REPRESENTAÇÃO GEOMÉTRICA DE IDEAIS DE CORPOS DE NÚMEROS

Este exemplar corresponde a redação final da tese devidamente corrigida e defendida pelo Sr. André Luiz Flores, e aprovada pela comissão julgadora.

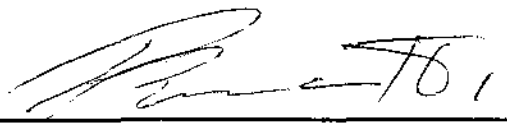
Campinas, 20 de março de 1.996

Prof. Dr. Antônio José Engler
orientador

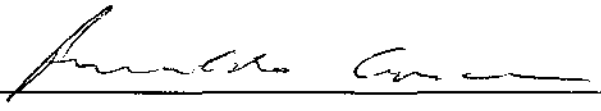
Prof. Dr. Trajano P. da Nóbrega Neto
co-orientador

Dissertação apresentada no Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para a obtenção do Título de MESTRE em Matemática.

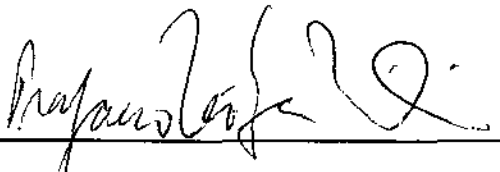
Tese de Mestrado defendida e aprovada em 15 de fevereiro de 1996 pela Banca Examinadora composta pelos Profs. Drs.



Prof (a). Dr (a). PAULO ROBERTO BRUMATTI



Prof (a). Dr (a). ARNALDO LEITE PINTO GARCIA



Prof (a). Dr (a). TRAJANO PIRES DA NOBREGA NETO

Á minha esposa Maria

Agradecimentos

Ao Prof. Dr. Trajano Nóbrega Neto, pela orientação, paciência e amizade, e como não poderia deixar de ser, pelo valioso incentivo que me foi dado desde o início da graduação;

Ao Prof. Dr. Antônio José Engler, pela simpatia, atenção e disposição para tratar dos mais diversos assuntos;

Ao CNPq, pelo apoio financeiro;

À minha esposa Maria, pela compreensão e carinho desprendidos durante todo este período;

Aos meus pais, pelo fervoroso incentivo.

Sumário

Resumo

O capítulo 1 trata de resultados gerais de Teoria dos Números. São expostos, nesta ordem, os seguintes assuntos: elementos integrais sobre um anel, elementos algébricos sobre um corpo, normas e traços, discriminante, corpos ciclotômicos e fatoração de ideais em um domínio de Dedekind.

No segundo Capítulo são estudados tópicos mais específicos, tais como norma de um ideal, anéis de fração, decomposição de um ideal primo em uma extensão e teoria de Galois aplicada a corpos de números.

O Capítulo 3 é direcionado para as aplicações. Inicia-se com o estudo de reticulados e densidade de empacotamento, e depois é exposto o homomorfismo canônico de um corpo de números. Finalmente, o estudo é particularizado para corpos ciclotômicos, e uma das aplicações é a obtenção de um reticulado em dimensão 6, que é o mais denso conhecido nesta dimensão.

Finalmente, o apêndice traz um resultado do Prof. Trajano Nóbrega, usado fortemente no corpo do trabalho.

Introdução

O desafio de se determinar o empacotamento esférico de R^n com a maior densidade é antigo e tem despertado interesse por parte dos estudiosos de vários ramos da ciência. Este problema ganhou notoriedade ao ser citado em 1900, por Hilbert, como sendo o 18^0_- de uma seleta lista de temas que viriam a ocupar destaque no desenvolvimento da ciencia moderna.

Muito se fez em torno deste assunto, e as teorias até então conhecidas que tinham alguma relação com o problema ganharam mais importância.

Um impulso marcante foi dado pelo artigo de Shannon, publicado em 1948, onde foi demonstrada a estreita relação entre bons códigos e reticulados densos. Com isto, o 18^0_- problema de Hilbert ganhou posição privilegiada na Teoria das comunicações.

Muitos modelos matemáticos foram desenvolvidos no intuito de colaborar com a solução do desafio, cada um com suas particularidades e nenhum forte candidato a resolver o problema. Entretanto, dentre estas receitas, surge uma com algumas vantagens sobre as demais. Esta receita foi originalmente proposta por Minkowiski, no início deste século, quando este estudava a Teoria dos Corpos de Classes.

O método, que motivou a redação deste texto, consiste na representação geométrica de ideais de corpos de números. No início, o interesse pelo assunto se restringia aos estudiosos de Teoria dos Números, cuja ênfase se caracterizava, até recentemente, na busca da solução do Último Teorema de Fermat.

Com a evolução dos fatos, o método de Minkowiski despertou interesse de um número maior de algebristas, e os resultados surgiram naturalmente. Um trabalho que marca a evolução do método é uma colaboração de dois matemáticos russos, Shafarevich e Golod, publicado em 1965. Nele é descrita

a melhor família de reticulados, no sentido assintótico. Contra esta família de reticulados pesa a dificuldade de se manipular tais estruturas.

Em 1978 surgem dois trabalhos do mesmo autor, Maurice Craig, onde ele mostra que o método de Minkowiski também contribui para a construção de reticulados densos em dimensão baixa. Nos seus artigos são construidos corpos de números e nestes escolhidos ideais ordinários convenientes cuja densidade de empacotamento é a melhor conhecida em suas respectivas dimensões, no caso em questão as dimensões são 6 e 24. Neste trabalho trataremos do caso de dimensão 6 de forma diferente daquela usada por Craig.

Alguns resultados aqui citados, principalmente no Capítulo 3, dependem fortemente de alguns resultados obtidos pelo Prof. Trajano Nóbrega. Alguns destes resultados foram publicados e outros encontram-se em fase de preparação. Reservamos o Apêndice B para listar estes resultados, cujas demonstrações fugiam do espírito deste trabalho.

Esta dissertação está dividida entre três Capítulos e 1 Apêndice.

O primeiro Capítulo abrange aspectos gerais de Teoria de Números, tais como norma e traço de um elemento, discriminante, corpos ciclotômicos e fatoração de um ideal primo em um domínio de Dedekind. Pela sua própria natureza, os resultados deste capítulo são enunciados para situações bastante gerais.

No Capítulo seguinte, os resultados apresentam caráter mais específico. O objetivo é fixar conceitos e resultados necessários para o desenvolvimento do Capítulo final. Os temas centrais são norma de um ideal e decomposição de um ideal primo em extensões galoisianas.

O terceiro e último Capítulo é voltado para as aplicações. É apresentado o método de Minkowiski, para obtenção de reticulados via representação geométrica de ideais em anéis de inteiros algébricos. Traz ainda um novo método para o cálculo da densidade de reticulados gerados através de ideais de em anéis de inteiros de $Q(\zeta_{p^n})$, p primo.

O apêndice apresenta resultados de ([*Nob*]), sobre os quais se baseiam grande parte do Capítulo 3. A escolha por esta classificação visa apenas a uniformidade técnica do texto.

Os resultados e notações foram em grande parte baseados nas referências [*Sam*] e [*Mar*], sobretudo os Capítulos 1 e 2. No início de cada resultado é indicada a fonte do mesmo. Embora não sejam traduções fiéis dos originais,

os resultados são equivalentes ou consequências dos mesmos. Para finalizar, cabe observar que o leitor mais experiente pode omitir a leitura dos Capítulos 1 e 2.

Índice de símbolos

N: conjunto dos números naturais
Z: conjunto dos números inteiros
R: conjunto dos números reais
C: conjunto dos números complexos
$card(X)$: cardinalidade do conjunto X
$X \times Y$: produto cartesiano de X por Y
(m, n): maior divisor comum de m e n
A^*: $A - \{0\}$
$\varphi(m)$: número de elementos de $(Z/mZ)^*$
$A[X]$: anel dos polinômios sobre A
AB (A, B anéis): Adjunção do anel B ao anel A.
$\subset, \supset$: está contido, contém
$\prod$: produto
$\sum$: soma
$R(z)$: parte real do número complexo z
$I(z)$: parte imaginária do número complexo z
$\forall$: para todo
$\exists$: existe
ζ_n: $e^{2\pi i/n}$
$m(X)$: medida de Lebesgue do conjunto X
$min(X)$: mínimo do conjunto X
δ_{ij}: δ de Kronecker
$a \mid b$: a divide b
$(G : H)$ (grupos): índice de H em G.

$[L : K]$ (corpos): grau de L sobre K
$Gal(L, K)$: grupo de Galois de L sobre K
$Ker(f)$: núcleo do homomorfismo f
$M_n(A)$: conjunto das $n \times n$ matrizes com entradas em A
M^t: transposta da matriz M
$det(M)$: determinante da matriz M
$\mid a \mid$: $(a_1^2 + \cdots + a_n^2)^{1/2}, a = (a_1, ..., a_n) \in R^n$
$\emptyset$: conjunto vazio
∂f: grau do polinômio f
a^{-1}: inverso multiplicativo do elemento a
$\overline{x}$: conjugado complexo da elemento x.
$f^{-1}(X)$: imagem inversa de X pela função f
$car(R)$: característica do anel R
$Tr_{L|K}$: traço com relação a L e K
$N_{L|K}$: norma com relação a L e K
D_K : discriminante absoluto do corpo K

Capítulo 1

Resultados gerais

Este capítulo é dedicado à obtenção de resultados básicos , sendo enunciados para situações bastante gerais. Dentre os assuntos tratados, podemos citar elementos integrais sobre um anel, elementos algébricos sobre um corpo, normas e traços de elementos e discriminante. Também é feito um estudo de propriedades elementares de corpos ciclotômicos, e para concluir o capítulo, mostramos a unicidade da fatoração de ideais em domínios de Dedekind.

1.1 Elementos integrais sobre um anel

Sejam $A \subset R$ anéis. Um elemento $x \in R$ é dito integral sobre A se este é raíz de um polinômio mônico com coeficientes em A.

Pode ser visto em ($[Sam]$, pg. 27, Teor.1), que se $A \subset B$ são anéis e $x \in A$ então são equivalentes:

(i) x é integral sobre A;
(ii) O anel $A[X]$ é um A-módulo finitamente gerado;
(iii) Existe um subanel B de R que contém A e x, e que é um submódulo finitamente gerado.

Façamos a prova:

(i)⇒(ii): Seja $f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} \in A[X]$ tal que $f(X) = 0$. Mostremos que $1, x, ..., x^{n-1}$ gera $A[X]$ sobre A. De fato, seja $y = g(x) \in A[x]$,

onde $g(X) \in A[X]$. Pelo algoritmo da divisão, existem $q(X)$ e $r(X) \in A[X]$ tais que $g(X) = q(X).f(X) + r(X)$, onde $r = 0$ ou $\partial r < \partial f$. Podemos supor $y \neq 0$, e daí

$$y = g(X) = r(X) = a_0 + a_1X + \cdots + a_{r-1}X^{r-1},$$

com $a_i \in A$; logo, $1, x, ..., x^{r-1}$ gera $A[X]$ sobre A.

(ii)⇒(iii): Imediato.

(iii)⇒(i): Seja $(y_1, ..., y_n)$ um conjunto finito de geradores para o A-módulo B. Sendo B subanel de R, tem-se $xy_i \in B$, para $i = 1, ..., n$. Portanto,

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

Segue que

$$\sum_{j=1}^{n}(\delta_{ij}x - a_{ij})y_j = 0\ \ , i = 1, ..., n,$$

onde $\delta_{ij} = 1$, se $i = j$ e 0, caso contrário.

Consideremos o sistema linear homogêneo definido pelas n equações nas variáveis $y_1, ..., y_n$. Seja $d = det(\delta_{ij}x - a_{ij})$. Pela regra de Crammer chegamos a $dy_i = 0$, para todo i. Isto significa que $db = 0$, para todo $b \in B$, em particular $d.1 = 0$, de onde $d = 0$. Para concluir basta observar que d é um polinômio mônico e não nulo em x, já que o termo de maior grau aparece na diagonal $\prod_{i=1}^{n}(x - a_{ii})$. □

Exemplo 1.1.1 *O elemento $x = \sqrt{2}$ é integral sobre $\mathbb{Z}$, pois x é raíz de $X^2 - 2$.*

Sejam R um anel, A um subanel de R e $x_1, ..., x_n$ elementos de R tais que x_i é integral sobre $A[x_1, ..., x_{i-1}]$. Então $A[x_1, ..., x_n]$ é um A-módulo finitamente gerado. A prova é feita usando indução sobre n. Para $n = 1$ é evidentemente verdadeiro. Suponhamos que seja verdadeiro para $n - 1$ elementos. Então $A[x_1, ..., x_n] = B[x_n]$, onde $B = A[x_1, ..., x_{n-1}]$ é por hipótese um A-módulo finitamente gerado. Sejam $c_1, ..., c_k$ um sistema de geradores de B sobre A. A família (c_ib_j) é um sistema de geradores de $B[x_n]$ sobre A. De fato, seja $y = \sum_1^k a_ic_i$ um elemento de $B[x_n]$, onde $a_i \in B$. Para cada índice i, seja $a_i = \sum_{j=1}^{t} r_{ij}b_j$, onde $r_{ij} \in A$. Então

$$y = \sum_{i=1}^{k}(\sum_{j=1}^{t} r_{ij}b_j).c_i = \sum_{i,j} r_{ij}.(c_i b_j),$$

e portanto vale o resultado afirmado acima.

Como consequência deste resultado podemos deduzir que se $A \subset R$ são anéis, então o conjunto A' dos elementos de R integrais sobre A é um subanel de R que contém A. De fato, sejam x e y dois elementos quaisquer de R integrais sobre A. Então $A[x, y]$ é um A-módulo finitamente gerado que contém A, $x + y$, $-x$ e xy. Além disso A' contém A, já que todo elemento $a \in A$ é raíz do polinômio mônico $X - a \in A[X]$.

O anel A', com a notação acima, será chamado de fecho integral de A em R. Quando A for um domínio, chamaremos de fecho integral de A ao fecho integral de A em seu corpo de frações. Se o fecho integral de um domínio A é o próprio A, então este é dito integralmente fechado. De modo geral, se R é um anel e A é um subanel de R, diz-se que R é integral sobre A se todo elemento de R é integral sobre A.

Proposição 1.1.2 *([Sam], pg.29, Prop.2) Sejam R um anel, B um subanel de R e A um subanel de B. Se R é integral sobre B e se B é integral sobre A, então R é integral sobre A.*

Demonstração: Sejam $x \in R$ e $b_0, ..., b_{n-1} \in B$ tais que $b_0 + \cdots + b_{n-1}X^{n-1} = 0$. Tal relação implica que x é integral sobre $A[b_0, ..., b_{n-1}]$. Como por hipótese cada b_i é integral sobre A, então os elementos $b_0, ..., b_{n-1}, b_n = x$ satisfazem: b_i é integral sobre $A[b_0, ..., b_{i-1}]$. A conclusão segue imediatamente dos resultados já apresentados.

Proposição 1.1.3 *([Sam], pg.29, Prop.3) Sejam R um domínio e A subanel de R tal que R é integral sobre A. Então R é um corpo se, e somente se A é um corpo.*

Demonstração: $\Rightarrow$) Seja $x \in A$ um elemento não nulo. O elemento $x^{-1} \in R$ satisfaz a equação

$$a_0 + a_1x^{-1} + \cdots + a_{n-1}(x^{-1})^{n-1} + (x^{-1})^n = 0,$$

onde $a_i \in A$. Multiplicando tal equação por $x^{n-1} \in A$, obtem-se

$$a_0 x^{n-1} + \cdots + a_{n-2} x + a_{n-1} = x^{-1},$$

e assim $x^{-1} \in A$.

$\Leftarrow$) Fixado um elemento não nulo, consideremos o espaço vetorial $A[x]$ sobre A. Neste espaço, a aplicação linear $a \mapsto ax$ é injetiva, já que R é domínio. Logo é sobrejetiva, e portanto existe $x \in R$ tal que $xy = 1$, ou seja, x é inversível em R. □

Todo anel fatorial é integralmente fechado. Para ver isto, sejam A um anel fatorial e $x = a/b$ um elemento do corpo de frações de A integral sobre A. Consideremos a equação

$$a_0 + a_1 x + ... + a_{n-1} x^{n-1} + x^n = 0,\ a_i \in A.$$

Multiplicando esta equação por b^n obtemos

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

Isto implica $b \mid a^n$, e aplicando o Lema de Euclides sucessivas vezes concluimos que $b \mid a$, isto é, b é um elemento inversível do anel A, e assim $x = a/b \in A$. □

1.2 Elementos algébricos sobre um corpo

Sejam R um anel e K um subcorpo de R. Um elemento $x \in R$ é dito algébrico sobre K se este é raíz de um polinômio mônico com coeficientes em K. Um elemento $x \in R$ que não é algébrico sobre K é dito transcendente sobre K. Se todo elemento de R for algébrico sobre K, dizemos que R é algébrico sobre K. No caso em que R é um corpo e R é algébrico sobre K, diz-se que R é uma extensão algébrica de K.

Sejam x um elemento algébrico sobre K e $f(X) \in K[X]$ tal que $f(X) = 0$. Se multiplicarmos o coeficiente dominante de $f(X)$ pelo seu inverso, então x será raíz de um polinômio mônico em $K[X]$; logo, sobre um corpo não há distinção entre elemento algébrico e integral, e assim a teoria desenvolvida anteriormente é aplicável a elementos algébricos sobre um corpo.

Uma caracterização dos elementos algébricos sobre um corpo K é:

$$x \text{ é algébrico sobre } K \iff [K[x] : K] \text{ é finito.}$$

Dado um elemento $x \in R$, consideremos o (único) homomorfismo de anéis $\sigma_x : K[X] \mapsto R$ definido por $\sigma_x(a) = a, \forall a \in K$, e $\sigma_x(X) = x$. A definição de elemento algébrico sobre K pode ser reformulada em termos do homomorfismo σ_x da seguinte forma:

$$x \text{ é algébrico sobre } K \iff Ker(\sigma_x) \neq (0).$$

Consequentemente, x é transcendente sobre K se, e somente se $Ker(\sigma_x) = (0)$. A imagem de σ_x é o subanel $K[x]$ de R. Se x for transcendente sobre K, então $K[x] \simeq K[X]$; se for algébrico, então

$$K[x] \simeq K[X]/Ker(\sigma_x).$$

Sendo $K[X]$ um domínio principal, o ideal $Ker(\sigma_x)$ é gerado por um polinômio $f(X) \in K[X]$, não constante no caso em que x é algébrico sobre K. Podemos supor $f(X)$ mônico, já que K é um corpo. Dessa forma, $f(X)$ é único, e será chamado o polinômio minimal de x sobre K.

É interessante sabermos quando $K[x]$ é um corpo. Para tal, temos a seguinte

Proposição 1.2.1 *([Sam], pg.32) Sejam R um anel, K um subcorpo de R, $x \in R$ algébrico sobre K e $f(X) \in K[X]$ o polinômio minimal de x sobre K. São equivalentes:*

(i)$K[x]$ é um corpo;
(ii) $K[x]$ é um domínio;
(iii) $f(X)$ é irredutível em $K[X]$.

Demonstração: A implicação (i)⇒(ii) é imediata. Suponhamos $K[x] \simeq K[X]/(f(X))$ um domínio. Então $(f(X))$ é ideal primo do anel $K[X]$; consequentemente f é irredutível em $K[X]$, e (ii) implica (iii). Para a implicação (iii)⇒(i), notemos que $f(X)$ irredutível implica que $(f(X))$ é um ideal primo do anel fatorial $K[X]$, logo um ideal maximal, e portanto $K[X]/(f(X)) \simeq K[x]$ é um corpo. □

Sejam K um corpo, L uma extensão algébrica de K , F uma extensão algébrica de L com K-bases $(x_i)_{i\in I}$ e $(y_j)_{j\in J}$, respectivamente. Mostraremos que o conjunto (x_iy_j), $i \in I$, $j \in J$ é base de F sobre K. De fato, seja

$$c = \sum_{i\in I} a_i x_i \ (a_i \in L),$$

um elemento qualquer de F. Para cada $i \in I$, existem $a_{ij} \in K$ tais que

$$a_i = \sum_{j\in J} a_{ij} y_j.$$

Assim, $c = \sum_{i,j} a_{ij}.(x_iy_j)$ é combinação linear, sobre K, dos elementos x_iy_j. Falta mostrar que o conjunto (x_iy_j) é linearmente independente sobre K. Sejam a_{ij}, $i \in I$, $j \in J$ elementos de K tais que

$$\sum_{i,j} x_iy_j = \sum_{j\in J}(\sum_{i\in I} a_{ij}.x_i)y_j = 0.$$

Da independência de (y_i) sobre L vem $\sum_{i\in I} a_{ij}x_i = 0$, e repetindo o argumento para a família $(x_i)_{i\in I}$ vem $a_{ij} = 0$. Isto mostra que (x_iy_j) é base de F sobre K, e que vale $[F : K] = [F : L].[L : K]$.

Sejam K um corpo e L, L' extensões de K. Dá-se o nome de K-monomorfismo de L em L' a todo monomorfismo $\sigma : L \mapsto L'$ satisfazendo $\sigma(x) = x$, para todo $x \in K$. Analogamente, define-se K-automorfismo de L. Se existir um K-isomorfismo $\sigma : L \mapsto L'$, diremos que L e L' são K-isomorfos (ou conjugados, no caso de L e L' serem extensões algébricas de K).

Definição 1.2.2 *Sejam K um corpo e $f(X) \in K[X]$ um polinômio não constante. Suponhamos que exista um corpo L satisfazendo as seguintes propriedades:*

(i) $K \subseteq L$;
(ii) $f(X)$ *se decompõe linearmente em* $L[X]$;
(iii) Se L' *é um corpo que satisfaz (i) e (ii), então* $L \subseteq L'$.

Nestas condições L *é dito ser um corpo de raízes de* f *sobre* K.

Em outras palavras, um corpo de raízes de um polinômio $f(X) \in K[X]$ é um corpo contendo K onde $f(X)$ tem todas suas raízes, e é o "menor" corpo com esta propriedade. L não é necessariamente único, mas veremos mais adiante que dois corpos de raízes são K-isomorfos.

Teorema 1.2.3 *([Mon], pg.37, Teor.4.3) Sejam* K *um corpo e* $f(X) \in K[X]$ *um polinômio irredutível e mônico. Então existe uma extensão simples* $K(x)$ *de* K, *onde* x *é uma raíz de* f.

Demonstração: Podemos considerar K como sendo subcorpo do corpo $K' = K[X]/(f(X))$ através do monomorfismo $a \mapsto \bar{a}$. Seja $\sigma : K[X] \mapsto K[X]/(f(X))$ o homomorfismo canônico. Então $\sigma(f(X)) = f(\sigma(X))$. Se colocarmos $x = \sigma(X) \in K'$, então $f(x) = f(\sigma(X)) = \sigma(f(X)) = 0$; isto prova o resultado desejado. □

Corolário 1.2.4 *([Mon], pg.39, Teor.4.6) Para todo polinômio não constante* $g(X) \in K[X]$, *existe um corpo de raízes de* g *sobre* K.

Demonstração: Faremos a prova usando indução sobre o grau ∂g de $g(X)$. Se $\partial g = 1$, K já é o corpo procurado. Suponhamos que seja verdadeiro para todo polinômio com grau menor do que n, e que $\partial g = n$. Sejam $f(X) \in K[X]$ um fator irredutível e unitário de $g(X)$, e x uma raíz de f na extensão simples $K[x]$. Segue que existe $h(X) \in K(x)[X]$ tal que

$$g(X) = (X - x).h(X).$$

Por hipótese existe um corpo de raízes F de h sobre $K[X]$, que é da forma

$$F = K(x)(x_1, ..., x_{n-1}) = K(x, x_1, ..., x_{n-1}),$$

onde x_i são as raízes de h (e portanto de g) em F; Isto mostra que F é o corpo desejado. □

Proposição 1.2.5 *(Mon], pg.38) Seja K um corpo, f(X) ∈ K[X] um polinômio irredutível e unitário em K[X] e x, x' duas raízes de f (em alguma extensão de K). Então existe um único K-isomorfismo θ:K(x)↦ K(x') tal que θ(x) = x'.*

Demonstração: Consideremos o homomorfismo $\theta : K(x) = K[x] \mapsto K(x')$, pondo para cada $y = g(x) \in K(x)$, $\theta(y) = g(x')$. A aplicação θ está bem definida, pois se $g(x) = h(x)$, então $(g - h)(x) = 0$, e portanto $f(X)$ divide $(g - h)(X)$ em $K[X]$; logo, $(g - h)(x') = 0$, e $\theta(g(x)) = \theta(h(X))$. O homomorfismo θ é um K-monomorfismo, pois $\theta(g(x)) = g(x') = 0$ implica que $f(X)$ divide $g(X)$, e assim $g(x) = 0$. Além disso, pela própria construção vale $\theta(x) = x'$. □

Se $g(X) \in K[X]$ é um polinômio não constante, é fato conhecido que dois corpos de raízes de g sobre K são K-isomorfos. Um corpo K é chamado algebricamente fechado se todo polinômio não constante em K[X] admite uma raíz em K. Isto equivale a dizer que todo polinômio não constante em $K[X]$ decompõe-se em fatores lineares de $K[X]$. Também sabe-se que todo corpo admite uma extensão algebricamente fechada (*[Lan], pg.169, Teor.1*).

Consideremos L e L' extensões de um corpo K. Dizemos que dois elementos x, x' pertencentes a L e L', respectivamente, são conjugados se existir um K-isomorfismo $\sigma : K(x) \mapsto K(x')$ tal que $\sigma(x) = x'$.

Lema 1.2.6 *([Sam], pg.33) Sejam K um corpo de característica zero ou um corpo finito e $f(X) \in K[X]$ um polinômio mônico irredutível. Então toda raíz de f em qualquer extensão é simples.*

Demonstração: Seja

$$f(X) = a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \ , \ a_i \in K.$$

Suponhamos que f admita uma raíz dupla x. Se $f'(X)$ é a derivada formal de $f(X)$, então $f'(x) = 0$, e sendo f irredutível vem

$$f'(X) = a_1 + 2a_2X + \cdots + nX^{n-1} \equiv 0.$$

Em particular, $n.1 = 0$, o que não é possível em característica zero. Suponhamos então que $car(K) = p > 0$, e que K seja finito. O homomorfismo $x \mapsto x^p$ de K em K é injetivo, pois $x^p = y^p$ implica $(x^p - y^p) = (x - y)^p = 0$, e portanto $x = y$. Sendo K finito, resulta que é um automorfismo. De $f' \equiv 0$ vem $f(X) \in K[X^p]$; isto somado à sobrejetividade do homomorfismo acima nos dá que $f(X) \in K^p[X^p]$ é da forma $(h(X))^p$, com $h(X) \in K[X]$. Mas este fato contradiz a irredutibilidade de $f(X)$, o que conclui a prova. □

Teorema 1.2.7 *([Sam], pg. 33, Teor.1) Seja K um corpo de característica zero ou um corpo finito, K' uma extensão de K de grau finito n e Ω um corpo algebricamente fechado contendo K. Então existem n K-isomorfismos distintos de K' em Ω.*

Demonstração: Se K' é da forma $K(x)$, então as n raízes distintas $x_1, ..., x_n$ do polinômio minimal de x sobre K induzem n K-monomorfismos distintos $\sigma_i : K' \mapsto \Omega$, definidos por $\sigma_i(x) = x_i$. Suponhamos agora que K' não seja uma extensão simples de K, e tomemos $x \in K'$ tal que $K \subset K(x) \subset K'$, com $[K(x) : K] = q > 1$. O resultado é provado usando-se indução sobre o grau da extensão. Pelo visto acima, existem q K-monomorfismos $\sigma_i : K[x] \mapsto \Omega$, cujas imagens denotaremos por K_i. Como $K(x)$ e K_i são isomorfos, é possível construir uma extensão K_i' de K_i e um isomorfismo $\sigma_i' : K \mapsto K_i'$ que extende σ_i. É claro que K_i é de característica zero ou um corpo finito. Aplicando a hipótese da indução à extensão $K_i' \mid K_i$, obtemos n/q K_i-monomorfismos $\theta_{ij} : K_i' \mapsto \Omega$. Construimos, assim $q.(n/q) = n$ monomorfismos $\theta_{ij} \circ \sigma_i : K' \mapsto \Omega$, que são dois a dois distintos, já que estes diferem em K ou em K_i. □

1.3 Normas e traços

Dados um anel R e uma matriz A em $M_n(R)$, definimos o traço de A (e indicaremos por $Tr(A)$) como sendo a soma dos elementos da diagonal principal de A.

Lema 1.3.1 *([Lan], pg. 323) Se A e B são duas matrizes de $M_n(R)$, onde R é um anel qualquer, então $Tr(AB)=Tr(BA)$.*

Demonstração: Sejam $A = (a_{ij})$ e $B = (b_{ij})$; Escrevendo $AB = (\gamma_{ij})$ e $BA = (\mu_{ij})$, onde

$$\gamma_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}, \text{ e } \mu_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj},$$

temos

$$Tr(AB) = \sum_{i=1}^{n} \gamma_{ii} = \sum_{i=1}^{n} (\sum_{k=1}^{n} a_{ik}b_{ki}) = \sum_{k=1}^{n} (\sum_{i=1}^{n} b_{ki}a_{ik}) = \sum_{k=1}^{n} \mu_{kk} = Tr(BA).$$

O Lema está provado. □

Aplicando o Lema anterior à matriz $B = CA^{-1}$, obtemos

$$Tr(ACA^{-1}) = Tr(C).$$

Sejam R um anel, E um R-módulo livre de posto finito e u um endomorfismo de E. Se (e_i) é uma R-base para E e se A é a matriz que representa u com respeito a essa base, define-se o traço de u (e indicaremos por $Tr(u)$) como sendo o traço da matriz A.

Com as notações anteriores, se u e v são endomorfismos de E e se $\lambda \in R$, então valem as propriedades

$$Tr(\lambda u) = \lambda Tr(u)$$
e
$$Tr(u + v) = Tr(u) + Tr(v).$$

Se A é uma matriz inversível, sabemos que $det(ACA^{-1}) = det(C)$. Isto nos sugere a definição de uma nova função definida no conjunto dos endomorfismos de E, a saber a função norma. Definimos o determinante de u (e indicaremos por $det(u)$) como sendo o determinante de A.

Ainda usando a mesma notação, definimos o polinômio característico de u (e indicaremos por $F_u(X)$) como sendo

$$F_u(X) = det(X.Id - A).$$

Proposição 1.3.2 *([Sam], pg. 36) Para um dado endomorfismo u, vale a identidade*

$$F_u(X) = X^n - Tr(u)X^{n-1} + \cdots + (-1)^n det(u).$$

Sejam B um anel e A um subanel de B tal que B é um A-módulo livre de posto finito n. Para cada $x \in B$, definimos o endomorfismo m_x de B por $m_x(y) = xy$. Assim, fica natural definirmos traço, norma e polinômio característico de x (relativamente à B e A) como sendo o traço, deteterminante e polinômio característico do endomorfismo m_x, respectivamente.

Denotaremos o traço de x relativamente a B e A (resp. norma) por $Tr_{B|A}(x)$ (resp. $N_{B|A}(x)$), ou simplesmente por $Tr(x)$ e $N(x)$, quando não há possibilidade de confusão. São elementos de A.

Exemplo 1.3.3 *Sejam* $B = \mathbb{Z}[\sqrt{2}]$, $A = \mathbb{Z}$, $\beta = (1, \sqrt{2})$ *uma* $\mathbb{Z}$*-base para* B *e* $x = a + b\sqrt{2}$ *e* $y = a_1 + b_1\sqrt{d}$ *elementos de* B. *As coordenadas de* xy *com relação a* β *são*

$$((aa_1 + 2bb_1), (ab_1 + ba_1)) = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \begin{pmatrix} a_1 \\ b_1 \end{pmatrix}.$$

Logo a matriz de m_x *é*

$$A = \begin{pmatrix} a & 2b \\ b & a \end{pmatrix},$$

de onde vem $Tr(x) = 2a$ *e* $N(x) = a^2 - 2b^2$.

Sejam $x, y \in B$ e $a \in A$. Valem as seguintes propriedades:

$$\begin{gathered} Tr(x+y) = Tr(x) + Tr(y); \\ Tr(ax) = aTr(x); \\ Tr(a) = na; \\ N(xy) = N(x).N(y)\ ; \\ N(a) = a^n. \end{gathered}$$

Veremos a seguir um resultado sobre normas e traços de elementos no caso particular de extensões finitas de corpos.

Lema 1.3.4 *([Sam], pg.29, Prop.1) Sejam K um corpo de característica zero ou um corpo finito, L uma extensão finita de K de grau n, $x \in L$ tal que $L = K(x)$ e $x_1, ..., x_n$ as raízes do polinômio minimal de x sobre K. Então*

$$\begin{gathered} Tr_{L|K}(x) = x_1 + \cdots + x_n \\ e \\ N_{L|K}(x) = x_1 ... x_n. \end{gathered}$$

Demonstração: Seja $f(X) = a_0 + a_1 X + ... + a_{n-1}X^{n-1} + X^n$ o polinômio minimal de x sobre K. Os elementos $1, x, ..., x^{n-1}$ formam uma base de L sobre K, e a matriz M do endomorfismo m_x com relação a esta base é

$$M = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \ddots & & & \vdots \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix},$$

como se verifica facilmente. O polinômio característico $F_x(X)$ é dado por

$$F_x(X) = det(X.Id - M) = det \begin{pmatrix} X & 0 & \cdots & 0 & a_0 \\ -1 & X & \cdots & 0 & a_1 \\ 0 & -1 & \cdots & 0 & a_1 \\ \vdots & \ddots & & & \vdots \\ 0 & \cdots & 0 & -1 & X + a_{n-1} \end{pmatrix}.$$

Vale

$$F_x(X) = f(X) = (X - x_1)(X - x_2)...(X - x_n) =$$

$$= X^n - (\sum_{i=1}^{n} x_i)X^{n-1} + \cdots + (-1)^n(\prod_{i=1}^{n} x_i);$$

assim,

$$Tr_{L|K}(x) = x_1 + ... + x_n \text{ e } N_{L|K}(x) = x_1...x_n \ ,$$

como queríamos. □

Teorema 1.3.5 *([Sam], pg. 36, Prop.1) Sejam K um corpo de característica zero ou um corpo finito, L uma extensão finita de K de grau n , $x \in L$ e $r = [L : K(x)]$. Então*

$$Tr_{L|K}(x) = r.Tr_{K(x)|K}(x)$$
$$e$$
$$N_{L|K}(x) = (N_{K(x)|K}(x))^r.$$

Demonstração: A representação xy_i com relação à base y_t será

$$M.(0 \cdots 1 \cdots 0)^t = (a_{i1} \cdots a_{is}).$$

Assim,

$$xy_i = \sum_{k=1}^{s} a_{ik}y_k.$$

Consideremos a base (y_iz_j) de L sobre K segundo a ordem

$$(y_1z_1, ..., y_sz_1, ..., y_1z_r, ..., y_sz_r),$$

e denotemos por $M' = (b_{ij})$ a matriz que representa a multiplicação por x em L com relação a esta base. Tem-se

$$x(y_iz_j) = (xy_i)z_j = (\sum_{k=1}^{s} a_{ik}y_k)z_j = \sum_{k=1}^{s} a_{ik}.(y_kz_j).$$

Por outro lado, a representação de xy_iz_j com relação à base M' será

$$M'.(0 \cdots 1 \cdots 0)^t = (b_{l1} \cdots b_{ln}),$$

onde $l = i.j$ e o número 1 aparece na l-ésima posição. Assim,

$$xy_iz_j = \sum_{p,q} b_{l,p.q}(y_py_q)$$

Comparando as igualdades obtidas, concluímos que M' é formada por r blocos diagonais, onde cada bloco é a matriz M. O resultado segue da representação

$$\begin{pmatrix} M & 0 & \cdots & 0 \\ 0 & M & \vdots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ 0 & \cdots & 0 & M \end{pmatrix},$$

aplicando-se a fórmula para o cálculo do discriminante de uma matriz formada por blocos diagonais. □

1.4 Discriminante

Veremos, no Capítulo 3, que o discriminante do corpo em questão tem relação com o cálculo da densidade de ideais. Iniciamos a seção com uma exposição bastante geral e finalizamos com uma fórmula que permite o cálculo explícito do discriminante, em um caso particular.

Definição 1.4.1 *Sejam $A \subset B$ anéis tais que B seja um A-módulo livre de posto finito n. Dá-se o nome de discriminante da n-upla $(x_1, ..., x_n) \in B^n$ ao elemento de A definido por*

$$D(x_1, \cdots, x_n) = det(Tr_{B|A}(x_ix_j)).$$

Lema 1.4.2 *([Sam], pg.38, Prop.1) Sejam* $(x_1, ..., x_n)$, $(y_1, ..., y_n) \in B^n$ *tais que* $y_i = \sum_{j=1}^{n} a_{ij}x_j$, *com* $a_{ij} \in A$. *Então*

$$D(y_1, ..., y_n) = (det(a_{ij}))^2.D(x_1, ..., x_n).$$

Demonstração: Tem-se

$$y_p y_q = \sum_{i,j} a_{pi}a_{qj}.(x_i y_j);$$

logo,

$$Tr(y_p y_q) = \sum_{i,j} a_{p,i}a_{q,j}.Tr(x_i x_j) = (a_{pi})_i.(Tr(x_i x_j))_{ij}.(a_{qj})^t_j,$$
$$\text{e}$$
$$Tr(y_p y_q) = (a_{pq}).(Tr(x_p x_q)).(a_{pq})^t.$$

Pondo $b_{ij} = a_{ji}$, temos:

$$Tr(y_p y_q) = (\sum_i a_{pi}.Tr(x_i x_q)).b_{pq} = \sum_i \sum_j a_{pi}.Tr(x_i x_j).b_{qj} = \sum_{i,j} a_{pi}a_{qj}.Tr(x_i x_j).$$

Tomando determinantes, obtemos

$$D(y_1, ..., y_n) = (det(a_{ij}))^2.D(x_1, ..., x_n). \square$$

O Lema acima nos diz que o discriminante de duas bases quaisquer de B sobre A são associados em A.

Dá-se o nome de discriminante de B sobre A (e será indicado por $\mathfrak{D}_{B|A}$) ao ideal principal de A gerado pelo discriminante de qualquer base de B sobre A.

O resultado a seguir caracteriza bases de B sobre A em termos do discriminante $\mathfrak{D}_{B|A}$, em um caso particular.

Proposição 1.4.3 *([Sam], pg.39, Prop.2) Sejam $B \subset A$ anéis tais que B seja um A-módulo livre de posto finito n. Suponhamos que A seja um domínio. Então um conjunto $(x_1, ..., x_n)$ é base de B sobre A se, e somente se $D(x_1, ..., x_n)$ gera $\mathfrak{D}_{B|A}$.*

Demonstração: A implicação ($\Rightarrow$) é imediata, valendo mesmo no caso em que A não é um domínio. Para provar a implicação contraria, tomemos uma base $(e_1, ..., e_n)$ de B sobre A e elementos $a_{ij} \in A$ tais que $x_i = \sum_{i=1}^{n} a_{ij} x_j$. Sejam $d = D(x_1, ..., x_n)$ e $d' = D(e_1, ..., e_n)$. Como $dA = d'A$, então existe $c \in A$ tal que $d' = cd$, e vale $d = (det(a_{ij}))^2.d'$. Segue que $d' = c.(det(a_{ij}))^2.d'$, resultando $c.(det(a_{ij}))^2 = 1$; isto mostra que $det(a_{ij})$ é inversível em A, e portanto $(x_1, \cdots, x_n)$ é também uma A-base para B. □

Lema 1.4.4 *([Sam], pg.39,) Sejam G um grupo e K um corpo. Então toda coleção finita de homomorfismos distintos de G em $K - \{0\}$ é linearmente independente sobre K.*

Demonstração: Façamos a prova usando indução sobre o número n de homomorfismos. Para $n = 1$ é trivialmente verdadeiro. Suponhamos $n \geq 2$, e que seja verdadeiro para $n - 1$ homomorfismos. Sejam $(a_1, ..., a_n)$ tais que

$$\sum_{i=1}^{n} a_i.\sigma_i(b) = 0,$$

para qualquer $b \in G$. Assim, para arbitrários b e c em G, vale

$$\sum_{i=1}^{n} a_i.\sigma_i(bc) = \sum_{i=1}^{n} a_i\sigma_i(b).\sigma_i(c) = 0.$$

Multiplicando a primeira equação por $\sigma_1(c)$ e subtraindo da anterior obtemos

$$\sum_{i=2}^{n} a_i(\sigma_i(c) - \sigma_1(c)).(\sigma_i(b)) = 0.$$

Pela hipótese da indução vale, $a_k(\sigma_k(c) - \sigma_1(c)) = 0$, e sendo os σ_i's dois a dois distintos resulta $a_k = 0$, para $k = 2, ..., n$, o que implica que também $a_1 = 0$. □

Proposição 1.4.5 *([Sam], pg.39, Prop.3) Seja K um corpo de característica zero ou um corpo finito, L uma extensão finita de K de grau n e $\sigma_1, ..., \sigma_n$ os n K-isomorfismos distintos de L num corpo algebricamente fechado Ω contendo K. Se $(x_1, ..., x_n)$ é uma K-base de para L, então*

$$D(x_1, ..., x_n) = det(\sigma_i(x_j))^2 \neq 0.$$

Demonstração: Pondo $a_{ij} = \sigma_j(x_i)$, temos

$$Tr(x_i x_j) = \sum_k \sigma_k(x_i x_j) = \sum_k \sigma_k(x_i)\sigma_k(x_j) = \sum_k a_{ik} a_{jk} = (a_{ij}).(a_{ij})^t.$$

Tomando determinantes, resulta

$$D(x_1, \cdots, x_n) = (det(\sigma_i(x_j))^2.$$

Se fosse $det(\sigma_i(x_j)) = 0$, então o sistema

$$\sum_{i=1}^n \sigma_i(x_j).X_i,\ j = 1, \cdots, n;$$

admitiria solução não trivial $(c_1, ..., c_n) \in K^n$, e para um elemento arbitrário $d = \sum_{i=1}^n a_i x_i$, por linearidade teríamos

$$\sum_{i=1}^n \sigma_i(d) = 0,$$

o que contraria o Lema 1.6.8. □

Lema 1.4.6 *([Sam], pg.40) Nas mesmas condições da Proposição 1.4.5, para toda base $(x_1, ..., x_n)$ de L sobre K, existe uma base $(y_1, ..., y_n)$ satisfazendo $Tr_{L|K}\ (x_i y_j) = \delta_{ij}$.*

Demonstração: Para cada $x \in L$, seja $s_x : L \mapsto K$ a aplicação definida por $s_x(y) = Tr_{L|K}(xy)$. Verifica-se facilmente que s_x é uma transformação K-linear de L. Consideremos agora a aplicação $\theta : L \mapsto Hom(L, K)$ (de K no seu espaço dual) dada por $\theta(x) = s_x$. Novamente, verifica-se que θ é uma aplicação K-linear de L em $Hom(L, K)$. A aplicação θ é injetiva, já que $Tr_{L|K}(xy) = 0$ para todo $y \in L$ implica $x = 0$. De fato, seja $(y_1, ..., y_n)$ uma K-base para L e $x \in L$ tal que $Tr_{L|K}(xy) = 0$, para todo y em L. Podemos supor $x \neq 0$, e daí

$$D(xy_1, ..., xy_n) = det(Tr_{L|K}\ (xy_i xy_j)) = det(0) = 0,$$

contra a Proposição 1.4.5. Logo θ é um isomorfismo, e assim existe uma base $(y_1, \cdots, y_n)$ tal que $Tr_{L|K}(x_i y_j) = \delta_{ij}$. □

Teorema 1.4.7 *([Sam], pg.40, Teor.1 e Corol.) Sejam A um domínio integralmente fechado de característica zero, K seu corpo de frações e L uma extensão finita de K de grau n. Então o fecho integral A' de A em L é um submódulo de um A-módulo livre de posto n. Se adicionarmos a hipótese de A ser principal, então A' será um A-módulo livre de posto finito n.*

Demonstração: Tomemos uma K-base $(x_1, ..., x_n)$ para L. Cada x_i é algébrico sobre K, e portanto satisfaz a uma equação

$$a_0 + a_1 x_i + \cdots + a_{n_i} x_i^n = 0,\ a_i \in K.$$

Desta igualdade verifica-se que $a_{n_i} x_i^n$ é integral sobre K. Colocando $x_i' = a_{n_i} x_i$, obtemos uma K-base (x_i') para L, contida em A'. Pelo Lema 1.4.6, existe uma outra K-base $(y_1, \cdots, y_n)$ tal que

$$Tr_{L|K}(x_i' . y_j) = \delta_{ij}.$$

Mostraremos que A' é submódulo do A-módulo livre $Ay_1 + \cdots + Ay_n$. Para tal, sejam $a \in A'$ e $c_1, \cdots, c_n$ elementos de K tais que $a = \sum_{i=1}^{n} c_i y_i$. Resta concluir que $c_i \in A$. De fato, para todo índice i vale $x_i' a \in A'$, de onde $Tr_{L|K}\ (x_i' a) \in A$. Mas

$Tr_{L|K}(x_i' a) = Tr_{L|K}\ (x_i'.\sum_{j=1}^{n}\ c_j y_j) = Tr_{L|K}\ (\sum_{j=1}^{n}\ c_j.(x_i' y_j)) = \sum_{j=1}^{n} c_j.$ $Tr_{L|K}(x_i' y_j) = \sum_{j=1}^{n}\ c_j \delta_{ij} = c_i$;

logo $c_i \in A$, como queríamos. □

Suponhamos agora A principal. Então A' é um A-módulo livre de posto finito $\leq n$. Como A' contém uma base de L sobre K, então A' terá posto n.

Apresentaremos agora uma fórmula para o cálculo do discriminante, para o caso particular $L = K(x)$, conforme o seguinte enunciado formal:

Proposição 1.4.8 *([Sam], pg.41) Sejam K um corpo de característica zero ou um corpo finito, L uma extensão finita simples de K (i.é, $L = K(x)$, $x \in L$) e $f(X)$ o polinômio minimal de x sobre K. Denotemos por $f'(X)$ a derivada formal do polinômio $f(X)$. Então*

$$D(1, x, ..., x^{n-1}) = (-1)^{n(n-1)/2}.N_{L|K}\ f'(x).$$

Demonstração: A fórmula de Vandermonde nos dá $det(x_i^j) = \prod_{i<j}(x_i - x_j)$. O resultado segue da sequência de igualdades seguinte, onde os σ_i representam os homomorfismos definidos no Teorema 1.2.7, $z_i = \sigma_i(x)$ as raízes de $f(X)$ e $c = (-1)^{n(n-1)/2}$:

$$D(1, x, ..., x^{n-1}) = det(\sigma_i(x^j))^2 = (det(x_i^j))^2 = c.\prod_{i \neq j}(x_i - x_j) =$$
$$c.\prod_i(\prod_{j \neq i}(x_i - x_j)) = c.\prod_i \sigma_i(f'(x)) = c.N_{L|K}\ (f'(x)).\ \square$$

1.5 Corpos ciclotômicos

Denotaremos $\zeta_n = e^{2\pi i/n}$ e chama-se corpo ciclotômico os corpos da forma $\mathbb{Q}(\zeta_n)$. Neste caso $K = \mathbb{Q}\ (\zeta_n)$ será chamado de n-ésimo corpo ciclotômico. Sobre a dimensão do $\mathbb{Q}$-espaço $\mathbb{Q}(\zeta_n)$, vale o seguinte resultado clássico:

Proposição 1.5.1 *([Mon], pg.112) O corpo $\mathbb{Q}(\zeta_n)$ é um espaço vetorial sobre $\mathbb{Q}$ de dimensão $\phi(n)$, e o conjunto dos ζ_n^j tais que $1 \leq j \leq n$ e $(j,n) = 1$ é uma base para este espaço vetorial.*

Por hora veremos alguns resultados no caso particular $\mathbb{Q}(\zeta_p)$, com p primo.

Fixado um número primo p, seja z uma raíz primitiva p-ésima da unidade. O número z é raíz do polinômio

$$\frac{X^p - 1}{X - 1} = X^{p-1} + \cdots + X + 1,$$

sendo chamado de p-ésimo polinômio ciclotômico. Vale o seguinte resultado:

Proposição 1.5.2 *([Sam], pg.42, Teor.2) Para todo número primo p, o polinômio ciclotômico $X^{p-1} + \cdots + X + 1$ é irredutível em $\mathbb{Q}[X]$.*

Demonstração: Pondo $X = Y + 1$, temos

$$X^{p-1}+\cdots+X+1 = \frac{X^p - 1}{X - 1} = \frac{(Y+1)^p - 1}{Y} = Y^{p-1}+\sum_{j=1}^{p-1} \binom{p}{j} Y^{j-1} = G(Y).$$

Aplicando o critério de irredutibilidade de Eisenstein ao polinômio $G(Y)$, conclui-se que este é irredutível, já que $\binom{p}{1} = 1$ e p^2 não divide nenhum dos coeficientes $\binom{p}{j}$. Disto segue que o p-ésimo polinômio ciclotômico também é irredutível. □

A irredutibilidade do p-ésimo polinômio ciclotômico implica imediatamente

$$Tr(z) = -1 \text{ e } Tr(1) = p - 1.$$

Logo $Tr(z^j) = -1$, para $j = 1, ..., p-1$, e como consequência

$$Tr(1 - z) = Tr(1 - z^2) = \cdots = Tr(1 - z^{p-1}) = p$$

Observe que os conjugados de $1-z$ são os elementos $1-z^j$, $j = 1, ..., p-1$. Da identidade

$$X^{p-1} + \cdots + X + 1 = \prod_{i=1}^{p-1}(X - \zeta_p^i),$$

para $X = 1$ obtem-se

$$p = \prod_{i=1}^{p-1}(1 - \zeta_p^i) = N(1 - \zeta_p).$$

Nesta seção denotaremos por A o anel de inteiros em $\mathbb{Q}(\zeta_{p^r})$.

Os resultados que seguem visam uma caracterização de A.

Lema 1.5.3 *([Sam], pg.43) Em $\mathbb{Q}(\zeta_p)$, valem*
(a): $A(1-z) \cap \mathbb{Z} = p\mathbb{Z}$.
(b): $Tr(y(1-z)) \in p\mathbb{Z}$, para todo $y \in A$.

Demonstração: (a): Sabemos que $p \in A(1-z)$, o que implica

$$A(1-z) \cap \mathbb{Z} \supset p\mathbb{Z} .$$

Suponhamos, por absurdo, que a igualdade em (a) seja falsa. Sendo $p\mathbb{Z}$ um ideal maximal de $\mathbb{Z}$, a relação $A(1-z) \cap \mathbb{Z} \neq p\mathbb{Z}$ implica

$$A(1-z) \cap \mathbb{Z} = \mathbb{Z} = p\mathbb{Z}.$$

ou seja, $1-z$ é uma unidade em A. Assim os conjugados $(1-z^j)$ de $1-z$ também são unidades; logo p é unidade em $A \cap \mathbb{Z}$, o que é evidentemente falso.

(b): Cada conjugado $y_j(1-z^j)$ de $y(1-z)$ é múltiplo de $1-z^j$ em A. Como

$$1 - z^j = (1-z)(1 + z + \cdots + z^{j-1}),$$

segue que $y_j(1-z^j)$ é também múltiplo de $1-z$. Sendo o traço a soma dos conjugados, temos

$$Tr(y(1-z)) \in A(1-z)$$

e de (a) vem

$$Tr(y(1-z)) \in A(1-z) \cap \mathbb{Z} = p\mathbb{Z}.$$

Teorema 1.5.4 *([Sam], pg.43, Teor.2) O anel A de inteiros do corpo* $\mathbb{Q}(\zeta_p)$ *é* $\mathbb{Z}[\zeta_p]$, *e* $(1, \zeta_p, ..., \zeta_p^{p-2})$ *é uma base para o* $\mathbb{Z}$*-módulo A.*

Demonstração: Seja $x = a_0 + a_1 z + \cdots + a_{p-2} z^{p-2}$ $(a_i \in \mathbb{Q}$) um elemento de A. Então

$$x(1-z) = a_0(1-z) + a_1(z-z^2) + \cdots + a_{p-2}(z^{p-2} - z^{p-1}).$$

Tomando traços e o Lema 1.5.3(a), obtemos

$$Tr(x(1-z)) = a_0 Tr(1-z) = a_o p.$$

Por (b) de 1.5.3, $pa_0 \in p\mathbb{Z}$, assim $a_0 \in \mathbb{Z}$. Como $z^{-1} \in A$, segue

$$(x - a_0)z^{-1} = a_1 + a_2 z + \cdots + a_{p-2} z^{p-3} \in A.$$

O mesmo argumento mostra que $a_1 \in \mathbb{Z}$. Aplicando o processo sucessivamente, concluimos que cada $a_i \in \mathbb{Z}$.

O resultado acima pode ser generalizado. Pode ser visto em [Was], pg. 11 , que o anel de inteiros de $K = \mathbb{Q}(\zeta_n)$ é $\mathbb{Z}[\zeta_n]$.

Para corpos ciclotômicos existe uma expressão para o cálculo do discriminante. Faremos a prova para um caso particular.

Proposição 1.5.5 *O discriminante de* $\mathbb{Q}(\zeta_{p^r})$ *vale*

$$\pm p^{\alpha}, \quad onde\ \alpha = p^{r-1}(pr - r - 1)\ .$$

Demonstração: O polinômio minimal de ζ_{p^r} sobre $\mathbb{Q}$ é

$$F(X) = (X^{p^r} - 1)/(X^{p^{r-1}} - 1),$$

e sabemos que $(1, \zeta_{p^r}, ..., \zeta_{p^r}^{\phi(p^r)-1})$ gera $K = \mathbb{Q}(\zeta_{p^r})$ como $\mathbb{Q}$-espaço vetorial. Pela Proposição 1.4.8, temos que

$$\mathfrak{D}_K = N_{K|\mathbb{Q}}(F'(\zeta_{p^r})) = N_{K|\mathbb{Q}}(p^r).N_{K|\mathbb{Q}}(\zeta_{p^r}^{p^r-1})/N_{K|\mathbb{Q}}(\zeta_{p^r}^{p^r-1} - 1).$$

Fazendo o cálculo parte por parte, tem-se

$$N_{K|\mathbb{Q}}(p^r) = p^{r(p-1)p^{r-1}}\ ;$$
$$N_{K|\mathbb{Q}}(\zeta_{p^r}^{p^{r-1}}) = (N_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(\zeta_p))^{p^{r-1}} = \pm 1\ ;$$
$$N_{K|\mathbb{Q}}(\zeta_{p^r}^{p^{r-1}} - 1) = (-N_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(1 - \zeta_p))^{p^{r-1}} = -p^{p^{r-1}}.$$

Substituindo na expressão acima, obtemos

$$\mathfrak{D}_K = \pm p^{p^{r-1}(p-1)r}.p^{-p^{r-1}} = \pm p^{p^{r-1}(pr-r-1)}\ ,$$

conforme o enunciado. □

Um resultado mais geral pode ser encontrado em [Was], pg. 12, Prop. 2.7: O discriminante do corpo $K = \mathbb{Q}(\zeta_n)$ vale

$$\mathfrak{D}_K = \pm \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}.$$

1.6 Fatoração de ideais em um domínio de Dedekind

Consideremos o anel de inteiros $A = \mathbb{Z}[\sqrt{-5}]$ em $\mathbb{Q}(\sqrt{-5})$. Observe que $(1+\sqrt{-5})(1-\sqrt{-5}) = 2.3$, e estes fatores têm normas $6, 6, 4$ e 9, respectivamente. Note que $1+\sqrt{-5}$ não tem divisor não trivial em A, já que a norma deste divisor é também um divisor não trivial de 6; isto é impossível, pois as equações $a^2+5b^2 = 2$ e $a^2+5b^2 = 3$ não têm solução em $\mathbb{Z}$. Tomando normas, conclui-se que o primo $1+\sqrt{-5}$ não divide 2.3, de forma que a fatoração de 6 em primos de $\mathbb{Z}[\sqrt{-5}]$ não é única.

Contudo, Kummer (1810-1893) observou que em certos anéis a fatoração de ideais em ideais primos é sempre única. Estes anéis são chamados de "anéis de Dedekind ". No que segue, faremos um estudo desses anéis objetivando demonstrar a unicidade da fatoração em ideais primos.

Um A-módulo M é dito Noetheriano se satisfaz as condições equivalentes seguintes:

(i) Toda coleção não vazia de submódulo de M contém um elemento maximal.
(ii) Toda cadeia crescente de submódulos de M é estacionária.
(iii) Todo submódulo de M é finitamente gerado.

Um anel A é dito Noetheriano sem, visto como A-módulo, for um módulo Noetheriano.

Proposição 1.6.1 *([Sam], pg. 46, Prop.1) Sejam A um anel, E um A-módulo e E' um submódulo de E. Então E é Noetheriano se, e somente se E' e E/E' são Noetherianos.*

Corolário 1.6.2 *([Sam], pg.47, Corol.1)Se $E_1, ..., E_n$ são A-módulo Noetheriano, então o A-módulo produto $E_1 \times \cdots \times E_n$ é Noetheriano.*

Se A é um anel Noetheriano e E um A-módulo de tipo finito, então E é um módulo Noetheriano.

Sabemos que todo ideal maximal $\mathfrak{m}$ de um anel A é um ideal primo não nulo. A recíproca nem sempre é verdadeira. Estudaremos mais adiante propriedades de anéis que satisfazem a esta condição.

Sejam $A \subset B$ anéis e $\mathfrak{p}$ um ideal primo de B. Consideremos a inclusão $i : A \mapsto B$, o homomorfismo canônico $h : B \mapsto B/\mathfrak{p}$ e a composição $f = h \circ i$. O núcleo de f é $A \cap \mathfrak{p}$, e portanto $A/A \cap \mathfrak{p} \simeq f(A) \subset B/\mathfrak{p}$; assim, $A/A \cap \mathfrak{p}$ é um domínio. Mostramos, assim, que $\mathfrak{p} \cap A$ é um ideal primo de A.

Dados dois ideais $\mathfrak{a}$ e $\mathfrak{b}$ de um anel A, define-se o produto de $\mathfrak{a}$ por $\mathfrak{b}$ (e indica-se por $\mathfrak{ab}$) como sendo o conjunto de todas as somas da forma $\sum_{i=1}^{n} a_i b_i$, com $a_i \in \mathfrak{a}$ e $b_i \in \mathfrak{b}$. O produto $\mathfrak{ab}$ é também um ideal de A, e vale a inclusão $\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b}$. Diremos também que $\mathfrak{a}$ divide $\mathfrak{b}$ se $\mathfrak{b} \subset \mathfrak{a}$. Indicaremos esta última relação por $\mathfrak{a} \mid \mathfrak{b}$.

Um domínio A é chamado de domínio de Dedekind se for integralmente fechado, Noetheriano e se todo ideal primo não nulo de A for maximal.

Teorema 1.6.3 *([Sam], pg.47, Prop.1) Sejam A um domínio de Dedekind de característica zero, K seu corpo de frações e L uma extensão finita de K. Então o fecho integral A' de A em L é um anel de Dedekind e um A-módulo de tipo finito.*

Demonstração: Sabemos que A' é um submódulo de um A-módulo Noetheriano. Usando ainda o mesmo resultado concluimos que o próprio A' é um A-módulo Noetheriano de tipo finito. Falta mostrar que todo ideal primo $\mathfrak{p}$ de A' é maximal. O ideal $\mathfrak{p} \cap A$ é um ideal primo de A; para mostrar que é também não nulo, seja $x \in \mathfrak{p} - (0)$ e $g(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ um polinômio de grau mínimo em $A[X]$ que anula x. A minimalidade do grau de g implica $a_0 \neq 0$. Logo,

$$a_0 \in xA' \cap A \subset \mathfrak{p} \cap A,$$

e assim $(0) \neq \mathfrak{p} \cap A$ é um ideal maximal de A. Os homomorfismos $A \mapsto A' \mapsto A'/\mathfrak{p}$ nos dão que $A/A \cap \mathfrak{p}$ pode ser considerado como um subanel de $A'/\mathfrak{p}$. O anel $A'/\mathfrak{p}$ é integral sobre $A/A \cap \mathfrak{p}$. De fato, seja $x' + \mathfrak{p} \in A'/\mathfrak{p}$ e $f(X) \in A[X]$ um polinômio que anula x'. Em $(A/A \cap \mathfrak{p})[X]$, seja

$$\bar{f}(X) = \bar{a}_0 + \cdots + \bar{a}_{n-1}X^{n-1} + X^n,$$

onde $\bar{a}_i = a_i + A \cap \mathfrak{p}$. Temos $\bar{f}(x' + \mathfrak{p}) = f(x') + \mathfrak{p} = 0 + \mathfrak{p} = 0$. Até o momento, sabemos que $A'/\mathfrak{p}$ é um domínio, é integral sobre $A/A \cap \mathfrak{p}$ e $A/A \cap \mathfrak{p}$ é um corpo. Portanto $A'/\mathfrak{p}$ é um corpo, e assim $\mathfrak{p}$ é maximal. □

Definição 1.6.4 *Seja A um domínio e K seu corpo de frações. Dizemos que um A-submódulo $\mathfrak{J}$ de K é um ideal fracionário de A se existir $d \in A$ não nulo tal que $d.\mathfrak{J} \subset A$. O elemento d será chamado um denominador comum para $\mathfrak{J}$.*

O produto $\mathfrak{J}\mathfrak{B}$ de dois ideais fracionários de A se define analogamente ao produto de ideais, e $\mathfrak{J}\mathfrak{B}$, $\mathfrak{J} \cap \mathfrak{B}$ e $\mathfrak{J} + \mathfrak{B}$ são ainda ideais fracionários de A. Definindo $\mathfrak{J}:\mathfrak{B} = \{x \in K; x\mathfrak{B} \subset \mathfrak{J}\}$, verifica-se que este é também um ideal fracionário de A.

Lema 1.6.5 *([Sam], pg.48, Lem.3) Seja A um domínio Noetheriano. Então todo ideal não nulo de A contém um produto de ideais primos não nulos.*

Demonstração: Seja Φ a coleção dos ideais não nulos de A que não contém um produto de ideais primos não nulos de A. Suponhamos por absurdo que $\Phi \neq \emptyset$, e seja $\mathfrak{m}$ um elemento maximal de Φ. Tal ideal $\mathfrak{m}$ não é primo, e $\mathfrak{m} \neq A$. Sendo assim, existem elementos $x, y \in A - \mathfrak{m}$ tais que $xy \in \mathfrak{m}$. Os ideais $\mathfrak{m} + xA$ e $\mathfrak{m} + yA$ contêm $\mathfrak{m}$ propriamente, e pela maximalidade de $\mathfrak{m}$ estes ideais não estão em Φ. Assim, existem ideais primos não nulos $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ tais que $\mathfrak{m} + Ax \supset \mathfrak{p}_1 \ldots \mathfrak{p}_r$ e $\mathfrak{m} + Ay \supset \mathfrak{q}_1 \ldots \mathfrak{q}_s$; daí $\mathfrak{m} = \mathfrak{m} + Axy = (\mathfrak{m} + Ax)(\mathfrak{m} + Ay) \supset \mathfrak{p}_1 \ldots \mathfrak{p}_r \mathfrak{q}_1 \ldots \mathfrak{q}_s$, como queríamos. □

Lema 1.6.6 *([Sam], pg. 49) Sejam A um anel Noetheriano e K seu corpo de frações. Então todo ideal fracionário de A é um A-módulo de tipo finito.*

Demonstração: Seja $\mathfrak{J}$ um ideal fracionário de A e $d \in A$ tal que $d\mathfrak{J} \subset A$. Então $\mathfrak{J} \subset d^{-1}A$, e sendo $d^{-1}A$ um A-módulo isomorfo à A, segue que $d^{-1}A$ é também Noetheriano ; logo $\mathfrak{J}$ é um A-módulo de tipo finito. □

Lema 1.6.7 *([Sam], pg.50 , Teor.2) Seja A um domínio de Dedekind. Para todo ideal primo não nulo $\mathfrak{p}$ de A, existe um ideal fracionário $\mathfrak{p}^{-1}$ de A tal que $\mathfrak{p}\mathfrak{p}^{-1} = A$.*

Demonstração: Consideremos em A o ideal fracionário

$$\mathfrak{p}^{-1} = \{x \in K; x\mathfrak{p} \subset A\}$$

Pela própria construção, vale $\mathfrak{p}\mathfrak{p}^{-1} \subset A$, e $A \subset \mathfrak{p}^{-1}$. Assim,

$$\mathfrak{p} = \mathfrak{p}A \subset \mathfrak{p}\mathfrak{p}^{-1} \subset A,$$

e pela maximalidade de $\mathfrak{p}$ vem

$$\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p} \text{ ou } \mathfrak{p}\mathfrak{p}^{-1} = A.$$

Suponhamos, por absurdo, que a primeira possibilidade seja verdadeira. Tomemos um elemento $x \in \mathfrak{p}^{-1}$, e consideremos o submódulo $A[x]$ de K. Este submódulo é um ideal fracionário de A, já que $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ implica $\mathfrak{p}x^n \subset \mathfrak{p}$, para todo n; como consequência, qualquer elemento de $\mathfrak{p}$ é um denominador comum para $A[x]$. Segue do Lema 1.6.6 que $A[x]$ é um A-módulo de tipo finito, e assim x é integral sobre A. Como A é integralmente fechado, então $x \in A$, e de $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ vem $\mathfrak{p}^{-1} = A$. Seja $a \in \mathfrak{p}$ um elemento não nulo. Consideremos ideais primos não nulos $\mathfrak{p}_1,...,\mathfrak{p}_n$ tais que $Aa \supset \mathfrak{p}_1...\mathfrak{p}_n$, onde supomos que n seja o maior possivel para o qual isto ocorra. De $\mathfrak{p} \supset Aa \supset \mathfrak{p}_1...\mathfrak{p}_n$, vem $\mathfrak{p} \supset \mathfrak{p}_i$, para algum índice i. Como $\mathfrak{p}$ foi tomado como máximo, então Aa não contém $\mathfrak{p}_2 ...\mathfrak{p}_n$. Seja $b \in \mathfrak{p}_2 ...\mathfrak{p}_n$ tal que b não pertença à Aa. De $\mathfrak{p}(\mathfrak{p}_2 ...\mathfrak{p}_n) \subset Aa$ vem $\mathfrak{p}\ b \subset Aa$, e daí $\mathfrak{p}\ ba^{-1} \subset A$; Pela definição de $\mathfrak{p}^{-1}$ tem-se $ba^{-1} \in \mathfrak{p}^{-1} = A$; mas b não está em Aa, de onde ba^{-1} não está em $A = \mathfrak{p}^{-1}$ (absudo). □

Corolário 1.6.8 *([Sam], pg.50, Teor.3) O conjunto dos ideais fracionários não nulos de um anel de Dedekind A é um grupo.*

Teorema 1.6.9 *([Sam], pg.50, Teor.3) Sejam A um anel de Dedekind e* $\mathfrak{a}$ *um ideal não nulo de A. Então existem ideais primos não nulos* $\mathfrak{p}_1,...,\mathfrak{p}_n$ *de A e inteiros positivos* $e_1, ..., e_n$ *tais que*

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

e esta expressão é única.

Demonstração: Sabemos que $\mathfrak{a}$ contém um produto finito de ideais primos não nulos, ou seja, existem $\mathfrak{p}_1,...,\mathfrak{p}_s$ ideais primos não nulos tais que $\mathfrak{p}_1...\mathfrak{p}_s \subset \mathfrak{a}$. Faremos a prova usando indução sobre s. Se $s = 1$, então $\mathfrak{a}$ é primo, e nada temos a provar. Suponhamos agora que $\mathfrak{p}_1...\mathfrak{p}_s \subset \mathfrak{a}$. Existe um ideal primo $\mathfrak{p}$ tal que

$$\mathfrak{p}...\mathfrak{p}_s \subset \mathfrak{a} \subset \mathfrak{p};$$

logo $\mathfrak{p}$ divide $\mathfrak{p}_1...\mathfrak{p}_s$, e sendo $\mathfrak{p}$ primo podemos supor $\mathfrak{p}=\mathfrak{p}_1$. Assim,

$$\mathfrak{p}_2...\mathfrak{p}_s \subset \mathfrak{p}^{-1}a \subset \mathfrak{p}^{-1}\mathfrak{p}=A$$

já que $\mathfrak{a} \subset \mathfrak{p}$. A hipótese da indução nos diz então que $\mathfrak{p}^{-1}\mathfrak{a}=\mathfrak{q}_1...\mathfrak{q}_t$, e portanto $\mathfrak{a}=\mathfrak{p}\mathfrak{q}_1...\mathfrak{q}_t$, como queríamos. Provemos novamente por indução que tal produto é único, a menos da ordem dos fatores. Sejam $\mathfrak{p}_1$, $\mathfrak{p}_s$, $\mathfrak{q}_1$, $\mathfrak{q}_t$ ideais primos não nulos tais que $\mathfrak{p}_1...\mathfrak{p}_s=\mathfrak{q}_1...\mathfrak{q}_t$. Suponhamos que para todo $r < min\{s,t\}$, seja verdadeira a seguinte afirmação: se $\mathfrak{a}_1,...,\mathfrak{a}_r,\mathfrak{b}_1,..,\mathfrak{b}_s$ são ideais primos não nulos tais que $\mathfrak{a}_1...\mathfrak{a}_r=\mathfrak{b}_1...b_s$, então $r = s$ e $\mathfrak{a}_i = \mathfrak{b}_i$, $i = 1,...,s$ (a menos da ordem). Se $min\{s,t\} = 1$, tomemos por exemplo $s = 1$. Então $\mathfrak{a}_1=\mathfrak{b}_1...\mathfrak{b}_t$, e como $\mathfrak{a}_1$ é primo tem-se $t = 1$. De $\mathfrak{p}_1 ...\mathfrak{p}_s=\mathfrak{q}_1...\mathfrak{q}_t \subset \mathfrak{q}_1$, tiramos $\mathfrak{q}_1 \mid \mathfrak{p}_1...\mathfrak{p}_s$, e sem perda de generalidade podemos supor $\mathfrak{q}_1=\mathfrak{p}_1$. Obtemos assim $\mathfrak{p}_2 ...\mathfrak{p}_s=\mathfrak{q}_2...\mathfrak{q}_t$. O resultado segue da hipótese da indução. □

Corolário 1.6.10 *([Sam], pg.50, Teor.3) Seja A um anel de Dedekind e* $\mathfrak{a}$ *um ideal fracionário não nulo de A. Então existem ideais primos não nulos* $\mathfrak{p}_1,...,\mathfrak{p}_n$ *e inteiros* $e_1, ..., e_n$ *tais que*

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

e esta expressão é única.

Demonstração: Seja $d \in A$ um denominador comum para a. Então $d\mathfrak{a}$ é um ideal de A, e o resultado vem do Teorema 1.6.9 e da igualdade

$$\mathfrak{a} = (d\mathfrak{a}).(Ad)^{-1}. \ \square$$

Capítulo 2

Extensão e norma de ideais

Iniciamos este capítulo com a definição de norma de um ideal e a apresentação de alguns resultados. Em seguida fazemos um breve estudo de anéis de frações , com o intuito de basear demonstrações da seção seguinte, que trata da decomposição de um ideal em uma extensão. Depois disto, passamos para o estudo desta decomposição em extensões galoisianas.

2.1 Norma de um ideal

Um caso especialmente importante de extensões de corpos são os chamados corpos de números, que são extensões finitas do corpo $\mathbb{Q}$ dos números racionais. Se a dimensão de um corpo de números K é n, diz-se que K é um corpo de números de dimensão n.

Os elementos de um corpo de números integrais sobre $\mathbb{Z}$ são chamados de inteiros de K. Se A é o anel de inteiros de um corpo de números K, pelo Lema 4.2 vemos que os discriminantes de duas bases quaisquer do $\mathbb{Z}$-módulo A são iguais. Definimos o discriminante absoluto do corpo de números K como sendo o discriminante de qualquer $\mathbb{Z}$-base do $\mathbb{Z}$-módulo livre A e será denotado por $\mathfrak{D}_K$.

Lema 2.1.1 *([Sam], pg.21, Teor.1) Seja A um anel principal, M um A-módulo livre de posto finito n e M' um submódulo de M. Então:*

(i) M' é livre de posto finito q, $0 \leq q \leq n$.
(ii) Se $M' \neq (0)$, então existe uma base $(e_1, ..., e_n)$ de M e elementos $a_1, ..., a_q \in A$ satisfazendo $a_i \mid a_{i+1}$, $i = 1, ..., q-1$, e tais que $(a_1e_1, ..., a_qe_q)$ é uma A-base para M'.

Lema 2.1.2 *([Sam], pg.52, Prop.1) Sejam K um corpo de números de grau n, A seu anel de inteiros e x um elemento não nulo de A. Então*

$$|N(x)| = card(A/Ax)$$

Demonstração: Sabemos que A é um $\mathbb{Z}$-módulo livre de posto finito n. Como a aplicação $y \mapsto yx$ de A em Ax é isomorfismo, então Ax é submódulo de A, também de posto n. Pelo Lema 2.1.1, existe uma $\mathbb{Z}$ -base $(e_1, ..., e_n)$ de A e elementos $c_1, ..., c_n \in \mathbb{N}$ tais que $(c_1a_1, ..., c_na_n)$ é uma base para Ax, e vale o isomorfismo

$$A/Ax \simeq \prod_{i=1}^{n} \mathbb{Z}/c_i\mathbb{Z};$$

logo, $card(A/Ax) = c_1...c_n$. Por outro lado, seja $u : A \mapsto Ax$ a aplicação $\mathbb{Z}$ -linear definida por $u(e_i) = c_ie_i$, $i = 1, ..., n$, cujo determinante é $det(u) = c_1...c_n$. Tem-se também que $(xe_1, ..., xe_n)$ é uma $\mathbb{Z}$-base para Ax. Assim, existe um automorfismo v de Ax tal que $v(c_ie_i) = xe_i$. Sendo isomorfismo, então $det(v)$ é inversível em $\mathbb{Z}$, e portanto $|\ det(v)| = 1$. Se $y = \sum a_ie_i$, então

$$(v \circ u)(y) = v(\sum_{i=1}^{n} a_iu(e_i)) = v(\sum_{i=1}^{n} a_ic_ie_i) = \sum_{i=1}^{n} a_i.v(c_ie_i) = xy,$$

ou seja, $v \circ u$ é a multiplicação por x; logo vale $v \circ u = N(x)$. Finalmente, o resultado segue como consequência das igualdades

$$|N(x)| = |\ det(v \circ u)| = |\ det(v)\ |\ .\ |\ det(u)| = |\ c_1...c_n| = card(A/Ax)\ .\ \square$$

Sejam A o anel de inteiros de um corpo de números, $\mathfrak{a}$ um ideal não nulo de A e $x \in \mathfrak{a}$ um elemento não nulo. Então $Ax \subset \mathfrak{a}$, e portanto

$$card(A/\mathfrak{a}) \leq card(A/Ax).$$

Dá-se o nome de norma de $\mathfrak{a}$ (e indicamos por $\mathrm{N}(\mathfrak{a})$) ao número $card(A/\mathfrak{a})$.

Lema 2.1.3 *([Sam], pg.52, Prop.2) Sejam A um anel de Dedekind e $\mathfrak{a}$, $\mathfrak{m}$ ideais de A, com $\mathfrak{m}$ maximal. Então*

$$card(\mathfrak{a}/\mathfrak{am}) = card(A/\mathfrak{m}).$$

Demonstração: Temos $\mathfrak{m}(\mathfrak{a}/\mathfrak{am}) = (0)$, e assim $\mathfrak{a}/\mathfrak{am}$ é um espaço vetorial sobre $A/\mathfrak{m}$ ([Ati], pg 19). Seus subespaços são seus A-módulos, e estes são da forma $\mathfrak{b}/\mathfrak{am}$, onde $\mathfrak{b}$ é um ideal tal que $\mathfrak{am} \subset \mathfrak{b} \subset \mathfrak{a}$. Mas a fatoração de $\mathfrak{a}$ em ideais primos implica que não há ideais entre $\mathfrak{am}$ e $\mathfrak{a}$. Consequentemente, $\mathfrak{a}/\mathfrak{am}$ é espaço vetorial de dimensão 1 sobre $A/\mathfrak{m}$, e portanto $card(\mathfrak{a}/\mathfrak{am}) = card(A/\mathfrak{m})$. □

Proposição 2.1.4 *([Sam], pg.52, Prop.2) Sejam A o anel de inteiros de um corpo de números e $\mathfrak{a}$, $\mathfrak{b}$ ideais não nulos de A. Então*

$$N(\mathfrak{ab}) = N(\mathfrak{a})N(\mathfrak{b}).$$

Demonstração: Se $\mathfrak{b}=\mathfrak{m}_1...\mathfrak{m}_t$, onde os $\mathfrak{m}_i$ são ideais maximais, então

$$N(\mathfrak{ab}) = N((\mathfrak{am}_1...\mathfrak{m}_{t-1})\mathfrak{m}_t).$$

Assim, será suficiente provar para $\mathfrak{m}$ maximal. O isomorfismo

$$A/\mathfrak{a} \simeq (A/\mathfrak{am})/(\mathfrak{a}/\mathfrak{am})$$

nos dá

$$card(A/\mathfrak{am}) = card(A/\mathfrak{a}).card(\mathfrak{a}/\mathfrak{am}).$$

O resultado vem imediatamente da Proposição anterior. □

Como consequência, se $\mathfrak{a}$ é um ideal tal que $N(\mathfrak{a}) = p$, com p primo, então$\mathfrak{a}$ é um ideal primo.

2.2 Anéis de fração

Um subconjunto S de um anel A é dito multiplicativamente fechado se $1 \in S$ e $x, y \in S$ implica $xy \in S$.

Consideremos a relação de equivalência em $A \times S$ definida por

$$(x,s) \equiv (y,r) \Longleftrightarrow \text{existe } t \in S \text{ tal que } (xr - ys).t = 0.$$

Denotemos por x/s a classe de (x,s) em $A \times S$ e por $S^{-1}A$ o conjunto de todas as classes. Verifica-se que o conjunto $S^{-1}A$ é um anel comutativo com elemento unidade, mediante as operações

$$x/s + y/r = xr + ys, \text{ e } (x/s).(y/r) = (xy)/(sr).$$

Se $\mathfrak{a}$ é um ideal de A, é fácil verificar que o conjunto

$$S^{-1}\mathfrak{a} = \{x/s; x \in \mathfrak{a} \text{ e } s \in S\}$$

é um ideal de $S^{-1}A$.

Lema 2.2.1 *([Ati], pg.41, Corol. 3.11) Todo ideal de $S^{-1}A$ é da forma $S^{-1}\mathfrak{a}$, para algum ideal $\mathfrak{a}$ de A.*

Demonstração: Sejam $\mathfrak{b}$ um ideal de $S^{-1}A$, e $\mathfrak{a} = f^{-1}(\mathfrak{b})$, onde $f : A \mapsto S^{-1}A$ é o homomorfismo definido por $f(x) = x/1$. Vale $\mathfrak{b} = S^{-1}\mathfrak{a}$, e este resultado é simples consequência das equivalências

$$x/s \in \mathfrak{b} \Leftrightarrow x/1 \in \mathfrak{b} \Leftrightarrow x \in \mathfrak{a}. \ \square$$

No restante desta seção continuaremos a indicar por f esta função

Proposição 2.2.2 *([Ati], pg.41, Prop.3.11) Sejam A um domínio e S um subconjunto multiplicativamente fechado de $A-(0)$. Então:*

(1) Para todo ideal $\mathfrak{b}=S^{-1}\mathfrak{a}$ de $S^{-1}A$ vale $f(\mathfrak{a})S^{-1}A=\mathfrak{b}$, e $S^{-1}\mathfrak{a} \mapsto \mathfrak{a}$ é uma injeção crescente do conjunto dos ideais de $S^{-1}A$ no conjunto dos ideais de A .

(2) Os ideais primos de $S^{-1}A$ estão em correspondência biunívoca ($\mathfrak{p} \leftrightarrow S^{-1}\mathfrak{p}$) com os ideais primos de A que não interceptam S.

Demonstração: (1): $\mathfrak{b} \cap A$ é um ideal de $S^{-1}A$; logo,

$$(\mathfrak{b} \cap A)S^{-1}A \subset \mathfrak{b} \cap A \subset \mathfrak{b}.$$

Seja agora $x = a/s \in \mathfrak{b}$, onde $a \in A$ e $s \in S$. Então $(s/1)x = a/1 \in \mathfrak{b}$ (já que $\mathfrak{b}$ é ideal) e assim $a \in \mathfrak{b} \cap A$. Daqui segue que $x = (1/s).a \in (\mathfrak{b} \cap A)S^{-1}A$, e desta forma fica estabelecida a igualdade

$$\mathfrak{b} = (\mathfrak{b} \cap A)S^{-1}A.$$

(2) Se $\mathfrak{q} = S^{-1}\mathfrak{a}$ é um ideal primo de $S^{-1}A$, então $f^{-1}(\mathfrak{q}) = \mathfrak{a}$ é ideal primo de A, e vale $\mathfrak{a} \cap S = \emptyset$, já que $\mathfrak{a} \cap S \neq \emptyset$ implica $S^{-1}\mathfrak{p}=S^{-1}A$. Reciprocamente, seja $\mathfrak{p}$ um ideal primo de A que não intercepta S. Seja $\bar{S}$ a imagem de S em $A/\mathfrak{p}$. $\bar{S}$ é um subconjunto multiplicativamente fechado de $A/\mathfrak{p}$, e a aplicação $x/s \mapsto \bar{x}/\bar{s}$ de $S^{-1}A$ em $\bar{S}^{-1}(A/\mathfrak{p})$ induz um isomorfismo

$$S^{-1}A/S^{-1}\mathfrak{p} \simeq \bar{S}^{-1}(A/\mathfrak{p}).$$

Como $\bar{S}^{-1}(A/\mathfrak{p})$ é nulo ou está contido no corpo de frações do domínio $A/\mathfrak{p}$ resulta que este é nulo ou um domínio; consequentemente, $S^{-1}\mathfrak{p}$ é primo ou $S^{-1}\mathfrak{p}=S^{-1}A$. Mas a última igualdade não ocorre, já que $S^{-1}\mathfrak{p}=S^{-1}A$ implica $\mathfrak{p} \cap A \neq \emptyset$; logo $S^{-1}\mathfrak{p}$ é primo. □

Corolário 2.2.3 *([Sam], pg.69) Se A é um domínio Noetheriano, então todo anel de fração $S^{-1}A$ é Noetheriano.*

Demonstração: Seja $\Omega = (S^{-1}\mathfrak{a}_i)_{i\in I}$ uma coleção qualquer de ideais de $S^{-1}A$, onde $\mathfrak{a}_i$ são ideais de A. Sendo A Noetheriano, existe um ideal $\mathfrak{a}_r$ $(r \in I)$ tal que $j \in I$ e $\mathfrak{a}_r \subset \mathfrak{a}_j$ implica $\mathfrak{a}_r = \mathfrak{a}_j$. A injeção $S^{-1}\mathfrak{a} \mapsto \mathfrak{a}$ obtida na Proposição 2.2.2(1) implica que $S^{-1}\mathfrak{a}_r$ é um elemento maximal da coleção Ω; logo $S^{-1}A$ é Noetheriano. □

Proposição 2.2.4 *([Sam], pg.69, Prop.2) Sejam R um domínio, A um subanel de R, S um subconjunto multiplicativamente fechado de $A-(0)$ e B o fecho integral de A em R. Então o fecho integral de $S^{-1}A$ em $S^{-1}R$ é $S^{-1}B$.*

Demonstração: Seja b/s $(b \in B, s \in S)$ um elemento de S^{-1} B, e $a_0 + a_1X + \cdots + a_{n-1}X^{n-1} + X^n \in A[X]$ tal que $f(b) = 0$. Então

$$a_0/(s^n) + ... + (a_{n-1}/s)(b/s)^{n-1} + (b/s)^n = 0,$$

e assim $S^{-1}B$ está contido no fecho integral de $S^{-1}A$ em $S^{-1}R$. Reciprocamente, seja x/s $(x \in R, s \in S)$ um elemento de S^{-1} R integral sobre $S^{-1}A$ .Então existe uma equação da forma

$$(a_o/t_o) + ... + (a_{n-1}/t_{n-1})(x/s)^{n-1} + (x/s)^n = 0$$

Multiplicando por $(t_0...t_{n-1})^n$, mostra-se que $xt_0...t_{n-1}/s$ é integral sobre A (portanto um elemento de B); logo

$$x/s = (xt_0...t_{n-1}/s).(1/t_0...t_{n-1}) \in S^{-1}\ B,$$

o que prova a inclusão contrária. □

Corolário 2.2.5 *([Sam], pg.70) Se A é integralmente fechado, então todo anel de fração $S^{-1}A$ é integralmente fechado.*

Demonstração: Basta tomar R na Proposição 2.2.4 como sendo o corpo de frações de A.

Proposição 2.2.6 *([Sam], pg.70, Prop.3) Se A é um anel de Dedekind, então $S^{-1}A$ é também um anel de Dedekind.*

Demonstração: O anel $S^{-1}A$ é Noetheriano (Corolário 2.2.3) e integralmente fechado (Corolário 2.2.5). Seja $S^{-1}\mathfrak{a}$ ($\mathfrak{a}$ ideal de A) um ideal primo de $S^{-1}A$. Segue que $\mathfrak{a}$ é ideal primo (Proposição 2.2.2) e portanto maximal de A, o que implica ser $S^{-1}\mathfrak{a}$ maximal em $S^{-1}A$; logo $S^{-1}A$ é de Dedekind. □

Proposição 2.2.7 *([Sam], pg.70, Prop.4) Sejam A um domínio de Dedekind, $\mathfrak{p}$ um ideal primo não nulo de A e $S = A - \mathfrak{p}$. Então $S^{-1}A$ é um ideal principal. Mais do que isto, existe um elemento primo $p \in S^{-1}A$ tal que os ideais não nulos de $S^{-1}A$ são da forma $(p^n), n \geq 0$.*

Demonstração: Como $\mathfrak{p}$ é o único ideal primo de A que não intercepta S, segue que $\mathfrak{q}=\mathfrak{p}$ $S^{-1}A$ é o único ideal primo de $S^{-1}A$, e portanto todos os seus ideais não nulos são da forma $\mathfrak{b}^n, n \geq 0$. Resta mostrar que $\mathfrak{b}$ é principal. Para tal, seja $b \in \mathfrak{b} - \mathfrak{b}^2$. Tem-se $(b) \subset \mathfrak{b}$ e $(b) \neq \mathfrak{b}^2$; logo $\mathfrak{b} = (b)$, como queríamos mostrar. □

Proposição 2.2.8 *([Sam], pg. 70, Prop.5) Sejam A um domínio, S um subconjunto multiplicativamente fechado de $A - (0)$ e $\mathfrak{m}$ um ideal maximal de A disjunto de S. Então*

$$S^{-1}A \ /\mathfrak{m}S^{-1}A \simeq A/\mathfrak{m}.$$

Demonstração: A composição dos homomorfismos

$$A \mapsto S^{-1}A \mapsto S^{-1}A/\mathfrak{m}S^{-1}A$$

tem núcleo $\mathfrak{m}S^{-1}A \cap A = \mathfrak{m}$, e portanto $A/\mathfrak{m}$ pode ser mergulhado injetivamente em $S^{-1}A/\mathfrak{m}S^{-1}A$ através do homomorfismo induzido Φ. Para mostrar que Φ é sobrejetiva,seja $x = a/s \in S^{-1}A$ e $\bar{x}$ a classe de x módulo $\mathfrak{m}S^{-1}A$. Como por hipótese $\mathfrak{m} \cap S = \emptyset$, então $s + \mathfrak{m}$ é inversível no corpo $A/\mathfrak{m}$, e assim existe $b \in A$ tal que $bs \equiv 1(mod\ \mathfrak{m})$. Tem-se

$$\Phi(ab) = \Phi((ab - a/s) + a/s) = \Phi(a/s) = \bar{x},$$

o que prova a sobrejetividade de Φ. □

2.3 Decomposição de um ideal primo em uma extensão

Nesta seção A, denotará um anel de Dedekind de característica zero, K seu corpo de frações, L uma extensão finita de K de grau n e B o fecho integral de A em L.

Proposição 2.3.1 *([Sam], pg.71, Prop.1) Seja* $\mathfrak{p}$ *um ideal primo não nulo de* A *e*

$$B\mathfrak{p} = \prod_{i=1}^{q} \mathfrak{b}_i^{e_i}$$

a decomposição de $B\mathfrak{p}$ *em ideais primos de* B. *Então os* $\mathfrak{b}_i$*'s são precisamente os ideais primos* $\mathfrak{q}$ *de* B *tais que* $\mathfrak{q} \cap A = \mathfrak{p}$.

Demonstração: Suponhamos que $\mathfrak{q}$ apareça no produto acima. Então $\mathfrak{q} \supseteq B\mathfrak{p} \supseteq \mathfrak{p}$, e portanto $\mathfrak{q} \cap A$ é um ideal primo de A que contém $\mathfrak{p}$; sendo $\mathfrak{p}$ maximal resulta uma igualdade. A recíproca vem da inclusão de $\mathfrak{q} \supseteq B\mathfrak{p}$.

O anel $A/\mathfrak{p}$ pode ser considerado como subanel de $B/\mathfrak{b}_i$ (resp.$B/B\mathfrak{p}$) através do homomorfismo induzido por $A \mapsto B \mapsto B/\mathfrak{b}_i$ (resp. $A \mapsto B \mapsto B/B\mathfrak{p}$). Mais do que isto, $A/\mathfrak{p}$ e $B/\mathfrak{b}_i$ são corpos e $B/\mathfrak{b}_i$ (resp.$B/B\mathfrak{p}$) é espaço vetorial de dimensão finita sobre $A/\mathfrak{p}$ (resp. $A/\mathfrak{p}$), já que B (e portanto $B/\mathfrak{b}_i$ e $B/B\mathfrak{p}$) é finitamente gerado como A-módulo (resp. $A/\mathfrak{p}$-módulo). □

Definição 2.3.2 *Indicaremos por* f_i *a dimensão* $[B/\mathfrak{b}_i{:}A/\mathfrak{p}]$ *e chamaremos de grau residual de* $\mathfrak{b}_i$ *sobre* A. *O elemento* e_i *é chamado de índice de ramificação de* $\mathfrak{b}_i$ *sobre* A, *e se* $e_i > 1$ *para algum índice* i, *diremos que* $\mathfrak{p}$ *é ramificado (ou* $\mathfrak{p}$ *se ramifica) em* B.

Mais adiante daremos uma caracterização dos ideais de A que se ramificam em B, mas antes veremos alguns resultados essenciais ao estudo de extensão de ideais:

Teorema 2.3.3 *([Sam], pg.71, teor.1) (Igualdade Fundamental) Com as mesmas notações,*

$$\sum_{i=1}^{q} e_i f_i = [B/B\mathfrak{p}:A/\mathfrak{p}] = n.$$

Demonstração: Consideremos a sequência de ideais

$$B \supset \mathfrak{b}_1 \supset \cdots \supset \mathfrak{b}_1^{e_i} \supset \mathfrak{b}_1^{e_i}\mathfrak{b}_2 \supset \cdots \supset \mathfrak{b}_1^{e_1}...\mathfrak{b}_q^{e_q} = B\mathfrak{p}.$$

Dois elementos consecutivos desta cadeia têm a forma $\mathfrak{b}$ e $\mathfrak{b}\mathfrak{b}_i$. Como não existe ideal estritamente contido entre $\mathfrak{b}$ e $\mathfrak{b}\mathfrak{b}_i$, então $\mathfrak{b}/\mathfrak{b}\mathfrak{b}_i$ é espaço vetorial de dimensão 1 sobre $B/\mathfrak{b}_i$. Logo é um espaço vetorial de dimensão f_i sobre $A/\mathfrak{p}$. Dado um índice i , existem exatamente e_i elementos consecutivos na sequência acima com quociente da forma $\mathfrak{b}/\mathfrak{b}\mathfrak{b}_i$, ou seja, de dimensão f_i sobre $A/\mathfrak{p}$. A dimensão total $[B/B\mathfrak{p} : A/\mathfrak{p}]$ é igual a soma das dimensões dos quocientes, que por sua vez é $\sum_{i=1}^{q} e_i f_i$.

A segunda igualdade é verdadeira, se A for principal. De fato, neste caso B é livre de posto finito n . Seja $(x_1, ..., x_n)$ uma A-base para B. Então $(x_1 + B\mathfrak{p}\ , ..., x_n + B\mathfrak{p})$ é uma base para $B/B\mathfrak{p}$ sobre $A/\mathfrak{p}$. A demonstração no caso geral é feita por redução ao caso anterior. Sabemos pela Proposição 2.2.7 que para $S = A - \mathfrak{p}$ o anel $A' = S^{-1}A$ é principal, que $\mathfrak{p}A'$ é o único ideal maximal de A' e que $B' = S^{-1}B$ é o fecho integral de $S^{-1}A$ em L (Prop. 2.2.4). Pelo que foi visto acima, temos

$$[B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = n$$

Seja

$$\mathfrak{p}B = \prod_{i=1}^{q} \mathfrak{b}_i^{e_i}$$

a fatoração de $\mathfrak{p}B$ em B. Então

$$\mathfrak{p}B' = \prod_{i=1}^{q}(B'\mathfrak{b}_i\ )^{e_i};$$

logo,

$$[B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = \sum_{i=1}^{q} e_i\ [B'/B'\mathfrak{b}_i : A'/\mathfrak{p}A'].$$

Mas pela Proposição 2.2.8 temos

$$A'/\mathfrak{p}A' \simeq A/\mathfrak{p}\ ,\ \text{e}\ B'/B'\mathfrak{b}_i \simeq B/\mathfrak{b}_i\ .$$

Portanto,

$$n = [B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = \sum_{i=1}^{q} e_i f_i\ .\ \square$$

Proposição 2.3.4 *([Sam], pg.72, Prop.2) Ainda com as mesmas notações , temos*

$$B/B\mathfrak{p} \simeq \prod_{i=1}^{q} B/\mathfrak{b}_i^{e_i}.$$

Lema 2.3.5 *([Sam], pg.73, Lem.1) Sejam A um anel, $B_1, ..., B_q$ anéis contendo A tais que sejam A-módulo de tipo finito, e $B = \prod_{i=1}^{q} B_i$ o anel produto. Então*

$$\mathfrak{D}_{B|A} = \prod_{i=1}^{q} \mathfrak{D}_{B_i|A}.$$

Demonstração: A prova se faz usando indução sobre o número de anéis q. Verifiquemos para $q = 2$: Sejam $(x_1, ..., x_m)$ e $(y_1, ..., y_n)$ A-bases para B_1 e B_2 , respectivamente. Identificando canonicamente B_1 e B_2 com os subanéis $B_1 \times (0)$ e $(0) \times B_2$ de B, então $(x_1, ..., x_m, y_1, ..., y_n)$ é A-base para B . Temos $x_i y_j = 0$; logo,

$$D(x_1, ..., x_m, y_1, ..., y_n) = det \begin{pmatrix} U & 0 \\ 0 & V \end{pmatrix} = D(x_1, ..., x_m).D(y_1, ..., y_n),$$

onde U é a $m \times m$ matriz $(Tr(x_i x_{i'}))$ e V é a $n \times n$ matriz $(Tr(y_j y_{j'}))$. Logo

$$\mathfrak{D}_{B|A} = A.(D(x_1, ..., x_m).D(y_1, ..., y_n)) = \mathfrak{D}_{B_1|A}.\mathfrak{D}_{B_2|A}.$$

A verificação para o caso $q > 2$ é simples aplicação do caso $q = 2$. □

Lema 2.3.6 *([Sam], pg.73, Lem.2) Sejam B um anel, A um subanel de B tal que B é A-módulo livre de posto finito n e $\mathfrak{a}$ um ideal de A. Se $(x_1, ..., x_n)$ é uma A-base para B e $\bar{x}$ representa a classe de x em $B/\mathfrak{a}B$, então $(\bar{x_1}, ..., \bar{x_n})$ é uma base para $B/\mathfrak{a}B$ sobre $A/\mathfrak{a}$, e*

$$D(\bar{x_1}, ..., \bar{x_n}) = \overline{D(x_1, ..., x_n)}$$

Dizemos que um anel A é reduzido se o único elemento nilpotente de A é o zero.

Lema 2.3.7 *([Sam], pg.65) Seja A um anel Noetheriano reduzido. Então (0) é a intersecção de um número finito de ideais primos.*

Demonstração: Sabemos que num anel Noetheriano todo ideal contém um produto de ideais primos $\mathfrak{p}_1, ..., \mathfrak{p}_n$; logo $(0) = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_n^{e_n}$. Seja $x \in \mathfrak{p}_1 \cap ... \cap \mathfrak{p}_n$. Então $x^n \in \mathfrak{p}_1 ... \mathfrak{p}_n = (0)$, e como o único elemento nilpotente de A é o zero resulta $x = 0$, de onde

$$(0) = \mathfrak{p}_1 ... \mathfrak{p}_n = \mathfrak{p}_1 \cap ... \cap \mathfrak{p}_n \ . \ \square$$

Lema 2.3.8 *([Sam], pg.73, Lem.3) Sejam K um corpo finito ou de característica zero e L uma K-álgebra de dimensão finita. Então L é reduzida se, e somente se $\mathfrak{D}_{L|K} \neq (0)$.*

Demonstração: Suponhamos que L não seja reduzida, e seja $x \in L$ um elemento nilpotente não nulo. Seja $(x_1, ..., x_n)$ uma K-base para L tal que

$x_1 = x$. Então x_1x_j é nilpotente, e portanto o endomofismo $m_{x_1x_j}$ (multiplicação por x_1x_j) de L é nilpotente; Assim, $Tr(x_1x_j) = 0$, o que implica $D(x_1, ..., x_n) = 0$.

Reciprocamente, Suponhamos que L seja reduzido. Então $(0) = \bigcap_{i=1}^{q} \mathfrak{b}_i$, onde os $\mathfrak{b}_i$'s são ideais primos dois a dois distintos de L. (Lema 2.3.7). Mas $L/\mathfrak{b}_i$ é um domínio e uma álgebra de dimensão finita sobre K; logo é um corpo, e portanto $\mathfrak{b}_i$ é maximal. Consequentemente, $\mathfrak{b}_i + \mathfrak{b}_j = 1$, para $i \neq j$, de onde vem

$$L \simeq \prod_{i=1}^{q} L/\mathfrak{b}_i,$$

e pelo Lema 2.3.5

$$\mathfrak{D}_{L|K} = \prod_{i=1}^{q} \mathfrak{D}_{L_i|K},$$

onde $L_i = L/\mathfrak{b}_i$. Já que K é um corpo finito ou de característica zero, as hipóteses da Proposição 1.4.5 estão satisfeitas para as extensões $(L/\mathfrak{b}_i) \mid K$, e portanto $\mathfrak{D}_{L_i|K} \neq (0)$, o que implica $\mathfrak{D}_{L|K} \neq (0)$. □

Dados um anel B e um subanel A de B, já definimos o discriminante de B com relação a A quando B é um A- módulo livre finitamente gerado. A seguir generalizamos tal definição, conforme a

Definição 2.3.9 *Sejam K e L corpos de números, com $K \subseteq L$ e A e B os anéis de inteiros de K e L, respectivamente. O discriminante de L sobre K (ou de B sobre A) é definido como sendo o ideal de A gerado pelos discriminantes de bases de L sobre K que estão contidas em B. Notação: $\mathfrak{D}_{L|K}$ ou $\mathfrak{D}_{B|A}$.*

Seja $(e_1, \cdots, e_n)$ uma base de B sobre A e $(x_1, ..., x_n)$ uma base de L sobre K contida em B. Então existem elementos $a_{ij} \in A$ tais que $x_i = \sum a_{ij}e_j$, e portanto

$$D(x_1, ..., x_n) = det(a_{ij})^2 . D(e_1, ..., e_n).$$

Vê-se que esta definição coincide com a definição anterior.

A seguir vem o resultado central desta seção, que é o

Teorema 2.3.10 *([Sam], pg. 74, Teor.1) Sejam K e L corpos de números, com $K \subseteq L$ e A , B os anéis de inteiros de K e L, respectivamente. Então uma condição necessária e suficiente para que um ideal primo $\mathfrak{p}$ de A se ramifique em B é que $\mathfrak{p}$ contenha $\mathfrak{D}_{B|A}$.*

Demonstração: Mostraremos primeiramente que $\mathfrak{p}$ ramificado é equivalente a $B/B\mathfrak{p}$ não reduzido. Suponhamos $\mathfrak{p}$ não ramificado, e $x + B\mathfrak{p}$ um elemento não nulo de $B/B\mathfrak{p}$ tal que $(x + B\mathfrak{p})^2 = 0$. Então

$$x^2 \in B\mathfrak{p} = \mathfrak{b}_1 ... \mathfrak{b}_q,$$

onde $\mathfrak{b}_i \neq \mathfrak{b}_j$, se $i \neq j$. Segue que $x^2 \in \mathfrak{b}_i$, e sendo os $\mathfrak{b}_i$'s primos vem $x \in \mathfrak{b}_i, i = 1, ..., q$, resultando

$$x \in \bigcap_{i=1}^{q} \mathfrak{b}_i = \prod_{i=1}^{q} \mathfrak{b}_i = B\mathfrak{p}$$

o que não pode ocorrer.

Reciprocamente, suponhamos que $\mathfrak{p}$ seja ramificado, e seja j tal que $e_j \geq 2$. Consideremos um elemento

$$x = x_1^{e_1} ... x_j^{e_j - 1} ... x_q^{e_q} \in B \ (x_i \in B_i)$$

satisfazendo $x \in B - B\mathfrak{p}$. Tal elemento x existe, pois se toda combinação do tipo acima estivesse em $B\mathfrak{p}$ então

$$B\mathfrak{p} = \mathfrak{b}_1^{e_1} ... \mathfrak{b}_j^{e_j - 1} ... \mathfrak{b}_q^{e_q}.$$

Assim,

$$x^2 = x_1^{2e_1}...x_j^{2(e_j-1)}...x_q^{2e_q}, \text{ e } 2(e_j-1) \geq e_j;$$

logo $x^2 \in B\mathfrak{p}$, e $y = (x + B\mathfrak{p}) \neq 0$ em $B/B\mathfrak{p}$ satisfaz $y^2 = 0$, mostrando que $B/B\mathfrak{p}$ é não reduzido. Da equivalência anterior e do Lema 2.3.8 vem $\mathfrak{D}_{(B/B\mathfrak{p})/(A/\mathfrak{p})} = (0)$, já que $A/\mathfrak{p}$ é um corpo finito. Ponhamos agora $S = A - \mathfrak{p}$, $A' = S^{-1}A$, $B' = S^{-1}B$ e $\mathfrak{p}' = \mathfrak{p}A'$. Segue por 2.2.7 que A' é principal, e por 2.2.8

$$A/\mathfrak{p} \simeq A'/\mathfrak{p}' \text{ e } B/B\mathfrak{p} \simeq B'/\mathfrak{p}'B'.$$

Tomemos uma A'-base $(e_1, ..., e_n)$ para B'. Do Lema 2.3.6 vem

$$\mathfrak{D}_{(B/B\mathfrak{p})/(A/\mathfrak{p})} = \mathfrak{D}_{(B'/B'\mathfrak{p}'/(A'/\mathfrak{p}')} = 0 \Leftrightarrow D(e_1, ..., e_n) \in \mathfrak{p}' .$$

Falta mostrar que esta condição é equivalente a $\mathfrak{p} \supseteq \mathfrak{D}_{B|A}$. Se $D(e_1, ..., e_n) \in \mathfrak{p}'$ e se $(x_1, ..., x_n)$ é uma base de L sobre K contida em B, então existe $a'_{ij} \in A'$ tais que $x_i = \sum a'_{ij}.e_j$; assim,

$$D(x_1, ..., x_n) = det(a'_{ij})^2.D((e_1, ..., e_n)\ ) \in \mathfrak{p}' .$$

Observando que $\mathfrak{p}' \cap A = \mathfrak{p}$, concluimos que $D(x_1, ..., x_n) \in \mathfrak{p}' \cap A = \mathfrak{p}$, o que implica $\mathfrak{D}_{B|A} \subseteq \mathfrak{p}$. Para $i = 1, ..., n$ podemos escrever $e_i = y_i/s$, com $y_i \in B$ e $s \in S$ de onde vem

$$D(e_1, ..., e_n) = s^{-2n}.D(y_1, ..., y_n) \in A'.\mathfrak{D}_{B|A} \subseteq A'\mathfrak{p} = \mathfrak{p}' .$$

O Teorema está provado. □

Como consequência, existe apenas um número finito de ideais primos de A que se ramifica em B.

2.4 Teoria de Galois e corpos de números

Quando se trata de uma extensão galoisiana, a decomposição obtida na seção anterior assume características particulares. Veremos, por exemplo, que os índice de ramificação e grau inercial dos ideais acima de um ideal primo $\mathfrak{p}$ são iguais.

Listaremos a seguir alguns dos resultados fundamentais sobre teoria de Galois, que serão utilizados nesta seção.

Dados um corpo L e um conjunto G de automorfismos de L, uma simples verificação mostra que o conjunto dos $x \in L$ tais que $\sigma(x) = x$, para todo $\sigma \in G$, é um subcorpo de L, chamado de corpo fixo de G. Se K é um subcorpo de L, verifica-se também que o conjunto dos K-automorfismos de L é um grupo.

Teorema 2.4.1 *([Sam], pg.86, Teor.1) Seja L uma extensão de grau finito n de K, onde K é um corpo de característica zero. São equivalentes:*

(a) K é o corpo fixo do grupo G dos K-automorfismos de L.
(b) Para todo $x \in L$, o polinômio mínimal de x sobre K tem todas suas raízes em L.
(c) L é o corpo de raízes de um polinômio em $K[X]$.

Demonstração: (a)⇒(b) : Para um elemento $x \in L$, consideremos o polinômio

$$P(X) = \prod_{\sigma \in G}(X - \sigma(x)).$$

Se $\tau \in G$, então $\tau(P(X)) = P(X)$. Isso mostra que $P(X) \in K[X]$. Sendo x uma raíz de $P(X)$, segue que o polinômio minimal de x divide $P(X)$, e assim (a) implica (b).

(b)⇒(c): Seja $x \in L$ tal que $L = K(x)$. Por hipótese, o polinômio minimal de x tem todas suas raízes em L, e claramente L é gerado pelas raízes desse polinômio.

(c)⇒(a): Por hipótese, L é gerado sobre K por um conjunto finito de elementos $(x^{(1)}, ..., x^{(q)})$ e por seus conjugados $(x_j^{(i)})$. Sob essas hipóteses, verifica-se que para todo K-automorfismo σ de L, $\sigma(L) \subset L$. Como todo K-automorfismo é K-linear e injetivo, considerando as dimensões chegamos a $\sigma(L) = L$. É fato conhecido que o grupo G dos K-automorfismos de L tem exatamente n elementos. Seja $x \in L$ um elemento do corpo fixo de G. Então todo $\sigma \in G$ é um $K[x]$-automorfismo de L. Também é fato conhecido que existem exatamente $[L : K[x]]$ $K[x]$-isomorfismos de L em uma extensão de L. Logo $n \leq [L : K[x]]$, que implica $n = [L : K[x]]$, $K[x] = K$ e $x \in K$. □

Ao longo da demonstração do Teorema 2.4.1, observamos que o grupo G dos K-automorfismos de L tem ordem n.

Se as condições do Teorema 2.4.1 são satisfeitas, L é chamada de extensão galoisiana de K, e G é chamado de grupo de Galois de L sobre K. Se G é abeliano (resp. cíclico) então L é chamada de extensão abeliana (resp. cíclica), ou simplesmente um corpo abeliano.

Corolário 2.4.2 *([Sam], pg.87) Sejam K um corpo finito ou de característica zero, L uma extensão de K de grau finito n e H um grupo de automorfismos de L tal que K é o corpo fixo de H. Então L é uma extensão galoisiana de K, e H é o grupo de Galois de L sobre K.*

Demonstração: Seja $x \in L$ e $P(X) = \prod_{\sigma \in H}(X - \sigma(X))$. Para $\tau \in H$, uma simples verificação mostra que $\tau(P(X)) = P(X)$, e assim $P(X) \in K[X]$. Sendo x uma raíz de $P(X)$, segue que o polinômio minimal de x sobre K divide $P(X)$. Pelo Teorema 2.4.1 L é uma extensão galoisiana de K. Seja G o grupo de Galois de L sobre K. Temos $H \subset G$ e $card(G) = n$. Tomemos um elemento $x \in L$ tal que $L = K(x)$. Então

$$n \leq \partial(P) = card(H) \leq card(G) = n,$$

o que implica $G = H$. □

Sejam K um corpo finito ou de característica zero, L uma extensão galoisiana de K e G o grupo de Galois de L sobre K. Para cada subgrupo G' de

G, $k(G')$ indicará o corpo fixo de G', e para cada subcorpo K' de L , $g(K')$ indicará o subgrupo de G formado pelos K'-automorfismos de L. Sobre as aplicações g e k vale o seguinte

Teorema 2.4.3 *([Sam], pg.87, Teor.2) (Teorema Fundamental da Teoria de Galois)*

(a): As aplicações g e k são bijeções, e uma é a inversa da outra. Ambas as aplicações são decrescentes com relação á inclusão em G e em L. Além disso, se K' é um corpo intermediário entre L e K, então L é uma extensão galoisiana de K'.

(b): Se K' é um corpo intermediário entre K e L, então K' é uma extensão galoisiana de K se, e somente se $g(K')$ é um subgrupo normal de G. Neste caso, o grupo de Galois de K' sobre K é isomorfo ao grupo quociente $G/g(K')$.

Demonstração: (a): Sejam K' um corpo intermediário entre K e L e $x \in L$. O polinômio minimal de x sobre K' divide o polinômio minimal de x sobre K. Logo todas suas raízes estão em L, e do Teorema 2.4.1 segue que L é uma extensão galoisiana de K'. Mas K' é o corpo fixo do grupo $g(K')$ dos K' automorfismos de L, ou seja, $k(g(K')) = K'$. Se G' um subgrupo qualquer de G, do Corolário 2.4.2 segue que G' é o grupo de Galois de L sobre $k(G')$, ou seja, $G' = g(k(G'))$. Essas duas últimas relações nos mostram que g e k são bijeções, e que uma é a inversa da outra.

(b): Sejam K' um corpo intermediário entre K e L e $x \in K'$. As raízes do polinômio minimal de x sobre K são elementos de L da forma $\sigma(x)$, onde $\sigma \in G$. Pelo Teorema 2.4.1(b), K' é uma extensão galoisiana de K se, e somente se $\sigma(x) \in K'$, para todo $x \in K'$ e todo $\sigma \in G$, ou equivalentemente, $\sigma(K') \in K'$, para todo $\sigma \in G$. Sejam $\tau \in g(K')$ e $x \in K'$. Segue que $\sigma^{-1}\tau\sigma(x) = \sigma^{-1}\sigma(x) = x$, de onde $\sigma^{-1}\tau\sigma \in g(K')$. Para provar a recíproca, suponhamos $g(K')$ normal em G. Sejam $x \in K'$, $\sigma \in G$ e $\tau \in g(K')$. De $\sigma^{-1}\tau\sigma \in g(K')$ vem $\tau\sigma(x) = \sigma\sigma^{-1}\tau\sigma(x)$; logo $\sigma(x)$ é invariante sob qualquer elemento de $g(K')$, ou seja, $\sigma(x) \in K'$. Consequentemente, $g(K')$ normal em G implica $\sigma(K') = K'$, e assim K' é extensão galoisiana de K.

Para determinar o grupo de Galois de K' sobre K, observe que $\sigma(K') \subset K'$ (e portanto $\sigma(K') = K'$) para todo $\sigma \in G$ implica que a restrição $\sigma \mid K'$ é um K-automorfismo de K'. A restrição $\sigma \mapsto \sigma \mid K'$ de G no grupo de Galois H de K' sobre K é um homomorfismo, e $g(K')$ é seu núcleo. Mas

$$card(H) = [K' : K] = [L : K].[L : K']^{-1} = card(G).card(g(K))^{-1} = card(G/g(K'));$$

logo a restrição acima definida é sobrejetiva, e portanto $H \simeq G/g(K')$. □

Teorema 2.4.4 *([Mon], pg.115, Teor.3.2(b)) Sejam K um corpo de característica zero, z uma raíz primitiva n-ésima da unidade e $L = K(z)$. Então L é uma extensão abeliana de K, e o grupo de Galois de L sobre K é isomorfo a um subgrupo de $(\mathbb{Z}/n\mathbb{Z})^*$.*

Demonstração: O polinômio minimal de z sobre K divide $X^n - 1$; logo suas raízes são raízes n-ésimas da unidade, e portanto potências de z. Do Teorema 2.4.1(c) segue que L é uma extensão galoisiana de K. Para provar que é cíclica, seja G o grupo de Galois de L sobre K. Todo automorfismo $\sigma \in G$ é definido pelo seu valor em $\sigma(z)$, que pela própria construção é uma potência $z^{j(\sigma)}$, onde $j(\sigma)$ é unicamente determinado módulo n. Para $\sigma, \tau \in G$ vale

$$\sigma\tau(z) = \sigma(z^{j(\tau)}) = \sigma(z)^{j(\tau)} = z^{j(\sigma)j(\tau)} ;$$

logo $j(\sigma\tau) \equiv j(\sigma)j(\tau)$ $(mod\ n)$. Dessa forma, $\sigma \to j(\sigma)$ define um homomorfismo de G em $(\mathbb{Z}/n\mathbb{Z})^*$. Verifica-se que este homomorfismo é injetivo, e portanto vale o resultado enunciado. □

Ainda com as hipóteses e notações do Teorema 2.4.4, se n é um número primo, então G é uma extensão cíclica de K.

Nesta seção K e L denotarão corpos de números satisfazendo $K \subseteq L$, $L \mid K$ é galoisiana com grupo de Galois G e $[L : K] = n$. Usaremos ainda as notações A e B para denotar os anéis de inteiros de K e L, respectivamente.

Lema 2.4.5 *([Sam], pg.89, Lem.1) Sejam R um anel e $\mathfrak{b}$, $\mathfrak{p}_1$,...,$\mathfrak{p}_q$ ideais primos de R tais que $\mathfrak{b}$ não esteja contido em $\mathfrak{p}_i$,para $i = 1, ..., q$. Então existe $b \in \mathfrak{b}$ tal que b não está em $\mathfrak{p}_i$, $i = 1, ..., q$.*

Demonstração: Sem perda de generalidade, podemos considerar o caso em que $\mathfrak{p}_j$ não está contido em $\mathfrak{p}_i$, para $j \neq i$. Tomemos elementos $x_{ij} \in \mathfrak{p}_j - \mathfrak{p}_i$ (para $j \neq i$, $1 \leq i$ e $j \leq q$) e elementos $a_i \in \mathfrak{b} - \mathfrak{p}_i$. Os elementos $b_i = a_i . \prod_{j \neq i} x_{ij}$ satisfazem $b_i \in \mathfrak{b}$, $b_i \in R - \mathfrak{p}_i$ e $b_i \in \mathfrak{p}_j$, para $i \neq j$. Pondo $b = b_1 + \cdots + b_q$, tem-se $b \in \mathfrak{b}$ e $b \equiv b_i \ (mod\ \mathfrak{p}_i)$, ou seja, $b \in \mathfrak{b} - \bigcup_{i=1}^{q} \mathfrak{p}_i$ é o elemento procurado. □

Diz-se que dois ideais $\mathfrak{q}$ e $\mathfrak{q}$' de B são conjugados se existir $\sigma \in G$ tal que $\sigma(\mathfrak{q}) = \mathfrak{q}$' .

Proposição 2.4.6 *([Sam], pg.89, Prop.1) Dado um ideal primo $\mathfrak{p}$ de A, então todos os primos $\mathfrak{q}_i$ de B acima de $\mathfrak{p}$ são conjugados e têm os mesmos indices de ramificação e grau residual f. Portanto $B\mathfrak{p}$ é da forma*

$$B\mathfrak{p} = (\prod_{i=1}^{g} \mathfrak{q}_i)^e,$$

onde $n = efg$.

Demonstração: Suponhamos por absurdo que existam ideais primos $\mathfrak{q}$ e $\mathfrak{q}$' acima de $\mathfrak{p}$ tais que $\sigma(\mathfrak{q}) \neq \mathfrak{q}$' , para todo $\sigma \in G$. Como $\mathfrak{q}$ e $\mathfrak{q}$' são maximais, podemos supor que $\mathfrak{q}$ não esteja contido em $\sigma(\mathfrak{q}')$, para $\sigma \in G$. Pelo Lema anterior existe um elemento $x \in \mathfrak{q} - \bigcup_{\sigma \in G} \sigma(\mathfrak{q}')$. Sendo x integral sobre A, uma simples verificação nos mostra que $\sigma(x)$ também é integral sobre A, de onde

$$\prod_{\sigma \in G} \sigma(x) = N(x)$$

é um elemento de $\mathfrak{q}$, e portanto um elemento de $\mathfrak{q} \cap A = \mathfrak{p}$. Por outro lado, $\sigma(x)$ não está em $\mathfrak{q}$', pois $\sigma(x) \in \mathfrak{q}$' implica

$$\sigma^{-1}(\sigma(x)) = x \in \sigma^{-1}(\mathfrak{q}'),$$

o que contraria a hipótese feita sobre x. Dessa forma, $N(x) = \prod_{\sigma \in G} \sigma(x)$ não pertence a $\mathfrak{q}$' (pois $\mathfrak{q}$' é primo), e assim $\mathfrak{p}$ não está contido em $\mathfrak{q}$' , que é um absurdo . □

Definição 2.4.7 *Dado um ideal primo $\mathfrak{q} \in B$ satisfazendo $\mathfrak{q} \cap A = \mathfrak{p}$, os conjuntos*

$$D = D(\mathfrak{q},\mathfrak{p}) = \{\sigma \in G; \sigma(\mathfrak{q}) = \mathfrak{q}\}$$
$$e$$
$$E = E(\mathfrak{q},\mathfrak{p}) = \{\sigma \in G; \sigma(x) \equiv x(\ mod\ \mathfrak{q}\ ),\ para\ todo\ x \in B\}$$

são subgrupos de G, e são chamados de grupo de decomposição e grupo inercial de $\mathfrak{q}$ com relação a $\mathfrak{p}$, respectivamente.

Proposição 2.4.8 *([Mar], pg.99) E é subgrupo normal de D, e o grupo quociente D/E está mergulhado no grupo de Galois $\bar{G}$ de $B/\mathfrak{q}$ sobre $A/\mathfrak{p}$.*

Demonstração: Cada $\sigma \in D$ induz um automorfismo $\bar{\sigma} : B/\mathfrak{q} \mapsto B/\mathfrak{q}$ da seguinte forma: O homomorfismo $x \mapsto \sigma(x) + \mathfrak{q}$ de B em $B/\mathfrak{q}$ é sobrejetivo e tem núcleo $\mathfrak{q}$; assim, a aplicação $\bar{\sigma} : B/\mathfrak{q} \mapsto B/\mathfrak{q}$ dada por $x + \mathfrak{q} \mapsto \sigma(x) + \mathfrak{q}$ é um isomorfismo. Além disso $\bar{\sigma}$ fixa o subcorpo $A/\mathfrak{p}$ pontualmente, já que σ fixa K (e portanto A) pontualmente. Isso mostra que $\bar{\sigma} \in \bar{G}$. Verifica-se que $\sigma \mapsto \bar{\sigma}$ é homomorfismo de D em $\bar{G}$, cujo núcleo é o subgrupo $E \subseteq D$. Portanto E é subgrupo normal de D, e D/E é subgrupo de $\bar{G}$. □

Adotaremos a seguinte notação : Para todo subgrupo H de G, L_H denotará o corpo fixo de H. Mais geralmente, se X é um subconjunto qualquer de L, então X_H denotará o subconjunto $X \cap L_H$. Assim, B_H é o anel de inteiros de L_H, e $\mathfrak{b}_H$ é o único ideal primo de B_H tal que $\mathfrak{b}$ está acima de $\mathfrak{b}_H$. Evidentemente $\mathfrak{q}_H$ está acima de $\mathfrak{p}$, e $B_H/\mathfrak{q}_H$ é um corpo intermediario entre $B/\mathfrak{q}$ e $A/\mathfrak{p}$.

Ainda com as mesmas notações, para $\sigma \in \bar{G}$ uma simples verificação mostra que

$$D(\sigma(\mathfrak{q}),\mathfrak{p}) = \sigma D(\mathfrak{q},\mathfrak{p})\sigma^{-1} \text{ e } I(\sigma(\mathfrak{q}),\mathfrak{p}) = \sigma I(\mathfrak{q},\mathfrak{p})\sigma^{-1}.$$

Teorema 2.4.9 *([Mar], pg.100, teor.28) Usando a notação anterior, vale o seguinte diagrama:*

		graus	*indice de ramificacão*	*grau inercial*
L	$\mathfrak{q}$			
$\cup$		e	e	1
L_E	$\mathfrak{q}_E$			
$\cup$		f	1	f
L_D	$\mathfrak{q}_D$			
$\cup$		g	1	1
K	$\mathfrak{p}$			

Demonstração: Consideremos a extensão $B\mathfrak{q}_D$ do ideal primo $\mathfrak{q}_D$ em B, e seja $\mathfrak{q}$' um ideal primo de B que está acima de $B\mathfrak{q}_D$. Como L é extensão galoisiana de L_D com grupo de Galois D, então existe $\sigma \in D$ tal que $\sigma(\mathfrak{q}) = \mathfrak{q}$', e assim $\mathfrak{q} = \mathfrak{q}$'. Logo $B\mathfrak{q}_D = \mathfrak{q}^{e(q,q')}$, e vale

$$e(\mathfrak{q},\mathfrak{q}_D).f(\mathfrak{q},\mathfrak{q}_D) = [L : L_D\ ] = card(D) = ef.$$

De

$$A/\mathfrak{p} \subseteq B_D/\mathfrak{q}_D \subseteq B/\mathfrak{q}$$

vem $f(\mathfrak{q},\mathfrak{q}_D) \leq f$; além disso, $\mathfrak{p}B_D \subseteq \mathfrak{q}_D$ implica

$$e(\mathfrak{q}_D,\mathfrak{p}) = f(\mathfrak{q}_D,\mathfrak{p}) = 1.$$

Mostraremos agora que $f(\mathfrak{q},\mathfrak{q}_E) = [B/\mathfrak{q} : B_E/\mathfrak{q}_E] = 1$, o que é equivalente a mostrar que o grupo de Galois G' de $B/\mathfrak{q}$ sobre $B_E/\mathfrak{q}_E$ é trivial. Para tal, mostraremos que dado $a \in B/\mathfrak{q}$, existe $m \geq 1$ tal que $(X-a)^m$ tem todos seus coeficientes em $B_E/\mathfrak{q}_E$. Assim, se $\sigma \in G'$, então $\sigma(a)$ será outra raíz de $(X-a)^m$, resultando $\sigma(a) = a$, para todo $\sigma \in G'$ e todo $a \in B/\mathfrak{q}$. Para obter m com a propriedade enunciada, fixemos um elemento $a' \in B$ representante de a em $B/\mathfrak{q}$. Consideremos o polinômio

$$g(x) = \prod_{\sigma \in E}(X - \sigma(a'))$$

Seus coeficientes estão em B (pois $a' \in B$), e qualquer elemento de E fixa tais coeficientes. Logo $g(X) \in B_E[X]$. Reduzindo módulo $\mathfrak{q}$, obtemos o polinômio

$$\bar{g}(X) = \prod_{\sigma \in E}(X - \sigma(a')) + \mathfrak{q} = \prod_{\sigma \in E}(X - a) \in B_E/\mathfrak{q}_E[X],$$

já que

$$a = a' + \mathfrak{q} \equiv \sigma(a') + \mathfrak{q} \ (mod\ \mathfrak{q}).$$

A prova fica completa pondo $m = card(E)$.

Até agora já sabemos que $f(\mathfrak{q}_D,\mathfrak{p}) = 1$. Como consequência temos $f(\mathfrak{q}_E,\mathfrak{q}_D) = f$. Dessa forma,

$$[L_E : L_D\ ] = \sum_{i=1}^{q} e_i(\mathfrak{q}_E,\mathfrak{q}_D).f \geq f.$$

Mas vimos que D/E está mergulhado em $\bar{G}$ (grupo de Galois de $B/\mathfrak{q}$ sobre $A/\mathfrak{p}$), onde $card(\bar{G}) = [B/\mathfrak{q} : A/\mathfrak{p}] = f$. Assim,

$$[L_E : L_D\ ] = card(D/E) \leq f,$$

resultando $[L_E : L_D] = f$. Usando novamente a relação $[L_E : L_D\ ] = \sum_{i=1}^{q} e_i(\mathfrak{q}_E,\mathfrak{q}_D).f = f$ concluimos que $e(\mathfrak{q}_E,\mathfrak{q}_D) = 1$.

Dos resultados anteriores obtem-se imediatamente

$$[L : L_E] = e = e(\mathfrak{q},\mathfrak{q}_E). \ \square$$

Existe uma certa "unicidade" nos resultados obtidos no Teorema 2.4.9, como se vê precisamente no

Teorema 2.4.10 *([Mar], pg. 104, Teor.29) Ainda com as mesmas notações, valem:*

(1) L_D é o maior corpo intermediário K' tal que $e(\mathfrak{p}',\mathfrak{p}) = f(\mathfrak{p}',\mathfrak{p}) = 1$;
(2) L_D é o menor corpo intermediário K' tal que $\mathfrak{q}$ é o único ideal primo de B acima de $\mathfrak{p}'$.
(3) L_E é o maior corpo intermediário K' tal que $e(\mathfrak{p}',\mathfrak{p}) = 1$;
(4) L_E é o menor corpo intermediário K' tal que $\mathfrak{q}$ se ramifica completamente sobre $\mathfrak{p}'$ (i. é., $e(\mathfrak{q},\mathfrak{p}') = [L : K']$).

Capítulo 3

Representação geométrica de ideais

Neste Capítulo apresentaremos as definições de reticulado, empacotamento esférico, densidade de empacotamento esférico e densidade de centro. Em seguida será apresentado o método de Minkowiski, para obtenção de reticulados via representação geométrica de ideais em anéis de inteiros algébricos. Veremos que a representação geométrica de um ideal é um reticulado, explicitaremos as fórmulas para a densidade de centro destes reticulados e, para alguns corpos de números, calcularemos explicitamente a densidade de centro de algumas famílias de ideais.

Ao estudar a densidade de empacotamento, um dos principais problemas é obter reticulados com densidade alta e que sejam ao mesmo tempo manipuláveis. Uma ilustração desta dificuldade pode ser vista no trabalho de Shafarevich e Golod (ver [Shaf]), onde os autores descrevem uma família de reticulados com boa densidade porém de difícil descrição.

O que faremos a seguir é introduzir os elementos básicos para manipular com os reticulados gerados pelo método de Minkowiski, no caso de corpos ciclotômicos com condutor potência de primo.

3.1 Reticulados e densidade

Sejam V um espaço vetorial de dimensão finita n sobre um corpo K, A um subanel de K e $b_1, ..., b_m$, $m \leq n$, vetores linearmente independentes de V. Dá-se o nome de A-reticulado (ou simplesmente reticulado) com base $(b_1, ..., b_m)$ ao conjunto dos elementos do tipo

$$x = \sum_{i=1}^{m} r_i b_i,$$

com $r_i \in A$. Nosso interesse maior será pelos casos em que $K = \mathbb{R}$, $A = \mathbb{Z}$, $V = \mathbb{R}^n$ e $m = n$. Quando falarmos em um reticulado Λ , ficará implícito que estamos nas condições acima.

Dados um reticulado Λ com base $(b_1, ..., b_n)$ e $c_1, ..., c_n$ elementos quaisquer de Λ , sejam $r_{ij} \in A$ tais que $c_i = \sum_{j=1}^{n} r_{ij} b_j$. É fato conhecido que uma condição necessária e suficiente para que $(c_1, ..., c_n)$ seja base para Λ é que $det(r_{ij}) \in A^*$.

Um empacotamento esférico em $\mathbb{R}^n$ é uma distribuição de esferas de mesmo raio em $\mathbb{R}^n$ de forma que a intersecção de duas tenha no máximo um ponto; chamaremos simplesmente de empacotamento. Pode-se descrever um empacotamento simplesmente indicando o conjunto dos centros das esferas e o raio. Um empacotamento reticulado é um empacotamento em que o conjunto dos centros forma um reticulado Λ de $\mathbb{R}^n$ e, a menos que se diga o contrário, daqui em diante todos os empacotamentos considerados serão reticulados, e quando o conjunto dos centros for Λ, diremos que o empacotamento é associado a Λ .

Dado um empacotamento em $\mathbb{R}^n$, define-se sua densidade de empacotamento como sendo a proporção do espaço $\mathbb{R}^n$ coberta pela união das esferas.

A seguir, introduziremos os elementos básicos que possibilitarão obter uma expressão para a densidade de um empacotamento.

Consideremos um reticulado $\Lambda \subset \mathbb{R}^n$ com $\mathbb{Z}$-base $\beta = (b_1, ..., b_n)$. Denomina-se região fundamental de Λ, com relacão à base β, o conjunto

$$\Lambda_\beta = \{x \in \mathbb{R}^n; x = \sum_{i=1}^n \lambda_i b_i \ , \ 0 \leq \lambda_i < 1\}$$

O espaço euclidiano $\mathbb{R}^n$ é a união disjunta dos conjuntos

$$C_k = \{x \in \mathbb{R}^n; x = \sum_{i=1}^n \alpha_i b_i \ ; k \leq \alpha_i < k+1\}, \ k \in \mathbb{Z} \ ,$$

que são translações da região fundamental Λ_β . Consideremos um empacotamento associado a Λ. Para o cálculo da proporção coberta pelas esferas, basta calcular a proporção em uma região fundamental Λ_β ; é o que faremos a seguir.

Fazendo $b_i = (b_{i1}, ..., b_{in})$, $i = 1, ..., n$, a medida de Lebesgue $m(\Lambda_\beta)$ de Λ_β é igual ao módulo do determinante da matriz

$$B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}.$$

Se β' é uma outra base para Λ , segue que $m(\Lambda_\beta) = m(\Lambda_{\beta'})$ já que β e β' diferem pelo produto de uma matriz inversível com entradas inteiras. Dessa forma, faz sentido definir o volume de Λ como sendo o volume de uma região fundamental, e será denotado por $v(\Lambda)$.

Interessará o empacotamento associado ao reticulado Λ tal que as esferas tenham raio máximo. Para a determinação deste raio, observe que fixado $k > 0$, a intersecção do conjunto compacto $\{x \in \mathbb{R}^n; \mid x \mid \leq k\}$ com o reticulado Λ é um conjunto finito, de onde segue que o número

$$\Lambda_{min} = min\{\mid v \mid; v \in \Lambda, v \neq 0\}$$

está bem definido.

Podemos observar que $\rho = \Lambda_{min}/2$ é o maior raio para o qual é possível distribuir esferas centradas nos pontos de Λ e obter um empacotamento. Dessa forma, estudar os empacotamentos reticulados equivale ao estudo dos reticulados. Com isto, quando citamos densidade do reticulado Λ, ficará

implícito que estamos falando da densidade do empacotamento com esferas de raio ρ associado a este reticulado , e que será denotada por $\Delta(\Lambda)$.

Denotando por $B(\rho)$ a esfera com centro na orígem e raio ρ, temos

$$\Delta(\Lambda) = \frac{Volume\ da\ região\ coberta\ pelas\ esferas}{Volume\ da\ região\ fundamental} = \frac{m(B(\rho))}{v(\Lambda)} =$$

$$= \frac{m(B(1)).\rho^n}{v(\Lambda)}.$$

Como $m(B(\rho)) = \rho^n.m(B(1))$, é conveniente o uso de um outro parâmetro, a saber a densidade de centro

$$\delta(\Lambda) = \frac{\rho^n}{v(\Lambda)}.$$

Pode ser visto em ([*Con*], pg. 13), que a densidade de centro é a quantidade média de centros de esferas por unidade de medida, no caso em que as esferas têm raio 1.

Exemplo 3.1.1 *Em dimensão 2, o reticulado* $\Lambda = \mathbb{Z}^2$, *que é gerado pelos vetores* $(1,0)$ *e* $(0,1)$ *; tem raio de empacotamento* $\rho = 1/2$, *volume* $v(\Lambda) = 1$ *e densidade de centro* $\delta(\Lambda) = 1/4$.

3.2 O homomorfismo canônico de um corpo de números

A seguir descreveremos o método de Minkowiski, para geração de reticulados via ideais de corpos de números. Antes disto, é necessário um breve estudo das imersões de um corpo de números no corpo dos números complexos.

Sejam K um corpo de números de grau n e $\sigma_i : K \mapsto \mathbb{C}$, $i = 1, ..., n$ as n imersões de K em $\mathbb{C}$. Seja r_1 o número de monomorfismos σ_i tais que

$\sigma_i(K) \subseteq \mathbb{R}$. Sem perda de generalidade, podemos supor que $\sigma_i(K) \subseteq \mathbb{R}$, para $i = 1, ..., r_1$. Denotemos por $\alpha : \mathbb{C} \mapsto \mathbb{C}$ a conjugação complexa. Então $\alpha \circ \sigma_i = \sigma_i$, para $i = 1, ..., r_1$, e $\alpha \circ \sigma_i = \sigma_j$ $(i \neq j)$, se $i > r_1$. Segue que $n - r_1$ é par, e fazendo $r_1 + 2r_2 = n$ podemos ainda supor que $\sigma_{j+r_2}(x) = \alpha\sigma_j(x)$, para $r_1 + 1 \leq j \leq r_1 + r_2$.

Denotando por $R(z)$ e $I(z)$ a parte real e imaginária do número complexo z, respectivamente, então o monomorfismo

$$\sigma : K \mapsto \mathbb{R}^n$$

definido por

$$\sigma(x) = \left(\sigma_1(x), ..., \sigma_{r_1}(x), R\sigma_{r_1+1}(x), I\sigma_{r_1+1}(x), ..., R\sigma_{r_1+r_2}(x), I\sigma_{r_1+r_2}(x) \right)$$

será chamado de homomorfismo canônico de K em $\mathbb{R}^n$.

Daqui para frente as notações K, n, r_1 e r_2 serão consideradas como nas relações acima.

Usaremos o homomorfismo canônico para gerar reticulados em $\mathbb{R}^n$ através de subconjuntos específicos de K. Uma das vantagens do método é a obtenção de uma expressão para o volume de tais reticulados. Isto pode ser visto de maneira formal no seguinte

Teorema 3.2.1 *([Sam], pg.56, Prop.1) Sejam M um $\mathbb{Z}$-módulo livre de K de posto n e $(x_1, ..., x_n)$ uma $\mathbb{Z}$-base para M. Então $\sigma(M)$ é um reticulado em $\mathbb{R}^n$, cujo volume é*

$$v(\sigma(M)) = 2^{-r_2} \mid det(\sigma_i(x_j)) \mid .$$

Um caso particularmente interessante ocorre quando M é um ideal ordinário não nulo de K. Neste caso, a expressão para o volume do reticulado fica totalmente determinada, como mostra o

Teorema 3.2.2 *([Samj], pg. 57, Prop.2) Sejam A o anel de inteiros de K e $\mathfrak{a}$ um ideal não nulo de A. Então $\sigma(A)$ e $\sigma(\mathfrak{a})$ são reticulados de $\mathbb{R}^n$, e valem as fórmulas*

$$v(\sigma(A)) = 2^{-r_2}.\mid \mathfrak{D}_K \mid^{1/2};$$
$$v(\sigma(\mathfrak{a})) = 2^{-r_2}.\mid \mathfrak{D}_K \mid^{1/2}.N(\mathfrak{a}),$$

onde $\mathfrak{D}_K$ é o discriminante absoluto de K e $N(\mathfrak{a})$ representa a norma do ideal $\mathfrak{a}$.

Chamaremos de realização geométrica de um ideal $\mathfrak{a}$ ao reticulado $\sigma(\mathfrak{a})$. Em consequência dos Teoremas 3.2.1 e 3.2.2 , a densidade de centro destes reticulados vale

$$\delta(\sigma(\mathfrak{a})) = \frac{2^{r_2}.\rho^n}{\mid \mathfrak{D}_K \mid^{1/2} N(\mathfrak{a})}.$$

A seguir exemplificamos um cálculo de densidade de centro:

Exemplo 3.2.3 *Sejam $K = \mathbb{Q}(\zeta_3)$ e $x = a + b\zeta_3$, $a, b \in \mathbb{Z}$, um inteiro algébrico. Temos*

$$N_{K|\mathbb{Q}}(x) = a^2 + b^2 - ab.$$

Por outro lado, sendo σ o homomorfismo canônico de K, vale

$$\mid \sigma(x) \mid^2 = a^2 + b^2 - ab = N_{K|\mathbb{Q}}(x).$$

Se Considerarmos o ideal principal $\mathfrak{a} = (x)$, então todo $y \in \mathfrak{a}$ é da forma $y = xz$, com $z \in A$, de onde

$$\mid \sigma(y) \mid^2 = \mid \sigma(zx) \mid^2 = N_{K|\mathbb{Q}}(xz) = N_{K|\mathbb{Q}}(x).N_{K|\mathbb{Q}}(z) \geq N_{K|\mathbb{Q}}(x) \ ,$$

pois $N_{K|\mathbb{Q}}(z) \geq 1$, *de onde segue que o menor valor que* $\mid \sigma(y) \mid^2$ *assume, para* $y \in \mathfrak{a}$ *e* $y \neq 0$, *é* $N_{K|\mathbb{Q}}(x)$.

Logo $\rho = \dfrac{\sqrt{N_{K|\mathbb{Q}}(x)}}{2}$, *e a densidade de centro é*

$$\delta(\mathfrak{a}) = \frac{2 \mid N(x) \mid}{4 \mid N(x) \mid . \mid \mathfrak{D}_K \mid^{1/2}} = \frac{1}{2\sqrt{3}}.$$

Observação: Como neste caso particular o anel $\mathbb{Z}[\zeta_3]$ é principal, a densidade de centro independe da escolha do ideal. Esta densidade de centro é a maior para a sua dimensão.

Lema 3.2.4 *([Con], pg. 225) Sejam* K *um corpo de números e* $x \in K$. *Então*

$$|\sigma(x)|^2 = c.Tr_{K|\mathbb{Q}}(x.\overline{x}) \ ,$$

onde $c = 1/2$, *se* K *for totalmente imaginário, e* $c = 1$, *se* K *for totalmente real.*

Quando K é um corpo totalmente imaginário, frequentemente escreveremos a expressão acima como

$$\mid \sigma(x) \mid^2 = (1/2).Tr_{K|\mathbb{Q}}(N_{K|K^+}(x)),$$

onde $K^+ = K \cap \mathbb{R}$.

3.3 Formas quadráticas e corpos ciclotômicos

Sejam Λ um reticulado com $\mathbb{Z}$-base $(v_1, ..., v_n)$ e $v = \sum_{i=1}^{n} a_i v_i$, $a_i \in \mathbb{Z}$, um elemento de Λ. Denotando por b_{ij} o produto escalar $v_i.v_j$ e por $\underline{v} = (a_1, ..., a_n) \in \mathbb{Z}^n$, tem-se

$$| v |^2 = v.v = (\sum_{i=1}^{n} a_i.v_i).(\sum_{i=1}^{n} a_i.v_i) = \sum_{i,j} a_i a_j.(v_i.v_j) = \sum_{i,j} a_i a_j.b_{ij} =$$

$$\begin{pmatrix} a_1 & \cdots & a_n \end{pmatrix} \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \underline{a}.H.\underline{a}^t,$$

onde H é a $n \times n$ matriz simétrica (b_{ij}); é chamada de Grammaniana do reticulado Λ. Observa-se que se $v = \sum_{i=1}^{n} a_i v_i$ e f é a função definida de $\mathbb{R}^n$ em $\mathbb{R}$ por

$$f(X_1, ..., X_n) = \sum_{i,j} b_{ij}.X_i X_j \ ,$$

então $| v |^2 = f(a_1, ..., a_n)$. Isto sugere a seguinte

Definição 3.3.1 *Sejam K um corpo e A um subanel de K. Dizemos que $f \in K[X_1, ..., X_n]$ é uma forma quadrática em n variáveis (ou simplesmente forma quadrática) se*

$$f(X_1, ..., X_n) = \sum_{i,j} a_{ij} X_i X_j,$$

$i, j = 1, ..., n$ com $a_{ij} = a_{ji} \in A$.

Observe que $b_{ij} = v_i.v_j = | v_i | . | v_j | .cos\theta_{ij}$, onde θ_{ij} é o ângulo formado pelos vetores v_i e v_j. Assim , H se decompõe como o produto

$$H = \begin{pmatrix} |\, v_1 \,| & \cdots & 0 \\ 0 & & \vdots \\ \vdots & \ddots & 0 \\ 0 & 0 & |\, v_n \,| \end{pmatrix} \begin{pmatrix} cos\theta_{11} & \cdots & cos\theta_{1n} \\ cos\theta_{21} & \cdots & cos\theta_{2n} \\ \vdots & \ddots & \vdots \\ cos\theta_{n1} & \cdots & cos\theta_{nn} \end{pmatrix} \begin{pmatrix} |\, v_1 \,| & \cdots & 0 \\ 0 & & \vdots \\ \vdots & \ddots & 0 \\ 0 & 0 & |\, v_n \,| \end{pmatrix}.$$

Veremos a seguir resultados de ([$Cra2$]) , que são necessários para o desenvolvimento de ([$Cra1$]) , onde neste último Craig obtém reticulados densos em dimensões 6 e 24, usando representação geométrica de ideais de corpos de números. Estes trabalhos de Craig também são descritos em ([Con] , pg. 226).

Sejam K um corpo de números de dimensão n, A seu anel de inteiros, $(\omega_1, ..., \omega_n)$ uma $\mathbb{Z}$-base para A e $\{\sigma_1, ..., \sigma_n\}$ as imersões de K no corpo dos números complexos; seja ainda H a matriz simétrica tal que a forma quadrática associada ao reticulado $\sigma(A)$, com relação à essa base, seja $\underline{x}.H.\underline{x}^t$. Se $V : A \to \mathbb{Z}^n$ é a aplicação definida por $V(a_1\omega_1 + \cdots + a_n\omega_n) = (a_1, ..., a_n)$, então dado um ideal $\mathfrak{a}$ de A, existe uma matriz U tal que $V(\mathfrak{a}) = U\mathbb{Z}^n$; tal matriz U é chamada de matriz associada ao ideal $\mathfrak{a}$..

Seja M uma matriz tal que $\sigma(A) = M\mathbb{Z}^n$; é chamada de matriz geradora do reticulado $\sigma(A)$, e neste caso $\sigma(\mathfrak{a})$ terá matriz geradora MU, e forma quadrática associada

$$\underline{x}.U^tHU.\underline{x}^t.$$

Percebe-se assim a importância de se determinar a matriz H do reticulado $\sigma(A)$ e a matriz U associada ao ideal em questão. Com este objetivo são colocados os resultados seguintes.

Considerando em A o elemento

$$x = \sum_{i=1}^{n} a_i.\omega_i \ , \ a_i \in \mathbb{Z} \ ,$$

tem-se

$$\sigma_k(x) = \sum_{i=1}^{n} a_i.\sigma_k(\omega_i).$$

Para cada $x \in A$, seja $M(x)$ a matriz definida por

$$x.\begin{pmatrix} \omega_1 & \cdots & \omega_n \end{pmatrix} = \begin{pmatrix} \omega_1 & \cdots & \omega_n \end{pmatrix}.M(x).$$

Então

$$\sigma_k(x).\begin{pmatrix} \sigma_k(\omega_1) & \cdots & \sigma_k(\omega_n) \end{pmatrix} = \begin{pmatrix} \sigma_k(\omega_1) & \cdots & \sigma_k(\omega_n) \end{pmatrix}.M(x) \ ,$$

de onde segue que

$$B.\Omega = \Omega.M(x) \ ,$$

onde

$$B = \begin{pmatrix} \sigma_1(x) & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \sigma_n(x) \end{pmatrix}.$$

Tomando determinantes, temos

$$det(M(x)) = N_{K|\mathbb{Q}}(x) \ .$$

Denotando $V(x)$ por $\underline{x}$, dado um elemento qualquer $z \in A$, então

$$V(xz) = M(x).V(z) = M(x).\underline{z}.$$

Quando o vetor z percorre todo A, então $\underline{z}$ percorre $\mathbb{Z}^n$, de onde segue

$$V(xA) = M(x)\mathbb{Z}^n.$$

Mais geralmente, se considerarmos t elementos $x_1, ..., x_t$, então

$$V(x_1z_1 + \cdots + x_tz_t) = V(x_1z_1) + \cdots + V(x_tz_t) =$$
$$M(x_1)V(x_1) + \cdots + M(x_t)V(x_t),$$

que claramente implica em

$$V(x_1A + \cdots + x_tA) = M(x_1)\mathbb{Z}^n + \cdots + M(x_t)\mathbb{Z}^n.$$

O membro direito desta igualdade é um $\mathbb{Z}$-módulo, com base, digamos, $u_1, ..., u_t$. Se $\mathfrak{a}$ é o ideal de A gerado por $x_1, ..., x_t$, então

$$V(\mathfrak{a}) = V(x_1A + \cdots + x_tA) = T\mathbb{Z}^n,$$

onde T é uma matriz cujas linhas são as coordenadas dos vetores $u_1, ..., u_t$.

Com isto, acabamos de provar o seguinte

Teorema 3.3.2 *([Cra2]) (a): Se $\mathfrak{a}$ é o ideal principal (x) , então $\sigma(\mathfrak{a})$ tem matriz geradora $M(x).\Omega$, e $det(M(x)) = N(x)$.*

(b): Se $\mathfrak{a} = (x_1, ..., x_t)$, então $\sigma(\mathfrak{a})$ tem matriz geradora $M\Omega$, onde M é uma matriz geradora do subreticulado de $\mathbb{Z}^n$ gerado pelas colunas das matrizes $M(x_1), ..., M(x_t)$.

Partiremos agora para a determinação da matriz H no caso particular $K = \mathbb{Q}(\zeta_n)$. Antes, porém, precisamos de um lema, que será enunciado para uma situação ainda geral.

Lema 3.3.3 *Usando a notação acima, então a matriz H do reticulado $\sigma(A) \subset \mathbb{R}^n$ é*

$$H = \overline{\Omega^t}\Omega \ ,$$

onde Ω é a $n \times n$ matriz definida por $\omega_{ij} = \sigma_i(\omega_j)$, e $\{\sigma_1, ..., \sigma_n\}$ é o conjunto das imersões de K no corpo dos números complexos.

Demonstração: O reticulado $\sigma(A)$ terá $\mathbb{Z}$-base $(\sigma(\omega_1), ..., \sigma(\omega_n))$, onde σ é o homomorfismo canônico; seja $x = \sum_{i=1}^{n} a_i \sigma(\omega_i)$, $a_i \in \mathbb{Z}$, um elemento de $\sigma(A)$. Mostraremos que $\overline{\Omega^t}\Omega$ é simétrica. De fato, se τ denota a conjugação complexa, então

$$\left(\overline{\Omega^t}\Omega\right)_{ij} = \sum_{k=1}^{n} \overline{\omega_{ki}}.\omega_{kj} = \sum_{k=1}^{n} \overline{\sigma_k(\omega_i)}.\sigma_k(\omega_j) = \sum_{k=1}^{n} \tau\sigma_k(\omega_i).\sigma_k(\omega_j) =$$

$$= \sum_{k=1}^{n} \sigma_k(\omega_i).\tau\sigma_k(\omega_j) = \sum_{k=1}^{n} \sigma_k(\omega_i).\overline{\sigma_k(\omega_j)} = \sum_{k=1}^{n} \omega_{ki}.\overline{\omega_{kj}} =$$

$$(\Omega^t\overline{\Omega})_{ij} = (\overline{\Omega^t}\Omega)^t_{ij} \ .$$

Isto mostra que $\overline{\Omega^t}\Omega$ é simétrica, e fazendo as contas obtem-se

$$\begin{pmatrix} a_1 & \dots & a_n \end{pmatrix} . \overline{\Omega^t}\Omega . \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \sum_{i=1}^{n} \sigma_i(x).\overline{\sigma_i(x)} \ . \ \square$$

Teorema 3.3.4 *A matriz $H = (h_{ij})$ do reticulado $\sigma(\mathbb{Z}[\zeta_n])$ com relação à $\mathbb{Z}$-base $(1, \zeta_n, ..., \zeta_n^{m-1})$, $m = \phi(n)$, é*

$$h_{ij} = \frac{\mu(d).\phi(n)}{\phi(d)} \ ,$$

onde $d = \dfrac{n}{(n, j-i)}$ *e* $\mu(d) = Tr_{\mathbb{Q}(\zeta_d)|\mathbb{Q}}(\zeta_d)$.

Demonstração: Pelo Lema 3.3.3, temos

$$h_{ij} = \sum_{k=1}^{m} \overline{\omega_{ki}}.\omega_{kj} = \sum_{k=1}^{m} \overline{\sigma_k(\zeta_n^i)}.\sigma_k(\zeta_n^j) =$$
$$= \sum_{k=1}^{m} \sigma_k(\zeta_n^{-i}).\sigma_k(\zeta_n^j) = \sum_{k=1}^{m} \sigma_k(\zeta_n^{j-i}).$$

Para $d = \dfrac{n}{(n, j-i)}$, tem-se $mdc(j-i, d) = 1$; portanto, ζ_n^{j-i} é uma raíz primitiva d-ésima da unidade. Assim, o elemento $\sum_{k=1}^{d} (\zeta_n^{j-i})^k = Tr_{\mathbb{Q}(\zeta_d)|\mathbb{Q}}(\zeta_d)$ aparece $\phi(n)/\phi(d)$ vezes, de onde

$$h_{ij} = \frac{\mu(d).\phi(n)}{\phi(d)} \ . \ \square$$

3.4 Aplicações aos corpos ciclotômicos

Iniciaremos esta seção com o estudo de uma forma quadrática que está relacionada com o cálculo de distâncias nos reticulados considerados. Esta relação pode ser vista no Teorema 3.4.3, que é um dos resultados centrais da seção. Depois disto, partimos para o estudo das densidades de potências do ideal principal $\mathfrak{p}$ definido na página 66.

Para cada inteiro n, seja Q_n a forma quadrática definida por

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

Da igualdade

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

obtem-se

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

Cabe observar que Q_n é positiva definida e totalmente simétrica, i.é., $Q_n(X_1, ..., X_n) = Q_n(X_{\sigma(1)}, ..., X_{\sigma(n)})$, onde σ é uma permutação qualquer do conjunto $\{1, ..., n\}$.

Será útil determinar o menor valor que Q_n assume, com entradas inteiras não todas nulas, para calcular o raio de empacotamento de certos reticulados. Para tal, enunciamos a seguinte

Proposição 3.4.1 *([Nob]) (i): O menor valor que $Q_n(X_1, ..., X_n)$ assume com entradas inteiras, não todas nulas, é n.*

(ii): Para $a \in \mathbb{Z}^n$, $Q_n(a) = n$ quando $a = \pm(1, 1, .., 1)$ ou $a = \pm e_i$, $i = 1, ..., n$; onde $\{e_i\}$ é a $\mathbb{Z}$-base canônica de $\mathbb{Z}^n$.

Demonstração: (i): Observe que

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

Se $a_1 = \cdots = a_{n-1} = 0$, então

$$Q_n(a_1, ..., a_n) = a_n^2 + (n-1)a_n^2 = na_n^2 \geq n \ ,$$

para $a_n \neq 0$. Caso contrário, por hipótese de indução vem

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

e neste caso vale

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

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, sendo que para $n = 1$ a verificação é imediata. Suponhamos que seja válido para $n - 1$, e sejam $a_1, ..., a_n \in \mathbb{Z}$ tais que $Q_n(a_1, ..., a_n) = n$. Observe que

$$a_n^2 + \sum_{i=1}^{n-1}(a_i - a_n)^2 > 0 \ ,$$

sendo na verdade igual a 1, pois caso contrário $Q_{n-1}(X_1, ..., X_{n-1})$ assumiria o valor $n - 2$, o que não ocorre pelo ítem (a). Uma verificação caso a caso mostra o resultado enunciado. □

O Lema seguinte será necessário para provar o Teorema 3.4.3, que relaciona a forma quadrática Q_n com distâncias em reticulados.

Lema 3.4.2 *([Nob]) Se p é um número primo, então*

$$Tr_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^r}^k) = \begin{cases} 0 & , \ se \ (k, p^r) < p^{r-1} \\ -p^{r-1} & , \ se \ (k, p^r) = p^{r-1} \\ p^{r-1} & , \ se \ (k, p^r) > p^{r-1} \end{cases} .$$

Demonstração: Observemos que $(\zeta_{p^r})^{p^s} = e^{2\pi i p^s/p^r} = \zeta_{p^{r-s}}$. De modo geral, se $Irr(x, K)$ representa o polinômio irredutível de x sobre um corpo K, então

$$Irr(\zeta_{p^r}, \mathbb{Q}) = X^{(p-1)p^{r-1}} + X^{(p-2)p^{r-1}} + \cdots + X^{p^{r-1}} + 1 \ ;$$

logo, se $r > 1$, então $Tr_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^r}) = 0$. Se $(k', p^r) = 1$, então $\zeta_{p^r}^{k'}$ é um conjugado de ζ_{p^r} ; logo tem o mesmo traço, e portanto $Tr_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^r}^{k'}) = 0$.

1°_ caso: $(k, p^r) = p^s$, $s \leq r - 2$: Observe que $\zeta_{p^r}^k = \zeta_{p^r}^{p^s k'} = \zeta_{p^{r-s}}^{k'}$. Segue que

$$Tr_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^r}^k) = Tr_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^{r-s}}^{k'}) = Tr_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^{r-s}}) =$$
$$= p^s . Tr_{\mathbb{Q}(\zeta_{p^{r-s}})|\mathbb{Q}}(\zeta_{p^{r-s}}) = p^s . 0 = 0.$$

2°_ caso: $(k, p^r) = p^{r-1}$: Observe que $\zeta_{p^r}^{p^{r-1}k'} = \zeta_p^{k'}$, onde p não divide k'. O polinômio minimal de ζ_p sobre $\mathbb{Q}$ é

$$X^{p-1} + \cdots + X + 1 \ ;$$

logo, $Tr_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(\zeta_p) = -1$, e daí

$$Tr_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_p) = p^{r-1} . Tr_{\mathbb{Q}(\zeta_p)|\mathbb{Q}}(\zeta_p) = p^{r-1}(-1) = -p^{r-1}$$

3°_ caso: $(k, p^r) > p^{r-1}$: Aqui vale $(k, p^r) = p^r$. Seja k' tal que $k = p^r k'$. Tem-se $(\zeta_{p^r})^k = \zeta_{p^r}^{p^r . k'} = 1$. Portanto,

$$Tr_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(\zeta_{p^r}^k) = Tr_{\mathbb{Q}(\zeta_{p^r})|\mathbb{Q}}(1) = (p-1)p^{r-1}. \ \square$$

Conforme o anunciado, finalmente chegamos ao

Teorema 3.4.3 *([Nob]) Sejam p primo, $m = \phi(p^r)$ e $x = a_0 + a_1\zeta_{p^r} + ... + a_{m-1}\zeta_{p^r}^{m-1}$ um inteiro algébrico de $K = \mathbb{Q}(\zeta_{p^r})$. Então*

$$| \sigma(x) |^2 = \frac{p^{r-1}}{2}.\tilde{Q}_r(\underline{x}),$$

onde

$$\tilde{Q}_r(\underline{x}) = Q_{p-1}(\underline{x_0}) + \cdots + Q_{p-1}(\underline{x_t}) \ , \ t = p^{r-1} - 1$$
$$e$$
$$\underline{x_k} = (a_k, a_{p^{r-1}+k}, ..., a_{(p-2)p^{r-1}+k}).$$

Demonstração: Temos

$$x.\bar{x} = \sum_{i=0}^{m-1} a_i^2 + \sum_{i=1}^{m-1} c_i.\alpha_i \ ,$$

onde

$$\alpha_i = \zeta_{p^r}^i + \zeta_{p^r}^{-i} \text{ e } c_i = \sum_{j=0}^{m-i-1} a_j.a_{j+i}$$

Sabemos também que

$$| \sigma(x) |^2 = \frac{1}{2}.Tr_{K|\mathbb{Q}}(x.\overline{x}).$$

Pelo Lema 3.4.2, os elementos $\zeta_{p^r}^k$, com $(k, p^r) < p^{r-1}$ têm traço nulo. Portanto basta considerar os elementos $\zeta_{p^r}^k$ tais que $(k, p^r) \geq p^{r-1}$. Mas $(k, p^r) > p^{r-1}$ implica $(k, p^r) = p^r$, e daí $k \geq p^r > (p-1)p^{r-1}$, o que não ocorre, pois $k \leq m - 1$. Assim, podemos apenas considerar as contribuições dos índices k tais que $(k, p^r) = p^{r-1}$. Tais k são $p^{r-1}, 2p^{r-1}, ..., (p-2)p^{r-1}$. Logo,

$$| \sigma(x) |^2 = \frac{1}{2}.Tr_{K|\mathbb{Q}}(x.\overline{x}) = \frac{1}{2}\left(Tr_{K|\mathbb{Q}}(\sum_{i=0}^{m-1} a_i^2) + \sum_{i=1}^{m-1} Tr_{K|\mathbb{Q}}(c_i\alpha_i)\right) =$$
$$= \frac{(p-1)}{2}.p^{r-1}.(\sum_{i=0}^{m-1} a_i^2) - p^{r-1}.(\sum_{j=1}^{p-2} c_{jp^{r-1}}) =$$
$$= \frac{p^{r-1}}{2}\left((p-1).(\sum_{i=0}^{m-1} a_i^2) - 2.\sum_{j=1}^{p-2} c_{jp^{r-1}}\right).$$

Escrevendo

$$(p-1).(\textstyle\sum_{i=0}^{m-1} a_i^2) = (p-1)b_0 + \cdots + (p-1)b_t \ ,$$

onde $t = p^{r-1} - 1$ e

$$b_0 = a_0^2 + a_{p^{r-1}}^2 + \cdots + a_{(p-2)p^{r-1}}^2 \ ;$$
$$b_1 = a_1^2 + a_{p^{r-1}+1}^2 + \cdots + a_{(p-2)p^{r-1}+1}^2 \ ;$$
$$\vdots$$
$$b_t = a_t^2 + a_{p^{r-1}+t}^2 + \cdots + a_{(p-2)p^{r-1}+t}^2 \ ,$$

tem-se

$$\mid \sigma(x) \mid^2 = \frac{p^{r-1}}{2} \left((p-1)b_0 + \cdots + (p-1)b_t - 2.\textstyle\sum_{j=1}^{p-2} c_{jp^{r-1}} \right).$$

Vejamos que

$$\textstyle\sum_{j=1}^{p-2} c_{jp^{r-1}} = \sum' a_i a_j \ ,$$

onde a última soma é tomada sobre todos os a_i's, $i = 0, ..., m-1$, satisfazendo $i < j$ e $i \equiv j \ (\ mod\ p^{r-1}\ )$.

De fato, seja $a_i a_j$ tal que $i < j$ e $i \equiv j \ (\ mod\ p^{r-1}\ )$. Existe $u \in \{1, ..., p-2\}$ tal que $j = i + up^{r-1}$; logo , $a_i a_j = a_i a_{i+up^{r-1}} \in c_{up^{r-1}}$. Observe que no primeiro somatório, um produto $a_i a_j$ aparece uma única vez, o que prova a igualdade.

Podemos agora reescrever

$$\mid \sigma(x) \mid^2 = \frac{p^{r-1}}{2} \left(\ (p-1)b_0 - 2d_0 + \cdots + (p-1)b_t - 2d_t \ \right),$$

onde

$$d_k = \textstyle\sum a_i a_j \ , \ i < j \text{ e } i, j \equiv k \ (\ mod\ p^{r-1}), \ k = 0, ..., t.$$

Mas

$$(p-1)b_k - 2d_k = Q_{p-1}(a_k, a_{k+p^{r-1}}, ..., a_{k+(p-2)p^{r-1}}),\ k = 0, ..., t\ ;$$

o que completa a demonstração. □

Daqui em diante, nosso objetivo será calcular explicitamente a densidade de centro de potências do ideal principal $\mathfrak{p}$ de $\mathbb{Z}[\zeta_{p^r}]$ gerado pelo elemento $(1-\zeta_{p^r})$.

Proposição 3.4.4 *([Nob]) Sejam $K = \mathbb{Q}(\zeta_{p^r})$ e $A = \mathbb{Z}[\zeta_{p^r}]$. A densidade dos ideais $\mathfrak{p}^j$, $j \in \mathbb{N}$ é periódica. Formalmente,*

$$\delta(\mathfrak{p}^n) = \delta(\mathfrak{p}^{n+m})\ ,$$

onde $m = \phi(p^r)$ e $n \in \mathbb{N}$.

Demonstração: Sabe-se que $\mathfrak{p}^m = pA$, pois p se ramifica completamente; logo, $\mathfrak{p}^{n+m} = p.\mathfrak{p}^n$, que implica $N(\mathfrak{p}^{n+m}) = p^{n+m}$. Com isto, $x \in \mathfrak{p}^{n+m}$ se, e somente se $x = py$, onde $y \in \mathfrak{p}^n$. Segue que

$$\tilde{Q}_r(\underline{x}) = p^2.\tilde{Q}_r(\underline{y})\ ,$$

valendo então

$$\rho(\mathfrak{p}^n) = min\left\{\frac{|\ \sigma(x)\ |}{2}; x \in \mathfrak{p}^n\right\}$$

e

$$\rho(\mathfrak{p}^{n+m}) = min\left\{\frac{|\ \sigma(x)\ |}{2}; x \in \mathfrak{p}^{n+m}\right\} = min\left\{\frac{|\ \sigma(x)\ |}{2}; x \in p.\mathfrak{p}^n\right\} = p.\rho(\mathfrak{p}^n).$$

Para a densidade de centro, temos:

$$\delta(\mathfrak{p}^{n+m}) = \frac{(\rho(\mathfrak{p}^{n+m}))^m}{|\mathfrak{D}_K|^{1/2}.p^{n+m}} = \frac{(\rho(\mathfrak{p}^n))^m}{|\mathfrak{D}_K|^{1/2}.p^n} = \delta(\mathfrak{p}^n). \square$$

Lema 3.4.5 *([Nob]) Sejam* $A = \mathbb{Z}[\zeta_{p^r}]$, $\alpha \in A$ *e* $f(X) \in \mathbb{Z}[X]$ *tal que* $f(\zeta_{p^r}) = \alpha$. *Se* $\alpha \in \mathfrak{p}^{i+1}$, $0 \leq i < m$ *então*

$$f(1) \equiv f'(1) \equiv \cdots \equiv f^{(i)}(1) \equiv 0 \ (\ mod\ p).$$

Demonstração: Sendo

$$h(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1}$$

o polinômio irredutível de ζ_{p^r} sobre $\mathbb{Q}$, então $A \simeq \mathbb{Z}[X]/(h(X))$. Se $\overline{t(X)}$ representa a classe de equivalência, módulo $h(X)$, do polinômio $t(X)$ em A, segue que

$$\alpha \in \mathfrak{p}^{i+1} \Rightarrow \text{existe } g(X) \in \mathbb{Z}[X] \text{ tal que } \overline{f(X)} = \overline{(1-X)^{i+1}.g(X)} \Rightarrow$$
$$\Rightarrow \text{existe } t(X) \in \mathbb{Z}[X] \text{ tal que } f(X) = (1-X)^{i+1}.g(X) + t(X)h(X).$$

Mas

$$h(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} \equiv \frac{(X-1)^{p^r}}{(X-1)^{p^{r-1}}} \equiv (X-1)^{(p-1)p^{r-1}} \ (\ mod\ p\mathbb{Z}[X]\ ).$$

Logo,

$$f(X) \equiv (1-X)^{i+1}.g(X) + t(X)(X-1)^{(p-1)p^{r-1}} \ (\ mod\ p\mathbb{Z}[X]\ ).$$

Colocando $(1-X)^{i+1}$ em evidência , encontramos $v(X) \in \mathbb{Z}[X]$ tal que

$$f(X) \equiv (1-X)^{i+1}.v(X) \ (\ mod\ p\mathbb{Z}[X]\ ),$$

ou seja, existe $u(X) \in \mathbb{Z}[X]$ tal que

$$f(X) = (1-X)^{i+1}.v(X) + p.u(X).$$

Assim, se $\alpha \in \mathfrak{p}^{r+1}$ então existe $u(X) \in \mathbb{Z}[X]$ tal que

$$f(X) = (1-X)^{i+1}.v(X) + p.u(X)\ ,$$

e esta igualdade implica

$$f(1) \equiv f'(1) \equiv \cdots \equiv f^{(i)}(1) \equiv 0\ (\ mod\ p\ )\ .\ \square$$

Lema 3.4.6 *([Nob]) Para $i \in \mathbb{N}$ vale $\zeta_{p^r}^i \equiv i\zeta_{p^r} - (i-1)$ (mod $\mathfrak{p}^2$).*

Demonstração: Provaremos usando indução sobre i. Para $i = 0$ a verificação é imediata. Suponhamos que seja válido para $i = 0, ..., k-1$, onde $k > 0$. Da congruência $\zeta_{p^r}^2 \equiv 2\zeta_{p^r} - 1$ $(mod\ \mathfrak{p}^2)$, temos

$$\zeta_{p^r}^k = \zeta_{p^r}.\zeta_{p^r}^{k-1} \equiv \zeta_{p^r}\left((k-1)\zeta_{p^r} - (k-2)\right) \equiv k\zeta_{p^r} - (k-1)\ (mod\ \mathfrak{p}^2)\ ,$$

e o Lema está provado. $\square$

Lema 3.4.7 *([Nob]) Sejam $x = a_0 + a_1\zeta_{p^r} + \cdots + a_{m-1}\zeta_{p^r}^{m-1}$ um elemento de $A = \mathbb{Z}[\zeta_{p^r}]$ e $f(X) = a_0 + a_1X + \cdots + a_{m-1}X^{m-1} \in \mathbb{Z}[X]$. Então $x \in \mathfrak{p}^2$ se, e somente se, $f(1) \equiv f'(1) \equiv 0$ (mod p) .*

Demonstração: Se $x \in \mathfrak{p}^2$, o Lema 3.4.5 implica imediatamente $f(1) \equiv f'(1) \equiv 0$ (*mod* p) . Por outro lado, aplicando o Lema 3.4.6, temos

$$f(\zeta_{p^r}) = \sum_{i=0}^{m-1} a_i\zeta_{p^r}^i \equiv \sum_{i=0}^{m-1} a_i(i\zeta_{p^r} - (i-1)) \equiv$$
$$\equiv \left(\sum_{i=0}^{m-1} i.a_i\right)\zeta_{p^r} - \sum_{i=0}^{m-1}(i-1)a_i\ (mod\ \mathfrak{p}^2\ ).$$

Observe que

$$\sum_{i=0}^{m-1} i a_i = f'(1)$$
$$\text{e}$$
$$\sum_{i=0}^{m-1} i a_i - \sum_{i=0}^{m-1}(i-1)a_i = \sum_{i=0}^{m-1} a_i = f(1).$$

Isto mostra que $f(1) \equiv f'(1) \equiv 0$ (*mod* p) implica $x = f(\zeta_{p^r}) \in \mathfrak{p}^2$. □

Denotaremos por I_d o conjunto $\{(a_1, ..., a_m) \in \mathbb{Z}^m; \mid a_i \mid \leq d\}$, e para simplificar a notação usaremos Q no lugar de Q_{p-1}.

Proposição 3.4.8 *([Nob]) Para $p > 2$, valem os seguintes resultados:*

(a) Se $r = 1$, o menor valor assumido por $Q(\underline{x})$, com $x \in \mathfrak{p}$ e $x \neq 0$ é $2p$;
(b) Se $r > 1$, o menor valor assumido por $Q_r(\underline{x})$, para $x \in \mathfrak{p}$ e $x \neq 0$, será $2(p-1)$.

Demonstração: (a) : Consideremos um elemento

$$x = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2} \in \mathfrak{p} ,$$

e suponhamos $(a_0, ..., a_{p-2}) \in I_1$. Sejam r e s o número de a_i's iguais a 1 e -1 , respectivamente; assim, o número de a_i's nulos será $p - r - s - 1$. Como a forma quadrática Q é totalmente simétrica, então

$$Q(a_0, ..., a_{p-2}) = Q(1, ..., 1, -1, ..., -1, 0, ..., 0) = -(r-s)^2 + p(r+s).$$

Já vimos que $x \in \mathfrak{p}$ implica $\sum_{i=0}^{p-2} a_i = r - s \equiv 0$ (*mod* p) , e consequentemente $r = s$, tendo em vista o intervalo de variação de r e s; portanto

$$Q(\underline{x}) = 2pr.$$

Evidentemente, $r = 1$ torna $Q(\underline{x}) = 2p$ o valor mínimo.

Para uma $(p-1)$-upla qualquer $(b_0, ..., b_{p-2})$ de $I_2 - I_1$, o Teorema $A.2$ nos mostra que

$$Q(b_0, ..., b_{p-2}) \geq Q(2, 1, ..., 1) = 2p,$$

e pelo Teorema $A.3$, para qualquer $d > 1$ e $(b_0, ..., b_{p-2}) \in I_d - I_{d-1}$ tem-se

$$Q(b_0, ..., b_{p-2}) \geq 2p.$$

Visto que para o elemento $x = 1 - \zeta_p \in \mathfrak{p}$ vale $Q(\underline{x}) = 2p$, concluimos que o menor valor assumido por $Q(\underline{x})$, com $x \in \mathfrak{p}$ e $x \neq 0$ é $2p$; conclui-se assim a prova da parte (a).

(b): Dado um elemento $x = a_0 + a_1\zeta_{p^r} + \cdots + a_{m-1}\zeta_{p^r}^{m-1} \in \mathbb{Z}[\zeta_{p^r}]$, podemos escrevê-lo de uma única maneira como

$$x = x_0 + x_1.\zeta_{p^r} + \cdots + x_t.\zeta_{p^r}^t \ ,$$

onde $t = p^{r-1} - 1$ e

$$\begin{aligned}
x_0 &= a_0 + a_{p^{r-1}}.\zeta_{p^r}^{p^{r-1}} + \cdots + a_{(p-2)p^{r-1}}.\zeta_{p^r}^{(p-2)p^{r-1}} \ ; \\
x_1 &= a_1 + a_{p^{r-1}+1}.\zeta_{p^r}^{p^{r-1}+1} + \cdots + a_{(p-2)p^{r-1}+1}.\zeta_{p^r}^{(p-2)p^{r-1}+1} \ ; \\
&\vdots \\
x_t &= a_t + a_{p^{r-1}+t}.\zeta_{p^r}^{p^{r-1}+t} + \cdots + a_{(p-2)p^{r-1}+t}.\zeta_{p^r}^{(p-2)p^{r-1}+t} \ .
\end{aligned}$$

Neste caso, o Teorema 3.4.3 nos mostra que

$$|\ \sigma(x)\ |^2 = \frac{p^{r-1}}{2}.\tilde{Q}_r(\underline{x}) = \frac{p^{r-1}}{2}\left(Q(\underline{x_1}) + \cdots + Q(\underline{x_t})\right).$$

Se $x \in \mathfrak{p}$ e aparecer um único x_j não nulo na decomposição acima, já vimos que $Q(\underline{x_j}) \geq 2p$, o que implica $\tilde{Q}_r(\underline{x}) \geq 2p > 2(p-1)$.

Visto que $p - 1$ é o menor valor que $Q(a)$ assume, com $a \in \mathbb{Z}^{p-1}$, segue que se o número de a_i's não nulos for maior do que 1, então $\tilde{Q}_r(\underline{x}) \geq 2(p-1)$.

Note que o elemento $z = 1 - \zeta_{p^r} \in \mathfrak{p}$ satisfaz

$$\tilde{Q}_r(\underline{z}) = 2(p-1).$$

Com isto, concluímos que $2(p-1)$ é o menor valor que $\tilde{Q}_r(\underline{x})$ assume, para $x \in \mathfrak{p}$ não nulos. □

Como consequência da parte (a) da Proposição acima, para o caso $r = 1$ a expressão para a densidade será

$$\delta(\mathfrak{p}) = \frac{1}{2^{(p-1)/2}.\sqrt{p}}.$$

No que segue, partiremos para a determinação da densidade de centro de potências de $\mathfrak{p}$ para os demais valores de r, fazendo primeiramente para o caso $r > 2$ e depois $r = 2$. Contudo, precisaremos de alguns lemas.

Dado um número primo p, denotaremos por $\gamma_p(n)$ a valorização p-ádica de n, i.é, o maior número j para o qual p^j divide o inteiro positivo n.

Lema 3.4.9 *([Cazt]) Sejam n um inteiro positivo, p um primo e $a_0, ..., a_s$ tais que $0 \leq a_i \leq p-1$ e $n = a_0 + a_1 p + \cdots + a_s p^s$. Então*

$$\gamma_p(n!) = \frac{n - \sum_{i=1}^{s} a_i}{p-1}.$$

Lema 3.4.10 *([Nob]) Sejam p primo, $r \geq 1$ e $m = p^{r-2}$. Então para $i = 1, ..., m-1$, vale*

$$\gamma_p \left(\begin{array}{c} m \\ i \end{array} \right) \geq 1 \ ,$$

onde $\left(\begin{array}{c} m \\ i \end{array} \right) = \frac{m!}{i!(m-i)!}$.

Demonstração: Sejam $b_1, ..., b_m, c_1, ...c_m$, 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

$(m-i) = c_0 + c_1 p + \cdots + c_m p^m$.

Pelo Lema 3.4.9, temos

$$\gamma_p(m!) = \frac{p^{r-2}-1}{p-1}\ ,$$

$$\gamma_p(i!) = \frac{i - \sum_{i=1}^{m} b_i}{p-1}$$

e

$$\gamma_p((m-i)!) = \frac{m - i - \sum_{i=1}^{m} c_i}{p-1},$$

de onde segue

$$\gamma_p \begin{pmatrix} m \\ i \end{pmatrix} = \frac{-1 + \sum_{i=1}^{m} b_i + \sum_{i=1}^{m} c_i}{p-1}$$

Para concluir a demonstração, basta observar que $\sum_{i=1}^{m} b_i + \sum_{i=1}^{m} c_i \geq 2$.

Lema 3.4.11 *([Nob]) O elemento* $(1 - \zeta_{p^r}^{p^{r-2}})$ *está em* $\mathfrak{p}^{p^{r-2}}$.

Demonstração: Pondo $A = \mathbb{Z}[\zeta_{p^r}]$, temos

$$pA = (1 - \zeta_{p^r})^{(p-1)p^{r-1}}.A\ ,$$

pois p se ramifica completamente em A. Sejam $c_i = \begin{pmatrix} p^{r-2} \\ i \end{pmatrix}$, $0 \leq i \leq p^{r-2}$, os coeficientes do desenvolvimento binomial de $(1 - \zeta_{p^r})^{p^{r-2}}$. Pelo Lema 3.4.9, para $i = 1, ..., p^{r-2} - 1$ vale $\gamma_p(c_i) \geq 1$, ou seja, p é um divisor de $(1 - \zeta_{p^r})^{p^{r-2}} - (1 - \zeta_{p^r}^{p^{r-2}})$. Consequentemente,

$$1 - \zeta_{p^r}^{p^{r-2}} \equiv (1 - \zeta_{p^r})^{p^{r-2}}\ (\ mod\ \mathfrak{p}^{(p-1)p^{r-1}})\ ,$$

o que implica

$$1 - \zeta_{p^r}^{p^{r-2}} \equiv (1 - \zeta_{p^r})^{p^{r-2}}\ (\ mod\ \mathfrak{p}^{p^{r-2}}).$$

Para concluir a prova, basta observar que $(1-\zeta_{p^r})^{p^{r-2}} \in \mathfrak{p}^{p^{r-2}}$. □

Teorema 3.4.12 *([Nob]) Para $r > 2$, a melhor densidade de centro entre os ideais $\mathfrak{p}^i$, $i = 1, ..., p^{r-2}$; ocorre em $i = 1$.*

Demonstração: O Lema 3.4.11 nos mostra que o elemento $x = 1 - \zeta_{p^r}^{p^{r-2}}$ está em $\mathfrak{p}^{p^{r-2}}$, e além disso vale $\tilde{Q}_r(\underline{x}) = 2(p-1)$. Assim, para $i = 1, ..., p$, tem-se

$$\rho(\mathfrak{p}^i) = \frac{\sqrt{(p-1)p^{r-1}}}{2},$$

e as densidades de centro serão

$$\delta(\mathfrak{p}^i) = \frac{((p-1)p^{r-1})^{m/2}}{2^{m/2}.\mid \mathfrak{D}_K \mid^{1/2}.p^i},$$

onde $m = \phi(p^r)$ e $\mid \mathfrak{D}_K \mid = p^{p^{r-1}(pr-r-1)}$. Isto mostra que $\mathfrak{p}$ tem a melhor densidade dentre os ideais considerados. □

Antes da apresentação do resultado que trata do caso $r = 2$, precisamos do seguinte

Lema 3.4.13 *([Nob]) A forma quadrática $Q_k(a)$ não atinge o valor $k+1$, para $a \in \mathbb{Z}^k$.*

Demonstração: Para $a \in I_1$, o resultado é verdadeiro. Tomemos $a \in I_2 - I_1$. Sem perda de generalidade, podemos supor que $a = (2, a_2, ..., a_k)$, para inteiros $a_2, ..., a_k$. Do Teorema $A.2$ vem

$$Q_k(a) \geq Q_k(2, 1, ..., 1) = 2k + 2 > k + 1,$$

e aplicando o Teorema $A.3$, concluimos que para todo j e $a \in I_j$ vale $Q_k(a) > k + 1$. □

Teorema 3.4.14 *([Nob]) Se $r = 2$ e $p > 2$, a melhor densidade entre os ideais $\mathfrak{p}^i$, $i = 1, ..., p$ ocorre para $i = 2$.*

Demonstração: Mostraremos que para $i = 2, ..., p^{r-1}$, o menor valor assumido por $\tilde{Q}_r(\underline{x})$, $x \in \mathfrak{p}^i$ é $2p$. Consideraremos primeiramente o caso $i = 2$. Sejam $x \in \mathfrak{p}^2$, e x_i's como na Proposição 3.4.8(b). Se apenas um dos x_i's não se anula, já vimos que $\tilde{Q}_r(\underline{x}) \geq 2p$, para $x \in \mathfrak{p}$. Visto que para $a \in \mathbb{Z}^n$ o menor valor que $Q(a)$ assume é $p-1$, segue que se o número de x_i's não nulos for maior do que 2 , então $\tilde{Q}_r(\underline{x}) \geq 3(p-1) \geq 2p$. Assim, resta considerar o caso em que dois dos x_i's não se anulam, digamos x_i e x_j. Mostraremos primeiramente que neste caso $\tilde{Q}_r(\underline{x})$ não atinge o valor $2(p-1)$. De fato, suponhamos que isto ocorra. Pelo que foi visto, devemos ter $Q(\underline{x_i}) = Q(\underline{x_j}) = (p-1)$, e isto ocorre apenas nos casos seguintes:

1^0_- caso: $\underline{x_i} = \pm e_l$ e $\underline{x_j} = \pm e_s$. Podemos supor, sem perda de generalidade, que $\underline{x_i} = e_l$; logo $\underline{x_j} = -e_s$, e existem $a, b \in \mathbb{N}$ tais que

$$x = \zeta_{p^r}^i x_i + \zeta_{p^r}^j x_j = \zeta_{p^r}^a - \zeta_{p^r}^b = f(\zeta_{p^r}),$$

onde $f(X) = X^a - X^b$. Como $x \in \mathfrak{p}^2$, então

$$f'(1) \equiv a - b \equiv 0 \ (mod\ p\ ).$$

Observe que $x = \zeta_{p^r}^a(1 - \zeta_{p^r}^{b-a})$. Como estamos considerando dois dos x_i's, então $a - b \equiv 0$ ($mod\ p$) não ocorre, o que é uma contradição.

2^0_- caso: $\underline{x_i} = (1, 1, ..., 1)$ e $\underline{x_j} = \pm e_s$. Aqui, $x \in \mathfrak{p}$ implica $\underline{x_j} = e_s$; logo, existe $a \in \mathbb{N}$ tal que x é da forma

$$x = \zeta_{p^r}^i x_i + \zeta_{p^r}^j x_j = \zeta_{p^r}^i + \zeta_{p^r}^{p+i} + \cdots + \zeta_{p^r}^{(p-2)p+i} + \zeta_{p^r}^{j+s} = f(\zeta_{p^r}) \ ,$$

onde $f(X) = X^i + \cdots + X^{j+s}$. Mas $x \in \mathfrak{p}^2$ implica

$$f'(1) \equiv i + \cdots + (p-2)p + i + j + s \equiv i - j \equiv 0 \ (\ mod\ p\ ) \ ,$$

o que não ocorre, pois $i, j \in \{0, ..., p-1\}$.

3^0_- caso: $\underline{x_i} = (1, 1, ..., 1)$ e $\underline{x_j} = \pm(-1, -1, ..., -1)$: Neste caso, $\underline{x_j} = (-1, -1, ..., -1)$, e

$$x = \zeta_{p^r}^i x_i + \zeta_{p^r}^j x_j = \zeta_{p^r}^i + \zeta_{p^r}^{p+i} + \cdots + \zeta_{p^r}^{(p-2)p+i} - \zeta_{p^r}^j - \cdots - \zeta_{p^r}^{(p-2)p+j} = f(\zeta_{p^r}),$$

onde $f\ (X) = X^i + \cdots + X^{(p-2)p+i} - X^j + \cdots + X^{(p-2)p+j}$. Mas

$$f'(1) \equiv i - j\ (\ mod\ p\ ),$$

o que novamente não ocorre.

Mostramos, assim, que para $x \in \mathfrak{p}^2$ e dois x_i's não nulos, o valor $2(p-1)$ não é atingido por $\tilde{Q}_r(\underline{x})$. Mas pelo Lema 3.4.13 o valor $2p-1$ também não é atingido, e portanto para $x \in \mathfrak{p}^2$ vale $\tilde{Q}_r(\underline{x}) \geq 2p$.

Observe que o elemento $x = 1 - \zeta_{p^r}^p$ está em $\mathfrak{p}^i$, para $i = 1, ..., p$, e $\tilde{Q}_r(\underline{x}) = 2p$; consequentemente, $\mid \sigma(x) \mid^2 = p^r$, o que implica $\rho(\mathfrak{p}^i) = \frac{\sqrt{p^r}}{2}$, $i = 2, ..., p$, e é claro que o ideal de menor norma, que é $\mathfrak{p}^2$, terá a melhor densidade de centro dentre estes.

Assim, para $i = 1, ..., p$, a melhor densidade de centro é obtida em $\mathfrak{p}$ ou $\mathfrak{p}^2$, cuja relação para o caso $r = 2$, é a seguinte:

$$\frac{\delta(\mathfrak{p}^2)}{\delta(\mathfrak{p})} = \left(\frac{p}{(p-1)}\right)^{\frac{(p-1)p}{2}-1} > 1.$$

Logo, $\mathfrak{p}^2$ é o mais denso dentre os ideais considerados , e sua densidade de centro será

$$\delta(\mathfrak{p}^2) = \frac{p^{(p-1)p}}{2^{(p-1)p/2} \mid \mathfrak{D}_K \mid^{1/2} p^2}. \ \square$$

Observação: Para o caso $\mathbb{Q}(\zeta_9)$, o reticulado $\sigma(\mathfrak{p}^2)$ coincide com Λ_6 (ver [Con]), e tem a melhor densidade conhecida para dimensão 6 . Este reticulado também é tratado em $[Cra1]$, e o método é diferente do aqui utilizado. Podemos computar facilmente a densidade de centro, cujo valor é

$$\delta(\mathfrak{p}^2) = \frac{1}{8\sqrt{3}}.$$

Apêndice

Apresentamos neste apêndice resultados de [*Nob*] , com suas respectivas demonstrações. Grande parte dos resultados presentes na seção 3.4 se baseiam sobre os Teoremas $A.2$ e $A.3$. Antes de apresentar estes Teoremas enunciamos um lema, que é uma interpretação geométrica da forma quadrática Q_n:

Lema A.1 *([Nob]) Sejam* $Q_n(X_1,...,X_n) = \sum_{i=1}^{n} X_1^2 + \sum_{i<j}(X_i - X_j)^2$, *e* $a = (a_1,...,a_n) \in \mathbb{R}^n$. *Então*

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

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

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

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

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

logo,

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

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

Teorema A.2 *([Nob]) Dados os números reais $a_1, ..., a_r$, $r < n$, seja*

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

Então F atinge seu mínimo com coordenadas inteiras no ponto

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

e $[z]$ 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 $P = (x, x, ..., x)$, onde $x = (\sum_{i=1}^{r} a_i)/(r+1)$ e tendo $(b_{r+1}, ..., b_n)$ como vetor diretor são da forma

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

Calculemos o valor de F sobre os pontos destas retas:

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

$$= At^2 + Bt + C \ ,$$

onde

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

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

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

Observe que esta expressão é uma função de segundo grau na variável t. Derivando com relação a t , obtem-se

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

Em $t = 0$, temos

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

Assim , sobre as retas passando por P , o gráfico de F é uma parábola com concavidade voltada para cima, cujo menor valor, pelo visto acima, é assumido em P.

Seja $Y_1 = (y, y, ..., y)$, onde $y = \left[\frac{\sum_{i=1}^{r} a_i}{r+1} \right]$. Suporemos 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 $v = (b_{r+1}, ..., b_n)$ e Q_{n-r} é a forma quadrática definida na seção 3.3.4. Pelo Lema $A.1$, este coeficiente dominante será

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

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 será

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

Logo, a direção de menor crescimento dessas parábolas se dará para $d^2(v,\Delta)$ 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, para $Y \in \mathbb{R}^{n-r}$ tal que $F(Y) = F(Y_1)$ vale

$$d(Y,P) \leq d(Y_1,P) \ ,$$

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

Dado o conjunto

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

vamos calcular $A \cap \mathbb{Z}$. Para tal, convém escrever A como a união disjunta dos conjuntos A_1 e A_2 , onde

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

e

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

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

1^0_- caso: $x < y + 1/2$. Aqui, $d(Y,P) = d(Y_1,P)$ ocorre apenas para $Y = Y_1$;

2^0_- 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 $Y_2 = (y+1, ..., y+1)$. Assim,

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

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

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

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

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

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

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

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

Bibliografia

[*Ati*] Atiyah, M.F. and Macdonald, I.G.: "*Introduction to Commutative Algebra* ". Addison-Wesley 1969.

[*Bor*] Borevich, Z. I. and Shafarevich, I. R.: "*Number Theory* ". Ac. Press, 1966.

[*Cas*] Cassels, A.: "*An Introduction to Geometry of Numbers* ". Springer-Verlag 1971.

[*Cazt*] Cazetta, M.: "*Dissertação de mestrado*" UNESP / S. J. Rio Preto, 1996.

[*Con*] Conway, J.H., Sloane, N.J.A.: "*Sphere Packing, Lattices and Groups* ". Springer-Verlag 1988.

[*Cra*1] Craig, M.: "*A Cyclotomic Construction for Leech's Lattice* ". Math. 25 (1978), 236-241.

[*Cra*2] Craig, M.: "*Extreme forms and Cyclotomy* ". Math. 25 (1978), 44-56.

[*Endl*] Endler, O.: "*Teoria dos Números Algébricos* ". IMPA (Projeto Euclides) 1986.

[*Her*] Herstein, I.N.: "*Tópicos de Álgebra* ". Editora da Universidade de São Paulo 1970.

[*Lan*] Lang, S.: "*Algebra* ". Addison-Wesley Publishing Company. 1972.

[*Mar*] Marcus, D.A.: "*Numbers Fields* ". Springer-Verlag 1977.

[*Mon*] Monteiro, L.H.J.: "*Teoria de Galois* ". Publicações do Intituto de Pesquisas Matemáticas da Universidade de São Paulo. 1.969.

[*Nob*] Nobrega, T. P.: "*Fatoração de Ideais Principais* ". (a aparecer).

[*Sam*] Samuel, P.: "*Algebraic Theory of Numbers* ". Hermann 1970.

[*Shaf*] Shafarevich, I. R. and Golod, E. S.: "*On Class Fiel Towers* ". Amer. Math. Sci. Transl. (2) 48 (1965), 91-102.

[*Shan*] Shannon, C. E.: "*A Mathematical Theory of Communication* ", Bell Syst., Tech. J., Vol. 27 (1948).

[*Was*] Washington, L.C.: "*Introduction to Cyclotomic Field* ". Springer-Verlag. 1982.