1 - Corpos de números

Carina Alves
Antonio Aparecido de Andrade

ALVES, C., and ANDRADE, AA. Corpos de números. In: *Reticulados via corpos ciclotômicos* [online]. São Paulo: Editora UNESP, 2014, pp. 23-68. ISBN 978-85-68334-39-3. Available from SciELO Books <http://books.scielo.org>.

1
Corpos de números

1.1 Introdução

Neste capítulo, apresentamos uma coletânea de resultados básicos de teoria algébrica dos números. O objetivo é fornecer a base teórica para o desenvolvimento dos demais capítulos. Aqui introduzimos os conceitos de módulos, elementos inteiros sobre um anel, elementos algébricos sobre um corpo e extensões algébricas, norma e traço em uma extensão, discriminante, anéis noetherianos e anéis de Dedekind, norma de um ideal e formas quadráticas sobre o $\mathbb{R}^n$.

1.2 Módulos

Iniciamos esta seção com as definições de módulos e submódulos. Em seguida apresentamos um teorema que será de grande utilidade posteriormente.

Definição 1.2.1. *Seja A um anel. Um A-***módulo** *M é um grupo abeliano (aditivo) munido de uma aplicação $A \times M \longrightarrow M$, denotada por $(a, m) \longrightarrow am$, tal que, para quaisquer $a, b \in A$ e $x, y \in M$, tem-se:*

i) $a(x + y) = ax + ay$;

ii) $(a + b)x = ax + bx$;

iii) $(ab)x = a(bx)$;

iv) $1x = x$.

Definição 1.2.2. *Sejam A um anel 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, também é um A-módulo.*

Um A-módulo M é dito **finitamente gerado** se existem $x_1, \cdots, x_r \in M$ tais que $M = Ax_1 + \cdots + Ax_r$ e, neste caso, dizemos que $x_1, \cdots, x_r$ formam um **sistema de geradores** de M. Um conjunto de elementos $y_1, \cdots, y_s \in M$ são linearmente independentes (sobre A) se a igualdade $\sum_{j=1}^{s} a_j y_j = 0$, com $a_j \in A$, implicar que $a_1 = \cdots = a_s = 0$. Mas, se além disso, $y_1, \cdots, y_s$ formarem um sistema de geradores de M, então eles formam uma base de M. Porém, é importante notar que nem todo módulo finitamente gerado possui um base. Um A-módulo que possui uma base é chamado de um A-**módulo livre**, e o número de elementos da base é chamado de **posto** de M.

Teorema 1.2.1. *Sejam A um anel principal, M um A-módulo livre de posto n, e M' um A-submódulo de M. Então:*
i) M' é livre de posto q, $0 \leq q \leq n$.
ii) Se $M' \neq 0$, então existe uma base $\{e_1, \cdots, e_n\}$ de M e elementos

não nulos $a_1, \cdots, a_q \in A$ *tais que* $\{a_1e_1, \cdots, a_qe_q\}$ *é uma base de* M' *e que* a_i *divide* a_{i+1}, $1 \leq i \leq q-1$.

Demonstração. (Samuel, 1976, p.21, Teo.1). ■

1.3 Elementos inteiros sobre um anel

Nesta seção apresentamos as definições de elemento algébrico, extensão algébrica e polinômio minimal.

Definição 1.3.1. *Sejam* B *um anel e* $A \subset B$ *um subanel. Um elemento* $\alpha \in B$ *é chamado* **inteiro** *sobre* A *se* α *é raiz de um polinômio mônico com coeficientes em* A. *Se* $A = \mathbb{Z}$ *e* $B \subset \mathbb{C}$, *dizemos que* α *é um* **inteiro algébrico**.

Observação 1.3.1. *Denotaremos o conjunto dos elementos que estão em* B *e são inteiros sobre* A *por* $\mathbb{A}_B$, *ou seja,* $\mathbb{A}_B = \{\alpha \in B : \alpha \text{ é inteiro sobre } A\}$.

Observação 1.3.2. $\mathbb{A}_B$ *é chamado* **fecho inteiro** *de* A *em* B *ou anel dos inteiros de* A *em* B. *Se* A *é um domínio e* $B = \mathbb{K}$ *é o corpo de frações de* A, *dizemos que* $\mathbb{A}_{\mathbb{K}}$ *é o fecho inteiro de* A *em* $\mathbb{K}$.

Exemplo 1.3.1. *O elemento* $\alpha = \sqrt{2} + \sqrt{3}$ *é inteiro sobre* $\mathbb{Z}$, *pois é raiz do seguinte polinômio* $X^4 - 10X^2 + 1 \in \mathbb{Z}[X]$.

Definição 1.3.2. *Sejam* B *um anel e* $A \subset B$ *um subanel. Seja* $p(X) \in B[X]$ *um polinômio mônico tal que* $p(\alpha) = 0$, *com* $\alpha \in B$. *A relação* $p(\alpha) = 0$ *é chamada uma* **equação de dependência inteira** *de* α *sobre* A.

Exemplo 1.3.2. *O elemento* $\alpha = \sqrt{2} \in \mathbb{R}$ *é inteiro sobre* $\mathbb{Z}$. *A relação* $\alpha^2 - 2 = 0$ *é uma equação de dependência inteira.*

Teorema 1.3.1. *(*Samuel,1967, p.27, Teo.1*) Sejam* B *um anel,* A *um subanel de* B *e* α *um elemento de* B*. Então as seguintes condições são equivalentes:*

1) α *é inteiro sobre* A*.*

2) *O anel* $A[\alpha]$ *é um* A*-módulo finitamente gerado.*

3) *Existe um subanel* R *de* B *tal que* R *é um* A*-módulo finitamente gerado contendo* A *e* α*.*

Demonstração (1) $\Longrightarrow$ (2) Como $\alpha \in B$ é inteiro sobre A, então $\alpha \in \mathbb{A}_B$, ou seja, α é raiz de um polinômio mônico com coeficientes em A. Logo existem $a_0, a_1, \cdots, a_{n-1} \in A$ não todos nulos tal que

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Seja $M = [1, \alpha, \alpha^2, \cdots, \alpha^{n-1}]$ o A-módulo finitamente gerado. Vamos mostrar que $A[\alpha] = M$. Por definição

$$A[\alpha] = \left\{ \sum_i a_i\alpha^i \ : \ a_i \in A \right\}$$

e assim, pelo modo como definimos M, segue que $M \subset A[\alpha]$. Por outro lado,

$$\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0) \tag{1.1}$$

e assim $\alpha^n \in M$. Portanto $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}, \alpha^n \in M$. Agora provaremos por indução sobre j que $\alpha^j \in M$, $\forall\, j = n+1, n+2, \cdots$. Para $j = 0, \cdots, n$ vimos acima que o resultado é válido. Agora suponhamos que o resultado seja válido para $j > n$ e provemos que o resultado vale para $j+1$. Sendo $\alpha^j = b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ com $b_i \in A$, então

$$\alpha^{j+1} = b_0\alpha + b_1\alpha^2 + \cdots + b_{n-2}\alpha^{n-1} + b_{n-1}\alpha^n. \tag{1.2}$$

Substituindo (1.1) em (1.2) temos

$$\alpha^{j+1} = -b_{n-1}a_0 + (b_0 - b_{n-1}a_1)\alpha + \cdots + (b_{n-2} - b_{n-1}a_{n-1})\alpha^{n-1}$$

e assim $\alpha^{j+1} \in M$. Portanto $A[\alpha] \subseteq M$. Portanto $A[\alpha] = M$.

(2) $\Longrightarrow$ (3) Como $A \subset A[\alpha]$, $\alpha \in A[\alpha]$ e, por hipótese, $A[\alpha]$ é um A-módulo finitamente gerado, então é suficiente tomar $R = A[\alpha]$.

(3) $\Longrightarrow$ (1) Seja R um A-módulo finitamente gerado que contém A e α e sejam $\{y_1, y_2, \cdots, y_n\}$ os geradores de R, ou seja, $R = Ay_1 + \cdots + Ay_n$. Como $\alpha \in R$ e como R é um subanel de B segue que $\alpha y_i \in R$, $\forall\, i = 1, \cdots, n$. Assim,

$$\begin{cases} \alpha y_1 = a_{11}y_1 + a_{12}y_2 + \cdots + a_{1n}y_n \\ \alpha y_2 = a_{21}y_1 + a_{22}y_2 + \cdots + a_{2n}y_n \\ \vdots \\ \alpha y_n = a_{n1}y_1 + a_{n2}y_2 + \cdots + a_{nn}y_n \end{cases}, \quad a_{ij} \in A.$$

Daí segue que $\sum_{j=1}^{n}(\delta_{ij}\alpha - a_{ij})y_j = 0$; onde $\delta_{ij} = 1$ se $i = j$ e $\delta_{ij} = 0$ se $i \neq j$.

Considere o sistema linear homogêneo definido pelas n equações nas variáveis $y_1, \cdots, y_n$. Ou seja,

$$\begin{cases} (\alpha - a_{11})y_1 - a_{12} - \cdots - a_{1n} = 0 \\ -a_{21} + (\alpha - a_{22})y_2 - \cdots - a_{2n} = 0 \\ \vdots \\ -a_{n1} - a_{n2} - \cdots + (\alpha - a_{nn})y_n = 0 \end{cases}$$

Seja $d = det(\delta_{ij}\alpha - a_{ij})$. Por Cramer $dy_i = 0$, $\forall\, i = 1, \cdots, n$. Portanto $db = 0$, $\forall\, b \in R$. Em particular $d \cdot 1 = d = 0$. Mas d é uma expressão polinomial em α e o coeficiente da maior potência de α é 1, pois o termo de maior grau aparece na expansão do produto $\prod_{i=1}^{n}(\alpha - a_{ii})$ das entradas da diagonal principal. Portanto α é inteiro sobre A.

■

Corolário 1.3.1. *(*Samuel, 1967, p.28, Prop.1*) Sejam B um anel, A um subanel de B e $\{\alpha_1, \alpha_2, \cdots, \alpha_n\} \subset B$. Se α_i é inteiro sobre $A[\alpha_1, \alpha_2, \cdots,$*

$\alpha_{i-1}]$, em particular, se α_i é inteiro sobre A para todo $i = i, \cdots, n$, então $A[\alpha_1, \alpha_2, \cdots, \alpha_n]$ é um A-módulo finitamente gerado.

Demonstração. A demonstração será feita por indução sobre n. Para $n = 1$ segue do Teorema 1.3.1, pois se α_1 é inteiro sobre A, então $A[\alpha_1]$, é um A-módulo finitamente gerado. Assim, suponhamos que o teorema seja verdadeiro para $n-1$ elementos e provaremos que o teorema é válido para n elementos. Por hipótese de indução temos que $R = A[\alpha_1, \cdots, \alpha_{n-1}]$ é um A-módulo finitamente gerado, isto é, $R = \sum_{j=1}^{n} Av_j$, onde $v_1, \cdots, v_n \in R$. Visto que α_n é inteiro sobre R temos, pelo Teorema 1.3.1, que $R[\alpha_n]$ é um R-módulo finitamente gerado, isto é, $R[\alpha_n] = \sum_{i=1}^{s} Rw_i$, onde $w_1, \cdots, w_s \in R[\alpha_n]$. Então $A[\alpha_1, \cdots, \alpha_n] = R[\alpha_n] = \sum_{i=1}^{s} Rw_i = \sum_{i=1}^{s}\left(\sum_{j=1}^{n} Av_j\right) w_i = \sum_{i,j} Av_j w_i$. Portanto $\{v_j w_i\}$ gera $A[\alpha_1, \cdots, \alpha_n]$ como um A-módulo. Portanto $A[\alpha_1, \cdots, \alpha_n]$ é um A-módulo finitamente gerado. ■

Teorema 1.3.2. *(*Stewart; Tall, 1987, p.47, Teo.2.9*) Se α é uma raiz de um polinômio mônico, onde os coeficientes são inteiros algébricos, então α é um inteiro algébrico.*

Demonstração. Seja $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$, tal que a_i, $i = 1, \cdots, n-1$ pertença ao conjunto de todos os números complexos que são raízes de polinômios mônicos com coeficientes em $\mathbb{Z}$. Fazendo $B = \mathbb{Z}[a_0, \cdots, a_{n-1}, \alpha]$ e $b_0 = a_0, \cdots, b_{n-1} = a_{n-1}$ e $b_n = \alpha$ e temos, pelo Corolário 1.3.1, que $\mathbb{Z}[b_0, \cdots, b_n]$ é um $\mathbb{Z}$-módulo finitamente gerado e portanto α é um inteiro algébrico. ■

Corolário 1.3.2. *(*Samuel, 1967, p.29, Corol.1 *) Sejam B um anel e A um subanel de B. Se $\alpha, \beta \in B$ são inteiros sobre A, então $\mathbb{A}, \alpha\beta \in \mathbb{A}_B$.*

Demonstração. Pela Observação 1.3.1, temos que mostrar que $\mathbb{A}, \alpha\beta$ são inteiros sobre A. Temos que $\mathbb{A}, \alpha\beta \in A[\alpha, \beta]$. Como α, β são inteiros sobre A temos então, pelo Corolário 1.3.1, que $A[\alpha, \beta]$ é um A-módulo finitamente gerado. Assim, existe um A-módulo finitamente gerado, $A[\alpha, \beta]$, que contém $\mathbb{A}$ e $\alpha\beta$. Deste modo, pelo Teorema 1.3.1, $\mathbb{A}$ e $\alpha\beta$ são inteiros sobre A, isto é, $\mathbb{A}, \alpha\beta \in \mathbb{A}_B$. ■

Corolário 1.3.3. *(*Samuel, 1967, p.29, Corol.2*) Sejam B um anel e A um subanel de B. O conjunto $\mathbb{A}_B$ dos elementos de B que são inteiros sobre A é um subanel de B que contém A.*

Demonstração. Pelo Corolário 1.3.2, segue que $\mathbb{A} \in \mathbb{A}_B$ e $\alpha\beta \in \mathbb{A}_B$,

$\forall\, \alpha, \beta \in \mathbb{A}_B$, assim $\mathbb{A}_B$ é subanel de B. Por outro lado $A \subset \mathbb{A}_B$, pois se $a \in A$, então a é raiz do polinômio mônico $p(X) = X - a$, que tem coeficientes em A, isto é, a é inteiro sobre A e assim $a \in \mathbb{A}_B$. ■

Definição 1.3.3. *Sejam B um anel e A um subanel de B. Dizemos que B é inteiro sobre A, se todo elemento de B é inteiro sobre A, isto é, se $\mathbb{A}_B = B$.*

Exemplo 1.3.3. *Dentre os anéis que satisfazem esta condição, citamos o anel dos inteiros de Gauss contendo $\mathbb{Z}$, pois todo elemento $a+bi$ de $\mathbb{Z}[i]$ é raiz do polinômio $X^2-2aX+(a^2+b^2) \in \mathbb{Z}[X]$.*

Proposição 1.3.1. *(*Samuel, 1967, p.29, Prop.2*) Sejam R um anel, B um subanel de R e A um subanel de B. Então R é inteiro sobre A se, e somente se, R é inteiro sobre B e B é inteiro sobre A.*

Demonstração. Suponhamos R inteiro sobre A e seja $\alpha \in B$. Como $B \subset R$, segue que α é inteiro sobre A, ou seja, B é inteiro sobre A. Para mostrar que R é inteiro sobre B, seja $\alpha \in R$. Então existem $a_0, a_1, \ldots, a_{n-1} \in A$ tal que $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$. Como $A \subset B$, segue que α é inteiro sobre B, ou seja, R é inteiro sobre B. Por outro lado, seja $\alpha \in R$. Como R é inteiro sobre B, então existem $b_0, b_1, \cdots, b_{n-1} \in B$, não todos nulos tal que $\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$. Seja $C = A[b_0, b_1, \cdots, b_{n-1}]$. Logo α é inteiro sobre C, pois α é raiz de um polinômio mônico com coeficientes em C. Como B é inteiro sobre A, segue que os $b_i^{'}s \in B$ são inteiros sobre A. Daí pelo Corolário 1.3.1 temos que $A[b_0, \cdots, b_{n-1}, \alpha] = C[\alpha]$ é um A-módulo finitamente gerado e pela parte (c) do Teorema 1.3.1, segue que α é inteiro sobre A. Portanto R é inteiro sobre A. ■

Proposição 1.3.2. *(*Samuel, 1967, p.29, Prop.3*) Sejam $A \subseteq B$ anéis com B um domínio e inteiro sobre A. Então A é um corpo se, e somente se, B é um corpo.*

Demonstração. Suponha que A seja um corpo. Seja $\alpha \in B$, $\alpha \neq 0$. Como B é inteiro sobre A então α é inteiro sobre A e portanto pelo Teorema 1.3.1 segue que $A[\alpha]$ é um espaço vetorial finitamente gerado sobre A, pois A é um corpo. Seja

$$\begin{aligned} \phi : A[\alpha] &\longrightarrow A[\alpha] \\ b &\longrightarrow b\alpha, \quad \forall\, b \in A[\alpha]. \end{aligned}$$

Temos que ϕ é A-linear e $Ker(\phi) = \{b \in A[\alpha] : \phi(b) = 0\} = \{0\}$, pois $\phi(b) = 0$ se, e somente se, $b\alpha = 0$ e como B é um domínio e $\alpha \neq 0$ segue que b=0. Deste modo, ϕ é injetora e como estamos considerando espaços de mesma dimensão finita, segue que ϕ é sobrejetora. Portanto ϕ é bijetora. Assim, como $1 \in A[\alpha]$ segue

que exite $b' \in A[\alpha]$ tal que $b'\alpha = 1$, ou seja, α é inversível em B. Portanto B é um corpo. Por outro lado, seja $\alpha \in A$, $\alpha \neq 0$. Como $A \subset B$ então $\alpha \in B$ e como B é um corpo segue que $\alpha^{-1} \in B$. Como B é inteiro sobre A, e $\alpha^{-1} \in B$ segue que

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

com $a_i \in A$ não todos nulos. Multiplicando por α^{n-1}, obtemos

$$\alpha^{-1} + a_{n-1} + \cdots + a_1\alpha^{n-2} + a_0\alpha^{n-1} = 0$$

e então $\alpha^{-1} = -(a_{n-1} + \cdots + a_1\alpha^{n-2} + a_0\alpha^{n-1}) \in A$.

Portanto A é um corpo. ■

Definição 1.3.4. *Um anel A é chamado* **integralmente fechado** *quando A é um domínio e é seu próprio fecho inteiro. Em outras palavras, um anel A é integralmente fechado se todo elemento do seu corpo de frações que é inteiro sobre A está em A.*

Proposição 1.3.3. *(*Samuel, 1967, p.30, Ex.1*) Se A é domínio, então $\mathbb{A}_B$ é integralmente fechado.*

Demonstração. Segue do fato de que o fecho inteiro de $\mathbb{A}_B$ é inteiro sobre $\mathbb{A}_B$, portanto sobre A. ■

Proposição 1.3.4. *(*Samuel, 1967, p.30, Ex.2*) Se A é um domínio principal então A é integralmente fechado.*

Demonstração. Seja $\mathbb{K}$ o corpo de frações de A. Seja $\alpha \in \mathbb{K}$ inteiro sobre A, isto é, $\alpha \in \mathbb{A}_{\mathbb{K}}$ tal que $\alpha = \frac{a}{b}$, $a, b \in A$, $b \neq 0$ e $mdc(a, b) = 1$. Então existem $a_i \in A$, $i = 0, 1, \cdots, n-1$, não todos nulos, tal que

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0.$$

Substituindo α por $\frac{a}{b}$ temos

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

Multiplicando por b^n ambos os lados, obtemos

$$a^n + a_{n-1}a^{n-1}b + \cdots + a_1ab^{n-1} + a_0b^n = 0,$$

e assim

$$a^n = -b(a_{n-1}a^{n-1} + \cdots + a_1ab^{n-2} + a_0b^{n-1}).$$

Portanto $b|a^n$ e como $mdc(a,b) = 1$ segue que $b|a$, ou seja, $a = bc$. Sendo $mdc(a, b) = 1$ então existe x_0, $y_0 \in A$ tal que $ax_0 + by_0 = 1 \Longrightarrow bcx_0 + by_0 = 1 \Longrightarrow b(cx_0 + y_0) = 1$. Portanto b é inversível em A. Assim, $\alpha = ab^{-1} \in A$. Portanto $\mathbb{A}_{\mathbb{K}} \subset A$ e como $A \subset \mathbb{A}_{\mathbb{K}}$ segue que $A = \mathbb{A}_{\mathbb{K}}$. Portanto A é integralmente fechado. ■

Exemplo 1.3.4. *O anel $\mathbb{Z}$ dos números inteiros é integralmente fechado, pois é principal.*

Exemplo 1.3.5. *Todo domínio fatorial é integralmente fechado, uma vez que é principal.*

1.4 Elementos algébricos sobre um corpo e extensões algébricas

Nesta seção apresentamos as definições de elemento algébrico, extensão algébrica e polinômio minimal.

Para isso, sejam A um anel e $\mathbb{K}$ um corpo de A. Dizemos que um elemento $\alpha \in A$ é **algébrico** sobre $\mathbb{K}$, se α é raiz de um polinômio não nulo, com coeficientes em $\mathbb{K}$. Se todo elemento de A for algébrico sobre $\mathbb{K}$, dizemos que A é algébrico sobre $\mathbb{K}$. Um elemento de A que não é algébrico sobre $\mathbb{K}$ é dito transcendente sobre

$\mathbb{K}$. Se A é um corpo então A é chamado uma extensão algébrica de $\mathbb{K}$. Um corpo de números é uma extensão finita dos racionais. Sabemos, pelo Teorema do Elemento Primitivo, que um corpo de números $\mathbb{K}$ de grau n é da forma $\mathbb{Q}(\alpha)$ para algum elemento $\alpha \in \mathbb{K}$. Como o polinômio minimal de α sobre $\mathbb{Q}$ é de grau n, segue que $\mathbb{Q}(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in \mathbb{Q}, i = 0, \cdots, n-1\}$, e esta representação é única, ou seja, $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base para o espaço vetorial $\mathbb{Q}(\alpha)$ sobre $\mathbb{Q}$.

Segundo a definição, sendo α um elemento algébrico sobre um corpo $\mathbb{K}$, α satisfaz uma equação do tipo, $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$, com $a_i \in \mathbb{K}$, $a_n \neq 0$. Multiplicando essa equação por a_n^{-1}, obtemos uma equação de dependência inteira, $\alpha^n + a_n^{-1}a_{n-1}\alpha^{n-1} + \cdots + a_n^{-1}a_1\alpha + a_n^{-1}a_0 = 0$, e portanto, sobre um corpo, o conceito de elemento algébrico coincide com o de elemento inteiro.

Exemplo 1.4.1. *O elemento* $\alpha = \sqrt{3} + \sqrt{-5}$ *é algébrico sobre* $\mathbb{Q}$, *pois é raiz do polinômio* $X^4 + 4X^2 + 64 \in \mathbb{Q}[X]$.

Definição 1.4.1. *Sejam* $\mathbb{K} \subseteq \mathbb{L}$ *uma extensão de corpos e* α *um elemento de* $\mathbb{L}$. *O polinômio mônico e de menor grau em* $\mathbb{K}[X]$ *que tem* α *como raiz é chamado de* **polinômio minimal** *de* α *sobre* $\mathbb{K}$ *e seu grau é* $[\mathbb{K}(\alpha) : \mathbb{K}]$.

1.5 Norma e traço em uma extensão

Nesta seção apresentamos os conceitos de norma e traço, onde a Proposição 1.5.2 e o Corolário 1.5.1 são os principais resultados.

Sejam A um anel e B um A-módulo livre de posto n. Sejam $\psi : B \longrightarrow B$ um homomorfismo de anéis e $\{e_1, e_2, \cdots, e_n\}$ uma

base de B sobre A. Então

$$\begin{cases} \psi(e_1) = a_{11}e_1 + a_{12}e_2 + \cdots + a_{1n}e_n \\ \psi(e_2) = a_{21}e_1 + a_{22}e_2 + \cdots + a_{2n}e_n \\ \vdots \\ \psi(e_n) = a_{n1}e_1 + a_{n2}e_2 + \cdots + a_{nn}e_n, \end{cases}$$

com $a_{ij} \in A$, para todo $i, j = 1, \cdots, n$. Assim

$$\begin{bmatrix} \psi(e_1) \\ \psi(e_2) \\ \vdots \\ \psi(e_n) \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ \vdots \\ e_n \end{bmatrix}.$$

Definição 1.5.1. *Definimos o* **traço** *de* ψ *por* $Tr(\psi) = \sum_{i=1}^{n} a_{ii}$, *a* **norma** *de* ψ *por* $N(\psi) = \det(a_{ij})$ *e o* **polinômio característico** *de* ψ *por* $g(X) = \det(X.I - \psi) = \det(X\delta_{ij} - a_{ij})$.

Como consequência imediata desta definição tem-se:

$$Tr(\psi + \psi') = Tr(\psi) + Tr(\psi'),$$
$$N(\psi\psi') = N(\psi)N(\psi'),$$
$$\det(X.I - \psi) = X^n - Tr(\psi)X^{n-1} + \cdots + (-1)^n \det(\psi).$$

Definição 1.5.2. *Sejam* A *um anel e* B *um* A*-módulo livre. Seja o endomorfismo* $\psi_\alpha : B \longrightarrow B$ *definido por* $\psi_\alpha(x) = \alpha x$, *para todo* $x \in B$. *Definimos o traço (respectivamente, norma e polinômio característico) de* $\alpha \in B$ *relativo a* A, *como o traço (respectivamente, determinante e polinômio característico) do endomorfismo* ψ_α.

Usaremos as notações $Tr_{B/A}(\alpha)$, $N_{B/A}(\alpha)$, ou simplesmente, $Tr(\alpha)$, $N(\alpha)$ quando não houver possibilidade de confusão.

Observação 1.5.1. i) *O traço e a norma são elementos de* A.

ii) *O polinômio característico é um polinômio mônico com coeficientes em* A.

iii) *Para* $\alpha, \alpha' \in B$ *e* $a \in A$ *temos que* $\psi_\alpha + \psi_{\alpha'} = \psi_{\alpha+\alpha'}$ *e* $\psi_\alpha \circ \psi_{\alpha'} = \psi_{\alpha\alpha'}$ *e* $\psi_{a\alpha} = a\psi_\alpha$. *Além disso, a matriz de* ψ_a *com respeito a uma base de* B *sobre* A *é a matriz diagonal cujas entradas não nulas são* a.

Proposição 1.5.1. *(*Samuel, 1967, p.36, Prop.1*) Sejam* $\mathbb{K}$ *um corpo de característica zero ou um corpo finito,* $\mathbb{L}$ *uma extensão algébrica de* $\mathbb{K}$ *de grau* n, α *um elemento de* $\mathbb{L}$ *e* $\alpha_1, \cdots, \alpha_n$ *as raízes do polinômio minimal de* α *sobre* $\mathbb{K}$. *Então* $Tr_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1 + \cdots + \alpha_n$, $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \alpha_1 \cdots \alpha_n$ *e* $g(X) = (X - \alpha_1) \cdots (X - \alpha_n)$.

Demonstração. Consideraremos primeiramente o caso em que α é um elemento primitivo de $\mathbb{L}$ sobre $\mathbb{K}$. Seja $f(X)$ o polinômio minimal de α sobre $\mathbb{K}$. Então $\mathbb{L}$ é $\mathbb{K}$-isomorfo a $\mathbb{K}[X]/ < f(X) >$ e $\{1, \alpha, \cdots, \alpha^{n-1}\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Tomando $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, com $a_i \in \mathbb{K}$, temos que a matriz do endomorfismo ψ_α com respeito a esta base é dada por

$$\begin{cases} \psi_\alpha(1) = \alpha \\ \psi_\alpha(\alpha) = \alpha^2 \\ \vdots \\ \psi_\alpha(\alpha^{n-1}) = \alpha^n \end{cases} \Longrightarrow M = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & & 1 & -a_{n-1} \end{bmatrix}.$$

Assim, $det(X.I - \psi_\alpha)$ é o determinante da matriz

$$X.I_n - M = \begin{bmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & X & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & \vdots \\ \vdots & 0 & \cdots & \vdots & \vdots \\ \vdots & \vdots & \cdots & X & a_{n-2} \\ 0 & 0 & \cdots & -1 & X + a_{n-1} \end{bmatrix}.$$

Expandindo esse determinante como um polinômio em X, obtemos o polinômio característico de α, que é igual a $f(X)$ e temos que $Tr(\alpha) = -a_{n-1}$ e $N(\alpha) = (-1)^n a_0$. Como α é primitivo, segue que $f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$ e igualando os coeficientes vemos que $Tr(\alpha) = \alpha_1 + \cdots + \alpha_n$ e $N(\alpha) = \alpha_1 \cdots \alpha_n$.

Consideremos agora o caso geral. Se $r = [\mathbb{L} : \mathbb{K}[\alpha]]$, é suficiente mostrarmos que o polinômio característico $g(X)$ de α, com relação a $\mathbb{L}$ sobre $\mathbb{K}$, é igual a r-ésima potência do polinômio minimal de α sobre $\mathbb{K}$. Seja $\{y_i\}_{i=1,\cdots,q}$ uma base de $\mathbb{K}[\alpha]$ sobre $\mathbb{K}$ e seja $\{z_j\}_{j=1,\cdots,r}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}[\alpha]$. Então $\{y_i z_j\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$ com $n = qr$. Se $M = (a_{ih})$ é a matriz de multiplicação por α em $\mathbb{K}[\alpha]$ com relação a base $\{y_i\}$, temos que $\alpha y_i = \sum_h a_{ih} y_h$. Então temos, $\alpha(y_i z_j) = \left(\sum_h a_{ih} y_h \right) z_j = \sum_h a_{ih} \left(y_h z_j \right)$. Logo,

$$\begin{cases} \alpha y_1 z_1 = a_{11} y_1 z_1 + a_{12} y_2 z_1 + \cdots + a_{1q} y_q z_1 \\ \alpha y_2 z_1 = a_{21} y_1 z_1 + a_{22} y_2 z_1 + \cdots + a_{2q} y_q z_1 \\ \vdots \\ \alpha y_q z_1 = a_{q1} y_1 z_1 + a_{q2} y_2 z_1 + \cdots + a_{qq} y_q z_1. \end{cases}$$

Assim, a matriz do endomorfismo de α em $\mathbb{L}$ com relação a base $\{y_i z_j\}$, ordenada lexicograficamente é dada por

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

isto é, M aparece r-vezes na diagonal como blocos na matriz M_1. Daí, a matriz $XI_n - M_1$ consiste de r blocos diagonais, cada um tem a forma $XI_q - M$, e consequentemente, $det(XI_n - M_1) = det(XI_q -$

$M_1)^r$. Assim $g(X) = det(XI_q - M)$ e $det(XI_q - M)$ é o polinômio característico de α sobre $\mathbb{K}$, de acordo com a primeira parte da demonstração. ■

Proposição 1.5.2. *(*Samuel, 1967, p.38, Prop.2*) Sejam A um domínio, $\mathbb{K}$ seu corpo de frações com característica zero, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ e α um elemento de $\mathbb{L}$ inteiro sobre A. Então os coeficientes do polinômio característico $g(X)$ de α relativo a $\mathbb{L}$ sobre $\mathbb{K}$, em particular, $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$, são inteiros sobre A.*

Demonstração. Pela Proposição 1.5.1, temos que $g(X) = (X - \alpha_1) \cdots$

$(X - \alpha_n)$. Como os coeficientes de $g(X)$ a menos de sinal, são somas de produtos dos $\alpha_i^{'}s$, é suficiente mostrarmos que cada α_i é inteiro sobre A. Mas cada α_i é um conjugado de α sobre $\mathbb{K}$, ou seja, existe um $\mathbb{K}$-isomorfismo $\sigma_i : \mathbb{K}[\alpha] \longrightarrow \mathbb{K}[\alpha_i]$ tal que $\sigma_i(\alpha) = \alpha_i$. Como α é inteiro sobre A, então

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

com $a_i \in A$ não todos nulos. Aplicando σ_i, obtemos

$$\sigma_i(\alpha)^n + a_{n-1}\sigma_i(\alpha)^{n-1} + \cdots + a_1\sigma_i(\alpha) + a_0 = 0,$$

ou seja, $\sigma_i(\alpha) = \alpha_i$ é inteiro sobre A, portanto $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$, são inteiros sobre A. ■

Corolário 1.5.1. *(*Samuel, 1967, p.38, Corol.1*) Nas condições da Proposição 1.5.2, se A é um anel integralmente fechado, então os coeficientes do polinômio característico de α, e em particular, $Tr_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha)$ são elementos de A.*

Demonstração. Por definição esses coeficientes são elementos de $\mathbb{K}$. Pela Proposição 1.5.2 são inteiros sobre A. Logo, são elementos de A, pois A é integralmente fechado. ■

Observação 1.5.2. *Observando a Proposição 1.5.2 temos que* $Tr(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$, $N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$ *e* $g_\alpha(X) = \prod_{i=1}^{n}(X - \sigma_i(\alpha))$, *onde* σ_i, $i = 1, \cdots, n$ *são os* $\mathbb{K}$*- monomorfismos de* $\mathbb{L}$ *em* $\mathbb{C}$.

Sejam $\mathbb{K} \subset \mathbb{L} \subset \mathbb{M}$ corpos de números, α, $\alpha' \in \mathbb{M}$ e $a \in \mathbb{K}$. Então valem as seguintes propriedades:

1. $Tr_{\mathbb{M}/\mathbb{K}}(\alpha + \alpha') = Tr_{\mathbb{M}/\mathbb{K}}(\alpha) + Tr_{\mathbb{M}/\mathbb{K}}(\alpha')$
2. $Tr_{\mathbb{M}/\mathbb{K}}(a\alpha) = aTr_{\mathbb{M}/\mathbb{K}}(\alpha)$
3. $Tr_{\mathbb{M}/\mathbb{K}}(a) = [\mathbb{M} : \mathbb{K}]a$
4. $Tr_{\mathbb{M}/\mathbb{K}}(\alpha) = Tr_{\mathbb{L}/\mathbb{K}}(Tr_{\mathbb{M}/\mathbb{L}}(\alpha))$.
5. $N_{\mathbb{M}/\mathbb{K}}(\alpha\alpha') = N_{\mathbb{M}/\mathbb{K}}(\alpha)N_{\mathbb{M}/\mathbb{K}}(\alpha')$
6. $N_{\mathbb{M}/\mathbb{K}}(a) = a^{[\mathbb{M}:\mathbb{K}]}$
7. $N_{\mathbb{M}/\mathbb{K}}(a\alpha) = a^{[\mathbb{M}:\mathbb{K}]}N_{\mathbb{M}/\mathbb{K}}(\alpha)$
8. $N_{\mathbb{M}/\mathbb{K}}(\alpha) = N_{\mathbb{L}/\mathbb{K}}(N_{\mathbb{M}/\mathbb{L}}(\alpha))$.

1.6 Discriminante

Nesta seção apresentamos o conceito de discriminante enfocando suas principais propriedades, e o Teorema 1.6.1 é o principal resultado.

Definição 1.6.1. *Sejam* B *um anel e* A *um subanel de* B *tal que* B *é um* A*-módulo livre de posto finito* n. *Dado* $(\alpha_1, \alpha_2, \cdots, \alpha_n) \in B^n$, *definimos o seu* **discriminante** *por*

$$D_{B/A}(\alpha_1, \alpha_2, \cdots, \alpha_n) = det(Tr(\alpha_i\alpha_j)).$$

Exemplo 1.6.1. *Sejam* $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ *um corpo de números e* $\{1, \sqrt{3}\}$ *uma base de* $\mathbb{K}$ *sobre* $\mathbb{Q}$. *Então*

$$D_{B/A}(1, \sqrt{3}) = \begin{vmatrix} Tr(1) & Tr(\sqrt{3}) \\ Tr(\sqrt{3}) & Tr(\sqrt{3})^2 \end{vmatrix} = \begin{vmatrix} 2 & 0 \\ 0 & 6 \end{vmatrix} = 12.$$

Proposição 1.6.1. *(*Samuel, 1967, p.38, Prop.1*) Seja* $(\alpha_1, \cdots, \alpha_n) \in B^n$. *Se* $(\beta_1, \cdots, \beta_n) \in B^n$ *é um conjunto de elementos de* B *tais que* $\beta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, *com* $a_{ij} \in A$, *então*

$$D_{B/A}(\beta_1, \cdots, \beta_n) = (det(a_{ij}))^2 D_{B/A}(\alpha_1, \cdots, \alpha_n).$$

Demonstração. Sejam $\beta_p = \sum_{i=1}^{n} a_{pi}\alpha_i$ e $\beta_q = \sum_{j=1}^{n} a_{qj}\alpha_j$, com $a_{pi},\ a_{qj} \in A$. Assim, $\beta_p\beta_q = \sum_{i=1}^{n} a_{pi}\alpha_i \sum_{j=1}^{n} a_{qj}\alpha_j = \sum_{i,j=1}^{n} a_{pi}a_{qj}\alpha_i\alpha_j$, e então $Tr(\beta_p\beta_q) = Tr(\sum_{i,j}^{n} a_{pi}a_{qj}\alpha_i\alpha_j) = \sum_{i,j}^{n} a_{pi}a_{qj}Tr(\alpha_i\alpha_j)$. Na forma matricial, temos $(Tr(\beta_p\beta_q)) = (a_{pi})(Tr(\alpha_i\alpha_j))(a_{qj})^t$. Pela Definição 1.6.1 temos que $D_{B/A}(\beta_1, \cdots, \beta_n) = det(Tr(\beta_p\beta_q))$. Logo

$$\begin{aligned} D_{B/A}(\beta_1, \cdots, \beta_n) &= det((a_{pi})(Tr(\alpha_i\alpha_j))(a_{qj})^t) \\ &= det(a_{pi})det(Tr(\alpha_i\alpha_j))det(a_{qj})^t \\ &= det(a_{ij})^2 D_{B/A}(\alpha_1, \cdots, \alpha_n). \end{aligned}$$ ■

Exemplo 1.6.2. *Pelo exe 1.6.1 vimos que o discriminante da base* $\{1, \sqrt{3}\}$ *do corpo de números* $\mathbb{K} = \mathbb{Q}(\sqrt{3})$ *é igual a* 12. *Agora, considerando uma outra base para o corpo* $\mathbb{K}$, *por exe,* $\{2-\sqrt{3}, 3+4\sqrt{3}\}$, *segue pela Proposição 1.6.1, que* $2-\sqrt{3} = 2\cdot 1 + (-1)\cdot\sqrt{3}$ *e* $3+4\sqrt{3} = 3\cdot 1 + 4\cdot\sqrt{3}$. *Assim*

$$D_{\mathbb{K}/\mathbb{Q}}(2-\sqrt{3}, 3+4\sqrt{3}) = \left(det\begin{pmatrix} 2 & -1 \\ 3 & 4 \end{pmatrix}\right)^2 D_{\mathbb{K}/\mathbb{Q}}(1, \sqrt{3}) = (11)^2 12.$$

Observação 1.6.1. *A Proposição 1.6.1 implica que o discriminante das bases de* B *sobre* A *são associados, isto é, a matriz* (a_{ij}) *que expressa uma base em termos da outra tem uma matriz inversa com entradas em* A. *Portanto, ambos* $det(a_{ij})$ *e* $det(a_{ij})^{-1}$ *são inversíveis em* A.

Definição 1.6.2. *Sejam B um anel e A um subanel de B tal que B é um A-módulo livre de posto finito n. O discriminante de B sobre A é um ideal de A, dado por*

$$\mathfrak{D}_{B/A} = \langle D_{B/A}(\alpha_1, \cdots, \alpha_n) \rangle,$$

onde $\{\alpha_1, \cdots, \alpha_n\}$ é base de B sobre A.

Proposição 1.6.2. *(*Samuel, 1967, p.39, Prop.2*) Suponhamos que $\mathfrak{D}_{B/A}$ contém um elemento que não é um divisor de zero. Então, para que $(\alpha_1, \cdots, \alpha_n) \in B^n$ seja uma base de B sobre A, é necessário e suficiente que, $D_{B/A}(\alpha_1, \cdots, \alpha_n)$ gera $\mathfrak{D}_{B/A}$.*

Demonstração. Se $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ é uma base de B sobre A, então pela Proposição 1.6.1, segue que $D_{B/A}(\alpha_1, \cdots, \alpha_n)$ gera $\mathfrak{D}_{B/A}$. Reciprocamente, suponhamos que $d = D_{B/A}(\alpha_1, \cdots, \alpha_n)$ gera $\mathfrak{D}_{B/A}$. Sejam $\{e_1, \cdots, e_n\}$ uma base de B sobre A, $d' = D_{B/A}(e_1, \cdots, e_n)$ e $\alpha_i = \sum_{j=1}^{n} a_{ij} e_j$ com $a_{ij} \in A$, $1 \leq i \leq n$. Pela Proposição 1.6.1, segue que $d = det(a_{ij})^2 d'$. Por hipótese, $Ad = \mathfrak{D}_{B/A} = Ad'$. Logo, existe um elemento $b \in A$ tal que $d' = bd$. Então $d = det(a_{ij})^2 bd$, e portanto $d(1 - det(a_{ij})^2 b) = 0$. Temos que d não é um divisor de zero, pois se fosse todo elemento de $Ad = \mathfrak{D}_{B/A}$ seria um divisor de zero, contrariando a hipótese. Logo, $1 - det(a_{ij})^2 b = 0$, e portanto $det(a_{ij})$ é inversível. Assim, a matriz $M = [a_{ij}]$ é inversível. Portanto, $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de B sobre A. ■

Lema 1.6.1. *(***Lema de Dedekind***) (*Samuel, 1967,p.39*) Sejam G um grupo, $\mathbb{K}$ um corpo e $\sigma_1, \cdots, \sigma_n$ homomorfismos distintos de G no grupo multiplicativo $\mathbb{K}^*$. Então $\{\sigma_1, \cdots, \sigma_n\}$ são linearmente independentes sobre $\mathbb{K}$.*

Demonstração. Suponhamos que os σ_i's sejam linearmente dependentes. Seja $\sum_{i=1}^{m} a_i \sigma_i = 0$, $a_i \in \mathbb{K}$ uma combinação linear mí-

nima com $a_i \neq 0, \forall i$. Logo, para qualquer $x \in \boldsymbol{G}$, temos que

$$a_1\sigma_1(x) + a_2\sigma_2(x) + \cdots + a_m\sigma_m(x) = 0. \tag{1.3}$$

Como os homomorfismos são distintos, então existe $c \in \boldsymbol{G}$ tal que $\sigma_1(c) \neq \sigma_m(c)$. Agora, como $cx \in \boldsymbol{G}$, segue que

$$a_1\sigma_1(cx) + a_2\sigma_2(cx) + \cdots + a_m\sigma_m(cx) = 0 \tag{1.4}$$

e então

$$a_1\sigma_1(c)\sigma_1(x) + a_2\sigma_2(c)\sigma_2(x) + \cdots + a_m\sigma_m(c)\sigma_m(x) = 0. \tag{1.5}$$

Multiplicando (1.3) por $\sigma_1(c)$, obtemos

$$a_1\sigma_1(c)\sigma_1(x) + a_2\sigma_1(c)\sigma_2(x) + \cdots + a_m\sigma_1(c)\sigma_m(x) = 0. \tag{1.6}$$

Subtraindo (1.5) de (1.6) obtemos

$$a_2\sigma_2(x)(\sigma_2(c) - \sigma_1(c)) + \cdots + a_m\sigma_m(x)(\sigma_m(c) - \sigma_1(c)) = 0. \tag{1.7}$$

Como isso vale para todo $x \in \boldsymbol{G}$ e m é mínimo, segue que $a_m(\sigma_m(c) - \sigma_1(c)) = 0$, ou seja, $\sigma_m(c) = \sigma_1(c)$ para todo $c \in \boldsymbol{G}$, visto que $a_m \neq 0$, o que contradiz a hipótese de que os homomorfismos são distintos. ■

Proposição 1.6.3. *(*Samuel, 1967, p.39, Prop.3*) Sejam $\mathbb{K}$ um corpo, $\mathbb{L}$ uma extensão finita de $\mathbb{K}$ de grau n e $\sigma_1, \cdots, \sigma_n$ os n $\mathbb{K}$-isomorfismos distintos de $\mathbb{L}$ em um corpo algebricamente fechado $\boldsymbol{F}$ contendo $\mathbb{K}$. Se $\{\alpha_1, \cdots, \alpha_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, então*

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

Demonstração. Temos que $\boldsymbol{D}_{\mathbb{L}/\mathbb{K}}(\alpha_1, \cdots, \alpha_n) = \det(\boldsymbol{Tr}(\alpha_i\alpha_j))$. Como o traço de $\alpha_i\alpha_j$ é a soma dos seus conjugados, segue que $\boldsymbol{D}_{\mathbb{L}/\mathbb{K}}(\alpha_1, \cdots$

$$\alpha_n) = \det(Tr(\alpha_i\alpha_j)) = \det\left(\sum_{k=1}^{n}\sigma_k(\alpha_i\alpha_j)\right) = \det\left(\sum_{k=1}^{n}\sigma_k(\alpha_i)\sigma_k(\alpha_j)\right) =$$

$\det(\sigma_k(\alpha_i))\det(\sigma_k(\alpha_j)) = (\det(\sigma_i(\alpha_j)))^2$, uma vez que

$$\begin{bmatrix} \sigma_1(\alpha_1) & \sigma_2(\alpha_1) & \cdots & \sigma_n(\alpha_1) \\ \sigma_1(\alpha_2) & \sigma_2(\alpha_2) & \cdots & \sigma_n(\alpha_2) \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_1(\alpha_n) & \sigma_2(\alpha_n) & \cdots & \sigma_n(\alpha_n) \end{bmatrix}\begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & \cdots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \cdots & \sigma_n(\alpha_n) \end{bmatrix} =$$

$$= \sum_{k=1}^{n}\sigma_k(\alpha_i\alpha_j).$$

Suponha por absurdo que $\det(\sigma_k(\alpha_j)) = 0$. Então existem $a_1, \cdots, a_n \in F$, não todos nulos, tal que $\sum_{i=1}^{n} a_i\sigma_i(\alpha_j) = 0$ para todo j. Se $\alpha \in \mathbb{L}$, então $\alpha = \sum_{i=1}^{n} b_i\alpha_i$, com $b_i \in \mathbb{K}$, e por linearidade concluímos que $\sum_{i=1}^{n} a_i\sigma_i(\alpha) = 0$. Mas isto contradiz o Lema de Dedekind e portanto $\det(\sigma_k(\alpha_j)) \neq 0$. ■

Corolário 1.6.1. *(*Ribeiro, 2013, p.21, Corol.2.4.1*) Sejam* $\mathbb{K}$ *um corpo,* $\mathbb{L}$ *uma extensão finita de* $\mathbb{K}$ *de grau* n *e* $\sigma_1, \sigma_2, \cdots, \sigma_n$ *os* n $\mathbb{K}$*-isomorfismos distintos de* $\mathbb{L}$ *em um corpo algebricamente fechado* F *contendo* $\mathbb{K}$*. Então a forma bilinear* $\psi : \mathbb{L}\times\mathbb{L} \longrightarrow \mathbb{R}$ *definida por* $\psi(\alpha,\beta) = Tr(\alpha\beta)$ *é não degenerada, isto é, se* $Tr(\alpha\beta) = 0$ *para todo* $\beta \in \mathbb{L}$*, então* $\alpha = 0$*.*

Demonstração. Seja $\{\alpha_1, \cdots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. É suficiente mostrar que se $Tr(\alpha\alpha_j) = 0$, para todo $j = 1, \cdots, n$, então $\alpha = 0$. Temos que $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$, com $a_i \in \mathbb{K}$, $i = 1, \cdots, n$. Assim, se $a_1Tr(\alpha_1\alpha_j) + a_2Tr(\alpha_2\alpha_j) + \cdots + \alpha_nTr(\alpha_n\alpha_j) = Tr(\alpha\alpha_j) = 0$, para todo $j = 1, \cdots, n$, então obtemos o seguinte sistema linear

homogêneo

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

Da Proposição 1.6.3, temos que $\det(Tr(\alpha_i\alpha_j)) \neq 0$, e portanto o sistema possui solução única dada por $a_1 = a_2 = \cdots = a_n = 0$. Portanto, $\alpha = 0$. ■

Corolário 1.6.2. *(*Ribeiro, 2013, p.22, Obs.2.4.1*) A aplicação* $\psi : \mathbb{L} \longrightarrow Hom_{\mathbb{L}}(\mathbb{L}, \mathbb{K})$ *definida por* $\psi(\alpha) = S_\alpha$, *onde* $S_\alpha(\beta) = Tr(\alpha\beta)$, $\beta \in \mathbb{L}$, *é um isomorfismo. Assim, se* $\{\alpha_1, \cdots, \alpha_n\}$ *é uma base de* $\mathbb{L}$ *sobre* $\mathbb{K}$, *então existe* $\{\psi_{\beta_1}, \cdots, \psi_{\beta_n}\}$ *base dual de* $Hom_{\mathbb{L}}(\mathbb{L}, \mathbb{K})$ *tal que* $Tr(\alpha\alpha_j) = \psi_{\beta_i}(\alpha_j) = \delta_{ij}$.

Demonstração.

i) ψ é $\mathbb{K}$-linear, uma vez que para $\beta \in \mathbb{L}$ temos que $S_{\alpha_1+\alpha_2}(\beta) = Tr((\alpha_1+\alpha_2)\beta) = Tr(\alpha_1\beta) + Tr(\alpha_2\beta) = S_{\alpha_1}(\beta) + S_{\alpha_2}(\beta) = (S_{\alpha_1} + S_{\alpha_2})(\beta)$. Portanto $\psi(\alpha_1+\alpha_2) = S_{\alpha_1+\alpha_2} = S_{\alpha_1} + S_{\alpha_2} = \psi(\alpha_1) + \psi(\alpha_2)$. Por outro lado, $S_{k\alpha}(\beta) = Tr((k\alpha)\beta) = Tr(k\alpha\beta) = kTr(\alpha\beta) = kS_\alpha(\beta)$. Portanto $\psi(k\alpha) = S_{k\alpha} = kS_\alpha = k\psi(\alpha)$.

ii) ψ é injetora: Seja $\alpha \in \mathbb{L}$ tal que $\psi(\alpha) = 0$. Então $\psi(\alpha) = S_\alpha = 0$, e isto implica que $S_\alpha(\beta) = Tr(\alpha\beta) = 0$, $\forall \beta \in \mathbb{L}$. Pelo Corolário 1.6.1 segue que $\alpha = 0$. Portanto $Ker(\psi) = \{0\}$, ou seja, ψ é injetora.

iii) ψ é sobrejetora: Como $dim_{\mathbb{K}}\mathbb{L} = dim_{\mathbb{K}}\mathbb{L}^*$, onde $\mathbb{L}^* = Hom(\mathbb{L}, \mathbb{K})$, segue que ψ é sobrejetora.

Por (i), (ii), *e* (iii) concluímos que ψ é um isomorfismo. ■

Teorema 1.6.1. *(*Samuel, 1967, p.40, Teo.1*) Sejam* A *um anel integralmente fechado,* $\mathbb{K}$ *seu corpo de frações com característica*

zero, $\mathbb{L}$ *uma extensão finita de* $\mathbb{K}$ *de grau* n *e* $\mathbb{A}_{\mathbb{L}}$ *o fecho inteiro de* $\mathbb{A}$ *em* $\mathbb{L}$*. Então* $A_{\mathbb{L}}$ *é um* A*-submódulo de um* A*-módulo livre de posto* n*.*

Demonstração. Seja $\{\alpha_1, \cdots, \alpha_n\}$ uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Como toda extensão finita é algébrica, segue que cada α_i é algébrico sobre $\mathbb{K}$ e assim existem $a_i \in A$, $i = 1, \cdots, n$, não todos nulos tal que

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

Suponhamos que $a_n \neq 0$ e multiplicando esta equação por a_n^{n-1}, temos que

$$a_n^{n-1}(a_n\alpha_i^n + a_{n-1}\alpha_i^{n-1} + \cdots + a_1\alpha_i + a_0) = 0,$$

ou seja,

$$(a_n\alpha_i)^n + a_{n-1}(a_n\alpha_i)^{n-1} + \cdots + a_1a_n^{n-2}(a_n\alpha_i) + a_n^{n-1}a_0.$$

Portanto $a_n\alpha_i \in \mathbb{A}_{\mathbb{L}}$, ou seja, $a_n\alpha_i$ é inteiro sobre A. Logo, $a_n\alpha_i = z_i$, com $z_i \in \mathbb{A}_{\mathbb{L}}$. Portanto $\{z_1, \cdots, z_n\}$ forma uma base de $\mathbb{L}$ sobre $\mathbb{K}$ contida em $\mathbb{A}_{\mathbb{L}}$, uma vez que se $b_1z_1 + \cdots + b_nz_n = 0$ com $b_i \in \mathbb{K}$, então $b_1(a_n\alpha_1) + \cdots + b_n(a_n\alpha_n) = 0$, ou seja, $(b_1a_n)\alpha_1 + \cdots + (b_na_n)\alpha_n = 0$. Como $\{\alpha_1, \cdots, \alpha_n\}$ é base de $\mathbb{L}$ sobre $\mathbb{K}$, segue que $b_ia_n = 0$, para todo i, e como $a_n \neq 0$, segue que $b_i = 0$, para todo i, o que prova que $\{z_1, \cdots, z_n\}$ é linearmente independente, e como possui n elementos, segue que é uma base de $\mathbb{L}$ sobre $\mathbb{K}$. Pelo Corolário 1.6.2 existe uma base $\{\beta_1, \cdots, \beta_n\}$ de $\mathbb{L}$ sobre $\mathbb{K}$, tal que $Tr(z_i\beta_j) = \delta_{ij}$. Tomando $\rho \in \mathbb{A}_{\mathbb{L}}$, e como $\{\beta_1, \cdots, \beta_n\}$ é uma base de $\mathbb{L}$ sobre $\mathbb{K}$, escrevemos $\rho = \sum_{j=1}^{n} c_j\beta_j$ com $c_j \in \mathbb{K}$. Para todo i temos $z_i\rho \in \mathbb{A}_{\mathbb{L}}$, uma vez que $z_i \in A$. Portanto, pelo Corolário 1.5.1, temos que $Tr(z_i\rho) \in A$. Assim, como $Tr(z_i\rho) = Tr\left(\sum_j c_jz_i\beta_j\right) =$

$\sum_j c_j Tr(z_i\beta_j) = \sum_j c_j\delta_{ij} = c_i$, concluímos que $c_i \in A$, para todo i, o que implica que $\mathbb{A}_{\mathbb{L}}$ é um submódulo do A-módulo livre $\sum_{j=1}^{n} A\beta_j$. ■

Corolário 1.6.3. *(*Samuel, 1967, p.40, Corol.1*) Considerando as hipóteses do Teorema 1.6.1, se A é um anel principal, então $\mathbb{A}_{\mathbb{L}}$ é um A-módulo livre de posto n.*

Demonstração. Pelo Teorema 1.2.1 temos que um submódulo de um A-módulo livre com A principal, é livre com posto $\leq n$. Pelo Teorema 1.6.1 vimos que $\mathbb{A}_{\mathbb{L}}$ contém uma base com n elementos de $\mathbb{L}$ sobre $\mathbb{K}$. Logo $\mathbb{A}_{\mathbb{L}}$ tem posto n. ■

Exemplo 1.6.3. *Sejam $\mathbb{K}$ uma extensão finita de $\mathbb{Q}$ e $A = \mathbb{Z}$. O anel $\mathbb{A}_{\mathbb{K}}$ dos inteiros algébricos de $\mathbb{K}$ é um $\mathbb{Z}$-módulo livre de posto $[\mathbb{L} : \mathbb{Q}]$, visto que $\mathbb{Z}$ é principal.*

Definição 1.6.3. *Sejam $\mathbb{K}$ uma extensão finita de $\mathbb{Q}$, $A = \mathbb{Z}$ e $\mathbb{A}_{\mathbb{K}}$ o anel dos inteiros algébricos de $\mathbb{K}$. Temos que $\mathbb{A}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto $[\mathbb{K} : \mathbb{Q}]$, cuja base é chamada de* **base integral**, *e seu discriminante é chamado de* **discriminante absoluto** *e denotamos por $D_{\mathbb{K}}$.*

Observação 1.6.2. *Qualquer base integral de $\mathbb{A}_{\mathbb{K}}$ é uma $\mathbb{Q}$-base de $\mathbb{K}$ mas nem toda $\mathbb{Q}$-base de $\mathbb{K}$ consistindo de inteiros algébricos é uma base integral de $\mathbb{A}_{\mathbb{K}}$.*

Exemplo 1.6.4. *Temos que $\{1, \sqrt{5}\}$ é uma $\mathbb{Q}$-base de $\mathbb{K} = \mathbb{Q}(\sqrt{5})$, mas não é uma base integral de $\mathbb{A}_{\mathbb{K}}$, pois o elemento $\frac{1+\sqrt{5}}{2}$ é raiz de $X^2 - X + 1$ e portanto inteiro algébrico, mas não é combinação linear, com coeficientes em $\mathbb{Z}$, de 1 e $\sqrt{5}$.*

Proposição 1.6.4. *(*Ribeiro, 2013, p.23, Prop.2.4.4*) Sejam* $\mathbb{K}$ *um corpo,* $\mathbb{L} = \mathbb{K}[\alpha]$ *uma extensão finita de* $\mathbb{K}$ *de grau* n *e* $f(X)$ *o polinômio minimal de* α *sobre* $\mathbb{K}$*. Então,*

$$D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \cdots, \alpha^{n-1}) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{L}/\mathbb{K}}(f'(\alpha)),$$

onde $f'(\alpha)$ *é a derivada de* $f(\alpha)$*.*

Demonstração. Se $\alpha_1, \cdots, \alpha_n$ são as raízes de $f(X)$ em alguma extensão de $\mathbb{K}$, então são conjugados de α. Pela Proposição 1.6.3 temos que $D_{\mathbb{L}/\mathbb{K}}(1, \alpha, \cdots, \alpha^{n-1}) = \left(det(\sigma_i(\alpha^j))\right)^2 = det(\alpha_i^j)^2$, com $i = 1, \cdots, n$ e $j = 0, \cdots, n-1$. Como $det(\alpha_i^j)$ é um determinante de Vandermonde segue que $\det(\alpha_i^j)^2 = \left[\prod_{1\leq k<i\leq n}(\alpha_i - \alpha_k)\right]^2 = \prod_{1\leq k<i\leq n}[(\alpha_i - \alpha_k)(\alpha_i - \alpha_k)] = (-1)^{\frac{1}{2}n(n-1)} \prod_{1\leq k<i\leq n,\, i\neq k}(\alpha_i - \alpha_k) = (-1)^{\frac{1}{2}n(n-1)} \prod_{i=1}^{n}\left[\prod_{k=1,\, k\neq i}^{n}(\alpha_i - \alpha_k)\right] = (-1)^{\frac{1}{2}n(n-1)} \prod_{i=1}^{n} f'(\alpha_i) = (-1)^{\frac{1}{2}n(n-1)} N_{\mathbb{L}/\mathbb{K}}(f'(\alpha))$. ■

Exemplo 1.6.5. *Sejam* $\mathbb{K} = \mathbb{Q}$, $\mathbb{L} = \mathbb{Q}(\sqrt{3})$ *e* $f(X) = X^2 - 3$ *o polinômio minimal de* $\sqrt{3}$ *sobre* $\mathbb{Q}$*. Então* $D_{\mathbb{L}/\mathbb{K}}(1, \sqrt{3}) = (-1)^{\frac{2\cdot 1}{2}} N_{\mathbb{L}/\mathbb{K}}(f'(\sqrt{3})) = -N_{\mathbb{L}/\mathbb{K}}(2\sqrt{3}) = -2^2 N_{\mathbb{L}/\mathbb{K}}(\sqrt{3}) = -4(\sqrt{3})(-\sqrt{3}) = 12$.

1.7 Anéis Noetherianos e anéis de Dedekind

Os principais objetivos desta seção são provar que o anel dos inteiros algébricos de um corpo de números é um domínio de Dedekind e mostrar a unicidade da fatoração de um ideal não nulo como um produto de ideais primos neste domínio.

Definição 1.7.1. *Sejam* A *um anel e* M *um* A*-módulo. Dizemos*

que M é um A-módulo **Noetheriano** *se satisfaz uma das seguintes condições:*

i) *Todo conjunto não vazio de submódulos de* M *contém um elemento maximal.*

ii) *Toda sequência crescente de submódulos de M é estacionária.*

iii) *Todo submódulo de M é finitamente gerado.*

Um anel A é chamado Noetheriano se quando considerado como um A-módulo for Noetheriano.

Exemplo 1.7.1. *Todo anel principal é Noetheriano, uma vez que seus ideais são submódulos gerados por um elemento.*

Proposição 1.7.1. *(*Samuel, 1967, p.46, Prop.1*) Sejam A um anel, M um A-módulo e* M' *um submódulo de* M*. Então M é Noetheriano se, e somente se,* M' *e* $\frac{M}{M'}$ *são Noetherianos.*

Demonstração. Suponhamos que M é Noetheriano. Seja $(M_n)_{n\geq 0}$ uma sequência crescente de submódulos de M', que também é uma sequência de submódulos de M. Como M é Noetheriano, segue que $(M_n)_{n\geq 0}$ é estacionária, ou seja, M' é Noetheriano. Para mostrarmos que $\frac{M}{M'}$ é Noetheriano, sejam $S = \{$conjunto dos submódulos de M contendo $M'\}$ e $S' = \{$conjunto dos submódulos de $\frac{M}{M'}\}$. Temos que existe uma aplicação bijetora $\phi : S \longrightarrow S'$ definida por $\phi(H) = \varphi(H)$ onde $\varphi : M \longrightarrow \frac{M}{M'}$ é o homomorfismo canônico. A inversa de ϕ é dada por $\theta : S' \longrightarrow S$, onde $\theta(H') = \varphi^{-1}(H')$. Através do isomorfismo φ temos que $\frac{M}{M'}$ também é Noetheriano, uma vez que se $(H'_n)_{n\geq 0}$ é uma sequência crescente de submódulos de $\frac{M}{M'}$, então $(\theta(H'_n))_{n\geq 0}$ é uma sequência crescente de submódulos de M e como M é Noetheriano, segue que $(\theta(H'_n))_{n\geq 0}$ é estacionária, o que implica que $(H'_n)_{n\geq 0}$ é estacionária, ou seja, $\frac{M}{M'}$ é Noetheriano.

Reciprocamente, suponha que M' e $\frac{M}{M'}$ são Noetherianos. Seja $(M_n)_{n\geq 0}$ uma sequência crescente de submódulos de M. Como M' é Noetheriano, segue que a sequência $(M' \cap M_n)_{n\geq 0}$ é estacionária, e como $\frac{M}{M'}$ é Noetheriano, segue que a sequência $\left(\frac{M_n + M'}{M'}\right)_{n\geq 0}$ é estacionária. Assim, a sequência $(M_n + M')_{n\geq 0}$ é estacionária e portanto $(M_n)_{n\geq 0}$ é estacionária, ou seja, M é Noetheriano. ■

Corolário 1.7.1. *(*Samuel, 1967, p.47, Corol.1*) Sejam A um anel e $M_1, \cdots, M_n$ A-módulos Noetherianos. Então $M_1 \times \cdots \times M_n$ é um A-módulo Noetheriano.*

Demonstração. Faremos a prova por indução sobre n. Para $n = 2$ identificando $M_1 \simeq M_1 \times \{0\} \subseteq M_1 \times M_2$ e $M_2 \simeq \{0\} \times M_2 \subseteq M_1 \times M_2$, temos que $\frac{M_1 \times M_2}{M_1 \times \{0\}}$ é isomorfo a M_2. Como M_2 e $M_1 \times \{0\}$ são Noetherianos, segue da Proposição 1.7.1 que $M_1 \times M_2$ é Noetheriano. Agora, suponha por hipótese de indução que $M = M_1 \times \cdots \times M_{n-1}$ é Noetheriano. Como M_n é Noetheriano, segue do caso $n = 2$ que $M = M_1 \times \cdots \times M_n$ é Noetheriano. ■

Corolário 1.7.2. *(*Samuel, 1967, p.47, Corol.2*) Sejam A um anel Noetheriano e M um A-módulo finitamente gerado. Então M é um A-módulo Noetheriano.*

Demonstração. Seja $\{e_1, \cdots, e_n\}$ um conjunto de geradores de M sobre A. Temos que a aplicação $\phi : A^n \longrightarrow M$ definida por $\phi(a_1, a_2, \cdots, a_n) = \sum_{i=1}^{n} a_i e_i$ é um homomorfismo sobrejetor e que $\frac{A^n}{Ker(\phi)}$ é isomorfo a M. Pelo Corolário 1.7.1 temos que A^n é Noetheriano, e da Proposição 1.7.1, segue que $Ker(\phi)$ e M são Noetherianos. ■

Proposição 1.7.2. *(*Samuel, 1967, p.47, Prop.1*) Sejam A um anel Noetheriano e integralmente fechado, $\mathbb{K}$ seu corpo de frações com característica zero, $\mathbb{L}$ uma extensão de $\mathbb{K}$ de grau n e $A_{\mathbb{L}}$ o fecho inteiro de A em $\mathbb{L}$. Então $A_{\mathbb{L}}$ é um A-módulo finitamente gerado e um anel Noetheriano.*

Demonstração. Segue do Teorema 1.6.1 que $\mathbb{A}_{\mathbb{L}}$ é um A-submódulo de um A-módulo livre de posto n, e portanto A' é um A-módulo finitamente gerado. Pelo Corolário 1.7.2, segue que $\mathbb{A}_{\mathbb{L}}$ é um A-módulo Noetheriano. Como os ideais de $\mathbb{A}_{\mathbb{L}}$ são A-submódulos de $\mathbb{A}_{\mathbb{L}}$, e sendo $\mathbb{A}_{\mathbb{L}}$ um A-módulo Noetheriano segue que os ideais de $\mathbb{A}_{\mathbb{L}}$ são Noetherianos. Portanto, $\mathbb{A}_{\mathbb{L}}$ é um anel Noetheriano. ■

Proposição 1.7.3. *(*Samuel, 1967, p.47, Lema 1*) Sejam B um anel, A um subanel de B e $\mathfrak{p}$ um ideal primo de B. Então $\mathfrak{p} \cap A$ é um ideal primo de A.*

Demonstração. Consideremos os seguintes homomorfismos $A \xrightarrow{i} B \xrightarrow{\pi} \frac{B}{\mathfrak{p}}$, onde i é a inclusão e π a projeção, e seja o homomorfismo $\theta = \pi \circ i : A \longrightarrow B/\mathfrak{p}$, definido por $\theta(a) = a + \mathfrak{p}$, $\forall a \in A$. Temos que θ é um homomorfismo, pois é composição de homomorfismos, e que $Ker(\theta) = A \cap \mathfrak{p}$, pois se $x \in Ker(\theta)$ então $x \in A$ e $\theta(x) = \overline{0}$ o que implica que $x \in A$ e $x + \mathfrak{p} = \overline{0}$, ou seja, $x \in A \cap \mathfrak{p}$. Logo, $Ker(\theta) \subset A \cap \mathfrak{p}$. Por outro lado, se $y \in A \cap \mathfrak{p}$ então $\theta(y) = (\pi \circ i)(y) = \pi(y) = y + \mathfrak{p} = \overline{0}$ e assim $y \in Ker(\theta)$, ou seja, $A \cap \mathfrak{p} \subset Ker(\theta)$. Portanto, $Ker(\theta) = A \cap \mathfrak{p}$. Logo, pelo Teorema do Isomorfismo de anéis, temos que $A/A \cap \mathfrak{p} \simeq Im(\theta) \subset B/\mathfrak{p}$. Mas como $B/\mathfrak{p}$ é um domínio, $Im(\theta)$ é um domínio. Portanto, $A/A \cap \mathfrak{p}$ é um domínio, ou seja, $A \cap \mathfrak{p}$ é um ideal primo. ■

Proposição 1.7.4. *(*Samuel, 1967, p.48, Lema 2*) Se um ideal primo $\mathfrak{p}$ de um anel A contém um produto $\mathfrak{a}_1 \cdots \mathfrak{a}_n$ de ideais de A, então $\mathfrak{p}$ contém pelo menos um dos ideais $\mathfrak{a}_i$.*

Demonstração. Suponhamos que $\mathfrak{a}_i \not\subset \mathfrak{p}$, $\forall\, i = 1, \cdots, n$. Então para cada $i = 1, \cdots, n$ existe um elemento $\alpha_j \in \mathfrak{a}_i - \mathfrak{p}$. Assim $\alpha_1 \cdots \alpha_n \notin \mathfrak{p}$, pois $\mathfrak{p}$ é um ideal primo, e $\alpha_1 \cdots \alpha_n \in \mathfrak{a}_1 \cdots \mathfrak{a}_n \subset \mathfrak{p}$ o que é um absurdo uma vez que $\alpha_i \notin \mathfrak{p}$, $\forall\, i = 1, \cdots, n$. Portanto, $\mathfrak{a}_i \subset \mathfrak{p}$, para algum $i = 1, \cdots, n$. ■

Proposição 1.7.5. *(*Samuel, 1967, p.48, Lema 3*) Se A é um anel Noetheriano, então todo ideal não nulo de A contém um produto de ideais primos não nulos de A.*

Demonstração. Sendo A Noetheriano, seus ideais são A-módulos Noetherianos. Seja F o conjunto de todos os ideais não nulos de A que não contém um produto de ideais primos não nulos de A. Suponha que $F \neq \emptyset$. Como A é Noetheriano segue que F possui um elemento maximal M. Temos que M não é primo, pois caso contrário, M não pertenceria a F. Além disso, temos que $M \neq A$. Por M não ser um ideal primo, existem elementos $x, y \in A - M$ tais que $xy \in M$, e que os ideais $< x > +M$ e $< y > +M$ contém M propriamente. Pela maximalidade de M estes ideais não estão em F, e assim existem ideais $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$, $\mathfrak{q}_1, \cdots, \mathfrak{q}_s$ primos não nulos de A, tais que $< x > +M \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r$ e $< y > +M \supset \mathfrak{q}_1 \cdots \mathfrak{q}_s$. Assim, $M \supset < xy > +M \supset \mathfrak{p}_1 \cdots \mathfrak{p}_r \mathfrak{q}_1 \cdots \mathfrak{q}_s$, o que é um absurdo. Assim $F = \emptyset$ e portanto todo ideal não nulo de A contém um produto de ideais primos não nulos de A. ■

Definição 1.7.2. *Um anel A é chamado um* **anel de Dedekind**, *se A é Noetheriano, integralmente fechado e se todo ideal primo não nulo de A é maximal.*

Exemplo 1.7.2. *Todo domínio A de ideais principais é um domínio de Dedekind. De fato, do exe 1.7.1 segue que A é Noetheriano. Da Proposição 1.3.4 segue que é A integralmente fechado. Além*

disso, em um domínio de ideais principais todo ideal primo não nulo é maximal. Portanto A é um domínio de Dedekind.

Teorema 1.7.1. *(*Samuel, 1967, p.49, Teo.1*) Sejam A um anel de Dedekind, $\mathbb{K}$ seu corpo de frações, $\mathbb{L}$ uma extensão de grau finita de $\mathbb{K}$ e $\mathbb{A}_{\mathbb{L}}$ o fecho inteiro de A em $\mathbb{L}$. Então $\mathbb{A}_{\mathbb{L}}$ é um anel de Dedekind.*

Demonstração. Sabemos que $\mathbb{A}_{\mathbb{L}}$ é integralmente fechado, Noetheriano e é um A-módulo finitamente gerado. Falta mostrar que todo ideal primo $\mathfrak{p} \neq \langle 0 \rangle$ de $\mathbb{A}_{\mathbb{L}}$ é maximal. Pela Proposição 1.7.3, temos que $\mathfrak{p} \cap A$ é um ideal primo de A. Seja $x \in \mathfrak{p} - \langle 0 \rangle$ e consideremos a equação de dependência inteira de x sobre A dada por $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$, com $a_i \in A$, $i = 1, \cdots, n-1$, não todos nulos, de grau mínimo. Assim $a_0 \neq 0$, pois caso contrário obteríamos uma equação de grau menor. Portanto temos que $a_0 = -x(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1) \in \mathbb{A}_{\mathbb{L}}x \cap A \subset \mathfrak{p} \cap A$, ou seja, $\mathfrak{p} \cap A \neq \langle 0 \rangle$. Como A é Dedekind, segue que $\mathfrak{p} \cap A$ é um ideal maximal de A e portanto $A/(\mathfrak{p} \cap A)$ é um corpo. Além disso, $A/\mathfrak{p} \cap A$ pode ser identificado com um subanel de $\mathbb{A}_{\mathbb{L}}/\mathfrak{p}$, e como $\mathbb{A}_{\mathbb{L}}$ é inteiro sobre A, segue que $\mathbb{A}_{\mathbb{L}}/\mathfrak{p}$ é inteiro sobre $A/\mathfrak{p} \cap A$. Assim, pela Proposição 1.3.2 temos que $\mathbb{A}_{\mathbb{L}}/\mathfrak{p}$ é corpo e portanto $\mathfrak{p}$ é maximal. ■

Exemplo 1.7.3. *Segue do Teorema 1.7.1 que o anel do inteiros de um corpo de números é um anel de Dedekind.*

Exemplo 1.7.4. *Seja o anel $Z[\sqrt{-5}]$. Temos que $Z[\sqrt{-5}]$ não é fatorial, uma vez que $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Além disso, $Z[\sqrt{-5}]$ não é um anel principal. De fato, temos que $N(1 + \sqrt{-5}) = N(1 - \sqrt{-5}) = 6$, $N(2) = 4$ e $N(3) = 9$, e que $1 + \sqrt{-5}$ não possui um divisor não trivial em $Z[\sqrt{-5}]$ pois se $a + b\sqrt{-5}$ é um*

divisor não trivial de $1+\sqrt{-5}$*, ou seja, se* $1+\sqrt{-5} = (a+b\sqrt{-5})y$*, com* $y \in Z[\sqrt{-5}]$*,* $y \neq \pm 1$ *e* $y \neq 1+\sqrt{-5}$*, então* $6 = N(1+\sqrt{-5}) = N(a+b\sqrt{-5})N(y)$ *e que* $N(a+b\sqrt{-5})$ *seria um divisor não trivial de 6, mas isto é impossível, pois* $a^2+5b^2 = 2$ *e* $a^2+5b^2 = 3$*, não possui solução em* $\mathbb{Z}$*. Assim,* $1+\sqrt{-5}$ *é um elemento primo. Agora, se* $Z[\sqrt{-5}]$ *fosse principal e como* $1+\sqrt{-5}$ *divide* $6 = 2\cdot 3$*, segue que* $1+\sqrt{-5}$ *divide 2 ou 3. Tomando as normas temos que 6 divide 4 ou 9, o que é um absurdo. Portanto* $Z[\sqrt{-5}]$ *não é um anel principal.*

Definição 1.7.3. *Sejam* A *um domínio e* $\mathbb{K}$ *seu corpo de frações. Um* A*-submódulo* I *de* $\mathbb{K}$ *é chamado de* **ideal fracionário** *de* A *se existe um* $d \in A - \{0\}$ *tal que* $d \cdot I \subset A$*. Quando* $d = 1$ *dizemos que* I *é um ideal inteiro.*

Observação 1.7.1. *Segue da Definição 1.7.3 que os elementos de um ideal fracionário* I *tem um denominador comum* $d \in A$*.*

Proposição 1.7.6. *(*Ribeiro, 2013, p.29*) Se* A *é um domínio Noetheriano então todo ideal fracionário* I *de* A *é um* A*-módulo finitamente gerado.*

Demonstração. Como I é um ideal fracionário, então existe $d \in A - \{0\}$ tal que $d \cdot I \subset A$. Assim, $I \subset d^{-1}A$. Além disso, $d^{-1}A$ é um A-módulo e a função $\phi : A \longrightarrow d^{-1}A$ tal que $\phi(x) = d^{-1}x$ define um isomorfismo entre A e $d^{-1}A$, e como A é Noetheriano então concluímos que $d^{-1}A$ é Noetheriano. Logo, I é um A-módulo finitamente gerado. ■

Proposição 1.7.7. *(*Ribeiro, 2013, p.29*) Sejam A um domínio e* $\mathbb{K}$ *seu corpo de frações. Todo A-submódulo finitamente gerado de* $\mathbb{K}$ *é um ideal fracionário.*

Demonstração. Se $\{x_1, \cdots, x_n\}$ é um conjunto finito de geradores de I, então os $x_i^{'}s$ tem um denominador comum d dado pelo produto dos denominadores d_i, onde $x_i = a_i d_i^{-1}$, com $a_i, d_i \in A$. Assim $dI \subset A$ e portanto I é um ideal fracionário. ■

Observação 1.7.2. *O produto $II^{'}$ de dois ideais fracionários I e $I^{'}$ é definido como o conjunto das somas $\sum_i x_i y_i$ com $x_i \in I$ e $y_i \in I$. Sendo I e $I^{'}$ ideais fracionários com denominadores comuns d e $d^{'}$, então os conjuntos $I \cap I^{'}$, $I + I^{'}$ e $II^{'}$ são ideais fracionários, os quais são A-submódulos de $\mathbb{K}$ e tem denominadores comuns d ou $d^{'}$, $dd^{'}$ e $dd^{'}$, respectivamente.*

Lema 1.7.1. *(*Ribeiro, 2013, p.31, Lema 2.7.1*) Sejam A um anel de Dedekind que não é um corpo e $\mathbb{K}$ seu corpo de frações. Seja $\mathfrak{m}$ um ideal maximal de A. Então $\mathfrak{m}^{'} = \{x \in \mathbb{K} : x\mathfrak{m} \subset A\}$ é um ideal fracionário de $\mathbb{K}$.*

Demonstração. Como A não é um corpo, temos que $\mathfrak{m} \neq \{0\}$ e que $\mathfrak{m}^{'} \neq \emptyset$, pois $0 \in \mathfrak{m}^{'}$. Sejam $x, y \in \mathfrak{m}^{'}$. Então pela definição de $\mathfrak{m}^{'}$, temos que $x\mathfrak{m} \subset A$ e $y\mathfrak{m} \subset A$, e portanto $(x + y)\mathfrak{m} = x\mathfrak{m} + y\mathfrak{m} \subset A$, ou seja, $x + y \in \mathfrak{m}^{'}$. Agora, sejam $x \in \mathfrak{m}^{'}$ e $a \in A$. Assim $x\mathfrak{m} \subset A$, e portanto $(xa)\mathfrak{m} = a(x\mathfrak{m}) \subset A$, ou seja, $xa \in \mathfrak{m}^{'}$. Finalmente, temos que $d\mathfrak{m} \subset A$, para todo $d \in A - \{0\}$, ou seja, $\mathfrak{m}^{'}$ é um ideal fracionário de $\mathbb{K}$. ■

Teorema 1.7.2. *(*Samuel, 1967, p.50, Teo. 2*) Sejam A um anel de Dedekind que não é um corpo e $\mathbb{K}$ seu corpo de frações. Todo ideal maximal de A é inversível no conjunto dos ideais fracionários de A.*

Demonstração. Seja $\mathfrak{m}$ um ideal maximal de A. Pelo Lema 1.7.1 temos que $\mathfrak{m}^{'} = \{x \in \mathbb{K} : x\mathfrak{m} \subset A\}$ é um ideal fracionário de $\mathbb{K}$.

Pela definição de $\mathfrak{m}'$, segue que $\mathfrak{m}'\mathfrak{m} \subset A$, e como $\mathfrak{m}$ é um ideal de A, segue que $\mathfrak{m} = \mathfrak{m}A \subset \mathfrak{m}\mathfrak{m}' \subset A$. Desde que $\mathfrak{m}$ é maximal, temos que $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$ ou $\mathfrak{m}\mathfrak{m}' = A$. Vamos mostrar que $\mathfrak{m}\mathfrak{m}' \neq \mathfrak{m}$. Para isto suponhamos que $\mathfrak{m}\mathfrak{m}' = \mathfrak{m}$. Seja $x \in \mathfrak{m}'$. Então $x\mathfrak{m} \subset \mathfrak{m}$; $x^2\mathfrak{m} \subset \mathfrak{m}; \cdots; x^n\mathfrak{m} \subset \mathfrak{m}$. Se $d \in \mathfrak{m}$ é não nulo, temos que $x^n d \in A$, para todo $n \in \mathbb{N}$. Assim, $A[x]$ é um ideal fracionário de A, e como A é Noetheriano, segue da Proposição 1.7.6 que $A[x]$ é um A-módulo finitamente gerado. Portanto, pelo Teorema 1.3.1 segue que x é inteiro sobre A, e como A é integralmente fechado, segue que $x \in A$, ou seja, $\mathfrak{m}' \subset A$. Como $A \subset \mathfrak{m}'$, segue que $A = \mathfrak{m}'$. Por outro lado, se $a \in \mathfrak{m} - < 0 >$, então pela Proposição 1.7.5, o ideal aA contém um produto de ideais primos não nulos $\mathfrak{p}_1 \cdots \mathfrak{p}_n$, de A com n o menor possível. Assim, $\mathfrak{m} \supset aA \supset \mathfrak{p}_1 \cdots \mathfrak{p}_n$. Pela Proposição 1.7.4 temos que $\mathfrak{m} \supset \mathfrak{p}_i$, para algum $i = 1, \cdots, n$, e sem perda de generalidade, digamos que $\mathfrak{m} \supset \mathfrak{p}_1$. Como $\mathfrak{p}_1$ é maximal pois A é Dedekind, segue que $\mathfrak{m} = \mathfrak{p}_1$. Tomando $\mathfrak{b} = \mathfrak{p}_2 \cdots \mathfrak{p}_n$, temos que $aA \supset \mathfrak{m}\mathfrak{b}$ e $aA \not\supset \mathfrak{b}$ devido a minimalidade de n. Assim, existe $z \in \mathfrak{b}$ tal que $z \notin aA$. Como $\mathfrak{m}\mathfrak{b} \subset aA$ segue que $\mathfrak{m}\frac{z}{a} \subset A$. Assim, $\frac{z}{a} \in \mathfrak{m}'$, e como $z \notin aA$, temos que $\frac{z}{a} \notin A$, ou seja, $\mathfrak{m}' \neq A$, o que contradiz o fato de $\mathfrak{m}' = A$. Portanto, $\mathfrak{m}\mathfrak{m}' = A$, ou seja, $\mathfrak{m}'$ é o inverso de $\mathfrak{m}$. ■

Teorema 1.7.3. *(*Samuel, 1967, p.50, Teo.3(a)*) Sejam A um anel de Dedekind e $\mathfrak{a} \neq A$ um ideal não nulo de A. Então existem ideais primos não nulos $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$ de A e inteiros positivos $\mathfrak{e}_1, \cdots, \mathfrak{e}_t$ tal que $\mathfrak{a} = \prod_{i=1}^{t} \mathfrak{p}_i^{e_i}$, e esta expressão é única.*

Demonstração. Pela Proposição 1.7.5, existem ideais primos $\mathfrak{p}_1, \cdots$

$, \mathfrak{p}_v$ não nulos de A tal que $\mathfrak{p}_1 . \cdots . \mathfrak{p}_v \subset \mathfrak{a}$. Provemos que $\mathfrak{a}$ é um

produto de ideais primos por indução sobre v. Se $v = 1$, temos que $\mathfrak{a} \subset \mathfrak{p}_1$, mas como $\mathfrak{p}_1$ é maximal, pois A é Dedekind, então $\mathfrak{a} = \mathfrak{p}_1$, e assim $\mathfrak{a}$ é primo. Agora, suponhamos que todo ideal que contém um produto com $v-1$ ideais primos não nulos de A é um produto de ideais primos de A. Temos que $\mathfrak{p}_1 \cdots \mathfrak{p}_v \subset \mathfrak{a}$, e como A é Dedekind segue que $\mathfrak{a}$ está contido em um ideal maximal $\mathfrak{m}$ de A. Seja $\mathfrak{m}^{-1}$ o ideal fracionário inverso de $\mathfrak{m}$. Como $\mathfrak{m} \supset \mathfrak{a} \supset \mathfrak{p}_1 \cdots \mathfrak{p}_v$, segue da Proposição 1.7.4, que $\mathfrak{m}$ contém um dos $\mathfrak{p}_i's$, para $i = 1, \cdots v$. Suponhamos que $\mathfrak{m} \supset \mathfrak{p}_v$, e assim, $\mathfrak{m} = \mathfrak{p}_v$, pois $\mathfrak{p}_v$ é maximal. Portanto $\mathfrak{p}_1 \cdots \mathfrak{p}_{v-1} \subset \mathfrak{a}\mathfrak{m}' \subset \mathfrak{m}\mathfrak{m}' = A$. Da hipótese de indução decorre que $\mathfrak{a}\mathfrak{m}^{-1} = \mathfrak{q}_1 \cdots \mathfrak{q}_s$, com $\mathfrak{q}_j's$, para $j = 1, \cdots, s$, ideais primos não nulos de A, e portanto $\mathfrak{a} = \mathfrak{q}_1 \cdots \mathfrak{q}_s\mathfrak{p}_v$, como queríamos. Para provar a unicidade suponhamos que $\prod_{i=1}^{t} \mathfrak{p}^{e_i} = \prod_{j=1}^{h} \mathfrak{p}^{e_j}$. Então $A = \prod \mathfrak{p}^{e_i - e_j}$. Se $e_i - e_j \neq 0$, podemos separar os expoentes positivos e os expoentes negativos e reescrevê-los como

$$\mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2} \cdots \mathfrak{p}_r^{\alpha_r} = \mathfrak{q}_1^{\beta_1}\mathfrak{q}_2^{\beta_2} \cdots \mathfrak{q}_v^{\beta_v},$$

com $\mathfrak{p}_i$, $\mathfrak{q}_j$ ideais primos não nulos de A e α_i, $\beta_j > 0$ para $\mathfrak{p}_i \neq \mathfrak{q}_j$, $\forall i, j$. Portanto $\mathfrak{p}_1$ contém $\mathfrak{q}_1^{\beta_1}\mathfrak{q}_2^{\beta_2} \cdots \mathfrak{q}_v^{\beta_v}$ e pela Proposição 1.7.4 segue que $\mathfrak{p}_1 \supset \mathfrak{q}_j$, para algum j. Suponhamos sem perda de generalidade que $\mathfrak{p}_1 \supset \mathfrak{q}_1$. Como $\mathfrak{p}_1$ e $\mathfrak{q}_1$ são ideais maximais, segue que $\mathfrak{p}_1 = \mathfrak{q}_1$. Portanto $e_i - e_j = 0$, isto é, $e_i = e_j$, o que é uma contradição pois $\mathfrak{p}_i \neq \mathfrak{q}_j$, $\forall\, i, j$ e assim concluímos que a expressão é única. ■

Corolário 1.7.3. *Se A é um anel de Dedekind, então o conjunto dos ideais fracionários não nulos de A formam um grupo com relação a multiplicação.*

Demonstração. (Samuel, 1967, p.50, Teo.3(b)). ■

1.8 Norma de um ideal

Sejam $\mathbb{K}$ uma extensão finita de $\mathbb{Q}$ e $\mathbb{A}_{\mathbb{K}}$ o anel dos inteiros de $\mathbb{K}$. Nesta seção apresentamos a norma de um ideal como uma generalização da norma de um elemento de $\mathbb{A}_{\mathbb{K}}$.

Definição 1.8.1. *Seja $\mathfrak{a}$ um ideal não nulo de $\mathbb{A}_{\mathbb{K}}$. A* **norma do ideal $\mathfrak{a}$**, *é definida como o número de elementos do anel quociente $\mathbb{A}_{\mathbb{K}}/\mathfrak{a}$, isto é, $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{a}) = \#(\mathbb{A}_{\mathbb{K}}/\mathfrak{a})$.*

Observação 1.8.1. *Quando não houver dúvida quanto ao anel que contém o ideal $\mathfrak{a}$, usaremos $N(\mathfrak{a})$ ao invés de $N_{\mathbb{K}/\mathbb{Q}}(\mathfrak{a})$.*

Exemplo 1.8.1. *Seja $\mathfrak{a}$ um ideal principal de $\mathbb{Z}[i]$, onde $i^2 = -1$, gerado por $2 - i$. Assim, $\frac{\mathbb{Z}[i]}{\mathfrak{a}} = \{x + \mathfrak{a};\ x \in \mathbb{Z}[i]\}$. A norma de $\mathfrak{a}$ é o número das classes laterais de $\mathfrak{a}$. Uma vez que $2 - i \equiv 0 (mod\ \mathfrak{a})$, segue que $2 \equiv i (mod\ \mathfrak{a})$. Assim para $x = a + bi$, com $a, b \in \mathbb{Z}$, temos que $x = a + bi \equiv a + 2b (mod\ \mathfrak{a})$. Como $(2 + i)(2 - i) = 5 \in \mathfrak{a}$, segue que as classes laterais de $\mathfrak{a}$ em $\mathbb{Z}[i]$ são $\{0, 1, 2, -1, -2\}$, ou seja, $N(\mathfrak{a}) = 5$.*

Proposição 1.8.1. *(*Samuel, 1967, p.52, Prop.1*) Se $\alpha \in \mathbb{A}_{\mathbb{K}}$, $\alpha \neq 0$, então $|N(\alpha)| = \#\mathbb{A}_{\mathbb{K}}/\mathbb{A}_{\mathbb{K}}\alpha$.*

Demonstração. Seja $\alpha \in \mathbb{A}_{\mathbb{K}}$, $\alpha \neq 0$. Então, pelo Corolário 1.5.1, temos que $N(\alpha) \in \mathbb{Z}$. Pelo Corolário 1.6.3 temos que $\mathbb{A}_{\mathbb{K}}$ é um $\mathbb{Z}$-módulo livre de posto n. Além disso, como $\psi : \mathbb{A}_{\mathbb{K}} \longrightarrow \mathbb{A}_{\mathbb{K}}\alpha$ definida por $\psi(a) = a\alpha$, com $a \in \mathbb{A}_{\mathbb{K}}$, é um isomorfismo, segue que $\mathbb{A}_{\mathbb{K}}\alpha$ é um $\mathbb{Z}$-submódulo livre de posto n de $\mathbb{A}_{\mathbb{K}}$. Pelo Teorema 1.2.1 existe uma base $\{e_1, e_2, \cdots, e_n\}$ do $\mathbb{Z}$-módulo $\mathbb{A}_{\mathbb{K}}$ e elementos $c_i \in \mathbb{N}$ tal que $\{c_1e_1, c_2e_2, \cdots, c_ne_n\}$ é uma base de $\mathbb{A}_{\mathbb{K}}\alpha$. Também temos que o grupo abeliano $\mathbb{A}_{\mathbb{K}}/\mathbb{A}_{\mathbb{K}}\alpha$ é isomorfo ao grupo abeliano $\prod_{i=1}^{n} \mathbb{Z}/c_i\mathbb{Z}$, cuja ordem é $c_1c_2 \cdots c_n$. Agora seja a aplicação linear

$\phi : \mathbb{A}_{\mathbb{K}} \longrightarrow \mathbb{A}_{\mathbb{K}}\alpha$ definida por $\phi(e_i) = c_i\alpha_i$, $i = 1, \cdots, n$. Temos que $\det(\phi) = c_1c_2\cdots c_n$. Por outro lado, como $\{\alpha e_1, \cdots, \alpha e_n\}$ também é uma base de $\mathbb{A}_{\mathbb{K}}\alpha$, segue que existe um endomorfismo de $\mathbb{Z}$-módulo $\varphi : \mathbb{A}_{\mathbb{K}}\alpha \longrightarrow \mathbb{A}_{\mathbb{K}}\alpha$, definido por $\varphi(c_ie_i) = \alpha e_i$, $i = 1\cdots, n$. Logo, como o $\det(\varphi) \in \mathbb{Z}$ e é inversível, segue que $\det(\varphi) = \pm 1$. Mas, a composição $\varphi\phi$ é um homomorfismo, que é a multiplicação por α, e seu determinante é por definição $N(\alpha)$. Portanto, como $\det(\varphi\phi) = \det(\varphi)\det(\phi)$, segue que $N(\alpha) = \pm c_1\cdots c_n = \pm\#(\mathbb{A}_{\mathbb{K}}/\mathbb{A}_{\mathbb{K}}\alpha)$. ■

Proposição 1.8.2. *(*Samuel, 1967, p.52*) Se $\mathfrak{a}$ é um ideal não nulo de $\mathbb{A}_{\mathbb{K}}$, então o quociente $\mathbb{A}_{\mathbb{K}}/\mathfrak{a}$ é finito.*

Demonstração. Seja $\alpha \in \mathfrak{a}$, $\alpha \neq 0$. Temos que $\mathbb{A}_{\mathbb{K}}\alpha \subset \mathfrak{a}$. Logo $\mathbb{A}_{\mathbb{K}}/\mathfrak{a} \simeq \dfrac{\mathbb{A}_{\mathbb{K}}/\mathbb{A}_{\mathbb{K}}\alpha}{\mathfrak{a}/\mathbb{A}_{\mathbb{K}}\alpha}$. Assim, $\#\dfrac{\mathbb{A}_{\mathbb{K}}}{\mathbb{A}_{\mathbb{K}}\alpha} = \#\dfrac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}}\#\dfrac{\mathfrak{a}}{\mathbb{A}_{\mathbb{K}}\alpha} < \infty$. Portanto, $N(\mathfrak{a}) = \#\dfrac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}}$ é finito. ■

Proposição 1.8.3. *(*Samuel, 1967, p.52, Prop.2*) Se $\mathfrak{a}$ e $\mathfrak{b}$ são ideais não nulos de $\mathbb{A}_{\mathbb{K}}$, então $N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b})$.*

Demonstração. Pelo Teorema 1.7.3, temos que $\mathfrak{b} = \prod_{i\in I}\mathfrak{p}_i^{\alpha_i}$, onde os $\mathfrak{p}_i's$ são ideais primos não nulos de $\mathbb{A}_{\mathbb{K}}$ e $\alpha_i \geq 0$, $i \in I$. Como $\mathbb{A}_{\mathbb{K}}$ é um domínio de Dedekind, então os ideais $\mathfrak{p}_i, i \in I$, são ideais maximais. Seja $\mathfrak{p}_i = \mathfrak{m}$, para algum $i \in I$. Por indução sobre o número de fatores, é suficiente provar que

$$N(\mathfrak{am}) = N(\mathfrak{a})N(\mathfrak{m}). \tag{1.8}$$

Segue da definição de norma que (1.8) se verifica se

$$\#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{am}}\right) = \#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}}\right)\cdot\#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{m}}\right). \tag{1.9}$$

Mas, do homomorfismo sobrejetor $\varphi : \frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{am}} \longrightarrow \frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}}$, definido por $\varphi(x+\mathfrak{am}) = x+\mathfrak{a}$, temos que $Ker(\varphi) = \frac{\mathfrak{a}}{\mathfrak{ap}}$, e pelo Teorema do Isomorfismo temos que, $\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{am}}/\frac{\mathfrak{a}}{\mathfrak{am}} \simeq \mathbb{A}_{\mathbb{K}}/\mathfrak{a}$. Logo,

$$\#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{am}}\right) = \#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}}\right) \cdot \#\left(\frac{\mathfrak{a}}{\mathfrak{am}}\right). \tag{1.10}$$

De (1.9) e (1.10), podemos concluir que (1.8) é verificado se $\#\left(\frac{\mathbb{A}}{\mathfrak{m}}\right) = \#\left(\frac{\mathfrak{a}}{\mathfrak{am}}\right)$. Agora, mostremos que $\frac{\mathfrak{a}}{\mathfrak{am}}$ é um espaço vetorial sobre $\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{m}}$ de dimensão 1. De fato, sejam as operações

$$\begin{aligned} + : \frac{\mathfrak{a}}{\mathfrak{am}} \times \frac{\mathfrak{a}}{\mathfrak{am}} &\longrightarrow \frac{\mathfrak{a}}{\mathfrak{am}} \\ (x+\mathfrak{am}, y+\mathfrak{am}) &\longrightarrow (x+y)+\mathfrak{am}. \end{aligned}$$

$$\begin{aligned} \cdot : \frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{m}} \times \frac{\mathfrak{a}}{\mathfrak{am}} &\longrightarrow \frac{\mathfrak{a}}{\mathfrak{am}} \\ (x+\mathfrak{m}, y+\mathfrak{am}) &\longrightarrow (\alpha x)+\mathfrak{am}. \end{aligned}$$

Estão bem definidas:

Soma: $x+\mathfrak{am} = x^{'}+\mathfrak{am}$ e $y+\mathfrak{am} = y^{'}+\mathfrak{am} \Longrightarrow \overline{x}-\overline{x^{'}} = \overline{0}$ e $\overline{y}-\overline{y^{'}} = \overline{0} \Longrightarrow \overline{x}+\overline{y} = \overline{x^{'}}+\overline{y^{'}} \Longrightarrow (x+\mathfrak{am})+(y+\mathfrak{am}) = (x^{'}+\mathfrak{am})+(y^{'}+\mathfrak{am}) \Longrightarrow (x+y)+\mathfrak{am} = (x^{'}+y^{'})+\mathfrak{am}$.

Produto: $x+\mathfrak{am} = x^{'}+\mathfrak{am}$ e $\alpha+\mathfrak{m} = \alpha^{'}+\mathfrak{m} \Longrightarrow x-x^{'} \in \mathfrak{am}$ e $\alpha-\alpha^{'} \in \mathfrak{m}$. Assim, $\alpha^{'}x^{'}-\alpha x = x^{'}(\alpha^{'}-\alpha)+(x^{'}-x)\alpha \in \mathfrak{am}$. Assim, $\frac{\mathfrak{a}}{\mathfrak{am}}$ é um espaço vetorial sobre $\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{m}}$. Temos que os $\mathbb{A}_{\mathbb{K}}$-submódulos de $\frac{\mathfrak{a}}{\mathfrak{am}}$ são ideais e são do tipo $\frac{\mathfrak{b}}{\mathfrak{am}}$, onde $\mathfrak{b}$ é um ideal tal que $\mathfrak{am} \subseteq \mathfrak{b} \subseteq \mathfrak{a}$. Mas, como todo ideal num domínio de Dedekind admite inverso, segue que

$$\mathfrak{a}^{-1}\mathfrak{am} \subseteq \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathfrak{a}^{-1}\mathfrak{a} \overset{a^{-1}a=\mathbb{A}_{\mathbb{K}}}{\Longrightarrow} \mathfrak{m} \subseteq \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathbb{A}_{\mathbb{K}} \overset{m\ maximal}{\Longrightarrow}$$
$$\mathfrak{m} = \mathfrak{a}^{-1}\mathfrak{b} \text{ ou } \mathfrak{a}^{-1}\mathfrak{b} = \mathbb{A}_{\mathbb{K}} \Longrightarrow \mathfrak{am} = \mathfrak{b} \text{ ou } \mathfrak{b} = \mathfrak{a}.$$

Portanto, não existe $\mathfrak{b}$ tal que $\mathfrak{a}\mathfrak{m} \subseteq \mathfrak{b} \subseteq \mathfrak{a}$. Assim, os $\mathbb{A}_{\mathbb{K}}$-submódulos de $\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}}$, ou os subespaços do espaço vetorial $\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}}$ são apenas os triviais. Portanto, $dim_{\frac{\mathbb{A}_{\mathbb{K}}}{m}} \frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}} = 1$ e então $\#\left(\frac{\mathbb{A}_{\mathbb{K}}}{\mathfrak{a}\mathfrak{m}}\right) = \#\left(\frac{\mathfrak{a}}{\mathfrak{a}\mathfrak{m}}\right)$. ■

1.9 Formas quadráticas sobre o $\mathbb{R}^n$

Nesta seção apresentamos as formas quadráticas sobre o $\mathbb{R}^n$, que serão muito útil no estudo das aplicações das formas quadráticas aos corpos ciclotômicos e desta forma calcular a densidade de centro dos reticulados obtidos via esses corpos.

Para cada inteiro n, seja $Q_n(\underline{X})$ a **forma quadrática** sobre o $\mathbb{R}^n$ definida por

$$Q_n(\underline{X}) = Q_n(X_1, \cdots, X_n) = \sum_{i=1}^{n} X_i^2 + \sum_{1 \leq i < j \leq n} (X_i - X_j)^2.$$

Da igualdade

$$\sum_{1 \leq i < j \leq n} (X_i - X_j)^2 = (n-1) \sum_{i=1}^{n} X_i^2 - 2 \sum_{1 \leq i < j \leq n} X_i X_j$$

obtém-se que

$$Q_n(X_1, \cdots, X_n) = n \sum_{i=1}^{n} X_i^2 - 2 \sum_{1 \leq i < j \leq n} X_i X_j.$$

Observamos que $Q_n(\underline{X})$ é uma função positiva definida e totalmente simétrica, isto é, $Q_n(X_1, \cdots, X_n) = Q_n(X_{\sigma(1)}, \cdots, X_{\sigma(n)})$, onde σ é uma permutação qualquer do conjunto $\{1, \cdots, n\}$.

A próxima proposição é de grande importância no cálculo do raio de empacotamento de certos reticulados.

Proposição 1.9.1. *(*Flores, 1996, p.64, Prop.3.4.1*)* **i)** *O menor valor que $Q_n(X_1, \cdots, X_n)$ assume com entradas inteiras não todas*

nulas é n.

ii) *Para $a \in \mathbb{Z}^n$, temos que $Q_n(\underline{a}) = n$ quando $\underline{a} = \pm(1, 1, \cdots, 1)$ ou $\underline{a} = \pm e_i$, $i = 1, \cdots, n$; onde $\{e_1, \cdots, e_n\}$ é a $\mathbb{Z}$-base canônica de $\mathbb{Z}^n$.*

Demonstração. i) Observe que

$$Q_n(X_1, \cdots, X_n) = Q_{n-1}(X_1, \cdots, X_{n-1}) + X_n^2 + \sum_{i=1}^{n-1}(X_i - X_n)^2.$$

Se $a_1 = \cdots = a_{n-1} = 0$, então $Q_n(a_1, \cdots, a_n) = a_n^2 + (n-1)a_n^2 = na_n^2 \geq n$, para $a_n \neq 0$. Caso contrário, por hipótese de indução, tem-se que

$$Q_{n-1}(a_1, \cdots, a_{n-1}) \geq n - 1,$$

e neste caso

$$a_n^2 + \sum_{i=1}^{n-1}(a_i - a_n)^2 \geq n - 1.$$

De fato, se $a_n \neq 0$ então $a_n^2 \geq 1$. Caso contrário, pelo menos uma das parcelas $(a_i - a_n)^2$ será não nula.

ii) A prova se faz usando novamente indução sobre n. Para $j = 1$ temos que $Q_1(\underline{a}) = Q_1(a_1) = a_1^2 = 1$, onde $a_1 = \pm 1$. Suponhamos que o resultado seja válido para $j = n - 1$. Observe que $a_n^2 + \sum_{i=1}^{n-1}(a_i - a_n)^2 > 0$. Assim temos que $Q_n(\underline{a}) = Q_n(a_1, \cdots, a_n) = Q_{n-1}(a_1, \cdots, a_{n-1}) + a_n^2 + \sum_{i=1}^{n-1}(a_i - a_n)^2 > n - 1 + 0 = n - 1$. Agora, se $a_n^2 + \sum_{i=1}^{n-1}(a_i - a_n)^2 \neq 1$ então $Q_n(a_1, \cdots, a_n)$ assumiria um valor maior que $n+1$, o que contraria o item (i). Portanto, $a_n^2 + \sum_{i=1}^{n-1}(a_i - a_n)^2 = 1$ e assim $Q_n(\underline{a}) = Q_n(a_1, \cdots, a_n) = n - 1 + 1 = n$, se $\underline{a} = \pm(1, \cdots, 1)$ ou $\underline{a} = \pm e_i$, $i = 1, \cdots, n$ onde $\{e_1, \cdots, e_n\}$ é a $\mathbb{Z}$-base canônica de $\mathbb{Z}^n$. ■

Lema 1.9.1. *(*Flores, 1996, p.80, Lema A.1*) Se $Q_n(X_1, \cdots, X_n) = \sum_{i=1}^{n} X_1^2 + \sum_{i<j}(X_i - X_j)^2$, e $a = (a_1, \cdots, a_n) \in \mathbb{R}^n$, então*

$$Q_n(a_1, \cdots, a_n) = d^2(a, 0) + n.d^2(a, \Delta),$$

onde $d^2(a,0)$ *e* $d^2(a,\Delta)$ *são os quadrados das distâncias euclidianas de* a *até a origem e de* a *até a diagonal de* $\mathbb{R}^n$, *respectivamente.*

Demonstração. Se $X = (x, \cdots, x)$ é um elemento qualquer da diagonal de $\mathbb{R}^n$, então

$$d(a, X)^2 = \sum_{i=1}^{n}(a_i - x)^2.$$

Esta distância será mínima quando $\frac{d}{dx}(\sum(a_i - x)^2) = 0$, e isto ocorre para $x = (1/n).\sum_{i=1}^{n} a_i$. Assim

$$\begin{aligned}
d^2(a,\Delta) &= \sum_{j=1}^{n}\left(a_j - (1/n).\left(\sum_{i=1}^{n} a_i\right)\right)^2 \\
&= \sum_{j=1}^{n}\left(a_j^2 - (2/n).a_j.\left(\sum_{i=1}^{n} a_i\right) + \left(\sum_{i=1}^{n} a_i\right)^2/n^2\right) \\
&= \sum_{j=1}^{n} a_j^2 - (2/n).\left(\sum_{j=1}^{n} a_j\right).\left(\sum_{i=1}^{n} a_i\right) + n.\left(\sum_{i=1}^{n} a_i\right)^2/n^2 \\
&= \sum_{j=1}^{n} a_j^2 - (2/n).\left(\sum_{j=1}^{n} a_j\right)^2 + (1/n).\left(\sum_{j=1}^{n} a_j\right)^2 \\
&= \left(\sum_{j=1}^{n} a_j^2\right) - (1/n).\left(\sum_{i=1}^{n} a_i\right)^2.
\end{aligned}$$

Logo,

$$n.d^2(P,a) = (n-1).\left(\sum_{i=1}^{n} a_i^2\right) - 2\left(\sum_{1\le i<j\le n} a_i.a_j\right),$$

e somando $d^2(P,0) = \sum_{i=1}^{n} a_i^2$ em ambos os membros chegamos ao resultado desejado. ■

Teorema 1.9.1. *(*Flores, 1996, p.81, Teo.A.2*) Sejam os números reais* $a_1, \cdots, a_r$, *com* $r < n$. *Se*

$$F(X_{r+1}, \cdots, X_n) = Q_n(a_1, \cdots, a_r, X_{r+1}, \cdots, X_n),$$

então F *atinge seu mínimo com coordenadas inteiras no ponto*

$$(y, y, \cdots, y), \text{ onde } y = \left[\left(\sum_{i=1}^{r} a_i \right) /(r+1) \right],$$

onde [z] denota o inteiro mais próximo de z. Caso $z + 1/2$ *seja inteiro, então* $[z]$ *denota* $z - 1/2$.

Demonstração. Os pontos da reta, em $\mathbb{R}^{n-r}$, passando por $P = (x, x, \cdots, x)$, onde $x = \left(\sum_{i=1}^{r} a_i \right) /(r+1)$ e tendo $(b_{r+1}, \cdots, b_n)$ como vetor diretor são da forma

$$X = P + t(b_{r+1}, \cdots, b_n) = (x + tb_{r+1}, \cdots, x + tb_n).$$

Assim

$$F(x + tb_{r+1}, \cdots, x + tb_n) = Q(a_1, \cdots, a_r, x + tb_{r+1}, \cdots, x + tb_n) =$$
$$\sum_{i=1}^{r} a_i^2 + \sum_{i=r+1}^{n} (x + tb_i)^2 + \sum_{i<j} (a_i - a_j)^2 + \sum_{i,j} (a_i - x - tb_j)^2 +$$
$$+ \sum_{i<j} t^2 (b_i - b_j)^2 = At^2 + Bt + C,$$

onde

$$A = (r+1) \sum_{j=r+1}^{n} b_i^2 + \sum_{i<j} (b_i - b_j)^2;$$

$$B = 2x(r+1) \sum_{j=r+1}^{n} b_j - 2 \left(\sum_{i=1}^{r} a_i \right) \left(\sum_{j=r+1}^{n} b_j \right) \text{ e}$$

$$C = (n-r+1) \sum_{i=1}^{r} a_i^2 + \sum_{i<j} (a_i - a_j)^2 + (r+1)(n-r)x^2 - 2x(n-r) \sum_{i=1}^{n} a_i.$$

Como esta expressão é uma função de segundo grau na variável t, segue que derivando com relação a t, obtemos que

$$\frac{dF}{dt}(x+tb_{r+1},\cdots,x+tb_n) = 2t(r+1)\sum_{j=r+1}^{n} b_i^2 +$$
$$+2t\sum_{i<j}(b_i-b_j)^2 + 2x(r+1)\sum_{j=r+1}^{n} b_j - 2\left(\sum_{i=1}^{r} a_i\right)\left(\sum_{j=r+1}^{n} b_j\right).$$

Em $t=0$, temos que

$$\frac{dF}{dt}(0) = 2x(1+r)\sum_{j=r+1}^{n} b_j - 2(\sum_{i=1}^{r} a_i)(\sum_{j=r+1}^{n} b_j) =$$
$$= -2\left(\sum_{i=1}^{r} a_i\right)\left(\sum_{j=r+1}^{n} b_j\right) - 2\left(\sum_{i=1}^{r} a_i\right)\left(\sum_{j=r+1}^{n} b_j\right) = 0.$$

Assim, sobre as retas passando por P, o gráfico de F é uma parábola com concavidade voltada para cima, cujo menor valor é assumido em P. Seja $Y_1 = (y, y, \cdots, y)$, onde $y = \left[\frac{\sum_{i=1}^{r} a_i}{r+1}\right]$. Supomos no que segue que $y \leq x$, sendo que para o caso $y \geq x$ a demonstração é análoga. As parábolas descritas acima têm coeficiente dominante

$$r\sum_{i=r+1}^{n} b_i^2 + \left(\sum_{i=r+1}^{n} b_i^2 + \sum_{i<j}(b_i-b_j)^2\right) = r\sum_{i=r+1}^{n} b_i^2 + Q_{n-r}(v),$$

onde $v = (b_{r+1},\cdots,b_n)$ e Q_{n-r} é a forma quadrática definida no início da seção. Pelo Lema 1.9.1, segue que este coeficiente dominante é

$$r\sum_{i=r+1}^{n} b_i^2 + d^2(v,0) + (n-r)d^2(v,\Delta),$$

onde $d^2(v,0)$ e $d^2(v,\Delta)$ representam os quadrados das distâncias de v até a origem e diagonal de $\mathbb{R}^{n-r}$, respectivamente. Para determinar a direção de menor crescimento destas parábolas, consideremos vetores diretores v com comprimento 1. Na direção de v, o coeficiente dominante da parábola passando por P é dado por

$$(r+1)+(n-r)d^2(v,\Delta).$$

Logo, a direção de menor crescimento dessas parábolas é dada com $d^2(v,\Delta)$ mínimo, ou seja, na direção de Y_1, que é a diagonal. Observe que para outra direção o crescimento dessas parábolas será estritamente maior. Consequentemente, se $Y \in \mathbb{R}^{n-r}$ é tal que $F(Y) = F(Y_1)$, temos que

$$d(Y,P) \leq d(Y_1,P), \tag{1.11}$$

com igualdade se, e somente se, Y estiver na diagonal de $\mathbb{R}^{n-r}$. Agora, dado o conjunto

$$A = \{Y \in \mathbb{R}^{n-r};\ F(Y) \geq F(Y_1)\},$$

vamos calcular $A \cap \mathbb{Z}$. Para isso, vamos escrever A como a união disjunta de dois conjuntos A_1 e A_2, onde

$$A_1 = \{Y \in \mathbb{R}^{n-r};\ F(Y) < F(Y_1)\}$$
$$\text{e}$$
$$A_2 = \{Y \in \mathbb{R}^{n-r};\ F(Y) = F(Y_1)\}$$

Temos que $A_1 \cap \mathbb{Z}^{n-r} = \emptyset$. Para calcular $A_2 \cap \mathbb{Z}$ note, por (1.11), que para todo Y em A_2 temos que $d(Y,P) < d(Y_1,P)$ ou Y está na diagonal de $\mathbb{R}^{n-r}$. Os Y que satisfazem a primeira possibilidade não são inteiros. Caso Y esteja na diagonal de $\mathbb{R}^{n-r}$, novamente, por (1.11), temos $d(Y,P) = d(Y_1,P)$. Para concluir, consideremos dois casos:

1º caso: $x < y + 1/2$. Aqui, $d(Y,P) = d(Y_1,P)$ ocorre apenas para $Y = Y_1$;

2º caso: $x = y + 1/2$. Neste caso, os únicos pontos da diagonal de $\mathbb{Z}^{n-r}$ satisfazendo $d(Y,P) = d(Y_1,P)$ são Y_1 e $Y_2 = (y+1, \cdots, y+1)$.

Assim,

$$A \cap \mathbb{Z}^{n-r} = \begin{cases} Y_1, \ se\ x < y + 1/2; \\ \{Y_1, Y_2\}, \ se\ x = y + 1/2. \end{cases}$$

Para concluir, observe que para todo ponto Y de $\mathbb{Z}^{n-r}$ temos que $F(Y) \geq F(Y_1)$, ou seja, Y_1 é o ponto de mínimo de F em $\mathbb{Z}^{n-r}$. ■

Teorema 1.9.2. *(*Flores, 1996, p.84, Teo.A.3*) Sejam $m \in \mathbb{N}$ e $Q_n^{'}(m) = Q_n(m, t, \cdots, t)$, onde $t = [m/2]$, isto é, $Q^{'}(m)$ é o menor valor que $Q_n(m, X_2, \cdots, X_n)$ assume fazendo $X_2, \cdots, X_n$ variar no conjunto dos números inteiros. Então $Q^{'}$ é uma função crescente de m.*

Demonstração. Se m for par, então $t = \dfrac{m}{2}$, é inteiro e

$$Q^{'}(m) = Q_n(m, m/2, \cdots, m/2) = m^2 + 2(n-1)(m^2/4).$$

Neste caso, $[m+1] = 1/2$, e

$$Q^{'}(m+1) = Q_n(m+1, m/2, \cdots, m/2) = \\ (m+1)^2 + (n-1)(m^2/4) + (n-1)(1 + m/2)^2.$$

Logo, $Q^{'}(m+1) > Q^{'}(m)$. A prova para o caso m ímpar se faz de modo análogo. ■

Denotaremos por I_d o conjunto $\{(a_1, \cdots, a_m) \in \mathbb{Z}^m;\ |a_i| \leq d\}$.

Lema 1.9.2. *(*Flores, 1996, p.76, Lema 3.4.13*) A forma quadrática $Q_n(a_1, \cdots, a_n)$ não atinge o valor $n+1$, para $(a_1, \cdots, a_n) \in \mathbb{Z}^n$.*

Demonstração. Para $a \in I_1 = \{(a_1, \cdots, a_n) \in \mathbb{Z}^n, |a_i| \leq 1\}$ o resultado é verdadeiro. Tomemos $a \in I_2 - I_1$. Sem perda de generalidade, podemos supor que $a = (2, a_2, \cdots, a_n)$, para inteiros $a_2, \cdots, a_n$. Pelo Teorema 1.9.1 temos que

$$Q_n(a) \geq Q_n(2, 1, \cdots, 1) = 4 + n - 1 + n - 1 = 2n + 2 > n + 1,$$

e pelo Teorema 1.9.2, $Q_n(a) > n+1$, $\forall\ j$ e $a \in I_j$. ■

Definição 1.9.1. *Dados p um número primo e m um número inteiro positivo, denotamos por $v_p(m)$ a* **valorização p-ádica** *de m, ou seja, o maior número α para o qual p^α divide m.*

Proposição 1.9.2. *(*Simonato, 2000, p.61, Lema A.1*) Se n é um número inteiro positivo, p um número primo e $b_0, b_1, \cdots, b_s \in \mathbb{Z}$, com $0 \leq b_i \leq p-1$ são tais que $n = b_0 + b_1 p + \cdots + b_s p^s$, então*

$$v_p(n!) = \frac{n - \sum_{i=0}^{s} b_i}{p-1},$$

onde $v_p(n!)$ é a valorização p-ádica de $n!$.

Demonstração. Faremos por indução sobre n.

i) Se n=1, a conclusão é imediata.

ii) Suponhamos verdadeira para n, onde $n = b_0 + b_1 p + \cdots + b_s p^s$ e mostremos que a asserção é verdadeira para $n+1$, onde

$$n+1 = \begin{cases} (b_0+1) + b_1 p + \cdots + b_s p^s, \ \ se \ \ b_0 \neq p-1 \\ (b_r+1)p^r + b_{r+1}p^{r+1} + \cdots + b_s p^s, \ \ se \ \ b_0 = \cdots = b_{r-1} = p-1 \\ e \ \ b_r \leq p-2. \end{cases}$$

1° Caso: $n+1 = (b_0+1) + b_1 p + \cdots + b_s p^s$, $se\ b_0 \neq p-1$. Pelo fato de que $p \nmid n+1$ pois $b_0 + 1 \not\equiv 0 (mod\ p)$, e da hipótese de indução segue que

$$v_p((n+1)!) = v_p(n!) = \frac{n - \sum_{i=0}^{s} b_i}{p-1} = \frac{n+1 - \left(\sum_{i=0}^{s} b_i + b_0 + 1\right)}{p-1}.$$

2° Caso: $n+1 = (b_r+1)p^r + b_{r+1}p^{r+1} + \cdots + b_s p^s$, $se\ b_0 = b_1 = \cdots = b_{r-1} = p-1$. Assim

$$n+1 = p^r[(b_r+1) + b_{r+1}p + \cdots + b_s p^{s-r}] \quad \text{e}$$
$$v_p((n+1)!) = r + v_p(n!)$$

Sendo $n = (p-1)+(p-1)p+\cdots+(p-1)p^{r-1}+b_r p^r+b_{r+1}p^{r+1}+\cdots+b_s p^s$, segue que

$$\begin{aligned} r + v_p(n!) &= r + \frac{n - \sum_{i=0}^{s} b_i}{p-1} \\ &= r + \frac{n - (r(p-1) + b_r + b_{r+1} + \cdots + b_s)}{p-1} \\ &= \frac{r(p-1) + n - r(p-1) - (b_r + b_{r+1} + \cdots + b_s)}{p-1} \\ &= \frac{n - (b_r + b_{r+1} + \cdots + b_s)}{p-1} \\ &= \frac{(n+1) - [(b_r+1) + b_{r+1} + \cdots + b_s]}{p-1}. \end{aligned}$$

■

Corolário 1.9.1. *(*Simonato, 2000, p.62, Corol.A.2*) Se p é um número primo e m, n são inteiros positivos com $m \leq n$ tais que*

$$\begin{aligned} n &= a_0 + a_1 p + \cdots + a_s p^s,\ 0 \leq a_i \leq p-1, \\ m &= b_0 + b_1 p + \cdots + b_s p^s,\ 0 \leq b_i \leq p-1, \\ n - m &= c_0 + c_1 p + \cdots + c_s p^s,\ 0 \leq c_i \leq p-1, \end{aligned}$$

então a valorização p-ádica de $\left(\begin{array}{c} n \\ m \end{array} \right)$ *é dada por*

$$v_p\left(\left(\begin{array}{c} n \\ m \end{array} \right) \right) = \frac{\sum_{i=0}^{s} b_i + \sum_{i=0}^{s} c_i - \sum_{i=0}^{s} a_i}{p-1},$$

Demonstração. Aplicação da Proposição 1.9.2. ■

Proposição 1.9.3. *(*Flores, 1996, p.74, Lema 3.4.10*) Sejam p um número primo, r um número inteiro positivo e $m = p^{r-2}$. Então*

$$v_p\left(\left(\begin{array}{c} m \\ i \end{array} \right) \right) \geq 1, \ \textit{onde} \left(\begin{array}{c} m \\ i \end{array} \right) = \frac{m!}{i!\,(m-i)!},$$

para $i = 1, \cdots, m-1$.

Demonstração. Sejam $b_1, \cdots, b_m, c_1, \cdots, c_m$, números naturais satisfazendo $0 \leq b_i \leq p-1$, $0 \leq c_i \leq p-1$ e tais que $i = b_0 + b_1 p + \cdots + a_m p^m$ e $(m-i) = c_0 + c_1 p + \cdots + c_m p^m$.

Pela Proposição 1.9.2, temos que

$$v_p(m!) = \frac{p^{r-2}-1}{p-1}, \quad v_p(i!) = \frac{i - \sum_{i=1}^{m} b_i}{p-1}, \quad v_p((m-i)!) = \frac{m-i-\sum_{i=1}^{m} c_i}{p-1},$$

de onde segue que

$$v_p\left(\left(\begin{array}{c} m \\ i \end{array}\right)\right) = \frac{-1 + \sum_{i=1}^{m} b_i + \sum_{i=1}^{m} c_i}{p-1}.$$

Como $\sum_{i=1}^{m} b_i + \sum_{i=1}^{m} c_i \geq 2$, o resultado segue. ∎