EQUAÇÕES DIOFANTINAS E NÚMEROS DE CLASSES

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida pela Sra. **Sonia Regina Di Giacomo** e aprovada pela Comissão Julgadora.

Campinas, 03 de maio de 1994.

Prof. Dr. Paulo Roberto Brumatti
orientador

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação da Universidade Estadual de Campinas, UNICAMP, como requesito parcial para obtenção do Título de MESTRE em Matemática.

Universidade Estadual de Campinas
IMECC

Dissertação de Mestrado

Equações Diofantinas e Números de Classes

Orientador: Prof. Dr. Paulo Roberto Brumatti
Aluna: Sonia Regina Di Giacomo

Janeiro de 1994

Aos meus pais

Ao Celso,
ao Matheus
e à Lívia.

AGRADECIMENTOS

- Ao prof. Dr. Paulo Roberto Brumatti pela atenção, paciência e disponibilidade.

- À UFMS e à CAPES pelo apoio financeiro.

- Aos colegas do Departamento de Matemática da UFMS pelo apoio e incentivo.

- Aos funcionários da PROPP/UFMS pelo apoio.

- Aos amigos do *prédinho* pela convivência carinhosa.

- Aos professores Franco, Paques, Kumpera, San Martim, Ávila, Tozzoni, Ari, Orlando, Patrocínio, Aluízio, Marco Antonio e Bordin pela amizade e incentivo.

- Aos funcionários da Secretaria de Pós Graduação e da Biblioteca do IMECC pela atenção.

- Aos colegas Rachidi e Cápua pelo apoio computacional.

- À Ana Helena e ao Júlio Cesar pelo carinho sempre presente.

ÍNDICE

INTRODUÇÃO

O problema de se solucionar equações diofantinas, que é tão importante quanto antigo dentro da ***Teoria de Números***, pode ser reescrito dentro da linguagem da ***Teoria dos Números Algébricos***. Assim, por exemplo, o problema de se saber quando a equação $A^2 - nB^2 = -1$ tem solução, problema este de mais de 1500 anos, pode aparecer dentro da ***Teoria de Corpos Quadráticos*** como o problema de se determinar quando o corpo quadrático $Q(\sqrt{n})$ tem unidade fundamental de norma negativa. As soluções inteiras da equação $A^2 - nB^2 = 1$, por sua vez, correspondem às unidades (elementos invertíveis) $a + b\sqrt{n}$ do anel $Z[\sqrt{n}]$ cuja norma é 1. De maneira geral, a questão da solubilidade de equações diofantinas do tipo $A^2 - nB^2 = t$ pode ser interpretada como o problema de se encontrar um elemento inteiro algébrico $a + b\sqrt{n}$ de $Q(\sqrt{n})$ cuja norma é t.

Dentro desse espírito, nos propomos neste trabalho examinar o ***número de classes*** de determinados corpos quadráticos, usando como ferramentas básicas apenas fatos elementares concernentes à teoria das equações diofantinas, além de propriedades fundamentais dos corpos quadráticos e de congruências. Trilharemos, pois, pelos caminhos clássicos da ***Teoria dos Números Algébricos***, isto é, sem fazermos uso da ***teoria de valorização*** e sem nos preocuparmos com os métodos analíticos e geométricos tão necessários para uma abordagem mais profunda sobre o ***número de classes***.

No primeiro capítulo, a ***unidade fundamental*** dos corpos quadráticos reais $Q(\sqrt{n})$, quando n for expresso na forma $n = m^2 + r$, com $r \mid 4m$, será determinada, a partir do seu relacionamento com as ***equações de Pell*** e com outras equações diofantinas. Também será estabelecido que o ***número de classes*** do corpo quadrático real $Q(\sqrt{m^2 - 1})$ é diferente de 1, e com isso teremos garantido que o anel de inteiros deste corpo não é um domínio fatorial. Como para estes resultados não encontramos na literatura pesquisada demonstrações que envolvessem apenas os conceitos básicos que nos propusemos utilizar, optamos por demonstrações próprias, nas quais utilizamos uma linguagem adequada aos nossos propósitos. Neste capítulo, algumas idéias contidas em *Degert* [5] foram utilizadas.

No capítulo 2, o resultado principal trata de condições suficientes para que o número de classes dos corpos quadráticos reais

$Q(\sqrt{m^2+r})$, onde $r \mid 4m$, seja não trivial. Este resultado estende os trabalhos de *Ankeny, Chowla e Hasse* [1], *Lang* [14], *Takeuchi* [24] e *Yamaguchi* [25]. Neste capítulo também serão estabelecidos dois resultados que tratam de condições necessárias para a solubilidade de determinadas equações diofantinas. Um desses resultados também generaliza os trabalhos de *Ankeny, Chowla e Hasse* [1] e *Lang* [14], e é uma boa alternativa de substituição para a falsa generalização de resultados de [1] e [14] contida em [17]. Neste capítulo baseamo-nos, fortemente, em *Mollin* [17] embora *Ankeny, Chowla e Hasse* [1] e *Lang* [14] foram de alguma forma utilizados.

No capítulo 3, serão determinadas condições necessárias e suficientes para que, numa dada extensão de corpos numéricos L / K, um inteiro algébrico de K, que não uma unidade, seja norma de um inteiro algébrico de L para o caso em que cada unidade fundamental de K seja norma de alguma unidade de L. Também serão estabelecidas condições suficientes para a divisibilidade do número de classes de corpos quadráticos imaginários $Q(\sqrt{n})$ por inteiros racionais dados quando n for expresso como $n = r^2 - 4m^t$, onde $m > 1$ e $t > 1$ ou como $n = r^2 - a^t$, onde a é ímpar, $r > 0$, $t > 1$ e $a > 1$. Estes resultados estendem os trabalhos de *Cowles* [4] e *Gross e Rohrlich* [8]. Demonstraremos ainda neste capítulo que, para os corpos quadráticos imaginários $Q(\sqrt{n})$, onde $n \not\equiv_8 5$ e $n \neq -1, -2, -7$, temos, necessariamente, que o número de classes é diferente de 1. Neste capítulo, voltamos a utilizar *Mollin*[17] e utilizamos também *Cowles* [4] e *Gross e Rohrlich* [8].

No Apêndice apresentamos definições e resultados, sem demonstrações, utilizados no decorrer do trabalho.

Nosso objetivo principal será, então, o de estabelecer condições suficientes para que o número de classes de certos corpos quadráticos seja não trivial; condições necessárias e suficientes para que um dado inteiro algébrico, que não uma unidade, seja norma de um inteiro algébrico, numa dada extensão de corpos numéricos e condições suficientes para a divisibilidade do número de classes de certos corpos quadráticos imaginários, além da determinação da unidade fundamental de determinados corpos quadráticos.

Muito embora os principais resultados obtidos sejam de Teoria Algébrica dos Números, alguns resultados da Teoria dos Números, mais especificamente de equações diofantinas, serão desenvolvidos devido a nossa proposta de trabalho.

Algumas tabelas ilustram os principais resultados estabelecidos.

CAPÍTULO 1

RESULTADOS PRELIMINARES

Neste capítulo, nosso objetivo será estabelecer dois resultados que serão essenciais para a demonstração do principal teorema do próximo capítulo. A importância desses resultados não nos permitiu tratá-los como simples lemas e assim eles serão os teoremas centrais deste capítulo. O primeiro deles nos dá uma fórmula explícita da ***unidade fundamental*** do corpo quadrático $Q(\sqrt{n})$ onde $n = m^2 + r$ com $-m < r \leq m$, $r \mid 4m$ e n livre de quadrados. O segundo nos garante que o anel de inteiros de $Q(\sqrt{n})$, onde $n = m^2 - 1$, não é um domínio principal.

1 - A unidade fundamental de $Q(\sqrt{m^2 + r})$

Conforme notação do ***Apêndice***, se $K = Q(\sqrt{n})$, denotaremos por $\mathbf{I}_K$ o anel dos inteiros algébricos de K, anel este que na realidade é um ***Domínio de Dedekind***. Estaremos interessados, particularmente, em conseguir uma expressão que nos dê a ***unidade fundamental*** de $Q(\sqrt{n})$, onde $n = m^2 + r$, com $r \mid 4m$, $-m < r \leq m$, é um inteiro livre de quadrados. Assim sendo, o nosso objetivo será mostrar que, para n nas condições acima a ***unidade fundamental*** de $Q(\sqrt{n})$ é

$$\xi = \frac{2m^2 + r}{|r|} + \frac{2m}{|r|}\sqrt{n}.$$

Note que, do fato de $-m < r \leq m$, já temos que $\xi > 1$. Vamos então garantir, inicialmente, que ξ é uma unidade:

Lema 1: *Se $n = m^2 + r$ é livre de quadrados com m e r inteiros não nulos tais que $m > 1$, $r \mid 4m$ e $-m < r \leq m$ então*

$$\xi = \frac{2m^2 + r}{|r|} + \frac{2m}{|r|}\sqrt{n}$$

é uma unidade para $\mathbf{Q}(\sqrt{n})$.

Demonstração: Observe, inicialmente que,

$$N(\xi) = \frac{4m^4 + 4m^2 r + r^2 - 4m^2(m^2 + r)}{r^2} = 1.$$

Assim, conforme ***proposição A2*** do Apêndice, basta mostrarmos que ξ é um inteiro algébrico. Dividiremos tal discussão nos casos $\boldsymbol{n \equiv_4 2, 3}$ e $\boldsymbol{n \equiv_4 1}$

(i) $n \equiv_4 2, 3$

Aqui $\mathbf{I}_K = \{ x + y\sqrt{n}, \text{ com } x, y \in \boldsymbol{Z} \}$.

Sejam $a = \frac{2m^2 + r}{|r|}$ e $b = \frac{2m}{|r|}$ e suponha que $a \notin \boldsymbol{Z}$.

Como $2a = \frac{4m^2 + 2r}{|r|} \in \boldsymbol{Z}$, temos que $2a$ é ímpar.

Mas $a^2 - nb^2 = 1$, assim segue que $4 = (2a)^2 - n(2b)^2$ e sendo $2a$ ímpar temos que $(2b)^2 n$ é ímpar, ou seja, $2b$ é ímpar.
Assim $(2a)^2 \equiv_4 (2b)^2 \equiv_4 1$, donde segue que $(2a)^2 - n(2b)^2 \equiv_4 (1-n)$.
Por outro lado, como $(2a)^2 - n(2b)^2 \equiv_4 0$, temos que $(n-1) \equiv_4 0$, ou seja $n \equiv_4 1$, um absurdo! Assim $a \in \boldsymbol{Z}$.
Suponha agora que $b \notin \boldsymbol{Z}$.

Como $r \mid 4m$, segue que $2b = \frac{4m}{|r|} \in \boldsymbol{Z}$ e como $b \notin \boldsymbol{Z}$ temos que $2b$ é ímpar.
Novamente, $4 = (2a)^2 - n(2b)^2$, logo $2a$ é também ímpar, pois do contrário $4 \mid n$ o que contraria o fato de n ser livre de quadrados.
Então temos que $(2a)^2 \equiv_4 (2b)^2 \equiv_4 1$ e $(2a)^2 - n(2b)^2 \equiv_4 0$, que já vimos ser uma contradição.
Assim $b \in \boldsymbol{Z}$, e em vista de $a \in \boldsymbol{Z}$, temos então que $\xi = a + b\sqrt{n}$ é uma unidade para $\boldsymbol{Q}(\sqrt{n})$.

(ii) $n \equiv_4 1$

Agora $\mathbf{I}_K = \{ \frac{x + y\sqrt{n}}{2}$, onde $x, y \in \boldsymbol{Z}$ e $x \equiv_2 y \}$.

Considere

$$\xi = \frac{4m^2 + 2r}{2|r|} + \frac{4m}{2|r|}\sqrt{n} = \frac{a + b\sqrt{n}}{2}.$$

Claramente, pelo fato de $r \mid 4m$, temos que $a, b \in \boldsymbol{Z}$. Mostraremos, então, que a e b têm a mesma paridade.

Suponha b par. Como $\boldsymbol{N(\xi) = 1}$, segue que $a^2 - nb^2 = 4$ donde, sendo b par, temos que a é par.

Por outro lado, suponha a par. Então como $4 \mid (a^2 - nb^2)$ temos que $4 \mid nb^2$. Observe que 4 não é divisor de n, uma vez que n é livre de quadrados, e sendo n ímpar temos que $4 \mid b^2$ donde b é par.

Assim, a e b têm a mesma paridade, e como $\boldsymbol{N(\xi) = 1}$ segue que ξ é uma unidade de $\boldsymbol{Q}(\sqrt{n})$. ■

Daqui para a frente, dividiremos, definitivamente, a discussão de que ξ é a unidade fundamental de $\boldsymbol{Q}(\sqrt{n})$ nos casos $\boldsymbol{n \equiv_4 1}$ e $\boldsymbol{n \equiv_4 2, 3}$.

1° caso: $n \equiv_4 2, 3$

Neste caso temos conhecido que o anel de inteiros de $\boldsymbol{Q}(\sqrt{n})$ é $\boldsymbol{Z} \oplus \boldsymbol{Z}\sqrt{n}$ e consequentemente as unidades $a + b\sqrt{n}$ satisfazem uma das ***equações de Pell***

$$\boldsymbol{A^2 - nB^2 = \pm 1}.$$

No que se segue, mostraremos inicialmente que ξ é a solução minimal (conforme definição abaixo) da ***equação de Pell positiva***, qual seja,

$$\boldsymbol{A^2 - nB^2 = 1}. \qquad \boldsymbol{(1)}$$

Em seguida mostraremos que para $n = m^2 + r$, dentro de nossas hipóteses, a ***equação de Pell negativa***,

$$\boldsymbol{A^2 - nB^2 = -1}, \qquad \boldsymbol{(2)}$$

não tem solução, o que garantirá que ξ é a ***unidade fundamental*** uma vez que $\boldsymbol{Q}(\sqrt{n})$ não terá unidades impróprias.

Vale observar que se n e t são números inteiros e se a e b são os menores valores inteiros tais que $a^2 - nb^2 = t$, com $a \geq 0$ e $b > 0$, dizemos então que o número $\alpha = a + b\sqrt{n}$ é a ***solução minimal*** (ou solução mínima, ou ainda solução fundamental) da equação diofantina $\boldsymbol{A^2 - nB^2 = t}$.

Comecemos então demonstrando o seguinte lema:

Lema 2: *Se* $n = m^2 + r$ *é livre de quadrado ,* $n \equiv_4 2, 3$, *com* m, r *inteiros não nulos tais que* $m > 1$, $r \mid 4m$, $-m < r \leq m$ *e* $r \neq -1$, *então*

$$\xi = \frac{2m^2 + r}{|r|} + \frac{2m}{|r|}\sqrt{n}$$

é a solução minimal da equação (1).

Demonstração: Pelo ***lema 1***, ξ é uma unidade, logo ξ é solução da ***equação (1)***. Para a minimidade, observe que

$$\frac{2m^2 + r}{|r|} = \frac{2(n - r) + r}{|r|} = \frac{2n - r}{|r|}.$$

Mas $|r| \geq 1$, assim temos que

$\frac{2n - r}{|r|} < 2n + 1$, se $|r| > 1$ ou

$\frac{2n - r}{|r|} = 2n - 1 < 2n + 1$, se $r = 1$.

Logo segue que

$$\frac{2m^2 + r}{|r|} < 2n + 1, \quad \forall r \neq -1 . \qquad (3)$$

Em vista desta avaliação, considere que $\xi_+ = a + b\sqrt{n}$ seja a *solução minimal* da ***equação (1)***

#***Afirmação:*** *Não existe solução da equação* $A^2 - nB^2 = 1$, *entre* ξ_+ *e* ξ_+^2.

Demonstração: Suponha que $x + y\sqrt{n}$ seja solução da ***equação (1)*** tal que

$$a + b\sqrt{n} < x + y\sqrt{n} < (a + b\sqrt{n})^2 .$$

Assim, segue que

$$(a + b\sqrt{n})(a - b\sqrt{n}) < (x + y\sqrt{n})(a - b\sqrt{n}) < (a - b\sqrt{n})(a + b\sqrt{n})^2.$$

Observe que $a - b\sqrt{n}$ é um número positivo, pois $(a + b\sqrt{n})(a - b\sqrt{n}) = 1$ e $a + b\sqrt{n} > 0$.

Como $a^2 - nb^2 = 1$ temos que:

$$1 < (ax - byn) + (ay - bx)\sqrt{n} < a + b\sqrt{n}. \qquad (4)$$

Seja $\alpha = (ax - byn) + (ay - bx)\sqrt{n}$ e observe que

$$\begin{aligned}(ax - byn)^2 - n(ay - bx)^2 &= a^2x^2 - 2axbyn + b^2y^2n^2 - n(a^2y^2 - 2axby + b^2x^2) \\ &= a^2(x^2 - ny^2) - nb^2(x^2 - ny^2) \\ &= (a^2 - nb^2)(x^2 - ny^2) = 1.\end{aligned}$$

Então α é solução da ***equação (1)***, o que é um absurdo, tendo em vista as desigualdades ***(4)*** e a minimidade de ξ_+.#

Agora, observe que em vista desta afirmação, a "segunda menor solução positiva" da ***equação 1*** é

$$\xi_+^2 = a^2 + nb^2 + 2ab\sqrt{n}.$$

Mas $a^2 + nb^2 = 2nb^2 + 1$ e como $a + b\sqrt{n}$ é solução mínima tem-se $b \geq 1$, logo segue que $a^2 + nb^2 \geq 2n + 1$.

Tendo em vista a ***avaliação (3)*** concluímos, então, que

$$a^2 + nb^2 > \frac{2m^2 + r}{|r|}.$$

Assim,

$$\left(\frac{2m^2+r}{|r|}\right)^2 - (2ab)^2 n < \left(a^2 + nb^2\right)^2 - (2ab)^2 n = 1 = \left(\frac{2m^2+r}{|r|}\right)^2 - \left(\frac{2m}{|r|}\right)^2 n,$$

donde concluimos que $2ab > \frac{2m}{|r|}$.

Então $\xi < \xi_+^2$ e em vista da afirmação anterior temos que $\xi = \xi_+$. ■

Observamos que no caso particular em que $r = -1$, caso este fora das hipóteses do ***lema 2***, a solução minimal da ***equação de Pell positiva*** é

$$\xi_+ = m + \sqrt{m^2 - 1}.$$

Demonstraremos, agora, que com as hipóteses do lema anterior, a ***equação de Pell negativa*** não tem solução:

Lema 3: *Se $n = m^2 + r$ é livre de quadrados , $n \equiv_4 2,3$, com m, n inteiros não nulos tais que $m > 1$, $r \mid 4m$, $-m < r \leq m$ e $|r| \neq 1$ então $\mathbf{Q}(\sqrt{n})$ não tem unidades impróprias.*

Demonstração: Suponha por absurdo, que a ***equação (2)***, $A^2 - nB^2 = -1$, tenha solução inteira. Seja , então, $\xi_- = a + b\sqrt{n}$ sua solução minimal. Continuaremos denotando por ξ_+ a solução minimal da ***equação de Pell positiva***.

#Afirmação: *Se $\xi_- = a + b\sqrt{n}$ é solução minimal para a equação (2) então $\xi_+ = \xi_-^2$.*

Demonstração: Suponha que $\xi_-^2 = (a^2 + n\,b^2) + 2a\,b\sqrt{n} > \xi_+$ (não podemos ter $\xi_+ > \xi_-^2$ devido a minimidade de ξ_+).

Pelo ***lema*** anterior, $\xi_+ = \xi$, assim,

$$1 < \frac{2m^2 + r}{|r|} + \frac{2m}{|r|}\sqrt{n} < (a^2 + nb^2) + 2ab\sqrt{n}.$$

Como $(-a + b\sqrt{n}) > 0$, pois

$$(-a + b\sqrt{n}).(a + b\sqrt{n}) = nb^2 - a^2 = 1,$$

temos que

$$-a + b\sqrt{n} < (-a + b\sqrt{n}).\left(\frac{2m^2 + r}{|r|} + \frac{2m}{|r|}\sqrt{n}\right) < (-a + b\sqrt{n}).(a + b\sqrt{n})^2.$$

Então

$$-a + b\sqrt{n} < \left(\frac{-2m^2a - ra}{|r|} + \frac{2mbn}{|r|}\right) + \left(\frac{-2ma}{|r|} + \frac{rb + 2bm^2}{|r|}\right)\sqrt{n} < a + b\sqrt{n}. \quad \textbf{(5)}$$

Mas,

$$\left(\frac{-2m^2a - ra + 2mbn}{|r|}\right)^2 - n\left(\frac{rb - 2ma + 2bm^2}{|r|}\right)^2 =$$

$$\frac{4m^2b^2n^2 + a^2(2m^2 + r)^2 - nb^2(2m^2 + r) - 4nm^2a^2}{r^2} =$$

$$\frac{(a^2 - b^2n)\left[(2m^2 + r)^2 - (2m)^2n\right]}{r^2} = (a^2 - nb^2).$$

Desta forma,

$$\left(\frac{-2m^2a - ra + 2mbn}{|r|}\right)^2 - n\left(\frac{rb - 2ma + 2bm^2}{|r|}\right)^2 = -1.$$

Como pelo ***lema 1*** temos que ξ é uma unidade, segue que $\frac{2m^2 + r}{|r|} \in \boldsymbol{Z}$ e $\frac{2m}{|r|} \in \mathbf{Z}$, uma vez que $n \equiv_4 2, 3$.

Assim podemos concluir que

$$\alpha = \frac{-2m^2a - ra + 2mbn}{|r|} + \left(\frac{rb - 2ma + 2bm^2}{|r|}\right)\sqrt{n}$$

é solução inteira da ***equação (2)***.

Se

$$x = \frac{-2m^2a - ra + 2mbn}{|r|} \quad e \quad y = \frac{rb - 2ma + 2bm^2}{|r|},$$

temos, pelas desigualdades *(5)* que

$$-a + b\sqrt{n} < \alpha = x + y\sqrt{n} < a + b\sqrt{n}. \quad \textbf{(5')}$$

Analisemos então, x *e* y :

(i) $x > 0$ e $y > 0$

Este caso não é possível pois do contrário teríamos que $1 < \alpha < a + b\sqrt{n}$, com α solução para a ***equação (2)***, o que contraria a minimidade de ξ_-.

(ii) $x < 0$ e $y < 0$

Estas desigualdades não podem ocorrer pois caso contrário teríamos que $\alpha < 0$ e como $(-a + b\sqrt{n}) > 0$ então teríamos que $\alpha < -a + b\sqrt{n}$, o que contraria as desigualdades ***(5')***.

(iii) $x > 0$ e $y < 0$

Este caso também não é possível, pois do contrário teríamos

$$2mbn > a(2m^2 + r) \qquad \text{e} \qquad b(2m^2 + r) < 2ma$$

e assim

$$4m^2bn > 2am(2m^2 + r) > b(2m^2 + r)^2,$$

donde concluiríamos que

$$b[(2m^2 + r)^2 - 4m^2n] < 0.$$

Como $b \geq 1$ segue que

$$(2m^2 + r)^2 - 4m^2n < 0,$$

o que é um absurdo, visto que $(2m^2 + r)^2 - 4m^2n = r^2$.

(iv) $x < 0$ *e* $y > 0$

Estas desigualdades também não são verdadeiras. De fato, suponha que as mesmas ocorram.

Como $\xi_- = a + b\sqrt{n} > 1$ e $(a + b\sqrt{n}).(a - b\sqrt{n}) = -1$, segue que

$$-a + b\sqrt{n} = -(a - b\sqrt{n}) = \frac{1}{a + b\sqrt{n}} = \frac{1}{\xi_-} < 1.$$

Como ξ_- é o menor número maior que 1 que satisfaz a ***equação (1)*** então $-a + b\sqrt{n} = \frac{1}{\xi_-}$ é o maior número menor que 1 dentre os números $\eta = \eta_1 + \eta_2\sqrt{n}$ que satisfazem a ***equação (2)***, com $\eta_1 < 0$ e $\eta_2 > 0$, η_1 *e* η_2 inteiros.

Assim, se $x < 0$ e $y > 0$, como $\alpha < 1$ (se $\alpha > 1$, como $\alpha < \xi_-$ teríamos uma contradição da minimidade de ξ_-) e α é solução da ***equação (2)*** então necessariamente $\alpha \leq a + b\sqrt{n}$, o que contraria as desigualdades ***(5')***.

(v) Os números x e y não podem ser nulos uma vez que $x^2 - ny^2 = -1$.

Assim da contradição dos itens acima segue a afirmação.#

Em vista da afirmação acima e do ***lema 2*** temos que

$$\xi_-^2 = (a^2 + b^2 n) + 2ab\sqrt{n} = \frac{2m^2 + r}{|r|} + \frac{2m}{|r|}\sqrt{n},$$

donde

$$a^2 + b^2 n = \frac{2m^2 + r}{|r|} = \frac{2(n-r) + r}{|r|} = \frac{2n - r}{|r|}.$$

Assim

$$a^2|r| + b^2|r|n = 2n - r,$$

ou ainda,

$$(2 - b^2|r|)n = (a^2 \pm 1)|r|.$$

Observe que $a^2 \neq 1$ pois do contrário, como $a^2 - b^2 n = -1$, teríamos necessariamente $n = 2$ e $b = 1$ e isso contraria nossas hipóteses uma vez que teríamos então $r = 1$.
Logo, como $a^2 \neq 1$, temos que $(a^2 \pm 1) > 0$, donde $(2 - b^2|r|) > 0$.
Com isso $2 > b^2|r|$ o que implica em $b^2|r| = 1$ e assim temos que $b^2 = 1$. Mas assim teremos que $n = a^2 + 1$ contrariando o fato de $r \neq 1$.
Portanto a ***equação (2)*** não tem solução donde $\boldsymbol{Q}(\sqrt{n})$ não tem unidades impróprias. ■

Concluiremos o caso $\boldsymbol{n \equiv_4 2,3}$ demonstrando, finalmente, o resultado a que nos propusemos :

Teorema 1: *Seja $n = m^2 + r$, livre de quadrados, $n \equiv_4 2,3$, com m , r inteiros não nulos tais que $m > 1$, $r \mid 4m$, $|r| \neq 1$ e $-m < r \leq m$. Então*

$$\xi = \frac{2m^2 + r}{|r|} + \frac{2m}{|r|}\sqrt{n}$$

é a unidade fundamental de $\boldsymbol{Q}(\sqrt{n})$.

Demonstração: Pelo ***lema 1***, ξ é uma unidade e pelo ***lema 2*** ξ é a solução minimal da equação $A^2 - n B^2 = 1$.
Como pelo ***lema 3*** $\mathbf{Q}(\sqrt{n})$ não tem unidades com norma negativa então a unidade fundamental será a menor unidade maior que um cuja norma é positiva. Assim segue que ξ é a unidade fundamental de $\mathbf{Q}(\sqrt{n})$. ■

Para finalizar este primeiro caso faremos uma observação sobre os valores de r fora das hipóteses do ***teorema 1***, a saber $r = 1$ e $r = -1$.

Se $r = 1$ temos que $n = m^2 + 1$ e nesse caso a unidade fundamental é

$$\mu = m + \sqrt{n} = m + \sqrt{m^2 + 1}$$

que é uma unidade imprópria e é, claramente, a solução minimal da ***equação de Pell negativa***.

Se $r = -1$ então $n = m^2 - 1$ e nesse caso, a unidade fundamental é

$$\alpha = m + \sqrt{n} = m + \sqrt{m^2 - 1},$$

uma vez que para $n = m^2 - 1$ o corpo $\mathbf{Q}(\sqrt{n})$ não tem unidades impróprias e que α é a solução minimal da ***equação de Pell positiva***.

Com efeito, se para $n = m^2 - 1$ o corpo $\mathbf{Q}(\sqrt{n})$ tivesse unidades impróprias então a unidade fundamental ζ seria uma unidade imprópria e nesse caso a solução minimal da equação de Pell positiva $\alpha = m + \sqrt{n}$ seria tal que $\alpha = \zeta^2$. Com isso, se $\zeta = a + b\sqrt{n}$, teríamos então que $(a^2 + b^2 n) + 2ab\sqrt{n} = m + \sqrt{n}$, o que não é possível uma vez que não existem $a, b \in \boldsymbol{Z}$ tais que $2ab = 1$.

2° caso: $n \equiv_4 1$

Agora o anel de inteiros algébricos, de $K = \mathbf{Q}(\sqrt{n})$ é

$$\mathbf{I}_K = \left\{ \frac{x + y\sqrt{n}}{2}, \text{ onde } x, y \in \boldsymbol{Z} \text{ e } x \equiv_2 y \right\},$$

e as unidades satisfazem uma das ***equações de Pell***:

$$\boldsymbol{A^2 - n B^2 = \pm 4}.$$

Observe que se $a + b\sqrt{n}$ é solução minimal da ***equação de Pell positiva***

$$\boldsymbol{A^2 - n B^2 = 4} \qquad \textbf{(6)}$$

então $\xi_+ = \dfrac{a + b\sqrt{n}}{2}$ é a menor unidade de $\mathbf{Q}(\sqrt{n})$ maior que 1 e de norma 1. A afirmação de que ξ_+ é unidade é evidente uma vez que $\mathbf{N}(\xi_+) = 1$ e que a e b têm a mesma paridade, pois já que como $a^2 - nb^2 = 4$ e $n \equiv_4 1$ então $a^2 - b^2 \equiv_4 0$.

Por outro lado, é a menor pois se $\alpha = \dfrac{x + y\sqrt{n}}{2}$ é uma unidade de norma 1 tal que $\alpha < \xi_+$, então $x + y\sqrt{n} < a + b\sqrt{n}$, o que contraria a minimidade de $a + b\sqrt{n}$, uma vez que $x + y\sqrt{n}$ é solução da ***equação (6)***.

Assim, como no caso anterior, mostraremos, inicialmente, que

$$\alpha = \frac{4m^2 + 2r}{|r|} + \frac{4m}{|r|}\sqrt{n}$$

é a solução minimal da ***equação (6)*** e com isso, pelas observações anteriores, teremos que

$$\xi_+ = \xi = \frac{1}{2}\left(\frac{4m^2+2r}{|r|} + \frac{4m}{|r|}\sqrt{n}\right)$$

é a menor unidade de $\mathbf{Q}(\sqrt{n})$ maior que 1 e de norma positiva.

Em seguida, mostraremos que a ***equação de Pell negativa***

$$\boldsymbol{A^2 - n\,B^2 = -4} \qquad (7)$$

não é solúvel, donde concluiremos que ξ_+ é a unidade fundamental procurada.

Iniciemos, então, demonstrando o seguinte lema:

Lema 4: *Se $n = m^2 + r$ é livre de quadrados, $n \equiv_4 1$, com $m, r \in Z^*$, $m > 1$, tais que $r \mid 4m$, $-m < r \leq m$ e $r \neq -4$, então*

$$\alpha = \frac{4m^2+2r}{|r|} + \frac{4m}{|r|}\sqrt{n}$$

é a solução minimal da equação $A^2 - nB^2 = 4$, exceto para $n = 5$, com $m = 2$ e $r = 1$.

Demonstração: Claramente α é solução.

Por outro lado,

$$\frac{4m^2+2r}{|r|} = \frac{4(n-r)+2r}{|r|} = \frac{4n-2r}{|r|}.$$

Como $|r| \geq 1$ segue que

$\frac{4n-2r}{|r|} \leq \frac{4n}{|r|} + 2 < 4n + 2$, se $|r| > 1$, ou

$\frac{4n-2r}{|r|} = 4n - 2 < 4n + 2$, se $r = 1$.

Assim

$$\frac{4m^2+2r}{|r|} < 4n + 2, \ \forall r. \qquad (8)$$

(observe que, como $n \equiv_4 1$, o caso $r = -1$ não ocorre)

Considere agora que $\beta = a + b\sqrt{n}$ é a solução minimal da ***equação (6)*** e seja $\xi_+ = \frac{a+b\sqrt{n}}{2}$ a unidade correspondente a essa solução.

#***Afirmação:*** *Não existe* $\gamma = \frac{x+y\sqrt{n}}{2}$, x , $y \in \boldsymbol{Z}$, *tal que* $\xi_+ < \gamma < \xi_+^2$ *com* $x + y\sqrt{n}$ *solução da equação (6).*

Demonstração: Suponha, por absurdo, que existe $\gamma = \frac{x+y\sqrt{n}}{2}$, tal que $\xi_+ < \gamma < \xi_+^2$, com $x^2 - ny^2 = 4$. Assim

$$\frac{a+b\sqrt{n}}{2} < \frac{x+y\sqrt{n}}{2} < \left(\frac{a+b\sqrt{n}}{2}\right)^2,$$

donde

$$a + b\sqrt{n} < x + y\sqrt{n} < \frac{\left(a+b\sqrt{n}\right)^2}{2}.$$

Como $a - b\sqrt{n} > 0$, pois $(a + b\sqrt{n}).(a - b\sqrt{n}) = 4$ e $a + b\sqrt{n} > 0$, segue que,

$$a^2 - nb^2 < (ax - byn) + (ay - bx)\sqrt{n} < (a^2 - nb^2)\frac{a+b\sqrt{n}}{2}$$

$$2 < \frac{(ax-byn)+(ay-bx)\sqrt{n}}{2} < a + b\sqrt{n}. \qquad \textbf{(9)}$$

Consideremos

$$\eta = \frac{(ax-byn)}{2} + \frac{(ay-bx)}{2}\sqrt{n}.$$

Assim, por ***(9)***,

$$1 < \eta < \beta. \qquad \textbf{(10)}$$

Observemos que

$$\left(\frac{ax-byn}{2}\right)^2 - n\left(\frac{ay-bx}{2}\right)^2 = \frac{a^2(x^2-ny^2) - nb^2(x^2-ny^2)}{4}$$

$$= \frac{(a^2-nb^2)(x^2-ny^2)}{4}$$

$$= \frac{a^2-nb^2}{4}(x^2-ny^2)$$

$$= 4.$$

Por outro lado, $a \equiv_2 b$, $x \equiv_2 y$ e $n \equiv_2 1$, donde segue que $byn \equiv_2 ax$ e $ay \equiv_2 bx$ e assim,

$$\frac{ay-bx}{2} \in \boldsymbol{Z} \quad \text{e} \quad \frac{ax-byn}{2} \in \boldsymbol{Z}.$$

Logo η é uma solução para a ***equação (6)***, o que é um absurdo em vista das desigualdades ***(10)*** e da minimidade de β.#

Deixemos de lado, por um momento, esta afirmação e observemos que

$$\frac{a^2+nb^2}{2} = \frac{(nb^2+4)+nb^2}{2} = nb^2 + 2.$$

Mas se $b = 1$, então $n = a^2 - 4$, donde $r = -4$, o que não é possível dentro das nossas hipóteses, logo $b \geq 2$ e assim, usando a igualdade acima, teremos a seguinte avaliação:

$$\frac{a^2 + nb^2}{2} \geq 4n + 2.$$

Tendo em vista a avaliação ***(8)***, concluimos, então, que

$$\frac{a^2 + nb^2}{2} > \frac{4m^2 + 2r}{|r|},$$

donde

$$\left(\frac{4m^2 + 2r}{|r|}\right)^2 - (ab)^2 n < \left(\frac{a^2 + nb^2}{2}\right)^2 - a^2b^2n = 4 = \left(\frac{4m^2 + 2r}{|r|}\right)^2 - \left(\frac{4m}{r}\right)^2.$$

Assim temos que $ab > \frac{4m}{r}$.

Então segue que

$$\frac{1}{2}\left(\frac{4m^2 + 2r}{|r|} + \frac{4m}{|r|}\sqrt{n}\right) < \frac{1}{2}\left(\frac{a^2 + nb^2}{2} + ab\sqrt{n}\right) = \xi_+^2.$$

Logo, pela afirmação acima, como α é uma solução da ***equação (6)*** e $\frac{\alpha}{2} < \xi_+^2$, temos que

$$\xi_+ = \frac{1}{2}\left(\frac{4m^2 + 2r}{|r|} + \frac{4m}{|r|}\sqrt{n}\right)$$

e daí segue o lema, uma vez que

$$a + b\sqrt{n} = \frac{4m^2 + 2r}{|r|} + \frac{4m}{|r|}\sqrt{n}. \blacksquare$$

Por este resultado temos conhecida a menor unidade maior que 1 cuja norma é positiva qual seja:

$$\xi_+ = \frac{1}{2}\left(\frac{4m^2 + 2r}{|r|} + \frac{4m}{|r|}\sqrt{n}\right).$$

Demonstraremos a seguir que ***a equação (7)*** não tem solução, mas antes, observemos que para $r = -4$, caso fora das hipóteses do lema anterior, segue trivialmente que a solução minimal para a ***equação (6)*** é

$$\alpha = m + \sqrt{m^2 - 4}$$

e, consequentemente, a menor unidade maior que 1 cuja norma é positiva é

$$\lambda = \frac{m + \sqrt{m^2 - 4}}{2}.$$

Lema 5: *Seja $n = m^2 + r$ um inteiro livre de quadrados, $n \equiv_4 1$, com $m, r \in \mathbf{Z}^*$, $m > 1$, tais que $r \mid 4m$, $-m < r \leq m$, $|r| \neq 1$ e $|r| \neq 4$. Então $\mathbf{Q}(\sqrt{n})$ não tem unidades impróprias.*

Demonstração: Suponha, por absurdo, que a equação $A^2 - nB^2 = -4$, tenha solução inteira e seja $\beta_- = a + b\sqrt{n}$ sua solução minimal. Então,

$$\xi_- = \frac{a + b\sqrt{n}}{2}$$

é a menor unidade maior que 1 cuja norma é negativa .

#***Afirmação:*** *Se $\beta_- = a + b\sqrt{n}$ é solução minimal para $A^2 - nB^2 = -4$ então $\xi_+ = \xi_-^2$.*

Demonstração:De fato, suponha que $1 < \xi_+ < \xi_-^2$.

Assim, como $(-a + b\sqrt{n}) > 0$ temos que

$$-a + b\sqrt{n} < (-a + b\sqrt{n}).\xi_+ < (-a + b\sqrt{n})\frac{\left(a + b\sqrt{n}\right)^2}{4}.$$

Então, se

$$\gamma = (-a + b\sqrt{n}).\ \xi_+ = \frac{2mnb - 2m^2a - ar}{|r|} + \frac{2bm^2 + rb - 2am}{2|r|}\sqrt{n},$$

segue que

$$-a + b\sqrt{n} < \gamma < \frac{b^2n - a^2}{4}(a + b\sqrt{n}),$$

logo

$$-a + b\sqrt{n} < \gamma < (a + b\sqrt{n})\ . \qquad \textbf{(11)}$$

Observe que $N(\gamma) = N(-a + b\sqrt{n}).N(\xi_+) = -4$.

Observe também que

$$\frac{4m^2 + 2r}{|r|} \in \mathbf{Z}, \quad \frac{4m}{|r|} \in \mathbf{Z}, \quad \frac{4m^2 + 2r}{|r|} \equiv_2 \frac{4m}{|r|}, \quad a \equiv_2 b \quad \text{e} \quad n \equiv_2 1,$$

logo, segue que

$$a\left(\frac{4m^2 + 2r}{|r|}\right) \equiv_2 bn\frac{4m}{|r|} \quad \text{e} \quad b\left(\frac{4m^2 + 2r}{|r|}\right) \equiv_2 a\frac{4m}{|r|}\ .$$

Como

$$\gamma = \frac{4mnb - 4m^2a - 2ar}{2|r|} + \frac{4bm^2 + 2rb - 4am}{2|r|}\sqrt{n},$$

então γ é solução inteira da ***equação (7).***

Se

$$x = \frac{2mnb - 2m^2a - ar}{|r|} \quad \text{e} \quad y = \frac{2bm^2 + rb - 2am}{|r|},$$

teremos que

$$-a + b\sqrt{n} < \gamma = x + y\sqrt{n} < (a + b\sqrt{n}),$$

com γ solução da equação $A^2 - n\,B^2 = -4$.

A mesma análise dos sinais de x e y feita no ***lema 3*** nos mostra que aqui também teremos um absurdo, logo segue a afirmação.#

Em vista desta afirmação e do lema anterior temos que

$$\frac{4m^2 + 2r}{|r|} = \frac{a^2 + b^2n}{2},$$

uma vez que $\xi_-^2 = \frac{1}{2}\left(\frac{a^2 + nb^2}{2} + ab\sqrt{n}\right)$.

Mas $n = m^2 + r$, assim

$$\frac{a^2 + b^2n}{2} = \frac{4n - 2r}{|r|}.$$

Logo,

$$a^2|r| + b^2|r|n = 8n - 4r,$$

donde segue que

$$(8 - b^2|r|)n = (a^2 \pm 4)|r|.$$

Observe que $a^2 \pm 4 > 0$, pois do contrário teríamos, necessariamente, que $a = 1$ ou $a = 2$ e isso implicaria em $n = 5$ ou $n = 2$ ou $n = 8$, casos fora de nossas hipóteses uma vez que $n \neq 5$ e $n \equiv_4 1$. Assim $a^2 \pm 4 > 0$ e com isso $8 - b^2|r| > 0$, donde $b^2|r| < 8$.

Desta forma, teremos que $b = 1$ ou $b = 2$.

(i) Se $b = 1$, segue que $n = a^2 + 4$.

Observe que $a > 4$ pois $a = 1$ ou $a = 2$ não é possível pela discussão acima; $a = 3$ implicaria em $n = 13 = 4^2 - 3$, donde $r = -3$ e $m = 4$, o que contraria a hipótese de que $r \mid 4m$ e finalmente $a = 4$ implica em $n = 20$ o que contraria a nossa hipótese de $n \equiv_4 1$.

Assim, temos $n = a^2 + 4$, com $a > 4$, donde $r = 4$ e isso contraria a nossa hipótese de que $|r| \neq 4$.

(ii) Se $b = 2$ então $|r| < 2$, donde $|r| = 1$, absurdo novamente uma vez que $|r| \neq 1$. Assim a equação $A^2 - n B^2 = -4$ não tem solução inteira e consequentemente $\boldsymbol{Q}(\sqrt{n})$ não tem unidades impróprias. ■

Temos então, para o caso em que $n \equiv_4 1$, um resultado análogo ao ***teorema 1***, qual seja:

Teorema 2: *Seja $n = m^2 + r$, livre de quadrados, $n \equiv_4 1$, com m , r inteiros não nulos tais que $m > 1$, $r \mid 4m$, $|r| \neq 1$, $|r| \neq 4$ e $-m < r \leq m$. Então*

$$\xi = \frac{1}{2}\left(\frac{4m^2 + 2r}{|r|} + \frac{4m}{|r|}\sqrt{n}\right)$$

é a unidade fundamental de $\boldsymbol{Q}(\sqrt{n})$.

Demonstração: A afirmação segue diretamente dos ***lemas 1, 4 e 5***.
O ***lema 1*** nos garante que ξ é uma unidade.
O ***lema 4*** mostra que

$$\frac{4m^2 + 2r}{|r|} + \frac{4m}{|r|}\sqrt{n}$$

é a solução minimal da equação $A^2 - n B^2 = 4$ e assim

$$\xi = \frac{1}{2}\left(\frac{4m^2 + 2r}{|r|} + \frac{4m}{|r|}\sqrt{n}\right)$$

é a menor unidade maior que 1 e cuja norma é positiva.
Como pelo ***lema 5*** $\boldsymbol{Q}(\sqrt{n})$ não tem unidades impróprias então ξ é de fato a unidade fundamental de $\boldsymbol{Q}(\sqrt{n})$. ■

Finalizamos esta seção analisando os casos $r = \pm 4$, fora das hipóteses do ***teorema 2***. Se tivermos $r = 4$ então a unidade fundamental será

$$\gamma = \frac{m + \sqrt{m^2 + 4}}{2},$$

que é uma unidade imprópria ,e

$$\beta = m + \sqrt{m^2 + 4}$$

é, claramente, a solução minimal da ***equação (7)***.

No caso de $r = -4$ a unidade fundamental é a unidade imprópria

$$\lambda = \frac{m + \sqrt{m^2 - 4}}{2},$$

pois $\alpha = m + \sqrt{m^2 - 4}$ é a solução minimal da ***equação (6)*** e $Q(\sqrt{m^2 - 4})$ não tem unidades impróprias. De fato, suponha que $Q(\sqrt{m^2 - 4})$ tivesse unidades impróprias. Então a unidade fundamental ζ seria uma unidade imprópria e nesse caso, $\lambda = \zeta^2$. Então, se

$$\zeta = \frac{a + b\sqrt{m^2 - 4}}{2},$$

teríamos que $ab = 1$, uma vez que

$$\zeta^2 = \frac{1}{2}\left(\frac{a^2 + nb^2}{2} + ab\sqrt{n}\right).$$

Assim, $a = b = 1$ e como $a^2 - nb^2 = -4$ concluiríamos que $n = 5$ o que não é possível visto que $5 = 2^2 + 1$ o que contraria o fato de $r = -4$.

Finalmente, se $n = 5$ sabemos que $\frac{1 + \sqrt{5}}{2}$ é a unidade fundamental de $Q(\sqrt{n})$.

2 - O anel de inteiros de $Q(\sqrt{m^2 - 1})$

Ao longo desta seção trabalharemos com o corpo quadrático real $K = Q(\sqrt{n})$, onde $n = m^2 - 1$. Tal corpo é um caso particular dos corpos quadráticos reais $Q(\sqrt{m^2 + r})$, tratados na seção anterior.

Observamos, mais uma vez, que nosso objetivo agora será mostrar que o anel $\mathbf{I}_K$ dos inteiros algébricos do corpo K não é um ***domínio principal***. Para tanto mostraremos que o ***grupo de classes de ideais*** de $\mathbf{I}_K$, que denotaremos por $\mathscr{C}\ell_K$, não é o trivial, uma vez que a condição necessária e suficiente para garantir que um ***domínio de Dedekind*** seja um ***domínio principal*** é que seu ***grupo de classes de ideais*** se reduza ao elemento neutro. Assim, mostraremos que a ordem de $\mathscr{C}\ell_K$, que sabemos ser finita e que usualmente é definida como ***número de classes*** de $\mathbf{I}_K$ (ou ***número de classes do corpo K)*** e denotada por h_K, é maior que 1.

Nesta seção usaremos outros conceitos e resultados mais específicos da ***teoria algébrica de números*** aplicada a ***corpos quadráticos***.

Particularmente, faremos uso da ***fatoração de ideais*** do tipo $p.\mathbf{I}_K$ ***em ideais primos*** de $\mathbf{I}_K$, onde p é um inteiro primo.
Dentro deste contexto usaremos, também, o conceito de ***discriminante absoluto*** do corpo K que denotaremos por d_K.

O teorema que se segue é o único desta seção e é o resultado que nos propusemos demonstrar.
Conforme dissemos na ***Introdução***, a demonstração desse resultado usa argumentos elementares bem apropriados à linguagem deste texto.

Teorema 3: *Seja $n = m^2 - 1$ um inteiro positivo livre de quadrados com m inteiro tal que $|m| > 2$. Então $K = \mathbf{Q}(\sqrt{n})$ é tal que $h_K > 1$.*

Demonstração: Observe, inicialmente, que sendo n livre de quadrados temos que m é par, pois do contrário $4 \mid n$, o que contraria o fato de n ser livre de quadrados.
Agora, sendo m par temos que $n = m^2 - 1 \equiv_4 -1$, isto é $n \equiv_4 3$.
Observamos também que, claramente, n não é primo, pois $|m| > 2$ (na realidade podemos supor sem perda de generalidade que $m > 2$, uma vez que $n = m^2 - 1$).
Por outro lado, a decomposição de n como produto de fatores primos (positivos) não é da forma $p_1 \cdot p_2 \cdot \ldots \cdot p_r$, onde cada primo p_i é tal que $p_i \equiv_4 1$, pois do contrário n seria da forma $4k + 1$, para algum $k \in Z$, o que contraria o fato de $n \equiv_4 3$. Assim, existe, necessariamente, um primo q tal que $q \mid n$ e $q \equiv_4 3$.
Mais que isso, temos na realidade um número ímpar de fatores primos da forma $4k + 3$, pois do contrário teríamos novamente $n \equiv_4 1$.
Em vista da discussão acima, concluimos que $n \equiv_4 3$ e sua decomposição em fatores primos (positivos) pode assumir uma dentre as duas formas:
$n = p_1 p_2 \cdot \ldots \cdot p_{2s+1}$ onde $s \in Z$, $s > 0$ e $p_i \equiv_4 3$, $i = 1,2,\ldots,2s + 1$ ou

$n = p_1 p_2 \cdot \ldots \cdot p_{2s+1} q_1 q_2 \cdot \ldots \cdot q_r$, onde r , $s \in Z$, $s \geq 0$, $r > 0$, com $p_i \equiv_4 3$, $i = 1,2,\ldots,2s + 1$ e $q_j \equiv_4 1$, $j = 1,2,\ldots,r$.
Feitas as considerações acima, suponhamos, por absurdo, que $h_K = 1$.
#***Afirmação 1:*** *Se p é um número primo tal que $p \mid n$ e $p \equiv_4 3$ então a equação*

$$A^2 - nB^2 = -p$$

tem solução.
Demonstração: Observe que se p é um primo tal que $p \mid n$ então $p \mid d_K$, uma vez que $n \equiv_4 3$ o que implica que $d_K = 4n$.
Desta forma temos que o ideal primo $p.\mathbf{I}_K$ de $\mathbf{I}_K$ é ramificado em K.
Assim $p.\mathbf{I}_K = \mathcal{P}^2$, onde $\mathcal{P}$ é o único ideal primo de $\mathbf{I}_K$ tal que $N(\mathcal{P}) = p$.

Como $\mathbf{I}_K$ é domínio principal então, particularmente, $\mathcal{P}$ é um ideal principal, assim existe $a + b\sqrt{n} \in \mathbf{I}_K$ tal que $\mathcal{P} = (a + b\sqrt{n}).\mathbf{I}_K$, donde $\exists\, a, b \in \mathbf{Z}$ tais que $a^2 - nb^2 = \pm p$.

Desta forma, uma das equações $A^2 - nB^2 = \pm p$ tem solução.

Suponhamos agora que $\exists\, c, d \in \mathbf{Z}$ tais que $c^2 - nd^2 = p$.

Como $n \equiv_4 3$ segue que $c^2 - 3d^2 \equiv_4 3$, ou ainda $c^2 + d^2 \equiv_4 3$, o que é impossível visto que $x^2 + y^2 \equiv_4 0, 1$ ou 2, $\forall\, x, y \in \mathbf{Z}$. Como, necessariamente, uma das equações $A^2 - nB^2 = \pm p$ tem solução segue o resultado.#

Na realidade demonstramos mais do que o enunciado na ***afirmação 1*** , ou seja, demonstramos que com as hipótese exigidas, "*das equações* $A^2 - nB^2 = \pm p$, *apenas a negativa tem solução*".

Usaremos a ***afirmação 1*** para garantir que n não pode ter dois fatores primos da forma $4k + 3$, o que nos garantirá que, na realidade, só poderá existir uma forma de decompormos n como produto de fatores primos positivos, a menos da ordem.

#***Afirmação 2:*** *O número n possui apenas um fator primo da forma* $4k + 3$.

Demonstração: A existência de um fator primo da forma $4k + 3$ é garantida pelas observações feitas no início da demonstração do teorema.

Para a unicidade, suponhamos que $\exists\, p$ e q, primos da forma $4k + 3$ tais que $p \mid n$ e $q \mid n$. O fato de n ser livre de quadrados nos garante que $p \neq q$.

Então pela ***afirmação 1*** temos que $\exists\, a, b, c, d \in \mathbf{Z}$ tais que $a^2 - nb^2 = -p$ e $c^2 - nd^2 = -q$.

Então, se $\left(\frac{-}{-}\right)$ denota o ***símbolo de Legendre***, teremos que

$$\left(\frac{-q}{p}\right) = \left(\frac{-p}{q}\right) = 1, \qquad \textbf{(12)}$$

uma vez que $a^2 \equiv_q -p$ e $c^2 \equiv_p -q$.

Por outro lado temos que

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

Como $p = 4k + 3$ e $q = 4t + 3$, para algum $k, t \in \mathbf{Z}$, temos que

$$\left(\frac{-q}{p}\right).\left(\frac{-p}{q}\right) = (-1)^{2k+1}.(-1)^{2t+1}.\left(\frac{q}{p}\right).\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right).\left(\frac{p}{q}\right).$$

Pela lei da ***reciprocidade quadrática*** segue que:

$$\left(\frac{q}{p}\right).\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} = (-1)^{(2k+1).(2t+1)} = -1,$$

assim concluimos que

$$\left(\frac{-q}{p}\right).\left(\frac{-p}{q}\right) = -1,$$

o que contradiz as igualdades ***(12)***.

Assim o número n tem apenas um fator primo da forma $4k + 3$.#

Com esta afirmação, e sabendo-se que n não é um número primo, podemos então garantir que existe uma única decomposição de n como produto de fatores primos positivos, a menos da ordem, qual seja

$\boldsymbol{n = q \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_r}$ com $q \equiv_4 3$ e $p_j \equiv_4 1$, $j = 1,2,\ldots,r$.

É essa a forma de n que assumiremos de agora em diante.

Por outro lado, sabemos que os números da forma $4k + 1$ podem ser da forma $8k + 1$ ou da forma $8k + 5$. Vamos agora determinar de que forma são os primos p_j , $j = 1,2,\ldots,r$. Para tanto, iniciamos demonstrando a afirmação seguinte , que como a ***afirmação 1*** , está relacionada com a resolução de equações diofantinas.

#***Afirmação 3:*** *Uma, e somente uma, das equações* $A^2 - nB^2 = \pm 2$ *tem solução*

Demonstração: Observe que sendo $\boldsymbol{d_K} = 4n$ então $2 \mid \boldsymbol{d_K}$, e assim segue que o ideal $\boldsymbol{2.I_K}$ de $\mathbf{I_K}$ também é ramificado em $\boldsymbol{K}$. Logo $\boldsymbol{2.I_K} = \mathcal{D}^2$, onde $\mathcal{D}$ é o único ideal primo de $\mathbf{I_K}$ tal que $N(\mathcal{D}) = 2$.

Assumindo a hipótese de que $\boldsymbol{h_K} = 1$, tem-se que o ideal $\mathcal{D}$ é um ideal principal, logo existe $c + d\sqrt{n} \in \mathbf{I_K}$ tal que $\mathcal{D} = (c + d\sqrt{n}).\mathbf{I_K}$, donde $\exists\, c , d \in \boldsymbol{Z}$ tais que $c^2 - nd^2 = \pm 2$ e assim temos assegurada a existência de solução para uma das equações dadas. Para a unicidade, suponha que ambas equações têm solução. Assim $\exists\, a , b , c , d \in \boldsymbol{Z}$ tais que $a^2 - nb^2 = 2$ e $c^2 - nd^2 = -2$

Então temos que $a^2 \equiv_q 2$ e $c^2 \equiv_q -2$, onde q é o fator primo de n da forma $4k + 3$. Logo, segue que

$$\left(\frac{2}{q}\right) = \left(\frac{-2}{q}\right) = 1. \qquad \textbf{(13)}$$

Mas

$$\left(\frac{2}{q}\right).\left(\frac{-2}{q}\right) = \left(\frac{2}{q}\right)^2.\left(\frac{-1}{q}\right) = \left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$$

e como $q = 4k + 3$, para algum $k \in \mathbf{Z}$, temos que

$$\left(\frac{2}{q}\right).\left(\frac{-2}{q}\right) = (-1)^{2k+1}$$

Com isso ,

$$\left(\frac{2}{q}\right)\cdot\left(\frac{-2}{q}\right) = -1,$$

o que contraria ***(13)***.

Logo segue a unicidade.#

Agora estamos aptos a verificar de que forma são os fatores primos de n do tipo $4k + 1$ e isso será feito na próxima afirmação:

#***Afirmação 4:*** *Os fatores primos de n da forma $4k + 1$ são necessariamente da forma $8t + 1$.*

Demonstração: Suponha que exista um fator primo p de n da forma $4k + 1$ tal que $p = 8t + 5$, para algum $t \in \boldsymbol{Z}$. Então,

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{8t^2+10t+3} = -1.$$

Por outro lado temos que

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2}}\cdot\left(\frac{2}{p}\right) = \left(\frac{2}{p}\right),$$

logo

$$\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right) = -1$$

e assim não existem a , $b \in \boldsymbol{Z}$ tais que $a^2 \equiv_p 2$ e $b^2 \equiv_p -2$, donde as equações $A^2 - nB^2 = 2$ e $A^2 - nB^2 = -2$ não têm solução, o que contraria ***afirmação 3***.

Assim, todos os fatores primos de n da forma $4k + 1$ são também da forma $8t + 1$.#

Temos agora, uma caracterização mais precisa da decomposição de n como produto de fatores primos, qual seja,

$$\boldsymbol{n = q\cdot p_1 p_2 \cdots p_r}, \text{ com } q \equiv_4 3 \text{ e } p_j \equiv_8 1,\ j = 1,2,\ldots,r.$$

Vejamos, agora, a forma do fator primo q em termos de congruência módulo 8, já que sendo q da forma $4k + 3$ q poderá ser da forma $8t + 3$ ou $8t + 7$. Veremos na afirmação abaixo que essa forma depende exclusivamente de qual das equações $A^2 - nB^2 = \pm 2$ tem solução.

#***Afirmação 5:*** *O fator primo de n da forma $4k + 3$ será da forma $8t + 3$ se e somente se a equação $A^2 - nB^2 = -2$ tiver solução.*

Demonstração: Seja q um fator primo de n da forma $8t + 3$.

Sabemos que $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$.

Como $q = 8t + 3$, para algum $t \in \boldsymbol{Z}$, segue que

$$\left(\frac{2}{q}\right) = (-1)^{8t^2+6t+1} = -1.$$

Assim, não existe $a \in \boldsymbol{Z}$ tal que $a^2 \equiv_q 2$ e consequentemente a equação $A^2 - nB^2 = 2$ não tem solução.

Como pela ***afirmação 3*** necessariamente uma das equações $A^2 - nB^2 = \pm 2$ tem solução temos que $A^2 - nB^2 = -2$ tem solução.

Reciprocamente, suponha que $q = 8t + 7$, para algum $t \in \boldsymbol{Z}$

É conhecido que

$$\left(\frac{-2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right) = (-1)^{\frac{q-1}{2}}.(-1)^{\frac{q^2-1}{8}} = (-1)^{4t+3}.(-1)^{8t^2+14t+6},$$

logo $\left(\frac{-2}{q}\right) = -1$, donde a equação $A^2 - nB^2 = -2$ não tem solução.#

Com esta afirmação, temos que o fator primo q de n da forma $4k + 3$ será da forma $8t + 3$ se a equação $A^2 - nB^2 = -2$ tiver solução e será da forma $8t + 7$ se a equação $A^2 - nB^2 = 2$ tiver solução.

A afirmação seguinte é o analogo da ***afirmação 1*** para os fatores primos de n da forma $4k + 1$ e, portanto, também está relacionada com resolução de equações diofantinas:

#***Afirmação 6:*** *Se p é um número primo tal que* $p \mid n$ *e* $p \equiv_4 1$ *então a equação*

$$A^2 - nB^2 = p$$

tem solução.

Demonstração: Como $p \mid n$ então $p \mid \boldsymbol{d}_{\mathbf{K}}$, logo o ideal $\boldsymbol{p}.\mathbf{I}_{\mathbf{K}}$ de $\mathbf{I}_{\mathbf{K}}$ se ramifica em $\boldsymbol{K}$. Assim $\boldsymbol{p}.\mathbf{I}_{\mathbf{K}} = \mathscr{R}^2$, onde $\mathscr{R}$ é o único ideal primo de $\mathbf{I}_{\mathbf{K}}$ tal que $N(\mathscr{R}) = p$.

No entanto, estamos supondo que $\mathbf{I}_{\mathbf{K}}$ é um domínio principal, portanto, $\mathscr{R}$ é um ideal principal. Assim, existe $a + b\sqrt{n} \in \mathbf{I}_{\mathbf{K}}$ tal que $(a + b\sqrt{n}).\mathbf{I}_{\mathbf{K}} = \mathscr{R}$, ou de outra forma , $\exists\, a$, $b \in \boldsymbol{Z}$ tais que $a^2 - nb^2 = \pm p$.

Assim, temos assegurada a existência de solução para uma das equações $A^2 - nB^2 = \pm p$. Mostraremos agora que é a equação positiva que tem solução.

Suponhamos, então, que $\exists\, c$, $d \in \boldsymbol{Z}$ tais que $c^2 - nd^2 = -p$.

Logo, $c^2 \equiv_q -p$, onde q é o fator primo de n que tem a forma $4k + 3$ e então

$$\left(\frac{-p}{q}\right) = 1. \qquad \textbf{(14)}$$

Por outro lado, como $q \mid n$ e $q \equiv_4 3$, *pela* ***afirmação 1,*** existem t , $s \in \boldsymbol{Z}$ tais que $t^2 - ns^2 = -q$, donde $t^2 \equiv_p -q$ e assim

$$\left(\frac{-q}{p}\right) = 1 \qquad \textbf{(15)}$$

Mas

$$\left(\frac{-p}{q}\right).\left(\frac{-q}{p}\right) = (-1)^{\frac{q-1}{2}}.\left(\frac{p}{q}\right).(-1)^{\frac{p-1}{2}}.\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).\left(\frac{q}{p}\right),$$

e usando novamente a ***lei da reciprocidade quadrática*** concluimos que

$$\left(\frac{-p}{q}\right).\left(\frac{-q}{p}\right) = -(-1)^{\frac{(p-1)(q-1)}{4}} = -1,$$

o que contradiz as igualdades ***(14)*** e ***(15)***.

Assim, como a equação negativa não tem solução, segue então a afirmação.#

Observe que, como na ***afirmação 1,*** demonstramos algo mais forte do que enunciamos. Na realidade mostramos que a equação positiva $A^2 - nB^2 = p$ é a única dentre as equações $A^2 - nB^2 = \pm p$ que possui solução.

Note que até agora, no decorrer desta demonstração, só usamos o fato de que $n \equiv_4 3$ e que $\boldsymbol{h}_K = 1$. A partir de agora, usaremos fortemente a hipótese de que $n = m^2 - 1$ e dividiremos o restante da demonstração nos casos $\boldsymbol{q \equiv_8 3}$ e $\boldsymbol{q \equiv_8 7}$. Antes observe que pelo fato de q dividir n e $n = (m + 1).(m - 1)$ temos que $q \mid (m + 1)$ ou $q \mid (m - 1)$ e apenas um desses casos, pois n é livre de quadrados (Estaremos sempre considerando $q > 0$).

1º caso: $\boldsymbol{q \equiv_8 3}$.

Se $q \mid (m - 1)$ então $m - 1 = 8k + 3$, para algum $k \in \boldsymbol{Z}$, donde $m + 1 = 8k + 5$, para algum $k \in \boldsymbol{Z}$. Mas isso é um absurdo visto que sendo q o único fator primo de n da forma $4k + 3$ então $m + 1$ é da forma $8k + 1$ (lembre-se que n é livre de quadrados).

Logo temos que $q \mid (m+1)$ e assim existe um inteiro primo p tal que $p \mid (m-1)$ e $p \equiv_4 1$, $p > 0$, uma vez que $m - 1 \geq 3$.

Pela ***afirmação 6***, temos que a equação $A^2 - nB^2 = p$ tem solução. Dentre as soluções $x + y\sqrt{n}$ da equação $A^2 - nB^2 = p$, seja então $a + b\sqrt{n}$ aquela solução tal que $a \geq 0$ e b é o menor inteiro positivo dentre os y possíveis.

Assim, $p = a^2 - nb^2$.

Por outro lado, $\boldsymbol{N}(m + \sqrt{n}) = \boldsymbol{N}(m + \sqrt{m^2 - 1}) = 1$ e como $\boldsymbol{N}(a - b\sqrt{n}) = p$, segue que

$$p = \boldsymbol{N}((a - b\sqrt{n}).(m + \sqrt{n})) = \boldsymbol{N}(am - bn + (a - bm)\sqrt{n}),$$

donde

$$(am - bn)^2 - n(a - bm)^2 = p$$

Assim, vemos que $\alpha = |am - bn| + |a - bm|\sqrt{n}$ é uma dentre as soluções $x + y\sqrt{n}$ da equação $A^2 - nB^2 = p$ tais que $x \geq 0$ e $y > 0$.
Assim, pela escolha de a e b temos que $|a - bm| \geq b$, o que acarreta em

$$a - bm \geq b \quad \text{ou} \quad a - bm \leq -b.$$

Por um lado, se $a - bm \geq b$ temos que $a \geq b(1 + m)$, donde segue que

$$p = a^2 - nb^2 \geq b^2(1 + m)^2 - nb^2 = b^2(1 + m)^2 - b^2(m^2 - 1)$$

$$= 2b + 2mb^2 \geq 2b + 2mb.$$

Logo,

$$p \geq 2b(1 + m) \geq 2(1 + m),$$

uma vez que $b \geq 1$, e assim segue que

$$p \geq 2(1 + m) > m - 1,$$

o que é um absurdo visto que $p \mid (m - 1)$.
Por outro lado, se $a - bm \leq -b$, temos que $a \leq b(m - 1)$ e assim

$$p = a^2 - nb^2 \leq b^2(m - 1)^2 - nb^2 = b^2(m - 1)^2 - b^2(m^2 - 1) = -2mb^2 + 2b^2.$$

Portanto,

$$p \leq -2b^2(m - 1) < 0,$$

o que contraria a escolha de p.
Logo este caso não pode ocorrer.

2º caso: $q \equiv_8 7$.

Se $q \mid (m+1)$ então $m + 1 = 8k + 7$, para algum $k \in \boldsymbol{Z}$, donde $m - 1 = 8k + 5$, o que contraria a ***afirmação 4***, pois sendo q o único fator primo de n da forma $4k + 3$, segue que $m - 1$ seria da forma $8k + 1$.
Assim, $q \mid (m - 1)$.
Pela ***afirmação 1***, temos então que a equação $A^2 - nB^2 = -q$ tem solução. Portanto seja $a + b\sqrt{n}$ a solução dessa equação tal que $a \geq 0$ e b é o menor inteiro positivo possível.
Assim $-q = a^2 - nb^2$.
Novamente, usaremos o fato de $N(m + \sqrt{n}) = N(m + \sqrt{m^2 - 1}) = 1$ e com isso teremos que:

$$-q = N((a - b\sqrt{n}).(m + \sqrt{n})) = N(am - bn + (a - bm)\sqrt{n}),$$

donde segue que

$$(am - bn)^2 - n(a - bm)^2 = -q$$

Assim, segue que

$$\alpha = |am - bn| + |a - bm|\sqrt{n}$$

é uma dentre as soluções $x + y\sqrt{n}$ da equação $A^2 - nB^2 = -q$ tais que $x \geq 0$ e $y > 0$.

Logo, pela escolha de a e b temos que

$$|a - bm| \geq b,$$

donde temos novamente que

$$a - bm \geq b \quad \text{ou} \quad a - bm \leq -b.$$

Então, se supomos $a - bm \geq b$ temos que $a \geq b(m + 1)$, donde segue que

$$-q = a^2 - nb^2 \geq b^2(m + 1)^2 - (m^2 - 1)b^2 = 2mb^2 + 2b^2.$$

Logo,

$$-q \geq 2b^2(m + 1) \geq 2(m + 1),$$

uma vez que $b \geq 1$.

Assim, $q \leq -2(m + 1) < 0$, o que contraria o fato de $q > 0$.

Por outro lado, se $a - bm \leq -b$ então $a \leq b(m - 1)$, donde

$$-q = a^2 - nb^2 \leq b^2(m - 1)^2 - (m^2 - 1)b^2 = -2mb^2 + 2b^2.$$

Com isso, temos que,

$$q \geq 2b^2(m - 1) \geq 2(m - 1) > m - 1,$$

o que contraria o fato de $q \mid (m - 1)$.

Portanto esse caso também não pode ocorrer.

Devido a impossibilidade de ocorrer os casos acima, concluimos que não existe um fator primo de n da forma $4k + 3$,o que contraria as observações iniciais feitas no início desta demonstração.

Assim, segue que $\boldsymbol{h}_{\mathbf{K}} > 1$. ■

3 - Comentários sobre a Literatura pesquisada referente a este Capítulo

A demonstração de que $\xi = \frac{2m^2 + r}{|r|} + \frac{2m}{|r|}\sqrt{n}$ é a unidade fundamental de $\boldsymbol{Q}(\sqrt{n})$, para $n = m^2 + r$, livre de quadrados, com m e r inteiros não nulos tais que $m > 1$, $r \mid 4m$ e $-m < r \leq m$, ***teoremas 1*** e ***2***, foi feita seguindo uma técnica diferente de encontrada na literatura pesquisada.

Na pouca literatura encontrada sobre como se calcular explicitamente a unidade fundamental dos corpos quadráticos $Q(\sqrt{n})$, os procedimentos usados são os relacionados com a teoria das ***frações contínuas***, conforme em [5].
Optamos, neste trabalho, por um tratamento que envolvesse apenas fatos elementares da ***teoria de corpos quadráticos***, de ***equações diofantinas*** e ***congruências.***

Com respeito ao ***teorema 3***, não encontramos na literatura pesquisada demonstração direta do fato de que $h_K > 1$ para $K = Q(\sqrt{m^2 - 1})$. Somente em [9] encontramos uma demonstração das condições necessárias e suficientes para que o número de classes de $Q(\sqrt{n})$ seja 1 (são elas: n inteiro primo da forma $4k + 1$, n primo positivo da forma $4k + 3$ ou $n = p.q$, com p e q primos positivos da forma $4k + 3$). No entanto, tal demonstração foge da linha deste trabalho uma vez que nela são utilizadas ferramentas mais sofisticadas tais como ***teoria de gêneros***.
A demonstração que fizemos é diferente e em certo sentido bem mais simples pois nela utilizamos, mais uma vez, apenas argumentos elementares de ***congruências, equações diofantinas*** e ***corpos quadráticos***, sendo assim, uma demonstração mais apropriada à linguagem deste texto.

4 - Unidades fundamentais de corpos quadráticos reais

A tabela que se segue traz as unidades fundamentais dos corpos quadráticos reais $Q(\sqrt{n})$, n livre de quadrados e $n \leq 101$. As letras I e P indicam, respectivamente, se tais unidades são impróprias ou próprias, isto é se têm norma negativa ou positiva.

Tabela I

n	μ	$m^2 + r$	m	r	P/I
2	$1+\sqrt{2}$	1^2+1	1	1	I
3	$2+\sqrt{3}$	2^2-1	2	-1	P
5	$\frac{1+\sqrt{5}}{2}$	2^2+1	2	1	I
6	$5+2\sqrt{6}$	2^2+2	2	2	P
7	$8+3\sqrt{7}$	2^2+3	3	-2	P

n	μ	m^2+r	m	r	P/I
10	$3+\sqrt{10}$	3^2+1	3	1	I
11	$10+3\sqrt{11}$	3^2+2	3	2	P
13	$\frac{3+\sqrt{13}}{2}$	4^2-3	4	-3	I
14	$15+4\sqrt{14}$	4^2-2	4	-2	P
15	$4+\sqrt{15}$	4^2-1	4	-1	P
17	$4+\sqrt{17}$	4^2+1	4	1	I
19	$170+39\sqrt{19}$	4^2+3	4	3	P
21	$\frac{5+\sqrt{21}}{2}$	5^2-4	5	-4	P
22	$197+92\sqrt{22}$	5^2-3	5	-3	P
23	$24+5\sqrt{23}$	5^2-2	5	-2	P
26	$5+\sqrt{26}$	5^2+1	5	1	I
29	$\frac{5+\sqrt{29}}{2}$	5^2+4	5	4	I
30	$11+2\sqrt{30}$	5^2+5	5	5	P
31	$1520+275\sqrt{31}$	6^2-5	6	-5	P
33	$23+4\sqrt{33}$	6^2-3	6	-3	P
34	$35+6\sqrt{34}$	6^2-2	6	-2	P
35	$6+\sqrt{35}$	6^2-1	6	-1	P
37	$6+\sqrt{37}$	6^2+1	6	1	I
38	$37+6\sqrt{38}$	6^2+2	6	2	P
39	$25+4\sqrt{39}$	6^2+3	6	3	P
41	$32+5\sqrt{41}$	6^2+5	6	5	I
42	$13+2\sqrt{42}$	6^2+6	6	6	P
43	$3482+531\sqrt{43}$	7^2-6	7	-6	P
46	$24335+3588\sqrt{46}$	7^2-3	7	-3	I
47	$48+7\sqrt{47}$	7^2-2	7	-2	P
51	$50+7\sqrt{51}$	7^2+2	7	2	P
53	$\frac{5+\sqrt{53}}{2}$	7^2+4	7	4	I
55	$89+12\sqrt{55}$	7^2+6	7	6	P
57	$151+20\sqrt{57}$	8^2-7	8	-7	P
58	$99+13\sqrt{58}$	8^2-6	8	-6	I
59	$530+69\sqrt{59}$	8^2-5	8	-5	P
61	$\frac{39+5\sqrt{61}}{2}$	8^2-3	8	-3	I
62	$3+8\sqrt{62}$	8^2-2	8	-2	P
65	$8+\sqrt{65}$	8^2+1	8	1	I
66	$65+8\sqrt{66}$	8^2+2	8	2	P
67	$48842+5967\sqrt{67}$	8^2+3	8	3	P
69	$\frac{25+3\sqrt{69}}{2}$	8^2+5	8	5	P

n	μ	$m^2 + r$	m	r	P/I
70	$251 + 30\sqrt{70}$	$8^2 + 6$	8	6	P
71	$3480 + 413\sqrt{71}$	$8^2 + 7$	8	7	P
73	$1068 + 125\sqrt{73}$	$9^2 - 8$	9	-8	I
74	$43 + 5\sqrt{74}$	$9^2 - 7$	9	-7	I
77	$\frac{9+\sqrt{77}}{2}$	$9^2 - 4$	9	-4	P
78	$53 + 6\sqrt{78}$	$9^2 - 3$	9	-3	P
79	$9 + \sqrt{82}$	$9^2 + 1$	9	1	I
83	$82 + 9\sqrt{83}$	$9^2 + 2$	9	2	P
85	$\frac{9+\sqrt{85}}{2}$	$9^2 + 4$	9	4	I
86	$10405 + 1122\sqrt{86}$	$9^2 + 5$	9	5	P
87	$28 + 3\sqrt{87}$	$9^2 + 6$	9	6	P
89	$500 + 53\sqrt{89}$	$9^2 + 8$	9	8	I
91	$1574 + 165\sqrt{89}$	$10^2 - 9$	10	-9	P
93	$\frac{29+3\sqrt{93}}{2}$	$10^2 - 7$	10	-7	P
94	$2143295 + 221064\sqrt{94}$	$10^2 - 6$	10	-6	P
95	$39 + 4\sqrt{95}$	$10^2 - 5$	10	-5	P
97	$5604 + 569\sqrt{97}$	$10^2 - 3$	10	-3	I
101	$10 + \sqrt{101}$	$10^2 + 1$	10	1	I

As unidades fundamentais da tabela acima foram extraidas de [2, páginas 168 - 171].

CAPÍTULO 2

OS CORPOS QUADRÁTICOS REAIS $Q(\sqrt{m^2+r})$

Neste capítulo, examinaremos o ***número de classes*** de certos corpos quadráticos reais. Mais uma vez, estaremos interessados nos corpos quadráticos $\boldsymbol{K} = \boldsymbol{Q(\sqrt{n})}$, já mencionados anteriormente, onde $n = m^2 + r$ com $-m < r \leq m$, $r \mid 4m$ e n livre de quadrados. Nosso objetivo principal será estabelecer condições suficientes para que o ***grupo de classes de ideais***, $\mathscr{C}\ell_K$, do anel $\mathbf{I}_K$ dos inteiros algébricos de $\boldsymbol{K}$ seja não trivial. Para tanto, como no capítulo anterior, faremos uso da solubilidade de determinadas ***equações diofantinas***.

1 - Condições necessárias para a solubilidade de certas equações diofantinas.

Os resultados que iremos demonstrar nesta seção serão usados como lemas para a demonstração do principal teorema deste capítulo.

No primeiro deles, ***lema 6***, a partir da solubilidade de equações diofantinas do tipo $A^2 - nB^2 = \pm t$, onde t é um inteiro positivo não quadrado, e n é um inteiro positivo livre de quadrados da forma $n = m^2 + r$ com $0 < r \leq m$ e $r \mid 4m$, obteremos relações de desigualdade entre t e m ou t e r. Tais desigualdades permitirão estabelecer condições suficientes para que o ***número de classes de*** $\boldsymbol{Q(\sqrt{n})}$ seja maior que 1 quando tivermos $n \equiv_4 1$ e $1 \leq r \leq m$.

O segundo resultado desta seção, ***lema 7***, relaciona, de certa forma, as soluções minimais de equações diofantinas do tipo $X^2 - nY^2 = 1$ com as soluções minimais das do tipo $A^2 - nB^2 = -t$.

A prova do ***lema 6*** baseia-se somente em fatos fundamentais referentes a teoria de equações diofantinas e, mais uma vez, em propriedades

básicas da teoria de corpos quadráticos. Nesse resultado estabeleceremos condições necessárias para a solubilidade de certas equações diofantinas.

Lema 6 : *Seja $n = m^2 + r$, livre de quadrados, com m , r inteiros positivos tais que $r \mid 4m$ e $0 < r \leq m$. Suponha também que t é um inteiro positivo não quadrado. Se a equação $A^2 - nB^2 = \pm t$ tem solução inteira segue que:*
(i) Se $r = 1$ então $t \geq 2m$;
(ii) Se $r = 4$ e $t \equiv_4 0$ então $(t/4) \geq m$;
(iii) Se $r \not\equiv_4 0$ e $r \neq 1$ então $t \geq r$
(iv) Se $r \equiv_4 0$, $r \neq 4$ e $n \not\equiv_4 1$ então $t \geq r$;
(v) Se $r \equiv_4 0$, $r \neq 4$, $n \equiv_4 1$ e $t \equiv_4 0$ então $t \geq r$;

Demonstração:
(i) Seja $r = 1$.
Por hipótese, a equação

$$A^2 - (m^2 + 1)B^2 = \pm t \qquad \textbf{(16)}$$

tem solução. Dentre suas soluções inteiras $x + y\sqrt{n}$, com $x \geq 0$ e $y > 0$, seja $a + b\sqrt{n}$ aquela na qual b é mínimo.
Temos então que

$$a^2 - (m^2 + 1)b^2 = \pm t. \qquad \textbf{(16')}$$

Por outro lado, $N(m + \sqrt{m^2 + 1}) = -1$ e assim segue que

$$N((a + b\sqrt{m^2 + 1}).(m + \sqrt{m^2 + 1})) = \pm t.$$

Então,

$$(am - b(m^2 + 1))^2 - (m^2 + 1).(a - bm)^2 = \pm t.$$

Com isso, vemos que $\alpha = |am - b(m^2 + 1)| + |a - bm|\sqrt{n}$ é solução para a ***equação (16)*** e como $|a - bm| > 0$ (caso contrário t seria negativo ou um quadrado, o que contraria as nossas hipóteses) e $|am - b(m^2 + 1)| \geq 0$, segue, pela minimidade de b que

$$|a - bm| \geq b.$$

Então temos que

$$a - bm \geq b \qquad \text{ou} \qquad bm - a \geq b.$$

Se $a - bm \geq b$ temos que $a \geq b(m + 1)$, logo, pela ***equação (16')***, tem-se que

$$\pm t \geq b^2(m + 1)^2 - (m^2 + 1)b^2 = b^2(m^2 + 2m + 1) - b^2(m^2 + 1) = 2mb^2.$$

Mas $b \geq 1$, logo $2mb^2 \geq 2m$ e assim $\pm t \geq 2m$.
Como $t > 0$ e $m > 0$, segue que $t \geq 2m$.

Por outro lado, se $bm - a \geq b$ então $a \leq b(m-1)$.
Assim, da ***equação (16)***, segue que

$$\pm t \leq b^2(m-1)^2 - (m^2+1)b^2 = b^2(m^2 - 2m + 1) - b^2(m^2+1) = -2mb^2.$$

Novamente, usando o fato que $b \geq 1$, temos que $-2mb^2 \leq -2m$ donde $\pm t \leq -2m$.
Mas, $t > 0$ e $m > 0$, logo $-t \leq -2m$ ou seja $t \geq 2m$.
Portanto segue a ***afirmação (i)***.

(ii) Seja agora $r = 4$ e $t = 4k$, para algum $k \in \boldsymbol{Z}$, k não quadrado.
Por hipótese, a equação

$$A^2 - (m^2+4)B^2 = \pm t = \pm 4k \qquad \textbf{(17)}$$

tem solução.
Escolha, então, dentre as soluções $a + b\sqrt{n}$ ***da equação (17)***, com $a \geq 0$ e $b > 0$, aquela tal que b é mínimo.
Assim,

$$a^2 - (m^2+4)b^2 = \pm 4k,$$

donde

$$N(a + b\sqrt{m^2+4}) = \pm 4k.$$

Como $N\left(\frac{m+\sqrt{m^2+4}}{2}\right) = -1$, segue que

$$N\left((a + b\sqrt{m^2+4}).\left(\frac{m+\sqrt{m^2+4}}{2}\right)\right) = \pm 4k.$$

Assim,

$$\left(\frac{am - b(m^2+4)}{2}\right)^2 - (m^2+4).\left(\frac{a-bm}{2}\right)^2 = \pm 4k. \qquad \textbf{(18)}$$

Por outro lado, temos que

$$a \equiv_2 a^2 \equiv_2 (m^2+4)b^2 \qquad \text{e} \qquad m \equiv_2 m^2 \equiv_2 (m^2+4),$$

donde

$$am \equiv_2 (m^2+4)^2b^2.$$

Assim segue que

$$am - (m^2+4)b \equiv_2 (m^2+4)^2b^2 - (m^2+4)b \equiv_2 0,$$

isto é

$$2 \mid (am - (m^2+4)b) \qquad \textbf{(19)}$$

Temos também que $mb \equiv_2 (m^2+4)b$, donde, segue que

$$a - bm \equiv_2 (m^2+4)^2b^2 - (m^2+4)b \equiv_2 0,$$

ou seja

$$2 \mid (a - bm) \qquad \textbf{(20)}$$

Assim, de ***(19)*** e ***(20)*** temos que

$$\frac{a-bm}{2} \in \boldsymbol{Z} \quad \text{e} \quad \frac{am-b(m^2+4)}{2} \in \boldsymbol{Z}.$$

Portanto de ***(18)*** e da escolha de b, segue que

$$\left|\frac{a-bm}{2}\right| \geq b.$$

Então,

$$a - bm \geq 2b \quad \text{ou} \quad bm - a \geq 2b.$$

Se $a - bm \geq 2b$ então $a \geq b(2 + m)$.
Como $a^2 - (m^2 + 4)b^2 = \pm 4k$ e $a \geq 0$ segue que

$$\pm 4k \geq b^2(2 + m)^2 - (m^2 + 4)b^2 = b^2(4 + 4m + m^2) - b^2(m^2 + 4) = 4b^2m.$$

Mas $b \geq 1$, logo $4b^2m \geq 4m$ e assim $\pm 4k \geq 4m$.
Como $t > 0$ e $m > 0$ temos que $4k \geq 4m$, ou seja $k \geq m$.
Por outro lado, se $bm - a \geq 2b$ então $a \leq b(m - 2)$.
Com isso, novamente de $a^2 - (m^2 + 4)b^2 = \pm 4k$ e $a \geq 0$, concluímos que

$$\pm 4k \leq b^2(m - 2)^2 - (m^2 + 4)b^2 = b^2(4 - 4m + m^2) - b^2(m^2 + 4) = -4b^2m.$$

Como $b \geq 1$ temos que $-4b^2m \leq -4m$ e com isso $\pm 4k \leq -4m$.
Do fato de $t > 0$ e $m > 0$ segue que $-4k \leq -4m$.
De ambos os casos, podemos concluir que $k \geq m$, donde,

$$t/4 \geq m,$$

e assim segue a desigualdade ***(ii)***.

(iii) Suponhamos agora que $r \not\equiv_4 0$ e $r \neq 1$.
Seja t um inteiro positivo não quadrado. Por hipótese, a equação

$$A^2 - nB^2 = \pm t = A^2 - (m^2 + r)B^2 = \pm t \qquad \textbf{(20)}$$

tem solução.
Tome, então, dentre suas soluções inteiras $a + b\sqrt{n}$ com $a \geq 0$ e $b > 0$, aquela tal que b é mínimo. Assim, $a^2 - nb^2 = \pm t$.
Considere também

$$\xi = \frac{2m^2 + r}{r} + \frac{2m}{r}\sqrt{n}.$$

Conforme ***lema 1***, capítulo 1, temos que $N(\xi) = 1$.

Como $N(a - b\sqrt{n}) = a^2 - nb^2 = \pm t$, segue que $N(\xi).N(a - b\sqrt{n}) = \pm t$ e assim,

$$\left(\frac{2am^2 + ar - 2mbn}{r}\right)^2 - n\left(\frac{2ma - 2bm^2 - br}{r}\right)^2 = \pm t, \qquad (21)$$

Se $d = mdc(r, 4)$ temos que $d = 1$ ou $d = 2$, uma vez que $r \not\equiv_4 0$.
Analisemos, então os dois possíveis valores para d:

(a) $d = 1$
Como por hipótese $r \mid 4m$ então $r \mid m$.
Assim

$$\left|\frac{2am^2 + ar - 2mbn}{r}\right| \in \boldsymbol{Z} \quad \text{e} \quad \left|\frac{2ma - 2bm^2 - br}{r}\right| \in \boldsymbol{Z}^*$$

(lembre que t é não quadrado).

(b) $d = 2$
Neste caso $r = 2r'$ onde r'é ímpar, uma vez que $r \not\equiv_4 0$.
Assim como $r \mid 4m$, segue que $4m = r.k$, com $k \in \boldsymbol{Z}$. Então, $4m = (2r').k$, donde $2m = r'k$. Logo, $2 \mid r'k$ e como r' é ímpar, temos que $2 \mid k$ ou seja $k = 2k'$, $k' \in \boldsymbol{Z}$.
Então de $4m = rk$ segue que $2m = r.k'$e assim $r \mid 2m$.
Temos então que

$$\left|\frac{2am^2 + ar - 2mbn}{r}\right| \in \boldsymbol{Z} \quad \text{e} \quad \left|\frac{2am - 2bm^2 - br}{r}\right| \in \boldsymbol{Z}^*$$

(lembre, novamente, que t é não quadrado).
Finalmente, de (a), (b) e ***(21)*** vemos que

$$\alpha = \left|\frac{2am^2 + ar - 2mbn}{r}\right| + \left|\frac{2ma - 2bm^2 - br}{r}\right|\sqrt{n}$$

é solução inteira da ***equação (20)*** e então, pela minimidade de b, segue que

$$\left|\frac{2ma - 2bm^2 - br}{r}\right| \geq b.$$

Logo,

$$2ma - 2m^2b - br \geq br \quad \text{ou} \quad br + 2m^2b - 2ma \geq br.$$

Por um lado, se $2ma - 2m^2b - br \geq br$ então

$$a \geq b\left(\frac{r + m^2}{m}\right).$$

Assim, de $a^2 - nb^2 = \pm t$, segue que

$$\pm t \geq \frac{b^2}{m^2}(r+m^2)^2 - (m^2+r)b^2 = \frac{b^2}{m^2}(r^2 + 2rm^2 + m^4) - b^2(m^2 + r).$$

Logo temos que

$$\pm t \geq \frac{b^2}{m^2} r^2 + b^2 r = b^2(\frac{r^2}{m^2} + r),$$

e como $b \geq 1$ segue que

$$\pm t \geq \frac{r^2}{m^2} + r.$$

Mas $r > 0$ e $m > 0$, logo podemos concluir que $\frac{r^2}{m^2} + r \geq r$ e assim $\pm t \geq r$.

Como $t > 0$ teremos então a desigualdade desejada, qual seja $t \geq r$.

Por outro lado, se $br + 2m^2b - 2ma \geq br$ teremos que $0 \leq a \leq mb$.

Novamente de $a^2 - nb^2 = \pm t$ segue que

$$\pm t \leq m^2b^2 - (m^2 + r)b^2 = -b^2r \leq -r,$$

uma vez que $b \geq 1$.

Como $t > 0$ e $r > 0$ segue que $-t \leq -r$, donde segue a desigualdade desejada, a saber $t \geq r$.

(iv) Consideremos agora que $r \equiv_4 0$, $r \neq 4$ e $n \not\equiv_4 1$.

Seja t um inteiro positivo não quadrado e considere, novamente

$$\xi = \frac{2m^2 + r}{r} + \frac{2m}{r}\sqrt{n}.$$

Por hipótese, a equação $A^2 - nB^2 = \pm t$ tem solução.

Assim, dentre suas soluções $a + b\sqrt{n}$, com $a \geq 0$ e $b > 0$, escolhemos aquela tal que b é mínimo.

Portanto, como no ítem anterior, $N(\xi) = 1$ e $N(a - b\sqrt{n}) = \pm t$. Assim, consequentemente, teremos aqui também a igualdade ***(21)***, qual seja,

$$\left(\frac{2am^2 + ar - 2mbn}{r}\right)^2 - n\left(\frac{2ma - 2bm^2 - br}{r}\right)^2 = \pm t.$$

Do ***lema 1***, capítulo 1, temos que ξ é uma unidade, logo como $n \equiv_4 2$ ou 3 teremos que

$$\frac{2m^2 + r}{r} \in \boldsymbol{Z} \quad \text{e} \quad \frac{2m}{r} \in \boldsymbol{Z}$$

e assim

$$\left|\frac{2am^2 + ar - 2mbn}{r}\right| = \left|a\left(\frac{2m^2 + r}{r}\right) - bn\left(\frac{2m}{r}\right)\right| \in \boldsymbol{Z}$$

e

$$\left|\frac{2ma-2bm^2-br}{r}\right| = \left|a\left(\frac{2m}{r}\right)-b\left(\frac{2m^2+r}{r}\right)\right| \in \boldsymbol{Z}$$

Desta forma, teremos que

$$\alpha = \left|\frac{2am^2+ar-2mbn}{r}\right| + \left|\frac{2ma-2bm^2-br}{r}\right|\sqrt{n}$$

é solução inteira da equação $A^2 - nB^2 = \pm t$,e como $\left|\frac{2ma-2bm^2-br}{r}\right| \neq 0$, pois caso contrário t seria um quadrado, segue, pela minimidade de b, que

$$\left|\frac{2ma-2bm^2-br}{r}\right| \geq b.$$

Da mesma forma que no ítem anterior, segue que $t \geq r$.

(v)Suponhamos, finalmente, que $r \equiv_4 0$, $r \neq 4$ e $n \equiv_4 1$
Considere ainda que t é um inteiro positivo não quadrado tal que $t \equiv_4 0$ e de modo que a equação $A^2 - nB^2 = \pm t$ tenha solução. Assim $t = 4k$, para algum k inteiro positivo e não quadrado.
Dentre as soluções inteiras da equação $A^2 - nB^2 = \pm 4k$, tome $a + b\sqrt{n}$ de forma que $a \geq 0$ e b é o menor inteiro possível tal que $b > 0$.
Considere, novamente,

$$\xi = \frac{2m^2+r}{r} + \frac{2m}{r}\sqrt{n}.$$

Então $N(\xi.(a - b\sqrt{n})) = \pm 4k$, donde,

$$\left(\frac{2am^2+ar-2mbn}{r}\right)^2 - n\left(\frac{2ma-2bm^2-br}{r}\right)^2 = \pm 4k. \qquad (22)$$

Observe que $a^2 - nb^2 = \pm 4k$, logo temos que a e b têm a mesma paridade. Com efeito, se a é um número par, então $4 \mid a^2$, logo $4 \mid nb^2$. Mas $n \equiv_4 1$, logo temos, necessariamente, que $4 \mid b^2$, donde concluimos que b é par. Por outro lado segue trivialmente que se b é par então a é par também.
Observe ainda que como $n \equiv_4 1$ o ***lema 1***, do capítulo 1, nos garante que

$$\xi = \frac{4m^2+2r}{2r} + \frac{4m}{2r}\sqrt{n}$$

é uma unidade.

Assim podemos afirmar que $\frac{4m^2+2r}{r} \equiv_2 \frac{4m}{r}$.

Mas por outro lado, temos que $a \equiv_2 b$, logo $\frac{(4m^2+2r)b}{r} \equiv_2 \frac{4ma}{r}$ e sendo assim

$$\frac{2am-2m^2b-br}{r} = \frac{1}{2}\left(\frac{4ma}{r} - \frac{(4m^2+2r)b}{r}\right) \in \boldsymbol{Z}. \qquad \textbf{(23)}$$

Temos também que $\frac{(4m^2+2r)a}{r} \equiv_2 \frac{4mb}{r}$ e então

$$\frac{2am^2+ar-2mbn}{r} = \frac{1}{2}\left(\frac{(4m^2+2r)a}{r} - \frac{4mbn}{r}\right) \in \boldsymbol{Z}. \qquad \textbf{(24)}$$

Assim de ***(22)***,***(23)*** e ***(24)*** segue que

$$\alpha = \left|\frac{2am^2+ar-2mbn}{r}\right| + \left|\frac{2ma-2bm^2-br}{r}\right|\sqrt{n}$$

é solução inteira da equação $A^2 - nB^2 = \pm 4k$.
Então, da minimidade de b, segue que

$$\left|\frac{2ma-2bm^2-br}{r}\right| \geq b,$$

isto é

$$2ma - 2m^2b - br \geq br \qquad \text{ou} \qquad br + 2m^2b - 2ma \geq br.$$

Se $2ma - 2m^2b - br \geq br$ então

$$a \geq \frac{m^2b+br}{m} = \frac{b(m^2+r)}{m}.$$

Assim de $a^2 - nb^2 = \pm 4k$ segue que

$$\pm 4k \geq \frac{b^2}{m^2}(m^2+r)^2 - (m^2+r)b^2 = b^2\left(\frac{r^2}{m^2}+r\right) \geq \frac{r^2}{m^2} + r,$$

uma vez que $b \geq 1$.
Como $r > 0$ temos que $\pm 4k > r$.
Mas $k > 0$ logo $4k > r$.
Por outro lado, se $br + 2m^2b - 2ma \geq br$ então $0 \leq a \leq mb$ e assim segue que

$$\pm 4k \leq m^2b^2 - (m^2+r)b^2 = -b^2r \leq -r,$$

pois $b \geq 1$.
Segue então que $-4k \leq -r$ e aqui também teremos $4k \geq r$.
Então em ambos os casos temos que $4k \geq r$ e sendo $t = 4k$ segue a afirmação de que $t \geq r$. ■

Passemos agora para o segundo lema a que nos propusemos demonstrar nesta seção.

Tal resultado , conforme já mencionamos, trata de soluções minimais de certas equações diofantinas e sua demonstração baseia-se apenas em propriedades elementares das equações diofantinas.

***Lema** 7: Sejam n, t números naturais, livres de quadrados. Se $x + y\sqrt{n}$ e $a + b\sqrt{n}$ são as soluções minimais das equações $X^2 - nY^2 = 1$ e $A^2 - nB^2 = -t$, respectivamente, então*

$$0 < b \leq \sqrt{\frac{t(x+1)}{2n}}.$$

Demonstração: Obviamente, temos que $b > 0$.
Observe que $a^2 - nb^2 = -t$ e que $x^2 - ny^2 = 1$ e assim segue que

$$x^2b^2 = (1 + y^2n).\left(\frac{t + a^2}{n}\right) = (a^2 + t).(\frac{1}{n} + y^2) > a^2y^2.$$

Desta forma, $xb - ay > 0$.
Por outro lado temos que

$$\begin{aligned}(ax - byn)^2 - n(xb - ya)^2 &= a^2x^2 - 2axbyn + b^2y^2n^2 - (x^2b^2 - 2xbya + y^2a^2)n \\ &= x^2(a^2 - nb^2) - y^2n(a^2 - nb^2) \\ &= (x^2 - y^2n).(a^2 - nb^2) \\ &= -t,\end{aligned}$$

donde segue que

$$\alpha = (ax - byn) + (xb - ya)\sqrt{n}$$

é também solução para a equação $A^2 - nB^2 = -t$.
Assim, como $xb - ay > 0$, devido à escolha de b podemos concluir que $xb - ay \geq b$, ou ainda, que $b(x - 1) \geq ya$.
Portanto temos que

$$\frac{y^2a^2}{b^2} \leq (x-1)^2 = \frac{(x^2-1).(x-1)}{x+1} = \frac{ny^2(x-1)}{x+1}$$

donde segue que

$$\frac{x-1}{x+1} \geq \frac{a^2}{nb^2} = \frac{nb^2 - t}{nb^2} = 1 + \frac{-t}{nb^2}.$$

Com isso,

$$\frac{-t}{nb^2} \leq \frac{x-1}{x+1} - 1 = \frac{-2}{x+1},$$

e assim,

$$\frac{t}{nb^2} \geq \frac{2}{x+1}.$$

Então,

$$b^2 \leq \frac{t(x+1)}{2n},$$

donde segue a desigualdade desejada, qual seja:

$$b \leq \sqrt{\frac{t(x+1)}{2n}}. \blacksquare$$

2 - O número de classes dos corpos quadráticos reais $Q(\sqrt{m^2+r})$

O fato do ***grupo de classes de ideais*** de um ***Domínio de Dedekind*** $\mathcal{D}$ não se reduzir ao elemento neutro caracteriza $\mathcal{D}$ como um ***domínio não principal***, e consequentemente ***não fatorial*** , uma vez que tais condições são equivalentes num ***Domínio de Dedekind***.

Veremos nesta seção que o comportamento do anel $\mathbf{I}_L$ dos inteiros algébricos do corpo $L = Q(\sqrt{m^2-1})$ quanto a não unicidade de fatoração, conforme podemos concluir do ***teorema 2*** do capítulo anterior (pois conforme ***proposição A6*** do apêndice, o anel dos inteiros algébricos de um corpo de números algébricos é, particularmente um domínio de Dedekind), não é um caso particular. Na realidade esse fato ocorre para o anel $\mathbf{I}_K$ dos inteiros algébricos de alguns corpos quadráticos reais do tipo $K = Q(\sqrt{n})$, onde $n = m^2 + r$ com $-m < r \leq m$, $r \mid 4m$ e n livre de quadrados, dentre os quais $L = Q(\sqrt{m^2-1})$ está incluido.

O próximo teorema estabelecerá, então, condições suficientes para que o ***grupo de classes de ideais***, $\mathcal{Cl}_K$, para K conforme acima descrito, seja não trivial.

Novamente, $\left(\frac{-}{}\right)$ denotará o ***símbolo de Legendre***, ao passo que $\left[\frac{-}{}\right]$ denotará o ***símbolo de Jacobi***, conhecida generalização do ***símbolo de Legendre***.

Teorema 4: *Seja $n = m^2 + r$ um inteiro positivo livre de quadrados, com m e r inteiros tais que $m > 0$, $-m < r \leq m$ e $r \mid 4m$.*
Se $\boldsymbol{h}_K$ é o número de classes de $\boldsymbol{K} = \boldsymbol{Q}(\sqrt{n})$ então $\boldsymbol{h}_K > 1$ sempre que :
(a) $n \equiv_4 1$, $1 \leq r \leq m$ e existe um inteiro primo p que divide m tal que $p > 2$ e $\left(\frac{r}{p}\right) = 1$, ou $p = 2$ e $n \equiv_8 1$.

Além disso, uma das condições abaixo deve ser satisfeita:
(i) Se $r = 1$ então $m > 2p$;
(ii) Se $r = 4$ então $m > p$;
(iii) Se $r \neq 1$ e $r \neq 4$ então $r > 4p$,
(b) $n \not\equiv_4 1$, $-2 < r \leq m$, $r \neq 2$ e $m > 2$. Ou se $r = -2$ então $m > 3$ e $m \equiv_3 0$.

Demonstração:
(a) Seja n um inteiro positivo tal que $n \equiv_4 1$, com $1 \leq r \leq m$. Seja também p o número primo dado pela condição ***(a)***.
Suponha, por absurdo, que $\boldsymbol{h}_K = 1$.
Observe que sendo $n \equiv_4 1$, temos que o anel dos inteiros algébricos de $\boldsymbol{K}$ é

$$\mathbf{I}_K = \left\{ \frac{x + y\sqrt{n}}{2}, \text{ onde } x, y \in \boldsymbol{Z} \text{ e } x \equiv_2 y \right\}.$$

#***Afirmação 1:*** *Uma das equações $A^2 - nB^2 = \pm 4p$ tem solução.*
Demonstração: Se $p = 2$, temos, por hipótese, que $n \equiv_8 1$.
Neste caso temos que o ideal primo $2.\mathbf{I}_K$ de $\mathbf{I}_K$ se decompõe em $\boldsymbol{K}$, ou seja, o ideal $2.\mathbf{I}_K$ de $\mathbf{I}_K$ é da forma $2.\mathbf{I}_K = \mathcal{D}_1.\mathcal{D}_2$, onde $\mathcal{D}_1$ e $\mathcal{D}_2$ são os únicos ideais primos de $\mathbf{I}_K$ cuja norma é 2.
Assumindo-se a hipótese de que $\boldsymbol{h}_K = 1$, tem-se que $\mathcal{D}_1$ e $\mathcal{D}_2$ são ideais principais e assim segue que existem inteiros a e b, de mesma paridade, tais que $\frac{a + b\sqrt{n}}{2}.\mathbf{I}_K = \mathcal{D}_1$.
Assim $N(\frac{a + b\sqrt{n}}{2}) = N(\mathcal{D}_1) = 2$ e com isso temos que $\frac{a^2}{4} - n\frac{b^2}{4} = \pm 2$, donde a equação $A^2 - nB^2 = \pm 8 = \pm 4p$ tem solução inteira.
Por outro lado, suponha que $p > 2$ e assim, por hipótese, $\left(\frac{r}{p}\right) = 1$.
Como $n = m^2 + r$ e $p \mid m$ então $n \equiv_p r$, e com isso,

$$\left(\frac{n}{p}\right) = \left(\frac{r}{p}\right) = 1.$$

Assim pela lei de decomposição de ideais $q.\mathbf{I}_K$, q primo, em ideais primos de $\mathbf{I}_K$, temos que o ideal $p.\mathbf{I}_K$ de $\mathbf{I}_K$ se decompõe em K, ou seja, o ideal $p.\mathbf{I}_K$ é tal que $p.\mathbf{I}_K = \mathcal{P}_1.\mathcal{P}_2$, onde $\mathcal{P}_1$ e $\mathcal{P}_2$ são os únicos ideais primos de $\mathbf{I}_K$ cuja norma é p.

Portanto, como $h_K = 1$, tem-se que existe $\frac{c+d\sqrt{n}}{2} \in \mathbf{I}_K$ tal que $\left(\frac{c+d\sqrt{n}}{2}\right).\mathbf{I}_K = \mathcal{P}_1$.

Assim, $\frac{c^2}{4} - n\frac{d^2}{4} = \pm p$, donde a equação $A^2 - nB^2 = \pm 4p$ tem solução inteira.#

Como a equação $A^2 - nB^2 = \pm 4p$ tem solução, segue, pelo ***lema 6*** deste capítulo, que:

1-) Se $r = 1$ então $4p \geq 2m$, donde temos que $2p \geq m$;

2-) Se $r = 4$ então $\frac{4p}{4} \geq m$, donde temos que $p \geq m$;

3-) Se $r \not\equiv_4 0$ e $r \neq 1$ então $4p \geq r$;

4-) Se $r \equiv_4 0$ e $r \neq 4$ então $4p \geq r$.

Mas as conclusões ***1-)***, ***2-)***, ***3-)*** e ***4-)*** contradizem, respectivamente, os ítens ***(i)***, ***(ii)***, ***(iii)*** e ***(iii)*** da hipótese ***(a)*** do teorema.
Portanto, dentro das hipóteses ***(a)*** do teorema, segue que $h_K > 1$.

(b) Suponhamos agora que $n \not\equiv_4 1$, assim teremos que

$$\mathbf{I}_K = \{ x + y\sqrt{n}, \text{ com } x,y \in \mathbf{Z} \}.$$

Suponhamos também que $m > 2$ e analisemos os diversos valores inteiros de r tais que $-2 \leq r \leq m$, com $r \neq 2$.

b_1) $r = -2$.
Por hipótese temos que $3 \mid m$ e $m > 3$.
Agora, suponha, por absurdo, que $h_K = 1$.
#***Afirmação 2:*** *Das equações $A^2 - nB^2 = \pm 3$, apenas a negativa, $A^2 - nB^2 = -3$, tem solução.*
Demonstração: Como $n = m^2 + r$ segue que $n + 2 = m^2$, e assim concluímos que $3 \mid (n + 2)$, ou seja $n \equiv_3 -2$.

Desta forma, pela definição do ***símbolo de Legendre***, segue que

$$\left(\frac{n}{3}\right) = \left(\frac{-2}{3}\right) = 1,$$

pois $-2 \equiv_3 1 = 1^2$.

Assim, o ideal primo $3.\mathbf{I}_K$ de $\mathbf{I}_K$ se decompõe em K, ou seja, o ideal $3.\mathbf{I}_K$ de $\mathbf{I}_K$ é da forma $3.\mathbf{I}_K = \mathcal{D}_1.\mathcal{D}_2$, onde $\mathcal{D}_1$ e $\mathcal{D}_2$ são os únicos ideais primos de $\mathbf{I}_K$ cuja norma é 3.

Como estamos supondo $h_K = 1$, temos que $\mathcal{D}_1$ e $\mathcal{D}_2$ são ideais principais e assim segue que existem inteiros a e b tais que $(a + b\sqrt{n}).\mathbf{I}_K = \mathcal{D}_1$.

Com isso concluímos que $a^2 - nb^2 = \pm 3$, uma vez que $N(\mathcal{D}_1) = 3$.

Assim, temos que uma das equações $A^2 - nB^2 = \pm 3$ tem solução. Provemos agora que é a equação negativa que tem solução.

Para tanto suponhamos que $A^2 - nB^2 = 3$ tenha solução. Então existem números inteiros c e d tais que $c^2 - nd^2 = 3$. Assim, como $c^2 \equiv_n 3$, segue que

$$\left[\frac{3}{n}\right] = \left[\frac{c^2}{n}\right] = \left[\frac{c}{n}\right]^2 = 1. \qquad (25)$$

(observe que n é ímpar)

Por outro lado, como $\left[\frac{-2}{3}\right] = 1$, segue que

$$\left[\frac{3}{n}\right] = \left[\frac{3}{n}\right].\left[\frac{-2}{3}\right]. \qquad (26)$$

Temos ainda que $n = m^2 - 2$, onde $m \equiv_3 0$, e assim

$$\left[\frac{3}{n}\right].\left[\frac{-2}{3}\right] = \left[\frac{3}{n}\right].\left[\frac{n}{3}\right]. \qquad (27)$$

Como o ***símbolo de Jacobi*** obedece a lei da reciprocidade quadrática, temos que

$$\left[\frac{3}{n}\right].\left[\frac{n}{3}\right] = (-1)^{\frac{(n-1).(3-1)}{4}} \qquad (28)$$

Mas observe que $(-1)^{\frac{n-1}{2}} = -1$, pois se $\frac{n-1}{2} = 2k$, para algum $k \in \mathbf{Z}$, então $n = 4k + 1$, o que contraria a hipótese de que $n \neq_4 1$.

Assim de ***(26)***, ***(27)*** e ***(28)***, segue que $\left[\frac{3}{n}\right] = -1$, o que contraria ***(25)***.

Assim $A^2 - nB^2 = 3$ não tem solução, donde segue a afirmação.#

Como a equação $A^2 - nB^2 = -3$ tem solução, seja $\alpha = c + d\sqrt{n}$ sua solução minimal.
Agora, pelo ***teorema 1***, temos que

$$\xi = \frac{2m^2 + r}{|r|} + \frac{2m}{|r|}\sqrt{n}$$

é a unidade fundamental de $\boldsymbol{Q}(\sqrt{n})$, donde ξ é a solução minimal da equação $A^2 - nB^2 = 1$, já que ξ é uma unidade própria.
Assim como

$$\xi = \frac{2m^2 + r}{|r|} + \frac{2m}{|r|}\sqrt{n}$$

é solução minimal da equação $A^2 - nB^2 = 1$ e

$$\alpha = c + d\sqrt{n}$$

é solução minimal da equação $A^2 - nB^2 = -3$, pelo ***lema 7*** deste capítulo, temos que

$$0 < d \leq \sqrt{\frac{3\left(\frac{2m^2 + r}{|r|} + 1\right)}{2n}} = \sqrt{\frac{3\left(\frac{2m^2 - 2}{2} + 1\right)}{2n}}.$$

Assim

$$0 < d \leq \sqrt{\frac{3m^2}{2n}} = \sqrt{\frac{3(n+2)}{2n}} = \sqrt{\frac{3}{2}\left(1 + \frac{2}{n}\right)}.$$

Como $m > 3$ então $n > 7$ e assim $\frac{2}{n} < 1$, donde $\frac{2}{n} + 1 < 2$.
Com isso temos que $0 < d < 2$, logo sendo d inteiro segue necessariamente que $d = 1$.
Mas se $d = 1$ então $c^2 = n - 3$ e assim $m^2 - c^2 = (n + 2) - (n - 3) = 5$, isto é $(m + c).(m - c) = 5$, ou ainda, $m = \pm 3$ o que contradiz a hipótese de que $m > 3$.
Portanto no caso de $n \not\equiv_4 1$ com $r = -2$, $m > 3$ e $m \equiv_3 0$ temos que $\boldsymbol{h}_K > 1$.

b₂) $r = -1$.
Neste caso $n = m^2 - 1$, então segue diretamente do ***teorema 3*** que $\boldsymbol{h}_K > 1$.

b₃) $1 \leq r \leq m$, com $r \neq 2$.
Suponha que aqui tenhamos também $\boldsymbol{h}_K = 1$.
Como $n \equiv_4 2$ ou 3 então o discriminante absoluto $\boldsymbol{d}_K = 4n$, assim $2 \mid \boldsymbol{d}_K$ donde se conclui que o ideal primo $2.\mathbf{I}_K$ de $\mathbf{I}_K$ se ramifica em $\boldsymbol{K} = \boldsymbol{Q}(\sqrt{n})$.

Com isso, temos que $2.\mathbf{I}_K = \mathcal{B}^2$, onde $\mathcal{B}$ é o único ideal primo de $\mathbf{I}_K$ cuja norma é 2.
Se assumimos que $\boldsymbol{h}_K = 1$ segue que, particularmente, $\mathcal{B}$ é um ideal principal e assim temos que existem c , $d \in \boldsymbol{Z}$ tais que $c^2 - nd^2 = \pm 2$, pois na realidade existe $(c + d\sqrt{n}) \in \mathbf{I}_K$ tal que $(c + d\sqrt{n}).\mathbf{I}_K = \mathcal{B}$.
Com isso temos que a equação $A^2 - nB^2 = \pm 2$ tem solução.
Analisemos então os possíveis valores de r, onde $1 \leq r \leq m$, com $r \neq 2$:
Se $r = 1$, como $A^2 - nB^2 = \pm 2$ tem solução segue do ***lema 6*** que então $2 \geq 2m$.
Desta forma, $m \leq 1$ e isso contraria a hipótese de que $m > 2$.
Para os demais valores inteiros de $r > 2$ teremos que:
Se $r \not\equiv_4 0$, da solubilidade da equação $A^2 - nB^2 = \pm 2$, segue do ***lema 6*** que $2 \geq r$, um absurdo!
Se $r \equiv_4 0$ e $r \neq 4$, como $n \not\equiv_4 1$, da solubilidade da equação $A^2 - nB^2 = \pm 2$ e do ***lema 6***, segue uma vez mais a contradição $2 \geq r$.
Finalmente, verifiquemos o caso em que $r = 4$.
Observe que do fato da equação $A^2 - nB^2 = \pm 2$ ter solução inteira podemos concluir que a equação $A^2 - nB^2 = \pm 8$ tem também solução inteira, logo pelo ***lema 6*** segue $\frac{8}{4} \geq m$, o que contradiz mais uma vez a hipótese de que $m > 2$.
Portanto temos novamente que $\boldsymbol{h}_K > 1$ e com isso concluímos a demonstração do teorema. ■

Encerraremos esta seção com algumas consequências imediatas deste teorema. Como no teorema, nos corolários abaixo assumiremos que $\boldsymbol{K} = \boldsymbol{Q}(\sqrt{n})$.

Corolário 1: *Se $n = (2qt)^2 + 1$ é livre de quadrados, com q primo e $t > 1$ e inteiro, então $\boldsymbol{h}_K > 1$.*
Demonstração: Com efeito, como $n = 4q^2t^2 + 1$ então $n \equiv_4 1$.
Observe que se $q = 2$ então $n \equiv_8 1$ e se $q > 2$ então $\left(\frac{r}{q}\right) = \left(\frac{1}{q}\right) = 1$.
Observe ainda que $r = 1$ e $m = 2qt > 2$, pois $t > 1$.
Assim segue do ***teorema 4*** que $\boldsymbol{h}_K > 1$. □

Corolário 2: *Se $n = (tq)^2 + 4$ é livre de quadrados, onde q é um primo ímpar e $t \geq 3$ é um inteiro também ímpar então $\boldsymbol{h}_K > 1$.*
Demonstração: De fato, observe os dois caso abaixo:
(a) $n \equiv_4 1$.

Como $m = tq$ então $q \mid m$, $q > 2$ e $\left(\frac{r}{q}\right) = \left(\frac{4}{q}\right) = 1$.

Também $r = 4$ e $m = tq > q$.

(b) $n \not\equiv_4 1$.
Note que $2 \leq r = 4 \leq m$, uma vez que $m \geq 9$.
Assim, segue do teorema que $\boldsymbol{h}_K > 1$. □

O corolário abaixo, é o análogo do ***corolário 1*** para o caso $n \equiv_4 3$.

Corolário 3: *Se* $n = (2t)^2 - 1$ *é livre de quadrados, onde* $t > 1$, *então* $\boldsymbol{h}_K > 1$.
Demonstração: Realmente, sendo $n = (2t)^2 - 1 = 4t^2 - 1$, segue que $n \equiv_4 3$.
Também, temos que $2 \leq r = -1 \leq m$, uma vez que $m > 4$.
Assim do teorema acima, segue o resultado. □

Corolário 4: *Se* $n = 9t^2 - 2$ *é um inteiro ímpar livre de quadrados, onde* $t > 1$, *então* $\boldsymbol{h}_K > 1$.
Demonstração: De fato, temos $n \not\equiv_4 1$, $r = -2$, $m > 3$ e $m = 9t^2 \equiv_3 0$, donde segue, pelo teorema, que $\boldsymbol{h}_K > 1$. □

Corolário 5: *Se* $n = t^2 + 2l$ *é livre de quadrados, com* $l > 1$ *inteiro ímpar tal que* $l \mid t$ *e* t *é par, então* $\boldsymbol{h}_K > 1$.
Demonstração: Com efeito,sendo n par, então $n \not\equiv_4 1$.
Neste caso temos $1 < r = 2l < m = t^2$, uma vez que $l > 1$ e que $l \leq t$ e $2 \leq t$.
Temos também $r \neq -2$, obviamente, e $m > 2$. Então, segue o resultado. □

3 - Comentários sobre a Literatura pesquisada referente a este Capítulo

O primeiro resultado deste capítulo, ***lema 6***, é uma generalização do [14, lema, página 70] e [1, lema, página 218]. Ambos tratam de condições necessárias para a solubilidade certas equações diofantinas, ou de outra forma, tratam de condições suficientes para a não solubilidade dessas equações.

No primeiro lema, [14], as equações são do tipo $A^2 - (m^2 + 4)B^2 = \pm 4t$, enquanto que no segundo [1] são do tipo $A^2 - (m^2 + 1)B^2 = \pm t$, onde m e t são

inteiros positivos com t não quadrado. Ambos os textos tratam do número de classes de corpos ciclotômicos.

Observamos que em [17, página 8] existe uma tentativa de generalização dos lemas acima referidos cujo enunciado é o que se segue:

« LEMA 1.1. *Seja* $n = m^2 + r$, *livre de quadrados, onde* m *e* r *são inteiros positivos tais que* $r \mid 4m$, $e\ r \in (0,m]$. *Também suponha* t *um inteiro positivo não quadrado. Se a equação* $A^2 - nB^2 = \pm t$ *tem soluções inteiras então*

(i) $r = 1$ e $t \geq 2m$, *ou*

(ii) $r = 4$, $t \equiv 0\ (mod 4)$ e $(t/4) \geq m$, *ou*

(iii) $r \neq 1, 4$ e $t \geq r$.»

No entanto, tal resultado não é verdadeiro. Com efeito, tome $n = 5^2 + 4$ e então teremos que a equação $A^2 - 29\,B^2 = -257$ tem solução inteira, a saber $a = 2$ e $b = 3$. Mas observe que $t \equiv_4 1$ muito embora tenhamos $r = 4$!

Além do resultado anterior ser falso na generalidade pretendida, observamos também que, no decorrer de sua demonstração, o autor usa inadequadamente a técnica de "minorar" uma solução de uma equação diofantina por sua solução minimal, conforme veremos a seguir:

« Ao assumir que a equação $A^2 - nB^2 = \pm t$ tem solução inteira, o autor considera u e v escolhidos de forma que $u^2 - nv^2 = \pm t$, com $u \geq 0$ e v o menor valor inteiro possível tal que $v > 0$. Depois de afirmar que

$$N\left(\left(u\left(\frac{2m^2+r}{r}\right)-\frac{2mvn}{r}\right)+\left(\frac{2mu-v(2m^2+r)}{r}\right)\sqrt{n}\right)=\pm t,$$

o autor conclui que devido a escolha de v tem-se que

$$\left|\frac{2mu-v(2m^2+r)}{r}\right| \geq v. \text{»}$$

Mas para que tal majoração tenha sentido devemos ter, necessariamente, que

$$\left|u\left(\frac{2m^2+r}{r}\right)-\frac{2mvn}{r}\right| \in \boldsymbol{Z} \quad \text{e} \quad \left|\frac{2mu-v(2m^2+r)}{r}\right| \in \boldsymbol{Z},$$

pois estamos trabalhando com as soluções inteiras da equação $A^2 - nB^2 = \pm t$, ou seja, soluções do tipo $x + y\sqrt{n}$, onde $x, y \in \boldsymbol{Z}$

No entanto, se considerarmos $n = 15^2 + 12$ teremos que a equação $A^2 - 237B^2 = -233$ tem solução minimal $u + v\sqrt{n} = 2 + \sqrt{n}$. Mas por outro lado, neste caso temos que

$$\left|\frac{2mu - v(2m^2 + r)}{r}\right| = \left|\frac{2m(u - vm)}{r} - 1\right| = \left|\frac{30 \cdot (-13)}{12}\right| = \frac{134}{4} \notin \mathbf{Z}.$$

O ***teorema 4***, [17, teorema 1.1, página 8], por sua vez, generaliza [1, teorema 1, página 217], [14, teorema 1, página 70], [24, teoremas 1 e 2] e [25, lemas 2,4 e 5, página 219] através de alguns de seus corolários.

Com efeito, o [1, teorema 1] e o [25, lema 4] são exatamente o ***Corolário 1*** do teorema, assim como [12, teorema 1] é o ***Corolário 2***.

Por outro lado, o ***Corolário 3*** generaliza [25, lemas 2 e 5] uma vez que esses lemas garantem que $h_K > 1$ para n positivo, livre de quadrados e da forma $n = (2tq)^2 - 1$, com q $\equiv_4 1$ e primo ou da forma $n = t^2 - 1 = 4ql + 3$, onde $q \equiv_{12} 1, 11$ é um primo tal que $q < 2t + 2$.

Finalmente, o ***Corolário 4*** é uma generalização de [24, teoremas 1 e 2] já que esses teoremas garantem que $h_K > 1$ nos seguintes casos: n primo da forma $(3(8t + 5))^2 - 2$, onde $12t + 7$ é primo e $t \geq 0$, ou n primo da forma $(3(8t + 7))^2 - 2$, com $12t + 11$ também primo e $t \geq 0$, respectivamente.

Observamos que os textos 24 e 25, a exemplo dos textos 1 e 14, tratam de corpos ciclotômicos.

4 - O número de classes de corpos quadráticos reais

A tabela que se segue, nos dá o ***número de classes*** de $Q(\sqrt{n})$ para diversos valores de n tais que $n \equiv_4 1$.

Tabela II

n	m	p	r	h_K
65	8	2	1	2
85	9	3	4	2
145	12	2	1	4
229	15	3	4	3
257	16	2	1	3
401	20	2	1	5
445	21	3	4	4
577	24	2	1	7
733	27	3	4	3
785	15	3	4	3
1093	16	2	1	3
1297	20	2	1	5
1601	21	3	4	4
1937	24	2	1	7
2029	45	3	4	7
2305	48	2	1	16
2605	51	3	4	8
2705	52	2	1	8
3137	56	2	1	9
3601	60	2	1	20
3973	63	3	4	6
4097	64	2	1	10
4765	69	3	4	6
5185	72	2	1	20
5629	75	3	4	12

n	m	p	r	$h_{\sqrt{}}$
6401	80	2	1	12
6565	81	3	4	8
7057	84	2	1	21
7573	87	3	4	9
7745	88	2	1	12
8465	92	2	1	14
8653	93	3	4	8
9217	96	2	1	18
9805	99	3	4	12

A tabela acima foi extraída de [17, página 10].

A próxima tabela, assim como a anterior, nos fornece o ***número de classes*** de $Q(\sqrt{n})$ para alguns valores de n, só que desta feita n é tal que $n \equiv_4 2,3$

Tabela III

n	r	m	$h_{\sqrt{}}$
10	1	3	2
15	-1	4	2
26	1	5	2
30	5	5	2
34	-2	6	2
35	-1	6	2

n	r	m	h_K
39	3	6	2
42	*6*	*6*	*2*
79	-2	9	3
82	1	9	4
122	1	11	2
170	1	13	4
223	-2	15	3
226	1	15	8
230	5	15	2
290	1	17	4
327	3	18	2
362	1	19	2
439	-2	21	5
442	1	21	8
530	1	23	4
579	3	24	4
626	1	25	4
727	-2	27	*5*
730	1	27	*12*
842	1	29	*6*
903	3	30	*4*
962	1	*31*	*4*
1087	-2	33	7
1090	1	33	12
1093	3	33	5

n	r	m	h_K
1226	1	35	10
1230	5	35	4
1370	1	37	4
1767	3	42	4
2210	1	47	8
2919	3	54	8
3722	1	61	10
4359	3	66	10
5626	1	75	28
5630	5	75	10
6562	1	81	16
6890	1	83	16
7567	-2	87	12
7922	1	89	8
8647	-2	93	13
9026	1	95	16
9219	3	96	12
9410	1	97	20
9799	-2	98	18

Esta tabela extraída de [17, página 12].

CAPÍTULO 3

NORMAS DE INTEIROS ALGÉBRICOS E NÚMERO DE CLASSES DE CERTOS CORPOS QUADRÁTICOS

Dada uma extensão de corpos numéricos L/K, trataremos, neste capítulo, do problema de se determinar a existência de um inteiro algébrico de K, que não uma unidade, que seja norma de um inteiro algébrico de L. Voltaremos, também, a tratar do número de classes de determinados corpos quadráticos estabelecendo desta feita condições suficientes para que um dado inteiro t seja divisor de h_K onde, novamente, h_K será o número de classes de $K = Q(\sqrt{n})$, onde n é um inteiro negativo, livre de quadrados, e da forma $n = r^2 - 4m^t$ ou $n = r^2 - a^t$, com a ímpar. Garantiremos, também, que se n é um inteiro negativo, livre de quadrados, tal que $n \not\equiv_8 5$ e $n \neq -1, -2, -7$, então o número de classes de $Q(\sqrt{n})$ é não trivial.

1 - Normas de inteiros algébricos

Dada uma extensão de corpos numéricos L/K, estabeleceremos nesta seção, através do próximo lema, condições necessárias e suficientes para que um dado inteiro algébrico de K, o qual não é uma unidade, possa ser a norma de um inteiro algébrico de L.

Usaremos a mesma simbologia dos capítulos anteriores, logo $\mathbf{I}_K$ e $\mathbf{I}_L$ denotarão, respectivamente, os anéis dos inteiros algébricos dos corpos numéricos dados K e L, enquanto que h_K e h_L denotarão, respectivamente, o número de classes dos mesmos corpos numéricos K e L.

Por outro lado, $\mathcal{U}_K$ e $\mathcal{U}_L$ denotarão, respectivamente, o grupo de unidades de $\mathbf{I}_K$ e $\mathbf{I}_L$. Além disso, se $\mathfrak{p}$ é um ideal primo de $\mathbf{I}_K$ e se $\mathcal{P}$ é um

ideal primo de $\mathbf{I}_L$ sobre $\mathfrak{p}$, isto é, tal que $\mathfrak{P} \cap \mathbf{I}_K = \mathfrak{p}$, então $f(\mathfrak{P}/\mathfrak{p})$ denotará o ***grau de inércia*** de $\mathfrak{P}$ de L sobre K.

Usaremos também o conceito de ***norma relativa*** de um ideal de ***L*** na extensão ***L/K*** e esta será denotada por $N_{L/K}(\,)$.

Sabemos que tal conceito coincide com o conceito de ***norma*** de um ideal, que denotaremos simplesmente por ***N( )***, quando $K = Q$ (nesse caso é costume se referir à essas normas como ***norma absoluta***). Finalmente, faremos uso, também, do símbolo $< \alpha >$ para denotar o ideal principal gerado por α.

Lema 8: *Sejam $K \subseteq L$ extensões finitas de Q tais que para cada unidade fundamental $u \in \mathcal{U}_K$ existe uma unidade $v \in \mathcal{U}_L$ tal que $N_{L/K}(v) = u$.*

Seja $\beta \in \mathbf{I}_K$, com $\beta = w\beta_1^{a_1} \cdot \ldots \cdot \beta_r^{a_r}$, onde cada β_i, $i = 1,\ldots,r$, é um elemento primo de $\mathbf{I}_K$ e $w \in \mathcal{U}_K$.

Então, existe $\alpha \in \mathbf{I}_L$ tal que $N_{L/K}(\alpha) = \beta$ se, e somente se, as seguintes condições forem satisfeitas:

(a) Para cada $i = 1,\ldots,r$ existem inteiros positivos b_{i_j} e ideais primos $\mathfrak{P}_{i_j}$ de $\mathbf{I}_L$ tais que $\mathfrak{P}_{i_j} \cap \mathbf{I}_K = \mathfrak{p}_i = < \beta_i >$ e $a_i = \sum_j b_{i_j} f_{i_j}$, onde $f_{i_j} = f(\mathfrak{P}_{i_j}/\mathfrak{p}_i)$ é o grau de inércia de $\mathfrak{P}_{i_j}$ de L sobre K.

(b) $\prod_{i=1}^{r} \prod_{i_j} \mathfrak{P}_{i_j}^{b_{i_j}}$ é principal.

Demonstração: $(\Rightarrow)$

Seja β de acordo com as hipótese exigidas e tome $\alpha \in \mathbf{I}_L$ tal que $N_{L/K}(\alpha) = \beta$.

Considere, agora a decomposição do ideal $< \alpha >$ como produto de ideais primos distintos $\mathfrak{D}_i$ de $\mathbf{I}_L$.

Assim,

$$< \alpha > = \mathfrak{D}_1^{b_1} \cdot \ldots \cdot \mathfrak{D}_s^{b_s},$$

donde segue que

$$N_{L/K}(< \alpha >) = N_{L/K}(\alpha . \mathbf{I}_L) = N_{L/K}(\alpha).\mathbf{I}_K = < \beta >,$$

conforme ***proposição A11 do Apêndice***.

Logo temos que

$$< \beta > = N_{L/K}(< \alpha >) = \prod_{j=1}^{s} N_{L/K}(\mathfrak{D}_j)^{b_j} \qquad (29)$$

Mas se para cada $j = 1, 2, ..., s$ tivermos $\mathcal{D}_j \cap \mathbf{I}_K = \mathcal{A}_j$ e $g_j = f(\mathcal{D}_j / \mathcal{A}_j)$ então a ***proposição A12 do Apêndice*** nos garante que $N_{L/K}(\mathcal{D}_j) = \mathcal{A}_j^{g_j}$, logo, de ***(29)*** segue que

$$< \beta > = \prod_{j=1}^{s} \mathcal{A}_j^{b_j \cdot g_j} . \qquad \textbf{(30)}$$

Observe que os $\mathcal{A}_j$, $j = 1, ..., s$, podem não serem todos distintos.
Neste caso, suponha, sem perda de generalidade, que $\mathcal{A}_1, \mathcal{A}_2, ..., \mathcal{A}_t$ ($t \leq s$) sejam os ideais distintos dentre os ideais $\mathcal{A}_1, \mathcal{A}_2, ..., \mathcal{A}_t, ..., \mathcal{A}_s$. Para cada $i = 1, 2, ..., t$ seja S_i o conjunto de $j \in \{1, 2, ..., s\}$ tal que $\mathcal{D}_j \cap \mathbf{I}_K = \mathcal{A}_i$.

Assim, segue de ***(30)*** que

$$N_{L/K}(< \alpha >) = < \beta > = \prod_{j=1}^{t} \mathcal{A}_j^{c_j} , \text{ onde } c_j = \sum_{i \in S_j} b_i \cdot g_i , \text{ para cada } j = 1, ..., t.$$

Então, pela unicidade de fatoração dos ideais de $\mathbf{I}_K$,o resultado segue se, depois de uma possível renumeração dos ideais $\mathcal{A}_i$, tomarmos $\mathcal{P}_i = \mathcal{A}_i$ e $a_i = c_i$, para $i = 1, ..., r$.

($\Leftarrow$)

Seja $\beta \in \mathbf{I}_K$, com $\beta = w\beta_1^{a_1} \cdot ... \cdot \beta_r^{a_r}$, onde cada β_i, $i = 1,...,r$, é um elemento primo de $\mathbf{I}_K$ e $w \in \mathcal{U}_K$.
Suponhamos que as condições **(a)** e **(b)** ocorram.
Por **(b)**, existe $\gamma \in \mathbf{I}_L$ tal que

$$< \gamma > = \prod_{i=1}^{r} \prod_{i_j} \mathcal{P}_{i_j}^{b_{i_j}} .$$

Observe que, então $N_{L/K}(< \gamma >) = \prod_{i=1}^{r} \prod_{i_j} N_{L/K}(\mathcal{P}_{i_j})^{b_{i_j}}$.

Mas, $N_{L/K}(\mathcal{P}_{i_j}) = \mathcal{P}_i^{f_{i_j}}$, segundo ***proposição A12 do Apêndice***, logo

$$N_{L/K}(< \gamma >) = \prod_{i=1}^{r} \prod_{i_j} \mathcal{P}_i^{f_{i_j} b_{i_j}} = \prod_{i=1}^{r} \mathcal{P}_i^{a_i} .$$

Desta forma,

$$N_{L/K}(\gamma) = u_1 \prod_{i=1}^{r} \beta_i^{a_i} , \text{ para alguma unidade } u_1 \in \mathcal{U}_K .$$

#***Afirmação:*** *Se $v \in \mathcal{U}_K$ então existe $\eta \in \mathcal{U}_L$ tal que $N_{L/K}(\eta) = v$.*

Demonstração: Observe, inicialmente, que se $\zeta \in K$ é uma raiz m-ésima de 1 (e o posto de $\mathcal{U}_K$ é $r \geq 1$) e $u \in \mathcal{U}_K$ é unidade fundamental, então ζu é também

unidade fundamental. Neste caso, por hipótese do ***lema***, existem β_1 e $\beta_2 \in \mathcal{U}_L$ tais que $N_{L/K}(\beta_1) = u$ e $N_{L/K}(\beta_2) = \zeta u$.
Com isso,

$$N_{L/K}(\beta_1^{-1} . \beta_2) = N_{L/K}(\beta_1^{-1}).N_{L/K}(\beta_2) = \zeta.$$

Agora de maneira geral, se $v \in \mathcal{U}_K$ então v é produto de uma raíz m-ésima de 1 por um número finito de unidades fundamentais de $\mathcal{U}_K$, logo qualquer $v \in \mathcal{U}_K$ é norma de algum elemento de $\mathcal{U}_L$.#

Sendo u_1 e w elementos de $\mathcal{U}_K$, pela afirmação anterior segue que existem η_1 e $\eta_2 \in \mathcal{U}_K$ tais que $N_{L/K}(\eta_1) = u_1$ e $N_{L/K}(\eta_2) = w$ e assim, como $N_{L/K}(\gamma) = u_1 \prod_{i=1}^{r} \beta_i^{a_i}$, segue que

$$N_{L/K}(\gamma . \eta_1^{-1} . \eta_2) = (u_1 \prod_{i=1}^{r} \beta_i^{a_i}).u_1^{-1}.w = w.\prod_{i=1}^{r} \beta_i^{a_i} = \beta.$$

Assim segue o resultado.■

Como, neste trabalho, estamos interessados fortemente nos ***corpos quadráticos***, temos, particularmente, o seguinte resultado:

Corolário 6: *Sejam* $L = \mathbf{Q}(\sqrt{n})$, $K = \mathbf{Q}$ *e* p *um primo racional. Então, existe* $\alpha = a + b\sqrt{n} \in \mathbf{I}_L$ *tal que* $p = N(\alpha)$ *se, e somente se, os primos* $\mathcal{P}$ *de* $\mathbf{I}_L$ *tais que* $\mathbf{Z} \cap \mathcal{P} = p\mathbf{Z}$ *são principais e* p *não é inerte em* L.

Demonstração: Nada temos a demonstrar, uma vez que sendo $p = p^1$ a decomposição de p em $\mathbf{I}_K$ segue que $r = 1$ e $a_1 = 1$, donde $f(\mathcal{P}/p.\mathbf{Z}) = 1$ para cada $\mathcal{P}$ primo de $\mathbf{I}_L$ tal que $\mathbf{Z} \cap \mathcal{P} = p.\mathbf{Z}$.□

Observamos que o lema anterior tem relevância em questões relativas ao número de classes de corpos quadráticos. Note que no decorrer da demonstração do ***teorema 3***, capítulo 1 e do ***teorema 4***, capítulo 2, usamos algumas vezes o fato de determinados inteiros racionais serem normas de inteiros algébricos e isso nos assegurou que $h_K > 1$. Desta forma veja, então, o seguinte resultado:

Corolário 7: *Seja* $\alpha \in \mathbf{I}_K$, $\alpha \notin \mathcal{U}_K$. *Se a condição (a) do Lema 8 é satisfeita, mas* α *não é norma de algum elemento de* $\mathbf{I}_L$ *então* $h_L > 1$.

Demonstração: De fato, a afirmação é trivialmente verificada, uma vez que nas condições acima o ideal indicado na condição **(b)** do ***Lema 8*** não será principal.□

2 - Certos corpos quadráticos imaginários

Nesta seção, estabeleceremos condições suficientes para a divisibilidade do número de classes de certos corpos quadráticos imaginários. Assim sendo, estaremos trabalhando com o corpo $\boldsymbol{Q(\sqrt{n})}$, onde n é um inteiro negativo livre de quadrados e da forma $n = r^2 - 4m^t$ ou $n = r^2 - a^t$, onde a é um inteiro ímpar.

Voltaremos, também, a tratar de corpos quadráticos $\boldsymbol{K}$ tais que número de classes, $\boldsymbol{h}_K$, é tal que $\boldsymbol{h}_K > 1$. Desta feita, porém, estaremos interessados em corpos quadráticos imaginários.

No primeiro resultado desta seção, estaremos trabalhando, fortemente, com elementos $\alpha = x + y\sqrt{n} \in \mathbf{I}_K$ tais que $m.d.c.(x, y) = 1$, se $x, y \in \boldsymbol{Z}$ ou $m.d.c.(2x, 2y) = 1$, se $x, y \notin \boldsymbol{Z}$. Tais elementos serão chamados de ***elementos primitivos***.

Teorema 5: *Sejam r, m e t inteiros positivos tais que m, t > 1 e $n = r^2 - 4m^t$ é livre de quadrados e negativo. Considere $K = \boldsymbol{Q}(\sqrt{n})$. Se m^c não é norma de um elemento primitivo de $\mathbf{I}_K$, sempre que c divide propriamente t, então $t \mid \boldsymbol{h}_K$.*

Demonstração: Observe, inicialmente, que r é ímpar, pois do contrário teríamos que $4 \mid n$, o que contraria o fato de n ser livre de quadrados. Assim $r^2 \equiv_4 1$ donde concluímos que $n \equiv_4 1$.

Considere agora a decomposição de m em fatores primos distintos $m = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$, com cada a_i inteiro positivo, para cada $i=1, 2, \ldots, s$.

#***Afirmação 1:*** *Para cada $i = 1, \ldots, s$, existe ideais primos $\mathcal{P}_i$ e $\mathcal{B}_i$ de $\mathbf{I}_K$, $\mathcal{P}_i \neq \mathcal{B}_i$, tais que $p_i \mathbf{I}_K = \mathcal{P}_i \mathcal{B}_i$.*

Demonstração: Se $p_i = 2$ então $n = r^2 - 8l$, para algum $l \in \boldsymbol{Z}$.
Mas sendo r ímpar, temos que $r \equiv_4 1$ ou $r \equiv_4 3$ e assim $r^2 \equiv_8 1$, donde $n \equiv_8 1$.

Assim, temos que o ideal $2 \cdot \mathbf{I}_K$ de $\mathbf{I}_K$ se decompõe em $\boldsymbol{K}$.

Se $p_i > 2$, então $p_i \nmid n$, pois do contrário $p_i \mid r$ e como $t > 1$ então n teria um fator quadrado.
Assim, como

$$\left(\frac{n}{p_i}\right)=\left(\frac{r^2-4m^t}{p_i}\right)=\left(\frac{r^2}{p_i}\right)=1,$$

segue que o ideal $p_i\cdot\mathbf{I}_K$ de $\mathbf{I}_K$ se decompõe em $\boldsymbol{K}$.

Assim em ambos os casos ($p_i = 2$ e $p_i \neq 2$) segue que $p_i\cdot\mathbf{I}_K = \mathscr{P}_i\mathscr{B}_i$, onde $\mathscr{P}_i$ e $\mathscr{B}_i$ são ideais primos distintos de $\boldsymbol{K}$, uma vez que o ideal $p_i\cdot\mathbf{I}_K$ se decompõe em $\boldsymbol{K}$.#

Suponha, agora, por absurdo, que $d = m.d.c.(t, \boldsymbol{h}_K)$ onde $t > d$, ou seja, suponha que $t \nmid \boldsymbol{h}_K$.

Por hipótese, como $d \mid t$ e $d \neq t$, m^d não é norma de um elemento primitivo em $\mathbf{I}_K$.

Por outro lado,

$$< m >^t = < \left(\frac{r-\sqrt{n}}{2}\right)\left(\frac{r+\sqrt{n}}{2}\right) >^t = < p_1^{a_1}\cdot\ldots\cdot p_s^{a_s} >^t =$$

$$= (\mathscr{P}_1^{a_1}\cdot\mathscr{B}_1^{a_1})^t\cdot\ldots\cdot(\mathscr{P}_s^{a_s}\cdot\mathscr{B}_s^{a_s})^t.$$

#***Afirmação 2 :*** *Para cada $i=1,\ldots,s$, temos que $\mathscr{P}_i$ divide somente um dentre os ideais $<\frac{r+\sqrt{n}}{2}>$ e $<\frac{r-\sqrt{n}}{2}>$.*

Demonstração: Suponha o contrário.

Então existe i, $i=1,\ldots,s$, tal que

$$r=\frac{r+\sqrt{n}}{2}+\frac{r-\sqrt{n}}{2}\in\mathscr{P}_i \text{ e } n=\left(\frac{r+\sqrt{n}}{2}-\frac{r-\sqrt{n}}{2}\right)^2\in\mathscr{P}_i.$$

Por outro lado, observe que $m.d.c.(r, n) = 1$ pois se $d = m.d.c.(r, n) \neq 1$, tome um inteiro primo q tal que $q \mid d$. Assim $q \mid r$ e $q \mid n$, donde $q \mid 4m^t$. Como r e n são ímpares, então $q \neq 2$, logo $q \mid m$ e como $t > 1$ teríamos necessariamente que $q^2 \mid n$, o que contraria a hipótese de n ser livre de quadrados.

Assim $m.d.c.(r, n) = 1$ e então $1 \in \mathscr{P}_i$, um absurdo, pois $\mathscr{P}_i$ é um ideal primo.

Portanto segue o resultado.#

Em vista da ***afirmação 2***, podemos supor que

$$<\frac{r+\sqrt{n}}{2}> = (\mathscr{D}_1^{a_1}\cdot\ldots\cdot\mathscr{D}_s^{a_s})^t,$$

onde , segundo uma escolha conveniente, $\mathscr{D}_i = \mathscr{P}_i$ ou $\mathscr{D}_i = \mathscr{B}_i$ para cada $i = 1,\ldots,s$.

Chame $\mathscr{A} = \mathscr{D}_1^{a_1}\cdot\ldots\cdot\mathscr{D}_s^{a_s}$ e assim teremos que $\mathscr{A}^t$ é principal.

Por outro lado, como $m.d.c.(t, h_K) = d$, segue que $ut + vh_K = d$, para inteiros v e u, donde

$$\mathcal{A}^d = (\mathcal{A}^t)^u (\mathcal{A}^{h_K v}).$$

Como $\mathcal{A}^{h_K v}$ é principal, temos que $\mathcal{A}^d$ é principal e assim existem a , $b \in \mathbf{Z}$, $a \equiv_2 b$ tais que

$$\mathcal{A}^d = \left(\frac{a + b\sqrt{n}}{2}\right).\mathbf{I}_K.$$

Logo, existe $\alpha = \frac{a + b\sqrt{n}}{2} \in \mathbf{I}_K$ tal que $|N_{L/K}(\alpha)| = N_{L/K}(\mathcal{A}^d)$.

Com isso, existe $\alpha \in \mathbf{I}_K$ tal que $N_{L/K}(\alpha) = m^d$, uma vez que $n < 0$.
Da mesma forma, temos que

$$<\frac{r - \sqrt{n}}{2}> = (\mathcal{V}_1^{a_1} \cdot \ldots \cdot \mathcal{V}_s^{a_s})^t,$$

onde segundo uma escolha conveniente, $\mathcal{V}_i = \mathcal{P}_i$ ou $\mathcal{V}_i = \mathcal{B}_i$ para cada $i = 1, \ldots, s$.

Se chamarmos de $\mathcal{W}^t = <\frac{r - \sqrt{n}}{2}> = (\mathcal{V}_1^{a_1} \cdot \ldots \cdot \mathcal{V}_s^{a_s})^t$, teremos que $\mathcal{W}^t$ é principal.

Assim, temos que $\mathcal{W}^d$ é também principal.

Por outro lado, $\mathcal{A}$ e $\mathcal{W}$ são comaximais, logo $\mathcal{A}^d$ e $\mathcal{W}^d$ são também comaximais, e assim,

$$\mathcal{A}^d + \mathcal{W}^d = \mathbf{I}_K .$$

Deixemos de lado, momentaneamente, essa igualdade e olhemos mais de perto para $\mathcal{W}^d$. Observamos então que:

#Afirmação 3: $\mathcal{W}^d = \left(\frac{a - b\sqrt{n}}{2}\right).\mathbf{I}_K$

Demonstração: Como $\mathcal{W}^d$ é principal, supor que, $\mathcal{W}^d = \left(\frac{c + d\sqrt{n}}{2}\right).\mathbf{I}_K$ onde $c, d \in \mathbf{Z}$ e $c \equiv_2 d$.

Considere, agora, σ: $\mathbf{Q}(\sqrt{n}) \to \mathbf{Q}(\sqrt{n})$ tal que

$$\sigma(x + y\sqrt{n}) = x - y\sqrt{n}.$$

Assim, temos que

$$\sigma(<\frac{r + \sqrt{n}}{2}>) = <\frac{r - \sqrt{n}}{2}>,$$

ou seja,

$$\sigma(\mathcal{A}^t) = \mathcal{W}^t .$$

Como $d \mid t$ então $t = d.g$, para algum $g \in \mathbf{Z}$, e com isso,

$$[\sigma(\mathcal{A}^d)]^g = [\mathcal{W}^d]^g$$

ou ainda

$$< \frac{a - b\sqrt{n}}{2} >^g = < \frac{c + d\sqrt{n}}{2} >^g. \qquad (31)$$

Mas, $n \equiv_4 1$ e $n < 0$, assim $n \leq -3$.
Mais ainda, $m > 1$ e $t > 1$, assim, $m^t \geq 4$ donde

$$n = r^2 - 4m^t \leq r^2 - 16.$$

Sendo então $n < -3$ temos que $\mathcal{U}_K = \{\pm 1\}$, logo de ***(31)*** segue que

$$\frac{c + d\sqrt{n}}{2} = \pm \frac{a - b\sqrt{n}}{2},$$

e assim segue o resultado. #

Com esses dados, teremos então que $\alpha = \frac{a + b\sqrt{n}}{2}$ é um elemento primitivo, pois do contrário existiria um primo p tal que $p \mid a$ e $p \mid b$ e neste caso teríamos então que $\mathcal{A}^d + \mathcal{W}^d \subseteq p.\mathbf{I}_K$, um absurdo !

Sendo α um elemento primitivo temos, então, que α é um elemento primitivo cuja norma é m^d, o que contraria a nossa hipótese uma vez que $d \mid t$.
Assim, segue o resultado. ■

Vejamos algumas consequências do teorema acima. Ainda denotaremos $\boldsymbol{K} = \boldsymbol{Q}(\sqrt{n})$.

Corolário 8: *Seja $n = r^2 - 4q^t$, negativo e livre de quadrados com t e q primos ímpares. Se um dos ideais primos $\mathcal{P}$ de $\mathbf{I}_U$ tais que $\boldsymbol{Z} \cap \mathcal{P} = q\,\boldsymbol{Z}$ não é principal, então $t \mid \boldsymbol{h}_K$.*

Demonstração: De fato, o resultado segue diretamente do ***teorema 5***, visto que pelo ***corolário 6*** temos que q não é norma de elementos de $\mathbf{I}_K$. □

O corolário que se segue é outra consequência do ***teorema 5*** e na prática mostra-se mais útil que o próprio teorema. Na ***tabela IV***, na ultima seção deste capítulo, encontram-se exemplos de aplicação deste resultado.

Corolário 9: *Seja $n = r^2 - 4m^t$, negativo e livre de quadrados, com r, m, t inteiros positivos tais que $m > 1$ e $t > 1$. Se $r^2 \leq 4m^{t-1}.(m - 1)$ então $t \mid \boldsymbol{h}_K$.*

Demonstração: Com efeito, o resultado segue do ***teorema 5*** se provarmos que m^c não é norma de um elemento primitivo de $\mathbf{I}_K$, para cada divisor próprio c de t, e observarmos que da hipótese $r^2 \leq 4m^{t-1}(m-1)$ segue que

$$n = r^2 - 4m^t \leq -4m^{t-1} < 0.$$

Suponha por absurdo que existe $a, b, c \in \boldsymbol{Z}$ tais que $c \mid t$, $c \neq t$, com $m.d.c.(a, b) = 1$ ou 2 e $a^2 - nb^2 = 4m^c$.
Nós temos que $-nb^2 < 4m^c$, donde segue que

$$4m^c > -b^2(r^2 - 4m^t) = 4m^t b^2 - r^2 b^2$$

ou ainda

$$r^2 b^2 + 4m^c > 4m^t b^2. \qquad (32)$$

Por outro lado, $b \neq 0$, pois se $b = 0$, como $m.d.c.(a, b) = 1$ ou 2 então $a = 1$ ou $a = 2$ e isto não é possível, visto que teríamos também $a^2 = 4m^c$ e $m > 1$.
Logo de ***(32)*** segue que

$$\frac{r^2}{4m^{t-1}} + \frac{1}{m^{t-c-1}b^2} > m. \qquad (33)$$

Mas por hipótese,

$$m - 1 \geq \frac{r^2}{4m^{t-1}} \qquad (34)$$

e como $t \geq c + 1$ segue que

$$1 \geq \frac{1}{m^{t-c-1}b^2}. \qquad (35)$$

Assim por ***(34)*** e ***(35)*** segue que

$$m = (m-1) + 1 \geq \frac{r^2}{4m^{t-1}} + \frac{1}{m^{t-c-1}b^2},$$

o que contraria ***(33)***.
Esta contradição estabelece, pois, o resultado. □

Observamos que a hipótese do corolário acima é, realmente, uma condição básica para que $t \mid \boldsymbol{h}_K$, pois, por exemplo, se $r = 11$, $m = 6$, $t = 2$ então $n = 11^2 - 4.6^2 = -23$ e neste caso $\boldsymbol{h}_K = 3$. Assim vemos que t não é divisor de $\boldsymbol{h}_K$.
Note que neste caso $r^2 = 121 > 4m^{t-1}(m-1) = 120$.

No caso de $r = 1$, o ***corolário 9*** produz o seguinte caso particular:

Corolário 10: *Seja $n = 1 - 4m^t$ um inteiro negativo livre de quadrados com $m > 1$ e t um primo. Então $t \mid \boldsymbol{h}_K$.*

O próximo resultado é um teorema com o mesmo teor do ***teorema 5***, só que agora trataremos com números inteiros negativos, livres de quadrados e da forma $n = r^2 - a^t$, onde a é um inteiro positivo ímpar. Mais uma vez, $\boldsymbol{K}$ denotará o corpo quadrático $\boldsymbol{Q}(\sqrt{n})$.

Teorema 6: *Seja n um inteiro negativo livre de quadrados da forma $n = r^2 - a^t$, com $r > 0$, $t > 1$ e $a > 1$ inteiros. Se a é ímpar e a^b não é norma de um elemento primitivo de $\mathbf{I}_K$ para cada divisor próprio b de t, então $t \mid \boldsymbol{h}_K$.*

Demonstração: Seja $a = p_1^{a_1} \cdot \ldots \cdot p_s^{a_s}$ a decomposição de a em fatores primos positivos.
Observe que para cada $i = 1, \ldots, s$, p_i é ímpar.
Mais ainda, observe também que

$$\left(\frac{n}{p_i}\right) = \left(\frac{r^2 - a^t}{p_i}\right) = \left(\frac{r^2}{p_i}\right) = 1.$$

Assim, segue que o ideal $p_i \cdot \mathbf{I}_K$ de $\mathbf{I}_K$ se decompõe em $\boldsymbol{K}$, ou seja, $p_i \cdot \mathbf{I}_K = \mathcal{P}_i \mathcal{B}_i$, onde $\mathcal{P}_i$ e $\mathcal{B}_i$ são distintos e são os únicos ideais primos de $\boldsymbol{K}$ cuja norma é p_i.
Por outro lado,

$$< a >^t = < (r - n^{\frac{1}{2}}) \cdot (r + n^{\frac{1}{2}}) > = < p_1^{a_1} \cdot \ldots \cdot p_s^{a_s} >^t =$$

$$= (\mathcal{P}_1^{a_1} \cdot \mathcal{B}_1^{a_1})^t \cdot \ldots \cdot (\mathcal{P}_s^{a_s} \cdot \mathcal{B}_s^{a_s})^t .$$

#***Afirmação:*** *Para cada $i=1,\ldots,s$, temos que $\mathcal{P}_i$ divide somente um dentre os ideais $< r + n^{\frac{1}{2}} >$ e $< r - n^{\frac{1}{2}} >$.*

Demonstração: Supor que existe i tal que

$$\mathcal{P}_i \mid < r + n^{\frac{1}{2}} > \quad \text{e} \quad \mathcal{P}_i \mid < r - n^{\frac{1}{2}} >.$$

Assim, teremos que

$$2r = (r + n^{\frac{1}{2}}) + (r - n^{\frac{1}{2}}) \in \mathcal{P}_i$$

e

$$4n = ((r + n^{\frac{1}{2}})) - ((r - n^{\frac{1}{2}}))^2 \in \mathcal{P}_i ,$$

donde $m.d.c.(2r, 4n) \in \mathcal{P}_i$.

Observe que $m.d.c.(r, n) = 1$ (Com efeito, se $m.d.c.(r, n) \neq 1$, existiria um primo q tal que $q \mid m.d.c.(r, n)$ e então $q \mid r$ e $q \mid n$, donde $q \mid a$. Assim, como $t > 1$ então $q^2 \mid n$ o que contraria o fato de n ser livre de quadrados.)

Então temos que $m.d.c.(2r, 4n) = 2$ e com isso $2 \in \mathcal{P}_i \subset \mathbf{I}_K$.

Como $\mathbf{I}_K$ é um domínio de Dedekind então podemos concluir que $2 \mid a$, um absurdo, visto que a é um inteiro ímpar.#

Em vista dessa afirmação, para uma escolha apropriada de $\mathcal{D}_i = \mathcal{P}_i$ ou $\mathcal{D}_i = \mathcal{B}_i$ para cada $i = 1,...,s$, temos que

$$<r + n^{\frac{1}{2}}> = (\mathcal{D}_1^{a_1} \cdot ... \cdot \mathcal{D}_s^{a_s})^t,$$

Chame $\mathcal{A} = \mathcal{D}_1^{a_1} \cdot ... \cdot \mathcal{D}_s^{a_s}$ e a demonstração segue análoga a demonstração do ***teorema 5***. ■

Temos para $n = r^2 - a^t$ negativo e livre de quadrados com $r > 0$, $t > 1$ e $a > 1$ inteiros e a ímpar, um resultado tão prático quanto o ***corolário 9*** do ***teorema 5***, a saber,

Corolário 11: *Seja n um inteiro negativo e livre de quadrados da forma* $n = r^2 - a^t$, *onde* $r > 0$, $a > 1$ *e* $t > 1$ *são inteiros. Se as condições*

(i) Se $a = 3$ *então* $t \neq 3$ *e* $t \neq 4$;

(ii) a é ímpar;

(iii) $r^2 \leq a^{t-1}(a - 1)$;

são simultaneamente satisfeitas então $t \mid \boldsymbol{h}_K$.

Demonstração: Com efeito, tendo em vista o teorema anterior, basta mostrarmos que a^b não é norma de um elemento inteiro primitivo, onde b é um divisor próprio qualquer de t.

Suponha, pois, que para algum divisor próprio b de t tenhamos que a^b seja norma de um inteiro primitivo.

Podemos então, sem perda de generalidade, supor que $4a^b = x^2 - ny^2$, para algum $x, y \in \boldsymbol{Z}$, tal que $m.d.c.(x, y) \leq 2$.

Observe que da igualdade $4a^b = x^2 - ny^2$, obtemos que $4a^b > -ny^2$, donde segue que

$$4a^b > -y^2(r^2 - a^t) = a^t y^2 - y^2 r^2$$

ou ainda

$$4a^b + y^2 r^2 > a^t y^2 .$$

Novamente, como no ***corolário 9***, como $m.d.c.(x, y) = 1$, ou 2, temos que $y \neq 0$, logo

$$a < \frac{4a^b + y^2r^2}{ya^{t-1}} = \frac{4}{y^2a^{t-b-1}} + \frac{r^2}{a^{t-1}} \qquad (36)$$

#***Afirmação:*** $4 \leq y^2a^{t-b-1}$.

De fato, suponha que $4 > y^2a^{t-b-1}$.

Então, necessariamente, teremos

$$y = 1,\ t - b - 1 = 1 \text{ e } a = 2 \text{ ou } a = 3.$$

Mas, por ***(ii)***, a é ímpar, logo teremos que $a = 3$.

Por outro lado, $b \mid t$, ou seja $t = kb$, para algum $k \in \boldsymbol{Z}$, então se $t - b = 2$ segue que $kb - b = 2$, donde $(k - 1)b = 2$, o que força que $k - 1 = 1$ e $b = 2$ ou $k - 1 = 2$ e $b = 1$, donde teremos que $b = 2$ e $t = 4$ ou $b = 1$ e $t = 3$.

Mas como $a = 3$, esses valores de t contradizem a hipótese ***(i)***.

Assim temos a desigualdade desejada.#

Em vista dessa afirmação, temos que

$$\frac{y^2a^{t-b-1}}{4} \geq 1,$$

e assim, segue de ***(36)*** que

$$a < \frac{r^2}{a^{t-1}} + 1,$$

o que contraria a hipótese ***(iii)***, uma vez que dela podemos concluir que

$$a \geq \frac{r^2}{a^{t-1}} + 1.$$

Assim temos que a^b não é norma de um elemento inteiro primitivo, onde b é um divisor próprio qualquer de t.

Logo do ***teorema 6*** segue o corolário.□

Na ***tabela V***, no final deste capítulo encontramos exemplos de aplicação deste resultado.

Finalizaremos esta seção abordando mais uma vez o problema do anel $\mathbf{I}_K$ de inteiros algébricos de determinados corpos quadráticos $\boldsymbol{K}$ não ser um ***domínio principal***.

Desta vez nos ocuparemos de certos corpos quadráticos imaginários e novamente mostraremos que o ***grupo de classes de ideais*** de $\mathbf{I}_K$, $\mathscr{C}\ell_K$, não é o trivial. Vejamos, pois o resultado pretendido:

Teorema *7: Se n é um inteiro negativo livre de quadrados é tal que* $n \not\equiv_8 5$ *e* $n \neq -1, -2$ *e* -7, *então* $\boldsymbol{h}_K > 1$.

Demonstração: Suponha que $h_K = 1$.

Como por hipótese $n \not\equiv_8 5$, então a decomposição de ideais em corpos quadráticos, ***Teorema A6*** do Apêndice, nos garante que o ideal $2.\mathbf{I}_K$ de $\mathbf{I}_K$ não é inerte em K. Assim, o ideal $2.\mathbf{I}_K$ se decompõe ou é ramificado em K, ou seja, $2.\mathbf{I}_K = \mathcal{P}^2$, onde $\mathcal{P}$ é o único ideal primo de $\mathbf{I}_K$ cuja norma é 2, ou $2.\mathbf{I}_K = \mathcal{P}.\mathcal{B}$, onde $\mathcal{P}$ e $\mathcal{B}$ são ideais primos distintos e são os únicos ideais primos de $\mathbf{I}_K$ cuja norma é 2.

De qualquer maneira, como estamos supondo $h_K = 1$, existe $\alpha \in \mathbf{I}_K$ tal que $|N(\alpha)| = N(\mathcal{P}) = 2$.

Mais ainda, como $n < 0$ então $N(\alpha) > 0$, e assim,

$$\exists \alpha \in \mathbf{I}_K \text{ tal que } N(\alpha) = 2. \qquad (37)$$

Desta forma, temos dois casos para discutir: $n \not\equiv_4 1$ e $n \equiv_4 1$.

Quando $n \not\equiv_4 1$ temos, pela afirmação ***(37)***, que existem $a, b \in Z$ tais que $a^2 - nb^2 = 2$, uma vez que neste caso

$$\mathbf{I}_K = \{ x + y\sqrt{n}, \text{ com } x,y \in Z \}.$$

Quando $n \equiv_4 1$, e aí na realidade, pela hipótese, $n \equiv_8 1$,temos pela afirmação ***(37)*** que existem $a, b \in Z$ tais que $a^2 - nb^2 = 8$, uma vez que neste caso

$$\mathbf{I}_K = \left\{ \frac{x + y\sqrt{n}}{2}, \text{ onde } x, y \in Z \text{ e } x \equiv_2 y \right\}.$$

Note que a equação $a^2 - nb^2 = 2$ tem sentido apenas para $n = -1$ e $n=-2$ (lembre que n é negativo), enquanto que a equação $a^2 - nb^2 = 8$ faz sentido para $n = -1, -2,...,-7$.

Como no primeiro caso temos $n \equiv_4 2,3$, então ambos valores -1 e -2 são verdadeiros.

No segundo caso, como $n \equiv_8 1$, temos que apenas o valor $n = -7$ faz sentido. Logo, $n = -1, -2$ e -7 e assim temos uma contradição, donde segue então o resultado.∎

3 - Comentários sobre a Literatura pesquisada referente a este Capítulo

Conforme já dissemos, o ***lema 8*** tem relevância em certas questões que envolvem o número de classes de determinados corpos quadráticos.

Um reforço a mais para essa afirmação poderá ser encontrados em [16, teorema 2.6, página 426].

Observamos que algorítimos finitos para encontrar números algébricos cuja norma é um dado número racional podem ser encontrados em [3, página 119] e [7]. Esses algorítimos assumem a existência de tais números algébricos.
Mais uma vez observamos que nesse sentido o ***lema 8*** difere desses dois resultados, uma vez que o mesmo fornece condições necessárias e suficientes para a existência de inteiros algébricos cuja norma é um dado inteiro algébrico.

O ***teorema 5*** generaliza [4, teorema] e resultados contidos em [8]. Mais precisamente, os ***corolários 8*** e ***10*** são resultados tratados em [4] e [8], respectivamente.

Notamos que a demonstração de [17, teorema 2.1, página 15] contém um erro de impressão na 9ª linha, a saber,

$$"r = \frac{r+n^{1/2}}{2} + \frac{r-n^{1/2}}{2} \text{ e } n = \left(\frac{r+n^{1/2}}{2} - \frac{r-n^{1/2}}{2}\right)^2 \text{ estão em } p_i .",$$

quando , na realidade, deveria ser

$$r = \frac{r+n^{1/2}}{2} + \frac{r-n^{1/2}}{2} \text{ e } n = \left(\frac{r+n^{1/2}}{2} - \frac{r-n^{1/2}}{2}\right)^2 \text{ estão em } \mathfrak{p}_i$$

($\mathfrak{p}_i$ ideal, enquanto que $p_i \in \boldsymbol{Z}$).

Por outro lado, existe na demonstração de [16, lema 2.1, página 13], a necessidade de se escrever o ideal $< \beta > = \prod_{k=1}^{s} \varphi_k^{b_k \cdot g_k}$ como produto de ideais distintos, uma vez que os φ_i's podem não ser em todos distintos. Para tanto, o autor usa o seguinte procedimento:

"Para um j fixado, seja S_j o conjunto de $k \in \{1,...,s\}$ tais que $\wp_k = \wp_i$. Assim, tem-se que $\prod_j \wp_j^{c_j} = < \beta >$, onde $c_j = \sum_{k \in S_j} b_k g_k$."

Observamos que por tal procedimento não é claro que o produto $\prod_j \wp_j^{c_j}$ tem como fatores apenas ideais distintos uma vez que j é um inteiro tal que $1 \leq j \leq s$ que é fixado sem restrição alguma.

4 - O número de classes de corpos quadráticos imaginários

As tabelas desta seção são aplicações do ***teorema 5*** e do ***teorema 6***.

Mais precisamente, a tabela a seguir é uma aplicação do ***teorema 5***, através do seu ***corolário 9*** .

Ela nos dá o ***número de classes*** de $K = Q(\sqrt{n})$ para diversos valores de n. Observe que no caso em que $r = 1$ (***corolário 10***), temos que $n \equiv_4 1$.

Tabela IV

r	m	t	$-n$	h_K
1	2	2	15	2
29	6	3	23	3
1	2	3	31	3
1	3	2	35	2
9	2	5	47	5
7	2	5	79	5
13	8	2	87	6
3	5	2	91	2
7	6	2	95	8
5	2	5	103	5
1	3	3	107	3
5	6	2	119	10
1	2	5	127	5
1	6	2	143	10
3	7	2	187	2
1	7	2	195	4
43	8	3	199	9
25	6	3	239	15
3	8	2	247	6
47	5	4	291	4

r	m	t	$-n$	h_{-n}
1	3	4	323	4
23	6	3	335	18
41	8	3	367	9
11	2	7	391	14
9	2	7	431	21
7	2	7	463	7
175	6	5	479	25
1	11	2	483	4
5	2	7	487	7
3	5	3	491	9
1	5	3	499	3
511	2	16	1023	16
31	2	9	1087	9
157	3	8	1595	16
11	2	9	1927	18
9	2	9	1967	36
7	2	9	1999	27
277	2	9	2003	9
3	2	9	2039	45
1	2	9	2047	18
349	2	15	9271	60

A tabela acima foi extraida de [17, página 17].

A próxima tabela nos dá exemplos de aplicações do ***teorema 6***, através de seu ***corolário 11***. Observe que para n temos valores negativos tais que $n \equiv_4 1,2$ ou 3.

Tabela V

r	a	t	$-n$	h_{-n}
2	5	2	21	4
2	15	2	221	16
2	15	3	3371	21
100	7	5	6807	40
20	3	7	1787	7
1	3	7	2186	42
7	3	7	2138	42

r	a	t	$-n$	h_v
19	3	7	1826	56
13	3	7	2018	28
100	3	9	9683	18
410	3	11	9047	88
1259	3	13	9242	78
3787	3	15	7538	60
2	3	8	6557	48

A tabela acima foi extraida de [17, página 18].

CONSIDERAÇÕES FINAIS

Os principais resultados obtidos neste trabalho foram:

(1) determinação da unidade fundamental dos corpos quadráticos $Q(\sqrt{m^2+r})$, onde $r \mid 4m$ e $-m < r \leq m$;

(2) condições suficientes para que o número de classes dos corpos quadráticos reais do tipo $Q(\sqrt{m^2+r})$, onde $r \mid 4m$ e $-m < r \leq m$, não seja trivial;

(3) condições necessárias e suficientes para que um dado inteiro algébrico, que não uma unidade, seja norma de um inteiro algébrico, numa dada extensão de corpos numéricos;

(4) condições suficientes para a divisibilidade do número de classes do corpo quadrático imaginário $Q(\sqrt{n})$, onde $n = r^2 - 4m^t$, por inteiros racionais;

(5) condições suficientes para a divisibilidade do número de classes do corpo quadráticos imaginário $Q(\sqrt{n})$, onde $n = r^2 - a^t$, com a ímpar, por inteiros racionais;

(6) condições suficientes para que o número de classes dos corpos quadráticos imaginários não seja trivial.

Observamos, novamente, que embora estes resultados digam respeito à Teoria Algébrica dos Números, pois tratam de números de classes, de normas e de unidades, alguns resultados intermediários sobre equações diofantinas foram também estabelecidos.

Gostaríamos de mencionar que podemos encontrar em [3] maneiras de se calcular efetivamente o número de classes de determinados corpos de números algébricos. No entanto, praticamente tal cálculo só é possível em casos bem simples.

Além disso, podemos encontrar em [3] ou em [15] fórmulas para se obter o número de classes para quaisquer corpos númericos, e em particular fórmulas explícitas quando se tratar de corpos quadráticos. Tal

abordagem é feita através de métodos analíticos sendo nela utilizada a função ***Zeta de Dedekind***.

Finalizamos mencionando, que trabalhos recentes ainda tratam do problema de se determinar o número de classes de corpos quadráticos do tipo $Q(\sqrt{m^2 + r})$, com $r / 4m$ e $-m < r \leq m$, estudados neste trabalho. Um exemplo dessa afirmação é o artigo de *Ming-Guang Leu,* publicado no Bull. London Math. Soc., **24** (1992), 309-312, no qual são estabelecidas condições suficientes para que o corpo quadrático $Q(\sqrt{m^2 + 4})$ tenha número de classes igual a 2.

APÊNDICE

Discutiremos neste apêndice alguns dos pré requisitos necessários para a leitura deste trabalho, enfocando as definições e resultados usados no decorrer do mesmo. Assumiremos, sem qualquer citação, as noções básicas sobre corpos, anéis e módulos e as propriedades elementares de congruências.

1 - Equações Diofantinas de 2° grau.

Definição 1: Seja $f(X_1, X_2, ..., X_n)$ um polinômio nas variáveis $X_1, X_2, ..., X_n$ com coeficiente inteiros ou racionais. A equação

$$f(X_1, X_2, ..., X_n) = 0 \qquad \textit{(A1)}$$

é chamada de ***equação Diofantina de grau n***.
Neste caso, a n-upla $(x_1, x_2, ..., x_n)$ de números inteiros ou racionais tal que $f(x_1, x_2, ..., x_n) = 0$ é dita uma ***solução*** para ***(A1)***.

Em geral, as ***equações (A1)*** são tratadas de forma que seus coeficientes sejam inteiros e também são consideradas apenas as soluções inteiras. Particularmente, neste trabalho, utilizaremos ***equações diofantinas do 2° grau*** do tipo:

$$X^2 - nY^2 = t, \text{ com } n, t \in \mathbf{Z}. \qquad \textit{(A2)}$$

No caso dos inteiros x, y serem tais que $x^2 - ny^2 = t$, trataremos o par ordenado solução (x, y) como a solução $\alpha = x + y\sqrt{n}$ de ***(A2)***.

A definição a seguir pode ser encontrada no próprio texto:

Definição 2: Se a equação ***(A2)*** tem solução, dentre todas suas soluções, a solução $\alpha = x + y\sqrt{n}$, tal que x é inteiro positivo e y é o menor inteiro positivo possível, é dita ***solução minimal*** ou ***solução fundamental*** de ***(A2)***.

2 - Resíduos quadráticos.

Definição 3: Seja n um inteiro não nulo e a um inteiro tal que $m.d.c(a, n) = 1$. Dizemos que a é um resíduo quadrático módulo n se, e somente se, $x^2 \equiv_n a$ é solúvel.

Observamos que estaremos denotando por $a \equiv_n b$ o fato de a ser côngruo a b módulo n, onde a, b, n são números inteiros quaisquer, com $n > 0$.

Definição 4: Seja p um primo ímpar. Definimos o ***símbolo de Legendre*** da seguinte maneira:

$$\left(\frac{a}{p}\right) = 1, \text{ quando } a \text{ é resíduo quadrático módulo } p$$

e

$$\left(\frac{a}{p}\right) = -1, \text{ quando } a \text{ não é resíduo quadrático módulo } p.$$

Propriedades elementares do símbolo de Legendre:

Sejam p e q primos ímpares distintos e a e b inteiros relativamente primos com p. Então:

1-) Se $a \equiv_p b$ então $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

2-) $\left(\frac{a}{p}\right).\left(\frac{b}{p}\right) = \left(\frac{a.b}{p}\right)$.

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

4-) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

5-) $\left(\frac{q}{p}\right).\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1).(q-1)}{4}}$.(***lei da reciprocidade quadrática)***

As demonstrações destas (e outras) propriedades do ***Símbolo de Legendre*** podem ser encontradas em [20, páginas 135-139 e 143], [21, páginas 73-79] e, finalmente em [23, páginas 90-93].

O símbolo de Legendre $\left(\frac{n}{p}\right)$ é definido apenas para p primo ímpar. Uma generalização desse símbolo, e válida para qualquer número ímpar n, é dada pela seguinte definição:

Definição 5: Seja a um inteiro qualquer e n um número inteiro ímpar tal que $n > 0$ e $m.d.c.(n, a) = 1$. Se $n = p_1 \cdot p_2 \cdot \ldots \cdot p_r$ é a decomposição de n como produto de primos (não necessariamente distintos), então o ***Símbolo de Jacobi*** é definido por

$$\left[\frac{a}{n}\right] = \prod_{j=1}^{r}\left(\frac{a}{p_j}\right),$$

onde $\left(\frac{a}{p_j}\right)$ é o símbolo de Legendre.

Propriedades elementares do símbolo de Jacobi:

Sejam n e m ímpares positivos tais que $m.d.c(n.m, a.b) = 1$. Então:

1-) $\left[\frac{a}{n}\right].\left[\frac{a}{n}\right] = \left[\frac{a}{n.m}\right]$.

2-) $\left[\frac{a}{n}\right].\left[\frac{b}{n}\right] = \left[\frac{a.b}{n}\right]$.

3-) Se $a \equiv_p b$ então $\left[\frac{a}{n}\right] = \left[\frac{b}{n}\right]$.

4-) $\left[\frac{-1}{n}\right] = (-1)^{\frac{n-1}{2}}$.

5-) $\left[\frac{2}{n}\right] = (-1)^{\frac{n^2-1}{8}}$.

6-) No caso de $m.d.c.(n,m) = 1$, então

$$\left[\frac{n}{m}\right].\left[\frac{m}{n}\right] = (-1)^{\frac{(n-1).(m-1)}{4}}$$ (reciprocidade quadrática).

As demonstrações destas (e outras) propriedades do ***Símbolo de Jacobi*** podem ser encontradas em [20, páginas 145-148] e [21, páginas 80-83]

3 - Domínios de Dedekind.

Estaremos, particularmente, interessados nesta seção em corpos quadráticos, isto é, sub corpos $K \subseteq C$ tais que $[K:Q] = 2$, ou ainda corpos K tais que $K = Q(\sqrt{n})$, para algum $n \in Z$ livre de quadrados. Se $n < 0$ K é dito um corpo quadrático imaginário e se $n > 0$ teremos um corpo quadrático real.

Definição 6 : Seja S um anel e R um sub anel de S. Um elemento $\alpha \in S$ é dito um ***inteiro sobre*** R se α for raíz de algum polinômio mônico cujos coeficientes estão em R. De outra maneira, α será um inteiro sobre R se existir um polinômio $f(X) \in R[X]$ tal que $f(\alpha) = 0$. Particularmente, se $S = C$ e $R = Z$, dizemos que os números inteiros sobre Z são ***inteiros algébricos***.

Se $K = Q(\sqrt{n})$ denotaremos por $\mathbf{I}_K$ o conjunto dos inteiros algébricos de K, conjunto este que é na realidade um sub anel de K que contém Z, conforme [6, página 11, corolário 1.3].

Proposição A1: Seja $K = Q(\sqrt{n})$, onde n é um inteiro livre de quadrados. Então
(a) Se $n \equiv_4 2$ ou $n \equiv_4 3$ então o anel de inteiros de K, $\mathbf{I}_K$, é o conjuntos dos elementos $a + b\sqrt{n}$, onde $a, b \in Z$.
(b) Se $n \equiv_4 1$ então o anel de inteiros de K, $\mathbf{I}_K$, é o conjuntos dos elementos $\frac{a+b\sqrt{n}}{2}$, onde a e b são inteiros racionais de mesma paridade.
A demonstração deste fato pode ser encontrada em [6, página 21, teorema 2.3] ou em [23, página 42, teorema 1].

Definição 7: Seja L um corpo numérico. Chamamos, por abuso de linguagem, de ***unidades de L*** aos elementos invertíveis do anel de inteiros de L.

Estas unidades formam um grupo multiplicativo, denotado por $\mathcal{U}_L$, e podem ser caracterizadas à partir de suas normas, conforme a proposição à seguir:

Proposição A2: Seja L um corpo numérico. Dizemos que um elemento $\alpha \in L$ é uma unidade se, e somente se, α for um inteiro algébrico de L e tiver norma igual a ± 1.

A demonstração desta proposição pode ser encontrada em [23, página 70, proposição 1].

Definição8: Dados um corpo numérico L e seu anel de inteiros $\mathbf{I}_L$, uma unidade de L é dita fundamental se ela faz parte de uma base livre da parte livre de $\mathcal{U}_L$. Particularmente, se u é uma unidade fundamental de L e ζ é uma raíz m-ésima de 1 então ζu é também uma unidade fundamentalde L.

As próximas definições são essenciais para a demonstração do teorema da decomposição de ideais em corpos quadráticos, resultado este tão utilizado neste trabalho.

Definição9: Seja L/K uma extensão finita de grau n. Para cada $\alpha \in L$, definimos o ***polinômio característico*** de α em relação a L/K , e denotamo-lo por $f_{\alpha,L/K}(X)$, como:

$$f_{\alpha,L/K}(X) = Det(X.\delta_{ij} - a_{ij}),$$

onde (a_{ij}) é a matriz de elementos a_{ij} de K tal que

$$\alpha.\beta_i = \sum_{j=1}^{n} a_{ij} \cdot \beta_j,$$

com $\beta_1, ...,\beta_n$ uma base de L sobre K e δ_{ij} o ***símbolo de Kronecker***.
(Demonstra-se que $f_{\alpha,L/K}(X)$ independe da escolha da base $\beta_1, ...,\beta_n$.)

A partir dessa definição, e com as mesmas notações dela, temos a definição que se segue:

Definição 10: Seja $f_{\alpha,L/K}(X) = X^n + f_1X^{n-1} + f_2X^{n-2} + ... + f_n$. Definimos o ***traço*** e a ***norma*** de α em relação a L/K, respectivamente por,

$$\mathcal{T}_{L/K}(\alpha) = -f_1 = \sum_{i=1}^{n} a_{ii}$$

e

$$\mathcal{N}_{L/K}(\alpha) = (-1)^n . f_n = det(a_{ij})$$

No caso de $L = Q(\sqrt{n})$ temos, para $\alpha = a + b\sqrt{n} \in L$, que

$$f_{\alpha,L/K}(X) = X^2 - 2aX + (a^2 - nb^2),$$

donde

$$\mathcal{T}_{L/K}(\alpha) = 2a \quad \text{e} \quad \mathcal{N}_{L/K}(\alpha) = a^2 - nb^2 .$$

Tal norma é tratada neste trabalho apenas por $N(\alpha)$.

A próxima definição é essencial para a verificação da ramificação ou não ramificação de um ideal de $\mathbf{I}_K$.

Definição 11: Seja L/K uma extensão finita de grau n e sejam $\alpha_1, \ldots, \alpha_n \in L$. Definimos o ***discriminante*** de $\alpha_1, \ldots \alpha_n$ como

$$disc_{L/K}(\alpha_1,\ldots,\alpha_n) = det(\mathcal{T}_{L/K}(\alpha_i.\alpha_j)) \in K.$$

Os discriminantes de diferentes *n-uplas* se relacionam segundo a seguinte relação:

Proposição A3: Sejam $\alpha_1,\ldots,\alpha_n \in L$ tais que $\gamma_i = \sum_{j=1}^{n} c_{ij}\alpha_j$, com $c_{ij} \in K$.

Então,

$$disc_{L/K}(\gamma_1,\ldots,\gamma_n) = (det(c_{ij}))^2 . disc_{L/K}(\alpha_1,\ldots,\alpha_n).$$

A demonstração deste fato pode ser encontrada em [6, página 39, afirmação 4.1].

Se nos restringirmos ao caso em que $L \subseteq C$ e $[L:Q] = n$ temos uma afirmação mais forte a respeito do discriminante de bases integrais de L. Lembramos que uma base integral de L, quando L é uma extensão finita de Q, é qualquer base do anel de inteiros de L.

Observe que tem sentido falarmos de base para $\mathbf{I}_L$, uma vez que neste caso $\mathbf{I}_L$ é um ***Z - módulo livre de posto n,*** conforme [6, página 52, corolário 5.5] ou [23, teorema 1, página 47]. Vejamos então o resultado sobre discriminante de bases integrais:

Proposição A4: Os discriminantes de todas as bases integrais de L coincidem.

A demonstração deste resultado pode ser encontrada em [6, página 44, afirmação 4.11].

Tendo em vista esta proposição, e sabendo que qualquer corpo de L tal que $L \subseteq C$ e $[L:Q] = n$ tem base integral $\beta_1, \ldots, \beta_n$, chamamos o discriminante $disc_{L/K}(\beta_1, \ldots, \beta_n)$ (que não depende da escolha desta base) de ***discriminante absoluto do corpo L*** e denotamo-lo por $\mathbf{d}_L$. No caso particular de $L = Q(\sqrt{n})$, com n livre de quadrados, temos que

$$\mathbf{d}_L = 4n, \text{ quando } n \equiv_4 2 \text{ ou } n \equiv_4 3$$

e

$$\mathbf{d}_L = n. \text{ quando } n \equiv_4 1.$$

Sabemos que para alguns corpos quadráticos L o anel de inteiros $\mathbf{I}_L$ nem sempre é fatorial (o exemplo mais clássico dessa afirmação talvez seja o anel de inteiros de $Q(\sqrt{-5})$). Dessa forma, a fatoração única em potências de elementos irredutíveis nem sempre é válida. Assim, surge a necessidade de outra forma de fatoração: a fatoração de um ideal não nulo de $\mathbf{I}_L$ em potências de ideais primos. Para alcançarmos tal tipo de fatoração trabalharemos, inicialmente com um caso particular de domínio: os ***Domínios Noetherianos***, conforme definição a seguir:

Definição 12: Seja R um anel. Um R- módulo M é ***Noetheriano*** quando todos seus sub módulos forem finitamente gerados e um anel A é ***Noetheriano*** se como A- modulo ele for Noetheriano.

Demonstra-se que para um R- módulo M ser Noetheriano é necessário e suficiente que o conjunto $\mathscr{M}$ dos sub módulos de M satisfaça a condição da ***cadeia ascendente***, isto é, para toda sequência $(m_j)_{j \in N}$ tal que $m_1 \leq m_2 \leq m_3 \leq \ldots$ existe $n \in N$ tal que $m_n = m_{n+1} = \ldots$.

Outra condição necessária e suficiente para que M seja Noetheriano é que o conjunto $\mathscr{M}$ dos sub módulos de M satisfaça a ***condição maximal***, isto é, para todo sub conjunto não vazio $\mathscr{B} \subseteq \mathscr{M}$ existe um $b_0 \in \mathscr{B}$ tal que para qualquer $b \in \mathscr{B}$ tenhamos $b \leq b_0$.

Para demonstração dessa dupla equivalência ver [6, página 63, afirmação 7.1] ou [23, página 24, teorema 1].

Num domínio Noetheriano, temos a garantia da fatoração em elementos irredutíveis, mesmo que tal domínio não seja fatorial:

Teorema A1: Seja R um domínio Noetheriano. Se $r \in R$ então existem $p_1, p_2, \ldots, p_n$ elementos irredutiveis de R tais que $r = u \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_n$, onde u é um elemento invertível de R.

Para demonstração deste teorema ver [6, página 67, Teorema 7.1].

Garantiremos agora que em $\mathbf{I}_L$ temos a fatoração de um elemento em produto de elementos irredutíveis:

Proposição A5: Seja L um corpo de números algébricos. Todo sub anel de $\mathbf{I}_L$ é Noetheriano como anel e como Z- módulo.

A demonstração deste fato pode ser encontrada em [6, página 68, corolário 7.12].

Assim como temos a unicidade da fatoração de elementos, de determinados anéis, em potências de elementos irredutíveis veremos que também temos unicidade de fatoração de um ideal não nulo em potências de ideais primos, em determinados anéis.
Isso é possível dentro dos ***Domínios de Dedekind***, dos quais $\mathbf{I}_L$ é um caso particular, onde $\boldsymbol{L}$ é um corpo de números algébricos.

Definição 13: Um domínio R é dito um ***Domínio de Dedekind*** se for integralmente fechado, Noetheriano e todo ideal primo não nulo for maximal.

Proposição A6: Seja L um corpo de números algébricos. Então $\mathbf{I}_L$ é um domínio de Dedekind.
Para demonstração, vide [6, página 70, Corolário 8.2].

A fatoração nos domínios de Dedekind a que nos referimos acima é garantida pelo seguinte teorema:

Teorema A2: Seja R um domínio de Dedekind. Então para qualquer ideal não nulo $\mathscr{I}$ de R existem ideais primos, $\mathscr{P}_1$, $\mathscr{P}_2$,..., $\mathscr{P}_n$, não nulos de R tais que

$$\mathscr{I} = \mathscr{P}_1 \cdot \mathscr{P}_2 \cdot \ldots \cdot \mathscr{P}_n .$$

Este teorema encontra-se demonstrado em [6, página 73, afirmação 8.7 b].

Observe que os ideais indicados no teorema acima não são, necessariamente distintos e também que a fatoração garantida pelo mesmo teorema ainda não é única. Esssa unicidade será garantida pelo próximo resultado:

Teorema A3: Seja R um domínio de Dedekind. Então para todo ideal não nulo $\mathscr{I}$ de R, existem ideais primos distintos de R, $\mathscr{P}_1$, $\mathscr{P}_2$,..., $\mathscr{P}_n$, e números naturais k_1, ...,k_n, todos univocamente determinados, tais que

$$\mathscr{I} = \prod_{i=1}^{n} \mathscr{P}_i^{k_i} .$$

Observamos que esse resultado pode ser estendido aos ideais fracionários que definiremos na próxima seção.

A demonstração deste teorema, inclusive a extensão aos ideais fracionários, pode ser encontrada [6, página74, teorema 8.8].

4 - Grupo de classes de ideais e número de classes.

Nesta seção, R é um domínio, $\boldsymbol{K}$ seu corpo de frações, e iremos considerar os submódulos do R- módulo $\boldsymbol{K}$.

Definição 14: Um submódulo M de $\boldsymbol{K}$ é dito um ***ideal fracionário*** de R de existir $d \in R \setminus \{0\}$ tal que $d \cdot M \subseteq R$. Neste caso, $d \cdot M$ é um ideal $\mathscr{I}$ de R tal que $M = d^{-1} \cdot \mathscr{I}$.

Observamos que os ideais de R são os ideais fracionários que estão contidos em R.

Se $\mathscr{M}$ é conjunto dos submódulos de $\boldsymbol{K}$ e $\mathscr{F}$ é o conjunto dos ideais fracionários de R temos que $\mathscr{F} \subset \mathscr{M}$, mais ainda, $\mathscr{M}$ é um monóide comutativo e R é a unidade tanto de $\mathscr{M}$ como de $\mathscr{F}$. Podemos afirmar algo mais forte que isso, para tanto necessitamos de mais uma definição:

Definição 15: Seja $M \in \mathscr{M}$. Dizemos que M é invertível se existir um $N \in \mathscr{M}$ tal que $M \cdot N = R$.

Conforme [6,página 71, afirmação 8.5], o inverso N de M é único e é usualmente denotado por M^{-1}. Este mesmo resultado garante também que os submódulos invertíveis de $\boldsymbol{K}$ são os fracionários de R. No entanto nada nos garante que, em geral, todo ideal fracionário seja invertível. Denotemos, então, por $\mathscr{G}$ o conjunto dos ideais fracionários invertíveis e observe que $\mathscr{G}$ é um grupo multiplicativo.

Observe que todo ideal principal fracionário não nulo, $x \cdot R$, onde $x \in \boldsymbol{K}$, é invertível e $(x \cdot R)^{-1} = x^{-1} \cdot R$. Assim se denotamos por $\mathscr{P}$ o conjunto dos ideais fracionários principais não nulos, notamos que $\mathscr{P}$ é sub grupo de $\mathscr{G}$.

O próximo resultado, cuja demonstração pode ser encontrada em [6, página 74, teorema 8.9], garantirá que em domínios de Dedekind temos que $\mathscr{G} = \mathscr{F}$:

Teorema A4: Seja R um domínio. Então as afirmações abaixo são equivalentes:
(a) R é um domínio de Dedekind.
(b) Todo $M \in \mathscr{F}$ é invertível.

Observe que com esse resultado, temos na realidade que em domínios de Dedekind $\mathscr{G} = \mathscr{F}$ é um grupo abeliano e assim temos que num domínio de Dedekind o conjunto $\mathscr{P}$ de ideais fracionários principais é um subgrupo do grupo abeliano $\mathscr{G} = \mathscr{F}$. Depois dessa observação faz sentido a próxima definição. Ela introduzirá um importante invariante numérico que é o ***número de classes***:

Definição 16: Em um domínio de Dedekind R, o grupo quociente $\mathscr{Cl}_{\mathbf{K}} = \mathscr{G} / \mathscr{P}$ é denominado o ***grupo de classes de ideais*** de R. A ordem, não necessariamente finita, de $\mathscr{Cl}_{\mathbf{K}}$ é denominada ***número de classes*** de R, e é denotada por $\boldsymbol{h}_{\mathrm{K}}$.

Consideremos agora o caso particular em que o domínio de Dedekind R é o anel de inteiros $\mathbf{I}_{\mathrm{L}}$, onde $\boldsymbol{L}$ é um corpo de números algébricos tal que $[\boldsymbol{L}:\boldsymbol{Q}] = n$. Neste caso dizemos que $\boldsymbol{h}_{L} = \boldsymbol{h}_{\mathrm{R}}$ e podemos garantir que esse número é finito:

Teorema A5: Se R é o anel de inteiros $\mathbf{I}_{\mathrm{L}}$, onde $\boldsymbol{L}$ é um corpo de números algébricos tal que $[\boldsymbol{L}:\boldsymbol{Q}] = n$ então o número de classes $\boldsymbol{h}_{L}$ é finito.

Esse teorema tem uma importante consequência imediata:

Corolário A1: Se $\mathscr{I}$ é um ideal não nulo de $\mathbf{I}_{\mathrm{L}}$ então $\mathscr{I}^{h_L}$ é um ideal principal.

Em vista da discussão acima, podemos concluir que uma condição necessária e suficiente para que $\mathbf{I}_{\mathrm{L}}$ seja principal é que o grupo de classes de ideais, $\mathscr{Cl}$, se reduza ao elemento neutro.

5 - Decomposição em corpos quadráticos.

Nesta seção $\boldsymbol{L}$ denotará, inicialmente, um corpo de números algébricos tal que $[\boldsymbol{L}:\boldsymbol{Q}] = n$ e $R = \mathbf{I}_{\mathrm{L}}$.

Como R é um domínio de Dedekind, para qualquer ideal primo não nulo $\mathscr{P}$ de R temos que $R / \mathscr{P}$ é um corpo.

Então dentro desse contexto temos o seguinte resultado:

Proposição A7: Seja $\mathcal{P}$ um ideal primo de $R = \mathbf{I}_L$. Então,
(a) $\mathcal{P} \cap \boldsymbol{Z} = p\boldsymbol{Z}$, onde p é o único número primo em $\mathcal{P}$.
(b) $R/\mathcal{P}$ é uma extensão finita do corpo $\boldsymbol{F}_p$, de grau $[R/\mathcal{P}:\boldsymbol{F}_p] \leq n$.
A demonstração deste fato é encontrada em [6, página 83, afirmação 9.3].

Em vista do ítem ***(b)*** do resultado acima, temos a seguinte definição:

Definição 17: O grau de $[R/\mathcal{P}:\boldsymbol{F}_p]$ é chamado de ***grau de inércia de*** $\mathcal{P}$ e é, usualmente, denotada por $f(\mathcal{P})$.

Mais uma definição se faz necessária:

Definição 18: Seja $\mathcal{I}$ um ideal de não nulo de R. Chamamos de norma do ideal $\mathcal{I}$, e denotamos por $N(\mathcal{I})$, ao seguinte número

$$N(\mathcal{I}) = \#(R/\mathcal{I}).$$

A proposição abaixo, cuja demonstração pode ser encontrada em [6, página 84, afirmação 9.4], garante, entre outras afirmações, que a norma de um ideal é sempre finita:

Proposição A8: Seja $\boldsymbol{L}$ um corpo de números algébricos tal que $[\boldsymbol{L}:\boldsymbol{Q}] = n$ e $R = \mathbf{I}_L$. Então:
(a) Para todo ideal primo não nulo $\mathcal{P}$ de R temos que $N(\mathcal{P}) = \mathcal{P}^f$, onde f é o grau de inércia de $\mathcal{P}$ e p o único número primo em $\mathcal{P}$.
(b) Para todo ideal não nulo $\mathcal{I}$ de R temos que $N(\mathcal{I}) \in \boldsymbol{N} - \{0\}$; em particular, $N(\mathcal{I}) = 1$ se e somente se $\mathcal{I} = R$.
(c) Para quaisquer ideais não nulos $\mathcal{I}$ e $\mathcal{A}$ de R temos que

$$N(\mathcal{I} \cdot \mathcal{A}) = N(\mathcal{I}).N(\mathcal{A}).$$

O próximo resultado nos dá uma importante igualdade referente a decomposição em $\mathbf{I}_L$ dos ideais $p\cdot\mathbf{I}_L$, com p primo racional.
Sua demonstração pode ser encontrada em [6, página 86, corolário 9.8] ou em [23, página 83,teorema 1].

Proposição A9: Seja p um número primo.

Seja também $p\cdot\mathbf{I}_L = \mathcal{P}_1^{e_1}\cdot\mathcal{P}_2^{e_2}\cdot\ldots\cdot\mathcal{P}_r^{e_r}$ a fatoração de $p\cdot\mathbf{I}_L$ em ideais primos distintos $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_r$, com $e_1 \geq 1, \ldots, e_r \geq 1$.
Então:

(a) $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_r$ são os únicos ideais primos $\mathcal{P}$ de R tais que $p \in \mathcal{P}$.

(b) $\sum_{j=1}^{r} e_j \cdot f_j = n$, onde f_j é o grau de inércia de $\mathcal{P}_j$, para $j = 1, \ldots, r$.

Vejamos agora a ***lei da decomposição*** em corpos quadráticos $\boldsymbol{L} = \boldsymbol{Q}(\sqrt{n})$. Através dela, teremos a decomposição de números primos em $\boldsymbol{L}$, isto é, teremos a fatoração de $p\cdot\mathbf{I}_L$ em ideais primos de $\mathbf{I}_L$. Antes de enunciarmos a ***lei da decomposição***, observe que a fórmula $\sum_{j=1}^{r} e_j \cdot f_j = 2$, dada pelo ítem ***(b)*** da ***proposição A9*** quando $\boldsymbol{L} = \boldsymbol{Q}(\sqrt{n})$, mostra que $r \leq 2$ e que apenas um, dentre os casos abaixo, pode ocorrer:
(1) $r = 1$, $e_1 = 2$ e $f_1 = 1$;

(2) $r = 1$, $e_1 = 1$ e $f_1 = 2$;

(3) $r = 2$, $e_1 = e_2 = 1$ e $f_1 = f_2 = 1$.

Temos, a partir dessa observação, a seguinte definição:

Definição 19: Com as mesmas notações acima definidas, dizemos que o ideal $p\cdot\mathbf{I}_L$ de $\mathbf{I}_L$ (ou mesmo que o número primo p)
(a) se ***ramifica*** em $\boldsymbol{L}$, se ocorre a condição ***(1)*** acima;
(b) é ***inerte*** em $\boldsymbol{L}$, se ocorre a condição ***(2)*** acima;
(c) se ***decompõe*** em $\boldsymbol{L}$, se ocorre a condição ***(3)*** acima.

Teorema A6:Seja $\boldsymbol{L} = \boldsymbol{Q}(\sqrt{n})$ um corpo quadrático, com n um inteiro livre de quadrados.
(a) Se decompõem em $\boldsymbol{L}$, os primos ímpares p tais que n é resíduo quadrático módulo p, e 2 se $n \equiv_8 1$.
(b) São inertes em $\boldsymbol{L}$, os primos ímpares p tais que n não é resíduo quadrático módulo p, e 2 se $n \equiv_8 5$;
(c) Se ramificam em $\boldsymbol{L}$ os divisores primos ímpares de n, e 2 se $n \equiv_4 2, 3$.
A demonstração desta proposição pode ser encontrada em [6, páginas 122-125, teorema 15.1, teorema 15.2 e corolário 15.3] ou [23, página 89, proposição 1]

6 - Norma de um ideal em uma extensão L / K.

Voltaremos ao problema de se definir norma de um ideal. Desta feita trabalharemos em uma extensão $\boldsymbol{L}$ / $\boldsymbol{K}$ de grau n, onde $\boldsymbol{L}$ e $\boldsymbol{K}$ são corpos de números algébricos ***quaisquer***. Suponha que A e B são, respectivamente, os anéis de inteiros de $\boldsymbol{K}$ e $\boldsymbol{L}$ e $\sigma_1,\ldots, \sigma_n$ são os $\boldsymbol{K}$- isomorfismos de $\boldsymbol{L}$.

Proposição A10: Seja $\mathcal{J}$ um ideal fracionário de $\boldsymbol{L}$. Então existe um único ideal fracionário $\mathcal{F}$ de $\boldsymbol{K}$ tal que

$$\prod_{i=1}^{n}\sigma_i(\mathcal{J}) = B.\mathcal{F}.$$

Mais ainda, se $\mathcal{J} \subseteq B$ então $\mathcal{F} \subseteq A$. Se $\mathcal{J} \neq 0$ então $\mathcal{F} \neq 0$.

A demonstração desta proposição pode ser encontrada em [22, página 165,**1G**].

A partir dessa ***proposição***, temos a definição da ***norma relativa*** de um ideal fracionário. Este conceito coincide com o de norma de um ideal, já visto, quando temos $\boldsymbol{K} = \boldsymbol{Q}$.

Definição 20: Com as notações acima, chamamos de ***norma relativa de*** $\mathcal{J}$ ***na extensão*** $\boldsymbol{L}$ /$\boldsymbol{K}$ ao ideal fracionário $\mathcal{F}$ de $\boldsymbol{K}$ tal que $\prod_{i=1}^{n}\sigma_i(\mathcal{J}) = B.\mathcal{F}$.

Usualmente, denotamos tal norma por $N_{L/K}(\mathcal{J})$.

No caso em que $\boldsymbol{K} = \boldsymbol{Q}$, a norma relativa (que coincide com a norma de um ideal) é dita ***norma absoluta***. Veremos, abaixo, uma propriedade da norma de um ideal que se generaliza para a norma relativa:

Proposição A11: Se $\mathcal{A}$ e $\mathcal{B}$ são ideais fracionários de $\boldsymbol{L}$ então

$$N_{L/K}(\mathcal{A}.\mathcal{B}) = N_{L/K}(\mathcal{A})\cdot N_{L/K}(\mathcal{B}).$$

Mais ainda, se $b \in B$, $b \neq 0$, então $N_{L/K}(b.B) = A\cdot N_{L/K}(b)$.

Para demonstração deste fato (e de outros) veja [22, página 166, **1H**].

Finalizando, veremos uma proposição fortemente usada no Capítulo 3:

Proposição A12: Se $\mathcal{Q}$ é um ideal primo de B tal que $\mathcal{Q} \cap A = \mathcal{P}$ então

$$N_{L/K}(\mathcal{Q}) = \mathcal{P}^f,$$

onde f é o grau de inércia de $\mathcal{Q}$ em $\boldsymbol{L/K}$.
(neste caso, o grau de inércia de $\mathcal{Q}$ em $\boldsymbol{L/K}$ é o grau de $B/\mathcal{Q}$ sobre $A/\mathcal{P}$)
A demonstração deste resultado é encontrada em [22, página 167, **1K**].

7 - Ideais comaximais.

Nesta seção R denotará um anel qualquer.

Definição 21: Dizemos que os ideais $\mathcal{A}$ e $\mathcal{B}$ de R são ***comaximais*** quando $\mathcal{A} + \mathcal{B} = R$.

Segue a propriedade de ideais comaximais usada no texto.
A demonstração desta e de outras propriedades de ideais comaximais pode ser encontrada em [6, página 57].

Proposição A13: Os ideais $\mathcal{A}$ e $\mathcal{B}$ são comaximais se e somente se $\sqrt{\mathcal{A}}, \sqrt{\mathcal{B}}$ forem também comaximais.
Neste caso, $\mathcal{A}^n$ e $\mathcal{B}^m$ são comaximais para quaisquer $n, m \in \boldsymbol{N}$.

REFERÊNCIAS

[1] *Ankeny, N. C.; Chowla, S.* and *Hasse, H.* : On the class number of the maximal real subfield of a cyclotomic field. J.Reine Angew. Math. **217** (1965), 217-220.

[2] *Bolker, E.C.*: elementary Number Theory. W. A. Benjamin, Ins, New York, 1970.

[3] *Borevich, Z. I.* and *Shafarevich, I. R.*: Number theory. Academic Press, New York, 1966.

[4] *Cowles, M. J.*: On divisibility of the class number of imaginary quadratic fields. J. of Number Theory, **12** (1980), 113-115.

[5] *Degert, D.*: Über die Bestimmung der Grundeinheit gewisser reel-quadratischer Zahlokörper. Abh. Math. Sem. Univ. Hamburg, **22** (1958), 92-97.

[6] *Endler, O.* : Teoria dos números algébricos. (Projeto Euclides) IMPA, Rio de Janeiro, 1986.

[7] *Garbanati, D.* : An algorithm for finding an algebraic number whose norm is a given rational number. J. Reine Angew. Math. **316** (1980), 1-13.

[8] *Gross, B. H.* and *Rohrlich, D. E.*: Some results on the Mordell- Weil group of the Jacobian of Fermat curve. Invent. Math., **44** (1978), 201-224.

[9] *Hancock, H.*, vol. I and II : Foundations of the Theory of Algebraic Numbers. Dover Publications, INC, New York, 1960.

[10] *Hardy, G. H.* and *Wright, E. M.* : An introduction to the theory of numbers. Clarendon Press, Oxford, 1975.

[11] *Hasse, H.* : Number theory. Springer-Verlag, New York, 1980.

[12] *Khintchine, A. Y.* : Continued Fractions. P. Noordhoff, Ltd., Groningen, The Netherlands, 1963.

[13] *Lang, S.* : Algebraic Numbers. Addison-Wesley, London, 1964.

[14] *Lang, S. D.*: Note on the class-numbers of the maximal real subfield of a cyclotomic field. J. Reine Angew. Math. **290** (1977), 70-72.

[15] *Marcus, D. A.* : Numbers Fields. Springer-Verlag, New York, 1977.

[16] *Mollin, R. A.* : Class numbers and a generalized Fermat Theorem. J. of Number Theory **16** (1983), 420-429.

[17] *Mollin, R. A.* : Diophantine Equations and Class Numbers. J. of Number Theory **24** (1986), 7-19.

[18] *Mollin, R. A.* : On the cyclotomic polynomial. J. Number Theory **17** (1983), 165-175.

[19] *Mordell, L. J.* : Diophantine Equations. Academic Press, London, 1969.

[20] *Nagell T.* : Introduction to Number Theory. Chelsea Publishing Company, New York, 1964.

[21] *Niven, I.* and *Zuckerman, H. S.* : Introduccion a la Teoría de los números. Editorial Limusa-Wiley S. A., 1969.

[22] *Ribenboim, P.* : Algebraic numbers. Wiley-Interscience, 1972.

[23] *Samuel, P.* : Teoría algebraica de números. Ediciones Omega, S.A., Barcelona, 1972.

[24] *Takeuchi, H.* : On the class-numbers of the maximal real subfield of a cyclotomic field. Canad. J. Math.**33** N° 1 (1981), 55-58.

[25] *Yamaguchi, I.* : On the class-number of the maximal real subfield of a cyclotomic field. J. Reine Angew. Math. **272** (1975), 217-220.