $A$ é inteiro sobre $B$ e, assim existem $b_0, b_1, \ldots, b_{n-1} \in B$ tais que

$$x^n + b_{n-1}x^{n-1} + \ldots + b_0 = 0.$$

Se $R = C[b_0, b_1, \ldots, b_{n-1}]$, então $x$ é inteiro sobre $R$. Mas, como $B$ é inteiro sobre $C$, segue que $b_i, i = 0, 1, \ldots, n-1$ são inteiros sobre $C$. Pela Proposição (2.1) segue que $R[x] = C[b_0, b_1, \ldots, b_{n-1}, x]$ é um $C$-módulo finitamente gerado. E pelo Teorema (2.2) segue que $x$ é inteiro sobre $C$. Portanto, $A$ é inteiro sobre $C$. □

**Definição 2.10.** *Sejam $A \subset B$ anéis. O conjunto $\mathcal{O}_B = \{\alpha \in B \mid \alpha$ é inteiro sobre $A\}$ é chamado de **anel dos inteiros** de $B$ em $A$. Se $A$ é um domínio e $B = \mathbb{K}$ é o seu corpo de frações, dizemos que $\mathcal{O}_B$ **é o anel dos inteiros de** $A$ **em** $\mathbb{K}$.*

**Definição 2.11.** *Sejam $A$ um domínio e $\mathbb{K}$ seu corpo de frações. Dizemos que $A$ é um **anel integralmente fechado** em $\mathbb{K}$ se ele contém o anel dos inteiros $A$.*

**Proposição 2.3** ([5], p.30)**.** *Todo domínio principal é integralmente fechado.*

*Demonstração.* Sejam $A$ um domínio principal, $\mathbb{K}$ seu corpo de frações e $x \in \mathbb{K}$ um inteiro sobre $A$ tal que $x = \dfrac{\alpha}{\beta}$, $\alpha, \beta \in A$ e $\text{mdc}(\alpha, \beta) = 1$. Assim, existem $a_0, a_1, \ldots, a_{n-1} \in A$ tais que

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + 1a_0 = 0.$$

Se substituirmos $x$ por $\dfrac{\alpha}{\beta}$, teremos

$$\begin{aligned}
\left(\frac{\alpha}{\beta}\right)^n + a_{n-1}\left(\frac{\alpha}{\beta}\right)^{n-1} + \ldots + a_1\left(\frac{\alpha}{\beta}\right) + a_0 &= 0 \\
\beta^n\left(\frac{\alpha}{\beta}\right)^n + a_{n-1}\beta^n\left(\frac{\alpha}{\beta}\right)^{n-1} + \ldots + a_1\beta^n\left(\frac{\alpha}{\beta}\right) + a_0\beta^n &= 0 \\
\alpha^n + a_{n-1}\alpha^{n-1}\beta + \ldots + a_1\alpha\beta^{n-1} + a_0\beta^n &= 0
\end{aligned}$$

Logo $\beta | \alpha^n$ e como $mdc(\alpha, \beta) = 1$, seguq que $\beta$ □

Até agora, vimos os elementos inteiros sobre um anel qualquer. A partir de agora veremos estes elementos sobre um anel específico, o anel dos inteiros $\mathbb{Z}$.

**Definição 2.12.** *Um número complexo $\alpha$ é um* ***inteiro algébrico*** *se existe um polinômio mônico $p$ com coeficientes inteiros tal que $p(\alpha) = 0$.*

**Observação 2.4.** *Como na Deninição (2.10), se $\mathbb{K}$ é um corpo de números, podemos definir o anel dos inteiros algébricos de $\mathbb{K}$ como o conjunto formado pelos inteiros algébricos de $\mathbb{K}$ e denotamos por $\mathcal{O}_{\mathbb{K}}$.*

**Teorema 2.3** ([6], p.47)**.** *Se $\alpha$ é um número complexo que satisfaz um polinômio mônico cujos coeficientes são inteiros algébricos, então $\alpha$ é um inteiro algébrico.*

*Demonstração.* Seja $\alpha$ raiz de $p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, onde $a_i$ é inteiro algébrico para $i = 0, 1, , 2, \ldots, n-1$. Temos que $\alpha$ é inteiro sobre $\mathbb{Z}[a_0, a_1, \ldots, a_{n-1}]$. Mas, pela Proposição (2.1) temos que $\mathbb{Z}[a_0, a_1, \ldots, a_{n-1}]$ é um $\mathbb{Z}$-módulo finitamente gerado. desta forma, novamente pela Proposição (2.1) temos que $\mathbb{Z}[a_0, a_1, \ldots, a_{n-1}, \alpha]$ é um $\mathbb{Z}$-módulo finitamente gerado. Pelo Teorema (2.2), segue que $\alpha$ é inteiro algébrico. □

**Proposição 2.4** ([5], p.30)**.** *Seja $A$ é um domíno, $\mathbb{L}$ o seu corpo de frações, $\mathbb{K}$ uma extensão finita de $\mathbb{L}$ de grau $n$ e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ sobre $A$. Logo, $\mathcal{O}_{\mathbb{K}}$ é integralmente fechado.*

*Demonstração.* Seja $M$ o corpo das frações de $\mathcal{O}_{\mathbb{K}}$. Temos que $\mathbb{L} \subset \mathbb{M} \subset \mathbb{K}$. Seja $x \in \mathbb{M}$ tal que $x$ pe inteiro sobre $\mathcal{O}_{\mathbb{K}}$. Como $\mathcal{O}_{\mathbb{K}}$ é inteiro sobre $A$, segue da demonstração da Proposição (2.2), que $x$ é inteiro sobre $A$. Assim, se $\mathcal{O}_{\mathbb{M}}$ é o conjunto dos elementos de $\mathbb{M}$ que são inteiros sobre $\mathcal{O}_{\mathbb{K}}$, então $\mathcal{O}_{\mathbb{M}} \subset \mathcal{O}_{\mathbb{K}}$. Como $\mathcal{O}_{\mathbb{K}} \subset \mathcal{O}_{\mathbb{M}}$, temos que $\mathcal{O}_{\mathbb{M}} = \mathcal{O}_{\mathbb{K}}$, o que implica que $\mathcal{O}_{\mathbb{K}}$ é integralmente fechado. □

**Definição 2.13.** *Sejam $\mathbb{K}$ um corpo de números de grau $n$ e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$. Chamamos de **base integral** de $\mathbb{K}$ ou de $\mathcal{O}_{\mathbb{K}}$ uma $\mathbb{Z}$-base para o grupo aditivo $\mathcal{O}_{\mathbb{K}}$.*

**Observação 2.5.** *Se $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base integral $\mathcal{O}_{\mathbb{K}}$, então todo elemento $\alpha \in \mathcal{O}_{\mathbb{K}}$ pode ser escrito de modo único como $\alpha = \sum_{i=1}^{n} a_i\alpha_i$, onde $a_i \in \mathbb{Z}$ para todo $i = 1, 2, \ldots, n$.*

## 2.2 Traço e Norma

**Definição 2.14.** *Sejam $\mathbb{K}/\mathbb{L}$ uma extensão de grau $n$ e $\sigma_1, \sigma_2, \ldots, \sigma_n$ os monomorfismos de $\mathbb{K}$ em $\mathbb{C}$. O **traço** e a **norma** de um elemento $\alpha \in \mathbb{K}$ relativamente a extensão $\mathbb{K}/\mathbb{L}$ são definidos respectivamente por*

$$\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \text{ e } \mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

**Observação 2.6.** *Sejam $\mathbb{K}/\mathbb{L}$ uma extensão de grau $n$. Se $\alpha, \beta \in \mathbb{K}$ e $x \in \mathbb{L}$, então valem as seguintes propriedades:*

1. $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(\alpha + \beta) = \mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(\alpha) + \mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(\beta)$;
2. $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(x\alpha) = x\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(\alpha)$;
3. $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(x) = nx$;
4. $\mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha\beta) = \mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha)\mathcal{N}_{\mathbb{K}/\mathbb{L}}(\beta)$;
5. $\mathcal{N}_{\mathbb{K}/\mathbb{L}}(x\alpha) = x^n\mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha)$;
6. $\mathcal{N}_{\mathbb{K}/\mathbb{L}}(x) = x^n$.

*Se tivermos $\mathbb{M} \subseteq \mathbb{L} \subseteq \mathbb{K}$ extensões finitas e $\alpha \in \mathbb{K}$ temos ainda que:*

1. $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(\alpha) = \mathrm{Tr}_{\mathbb{K}/\mathbb{L}}\big(\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(\alpha)\big)$;

2. $\mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha) = \mathcal{N}_{\mathbb{K}/\mathbb{L}}\big(\mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha)\big)$.

*E se tivermos $\mathbb{M} \subseteq \mathbb{L} \subseteq \mathbb{K}$ extensões finitas e $\alpha \in \mathbb{L}$ temos ainda que:*

1. $\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(\alpha) = [\mathbb{K} : \mathbb{L}]\mathrm{Tr}_{\mathbb{K}/\mathbb{L}}(\alpha)$;

2. $\mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha) = \mathcal{N}_{\mathbb{K}/\mathbb{L}}(\alpha)^{[\mathbb{K}:\mathbb{L}]}$.

**Observação 2.7.** *Denotaremos o traço e a norma simplesmente e respectivamente por* $\mathrm{Tr}(\alpha)$ *e* $\mathcal{N}(\alpha)$ *quando não houver dúvida quanto a extensão que contém o elemento* $\alpha$.

**Proposição 2.5** ([5], p.36)**.** *Sejam* $\mathbb{L}$ *um corpo de característica zero ou um corpo finito,* $\mathbb{K}$ *uma extensão algébrica de grau* $n$ *de* $\mathbb{L}$ *e* $\alpha \in \mathbb{K}$*. Se* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *são as raízes do polinômio minimal de* $\alpha$ *sobre* $\mathbb{L}$*, então*

$$\begin{aligned} \mathrm{Tr}\alpha) &= \sum_{i=1}^{n} \alpha_i \\ \mathcal{N}(\alpha) &= \prod_{i=1}^{n} \alpha_i \\ p(x) &= (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n) \end{aligned}$$

*onde* $p$ *é um polinômio mônico com coeficientes em* $\mathbb{K}$ *chamado de polinômio característico.*

*Demonstração.* **(1)** Primeiro vamos fazer a demonstração para o caso em que $\alpha$ é um elemento primitivo de $\mathbb{K}$ sobre $\mathbb{L}$, ou seja, $\mathbb{K} = \mathbb{L}[\alpha]$. Se $f$ é o polinômio minimal de $\alpha$ sobre $\mathbb{L}$, isto é, $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, então $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{L}$. Temos que a matriz do endomorfismo $\sigma_\alpha$ com respeito a esta base é dada por

$$\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 0 & 1 & -a_{n-1} \end{bmatrix}.$$

Assim, $\det(xI_n - M)$ é o determinante da matriz

$$xI_n - M = \begin{bmatrix} x & 0 & 0 & \cdots & 0 & 0 & a_0 \\ -1 & x & 0 & \cdots & 0 & 0 & a_1 \\ 0 & -1 & x & \cdots & 0 & 0 & a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & -1 & x & a_{n-2} \\ 0 & 0 & 0 & \cdots & 0 & -1 & x + a_{n-1} \end{bmatrix}. \tag{2.1}$$

Ao calcular o determinante da matriz (2.1), obtemos o polinômio característico em $\alpha$, que é igual a $f$, o polinômio minimal de $\alpha$. Sabemos que

$$p(x) = \det(xI_n - M) = x^n - \big(\mathrm{Tr}(\alpha)\big)x^{n-1} + \ldots + (-1)^n \det(M).$$

Como $\alpha$ é primitivo, segue que

$$\begin{aligned} p(x) &= f(x) \\ &= (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n) \\ &= x^n - \left(\sum_{i=1}^{n} \alpha_i\right)x^{n-1} + \ldots + (-1)^n \left(\prod_{i=1}^{n} \alpha_i\right). \end{aligned}$$

Logo, $\mathrm{Tr}(\alpha) = \sum_{i=1}^{n} \alpha_i$ e $\mathcal{N}(\alpha) = \prod_{i=1}^{n} \alpha_i$.

**(2)** Para o caso geral, seja $r = \big[\mathbb{K} : \mathbb{L}[\alpha]\big]$. É suficiente mostrar que o polinômio característico $p$ de $\alpha$, com relação a $\mathbb{K}$ sobre $\mathbb{L}$, é igual a $r$-ésima potência do polinômio minimal de $\alpha$ sobre $\mathbb{L}$. Seja $\{y_1, y_2, \ldots, y_q\}$ uma base de $\mathbb{L}[\alpha]$ sobre $\mathbb{L}$ e seja $\{z_1, z_2, \ldots, z_r\}$ uma base de $\mathbb{K}$ sobre $\mathbb{L}[\alpha]$ com $n = qr$. Seja $M = (a_{ih})$ a matriz do endomorfismo de $\mathbb{L}[a]$ sobre $\mathbb{L}$ com relação a base $\{y_1, y_2, \ldots, y_q\}$. Assim, $\alpha y_i = \sum_{h=1}^{q} (a_{ih}) y_h$ e

$$\alpha(y_i z_j) = \left(\sum_{h=1}^{q} a_{ih} y_h\right) z_j = \sum_{h=1}^{q} a_{ih}(y_h z_j).$$

Logo,

$$\begin{cases} \alpha y_1 z_1 = a_{11} y_1 z_1 + a_{21} y_2 z_1 + \ldots + a_{q1} y_q z_1 \\ \alpha y_1 z_1 = a_{11} y_1 z_1 + a_{21} y_2 z_1 + \ldots + a_{q1} y_q z_1 \\ \vdots \\ \alpha y_1 z_1 = a_{11} y_1 z_1 + a_{21} y_2 z_1 + \ldots + a_{q1} y_q z_1. \end{cases}$$

Ordenamos a base $y_i z_j$ de $\mathbb{K}$ sobre $\mathbb{L}$, de modo que a matriz do endomorfismo seja da seguinte forma:

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

isto é, $M$ repete $r$-vezes na diagonal como blocos na matriz $M_1$. A matriz $xI_n - M_1$ consiste de $r$-blocos diagonais, cada um tem a forma $xI_q - M$ e, consequentemente, $\det(xI_n - M_1) = \det(xI_q - M)^r$. Assim, $p(x) = \det(xI_n - M_1)$ e $\det(xI_q - M)$ é o polinômio minimal de $\alpha$ sobre $\mathbb{L}$, de acordo com a primeira parte da demonstração. □

**Proposição 2.6** ([5], p.38)**.** *Sejam $A$ um domínio, $\mathbb{L}$ seu corpo de frações (de característica zero) e $\mathbb{K}$ uma extensão finita de $\mathbb{L}$. Se $\alpha$ é um elemento de $\mathbb{K}$ inteiro sobre $A$, então os coeficientes do polinômio característico $p$ de $\alpha$ relativo a $\mathbb{K}$ e $\mathbb{L}$, em particular* $\mathrm{Tr}(\alpha)$ *e* $\mathcal{N}(\alpha)$*, são inteiros sobre $A$.*

*Demonstração.* Pela Proposição (2.5), temos que $p(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$. Os coeficientes de $p$ são as somas de produtos de $\alpha_i'$, a menos de sinal. Assim, é suficiente provar que cada $\alpha_i$ é inteiro sobre $A$. Mas, cada $\alpha_i$ é um conjugado de $\alpha$ sobre $\mathbb{L}$. Isto é, existe um isomorfismo $\sigma_i : \mathbb{L}[\alpha] \to \mathbb{L}[\alpha_i]$ tal que $\sigma_i(\alpha) = \alpha_i$. Assim, aplicando $\sigma_i$ na equação de dependência integral de $\alpha$ sobre $A$, obtemos uma equação de dependência integral de $\alpha_i$ sobre $A$. □

**Corolário 2.2** ([5], p. 38)**.** *Se $A$ é um anel integralmente fechado, então os coeficientes do polinômio característico de $\alpha \in \mathbb{K}$, em particular,* $\mathrm{Tr}(\alpha)$ *e* $\mathcal{N}(\alpha)$ *são elementos de $A$.*

*Demonstração.* Por definição, esses coeficientes são elementos dos corpos de frações $\mathbb{L}$ de $A$.

Pela Proposição (2.6), temos que são inteiros sobre $A$ e como $A$ é integralmente fechado, segue que são elementos de $A$. □

**Lema 2.1** ([4], p.34)**.** *Sejam $A$ um anel integralmente fechado, $\mathbb{L}$ seu corpo de frações, $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau $n$ e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros algébricos $\mathbb{K}$. Seja $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{Q}$ onde $\det\big(\mathrm{Tr}(\alpha_i\alpha_j)\big) \neq 0$. Seja $\alpha \in \mathbb{K}$. Se $\mathrm{Tr}(\alpha\beta) = 0$ para todo $\beta \in \mathbb{K}$, então $\alpha = 0$.*

*Demonstração.* Por hipótese, $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Assim, se $\alpha$ é um elemente de $\mathbb{K}$, então existem $a_1, a_2, \ldots, a_n \in \mathbb{Q}$ tal que $\alpha = \sum_{i=1}^{n} a_i\alpha_i$. Logo, é suficiente mostrar que se $\mathrm{Tr}(\alpha\alpha_j) = 0$, para cada $j = 1, 2, \ldots, n$, então $\alpha = 0$. Assim, para cada $j = 1, 2, \ldots, n$, temos que

$$\begin{aligned} 0 &= \mathrm{Tr}(\alpha\alpha_j) \\ &= \mathrm{Tr}\left(\sum_{i=1}^{n} a_i\alpha_i\alpha_j\right) \\ &= \sum_{i=1}^{n} \mathrm{Tr}(a_i\alpha_i\alpha_j) \\ &= \sum_{i=1}^{n} a_i\mathrm{Tr}(\alpha_i\alpha_j) \end{aligned}$$

Na forma matricial, temos que

$$\begin{bmatrix} \mathrm{Tr}(\alpha_1\alpha_1) & \mathrm{Tr}(\alpha_2\alpha_1) & \cdots & \mathrm{Tr}(\alpha_n\alpha_1) \\ \mathrm{Tr}(\alpha_1\alpha_2) & \mathrm{Tr}(\alpha_2\alpha_2) & \cdots & \mathrm{Tr}(\alpha_n\alpha_2) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(\alpha_1\alpha_n) & \mathrm{Tr}(\alpha_2\alpha_n) & \cdots & \mathrm{Tr}(\alpha_n\alpha_n) \end{bmatrix} \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

Como $\det\big(\mathrm{Tr}(\alpha_i\alpha_j)\big) \neq 0$, segue que $a_1 = a_2 = \ldots = a_n = 0$. Portanto, $\alpha = 0$. □

**Lema 2.2** ([4], p. 34)**.** *A aplicação $\rho : \mathbb{L} \to \mathrm{Hom}_{\mathbb{Q}}(\mathbb{K}, \mathbb{Q})$ definida por $\rho(\alpha) = S_\alpha$, onde $S_\alpha(\beta) = \mathrm{Tr}(\alpha\beta)$, com $\beta \in \mathbb{K}$, é um isomorfismo.*

*Demonstração.* Se $\alpha_1, \alpha_2 \in \mathbb{K}$, então

$$\begin{aligned}
\rho(\alpha_1+\alpha_2)(\beta) &= S_{\alpha_1+\alpha_2}(\beta) \\
&= \mathrm{Tr}\big((\alpha_1+\alpha_2)\beta\big) \\
&= \mathrm{Tr}(\alpha_1\beta) + \mathrm{Tr}(\alpha_2\beta) \\
&= S_{\alpha_1}(\beta) + S_{\alpha_2}(\beta) \\
&= \big(\rho(\alpha_1)+\rho(\alpha_2)\big)(\beta)
\end{aligned}$$

e

$$\begin{aligned}
\rho(a\alpha)(\beta) &= S_{a\alpha}(\beta) \\
&= \mathrm{Tr}(a\alpha\beta) \\
&= a\mathrm{Tr}(\alpha\beta) \\
&= aS_{\alpha}(\beta) \\
&= a\rho(\alpha)(\beta)
\end{aligned}$$

para todo $\beta \in \mathbb{K}$. Logo, $\rho$ é um homomorfismo.

Agora, se $\alpha \in \mathbb{K}$ tal que $\rho(\alpha) = 0$, então, $\rho(\alpha)(\beta) = S_\alpha(\beta) = \mathrm{Tr}(\alpha\beta) = 0$, para todo $\beta \in \mathbb{K}$. Assim, pelo Lema (2.1), segue que $\alpha = 0$. Logo, $Ker(\rho) = \{0\}$ e, então $\rho$ é injetiva.

Finalmente, como $\dim_{\mathbb{Q}} \mathbb{K} = \dim_{\mathbb{Q}}\big(Hom_{\mathbb{Q}}(\mathbb{K}, \mathbb{Q})\big)$, segue que $\rho$ é sobrejetiva.

Portanto, $\rho$ é isomorfismo. □

**Teorema 2.4** ([4], p.35)**.** *Se $A$ é um anel integralmente fechado, $\mathbb{L}$ o seu corpo de frações, $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau $n$ e $\mathcal{O}_\mathbb{K}$ o anel dos inteiros algébricos $\mathbb{K}$, então $\mathcal{O}_\mathbb{K}$ é um $A$-submódulo livre de posto $n$.*

*Demonstração.* Seja $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ uma base de $\mathbb{K}$ sobre $\mathbb{L}$. Como toda extensão finita é algébrica, segue que todos os $\alpha_i$ são algébricos sobre $\mathbb{L}$, ou seja, existem $a_{ij} \in A$, para $i = 1, 2, \ldots, n$, pelo menos um não-nulo tais que

$$a_{in}\alpha_i^n + a_{i(n-1)}\alpha_i^{n-1} + \ldots + a_{i0} = 0.$$

Suponhamos que $a_{in} \neq 0$. Multiplicando a equação acima por $a_{in}^{n-1}$, temos que $a_{in}\alpha_i$ é inteiro sobre $A$, pois

$$\begin{aligned} a_{in}^{n-1}(a_{in}\alpha_i^n + a_{i(n-1)}\alpha_i^{n-1} + \ldots + a_{i0}) &= (a_{in}\alpha_i)^n + a_{i(n-1)}(a_{in}\alpha_i)^{n-1} + \ldots + a_{in}^{n-1}a_{i0} \\ &= 0. \end{aligned}$$

Tomando $a_{in}\alpha_i = z_i \in \mathcal{O}_{\mathbb{K}}$, para cada $i = 1, 2, \ldots, n$. Mostraremos que $\{z_1, z_2, \ldots, z_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{L}$. Para isso, suponhamos que $\sum_{i=1}^{n} b_i z_i = 0$, onde $b_i \in A$, para $i = 1, 2, \ldots, n$. Assim, $\sum_{i=1}^{n} b_i a_{in}\alpha_i = 0$. Mas, como $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{L}$, segue que $b_i a_{in} = 0$ eportanto $b_i = 0$ para $i = 1, 2, \ldots, n$. Portanto, $\{z_1, z_2, \ldots, z_n\}$ é linearmente independente e, como possui $n$ elementos, segue que é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Pelo Lema (2.2), existe uma base dual $\{y_1, y_2, \ldots, yn\}$ tal que

$$\rho(z_i)(y_i) = S_{z_i}(y_j) = Tr(z_i y_j) = \delta_{ij} \text{ para } i, j = 1, 2, \ldots, n.$$

Agora, se $\alpha \in \mathcal{O}_{\mathbb{L}}$, então $\alpha z_i \in \mathcal{O}_{\mathbb{L}}$, para $i = 1, 2, \ldots, n$. Pelo Corolário (2.2), segue que $\mathrm{Tr}(\alpha z_i) \in A$ para $i = 1, 2, \ldots, n$. Como $\alpha = \sum_{i=1}^{n} c_i y_i$, com $c_i \in \mathbb{K}$ para $i = 1, 2, \ldots, n$, segue que $\mathrm{Tr}(\alpha z_i) = c_i \in A$, para $i = 1, 2, \ldots, n$. Portanto, $\mathcal{O}_{\mathbb{K}}$ é um submódulo de um $A$-módulo livre gerado por $\{z_1, z_2, \ldots, z_n\}$. □

**Proposição 2.7** ([5], p.47)**.** *Seja $A$ um anel noetheriano e integralmente fechado. Se $\mathbb{L}$ é o corpo de frações de $A$, $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau $n$ e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $A$ em $\mathbb{K}$, então $\mathcal{O}_{\mathbb{K}}$ é um $A$-módulo finitamente gerado e $\mathcal{O}_{\mathbb{K}}$ é um anel noetheriano.*

*Demonstração.* Pelo Teorema (2.4), temos que $\mathcal{O}_{\mathbb{K}}$ é um submódulo de um $A$-módulo livre de posto $n$. Pelo Corolário (1.2), temos que $\mathcal{O}_{\mathbb{K}}$ é um $A$-módulo noetheriano e, portanto, finitamente gerado. Como os ideais de $\mathcal{O}_{\mathbb{K}}$ são $A$-submódulos de $\mathcal{O}_{\mathbb{K}}$, segue que satisfazem a condição de maximilidade da Definição (1.27). Portanto, $\mathcal{O}_{\mathbb{K}}$ é um anel noetheriano. □

## 2.3 Norma de um Ideal

**Definição 2.15.** *Sejam $\mathbb{K}$ um corpo de números, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\mathfrak{a}$ um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$. A* ***norma do ideal*** $\mathfrak{a}$ *é definida como sendo a cardinalidade do anel quociente $\mathcal{O}_{\mathbb{K}}/\mathfrak{a}$, isto é,*

$$\mathcal{N}(\mathfrak{a}) = \#\mathcal{O}_{\mathbb{K}}/\mathfrak{a}.$$

**Teorema 2.5** ([5], p.52)**.** *Sejam $\mathbb{K}$ um corpo de números e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$. Se $\mathfrak{a} = \langle\alpha\rangle$ é um ideal principal de $\mathcal{O}_{\mathbb{K}}$, então $\mathcal{N}(\mathfrak{a}) = \big|\mathcal{N}(\alpha)\big|$.*

*Demonstração.* Como $\alpha \in \mathcal{O}_{\mathbb{K}}$ e $\alpha \neq 0$, segue, pelo Corolário (2.2), que $\mathcal{N}(\alpha) \in \mathbb{Z}$. Pelo Teorema (2.4), temos que $\mathcal{O}_{\mathbb{K}}$ é um $Z$-módulo livre de posto $n$. Como $\varphi : \mathcal{O}_{\mathbb{K}} \to \mathcal{O}_{\mathbb{K}}\alpha$, definida por $\varphi(a) = a\alpha$, onde $\alpha \in \mathcal{O}_{\mathbb{K}}$, é um isomorfismo, segue que $\mathcal{O}_{\mathbb{K}}\alpha$ é um $\mathbb{Z}$-módulo livre de posto $n$. Como $\mathbb{Z}$ é um anel principal e $\mathcal{O}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre, segue pelo Teorema (1.4) que existem uma $\mathbb{Z}$-base $\{e_1, e_2, \ldots, e_n\}$ de $\mathcal{O}_{\mathbb{K}}$ e inteiros $c_1, c_2, \ldots, c_n$ tais que $\{c_1e_1, c_2e_2, \ldots, c_ne_n\}$ é $\mathbb{Z}$-base de $\mathcal{O}_{\mathbb{K}}\alpha$. A aplicação $\psi : \mathcal{O}_{\mathbb{K}} \to \prod_{i=1}^{n} \mathbb{Z}/c_i\mathbb{Z}$ definida por $\psi\big(\sum_{i=1}^{n} a_ie_i\big) = (\bar{a}_1, \bar{a}_2, \ldots, \bar{a}_n)$, é um epimorfismo e $\mathrm{Ker}(\psi) = \mathcal{O}_{\mathbb{K}}\alpha$, pois

$$\begin{aligned}
a \in \mathrm{Ker}(\psi) &\Leftrightarrow \psi(a) = \bar{0} \\
&\Leftrightarrow \bar{a}_i = \bar{0} \text{ para } i = 1, 2, \ldots, n \\
&\Leftrightarrow a_i \in c_i\mathbb{Z} \\
&\Leftrightarrow c_i | a_i \\
&\Leftrightarrow a = \sum_{i=1}^{n} a_ie_i = \sum_{i=1}^{n} b_ic_ie_i \in \mathcal{O}_{\mathbb{K}}.
\end{aligned}$$

Assim, $\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha \simeq \prod_{i=1}^{n} \mathbb{Z}/c_i\mathbb{Z}$. Logo $\#(\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha) = c_1c_2\ldots c_n$.

Seja a aplicação $\mathbb{Z}$-linear $\mu : \mathcal{O}_{\mathbb{K}} \to \mathcal{O}_{\mathbb{K}}\alpha$, definida por $\mu(e_i) = c_ie_i$ para $i = 1, 2, \ldots, n$. Logo,

$$\begin{aligned}
\mu(e_1) &= c_1e_1 + 0e_2 + \ldots + 0e_n \\
\mu(e_2) &= 0e_1 + c_2e_2 + \ldots + 0e_n \\
&\vdots \\
\mu(e_n) &= 0e_1 + 0e_2 + \ldots + c_ne_n
\end{aligned}$$

e

$$\det(\mu) = \prod_{i=1}^{n} c_i.$$

Por outro lado, temos que $B = \{c_1e_1, c_2e_2, \ldots, c_ne_n\}$ e $C = \{\alpha e_1, \alpha e_2, \ldots, \alpha e_n\}$ são $\mathbb{Z}$-bases de $\mathcal{O}_{\mathbb{K}}\alpha$. Portanto, existe um automorfismo $\varphi : \mathcal{O}_{\mathbb{K}}\alpha \to \mathcal{O}_{\mathbb{K}}\alpha$ tal que $\varphi(c_ie_i) = \alpha e_i$, para $i = 1, 2, \ldots, n$. Como a matriz mudança de base é inversível, segue que $\det(\varphi)$ é inversível em $\mathbb{Z}$, isto é, $\det(\varphi) = \pm 1$. Também, $(\varphi \circ \mu)(e_i) = \varphi\big(\mu(e_i)\big) = \varphi(c_ie_i) = \alpha e_i$, para $i = 1, 2, \ldots, n$. Assim, $(\varphi \circ \mu) = \alpha a$ para todo $a \in \mathcal{O}_{\mathbb{K}}$.

Finalmente, pela Proposição (2.5), temos que $\mathcal{N}_{\mathbb{K}/\mathbb{Q}}(\alpha) = \det(\varphi\circ\mu) = \det(\varphi)\det(\mu) = \pm 1c_1c_2\ldots c_n = \pm\#(\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha)$. Portanto, $\big|\mathcal{N}(\alpha)\big| = \#(\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha) = \mathcal{N}(\mathfrak{a})$. □

**Proposição 2.8** ([5], p.52)**.** *A norma $\mathcal{N}(\mathfrak{a})$ é finita.*

*Demonstração.* Se $\alpha \in \mathfrak{a}$ é um elemento não nulo, então $\mathcal{O}_{\mathbb{K}}\alpha \subset \mathfrak{a}$. Consideremos a aplicação $\varphi : (\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha) \to (\mathcal{O}_{\mathbb{K}}/\mathfrak{a})$ dada por $\varphi(x + \mathcal{O}_{\mathbb{K}}\alpha) = x + \mathfrak{a}$. Temos que $\varphi$ é um epimorfismo e $\mathrm{Ker}(\varphi) = (\mathfrak{a}/\mathcal{O}_{\mathbb{K}}\alpha)$. De fato, $x + \mathcal{O}_{\mathbb{K}}\alpha \in \mathrm{Ker}(\varphi)$ se, e somente se $\varphi(x + \mathcal{O}_{\mathbb{K}}\alpha) = x + \mathfrak{a} = 0$ se, e somente se $x \in \mathfrak{a}$. Desta forma, pelo Teorema (1.4), segue que

$$\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right)\Big/\left(\frac{\mathfrak{a}}{\mathcal{O}_{\mathbb{K}}\alpha}\right) \simeq \left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right).$$

Daí, segue que

$$\#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathcal{O}_{\mathbb{K}}\alpha}\right) = \#\left(\frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{a}}\right)\#\left(\frac{\mathfrak{a}}{\mathcal{O}_{\mathbb{K}}\alpha}\right).$$

Pelo Teorema (2.5), temos que $\#(\mathcal{O}_{\mathbb{K}}/\mathcal{O}_{\mathbb{K}}\alpha)$ é finito. Portanto, $\mathcal{N}(\mathfrak{a}) = \#(\mathcal{O}_{\mathbb{K}}/\mathfrak{a})$ é finito. □

**Lema 2.3** ([5], p.52)**.** *Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais não nulos de $\mathcal{O}_{\mathbb{K}}$, então $\mathcal{N}(\mathfrak{ab}) = \mathcal{N}(\mathfrak{a})\mathcal{N}(\mathfrak{b})$.*

**Proposição 2.9** ([3], p.84; [6], p.129)**.** *Se $\mathfrak{a}$ é um ideal não nulo de $\mathcal{O}_{\mathbb{K}}$, então:*

1. *$\mathcal{N}(\mathfrak{a}) = 1$ se, e somente se $\mathfrak{a} = \mathcal{O}_{\mathbb{K}}$;*

2. *Se $\mathcal{N}(\mathfrak{a})$ for um número primo, então o ideal $\mathfrak{a}$ é primo.*

*Demonstração.* **(1)** $\mathcal{N}(\mathfrak{a}) = 1 \Leftrightarrow \#(\mathcal{O}_{\mathbb{K}}/\mathfrak{a}) = 1 \Leftrightarrow \mathfrak{a} = \mathcal{O}_{\mathbb{K}}$;

**(2)** Suponhamos por absurdo que $\mathfrak{a}$ não seja um ideal primo. Assim, $\mathfrak{a} = \mathcal{O}_{\mathbb{K}}$ ou $\mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2$, onde $\mathfrak{q}_1$ e $\mathfrak{q}_2$ são ideais não nulos distintos de $\mathcal{O}_{\mathbb{K}}$.

Se $\mathfrak{a} = \mathcal{O}_{\mathbb{K}}$, pelo item **(1)**, temos que $\mathcal{N}(\mathfrak{a}) = 1$, o que é contra a hipótese.

Se $\mathfrak{a} = \mathfrak{q}_1\mathfrak{q}_2$, temos pelo Lema (2.3) que $\mathcal{N}(\mathfrak{a}) = \mathcal{N}(\mathfrak{q}_1)\mathcal{N}(\mathfrak{q}_2)$ e, como por hipótese, $\mathcal{N}(\mathfrak{a}) = p$,com $p$ primo, segue que $\mathcal{N}(\mathfrak{q}_1) = 1$ e $\mathcal{N}(\mathfrak{q}_2) = p$ ou $\mathcal{N}(\mathfrak{q}_1) = p$ e $\mathcal{N}(\mathfrak{q}_2) = 1$. Logo, $\mathfrak{q}_1 = \mathcal{O}_{\mathbb{K}}$ ou $\mathfrak{q}_2 = \mathcal{O}_{\mathbb{K}}$, o que é contra a hipótese.

Portanto, $\mathfrak{a}$ é um ideal primo de $\mathcal{O}_{\mathbb{K}}$. □

## 2.4 Discriminante

**Definição 2.16.** *Sejam $B \subseteq A$ anéis tais que $A$ é um $B$-módulo livre de posto $n$ e $\{\alpha_1, \alpha_2, \ldots, \alpha_n\} \in A^n$. Definimos **discriminante** de $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ por*

$$\mathcal{D}_{A/B}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det\big(Tr_{A/B}(\alpha_i\alpha_j)\big).$$

**Proposição 2.10** ([5], p.38)**.** *Sejam $B \subseteq A$ anéis. Se $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}, \{\beta_1, \beta_2, \ldots, \beta_n\} \in A^n$ são tais que $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, com $a_{ij} \in B$, então*

$$\mathcal{D}_{A/B}(\beta_1, \beta_2, \ldots, \beta_n) = \big(\det(a_{ij})\big)^2 \mathcal{D}_{A/B}(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

*Demonstração.* Consideremos $\beta_p = \sum_{i=1}^{n} a_{pi}\alpha_i$ e $\beta_q = \sum_{j=1}^{n} a_{qj}\alpha_j$, com $a_{pi}, a_{qj} \in B$, $1 \leq p$ e $q \leq n$. Assim,

$$\beta_p\beta_q = \sum_{i=1}^{n} a_{pi}\alpha_i \sum_{j=1}^{n} a_{qj}\alpha_j = \sum_{1\leq i,j\leq n} a_{pi}a_{qj}\alpha_i\alpha_j,$$

e então

$$\mathrm{Tr}_{A/B}(\beta_p\beta_q) = \mathrm{Tr}_{A/B}\left(\sum_{1\leq i,j\leq n} a_{pi}a_{qj}\alpha_i\alpha_j\right) = \sum_{1\leq i,j\leq n} a_{pi}a_{qj}\mathrm{Tr}_{A/B}(\alpha_i\alpha_j).$$

Na forma matricial, teremos

$$\big(\mathrm{Tr}_{A/B}(\beta_p\beta_q)_{p,q=1}^{n}\big) = (a_{pi})_{p,i=1}^{n}\big(\mathrm{Tr}_{A/B}(\alpha_i\alpha_j)\big)_{i,j=1}^{n}\big((a_{qj})_{q,j=1}^{n}\big)^{\mathrm{T}}.$$

Aplicando o determinante em ambos os lados, segue que

$$\begin{aligned}
\mathcal{D}_{A/B}(\beta_1, \beta_2, \ldots, \beta_n) &= \det\big(\mathrm{Tr}_{A/B}(\beta_p\beta_q)\big) \\
&= \det\Big((a_{pi})\big(\mathrm{Tr}_{A/B}(\alpha_i\alpha_j)\big)(a_{qj})^{\mathrm{T}}\Big) \\
&= \det(a_{pi})\det\big(\mathrm{Tr}_{A/B}(\alpha_i\alpha_j)\big)\det\Big((a_{qj})^{\mathrm{T}}\Big) \\
&= \det(a_{pi})\det\Big((a_{qj})^{\mathrm{T}}\Big)\det\big(\mathrm{Tr}_{A/B}(\alpha_i\alpha_j)\big) \\
&= \det(a_{ij})^2\mathcal{D}_{A/B}(\alpha_1, \alpha_2, \ldots, \alpha_n),
\end{aligned}$$

como queríamos provar. □

**Observação 2.8.** *Sejam $B \subseteq A$ anéis. Se $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ e $\{\beta_1, \beta_2, \ldots, \beta_n\}$ são duas bases de $A$ sobre $B$ tais que $\beta_j = \sum_{j=1}^{n} a_{ij}\alpha_j$ e $\alpha_j = \sum_{j=1}^{n} b_{ij}\beta_j$, onde $a_{ij}, b_{ij} \in B$, temos pela Proposição (2.10) que o discriminante dessas bases são associados em $B$, isto é, que o discriminante de uma base pode ser escrita em função da outra e vice-versa, ou ambas possuem determinantes nulos. Ou seja, se $(a_{ij})$ é a matriz mudança de base $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ para $\{\beta_1, \beta_2, \ldots, \beta_n\}$, então a matriz inversa $(a_{ij})^{-1}$ tem entradas em $A$. Portanto, $\det(a_{ij})$ e $\det(a_{ij})^{-1}$ são unitários em $B$.*

**Definição 2.17.** *Sejam $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau $n$, $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ e $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ uma base de $\mathcal{O}_{\mathbb{K}}$. Definimos o* ***discriminante*** *de $\mathbb{K}$ como sendo um ideal principal de $\mathbb{Z}$ gerado por $\mathcal{D}_{\mathbb{K}/\mathbb{L}}(\alpha_1, \alpha_2, \ldots, \alpha_n)$ e denotamos por $\mathcal{D}_{\mathbb{K}}$.*

**Observação 2.9.** *Note que o ideal da Definição (2.17) independe da base escolhida pois pela Observação (2.8) os determinantes de quaisquer duas bases são associados e então estes geram o mesmo ideal.*

**Lema 2.4** ([5], p.39)**.** (Lema de Dedekind). *Sejam $G$ um grupo e $\mathbb{K}$ um corpo. Se $\sigma_1, \sigma_2, \ldots, \sigma_n$ são homomorfismos distintos de $G$ no grupo multiplicativo $\mathbb{K}^*$, então $\{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ são linearmentes independentes sobre $\mathbb{K}$.*

*Demonstração.* Se $\sigma_1, \sigma_2, \ldots, \sigma_n$ são linearmentes diferentes, então existe $a_1, a_2, \ldots, a_n \in \mathbb{K}$ tais que $\sum_{i=1}^{n} a_i\sigma_i = 0$. Suponhamos que a quantidade $q$ de $a_1, a_2, \ldots, a_n$ não nulos seja mínima.

Ao reordenarmos, vamos supor que

$$\sum_{i=1}^{q} a_1\sigma_1(x) = 0, \text{para todo } x \in G. \tag{2.2}$$

Temos $q \geq 2$ desde que $\sigma_1, \sigma_2, \ldots, \sigma_q$ sejam não nulos. Para elementos $x, y \in G$, temos

$$\sum_{i=1}^{q} a_i\sigma_i(xy) = \sum_{i=1}^{q} a_i\sigma_i(x)\sigma_i(y) = 0. \tag{2.3}$$

Se multiplicarmos a equação (2.2) por $\sigma_1(y)$, temos

$$\sigma_1(y)\sum_{i=1}^{q} a_i\sigma_i(x) = \sum_{i=1}^{q} \sigma_1(y)a_i\sigma_i(x) = \sum_{i=1}^{q} a_i\sigma_1(y)\sigma_i(x) = 0. \tag{2.4}$$

Subtraindo a equação (2.4) pela equação (2.3), obtemos

$$\begin{aligned}
&\sum_{i=1}^{q} a_i\sigma_1(y)\sigma_i(x) - \sum_{i=1}^{q} a_i\sigma_i(x)\sigma_i(y) &&= 0\\
\Rightarrow\quad &\sum_{i=1}^{q} \big(a_i\sigma_1(y)\sigma_i(x) - a_i\sigma_i(x)\sigma_i(y)\big) &&= 0\\
\Rightarrow\quad &\sum_{i=2}^{q} \big(a_i\sigma_1(y)\sigma_i(x) - a_i\sigma_i(x)\sigma_i(y)\big) &&= 0, \text{ pois para } i = 1 \text{ a parcela zera}\\
\Rightarrow\quad &\sum_{i=2}^{q} a_i\big(\sigma_1(y) - \sigma_i(y)\big)\sigma_i(x) &&= 0.
\end{aligned}$$

Como isto acontece para qualquer $x \in G$ e como $q$ é tomado como o menor valor possível, então podemos tomar a parcela $a_2\big(\sigma_1(y) - \sigma_2(y)\big)$. Como a última equação é linearmente independente, segue que $a_i\big(\sigma_1(y) - \sigma_i(y)\big) = 0$. Assim $\sigma_1(y) = \sigma_2(y)$ para todo $y \in G$, desde que $a_2 \neq 0$. Mas, isto contradiz com a hipótese de que $\sigma_1, \sigma_2, \ldots, \sigma_n$ são distintos.

□

**Proposição 2.11** ([5], p.39)**.** *Sejam $\mathbb{K}/\mathbb{L}$ uma extensão finita de grau $n$ e $\sigma_1, \sigma_2, \ldots, \sigma_n$ são os monomorfismos distintos de $\mathbb{K}$ em um corpo algebricamente fechado $\mathbb{F}$ contendo $\mathbb{L}$. Se $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{L}$, então*

$$\mathcal{D}_{\mathbb{K}/\mathbb{L}}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det\big(\sigma_i(\alpha_j)\big)^2 \neq 0.$$

*Demonstração.* Por definição, temos que $\mathcal{D}_{\mathbb{K}/\mathbb{L}}(\alpha_1, \alpha_2, \ldots, \alpha_n) = \det\big(\mathrm{Tr}(\alpha_i\alpha_j)\big)$. Como o traço $\alpha_i\alpha_j$ é a soma dos seus conjugados, segue que

$$\begin{aligned}
\mathcal{D}_{\mathbb{K}/\mathbb{L}}(\alpha_1, \alpha_2, \ldots, \alpha_n) &= \det\big(\mathrm{Tr}(\alpha_i\alpha_j)\big) \\
&= \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j)\right) \\
&= \det\left(\sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j)\right) \\
&= \det\big(\sigma_k(\alpha_i)\big)\det\big(\sigma_k(\alpha_j)\big) \\
&= \Big(\det\big(\sigma_i(\alpha_j)\big)\Big)^2.
\end{aligned}$$

Resta mostrar que $\det\big(\sigma_i(\alpha_j)\big) \neq 0$. Suponhamos por absurdo que $\det\big(\sigma_i(\alpha_j)\big) = 0$. Então, as colunas da matriz $\big(\sigma_k(\alpha_j)\big)_{j,k=1}^{n}$ são linearmentes dependentes. Assim, existem $a_1, a_2, \ldots, a_n \in \mathbb{F}$ não todos nulos tais que $\sum_{i=1}^{n} a_i\sigma_i(\alpha_j) = 0$, para todo $j = 1, 2, \ldots, n$. Assim, pela linearidade concluímos que $\sum_{i=1}^{n} a_i\sigma_i(\alpha) = 0$, para todo $\alpha \in \mathbb{K}$, o que contradiz o Lema de Dedekind. Portanto, $\det\big(\sigma_i(\alpha_j)\big) \neq 0$. □

**Proposição 2.12** ([6], p.55)**.** *Se $\mathbb{K}/\mathbb{L}$ é uma extensão finita de grau $n$ tal que $\mathbb{K} = \mathbb{L}(\alpha)$ e $p$ o polinômio minimal de $\alpha$ sobre $\mathbb{L}$, então*

$$\mathcal{D}_{\mathbb{K}/\mathbb{L}}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)}\mathcal{N}\big(f'(\alpha)\big),$$

*onde $f'$ é a derivada de $f$.*

*Demonstração.* Se $\alpha_1, \alpha_2, \ldots, \alpha_n$ são as raízes de $p$ em alguma extensão de $\mathbb{K}$, então são conjugados de $\alpha$. Pela Proposição (2.11) temos que $\mathcal{D}_{\mathbb{K}/\mathbb{L}}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \Big(\det\big(\sigma_i(\alpha_j)\big)\Big)^2 = \big(\det(\alpha_j^i)\big)^2$, com $i = 1, 2, \ldots, n$ e $j = 0, 1, \ldots, n-1$. Como $\det(\alpha_j^i)$ é um determinante de

Vandermonde, segue que

$$\begin{aligned}
\big(\det(\alpha_j^i)\big)^2 &= \left(\prod_{1\le k<i\le n}(\alpha_i-\alpha_k)\right)^2 \\
&= \prod_{1\le k<i\le n}\big((\alpha_i-\alpha_k)(\alpha_i-\alpha_k)\big) \\
&= (-1)^{\frac{1}{2}n(n-1)}\prod_{1\le k<i\le n,k\neq i}(\alpha_i-\alpha_k) \\
&= (-1)^{\frac{1}{2}n(n-1)}\prod_{i=1}^{n}\left(\prod_{k=1,k\neq i}^{n}(\alpha_i-\alpha_k)\right) \\
&= (-1)^{\frac{1}{2}n(n-1)}\prod_{i=1}^{n}f'(\alpha) \\
&= (-1)^{\frac{1}{2}n(n-1)}\mathcal{N}\big(f'(\alpha)\big),
\end{aligned}$$

como queríamos provar. □

**Teorema 2.6** ([6], p.44)**.** *O discriminante de qualquer base de $\mathbb{K}=\mathbb{Q}(\theta)$ é racional e não nulo. Se todos os $\mathbb{K}$-monomorfismos de $\theta$ são reais, então o discriminante de qualquer base é positivo.*

*Demonstração.* Seja $\{1,\alpha,\alpha^2,\ldots,\alpha^{n-1}\}$ uma base de $\mathbb{K}=\mathbb{Q}(\theta)$. Se os conjugados de $\alpha$ são $\theta_1,\theta_2,\ldots,\theta_n$, então

$$\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1,\alpha,\ldots,\alpha^{n-1})=\begin{vmatrix}\sigma_1(1) & \sigma_1(\alpha) & \cdots & \sigma_1(\alpha^{n-1})\\ \sigma_2(1) & \sigma_2(\alpha) & \cdots & \sigma_2(\alpha^{n-1})\\ \vdots & \vdots & \ddots & \vdots\\ \sigma_n(1) & \sigma_n(\alpha) & \cdots & \sigma_n(\alpha^{n-1})\end{vmatrix}^2=\begin{vmatrix}1 & \theta_1 & \cdots & \theta_1^n\\ 1 & \theta_2 & \cdots & \theta_2^n\\ \vdots & \vdots & \ddots & \vdots\\ 1 & \theta_n & \cdots & \theta_n^n\end{vmatrix}^2=\big(\det(\theta_i^j)\big)^2.$$

Um determinante da forma $\Delta=\det(t_i^j)$ é chamado de **Determinante de Vandermonde** e é dado por

$$\Delta=\prod_{1\le i<j\le n}(t_i-t_j).$$

Para verificar isto, vamos pensar em tudo como pertecente a $\mathbb{Q}[t_1,t_2,\ldots,t_n]$. Então para $t_i=t_j$ o determinante tem duas linhas (ou colunas) múltiplas, logo, o determinante tem valor zero. Temos que $\Delta$ é divisível por cada $(t_i-t_j)$. Para evitar que se repita algum

fator, tomemos $i < j$. Comparando os graus que $\Delta$ não tem outros fatores não constantes, comparando os coeficientes de $t_1, t_2^2, \ldots, t_n^n$. Logo

$$\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) = \left( \prod_{1 \leq j < i \leq n} (\theta_i - \theta_j) \right)^2.$$

Logo, $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ é racional desde que $\theta_i$ sejam distintos e

$$\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) \neq 0.$$

Agora, se $\{\beta_1, \beta_2, \ldots, \beta_n\}$ é uma outra base de $\mathbb{K}$, então

$$\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n) = \big(\det(c_{ik})\big)^2 \mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}),$$

para $c_{ik} \in \mathbb{Q}$, com $\det(c_{ik}) \neq 0$, tal que $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n) \neq 0$ e $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n) \in \mathbb{Q}$. Logo, se todos os $\theta_i$ são reais, então $\mathcal{D}_{\mathbb{K}/\mathbb{Q}}(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ é um número real positivo. □

## 2.5 Anéis de Dedekind

**Definição 2.18.** *Dizemos que um anel $A$ é um **anel de Dedekind** de satisfaz as seguintes condições:*

1. *$A$ é integralmente fechado;*
2. *$A$ é noetheriano;*
3. *Todo ideal primo não nulo de $A$ é maximal.*

**Teorema 2.7** ([5], p.49)**.** *Se $A$ é um anel de Dedekind, $\mathbb{L}$ é o seu corpo de frações, $\mathbb{L} \subseteq \mathbb{K}$ uma extensão finita de grau $n$ e $\mathcal{O}_\mathbb{K}$ o anel dos inteiros de $\mathbb{K}$ sobre $A$. Então $\mathcal{O}_\mathbb{K}$ é um anel de Dedekind.*

*Demonstração.* Pelas Proposições (2.4) e (2.7), temos que $\mathcal{O}_\mathbb{K}$ é integralmente fechado e noetheriano, respectivamente. Assim, falta mostrar que todo ideal primo não nulo de $\mathcal{O}_\mathbb{K}$ é maximal.

Seja $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$ um ideal primo não nulo. Como $A \subset \mathcal{O}_{\mathbb{K}}$, segue pela Proposição (1.5) que $\mathfrak{p} \cap A$ é um ideal primo de $A$. Vamos mostrar que $\mathfrak{p} \cap A$ é não nulo. Seja $\alpha \in \mathfrak{p}$ e $\alpha \neq 0$. Como $\mathfrak{p} \subset \mathcal{O}_{\mathbb{K}}$, segue que $\alpha \in \mathcal{O}_{\mathbb{K}}$. Assim, existem $a_i \in A$, para $i = 0, 1, \ldots, n-1$, não todos nulos tais que

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0,$$

e que $n$ seja mínimo. Logo, $a_0 \neq 0$ pois caso contrário, obteríamos uma equação de grau menor. Assim,

$$a_0 = \alpha(-\alpha^{n-1} - a_{n-1}\alpha^{n-2} - \ldots - a_1) \in \alpha\mathcal{O}_{\mathbb{K}} \cap A \subset \mathfrak{p} \cap A.$$

Portanto, $\mathfrak{p} \cap A \neq 0$. Como $\mathfrak{p} \cap A$ é um ideal primo de $A$ e $A$ é Dedekind, segue que $\mathfrak{p} \cap A$ é um ideal maximal de $A$ e assim $\dfrac{A}{\mathfrak{p} \cap A}$ é corpo.

Seja a aplicação $\varphi : A \xrightarrow{i} \mathcal{O}_B \xrightarrow{\pi} \mathcal{O}_{\mathbb{K}}/\mathfrak{p}$, onde $i$ é a inclusão e $\pi$ é a projeção. Como $\mathcal{O}_{\mathbb{K}}$ é inteiro sobre $A$, segue que $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ é inteiro sobre $\dfrac{A}{\mathfrak{p} \cap A}$. Assim,

$$\frac{A}{\mathfrak{p} \cap A} \simeq \mathrm{Im}(\varphi) \subset \frac{\mathcal{O}_{\mathbb{K}}}{\mathfrak{p}}.$$

Logo, como $\dfrac{A}{\mathfrak{p} \cap A}$ é um corpo, segue que $\mathcal{O}_{\mathbb{K}}/\mathfrak{p}$ é um corpo. Portanto, $\mathfrak{p}$ é maximal.

□

**Corolário 2.3** ([1], p.43)**.** *Se $\mathbb{K}$ é um corpo de números de grau $n$, então o anel dos inteiros algébricos de $\mathbb{K}$ é um anel de Dedekind.*

*Demonstração.* Como $\mathbb{Z}$ é um anel de Dedekind, pelo Teorema (2.7) segue o resultado. □

**Observação 2.10.** *O anel dos inteiros $\mathcal{O}_{\mathbb{K}}$ de um corpo de números é um anel de Dedekind, mas nem sempre é principal. De fato, vimos que em $\mathcal{O}_{\mathbb{K}} = \mathbb{Z}[\sqrt{-5}]$, $(1+\sqrt{-5})(1-\sqrt{-5}) = 2 \cdot 3$ São duas fatorações distintas de $6$, cujas normas são $6$, $6$, $4$ e $9$, respectivamente. Logo, $\mathcal{O}_{\mathbb{K}}$ não é um domínio fatorial. Se o elemento $1+\sqrt{-5}$ possuisse um divisor não trivial, então $\mathcal{N}(1-\sqrt{-5}) = 6$ também possuiria um divisor não trivial. Mas isso é impossível, pois a equação $a^2 + 5b^2 = 2$ ou $3$ não possui solução inteira. Assim, $1+\sqrt{-5}$ é um elemento primo.*

*Agora, se $\mathcal{O}_{\mathbb{K}}$ fosse principal e como $1+\sqrt{-5}$ divide $2 \cdot 3$, teríamos que $1+\sqrt{-5}$ divide $2$ ou $3$. Tomando as normas obtemos que $6$ divide $4$ ou $9$, o que é um absurdo. Portanto, $\mathcal{O}_{\mathbb{K}}$ não é principal.*

## 2.6 Ideais Fracionários

**Definição 2.19.** *Seja $\mathbb{K}$ um corpo de números. Um $\mathcal{O}_{\mathbb{K}}$-módulo $\mathfrak{I}$ de $\mathbb{K}$ é um* ***ideal fracionário*** *se existe $d \in \mathcal{O}_{\mathbb{K}}$ não nulo tal que $d\mathfrak{I} \subseteq \mathcal{O}_{\mathbb{K}}$. Em particular, os ideais inteiros de $A$ são ideais fracioários com $d = 1$.*

**Observação 2.11.** *Segue da Definição (2.19) que os elementos de um ideal fracionário $\mathfrak{I}$ tem um denominador comum $d \in A$.*

**Lema 2.5** ([1], p.43)**.** *Sejam $\mathbb{K}$ um corpo de números de grau $n$ e $\mathcal{O}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$ sobre $\mathbb{Z}$. Se $\mathfrak{I}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, então existe $d \in \mathbb{Z} - \{0\}$ tal que $d\mathfrak{I} \subset \mathcal{O}_{\mathbb{K}}$.*

*Demonstração.* Como $\mathbb{K}$ é um corpo de números de grau $n$, temos pelo Teorema (2.1) que existe $\alpha \in \mathbb{K}$ tal que $\mathbb{K} = \mathbb{Q}(\alpha)$ e $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ é uma base de $\mathbb{K}$ sobre $\mathbb{Q}$. Como $\mathfrak{I}$ é um ideal fracionário de $\mathcal{O}_{\mathbb{K}}$, segue que $\mathfrak{I}$ é um $\mathbb{Z}$-módulo livre de posto $n$.

Seja $\{\gamma_1, \gamma_2, \ldots, \gamma_n\}$ uma base de $\mathfrak{I}$. Para cada $i$, temos que $\gamma_i = \sum_{j=0}^{n-1} a_{ij}\alpha^j$ tal que $a_{ij} \in \mathbb{Q}$, para todo $i = 1, 2, \ldots n$ e $j = 0, 1, \ldots, n-1$. Como $a_{ij} \in \mathbb{Q}$, para todo $i, j = 1, 2, \ldots, n$, segue que $a_{ij} = \dfrac{b_{ij}}{c_{ij}}$, com $b_{ij}, c_{ij} \in \mathbb{Z}, c_{ij} \neq 0$, para todo $i, j = 1, 2, \ldots, n$.

Seja $d = \text{mmc}\{c_{ij} \mid i = 1, 2, \ldots, n \text{ e } j = 0, 1, \ldots, n-1\}$. Temos que $d\gamma_i \in \mathbb{Z}[\alpha]$, para todo $i = 1, 2, \ldots, n$. Como $\mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbb{K}}$, temos que

$$d\mathfrak{I} = d\sum_{i=1}^{n} \mathbb{Z}\gamma_i = \sum_{i=1}^{n} \mathbb{Z}d\gamma_i \subset \mathbb{Z}[\alpha] \subset \mathcal{O}_{\mathbb{K}},$$

como queríamos provar. □

**Proposição 2.13** ([4], p.42)**.** *Se $A$ é um domínio noetheriano, então todo ideal fracionário $\mathfrak{I}$ de $A$ é um $A$-módulo finitamente gerado.*

*Demonstração.* Como $\mathfrak{I}$ é um ideal fracionário de $A$, segue pelo Lema (2.5) que existe $d \in A - \{0\}$ tal que $d\mathfrak{I} \subseteq A$. Assim, $\mathfrak{I} \subseteq d^{-1}A$. A aplicação $\varphi : A \longrightarrow d^{-1}A$, definida por $\varphi(x) = d^{-1}x$ é um isomorfismo. Assim, $A$ é isomorfo a $d^{-1}A$. Como $A$ é noetheriano, segue que $d^{-1}A$ também é noetheriano. Logo, $\mathfrak{I}$ é um $A$-módulo finitamente gerado. □

**Proposição 2.14** ([5], p.50)**.** *Se $A$ é um anel de Dedekind que não é corpo, $\mathbb{K}$ seu corpo de frações e $\mathfrak{m}$ um ideal maximal de $A$, então o conjunto $\mathfrak{m}' = \{x \in \mathbb{K} \mid x\mathfrak{m} \subset A\}$ é um ideal fracionário de $A$.*

*Demonstração.* Seja $\mathfrak{m}$ um ideal maximal de $A$. Como $A$ não é um corpo, segue que $\mathfrak{m} \neq \{0\}$. Consideremos $\mathfrak{n}' = \{x \in \mathbb{K} \mid x\mathfrak{m} \subset A\}$. Temos que $\mathfrak{n}'$ é um ideal fracionário, pois $\mathfrak{n}'$ é um $A$-módulo tal que $\mathfrak{n}' \subseteq \mathbb{K}$ e se $c \in \mathfrak{m}, c \neq 0$, então $c\mathfrak{m}' \subseteq A$. □

**Lema 2.6** ([4], p.44)**.** *Se $A$ é um anel de Dedekind que não é um corpo e $\mathbb{K}$ o seu corpo de frações, então todo ideal maximal $\mathfrak{m}$ de $A$ é inversível no conjunto dos ideais fracionários de $A$.*

*Demonstração.* Considere o ideal fracionário $\mathfrak{n} = \{x \in \mathbb{K} \mid x\mathfrak{m} \subset A\}$. Vamos mostrar que $\mathfrak{nm} = A$. Pela definição de $\mathfrak{n}$ temos $\mathfrak{nm} \subset A$. Por outro lado, $A \subset \mathfrak{n}$, pois $\mathfrak{m}$ é um ideal de $A$. Assim, $\mathfrak{m} = \mathfrak{m}A \subset \mathfrak{mn} \subset A$. Como $\mathfrak{m}$ é maximal, segue que $\mathfrak{m} = \mathfrak{nm}$ ou $\mathfrak{nm} = A$.

Suponhamos que $\mathfrak{m} = \mathfrak{nm}$ e consideremos $\alpha \in \mathfrak{n}$. Então $\alpha\mathfrak{m} \subset \mathfrak{m}$, $\alpha^2\mathfrak{m} \subset \alpha\mathfrak{m} \subset \mathfrak{m}$ e $\alpha^n\mathfrak{m} \subset \mathfrak{m}$, para todo $n \in \mathbb{N}$. Seja $d \in \mathfrak{m}, d \neq 0$. Então $d\alpha^n \in A$. Portanto, $A[\alpha]$ é um ideal fracionário.

Como $A$ é noetheriano, pela Proposição (**??**), segue que $A[\alpha]$ é um $A$-módulo finitamente gerado. Pelo Teorema (2.2), segue que $\alpha$ é inteiro sobre $A$. Sendo $A$ integralmente fechado, segue que $\alpha \in A$. Assim, $\mathfrak{n} \subset A$ e como $A \subset \mathfrak{n}$, segue que $\mathfrak{n} = A$. Falta mostrar que esta igualdade é impossível.

Seja $a \in \mathfrak{m}$. Pela Proposição (1.6), temos que $\langle a \rangle = aA \supset \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$, onde os $\mathfrak{p}_i$ são ideais primos não nulos de $A$, com $n$ o menor valor possível. Assim, $\mathfrak{m} \supset aA \supset \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_n$. Pela Proposição (1.5), $\mathfrak{m}$ contém um dos $\mathfrak{p}_i$, para algum $i = 1, 2, \dots, n$.

Sem perda de generalidade, digamos que seja $\mathfrak{p}_1$, isto é, $\mathfrak{m} \supset \mathfrak{p}_1$. Como $A$ é Dedekind, segue que $\mathfrak{m} = \mathfrak{p}_1$, pois $\mathfrak{p}_1$ é maximal.

Agora, consideremos que $\mathfrak{q} = \mathfrak{q}_2\mathfrak{q}_3 \dots \mathfrak{q}_n$. Então $aA \supset \mathfrak{mq}$ e $aA \neq \mathfrak{q}$ pela minimidade de $n$. Assim, existe $b \in \mathfrak{q}$ e $b \notin \langle a \rangle$ tal que $\mathfrak{m}b \subset \langle a \rangle$. Logo, $(b/a)\mathfrak{m} \subseteq A$ e, assim $b/a \in \mathfrak{n}$. Como $b \notin \langle a \rangle$, segue que $b/a \notin A$. Logo $\mathfrak{n} \neq A$. Portanto, $\mathfrak{mn} = A$. □

**Teorema 2.8** ([5], p.50)**.** *Se $A$ é um anel de Dedekind que não é corpo, então:*

1. *Todo ideal fracionário $\mathfrak{I}$ não nulo de $A$ é um produto de ideais primos de $A$, de modo único, isto é,*

$$\mathfrak{I} = \prod_{i=1}^{n} \mathfrak{p}_i^{e_i},$$

*onde $e_1, e_2, \dots, e_n$ são inteiros positivos;*

*2. O conjunto dos ideais fracionários de $A$ formam um grupo.*

*Demonstração.* **(1)** Se $\mathfrak{I}$ é um ideal fracionário de $A$, então existe $d \in A - \{0\}$ tal que $d\mathfrak{I} \subseteq A$. Notemos que $\mathfrak{I} = (d\mathfrak{I})(d^{-1}A)$. Assim, é suficiente mostrar o resultado para ideais inteiros.

Seja $F$ a família dos ideais inteiros de $A$, não nulos e que não são um produto de ideais primos de $A$. Suponhamos que $F \neq \varnothing$. Como $A$ é noetheriano, segue que $F$ tem um elemento maximal $\mathfrak{m}$. Temos que $\mathfrak{m} \neq A$, pois $A$ é o produto da coleção vazia de ideais primos. Assim, $\mathfrak{m} \subseteq \mathfrak{p}$, onde $\mathfrak{p}$ é um ideal maximal de $A$.

Pelo Lema (2.6), temos que $\mathfrak{q} = \{x \in \mathbb{K} \mid x\mathfrak{p} \subset A\}$ tal que $\mathfrak{pq} = A$. Como $\mathfrak{m} \subseteq \mathfrak{p}$, segue que $\mathfrak{mq} \subseteq \mathfrak{pq} = A$. Além disso, como $A \subset \mathfrak{q}$, segue que $\mathfrak{m} = \mathfrak{m}A \subset \mathfrak{mq} \subset A$. Temos que $\mathfrak{m} \subsetneq \mathfrak{mq}$, pois se $\mathfrak{m} = \mathfrak{mq}$ e também se $\alpha \in \mathfrak{q}$, então $\mathfrak{am} \subset \mathfrak{m}$, $\alpha^2\mathfrak{m} \subset \alpha\mathfrak{m} \subset \mathfrak{m}$ e $\alpha^n\mathfrak{m} \subset \mathfrak{m}$, para todo $n \in \mathbb{N}$. Assim, se $d \in \mathfrak{m} - \{0\}$, então $a\alpha^n \in \mathfrak{m} \subseteq A$. Portanto, $A[\alpha]$ é um ideal fracionário de $A$.

Como $A$ é noetheriano, pela Proposição (**??**), segue que $A[\alpha]$ é um $A$-módulo finitamente gerado. Pelo Teorema (2.2), segue que $\alpha$ é inteiro sobre $A$, e como $A$ é integralmente fechado, segue que $\alpha \in A$. Portanto, $\mathfrak{q} \subset A$ e assim $\mathfrak{q} = A$. Mas, isto é impossível, pois se $\mathfrak{q} = A$, então $\mathfrak{p} = \mathfrak{p}A = \mathfrak{pq} = A$, o que é um absurdo, pois $\mathfrak{p}$ é um ideal primo.

Pela maximidade de $\mathfrak{m}$ e como $\mathfrak{m} \subseteq \mathfrak{mq}$ temos que $\mathfrak{mq} \notin F$, ou seja, $\mathfrak{mq} = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_n$, onde os $\mathfrak{p}_i$ são ideais primos de A, para $i = 1, 2, \ldots, n$. Multiplicando por $\mathfrak{p}$ ambos os lados, temos que $\mathfrak{m} = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_n\mathfrak{p}$, o que é um absurdo, pois $\mathfrak{m} \in F$. Portanto, $F = \varnothing$.

**(2)** Pelo Lema (2.6), temos que todo ideal $\mathfrak{m}$ de $A$ é inversível. Além disso, $A$ é o elemento neutro e a multiplicação de ideais é associativa. □

# Considerações Finais

Ao realizar a graduação de Matemática, pude observar que ela pode ser dividida em áreas. Porém, o que é visto na graduação é partes enxutas e breves dos conteúdos. Para querer se aprofundar, é preciso buscar outros tópicos, como a teoria dos números algébricos. Com o propósito de aprofundar os conhecimentos na álgebra, realizamos este trabalho.

Pudemos notar que a teoria dos números algébricos é uma extensão natural da teoria dos números inteiros. Enquanto esse último trabalha com as propriedades do conjunto dos números inteiros Z, a primeira surgiu como parte da busca de soluções dos problemas da teoria dos números. Na teoria dos números algébricos, com o apoio da álgebra, pudemos estender as propriedades clássicas dos anéis, corpos e ideais para módulos, módulos noetherianos, os anéis dos inteiros, ...

Com este trabalho, poderemos dar continuidade para estudar outras estruturas importantes da teoria dos números algébricos. Corpos quadráticos, corpos ciclotômicos, ramificações de ideais e reticulados são alguns exemplos dessas estruturas.

As aplicações da teoria dos números algébricos vão além da própria matemática. Fatoração de inteiros usando crivos de um corpo de números, teste de primalidade, a demonstração do Último Teorema de Fermat por Andrew Wiles, geometria aritmética, construção de reticulados e aplicações nas equações diofantinas são alguns exemplos da aplicabilidade da teoria dos números algébricos. Áreas da Ciências da Computação e Engenharias acabam por empregar as aplicações.

# Referências Bibliográficas


[1] BENEDITO, C. W. O. **Família de Reticulados Algébricos e Reticulados Ideais**. Dissertação (Mestrado em Matemática) - Universidade Estadual Paulista, São José do Rio Preto, 2010.

[2] DOMINGUES, H. H.; IEZZI, G. **Álgebra Moderna**. 3. ed. São Paulo: Atual, 1995.

[3] ENDLER, O. **Teoria dos Números Algébricos**. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 1986. (Coleção Projeto Euclides).

[4] JORGE, G. C. **Reticulados Ideais Via Corpos Abelianos**. Dissertação (Mestrado em Matemática) - Universidade Estadual Paulista, São José do Rio Preto Atual, 2008.

[5] SAMUEL, P. **Algebraic Theory of Numbers**. Paris: Hermann, 1970.

[6] STEWART, I. N.; TALL, D. O. **Algebraic Number Theory**. London: Chapman and Hall, 1987.