UNIVERSIDADE FEDERAL DO CEARÁ
CENTRO DE CIÊNCIAS
PÓS – GRADUAÇÃO EM MATEMÁTICA
DISSERTAÇÃO DE MESTRADO

O NÚMERO DE CLASSES DO SUBCORPO REAL MAXIMAL DE UM CORPO CICLOTÔMICO

Fernando Neres de Oliveira

Fortaleza
2010

Fernando Neres de Oliveira

O NÚMERO DE CLASSES DO SUBCORPO REAL MAXIMAL DE UM CORPO CICLOTÔMICO

Dissertação submetida à Coordenação do Curso de Pós-Graduação em Matemática, da Universidade Federal do Ceará, para a obtenção do grau de Mestre em Matemática.

Área de Concentração: Álgebra.

Orientador: Prof. Dr. José Othon Dantas Lopes.

Fortaleza

2010

.

Oliveira, Fernando Neres de

O47n O número de classes do subcorpo real maximal de um corpo ciclotômico / Fernando Neres de Oliveira. - Fortaleza: 2010.

147 f

Orientador: Prof. Dr. José Othon Dantas Lopes.

Área de Concentração: Álgebra.

Dissertação (mestrado) - Universidade Federal do Ceará, Departamento de Matemática, Fortaleza, 2010.

1. Teoria dos Números.

CDD 512.7

Aos meus pais e irmãos,

amo muito vocês ...

Agradecimentos

Agradeço primeiramente a Deus, sem suas bênçãos não teria conseguido chegar aonde cheguei.

Aos meus pais, Maria Eliene Neres de Oliveira e Francisco Caúla de Oliveira Guerra, por terem sempre priorizado a educação de seus filhos.

Ao meu orientador, Professor José Othon Dantas Lopes, por ter contribuido diretamente com o meu progresso dentro da universidade. Agradeço a ele pela orientação que me deu desde os tempos de iniciação científica até a conclusão do presente trabalho. Quero agradecer também a ele, por sempre ter ouvido e dirimido as minhas inúmeras dúvidas.

Ao CNPq pelo apoio financeiro e à Universidade Federal do Ceará por ter me dado a oportunidade de concluir esse curso de pós-graduação.

Aos funcionários da secretaria da pós-graduação, especialmente Andréa Costa Dantas, pelas informações e esclarecimentos.

Aos funcionários da biblioteca, pela atenção dada a nós alunos.

A minha namorada, Ana Paula, pela paciência, companheirismo e carinho.

Ao meu irmão, por sempre ter me ajudado.

A todos os amigos que fiz durante a graduação e no mestrado: Vânia, Kiara, Davi, Shirley, Eduardo, Horácio, Juscileide, Marcília, Joserlan, Edinardo, João Francisco, Tadeu, Paulo Ricardo...

A todos os meus professores da graduação e do mestrado. Todos eles foram

fundamentais para a minha formação.

A minha amiga, Kiara, por ter digitado o texto deste trabalho.

Aos professores que integraram a banca examinadora e a todos aqueles que estiveram presentes no dia da minha defesa.

Todas as pessoas que passaram em minha vida e contribuíram de alguma forma para o meu crescimento pessoal e estudantil são merecedoras do meu agradecimento, pois elas foram determinantes para a construção da realidade que vivo hoje. Muito obrigado a todos...

“A Matemática é a rainha das ciências e a teoria dos números é a rainha das matemáticas.”

Gauss

Resumo

Os objetivos deste trabalho são os seguintes: Primeiro apresentar a prova, devida a N.C. Ankeny, S. Chowla e H. Hasse, de que o número de classes $H(p)$ do subcorpo real maximal $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ de $\mathbb{Q}(\zeta_p)$ é maior do que 2, para os primos $p = (2qn)^2 + 1$ com primo q ímpar e $n > 1$ inteiro. E depois mostrar a condição suficiente, dada por Hideo Yokoi, para que o número de classes $H(4p)$ do subcorpo real maximal $\mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$ de $\mathbb{Q}(\zeta_{4p})$ seja maior do que 1, onde p são primos do tipo $((2n+1)q)^2 \pm 2$, com q primo ímpar e $n \geq 0$ inteiro.

Abstract

The objectives of this work are the following: First present the proof, due to N.C. Ankeny, S. Chowla and H. Hasse, of that the class number $H(p)$ of the maximal real subfield $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ of $\mathbb{Q}(\zeta_p)$ is greater than 2, for the prime $p = (2qn)^2 + 1$ with q odd prime and $n > 1$ integer. And then show the sufficient condition, given by Hideo Yokoi, for that the class number $H(4p)$ of the maximal real subfield $\mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$ of $\mathbb{Q}(\zeta_{4p})$ is larger than 1, where p are prime of the type $((2n+1)q)^2 \pm 2$, with q odd prime and $n \geq 0$ integer.

Sumário

Introdução

O objetivo deste texto é apresentar alguns resultados, relativos ao número de classes do subcorpo real maximal de um corpo ciclotômico. Para isso, iremos no Capítulo 1, aplicar a representação geométrica dos ideais de um corpo numérico para provar a finitude do grupo das classes de ideais. O Capítulo 2, dedicado aos anéis de frações tem por objetivo dá ao leitor os pré-requisitos necessários para a compreensão do próximo capítulo. Já no Capítulo 3, usaremos as informações obtidas sobre anéis de frações, para fazermos um breve estudo sobre a decomposição de ideais primos em uma extensão. Em seguida, no Capítulo 4, apresentaremos o subcorpo real maximal $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ do corpo ciclotômico $\mathbb{Q}(\zeta_m)$ e usaremos alguns resultados relativos a caracteres e somas gaussianas, para justificar na íntegra a imersão do corpo quadrático $\mathbb{Q}(\sqrt{m})$ em $\mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1})$. Tal imersão é mencionada no artigo de Itaru Yamaguchi denominado On the class-number of the maximal real subfield of a cyclotomic field. Feito isso, ficaremos focados em dois artigos, o primeiro de N.C. Ankeny, S. Chowla e H. Hasse, e o segundo de Hideo Yokoi. Ambos têm por objetivo, estudar o número de classes do subcorpo real maximal de um corpo ciclotômico. No artigo do Chowla, é mostrado que para os primos $p = (2qn)^2 + 1$ com q primo ímpar e $n > 1$ inteiro, o número de classes $H(p)$ do subcorpo real maximal $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ de $\mathbb{Q}(\zeta_p)$ é maior do que 2. Este resultado será provado no Capítulo 5. Já no artigo do Yokoi, é apresentada uma condição suficiente para que o número de classes $H(4p)$ do subcorpo real

maximal $\mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$ de $\mathbb{Q}(\zeta_{4p})$ seja maior do que 1, onde p são primos do tipo $((2n+1)q)^2 \pm 2$ com q primo ímpar e $n \geq 0$ inteiro. Essa condição será dada pelo último teorema do Capítulo 6.

Capítulo 1

A Finitude do Grupo das Classes de Ideais

1.1 Preliminares sobre os grupos discretos de $\mathbb{R}^n$

Um subgrupo aditivo H de $\mathbb{R}^n$ é discreto se e somente se para todo compacto K de $\mathbb{R}^n$, a interseção $H \cap K$ é finita.

Exemplo 1.1 *$\mathbb{Z}^n$ é subgrupo discreto de $\mathbb{R}^n$.*

Teorema 1.1 *Sejam A um anel principal, M um A - módulo livre de dimensão finita n e M' um submódulo de M. Então:*

(a) *M' é livre de dimensão q, $0 \leq q \leq n$;*

(b) *Se $M' \neq (0)$ então existe uma base $(e_1, \ldots, e_n)$ de M e elementos não-nulos $a_1, \ldots, a_q \in A$ tal que $(a_1 e_1, \ldots, a_q e_q)$ é uma base de M' e a_i divide a_{i+1}, para $i = 1, 2, \ldots, q-1$.*

Demonstração: Ver [10], página 21.

Teorema 1.2 *Seja H um subgrupo discreto de $\mathbb{R}^n$. Então H é gerado (como $\mathbb{Z}$ - módulo) por r vetores linearmente independentes sobre $\mathbb{R}$ (onde $r \leq n$).*

Observação 1.1 *Temos que H é subgrupo discreto de $\mathbb{R}^n$, logo, H é subgrupo aditivo de $\mathbb{R}^n$. Mas, como $\mathbb{R}^n$ é grupo aditivo abeliano, então H é subgrupo aditivo abeliano. Logo, posso vê-lo como $\mathbb{Z}$ - módulo. Basta definir a seguinte operação externa.*

$$\cdot : \mathbb{Z} \times H \to H$$

$$(c,h) \mapsto c \cdot h = \begin{cases} \underbrace{h+h+\ldots+h}_{c \text{ vezes}}, & \text{se} \quad c \geq 0 \\ \underbrace{(-h)+(-h)+\ldots+(-h)}_{c \text{ vezes}}, & \text{se} \quad c < 0 \end{cases}$$

É fácil verificar que,

$$a\cdot(x+y) = a\cdot x + a\cdot y \ \ , \ \ a\cdot(b\cdot x) = (a\cdot b)\cdot x \ \ , \ \ (a+b)\cdot x = a\cdot x + b\cdot x \ \ , \ \ 1\cdot x = x$$

$\forall a, b \in \mathbb{Z}$ e $x, y \in H$.

Demonstração (Teorema 1.2): Seja $(e_1, \ldots, e_r)$ um sistema de elementos de H linearmente independentes sobre $\mathbb{R}$ e tais que r seja máximo. Seja

$$P = \left\{ \sum_{i=1}^{r} \alpha_i e_i | 0 \leq \alpha_i \leq 1 \right\} \subset \mathbb{R}^n$$

o paralelepípedo construído sobre estes vetores; é evidente que P é compacto, e portanto $P \cap H$ é finito. Seja então $x \in H$. Dado o caráter maximal de (e_i), x se escreve da seguinte forma, $x = \sum_{i=1}^{r} \lambda_i e_i$ com $\lambda_i \in \mathbb{R}$. Consideremos então para $j \in \mathbb{Z}$, o elemento,

$$(*) \quad x_j = jx - \sum_{i=1}^{r} [j\lambda_i] e_i$$

(onde [μ] designa a parte inteira de $\mu \in \mathbb{R}$).

Logo,

$$\begin{aligned} x_j &= j \cdot \sum_{i=1}^{r} \lambda_i e_i - \sum_{i=1}^{r} [j\lambda_i] e_i = \sum_{i=1}^{r} j\lambda_i e_i - \sum_{i=1}^{r} [j\lambda_i] e_i \\ &= \sum_{i=1}^{r} (j\lambda_i e_i - [j\lambda_i] e_i) = \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i])\, e_i. \end{aligned}$$

Como, $0 \leq j\lambda_i - [j\lambda_i] < 1$ então $x_j \in P$. De $(*)$ concluimos que, $x_j \in H$. Assim, $x_j \in P \cap H$. Temos que, $x = x_1 + \sum_{i=1}^{r} [\lambda_i] e_i$. Logo, o $\mathbb{Z}$ - módulo H é gerado por $P \cap H$, e portanto, é de tipo finito. Por outro lado, como $P \cap H$ é finito e $\mathbb{Z}$ é infinito, então, existem dois inteiros distintos j e k tais que $x_j = x_k$. Mas, note que,

$$\begin{aligned} x_j = x_k &\Rightarrow \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i])\, e_i = \sum_{i=1}^{r} (k\lambda_i - [k\lambda_i])\, e_i \\ &\Rightarrow \sum_{i=1}^{r} (j\lambda_i - [j\lambda_i])\, e_i - \sum_{i=1}^{r} (k\lambda_i - [k\lambda_i])\, e_i = 0 \\ &\Rightarrow \sum_{i=1}^{r} ((j\lambda_i - [j\lambda_i]) - (k\lambda_i - [k\lambda_i]))\, e_i = 0 \\ &\Rightarrow (j\lambda_i - [j\lambda_i]) - (k\lambda_i - [k\lambda_i]) = 0, \forall i = 1, \ldots, r \\ &\Rightarrow j\lambda_i - [j\lambda_i] = k\lambda_i - [k\lambda_i], \forall i = 1, \ldots, r \\ &\Rightarrow (j-k)\lambda_i = [j\lambda_i] - [k\lambda_i], \forall i = 1, \ldots, r \\ &\Rightarrow \lambda_i = \frac{[j\lambda_i] - [k\lambda_i]}{j-k}, \forall i = 1, \ldots, r \\ &\Rightarrow \lambda_i \in \mathbb{Q}, \forall i = 1, \ldots, r. \end{aligned}$$

Assim, o $\mathbb{Z}$-módulo H é gerado por um número finito de elementos que são combinações lineares a coeficientes racionais dos (e_i). Seja d um denominador comum $(d \in \mathbb{Z}, d \neq 0)$ destes coeficientes; então $dH \subset \sum_{i=1}^{r} \mathbb{Z} e_i$. Logo, pelo Teorema 1.1, existe uma base (f_i) do $\mathbb{Z}$- módulo $\sum_{i=1}^{r} \mathbb{Z} e_i$, e inteiros $\alpha_i \in \mathbb{Z}$ tais

que $(\alpha_1 f_1, \ldots, \alpha_r f_r)$ geram dH. Como o $\mathbb{Z}$-módulo dH tem a mesma dimensão que H, e dado que $H \supset \sum_{i=1}^{r} \mathbb{Z} e_i$, a dimensão de dH é $\geq r$; portanto, é igual a r e os α_i são não-nulos. Assim como os (e_i), temos que os (f_i) são também linearmente independentes sobre $\mathbb{R}$, então, dH (e em consequência H), é gerado (sobre $\mathbb{Z}$) por r elementos linearmente independentes sobre $\mathbb{R}$.

■

Definição 1.1 *Um subgrupo discreto de dimensão n de $\mathbb{R}^n$ se chama uma rede de $\mathbb{R}^n$.*

Segundo o Teorema 1.2, uma rede de $\mathbb{R}^n$ é gerada sobre $\mathbb{Z}$ por uma base de $\mathbb{R}^n$, que é então uma $\mathbb{Z}$-base da dita rede. Para cada $\mathbb{Z}$-base $e = (e_1, \ldots, e_n)$ de uma rede H, se designará por P_e o paralelepípedo semi-aberto,

$$P_e = \left\{ \sum_{i=1}^{r} \alpha_i e_i | 0 \leq \alpha_i < 1 \right\}.$$

Assim todo ponto de $\mathbb{R}^n$ é congruente módulo H a um ponto e somente um ponto de P_e (se diz então que P_e é um domínio fundamental para H).

Designaremos por μ a medida de Lebesgue em $\mathbb{R}^n$; assim para toda parte integrável S de $\mathbb{R}^n$, $\mu(S)$ designará sua medida (que também chamaremos seu volume).

1.2 Propriedades do Volume

Sejam C e C' subconjuntos de $\mathbb{R}^n$ que são reuniões finitas de paralelepípedos, então valem as seguintes propriedades:

(a) $\mu(P_v) = |\det(a_{ij})|$ sendo $v_i = \sum_{j=1}^{n} a_{ij} \cdot e_j (i = 1, \ldots, n; a_{ij} \in \mathbb{R})$;

(b) $\mu(x + C) = \mu(C)$, para qualquer $x \in \mathbb{R}^n$;

(c) $\mu(\gamma \cdot C) = \gamma^n \cdot \mu(C)$ para qualquer $0 < \gamma \in \mathbb{R}$;

(d) Se $C \cap C' = \emptyset$ então $\mu(C \cup C') = \mu(C) + \mu(C')$;

De (a) resulta imediatamente que, $v = (v_1, \ldots, v_n)$ é base de uma rede de $\mathbb{R}^n$ se e somente se $\mu(P_v) \neq 0$.

Usando a multiplicatividade do determinante, concluímos que se, $w_i = \sum_{j=1}^{n} \omega_{ij} \cdot v_j (i = 1, \ldots, n)$, com $\omega_{ij} \in \mathbb{R}$. Então, $\mu(P_w) = |\det(\omega_{ij})| \cdot \mu(P_v)$.

Lema 1.3 *O volume $\mu(P_e)$ é independente da base e elegida para a rede H.*

Demonstração: Seja $f = (f_1, \ldots, f_n)$ outra base de H. Como cada $f_i \in H$ e $e = (e_1, \ldots, e_n)$ é $\mathbb{Z}$ - base da rede H, então temos que, $f_i = \sum_{j=1}^{n} a_{ij} \cdot e_j$ com $a_{ij} \in \mathbb{Z}$. Logo, $\mu(P_f) = |\det(a_{ij})| \cdot \mu(P_e)$. Mas, como $\det(a_{ij})$ é um determinante de mudança de base e $a_{ij} \in \mathbb{Z}(i, j = 1, \ldots, n)$ então $\det(a_{ij})$ é invertível em $\mathbb{Z}$. Logo, $\det(a_{ij}) \in \{1, -1\} \Rightarrow |\det(a_{ij})| = 1$. Portanto, $\mu(P_f) = \mu(P_e)$.

■

Definição 1.2 *O volume de um qualquer dos P_e se chama o volume da rede H e se escreve $v(H)$.*

Teorema 1.4 (Minkowski) *Sejam H uma rede de $\mathbb{R}^n$ e S um subconjunto integrável de $\mathbb{R}^n$ tais que $\mu(S) > v(H)$. Então, existem dois elementos x, y de S distintos tais que $x - y \in H$.*

Demonstração: Sejam $e = (e_1, \ldots, e_n)$ uma $\mathbb{Z}$ - base de H e P_e o paralelepípedo semi - aberto construído sobre e . Como P_e é um domínio fundamental para H, então, S é a reunião disjunta dos $S \cap (h + P_e)(h \in H)$, ou seja,

$S = \bigcup_{h\in H} S \cap (h + P_e)$. Logo, pelo item (d) das propriedades do volume, temos que, $\mu(S) = \sum_{h\in H} \mu(S \cap (h + P_e))$. Pelo item (b) das propriedades do volume, temos que, μ é invariante por translações, logo, $\mu(S\cap(h+P_e)) = \mu((-h+S)\cap P_e)$. Mas, os conjuntos $(-h + S) \cap P_e)(h \in H)$ não podem ser disjuntos dois a dois, caso contrário, $\mu(P_e) \geq \sum_{h\in H}(-h + S) \cap P_e)$, contrariando a hipótese de que $v(H) < \mu(S)$. Assim, existem dois elementos distintos $h, h' \in H$ tais que,

$$(-h + S) \cap P_e) \cap ((-h' + S) \cap P_e) \neq \varnothing \Rightarrow P_e \cap (-h + S) \cap (-h' + S) \neq \varnothing.$$

Logo, $\exists a \in P_e$ tal que $a = -h + x$ e $a = -h' + y(x, y \in S)$. Note que, $x \neq y$, pois $h \neq h'$. E além disso, $-h + x = -h' + y \Rightarrow x - y = h - h' \in H$.

■

Definição 1.3 *Um subconjunto X de $\mathbb{R}^n$ será chamado simétrico se, para qualquer $a \in X$, tivermos que $-a \in X$.*

Definição 1.4 *Um subconjunto X de $\mathbb{R}^n$ será chamado convexo se, para quaisquer $x, y \in X$, o conjunto $\{\rho \cdot x + (1 - \rho) \cdot y | 0 \leq \rho \leq 1\}$ estiver contido em X. Note que este conjunto consiste dos pontos situados entre x e y, na reta que liga estes dois pontos.*

Por exemplo um círculo, um quadrado, uma elipse, ou um triângulo são convexos em $\mathbb{R}^2$, mas uma coroa circular ou um "quarto crescente" não são.

Corolário 1.1 *Sejam H uma rede de $\mathbb{R}^n$ e S uma parte integrável simétrica em relação a 0 e convexa de $\mathbb{R}^n$. Se supõe que uma das relações seguintes é certa :*

(a) *Tem-se $\mu(S) > 2^n \cdot v(H)$*

(b) *Tem-se $\mu(S) \geq 2^n \cdot v(H)$ e S é compacto.*

Então, $S \cap H$ contém um ponto distinto de 0.

Demonstração: No caso (a) se aplica o Teorema 1.4 a $S' = \frac{1}{2}S$ (pois,

$$\mu(S') = \mu\left(\frac{1}{2}S\right) = \left(\frac{1}{2}\right)^n \cdot \mu(S) = \frac{1}{2^n}\mu(S) > \frac{1}{2^n} \cdot 2^n v(H) = v(H)\Big).$$

Logo, existem dois pontos distintos y, z de S' tais que $y - z \in H$. Como $y, z \in S'$ então, $y = \frac{1}{2}r (r \in S) \Rightarrow 2y \in S$ e $z = \frac{1}{2}s (s \in S) \Rightarrow 2z \in S \Rightarrow -2z \in S$. Da convexidade de S, temos que,

$$\frac{1}{2} \cdot 2y + \left(1 - \frac{1}{2}\right) \cdot (-2z) \in S \Rightarrow \frac{1}{2} \cdot 2y + \frac{1}{2} \cdot (-2z) \in S \Rightarrow y - z \in S.$$

Assim, temos que $y - z \neq 0$ (pois, y e z são distintos) e $y - z \in S \cap H$. Logo, $S \cap H$ contém um ponto distinto de 0. No caso (b) se aplica o caso (a) a $(1+\varepsilon)S (\varepsilon > 0)$. Pois,

$$\mu\left((1+\varepsilon)S\right) = (1+\varepsilon)^n \cdot \mu(S) \geq (1+\varepsilon)^n \cdot 2^n \cdot v(H) > 1 \cdot 2^n \cdot v(H) = 2^n \cdot v(H).$$

Logo, pelo item (a) existe $0 \neq x \in H \cap (1+\varepsilon)S$. Pondo, $H' = H - \{0\}$ temos que, $x \in H' \cap (1+\varepsilon)S$, ou seja, $H' \cap (1+\varepsilon)S$ é não-vazio. E é finito por ser compacto e discreto. Então, temos que, $\bigcap_{\varepsilon>0} H' \cap (1+\varepsilon)S$ não é vazio. Logo, existe $b \in \mathbb{R}^n$ tal que, $b \in \bigcap_{\varepsilon>0} H' \cap (1+\varepsilon)S \Leftrightarrow b \in H'$ e $b \in (1+\varepsilon)S, \forall \varepsilon > 0 \Leftrightarrow 0 \neq b \in H$ e $b \in \bigcap_{\varepsilon>0}(1+\varepsilon)S = S \Leftrightarrow 0 \neq b \in S \cap H$. Portanto, $S \cap H$ contém um ponto distinto de 0.

■

Definição 1.5 *Se chama corpo de números algébricos (ou corpo numérico) a toda extensão de grau finito (e portanto algébrica) de $\mathbb{Q}$. Dado um corpo numérico K, o grau $[K : \mathbb{Q}]$ se chama o grau de K.*

Exemplo 1.2 *K = corpo quadrático é um corpo numérico, pois, $[K : \mathbb{Q}] = 2$.*

Teorema 1.5 *Sejam K um corpo de característica 0 ou finito, K' uma extensão de grau finito n de K e C um corpo algebricamente fechado que contém K. Então, existem n K-isomorfismos distintos de K' em C.*

Demonstração: Ver [10], página 33.

1.3 A imersão canônica de um corpo numérico

Seja K um corpo numérico e n seu grau. Então, pelo Teorema 1.5 existem n $\mathbb{Q}$-isomorfismos distintos $\sigma_i : K \to \mathbb{C}$.

Seja $\alpha : \mathbb{C} \to \mathbb{C}$ a conjugação complexa, ou seja, $\alpha(z) = \overline{z}, z \in \mathbb{C}$. Então, para todo i, $\alpha \circ \sigma_i$ é um dos σ_j, e é igual a σ_i se e somente se $\sigma_i(K) \subset \mathbb{R}$. Seja r_1, o número dos índices i tais que $\sigma_i(K) \subset \mathbb{R}$; então os demais índices são em número par $2r_2$, e tem-se, $r_1 + 2r_2 = n$.

Numeraremos os σ_i de modo que $\sigma_i(K) \subset \mathbb{R}$ para $1 \leq i \leq r_1$ e que $\sigma_{j+r_2}(x) = \overline{\sigma_j(x)}$ para $r_1 + 1 \leq j \leq r_1 + r_2$; assim os $r_1 + r_2$ primeiros σ_i determinam os r_2 restantes. Para $x \in K$, ponhamos

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1+r_2}(x)) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

Chamaremos σ de a imersão canônica de K em $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, a qual é um homomorfismo injetivo para as estruturas de anel. Frequentemente, identificaremos $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ com $\mathbb{R}^n$.

Observação 1.2 *No que segue, quando não for especificado o significado de qualquer uma das notações σ, K, n, r_1, r_2 então ela terá o mesmo significado dado acima.*

Definição 1.6 *Sejam B um anel e A um subanel de B tal que B seja um A- módulo livre de dimensão finita n. Para $(x_1, \ldots, x_n) \in B^n$, se chama o dis-*

criminante do sistema $(x_1, \ldots, x_n)$ *ao elemento de* A *definido por,*

$$D(x_1, \ldots, x_n) = \textit{det}\left(\textit{Tr}_{B/A}(x_i x_j)\right).$$

Proposição 1.1 *Se* $(y_1, \ldots, y_n) \in B^n$ *é outro sistema de elementos de* B*, tal que,* $y_i = \sum_{j=1}^{n} a_{ij} \cdot x_j$ *com* $a_{ij} \in A$ *então* $D(y_1, \ldots, y_n) = (\textit{det}(a_{ij}))^2 \cdot D(x_1, \ldots, x_n)$*.*

Demonstração: Ver [10], página 38.

Proposição 1.2 *Sejam* K *um corpo finito ou de característica* 0*,* L *uma extensão de grau finito* n *de* K *e* $\sigma_1, \ldots, \sigma_n$ *os* n K *- isomorfismos distintos de* L *em um corpo algebricamente fechado* C *que contém* K*. Se* $(x_1, \ldots, x_n)$ *é uma base de* L *sobre* K*, então* $D(x_1, \ldots, x_n) = \textit{det}\left(\sigma_i(x_j)\right)^2 \neq 0$*.*

Demonstração: Ver [10], página 39.

Proposição 1.3 *Se* M *é um sub-*$\mathbb{Z}$*-módulo livre de dimensão* n *de* K*, e se* $(x_i)_{1 \leq i \leq n}$ *é uma* $\mathbb{Z}$*-base de* M*, então* $\sigma(M)$ *é uma rede de* $\mathbb{R}^n$*, cujo volume é dado por,*

$$v\left(\sigma(M)\right) = 2^{-r_2} \cdot \left|\textit{det}\left(\sigma_i(x_j)\right)\right|, \quad 1 \leq i, j \leq n.$$

Demonstração: Para i fixo, as componentes de $\sigma(x_i)$ com respeito a base canônica de $\mathbb{R}^n$ são dadas por

$$\sigma_1(x_i), \ldots, \sigma_{r_1}(x_i), R(\sigma_{r+1}(x_i)), I(\sigma_{r+1}(x_i)), \ldots, R(\sigma_{r_1+r_2}(x_i)), I(\sigma_{r_1+r_2}(x_i))$$

onde R e I designam a parte real e imaginária. Calculemos o determinante D cuja i-ésima coluna é formada pelas componentes de $\sigma(x_i)$ com respeito a base canônica de $\mathbb{R}^n$.

$$D = \begin{vmatrix} \sigma_1(x_1) & \dots & \sigma_1(x_i) & \dots & \sigma_1(x_n) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_{r_1}(x_1) & \dots & \sigma_{r_1}(x_i) & \dots & \sigma_{r_1}(x_n) \\ R(\sigma_{r_1+1}(x_1)) & \dots & R(\sigma_{r_1+1}(x_i)) & \dots & R(\sigma_{r_1+1}(x_n)) \\ I(\sigma_{r_1+1}(x_1)) & \dots & I(\sigma_{r_1+1}(x_i)) & \dots & I(\sigma_{r_1+1}(x_n)) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ R(\sigma_{r_1+r_2}(x_1)) & \dots & R(\sigma_{r_1+r_2}(x_i)) & \dots & R(\sigma_{r_1+r_2}(x_n)) \\ I(\sigma_{r_1+r_2}(x_1)) & \dots & I(\sigma_{r_1+r_2}(x_i)) & \dots & I(\sigma_{r_1+r_2}(x_n)) \end{vmatrix}$$

Utilizando as fórmulas $R(z) = \frac{1}{2}(z + \overline{z})$ e $I(z) = \frac{1}{2i}(z - \overline{z})(z \in \mathbb{C})$ e a linearidade com respeito as filas, se obtém, $D = \pm(2i)^{-r_2} \cdot \det(\sigma_j(x_i))$. Como, $(x_i)_{1\leq i\leq n}$ é uma $\mathbb{Z}$-base do sub-$\mathbb{Z}$-módulo $M \subset K$ e K é um corpo numérico de grau n então $(x_i)_{1\leq i\leq n}$ é base de K sobre $\mathbb{Q}$ (já que, $(x_i)_{1\leq i\leq n}$ L.I. sobre $\mathbb{Z} \Rightarrow$ $\Rightarrow (x_i)_{1\leq i\leq n}$ L.I. sobre $\mathbb{Q}$). Logo, pela Proposição 1.2 temos que $\det(\sigma_j(x_i)) \neq 0$. Assim, $D \neq 0$. E daí, os vetores $\sigma(x_i)$ são L.I. em $\mathbb{R}^n$, ou seja, $(\sigma(x_i))_{1\leq i\leq n}$ é base de $\mathbb{R}^n$. Consequentemente, o $\mathbb{Z}$-módulo gerado pelos vetores $\sigma(x_i)$,

$$\mathbb{Z}\sigma(x_1) + \mathbb{Z}\sigma(x_2) + \ldots + \mathbb{Z}\sigma(x_n)$$

é uma rede de $\mathbb{R}^n$. Mas, note que, $\mathbb{Z}\sigma(x_1) + \mathbb{Z}\sigma(x_2) + \ldots + \mathbb{Z}\sigma(x_n) = \sigma(M)$. De fato,

$$\begin{array}{lll} & a \in \mathbb{Z}\sigma(x_1) + \mathbb{Z}\sigma(x_2) + \ldots + \mathbb{Z}\sigma(x_n) \\ \Rightarrow & a = z_1\sigma(x_1) + z_2\sigma(x_2) + \ldots + z_n\sigma(x_n), z_i \in \mathbb{Z} \\ \underbrace{\Rightarrow}_{\sigma \text{ é } \mathbb{Z}\text{–linear}} & a = \sigma(z_1x_1) + \sigma(z_2x_2) + \ldots + \sigma(z_nx_n), z_i \in \mathbb{Z} \\ \underbrace{\Rightarrow}_{\sigma \text{ é } \mathbb{Z}\text{–linear}} & a = \sigma(z_1x_1 + z_2x_2 + \ldots + z_nx_n), z_i \in \mathbb{Z} \\ \Rightarrow & a \in \sigma(M). \end{array}$$

$$
\begin{array}{lll}
b \in \sigma(M) & \Rightarrow & b = \sigma(z_1x_1 + z_2x_2 + \ldots + z_nx_n), z_i \in \mathbb{Z} \\
 & \underbrace{\Rightarrow}_{\sigma \text{ é } \mathbb{Z}\text{–linear}} & b = z_1\sigma(x_1) + z_2\sigma(x_2) + \ldots + z_n\sigma(x_n), z_i \in \mathbb{Z} \\
 & \Rightarrow & b \in \mathbb{Z}\sigma(x_1) + \mathbb{Z}\sigma(x_2) + \ldots + \mathbb{Z}\sigma(x_n).
\end{array}
$$

Então, $\sigma(M)$ é uma rede de $\mathbb{R}^n$, cuja $\mathbb{Z}$-base é $f = (\sigma(x_1), \ldots, \sigma(x_n))$. Logo,

$$
\begin{aligned}
v(\sigma(M)) &= \mu(P_f) = |\det[\sigma(x_1) \cdots \sigma(x_n)]| = | \pm (2i)^{-r_2} \cdot \det(\sigma_j(x_i))| = \\
&= 2^{-r_2} \cdot |\det(\sigma_j(x_i))|.
\end{aligned}
$$

■

Corolário 1.2 *Sejam R um anel e A um subanel de R. O conjunto A' dos elementos de R que são inteiros sobre A é um subanel de R que contém A.*

Demonstração: Ver [10], página 29.

Corolário 1.3 *Sejam A um anel principal integralmente fechado, K seu corpo de frações, L uma extensão de grau finito n de K e A' o fecho integral de A em L. Supõe-se K de característica 0. Então, A' é um A-módulo livre de dimensão n.*

Demonstração: Ver [10], página 40.

1.4 Terminologia dos Corpos Numéricos

Dado um corpo numérico K, os elementos de K que são inteiros sobre $\mathbb{Z}$ se chamam os inteiros de K. Esses elementos formam um subanel A (de K) que é um $\mathbb{Z}$ - módulo livre de dimensão $[K : \mathbb{Q}]$ (Corolários 1.2 e 1.3). Os discriminantes das bases do $\mathbb{Z}$ - módulo A (chamadas bases integrais de K) diferem em

um elemento invertível de $\mathbb{Z}$, que é inclusive um quadrado (Proposição 1.1). Este elemento não pode ser outro que $+1$, de modo que os discriminantes das bases do $\mathbb{Z}$ - módulo A são todos iguais. O discriminante de uma base integral qualquer de K é chamado discriminante absoluto de K ou discriminante do corpo K.

Exemplo 1.3 *Considere* $K = \mathbb{Q}(\sqrt{m})$ *um corpo quadrático. Seja* $\alpha = r + s\sqrt{m}(r, s \in \mathbb{Q})$ *um elemento qualquer de* $K = \mathbb{Q}(\sqrt{m})$*. Temos que,*

$$\alpha^2 = r^2 + 2rs\sqrt{m} + s^2m = r^2 + s^2m + 2rs\sqrt{m}$$

(i)

$$(\alpha - r)^2 = s^2m \Rightarrow \alpha^2 - 2r\alpha + r^2 = s^2m \Rightarrow \alpha^2 - 2r\alpha + r^2 - s^2m = 0 \Rightarrow$$

$$\Rightarrow X^2 - 2rX + r^2 - s^2m \text{ é o polinômio minimal de } \alpha \text{ sobre } \mathbb{Q}.$$

(ii)

$$\begin{aligned} & \left(\alpha^2 - (r^2 + s^2m)\right)^2 = 4r^2s^2m \Rightarrow \\ \Rightarrow \quad & (\alpha^2)^2 - 2 \cdot (r^2 + s^2m)\alpha^2 + (r^2 + s^2m)^2 = 4r^2s^2m \Rightarrow \\ \Rightarrow \quad & (\alpha^2)^2 - 2(r^2 + s^2m)\alpha^2 + (r^2 + s^2m)^2 - 4r^2s^2m = 0 \Rightarrow \\ \Rightarrow \quad & X^2 - 2(r^2 + s^2m)X + (r^2 + s^2m)^2 - 4r^2s^2m \end{aligned}$$

é o polinômio minimal de α^2 *sobre* $\mathbb{Q}$*.*

Logo,

$$Tr(\alpha) = 2r \quad e \quad Tr(\alpha^2) = 2(r^2 + s^2m).$$

E daí,

$$\begin{aligned} D_{K|\mathbb{Q}}(1, \alpha) &= \det \begin{bmatrix} Tr(1) & Tr(\alpha) \\ Tr(\alpha) & Tr(\alpha^2) \end{bmatrix} = \det \begin{bmatrix} 2 \cdot 1 & 2r \\ 2r & 2(r^2 + s^2m) \end{bmatrix} \\ &= 4r^2 + 4s^2m - 4r^2 = 4s^2m. \end{aligned}$$

Em particular, $D_{K|\mathbb{Q}}(1, \sqrt{m}) = 4m$ *e* $D_{K|\mathbb{Q}}\left(1, \frac{1+\sqrt{m}}{2}\right) = m$. *Como* $1, \sqrt{m}$ *(respectivamente* $1, \frac{1+\sqrt{m}}{2}$*) formam uma base integral de* $K = \mathbb{Q}(\sqrt{m})$ *no caso em que* $m \equiv 2$ *ou* $3 (\mathrm{mod}\ 4)$ *(respectivamente* $\equiv 1$*)* $\mathrm{mod}\ 4$ *então concluímos que o discriminante* d *de* $\mathbb{Q}(\sqrt{m})$ *é dado por,*

$$d = \begin{cases} 4m, & \text{se } m \equiv 2 \text{ ou } 3 (\mathrm{mod}\ 4) \\ m, & \text{se } \quad m \equiv 1 (\mathrm{mod}\ 4). \end{cases}$$

Sejam A um anel de integridade e K seu corpo de frações. Se chama ideal fracionário de A (ou de K respeito a A) a todo sub - A - módulo I de K tal que existe $0 \neq d \in A$ que verifique $I \subset d^{-1}A$. Isto equivale a dizer que os elementos de I tem um "denominador comum" $d \in A$.

Exemplo 1.4 *Os ideais fracionários de* $\mathbb{Z}$ *são da forma* $r\mathbb{Z}$ *onde* $0 \neq r \in \mathbb{Q}$.

Os ideais fracionários (com $d = 1$) são chamados de ideais ordinários (ou inteiros) de A.
Os ideais fracionários não - nulos de A formam um monóide (isto é, um semigrupo com unidade) comutativo para a multiplicação.

Teorema 1.6 *Sejam* A *um anel e* M *um* A *- módulo. As condições seguintes são equivalentes:*

- **(a)** *Toda família não vazia de submódulos de* M *contém um elemento maximal (sob a relação de inclusão).*
- **(b)** *Toda sequência crescente* $(M_n)_{n \geq 0}$ *(para a relação de inclusão) de submódulos de* M *é estacionária (isto é, existe* n_o *tal que* $M_n = M_{n_o}$ *para todo* $n \geq n_o$*).*
- **(c)** *Todo submódulo de* M *é de tipo finito.*

Demonstração: Ver [10], página 20.

Definição 1.7 *Um A - módulo M é chamado noetheriano se satisfaz as condições equivalentes do Teorema 1.6. Um anel A é chamado noetheriano se considerado como A - módulo é um módulo noetheriano.*

Definição 1.8 *Um anel A é chamado anel de Dedekind se é noetheriano, integralmente fechado (portanto, de integridade) e se todo ideal primo não - nulo de A é maximal.*

Exemplo 1.5 *$\mathbb{Z}$ é um anel de Dedekind.*

Teorema 1.7 *Sejam A um anel de Dedekind, K seu corpo de frações, L uma extensão de grau finito de K e A' o fecho integral de A em L. Supõe-se K de característica 0. Então A' é um anel de Dedekind e um A - módulo de tipo finito.*

Demonstração: Ver [10], página 49.

Do Teorema 1.7, concluímos que o anel dos inteiros de um corpo numérico é um anel de Dedekind.

Corolário 1.4 *Sejam A um anel integralmente fechado, K seu corpo de frações, L uma extensão de grau finito de K e x um elemento de L inteiro sobre A. Supõe-se K de característica 0. Então, os coeficientes do polinômio característico de x com respeito a L e K, em particular $Tr_{L/K}(x)$ e $N_{L/K}(x)$ são elementos de A.*

Demonstração: Ver [10], página 38.

1.5 Norma de um Ideal

Proposição 1.4 *Sejam K um corpo numérico, n seu grau e A o anel dos inteiros de K . Se x é um elemento não - nulo de A então $|N(x)| = Card(A/Ax)$.*

Demonstração: Ver [10], página 52.

Observação 1.3 *Como $x \in A$ então $N(x) \in \mathbb{Z}$ (Corolário 1.4). De modo que, a fórmula escrita tem sentido.*

Observação 1.4 *Escrevemos $N(x)$ no lugar de $N_{K/\mathbb{Q}}(x)$ para designar a norma do elemento x.*

Definição 1.9 *Sejam K um corpo numérico e A o anel dos inteiros de K. Dado um ideal inteiro não - nulo I de A, se chama norma de I, e se escreve $N(I)$, o número Card(A/I).*

$$N(I) = \text{Card}(A/I).$$

Notemos que, $N(I)$ é finito. Com efeito, se a é um elemento não - nulo de I então $Aa \subset I$, e A/I se identifica a um quociente de A/Aa, donde, Card$(A/I) \leq$ Card(A/Aa), que é finito pela Proposição 1.4. Por outro lado, isto mostra que para um ideal principal Ab, tem-se $N(Ab) = |N(b)|$.

Proposição 1.5 *Sejam K um corpo numérico e A o anel dos inteiros de K. Se I e J são dois ideais inteiros não - nulos de A então $N(IJ) = N(I) \cdot N(J)$.*

Demonstração: Ver [10], página 52.

Proposição 1.6 *Sejam d o discriminante absoluto de K, A seu anel de inteiros, e I um ideal inteiro não - nulo de A. Então, $\sigma(A)$ e $\sigma(I)$ são redes e tem-se que:*

$$v(\sigma(A)) = 2^{-r_2} \cdot |d|^{\frac{1}{2}} \quad \textit{e} \quad v(\sigma(I)) = 2^{-r_2} \cdot |d|^{\frac{1}{2}} \cdot N(I).$$

Demonstração: Temos que A e I são $\mathbb{Z}$ - módulos livres de dimensão n. Assim, podemos aplicar a Proposição 1.3. Por outro lado, se $(x_i)_{1 \leq i \leq n}$ é uma $\mathbb{Z}$ - base de A, então, $d = D(x_1, \ldots, x_n)$. Como, $(x_i)_{1 \leq i \leq n}$ é $\mathbb{Z}$ - base de A, então, $(x_i)_{1 \leq i \leq n}$

são L.I. sobre $\mathbb{Z}$, logo $(x_i)_{1\leq i\leq n}$ são L. I. sobre $\mathbb{Q}$. Assim, $(x_i)_{1\leq i\leq n}$ é uma base de K sobre $\mathbb{Q}$, logo, pela Proposição 1.2, $D(x_1,\ldots,x_n) = \det(\sigma_i(x_j))^2$. Então, temos que,

$$\begin{aligned} d &= D(x_1,\ldots,x_n) = \det(\sigma_i(x_j))^2 = \det(\sigma_i(x_j)\cdot\sigma_i(x_j)) = \\ &= \det(\sigma_i(x_j))\cdot\det(\sigma_i(x_j)) \Rightarrow \\ \Rightarrow |d| &= |\det(\sigma_i(x_j))|\cdot|\det(\sigma_i(x_j))| = |\det(\sigma_i(x_j))|^2 \\ \Rightarrow |d|^{\frac{1}{2}} &= |\det(\sigma_i(x_j))|. \end{aligned}$$

Usando agora a Proposição 1.3 , temos que, $\sigma(A)$ e $\sigma(I)$ são redes de $\mathbb{R}^n$. E além disso,

$$v(\sigma(A)) = 2^{-r_2}\cdot|\det(\sigma_i(x_j))| = 2^{-r_2}\cdot|d|^{\frac{1}{2}}.$$

Para deduzir a fórmula do volume da rede $\sigma(I)$, basta usar a fórmula do volume da rede $\sigma(A)$, notar que $\sigma(I)$ é um subgrupo de índice $N(I)$ de $\sigma(A)$, e que portanto se obtém um domínio fundamental P para a rede $\sigma(I)$ pela reunião disjunta de $N(I)$ domínios fundamentais $(P_1,\ldots,P_{N(I)})$ para a rede $\sigma(A)$. Temos então que,

$$\begin{aligned} v(\sigma(I)) &= \mu(P) = \mu(P_1)+\ldots+\mu(P_{N(I)}) = \underbrace{v(\sigma(A))+\ldots+v(\sigma(A))}_{N(I)\text{parcelas}} = \\ &= N(I)\cdot v(\sigma(A)) = N(I)\cdot 2^{-r_2}\cdot|d|^{\frac{1}{2}} = 2^{-r_2}\cdot|d|^{\frac{1}{2}}\cdot N(I). \end{aligned}$$

■

1.6 Finitude do grupo das classes de ideais

Proposição 1.7 *Sejam K um corpo numérico, n seu grau, r_1 e r_2 os inteiros definidos anteriormente, d seu discriminante absoluto e I um ideal inteiro não-nulo de K. Então, I contém um elemento não-nulo x tal que,*

$$\left|N_{K/\mathbb{Q}}(x)\right| \leq \left(\frac{4}{\pi}\right)^{r_2}\cdot\frac{n!}{n^n}\cdot|d|^{\frac{1}{2}}\cdot N(I).$$

Demonstração: Seja σ a imersão canônica de K em $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Sejam t um número real positivo e B_t o conjunto dos $(y_1, \ldots, y_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, tais que, $\sum_{i=1}^{r_1} |y_i| + 2 \cdot \sum_{j=1}^{r_2} |z_j| \leq t$. Então, B_t é um conjunto compacto, convexo e simétrico com respeito a 0 e cujo volume é dado por, $\mu(B_t) = 2^{r_1} \cdot \left(\frac{\pi}{2}\right)^{r_2} \cdot \frac{t^n}{n!}$. Escolhamos t tal que, $\mu(B_t) = 2^n \cdot v\left(\sigma(I)\right)$, isto é, tal que

$$2^{r_1} \cdot \left(\frac{\pi}{2}\right)^{r_2} \cdot \frac{t^n}{n!} = 2^{n-r_2} \cdot |d|^{\frac{1}{2}} \cdot N(I),$$

ou seja, tal que, $t^n = 2^{n-r_1} \cdot \pi^{-r_2} \cdot n! \cdot |d|^{\frac{1}{2}} \cdot N(I)$. Por outro lado, como B_t é compacto e $\mu(B_t) = 2^n \cdot v\left(\sigma(I)\right)$ então pelo item (b) do Corolário 1.1, temos que, $\exists 0 \neq y \in B_t \cap \sigma(I)$, ou seja, $\exists 0 \neq x \in I$ tal que $\sigma(x) = y \in B_t$. Calculemos sua norma,

$$\begin{aligned}
N(x) &= \sigma_1(x) \cdot \ldots \cdot \sigma_{r_1}(x) \cdot \sigma_{r_1+1}(x) \cdot \overline{\sigma}_{r_1+1}(x) \cdot \ldots \cdot \sigma_{r_1+r_2}(x) \cdot \overline{\sigma}_{r_1+r_2}(x) \\
|N(x)| &= |\sigma_1(x)| \cdot \ldots \cdot |\sigma_{r_1}(x)| \cdot |\sigma_{r_1+1}(x)| \cdot |\overline{\sigma}_{r_1+1}(x)| \cdot \ldots \\
&\quad \ldots \cdot |\sigma_{r_1+r_2}(x)| \cdot |\overline{\sigma}_{r_1+r_2}(x)| \\
|N(x)| &= |\sigma_1(x)| \cdot \ldots \cdot |\sigma_{r_1}(x)| \cdot |\sigma_{r_1+1}(x)|^2 \cdot \ldots \cdot |\sigma_{r_1+r_2}(x)|^2
\end{aligned}$$

Usando agora a desigualdade entre as médias aritmética e geométrica, temos que,

$$
\begin{aligned}
& \sqrt[n]{|\sigma_1(x)| \cdot \ldots \cdot |\sigma_{r_1}(x)| \cdot |\sigma_{r_1+1}(x)| \cdot |\overline{\sigma}_{r_1+1}(x)| \cdot \ldots \cdot |\sigma_{r_1+r_2}(x)| \cdot |\overline{\sigma}_{r_1+r_2}(x)|} \leq \\
\leq \; & \frac{|\sigma_1(x)| + \ldots + |\sigma_{r_1}(x)| + |\sigma_{r_1+1}(x)| + |\overline{\sigma}_{r_1+1}(x)| + \ldots + |\sigma_{r_1+r_2}(x)| + |\overline{\sigma}_{r_1+r_2}(x)|}{n} \\
\Rightarrow \; & |\sigma_1(x)| \cdot \ldots \cdot |\sigma_{r_1}(x)| \cdot |\sigma_{r_1+1}(x)|^2 \cdot \ldots \cdot |\sigma_{r_1+r_2}(x)|^2 \leq \\
\leq \; & \frac{(|\sigma_1(x)| + \ldots + |\sigma_{r_1}(x)| + 2 \cdot |\sigma_{r_1+1}(x)| + \ldots + 2 \cdot |\sigma_{r_1+r_2}(x)|)^n}{n^n} \Rightarrow \\
\Rightarrow \; & n^n \cdot \left(|\sigma_1(x)| \cdot \ldots \cdot |\sigma_{r_1}(x)| \cdot |\sigma_{r_1+1}(x)|^2 \cdot \ldots \cdot |\sigma_{r_1+r_2}(x)|^2\right) \leq \\
\leq \; & (|\sigma_1(x)| + \ldots + |\sigma_{r_1}(x)| + 2 \cdot (|\sigma_{r_1+1}(x)| + \ldots + \cdot |\sigma_{r_1+r_2}(x)|))^n = \\
= \; & \left(\sum_{i=1}^{r_1} |\sigma_i(x)| + 2 \cdot \sum_{j=r_1+1}^{r_1+r_2} |\sigma_j(x)|\right)^n \underbrace{\leq}_{\sigma(x) \in B_t} t^n \Rightarrow n^n \cdot |N(x)| \leq t^n \Rightarrow \\
\Rightarrow \; & |N(x)| \leq \frac{t^n}{n^n} = 2^{n-r_1} \cdot \pi^{-r_2} \cdot n! \cdot |d|^{\frac{1}{2}} \cdot N(I) \cdot \frac{1}{n^n} = \\
& = 2^{n-r_1} \cdot \pi^{-r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}} \cdot N(I) = \\
= \; & 2^{2r_2} \cdot \pi^{-r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}} \cdot N(I) = \frac{(2^2)^{r_2}}{\pi^{r_2}} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}} \cdot N(I) = \\
= \; & \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}} \cdot N(I) \Rightarrow |N(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}} \cdot N(I).
\end{aligned}
$$

■

Teorema 1.8 *Sejam A um anel de Dedekind e P o conjunto dos ideais primos não-nulos de A. Então:*

(a) *Todo ideal fracionário não-nulo B de A pode ser unicamente expresso na forma $B = \prod_{J \in P} J^{n_J(B)}$, onde, para qualquer $J \in P$, $n_J(B) \in \mathbb{Z}$ e, para quase todo $J \in P$, $n_J(B) = 0$.*

(b) *O monóide dos ideais fracionários não-nulos de A é um grupo.*

Demonstração: Ver [10], página 50.

Observação 1.5 *$n_J(B)$ designa o expoente de J na decomposição de B em produto de ideais primos.*

Observação 1.6 **(i)** $n_J(BB') = n_J(B) + n_J(B')$.

(ii) $B \subset A \Leftrightarrow n_J(B) \geq 0$ *para todo* $J \in P$.

(iii) $B \subset B' \Leftrightarrow n_J(B) \geq n_J(B')$ *para todo* $J \in P$.

Nota 1.1 *Temos que o monóide $I(A)$ dos ideais fracionários não-nulos de um anel de Dedekind é um grupo. Os ideais fracionários principais (isto é, da forma $Ax, x \in K^*$) formam um subgrupo $F(A)$ de $I(A)$ (pois, $(Ax)\cdot(Ay)^{-1} = Axy^{-1}$). Por outro lado, o grupo $I(A)$ é abeliano. Com efeito, sejam I, J ideais fracionários não nulos de A. Então, existem $0 \neq d, g \in A$ tais que $I \subset d^{-1}A$ e $J \subset g^{-1}A$. Note agora que,*

$$x \in IJ \Leftrightarrow x = \frac{a_1}{d}\cdot\frac{b_1}{g} + \ldots + \frac{a_n}{d}\cdot\frac{b_n}{g} = \frac{b_1}{g}\cdot\frac{a_1}{d} + \ldots + \frac{b_n}{g}\cdot\frac{a_n}{d} \in IJ$$

onde $a_i, b_i \in A$.
Ou seja,

$$IJ = JI.$$

Como $I(A)$ é abeliano então $F(A)$ é um subgrupo normal de $I(A)$. O grupo quociente $C(A) = I(A)/F(A)$ se chama o grupo das classes de ideais de A.

Observação 1.7 *Sejam K um corpo numérico e A o anel dos inteiros de K. Temos que A é um anel de Dedekind, então, podemos definir o grupo quociente $C(A) = I(A)/F(A)$, que é neste caso chamado, grupo das classes de ideais de K.*

Observação 1.8 *$J^{-1} = \{x \in K' | xJ \subset A\}$, onde, A é o anel dos inteiros de K e K' é o corpo de frações de A.*

Observação 1.9 *Sejam I e J dois ideais fracionários do anel A dos inteiros de K e K' o corpo de frações de A. Então, I e J pertencem a mesma classe de ideais de $K \Leftrightarrow \exists \gamma \in K'$ tal que $I = \gamma J$.*

Corolário 1.5 *Com as mesmas notações, toda classe de ideais de K contém um ideal inteiro I tal que,*

$$N(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}}.$$

Demonstração: Seja J' um ideal da classe dada. Por homotetia podemos supor que $J = J'^{-1}$ é um ideal inteiro. Então, pela Proposição 1.7, existe um elemento não-nulo x de J, tal que,

$$|N(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}} \cdot N(J).$$

E daí, temos que, $I = xJ^{-1}$ é um ideal inteiro da classe dada. De fato,

$$x \in J \subset A \Rightarrow x \in A \Rightarrow x \in K' \quad (\text{corpo de frações de} \quad A)$$

$$\begin{aligned} z \in I \quad &\Rightarrow \quad z \in xJ^{-1} \Rightarrow z = xy, y \in J^{-1} \Rightarrow z = xy, yJ \subset A \\ &\underbrace{\Rightarrow}_{x,y \in K'} \quad z = yx, yJ \subset A \Rightarrow z \in A \therefore I \subset A \end{aligned}$$

Temos então que,

$$\begin{aligned} I = xJ^{-1} \quad &\Rightarrow \quad x = J \cdot I \Rightarrow N(x) = N(J \cdot I) \underbrace{=}_{Prop.1.5} N(J) \cdot N(I) \Rightarrow \\ &\Rightarrow \quad N(I) = \frac{N(x)}{N(J)} \Rightarrow |N(I)| = \frac{|N(x)|}{|N(J)|} \leq \\ &\qquad \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}} \cdot N(J) \cdot \frac{1}{N(J)} = \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}} \\ &\Rightarrow \quad N(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}}. \end{aligned}$$

■

Corolário 1.6 *Sejam K um corpo numérico, n seu grau e d seu discriminante absoluto. Então, para $n \geq 2$ temos que $|d| \geq \frac{\pi}{3} \cdot \left(\frac{3\pi}{4}\right)^{n-1}$ e $\frac{n}{\log|d|}$ está limitado por uma constante independente de K.*

Demonstração: Temos que, $1 \leq N(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}}$, logo,

$$\left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}} \geq 1 \Rightarrow |d|^{\frac{1}{2}} \geq \left(\frac{\pi}{4}\right)^{r_2} \cdot \frac{n^n}{n!} \Rightarrow |d| \geq \left(\frac{\pi}{4}\right)^{2r_2} \cdot \frac{n^{2n}}{(n!)^2}.$$

Como $0 < \frac{\pi}{4} < 1$ e $2r_2 \leq n$ então,

$$\left(\frac{\pi}{4}\right)^{2r_2} \geq \left(\frac{\pi}{4}\right)^{n} \Rightarrow \left(\frac{\pi}{4}\right)^{2r_2} \cdot \frac{n^{2n}}{(n!)^2} \geq \left(\frac{\pi}{4}\right)^{n} \cdot \frac{n^{2n}}{(n!)^2}.$$

Logo,

$$|d| \geq \left(\frac{\pi}{4}\right)^{n} \cdot \frac{n^{2n}}{(n!)^2},$$

ou seja, $|d| \geq a_n (\forall n \in \mathbb{N})$ onde $a_n = \left(\frac{\pi}{4}\right)^{n} \cdot \frac{n^{2n}}{(n!)^2}$. Temos então que,

$$a_2 = \left(\frac{\pi}{4}\right)^{2} \cdot \frac{2^4}{2^2} = \frac{\pi^2}{2^4} \cdot 2^2 = \frac{\pi^2}{2^2} = \frac{\pi^2}{4}$$

e

$$\begin{aligned} \frac{a_{n+1}}{a_n} &= \frac{\left(\frac{\pi}{4}\right)^{n+1} \cdot \frac{(n+1)^{2n+2}}{[(n+1)!]^2}}{\left(\frac{\pi}{4}\right)^{n} \cdot \frac{n^{2n}}{(n!)^2}} = \frac{\left(\frac{\pi}{4}\right)^{n} \cdot \frac{\pi}{4} \cdot \frac{(n+1)^{2n} \cdot (n+1)^2}{(n+1)^2 \cdot (n!)^2}}{\left(\frac{\pi}{4}\right)^{n} \cdot \frac{n^{2n}}{(n!)^2}} \\ &= \frac{\pi}{4} \cdot \frac{(n+1)^{2n}}{n^{2n}} = \frac{\pi}{4} \cdot \left(\frac{n+1}{n}\right)^{2n} = \frac{\pi}{4} \cdot \left(1 + \frac{1}{n}\right)^{2n}. \end{aligned}$$

Usando agora a fórmula do binômio de Newton, concluímos que,

$$\left(1 + \frac{1}{n}\right)^{2n} = 1 + 2 + \text{termos positivos.}$$

Assim,

$$\frac{a_{n+1}}{a_n} = \frac{\pi}{4} \cdot (1 + 2 + \text{termos positivos}) \geq \frac{3\pi}{4}.$$

Afirmação: $a_n \geq \frac{\pi^2}{4} \cdot \left(\frac{3\pi}{4}\right)^{n-2}$, $\forall n \geq 2$.

De fato, para $n = 2$ teríamos que $a_2 \geq \frac{\pi^2}{4}$ (o que é verdade). Suponha que a desigualdade acima seja verdadeira para um certo $n = k \geq 2$, ou seja, $a_k \geq \frac{\pi^2}{4} \cdot \left(\frac{3\pi}{4}\right)^{k-2}$. Então, para $n = k + 1$, temos que,

$$a_{k+1} \geq \frac{3\pi}{4} \cdot a_k = \frac{3\pi}{4} \cdot \frac{\pi^2}{4} \cdot \left(\frac{3\pi}{4}\right)^{k-2} = \frac{\pi^2}{4} \cdot \left(\frac{3\pi}{4}\right)^{k+1-2}.$$

Logo, para $n \geq 2$, temos que,

$$|d| \geq a_n \geq \frac{\pi^2}{4} \cdot \left(\frac{3\pi}{4}\right)^{n-2} \Rightarrow |d| \geq \frac{\pi^2}{4} \cdot \left(\frac{3\pi}{4}\right)^{n-2}.$$

Mas, note que,

$$\frac{\pi^2}{4} \cdot \left(\frac{3\pi}{4}\right)^{n-2} = \frac{\pi^2}{4} \cdot \left(\frac{3\pi}{4}\right)^{n-1} \cdot \left(\frac{3\pi}{4}\right)^{-1} = \pi \cdot \frac{\pi}{4} \cdot \left(\frac{3\pi}{4}\right)^{n-1} \cdot \frac{4}{3\pi} = \frac{\pi}{3} \cdot \left(\frac{3\pi}{4}\right)^{n-1}.$$

Portanto,

$$|d| \geq \frac{\pi}{3} \cdot \left(\frac{3\pi}{4}\right)^{n-1}, \forall n \geq 2.$$

A limitação uniforme de $\frac{n}{\log|d|}$ se obtém tomando logaritmos.

■

Teorema 1.9 (Hermite - Minkowski) *Para todo corpo numérico $K \neq \mathbb{Q}$, o discriminante absoluto d de K é $\neq \pm 1$.*

Demonstração: Como $K \neq \mathbb{Q}$ então $[K : \mathbb{Q}] \neq 1$. Consequentemente, $[K : \mathbb{Q}] \geq 2$. Assim pelo Corolário 1.6, temos que, $|d| \geq \frac{\pi}{3} \cdot \left(\frac{3\pi}{4}\right)^{n-1}$. Mas, note que, $\frac{\pi}{4} > 1$ e $\frac{3\pi}{4} > 1$. Logo, $|d| > 1$. Portanto, $d \neq \pm 1$.

■

Teorema 1.10 (Dirichlet) *Para todo corpo numérico K, o grupo das classes de ideais de K é finito.*

Demonstração: Seja G o conjunto dos ideais inteiros I de K, cuja norma é um certo $q \in \mathbb{Z}$.

$$G = \{I \subset A | I \text{ é ideal e } N(I) = q\}.$$

Afirmação: G é finito.
De fato, se $I \in G$ então $N(I) = q$. Ou seja, Card$(A/I) = q$. Temos que, A/I é anel quociente, logo, $< A/I, + >$ é grupo abeliano.

$$\begin{aligned} + \quad &: A/I \times A/I \to A/I \\ &(a+I, a'+I) \mapsto (a+I)+(a'+I) = (a+a')+I, \forall a, a' \in A \end{aligned}$$

Note que, $1 \in A$ (pois, $1 \in \mathbb{Q} \subset K$ e 1 é raiz de $P(X) = X - 1 \in \mathbb{Z}[X]$). Logo $1 + I \in A/I$. Assim,

$$\begin{aligned} &(1+I)^{|A/I|} = 0 + I \Rightarrow (1+I)^{\text{CArd}(A/I)} = 0 + I \Rightarrow (1+I)^q = 0 + I \\ &\Rightarrow q + I = I \Rightarrow q + b = b'(b, b' \in I) \Rightarrow q = b' - b \in I \Rightarrow q \in I \end{aligned}$$

Consequentemente, $Aq \subset I$. Então, nossos ideais I estão entre os que contém a Aq. Pelo item (a) do Teorema 1.8 podemos decompor de maneira única os ideais Aq e I como produtos dos ideais primos não-nulos de A. Sejam então, $J_1^{n_{J_1}(Aq)} \cdot \ldots \cdot J_s^{n_{J_s}(Aq)}$ e $J_1^{n_{J_1}(I)} \cdot \ldots \cdot J_s^{n_{J_s}(I)}$ tais decomposições, onde $J_1, \ldots, J_s$ são os ideais primos não-nulos de A. Como $Aq \subset I$ então pela Observação 1.6, $0 \leq n_{J_i}(I) \leq n_{J_i}(Aq)$ para todo $J_i (i = 1, \ldots, s)$. Assim, existe apenas um número finito desses ideais I. Logo, G é finito. E daí, o conjunto dos ideais inteiros

I de K tal que, $N(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}}$ é finito. Mas, pelo Corolário 1.5, toda classe de ideais de K contém, um ideal inteiro I de K tal que,

$$N(I) \leq \left(\frac{4}{\pi}\right)^{r_2} \cdot \frac{n!}{n^n} \cdot |d|^{\frac{1}{2}}.$$

Logo, a quantidade de classes deve ser finita. Portanto, o grupo das classes de ideais de K é finito.

■

Capítulo 2

Anéis de Frações

Definição 2.1 *Seja A um anel de integridade, K seu corpo de frações e S uma parte de A, estável para a multiplicação (isto é, $a \cdot b \in S$ para quaisquer $a, b \in S$), que não contém o "0" e sim o "1". Se chama anel de frações de A respeito a S, e se escreve $S^{-1}A$ ao conjunto dos elementos $\frac{a}{s} \in K$ com $a \in A$ e $s \in S$.*

$$S^{-1}A = \left\{ \frac{a}{s} \in K; a \in A \quad e \quad s \in S \right\}.$$

Observação 2.1 **(a)** *$S^{-1}A$ é um anel comutativo com identidade multiplicativa, pois*

$$\frac{a}{s} + \frac{a'}{s'} = \frac{s'a + a's}{ss'} \in S^{-1}A \quad e \quad \frac{a}{s} \cdot \frac{a'}{s'} = \frac{a \cdot a'}{s \cdot s'} \in S^{-1}A.$$

$\frac{0}{1}$ é a identidade aditiva e $\frac{1}{1}$ é a identidade multiplicativa.

(b) *$S^{-1}A$ contém A, pois $1 \in S$ $\left(a = \frac{a}{1} \in S^{-1}A, \forall a \in A \right)$.*

(c) *Se S é o conjunto dos elementos não nulos de A então $S^{-1}A = K$.*

$$S^{-1}A = (A\backslash\{0\})^{-1} A = \left\{ \frac{a}{s} \in K; a \in A \quad e \quad s \in A\backslash\{0\} \right\} = K.$$

(d) *Se $S = \{1\}$ ou S está formado pelos elementos invertíveis de A (isto é, $S = A^*$) então $S^{-1}A = A$.*

Proposição 2.1 *Sejam A um anel de integridade, S uma parte multiplicativa fechada de A que contém o 1 e não contém o 0, e $A' = S^{-1}A$.*

(1) *Para todo ideal $\mathfrak{b}'$ de A' tem-se $(\mathfrak{b}' \cap A)A' = \mathfrak{b}'$ de modo que $\mathfrak{b}' \mapsto \mathfrak{b}' \cap A$ é uma injeção crescente (para a inclusão) do conjunto de ideais de A' no conjunto de ideais de A.*

(2) *A aplicação $\mathfrak{p}' \mapsto \mathfrak{p}' \cap A$ é um isomorfismo do conjunto ordenado (por inclusão) dos ideais primos de A' sobre o conjunto dos ideais primos $\mathfrak{p}$ de A tais que $\mathfrak{p} \cap S = \emptyset$. A aplicação inversa é $\mathfrak{p} \mapsto \mathfrak{p}A'$.*

Observação 2.2 *$\mathfrak{b}' \cap A$ é um ideal de A , para todo $\mathfrak{b}'$ ideal de $A' = S^{-1}A$.*

Com efeito, sejam $b \in \mathfrak{b}' \cap A$ e $a \in A$. Logo,

$$\left.\begin{array}{lllll} b \in A & e & a \in A & \Rightarrow & ba \in A \\ b \in \mathfrak{b}' & e & a \in A \subset A' & \underbrace{\Rightarrow}_{\mathfrak{b}' \text{ é ideal de } A'} & ba \in \mathfrak{b}' \end{array}\right| \Rightarrow ba \in \mathfrak{b}' \cap A$$

Observação 2.3 *Seja C o conjunto dos ideais de A' e D o conjunto dos ideais de A. Então a aplicação*

$$\begin{array}{rcl} \varphi : C & \to & D \\ \mathfrak{b}' & \mapsto & \mathfrak{b}' \cap A \end{array}$$

está bem definida, isto é, $\varphi(\mathfrak{b}') \in D, \forall \mathfrak{b}' \in C$.

O item (1) nos diz então que para quaisquer $\mathfrak{b}_1, \mathfrak{b}_2 \in C$ tal que $\mathfrak{b}_1 \subset \mathfrak{b}_2$ tem-se $\varphi(\mathfrak{b}_1) \subset \varphi(\mathfrak{b}_2)$ (crescente para a inclusão).

Demonstração (Proposição 2.1):

(1) Seja $\mathfrak{b}'$ um ideal de A'. Temos que $\mathfrak{b}' \cap A \subset \mathfrak{b}'$ logo, $(\mathfrak{b}' \cap A)A' \subset \mathfrak{b}'$ pois $\mathfrak{b}'$ é um ideal de A'. Tome agora,

$$x \in \mathfrak{b}' \Rightarrow x = \frac{a}{s} \quad \text{com} \quad a \in A \quad \text{e} \quad s \in S.$$

Por outro lado,

$$x \in \mathfrak{b}' \quad \text{e} \quad s \in S \subset A \subset A' \underbrace{\Rightarrow}_{\mathfrak{b}' \text{ é um ideal de } A'} xs \in \mathfrak{b}' \Rightarrow \frac{a}{s} \cdot s \in \mathfrak{b}' \Rightarrow a \in \mathfrak{b}'.$$

Assim temos que, $a \in \mathfrak{b}' \cap A$.

E daí,

$$x = a \cdot \underbrace{\frac{1}{s}}_{\in A'} \in (\mathfrak{b}' \cap A)A'.$$

Logo, $\mathfrak{b}' \subset (\mathfrak{b}' \cap A)A'$. Portanto, $(\mathfrak{b}' \cap A)A' = \mathfrak{b}'$ para todo $\mathfrak{b}' \in C$.

Considere agora a aplicação,

$$\begin{aligned} \theta : D &\to C \\ \mathfrak{b} &\mapsto \mathfrak{b}A'. \end{aligned}$$

Afirmação 2.1 *$\mathfrak{b}A'$ é um ideal de A' para todo ideal $\mathfrak{b}$ de A.*

Com efeito, sejam $c \in \mathfrak{b}A'$ e $x \in A'$. Logo,

$$\left.\begin{array}{rl} c = b \cdot \frac{a}{s}; b \in \mathfrak{b}, a \in A & \text{e} \quad s \in S \\ x = \frac{t}{r}, t \in A & \text{e} \quad r \in S \end{array}\right| \Rightarrow cx = b \cdot \frac{a}{s} \cdot \frac{t}{r} = b \cdot \frac{\overbrace{at}^{\in A}}{\underbrace{sr}_{\in S}} \Rightarrow cx \in \mathfrak{b}A'$$

Com isso, θ está bem definida, isto é, $\theta(\mathfrak{b}) \in C, \forall \mathfrak{b} \in D$. E daí, a aplicação $\theta \circ \varphi : C \to C$ é a identidade. Com efeito,

$$(\theta \circ \varphi)(\mathfrak{b}') = \theta(\theta(\mathfrak{b}')) = \theta(\mathfrak{b}' \cap A) = (\mathfrak{b}' \cap A)A' = \mathfrak{b}', \forall \mathfrak{b}' \in C.$$

Afirmação 2.2 *φ é injetiva.*

Com efeito,

$$\varphi(\mathfrak{b}_1) = \varphi(\mathfrak{b}_2) \Rightarrow \theta(\varphi(\mathfrak{b}_1)) = \theta(\varphi(\mathfrak{b}_2)) \Rightarrow (\theta \circ \varphi)(\mathfrak{b}_1) = (\theta \circ \varphi)(\mathfrak{b}_2) \underbrace{\Rightarrow}_{\theta \circ \varphi = \text{id}} \mathfrak{b}_1 = \mathfrak{b}_2.$$

E além disso, φ é crescente para a inclusão, isto é, $\mathfrak{b}_1 \subset \mathfrak{b}_2 \Rightarrow \varphi(\mathfrak{b}_1) \subset \varphi(\mathfrak{b}_2)$. Com efeito,

$$\mathfrak{b}_1 \subset \mathfrak{b}_2 \Rightarrow \mathfrak{b}_1 \cap A \subset \mathfrak{b}_2 \cap A \Rightarrow \varphi(\mathfrak{b}_1) \subset \varphi(\mathfrak{b}_2).$$

(2) C': conjunto dos ideais primos de A'.

D': conjunto dos ideais primos $\mathfrak{p}$ de A tais que $\mathfrak{p} \cap S = \emptyset$.

Afirmação 2.3 *A aplicação*

$$\begin{aligned} \phi : C' &\to D' \\ \mathfrak{p}' &\mapsto \mathfrak{p}' \cap A \end{aligned}$$

é um isomorfismo (no sentido bijetivo) e crescente para a inclusão.

Vejamos isso:

Seja $\mathfrak{p}'$ um ideal primo de $A' = S^{-1}A$.

Afirmação 2.4 $\mathfrak{p} = \mathfrak{p}' \cap A$ *é um ideal primo de* A.

Com efeito, $\mathfrak{p}' \cap A \neq A$, caso contrário,

- $1 \in A = \mathfrak{p}' \cap A \Rightarrow 1 \in \mathfrak{p}' \Rightarrow \dfrac{1}{1} \in \mathfrak{p}' \Rightarrow \mathfrak{p}' = A'$ (CONTRADIÇÃO)
- Sejam $x, y \in A$ tais que $xy \in \mathfrak{p}' \cap A$.

$xy \in \mathfrak{p}' \cap A \Rightarrow xy \in \mathfrak{p}' \Rightarrow x \in \mathfrak{p}'$ ou $y \in \mathfrak{p}' \Rightarrow x \in \mathfrak{p}' \cap A$ ou $y \in \mathfrak{p}' \cap A$.

E além disso, $\mathfrak{p} \cap S = \emptyset$. Caso contrário, teríamos:

$s \in \mathfrak{p} \cap S \Rightarrow s \in \mathfrak{p}'$ e $s \in S \Rightarrow$

$$\Rightarrow 1 = \frac{1}{s} \cdot s \in A'\mathfrak{p}' \underbrace{=}_{(2.1) \text{ e } (2.2) \text{ abaixo}} \mathfrak{p}' \Rightarrow \mathfrak{p}' = A' \text{ (CONTRADIÇÃO)}$$

$$x \in A'\mathfrak{p}' \Rightarrow x = a_1p_1 + \ldots + a_np_n, a_i \in A' \text{ e } p_i \in \mathfrak{p}' \underbrace{\Rightarrow}_{\mathfrak{p}' \text{ é ideal de } A'} x \in \mathfrak{p}' \quad (2.1)$$

$$x \in \mathfrak{p}' \Rightarrow x = \frac{p}{s}, \quad \text{com} \quad p \in A \text{ e } s \in S \Rightarrow x = \frac{p}{s} = \frac{1}{1} \cdot \frac{p}{s} \in A'\mathfrak{p}'. \quad (2.2)$$

Ou seja, para todo ideal primo $\mathfrak{p}'$ de A' tem-se que $\mathfrak{p} = \mathfrak{p}' \cap A$ é um ideal primo de A tal que $\mathfrak{p} \cap S = \emptyset$.

Inversamente, seja $\mathfrak{p}$ um ideal primo de A tal que $\mathfrak{p} \cap S = \emptyset$. Vamos demonstrar que, $\mathfrak{p}A'$ é um ideal primo de A' e que $\mathfrak{p}A' \cap A = \mathfrak{p}$.

Note primeiro que $\mathfrak{p}A'$ é o conjunto dos $\frac{p}{s}$ com $p \in \mathfrak{p}$ e $s \in S$.

$$\mathfrak{p}A' = \left\{ \frac{p}{s}; p \in \mathfrak{p} \quad \text{e} \quad s \in S \right\}.$$

Com efeito,

- $\frac{p}{s} = p \cdot \frac{1}{s} \in \mathfrak{p}A', \forall p \in \mathfrak{p} \quad \text{e} \quad s \in S \Rightarrow \left\{ \frac{p}{s}; p \in \mathfrak{p} \quad \text{e} \quad s \in S \right\} \subset \mathfrak{p}A'$
- $x \in \mathfrak{p}A' \Rightarrow x = p_1\frac{a_1}{s_1} + \ldots + p_n\frac{a_n}{s_n} =$
  $= p_1\frac{\overbrace{b_1a_1}^{\in A}}{s} + p_2\frac{\overbrace{b_2a_2}^{\in A}}{s} + \ldots + p_n\frac{\overbrace{b_na_n}^{\in A}}{s}, \text{ com } b_i \in S \text{ e } s \in S \Rightarrow$
  $\underbrace{\Rightarrow}_{\mathfrak{p} \text{ é ideal de } A} x = \frac{\overbrace{p_1b_1a_1}^{\in \mathfrak{p}} + \overbrace{p_2b_2a_2}^{\in \mathfrak{p}} + \ldots + \overbrace{p_nb_na_n}^{\in \mathfrak{p}}}{s} \in \left\{ \frac{p}{s}; p \in \mathfrak{p} \quad \text{e} \quad s \in S \right\}.$

Afirmação 2.5 $1 \notin \mathfrak{p}A'$

Com efeito,

$$1 \in \mathfrak{p}A' \Rightarrow 1 = \frac{p}{s}, \quad \text{para algum} \quad p \in \mathfrak{p} \quad \text{e para algum} \quad s \in S$$
$$\Rightarrow \underbrace{p}_{\in \mathfrak{p}} = s \in S \Rightarrow \mathfrak{p} \cap S \neq \emptyset. (\text{CONTRADIÇÃO})$$

Como $1 \notin \mathfrak{p}A'$ então $\mathfrak{p}A' \neq A'$. Demonstraremos que $\mathfrak{p}A'$ é um ideal (já justificado em (1)) primo de A'. Sejam $\frac{a}{s} \in A'$ e $\frac{b}{t} \in A'$ tais que, $\frac{a}{s} \cdot \frac{b}{t} \in \mathfrak{p}A'$, logo, $\frac{a}{s} \cdot \frac{b}{t} = \frac{p}{u}$ com $p \in \mathfrak{p}$ e $u \in S$, donde $abu = p\underbrace{ts}_{\in S} \in \mathfrak{p}$. Como $\mathfrak{p} \cap S = \emptyset$ e $u \in S$ então $u \notin \mathfrak{p}$. Mas, $abu \in \mathfrak{p}$ e $\mathfrak{p}$ é um ideal primo de A, logo $ab \in \mathfrak{p}$. E daí, pelo mesmo motivo, $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$.

Consequentemente, $\frac{a}{s} \in \mathfrak{p}A'$ ou $\frac{b}{t} \in \mathfrak{p}A'$. Portanto, $\mathfrak{p}A'$ é um ideal primo de A'. Demonstraremos finalmente que, $\mathfrak{p} = \mathfrak{p}A' \cap A$.

- $x \in \mathfrak{p} \Rightarrow x = p \in \mathfrak{p} \Rightarrow \left\{ \begin{array}{c} x = p = p \cdot \frac{1}{1} \in \mathfrak{p}A' \\ x \in \mathfrak{p} \subset A \end{array} \right| \Rightarrow x \in \mathfrak{p}A' \cap A$

- $x \in \mathfrak{p}A' \cap A \Rightarrow x \in \mathfrak{p}A' \Rightarrow x = \frac{p}{s} \, (p \in \mathfrak{p} \quad \text{e} \quad s \in S) \Rightarrow sx = p \in \mathfrak{p}$

Como $\mathfrak{p} \cap S = \emptyset$ e $s \in S$ então $s \notin \mathfrak{p}$. Mas, $\mathfrak{p}$ é ideal primo de A e $sx \in \mathfrak{p}$, logo, $x \in \mathfrak{p}$.

As fórmulas, $\mathfrak{p}' = (\mathfrak{p}' \cap A)A'$ para todo ideal $\mathfrak{p}'$ de A' (vimos em (1)) e $\mathfrak{p} = \mathfrak{p}A' \cap A$ para todo ideal primo de A mostram que a aplicação

$$\begin{array}{rcl} \phi : C' & \to & D' \\ \mathfrak{p}' & \mapsto & \mathfrak{p}' \cap A \end{array}$$

é um bijeção, cuja inversa é

$$\begin{array}{rcl} \beta : D' & \to & C' \\ \mathfrak{p} & \mapsto & \mathfrak{p}A'. \end{array}$$

Com efeito,

$$(\phi \circ \beta)(\mathfrak{p}) = \phi(\beta(\mathfrak{p})) = \phi(\mathfrak{p}A') = \mathfrak{p}A' \cap A = \mathfrak{p}.$$

$$(\beta \circ \phi)(\mathfrak{p}') = \beta(\phi(\mathfrak{p}')) = \beta(\mathfrak{p}' \cap A) = (\mathfrak{p}' \cap A) \cap A' = \mathfrak{p}'.$$

Além disso, ϕ e β são trivialmente crescentes para a inclusão.

- $\mathfrak{p}_1, \mathfrak{p}_2 \in C'$

$\mathfrak{p}_1 \subset \mathfrak{p}_2 \Rightarrow \mathfrak{p}_1 \cap A \subset \mathfrak{p}_2 \cap A \Rightarrow \phi(\mathfrak{p}_1) \subset \phi(\mathfrak{p}_2)$

- $\mathfrak{p}_1, \mathfrak{p}_2 \in D'$

$\mathfrak{p}_1 \subset \mathfrak{p}_2 \Rightarrow \mathfrak{p}_1 A' \subset \mathfrak{p}_2 A' \Rightarrow \beta(\mathfrak{p}_1) \subset \beta(\mathfrak{p}_2)$.

■

Corolário 2.1 *Se A é um anel noetheriano de integridade então todo anel de frações $S^{-1}A$ é noetheriano.*

Observação 2.4 *Como $A' = S^{-1}A$ é um anel, então os ideais de A' são os sub-A'-módulos de A', pois todo ideal de A' é um sub-A'-módulo de A' e todo sub-A'-módulo de A' é um ideal de A'.*

Demonstração (Corolário 2.1): Temos pela Proposição 2.1 (1), que a aplicação

$$\begin{aligned} \phi : C &\rightarrow D \\ \mathfrak{b}' &\mapsto \mathfrak{b}' \cap A \end{aligned}$$

é uma injeção crescente para a inclusão. Seja $\{\mathfrak{b}_i\}_{i\in\mathbb{N}}$ uma sequência crescente de sub-A'-módulos de A', isto é, de ideais de A'. E daí,

$$\begin{aligned} \mathfrak{b}_i \subset \mathfrak{b}_{i+1}, \forall i \in \mathbb{N} &\underbrace{\Rightarrow}_{\varphi \text{ é injeção crescente (para a inclusão)}} \varphi(\mathfrak{b}_i) \subset \varphi(\mathfrak{b}_{i+1}), \forall i \in \mathbb{N} \\ &\Rightarrow \{ \underbrace{\varphi(\mathfrak{b}_i)}_{\texttt{ideais de A}} \}_{i\in\mathbb{N}} \text{ é sequência crescente de sub-A-módulos de A} \\ &\underbrace{\Rightarrow}_{A \text{ é noetheriano}} \{\varphi(\mathfrak{b}_i)\}_{i\in\mathbb{N}} \text{ é estacionária} \\ &\Rightarrow \exists i_o \in \mathbb{N} \text{ tal que } \varphi(\mathfrak{b}_i) = \varphi(\mathfrak{b}_{i_o}), \forall i \geq i_o \\ &\underbrace{\Rightarrow}_{\varphi \text{ é injetiva}} \exists i_o \in \mathbb{N} \text{ tal que } \mathfrak{b}_i = \mathfrak{b}_{i_o}, \forall i \geq i_o \\ &\Rightarrow \{\mathfrak{b}_i\}_{i\in\mathbb{N}} \text{ é estacionária.} \end{aligned}$$

Como $\{\mathfrak{b}_i\}_{i\in\mathbb{N}}$ é uma sequência crescente arbitrária de sub-A'-módulos de A' então, concluímos que $A' = S^{-1}A$ é noetheriano.

■

Proposição 2.2 *Sejam R um anel de integridade, A um subanel de R, S uma parte multiplicativa estável de A com $1 \in S$ e $0 \notin S$, e B o fecho integral de A em R. Então, o fecho integral de $S^{-1}A$ em $S^{-1}R$ é $S^{-1}B$.*

Observação 2.5 *O anel A também é de integridade, pois A é subanel de um anel de integridade.*

Observação 2.6 *S é também uma parte multiplicativa estável de R.*

Observação 2.7 *B é um subanel de R que contém A. Logo, B é de integridade e S é também uma parte multiplicativa estável de B.*

Demonstração (Proposição 2.2): Note que faz sentido falarmos nos anéis de frações $S^{-1}A, S^{-1}R$ e $S^{-1}B$ devido as observações acima.

Sejam $x \in S^{-1}B \subset S^{-1}R$. Então, $x = \dfrac{b}{s}$ com $b \in B$ e $s \in S$. Como $b \in B$ então existe $P(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in A[X]$ tal que $P(b) = 0$. E daí,

$$b^n + a_{n-1}b^{n-1} + \ldots + a_1b + a_0 = 0, \text{ com } a_i \in A \tag{2.3}$$

Dividindo (2.3) por s^n, obtemos então que,

$$\left(\frac{b}{s}\right)^n + \underbrace{\frac{a_{n-1}}{s}}_{\in S^{-1}A}\left(\frac{b}{s}\right)^{n-1} + \ldots + \underbrace{\frac{a_1}{s^{n-1}}}_{\in S^{-1}A}\left(\frac{b}{s}\right) + \underbrace{\frac{a_0}{s^n}}_{\in S^{-1}A} = 0,$$

o que mostra que $x = \dfrac{b}{s}$ é inteiro sobre $S^{-1}A$. Logo, x pertence ao fecho integral de $S^{-1}A$ em $S^{-1}R$.

Reciprocamente, seja $\frac{a}{s}(a \in R, s \in S)$ um elemento de $S^{-1}R$ inteiro sobre $S^{-1}A$. Logo, existe

$$Q(X) = X^n + \frac{a_{n-1}}{t_{n-1}}X^{n-1} + \ldots + \frac{a_1}{t_1}X + \frac{a_0}{t_0} \in S^{-1}A[X]$$

tal que $Q\left(\frac{a}{s}\right) = 0$. E daí,

$$\left(\frac{a}{s}\right)^n + \frac{a_{n-1}}{t_{n-1}}\left(\frac{a}{s}\right)^{n-1} + \ldots + \frac{a_1}{t_1}\left(\frac{a}{s}\right) + \left(\frac{a_0}{t_0}\right) = 0 \tag{2.4}$$

com $a_i \in A$ e $t_i \in S$. Multiplicando (2.4) por $(st_0 \cdot t_1 \cdot \ldots \cdot t_{n-1})^n$ teremos que,

$$(at_0t_1 \cdot \ldots \cdot t_{n-1})^n + \underbrace{s \cdot a_{n-1}t_0 \cdot t_1 \cdot \ldots \cdot t_{n-2}}_{\in A}(at_0t_1 \cdot \ldots \cdot t_{n-1})^{n-1} + \ldots +$$
$$+ \underbrace{s^{n-1} \cdot a_1 t_1^{n-2}\,(t_0t_2 \cdot \ldots \cdot t_{n-1})^{n-1}}_{\in A} \cdot (at_0t_1 \cdot \ldots \cdot t_{n-1}) +$$
$$+ \underbrace{s^n \cdot a_0 t_0^{n-1}\,(t_1t_2 \cdot \ldots \cdot t_{n-1})^n}_{\in A} = 0.$$

O que nos diz que, $at_0t_1 \cdot \ldots \cdot t_{n-1} \in R$ é inteiro sobre A. Mas, B é o fecho integral de A em R. Logo, $at_0t_1 \cdot \ldots \cdot t_{n-1} \in B$. Com isso,

$$\frac{a}{s} = \frac{1}{\underbrace{st_0t_1 \cdot \ldots \cdot t_{n-1}}_{\in S}} \cdot \underbrace{at_0t_1 \cdot \ldots \cdot t_{n-1}}_{\in B} \in S^{-1}B.$$

Portanto, $S^{-1}B$ é o fecho integral de $S^{-1}R$ em $S^{-1}A$.

■

Corolário 2.2 *Se A é um anel integralmente fechado então todo anel de frações $S^{-1}A$ é integralmente fechado.*

Demonstração: Seja K o corpo de frações de A. Como A é integralmente fechado então A é de integridade e o fecho integral de A em K é o próprio A. Aqui temos que, S é uma parte multiplicativamente estável de A.

Afirmação 2.6 *$Q(S^{-1}A) = S^{-1}K$ onde $Q(S^{-1}A)$ é o corpo de frações de $S^{-1}A$.*

Com efeito,

$$Q(S^{-1}A) = \left\{ \frac{a}{b}; a, b \in S^{-1}A \quad \text{e} \quad b \neq 0 \right\} \quad ; \quad S^{-1}K = \left\{ \frac{k}{s}; k \in K \quad \text{e} \quad s \in S \right\}.$$

$$\frac{a}{b} \in Q(S^{-1}A) \Rightarrow \frac{a}{b} = \frac{\frac{a'}{s'}}{\frac{b'}{r'}} = \frac{a'}{s'} \cdot \frac{r'}{b'} = \frac{a'r'}{b'} \cdot \frac{1}{s'} = \frac{\frac{a'r'}{b'}}{s'} \in S^{-1}K$$

$$\frac{k}{s} \in S^{-1}K \Rightarrow \frac{k}{s} = \frac{\frac{a}{b}}{s} = \frac{a}{b} \cdot \frac{1}{s} = \frac{a}{bs} \Rightarrow \frac{k}{s} \in Q(S^{-1}A)$$

Temos que K é um anel de integridade, A é subanel de K, S é uma parte multiplicativamente estável de A e A é o fecho integral de A em K. Então, pela Proposição 2.2, o fecho integral de $S^{-1}A$ em $S^{-1}K$ é $S^{-1}A$, e além disso, $S^{-1}A$ é de integridade, pois A é integralemente. Portanto, $S^{-1}A$ é integralmente fechado.

■

Proposição 2.3 *Se A é um anel de Dedekind, então todo anel de frações $S^{-1}A$ é um anel de Dedekind.*

Demonstração: Temos que A é anel de Dedekind, logo, A é noetheriano, integralmente fechado (portanto, de integridade) e além disso, todo ideal primo não nulo de A é maximal. E daí, $S^{-1}A$ é noetheriano (Corolário da Proposição 2.1) e também é integralmente fechado (Corolário da Proposição 2.2). Resta mostrar que todo ideal primo não nulo de $S^{-1}A$ é maximal.

Seja $\mathfrak{p}'$ um ideal primo não nulo de $A' = S^{-1}A$.

Afirmação 2.7 *$\mathfrak{p}'$ é um ideal maximal de A'.*

Com efeito, seja J' um ideal de A' tal que $\mathfrak{p}' \subset J' \subset A'$. Pela Proposição 2.1 (2), temos que, $\mathfrak{p}' \cap A$ é um ideal primo não nulo de A tal que $(\mathfrak{p}' \cap A) \cap S = \emptyset$. Como

todo ideal primo não nulo de A é maximal então $\mathfrak{p}' \cap A$ é ideal maximal de A. Por outro lado,

$$\begin{aligned} \mathfrak{p}' \cap A \subset J' \cap A \subset A' \cap A = A \quad &\Rightarrow \quad J' \cap A = \mathfrak{p}' \cap A \quad \text{ou} \quad J' \cap A = A' \cap A \\ &\Rightarrow \quad \varphi(J') = \varphi(\mathfrak{p}') \quad \text{ou} \quad \varphi(J') = \varphi(A') \\ &\Rightarrow \quad J' = \mathfrak{p}' \quad \text{ou} \quad J' = A' \end{aligned}$$

onde

$$\begin{aligned} \varphi \ : \ & C \to D \\ & \mathfrak{p}' \mapsto \mathfrak{p}' \cap A \end{aligned}$$

é injetiva e crescente para a inclusão, C é o conjunto dos ideais de A' e D é o conjunto dos ideais de A.

Com isso, $\mathfrak{p}'$ é ideal maximal de A'. Portanto, $A' = S^{-1}A$ é um anel de Dedekind.

■

Proposição 2.4 *Sejam A um anel de Dedekind, $\mathfrak{p}$ um ideal primo não nulo de A e $S = A - \mathfrak{p}$. Então, $S^{-1}A$ é um anel principal, e existe um elemento primo p de $S^{-1}A$ tal que os únicos ideais não nulos de $S^{-1}A$ são os $(p^n)_{n\geq 0}$.*

Demonstração: Inicialmente afirmamos que $\mathfrak{p}$ é o único ideal primo não nulo de A que não intercepta S ($\mathfrak{p} \cap S = \emptyset$). Com efeito, seja $\mathfrak{q}$ um ideal primo não nulo de A tal que $\mathfrak{q} \cap S = \emptyset$. Logo, $\mathfrak{q} \subset \mathfrak{p} \subset A$ $(*)$. Mas, como A é anel de Dedekind então $\mathfrak{q}$ é um ideal maximal de A. E daí, temos de $(*)$ que $\mathfrak{p} = \mathfrak{q}$ ou $\mathfrak{p} = A$. Note que a última igualdade não pode ocorrer, pois $\mathfrak{p}$ é ideal primo de A. Portanto, $\mathfrak{p} = \mathfrak{q}$.

Com isso, pela Proposição 2.1(2) podemos dizer também que existe um único ideal primo não nulo de $S^{-1}A$, que é dado por $\mathcal{B} = \mathfrak{p}S^{-1}A$.

Como A é de Dedekind então $S^{-1}A$ é de Dedekind. Logo, podemos decompor qualquer ideal não nulo J de $S^{-1}A$ como produto de ideais primos não nulos de $S^{-1}A$, mas como $\mathcal{B}$ é o único ideal primo não nulo de $S^{-1}A$. E daí, $J = \mathcal{B}^n$ para algum $n \geq 0$. Com isso, os únicos ideais não nulos de $S^{-1}A$ são da forma $\mathcal{B}^n (n \geq 0)$. Note que, $\mathcal{B} \not\subset \mathcal{B}^2$. Caso contrário,

$$\mathcal{B} \subset \mathcal{B}^2 \Rightarrow n_{\mathcal{B}}(\mathcal{B}) \geq n_{\mathcal{B}}(\mathcal{B}^2) \Rightarrow 1 \geq 2 \quad (ABSURDO).$$

Logo, $\mathcal{B} - \mathcal{B}^2 \neq \emptyset$.

Tomemos então, $p \in \mathcal{B} - \mathcal{B}^2$. O ideal (p) está contido em $\mathcal{B}$ e não está contido em $\mathcal{B}^2$. Como (p) é um ideal não nulo de $S^{-1}A$ então $(p) = \mathcal{B}^m$ para algum $m \geq 0$.

$$\left.\begin{array}{lllllll} (p) & \subset & \mathcal{B} & \Rightarrow & n_{\mathcal{B}}((p)) & \geq & n_{\mathcal{B}}(\mathcal{B}) \quad \Rightarrow \quad m \geq 1 \\ (p) & \not\subset & \mathcal{B}^2 & \Rightarrow & n_{\mathcal{B}}((p)) & < & n_{\mathcal{B}}(\mathcal{B}^2) \quad \Rightarrow \quad m < 2 \end{array}\right| \Rightarrow 1 \leq m < 2 \Rightarrow m = 1.$$

E daí, $(p) = \mathcal{B}$. Além disso, $\mathcal{B}$ é ideal primo de $S^{-1}A$, então p é elemento primo de $S^{-1}A$. Como $\mathcal{B} = (p)$ então $\mathcal{B}^n = (p^n)$.

Portanto, os únicos ideais não nulos de $S^{-1}A$ são os (p^n) e além disso, $S^{-1}A$ é principal.

■

Proposição 2.5 *Sejam A um anel de integridade, S uma parte multiplicativa estável de A ($1 \in S, 0 \notin S$) e $\mathfrak{m}$ um ideal maximal de A tal que $\mathfrak{m} \cap S = \emptyset$. Então,*

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

Demonstração: Temos que,

$$\begin{array}{ccc} \phi : A & \to & S^{-1}A \\ a & \mapsto & \dfrac{a}{1} \end{array}$$

e

$$\begin{array}{rccl} \psi : S^{-1}A & \to & S^{-1}A/\mathfrak{m}S^{-1}A \\ \dfrac{r}{s} & \mapsto & \dfrac{r}{s} + \mathfrak{m}S^{-1}A \end{array}$$

são homomorfismos. E daí,

$$\begin{array}{rccl} \beta = \psi \circ \phi : & A & \to & S^{-1}A/\mathfrak{m}S^{-1}A \\ & a & \mapsto & \dfrac{a}{1} + \mathfrak{m}S^{-1}A \end{array}$$

é um homomorfismo.

Afirmação 2.8 *Ker*$\beta = \mathfrak{m}S^{-1}A \cap A$.

Com efeito,

$$\begin{array}{rcl} x \in \text{Ker}\beta & \Leftrightarrow & x \in A \quad \text{e} \quad \beta(x) = \dfrac{0}{1} + \mathfrak{m}S^{-1}A \\ & \Leftrightarrow & x \in A \quad \text{e} \quad \dfrac{x}{1} + \mathfrak{m}S^{-1}A = \dfrac{0}{1} + \mathfrak{m}S^{-1}A \\ & \Leftrightarrow & x \in A \quad \text{e} \quad \dfrac{x}{1} - \dfrac{0}{1} \in \mathfrak{m}S^{-1}A \\ & \Leftrightarrow & x \in A \quad \text{e} \quad \dfrac{x}{1} \in \mathfrak{m}S^{-1}A \\ & \Leftrightarrow & x \in A \quad \text{e} \quad x \in \mathfrak{m}S^{-1}A \\ & \Leftrightarrow & x \in \mathfrak{m}S^{-1}A \cap A. \end{array}$$

Como $\mathfrak{m}$ é um ideal maximal de A então $\mathfrak{m}$ é um ideal primo de A. E além disso, $\mathfrak{m} \cap S = \emptyset$. Logo, pelo que foi visto na demonstração da Proposição 2.1, temos que, $\mathfrak{m}S^{-1}A \cap A = \mathfrak{m}$.

Temos então que,

$$\begin{array}{rccl} \beta : A & \to & S^{-1}A/\mathfrak{m}S^{-1}A \\ a & \mapsto & \dfrac{a}{1} + \mathfrak{m}S^{-1}A \end{array}$$

é um homomorfismo e Ker$\beta = \mathfrak{m}$, logo, pelo Teorema dos Homomorfismos, existe um único homomorfismo injetivo $\varphi : A/\mathfrak{m} \to S^{-1}A/\mathfrak{m}S^{-1}A$ tal que

$\beta = \varphi \circ h$, onde

$$\begin{aligned} h : A &\to A/\mathfrak{m} \\ a &\mapsto a + \mathfrak{m} \end{aligned}$$

é o homomorfismo canônico. Com isso,

$$\varphi(a + \mathfrak{m}) = \varphi(h(a)) = \beta(a) = \frac{a}{1} + \mathfrak{m}S^{-1}A, \forall a \in A.$$

Resta mostrar que φ é sobrejetiva. Seja, $\frac{a}{s} + \mathfrak{m}S^{-1}A \in S^{-1}A/\mathfrak{m}S^{-1}A$. E daí, $s \in S$. Mas, $\mathfrak{m} \cap S = \emptyset$. Logo,

$$\begin{aligned} & s \notin \mathfrak{m} \Rightarrow s - 0 \notin \mathfrak{m} \Rightarrow s \not\equiv 0 (\text{mod } \mathfrak{m}) \Rightarrow s + \mathfrak{m} \neq 0 + \mathfrak{m} \Rightarrow \\ \underbrace{\Rightarrow}_{A/\mathfrak{m} \text{ é corpo}} & \exists b + \mathfrak{m} \in A/\mathfrak{m} \text{ tal que } (s + \mathfrak{m})(b + \mathfrak{m}) = (b + \mathfrak{m}) \cdot (s + \mathfrak{m}) = 1 + \mathfrak{m} \\ \Rightarrow & \exists b + \mathfrak{m} \in A/\mathfrak{m} \text{ tal que } bs + \mathfrak{m} = 1 + \mathfrak{m} \\ \Rightarrow & \exists b \in A \text{ tal que } bs - 1 \in \mathfrak{m}. \end{aligned}$$

Então, $\frac{a}{s} - ab = \frac{a}{s}(1 - bs) \in \mathfrak{m}S^{-1}A$. Ou seja,

$$\frac{a}{s} \equiv ab (\text{mod } \mathfrak{m}S^{-1}A) \Rightarrow \frac{a}{s} + \mathfrak{m}S^{-1}A = ab + \mathfrak{m}S^{-1}A = \varphi(\underbrace{ab + \mathfrak{m}}_{\in A/\mathfrak{m}}).$$

Portanto,

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

■

Capítulo 3

Decomposição dos ideais primos em uma extensão

3.1 Ideais Primos e Maximais

Seja A um anel comutativo com identidade multiplicativa 1.

Definição 3.1 *Um ideal P de A é dito ser um ideal primo quando ele satisfaz as seguintes condições:*

(a) $P \neq A$.

(b) *Se $a, b \in A$, $a \cdot b \in P$ então ou $a \in P$ ou $b \in P$.*

Consequência: P é um ideal primo de A se, e só se, A/P é um domínio.

Definição 3.2 *Um ideal M de A é dito ser um ideal maximal quando:*

(a) $M \neq A$

(b) *Não existe J de A tal que $M \subset J \subset A$.*

Consequência: M é um ideal maximal de A se, e só se, A/M é um corpo.

Logo, todo ideal maximal é um ideal primo.

3.2 Decomposição de um ideal primo em uma extensão

Sejam A um anel de Dedekind de característica zero, K seu corpo de frações, L uma extensão de grau finito n de K e B o fecho integral de A em L. Pelo Teorema 1.7, temos que B é um anel de Dedekind e um A-módulo de tipo finito.

Seja $\mathfrak{p}$ um ideal primo não nulo de A. Então, $B\mathfrak{p}$ é um ideal não nulo de B, e portanto, ideal fracionário não nulo de B.

$$B\mathfrak{p} = \{b_1p_1 + \ldots + b_mp_m; b_j \in B \text{ e } p_j \in \mathfrak{p}\}.$$

Sendo B de Dedekind então podemos decompor $B\mathfrak{p}$ como produto de ideais primos não nulos de B, isto é,

$$B\mathfrak{p} = \prod_{i=1}^{q} \mathcal{B}_i^{e_i}, \tag{3.1}$$

onde os $\mathcal{B}_i's$ são ideais primos de B, distintos dois a dois, e os $e_i's$ são inteiros ≥ 1.

Proposição 3.1 *Os $\mathcal{B}_i's$ são exatamente os ideais primos D de B tais que $D \cap A = \mathfrak{p}$.*

Demonstração: Afirmamos que para um ideal primo D de B, tem-se que,

$$D \cap A = \mathfrak{p} \Leftrightarrow D \supset \mathfrak{p}B.$$

$(\Rightarrow) x \in \mathfrak{p}B \Rightarrow x = p_1b_1 + \ldots + p_mb_m; b_j \in B \text{ e } p_j \in \mathfrak{p} \subset D \Rightarrow x \in D$

$$\therefore D \supset \mathfrak{p}B$$

$(\Leftarrow)$ Tem-se que $D \cap A \subset A$ é ideal primo de A. Com efeito, sejam $x, y \in A \subset B$ tais que $xy \in D \cap A$. Logo,

$$xy \in D \underbrace{\Rightarrow}_{D \text{ é ideal primo de } B} x \in D \text{ ou } y \in D \underbrace{\Rightarrow}_{x,y \in A} x \in D \cap A \text{ ou } y \in D \cap A$$

$$\therefore D \cap A \text{ é ideal primo de } A.$$

Sendo $D \cap A$ ideal primo de A então $D \cap A \neq A$. Por outro lado,

$$\mathfrak{p} \underbrace{\subset}_{(*)} \mathfrak{p}B \underbrace{\subset}_{\text{hipótese}} D \quad \Rightarrow \quad \mathfrak{p} \cap A \subset D \cap A \underbrace{\Rightarrow}_{\mathfrak{p} \subset A} \mathfrak{p} \subset D \cap A \subset A$$

$$\overbrace{\Rightarrow}^{(**)} \quad D \cap A = \mathfrak{p} \text{ ou } D \cap A = A \underbrace{\Rightarrow}_{D \cap A \neq A} D \cap A = \mathfrak{p}$$

$(*)$: $\forall p \in \mathfrak{p}$ tem-se $p = p \cdot 1 \in \mathfrak{p}B$

$(**)$: $\mathfrak{p}$ é ideal maximal de A (pois, A é de Dedekind)

(i): formulário dos anéis de Dedekind(Observação 1.6)

(ii): Afirmação apresentada no início da demonstração.

Seja P o conjunto dos ideais primos não nulos de B. Temos que, para todo $i = 1, \ldots, q, 1 \leq e_i =$ expoente de $\mathcal{B}_i$ na decomposição de $\mathfrak{p}B$. Logo,

$$n_J(\mathfrak{p}B) \geq n_J(\mathcal{B}_i) \text{ para todo } J \in P \underbrace{\Rightarrow}_{(i)} \mathfrak{p}B \subset \mathcal{B}_i \underbrace{\Rightarrow}_{(ii)} \mathcal{B}_i \cap A = \mathfrak{p}.$$

■

Assim $A/\mathfrak{p}$ se identifica a um subanel de $B/\mathcal{B}_i$. Com efeito,

Sejam $\alpha : A \to B$ e $\beta : B \to B/\mathcal{B}_i$ homomorfismos de anéis dados por $\alpha(a) = a$ e $\beta(b) = b + \mathcal{B}_i$. Logo,

$$\begin{aligned} \varphi = \beta \circ \alpha \quad : \quad & A \to B/\mathcal{B}_i \\ & a \mapsto a + \mathcal{B}_i \end{aligned}$$

é um homomorfismo de anéis cujo núcleo Ker$\varphi = \mathcal{B}_i \cap A = \mathfrak{p}$. E daí, pelo Teorema dos homomorfismos de anéis, existe um único homomorfismo injetivo $\overline{\varphi} : A/\mathfrak{p} \to B/\mathcal{B}_i$ tal que, $\varphi = \overline{\varphi} \circ h$ onde

$$\begin{aligned} h \quad : \quad & A \to A/\mathfrak{p} \\ & a \mapsto a + \mathfrak{p}. \end{aligned}$$

Note que a identificação se dá do seguinte modo:

$$\begin{array}{ccc} A/\mathfrak{p} & \overset{\overline{\varphi}}{\to} & B/\mathcal{B}_i \\ a+\mathfrak{p} & \mapsto & a+\mathcal{B}_i \end{array}$$

Estes dois anéis são corpos. Veja

$$\mathfrak{p} \text{ é ideal primo não nulo de} A \underbrace{\Rightarrow}_{A \text{ é anel de Dedekind}} \mathfrak{p} \text{ é ideal maximal de} A \Rightarrow A/\mathfrak{p} \text{ é corpo}$$

$$\mathcal{B}_i \text{ é ideal primo não nulo de} B \underbrace{\Rightarrow}_{B \text{ é anel de Dedekind}} \mathcal{B}_i \text{ é ideal maximal de} B \Rightarrow B/\mathcal{B}_i \text{ é corpo}$$

Temos então que $B/\mathcal{B}_i$ é um anel de divisão (pois, é corpo) e $A/\mathfrak{p}$ é um subanel de $B/\mathcal{B}_i$. Logo, $B/\mathcal{B}_i$ é um espaço vetorial sobre $A/\mathfrak{p}$.

Como B é um A-módulo de tipo finito, isto é, $B = At_1 + \ldots + At_n (t_j \in B)$, então $B/\mathcal{B}_i$ é um espaço vetorial de dimensão finita sobre $A/\mathfrak{p}$. Com efeito,

$$\begin{aligned} x \in B/\mathcal{B}_i &\Leftrightarrow x = b + \mathcal{B}_i, b \in B \\ &\Leftrightarrow x = (a_1t_1 + \ldots + a_nt_n) + \mathcal{B}_i \\ &= (a_1t_1 + \mathcal{B}_i) + \ldots + (a_nt_n + \mathcal{B}_i) \\ &= (a_1 + \mathcal{B}_i)(t_1 + \mathcal{B}_i) + \ldots + (a_n + \mathcal{B}_i)(t_n + \mathcal{B}_i) \\ &= (a_1 + \mathfrak{p})(t_1 + \mathcal{B}_i) + \ldots + (a_n + \mathfrak{p})(t_n + \mathcal{B}_i) \in \\ &\in (t_1 + \mathcal{B}_i) A/\mathfrak{p} + \ldots + (t_n + \mathcal{B}_i) A/\mathfrak{p}. \end{aligned}$$

Logo,

$$B/\mathcal{B}_i = (t_1 + \mathcal{B}_i) A/\mathfrak{p} + \ldots + (t_n + \mathcal{B}_i) A/\mathfrak{p}.$$

Ou seja, $B/\mathcal{B}_i$ é gerado sobre $A/\mathfrak{p}$ pelos elementos $t_1 + \mathcal{B}_i, \ldots, t_n + \mathcal{B}_i$. E daí, podemos extrair do conjunto de geradores $\{t_1 + \mathcal{B}_i, \ldots, t_n + \mathcal{B}_i\}$, uma base para $B/\mathcal{B}_i$, consequentemente $[B/\mathcal{B}_i : A/\mathfrak{p}]$ é finito.

Designaremos por f_i esta dimensão e a chamaremos de o grau residual de $\mathcal{B}_i$ sobre A.

$$f_i = [B/\mathcal{B}_i : A/\mathfrak{p}].$$

O expoente e_i em (3.1) se chama o índice de ramificação de $\mathcal{B}_i$ sobre A. Notemos, finalmente que $B\mathfrak{p} \cap A = \mathfrak{p}$.

- $\left.\begin{array}{c} \mathfrak{p} \subset A \\ \mathfrak{p} \subset B\mathfrak{p} \end{array}\right| \Rightarrow \mathfrak{p} \subset B\mathfrak{p} \cap A.$
- $x \in B\mathfrak{p} \cap A \Rightarrow x \in B\mathfrak{p}$ e $x \in A$.

$$\begin{array}{rl} & x \in B\mathfrak{p} = \prod_{i=1}^{q} \mathcal{B}_i^{e_i} \Rightarrow \\ \Rightarrow & x = a_1^1 a_2^1 \cdot \ldots \cdot a_i^1 \cdot \ldots \cdot a_q^1 + a_1^2 a_2^2 \cdot \ldots \cdot a_i^2 \cdot \ldots \cdot a_q^2 + \ldots + \\ & + a_1^m a_2^m \cdot \ldots \cdot a_i^m \cdot \ldots \cdot a_q^m \quad \text{com} \quad a_i^j \in \mathcal{B}_i^{e_i}, \forall j = 1, \ldots, m \\ \underbrace{\Rightarrow}_{\mathcal{B}_i^{e_i} \text{ é ideal de } B} & x \in \mathcal{B}_i^{e_i} \subset \mathcal{B}_i. \end{array}$$

E daí, $x \in \mathcal{B}_i$ e $x \in A$. Logo, $x \in \mathfrak{p} = \mathcal{B}_i \cap A$.

$$\therefore B\mathfrak{p} \cap A \subset \mathfrak{p}.$$

Note que $B/B\mathfrak{p}$ é um $A/\mathfrak{p}$-módulo e $A/\mathfrak{p}$ é corpo, logo $B/B\mathfrak{p}$ é um espaço vetorial sobre $A/\mathfrak{p}$. Afirmação: $B/B\mathfrak{p}$ é um espaço vetorial de dimensão finita sobre $A/\mathfrak{p}$. Com efeito, considere os homomorfismos de anéis abaixo:

$$\begin{array}{ccccc} A & \stackrel{\alpha}{\to} & B & \stackrel{\beta}{\to} & B/B\mathfrak{p} \\ a & \mapsto & a & \mapsto & a + B/B\mathfrak{p} \end{array}$$

Então,

$$\begin{array}{rcl} \varphi = \beta \circ \alpha & : & A \to B/B\mathfrak{p} \\ & & a \mapsto a + B\mathfrak{p} \end{array}$$

é um homomorfismo de anéis. E além disso, o núcleo Ker$\varphi = B\mathfrak{p} \cap A = \mathfrak{p}$. Logo, pelo Teorema dos homomorfismos de anéis existe um único homomorfismo injetivo $\overline{\varphi} : A/\mathfrak{p} \to B/B\mathfrak{p}$ tal que $\varphi = \overline{\varphi} \circ h$ onde

$$\begin{aligned} h &: A \to A/\mathfrak{p} \\ &\quad a \mapsto a + \mathfrak{p}. \end{aligned}$$

Com isso podemos identificar $A/\mathfrak{p}$ a um subanel de $B/B\mathfrak{p}$.

$$a + \mathfrak{p} \leftrightarrow a + B\mathfrak{p} = \overline{\varphi}(a + \mathfrak{p}).$$

Sendo B um A-módulo de tipo finito então $B = At_1 + \ldots + At_n (t_j \in B)$.

Afirmação 3.1 $B/B\mathfrak{p} = (t_1 + B\mathfrak{p})\, A/\mathfrak{p} + \ldots + (t_n + B\mathfrak{p})\, A/\mathfrak{p}$.

$$\begin{aligned} x \in B/B\mathfrak{p} \quad &\Leftrightarrow \quad x = b + B\mathfrak{p}, b \in B \\ &\Leftrightarrow \quad x = (a_1t_1 + \ldots + a_nt_n) + B\mathfrak{p} \\ &\qquad = (a_1t_1 + B\mathfrak{p}) + \ldots + (a_nt_n + B\mathfrak{p}) \\ &\qquad = (a_1 + B\mathfrak{p})\,(t_1 + B\mathfrak{p}) + \ldots + (a_n + B\mathfrak{p})\,(t_n + B\mathfrak{p}) \\ &\qquad = (a_1 + \mathfrak{p})\,(t_1 + B\mathfrak{p}) + \ldots + (a_n + \mathfrak{p})\,(t_n + B\mathfrak{p}) \in \\ &\qquad \in (t_1 + B\mathfrak{p})\, A/\mathfrak{p} + \ldots + (t_n + B\mathfrak{p})\, A/\mathfrak{p}. \end{aligned}$$

Ou seja, $B/B\mathfrak{p}$ é gerado sobre $A/\mathfrak{p}$ pelos elementos $t_1 + B\mathfrak{p}, \ldots, t_n + B\mathfrak{p}$. Como $B/B\mathfrak{p}$ é um $A/\mathfrak{p}$-espaço vetorial, então podemos extrair do conjunto de geradores $\{t_1 + B\mathfrak{p}, \ldots, t_n + B\mathfrak{p}\}$, uma base para $B/B\mathfrak{p}$, consequentemente $[B/B\mathfrak{p} : A/\mathfrak{p}]$ é finito.

Teorema 3.1 *Com as mesmas notações, tem-se que,*

$$\sum_{i=1}^{q} e_i f_i = [B/B\mathfrak{p} : A/\mathfrak{p}] = n = [L : K]\,. \tag{3.2}$$

Demonstração: A primeira igualdade é fácil. Consideremos a sucessão de ideais de B,

$$\begin{aligned} B \supset\ & \mathcal{B}_1 \supset \mathcal{B}_1^2 \supset \ldots \supset \mathcal{B}_1^{e_1} \supset \mathcal{B}_1^{e_1}\mathcal{B}_2 \supset \mathcal{B}_1^{e_1}\mathcal{B}_2^2 \supset \ldots \supset \mathcal{B}_1^{e_1}\mathcal{B}_2^{e_2} \supset \\ \supset\ & \mathcal{B}_1^{e_1}\mathcal{B}_2^{e_2}\mathcal{B}_3 \supset \mathcal{B}_1^{e_1}\mathcal{B}_2^{e_2}\mathcal{B}_3^2 \supset \ldots \supset \mathcal{B}_1^{e_1}\mathcal{B}_2^{e_2}\mathcal{B}_3^{e_3} \supset \\ \supset\ & \ldots \supset \mathcal{B}_1^{e_1}\mathcal{B}_2^{e_2} \cdot \ldots \cdot \mathcal{B}_q^{e_q} = B\mathfrak{p}. \end{aligned}$$

Dois termos consecutivos são da forma $\mathcal{B}$ e $\mathcal{B}\mathcal{B}_i$. Por outro lado, como não existem ideais compreendidos estritamente entre $\mathcal{B}$ e $\mathcal{B}\mathcal{B}_i$ então $\mathcal{B}/\mathcal{B}\mathcal{B}_i$ é um espaço vetorial de dimensão 1 sobre $\mathcal{B}/\mathcal{B}_i$. Logo, $\mathcal{B}/\mathcal{B}\mathcal{B}_i$ é um espaço vetorial de dimensão f_i sobre $A/\mathfrak{p}$.

Note também que, na sucessão acima existem e_i quocientes de termos consecutivos da forma $\mathcal{B}/\mathcal{B}\mathcal{B}_i$, com i dado. E daí, a dimensão $[B/B\mathfrak{p} : A/\mathfrak{p}]$ é igual a soma das dimensões destes quocientes, isto é,

$$\sum_{i=1}^{q} e_i f_i = \sum_{i=1}^{q} \left(e_i \cdot [B/\mathcal{B}_i : A/\mathfrak{p}]\right).$$

A segunda igualdade é simples no caso em que B é um A-módulo livre, em particular quando A é principal. Com efeito, uma base $(x_1, \ldots, x_n)$ do A-módulo B dá por redução mod $B\mathfrak{p}$, uma base de $B/B\mathfrak{p}$ sobre $A/\mathfrak{p}$. Veja:

Seja $(x_1, \ldots, x_n)$ base de B sobre A. Obviamente, que

$$(x_1 + B\mathfrak{p})A/\mathfrak{p} + \ldots + (x_n + B\mathfrak{p})A/\mathfrak{p} \subset B/B\mathfrak{p}$$

já que $B/B\mathfrak{p}$ é um $A/\mathfrak{p}$-espaço vetorial.

E além disso,

$$\begin{aligned}
x \in B/B\mathfrak{p} &\Rightarrow x = b + B\mathfrak{p}, b \in B \\
&\Rightarrow x = (a_1x_1 + \ldots + a_nx_n) + B\mathfrak{p}, a_i \in A \quad \text{e} \quad x_i \in B \\
&\Rightarrow x = (a_1x_1 + B\mathfrak{p}) + \ldots + (a_nx_n + B\mathfrak{p}) \\
&\qquad = (a_1 + B\mathfrak{p}))(x_1 + B\mathfrak{p}) + \ldots + (a_n + B\mathfrak{p}))(x_n + B\mathfrak{p}) \\
&\qquad \underbrace{=}_{a_i+\mathfrak{p}\leftrightarrow a_i+B\mathfrak{p}} (a_1 + \mathfrak{p}))(x_1 + B\mathfrak{p}) + \ldots + (a_n + \mathfrak{p}))(x_n + B\mathfrak{p}) \\
&\Rightarrow x \in (x_1 + B\mathfrak{p})A/\mathfrak{p} + \ldots + (x_n + B\mathfrak{p})A/\mathfrak{p}.
\end{aligned}$$

Portanto,

$$B/B\mathfrak{p} = (x_1 + B\mathfrak{p})A/\mathfrak{p} + \ldots + (x_n + B\mathfrak{p})A/\mathfrak{p}.$$

Por outro lado, $\{x_1 + B\mathfrak{p}, \ldots, x_n + B\mathfrak{p}\}$ é linearmente independente sobre $A/\mathfrak{p}$. Veja,

$$(a_1 + \mathfrak{p}) \cdot (x_1 + B\mathfrak{p}) + \ldots + (a_n + \mathfrak{p}) \cdot (x_n + B\mathfrak{p}) = 0 + B\mathfrak{p} \Rightarrow$$

$$\Rightarrow (a_1 + B\mathfrak{p}) \cdot (x_1 + B\mathfrak{p}) + \ldots + (a_n + B\mathfrak{p}) \cdot (x_n + B\mathfrak{p}) = 0 + B\mathfrak{p} \Rightarrow$$

$$\Rightarrow (a_1x_1 + \ldots + a_nx_n) + B\mathfrak{p} = 0 + B\mathfrak{p} \Rightarrow$$

$$\Rightarrow a_1x_1 + \ldots + a_nx_n \in B\mathfrak{p}$$

$$\Rightarrow a_1x_1 + \ldots + a_nx_n = \sum_{i=1}^{s} b_ip_i, b_i \in B \text{ e } p_i \in \mathfrak{p}$$

$$\underbrace{\Rightarrow}_{B=Ax_1+\ldots+Ax_n} \quad a_1x_1 + \ldots + a_nx_n = \sum_{i=1}^{s}(a_{i1}x_1 + \ldots + a_{in}x_n)p_i,$$

$$a_{ij} \in A(i = 1, \ldots, s; j = 1, \ldots, n)$$

$$\Rightarrow \quad a_1x_1 + \ldots + a_nx_n = \sum_{i=1}^{s}(\underbrace{a_{i1}p_i}_{\in\mathfrak{p}}x_1 + \ldots + \underbrace{a_{in}p_i}_{\in\mathfrak{p}}x_n),$$

$$a_{ij} \in A(i = 1, \ldots, s; j = 1, \ldots, n)$$

$$\underbrace{\Rightarrow}_{\mathfrak{p} \text{ é ideal de } A} \quad a_1x_1 + \ldots + a_nx_n = \sum_{i=1}^{s}(r_{i1}x_1 + \ldots + r_{in}x_n),$$

$$r_{ij} \in \mathfrak{p}(i = 1, \ldots, s; j = 1, \ldots, n)$$

$$\Rightarrow \quad a_1x_1 + \ldots + a_nx_n = \overbrace{(r_{11} + r_{21} + \ldots + r_{s1})}^{\in\mathfrak{p}}x_1 +$$

$$+\overbrace{(r_{12} + r_{22} + \ldots + r_{s2})}^{\in\mathfrak{p}}x_2 + \ldots + \overbrace{(r_{1n} + r_{2n} + \ldots + r_{sn})}^{\in\mathfrak{p}}x_n$$

$$\Rightarrow \quad a_1x_1 + \ldots + a_nx_n = c_1x_1 + \ldots + c_nx_n, c_j \in \mathfrak{p}$$

$$\Rightarrow \quad \underbrace{(a_1 - c_1)}_{\in A}x_1 + \ldots + \underbrace{(a_n - c_n)}_{\in A}x_n = 0$$

$$\underbrace{\Rightarrow}_{\{x_1,\ldots,x_n\} \text{ LI sobre A}} \quad a_1 - c_1 = 0, \ldots, a_n - c_n = 0$$

$$\Rightarrow \quad a_1 = c_1 \in \mathfrak{p}, \ldots, a_n = c_n \in \mathfrak{p}$$

$$\Rightarrow \quad a_1 - 0 \in \mathfrak{p}, \ldots, a_n - 0 \in \mathfrak{p}$$

$$\Rightarrow \quad a_1 + \mathfrak{p} = 0 + \mathfrak{p}, \ldots, a_n + \mathfrak{p} = 0 + \mathfrak{p}.$$

Com isso, $\{x_1 + B\mathfrak{p}, \ldots, x_n + B\mathfrak{p}\}$ é uma base de $B/B\mathfrak{p}$ sobre $A/\mathfrak{p}$. Logo,

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

Vamos nos reduzir a este caso considerando a parte multiplicativamente estável $S = A - \mathfrak{p}$ de A e os anéis de frações $A' = S^{-1}A$ e $B' = S^{-1}B$. Pela Proposição 2.4 temos que A' é um anel principal, cujo único ideal maximal é $\mathfrak{p}A'$. E pela

Proposição 2.2, $B' = S^{-1}B$ é o fecho integral de $A' = S^{-1}A$ em $L = S^{-1}L$. Como A' é principal então, $B' = S^{-1}B$ é um A-módulo livre de dimensão $n = [S^{-1}L : S^{-1}K]$. E daí, pelo que vimos acima,

$$[B'/B'\mathfrak{p}A' : A'/\mathfrak{p}A'] = n, \quad \text{isto é,} \quad [B'/\mathfrak{p}B' : A'/\mathfrak{p}A'] = n.$$

Consideremos então a decomposição do ideal $\mathfrak{p}B'$ no anel de Dedekind (pois, B é de Dedekind) B'. De $\mathfrak{p}B = \prod_{i=1}^{q} \mathcal{B}_i^{e_i}$ se deduz que $\mathfrak{p}B' = \prod_{i=1}^{q} (B'\mathcal{B}_i)^{e_i}$. Como $\mathcal{B}_i \cap A = \mathfrak{p}$ (Proposição 3.1) então $\mathcal{B}_i \cap S = \emptyset$, onde $S = A - \mathfrak{p}$. Caso contrário, existiria x tal que,

$$x \in \mathcal{B}_i \cap S \Rightarrow x \in \mathcal{B}_i \quad \text{e} \quad x \in S = A - \mathfrak{p} \Rightarrow$$

$$\Rightarrow x \in \mathcal{B}_i \cap A = \mathfrak{p} \quad \text{e} \quad x \notin \mathfrak{p} \quad (\text{CONTRADIÇÃO}).$$

Logo, pela Proposição 2.1, $B'\mathcal{B}_i$ é um ideal primo não nulo de B' tal que $\mathcal{B}_i \cap S = \emptyset$.

Portanto, a primeira parte da demonstração nos dá,

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

onde $[B'/B'\mathcal{B}_i : A'/\mathfrak{p}A'] = f_i$ é o grau residual de $B'\mathcal{B}_i$ sobre A'.

Como $\mathfrak{p} \cap S = \emptyset$ ($\mathfrak{p} \subset A$ e $S = A - \mathfrak{p}$) e $\mathcal{B}_i \cap S = \emptyset$ então pela Proposição 2.5,

$$S^{-1}A/\mathfrak{p}S^{-1}A \cong A/\mathfrak{p} \quad \text{e} \quad S^{-1}B/\mathcal{B}_iS^{-1}B \cong B/\mathcal{B}_i,$$

isto é,

$$A'/\mathfrak{p}A' \cong A/\mathfrak{p} \quad \text{e} \quad B'/\mathcal{B}_iB' \cong B/\mathcal{B}_i.$$

Logo,

$$[B/\mathcal{B}_i : A/\mathfrak{p}] = [B'/\mathcal{B}_iB' : A'/\mathfrak{p}A'] \, .$$

E daí,

$$n = [B'/B'\mathfrak{p} : A'/A'\mathfrak{p}] = \sum_{i=1}^{q} (e_i \cdot [B/\mathcal{B}_i : A/\mathfrak{p}]) = [B/B\mathfrak{p} : A/A\mathfrak{p}] \, .$$

■

Lema 3.2 *Se um ideal primo* $\mathfrak{p}$ *de um anel* A *contém um produto* $\mathfrak{a}_1\mathfrak{a}_2 \cdot \ldots \cdot \mathfrak{a}_n$ *de ideais então* $\mathfrak{p}$ *contém um deles.*

Demonstração: Suponha que, $\mathfrak{a}_i \not\subset \mathfrak{p}$ para todo i. Logo, existe $a_i \in \mathfrak{a}_i$ tal que $a_i \notin \mathfrak{p}$. Como $\mathfrak{p}$ é primo então $a_1 \cdot \ldots \cdot a_n \notin \mathfrak{p}$. Por outro lado, $a_1 \cdot \ldots \cdot a_n \in \mathfrak{a}_1\mathfrak{a}_2 \cdot \ldots \cdot \mathfrak{a}_n \subset \mathfrak{p}$ (CONTRADIÇÃO).

■

Lema 3.3 *Sejam* A *um anel e* $(\mathfrak{a}_i)_{1\leq i\leq r}$ *uma família finita de ideais de* A *tais que* $\mathfrak{a}_i + \mathfrak{a}_j = A$ *para* $i \neq j$*. Então, existe um isomorfismo canônico de* $A/\mathfrak{a}_1\mathfrak{a}_2 \cdot \ldots \cdot \mathfrak{a}_r$ *sobre* $\prod_{i=1}^{r} A/\mathfrak{a}_i$.

Demonstração: Ver [10], página 18.

Proposição 3.2 *Com as mesmas notações, o anel* $B/B\mathfrak{p}$ *é isomorfo a* $\prod_{i=1}^{q} B/\mathcal{B}_i^{e_i}$.

Demonstração: Temos que $\mathcal{B}_i$ é ideal maximal ($\mathcal{B}_i$ é ideal primo de B e B é de Dedekind) de B que contém $\mathcal{B}_i^{e_i}$ ($\mathcal{B}_i^{e_i} \subset \mathcal{B}_i$).

Afirmação 3.2 $\mathcal{B}_i$ *é o único ideal maximal com tal propriedade.*

Com efeito, seja J um ideal maximal (logo, é primo) de B que contém $\mathcal{B}_i^{e_i}$. Logo,

$$\begin{aligned} \mathcal{B}_i^{e_i} \subset J \subset B \quad &\underbrace{\Rightarrow}_{Lema\ 3.2} \quad \mathcal{B}_i \subset J \subset B \\ &\underbrace{\Rightarrow}_{\mathcal{B}_i \text{ é maximal}} \quad J = \mathcal{B}_i \quad \text{ou} \quad J = B (\text{essa igualdade} \\ & \qquad\qquad\quad (\text{não pode ocorrer, pois J é ideal primo de B}) \\ &\Rightarrow \quad J = \mathcal{B}_i, \end{aligned}$$

o que mostra a unicidade de $\mathcal{B}_i$. Da afirmação segue-se que, $\mathcal{B}_i^{e_i} + \mathcal{B}_j^{e_j} = B$, $\forall i \neq j$. Com efeito, suponha para $i \neq j$ que $\mathcal{B}_i^{e_i} + \mathcal{B}_j^{e_j} \neq B$ então $\mathcal{B}_i^{e_i} + \mathcal{B}_j^{e_j} \subset M$, para algum ideal maximal M de B. E daí,

$$\left.\begin{array}{rcl} \mathcal{B}_i^{e_i} \subset \mathcal{B}_i^{e_i} + \mathcal{B}_j^{e_j} \subset M \subset B & \Rightarrow & M = \mathcal{B}_i \\ \mathcal{B}_j^{e_j} \subset \mathcal{B}_i^{e_i} + \mathcal{B}_j^{e_j} \subset M \subset B & \Rightarrow & M = \mathcal{B}_j \end{array}\right| \Rightarrow \mathcal{B}_i = \mathcal{B}_j (\text{CONTRADIÇÃO}).$$

Então pelo Lema 3.3 existe um isomorfismo de $B/\mathcal{B}_1^{e_1} \cdot \ldots \cdot \mathcal{B}_q^{e_q}$ sobre $\prod_{i=1}^{q} B/\mathcal{B}_i^{e_i}$, ou seja, $B/B\mathfrak{p}$ é isomorfo a $\prod_{i=1}^{q} B/\mathcal{B}_i^{e_i}$.

■

3.3 Exemplo dos Corpos Ciclotômicos

Sejam p um número primo, $r \in \mathbb{N}$ e $z \in \mathbb{C}$ uma raiz primitiva p^r-ésima da unidade. As raízes p^r-ésimas da unidade em $\mathbb{C}$, são então $z^j (j = 1, \ldots, p^r)$. E as raízes primitivas p^r-ésimas da unidade são as z^j tais que j não seja múltiplo de p. Portanto, existe um número de

$$\varphi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1)$$

raízes primitivas p^r-ésimas da unidade, onde φ é a função de Euler.

Estas raízes primitivas p^r-ésimas da unidade são as raízes do polinômio ciclotômico,

$$F(X) = \frac{X^{p^r} - 1}{X^{p^{r-1}} - 1} = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \ldots + X^{p^{r-1}} + 1. \qquad (3.3)$$

Note que, $w^{p^{r-1}} \neq 1$ para qualquer w raiz primitiva p^r-ésima da unidade.

O nosso objetivo agora é mostrar que $[\mathbb{Q}[z] : \mathbb{Q}] = p^{r-1}(p-1)$, isto é, que $F(X)$ é irredutível sobre $\mathbb{Q}$.

Ponhamos $e = p^{r-1}(p-1)$ e sejam $z_1, \ldots, z_e$ as raízes primitivas p^r-ésimas da unidade. Temos que,

$$F(X+1) = (X+1)^{p^{r-1}(p-1)} + (X+1)^{p^{r-1}(p-2)} + \ldots + (X+1)^{p^{r-1}} + 1.$$

Logo, o termo constante de $F(X+1)$ é,

$$F(0+1) = (0+1)^{p^{r-1}(p-1)} + (0+1)^{p^{r-1}(p-2)} + \ldots + (0+1)^{p^{r-1}} + 1 = p.$$

Afirmação 3.3

$$\prod_{j=1}^{e}(z_j - 1) = \pm p.$$

Com efeito,

$$F(X) = \prod_{j=1}^{e}(X - z_j) = (-1)^e \cdot \prod_{j=1}^{e}(z_j - X).$$

$$F(1) = (-1)^e \cdot \prod_{j=1}^{e}(z_j - 1) \Rightarrow p = \pm 1 \cdot \prod_{j=1}^{e}(z_j - 1) \Rightarrow \prod_{j=1}^{e}(z_j - 1) = \pm p.$$

Neste caso, temos que o anel dos inteiros de $\mathbb{Q}[z]$ é $B = \mathbb{Z}[z]$. É claro que, $z_j \in B$ (pois, $z_j \in \mathbb{Q}[z]$ e z_j é raiz de $F(X) \in \mathbb{Z}[X]$).

Note também que, os ideais $B(z_k - 1)$ são todos iguais, isto é, $B(z_k - 1) = B(z_j - 1), k \neq j$. Com efeito, para $k \neq j$ temos que z_j, z_k são geradores do grupo cíclico G das raízes p^r-ésimas da unidade.

$$G = \langle z_j \rangle \tag{3.4}$$

$$G = \langle z_k \rangle \tag{3.5}$$

Mas, z_j é uma raiz p^r-ésima da unidade, logo, de (3.5) temos que $z_j = z_k^q$. Por outro lado, z_k é uma raiz p^r-ésima da unidade, logo, de (3.4) temos que $z_k = z_j^s$.

$$\begin{aligned}
\hookrightarrow x \in B(z_k-1) &\Rightarrow x = b(z_k-1), b \in B \\
&\Rightarrow x = b(z_j^s-1) = b\cdot(z_j-1)\cdot(z_j^{s-1}+\ldots+z_j+1) = \\
&= \underbrace{b}_{\in B}\cdot\underbrace{(z_j^{s-1}+\ldots+z_j+1)}_{\in B}(z_j-1) \in B(z_j-1) \\
&\therefore B(z_k-1) \subset B(z_j-1).
\end{aligned}$$

$$\begin{aligned}
\hookrightarrow x \in B(z_j-1) &\Rightarrow x = b(z_j-1), b \in B \\
&\Rightarrow x = b(z_k^q-1) = b\cdot(z_k-1)\cdot(z_k^{q-1}+\ldots+z_k+1) = \\
&= \underbrace{b}_{\in B}\cdot\underbrace{(z_k^{q-1}+\ldots+z_k+1)}_{\in B}(z_k-1) \in B(z_k-1) \\
&\therefore B(z_j-1) \subset B(z_k-1).
\end{aligned}$$

E daí, $Bp = B(z_1-1)^e$. Com efeito,

$$\begin{aligned}
Bp &= B(\pm p) = B\left(\prod_{j=1}^{e}(z_j-1)\right) = B\left((z_1-1)\cdot(z_2-1)\cdot\ldots\cdot(z_e-1)\right) \\
&= B(z_1-1)\cdot B(z_2-1)\cdot\ldots B(z_e-1) \qquad \underbrace{=}_{\text{Os } B(z_k-1) \text{ são todos iguais}} \\
&= B(z_1-1)\cdot B(z_1-1)\cdot\ldots B(z_1-1) \\
&= B\left((z_1-1)\cdot(z_1-1)\cdot\ldots\cdot(z_1-1)\right) = B(z_1-1)^e.
\end{aligned}$$

Como B é de Dedekind, então

$$Bp = \prod_{i=1}^{q}\mathcal{B}_i^{e_i}$$

onde os $\mathcal{B}_i's$ são ideais primos de B. Temos que $Bp = B(z_1-1)^e = (B(z_1-1))^e$. Logo a decomposição de $B(z_1-1)$ em produtos de ideais primos, deve necessariamente, apresentar os mesmos ideais primos que aparecem na decomposição de

Bp, caso contrário, perderíamos a unicidade da decomposição de Bp em produto de ideais primos. Então

$$B(z_1 - 1) = \prod_{i=1}^{q} \mathcal{B}_i^{e_i'}.$$

E daí,

$$Bp = (B(z_1 - 1))^e = \left(\prod_{i=1}^{q} \mathcal{B}_i^{e_i'} \right)^e = \prod_{i=1}^{q} \mathcal{B}_i^{e_i' e}.$$

Usando agora a unicidade da decomposição de Bp em produto de ideais primos, concluímos que,

$$e_i = e_i' e, \forall i \quad \Rightarrow \quad e | e_i, \forall i \quad \Rightarrow \quad e_i \quad \text{é múltiplo de} \quad e, \forall i.$$

Pelo Teorema 3.1,

$$\sum_{i=1}^{q} e_i f_i = [B/Bp\mathbb{Z} : \mathbb{Z}/p\mathbb{Z}] = [\mathbb{Q}[z] : \mathbb{Q}] \underbrace{\leq}_{(3.3)} e.$$

Com isso,

$$e \geq e_1 f_1 + \ldots + e_q f_q \underbrace{=}_{e|e_i, \forall i} r_1 e f_1 + \ldots + r_q e f_q = (r_1 f_1 + \ldots + r_q f_q) e \geq$$
$$\geq 1 \cdot e = e \Rightarrow e = e_1 f_1 + \ldots + e_q f_q = [\mathbb{Q}[z] : \mathbb{Q}] \Rightarrow$$
$$\Rightarrow [\mathbb{Q}[z] : \mathbb{Q}] = e = p^{r-1}(p-1).$$

Da igualdade, $e = e_1 f_1 + \ldots + e_q f_q$ e do fato de $e|e_i, \forall i$ concluímos que,

$$e = e_1 f_1 \Rightarrow e = r_1 e f_1 \Rightarrow r_1 f_1 = 1 \Rightarrow r_1 = 1 \quad \text{e} \quad f_1 = 1 \Rightarrow e_1 = e \quad \text{e} \quad f_1 = 1.$$

Logo,

$$Bp = \mathcal{B}_1^{e_1} = (B(z_1 - 1))^e = (B(z_1 - 1))^{e_1} \Rightarrow \mathcal{B}_1 = B(z_1 - 1)$$

$$\Rightarrow B(z_1 - 1) \quad \text{é um ideal primo de B de grau residual} \quad f_1 = 1.$$

Resumindo, temos o seguinte:

(a) $[\mathbb{Q}[z] : \mathbb{Q}] = e = p^{r-1}(p-1)$.

(b) $B(z_1 - 1)$ é um ideal primo de B, de grau residual 1.

(c) $Bp = B(z_1 - 1)^e$.

3.4 Discriminação e Ramificação

Com as mesmas notações (ou seja, $B\mathfrak{p} = \prod_{i=1}^{q} \mathcal{B}_i^{e_i}$), dizemos que um ideal primo $\mathfrak{p}$ de A se ramifica em B (ou em L) se um dos índices de ramificação e_i é maior ou igual a 2. Diremos também que L é não ramificada se nenhum ideal primo $\mathfrak{p}$ de A se ramifica em B (ou em L).

Fazendo uso da teoria dos discriminantes, iremos agora determinar os ideais primos de A que se ramificam em B, e ver que existe somente um número finito de tais ideais. Alguns lemas sobre discriminantes serão úteis.

Definição 3.3 *Sejam B um anel e A um subanel de B tal que B seja um A-módulo livre de dimensão finita. Se chama discriminante de B sobre A, e se escreve $\mathcal{D}_{B/A}$, ao ideal principal de A gerado pelo discriminante de qualquer base de B sobre A.*

Lema 3.4 *Sejam A um anel, $B_1, \ldots, B_q$ anéis que contém A e que são A-módulos livres de dimensão finita e $B = \prod_{i=1}^{q} B_i$ seu anel produto. Então,*

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

Demonstração: Basta demonstrar para $q = 2$, pois o resultado ficará provado usando recorrência e também o seguinte fato:

$$B = B_1 \times B_2 \Rightarrow \mathcal{D}_{B/A} = \mathcal{D}_{B_1/A} \cdot \mathcal{D}_{B_2/A}.$$

Sejam então $(x_1, \ldots, x_m)$ e $(y_1, \ldots, y_n)$ bases de B_1 sobre A e de B_2 sobre A, respectivamente. Com a identificação clássica de B_1 e B_2 com $B_1 \times (0)$ e $(0) \times B_2$, tem-se que $(x_1, \ldots, x_m, y_1, \ldots, y_n)$ é uma base de $B = B_1 \times B_2$ sobre A. Usando a definição da estrutura de anel produto, podemos também concluir que, $x_i y_j = 0$. Veja,

$$\left.\begin{array}{rcl} x_i \in B_1 \sim B_1 \times (0) & \Rightarrow & x_i = (a_{1i}, \ldots, a_{mi}, 0, \ldots, 0) \\ y_j \in B_2 \sim (0) \times B_2 & \Rightarrow & y_j = (0, \ldots, 0, b_{1j}, \ldots, b_{nj}) \end{array}\right| \Rightarrow$$

$$\Rightarrow x_i y_j = a_{1i} \cdot 0 + \ldots + a_{mi} \cdot 0 + 0 \cdot b_{1j} + \ldots + 0 \cdot b_{nj} = 0.$$

E daí, $\mathrm{Tr}(x_i y_j) = 0$. Assim, o determinante $D(x_1, \ldots, x_m, y_1, \ldots, y_n)$ se escreve do seguinte modo:

$$\left|\begin{array}{cc} \mathrm{Tr}(x_i x_{i'}) & O \\ O & \mathrm{Tr}(y_j y_{j'}) \end{array}\right| = \det\left(\mathrm{Tr}(x_i x_{i'})\right) \cdot \det\left(\mathrm{Tr}(y_j y_{j'})\right).$$

Portanto,

$$D(x_1, \ldots, x_m, y_1, \ldots, y_n) = D(x_1, \ldots, x_m) \cdot D(y_1, \ldots, y_n).$$

■

Lema 3.5 *Sejam B um anel, A um subanel de B e $\mathfrak{a}$ um ideal de A. Assuma que B é um A-módulo livre com base $(x_1, \ldots, x_n)$. Para $x \in B$ escreva $\overline{x}$ para a classe residual de x em $B/\mathfrak{a}B$. Então, $(\overline{x_1}, \ldots, \overline{x_n})$ é uma base de $B/\mathfrak{a}B$ sobre $A/\mathfrak{a}$ e além disso,*

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

Demonstração: Ver [10], página 73.

Definição 3.4 *Dado um anel A, uma A-álgebra é um anel B dotado de um homomorfismo $\varphi : A \to B$. Se A é um corpo, φ é injetivo, e identificamos então A com sua imagem $\varphi(A)$ (que é um subanel de B).*

Sejam $\varphi : A \to B$ homomorfismo e A corpo. Então,

$$\mathrm{Ker}\varphi \quad \text{é um ideal de} \quad A \quad \underbrace{\Rightarrow}_{\text{A é corpo}} \quad \mathrm{Ker}\varphi = \{0\} \quad \text{ou} \quad \mathrm{Ker}\varphi = A$$

$\Rightarrow$ $\mathrm{Ker}\varphi = \{0\}$, pois $\varphi(e_A) = e_B$

onde e_A e e_B são as identidades multiplicativas de A e B

$\Rightarrow$ φ é injetivo.

Lema 3.6 *Em um anel noetheriano reduzido A, o ideal (0) é interseção finita de ideais primos.*

Demonstração: Ver [10], página 65.

Proposição 3.3 *Sejam B um domínio de integridade e A um subanel de B tal que B seja inteiro sobre A. Então, B é corpo se, e somente se, A é corpo.*

Demonstração: Ver [10], página 29.

Lema 3.7 *Sejam K um corpo finito ou de característica zero, e L uma K-álgebra de dimensão finita sobre K. Para que L seja reduzida (isto é, 0 (zero) é o único elemento nilpotente de L), é necessário e suficiente que $\mathcal{D}_{L/K} \neq (0)$.*

Observação 3.1 **(i)** *$\mathcal{D}_{L/K}$ é ideal principal de K gerado pelo discriminante de qualquer base de L sobre K.*

(ii) *Sendo L uma K-álgebra, existe então um homomorfismo injetivo $\varphi : K \to L$. E daí, podemos identificar K a um subanel de $L(k \leftrightarrow \varphi(k))$.*

Demonstração (Lema 3.7): ($\Leftarrow$) Suponha que L não é reduzida e $\mathcal{D}_{L/K} \neq (0)$. Seja então $x \in L$ um elemento nilpotente não nulo (existe tal elemento, pois, 0 (zero) não é o único elemento nilpotente de L). Seja $x_1 = x$. Como o elemento $x_1 = x \neq 0$ então podemos construir uma base de L sobre K a partir desse elemento. Seja $(x_1, \ldots, x_n)$ tal base. Logo, x_1x_j é nilpotente.

Afirmação 3.4 $\begin{array}{rccc} m_{x_1x_j}: & L & \to & L \\ & y & \mapsto & x_1x_jy \end{array}$ *é um endomorfismo nilpotente.*

Com efeito,

$$m_{x_1x_j}(y_1 + y_2) = x_1x_j(y_1 + y_2) = x_1x_jy_1 + x_1x_jy_2 = m_{x_1x_j}(y_1) + m_{x_1x_j}(y_2).$$

Seja $y \in L$ nilpotente, logo, $y^m = 0$ para algum m. Então,

$$\big(m_{x_1x_j}(y)\big)^m = (x_1x_jy)^m = (x_1x_j)^m \cdot y^m = 0 \Rightarrow m_{x_1x_j}(y) \quad \text{é nilpotente.}$$

E daí, todos os valores próprios de $m_{x_1x_j}$ são nulos. E com isso,

$$\mathrm{Tr}(x_1x_j) = \mathrm{Tr}(m_{x_1x_j}) = 0.$$

Logo, a matriz de $(\mathrm{Tr}(x_1x_j))$ tem uma fila nula. Veja,

$$\begin{bmatrix} 0 & 0 & \ldots & 0 \\ \mathrm{Tr}(x_2x_1) & \mathrm{Tr}(x_2x_2) & \ldots & \mathrm{Tr}(x_2x_n) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}(x_nx_1) & \mathrm{Tr}(x_nx_2) & \ldots & \mathrm{Tr}(x_nx_n) \end{bmatrix}.$$

Com isso,

$$\det(\mathrm{Tr}(x_ix_j)) = 0 \Rightarrow D(x_1, \ldots, x_n) = 0 \Rightarrow \mathcal{D}_{L/K} = (0) \quad \text{(CONTRADIÇÃO)}.$$

($\Rightarrow$) Suponha agora que L é reduzida. Temos que L é um K-módulo de tipo finito, logo todo sub-K-módulo de L é de tipo finito. Como todo sub-L-módulo

de L é um sub-K-módulo de L, então concluímos que, todo sub-L-módulo de L é de tipo finito. Portanto, L é um anel noetheriano. E além disso, L é reduzido. Logo, pelo Lema 3.6, o ideal (0) de L é interseção finita de ideais primos de L, isto é,

$$(0) = \bigcap_{i=1}^{q} \mathcal{B}_i,$$

onde $\mathcal{B}_i$ é ideal primo de L, $\forall i$.

Afirmação 3.5 *$L/\mathcal{B}_i$ é uma álgebra de integridade de dimensão finita sobre K.*

Com efeito, $L/\mathcal{B}_i$ é de integridade (pois, $\mathcal{B}_i$ é ideal de L) e é uma K-álgebra (pois, $\begin{array}{ccc} \varphi : K & \to & L/\mathcal{B}_i \\ k & \mapsto & k + \mathcal{B}_i \end{array}$ é um homomorfismo). Considere agora $(x_1, \ldots, x_n)$ base de L sobre K. Então, $L/\mathcal{B}_i$ é uma K-combinação linear de $x_1 + \mathcal{B}_i, \ldots, x_n + \mathcal{B}_i$. Vejamos:

Como K é corpo então $\begin{array}{ccc} \varphi : K & \to & L/\mathcal{B}_i \\ k & \mapsto & k + \mathcal{B}_i \end{array}$ é um homomorfismo injetivo, e daí, podemos identificar K a um subanel de $L/\mathcal{B}_i$.

$$k \in K \leftrightarrow \varphi(k) = k + \mathcal{B}_i \tag{3.6}$$

$$\begin{aligned} x \in L/\mathcal{B}_i \quad &\Rightarrow \quad x = l + \mathcal{B}_i, l \in L \\ &\Rightarrow \quad x = (k_1x_1 + \ldots + k_nx_n) + \mathcal{B}_i, k_j \in K \\ &\Rightarrow \quad x = (k_1x_1 + \mathcal{B}_i) + \ldots + (k_nx_n + \mathcal{B}_i), k_j \in K \\ &\Rightarrow \quad x = (k_1 + \mathcal{B}_i)(x_1 + \mathcal{B}_i) + \ldots + (k_n + \mathcal{B}_i)(x_n + \mathcal{B}_i), k_j \in K \\ &\underbrace{\Rightarrow}_{(3.6)} \quad x = k_1(x_1 + \mathcal{B}_i) + \ldots + k_n(x_n + \mathcal{B}_i), k_j \in K \end{aligned}$$

Temos que $L/\mathcal{B}_i$ é um anel de divisão e K é um subanel de $L/\mathcal{B}_i$ que é corpo, logo, $L/\mathcal{B}_i$ é um espaço vetorial sobre K. Como $\{x_1 + \mathcal{B}_i, \ldots, x_n + \mathcal{B}_i\}$ é um

conjunto de geradores de $L/\mathcal{B}_i$ sobre K, então podemos extrair dele uma base de $L/\mathcal{B}_i$ sobre K. Portanto, $L/\mathcal{B}_i$ é uma K-álgebra de integridade de dimensão finita.

Afirmação 3.6 *$L/\mathcal{B}_i$ é inteiro sobre K.*

Com efeito, $[L/\mathcal{B}_i : K] < \infty$ então o anel $L/\mathcal{B}_i$ é algébrico sobre K. Como K é corpo então $L/\mathcal{B}_i$ é inteiro sobre K. E daí, pela Proposição 3.3, $L/\mathcal{B}_i$ é corpo. Logo, $\mathcal{B}_i$ é ideal maximal de L.

Afirmação 3.7 *$\mathcal{B}_i + \mathcal{B}_j = L$ para $i \neq j$.*

Com efeito,

$$\mathcal{B}_i \subset \mathcal{B}_i + \mathcal{B}_j \subset L \quad \underbrace{\Rightarrow}_{\mathcal{B}_i \text{ é ideal maximal de } L} \quad \Rightarrow \mathcal{B}_i + \mathcal{B}_j = \mathcal{B}_i \quad \text{ou} \quad \mathcal{B}_i + \mathcal{B}_j = L.$$

A igualdade $\mathcal{B}_i + \mathcal{B}_j = \mathcal{B}_i$ não pode ocorrer para $i \neq j$. Vejamos,

$$\mathcal{B}_j \subset \mathcal{B}_i + \mathcal{B}_j = \mathcal{B}_i \subset L \quad \underbrace{\Rightarrow}_{\mathcal{B}_j \text{ é ideal maximal de } L} \quad \mathcal{B}_i = \mathcal{B}_j \quad \text{ou} \quad \mathcal{B}_i = L \Rightarrow$$

$$\Rightarrow \mathcal{B}_i = \mathcal{B}_j \quad \text{(CONTRADIÇÃO)}.$$

Temos que, $\begin{array}{ccc} \varphi : L & \to & L/\mathcal{B}_1 \cdot \ldots \cdot \mathcal{B}_q \\ l & \mapsto & l + \mathcal{B}_1 \cdot \ldots \cdot \mathcal{B}_q \end{array}$ é um isomorfismo, pois

$$\mathrm{Ker}\varphi = \mathcal{B}_1 \cdot \ldots \cdot \mathcal{B}_q \subset \mathcal{B}_1 \cap \mathcal{B}_2 \cap \ldots \cap \mathcal{B}_q = (0) \Rightarrow \mathrm{Ker}\varphi = (0).$$

Além disso, o Lema 3.3 nos garante que, $L/\mathcal{B}_1 \cdot \ldots \cdot \mathcal{B}_q$ é isomorfo ao produto $\prod_{i=1}^{q} L/\mathcal{B}_i$. Logo, L é isomorfo ao produto $\prod_{i=1}^{q} L/\mathcal{B}_i$.

E daí, pelo Lema 3.4 concluímos que,

$$\mathcal{D}_{L/K} = \prod_{i=1}^{q} \mathcal{D}_{(L/\mathcal{B}_i)/K}.$$

Observe que, $L/\mathcal{B}_i$ é um K-módulo livre de dimensão finita, pois $L/\mathcal{B}_i$ é uma K-álgebra de dimensão finita.

Por outro lado, como K é finito ou de característica zero, então pela Proposição 1.2,

$$\mathcal{D}_{(L/\mathcal{B}_i)/K} \neq (0).$$

Portanto,

$$\mathcal{D}_{L/K} \neq (0).$$

■

Definição 3.5 *Sejam K e L dois corpos numéricos com $K \subset L$, A e B os anéis dos inteiros de K e L. Se chama ideal discriminante de B sobre A (ou de L sobre K), e se escreve $\mathcal{D}_{B/A}$ ou $\mathcal{D}_{L/K}$ ao ideal de A gerado pelos discriminantes das bases de L sobre K que estão contidas em B.*

Nota 3.1 *Se $(x_1, \ldots, x_n)$ é uma base de L sobre K contida em B então $\mathrm{Tr}_{L/K}(x_i x_j) \in A$.*

Com efeito,

$x_i, x_j \in B \Rightarrow x_i x_j \in B \Rightarrow x_i x_j$ é um elemento de L que é inteiro sobre A.

A é o anel dos inteiros de K $\Rightarrow$ A é de Dedekind $\Rightarrow$

$\Rightarrow$ A é integralmente fechado.

Logo, pelo Corolário 1.4, $\mathrm{Tr}_{L/K}(x_i x_j) \in A$.

E daí,

$$D(x_1, \ldots, x_n) = \det\left(\mathrm{Tr}(x_i x_j)\right) \in A.$$

Assim,

$$\mathcal{D}_{B/A} = D(x_1, \ldots, x_n)A \subset A$$

é um ideal inteiro de A. E além disso, pela Proposição 1.2, $D(x_1, \ldots, x_n) \neq 0$. Portanto,

$$\mathcal{D}_{B/A} \neq (0).$$

Nota 3.2 *Quando B é um A-módulo livre (por exemplo, se A é principal) já definimos o ideal discriminante $\mathcal{D}_{B/A}$ como o ideal gerado por $D(e_1, \ldots, e_n)$ onde $(e_1, \ldots, e_n)$ é uma base de B sobre A (Definição 3.3). Esta definição coincide com a que acabamos de apresentar, pois para toda base (x_i) de L sobre K contida em B, tem-se que,*

$$x_j = \sum_j a_{ij} e_j \quad \textit{com} \quad a_{ij} \in A.$$

E daí, pela Proposição 1.1 temos que,

$$D(x_1, \ldots, x_n) = \underbrace{\det(a_{ij})^2}_{\in A} \cdot \underbrace{D(e_1, \ldots, e_n)}_{\in A} \in A.$$

Teorema 3.8 *Com as notações da definição, para que um ideal primo $\mathfrak{p}$ de A se ramifique em B, é necessário e suficiente que $\mathfrak{p}$ contenha o ideal discriminante $\mathcal{D}_{B/A}$. E além disso, existe somente um número finito de ideais primos de A que se ramificam em B.*

Demonstração: A segunda afirmação segue-se da primeira. Senão vejamos, A é de Dedekind e $\mathcal{D}_{B/A}$ é um ideal não nulo de A. Logo,

$$\mathcal{D}_{B/A} = \mathfrak{p}_1^{c_1} \mathfrak{p}_2^{c_2} \cdot \ldots \cdot \mathfrak{p}_s^{c_s}$$

onde os $\mathfrak{p}_j$ são ideais primos não nulos de A distintos dois a dois e os $1 \leq c_j \in \mathbb{Z}$.

Considere agora $\mathfrak{p}$ um ideal primo de A que se ramifica em B. Usando a

primeira afirmação do Teorema 3.8, temos que,

$$\begin{aligned}
\mathfrak{p}_1^{c_1}\mathfrak{p}_2^{c_2}\cdot\ldots\cdot\mathfrak{p}_s^{c_s}\subset\mathfrak{p} \quad &\underbrace{\Rightarrow}_{\mathfrak{p}\text{ é ideal primo}} \quad \mathfrak{p}_j^{c_j}\subset\mathfrak{p}, \text{para algum j}\\
&\underbrace{\Rightarrow}_{\mathfrak{p}\text{ é ideal primo}} \quad \mathfrak{p}_j\subset\mathfrak{p}\subset A, \text{para algum j}\\
&\underbrace{\Rightarrow}_{\mathfrak{p}_j\text{ é ideal maximal}} \quad \mathfrak{p}=\mathfrak{p}_j, \text{para algum j}\\
&\Rightarrow \quad \mathfrak{p} \quad \text{é um ideal primo de A que aparece na decomposição de} \quad \mathcal{D}_{B/A}.
\end{aligned}$$

Como há somente um número finito de ideais primos de A que aparecem na decomposição de $\mathcal{D}_{B/A}(\mathfrak{p}_1,\mathfrak{p}_2,\ldots,\mathfrak{p}_s)$, então existe somente um número finito de ideais primos de A que se ramificam em B.

Vamos então agora demonstrar a primeira afirmação.

Seja $\mathfrak{p}$ um ideal primo de A. Como B é de Dedekind, então,

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

onde os $\mathcal{B}_i'$s são ideais primos não nulos de B distintos dois a dois e os $1\leq e_i's\in\mathbb{Z}$. Pela Proposição 3.2 temos que

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

Afirmação 3.8 $\mathfrak{p}$ *se ramifica em* $B\Leftrightarrow B/B\mathfrak{p}$ *é não reduzido.*

Suponha que $\mathfrak{p}$ se ramifica em B então existe $e_j\geq 2$ para algum j. Seja $c_j\in\mathcal{B}_j$ não nulo. Logo,

$$x=\left(0+\mathcal{B}_1^{e_1},0+\mathcal{B}_2^{e_2},\ldots,c_j+\mathcal{B}_j^{e_j},0+\mathcal{B}_{j+1}^{e_{j+1}},\ldots,0+\mathcal{B}_q^{e_q}\right)\in\prod_{i=1}^{q}B/\mathcal{B}_i^{e_i}\simeq B/B\mathfrak{p}.$$

E daí,

$$\begin{aligned} x^{e_j} &= \left(0^{e_j}+\mathcal{B}_1^{e_1}, 0^{e_j}+\mathcal{B}_2^{e_2}, \ldots, c_j^{e_j}+\mathcal{B}_j^{e_j}, 0^{e_j}+\mathcal{B}_{j+1}^{e_{j+1}}, \ldots, 0^{e_j}+\mathcal{B}_q^{e_q}\right) \\ &= \left(0+\mathcal{B}_1^{e_1}, 0+\mathcal{B}_2^{e_2}, \ldots, 0+\mathcal{B}_j^{e_j}, 0+\mathcal{B}_{j+1}^{e_{j+1}}, \ldots, 0+\mathcal{B}_q^{e_q}\right), \end{aligned}$$

ou seja, x é um elemento nilpotente não nulo de $B/B\mathfrak{p}$. Portanto, $B/B\mathfrak{p}$ é não reduzido.

Mostraremos agora que quando o anel $B/\mathfrak{p}B \simeq \prod_{i=1}^{q} B/\mathcal{B}_i^{e_i}$ é não reduzido então $\mathfrak{p}$ se ramifica em B.

Suponha que $\mathfrak{p}$ não se ramifique em B. Então, os índices de ramificação e_i são todos iguais a 1. E daí,

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

Considere agora, $(b_1+\mathcal{B}_1, \ldots, b_q+\mathcal{B}_q) \in B/\mathfrak{p}B \simeq \prod_{i=1}^{q} B/\mathcal{B}_i$ um nilpotente qualquer. Logo, existe um inteiro positivo m tal que,

$$(b_1+\mathcal{B}_1, \ldots, b_q+\mathcal{B}_q)^m = (0+\mathcal{B}_1, \ldots, 0+\mathcal{B}_q) \Rightarrow$$

$$\Rightarrow \begin{cases} b_1^m+\mathcal{B}_1 = 0+\mathcal{B}_1 \\ \vdots \\ b_q^m+\mathcal{B}_q = 0+\mathcal{B}_q \end{cases} \Rightarrow \begin{cases} b_1^m \in \mathcal{B}_1 \\ \vdots \\ b_q^m \in \mathcal{B}_q \end{cases} \underbrace{\Rightarrow}_{\mathcal{B}_i \text{ é ideal primo de } B}$$

$$\Rightarrow \begin{cases} b_1 \in \mathcal{B}_1 \\ \vdots \\ b_q \in \mathcal{B}_q \end{cases} \Rightarrow \begin{cases} b_1+\mathcal{B}_1 = 0+\mathcal{B}_1 \\ \vdots \\ b_q+\mathcal{B}_q = 0+\mathcal{B}_q \end{cases}$$

Com isso, não existe elemento nilpotente não nulo de $B/B\mathfrak{p}$. Portanto, o anel $B/B\mathfrak{p}$ é reduzido.

Por outro lado, o Lema 3.7 nos garante que,

$$B/B\mathfrak{p} \quad \text{é não reduzido} \Leftrightarrow \mathcal{D}_{(B/B\mathfrak{p})/(A/\mathfrak{p})} = (0),$$

já que $A/\mathfrak{p}$ é um corpo finito e $B/B\mathfrak{p}$ é uma $A/\mathfrak{p}$-álgebra de dimensão finita sobre $A/\mathfrak{p}$.

$$\begin{array}{ccccc} A & \to & B & \to & B/B\mathfrak{p} \\ a & \mapsto & a & \mapsto & a+B\mathfrak{p} \end{array} \quad , \quad \begin{array}{ccc} A & \stackrel{\varphi}{\to} & B/B\mathfrak{p} \\ a & \mapsto & a+B\mathfrak{p} \end{array} \quad \text{homomorfismos.}$$

$$\mathrm{Ker}\varphi = B\mathfrak{p} \cap A = \mathfrak{p},$$

$\exists!\ \overline{\varphi} : A/\mathfrak{p} \to B/B\mathfrak{p}$ homomorfismo injetivo tal que, $\varphi = \overline{\varphi} \circ h$ onde

$$h: \begin{array}{ccc} A & \to & A/\mathfrak{p} \\ a & \mapsto & a+\mathfrak{p} \end{array}$$ é o homomorfismo canônico.

$$a + \mathfrak{p} \leftrightarrow \varphi(a+\mathfrak{p}) = a + B\mathfrak{p}$$

Ponhamos $S = A - \mathfrak{p}, A' = S^{-1}A, B' = S^{-1}B$ e $\mathfrak{p}' = \mathfrak{p}A'$. Então, A' é um anel principal (Proposição 2.4), B' é um A-módulo livre, e além disso, pela Proposição 2.5 tem-se que,

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

Seja $(e_1, \ldots, e_n)$ uma base de B' sobre A'. Pelo Lema 3.5 $(\overline{e_1}, \ldots, \overline{e_n})$ é base de $B'/\mathfrak{p}'B'$ sobre $A'/\mathfrak{p}'$ e $D(\overline{e_1}, \ldots, \overline{e_n}) = \overline{D(e_1, \ldots, e_n)} \in A'/\mathfrak{p}'$, onde $\overline{e_i}$ é a classe de e_i em $B'/\mathfrak{p}'B'$.

Como $A/\mathfrak{p} \simeq A'/\mathfrak{p}'$ e $B/\mathfrak{p}B \simeq B'/\mathfrak{p}'B'$ então $(\overline{e_1}, \ldots, \overline{e_n})$ é base de $B/\mathfrak{p}B$ sobre $A/\mathfrak{p}$. Logo,

$$\mathcal{D}_{(B/B\mathfrak{p})/(A/\mathfrak{p})} = D(\overline{e_1}, \ldots, \overline{e_n})A/\mathfrak{p}.$$

E daí temos a seguinte equivalência,

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

Com efeito,

$$D(e_1, \ldots, e_n) \in \mathfrak{p}' \Leftrightarrow D(e_1, \ldots, e_n) - 0 \in \mathfrak{p}' \Leftrightarrow \overline{D(e_1, \ldots, e_n)} = \overline{0} \Leftrightarrow$$

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

Temos então que,

$$\mathfrak{p} \quad \text{se ramifica em} \quad B \Leftrightarrow \mathcal{D}_{(B/B\mathfrak{p})/(A/\mathfrak{p})} = (\overline{0}) \Leftrightarrow D(e_1, \ldots, e_n) \in \mathfrak{p}',$$

onde $(e_1, \ldots, e_n)$ é base de B' sobre A'.

Logo, se $D(e_1, \ldots, e_n) \in \mathfrak{p}'$ e $(x_1, \ldots, x_n)$ é uma base de L sobre K contida em B então,

$$x_i = \sum a'_{ij} e_j \quad \text{com} \quad a'_{ij} \in A' \quad (\text{pois, } B \subset B').$$

Em decorrência disso,

$$D(x_1, \ldots, x_n) = \underbrace{\det(a'_{ij})^2}_{\in A'} \cdot \underbrace{D(e_1, \ldots, e_n)}_{\in \mathfrak{p}'} \quad \underbrace{\Rightarrow}_{\mathfrak{p}' \text{ é ideal de } A'} \quad D(x_1, \ldots, x_n) \in \mathfrak{p}'.$$

Como $\mathfrak{p}' \cap A = \mathfrak{p}$ então podemos deduzir que $D(x_1, \ldots, x_n) \in \mathfrak{p}$, já que $D(x_1, \ldots, x_n) \in A$ pela Nota 3.1.

E daí,

$$\mathcal{D}_{B/A} = \underbrace{D(x_1, \ldots, x_n)}_{\in \mathfrak{p}} A \subset \mathfrak{p} \Rightarrow \mathcal{D}_{B/A} \subset \mathfrak{p}.$$

Ou seja, quando $\mathfrak{p}$ se ramifica em B vale a seguinte inclusão $\mathfrak{p} \supset \mathcal{D}_{B/A}$. Reciprocamente, se $\mathfrak{p} \supset \mathcal{D}_{B/A}$ então $D(e_1, \ldots, e_n) \in \mathfrak{p}'$ (isto é, $\mathfrak{p}$ se ramifica em B). Com efeito, como $e_i \in B' = S^{-1}B$ então podemos escrever, $e_i = \dfrac{y_i}{s}$ com $y_i \in B$ e $s \in S$ para $1 \leq i \leq n$. Consequentemente,

$$D(e_1, \ldots, e_n) = s^{-2n} \cdot D(y_1, \ldots, y_n) \in A'\mathcal{D}_{B/A} \subset A'\mathfrak{p} = \mathfrak{p}' \Rightarrow$$

$$\Rightarrow D(e_1, \ldots, e_n) \in \mathfrak{p}' \Rightarrow \mathfrak{p} \quad \text{se ramifica em} \quad B.$$

■

3.5 Ideais primos que se ramificam em um corpo quadrático

Tomemos $K = \mathbb{Q}$ e $L = \mathbb{Q}[\sqrt{d}]$ onde d é um inteiro sem fatores quadrados.

(a) Se $d \equiv 2$ ou $3 (\mathrm{mod}\ 4)$ então $(1, \sqrt{d})$ é uma base do anel B dos inteiros de $L = \mathbb{Q}[\sqrt{d}]$. Como $\mathrm{Tr}(1) = 2, \mathrm{Tr}(\sqrt{d}) = 0$ e $\mathrm{Tr}(d) = 2d$ então,

$$\begin{aligned} D(1, \sqrt{d}) &= \det \begin{bmatrix} \mathrm{Tr}(1 \cdot 1) & \mathrm{Tr}(1 \cdot \sqrt{d}) \\ \mathrm{Tr}(\sqrt{d} \cdot 1) & \mathrm{Tr}(\sqrt{d} \cdot \sqrt{d}) \end{bmatrix} \\ &= \det \begin{bmatrix} \mathrm{Tr}(1) & \mathrm{Tr}(\sqrt{d}) \\ \mathrm{Tr}(\sqrt{d}) & \mathrm{Tr}(d) \end{bmatrix} = \det \begin{bmatrix} 2 & 0 \\ 0 & 2d \end{bmatrix} = 4d. \end{aligned}$$

O ideal discriminante $\mathcal{D}_{B/\mathbb{Z}}$ é um ideal de $\mathbb{Z}$ gerado por $D(1, \sqrt{d})$, isto é, $\mathcal{D}_{B/\mathbb{Z}} = 4d\mathbb{Z}$.

Um ideal primo $p\mathbb{Z}$ de $\mathbb{Z}$ se ramifica em B se, e só se, $4d\mathbb{Z} \subset p\mathbb{Z}$ se, e só se, p divide $4d$. Como p é primo então $p = 2$ ou p é um divisor primo de d. Portanto, os ideais primos de $\mathbb{Z}$ que se ramificam em B (ou em $L = \mathbb{Q}[\sqrt{d}]$) são $2\mathbb{Z}$ e $p\mathbb{Z}$ onde p é um divisor primo de d.

(b) Se $d \equiv 1 (\mathrm{mod}\ 4)$ então $\left(1, \dfrac{1+\sqrt{d}}{2}\right)$ é uma base do anel dos inteiros de $L = \mathbb{Q}[\sqrt{d}]$.

Como $\mathrm{Tr}(1) = 2, \mathrm{Tr}\left(\dfrac{1+\sqrt{d}}{2}\right) = 1$ e $\mathrm{Tr}\left(\left(\dfrac{1+\sqrt{d}}{2}\right)^2\right) = \dfrac{d+1}{2}$

então,

$$D\left(1, \frac{1+\sqrt{d}}{2}\right) = \det \begin{bmatrix} \mathrm{Tr}(1) & \mathrm{Tr}\left(\frac{1+\sqrt{d}}{2}\right) \\ \mathrm{Tr}\left(\frac{1+\sqrt{d}}{2}\right) & \mathrm{Tr}\left(\left(\frac{1+\sqrt{d}}{2}\right)^2\right) \end{bmatrix}$$

$$= \det \begin{bmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{bmatrix} = d + 1 - 1 = d.$$

Assim, $\mathcal{D}_{B/\mathbb{Z}} = d\mathbb{Z}$. Logo, um ideal primo $p\mathbb{Z}$ se ramifica em B se, e somente se, $d\mathbb{Z} \subset p\mathbb{Z}$ se, e somente se, p divide d.

Portanto, os ideais primos de $\mathbb{Z}$ que se ramificam em B (ou em $L = \mathbb{Q}[\sqrt{d}]$) são da forma $p\mathbb{Z}$ onde p é um divisor primo de d.

Vimos na Seção 3.3 que o polinômio ciclotômico,

$$F(X) = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \ldots + X^{p^{r-1}} + 1$$

(onde p é um número primo e $r \in \mathbb{N}$) é irredutível sobre $\mathbb{Q}$. Para $r = 1 \in \mathbb{N}$ temos o seguinte resultado:

Teorema 3.9 *Para todo número primo p, o polinômio ciclotômico*

$$X^{p-1} + X^{p-2} + \ldots + X + 1$$

é irredutível em $\mathbb{Q}[X]$.

Teorema 3.10 *Sejam p um número primo e z uma raiz primitiva p-ésima da unidade (em $\mathbb{C}$). Então, o anel A dos inteiros do corpo ciclotômico $\mathbb{Q}[z]$ é $\mathbb{Z}[z]$, e $(1, z, \ldots, z^{p-2})$ é uma base do $\mathbb{Z}$- módulo A.*

Demonstração: Ver [10], página 43.

3.6 Ideais primos que se ramificam em um corpo ciclotômico

Sejam p um número primo, $z \in \mathbb{C}$ uma raiz primitiva p-ésima da unidade e $L = \mathbb{Q}[z]$ o corpo ciclotômico correspondente. Sabemos pelo Teorema 3.10 acima que o anel B dos inteiros de L admite $(1, z, \ldots, z^{p-2})$ como base sobre $\mathbb{Z}$, e pelo Teorema 3.9 temos que o polinômio minimal $F(X)$ de z sobre $\mathbb{Q}$ satisfaz a equação $(X-1)F(X) = X^p - 1$, já que

$$F(X) = X^{p-1} + X^{p-2} + \ldots + X + 1 = \frac{X^p - 1}{X - 1}.$$

Vamos calcular o ideal discriminante $\mathcal{D}_{\mathbb{Z}[z]/\mathbb{Z}}$ utilizando a fórmula,

$$D(1, z, \ldots, z^{p-2}) = N(F'(z)) \cdot (-1)^{\frac{(p-1)(p-2)}{2}}.$$

Derivando a equação $(X-1)F(X) = X^p - 1$ obtemos,

$$F(X) + (X-1)F'(X) = p \cdot X^{p-1}.$$

E daí, $\underbrace{F(z)}_{=0} + (z-1)F'(z) = p \cdot z^{p-1}$, implicando então que,

$$(z-1)F'(z) = pz^{p-1}. \tag{3.7}$$

Por outro lado, $N(p) = p^{p-1}$ e $N(z) = \pm 1$. Além disso, decorre do Teorema 3.9 que, $N(z-1) = \pm p$.

E de (3.7), temos que,

$$N(z-1) \cdot N(F'(z)) = N(p)(N(z))^{p-1} \Rightarrow$$

$$\Rightarrow (\pm p) \cdot N(F'(z)) = p^{p-1} \cdot (\pm 1)^{p-1}$$

$$\Rightarrow N(F'(z)) = \pm p^{p-2} \Rightarrow D(1, z, \ldots, z^{p-2}) = (\pm p^{p-2}) \cdot (-1)^{\frac{(p-1)(p-2)}{2}} = \pm p^{p-2}.$$

Com isso,

$$\mathcal{D}_{\mathbb{Z}[z]/\mathbb{Z}} = D(1, z, \ldots, z^{p-2})\mathbb{Z} = \pm p^{p-2}\mathbb{Z} = p^{p-2}\mathbb{Z}.$$

Então, um ideal primo $q\mathbb{Z}$ de $\mathbb{Z}$ se ramifica em $\mathbb{Z}[z]$ (ou em $\mathbb{Q}[z]$) se, e somente se, $p^{p-2}\mathbb{Z} \subset q\mathbb{Z}$ se, e somente se, $q|p^{p-2}$ se, e somente se, $q|p$. Como p e q são primos então $p = q$.

Portanto, $p\mathbb{Z}$ é o único ideal primo de $\mathbb{Z}$ que se ramifica em $\mathbb{Z}[z]$ (ou em $\mathbb{Q}[z]$).

Proposição 3.4 *Sejam L um corpo numérico de grau n sobre $\mathbb{Q}$ e $(x_1, \ldots, x_n)$ inteiros de L que formam uma base de L sobre $\mathbb{Q}$. Se o discriminante $D(x_1, \ldots, x_n)$ não tem fatores quadrados então $(x_1, \ldots, x_n)$ é uma base sobre $\mathbb{Z}$ do anel B dos inteiros de L.*

Demonstração: Temos que B é um $\mathbb{Z}$-módulo livre de dimensão $[L : \mathbb{Q}] = n$. Seja então $(e_1, \ldots, e_n)$ uma base de B sobre $\mathbb{Z}$. Como os $x_i's$ são inteiros de L então $x_i \in B, \forall i$. Logo,

$$x_i = \sum_{j=1}^{n} a_{ij}e_j \quad \text{com} \quad a_{ij} \in \mathbb{Z}.$$

E daí,

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

$$D(x_1, \ldots, x_n) = [\det(a_{ij})]^2 \cdot D(e_1, \ldots, e_n).$$

Como $D(x_1, \ldots, x_n)$ não tem fatores quadrados então $\det(a_{ij}) = \pm 1$. Ou seja, $\det(a_{ij}) \neq 0$. E daí, os $x_i's$ são linearmente independentes sobre $\mathbb{Z}$.

Portanto, $(x_1, \ldots, x_n)$ é uma base de B sobre $\mathbb{Z}$.

■

3.7 Decomposição de um número primo em um corpo quadrático

Nos dois últimos capítulos deste texto precisaremos conhecer os tipos de decomposições de ideais primos em um corpo quadrático. No que segue, iremos usar a igualdade fundamental

$$\sum_{i=1}^{q} e_i f_i = [L : K]$$

para classificar tais decomposições.

Sejam $d \in \mathbb{Z}$ um inteiro sem fatores quadrados, L o corpo quadrático $L = \mathbb{Q}[\sqrt{d}]$, B o anel dos inteiros de L e p um número primo. Considere agora a decomposição do ideal estendido Bp em produto de ideais primos de B, isto é,

$$Bp = \prod_{i=1}^{q} \mathcal{B}_i^{e_i}.$$

A fórmula $\sum_{i=1}^{q} e_i f_i = 2$ nos diz que $q \leq 2$ e que somente podem ocorrer os três casos abaixo:

(a) $q = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$; se diz então que p se decompõe em L.

(b) $q = 1$, $e_1 = 1$, $f_1 = 2$; se diz então que p é inerte em L.

(c) $q = 1$, $e_1 = 2$, $f_1 = 1$; isto significa que p se ramifica em L.

Enunciaremos agora um resultado que estabelece condições suficientes para cada uma dessas classificações.

Proposição 3.5 *Seja $L = \mathbb{Q}[\sqrt{d}]$ um corpo quadrático, onde $d \in \mathbb{Z}$ não tem fatores quadrados.*

(a) *Se decompõem em L, os números primos ímpares p tais que d seja resíduo quadrático módulo p, e 2 se $d \equiv 1(\mathrm{mod}\ 8)$;*

(b) *São inertes em L, os números primos ímpares p tais que d seja não resíduo quadrático módulo p, e 2 se $d \equiv 5(\mathrm{mod}\ 8)$;*

(c) *Se ramificam em L, os divisores primos ímpares de d, e 2 se $d \equiv 2$ ou $3(\mathrm{mod}\ 4)$.*

Demonstração: Ver [10], página 77.

Capítulo 4

O subcorpo real maximal de um corpo ciclotômico

4.1 Caracteres de Grupos Abelianos Finitos

Seja G um grupo abeliano (com a operação escrita multiplicativamente) contendo n elementos. Seja $\mathbb{C}^\bullet$ o grupo multiplicativo dos números complexos não nulos, isto é, $\mathbb{C}^\bullet = \mathbb{C} - \{0\}$.

Definição 4.1 *Todo homomorfismo $\chi : G \to \mathbb{C}^\bullet$ é chamado um caráter de G (com valores complexos).*

Então, $\chi(a) \neq 0, \forall a \in G$ e $\chi(ab) = \chi(a) \cdot \chi(b), \forall a, b \in G$. Em particular, se e_G é a identidade multiplicativa de G então $\chi(e_G) = e_{\mathbb{C}^\bullet} = 1$.

Se χ é um caráter de G e $a^n = e_G$ para todo $a \in G$, então nós deduzimos que,

$(\chi(a))^n = \chi(a^n) = \chi(e_G) = 1 \Rightarrow \chi(a)$ é raiz n-ésima da unidade, $\forall a \in G$;

logo, $\chi(G)$ é um subgrupo do grupo multiplicativo cíclico das raízes n-ésimas da unidade. E daí, $\chi(G)$ é um grupo multiplicativo cíclico.

$$\chi(G) \subset \underbrace{\{\text{raízes n-ésimas da unidade}\}}_{\text{grupo multiplicativo cíclico}}$$

$$x, y \in \chi(G) \Rightarrow x = \chi(a) \quad \text{e} \quad y = \chi(b); a, b \in G.$$

$$xy^{-1} = \chi(a) \cdot \chi(b^{-1}) = \chi(\underbrace{ab^{-1}}_{\in G}) \in \chi(G) \Rightarrow \chi(G) \quad \text{é subgrupo.}$$

Seja $\widehat{G}$ o conjunto dos caracteres de G, isto é,

$$\widehat{G} = \{\chi : G \to \mathbb{C}^{\bullet}; \chi \quad \text{é homomorfismo}\}.$$

Definamos agora uma operação(multiplicativa) em $\widehat{G}$ da seguinte forma,

$$\begin{array}{rccc} \cdot : & \widehat{G} \times \widehat{G} & \to & \widehat{G} \\ & (\chi, \chi') & \mapsto & \chi \cdot \chi' \end{array}$$

$$\begin{array}{rcl} \chi \cdot \chi' & : & G \to \mathbb{C}^{\bullet} \\ (\chi \cdot \chi')(a) & := & \chi(a) \cdot \chi'(a), \forall a \in G. \end{array}$$

Com essa operação o conjunto $\widehat{G}$ passa a ser um grupo multiplicativo.

A identidade multiplicativa de $\widehat{G}$ é o caráter χ_o, definido por $\chi_o(a) = 1$ para todo $a \in G$. E o inverso de $\chi \in \widehat{G}$ é dado por $\chi^{-1}(a) = (\chi(a))^{-1}$ para todo $a \in G$.

Definição 4.2 *Se a ordem de um caráter χ é igual a 2, nós chamamos ele um caráter quadrático.*

$$\mathcal{O}(\chi) = |\langle\chi\rangle| = 2 \Rightarrow \chi \quad \text{é um caráter quadrático.}$$

$$\chi^2 = \chi_o \quad , \quad \chi \cdot \chi = \chi_o.$$

Definição 4.3 *Seja $m > 1$ um inteiro. Uma aplicação $\chi : \mathbb{Z} \to \mathbb{C}$ é chamada caráter modular (com módulo m) quando ela satisfaz as seguintes condições:*

(1) $\chi(a) = 0$ *se, e somente se,* $\mathrm{mdc}(a, m) > 1$*;*

(2) *Se* $a \equiv b(\mathrm{mod}\ m)$ *então* $\chi(a) = \chi(b)$*; e*

(3) $\chi(ab) = \chi(a) \cdot \chi(b)$.

O suporte de χ é $\{a \in \mathbb{Z}; \mathrm{mdc}(a, m) = 1\}$.

Note que, $\chi(1) = 1$. De fato,

$$\begin{aligned}
\chi(1) = \chi(1 \cdot 1) = \chi(1) \cdot \chi(1) \quad &\Rightarrow \quad \chi(1) - \chi(1) \cdot \chi(1) = 0 \\
&\Rightarrow \quad \chi(1) \cdot (1 - \chi(1)) = 0 \\
&\underbrace{\Rightarrow}_{\mathbb{C} \text{ é um DI}} \quad \chi(1) = 0 \quad \text{ou} \quad 1 - \chi(1) = 0 \\
&\Rightarrow \quad \chi(1) = 0 \quad \text{ou} \quad \chi(1) = 1 \\
&\underbrace{\Rightarrow}_{\mathrm{mdc}(1,m)=1 \Rightarrow \chi(1) \neq 0} \quad \chi(1) = 1.
\end{aligned}$$

Claramente, $\chi(a) = 1$ para todo $a \in \mathbb{Z}$ tal que $a \equiv 1(\mathrm{mod}\ m)$.

Definição 4.4 *O caráter trivial* χ_o *módulo* m*, é definido da seguinte forma:*

$$\begin{cases} \chi_o(a) = 1 \quad , \qquad \textit{quando} \quad \mathrm{mdc}(a, m) = 1 \\ \chi_o(a) = 0 \quad , \qquad \textit{quando} \quad \mathrm{mdc}(a, m) > 1. \end{cases}$$

Proposição 4.1 *Para todo* $m > 1$ *existe uma correspondência natural* $1 - 1$ *entre os caracteres do grupo multiplicativo* $P(m) = (\mathbb{Z}/(m))^{\bullet}$ *e os caracteres modulares com módulo* m*.*

Demonstração: Ver [9], página 473.

Seja χ um caráter módulo m. Considere o seguinte conjunto M_χ de inteiros $m' \geq 1$ que satisfazem a seguinte propriedade:

$$Se \quad \mathrm{mdc}(a, m) = \mathrm{mdc}(b, m) = 1 \quad \text{e} \quad a \equiv b(\mathrm{mod}\ m') \quad \text{então} \quad \chi(a) = \chi(b).$$

Cada elemento de M_χ é chamado um módulo de definição de χ.

Por exemplo $m \in M_\chi$.

Se $m_1 \in M_\chi$ e m_1 divide m_2 então $m_2 \in M_\chi$.

$m_1|m_2 \Rightarrow m_2 = rm_1$, com $r \in \mathbb{Z}$.

Seja $a, b \in \mathbb{C}$ tais que, $\mathrm{mdc}(a, m) = \mathrm{mdc}(b, m) = 1$ e

$$a \equiv b(\mathrm{mod}\ m_2) \Rightarrow m_2|(a-b) \Rightarrow a - b = sm_2 = srm_1 \Rightarrow$$

$$\Rightarrow m_1|(a-b) \Rightarrow a \equiv b(\mathrm{mod}\ m_1).$$

E daí, como $m_1 \in M_\chi$ então $\chi(a) = \chi(b)$. Portanto, $m_2 \in M_\chi$.

Definição 4.5 *O menor inteiro positivo pertencente à M_χ é chamado o condutor de χ e denotado por f_χ.*

Definição 4.6 *Um caráter ψ módulo f, com condutor $f_\psi = f$ é chamado um caráter primitivo.*

Observação 4.1 *Se o caráter χ módulo m corresponde a um caráter quadrático do grupo $P(m)$, nós dizemos que χ é um caráter quadrático modular.*

Definição 4.7 *Sejam p um primo ímpar e a um inteiro não-nulo que não seja múltiplo de p. Nós definimos o símbolo de Legendre $\left(\frac{a}{p}\right)$ de a, relativo a p, da seguinte forma:*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 \quad , & \textit{quando} \quad a \quad \textit{é um resíduo quadrático módulo} \quad p \\ -1 \quad , & \textit{quando} \quad a \quad \textit{é um não resíduo quadrático módulo} \quad p \end{cases}$$

Proposição 4.2 *O símbolo de Legendre tem as seguintes propriedades:*

(L1) *Se* $a \equiv b(\mathrm{mod}\ p)$ *então* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(L2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

Demonstração: Ver [9], página 63.

Proposição 4.3 *Seja p um primo ímpar. O único caráter quadrático módulo p é χ dado pelo símbolo de Legendre: $\chi(a) = \left(\frac{a}{p}\right)$ para todo $a \in \mathbb{Z}$; este caráter é primitivo com condutor p.*

Demonstração: Ver [9], página 477.

Sejam $m \geq 2$, χ um caráter módulo m e $\zeta = \cos\left(\frac{2\pi}{m}\right) + i\text{sen}\left(\frac{2\pi}{m}\right)$.

Definição 4.8 *As expressões*

$$\tau_k(\chi) = \sum_{\substack{\overline{a} \in P(m) \\ 1 \leq a < m}} \chi(a)\zeta^{ak} \quad \textit{para } k = 0, 1, \ldots, m-1$$

são chamadas as Somas Gaussianas associadas ao caráter χ (e a raiz primitiva m-ésima da unidade ζ).

Para $k = 0$ nós temos,

$$\tau_o(\chi) = \sum_{\substack{\overline{a} \in P(m) \\ 1 \leq a < m}} \chi(a) = \begin{cases} \varphi(m) & , \text{ quando } \chi = \chi_o \\ 0 & , \text{ quando } \chi \neq \chi_o. \end{cases}$$

A Soma Gaussiana Principal é

$$\tau_1(\chi) = \sum_{\substack{\overline{a} \in P(m) \\ 1 \leq a < m}} \chi(a) \cdot \zeta^a.$$

4.2 O subcorpo real maximal de $\mathbb{Q}(\zeta_m)$

Sejam m um inteiro positivo e ζ_m uma raiz primitiva m-ésima da unidade. Considere os corpos $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ e $\mathbb{Q}(\zeta_m)$, onde $\mathbb{Q}$ é o corpo dos números racionais.

Proposição 4.4 *$\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ é o subcorpo real maximal do corpo ciclotômico $\mathbb{Q}(\zeta_m)$.*

Demonstração: Temos que, $\mathbb{Q}(\zeta_m + \zeta_m^{-1}) \subset \mathbb{Q}(\zeta_m)$ pois $\mathbb{Q}(\zeta_m)$ é corpo e $\zeta_m \in \mathbb{Q}(\zeta_m)$.

Por outro lado,

$$\zeta_m^m = 1 \quad \Rightarrow \quad \overline{\zeta_m^m} = \overline{1} = 1 \Rightarrow \overline{\zeta_m}^m = 1 \Rightarrow \zeta_m^m \cdot \overline{\zeta_m}^m = 1$$

$$\underbrace{\Rightarrow}_{\mathbb{C} \text{ é corpo}} \quad \left(\zeta_m \cdot \overline{\zeta_m}\right)^m = 1 \quad \underbrace{\Rightarrow}_{0<\zeta_m\overline{\zeta_m}=|\zeta_m|^2\in\mathbb{R}} \quad \zeta_m \cdot \overline{\zeta_m} = 1 \Rightarrow \overline{\zeta_m} = \zeta_m^{-1}.$$

E daí,

$$\zeta_m + \zeta_m^{-1} = \zeta_m + \overline{\zeta_m} = 2 \cdot \mathrm{Re}\,(\zeta_m) \in \mathbb{R}.$$

E além disso, $X^2 - (\zeta_m + \zeta_m^{-1})\,X + 1$ é o polinômio minimal de ζ_m sobre $\mathbb{Q}\,(\zeta_m + \zeta_m^{-1})$. Logo, $[\mathbb{Q}\,(\zeta_m + \zeta_m^{-1})\,(\zeta_m) : \mathbb{Q}\,(\zeta_m + \zeta_m^{-1})] = 2$, ou seja,

$$\left[\mathbb{Q}\,(\zeta_m) : \mathbb{Q}\left(\zeta_m + \zeta_m^{-1}\right)\right] = 2.$$

Com isso, se K é um subcorpo real arbitrário de $\mathbb{Q}\,(\zeta_m)$ tal que,

$$\mathbb{Q}\left(\zeta_m + \zeta_m^{-1}\right) \subset K \subset \mathbb{Q}\,(\zeta_m)$$

então $K = \mathbb{Q}\,(\zeta_m + \zeta_m^{-1})$.

Portanto, $\mathbb{Q}\,(\zeta_m + \zeta_m^{-1})$ é o subcorpo real maximal de $\mathbb{Q}\,(\zeta_m)$.

■

4.3 Imersão de $\mathbb{Q}(\sqrt{m})$ em $\mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1})$

4.3.1 O símbolo Kronecker

Seja $0 \neq a \in \mathbb{Z}$ e p um número primo qualquer. Nós definimos o símbolo Kronecker $\left\{\dfrac{a}{p}\right\} = \{a/p\}$ da seguinte forma: Se $p|a$ então $\{a/p\} = 0$; se p é

ímpar e $p \nmid a$ então $\{a/p\} = (a/p)$ (o símbolo de Legendre); Se $p = 2$, nós definimos

$$\left\{\frac{a}{2}\right\} = \begin{cases} +1 & , \text{ se } a \equiv 1 (\mathrm{mod}\ 8), \\ -1 & , \text{ se } a \equiv 5 (\mathrm{mod}\ 8), \\ \text{não definido} & , \text{ se } a \equiv 3 (\mathrm{mod}\ 4). \end{cases}$$

Se $b = p_1 \cdot \ldots \cdot p_r$ ($p_1, \ldots, p_r$ primos ímpares, não necessariamente distintos), nós definimos

$$\left\{\frac{a}{b}\right\} = \left\{\frac{a}{-b}\right\} = \prod_{i=1}^{r} \left\{\frac{a}{p_i}\right\}.$$

Se $b = 2^e b'$, onde $e \geq 1$ e b' é ímpar, então nós definimos

$$\left\{\frac{a}{b}\right\} = \begin{cases} \left\{\frac{a}{b'}\right\} & , \text{ se } e \text{ é par,} \\ \\ \left\{\frac{a}{2}\right\}\left\{\frac{a}{b'}\right\} & , \text{ se } e \text{ é ímpar.} \end{cases}$$

(Note que $\left\{\frac{a}{b}\right\} = 0$ se e é ímpar e a é par, e ele é não definido quando e é ímpar e $a \equiv 3 (\mathrm{mod}\ 4)$).

Se $b = -1$, nós definimos

$$\left\{\frac{a}{-1}\right\} = \mathrm{sign}(a).$$

Note que, $\mathrm{sign}(a) = 1$ se $a > 0$ e $\mathrm{sign}(a) < 0$ se $a < 0$.

Propriedades:

(a) $\left\{\frac{a}{bb'}\right\} = \left\{\frac{a}{b}\right\} \cdot \left\{\frac{a}{b'}\right\}$

(b) Se $a \equiv 0$ ou $1 (\mathrm{mod}\ 4)$ então,

$$\left\{\frac{a}{|a|-1}\right\} = \begin{cases} 1, & \text{quando } a > 0 \\ -1, & \text{quando } a < 0 \end{cases}$$

(c) Se $a \equiv 0$ ou $1 (\mathrm{mod}\ 4)$ e $b \equiv -b' (\mathrm{mod}\ |a|)$ então,

$$\left\{\frac{a}{b}\right\} = \begin{cases} \left\{\frac{a}{b'}\right\} & \text{quando} \quad a > 0 \\ -\left\{\frac{a}{b'}\right\} & \text{quando} \quad a < 0 \end{cases}$$

Essas propriedades podem ser vistas em [9], página 81.

4.3.2 Caracteres Primitivos Reais

Caracteres primitivos reais são fáceis de caracterizar. Lembre que um discriminante fundamental é 1 ou o discriminante de um corpo quadrático real, em outras palavras é um inteiro livre de quadrados congruente a 1 módulo 4, ou 4 vezes um inteiro livre de quadrados congruente a 2 ou 3 módulo 4.

Proposição 4.5 *Se D é um discriminante fundamental, o símbolo Kronocker $\left\{\frac{D}{n}\right\}$ define um caráter primitivo real módulo $m = |D|$. Reciprocamente, se χ é um caráter primitivo real módulo m então $D = \chi(-1)m$ é um discriminante fundamental e $\chi(n) = \left\{\frac{D}{n}\right\}$.*

Demonstração: Ver [3], página 43.

Proposição 4.6 *Seja χ um caráter primitivo real módulo m, de modo que $\chi(n) = \left\{\frac{D}{n}\right\}$ para $D = \chi(-1)m$ um discriminante fundamental. Então,*

$$\tau_1(\chi) = \begin{cases} m^{1/2} & \textit{se} \quad \chi(-1) = 1, \\ m^{1/2}i & \textit{se} \quad \chi(-1) = -1. \end{cases}$$

Demonstração: Ver [3], página 49.

Teorema 4.1 *Seja m um inteiro positivo livre de quadrados. Então, $k = \mathbb{Q}(\sqrt{m})$ está imerso no subcorpo real maximal $K_o = \mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1})$ de $\mathbb{Q}(\zeta_{4m})$, isto é, $k = \mathbb{Q}(\sqrt{m}) \subset K_o = \mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1})$.*

Demonstração: Como ζ_{4m} é uma raiz $4m$-ésima da unidade então,

$$\begin{aligned}
\zeta_{4m}^{4m}=1 \quad &\Rightarrow \quad \overline{\zeta_{4m}^{4m}}=\overline{1}=1\Rightarrow \overline{\zeta_{4m}}^{4m}=1\\
&\Rightarrow \quad \zeta_{4m}^{4m}\cdot\overline{\zeta_{4m}}^{4m}=1 \underbrace{\Rightarrow}_{\substack{\mathbb{C}\text{ é corpo}}} \left(\zeta_{4m}\cdot\overline{\zeta_{4m}}\right)^{4m}\\
&\underbrace{\Rightarrow}_{0\leq|\zeta_{4m}|^2=\zeta_{4m}\cdot\overline{\zeta_{4m}}\in\mathbb{R}} \quad \zeta_{4m}\cdot\overline{\zeta_{4m}}=1\Rightarrow\overline{\zeta_{4m}}=\zeta_{4m}^{-1}.
\end{aligned}$$

Logo,

$$\overline{\zeta_{4m}}^{2}=\zeta_{4m}^{-2} \quad , \quad \overline{\zeta_{4m}}^{3}=\zeta_{4m}^{-3} \quad , \quad \dots \quad , \quad \overline{\zeta_{4m}}^{(4m-2)/2}=\zeta_{4m}^{-(4m-2)/2}.$$

E daí,

$$\zeta_{4m}+\zeta_{4m}^{-1}=\zeta_{4m}+\overline{\zeta_{4m}}\in\mathbb{R}$$

$$\zeta_{4m}^{2}+\zeta_{4m}^{-2}=\zeta_{4m}^{2}+\overline{\zeta_{4m}}^{2}=\zeta_{4m}^{2}+\overline{\zeta_{4m}^{2}}\in\mathbb{R}$$

$$\vdots$$

$$\zeta_{4m}^{(4m-2)/2}+\zeta_{4m}^{-(4m-2)/2}=\zeta_{4m}^{(4m-2)/2}+\overline{\zeta_{4m}}^{(4m-2)/2}=\zeta_{4m}^{(4m-2)/2}+\overline{\zeta_{4m}^{(4m-2)/2}}\in\mathbb{R}.$$

Note que, $\zeta_{4m}^{j}+\zeta_{4m}^{-j}\in\mathbb{Q}(\zeta_{4m})$ para todo $j=1,\dots,\dfrac{4m-2}{2}$; pois $\zeta_{4m}\in\mathbb{Q}(\zeta_{4m})$ e $\mathbb{Q}(\zeta_{4m})$ é corpo.

Com isso,

$$\mathbb{Q}(\zeta_{4m}^{2}+\zeta_{4m}^{-2})\subset\mathbb{Q}(\zeta_{4m}) \quad \text{é um subcorpo real de} \quad \mathbb{Q}(\zeta_{4m})$$

$$\mathbb{Q}(\zeta_{4m}^{3}+\zeta_{4m}^{-3})\subset\mathbb{Q}(\zeta_{4m}) \quad \text{é um subcorpo real de} \quad \mathbb{Q}(\zeta_{4m})$$

$$\vdots$$

$$\mathbb{Q}(\zeta_{4m}^{(4m-2)/2}+\zeta_{4m}^{-(4m-2)/2})\subset\mathbb{Q}(\zeta_{4m}) \quad \text{é um subcorpo real de} \quad \mathbb{Q}(\zeta_{4m}).$$

Mas, $\mathbb{Q}(\zeta_{4m}+\zeta_{4m}^{-1})$ é o subcorpo real maximal de $\mathbb{Q}(\zeta_{4m})$. Então,

$$\left\{\begin{array}{c}
\mathbb{Q}(\zeta_{4m}^{2}+\zeta_{4m}^{-2})\subset\mathbb{Q}(\zeta_{4m}+\zeta_{4m}^{-1})\\
\mathbb{Q}(\zeta_{4m}^{3}+\zeta_{4m}^{-3})\subset\mathbb{Q}(\zeta_{4m}+\zeta_{4m}^{-1})\\
\vdots\\
\mathbb{Q}(\zeta_{4m}^{(4m-2)/2}+\zeta_{4m}^{-(4m-2)/2})\subset\mathbb{Q}(\zeta_{4m}+\zeta_{4m}^{-1})
\end{array}\right. \Rightarrow$$

$$\Rightarrow \begin{cases} \zeta_{4m}^{2} + \zeta_{4m}^{-2} \in \mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1}) \\ \zeta_{4m}^{3} + \zeta_{4m}^{-3} \in \mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1}) \\ \vdots \\ \zeta_{4m}^{(4m-2)/2} + \zeta_{4m}^{-(4m-2)/2} \in \mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1}) \end{cases}$$

Seja d o discriminante do corpo quadrático real $\mathbb{Q}(\sqrt{m})$. Logo,

$$d = \begin{cases} 4m, & \text{se } m \equiv 2 \text{ ou } 3 (\mathrm{mod}\ 4) \\ m, & \text{se} \quad m \equiv 1 (\mathrm{mod}\ 4). \end{cases}$$

Como d é um discriminante fundamental então pela Proposição 4.5 o símbolo Kronocker $\left\{\frac{d}{a}\right\}$ define um caráter primitivo real χ módulo $|d| = d$. Seja ζ_d uma raiz primitiva d-ésima da unidade. Considere agora a Soma de Gauss Principal associada ao caráter χ e a ζ_d,

$$\tau_1(\chi) = \sum_{\substack{a \in P(d) \\ 1 \leq a < d}} \left\{\frac{d}{a}\right\} \cdot \zeta_d^a.$$

Temos também que, $\chi(-1) = \left\{\frac{d}{-1}\right\} = \mathrm{sign}(d) = 1$, pois $d > 0$. Então pela Proposição 4.6,

$$\tau_1(\chi) = \sqrt{d} \quad \Rightarrow \quad \sqrt{d} = \sum_{\substack{a \in P(d) \\ 1 \leq a < d}} \left\{\frac{d}{a}\right\} \cdot \zeta_d^a.$$

Analisemos agora os seguintes casos: $m \equiv 2$ ou $3 (\mathrm{mod}\ 4)$ e $m \equiv 1 (\mathrm{mod}\ 4)$.

(I) $m \equiv 2$ ou $3 (\mathrm{mod}\ 4) \rightarrow d = 4m$

$$\sqrt{4m} = \sum_{\substack{a \in P(4m) \\ 1 \leq a < 4m}} \left\{\frac{4m}{a}\right\} \cdot \zeta_{4m}^a = \left\{\frac{4m}{1}\right\} \cdot \zeta_{4m} + \left\{\frac{4m}{2}\right\} \cdot \zeta_{4m}^2 + \ldots + \left\{\frac{4m}{4m-1}\right\} \cdot \zeta_{4m}^{4m-1}.$$

Note que,

$$m \equiv 2 \text{ ou } 3 (\mathrm{mod}\ 4) \Rightarrow 4m \equiv 8 \text{ ou } 12 (\mathrm{mod}\ 4) \Rightarrow 4m \equiv 0 (\mathrm{mod}\ 4) \text{ e } 4m > 0.$$

Além disso,

$$\begin{array}{c|c} \begin{array}{c} 1 \equiv -(4m-1)(\mathrm{mod}\ |4m|) \\ 2 \equiv -(4m-2)(\mathrm{mod}\ |4m|) \\ \vdots \\ \dfrac{4m}{2} - 1 \equiv -\left(\dfrac{4m}{2}+1\right)(\mathrm{mod}\ |4m|) \end{array} & \begin{array}{c} \left\{\dfrac{4m}{1}\right\} = \left\{\dfrac{4m}{4m-1}\right\} \\ \left\{\dfrac{4m}{2}\right\} = \left\{\dfrac{4m}{4m-2}\right\} \\ \vdots \\ \left\{\dfrac{4m}{\frac{4m}{2}-1}\right\} = \left\{\dfrac{4m}{\frac{4m}{2}+1}\right\} \end{array} \end{array}$$

$$\underbrace{\Rightarrow}_{Propriedades\ (c)}$$

E daí,

$$\sqrt{4m} = \left\{\frac{4m}{1}\right\}\zeta_{4m} + \left\{\frac{4m}{2}\right\}\zeta_{4m}^{2} + \ldots + \left\{\frac{4m}{\frac{4m}{2}-1}\right\}\zeta_{4m}^{\frac{4m}{2}-1} + \left\{\frac{4m}{\frac{4m}{2}}\right\}\zeta_{4m}^{\frac{4m}{2}} +$$

$$+ \left\{\frac{4m}{\frac{4m}{2}+1}\right\}\zeta_{4m}^{\frac{4m}{2}+1} + \ldots + \left\{\frac{4m}{4m-2}\right\}\zeta_{4m}^{4m-2} + \left\{\frac{4m}{4m-1}\right\}\zeta_{4m}^{4m-1}.$$

Temos também da igualdade $\zeta_{4m}^{4m} = 1$ que,

$$\begin{cases} \zeta_{4m}^{4m-1} = \zeta_{4m}^{-1} \\ \zeta_{4m}^{4m-2} = \zeta_{4m}^{-2} \\ \vdots \\ \zeta_{4m}^{4m-(\frac{4m}{2}-1)} = \zeta_{4m}^{-(\frac{4m}{2}-1)} \end{cases}$$

E além disso,

$$\left\{\frac{4m}{\frac{4m}{2}}\right\} = \left\{\frac{4m}{2m}\right\} \underbrace{=}_{\text{Propriedades (a)}} \left\{\frac{4m}{2}\right\} \cdot \left\{\frac{4m}{m}\right\} \underbrace{=}_{\text{Definição}} 0 \cdot \left\{\frac{4m}{m}\right\} = 0.$$

Com isso,

$$\sqrt{4m} = \underbrace{\left\{\frac{4m}{1}\right\}}_{\in\mathbb{Z}\subset\mathbb{Q}\subset K_o} \underbrace{\left[\zeta_{4m} + \zeta_{4m}^{-1}\right]}_{\in K_o} + \underbrace{\left\{\frac{4m}{2}\right\}}_{\in\mathbb{Z}\subset\mathbb{Q}\subset K_o} \underbrace{\left[\zeta_{4m}^{2} + \zeta_{4m}^{-2}\right]}_{\in K_o} +$$

$$+\ldots+\underbrace{\left\{\frac{4m}{\frac{4m-2}{2}}\right\}}_{\in\mathbb{Z}\subset\mathbb{Q}\subset K_o}\underbrace{\left[\zeta_{4m}^{\frac{4m-2}{2}}+\zeta_{4m}^{-(\frac{4m-2}{2})}\right]}_{\in K_o}\in K_o\Rightarrow$$

$$\Rightarrow\sqrt{4m}\in K_o\Rightarrow 2\sqrt{m}\in K_o\Rightarrow\sqrt{m}\in K_o.$$

Portanto,

$$k=\mathbb{Q}(\sqrt{m})\subset K_o=\mathbb{Q}(\zeta_{4m}+\zeta_{4m}^{-1}).$$

(II) $m\equiv 1(\mathrm{mod}\ 4)\rightarrow d=m$

$$\sqrt{m}=\sum_{\substack{a\in P(m)\\ 1\leq a<m}}\left\{\frac{m}{a}\right\}\cdot\zeta_m^a=\left\{\frac{m}{1}\right\}\cdot\zeta_m+\left\{\frac{m}{2}\right\}\cdot\zeta_m^2+\ldots+\left\{\frac{m}{\frac{m-1}{2}}\right\}\cdot\zeta_m^{\frac{m-1}{2}}+$$

$$+\left\{\frac{m}{\frac{m+1}{2}}\right\}\cdot\zeta_m^{\frac{m+1}{2}}+\ldots+\left\{\frac{m}{m-2}\right\}\cdot\zeta_m^{m-2}+\left\{\frac{m}{m-1}\right\}\cdot\zeta_m^{m-1}.$$

Temos que $m\equiv 1(\mathrm{mod}\ 4), m>0$ e além disso:

$$\begin{array}{c|l}\begin{array}{c}\\ 1\equiv-(m-1)(\mathrm{mod}\ |m|)\\ 2\equiv-(m-2)(\mathrm{mod}\ |m|)\\ \vdots\\ \frac{m-1}{2}\equiv-\frac{m+1}{2}(\mathrm{mod}\ |m|)\end{array} & \begin{array}{l}\left\{\frac{m}{1}\right\}=\left\{\frac{m}{m-1}\right\}\\ \\ \left\{\frac{m}{2}\right\}=\left\{\frac{m}{m-2}\right\}\\ \vdots\\ \left\{\frac{m}{\frac{m-1}{2}}\right\}=\left\{\frac{m}{\frac{m+1}{2}}\right\}\end{array}\end{array}\quad\overbrace{\Rightarrow}^{\text{Propriedades (c)}}$$

Temos também da igualdade $\zeta_m^m=1$ que,

$$\begin{cases}\zeta_m^{m-1}=\zeta_m^{-1}\\ \zeta_m^{m-2}=\zeta_m^{-2}\\ \quad\vdots\\ \zeta_m^{\frac{m+1}{2}}=\zeta_m^{-\frac{m-1}{2}}\end{cases}$$

Com isso,

$$\sqrt{m}=\left\{\frac{m}{1}\right\}\cdot\left[\zeta_m+\zeta_m^{-1}\right]+\left\{\frac{m}{2}\right\}\cdot\left[\zeta_m^2+\zeta_m^{-2}\right]+\ldots+\left\{\frac{m}{\frac{(m-1)}{2}}\right\}\cdot\left[\zeta_m^{\frac{(m-1)}{2}}+\zeta_m^{-\frac{(m-1)}{2}}\right].$$

Temos que,

$$(\zeta_m)^{4m} \underbrace{=}_{\mathbb{C} \text{ é corpo}} (\zeta_m^m)^4 = 1^4 = 1.$$

Logo, ζ_m é uma raiz $4m$-ésima da unidade. E daí,

$$\zeta_m = (\zeta_{4m})^r, \quad \text{para algum} \quad r.$$

Como $\mathbb{Q}(\zeta_{4m})$ é corpo então $(\zeta_{4m})^r \in \mathbb{Q}(\zeta_{4m})$. Logo,

$$\begin{aligned}
\hookrightarrow \zeta_m, \zeta_m^{-1} \in \mathbb{Q}(\zeta_{4m}) \quad &\Rightarrow \quad \underbrace{\zeta_m + \zeta_m^{-1}}_{\in\mathbb{R}} \in \mathbb{Q}(\zeta_{4m}) \\
&\Rightarrow \quad \mathbb{Q}(\zeta_m + \zeta_m^{-1}) \subset \mathbb{Q}(\zeta_{4m}) \text{ é subcorpo real de } \mathbb{Q}(\zeta_{4m}) \\
&\Rightarrow \quad \mathbb{Q}(\zeta_m + \zeta_m^{-1}) \subset \mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1}) \\
&\Rightarrow \quad \zeta_m + \zeta_m^{-1} \in \mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1}) = K_o
\end{aligned}$$

$$\begin{aligned}
\hookrightarrow \zeta_m^2, \zeta_m^{-2} \in \mathbb{Q}(\zeta_{4m}) \quad &\Rightarrow \quad \underbrace{\zeta_m^2 + \zeta_m^{-2}}_{\in\mathbb{R}} \in \mathbb{Q}(\zeta_{4m}) \\
&\Rightarrow \quad \mathbb{Q}(\zeta_m^2 + \zeta_m^{-2}) \subset \mathbb{Q}(\zeta_{4m}) \text{ é subcorpo real de } \mathbb{Q}(\zeta_{4m}) \\
&\Rightarrow \quad \mathbb{Q}(\zeta_m^2 + \zeta_m^{-2}) \subset \mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1}) \\
&\Rightarrow \quad \zeta_m^2 + \zeta_m^{-2} \in \mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1}) = K_o
\end{aligned}$$

$$\vdots$$

$$\begin{aligned}
\hookrightarrow \zeta_m^{\frac{m-1}{2}}, \zeta_m^{-\frac{m-1}{2}} \in \mathbb{Q}(\zeta_{4m}) \quad &\Rightarrow \quad \underbrace{\zeta_m^{\frac{m-1}{2}} + \zeta_m^{-\frac{m-1}{2}}}_{\in\mathbb{R}} \in \mathbb{Q}(\zeta_{4m}) \\
&\Rightarrow \quad \mathbb{Q}(\zeta_m^{\frac{m-1}{2}} + \zeta_m^{-\frac{m-1}{2}}) \subset \mathbb{Q}(\zeta_{4m}) \\
&\qquad \text{é subcorpo real de } \mathbb{Q}(\zeta_{4m}) \\
&\Rightarrow \quad \mathbb{Q}(\zeta_m^{\frac{m-1}{2}} + \zeta_m^{-\frac{m-1}{2}}) \subset \mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1}) \\
&\Rightarrow \quad \zeta_m^{\frac{m-1}{2}} + \zeta_m^{-\frac{m-1}{2}} \in \mathbb{Q}(\zeta_{4m} + \zeta_{4m}^{-1}) = K_o.
\end{aligned}$$

Então,

$$\sqrt{m} = \underbrace{\left\{\frac{m}{1}\right\}}_{\in\mathbb{Z}\subset\mathbb{Q}\subset K_o}\underbrace{\left[\zeta_m+\zeta_m^{-1}\right]}_{\in K_o}+\underbrace{\left\{\frac{m}{2}\right\}}_{\in\mathbb{Z}\subset\mathbb{Q}\subset K_o}\underbrace{\left[\zeta_m^2+\zeta_m^{-2}\right]}_{\in K_o}+$$

$$+\ldots+\underbrace{\left\{\frac{m}{\frac{(m-1)}{2}}\right\}}_{\in\mathbb{Z}\subset\mathbb{Q}\subset K_o}\underbrace{\left[\zeta_m^{\frac{m-1}{2}}+\zeta_m^{-\frac{m-1}{2}}\right]}_{\in K_o}\in K_o \Rightarrow \sqrt{m}\in K_o.$$

Portanto,

$$k=\mathbb{Q}(\sqrt{m})\subset K_o=\mathbb{Q}(\zeta_{4m}+\zeta_{4m}^{-1}).$$

■

Capítulo 5

O número de classes do subcorpo real maximal de $\mathbb{Q}(\zeta_p)$

Sejam m um inteiro positivo, ζ_m uma raiz primitiva m-ésima da unidade e $H(m)$ o número de classes do subcorpo real maximal $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$ de $\mathbb{Q}(\zeta_m)$.

Designaremos por $h(m)$ o número de classes do corpo quadrático real $\mathbb{Q}(\sqrt{m})$.

O objetivo deste capítulo é mostrar que para os primos da forma $p = (2qn)^2+1$ com q primo ímpar e $n > 1$ inteiro, o número $H(p)$ é maior do que 1.

Teorema 5.1 *Se $p = (2qn)^2 + 1$ é um primo, com q primo ímpar e $n > 1$ inteiro, então $h(p) > 1$.*

Para provarmos o Teorema 5.1 precisaremos do seguinte Lema e de alguns resultados relativos a decomposição de ideais primos em uma extensão.

Lema 5.2 *Sejam l, m inteiros positivos e m um não quadrado. A equação*

$$u^2 - \left(l^2 + 1\right) v^2 = \pm m \tag{5.1}$$

não tem soluções em inteiros u, v, a menos que $m \geq 2l$.

Demonstração: Suponha que (u', v') seja uma solução em inteiros u', v' de (5.1).

Afirmação 5.1 $v' \neq 0$

Com efeito,

$$u'^2 - (l^2+1)v'^2 = \pm m$$

$v' = 0 \Rightarrow u'^2 = \pm m \underbrace{\Rightarrow}_{u'^2 = -m < 0}$ $u'^2 = m$, contradição, pois m não é quadrado.

Afirmação 5.2 *Existe uma solução* (u, v) *de (5.1) tal que* $u, v \in \mathbb{Z}$ *com* $u \geq 0$ *e* v *o menor inteiro positivo possível.*

Com efeito,

$$v' > 0 \to |u'| \geq 0 \quad \text{e} \quad v' > 0 \to \text{Basta tomar} \quad (u, v) \quad \text{com} \quad u = |u'|$$
$$\text{e} \quad v = \min\{w \in \mathbb{Z}; 0 < w \leq v' \quad \text{e} \quad (|u'|, w) \quad \text{é solução de (5.1)}\}$$

$$v' < 0 \to |u'| \geq 0 \quad \text{e} \quad -v' > 0 \to \text{Basta tomar} \quad (u, v) \quad \text{com} \quad u = |u'|$$
$$\text{e} \quad v = \min\{w \in \mathbb{Z}; 0 < w \leq -v' \quad \text{e} \quad (|u'|, w) \quad \text{é solução de (5.1)}\}.$$

Se $K = \mathbb{Q}\left(\sqrt{l^2+1}\right)$ então $N_{K|\mathbb{Q}}\left(u - v\sqrt{l^2+1}\right) = \pm m$.

Com efeito,

$$x = u - v\sqrt{l^2+1} \Rightarrow x - u = -v\sqrt{l^2+1} \Rightarrow x^2 - 2ux + u^2 = v^2(l^2+1)$$
$$\Rightarrow x^2 - 2ux + u^2 - v^2(l^2+1) = 0 \Rightarrow x^2 - 2ux \pm m = 0$$

Temos então que, $\sqrt{l^2+1}$ é um elemento primitivo de $\mathbb{Q}(\sqrt{l^2+1})|\mathbb{Q}$ e $X^2 - 2uX \pm m$ é o polinômio minimal de $\sqrt{l^2+1}$ sobre $\mathbb{Q}$. Nesse caso, o

polinômio característico de $u - v\sqrt{l^2+1}$ com respeito à K e $\mathbb{Q}$ coincide com o polinômio minimal de $u - v\sqrt{l^2+1}$ sobre $\mathbb{Q}$. Logo,

$$N_{K|\mathbb{Q}}\left(u - v\sqrt{l^2+1}\right) = \pm m = \text{produto das raízes de} \quad X^2 - 2uX \pm m. \quad (5.2)$$

Usando esse mesmo argumento, conclui-se que,

$$N_{K|\mathbb{Q}}\left(l + \sqrt{l^2+1}\right) = -1. \quad (5.3)$$

$x = l+\sqrt{l^2+1} \Rightarrow x-l = \sqrt{l^2+1} \Rightarrow x^2-2lx+l^2 = l^2+1 \Rightarrow x^2-2lx-1 = 0.$

Multiplicando (5.2) e (5.3) teremos que,

$$\begin{aligned}
&N_{K|\mathbb{Q}}\left(u - v\sqrt{l^2+1}\right) \cdot N_{K|\mathbb{Q}}\left(l + \sqrt{l^2+1}\right) = \pm m \Rightarrow \\
&\Rightarrow N_{K|\mathbb{Q}}\left(\left(u - v\sqrt{l^2+1}\right) \cdot \left(l + \sqrt{l^2+1}\right)\right) = \pm m \\
&\Rightarrow N_{K|\mathbb{Q}}\left(ul + u\sqrt{l^2+1} - vl\sqrt{l^2+1} - v(l^2+1)\right) = \pm m \\
&\Rightarrow N_{K|\mathbb{Q}}\left(\left(lu - v(l^2+1)\right) + (u - lv)\sqrt{l^2+1}\right) = \pm m.
\end{aligned}$$

Note que,

$$x = \left(lu - v(l^2+1)\right)+(u-lv)\sqrt{l^2+1} \Rightarrow x-\left(lu - v(l^2+1)\right) = (u-lv)\sqrt{l^2+1}$$

$$\Rightarrow x^2 - 2\left(lu - v(l^2+1)\right)x + \left(lu - v(l^2+1)\right)^2 = (u-lv)^2 \cdot (l^2+1)$$

$$\Rightarrow x^2 - 2\left(lu - v(l^2+1)\right)x + \underbrace{\left(lu - v(l^2+1)\right)^2 - (u-lv)^2 \cdot (l^2+1)}_{\text{produto das raízes}} = 0.$$

Então,

$$X^2 - 2\left(lu - v(l^2+1)\right)X + \left(lu - v(l^2+1)\right)^2 - (u-lv)^2 \cdot (l^2+1)$$

é o polinômio minimal de $(lu - v(l^2+1)) + (u-lv)\sqrt{l^2+1}$ sobre $\mathbb{Q}$.

Com isso,

$$\pm m = N_{K|\mathbb{Q}}\left((lu - v(l^2+1)) + (u - lv)\sqrt{l^2+1}\right) =$$

$$= \left[lu - v(l^2+1)\right]^2 - (u-lv)^2 \cdot (l^2+1) = \left[lu - v(l^2+1)\right]^2 - (u-lv)^2 \cdot (l^2+1) =$$

$$= \left|lu - v(l^2+1)\right|^2 - (l^2+1) \cdot |u - lv|^2.$$

Portanto, $(|lu - (l^2+1)v|, |u - lv|)$ é uma solução em inteiros de (5.1) tal que $|lu - (l^2+1)v| \geq 0$ e $|u - lv| > 0$, já que m não é um quadrado. Por causa da escolha mínima de v, necessariamente $|u - lv| \geq v$, isto é,

$$\begin{array}{ccc} u - lv \geq v & \text{ou} & -(u - lv) \geq v \Rightarrow \\ \Rightarrow u \geq lv + v & \text{ou} & u - lv \leq -v \\ \Rightarrow u \geq (l+1)v & \text{ou} & 0 \leq u \leq lv - v = (l-1)v \end{array}$$

Inserindo essas informações em (5.1), obtemos que,

$$\pm m = u^2 - (l^2+1)v^2 \geq (l+1)^2v^2 - (l^2+1)v^2 =$$

$$= (l^2 + 2l + 1 - l^2 - 1)v^2 = 2lv^2 \geq 2l \Rightarrow m \geq 2l$$

(pois, $-m \geq 2l \Rightarrow m \leq -2l < 0 \Rightarrow m < 0$(contradição))
ou,

$$\pm m = u^2 - (l^2+1)v^2 \leq (l-1)^2v^2 - (l^2+1)v^2 = (l^2 - 2l + 1)v^2 - (l^2+1)v^2 =$$

$$= l^2v^2 - 2lv^2 + v^2 - l^2v^2 - v^2 = -2lv^2 \leq -2l \Rightarrow -m \leq -2l \Rightarrow m \geq 2l.$$

■

Seja A um domínio qualquer e K seu corpo de frações. Vimos no Capítulo 1 que um A-módulo M, contido em K, é dito ser um ideal fracionário de A quando existe um elemento $a \in A$, $a \neq 0$, tal que $aM \subset A$.

Consequências:

(i) Todo ideal de A é também um ideal fracionário.

$$I \subset A \quad \text{ideal} \quad , \quad \begin{array}{rcccc} + & : & I \times I & \to & I \\ \cdot & : & I \times A & \to & I \end{array}$$

I é um A-módulo e $I \subset K$ (pois, $I \subset A \subset K$); $0 \neq 1 \in A$ e $1 \cdot I \subset A$.

(ii) O próprio K não é ideal fracionário de A (a menos que, $A = K$).

Suponha que $K =$ (corpo de frações) é ideal fracionário do domínio A. Então, $\exists a \in A, a \neq 0$ tal que $aK \subset A$, ou seja, $\exists 0 \neq a \in A$ tal que $K \subset A\left(\frac{1}{a}\right)$.

Note que, $A\left(\frac{1}{a}\right) \subset K$ (pela definição do conjunto K). Logo, $K = A \cdot \left(\frac{1}{a}\right)$.

Note também que, $A \subset A\left(\frac{1}{a}\right)$ (com efeito,

$$c \in A \Rightarrow c = ca \cdot \frac{1}{a} \in A \cdot \left(\frac{1}{a}\right) \quad \therefore \quad A \subset A\left(\frac{1}{a}\right)\Big).$$

Afirmação 5.3 $\frac{1}{a} \in A$.

Com efeito,

$$\frac{1}{a^2} \in K = A \cdot \left(\frac{1}{a}\right) \Rightarrow \frac{1}{a^2} = b \cdot \frac{1}{a} \quad \text{com} \quad b \in A \underbrace{\Rightarrow}_{a \neq 0} \frac{1}{a} = b \in A.$$

E daí, $A \cdot \left(\frac{1}{a}\right) \subset A$. Ou seja, $A \cdot \left(\frac{1}{a}\right) = A$. Portanto, $K = A$.

Demonstração (Teorema 5.1): Seja B o anel dos inteiros de $\mathbb{Q}(\sqrt{p})$. Como $p \equiv 1 (\mathrm{mod}\ 4)$ então os elementos de B são da forma $(u + v\sqrt{p})/2$ com $u, v \in \mathbb{Z}$ de mesma paridade.

Temos que p é um resíduo quadrático módulo q, pois $p \equiv 1^2 (\mathrm{mod}\ q)$ e 1 é um resíduo quadrático módulo q, pois $1 \equiv 1^2 (\mathrm{mod}\ q)$. Logo, pela definição de símbolo de Legendre,

$$\left(\frac{p}{q}\right) = \left(\frac{1}{q}\right) = 1.$$

Como B é um anel de Dedekind que não é corpo e Bq é um ideal de B então Bq se decompõe como produto de ideais primos não-nulos de B. Ou seja,

$$Bq = \prod_{i=1}^{r} \mathcal{B}_i^{e_i},$$

onde os $\mathcal{B}_i's$ são ideais primos não nulos de B, distintos dois a dois e os $e_i's$ (inteiros ≥ 1)são os índices de ramificação de $\mathcal{B}_i$ sobre $\mathbb{Z}$.

Temos que, $B/\mathcal{B}_i$ é um espaço vetorial de dimensão finita f_i sobre $\mathbb{Z}/q\mathbb{Z}$. Essa dimensão é exatamante o grau residual de $\mathcal{B}_i$ sobre $\mathbb{Z}$.

Pelo Teorema 3.1 temos que, $\sum_{i=1}^{r} e_i f_i = [\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$. E daí,

$$e_1f_1 + e_2f_2 + \ldots + e_rf_r = 2 \underbrace{\Rightarrow}_{(*)} r \leq 2 \Rightarrow \begin{cases} e_1f_1 + e_2f_2 = 2 \\ \text{ou} \\ e_1f_1 = 2 \end{cases}$$

$(*)$ Se $r > 2$ então,

$2 < r = 1 + 1 + \ldots + 1 \leq e_1f_1 + e_2f_2 + \ldots + e_rf_r = 2$ (contradição).

Além disso, podem ocorrer somente os seguintes casos:

(a) $r = 2$, $e_1 = e_2 = 1$, $f_1 = f_2 = 1$; se diz então que q se decompõe em $\mathbb{Q}(\sqrt{p})$. Neste caso, $Bq = \mathcal{B}_1\mathcal{B}_2$.

(b) $r = 1$, $e_1 = 1$, $f_1 = 2$; se diz então que q é inerte em $\mathbb{Q}(\sqrt{p})$. Neste caso, $Bq = \mathcal{B}_1$.

(c) $r = 1$, $e_1 = 2$, $f_1 = 1$; isto significa que q se ramifica em $\mathbb{Q}(\sqrt{p})$. Neste caso, $Bq = \mathcal{B}_1^2$.

Como q é um primo ímpar tal que, p é resíduo quadrático módulo q, então pela Proposição 3.5, q se decompõe em $\mathbb{Q}(\sqrt{p})$. Logo, $Bq = QQ'$ onde Q, Q' são

ideais primos distintos de B. E daí,

$$N(Q) = q.$$

Com efeito,

$$N(Q) \cdot N(Q') = N(QQ') = N(Bq) = |N_{\mathbb{Q}(\sqrt{p})|\mathbb{Q}}(q)| = q^{[\mathbb{Q}(\sqrt{p}):\mathbb{Q}]} = q^2 \Rightarrow$$

$$\Rightarrow \quad N(Q) \cdot N(Q') = q^2 \Rightarrow N(Q)|q^2 \Rightarrow N(Q) = 1, q \text{ ou } q^2.$$

Se,

$$N(Q) = 1 \Rightarrow \mathrm{Card}\,(B/Q) = 1 \Rightarrow B = Q \Rightarrow$$

$$\Rightarrow Q \text{ não é ideal primo de } B \text{ (contradição)}$$

$$N(Q) = q^2 \quad \Rightarrow \quad N(Q) = N(Q) \cdot N(Q') \Rightarrow N(Q') = 1 \Rightarrow \mathrm{Card}\,(B/Q) = 1$$

$$\Rightarrow \quad B = Q' \Rightarrow Q' \text{ não é ideal primo de } B \text{ (contradição)}$$

Portanto,

$$N(Q) = q.$$

Seja $I(B)$ o monóide (semigrupo com unidade) dos ideais fracionários não-nulos do anel de Dedekind B. Já sabemos que $I(B)$ é um grupo e que os ideais fracionários principais (isto é, da forma $Bx, x \in \mathrm{Cf}(B)$) formam um subgrupo normal $F(B)$ de $I(B)$. Considere então, o grupo quociente:

$$C(B) = I(B)/F(B),$$

isto é, o grupo das classes de ideais de $\mathbb{Q}(\sqrt{p})$. O Teorema de Dirichlet nos garante que $h(p)$ é finito. Suponha agora que $h(p)$ não seja maior do que 1. Então $h(p) = 1$.

Afirmação 5.4 *B é um domínio principal.*

Com efeito,

Pelo Teorema de Lagrange, temos que,

$$|I(B)| = |F(B)| \cdot \underbrace{[I(B) : F(B)]}_{\text{índice de } F(B) \text{ em } I(B)}.$$

Sendo $h(p) = 1$, temos:

$$1 = h(p) = |C(B)| = [I(B) : F(B)].$$

E daí,

$$|I(B)| = |F(B)| \cdot 1 = |F(B)| \underbrace{\Rightarrow}_{F(B) \subset I(B)} I(B) = F(B).$$

Considere agora J um ideal não nulo qualquer de B. Logo, J é um ideal fracionário não nulo de B. E daí,

$$J \in I(B) = F(B) \Rightarrow J \in F(B) \Rightarrow J = Bx, \quad \text{onde} \quad x \in \mathrm{Cf}(B).$$

Por outro lado, J é um ideal de B. Então,

$$J \subset B \Rightarrow Bx \subset B.$$

E daí,

$$x = 1 \cdot x \in Bx \subset B \Rightarrow x \in B.$$

Ou seja, J é um ideal principal de B. Portanto, B é um domínio principal.
Como Q é um ideal de B então $Q = B\left(\frac{u + v\sqrt{p}}{2}\right)$ onde $u, v \in \mathbb{Z}$ e $u \equiv v (\mathrm{mod}\ 2)$, já que, os elementos de B são da forma $\frac{u + v\sqrt{p}}{2}$, com $u, v \in \mathbb{Z}$ e $u \equiv v (\mathrm{mod}\ 2)$. Com isso,

$$q = N(Q) = N\left(B\left(\frac{u + v\sqrt{p}}{2}\right)\right) = \left|N_{\mathbb{Q}(\sqrt{p})|\mathbb{Q}}\left(\frac{u + v\sqrt{p}}{2}\right)\right|.$$

Note que,

$$x = \frac{u + v\sqrt{p}}{2} \Rightarrow x - \frac{u}{2} = \frac{v}{2}\sqrt{p} \Rightarrow x^2 - 2ux + \frac{u^2}{4} = \frac{v^2}{4}p \Rightarrow$$
$$\Rightarrow \quad x^2 - 2ux + \frac{u^2}{4} - \frac{v^2}{4}p = 0 \Rightarrow x^2 - 2ux + \frac{u^2 - v^2 p}{4} = 0.$$

Então, $X^2 - 2uX + \dfrac{u^2 - pv^2}{4}$ é o polinômio minimal de $\dfrac{u + v\sqrt{p}}{2}$ sobre $\mathbb{Q}$. Como $\mathbb{Q}(\sqrt{p}) = \mathbb{Q}\left(\dfrac{u + v\sqrt{p}}{2}\right)$ então $\dfrac{u + v\sqrt{p}}{2}$ é um elemento primitivo de $\mathbb{Q}(\sqrt{p})$ sobre $\mathbb{Q}$. Nesse caso, o polinômio característico de $\dfrac{u + v\sqrt{p}}{2}$ com respeito à $\mathbb{Q}(\sqrt{p})$ e $\mathbb{Q}$ coincide com o polinômio minimal de $\dfrac{u + v\sqrt{p}}{2}$ sobre $\mathbb{Q}$. E daí,

$$N_{\mathbb{Q}(\sqrt{p})|\mathbb{Q}}\left(\frac{u + v\sqrt{p}}{2}\right) = \frac{u^2 - pv^2}{4}.$$

Logo,

$$\begin{aligned} & q = \left| N_{\mathbb{Q}(\sqrt{p})|\mathbb{Q}}\left(\frac{u + v\sqrt{p}}{2}\right)\right| = \left|\frac{u^2 - pv^2}{4}\right| \Rightarrow \\ \Rightarrow \quad & \frac{u^2 - pv^2}{4} = \pm q \Rightarrow u^2 - pv^2 = \pm 4q \Rightarrow u^2 - \left((2qn)^2 + 1\right)v^2 = \pm 4q \\ \Rightarrow \quad & (u, v) \quad \text{é solução de} \quad x^2 - \left((2qn)^2 + 1\right)y^2 = \pm 4q \end{aligned}$$

Como $2qn$, $4q$ são inteiros e $4q$ não é um quadrado (pois, q é primo) então, pelo Lema 5.2, concluímos que,

$$4q \geq 2(2qn) = 4qn \Rightarrow 1 \geq n \quad \text{(contradição), pois} \quad n > 1.$$

Portanto,

$$h(p) > 1.$$

■

Teorema 5.3 *Sejam k um corpo de números algébricos, $K|k$ uma extensão finita e seja $h(k)$, $h(K)$ o número de classes de k, K, respectivamente. Se nenhuma extensão abeliana não ramificada de k está contida em K, então $h(k)|h(K)$.*

Antes de provarmos o Teorema 5.3, precisaremos de algumas definições e de alguns resultados relativos à teoria de Galois e ao corpo de classes de Hilbert de um corpo numérico.

5.1 Teoria de Galois

Dados um corpo L e um conjunto G de automorfismos de L, o conjunto dos $x \in L$ tais que $\sigma(x) = x$ para todo $\sigma \in G$ é, como podemos vê imediatamente, um subcorpo de L, que se chama o corpo dos invariantes de G.

$$W = \{x \in L \quad ; \quad \sigma(x) = x \quad \text{para todo} \quad \sigma \in G\}.$$

Observe que,

$$y \cdot y^{-1} = e_L \Rightarrow \sigma(y) \cdot \sigma(y^{-1}) = \sigma(e_L) = e_L \Rightarrow$$

$$\Rightarrow y \cdot \sigma(y^{-1}) = e_L \Rightarrow \sigma(y^{-1}) = y^{-1} \cdot e_L = y^{-1}.$$

$x, y \in W \subset L$
$\sigma(x \cdot y^{-1}) = \sigma(x) \cdot \sigma(y^{-1}) = x \cdot y^{-1} \Rightarrow xy^{-1} \in W.$

Por outro lado, dada uma extensão L de um corpo K, o conjunto dos K-automorfismos de L é um grupo para a composição de aplicações. O corpo dos invariantes desse grupo contém K.

Teorema 5.4 *Seja L uma extensão de grau finito n de um corpo K finito ou de característica zero. As seguintes condições são equivalentes:*

(a) *K é o corpo dos invariantes do grupo G dos K-automorfismos de L;*

(b) *Para todo $x \in L$, o polinômio minimal de x sobre K tem todas as suas raízes em L;*

(c) *L é gerada pelas raízes de um polinômio sobre K.*

Nestas condições o grupo G dos K-automorfismos de L tem $n = [L : K]$ elementos.

Demonstração: Ver [10], página 86.

Definição 5.1 *Se são satisfeitas as condições do Teorema 5.4, se diz que* L *é uma extensão de Galois sobre* K*, e que* G *é o grupo de Galois de* L *sobre* K*, o qual denotaremos por* $G(L|K)$*. Se* $G(L|K)$ *é abeliano (respectivamente cíclico) se diz que* L *é uma extensão abeliana (respectivamente cíclica) de* K*.*

Corolário 5.1 *Sejam* K *um corpo finito ou de característica* 0 *(zero),* L *uma extensão de grau finito* n *de* K*, e* H *um grupo de automorfismos de* L *que admite* K *como corpo de invariantes. Então,* L *é uma extensão de Galois de* K *e* H *é seu grupo de Galois.*

Demonstração: Ver [10], página 87.

Teorema 5.5 *Sejam* K *um corpo finito ou de característica* 0 *(zero),* L *uma extensão de Galois de* K*, e* G *seu grupo de Galois. A todo subgrupo* G' *de* G *lhe associamos o corpo dos invariantes* $k(G')$ *de* G'*, e a todo subcorpo* K' *de* L *que contenha* K *lhe associamos o subgrupo* $g(K') \subset G$ *dos* K'*-automorfismos de* L*.*

- **(a)** *As aplicações* g *e* k *são bijeções recíprocas entre si, decrescentes para as relações de inclusão. E além disso,* L *é extensão de Galois de todo corpo intermediário* K' *(isto é,* $K \subset K' \subset L$*).*

- **(b)** *Para que um corpo intermediário* K' *seja extensão de Galois de* K*, é necessário e suficiente que* $g(K')$ *seja um subgrupo invariante de* G*(normal de* G*). Neste caso o grupo de Galois de* K' *sobre* K *se identifica com o grupo quociente* $G/g(K')$*.*

Demonstração: Ver [10], página 87.

Definição 5.2 *Seja* $\widetilde{K}$ *uma extensão de* K*, sejam* L*,* L' *subcorpos de* $\widetilde{K}$ *contendo* K*. O compósito de* L*,* L' *em* $\widetilde{K}$ *é o menor subcorpo de* $\widetilde{K}$ *contendo* L *e* L'*. Nós denotamos ele por* LL' *ou* $L'L$*.*

Observação 5.1 *Se* $L|K$ *é uma extensão de Galois, então o compósito* LL' *é uma extensão de Galois de* L' *e* $G(LL'|L') \simeq G(L|L \cap L')$*. Explicitamente, todo* $(L \cap L')$*-automorfismo de* L *pode ser unicamente estendido a um* L'*-automorfismo de* LL'*.*

Observação 5.2 *Se* $L|K$ *e* $L'|K$ *são extensões de Galois, então o compósito* LL' *é também uma extensão de Galois de* K*.*

5.2 O corpo de classes de Hilbert de um corpo numérico

Definição 5.3 *Seja* K *um corpo de números algébricos, e seja* $L|K$ *uma extensão galosiana de grau finito.* L *é dito ser o corpo de classes de Hilbert de* K *quando a seguinte condição é satisfeita: Os únicos ideais primos de* K*, que se decompõem completamente em ideais primos de grau residual* 1 *sobre* $\mathbb{Q}$*, são os ideais primos principais com grau residual* 1 *sobre* $\mathbb{Q}$*.*

Com esta definição, Hilbert provou os seguintes teoremas:

Teorema 5.6 (Existência e Unicidade) *Para todo corpo de números algébricos* K*, existe um e somente um (a menos de* K*-isomorfismo) corpo de classes de Hilbert de* K*.*

Teorema 5.7 (Isomorfismo) *Se* L *é o corpo de classes de Hilbert de* K*, então* $G(L|K) \simeq C(B) = I(B)/F(B)$ *(grupo das classes de ideais de* K*).*

Nota 5.1 *Seja* L *o corpo das classes de Hilbert de* K*. Logo pelo Teorema 5.7* $G(L|K) \simeq I(B)/F(B)$*. E daí,* $|G(L|K)| = |I(B)/F(B)|$*. Como* $[L : K] < \infty$ *então* $|G(L|K)| = [L : K]$*. Com isso, temos que,*

$$[L : K] = |G(L|K)| = |I(B)/F(B)| = n^\circ \text{ de classes de } K.$$

Como $C(B) = I(B)/F(B)$ *é abeliano e* $G(L|K) \simeq C(B)$ *então* $G(L|K)$ *é abeliano. Portanto,* L *é uma extensão abeliana de* K.

Teorema 5.8 (O discriminante) *Se* L *é o corpo de classes de Hilbert de* K *então o ideal discriminante* $\mathcal{D}_{L|K}$ *de* L *sobre* K *é o ideal unidade* B_K*(anel dos inteiros de* K*).*

Nota 5.2 *Do Teorema 5.8 segue-se que todo ideal primo de* K *é não ramificado no corpo de Classes de Hilbert de* K.
Com efeito, seja L *o corpo de Classes de Hilbert de* K. *Suponha que* $\mathfrak{p}$ *seja um ideal primo de* B_K *(ou de* K*) que se ramifica em* L. *Então pelo Teorema 3.8, temos que,*

$$\mathfrak{p} \supset \mathcal{D}_{L/K}.$$

Mas, o Teorema 5.8 nos diz que $\mathcal{D}_{L/K} = B_K$ *(anel dos inteiros de* K*). Então,*

$$\mathfrak{p} \supset B_K \Rightarrow \mathfrak{p} = B_K,$$

o que é um absurdo (pois, $\mathfrak{p}$ *é ideal primo).*

Logo, nenhum ideal primo de K *se ramifica em* L.

Portanto, $L|K$ *é não ramificada.*

Teorema 5.9 (Decomposição) *Os ideais primos de* K *se decompõem no corpo de classes de Hilbert* L *de* K*, de acordo com a seguinte regra: Se* $f \geq 1$ *é o menor inteiro tal que,* $\mathfrak{p}^f$ *é um ideal principal de* K*, então* $\mathfrak{p}$ *se decompõe em um produto de* $\dfrac{[L:K]}{f}$ *ideais primos distintos de* L*, cada um com grau residual* f *sobre* K.

Demonstração (Teorema 5.3): Temos que $[k : \mathbb{Q}] < \infty$, pois k é corpo numérico. Por hipótese, $K|k$ é uma extensão finita, isto é, $[K : k] < \infty$. Com isso,

$$[K : \mathbb{Q}] = \underbrace{[K : k]}_{<\infty} \cdot \underbrace{[k : \mathbb{Q}]}_{<\infty} < \infty.$$

Logo, K é um corpo numérico. Considere agora (pelo Teorema 5.6) $\overline{k}$ e $\overline{K}$ os corpos de classes de Hilbert de k e K, respectivamente.

Afirmação 5.5 $\left(K \cap \overline{k}\right)|k$ *é uma extensão abeliana não ramificada contida em* K.

Com efeito, sendo $\overline{k}$ o corpo de classes de Hilbert de k então $\overline{k}|k$ é galoisiana de grau finito (Definição 5.3). E daí, pela Observação 5.1 tem-se que $K\overline{k}|K$ é de Galois, e além disso, $G\left(K\overline{k}|K\right) \simeq G\left(\overline{k}|K \cap \overline{k}\right)$. Como $G\left(\overline{k}|k\right)$ é abeliano e $G\left(\overline{k}|K \cap \overline{k}\right)$ é um subgrupo de $G\left(\overline{k}|k\right)$ então $G\left(\overline{k}|K \cap \overline{k}\right)$ é um subgrupo invariante de $G\left(\overline{k}|k\right)$ (isto é, $G\left(\overline{k}|K \cap \overline{k}\right) \lhd G\left(\overline{k}|k\right)$). E daí, pelo item (b) do Teorema 5.5, $K \cap \overline{k}|k$ é de Galois e

$$G\left(K \cap \overline{k}|k\right) \simeq G\left(\overline{k}|k\right)/G\left(\overline{k}|K \cap \overline{k}\right).$$

Mas, $G\left(\overline{k}|k\right)/G\left(\overline{k}|K \cap \overline{k}\right)$ é abeliano, pois $G\left(\overline{k}|k\right)$ é abeliano. Logo, $G\left(K \cap \overline{k}|k\right)$ é abeliano, isto é, $K \cap \overline{k}|k$ é abeliana. Por outro lado, como $\overline{k}|k$ é não ramificada então $K \cap \overline{k}|k$ é não ramificada (pois, se tivesse algum ideal primo $\mathfrak{p}$ que se ramificasse em $K \cap \overline{k}$ ele se ramificaria em $\overline{k}$).

Como $\left(K \cap \overline{k}\right)|k$ é uma extensão abeliana não ramificada contida em K, então da hipótese que temos, concluímos que, $K \cap \overline{k} = k$.

Afirmação 5.6 $K\overline{k}|K$ *é uma extensão abeliana não ramificada.*

Com efeito, na afirmação anterior vimos que,

$$G\left(K\overline{k}|K\right) \simeq G\left(\overline{k}|K \cap \overline{k}\right).$$

Mas, por outro lado, $K \cap \overline{k} = k$. E daí,

$$G\left(K\overline{k}|K\right) \simeq G\left(\overline{k}|k\right),$$

que é abeliano. Logo, $G\left(K\overline{k}|K\right)$ é abeliano, ou seja, $K\overline{k}|K$ é abeliana.

Como $\overline{k}|k$ é não ramificada e $G\left(K\overline{k}|K\right) \simeq G\left(\overline{k}|k\right)$ então $K\overline{k}|K$ é também não ramificada.

Temos também que, $\overline{K}$[1] é maximal (isto é, se $\widetilde{K}$ é qualquer outra extensão abeliana não ramificada de K então $\widetilde{K} \subset \overline{K}$).

Logo, $K\overline{k} \subset \overline{K}$.

Afirmação 5.7 $[K\overline{k} : K] = [\overline{k} : k]$.

Com efeito, como $\overline{k}|k$ é de Galois então $K\overline{k}|K$ é de Galois e $G\left(K\overline{k}|K\right) \simeq G\left(\overline{k}|K \cap \overline{k}\right)$. Note agora que,

$$G\left(K\overline{k}|K\right) \simeq G\left(\overline{k}|K \cap \overline{k}\right) \Rightarrow \left|G\left(K\overline{k}|K\right)\right| = \left|G\left(\overline{k}|K \cap \overline{k}\right)\right| \Rightarrow$$

$$\Rightarrow [K\overline{k} : K] = [\overline{k} : K \cap \overline{k}] = [\overline{k} : k].$$

Como $K\overline{k} \subset \overline{K}$ então decorre que,

$$[\overline{K} : K] = [\overline{K} : K\overline{k}]\cdot[K\overline{k} : K] = \underbrace{[\overline{K} : K\overline{k}]}_{<\infty}\cdot[\overline{k} : k] \Rightarrow [\overline{k} : k]\Big|[\overline{K} : K] \Rightarrow h(k)\Big|h(K).$$

■

Definição 5.4 *Com as mesmas notações da Seção* 3.2*, diremos que o ideal primo* $\mathfrak{p}$ *de* A *é*

(a) *totalmente decomposto em* L*, quando* $q = n$*, ou seja, quando* $e_i = f_i = 1$ *para todo* i*.*

(b) *totalmente inerte em* L*, quando* $q = 1$ *e* $e_1 = 1$*, ou seja, quando* $f_1 = n = [L : K]$.

[1] Ver [13], página 399

(c) *totalmente ramificado em* L*, quando* $q = 1$ *e* $f_1 = 1$*, ou seja, quando* $e_1 = n = [L : K]$.

Lema 5.10 *Seja* $K \subset L \subset L'$ *uma torre de corpos numéricos, e seja* P *um ideal primo de* K*. Se* P *é totalmente ramificado em* $L'|K$*, então* P *é totalmente ramificado em* $L|K$.

Demonstração: Ver [4], página 32.

Proposição 5.1 *Sejam* $K \subseteq L \subseteq L'$ *corpos de números algébricos, com anéis de inteiros* $A \subseteq B \subseteq B'$*; seja* Q' *um ideal primo não nulo de* $B', Q = Q' \cap B$, $P = Q \cap A$*. Então* $e'' = ee'$, $f'' = ff'$*, onde* e, f *correspondem respectivamente, ao índice de ramificação e ao grau residual de* Q *em* $L|K$*, e similarmente* e', f' *correspondendo a* Q' *em* $L'|L$ *e* e'', f'' *correspondendo a* Q' *em* $L'|K$.

Demonstração: Ver [8], página 162.

Proposição 5.2 *Se* $BP = \prod_{i=1}^{g} Q_i^{e_i}$ *e* g_i' *é o número de decomposição de* Q_i *em* $L'|L$ *então o número de decomposição de* P *em* $L'|K$ *é* $g'' = \sum_{i=1}^{g} g_i'$.

Proposição 5.3 *Se* $L|K$ *é uma extensão galoisiana de grau* n*,* $BP = \prod_{i=1}^{g} Q_i^{e_i}$ *e* $[B/Q_i : A/P] = f_i$ *então* $e_1 = \ldots = e_g$ *e* $f_1 = \ldots = f_g$.

Demonstração: Ver [8], página 163.

A Proposição 5.2 pode ser vista também em [8], página 163.

Proposição 5.4 (Critério de Euler) *Seja* p *um primo ímpar e seja* a *um inteiro não múltiplo de* p*. Então,*

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} (\mathrm{mod}\ p).$$

Demonstração: Seja $a \equiv w^t (\mathrm{mod}\ p)$, onde w é uma raiz primitiva módulo p e $0 \leq t < p-1$. Como $\overline{w}$ não é um quadrado em $P(p) = (\mathbb{Z}/(p))^{\bullet}$ e $w^{(p-1)/2} \equiv -1 (\mathrm{mod}\ p)$, então temos que,

$$\left(\frac{a}{p}\right) = \left(\frac{w^t}{p}\right) = \left(\frac{w}{p}\right)^t = (-1)^t \equiv \left(w^{(p-1)/2}\right)^t = \left(w^t\right)^{(p-1)/2} \equiv a^{(p-1)/2} (\mathrm{mod}\ p).$$

■

Proposição 5.5 -1 *é um resíduo quadrático módulo* p *se, e somente se,* $p \equiv 1 (\mathrm{mod}\ 4)$.

Demonstração: $\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} (\mathrm{mod}\ p)$ (Critério de Euler) implica na igualdade $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ (já que estes inteiros são ou 1 ou -1). E daí, $\left(\frac{-1}{p}\right) = 1$ exatamente quando $p \equiv 1 (\mathrm{mod}\ 4)$.

■

Usaremos agora o Teorema 5.3 e um teorema auxiliar para provarmos o seguinte teorema:

Teorema 5.11 *Se* p *é um primo tal que* $p \equiv 1 (\mathrm{mod}\ 4)$ *então* $h(p) | H(p)$.

O teorema auxiliar é o seguinte:

Teorema 5.12 *Seja* p *um número primo ímpar, e seja* $\chi(n) = \left(\frac{n}{p}\right)$ *o símbolo de Legendre. Então,*

$$\tau_1(\chi) = \begin{cases} p^{1/2} & \text{se } p \equiv 1 (\mathrm{mod}\ 4), \\ p^{1/2} i & \text{se } p \equiv 3 (\mathrm{mod}\ 4). \end{cases}$$

Uma prova do Teorema 5.12 pode ser vista em [3], página 47.

Demonstração (Teorema 5.11): Sejam χ o caráter quadrático módulo p dado pelo símbolo de Legendre,

$$\chi(m) = \left(\frac{m}{p}\right)$$

e $\zeta_p = \cos\left(\frac{2\pi}{p}\right) + i\text{sen}\left(\frac{2\pi}{p}\right)$ raiz primitiva p-ésima da unidade. Considere agora a soma de Gauss Principal associada ao caráter χ e a raiz primitiva p-ésima da unidade ζ_p,

$$\tau_1(\chi) = \sum_{\substack{\overline{m}\in P(p)\\ 1\leq m<p}} \left(\frac{m}{p}\right)\zeta_p^m.$$

Como $p \equiv 1(\text{mod } 4)$ então pelo Teorema 5.12 concluímos que,

$$\tau_1(\chi) = \sqrt{p} \quad \Rightarrow \quad \sqrt{p} = \sum_{\substack{\overline{m}\in P(p)\\ 1\leq m<p}} \left(\frac{m}{p}\right)\zeta_p^m. \tag{5.4}$$

Sendo ζ_p raiz p-ésima da unidade então,

$$\begin{aligned}
\zeta_p^p = 1 \qquad &\Rightarrow \qquad \overline{\zeta_p^p} = \overline{1} = 1 \Rightarrow \overline{\zeta_p}^p = 1\\
&\Rightarrow \qquad \zeta_p^p \cdot \overline{\zeta_p}^p = 1 \underbrace{\Rightarrow}_{\mathbb{C}\text{ é corpo}} \left(\zeta_p \cdot \overline{\zeta_p}\right)^p = 1 \Rightarrow\\
&\underbrace{\Rightarrow}_{0\leq|\zeta_p|^2=\zeta_p\cdot\overline{\zeta_p}\in\mathbb{R}} \qquad \zeta_p \cdot \overline{\zeta_p} = 1 \Rightarrow \overline{\zeta_p} = \zeta_p^{-1}.
\end{aligned}$$

Logo,

$$\overline{\zeta_p}^2 = \zeta_p^{-2} \quad , \quad \overline{\zeta_p}^3 = \zeta_p^{-3} \quad , \quad \cdots \quad , \quad \overline{\zeta_p}^{(p-1)/2} = \zeta_p^{-(p-1)/2}.$$

E daí,

$$\zeta_p + \zeta_p^{-1} = \zeta_p + \overline{\zeta_p} \in \mathbb{R}.$$

$$\zeta_p^2 + \zeta_p^{-2} = \zeta_p^2 + \overline{\zeta_p}^2 = \zeta_p^2 + \overline{\zeta_p^2} \in \mathbb{R}.$$

$$\vdots$$

$$\zeta_p^{(p-1)/2} + \zeta_p^{-(p-1)/2} = \zeta_p^{(p-1)/2} + \overline{\zeta_p}^{(p-1)/2} = \zeta_p^{(p-1)/2} + \overline{\zeta_p^{(p-1)/2}} \in \mathbb{R}.$$

Com isso,

$$\mathbb{Q}(\zeta_p^2+\zeta_p^{-2})\subset\mathbb{Q}(\zeta_p) \quad \text{é um subcorpo real de} \quad \mathbb{Q}(\zeta_p)$$

$$\mathbb{Q}(\zeta_p^3+\zeta_p^{-3})\subset\mathbb{Q}(\zeta_p) \quad \text{é um subcorpo real de} \quad \mathbb{Q}(\zeta_p)$$

$$\vdots$$

$$\mathbb{Q}(\zeta_p^{(p-1)/2}+\zeta_p^{-(p-1)/2})\subset\mathbb{Q}(\zeta_p) \quad \text{é um subcorpo real de} \quad \mathbb{Q}(\zeta_p).$$

Mas, $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ é o subcorpo real maximal de $\mathbb{Q}(\zeta_p)$.

Então,

$$\begin{array}{c}\mathbb{Q}(\zeta_p^2+\zeta_p^{-2})\subset\mathbb{Q}(\zeta_p+\zeta_p^{-1})\\ \mathbb{Q}(\zeta_p^3+\zeta_p^{-3})\subset\mathbb{Q}(\zeta_p+\zeta_p^{-1})\\ \vdots\\ \mathbb{Q}(\zeta_p^{(p-1)/2}+\zeta_p^{-(p-1)/2})\subset\mathbb{Q}(\zeta_p+\zeta_p^{-1})\end{array} \Rightarrow \left\{\begin{array}{c}\zeta_p^2+\zeta_p^{-2}\in\mathbb{Q}(\zeta_p+\zeta_p^{-1})\\ \zeta_p^3+\zeta_p^{-3}\in\mathbb{Q}(\zeta_p+\zeta_p^{-1})\\ \vdots\\ \zeta_p^{(p-1)/2}+\zeta_p^{-(p-1)/2}\in\mathbb{Q}(\zeta_p+\zeta_p^{-1}).\end{array}\right.$$

Por outro lado, como $\left(\dfrac{-1}{p}\right)=1$, então

$$\left(\frac{m}{p}\right)=\left(\frac{(-1)\cdot(-m)}{p}\right)=\left(\frac{-1}{p}\right)\cdot\left(\frac{-m}{p}\right)=\left(\frac{-m}{p}\right)\Rightarrow$$

$$\Rightarrow\left(\frac{m}{p}\right)=\left(\frac{-m}{p}\right),\forall 1\leq m<p. \tag{5.5}$$

Retornando agora a igualdade (5.4) temos que,

$$\sqrt{p}=\sum_{\substack{\overline{m}\in P(p)\\ 1\leq m<p}}\left(\frac{m}{p}\right)\zeta_p^m=\left(\frac{1}{p}\right)\zeta_p+\left(\frac{2}{p}\right)\zeta_p^2+\ldots+$$

$$+\left(\frac{(p-1)/2}{p}\right)\zeta_p^{(p-1)/2}+\ldots+\left(\frac{p-1}{p}\right)\zeta_p^{p-1}.$$

Note também que,

$$-1\equiv(p-1)(\mathrm{mod}\ p) \quad \text{e} \quad \zeta_p^p=1 \quad \Rightarrow \quad \left(\frac{-1}{p}\right)=\left(\frac{p-1}{p}\right) \quad \text{e} \quad \zeta_p^{p-1}=\zeta_p^{-1}$$

$$-2 \equiv (p-2)(\mathrm{mod}\ p) \quad \text{e} \quad \zeta_p^p = 1 \quad \Rightarrow \quad \left(\frac{-2}{p}\right) = \left(\frac{p-2}{p}\right) \quad \text{e} \quad \zeta_p^{p-2} = \zeta_p^{-2}$$

$$\vdots$$

$$-\frac{p-1}{2} \equiv \underbrace{\left(\frac{p-1}{2}+1\right)}_{\frac{p+1}{2}} (\mathrm{mod}\ p) \quad \text{e} \quad \zeta_p^p = 1 \quad \Rightarrow$$

$$\Rightarrow \left(\frac{-\frac{p-1}{2}}{p}\right) = \left(\frac{\frac{p+1}{2}}{p}\right) \quad \text{e} \quad \zeta_p^{\frac{p+1}{2}} = \zeta_p^{-\frac{p-1}{2}}.$$

Logo,

$$\begin{aligned}\sqrt{p} &= \sum_{\substack{m \in P(p) \\ 1 \le m < p}} \left(\frac{m}{p}\right)\zeta_p^m = \left[\left(\frac{1}{p}\right)\zeta_p + \left(\frac{-1}{p}\right)\zeta_p^{-1}\right] + \left[\left(\frac{2}{p}\right)\zeta_p^2 + \left(\frac{p-2}{p}\right)\zeta_p^{-2}\right] + \\ &\quad + \ldots + \left[\left(\frac{(p-1)/2}{p}\right)\zeta_p^{(p-1)/2} + \left(\frac{-(p-1)/2}{p}\right)\zeta_p^{-(p-1)/2}\right] \underbrace{=}_{(5.5)} \\ &= \overbrace{\left(\frac{1}{p}\right)}^{\in \mathbb{Z} \subset \mathbb{Q} \subset K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})} \cdot \underbrace{(\zeta_p + \zeta_p^{-1})}_{\in K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})} + \overbrace{\left(\frac{2}{p}\right)}^{\in \mathbb{Z} \subset \mathbb{Q} \subset K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})} \cdot \underbrace{(\zeta_p^2 + \zeta_p^{-2})}_{\in K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})} + \ldots + \\ &\quad + \overbrace{\left(\frac{(p-1)/2}{p}\right)}^{\in \mathbb{Z} \subset \mathbb{Q} \subset K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})} \cdot \underbrace{(\zeta_p^{(p-1)/2} + \zeta_p^{-(p-1)/2})}_{\in K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})}.\end{aligned}$$

Ou seja,

$$\sqrt{p} \in K = \mathbb{Q}(\zeta_p + \zeta_p^{-1}).$$

Portanto,

$$\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p + \zeta_p^{-1}).$$

Temos então que, $\mathbb{Q}(\sqrt{p})$ é um corpo numérico e $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ é uma extensão finita de $\mathbb{Q}(\sqrt{p})$.

Afirmação 5.8 *Nenhuma extensão abeliana não ramificada de* $\mathbb{Q}(\sqrt{p})$ *está contida em* $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$.

Com efeito, suponha que exista uma extensão abeliana não ramificada L de $\mathbb{Q}(\sqrt{p})$ contida em $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$. Sendo $[L : \mathbb{Q}(\sqrt{p})] > 1$ segue-se que $[L : \mathbb{Q}] > 3$. Como p é totalmente ramificado em $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ então pelo Lema 5.10, p é totalmente ramificado em $L|\mathbb{Q}$. Logo, o índice de ramificação $e''(p)$ de p em $L|\mathbb{Q}$ é igual à $[L : \mathbb{Q}]$. Temos também que p se ramifica completamente em $\mathbb{Q}(\sqrt{p})$, pois p é um divisor primo ímpar de p. E daí, o índice de ramificação $e(p)$ de p em $\mathbb{Q}(\sqrt{p})|\mathbb{Q}$ é igual à $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$. Ou seja, se B representa o anel dos inteiros de $\mathbb{Q}(\sqrt{p})$ então, $Bp = q^2$, onde q é um ideal primo de B.

Como L é corpo intermediário da extensão ciclotômica $\mathbb{Q}(\zeta_{4p})$ de $\mathbb{Q}$ então L é extensão de Galois de $\mathbb{Q}$, e daí, L é extensão de Galois de $\mathbb{Q}(\sqrt{p})$.

Por outro lado, como $L|\mathbb{Q}(\sqrt{p})$ é não ramificada então o índice de ramificação $e'(q)$ de q em $L|\mathbb{Q}(\sqrt{p})$ é igual à 1.

Usando agora a multiplicatividade do índice de ramificação (garantida pela Proposição 5.1) obtém-se que,

$$e''(p) = e(p) \cdot e'(q) \Rightarrow [L : \mathbb{Q}] = 2 \cdot 1 = 2 \Rightarrow 2 = [L : \mathbb{Q}] > 3 \quad \text{(contradição)}.$$

Portanto, não existe extensão abeliana não ramificada de $\mathbb{Q}(\sqrt{p})$ contida em $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$. E daí, pelo Teorema 5.3, $h(p)|H(p)$.

■

Usaremos agora os Teoremas 5.1 e 5.11 para provarmos o seguinte teorema:

Teorema 5.13 *Se* $p = (2qn)^2 + 1$ *é um primo, com* q *primo ímpar e* $n > 1$ *inteiro então* $H(p) > 1$, *mais precisamente,* $H(p) > 2$.

Antes de provarmos o Teorema 5.13 vamos enunciar um resultado que também será usado em tal prova.

Proposição 5.6 *Se* p *é um primo tal que* $p \equiv 1(\mathrm{mod}\ 4)$ *então o número de classes* $h(p)$ *do corpo quadrático real* $\mathbb{Q}(\sqrt{p})$ *é ímpar.*

O resultado acima pode ser visto em [2], página 354.

Demonstração (Teorema 5.13): Pelo Teorema 5.1 e pela Proposição 5.6 acima temos que $h(p) > 1$ e ímpar, ou seja, $h(p) > 2$. Por outro lado, como $p \equiv 1(\mathrm{mod}\ 4)$ então pelo Teorema 5.11, concluímos que $h(p)|H(p)$. E daí, $H(p) \geq h(p) > 2$. Portanto, $H(p) > 2$.

■

Tomando por exemplo $q = 2, 3, 5$ em $p = (2qn)^2 + 1$, vemos facilmente que para os seguintes primos menores que 10000 : $p = 257, 401, 577, 1297, 1601, 2917, 3137, 4357, 7057, 8101$ temos $H(p) > 2$.

Capítulo 6

O número de classes do subcorpo real maximal de $\mathbb{Q}(\zeta_{4p})$

Seja $H(m)$ o número de classes do corpo $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$, onde $\mathbb{Q}$ é o corpo dos números racionais e ζ_m é uma raiz primitiva m-ésima da unidade para um inteiro positivo m.

No ($\S 1$) iremos considerar as equações diofantinas $x^2 - py^2 = \pm 4q$ com p, q primos ímpares distintos e estabelecer uma condição necessária e suficiente para que elas tenham solução. Em seguida, no $(\S 2)$ mostraremos que para p, q primos ímpares distintos satisfazendo $p = ((2n+1)q)^2 \pm 2$ com $n \geq 0$ inteiro, a equação diofantina $x^2 - py^2 = \pm q$ não tem solução (x, y) em inteiros, exceto para o caso $p = 7 (n = 0, q = 3)$.

Além disso, na Seção 3, daremos uma condição suficiente para que o número de classes $h(p)$ do corpo quadrático real $\mathbb{Q}(\sqrt{p})$ seja maior do que 1, onde p são primos do tipo $((2n+1)q)^2 \pm 2$ com q primo ímpar e $n \geq 0$ inteiro. Aplicando este resultado ao subcorpo real maximal de um corpo ciclotômico, apresentaremos também uma condição suficiente para que $H(4p)$ seja maior do que 1, onde p são primos do tipo $((2n+1)q)^2 \pm 2$ com q primo ímpar e $n \geq 0$ inteiro.

Para finalizar, apresentaremos a lista de todos os primos $p < 100000$ satisfazendo $p = ((2n+1)q)^2 - 2$ com $q \equiv 1$ ou $3 (\mathrm{mod}\ 8)$ primo ($n \geq 0$ inteiro) e $p = ((2n+1)q)^2 + 2$ com $q \equiv 1$ ou $7 (\mathrm{mod}\ 8)$ primo ($n \geq 0$ inteiro), para os quais $h(p)$ e $H(4p)$ são maiores do que 1.

6.1 Solubilidade da equação $x^2 - py^2 = \pm 4q$

Consideraremos nesta seção, a equação diofantina $x^2 - py^2 = \pm 4q$ para primos ímpares distintos p, q. No entanto, o seguinte fato é notável: Quando a equação $x^2 - py^2 = \pm q$ tem uma solução (u, v) em inteiros, o dobro da solução $(2u, 2v)$ é também uma solução da equação $x^2 - py^2 = \pm 4q$. Veja,

$$(2u)^2 - p(2v)^2 = 4u^2 - 4pv^2 = 4(u^2 - pv^2) = 4(\pm q) = \pm 4q.$$

Reciprocamente, no caso $p \not\equiv 1 (\mathrm{mod}\ 4)$ todas as soluções de $x^2 - py^2 = \pm 4q$ podem ser obtidas das soluções de $x^2 - py^2 = \pm q$, enquanto que no caso $p \equiv 1 (\mathrm{mod}\ 4)$ nem todas as soluções podem necessariamente ser achadas das soluções de $x^2 - py^2 = \pm q$.

O resultado que segue irá relacionar a solubilidade da equação $x^2 - py^2 = \pm 4q$ com o número de classes do corpo quadrático real $\mathbb{Q}(\sqrt{p})$.

Teorema 6.1 *Sejam p e q dois primos ímpares distintos. Então, a equação diofantina $x^2 - py^2 = \pm 4q$ tem pelo menos uma solução (x, y) em inteiros se, e somente se, o primo q se decompõe completamente no corpo quadrático real $\mathbb{Q}(\sqrt{p})$ como produto de um ideal primo principal $\mathfrak{q}$ com grau 1 e seu conjugado $\mathfrak{q}'$: $Bq = \mathfrak{q} \cdot \mathfrak{q}'$, ($\mathfrak{q} \neq \mathfrak{q}'$, $N(\mathfrak{q}) = N(\mathfrak{q}') = q$, $\mathfrak{q} = (w)$, $\mathfrak{q}' = (w')$ com w, w' em B).*

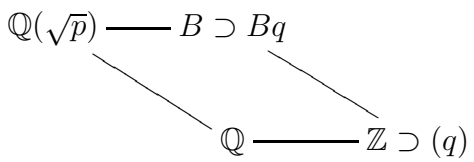
Observação 6.1 *No enunciado acima B representa o anel dos inteiros de $\mathbb{Q}(\sqrt{p})$.*

Demonstração: Se existe uma solução (u, v) em inteiros de $x^2 - py^2 = \pm 4q$, então $u^2 - pv^2 = \pm 4q$ implicando que $pv^2 \equiv u^2 (\mathrm{mod}\ q)$. Ou seja, pv^2 é um resíduo quadrático módulo q. E daí,

$$1 = \left(\frac{pv^2}{q}\right) = \left(\frac{p}{q}\right) \cdot \left(\frac{v^2}{q}\right) = \left(\frac{p}{q}\right) \cdot 1 = \left(\frac{p}{q}\right)$$

$\Rightarrow$ p é um resíduo quadrático módulo q

$\Rightarrow$ q se decompõe completamente em $\mathbb{Q}(\sqrt{p})$.



Logo, $Bq = \mathfrak{q} \cdot \mathfrak{q}'$ onde $\mathfrak{q}, \mathfrak{q}'$ são ideais primos distintos de B.

Por outro lado,

$$\begin{aligned}
u^2 - pv^2 = \pm 4q \quad &\Rightarrow \quad \left(\frac{u}{2}\right)^2 - \left(\frac{v\sqrt{p}}{2}\right)^2 = \pm q \\
&\Rightarrow \quad \left(\frac{u + v\sqrt{p}}{2}\right) \cdot \left(\frac{u - v\sqrt{p}}{2}\right) = \pm q \\
&\Rightarrow \quad B\left(\left(\frac{u + v\sqrt{p}}{2}\right) \cdot \left(\frac{u - v\sqrt{p}}{2}\right)\right) = \pm Bq = Bq \\
&\Rightarrow \quad B\left(\frac{u + v\sqrt{p}}{2}\right) \cdot B\left(\frac{u - v\sqrt{p}}{2}\right) = Bq = \mathfrak{q} \cdot \mathfrak{q}' \\
&\Rightarrow \quad \mathfrak{q} = B\left(\frac{u + v\sqrt{p}}{2}\right) \quad \text{e} \quad \mathfrak{q}' = B\left(\frac{u - v\sqrt{p}}{2}\right) \quad \text{ou} \\
&\qquad\ \ \mathfrak{q} = B\left(\frac{u - v\sqrt{p}}{2}\right) \quad \text{e} \quad \mathfrak{q}' = B\left(\frac{u + v\sqrt{p}}{2}\right) \\
&\Rightarrow \quad \mathfrak{q} \quad \text{e} \quad \mathfrak{q}' \quad \text{são ideais primos principais de} \quad B.
\end{aligned}$$

Além disso,

$$N(\mathfrak{q}) \cdot N(\mathfrak{q}') = N(\mathfrak{q}\mathfrak{q}') = N(Bq) = \left|N_{\mathbb{Q}(\sqrt{p})|\mathbb{Q}}(q)\right| = q^{[\mathbb{Q}(\sqrt{p}):\mathbb{Q}]} = q^2 \Rightarrow$$

$$\Rightarrow \quad N(\mathfrak{q}) \cdot N(\mathfrak{q}') = q^2 \Rightarrow N(\mathfrak{q}) | q^2 \Rightarrow N(\mathfrak{q}) = 1, q \text{ ou } q^2.$$

Se,

$$\bullet N(\mathfrak{q}) = 1 \Rightarrow \mathrm{Card}\,(B/\mathfrak{q}) = 1 \Rightarrow B = \mathfrak{q} \Rightarrow$$

$$\Rightarrow \mathfrak{q} \quad \text{não é ideal primo de} \quad B \quad \text{(contradição)}$$

$\bullet N(\mathfrak{q}) = q^2 \;\Rightarrow\; N(\mathfrak{q}) = N(\mathfrak{q}) \cdot N(\mathfrak{q}') \Rightarrow N(\mathfrak{q}') = 1 \Rightarrow \mathrm{Card}\,(B/\mathfrak{q}') = 1 \Rightarrow$

$\Rightarrow \; B = \mathfrak{q}' \Rightarrow \mathfrak{q}'$ não é ideal primo de B (contradição).

Logo, $N(\mathfrak{q}) = q$.

Analogamente, conclui-se que $N(\mathfrak{q}') = q$.

Portanto, $\mathfrak{q}$ e $\mathfrak{q}'$ são ideais primos principais de B de graus residuais iguais a 1.

Reciprocamente, suponha que q se decompõe completamente em $\mathbb{Q}(\sqrt{p})$ como produto de um ideal primo principal $\mathfrak{q}$ de grau residual 1 e seu conjugado $\mathfrak{q}'$, isto é, $Bq = \mathfrak{q} \cdot \mathfrak{q}'$, onde $\mathfrak{q} \neq \mathfrak{q}'$, $N(\mathfrak{q}) = N(\mathfrak{q}') = q$, $\mathfrak{q} = (w)$, $\mathfrak{q}' = (w')$ com $w, w' \in B$. Como p é primo ímpar então $p \equiv 1$ ou $3 (\mathrm{mod}\ 4)$.

$\hookrightarrow p \equiv 3 (\mathrm{mod}\ 4)$

Neste caso, $B = \{u + v\sqrt{p}; u, v \in \mathbb{Z}\}$.

Com isso, existem $u, v \in \mathbb{Z}$ tais que $w = u + v\sqrt{p}$ e $w' = u - v\sqrt{p}$. Logo,

$$q = N(\mathfrak{q}) = N((w)) = N(Bw) = \left|N_{\mathbb{Q}(\sqrt{p})|\mathbb{Q}}(w)\right| =$$

$$= |u^2 - pv^2| \Rightarrow u^2 - pv^2 = \pm q \Rightarrow$$

$\Rightarrow \quad (u, v) \quad$ é uma solução em inteiros para a equação $\quad x^2 - py^2 = \pm q$

$\Rightarrow \quad (2u, 2v) \quad$ é uma solução em inteiros para a equação $\quad x^2 - py^2 = \pm 4q.$

$\hookrightarrow p \equiv 1 (\mathrm{mod}\ 4)$

Neste caso, $B = \left\{\dfrac{u + v\sqrt{p}}{2}; u, v \in \mathbb{Z} \text{ e têm a mesma paridade}\right\}$. Com isso,

existem $u, v \in \mathbb{Z}$ tais que $w = \dfrac{u + v\sqrt{p}}{2}$ e $w' = \dfrac{u - v\sqrt{p}}{2}$. Logo,

$$q = N(\mathfrak{q}) = N((w)) = N(Bw) = \left|N_{\mathbb{Q}(\sqrt{p})|\mathbb{Q}}(w)\right| = \left|\frac{u^2 - pv^2}{4}\right| \Rightarrow$$

$$\Rightarrow \quad \frac{u^2 - pv^2}{4} = \pm q \Rightarrow u^2 - pv^2 = \pm 4q$$

$$\Rightarrow \quad (u, v) \quad \text{é uma solução em inteiros para a equação} \quad x^2 - py^2 = \pm 4q.$$

■

Exemplo 6.1 *Sejam p e q dois primos ímpares satisfazendo $p = 4q^2 + 1$ ou $p = q^2 + 4$. Então, a equação $x^2 - py^2 = \pm 4q$ tem uma solução $(2q \pm 1, 1)$ ou $(q \pm 2, 1)$ em inteiros, respectivamente. Por outro lado, o primo q se decompõe completamente em $\mathbb{Q}(\sqrt{p})$, da seguinte forma:*

$$Bq = \mathfrak{q} \cdot \mathfrak{q}' \quad ; \quad \mathfrak{q} = \left(\frac{2q \pm 1 + \sqrt{p}}{2}\right) \quad e \quad \mathfrak{q}' = \left(\frac{2q \pm 1 - \sqrt{p}}{2}\right)$$

ou

$$\mathfrak{q} = \left(\frac{q \pm 2 + \sqrt{p}}{2}\right) \quad e \quad \mathfrak{q}' = \left(\frac{q \pm 2 - \sqrt{p}}{2}\right),$$

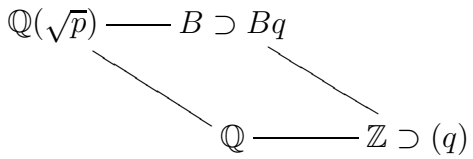
respectivamente.

Usando o Teorema 6.1 podemos deduzir facilmente o seguinte resultado:

Corolário 6.1 *Sejam p e q dois primos ímpares satisfazendo $p = (nq)^2 + r^2$ para números naturais n, r. Então, o número de classes $h(p)$ do corpo quadrático real $\mathbb{Q}(\sqrt{p})$ não é igual à 1 (isto é, $h(p) > 1$) se $x^2 - py^2 = \pm 4q$ não tem solução (x, y) em inteiros.*

Demonstração: Como $p = (nq)^2 + r^2$ então $p \equiv r^2 (\mathrm{mod}\ q)$. Ou seja, p é um resíduo quadrático módulo q. E daí, q se decompõe completamente em $\mathbb{Q}(\sqrt{p})$.

Ou seja, $Bq = \mathfrak{q} \cdot \mathfrak{q}'$ onde $\mathfrak{q}, \mathfrak{q}'$ são ideais primos distintos de B. É claro que, $N(\mathfrak{q}) = N(\mathfrak{q}') = q$.



Suponha agora que $h(p) = 1$ e que a equação $x^2 - py^2 = \pm 4q$ não tenha solução (x, y) em inteiros. Da igualdade $h(p) = 1$ conclui-se que B é um domínio principal[1]. E daí, $\mathfrak{q} = (w)$ e $\mathfrak{q}' = (w')$ onde $w, w' \in B$.

Com isso, q se decompõe completamente em $\mathbb{Q}(\sqrt{p})$ como produto de um ideal primo principal $\mathfrak{q} = (w)$ de grau 1 e seu conjugado $\mathfrak{q}' = (w')$. Decorre então do Teorema 6.1 que a equação $x^2 - py^2 = \pm 4q$ tem pelo menos uma solução (x, y) em inteiros (contradição). Portanto, $h(p) > 1$.

■

6.2 Solubilidade da equação $x^2 - py^2 = \pm q$ para $p = ((2n+1)q)^2 \pm 2$

Teorema 6.2 *Sejam* p *e* q *dois primos ímpares satisfazendo* $p = ((2n+1)q)^2 \pm 2$ *com* $n \geq 0$ *inteiro. Então, a equação diofantina* $x^2 - py^2 = \pm q$ *tem pelo menos uma solução* (x, y) *em inteiros se, e somente se,* $p = 7$ *e* $q = 3 (n = 0)$*, isto é, somente a equação* $x^2 - 7y^2 = -3$ *tem uma solução em inteiros, por exemplo* $(x, y) = (2, 1)$.

Demonstração: (1) Sejam p e q dois primos ímpares satisfazendo $p = ((2n+1)q)^2 - 2$ com $n \geq 0$ inteiro e ponha $l = (2n+1)q$.

[1] Ver Afirmação 5.4

Assuma primeiro que $x^2-py^2=q$ tenha pelo menos uma solução em inteiros, e seja[2] (u,v) uma solução de $x^2-py^2=q$ tal que $u>0$ e v é o menor inteiro positivo possível: $u^2-pv^2=q$.

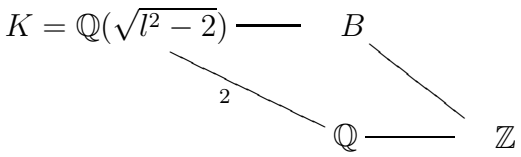
No caso $q>2v^2$, onde $q=u^2-pv^2=u^2-l^2v^2+2v^2$ temos que $(u-lv)(u+lv)=q-2v^2>0$. Como $a=u+lv>0$ então $b=u-lv>0$. Além disso, $l=\dfrac{a-b}{2v}$ e $q=ab+2v^2$. Por outro lado, como $a\geq 1$, $b\geq 1$ e $(a+1)(b-1)=ab-a+b-1$, então $ab-1\geq a-b$. Portanto,

$$\begin{aligned} 0\leq 2nq=l-q=\frac{a-b}{2v}-ab-2v^2=\frac{1}{2v}(a-b-2vab-4v^3)\leq \\ \leq \quad \frac{1}{2v}(ab-1-2vab-4v^3)=\frac{-1}{2v}\left((4v^3+1)+(2v-1)ab\right)<0, \end{aligned}$$

o que é claramente um absurdo.

No caso $q<2v^2$, considere os elementos

$$l^2-1+l\sqrt{l^2-2}, u-v\sqrt{l^2-2}\in K=\mathbb{Q}(\sqrt{l^2-2}).$$



Note agora que,

$$\begin{aligned} x=l^2-1+l\sqrt{l^2-2} \quad &\Rightarrow \quad x-(l^2-1)=l\sqrt{l^2-2} \\ &\Rightarrow \quad x^2-2(l^2-1)x+(l^2-1)^2=l^2\cdot(l^2-2) \\ &\Rightarrow \quad x^2-2(l^2-1)x+l^4-2l^2+1-l^4+2l^2=0 \\ &\Rightarrow \quad x^2-2(l^2-1)x+1=0. \end{aligned}$$

[2]Ver Afirmação 5.2

e

$$\begin{aligned} z = u - v\sqrt{l^2-2} &\Rightarrow z - u = v\sqrt{l^2-2} \\ &\Rightarrow z^2 - 2uz + u^2 = v^2 \cdot (l^2-2) \\ &\Rightarrow z^2 - 2uz + u^2 - v^2l^2 + 2v^2 = 0 \\ &\Rightarrow z^2 - 2uz + q = 0. \end{aligned}$$

Logo, $X^2 - 2(l^2-1)X + 1$ é o polinômio minimal de $l^2 - 1 + l\sqrt{l^2-2}$ sobre $\mathbb{Q}$ e $X^2 - 2uX + q$ é o polinômio minimal de $u - v\sqrt{l^2-2}$ sobre $\mathbb{Q}$.

Além disso, $l^2 - 1 + l\sqrt{l^2-2}$ e $u - v\sqrt{l^2-2}$ são elementos primitivos de K sobre $\mathbb{Q}$, já que,

$$\mathbb{Q}(\sqrt{l^2-2}) = \mathbb{Q}\left((l^2-1) + l\sqrt{l^2-2}\right) \quad \text{e} \quad \mathbb{Q}(\sqrt{l^2-2}) = \mathbb{Q}(u - v\sqrt{l^2-2}).$$

Nesse caso, o polinômio característico de $(l^2-1) + l\sqrt{l^2-2}$ com respeito à K e $\mathbb{Q}$ coincide com o polinômio minimal de $(l^2-1) + l\sqrt{l^2-2}$ sobre $\mathbb{Q}$. Pelo mesmo motivo, o polinômio característico de $u - v\sqrt{l^2-2}$ com respeito à K e $\mathbb{Q}$ coincide com o polinômio minimal de $u - v\sqrt{l^2-2}$ sobre $\mathbb{Q}$. E daí,

$$N_{K|\mathbb{Q}}\left((l^2-1) + l\sqrt{l^2-2}\right) = 1 \quad \text{e} \quad N_{K|\mathbb{Q}}\left(u - v\sqrt{l^2-2}\right) = q.$$

Multiplicando ambos os membros das igualdades acima obtemos o seguinte:

$$\begin{aligned} q &= N_{K|\mathbb{Q}}\left((l^2-1) + l\sqrt{l^2-2}\right) \cdot N_{K|\mathbb{Q}}\left(u - v\sqrt{l^2-2}\right) \\ &= N_{K|\mathbb{Q}}\left[\left((l^2-1) + l\sqrt{l^2-2}\right) \cdot \left(u - v\sqrt{l^2-2}\right)\right] \\ &= N_{K|\mathbb{Q}}\left[\{(l^2-1)u - lv(l^2-2)\} + \{lu - (l^2-1)v\}\sqrt{l^2-2}\right] \\ &= \{(l^2-1)u - lv(l^2-2)\}^2 - (l^2-2)\{lu - (l^2-1)v\}^2 \\ &= \left|(l^2-1)u - lv(l^2-2)\right|^2 - p\left|lu - (l^2-1)v\right|^2. \end{aligned}$$

Ou seja, $(|(l^2-1)u - lv(l^2-2)|, |lu - (l^2-1)v|)$ é uma solução em inteiros positivos de $x^2 - py^2 = q$. Da minimalidade de v concluímos que,

$$\left|lu - (l^2-1)v\right| \geq v.$$

Se $lu-(l^2-1)v \geq v$ (isto é, $u \geq lv$) então,

$$q = u^2-(l^2-2)v^2 \geq l^2v^2-(l^2-2)v^2 = 2v^2,$$

o que contradiz o fato de q ser menor que $2v^2$.

Se $(l^2-1)v-lu \geq v$ (isto é, $(l^2-2)v \geq lu$) então,

$$\begin{aligned} l^2q = l^2u^2-l^2(l^2-2)v^2 &\leq (l^2-2)^2v^2-l^2(l^2-2)v^2 = \\ &= (l^2-2)v^2[l^2-2-l^2] = -2(l^2-2)v^2 < 0, \end{aligned}$$

que é também uma contradição.

Portanto, é impossível que para o primo $p = ((2n+1)q)^2-2$ a equação $x^2-py^2 = q$ tenha uma solução em inteiros.

Assuma agora que $x^2-py^2 = -q$ tem pelo menos uma solução em inteiros, e seja[3] (u,v) uma solução de $x^2-py^2 = -q$ tal que $u > 0$ e v é o menor inteiro positivo possível: $u^2-pv^2 = -q$.

No caso $q = 3, v = 1$ temos que,

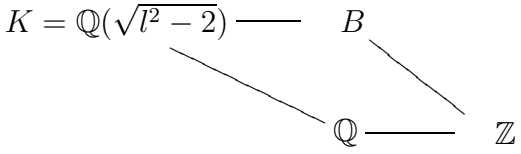
$$\begin{aligned} 3 = -q = u^2-pv^2 = u^2-l^2+2 &\Rightarrow (l-u)(l+u) = 5 \Rightarrow \\ &\Rightarrow l-u = 1 \text{ e } l+u = 5 \Rightarrow l = 3 \text{ e } u = 2. \end{aligned}$$

E daí, $p = 7$. Iremos concluir que esse é o único caso possível de solubilidade da equação $x^2-py^2 = \pm q$ (em inteiros) para $p = ((2n+1)q)^2 \pm 2$.

No caso $q = 3, v \geq 2$ ou $q > 3, v \geq q$ iremos proceder analogamente ao que já havíamos feito para $x^2-py^2 = q$. Considere as normas,

$$N_{K|\mathbb{Q}}\left((l^2-1)+l\sqrt{l^2-2}\right) = 1 \quad \text{e} \quad N_{K|\mathbb{Q}}\left(u-v\sqrt{l^2-2}\right) = -q$$

dos elementos $(l^2-1)+l\sqrt{l^2-2}, u-v\sqrt{l^2-2} \in K = \mathbb{Q}(\sqrt{l^2-2})$.



[3]Ver Afirmação 5.2

Multiplicando membro a membro obtemos o seguinte:

$$\begin{aligned}
-q &= N_{K|\mathbb{Q}}\left((l^2-1)+l\sqrt{l^2-2}\right)\cdot N_{K|\mathbb{Q}}\left(u-v\sqrt{l^2-2}\right)\\
&= N_{K|\mathbb{Q}}\left[\left((l^2-1)+l\sqrt{l^2-2}\right)\cdot\left(u-v\sqrt{l^2-2}\right)\right]\\
&= N_{K|\mathbb{Q}}\left[\{(l^2-1)u-lv(l^2-2)\}+\{lu-(l^2-1)v\}\sqrt{l^2-2}\right]\\
&= \{(l^2-1)u-lv(l^2-2)\}^2-(l^2-2)\{lu-(l^2-1)v\}^2\\
&= \left|(l^2-1)u-lv(l^2-2)\right|^2-p\left|lu-(l^2-1)v\right|^2.
\end{aligned}$$

Ou seja, $(|(l^2-1)u-lv(l^2-2)|,|lu-(l^2-1)v|)$ é uma solução em inteiros positivos de $x^2-py^2=-q$. Da minimalidade de v concluímos que,

$$\left|lu-(l^2-1)v\right|\geq v.$$

Se $lu-(l^2-1)v\geq v$ então,

$$-q=u^2-(l^2-2)v^2\geq l^2v^2-(l^2-2)v^2=2v^2>0,$$

que é uma contradição.

Se $(l^2-1)v-lu\geq v$ então,

$$-l^2q=l^2u^2-l^2(l^2-2)v^2\leq(l^2-2)^2v^2-l^2(l^2-2)v^2=$$

$$=-2(l^2-2)v^2\Rightarrow l^2q\geq 2(l^2-2)v^2.$$

Portanto, no caso de $q=3$ e $v\geq 2$, $3l^2\geq 2(l^2-2)v^2\geq 8(l^2-2)$ implicando então que $16\geq 5l^2\geq 45$, que é uma contradição. No caso de $v\geq q>3$, $l^2v\geq l^2q\geq 2l^2v^2-4v^2$ implicando então que $4v^2\geq(2v^2-v)l^2\geq v(2v-1)q^2$, e daí

$$q^2\leq\frac{4v}{2v-1}=2+\frac{2}{2v-1}<2+\frac{2}{5}<3,$$

que é uma contradição.

No caso $q>3, v<q$ onde $-q=u^2-pv^2=u^2-l^2v^2+2v^2$ tem-se que, $(lv-u)(lv+u)=q+2v^2>0$, $a=lv-u$ e $b=lv+u$ são inteiros

positivos, $l = \dfrac{a+b}{2v}$ e $q = ab - 2v^2$. Por outro lado, como $a \geq 1, b \geq 1$ e $(a-1)(b-1) = ab - (a+b) + 1$ então $ab + 1 \geq a + b$. Portanto,

$$\begin{aligned} & 0 \leq 2nq = l - q = \frac{a+b}{2v} - ab + 2v^2 = \frac{1}{2v}(a + b - 2vab + 4v^3) \leq \\ \leq \quad & \frac{1}{2v}(ab + 1 - 2vab + 4v^3) = \frac{1}{2v}\left((4v^3+1) - (2v-1)ab\right) \Rightarrow \\ \Rightarrow \quad & 4v^3 + 1 \geq (2v-1)ab \Rightarrow ab \leq \frac{4v^3+1}{2v-1}. \end{aligned}$$

E daí,

$$q = ab - 2v^2 \leq \frac{4v^3+1}{2v-1} - 2v^2 = \frac{2v^2+1}{2v-1} = v + \frac{v+1}{2v-1}.$$

Se $v = 1$ ou 2 então $q \leq v + \dfrac{v+1}{2v-1} = 3$, que é uma contradição.

Se $v \geq 3$ então $0 < \dfrac{v+1}{2v-1} < 1$, que implica em $q \leq v + \dfrac{v+1}{2v-1} < v + 1$, contradizendo o fato de q ser maior que v (isto é, de q ser maior ou igual à $v + 1$).

Portanto, é impossível (exceto para o caso de $p = 7, q = 3 (n = 0)$) que para $p = ((2n+1)q)^2 - 2$ a equação $x^2 - py^2 = -q$ tenha uma solução em inteiros.

(2) Sejam p e q dois primos ímpares satisfazendo $p = ((2n+1)q)^2 + 2$ com $n \geq 0$ inteiro e ponha $l = (2n+1)q$.

Assuma primeiro que $x^2 - py^2 = q$ tenha pelo menos uma solução em inteiros, e seja[4] (u, v) uma solução de $x^2 - py^2 = q$ tal que $u > 0$ e v é o menor inteiro positivo possível: $u^2 - pv^2 = q$.

No caso $q > v$, onde $q = u^2 - l^2v^2 - 2v^2$ tem-se que $(u - lv)(u + lv) = = q + 2v^2 > 0$, $a = u - lv$ e $b = u + lv$ são inteiros positivos, $l = \dfrac{b-a}{2v}$ e

[4]Ver Afirmação 5.2

$q = ab - 2v^2$. E daí, pelo que já vimos,

$$\begin{aligned} & 0 \leq 2nq = l - q = \frac{b-a}{2v} - (ab - 2v^2) = \frac{1}{2v}(b - a - 2vab + 4v^3) \leq \\ \leq \quad & \frac{1}{2v}(ab - 1 - 2vab + 4v^3) = \frac{1}{2v}\left((4v^3 - 1) - (2v-1)ab\right) \Rightarrow \\ \Rightarrow \quad & ab \leq \frac{4v^3 - 1}{2v - 1}. \end{aligned}$$

Portanto,

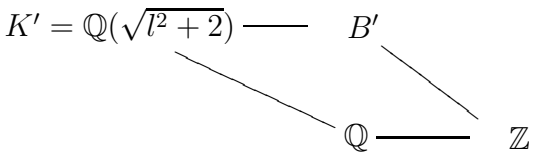
$$q = ab - 2v^2 \leq \frac{4v^3 - 1}{2v - 1} - 2v^2 = \frac{2v^2 - 1}{2v - 1} = v + \frac{v - 1}{2v - 1} < v + 1,$$

o que contradiz o fato de q ser maior que v (isto é, de q ser maior ou igual à $v+1$).

No caso $q \leq v$, iremos proceder de modo análogo ao que já havíamos feito em $x^2 - py^2 = \pm q$ com $p = ((2n+1)q)^2 - 2$. Considere as normas,

$$N_{K'|\mathbb{Q}}\left((l^2+1) + l\sqrt{l^2+2}\right) = 1 \quad \text{e} \quad N_{K'|\mathbb{Q}}\left(u - v\sqrt{l^2+2}\right) = q$$

dos elementos $(l^2+1) + l\sqrt{l^2+2}, u - v\sqrt{l^2+2} \in K' = \mathbb{Q}(\sqrt{l^2+2})$.



Multiplicando membro a membro obtemos o seguinte:

$$\begin{aligned} q &= N_{K'|\mathbb{Q}}\left((l^2+1) + l\sqrt{l^2+2}\right) \cdot N_{K'|\mathbb{Q}}\left(u - v\sqrt{l^2+2}\right) \\ &= N_{K'|\mathbb{Q}}\left[\left((l^2+1) + l\sqrt{l^2+2}\right) \cdot \left(u - v\sqrt{l^2+2}\right)\right] \\ &= N_{K'|\mathbb{Q}}\left[\{(l^2+1)u - lv(l^2+2)\} + \{lu - (l^2+1)v\}\sqrt{l^2+2}\right] \\ &= \{u(l^2+1) - lv(l^2+2)\}^2 - (l^2+2)\{lu - (l^2+1)v\}^2 \\ &= \left|u(l^2+1) - lv(l^2+2)\right|^2 - p\left|lu - (l^2+1)v\right|^2. \end{aligned}$$

Ou seja, $(|u(l^2+1) - lv(l^2+2)|, |lu - (l^2+1)v|)$ é uma solução em inteiros positivos de $x^2 - py^2 = q$. Da minimalidade de v concluímos que,

$$\left|lu - (l^2+1)v\right| \geq v.$$

Se $lu-(l^2+1)v \geq v$ (isto é, $lu \geq (l^2+2)v$) então,

$$l^2q = l^2u^2 - l^2(l^2+2)v^2 \geq (l^2+2)^2v^2 - l^2(l^2+2)v^2 = 2(l^2+2)v^2 \geq 2(l^2+2)q^2,$$

e daí, $q \leq \dfrac{l^2}{2(l^2+2)} < \dfrac{1}{2}$, que é uma contradição.

Se $(l^2+1)v - lu \geq v$ (isto é, $u \leq lv$) então,

$$q = u^2 - (l^2+2)v^2 \leq l^2v^2 - (l^2+2)v^2 = -2v^2 < 0,$$

que é também uma contradição.

Assuma agora que $x^2 - py^2 = -q$ tenha pelo menos uma solução em inteiros, e seja[5] (u,v) uma solução de $x^2 - py^2 = -q$ com $u > 0$ e v o menor inteiro positivo possível: $u^2 - pv^2 = -q$.

No caso $q > 2v^2$, onde $-q = u^2 - l^2v^2 - 2v^2$ tem-se que $(lv-u)(lv+u) = q - 2v^2 > 0$, $a = lv - u$ e $b = lv + u$ são inteiros positivos, $l = \dfrac{a+b}{2v}$ e $q = ab + 2v^2$. E daí, pelo que já vimos,

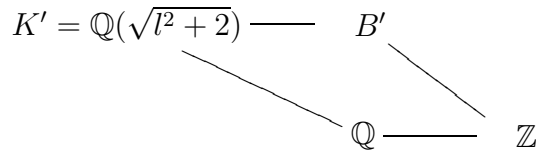
$$\begin{aligned} 0 \leq l - q = \frac{a+b}{2v} - (ab+2v^2) = \frac{1}{2v}(a+b-2vab-4v^3) \leq \\ \leq \frac{1}{2v}(ab+1-2vab-4v^3) = \frac{-1}{2v}\left((2v-1)ab + (4v^3-1)\right) < 0, \end{aligned}$$

que é um absurdo.

No caso $q < 2v^2$, considere as normas,

$$N_{K'|\mathbb{Q}}\left((l^2+1) + l\sqrt{l^2+2}\right) = 1 \quad \text{e} \quad N_{K'|\mathbb{Q}}\left(u - v\sqrt{l^2+2}\right) = -q$$

dos elementos $(l^2+1) + l\sqrt{l^2+2}, u - v\sqrt{l^2+2} \in K' = \mathbb{Q}(\sqrt{l^2+2})$.



[5] Ver Afirmação 5.2

Multiplicando membro a membro as igualdades acima, obtemos o seguinte:

$$\begin{aligned} -q &= N_{K'|\mathbb{Q}}\left((l^2+1)+l\sqrt{l^2+2}\right)\cdot N_{K'|\mathbb{Q}}\left(u-v\sqrt{l^2+2}\right) \\ &= N_{K'|\mathbb{Q}}\left[\left((l^2+1)+l\sqrt{l^2+2}\right)\cdot\left(u-v\sqrt{l^2+2}\right)\right] \\ &= N_{K'|\mathbb{Q}}\left[\{(l^2+1)u-lv(l^2+2)\}+\{lu-(l^2+1)v\}\sqrt{l^2+2}\right] \\ &= \{u(l^2+1)-lv(l^2+2)\}^2-(l^2+2)\{lu-(l^2+1)v\}^2 \\ &= \left|u(l^2+1)-lv(l^2+2)\right|^2-p\left|lu-(l^2+1)v\right|^2. \end{aligned}$$

Ou seja, $\left(\left|u(l^2+1)-lv(l^2+2)\right|,\left|lu-(l^2+1)v\right|\right)$ é uma solução em inteiros positivos de $x^2-py^2=-q$. Da minimalidade de v concluímos que,

$$\left|lu-(l^2+1)v\right|\geq v.$$

Se $lu-(l^2+1)v\geq v$ (isto é, $lu\geq(l^2+2)v$) então,

$$-l^2q=l^2u^2-l^2(l^2+2)v^2\geq(l^2+2)^2v^2-l^2(l^2+2)v^2=2(l^2+2)v^2=2pv^2>0,$$

que é uma contradição.

Se $(l^2+1)v-lu\geq v$ (isto é, $u\leq lv$) então,

$$-q=u^2-(l^2+2)v^2\leq l^2v^2-(l^2+2)v^2=-2v^2,$$

o que contradiz o fato de q ser menor que $2v^2$.

Portanto, é impossível que para $p=((2n+1)q)^2+2$ a equação $x^2-py^2=\pm q$ tenha uma solução em inteiros.

■

6.3 O número de classes de subcorpos reais de um corpo ciclotômico

Nesta seção, vamos considerar o número de classes $h(p)$ do corpo quadrático real $\mathbb{Q}(\sqrt{p})$ e o número de classes $H(4p)$ do subcorpo real maximal $\mathbb{Q}(\zeta_{4p}+\zeta_{4p}^{-1})$

do corpo ciclotômico $\mathbb{Q}(\zeta_{4p})$:

$$\mathbb{Q} \subset \mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1}) \subset \mathbb{Q}(\zeta_{4p}).$$

Usaremos agora os Teoremas 6.1 e 6.2 para provar o seguinte teorema:

Teorema 6.3 (1) *Se* $p = ((2n+1)q)^2 - 2$ *é um primo, onde* q *é um primo ímpar satisfazendo* $q \equiv 1$ *ou* $3 (\mathrm{mod}\ 8)$ *e* $n \geq 0$ *é um inteiro, então o número de classes* $h(p)$ *do corpo quadrático real* $\mathbb{Q}(\sqrt{p})$ *não é igual à* 1 *(exceto para o caso de* $p = 7 (n = 0, q = 3)$*), isto é,* $h(p) > 1$.
(2) *Se* $p = ((2n+1)q)^2 + 2$ *é um primo, onde* q *é um primo ímpar satisfazendo* $q \equiv 1$ *ou* $7 (\mathrm{mod}\ 8)$ *e* $n \geq 0$ *é um inteiro, então o número de classes* $h(p)$ *do corpo quadrático real* $\mathbb{Q}(\sqrt{p})$ *não é igual à* 1*, isto é,* $h(p) > 1$.

Antes de provarmos o Teorema 6.3, vamos enunciar uma proposição relativa à resíduos quadráticos, que será usada em tal prova.

Proposição 6.1 2 *é um resíduo quadrático módulo* p *se, e somente se,* $p \equiv \pm 1 (\mathrm{mod}\ 8)$*; explicitamente* $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$.

A prova da Proposição 6.1 pode ser vista em [9], página 65.

Demonstração (Teorema 6.3): (1) Como $p = ((2n+1)q)^2 - 2$ é um primo e $n \geq 0$ é um inteiro então $p \equiv -2 (\mathrm{mod}\ q)$. E daí, pelas propriedades do símbolo de Legendre,

$$\left(\frac{p}{q}\right) = \left(\frac{-2}{q}\right) = \left(\frac{-1}{q}\right) \cdot \left(\frac{2}{q}\right).$$

Suponha primeiro que, $q \equiv 1 (\mathrm{mod}\ 8)$. Então, pelas Proposições 5.5 e 6.1 concluímos que -1 e 2 são resíduos quadráticos módulo q, ou seja, $\left(\frac{-1}{q}\right) = \left(\frac{2}{q}\right) = 1$. Admita agora que, $q \equiv 3 (\mathrm{mod}\ 8)$. Nesse caso, $q \not\equiv 1 (\mathrm{mod} 4)$ e $q \not\equiv \pm 1 (\mathrm{mod} 8)$. Decorre então das Proposições 5.5 e 6.1 que -1 e 2 são não resíduos quadráticos módulo q, ou seja, $\left(\frac{-1}{q}\right) = \left(\frac{2}{q}\right) = -1$. Em qualquer

caso, p é um resíduo quadrático módulo q. E daí, q se decompõe completamente em $\mathbb{Q}(\sqrt{p})$. Vamos agora supor que $h(p) = 1$ (isto é, $h(p)$ não é maior do que 1). Logo, o anel B dos inteiros de $\mathbb{Q}(\sqrt{p})$ é principal[6]. Desse modo, q se decompõe completamente em $\mathbb{Q}(\sqrt{p})$ como produto de um ideal primo principal de grau residual 1 e seu conjugado. Vimos no Teorema 6.1, que quando isso acontece a equação $x^2 - py^2 = \pm q$ tem pelo menos uma solução em inteiros. Por outro lado, excetuando o caso $p = 7(n = 0, q = 3)$, isso é uma contradição ao Teorema 6.2. Portanto, com exceção do caso $p = 7(n = 0, q = 3)$, o número de classes $h(p)$ do corpo quadrático real $\mathbb{Q}(\sqrt{p})$ é sempre maior do que 1.

(2) Como $p = ((2n+1)q)^2 + 2$ é um primo e $n \geq 0$ é um inteiro então $p \equiv 2(\mathrm{mod}\ q)$. E daí, pelas propriedades do símbolo de Legendre,

$$\left(\frac{p}{q}\right) = \left(\frac{2}{q}\right).$$

Temos que, $q \equiv 1$ ou $7(\mathrm{mod}\ 8)$, isto é, $q \equiv \pm 1(\mathrm{mod} 8)$. Então, pela Proposição 6.1 concluímos que 2 é um resíduo quadrático módulo q, ou seja, $\left(\frac{2}{q}\right) = 1$. Consequentemente, p é um resíduo quadrático módulo q. E daí, q se decompõe completamente em $\mathbb{Q}(\sqrt{p})$. Vamos agora supor que $h(p) = 1$ (isto é, $h(p)$ não é maior do que 1). Logo, o anel B' dos inteiros de $\mathbb{Q}(\sqrt{p})$ é principal[7]. Desse modo, q se decompõe completamente em $\mathbb{Q}(\sqrt{p})$ como produto de um ideal primo principal de grau residual 1 e seu conjugado. Pelo que vimos no Teorema 6.1, quando isso acontece a equação $x^2 - py^2 = \pm q$ tem pelo menos uma solução em inteiros. Por outro lado, isso é uma contradição ao Teorema 6.2. Portanto, o número de classes $h(p)$ do corpo quadrático real $\mathbb{Q}(\sqrt{p})$ é sempre maior do que 1.

■

[6]Ver Afirmação 5.4

[7]Ver Afirmação 5.4

A condição suficiente para que $H(4p)$ seja maior do que 1 será determinada a partir do seguinte teorema:

Teorema 6.4 *Para um inteiro positivo* m*, seja* ζ_m *uma raiz primitiva* m*-ésima da unidade e denote por* $H(m), h(m)$ *o número de classes do corpo* $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$, $\mathbb{Q}(\sqrt{m})$ *respectivamente. Se um primo* p *satisfaz* $p \equiv 3 (\mathrm{mod}\ 4)$*, então* $h(p)|H(4p)$.

Antes de provarmos o Teorema 6.4, vamos enunciar um resultado que será usado em tal prova.

Proposição 6.2 *Sejam* q *um primo ímpar e* ζ *uma raiz primitiva* q*-ésima da unidade. Então,* $E = \mathbb{Q}(\zeta)$ *contém exatamente um corpo quadrático* E'*, a saber,*

$$E' = \mathbb{Q}\left(\sqrt{(-1)^{(q-1)/2}q}\right).$$

A prova da Proposição 6.2 pode ser vista em [14], página 260.

Demonstração (Teorema 6.4): Considere a soma de Gauss

$$\sqrt{d} = \sum_{\substack{\overline{a} \in P(|d|) \\ 1 \leq a < |d|}} \left\{\frac{d}{a}\right\} \zeta_{|d|}^{a},$$

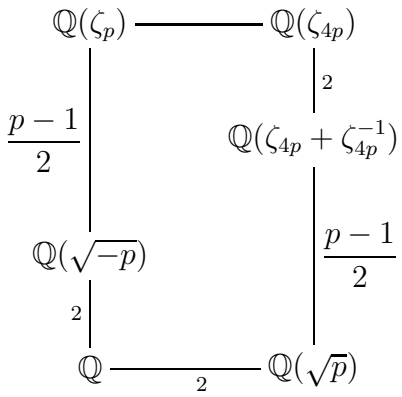
onde d é o discriminante de $\mathbb{Q}(\sqrt{p})$ e $\left\{\dfrac{d}{a}\right\}$ representa o símbolo Kronecker. Já vimos no Teorema 4.1 que usando tal soma e as propriedades do símbolo de Kronecker, conclui-se que $\mathbb{Q}(\sqrt{p})$ está imerso em $K = \mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$, isto é, $\mathbb{Q}(\sqrt{p}) \subset K = \mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$. Pela Proposição 6.2, $\mathbb{Q}(\zeta_p)$ contém exatamente um corpo quadrático, a saber,

$$\mathbb{Q}\left(\sqrt{(-1)^{(p-1)/2}p}\right).$$

Como $p \equiv 3 (\mathrm{mod}\ 4)$ então $\dfrac{p-1}{2}$ não pode ser par, caso contrário, 2 dividiria 1. Logo,

$$\mathbb{Q}\left(\sqrt{(-1)^{(p-1)/2}p}\right) = \mathbb{Q}(\sqrt{-p}).$$

Ou seja, $\mathbb{Q}(\sqrt{-p})$ é o único corpo quadrático contido em $\mathbb{Q}(\zeta_p)$.



Como $\mathbb{Q}(\sqrt{p})|\mathbb{Q}$ é galoisiana então $\mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p)|\mathbb{Q}(\zeta_p)$ é galoisiana, e além disso, os grupos de Galois $G\left(\mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p)|\mathbb{Q}(\zeta_p)\right)$ e $G\left(\mathbb{Q}(\sqrt{p})|\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\zeta_p)\right)$ são isomorfos. Logo,

$$|G\left(\mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p)|\mathbb{Q}(\zeta_p)\right)| = |G\left(\mathbb{Q}(\sqrt{p})|\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\zeta_p)\right)|\,.$$

Por outro lado, como as extensões $\mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p)|\mathbb{Q}(\zeta_p)$ e $\mathbb{Q}(\sqrt{p})|\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\zeta_p)$ são finitas, então:

$$[\mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p):\mathbb{Q}(\zeta_p)] = |G\left(\mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p)|\mathbb{Q}(\zeta_p)\right)| =$$

$$= |G\left(\mathbb{Q}(\sqrt{p})|\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\zeta_p)\right)| = [\mathbb{Q}(\sqrt{p}):\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\zeta_p)]\,.$$

Mostraremos agora que, $\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\zeta_p) = \mathbb{Q}$ e $\mathbb{Q}(\zeta_{4p}) = \mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p)$. Suponha que, $\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\zeta_p) \neq \mathbb{Q}$. Então, $\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\zeta_p) = \mathbb{Q}(\sqrt{p})$. Logo, $\mathbb{Q}(\sqrt{p}) \subset \mathbb{Q}(\zeta_p)$, e daí, $\mathbb{Q}(\sqrt{p})$ é um corpo quadrático diferente de $\mathbb{Q}(\sqrt{-p})$ contido em $\mathbb{Q}(\zeta_p)$ (contradição), pois $\mathbb{Q}(\sqrt{-p})$ é o único corpo quadrático com tal propriedade. Portanto, $\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\zeta_p) = \mathbb{Q}$. Essa igualdade implica na seguinte relação entre os graus:

$$[\mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p):\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\zeta_p)] = [\mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p):\mathbb{Q}(\zeta_p)]\cdot[\mathbb{Q}(\zeta_p):\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\zeta_p)]$$

$$[\mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p):\mathbb{Q}] = [\mathbb{Q}(\sqrt{p}):\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\zeta_p)]\cdot[\mathbb{Q}(\zeta_p):\mathbb{Q}(\sqrt{p})\cap\mathbb{Q}(\zeta_p)]$$

$$[\mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p):\mathbb{Q}] = [\mathbb{Q}(\sqrt{p}):\mathbb{Q}]\cdot[\mathbb{Q}(\zeta_p):\mathbb{Q}]$$

$$[\mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p):\mathbb{Q}] = 2\cdot\varphi(p) = 2\cdot(p-1).$$

Por outro lado,

$$\mathbb{Q}(\sqrt{p})\subset\mathbb{Q}(\zeta_{4p}+\zeta_{4p}^{-1})\subset\mathbb{Q}(\zeta_{4p}) \quad \text{e} \quad \mathbb{Q}(\zeta_p)\subset\mathbb{Q}(\zeta_{4p}) \;\Rightarrow\; \mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p)\subset\mathbb{Q}(\zeta_{4p}).$$

E além disso,

$$[\mathbb{Q}(\zeta_{4p}):\mathbb{Q}] = \varphi(4p) = \varphi(2^2\cdot p) = \varphi(2^2)\cdot\varphi(p) = 2^2\cdot\left(1-\frac{1}{2}\right)\cdot(p-1) = 2(p-1).$$

Logo, $\left[\mathbb{Q}(\zeta_{4p}):\mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p)\right] = 1$. Implicando então que,

$$\mathbb{Q}(\zeta_{4p}) = \mathbb{Q}(\sqrt{p})\mathbb{Q}(\zeta_p).$$

Afirmação 6.1 *Nenhuma extensão abeliana não ramificada de* $\mathbb{Q}(\sqrt{p})$ *está contida em* $\mathbb{Q}(\zeta_{4p}+\zeta_{4p}^{-1})$.

Com efeito, suponha que exista uma extensão abeliana não ramificada L de $\mathbb{Q}(\sqrt{p})$ contida em $\mathbb{Q}(\zeta_{4p}+\zeta_{4p}^{-1})$. Então, $n = [L:\mathbb{Q}(\sqrt{p})] > 2$ já que, $[\mathbb{Q}(\zeta_{4p}+\zeta_{4p}^{-1}):\mathbb{Q}(\sqrt{p})] = \dfrac{p-1}{2}$ é ímpar.

Sejam B, B' e B'' os anéis dos inteiros de $\mathbb{Q}(\sqrt{p})$, L e $\mathbb{Q}(\zeta_{4p})$, respectivamente. Como $\mathbb{Q}(\zeta_{4p})|\mathbb{Q}$ é galoisiana então pela Proposição 5.3 os índices de ramificação são todos iguais, o mesmo ocorrendo para os graus residuais. Sejam então $e''(p)$ o índice de ramificação de p em $\mathbb{Q}(\zeta_{4p})|\mathbb{Q}$, $f''(p)$ o grau residual de p em $\mathbb{Q}(\zeta_{4p})|\mathbb{Q}$ e $r''(p)$ o número de decomposição de p em $\mathbb{Q}(\zeta_{4p})|\mathbb{Q}$. Logo, pela igualdade fundamental,

$$e''(p)\cdot f''(p)\cdot r''(p) = \varphi(4p) = 2\cdot(p-1) \Rightarrow$$

$$\Rightarrow e''(p) = \frac{2\cdot(p-1)}{f''(p)\cdot r''(p)}. \tag{6.1}$$

Sendo p um divisor primo ímpar de p então p se ramifica completamente em $\mathbb{Q}(\sqrt{p})$. Logo, seu índice de ramificação $e(p)$ em $\mathbb{Q}(\sqrt{p})|\mathbb{Q}$ é igual à 2, seu grau residual $f(p)$ em $\mathbb{Q}(\sqrt{p})|\mathbb{Q}$ é igual à 1 e seu número de decomposição $r(p)$ é igual à 1. Seja q o primo que aparece na decomposição de Bp (isto é, $Bp = q^2$). Como L é corpo intermediário da extensão ciclotômica $\mathbb{Q}(\zeta_{4p})$ de $\mathbb{Q}$ então L é extensão de Galois de $\mathbb{Q}$, e daí, L é extensão de Galois de $\mathbb{Q}(\sqrt{p})$. Considere então, $e'(q)$ o índice de ramificação de q em $L|\mathbb{Q}(\sqrt{p})$, $f'(q)$ o grau residual de q em $L|\mathbb{Q}(\sqrt{p})$ e $r'(q)$ o número de decomposição de q em $L|\mathbb{Q}(\sqrt{p})$. Como $L|\mathbb{Q}(\sqrt{p})$ é não ramificada então $e'(q) = 1$. Ou seja,

$$B'q = q_1 \cdot q_2 \cdot \ldots \cdot q_{r'(q)},$$

onde q_j é ideal primo de B' para todo $j = 1, \ldots, r'(q)$.

Como L é corpo intermediário da extensão galoisiana $\mathbb{Q}(\zeta_{4p})|\mathbb{Q}$ então $\mathbb{Q}(\zeta_{4p})|L$ é galoisiana.

Para cada $j = 1, \ldots, r'(q)$ sejam $e''(q_j)$ o índice de ramificação de q_j em $\mathbb{Q}(\zeta_{4p})|L$, $f''(q_j)$ o grau residual de q_j em $\mathbb{Q}(\zeta_{4p})|L$ e $r''(q_j)$ o número de decomposição de q_j em $\mathbb{Q}(\zeta_{4p})|L$. Ou seja,

$$B''q_1 = \left(\mathcal{B}_{11} \cdot \ldots \cdot \mathcal{B}_{1r''(q_1)}\right)^{e''(q_1)}$$

$$B''q_2 = \left(\mathcal{B}_{21} \cdot \ldots \cdot \mathcal{B}_{2r''(q_2)}\right)^{e''(q_2)}$$

$$\vdots$$

$$B''q_{r'(q)} = \left(\mathcal{B}_{r'(q)1} \cdot \ldots \cdot \mathcal{B}_{r'(q)r''(q_{r'(q)})}\right)^{e''(q_{r'(q)})}$$

onde $\mathcal{B}_{11}, \ldots, \mathcal{B}_{1r''(q_1)}$; $\mathcal{B}_{21}, \ldots, \mathcal{B}_{2r''(q_2)}$; $\ldots$; $\mathcal{B}_{r'(q)1}, \ldots, \mathcal{B}_{r'(q)r''(q_{r'(q)})}$ são ideais primos de B''. Pela Proposição 5.1 temos então que,

$$e''(p) = e(p) \cdot e'(q) \cdot e''(q_1) = e(p) \cdot e''(q_1)$$

$$e''(p) = e(p) \cdot e'(q) \cdot e''(q_2) = e(p) \cdot e''(q_2)$$

$$\vdots$$

$$e''(p) = e(p) \cdot e'(q) \cdot e''(q_{r'(q)}) = e(p) \cdot e''(q_{r'(q)}).$$

E daí,

$$\frac{e''(p)}{e(p)} = e''(q_1) = e''(q_2) = \ldots = e''(q_{r'(q)}).$$

Analogamente,

$$\frac{f''(p)}{f'(q)} = f''(q_1) = f''(q_2) = \ldots = f''(q_{r'(q)}).$$

Pela Proposição 5.2, temos também que,

$$r''(p) = r''(q_1) + r''(q_2) + \ldots + r''(q_{r'(q)}) \tag{6.2}$$

E além disso,

$$e''(q_1)f''(q_1)r''(q_1) = e''(q_2)f''(q_2)r''(q_2) = \ldots =$$

$$= e''(q_{r'(q)})f''(q_{r'(q)})r''(q_{r'(q)}) = \frac{p-1}{n}.$$

Substituindo essas igualdades em (6.2), obtemos que:

$$\begin{aligned} r''(p) &= \frac{p-1}{n} \cdot \left[\frac{1}{e''(q_1)f''(q_1)} + \frac{1}{e''(q_2)f''(q_2)} + \ldots + \frac{1}{e''(q_{r'(q)})f''(q_{r'(q)})} \right] \\ &= \frac{p-1}{n} \cdot \left[\frac{1}{e''(q_1)f''(q_1)} + \frac{1}{e''(q_1)f''(q_1)} + \ldots + \frac{1}{e''(q_1)f''(q_1)} \right] \\ &= \frac{p-1}{n} \cdot \frac{r'(q)}{e''(q_1)f''(q_1)} \\ &= r''(q_1)r'(q). \end{aligned}$$

Usando agora a igualdade fundamental em $L|\mathbb{Q}(\sqrt{p})$, tem-se que:

$$e'(q) \cdot f'(q) \cdot r'(q) = n \Rightarrow f'(q) \cdot r'(q) = n.$$

Retornando a igualdade (6.1), obtém-se que:

$$\begin{aligned}
& e''(p) = \frac{2\cdot(p-1)}{f'(q)\cdot f''(q_1)\cdot r''(q_1)\cdot r'(q)} = \frac{2\cdot(p-1)}{n\cdot f''(q_1)\cdot r''(q_1)} \Rightarrow \\
\Rightarrow \quad & \frac{2\cdot(p-1)}{n} = e''(p)\cdot f''(q_1)\cdot r''(q_1) \\
\Rightarrow \quad & e''(p) \quad \text{divide} \quad \frac{2\cdot(p-1)}{n} \\
\underbrace{\Rightarrow}_{n>2} \quad & e''(p) \leq \frac{2\cdot(p-1)}{n} < p-1 \\
\Rightarrow \quad & e''(p) < p-1.
\end{aligned}$$

Como p se ramifica completamente em $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ então o índice de ramificação $\widetilde{e}(p)$ de p em $\mathbb{Q}(\zeta_p)|\mathbb{Q}$ é igual à $\varphi(p) = p-1$. Além disso, como $\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{4p})$ então $\widetilde{e}(p)$ divide $e''(p)$. Logo,

$$e''(p) \geq \widetilde{e}(p) = p-1 \quad \text{(contradição)}.$$

Portanto, não existe extensão abeliana não ramificada de $\mathbb{Q}(\sqrt{p})$ contida em $\mathbb{Q}(\zeta_{4p}+\zeta_{4p}^{-1})$. E daí, pelo Teorema 5.3, concluímos que, $h(p)|H(4p)$.

■

Observação 6.2 *A Afirmação 5.8 pode ser também justificada com os mesmos argumentos que foram usados na Afirmação 6.1. Veja,*

$$\zeta_{4p} \leftrightarrow \zeta_p \quad , \quad n = [L:\mathbb{Q}(\sqrt{p})].$$

$$e''(p)\left|\frac{p-1}{n}\right. \Rightarrow e''(p) \leq \frac{p-1}{n} \underbrace{<}_{n>1} p-1 \Rightarrow e''(p) < p-1 \quad \textit{(contradição)},$$

pois $\quad e''(p) = p-1.$

Vamos agora finalmente apresentar a condição suficiente para que $H(4p)$ seja maior do que 1, onde p é um primo da forma $((2n+1)q)^2 \pm 2$, com q primo ímpar e $n \geq 0$ inteiro.

Teorema 6.5 **(1)** *Se* $p = ((2n+1)q)^2 - 2$ *é um primo, onde* q *é um primo ímpar satisfazendo* $q \equiv 1$ *ou* $3 (\mathrm{mod}\ 8)$ *e* $n \geq 0$ *é um inteiro, então o número de classes* $H(4p)$ *de* $\mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$ *é maior do que* 1 *(exceto para o caso de* $p = 7$ *(*$n = 0, q = 3$*)).*

(2) *Se* $p = ((2n+1)q)^2 + 2$ *é um primo, onde* q *é um primo ímpar satisfazendo* $q \equiv 1$ *ou* $7 (\mathrm{mod}\ 8)$ *e* $n \geq 0$ *é um inteiro, então o número de classes* $H(4p)$ *de* $\mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$ *é maior do que* $1 : H(4p) > 1$.

Demonstração: (1) Como $q \equiv 1$ ou $3 (\mathrm{mod}\ 8)$ então $q^2 \equiv 1$ ou $9 (\mathrm{mod}\ 8)$. Em qualquer caso, $q^2 \equiv 1 (\mathrm{mod}\ 8)$. E daí, 4 divide $q^2 - 1$. Por outro lado,

$$p - 3 = ((2n+1)q)^2 - 5 = (2n+1)^2 q^2 - 5 = (4n^2 + 4n + 1)q^2 - 5 =$$

$$= 4n^2q^2 + 4nq^2 + (q^2 - 1) - 4 \Rightarrow 4 \quad \text{divide} \quad p - 3 \Rightarrow p \equiv 3 (\mathrm{mod}\ 4).$$

Com isso, pelo Teorema 6.4, $h(p) | H(4p)$. Consequentemente, $H(4p) \geq h(p)$. O Teorema 6.3(1) nos garante também que $h(p) > 1$ (exceto para o caso de $p = 7$ ($n = 0, q = 3$)). Portanto, o número de classes $H(4p)$ de $\mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$ é maior do que 1 (exceto para o caso de $p = 7$ ($n = 0, q = 3$)).

(2) Como $q \equiv 1$ ou $7 (\mathrm{mod}\ 8)$ então $q \equiv 1$ ou $-1 (\mathrm{mod}\ 8)$. Em qualquer caso, $q^2 \equiv 1 (\mathrm{mod}\ 8)$. E daí, 4 divide $q^2 - 1$. Por outro lado,

$$p - 3 = ((2n+1)q)^2 - 1 = 4n^2q^2 + 4nq^2 + (q^2 - 1) \Rightarrow$$

$$\Rightarrow 4 \quad \text{divide} \quad p - 3 \Rightarrow p \equiv 3 (\mathrm{mod}\ 4).$$

Com isso, pelo Teorema 6.4, $h(p) | H(4p)$. Consequentemente, $H(4p) \geq h(p)$. O Teorema 6.3(2) nos garante também que $h(p) > 1$. Portanto, o número de classes $H(4p)$ de $\mathbb{Q}(\zeta_{4p} + \zeta_{4p}^{-1})$ é maior do que 1 .

■

Vamos finalizar com a apresentação da lista de todos os primos $p < 100000$, satisfazendo $p = ((2n+1)q)^2 - 2$ com $q \equiv 1$ ou $3(\mathrm{mod}8)$ primo ($n \geq 0$ inteiro), e $p = ((2n+1)q)^2 + 2$ com $q \equiv 1$ ou $7(\mathrm{mod}8)$ primo ($n \geq 0$ inteiro), para os quais $h(p)$ e $H(4p)$ são maiores do que 1.

Para esta apresentação consultamos a tabela do número de classes de corpos quadráticos reais em [12].

Tabela 6.1: $p = ((2n+1)q)^2 - 2$

p	n	q	$h(p)$	p	n	q	$h(p)$
7	0	3	1	357	0	19	3
79	1	3	3	1.087	1	11	7
223	2	3	3	1.847	1	11	7
439	3	3	5	3.023	2	11	3
727	4	3	5	5.927	3	11	5
1.087	5	3	7	7.919	0	89	7
3.967	10	3	5	11.447	0	107	7
4.759	11	3	13	14.159	3	17	9
5.623	12	3	9	14.639	5	11	17
8.647	15	3	13	17.159	0	131	15
13.687	19	3	21	19.319	0	139	11
18.223	22	3	17	31.327	1	59	27
31.327	29	3	27	42.023	2	41	15
33.487	30	3	19	44.519	0	211	11
53.359	38	3	37	53.359	10	11	37
56.167	39	3	27	54.287	0	233	15
71.287	44	3	19	61.007	6	19	15
74.527	45	3	23	64.007	11	11	11
77.839	46	3	37	66.047	0	257	13
81.223	47	3	33	71.287	1	89	19
91.807	50	3	45	81.223	7	19	33
95.479	51	3	33	90.599	3	43	19
99.223	52	3	29	97.967	0	313	25

Tabela 6.2: $p = ((2n+1)q)^2 + 2$

p	n	q	$h(p)$	p	n	q	$h(p)$
443	1	7	3	56.171	1	79	11
11.027	7	7	9	65.027	7	17	21
15.131	1	41	15	74.531	19	7	17
21.611	10	7	15	95.483	1	103	11
47.963	1	73	9				

Referências Bibliográficas

[1] ANKENY, N. C.; CHOWLA, S.; HASSE, H. On the class-number of the maximal real subfield of a cyclotomic field. **J. reine angew. Math.**, v. 217, p. 217-220, 1965.

[2] BOREVICH, Z. I.; SHAFAREVICH, I. R. **Number theory**. New York: Academic Press, 1966. 435 p.

[3] COHEN, H. **Number theory, volume I: Tools and diophantine equations**. New York: Springer-Verlag, 2007. 650 p.

[4] CORREIA, Sergio Alvarez Araujo. **Base integral de** $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$. 2005. 64f. Dissertação (Mestrado em Matemática). Universidade Federal do Ceará.

[5] ENDLER, O. **Teoria dos números algébricos**. Rio de Janeiro: IMPA, 1986. 199 p. (Projeto Euclides)

[6] _____. **Teoria dos corpos**. Rio de Janeiro: IMPA, 1987. 204 p. (Monografias de Matemática nº44)

[7] MARCUS, Daniel A. **Number fields**. New York: Springer-Verlag, 1977. 279 p.

[8] RIBENBOIM, Paulo. **Algebraic numbers**. New York: Wiley-Interscience, 1972. 300 p.

[9] _____. **Classic theory of algebraic numbers**. New York: Springer-Verlag, 2001. 681 p.

[10] SAMUEL, P. **Théorie algébrique des nombres**. Paris: Hermann, 1967. 130 p.

[11] STEWART, I.; TALL, David O. **Algebraic number theory**. New York: Chapman and Hall, 1979. 257 p.

[12] WADA, H. A table of ideal class numbers of real quadratic fields. **Kδkyŭroku in Math**., n. 10, 1981.

[13] WASHINGTON, Lawrence C. **Introduction to cyclotomic fields**. New York: Springer-Verlag, 1996. 487 p.

[14] WEISS, E. **Algebraic number theory**. New York: McGraw-Hill, 1963. 275 p.

[15] YAMAGUCHI, I. On the class-number of the maximal real subfield of a cyclotomic field. **J. reine angew. Math**., v. 272, p. 217-220, 1975.

[16] YAMAGUCHI, I; OOZEKI, K; On the class number of the real quadratic field. **J. TRU mathematics,** v.8, p. 13 - 14, 1972.

[17] YOKOI, H. On the diophantine equation $x^2 - py^2 = \pm 4q$ and the class number of real subfields of a cyclotomic field. **Nagoya Math. J.**, v. 91, p. 151-161, 1983.