BASES INTEGRAIS PARA EXTENSÕES BIQUADRÁTICAS SOBRE SUBCORPOS QUADRÁTICOS

Este exemplar corresponde a redação final da tese devidamente corrigida e defendida pela Srta Emília de Mendonça Rosa e aprovada pela Comissão Julgadora.

Campinas, 18 de Julho de 1990.

Prof.Dr. _____

Paulo Roberto Brumatti

Dissertação apresentada ao Instituto de Matemática, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para obtenção do Título de Mestre em Matemática.

AGRADECIMENTOS

- Ao professor Paulo R. Brumatti pela orientação, dedicação e amizade à mim concedida.

- A meus pais, Samuel e Dirce e a meus irmãos, pelo apoio e carinho dedicados.

- A meu avô Heitor e demais parentes pelas orações.

- Aos amigos, Geraldo, Eugenia, Carlos, Jéssica , Sérgio e Gustavo, pelo auxílio, amizade e companheirismo.

- Às amigas Márcia, Dirce, Mary e Édna pela paciência, apoio e carinho.

- Aos amigos do "predinho" pelo incentivo e força.

- A todos aqueles que de uma forma direta ou indereta colaboraram na confecção deste trabalho.

- Ao CNPq , CAPES e UNICAMP pelo auxilio financeiro.

- Acima de tudo, à Deus pela direção e sustentação da minha vida, sem o que, seria impossível a realização deste trabalho.

Emília

A meus pais

ÍNDICE

INTRODUÇÃO

Na Teoria dos Números Algébricos existe uma questão bastante clássica, que indaga : "Quando um corpo $\mathbb{K}$, de números algébricos, possui uma base integral sobre um subcorpo k ?", ou em outras palavras : "Quando $\mathbb{B}$, o anel de inteiros do corpo de números algébricos $\mathbb{K}$, é um $\mathbb{A}$-módulo livre de posto finito, sendo $\mathbb{A}$ o anel de inteiros do subcorpo k ?".

Motivados então por este questionamento, este trabalho é a resposta completa e explícita , no caso em que $\mathbb{K}$ é um corpo biquadrático bicíclico [1] (isto é, $\mathbb{K} = \mathbb{Q}(\sqrt{m},\sqrt{n})$ com $\mathbb{Q}$ o corpo dos números racionais; $m,n \in \mathbb{Z}$, livres de quadrados e distintos) e k é um corpo quadrático (isto é, $k = \mathbb{Q}(\sqrt{m})$ com $m \in \mathbb{Z}$ e livre de quadrados), portanto subcorpo de $\mathbb{K}$.

Assim temos as extensões quadráticas $\mathbb{K}/k$ e $k/\mathbb{Q}$, e também a extensão biquadrática bicíclica $\mathbb{K}/\mathbb{Q}$.

---

1)O nome bicíclico se deve ao fato do Grupo de Galois de $\mathbb{K}/\mathbb{Q}$ ser isomorfo ao Grupo de Klein.

Nosso capítulo primeiro é somente uma recordação de resultados básicos da Teoria dos Números Algébricos, os quais são o embasamento deste trabalho. Também o capítulo 1 se destina à uma unificação das notações por nós utilizadas.

Inicialmente trabalhamos com as extensões biquadráticas bicíclicas, ou seja, as do tipo $\mathbb{K}/\mathbb{Q}$ com $\mathbb{K} = \mathbb{Q}(\sqrt{m},\sqrt{n})$. Este estudo constitui nosso segundo capítulo, que está baseado no trabalho de K. S. Williams [06]. Note que, com relação à este tipo de extensão a questão inicial é trivialmente respondida, pois $\mathbb{Z}$ - o anel de inteiros de $\mathbb{Q}$ - é principal. Porém, como dissemos no início, nossa resposta será explícita e para isso usamos a congruência módulo 4, uma vez que os inteiros m e n são livres de quadrados, obtendo casos de acordo com m e n serem congruos à 1, 2 ou 3. Estudamos cada caso apresentando uma base integral, fazendo também a caracterização do anel dos inteiros do corpo $\mathbb{K}$.

Já no capítulo 3, baseados nos resultados contidos no trabalho feito por R. H. Bird e C. J. Parry [01], passamos a estudar as extensões quadráticas $\mathbb{K}/k$, onde k é um corpo de números quadrático real ($m > 0$) ou imaginário ($m < 0$). Neste instante nos deparamos com resultados essenciais cujas provas encontradas na literatura em questão, envolvem um conceito mais sofisticado, a saber, o **diferente**. Assim, visando o caráter elementar deste nosso trabalho procuramos demonstrá-los sem esse recurso. Conseguimos o proposto, porém as demonstrações, um tanto longas, foram inseridas no apêndice para que não se perdesse a unidade do capítulo.

O capítulo 3 ,portanto, nos apresenta respostas à pergunta feita inicialmente considerando, como no anterior, apenas condições sobre m e n, explicitando uma base integral sempre que ocorra sua existência.

Note que nosso estudo não engloba todos os casos de extensões de grau quatro. *Blair K.Spearman* e *Kenneth S.Williams* [05], fazem o estudo onde K é quártico cíclico.

Entendemos que este é um bom elo deste trabalho com outros que porventura possamos fazer.

O que nos motiva nesta linha de estudo é seu caráter atual.

CAPÍTULO 1

RESULTADOS GERAIS SOBRE ANÉIS DE INTEIROS

1.1. INTRODUÇÃO:

Este capítulo tem por objetivo a introdução do leitor à notação usada neste trabalho e também uma breve recordação de resultados básicos da Teoria dos Números Algébricos, nos quais se baseiam os resultados obtidos neste trabalho.

Na maioria das vezes apenas enunciaremos os resultados, uma vez que a demonstração dos mesmos encontra-se na literatura básica de Teoria dos Números Algébricos [02],[04].

Consideraremos $\mathbb{Q}$ o corpo dos racionais, $\mathbb{Z}$ o anel de inteiros racionais, $\mathbb{A}$ anel comutativo com indentidade e sempre que $\mathbb{A}$ for domínio, cfr($\mathbb{A}$) será o corpo de frações de $\mathbb{A}$.

DEFINIÇÃO 1: Seja $\mathbb{A}$ domínio, $\mathbb{K}$ = cfr($\mathbb{A}$) e $\mathbb{L}/\mathbb{K}$ uma extensão de corpos. Chamamos de *fecho inteiro de* $\mathbb{A}$ em $\mathbb{L}$, ao domínio $\overline{\mathbb{A}} = \{ \alpha \in \mathbb{L} \ ; \ \alpha$ é inteiro sobre $\mathbb{A} \}$.

DEFINIÇÃO 2: O domínio $\mathbb{A}$ será dito *domínio integralmente fechado* quando tomando-se $\mathbb{L} = \mathbb{K}$ tem-se $\overline{\mathbb{A}} = \mathbb{A}$.

PROPOSIÇÃO 1: Seja $\mathbb{L}/\mathbb{K}$ extensão algébrica de corpos e $\mathbb{A} \subseteq \mathbb{K}$ subanel tal que $\mathrm{cfr}(\mathbb{A}) = \mathbb{K}$. Então $\overline{\mathbb{A}}$, o fecho inteiro de $\mathbb{A}$ em $\mathbb{L}$, satisfaz:

a) $\mathrm{cfr}(\overline{\mathbb{A}}) = \mathbb{L}$.

b) $\overline{\mathbb{A}}$ é integralmente fechado.

c) Se $\mathbb{A}$ é integralmente fechado, então $\overline{\mathbb{A}} \cap \mathbb{K} = \mathbb{A}$.

Considere, agora, a seguinte situação: $\mathbb{B}/\mathbb{A}$ é uma extensão de anéis tal que $\mathbb{B}$ é um $\mathbb{A}$-módulo livre de posto n. Assim existe uma base livre $\mathbb{E} = \{e_1,\ldots,e_n\}$ de $\mathbb{B}/\mathbb{A}$. Para $x \in \mathbb{B}$, considere a transformação $\mathbb{A}$-linear m_x, dada por

$$\begin{aligned} m_x : \mathbb{B} &\longrightarrow \mathbb{B} \\ y &\longrightarrow xy \end{aligned}$$

e tome $\mathbb{M} = (a_{ij})$ matriz dada por $m_x(e_i) = \sum_{j=1}^{n} a_{ij} e_j$. Como sabemos o traço de $\mathbb{M}$ e o determinante de $\mathbb{M}$, não dependem da particular base $\mathbb{E}$. Assim definimos:

DEFINIÇÃO 3: Seja $x \in \mathbb{B}$, chamamos o *traço de* x, ao traço de $\mathbb{M}$ e denotamos $\mathrm{Tr}_{\mathbb{B}/\mathbb{A}}(x)$. Chamamos *norma de* x ao $\det(\mathbb{M})$, denotada por $N_{\mathbb{B}/\mathbb{A}}(x)$.

TEOREMA 1: Sejam $\mathbb{L}/\mathbb{K}$ uma extensão de corpos de grau n, $\mathbb{L} \subseteq \mathcal{K}^a$, ($\mathcal{K}^a$ corpo algebricamente fechado), ch$\mathbb{K}$ = 0 ou finita

$\text{Iso}_{\mathbb{K}}(\mathbb{L}:\mathcal{K}^a) = \{ \mu_i : \mathbb{L} \longrightarrow \mathcal{K}^a$, $\mathbb{K}$-isomorfismo de $\mathbb{L}$ em $\mathcal{K}^a$,$\forall$ i=1,...,n $\}$

Se $\alpha \in \mathbb{K}$ então $\text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^{n} \mu_i(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^{n} \mu_i(\alpha)$.

COROLÁRIO 1.1: Nas condições do teorema 1, se $\alpha \in \mathbb{L}$ é inteiro sobre $\mathbb{A}$ então $\text{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha)$ e $N_{\mathbb{L}/\mathbb{K}}(\alpha) \in \mathbb{K}$ e são inteiros sobre $\mathbb{A}$.

DEFINIÇÃO 4: Sejam $\mathbb{B}/\mathbb{A}$ uma extensão de anéis, $\mathbb{B}$ é $\mathbb{A}$-módulo livre de posto n e $(\alpha_1,\ldots,\alpha_n) \in \mathbb{B}^n$. Definimos o *discriminante de* $(\alpha_1,\ldots,\alpha_n)$ *sobre* $\mathbb{A}$ como sendo $D_{\mathbb{B}/\mathbb{A}}(\alpha_1,\ldots,\alpha_n) = \det(\text{Tr}(\alpha_i\alpha_j)) \in \mathbb{A}$, para $i,j \in \{1,\ldots,n\}$.

Nas condições da definição 4, temos o seguinte resultado:

PROPOSIÇÃO 2: Se $(\psi_1,\ldots,\psi_n) \in \mathbb{B}^n$ e $\psi_j = \sum_{i=1}^{n} a_{ij}\,\alpha_i$, então

$$D(\psi_1,\ldots,\psi_n) = \left[\det(a_{ij})\right]^2 D(\alpha_1,\ldots,\alpha_n).$$

DEFINIÇÃO 5: Sejam $\mathbb{L}/\mathbb{K}$ extensão de corpos de grau n, $\mathbb{A}$ subanel de $\mathbb{K}$, $\mathbb{A}$ integralmente fechado tal que cfr($\mathbb{A}$) = $\mathbb{K}$ e $\mathbb{B}$ o fecho inteiro de $\mathbb{A}$ em $\mathbb{L}$. O ideal de $\mathbb{A}$ gerado por $\left\{ D_{\mathbb{L}/\mathbb{K}}(\alpha_1,\ldots,\alpha_n)$, onde $\{\alpha_1,\ldots,\alpha_n\} \subseteq \mathbb{B}$ e é base de $\mathbb{L}/\mathbb{K} \right\}$ é chamado o *ideal discriminante de* $\mathbb{B}/\mathbb{A}$. Notação: $\mathcal{D}_{\mathbb{B}/\mathbb{A}}$.

OBSERVAÇÃO 1: Quando $\mathbb{B}$ é $\mathbb{A}$-módulo livre vemos pela proposição 2 que $\mathcal{D}_{\mathbb{B}/\mathbb{A}} = d\mathbb{A}$, onde $d = D_{\mathbb{B}/\mathbb{A}}(\alpha_1,\ldots,\alpha_n)$ e $\{\alpha_1,\ldots,\alpha_n\}$ é base de $\mathbb{B}/\mathbb{A}$.

PROPOSIÇÃO 3: Na situação da definição 4 se $\mathbb{B}$ é um $\mathbb{A}$-módulo livre e $(\alpha_1,\ldots,\alpha_n) \in \mathbb{B}^n$ então $\{\alpha_1,\ldots,\alpha_n\}$ é base de $\mathbb{B}/\mathbb{A}$, se e somente se, $d = D(\alpha_1,\ldots,\alpha_n)$ gera o ideal discriminante, isto é, $\mathcal{D}_{\mathbb{B}/\mathbb{A}} = d\mathbb{A}$.

Uma outra forma de calcular $D(\alpha_1,\ldots,\alpha_n)$ aparece na seguinte proposição:

PROPOSIÇÃO 4: Sejam $\mathbb{L}/\mathbb{K}$ extensão de corpos , $ch\mathbb{K} = 0$ ou finita, $[\mathbb{L}:\mathbb{K}] = n$, $\{\mu_i\}_{i=1}^{n} = Iso_{\mathbb{K}}(\mathbb{L}:\mathbb{C})$ onde $\mathbb{C}$ é corpo algebricamente fechado e $\mathbb{L} \subseteq \mathbb{C}$. Se $\{\alpha_i\}_{i=1}^{n}$ é base de $\mathbb{L}/\mathbb{K}$ então $D(\alpha_1,\ldots,\alpha_n) = \left[\det(\mu_i(\alpha_j))\right]^2$, $\forall\ i,j = 1,\ldots,n$.

TEOREMA 2: Sejam $\mathbb{A}$ domínio integralmente fechado, $\mathbb{K} = cfr(\mathbb{A})$ tal que $ch(\mathbb{K}) = 0$, $[\mathbb{L}:\mathbb{K}] = n$ e $\overline{\mathbb{A}}$ o fecho inteiro de $\mathbb{A}$ em $\mathbb{L}$. Então $\overline{\mathbb{A}}$ é um $\mathbb{A}$-submódulo de um $\mathbb{A}$-módulo livre de posto n e também $\overline{\mathbb{A}}$ contém um $\mathbb{A}$-módulo livre de posto n.

Usando o Teorema de módulos sobre domínios principais obtemos o corolário a seguir:

COROLÁRIO 2.1: Se $\mathbb{A}$ é domínio principal, $\mathbb{K} = cfr(\mathbb{A})$, $ch(\mathbb{K}) = 0$, $\mathbb{L}/\mathbb{K}$ extensão de corpos tal que $[\mathbb{L}:\mathbb{K}] = n$, então $\overline{\mathbb{A}}$ é um $\mathbb{A}$-módulo livre de posto n.

DEFINIÇÃO 6: Chama-se *corpo de números algébricos* à toda extensão $\mathbb{K}$ de grau finito de $\mathbb{Q}$. Chamamos de *anel de inteiros de* $\mathbb{K}$ ao fecho inteiro de $\mathbb{Z}$ em $\mathbb{K}$.

Usando o corolário 2.1 obtem-se:

COROLÁRIO 2.2: Se $\mathbb{K}$ é um corpo de números algébricos de grau n e $\mathbb{A}$ é o anel de inteiros de $\mathbb{K}$ então $\mathbb{A}$ é um $\mathbb{Z}$-módulo livre de posto n.

OBSERVAÇÃO 2: Nas condições do corolário 2.2 temos que existe um único número $d \in \mathbb{Z}$ tal que $d > 0$ e $\mathcal{D}_{\mathbb{A}/\mathbb{Z}} = d\mathbb{Z}$. Tal número d é chamado de *o discriminante absoluto de* $\mathbb{K}$.

O corolário 2.2 sugere uma outra consequência importante do Teorema 2, a saber:

PROPOSIÇÃO 5: Se $\mathbb{A}$ é um domínio noetheriano e integralmente fechado, $\mathbb{K} = cfr(\mathbb{A})$, $ch(\mathbb{A}) = 0$ e $\mathbb{L}/\mathbb{K}$ uma extensão finita de corpos, então $\overline{\mathbb{A}}$, o fecho integral de $\mathbb{A}$ em $\mathbb{L}$, é noetheriano e integralmente fechado.

Neste trabalho estamos interessados em anéis de inteiros que, pela proposição 5, são noetherianos. Lembramos que um anel noetheriano se caracteriza pelo fato de que todo ideal é finitamente gerado. Assim agora faremos algumas observações à respeito dos ideais de um anel noetheriano $\mathbb{A}$.

DEFINIÇÃO 7: Sejam $\mathbb{A}$ um domínio e $\mathbb{K} = \text{cfr}(\mathbb{A})$. Um subconjunto I de $\mathbb{K}$ é dito *ideal fracionário* se é um $\mathbb{A}$-submódulo de $\mathbb{K}$ e se existe $d \in \mathbb{A}$, $d \neq 0$ tal que $dI \subseteq \mathbb{A}$, isto é, $I = \frac{J}{d}$ onde J é um ideal de $\mathbb{A}$.

Observe que quando $\mathbb{A}$ é um domínio noetheriano, um ideal fracionário de $\mathbb{A}$ é um $\mathbb{A}$-submódulo de $\mathbb{K}$ finitamente gerado.

Agora, dado um domínio $\mathbb{A}$, se chamamos $\mathfrak{F}(\mathbb{A})$ o conjunto dos ideais fracionários não nulos de $\mathbb{A}$, então em $\mathfrak{F}(\mathbb{A})$ podemos definir, de maneira natural, uma multiplicação.

Se I_1 e $I_2 \in \mathfrak{F}(\mathbb{A})$ então por definição

$$I_1 I_2 = \left\{ \sum_{i=1}^{n} x_i y_i \; ; \; x_i \in I_1 \text{ e } y_i \in I_2 \right\}.$$

Com esta multiplicação $\mathfrak{F}(\mathbb{A})$ se torna um monóide cujo elemento neutro é $\mathbb{A}$. Uma pergunta natural seria: Quando $\mathfrak{F}(\mathbb{A})$ é um grupo? Esta pergunta, motiva a definição de domínios de Dedekind.

DEFINIÇÃO 8: Um domínio $\mathbb{A}$ é dito *domínio de Dedekind* se:

i) $\mathbb{A}$ é noetheriano.

ii) $\mathbb{A}$ é integralmente fechado.

iii) Todo ideal primo não nulo é maximal.

A motivação feita anteriormente é obtida do seguinte fato.

TEOREMA 3: Sejam $\mathbb{A}$ um domínio de Dedekind e $\mathfrak{P}$ o conjunto dos ideais primos não nulos de $\mathbb{A}$, então temos:

a) Todo ideal fracionário, I, não nulo de $\mathbb{A}$ se escreve, de maneira única, na forma $I = \prod_{P \in \mathfrak{P}} P^{n_P}$, onde $n_p \in \mathbb{Z}$ para qualquer P e são quase todos nulos.

b) $\mathfrak{J}(\mathbb{A})$ com a multiplicação é um grupo abeliano.

OBSERVAÇÃO 3: Sejam $\mathbb{A}$ um domínio de Dedekind e $\mathbb{K} = cfr(\mathbb{A})$. Um ideal fracionário $\mathfrak{h}$ de $\mathbb{A}$ é dito principal se $\mathfrak{h} = \xi\mathbb{A}$, onde $\xi \in \mathbb{K}$ e $\xi \neq 0$. Considere $\mathcal{P}(\mathbb{A})$ o conjunto dos ideais fracionários principais de $\mathbb{A}$. É fácil verificar que $\mathcal{P}(\mathbb{A})$ é um subgrupo de $\mathfrak{J}(\mathbb{A})$. O grupo $\mathcal{H}(\mathbb{A}) := \frac{\mathfrak{J}(\mathbb{A})}{\mathcal{P}(\mathbb{A})}$ é chamado de o *grupo de classes de* $\mathbb{A}$.

O próximo resultado é motivado pela definição de domínio de Dedekind e pela proposição 5.

TEOREMA 4: Se $\mathbb{A}$ é um domínio de Dedekind, $\mathbb{K} = cfr(\mathbb{A})$, $ch(\mathbb{A}) = 0$, $\mathbb{L}/\mathbb{K}$ uma extensão finita de corpos e $\overline{\mathbb{A}}$ é o fecho inteiro de $\mathbb{A}$ em $\mathbb{L}$, então $\overline{\mathbb{A}}$ é um anel de Dedekind, mais ainda, existe um $\mathbb{A}$-módulo livre de posto finito $\mathbb{B}$ tal que $\mathbb{A} \subseteq \mathbb{B}$ e portanto $\overline{\mathbb{A}}$ é um $\mathbb{A}$-módulo finitamente gerado.

Uma consequência natural do teorema 4 é :

COROLÁRIO 4.1: Se $\mathbb{K}$ é um corpo numérico então o anel de inteiros de $\mathbb{K}$ é um domínio de Dedekind.

Considere, novamente, a situação; $\mathbb{A}$ é um domínio de Dedekind, $\mathbb{K} = cfr(\mathbb{A})$, $ch(\mathbb{A}) = 0$, $\mathbb{L}/\mathbb{K}$ uma extensão de corpos de grau n e $\mathbb{B}$ o fecho inteiro de $\mathbb{A}$ em $\mathbb{L}$. Como já vimos $\mathbb{B}$ é um domínio de Dedekind, assim se P é um ideal primo não nulo de $\mathbb{A}$ então o ideal gerado por P em $\mathbb{B}$, isto é, $P\mathbb{B}$ se escreve de maneira única na forma : $P\mathbb{B} = \prod_{i=0}^{s} Q_i^{e_i}$, onde os Q_i são ideais primos de $\mathbb{B}$, dois à dois distintos e os e_i são inteiros maiores ou iguais à 1.

PROPOSIÇÃO 6: Na situação acima os Q_i são, exatamente, os ideais de $\mathbb{B}$ tais que $Q_1 \cap \mathbb{A} = P$.

Considerando ainda a mesma situação observe que pelo fato de, $Q_i \cap \mathbb{A} = P$ e $\mathbb{B}$ ser um $\mathbb{A}$-módulo finitamente gerado; temos que $\frac{\mathbb{A}}{P}$ pode ser considerado como subcorpo de $\frac{\mathbb{B}}{Q_1}$ e também que

$\left[\frac{\mathbb{B}}{Q_i} : \frac{\mathbb{A}}{P}\right] = f_i < \infty$. Tal f_i é chamado *grau de inércia de* Q_i *sobre* $\mathbb{A}$ e o e_i que aparece na fórmula de $P\mathbb{B}$, é chamado de *índice de ramificação de* Q_i *sobre* $\mathbb{A}$. Observe ainda que $P\mathbb{B} \cap \mathbb{A} = P$, assim $\frac{\mathbb{A}}{P}$ se identifica como um corpo contido em $\frac{\mathbb{B}}{P\mathbb{B}}$ e portanto $\frac{\mathbb{B}}{P\mathbb{B}}$ é um $\frac{\mathbb{A}}{P}$ espaço vetorial, e denotaremos por $\left[\frac{\mathbb{B}}{P\mathbb{B}} : \frac{\mathbb{A}}{P}\right]$ a dimensão de $\frac{\mathbb{B}}{P\mathbb{B}}$ sobre $\frac{\mathbb{A}}{P}$.

TEOREMA 5: Na situação descrita acima temos:

$$\sum_{i=1}^{s} e_i f_i = \left[\frac{\mathbb{B}}{P\mathbb{B}} : \frac{\mathbb{A}}{P}\right] = n \quad ,$$

onde $n = [L:K]$ e $f_i = \left[\frac{\mathbb{B}}{Q_i} : \frac{\mathbb{A}}{P}\right]$.

Dentro desta mesma situação, damos as seguintes definições:

DEFINIÇÃO 9: Dado um ideal primo não nulo P de $\mathbb{A}$ dizemos que:

a)P *se ramifica em* $\mathbb{B}$ se existe $i \in \mathbb{N}$ tal que $e_i \geq 2$.

b)P é dito *inerte* se $P\mathbb{B}$ é ideal primo, isto é, $s = 1$ e $e_i = 1$.

TEOREMA 6: Sejam $\mathbb{L}$ e $\mathbb{K}$ corpos numéricos tais que $[\mathbb{L}:\mathbb{K}] = n$.

Considere $\mathbb{A}$ o anel de inteiros de $\mathbb{K}$ e $\mathbb{B}$ o anel de inteiros de $\mathbb{L}$ ($\mathbb{B}$ é também o fecho inteiro de $\mathbb{A}$ em $\mathbb{L}$). Então temos que um ideal primo não nulo $P \subseteq \mathbb{A}$ se ramifica em $\mathbb{B}$, se e somente se, $\mathcal{D}_{\mathbb{B}/\mathbb{A}} \subseteq P$.

Note que se a extensão $\mathbb{L}/\mathbb{K}$ é Galoisiana e $[\mathbb{L}:\mathbb{K}] = n$ tem-se um resultado mais forte que o Teorema 5, a saber:

TEOREMA 7: Seja $\mathbb{L}/\mathbb{K}$ uma extensão de corpos galoisiana de grau n, onde $ch(\mathbb{K}) = 0$. Considere $\mathbb{A}$ um domínio de Dedekind tal que $cfr(\mathbb{A}) = \mathbb{K}$ e $\mathbb{B}$ o fecho integral de $\mathbb{A}$ em $\mathbb{L}$. Se P é um ideal primo não nulo de $\mathbb{A}$ e $P\mathbb{B} = \prod_{i=0}^{s} Q_i^{e_i}$ então $e_1 = \ldots = e_s = e$, $f_1 = \ldots = f_s = f$ e $n = efs$, isto é, $P\mathbb{B} = \left(\prod_{i=0}^{s} Q_i\right)^{e}$ e $f_1 = \ldots = f_s$.

Agora, como o caso $\mathbb{K} = \mathbb{Q}(\sqrt{m})$, onde $m \in \mathbb{Z}$ e m livre de quadrados é fundamental neste trabalho vamos apresentar dois resultados essenciais a respeito dele.

PROPOSIÇÃO 7: Seja $\mathbb{K} = \mathbb{Q}(\sqrt{m})$, onde $m \in \mathbb{Z}$, $m \neq 0$ e m livre de quadrados. Seja $\mathbb{A}$ o anel de inteiros de $\mathbb{K}$ então temos:

a)Se $m \equiv_4 2$ ou 3 então $\mathbb{A} = \mathbb{Z} \oplus \mathbb{Z}(\sqrt{m})$.

b)Se $m \equiv_4 1$ então $\mathbb{A} = \mathbb{Z} \oplus \mathbb{Z}\left(\frac{1 + \sqrt{m}}{2}\right)$, ou seja,

$$\mathbb{A} = \left\{ \frac{a + b\sqrt{m}}{2} , a, b \in \mathbb{Z} \text{ e } a \equiv_2 b \right\} .$$

PROPOSIÇÃO 8: Nas condições da proposição 7, se $P \in \mathbb{Z}$ é um número primo então:

i)P é decomposto em $\mathbb{A}$, isto é, $P\mathbb{A} = Q_1 Q_2$, se e somente se,

$$\begin{cases} P = 2 \text{ e } m \equiv_8 1 \\ \text{ou} \\ P \neq 2 \text{ e } \overline{m} \in \dot{\mathbb{F}}_p^2 \end{cases}$$

onde $\mathbb{F}_p$ é o corpo com P elementos.

ii)P é inerte em $\mathbb{A}$, isto é, $P\mathbb{A} = Q$, se e somente se,

$$\begin{cases} P = 2 \text{ e } m \equiv_8 5 \\ \text{ou} \\ P \neq 2 \text{ e } \overline{m} \notin \dot{\mathbb{F}}_p^2 \end{cases}$$

iii)P se ramifica em $\mathbb{A}$, isto é, $P\mathbb{A} = Q^2$, se e somente se,

$$\begin{cases} P = 2 \text{ e } m \equiv_4 2 \text{ ou } 3 \\ \text{ou} \\ P \neq 2 \text{ e } p \mid m \end{cases}$$

Agora gostaríamos de falar um pouco sobre as unidades de um domínio $\mathbb{A}$.

DEFINIÇÃO 10: Dado um anel $\mathbb{A}$. Dizemos que $u \in \mathbb{A}$ é uma *unidade de* $\mathbb{A}$ se existe $u^{-1} \in \mathbb{A}$ tal que $uu^{-1} = 1$. O conjunto das unidades de $\mathbb{A}$ denotaremos por $\mathcal{U}(\mathbb{A})$. Note que $\mathcal{U}(\mathbb{A})$ é um grupo multiplicativo.

Observe que, dados um domínio $\mathbb{A}$ e $d_1, d_2 \in \mathbb{A}$ tais que $d_1 \neq 0$ e $d_2 \neq 0$ então $d_1\mathbb{A} = d_2\mathbb{A}$, se e somente se, $d_1 = ud_2$ com $u \in \mathcal{U}(\mathbb{A})$. Portanto se estamos interessados em escolher um gerador apropriado para um determinado ideal principal de $\mathbb{A}$ é natural que o conhecimento de $\mathcal{U}(\mathbb{A})$ ajuda muito. O fato é que quando $\mathbb{A}$ é um anel de inteiros de um corpo de números $\mathbb{K}$, $\mathcal{U}(\mathbb{A})$ é um grupo com uma descrição bastante boa. Vamos, agora, apresentar tal descrição.

PROPOSIÇÃO 9: Dado um corpo numérico $\mathbb{K}$. Considere $\mathbb{A}$ o anel de inteiros de $\mathbb{K}$ e $\alpha \in \mathbb{A}$. Então $\alpha \in \mathcal{U}(\mathbb{A})$, se e somente se, $N_{\mathbb{K}/\mathbb{Q}}(\alpha) = \pm 1$, ($\alpha \in \mathcal{U}(\mathbb{A})$ também é definido como sendo unidade de $\mathbb{K}$).

Quando $\mathbb{K}$ é um corpo numérico e $[\mathbb{K}:\mathbb{Q}] = n$, sabemos que $\#\left(\text{Iso}(\mathbb{K},\mathbb{C})\right) = n$, onde $\mathbb{C}$ é corpo dos números complexos e $\text{Iso}(\mathbb{K},\mathbb{C}) = \{ \mu : \mathbb{K} \longrightarrow \mathbb{C}$, μ isomorfismo de $\mathbb{K}$ em $\mathbb{C} \}$.

DEFINIÇÃO 11: Dado $\mu \in \text{Iso}(\mathbb{K},\mathbb{C})$, dizemos que μ é um isomorfismo real se $\mu(\mathbb{K}) \subseteq \mathbb{R}$.

OBSERVAÇÃO 4: Se $\mu \in \text{Iso}(\mathbb{K},\mathbb{C})$ então podemos definir $\overline{\mu} : \mathbb{K} \longrightarrow \mathbb{C}$, por $\overline{\mu}(x) = \overline{\mu(x)}$ = conjugado de $\mu(x)$, onde $x \in \mathbb{K}$.

Observe que μ é real, se e somente se, $\mu = \overline{\mu}$, $\overline{\mu}$ é chamado o isomorfismo conjugado de μ. Assim se r é o número de isomorfismos reais de $\mathbb{K}$ em $\mathbb{C}$ e t é o número de isomorfismos não reais e não conjugados de $\mathbb{K}$ em $\mathbb{C}$ então $n = [\mathbb{K}:\mathbb{Q}] = r + 2t$.

Agora estamos em condições de enunciar o Teorema de Dirichlet a respeito das unidades de um corpo numérico

TEOREMA 8 (TEOREMA DE DIRICHLET): Sejam $\mathbb{K}$ um corpo numérico tal que $[\mathbb{K}:\mathbb{Q}] = n$; r, t definidos como na observação 3 e $\mathbb{A}$ o anel de inteiros de $\mathbb{K}$. Então o grupo das unidades $\mathcal{U}(\mathbb{A})$ é isomorfo à $\mathbb{Z}^s \times \mathbb{G}$, onde $s = r + t - 1$ e $\mathbb{G}$ é o grupo finito formado pelas raízes da unidade que estão contidas em $\mathbb{K}$. Mais precisamente, existem $\varepsilon_1,\ldots,\varepsilon_s \in \mathcal{U}(\mathbb{A})$ (chamadas unidades fundamentais), tais que para todo $u \in \mathcal{U}(\mathbb{A})$ existem únicos

$\ell_1,\ldots,\ell_s \in \mathbb{Z}$ e único $\xi \in \mathbb{K}$ com $\xi^m = 1$ para algum natural m, tal que $u = \xi\, \varepsilon_1^{\ell_1} \ldots \varepsilon_s^{\ell_s}$.

Voltando ao caso $\mathbb{K} = \mathbb{Q}(\sqrt{m})$, $m \in \mathbb{Z}$ e m livre de quadrados temos que o Teorema de Dirichlet se traduz em:

PROPOSIÇÃO 10: Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{m})$ e $\mathbb{A}$ o anel de inteiros de $\mathbb{K}$. Então temos:

a)Se $m > 0$ então $\mathcal{U}(\mathbb{A}) \approx \{\pm 1\} \times \mathbb{Z}$, e neste caso o grupo das unidades positivas de $\mathbb{K}$ é isomorfo à $\mathbb{Z}$.

b)Se $m < 0$, $m \neq -1$ e $m \neq -3$ então $\mathcal{U}(\mathbb{A}) = \{\pm 1\}$.

c)Se $m = -1$ então $\mathcal{U}(\mathbb{A}) = \{\pm 1, \pm i\}$.

d)Se $m = -3$ então $\mathcal{U}(\mathbb{A}) = \left\{ \left(\frac{1 + i\sqrt{3}}{2} \right)^j ;\ j = 0,\ldots,5 \right\}$.

OBSERVAÇÃO 5: Se $m > 0$ e ε é uma unidade fundamental positiva de $\mathbb{A}$ então $\varepsilon^3 = a + b\sqrt{m}$, com $a, b \in \mathbb{Z}$, mesmo que $m \equiv_4 1$ (veja [04], p.76).

Para encerrar este capítulo gostariamos e enunciar e provar um resultado que será fundamental para o transcorrer do trabalho.

TEOREMA 9: Sejam $\mathbb{L}/\mathbb{K}$ extensão separável de corpos de grau n , $\mathbb{A}$ domínio integralmente fechado tal que $cfr(\mathbb{A}) = \mathbb{K}$ e $\mathbb{B}$ o fecho inteiro de $\mathbb{A}$ em $\mathbb{L}$. Então $\mathbb{B}$ tem base integral sobre $\mathbb{A}$, se e sómente se, $\mathcal{D}_{\mathbb{L}/\mathbb{K}} = d\mathbb{A}$ onde $d = D(\psi_1,\ldots,\psi_n)$, sendo $\{\psi_1,\ldots,\psi_n\} \subseteq \mathbb{B}$ base de $\mathbb{L}/\mathbb{K}$.

DEMONSTRAÇÃO:

$\Rightarrow$: Proposição 3.

$\Leftarrow$: Seja $x \in \mathbb{B}$ então $x = \sum_{i=1}^{n} a_i\psi_i$, com $a_i \in \mathbb{K}$ e $\{\psi_i\}_{i=1}^{n}$ base de $\mathbb{L}/\mathbb{K}$ contida em $\mathbb{B}$, dada pela hipótese.

Afirmamos que $a_i \in \mathbb{A}$, $\forall\ i \in \{1,\ldots,n\}$. De fato, pois se

1) $a_i = 0$, cqd.

2) $a_i \neq 0$ implica $\psi_1 = \left(\frac{-a_1}{a_1}\right)\psi_1 + \ldots + \left(\frac{-x}{a_1}\right) + \ldots + \left(\frac{-a_n}{a_1}\right)\psi_n$ e

então obtemos que $\{\ \psi_1\ ,\ \ldots\ ,\ \psi_{i-1}\ ,\ x\ ,\ \psi_{i+1}\ \ldots\ ,\ \psi_n\ \}$ é base de $\mathbb{L}/\mathbb{K}$.

Usando os isomorfismos μ_j em x e denotando por $\mu_j(x) = x^{(j)}$, temos o seguinte sistema:

$$\begin{cases} x = a_1\psi_1 + \ldots + a_i\psi_i + \ldots + a_n\psi_n \\ x^{(2)} = a_1\psi_1^{(2)} + \ldots + a_i\psi_i^{(2)} + \ldots + a_n\psi_n^{(2)} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x^{(n)} = a_1\psi_1^{(n)} + \ldots + a_i\psi_i^{(n)} + \ldots + a_n\psi_n^{(n)} \end{cases}$$

Pela Regra de Cramer, temos:

$$a_i^2 = \frac{\begin{vmatrix} \psi_1 & \psi_2 & \cdots & \alpha & \cdots & \psi_n \\ \psi_1^{(2)} & \psi_2^{(2)} & \cdots & \alpha^{(2)} & \cdots & \psi_n^{(2)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \psi_1^{(n)} & \psi_2^{(n)} & \cdots & \alpha^{(n)} & \cdots & \psi_n^{(n)} \end{vmatrix}^2}{\begin{vmatrix} \psi_1 & \psi_2 & \cdots & \psi_i & \cdots & \psi_n \\ \psi_1^{(2)} & \psi_2^{(2)} & \cdots & \psi_i^{(2)} & \cdots & \psi_n^{(2)} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \psi_1^{(n)} & \psi_2^{(n)} & \cdots & \psi_i^{(n)} & \cdots & \psi_n^{(n)} \end{vmatrix}^2}$$

Assim $a_i^2 = \dfrac{D(\psi_1, \ldots, \alpha, \ldots, \psi_n)}{d}$.

Como $\{ \psi_1, \ldots, \alpha, \ldots, \psi_n \} \subseteq \mathbb{B}$ e é base de $\mathbb{L}/\mathbb{K}$, temos $D(\psi_1, \ldots, \alpha, \ldots, \psi_n) \in \mathcal{D}_{\mathbb{B}/\mathbb{A}} = d\mathbb{A}$ e portanto como $a_i \in \mathbb{K}$ e $a_i^2 \in \mathbb{A}$ então a_i satisfaz o polinômio $p(X) = X^2 - a_i^2$. Logo a_i é inteiro sobre $\mathbb{A}$. Mas $\mathbb{A}$ é integralmente fechado e portanto $a_i \in \mathbb{A}$ ■

CAPÍTULO 2

EXTENSÕES BIQUADRÁTICAS DO CORPO Q

2.1. INTRODUÇÃO:

Seja $\mathbb{K} = \mathbb{Q}(\sqrt{m},\sqrt{n})$, onde m,n são números inteiros, distintos e livres de quadrados. Já vimos, no capítulo 1, que o anel de inteiros de $\mathbb{K}$ possue uma base integral sobre $\mathbb{Z}$ (anel de inteiros de $\mathbb{Q}$).

Neste capítulo pretendemos :

1) Explicitar a forma dos inteiros do corpo $\mathbb{K}$.

2) Determinar uma base integral de $\mathbb{K}$ sobre $\mathbb{Q}$.

3) Calcular o discriminante absoluto da extensão $\mathbb{K}/\mathbb{Q}$.

Inicialmente, façamos certas considerações sobre m e n.

Seja λ o máximo divisor comum de m e n, assim podemos escrever

$$\begin{cases} m = \lambda m_1 \\ n = \lambda n_1 \end{cases} \qquad \text{com } (m_1,n_1) = 1$$

Como m, n são livres de quadrados temos que m, n $\not\equiv_4 0$ podemos considerar as possibilidades para m, n, m_1n_1 e λ.

Tomemos $(m,n) \equiv_4 (1,1)$, logo λ é impar e assim consideremos:

$$\lambda \equiv_4 1 \quad \Rightarrow \quad \begin{cases} 1 \equiv_4 m = \lambda m_1 \equiv_4 m_1 \\ 1 \equiv_4 n = \lambda n_1 \equiv_4 n_1 \end{cases} \quad \Rightarrow \quad m_1n_1 \equiv_4 1.$$

$$\lambda \equiv_4 3 \quad \Rightarrow \quad \begin{cases} 1 \equiv_4 m = \lambda m_1 \equiv_4 3m_1 \\ 1 \equiv_4 n = \lambda n_1 \equiv_4 3n_1 \end{cases} \quad \Rightarrow$$

$$\Rightarrow \quad m_1 \equiv_4 n_1 \equiv_4 3 \quad \Rightarrow \quad m_1n_1 \equiv_4 1 .$$

Repetindo esta análise em cada caso, obtemos a seguinte tabela.

TABELA 1

$m \equiv_4$	$n \equiv_4$	$m_1n_1 \equiv_4$
1	1	1
1	2	2
1	3	3
2	1	2
2	2	1 ou 3
2	3	2
3	1	3
3	2	2
3	3	1

Pode-se verificar facilmente que:

$$\mathbb{Q}(\sqrt{m},\sqrt{n}) = \mathbb{Q}(\sqrt{m},\sqrt{m_1 n_1}) = \mathbb{Q}(\sqrt{n},\sqrt{m_1 n_1}) = \mathbb{Q}(\sqrt{n},\sqrt{m}) ,$$

assim analizando a Tabela 1 e fazendo uma permutação entre m, n e $m_1 n_1$, quando necessário, podemos sem perda de generalidade supor que :

$$(m,n) \equiv_4 (1,1),\ (1,2),\ (2,3) \text{ ou } (3,3). \qquad (1)$$

2.2. ANEL DE INTEIROS:

Já estamos, agora, em condições de explicitar os inteiros da extensão $\mathbb{K} = \mathbb{Q}(\sqrt{m},\sqrt{n})$ sobre $\mathbb{Q}$, onde m, n satisfazem (1).

Neste intento nos deparamos com o seguinte resultado:

TEOREMA 1: Neste teorema denotaremos por x_0, x_1, x_2, x_3 números racionais inteiros.

Temos que o anel $\mathbb{B}$, de inteiros de $\mathbb{K} = \mathbb{Q}(\sqrt{m},\sqrt{n})$ é dado como se segue:

i) Se $(m,n) \equiv_4 (m_1,n_1) \equiv_4 (1,1)$ e $\theta \in \mathbb{B}$ então

$$\theta = \frac{1}{4}\,(x_0 + x_1\sqrt{m} + x_2\sqrt{n} + x_3\sqrt{m_1 n_1})$$

com $x_0 \equiv_2 x_1 \equiv_2 x_2 \equiv_2 x_3$ e $x_0 - x_1 + x_2 - x_3 \equiv_4 0$.

ii) Se $(m,n) \equiv_4 (1,1)$ e $(m_1,n_1) \equiv_4 (3,3)$ e $\Theta \in \mathbb{B}$

então

$$\Theta = \frac{1}{4}(x_0 + x_1\sqrt{m} + x_2\sqrt{n} + x_3\sqrt{m_1 n_1})$$

com $x_0 \equiv_2 x_1 \equiv_2 x_2 \equiv_2 x_3$ e $x_0 - x_1 - x_2 - x_3 \equiv_4 0$.

iii) Se $(m,n) \equiv_4 (1,2)$ e $\Theta \in \mathbb{B}$ então

$$\Theta = \frac{1}{2}(x_0 + x_1\sqrt{m} + x_2\sqrt{n} + x_3\sqrt{m_1 n_1})$$

com $x_0 \equiv_2 x_1$, $x_2 \equiv_2 x_3$.

iv) Se $(m,n) \equiv_4 (2,3)$ e $\Theta \in \mathbb{B}$ então

$$\Theta = \frac{1}{2}(x_0 + x_1\sqrt{m} + x_2\sqrt{n} + x_3\sqrt{m_1 n_1})$$

com $x_0 \equiv_2 x_2 \equiv_2 0$, $x_1 \equiv_2 x_3$.

v) Se $(m,n) \equiv_4 (3,3)$ e $\Theta \in \mathbb{B}$ então

$$\Theta = \frac{1}{2}(x_0 + x_1\sqrt{m} + x_2\sqrt{n} + x_3\sqrt{m_1 n_1})$$

com $x_0 \equiv_2 x_3$, $x_1 \equiv_2 x_2$.

DEMONSTRAÇÃO:

Temos que $\theta \in \mathbb{K}$ pode ser escrito como:

$$\theta = a_0 + a_1\sqrt{m} + a_2\sqrt{n} + a_3\sqrt{m_1 n_1} \quad \begin{cases} \text{com } a_i \in \mathbb{Q} \\ i = 0,1,2,3 \end{cases} \qquad (2)$$

Assim os conjugados de θ são:

$$\begin{cases} \theta' = a_0 + a_1\sqrt{m} - a_2\sqrt{n} - a_3\sqrt{m_1 n_1} \\ \theta'' = a_0 - a_1\sqrt{m} + a_2\sqrt{n} - a_3\sqrt{m_1 n_1} \\ \theta''' = a_0 - a_1\sqrt{m} - a_2\sqrt{n} + a_3\sqrt{m_1 n_1} \end{cases} \qquad (3)$$

Agora se tomarmos $\theta \in \mathbb{B}$ vamos ter que θ',θ'' e θ''' também estão em $\mathbb{B}$ e portanto,

$$\begin{cases} \theta + \theta' = 2a_0 + 2a_1\sqrt{m} & \in \mathbb{Q}(\sqrt{m}) \\ \theta + \theta'' = 2a_0 + 2a_2\sqrt{n} & \in \mathbb{Q}(\sqrt{n}) \\ \theta + \theta''' = 2a_0 + 2a_3\sqrt{m_1 n_1} & \in \mathbb{Q}(\sqrt{m_1 n_1}) \end{cases} \qquad (4)$$

também são inteiros sobre $\mathbb{Z}$, assim são inteiros dos corpos $\mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$, $\mathbb{Q}(\sqrt{m_1 n_1})$, respectivamente.

Analisemos primeiro os casos $(m,n) \equiv_4 (1,2),(2,3)$ e $(3,3)$. Nestes casos, proposição 7 do capítulo 1 e observando a Tabela 1, pelo menos dois de (4) têm coeficientes inteiros; mas $2a_0$ é comum à todas as sentenças de (4), assim a terceira deve também ter coeficientes inteiros.

Portanto $2a_0$, $2a_1$, $2a_2$, $2a_3 \in \mathbb{Z}$ e fazendo $b_i = 2a_i$, para $i = 0,1,2,3$; podemos reescrever (2) obtendo :

$$\theta = \frac{1}{2}(b_0 + b_1\sqrt{m} + b_2\sqrt{n} + b_3\sqrt{m_1 n_1}) \ , \ b_i \in \mathbb{Z} \text{ para } i = 0,1,2,3 \qquad (5)$$

O polinômio característico de θ sobre $\mathbb{Q}$ é dado por:

$p(X) = (X - \theta)(X - \theta')(X - \theta'')(X - \theta''') \in \mathbb{Z}[X]$. Assim

$$p(X) = X^4 - 2b_0X^3 + \left(c + \frac{d}{2}\right)X^2 + \left(\frac{b_3 m_1 n_1 e - b_0 d}{2}\right)X + \left(\frac{d^2 - m_1 n_1 e^2}{16}\right) \qquad (6)$$

$$\text{onde} \quad \begin{cases} c = b_0^2 - m_1 n_1 b_3^2 \\ d = b_0^2 - mb_1^2 - nb_2^2 + m_1 n_1 b_3^2 \\ e = 2(b_0 b_3 - b_1 b_2 \lambda) \end{cases} \qquad (7)$$

Portanto temos que os coeficientes de (6) devem ser todos inteiros.

Façamos agora algumas observações que usaremos no transcorrer desta prova.

(a) Por (6), temos que $2c + d \equiv_2 0$, isto é, d é par e portanto $d^2 \equiv_4 0$.

(b) Também de (6) obtemos que $d^2 - m_1 n_1 e^2 \equiv_{16} 0$. Então:

i) Se $m_1 n_1 \equiv_4 1$ então $4m_1 n_1 \equiv_{16} 4$.

Mas $e = 2(b_0 b_3 - b_1 b_2 \lambda)$ o que implica $e^2 = 4(b_0 b_3 - b_1 b_2 \lambda)^2$, assim:

$$d^2 \equiv_{16} m_1 n_1 e^2 = 4m_1 n_1 (b_0 b_3 - b_1 b_2 \lambda)^2 \equiv_{16} 4(b_0 b_3 - b_1 b_2 \lambda)^2 = e^2$$

Portanto $d^2 \equiv_{16} e^2$.

Suponha que $d \not\equiv_4 e$ então $d \equiv_4 0$ e $e \equiv_4 2$, ou vice versa, logo $d^2 \not\equiv_{16} e^2$, o que é contradição.

Logo $d \equiv_4 e$.

ii) Se $m_1 n_1 \equiv_4 2$, e como e é par então $e^2 \equiv_4 0$. Assim:

$$m_1 n_1 e^2 \equiv_8 0 \Rightarrow d^2 \equiv_8 0 \Rightarrow d \equiv_4 0.$$

Mas $d^2 \equiv_{16} m_1 n_1 e^2$, logo $m_1 n_1 e^2 \equiv_{16} 0$. Como $4m_1 n_1 \equiv_{16} 8$ temos que $0 \equiv_{16} d^2 \equiv_{16} 8(b_0 b_3 - b_1 b_2 \lambda)^2 = 2e^2$. Assim $e^2 \equiv_8 0$ e portanto $e \equiv_4 0$.

Assim $d \equiv_4 e$.

iii) Se $m_1 n_1 \equiv_4 3$ então $4m_1 n_1 \equiv_{16} -4$.

Mas $e = 2(b_0 b_3 - b_1 b_2 \lambda)$, logo $e^2 = 4(b_0 b_3 - b_1 b_2 \lambda)^2$; assim

$$d^2 \equiv_{16} m_1 n_1 e^2 = 4m_1 n_1 (b_0 b_3 - b_1 b_2 \lambda)^2 \equiv_{16} -4(b_0 b_3 - b_1 b_2 \lambda)^2 = -e^2$$

Portanto $d^2 + e^2 \equiv_{16} 0$ e daí $d \equiv_4 e \equiv_4 0$.

Após estas observações consideremos cada caso.

Se $(m,n) \equiv_4 (1,2)$ temos que λ é ímpar e $m_1 n_1 \equiv_4 2$ (Tabela 1).

Pela observação (b) parte (ii) $d \equiv_4 e \equiv_4 0$.

Temos então que $b_0^2 - b_1^2 + 2(b_2^2 + b_3^2) \equiv_4 d \equiv_4 0$ (7)

e também:

$$0 \equiv_4 2(b_0 b_3 - b_1 b_2 \lambda) \Rightarrow b_0 b_3 - b_1 b_2 \equiv_2 0 \Rightarrow b_0 b_3 \equiv_2 b_1 b_2 \quad (7b)$$

Se $b_0 \not\equiv_2 b_1$ então $b_0^2 - b_1^2 \equiv_4 1$ e desta forma (7) é insolúvel. Assim $b_0 \equiv_2 b_1$ implica que $b_0^2 \equiv_4 b_1^2$, logo $2(b_2^2 + b_3^2) \equiv_4 0$ que nos dá $b_2 \equiv_2 b_3$. Portanto o caso (iii) do teorema está provado, uma vez que (7b) está satisfeito.

Se $(m,n) \equiv_4 (2,3)$ temos que λ é ímpar e $m_1 n_1 \equiv_4 2$, assim pela observação (b)

$$0 \equiv_4 b_0^2 + b_2^2 - 2(b_1^2 - b_3^2) \qquad (8)$$

e também

$$b_0 b_3 - b_1 b_2 \equiv_2 0 \qquad (8b)$$

Se b_0 ou b_2 é ímpar então por (8) obtemos que o outro também o é, e de (8b) vem que $b_1 \equiv_2 b_3$ e portanto $b_1^2 - b_3^2 \equiv_2 0$, logo (8) nos dá uma contradição. Agora se b_0 e b_2 são pares então, por (8), $b_1 \equiv_2 b_3$, o que prova o caso (iv).

Se $(m,n) \equiv_4 (3,3)$ então λ é ímpar e $m_1 n_1 \equiv_2 1$, logo da observação (b) parte (i), temos:

$$b_0^2 + b_1^2 + b_2^2 + b_3^2 \equiv_4 2(b_0 b_3 - b_1 b_2) \Rightarrow$$

$$\Rightarrow (b_0 - b_3)^2 + (b_1 + b_2)^2 \equiv_4 0$$

$$\Rightarrow b_0 - b_3 \equiv_2 0 \quad \text{e} \quad b_1 + b_2 \equiv_2 0$$

$$\Rightarrow b_0 \equiv_2 b_3 \quad \text{e} \quad b_1 \equiv_2 b_2, \text{ que prova o caso (v).}$$

Consideremos agora $(m,n) \equiv_4 (1,1)$ então $m_1 n_1 \equiv_4 1$ e de (4) temos que $2a_0, 2a_1, 2a_2, 2a_3 \in \mathbb{Z}$ ou são todos metade de números ímpares (ou seja, não são inteiros).

No caso de todos serem inteiros teremos, como pela observação (b), $d \equiv_4 e$, o que implica em :

$$b_0^2 - b_1^2 - b_2^2 + b_3^2 \equiv_4 2(b_0b_3 - b_1b_2) \quad \Rightarrow \quad (b_0 - b_3)^2 \equiv_4 (b_1 - b_2)^2$$

$$b_0 - b_3 \equiv_2 b_1 - b_2 \quad \Rightarrow \quad b_0 - b_1 + b_2 - b_3 \equiv_2 0 .$$

Escrevendo $\theta = \frac{1}{4}(2b_0 + 2b_1\sqrt{m} + 2b_2\sqrt{n} + 2b_3\sqrt{m_1n_1})$ (9)

e chamando $c_i = 2b_i \in \mathbb{Z}$ para $i = 0,1,2,3$ teremos:

$$c_0 \equiv_2 c_1 \equiv_2 c_2 \equiv_2 c_3 \equiv_2 0 \quad e$$

$$c_0 - c_1 \pm c_2 - c_3 = 2(b_0 - b_3) \pm 2(b_2 - b_1) \equiv_4 0 .$$

Portanto valem os casos (i) e (ii) do teorema.

Se $2a_i = b_i$ é metade de um inteiro ímpar podemos escrever (2) como $\theta = \frac{1}{4}(c_0 + c_1\sqrt{m} + c_2\sqrt{n} + c_3\sqrt{m_1n_1})$ com $c_i \in \mathbb{Z}$, $\forall i$ e $c_0 \equiv_2 c_1 \equiv_2 c_2 \equiv_2 c_3 \equiv_2 1$.

Com isso temos
$$\begin{cases} c = \dfrac{c_0^2 - m_1n_1c_3^2}{4} \in \mathbb{Z} \\ d = \dfrac{c_0^2 - mc_1^2 - nc_2^2 + m_1n_1c_3^2}{4} \in \mathbb{Z} \\ e = \dfrac{c_0c_3 - c_1c_2\lambda}{2} \in 2\mathbb{Z} \end{cases} \quad (10)$$

e sendo $\lambda \equiv_2 1$, $m \equiv_4 n \equiv_4 m_1n_1 \equiv_4 1$.

Como $c_0^2 - mc_1^2 - nc_2^2 + m_1n_1c_3^2 \equiv_8 1 - m - n + m_1n_1$

$$\equiv_8 1 - m - n + m_1n_1\lambda^2 \quad (11)$$

e $\lambda m_1 = m$, $\lambda n_1 = n$ temos de (11) que:

$$c_0^2 - mc_1^2 - nc_2^2 + m_1 n_1 c_3^2 \equiv_8 (1 - m)(1 - n) \equiv_8 0 .$$

Assim podemos concluir que d é par.

Sabemos de (7) que θ satisfaz o polinômio abaixo,

$$X^4 - c_0 X^3 + \left(c + \frac{d}{2}\right)X^2 + \left(\frac{c_3 m_1 n_1 e - c_0 d}{4}\right)X + \left(\frac{d^2 - m_1 n_1 e^2}{16}\right) \qquad (12)$$

e também que $\theta \notin \mathbb{Q}(\sqrt{m})$, $\mathbb{Q}(\sqrt{n})$, $\mathbb{Q}(\sqrt{m_1 n_1})$, pois caso contrário teríamos $c_i \equiv_2 0$ para algum i.

Já que os coeficientes de (12) devem ser inteiros, temos:

$$d^2 - m_1 n_1 e^2 \equiv_{16} 0 \qquad (13)$$

Porém como $d \equiv_2 0$ e $m_1 n_1 \equiv_4 1$, de (13) obtemos pela observação (b) parte (i) que $d \equiv_4 e$.

Escrevendo $c_i = 2d_i + 1$ $(i = 0,1,2,3)$ temos:

$$d = \frac{c_0^2 - mc_1^2 - nc_2^2 + m_1 n_1 c_3^2}{4}$$

$$= \frac{(2d_0 + 1)^2 - m(2d_1 + 1)^2 - n(2d_2 + 1)^2 + m_1 n_1 (2d_3 + 1)^2}{4}$$

$$= \left(d_0^2 - md_1^2 - nd_2^2 + m_1 n_1 d_3^2\right) + \left(d_0 - md_1 - nd_2 + m_1 n_1 d_3\right) + \frac{1 - m - n + m_1 n_1}{4}$$

Agora observe que :

$1 - m - n + m_1n_1 = (1 - m_1)(1 - n_1) + (1 - \lambda)(m_1 + n_1)$ e portanto

$1 - m - n + m_1n_1 - 2(1 - \lambda) = (1 - m_1)(1 - n_1) + (1 - \lambda)(m_1 + n_1 - 2)$

Assim, se $\lambda \equiv_4 1$, como $(m_1,n_1) \equiv_4 (1,1)$, teremos que

$1 - m - n + m_1n_1 - 2(1 - \lambda) \equiv_{16} 0$, isto é, $\dfrac{1 - m - n + m_1n_1}{4} \equiv_4 \dfrac{1 - \lambda}{2}$

e desta forma $d \equiv_4 \left(d_0^2 - d_1^2 - d_2^2 + d_3^2\right) + d_0 - d_1 - d_2 + d_3 + \dfrac{1 - \lambda}{2}$

Agora $e = \dfrac{(c_0c_3 - c_1c_2\lambda)}{2}$, logo

$$e = \frac{4d_0d_3 + 2d_0 + 2d_3 + 1 - 4d_1d_2\lambda - 2d_1\lambda - 2d_2\lambda - \lambda}{2}$$

$$= (2d_0d_3 - 2d_1d_2\lambda) + (d_0 - \lambda d_1 - \lambda d_2 + d_3) + \left(\frac{1 - \lambda}{2}\right)$$

Assim se $\lambda \equiv_4 1$ e $(m_1,n_1) \equiv_4 (1,1)$ temos que, $d \equiv_4 e$ implica que $(d_0 - d_3)^2 - (d_1 - d_2)^2 \equiv_4 0$, isto é, $d_0 - d_3 \equiv_2 d_1 - d_2$; ou $c_0 - c_1 + c_2 - c_3 \equiv_4 0$ o que completa a prova do caso (1).

Se $\lambda \equiv_4 3$ e $(m_1,n_1) \equiv_4 (3,3)$, como :

$1 - m - n + m_1n_1 = (1 - m_1)(1 - n_1) + (1 - \lambda)(m_1 + n_1)$

temos que :

$1 - m - n + m_1 n_1 - 2(1 + \lambda) = (1 + m_1)(1 + n_1) - (1 + \lambda)(m_1 + n_1 + 2) \equiv_{16} 0,$

isto é,

$$\frac{1 - m - n + m_1 n_1}{4} \equiv_4 \frac{1 - \lambda}{2} .$$

Assim:

$$d \equiv_4 \left(d_0^2 - d_1^2 - d_2^2 + d_3^2\right) + d_0 - d_1 - d_2 + d_3 + \frac{1 + \lambda}{2}$$

Agora como $d \equiv_4 e$ e $e \equiv_4 2d_0d_3 + 2d_1d_2 + d_0 + d_1 + d_2 + d_3 + \frac{\lambda - 1}{2}$

temos que , $(d_0 - d_3)^2 - (d_1 + d_2)^2 - 2(d_1 + d_2) - 1 \equiv_4 0$, isto é,

$d_0 - d_3 \equiv_2 d_1 + d_2 + 1$, o que implica em $c_0 - c_1 - c_2 - c_3 \equiv_4 0$,

como queríamos para provar o caso (ii) do teorema ■

De posse deste resultado, fica bastante facilitado o trabalho de explicitar inteiros de um corpo biquadrático e também, ao examinarmos sua demonstração obtemos um algorítmo para o cálculo do polinômio característico de um elemento inteiro.

Vejamos isto nos exemplos a seguir.

Exemplo 1 : Seja $\theta = \frac{1}{4}(5 + 3\sqrt{5} + \sqrt{13} + 3\sqrt{65})$.

Podemos afirmar que θ é um inteiro de $\mathbb{Q}(\sqrt{5},\sqrt{13})$ e mais, que θ é raíz do polinômio

$$f(X) = X^4 - 5X^3 - 71X^2 + 120X + 1044 .$$

De fato, $\begin{cases} m = 5 \\ n = 13 \end{cases}$, o que implica $\lambda = 1$, $m_1 = 5$ e $n_1 = 13$.

Logo $(m,n) \equiv_4 (m_1,n_1) \equiv_4 (1,1)$ o que, pelo teorema 1 parte (i), nos dá a forma dos inteiros de $\mathbb{Q}(\sqrt{5},\sqrt{13})$, isto é, θ é inteiro de $\mathbb{Q}(\sqrt{5},\sqrt{13})$ se podemos escrevê-lo como:

$$\theta = \frac{1}{4}(x_0 + x_1\sqrt{5} + x_2\sqrt{13} + x_3\sqrt{65})$$

onde $x_0 \equiv_2 x_1 \equiv_2 x_2 \equiv_2 x_3$ e $x_0 - x_1 + x_2 - x_3 \equiv_4 0$.

De fato $5 \equiv_2 3 \equiv_2 1$ e $5 - 3 + 1 - 3 \equiv_4 0$ então o θ dado é inteiro de $\mathbb{Q}(\sqrt{5}, \sqrt{13})$.

Da demonstração temos que θ é raíz do polinômio $f(X)$ dado, pois calculando os valores de c, d, e, obtemos:

$$c = -140, \quad d = 138, \quad e = 6 \ \blacksquare$$

Exemplo 2 : Será $\theta = \frac{1}{4}(1 + \sqrt{21} + \sqrt{33} - \sqrt{77})$ inteiro do corpo $\mathbb{Q}(\sqrt{21},\sqrt{33})$?

Sim , pois $\begin{cases} m = 21 \\ n = 33 \end{cases}$, o que implica $\lambda = 3$, $m_1 = 7$ e $n_1 = 11$

Assim $(m_1,n_1) \equiv_4 (3,3)$ e $(m,n) \equiv_4 (1,1)$ e portanto pelo teorema 1 parte (ii), temos que os inteiros de $\mathbb{Q}(\sqrt{21}, \sqrt{33})$ são da forma:

$$\theta = \frac{1}{4}(x_0 + x_1\sqrt{21} + x_2\sqrt{33} + x_3\sqrt{77})$$

com $x_0 \equiv_2 x_1 \equiv_2 x_2 \equiv_2 x_3$ e $x_0 - x_1 - x_2 - x_3 \equiv_4 0$.

Como $1 \equiv_2 -1$, temos o que queríamos; e mais , calculando c, d, e como descrito na demonstração obtemos:

$$c = -19 \quad , \quad d = 6 \quad , \quad e = -2$$

Logo θ é raíz do polinômio $X^4 - X^3 - 16X^2 + 37X - 17$ ■

2.3. BASE INTEGRAL :

Como sabemos $\mathbb{Z}$ é principal e porisso a extensão de corpos $\mathbb{K}/\mathbb{Q}$ possui sempre uma base integral, isto é, o anel de inteiros, $\mathbb{B}$, de $\mathbb{K}$ é sempre um $\mathbb{Z}$-módulo livre.

De posse da forma explícita do anel $\mathbb{B}$, em cada caso, poderemos procurar uma base integral de $\mathbb{K}$ sobre $\mathbb{Q}$, já que ela existe.

Seja Θ um inteiro de $\mathbb{K} = \mathbb{Q}(\sqrt{m},\sqrt{n})$.

Se $(m,n) \equiv_4 (1,1)$ e $(m_1,n_1) \equiv_4 (1,1)$. Pela parte (i) do teorema 1 temos

$$\Theta = \frac{1}{4}(x_0 + x_1\sqrt{m} + x_2\sqrt{n} + x_3\sqrt{m_1 n_1})$$

com $x_0 \equiv_2 x_1 \equiv_2 x_2 \equiv_2 x_3$ e $x_0 - x_1 + x_2 - x_3 \equiv_4 0$.

Fazendo $z_3 = x_3$ então $x_0 \equiv_2 x_1 \equiv_2 x_2 \equiv_2 z_3$ e portanto existem $y, z_1, z_2 \in \mathbb{Z}$ tal que $\begin{cases} x_0 = z_3 + 2y \\ x_1 = z_3 + 2z_1 \\ x_2 = z_3 + 2z_2 \end{cases}$

Agora, como $x_0 - x_1 + x_2 - x_3 \equiv_4 0$, nós temos

$$z_3 + 2y - z_3 - 2z_1 + z_3 + 2z_2 - z_3 \equiv_4 0 \quad \Rightarrow$$

$$2y - 2z_1 + 2z_2 \equiv_4 0 \quad \Rightarrow \quad y - z_1 + z_2 \equiv_2 0 \quad \Rightarrow$$

$y \equiv_2 z_2 + z_1$, isto é existe $z_0 \in \mathbb{Z}$ tal que $y = 2z_0 + z_1 + z_2$.

Substituindo os resultados conseguidos acima na expressão de Θ obtemos

$$\Theta = z_0 + z_1\left(\frac{1 + \sqrt{m}}{2}\right) + z_2\left(\frac{1 + \sqrt{n}}{2}\right) + z_3\left(\frac{1 + \sqrt{m} + \sqrt{n} + \sqrt{m_1 n_1}}{4}\right)$$

e como $\frac{1 + \sqrt{m}}{2}$, $\frac{1 + \sqrt{n}}{2}$, $\frac{1 + \sqrt{m} + \sqrt{n} + \sqrt{m_1 n_1}}{4}$ são inteiros da extensão $\mathbb{K}/\mathbb{Q}$ encontramos aí uma base integral, a saber,

$$\left\{ 1 , \frac{1 + \sqrt{m}}{2} , \frac{1 + \sqrt{n}}{2} , \frac{1 + \sqrt{m} + \sqrt{n} + \sqrt{m_1 n_1}}{4} \right\}.$$

Se $(m,n) \equiv_4 (1,2)$, pela parte (iii) do teorema 1

$\Theta = \frac{1}{2} (x_0 + x_1\sqrt{m} + x_2\sqrt{n} + x_3\sqrt{m_1 n_1})$ com $x_0 \equiv_2 x_1$, $x_2 \equiv_2 x_3$.

Chamemos $\begin{cases} z_1 = x_1 \\ z_3 = x_3 \end{cases}$ então $\begin{cases} x_2 = 2z_2 + z_3 \\ x_0 = 2z_0 + z_1 \end{cases}$ e daí :

$$\Theta = \frac{1}{2} (z_1 + 2z_0 + z_1\sqrt{m} + z_3\sqrt{n} + 2z_2\sqrt{n} + z_3\sqrt{m_1 n_1}) =$$

$$= z_0 + z_1\left(\frac{1 + \sqrt{m}}{2} \right) + z_2\sqrt{n} + z_3\left(\frac{\sqrt{n} + \sqrt{m_1 n_1}}{2} \right).$$

Logo $\left\{ 1 , \frac{1 + \sqrt{m}}{2}, \sqrt{n} , \frac{\sqrt{n} + \sqrt{m_1 n_1}}{2} \right\}$ é uma base integral de $\mathbb{K}/\mathbb{Q}$.

Para o caso $(m,n) \equiv_4 (2,3)$, procedendo da mesma maneira obtemos a seguinte base integral para a extensão de corpos $\mathbb{K}/\mathbb{Q}$:

$$\left\{ 1 , \sqrt{m} , \sqrt{n} , \frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right\}$$

e para $(m,n) \equiv_4 (3,3)$ obtemos como base integral os elementos

$$\left\{ 1 \, , \, \sqrt{m} \, , \, \frac{\sqrt{m} + \sqrt{n}}{2} \, , \, \frac{1 + \sqrt{m_1 n_1}}{2} \right\}.$$

Podemos então sintetizar os resultados obtidos anteriormente no que será nosso resultado principal deste parágrafo.

TEOREMA 2 : Uma base integral para a extensão de corpos $\mathbb{K}/\mathbb{Q}$ é dada por:

i) $$\left\{ 1 \, , \, \frac{1 + \sqrt{m}}{2} \, , \, \frac{1 + \sqrt{n}}{2} \, , \, \frac{1 + \sqrt{m} + \sqrt{n} + \sqrt{m_1 n_1}}{4} \right\}$$

se $(m,n) \equiv_4 (1,1)$ e $(m_1,n_1) \equiv_4 (1,1)$.

ii) $$\left\{ 1 \, , \, \frac{1 + \sqrt{m}}{2} \, , \, \frac{1 + \sqrt{n}}{2} \, , \, \frac{1 - \sqrt{m} + \sqrt{n} + \sqrt{m_1 n_1}}{4} \right\}$$

se $(m,n) \equiv_4 (1,1)$ e $(m_1,n_1) \equiv_4 (3,3)$.

iii) $$\left\{ 1 \, , \, \frac{1 + \sqrt{m}}{2} \, , \, \sqrt{n} \, , \, \frac{\sqrt{n} + \sqrt{m_1 n_1}}{2} \right\}$$

se $(m,n) \equiv_4 (1,2)$.

iv) $\left\{ 1 , \sqrt{m} , \sqrt{n} , \frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right\}$

se $(m,n) \equiv_4 (2,3)$.

v) $\left\{ 1 , \sqrt{m} , \frac{\sqrt{m} + \sqrt{n}}{2} , \frac{1 + \sqrt{m_1 n_1}}{2} \right\}$

se $(m,n) \equiv_4 (3,3)$.

Com a finalidade de exemplificar o teorema 2 vejamos:

EXEMPLO 3 : Seja $\mathbb{K} = \mathbb{Q}(\sqrt{5}, \sqrt{13})$ como no exemplo 1.

Vimos que $\theta = \frac{1}{4}(5 + 3\sqrt{5} + \sqrt{13} + 3\sqrt{65})$ é inteiro da extensão $\mathbb{K} = \mathbb{Q}(\sqrt{5}, \sqrt{13})$ sobre $\mathbb{Q}$ e, em termos da base integral

$$\left\{ \alpha_0 , \alpha_1 , \alpha_2 , \alpha_3 \right\} =$$

$$= \left\{ 1 , \frac{1 + \sqrt{5}}{2} , \frac{1 + \sqrt{13}}{2} , \frac{1 + \sqrt{5} + \sqrt{13} + \sqrt{65}}{4} \right\}$$

é dado por $\theta = \alpha_0 - \alpha_2 + 3\alpha_3$ ■

2.4.DISCRIMINANTE ABSOLUTO :

Como sabemos, o ideal discriminante de um corpo de números algébricos é gerado por elementos, que são discriminantes de bases integrais; logo em $\mathbb{Z}$ tais discriminantes se diferem por $\pm$ 1.

Assim, uma vez conhecida uma base integral da extensão $K/\mathbb{Q}$ podemos provar o resultado seguinte, o qual será ponto de partida no nosso próximo capítulo.

TEOREMA 3 : O discriminante absoluto de $K = \mathbb{Q}(\sqrt{m},\sqrt{n})$ sobre $\mathbb{Q}$ é dado por:

i) $\lambda^2 m_1^2 n_1^2$, se $(m,n) \equiv_4 (1,1)$.

ii) $16\lambda^2 m_1^2 n_1^2$, se $(m,n) \equiv_4 (1,2)$ ou $(3,3)$.

iii) $64\lambda^2 m_1^2 n_1^2$, se $(m,n) \equiv_4 (2,3)$.

DEMONSTRAÇÃO:

1)Do teorema 2 obtemos

$$\left\{ \alpha_0 \ , \ \alpha_1 \ , \ \alpha_2 \ , \ \alpha_3 \right\} =$$

$$= \left\{ 1 \ , \ \frac{1 + \sqrt{m}}{2}, \ \frac{1 + \sqrt{n}}{2}, \ \frac{1 \pm \sqrt{m} + \sqrt{n} \pm \sqrt{m_1 n_1}}{4} \right\}$$

uma base integral se $(m,n) \equiv_4 (1,1)$.

Chamemos $d = D(\alpha_0,\alpha_1,\alpha_2,\alpha_3)$.

Sabemos portanto que:

$$d = \begin{vmatrix} Tr(\alpha_0^2) & Tr(\alpha_1) & Tr(\alpha_2) & Tr(\alpha_3) \\ Tr(\alpha_1) & Tr(\alpha_1^2) & Tr(\alpha_1\alpha_2) & Tr(\alpha_1\alpha_3) \\ Tr(\alpha_2) & Tr(\alpha_2\alpha_1) & Tr(\alpha_2^2) & Tr(\alpha_2\alpha_3) \\ Tr(\alpha_3) & Tr(\alpha_3\alpha_1) & Tr(\alpha_3\alpha_2) & Tr(\alpha_3^2) \end{vmatrix} =$$

$$= \begin{vmatrix} 4 & 2 & 2 & 1 \\ 2 & 1+m & 1 & \frac{1+m}{2} \\ 2 & 1 & 1+n & \frac{1+n}{2} \\ 1 & \frac{1+m}{2} & \frac{1+n}{2} & \frac{1+m+n+m_1n_1}{4} \end{vmatrix} =$$

$$= mnm_1n_1 = \lambda^2 m_1^2 n_1^2 .$$

Nos casos (ii) e (iii) a prova é análoga □

EXEMPLO 4 : O discriminante do corpo $\mathbb{K} = \mathbb{Q}(\sqrt{2},\sqrt{3})$ é 256 pois,

$(m,n) \equiv_4 (2,3)$, $\lambda = 1$, $m_1 = 2$ e $n_1 = -1$.

Logo $d = 64\lambda^2 m_1^2 n_1^2 = 256$ ■

CAPÍTULO 3

BASE INTEGRAL DE UM CORPO BIQUADRÁTICO BICÍCLICO SOBRE UM SUBCORPO QUADRÁTICO

3.1. INTRODUÇÃO :

Dados $\mathbb{K}$ um corpo biquadrático bicíclico e k um subcorpo quadrático de $\mathbb{K}$, sabemos que o anel $\mathbb{A}$, dos inteiros do corpo k, é um anel de Dedekind que nem sempre é principal. Desta forma, a indagação primeira do nosso trabalho, **"Quando $\mathbb{B}$, anel de inteiros do corpo biquadratico $\mathbb{K}$ e um $\mathbb{A}$-modulo livre?"**, não possui uma resposta imediata.

Neste contexto o estudo feito aqui tem como objetivos:

1)Responder, explicitando condições, esta questão.

2)Fornecer uma base integral da extensão $\mathbb{K}/k$, sempre que exista.

Com este intuito dividiremos nosso trabalho em dois casos, primeiramente considerando k um corpo quadrático

imaginário, isto é, $k = \mathbb{Q}(\sqrt{m})$ com $m < 0$; e em segundo lugar o caso em que k é um corpo real, ou seja, $m > 0$.

Observe que como $\mathbb{K}$ é corpo biquadrático e $k = \mathbb{Q}(\sqrt{m})$, onde $m \in \mathbb{Z}$ e é livre de quadrados, podemos encontrar um inteiro n, também livre de quadrados tal que $\mathbb{K} = \mathbb{Q}(\sqrt{m},\sqrt{n})$.

Como no capítulo anterior usaremos congruência módulo 4 para m, n, $m_1 n_1$ (lembre-se que $m = \lambda m_1$ e $n = \lambda n_1$, onde $mdc(m,n) = \lambda$).

Note que $\mathbb{Q}(\sqrt{m},\sqrt{n}) = \mathbb{Q}(\sqrt{m},\sqrt{m_1 n_1})$, logo podemos considerar apenas os casos :

$$(m,n) \equiv_4 (1,1),\ (1,2),\ (1,3),\ (2,1),\ (2,3),\ (3,1) \text{ e } (3,2)$$

Para atacar os objetivos citados os próximos dois resultados, **Criterio de Mann**, [02], e **Lema 1**, [06], são fundamentais. As demonstrações que encontramos, destes resultados, na literatura envolvem o conceito de **diferente**, que é um conceito mais sofisticado. Assim para que o nosso trabalho mantivesse um caráter mais elementar preferimos procurar demonstrá-los evitando o conceito de diferente. Conseguimos fazer isto, mas as demonstrações ficaram um tanto longas, assim optamos por apresentá-las num apêndice.

Portanto neste capítulo apenas enunciaremos os tais resultados.

TEOREMA 1 (CRITÉRIO DE MANN): Sejam $\mathbb{K}/k$ uma extensão quadrática, com $ch\mathbb{K} = 0$ [1] e $\mathcal{D}_{\mathbb{K}/k}$ o ideal discriminante de $\mathbb{K}/k$.

Então existe uma base integral de $\mathbb{K}/k$, se e somente se, $\mathbb{K} = k(\sqrt{d})$, onde $\mathcal{D}_{\mathbb{K}/k} = d\mathbb{A}$.

LEMA 1 : Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{m},\sqrt{n})$, $k = \mathbb{Q}(\sqrt{m})$ e $\mathcal{D}_{\mathbb{K}/k}$ o ideal discriminante de $\mathbb{K}/k$. Como sempre $\mathbb{A}$ é o anel de inteiros de k e $\mathbb{B}$ o anel de inteiros de $\mathbb{K}$.

i) Se $n \equiv_4 1$ ou $m_1 n_1 \equiv_4 1$ então

$$\mathcal{D}_{\mathbb{K}/k} = n_1\mathbb{A}.$$

ii) Se $n \not\equiv_4 1$ e $m \equiv_4 1$ então

$$\mathcal{D}_{\mathbb{K}/k} = 4n_1\mathbb{A}.$$

iii) Se $m \not\equiv_4 1$, $n \not\equiv_4 1$ e $m_1 n_1 \not\equiv_4 1$ então

$$\mathcal{D}_{\mathbb{K}/k} = 2n_1\mathbb{A}.$$

De posse destes resultados partimos em busca de respostas mais objetivas.

---

1) Vale igualmente para $ch\mathbb{K} \neq 2$ [03].

3.2. CORPO QUADRÁTICO IMAGINÁRIO :

Nesta parte do trabalho temos como resultado importante o teorema que passamos a enunciar.

TEOREMA 2 : Seja $k = \mathbb{Q}(\sqrt{m})$ corpo quadrático imaginário ($m < 0$).

Então a extensão $\mathbb{K}/k$ possui base integral, se e somente se, vale uma das condições abaixo:

a) $\left[(m \equiv_4 1 \text{ ou } n \equiv_4 1\right] e \left[\lambda = 1 \text{ ou } \lambda = -m\right]$.

b) $(m,n) \equiv_4 (2,3)$ e $m = -2\lambda$.

c) $m = -1$.

DEMONSTRAÇÃO:

Se $m = -1$ ou $m = -3$, já sabemos que o anel de inteiros de $\mathbb{Q}(\sqrt{m})$ é principal e portanto nestes casos o teorema é verdadeiro. Logo podemos supor que $m \neq -1$ e $m \neq -3$ e assim o grupo de unidades de $\mathbb{Q}(\sqrt{m})$ é $\{\pm 1\}$.

a) Seja $m \equiv_4 1$ ou $n \equiv_4 1$.

Desejamos mostrar que:

$\mathbb{K}/k$ tem base integral $\Leftrightarrow$ $\lambda = 1$ ou $\lambda = -m$

AFIRMAÇÃO : $\mathbb{K}/k$ tem base integral $\Leftrightarrow$ $\mathbb{K} = k(\sqrt{\pm n_1})$.

De fato, pelo Lema 1 temos $\mathcal{D}_{\mathbb{K}/k} = n_1\mathbb{A}$ ou $4n_1\mathbb{A}$, isto é , $d = \pm n_1$ ou $d = \pm 4n_1$ para $\mathcal{D}_{\mathbb{K}/k} = d\mathbb{A}$.

Assim usando o Teorema 1 obtemos o que queríamos, pois $\mathbb{K} = k(\sqrt{\pm 4n_1}) = k(2\sqrt{\pm n_1}) = k(\sqrt{\pm n_1})$.

Mediante o resultado provado, podemos concluir que $\mathbb{Q}(\sqrt{\pm n_1})$ é um subcorpo quadrático de $\mathbb{K}$ e neste caso $\mathbb{Q}(\sqrt{\pm n_1}) = \mathbb{Q}(\sqrt{n})$ ou $\mathbb{Q}(\sqrt{m_1 n_1})$. Portanto consideremos os casos:

i) $\mathbb{Q}(\sqrt{\pm n_1}) = \mathbb{Q}(\sqrt{n}) \Rightarrow \psi = \dfrac{\sqrt{n}}{\sqrt{\pm n_1}} \in \mathbb{Q} \Rightarrow \psi = \sqrt{\pm\lambda} \in \mathbb{Q} \Rightarrow$ $\lambda = \pm\psi^2$ com $\psi \in \mathbb{Q}$ e λ livre de quadrados .Logo $\psi = \pm 1$ e assim $\lambda = 1$, pois $\lambda > 0$.

ii) $\mathbb{Q}(\sqrt{\pm n_1}) = \mathbb{Q}(\sqrt{m_1 n_1}) \Rightarrow \psi = \dfrac{\sqrt{m_1 n_1}}{\sqrt{\pm n_1}} \in \mathbb{Q} \Rightarrow \psi = \sqrt{\pm m_1} \in \mathbb{Q} \Rightarrow$ $\pm m_1 = \psi^2$ com $\psi \in \mathbb{Q}$ e m_1 livre de quadrados. Logo $\psi = \pm 1$ e portanto $m_1 = -1$, pois $\lambda > 0$.

b) Seja agora $(m,n) \equiv_4 (2,3)$ e mostremos que:

$\mathbb{K}/k$ possui base integral, se e somente se, $m = -2\lambda$.

Do Lema 1 e Critério de Mann obtemos:

$\mathbb{K}/k$ tem base integral, se e somente se, $\mathbb{K} = k(\sqrt{2n_1})$.

Logo $\mathbb{Q}(\sqrt{\pm 2n_1})$ é um subcorpo quadrático do corpo $\mathbb{K}$ e portanto $\mathbb{Q}(\sqrt{\pm 2n_1}) = \mathbb{Q}(\sqrt{n})$ ou $\mathbb{Q}(\sqrt{m_1 n_1})$. Porem note que :

i) $\mathbb{Q}(\sqrt{\pm 2n_1}) = \mathbb{Q}(\sqrt{n}) \Rightarrow \psi = \dfrac{\sqrt{n}}{\sqrt{\pm 2n_1}} \in \mathbb{Q} \Rightarrow \psi = \dfrac{\sqrt{\lambda}}{\sqrt{\pm 2}} \in \mathbb{Q}$

$\dfrac{\lambda}{2} = \pm\psi^2$ com $\psi \in \mathbb{Q}$ e λ livre de quadrados.

Então $\psi = \pm 1$, que implica $\lambda = 2$. Logo $n = 2n_1 \equiv_4 0$ ou 2 , que é uma contradição.

ii) $\mathbb{Q}(\sqrt{\pm 2n_1}) = \mathbb{Q}(\sqrt{m_1 n_1}) \Rightarrow \psi = \dfrac{\sqrt{m_1 n_1}}{\sqrt{\pm 2n_1}} \in \mathbb{Q} \Rightarrow \psi = \dfrac{\sqrt{m_1}}{\sqrt{\pm 2}} \in \mathbb{Q}$

$m_1 = \pm 2\psi^2$ com $\psi \in \mathbb{Q}$ e m_1 livre de quadrados.

Logo $\psi = \pm 1$, que nos dá $m_1 = -2$ e portanto $m = -2\lambda$.

c) Consideremos, para finalizar, $(m,n) \equiv_4 (3,2)$.

Nosso interesse aqui é provar que $\mathbb{K}/k$ tem base integral, se e somente se, $m = -1$.

Suponhamos então que $m \neq -1$. Como também, $m \neq -3$ temos que as unidades de k são ± 1.

Do Lema 1 e do Critério de Mann sabemos que:

$\mathbb{K}/k$ tem base integral, se e somente se, $\mathbb{K} = k(\sqrt{\pm 2n_1})$.

Repetindo o argumento usado em (a) e (b) obtemos:

$$\mathbb{Q}(\sqrt{\pm 2n_1}) = \mathbb{Q}(\sqrt{n}) \quad \text{ou} \quad \mathbb{Q}(\sqrt{m_1 n_1})$$

Mas novamente $\mathbb{Q}(\sqrt{\pm 2n_1}) = \mathbb{Q}(\sqrt{n})$, nos dá uma contradição e também $\mathbb{Q}(\sqrt{\pm 2n_1}) = \mathbb{Q}(\sqrt{m_1 n_1})$, implica que $m_1 = \pm 2$, que é impossível.

Portanto $m = -1$ ■

Agora apresentaremos bases integrais para as extensões de corpos $\mathbb{K}/k$ onde $\mathbb{K} = k(\sqrt{n})$ e $k = \mathbb{Q}(\sqrt{m})$, em cada caso que exista.

TABELA 1

BASE	$(m,n) \equiv_4$	CONDIÇÕES
$1\ ,\ (1 + \sqrt{n})/2$	$(m,1)$	$\lambda = 1$
$1\ ,\ (\sqrt{m} + \sqrt{m_1 n_1})/2$	$(m,1)$	$\lambda = \lvert m \rvert$
$1\ ,\ \sqrt{n_1}$	$(1,n), n \not\equiv_4 1$	$\lambda = 1$ ou $\lvert m \rvert$
$1\ ,\ (\sqrt{m} + \sqrt{m_1 n_1})/2$	$(2,3)$	$\lambda = \lvert m/2 \rvert$
$1\ ,\ (\sqrt{n} + \sqrt{-n})/2$	$(3,2)$	$m = -1$

Observamos que, verdadeiramente, estas são bases integrais em cada caso especificado.

Para o caso $(m,n) \equiv_4 (m,1)$ com $\lambda = 1$ sabemos da proposição 4, capítulo 1 que:

$$D\left[1,(1 + \sqrt{n})/2\right] = \begin{vmatrix} 1 & \frac{1 + \sqrt{n}}{2} \\ 1 & \frac{1 - \sqrt{n}}{2} \end{vmatrix}^2 = n = n_1 \quad \text{pois } \lambda = 1.$$

Pelo Lema 1 parte (a), $\mathcal{D}_{\mathbb{K}/k} = n_1 \mathbb{A}$, portanto do Critério de Mann $\left\{1,(1 + \sqrt{n})/2\right\}$ é uma base integral para $\mathbb{K}/k$. Mas se $\lambda = -m$ obtemos:

$$D\left(1,(\sqrt{m}+\sqrt{m_1 n_1})/2\right) = \begin{vmatrix} 1 & \dfrac{\sqrt{m}+\sqrt{m_1 n_1}}{2} \\ 1 & \dfrac{\sqrt{m}-\sqrt{m_1 n_1}}{2} \end{vmatrix}^2 = m_1 n_1 = n_1$$

pois $\lambda = -m$ e então $m_1 = 1$. Logo pelo Critério de Mann $\left\{ 1 , (\sqrt{m}+\sqrt{m_1 n_1})/2 \right\}$ é base integral.

Para o caso $(m,n) \equiv_4 (1,n)$ com $n \not\equiv_4 1$ e $\lambda = 1$ ou $-m$, temos que:

$$D\left(1,\sqrt{n}\right) = \begin{vmatrix} 1 & \sqrt{n_1} \\ 1 & -\sqrt{n_1} \end{vmatrix}^2 = 4n_1$$

assim pelo Lema 1 e Critério de Mann podemos concluir que $\left\{ 1 , \sqrt{n} \right\}$ é base integral para $\mathbb{K}/k$.

Para $(m,n) \equiv_4 (2,3)$ e $\lambda = \dfrac{m}{2}$, temos :

$$D\left(1,(\sqrt{m}+\sqrt{m_1 n_1})/2\right) = \begin{vmatrix} 1 & \dfrac{\sqrt{m}+\sqrt{m_1 n_1}}{2} \\ 1 & \dfrac{\sqrt{m}-\sqrt{m_1 n_1}}{2} \end{vmatrix}^2 = m_1 n_1 \quad , \text{ mas como}$$

$m = \lambda m_1$ concluimos que $D\left(1,(\sqrt{m}+\sqrt{m_1 n_1})/2\right) = 2n_1$.

Logo temos, novamente pelo Critério de Mann, uma base integral de $\mathbb{K}/k$, no caso de $(m,n) \equiv_4 (2,3)$.

Para o caso $(m,n) \equiv_4 (3,2)$ com $m = -1$ obtemos:

$$D\left(1,(\sqrt{n} + \sqrt{-n})/2\right) = \begin{vmatrix} 1 & \frac{\sqrt{n} + \sqrt{-n}}{2} \\ 1 & \frac{-\sqrt{n} - \sqrt{-n}}{2} \end{vmatrix}^2 = 2n = 2n_1$$

pois $m = -1$ implica $\lambda = 1$.

Assim concluímos que $\left\{ 1 , (\sqrt{n} + \sqrt{-n})/2 \right\}$ é uma base integral para $\mathbb{K}/k$.

Nosso próximo resultado é uma versão forte do Teorema 4 de [03] para o caso quadrático.

COROLÁRIO 1: Seja $k = \mathbb{Q}(\sqrt{m})$ um corpo imaginário. Então k tem número de classe ímpar, se e somente se, $\mathbb{K} = k(\sqrt{n})$ tem uma base integral sobre k, qualquer que seja n inteiro tal que n é livre de quadrados.

DEMONSTRAÇÃO:

Se o número de classe é 1 então $\mathbb{A}$ é principal, logo existe sempre uma base integral de $\mathbb{K}/k$.

Por outro lado sabe-se (veja [01]) que $k = \mathbb{Q}(\sqrt{m})$ com $m < 0$ tem número de classe ímpar, se e somente se, $m = -1$, -2 ou $-p$ sendo p primo ímpar e $p \equiv_4 3$. Como é sabido, para $m = -1$ ou -2

temos $\mathbb{A}$ principal. Assim basta que nos restrinjamos a $m \neq -1$ e $m \neq -2$.

Se $m = -p$ com p primo e $p \equiv_4 3$, temos que $m \equiv_4 1$ e assim $\lambda = 1$ ou p . Logo, pelo Teorema 2 parte (a), segue que para qualquer n livre de quadrados, $\mathbb{K} = k(\sqrt{n})$ tem base integral sobre k.

Reciprocamente se existem p e p' primos distintos tais que $p|m$ e $p'|m$ então tomando $n = ap$ onde $a \in \mathbb{Z}$, $mdc(a,m) = 1$ e $ap \equiv_4 1$, segue do teorema 2 parte (a) que $\mathbb{K} = k(\sqrt{n})$ não possui base integral sobre k .

Finalmente se $m = -p$ com p primo e $p \equiv_4 1$, então $m \equiv_4 3$ e desta maneira tomando n tal que $n \equiv_4 2$ segue pelo Teorema 2 que $\mathbb{K} = k(\sqrt{n})$ não possui base integral sobre k. Portanto $m = -1$, -2 , ou $-p$ com $p \equiv_4 3$.

3.3.CORPO QUADRÁTICO REAL:

Neste caso $k = \mathbb{Q}(\sqrt{m})$, com $m > 0$.

Já é sabido, utilizando o Critério de Mann e o Lema 1, que para a existência de base integral da extensão $\mathbb{K}/k$ é necessário e suficiente que $\mathbb{K} = k\left(\sqrt{2^{e}\varepsilon n_1}\right)$, onde $e = 0$ ou 1 e ε é uma unidade de k. Também sabemos que, se $\varepsilon \in \mathcal{U}(\mathbb{A})$ então existe $j \in \mathbb{Z}$ tal que $\varepsilon = \pm \varepsilon_0^j$, onde ε_0 é uma <u>unidade fundamental de k</u>. (2)

---

2) $\varepsilon \in \mathcal{U}(\mathbb{A}) \Rightarrow N(\varepsilon) \in \mathcal{U}(\mathbb{Z})$, ou seja, $N(\varepsilon) = \pm 1$.

Uma vez que trabalharemos com $\sqrt{\varepsilon}$, de j somente nos interessa a paridade, logo podemos colocar j = 0 , 1 ou 3 (esta última escolha feita apenas para podermos assumir que $\varepsilon = b + c\sqrt{m}$ com b,c $\in \mathbb{Z}$) (veja [04], p.76). Além disto quando $N(\varepsilon) = -1$, observe que j = 0 pois, suponhamos j = 1 . Logo

$$\mathbb{K} = k(\sqrt{n}) = k\left(\sqrt{2^e \varepsilon n_1}\right) \quad \text{e então}$$

$$x = \frac{\sqrt{2^e \varepsilon_0 n_1}}{\sqrt{n}} \in k = \mathbb{Q}(\sqrt{m}) \text{ , portanto}$$

$$N(x) = N\left(\frac{\sqrt{2^e \varepsilon_0}}{\sqrt{\lambda}}\right) \in \mathbb{Q} \text{ , e } \left[N(x)\right]^2 = N\left(\frac{2^e}{\lambda}\varepsilon_0\right) = \left(\frac{2^e}{\lambda}\right)^2 N(\varepsilon_0) = -\left(\frac{2^e}{\lambda}\right)^2$$

o que nos dá um absurdo, uma vez que $N(x) \in \mathbb{Q}$.

Agora se j = 0 então as condições do teorema 2 são necessárias e suficientes para garantir a existência de base integral de $\mathbb{K}$ sobre k. Sendo assim nos ocuparemos de corpos quadráticos reais k, onde $N(\varepsilon_0) = N(\varepsilon) = 1$.

Inicialmente demonstraremos um resultado sobre unidades o qual será várias vezes citado.

LEMA 2: Seja $\varepsilon = \varepsilon_0$ ou ε_0^3 da forma $b + c\sqrt{m}$ com $b,c \in \mathbb{Z}$ e $N(\varepsilon) = 1$.

i)Se $m \equiv_4 1$ ou 2 então $(b,c) \equiv_2 (1,0)$ e $c \equiv_4 0$ sempre que $m \equiv_4 1$. Além disto :

$$\sqrt{\varepsilon} = s\sqrt{u} + t\sqrt{v} \text{ com } mdc(u,v) = 1 \text{ e } uv = m \qquad (1)$$

ii)Se $m \equiv_4 3$ então $c \equiv_4 0$ e vale (1) ou

$$(b,c) \equiv_2 (0,1) \text{ e } \sqrt{\varepsilon} = \frac{s\sqrt{2u} + t\sqrt{2v}}{2} \text{ com } \begin{cases} mdc(u,v) = 1 \\ \text{e} \\ uv = m \end{cases} \qquad (2)$$

DEMONSTRAÇÃO:

Verifiquemos as condições de congruência.

Sabemos que $\varepsilon = b + c\sqrt{m}$ e $N(\varepsilon) = 1$, logo $b^2 - c^2m = 1$. Portanto no caso (i), isto é, quando $m \equiv_4 1$ ou 2 temos que $b^2 \equiv_4 1 + c^2$ ou $b^2 \equiv_4 1 + 2c^2$. Mas em $\mathbb{Z}_4$ os quadrados possíveis são 0 e 1 , portanto $c^2 \equiv_4 0$ e $b^2 \equiv_4 1$, isto é, $(b,c) \equiv_4 (1,0)$. Já no caso (ii), ou seja, quando $m \equiv_4 3$ temos que $b^2 \equiv_4 1 + 3c^2$, assim $(b,c) \equiv_2 (1,0)$ ou $(b,c) \equiv_2 (0,1)$.

Note que se $\varepsilon = b + c\sqrt{m}$ então $\varepsilon + 1 = (b + 1) + c\sqrt{m}$ e $\varepsilon - 1 = (b - 1) + c\sqrt{m}$. Logo observando as normas temos:

$$N(\varepsilon + 1) = (b + 1)^2 - c^2m = b^2 + 2b + 1 - c^2m = N(\varepsilon) + 2b + 1 =$$

$$= 2(b + 1)$$

$$-N(\varepsilon - 1) = -\left[(b - 1)^2 - c^2 m\right] = -\left[b^2 - 2b + 1 - c^2 m\right] = -\left[N(\varepsilon) - 2b + 1\right]$$

$$= 2(b - 1)$$

Portanto $\dfrac{\sqrt{N(\varepsilon + 1)} + \sqrt{-N(\varepsilon - 1)}}{2} =$

$$= \frac{\sqrt{2(b + 1)} + \sqrt{2(b - 1)}}{2}$$

Note também que:

$$\left[\frac{\sqrt{2(b + 1)} + \sqrt{2(b - 1)}}{2}\right]^2 =$$

$$= \frac{N(\varepsilon + 1) - N(\varepsilon - 1) + 2\sqrt{-N(\varepsilon + 1)(N(\varepsilon - 1)}}{4}$$

$$= \frac{4b + 2\sqrt{4b^2 - 4}}{4} = b + \sqrt{b^2 - 1} = b + c\sqrt{m} = \varepsilon. \qquad (3)$$

Assim,

$$\sqrt{\varepsilon} = \frac{\sqrt{N(\varepsilon + 1)} + \sqrt{-N(\varepsilon - 1)}}{2} = \frac{\sqrt{2(b + 1)} + \sqrt{2(b - 1)}}{2}.$$

---

3) $N(\varepsilon) = b^2 - c^2 m = 1 \Rightarrow b^2 - 1 = c^2 m \Rightarrow \sqrt{b^2 - 1} = c\sqrt{m}$

Quando b é ímpar então $\begin{cases} 2(b+1) = 4s^2u \\ 2(b-1) = 4t^2v \end{cases}$ (*)

sendo u, v livres de quadrados e mdc(u,v) = 1, pois $4 = 2(b+1) - 2(b-1) = 4(s^2u - t^2v)$ e portanto $1 = s^2u - t^2v$.

Desta forma:

$4(b+1)(b-1) = 4(4s^2t^2uv) \Rightarrow (b^2 - 1) = 4s^2t^2uv.$

Porem $(b^2 - c^2m) = N(\varepsilon) = 1$ então $c^2m = 4s^2t^2uv$,

assim $m = uv$ com mdc(u,v) = 1.

Concluimos, então, que:

$$\sqrt{\varepsilon} = \frac{\sqrt{2(b+1)} + \sqrt{2(b-1)}}{2} = \frac{2s\sqrt{u} + 2t\sqrt{v}}{2} = s\sqrt{u} + t\sqrt{v}\ .$$

Quando b é par temos $\begin{cases} b + 1 = s^2u \\ b - 1 = t^2v \end{cases}$, (**)

com u,v livres de quadrados.

Suponhamos que existe um p primo tal que $p \mid (b+1)$ e $p \mid (b-1)$, então p é ímpar e $p \mid 2b$, assim $p \mid b$ e $p \mid (b+1)$ absurdo. Logo mdc(b + 1, b - 1) = 1 e portanto, de (**), mdc(u,v) = 1 e mais :

$(b^2 - c^2m) = N(\varepsilon) = 1$

Logo $c^2m = (b^2 - 1) = (b + 1)(b - 1) = s^2t^2uv$ e então $m = uv$.

Assim:

$$\sqrt{\varepsilon} = \frac{s\sqrt{2u} + t\sqrt{2v}}{2} .$$

Provemos agora que quando $m \equiv_4 1$ temos $c \equiv_4 0$.

De fato, pois temos que :

$$c^2m = (b^2 - 1) = (b + 1)(b - 1) = 4s^2t^2uv$$

e como sabemos $b \equiv_2 1$, logo $(b + 1) \equiv_4 0$ ou $(b - 1) \equiv_4 0$, assim $s^2t^2uv \equiv_2 0$ então $s \equiv_2 0$ ou $t \equiv_2 0$. Portanto de (*) concluimos que :

$$b + 1 \equiv_{16} 0 \quad \text{ou} \quad b - 1 \equiv_{16} 0$$

Assim $c^2m \equiv_{16} 0$ e daí $c \equiv_4 0$.

Analogamente temos que se $m \equiv_4 3$ e b é ímpar , então $c \equiv_4 0$.

Nosso maior interesse nesta seção é o seguinte resultado:

TEOREMA 3: Seja $k = \mathbb{Q}(\sqrt{m})$ um corpo quadrático real.

Então a extensão $\mathbb{K}/k$ tem base integral, se e somente se, vale uma das seguintes condições :

a) $\left[m \equiv_4 1 \text{ ou } n \equiv_4 1 \right]$ e $\left[\lambda = 1, m, u \text{ ou } v \right]$

b) $(m,n) \equiv_4 (2,3)$ e $2\lambda = m$, u ou v

c) $(m,n) \equiv_4 (3,2)$ e $\lambda = u$ ou v

sendo u e v determinados no Lema 2.

DEMONSTRAÇÃO:

Observemos primeiramente que se $\lambda = 1$, m ou $\frac{m}{2}$ as condições do teorema 2 (seção 3.2), são suficientes.

a)Se $m \equiv_4 1$ ou $n \equiv_4 1$.

Sabemos que neste caso $\mathcal{D}_{\mathbb{K}/k} = n_1\mathbb{A}$ e usando o Critério de Mann, nós queremos mostrar que:

$$\mathbb{K} = k(\sqrt{\varepsilon n_1}) \quad \Leftrightarrow \quad \lambda = u \text{ ou } v.$$

Sabemos do Lema 2 que :

$$\sqrt{\varepsilon} = \frac{s\sqrt{ru} + t\sqrt{rv}}{r}, \text{ com } \begin{cases} \left(r = 1 \text{ se } m \equiv_4 1 \text{ ou } 2\right) \text{ e } \left(r = 2 \text{ se } m \equiv_4 3\right) \\ uv = m \ , \ mdc(u,v) = 1 \end{cases}$$

Portanto neste caso $r = 1$ e temos $\sqrt{\varepsilon} = s\sqrt{u} + t\sqrt{v}$.

Por outro lado, também é sabido que $\mathbb{K} = k(\sqrt{n})$. Logo

$\mathbb{K} = k(\sqrt{\varepsilon n_1}) \quad \Leftrightarrow \quad \dfrac{\sqrt{\varepsilon n_1}}{\sqrt{n}} = \dfrac{s\sqrt{\lambda u} + t\sqrt{\lambda v}}{\lambda} \in k = \mathbb{Q}(\sqrt{m})$. Portanto se

$\lambda = u$ ou v temos que $\dfrac{\sqrt{\varepsilon n_1}}{\sqrt{n}} = \dfrac{su + t\sqrt{m}}{\lambda}$ ou $\dfrac{s\sqrt{m} + tv}{\lambda}$, isto é,

$\dfrac{\sqrt{\varepsilon n_1}}{\sqrt{n}} \in k$ e $\mathbb{K} = k(\sqrt{\varepsilon n_1})$.

Assim, neste caso, resta-nos provar que $\mathbb{K} = k(\sqrt{\varepsilon n_1})$ implica em $\lambda = u$ ou v. Agora de $\mathbb{K} = k(\sqrt{\varepsilon n_1})$ obtemos

$x = \dfrac{\sqrt{\varepsilon n_1}}{\sqrt{n}} \in k$ e então $s\sqrt{\lambda u} + t\sqrt{\lambda v} \in k = \mathbb{Q}(\sqrt{m})$.

AFIRMAÇÃO: $\sqrt{\lambda u} \in \mathbb{Q}$ ou $\sqrt{\lambda v} \in \mathbb{Q}$.

De fato, suponhamos agora que $\sqrt{\lambda u} \notin \mathbb{Q}$ e $\sqrt{\lambda v} \notin \mathbb{Q}$.

Assim

$\sqrt{\lambda u} \in \mathbb{Q}(\sqrt{\lambda v}) \Leftrightarrow \sqrt{\lambda u} = c + d\sqrt{\lambda v} \Leftrightarrow \lambda u = c^2 + d^2 m_1 u + 2cd\sqrt{\lambda v} \Leftrightarrow$

$c = 0$ ou $d = 0$

1) $c = 0 \Rightarrow \lambda u = d^2 \lambda v \Rightarrow u = d^2 v \Rightarrow d = \pm 1$, pois u é livre de quadrados logo $u = v$, absurdo pois m é livre de quadrados.

2) $d = 0 \Rightarrow \lambda u = c^2$, absurdo pois $\sqrt{\lambda u} \notin \mathbb{Q}$.

Portanto $\sqrt{\lambda u} \notin \mathbb{Q}(\sqrt{\lambda v})$ logo $\left[\mathbb{Q}(\sqrt{\lambda u}, \sqrt{\lambda v}) : \mathbb{Q}\right] = 4$ o que nos dá uma contradição, pois sabemos que $s\sqrt{\lambda u} + t\sqrt{\lambda v} \in \mathbb{Q}(\sqrt{m})$.

Desta maneira concluimos, como queríamos, que

$$\sqrt{\lambda u} \in \mathbb{Q} \quad \text{ou} \quad \sqrt{\lambda v} \in \mathbb{Q} .$$

Disto obtemos dois casos:

i)$\lambda u = \ell_1^2$ com $\ell \in \mathbb{Z}$ mas λ ,u e v são livres de quadrados logo

$$\ell_1 | u \text{ e } \ell_1 | \lambda \quad \text{e assim } \lambda = u.$$

ii)$\lambda v = \ell_1^2$ com $\ell_1 \in \mathbb{Z}$, e analogamente $\lambda = v$.

b)$(m,n) \equiv_4 (2,3)$.

Seguindo o mesmo raciocínio da parte (a) e sabendo que $r = 1$ e $\mathcal{D}_{\mathbb{K}/k} = (2n_1)$, isto é, $\dfrac{\sqrt{2\varepsilon n_1}}{\sqrt{n}} = \dfrac{s\sqrt{2\lambda u} + t\sqrt{2\lambda v}}{\lambda}$, obtemos que $(2\lambda = u \quad \text{ou} \quad \lambda = 2u) \quad \text{ou} \quad (2\lambda = v \text{ ou } \lambda = 2v)$.

Mas, $\lambda = 2u$ implica que, $2 \equiv_4 mn = \lambda^2 m_1 n_1 = 4u^2 m_1 n_1 \equiv_4 0$, contradição. Idem para $\lambda = 2v$.

Assim concluimos que $2\lambda = u$ ou v.

c) $(m,n) \equiv_4 (3,2)$.

Do Critério de Mann e Lema 1, temos:

$$\mathbb{K} = K(\sqrt{2\varepsilon n_1}) \Leftrightarrow x = \frac{\sqrt{2\varepsilon n_1}}{\sqrt{n}} \in k \Leftrightarrow \frac{\sqrt{2\varepsilon}}{\sqrt{\lambda}} = \frac{s\sqrt{2ru} + t\sqrt{2rv}}{r\sqrt{\lambda}} \in k$$

$$\Leftrightarrow \quad c + d\sqrt{m} = \frac{(s\sqrt{2ru} + t\sqrt{2rv})}{r\sqrt{\lambda}} \quad \Leftrightarrow$$

$$\Leftrightarrow \quad cr\sqrt{\lambda} + dr\lambda\sqrt{m_1} = \sqrt{2ru} + t\sqrt{2rv} \qquad (*_1)$$

Multiplicando $(*_1)$ por $\sqrt{2ru}$ obtemos que $cr\sqrt{2ru\lambda} + dr\lambda\sqrt{2rum_1} = 2sru + 2rt\sqrt{m}$ e usando o mesmo argumento de (a) temos $\sqrt{2ru\lambda} \in \mathbb{Q}$ ou $\sqrt{2rum_1} \in \mathbb{Q}$, isto é, $2ru\lambda = \gamma^2$ ou $2rum_1 = \gamma^2$ com $\gamma \in \mathbb{Z}$. Mas u, λ, m_1 são livres de qradrados, dividem m e $m \equiv_4 3$. Logo $r = 2$ e $u = \lambda$ ou $r = 2$ e $u = m_1$, mas como $uv = m = \lambda m_1$, temos $u = \lambda$ ou $v = \lambda$ ∎

Como dissemos no início deste capítulo é também nosso objetivo determinar uma base integral sempre que ela exista. Sendo assim iniciamos nossa busca observando que a demonstração do Critério de Mann, juntamente com o Lema 1, nos fornecem uma base integral para a extensão, dada por:

$$\left\{ 1 , \frac{a + \sqrt{2^f \varepsilon n_1}}{2} \right\}$$ onde $a \in \mathbb{A}$, $f = 0$ ou 1 e ε é uma

unidade de $\mathbb{A}$, sendo que :

$$a^2 \equiv_{4\mathbb{A}} 2^f \varepsilon n_1 \equiv_{4\mathbb{A}} 2^f (bn_1 + cn_1\sqrt{m}) \qquad (2)$$

pois $N\left(\frac{a + \sqrt{2^f \varepsilon n_1}}{2}\right) \in \mathbb{A}$.

Consideremos portanto os casos:

i)Quando $m \equiv_4 n \equiv_4 1$ então $a = h + j\left(\frac{1 + \sqrt{m}}{2}\right)$, com

$h , j \in \mathbb{Z}$. Logo de (2) obtemos:

$$h^2 + j^2\left(\frac{1 + \sqrt{m}}{2}\right)^2 + 2hj\left(\frac{1 + \sqrt{m}}{2}\right) =$$

$$= h^2 + j^2\left(\frac{m - 1}{2}\right) + (2hj + j^2)\left(\frac{1 + \sqrt{m}}{2}\right) = a^2 \equiv_4 bn_1,$$

pois neste caso do Lema 2 vem que $c \equiv_4 0$.

Assim concluimos que $j \equiv_2 0$, logo $h^2 \equiv_4 1$ e assim $h \equiv_2 1$. Portanto chamamos $h = 1$ e $j = 0$ temos que

$$\left\{ 1 , \frac{1 + \sqrt{\varepsilon n_1}}{2} \right\}$$ é uma base integral de $\mathbb{K}/k$.

ii)Quando $m \not\equiv_4 1$ e $n \equiv_4 1$ então $a = h + j\sqrt{m}$

com $h,j \in \mathbb{Z}$.

De (2) podemos dizer que:

$$h^2 + j^2m + 2hj\sqrt{m} = a^2 \equiv bn_1 + cn_1\sqrt{m} \qquad (3)$$

de onde vem que $2hj \equiv_4 cn_1$ e então $c \equiv_2 0$. Portanto $c \equiv_4 0$ ou 2.

i) $c \equiv_4 0 \quad \Rightarrow \quad 2hj \equiv_4 0 \quad \Rightarrow$

$$\begin{cases} j \equiv_2 0 \quad \Rightarrow \quad h^2 \equiv_4 bn_1 \equiv_2 1 \quad \Rightarrow \quad h \equiv_2 1. \\ h \equiv_2 0 \quad \Rightarrow \quad j \equiv_2 1 \text{ , senão } a^2 \equiv_4 0. \end{cases}$$

De (3) temos que $bn_1 \equiv_4 h^2 + j^2m \equiv_4 1$ ou m. Mas bn_1 é ímpar , então $m \equiv_4 3$.

Logo quando $c \equiv_4 0$ uma base integral será dada por

$$\left\{ 1 , \frac{1 + \sqrt{\varepsilon n_1}}{2} \right\} \text{ ou } \left\{ 1 , \frac{\sqrt{m} + \sqrt{\varepsilon n_1}}{2} \right\}$$

2) $c \equiv_4 2 \Rightarrow hj \equiv_2 n_1 \equiv_2 1 \Rightarrow h \equiv_2 1$ e $j \equiv_2 1$.

Assim $\left\{ 1 , \frac{1 + \sqrt{m} + \sqrt{\varepsilon n_1}}{2} \right\}$ é uma base integral da extensão.

iii)Quando $m \equiv_4 1$ e $n \not\equiv_4 1$, de (2) temos que:

$a^2 \equiv_4 0$ e assim se chamamos a = 0 obtemos $\left\{ 1 , \frac{\sqrt{\varepsilon n_1}}{2} \right\}$ como base integral.

iv)Quando $m \not\equiv_4 1$ e $n \not\equiv_4 1$, temos dois casos:

a) $(m,n) \equiv_4 (3,2) \Rightarrow a = h + j\sqrt{m}$ com $h,j \in \mathbb{Z}$.

De (2) vem $h^2 + j^2m + 2hj\sqrt{m} = a^2 \equiv_4 2\varepsilon n_1 = 2(bn_1 + cn_1\sqrt{m})$.

Assim $\begin{cases} 2hj \equiv_4 2cn_1 \equiv_4 0 \Rightarrow hj \equiv_2 0 \Rightarrow h \equiv_2 0 \text{ ou } j \equiv_2 0 \\ h^2 + j^2m \equiv_4 2bn_1 \equiv_4 0 \Rightarrow h^2 \equiv_4 j^2m \equiv_4 0 \Rightarrow h \equiv_2 j \equiv_2 0 \end{cases}$

Podemos então chamar a = 0 e teremos uma base integral dada por $\left\{ 1 , \frac{\sqrt{2\varepsilon n_1}}{2} \right\}$.

b) $(m,n) \equiv_4 (2,3) \Rightarrow a = h + j\sqrt{m}$ com $h,j \in \mathbb{Z}$.

De (2) $h^2 + j^2m + 2hj\sqrt{m} = a^2 \equiv_4 2\varepsilon n_1 = 2(bn_1 + cn_1\sqrt{m})$.

Assim $\begin{cases} 2hj \equiv_4 2cn_1 \equiv_4 0 \quad (\text{ pois } c \equiv_2 0) \Rightarrow h \equiv_2 0 \text{ ou } j \equiv_2 0 \\ h^2 + j^2m \equiv_4 2bn_1 \Rightarrow h^2 \equiv_2 0 \Rightarrow h \equiv_2 0 \end{cases}$

Se $j \equiv_2 0$ então $j^2 \equiv_4 0$ e daí $2bn_1 \equiv_4 0$, que é um absurdo, pois bn_1 é ímpar. Logo podemos chamar h = 0 e j = 1 para obter $\left\{ 1 , \frac{\sqrt{m} + \sqrt{2\varepsilon n_1}}{2} \right\}$.

Assim podemos sintetizar nossos resultados na tabela que se segue.

TABELA 2

BASE	$(m,n) \equiv_4$	CONDIÇÕES
$1 , (1 + \sqrt{\varepsilon n_1})/2$	(m,1)	$bn_1 \equiv_4 1 , c \equiv_4 0$
$1 , (\sqrt{m} + \sqrt{\varepsilon n_1})/2$	(3,1)	$bn_1 \equiv_4 3 , c \equiv_4 0$
$1 , (1 + \sqrt{m} + \sqrt{\varepsilon n_1})/2$	(2,1)	$bn_1 \equiv_4 3 , c \equiv_4 2$
$1 , \sqrt{\varepsilon n_1}$	(1,3) ou (1,2)	
$1 , (\sqrt{2\varepsilon n_1})/2$	(3,2)	$r = 2$
$1 , (\sqrt{m} + \sqrt{2\varepsilon n_1})/2$	(2,3)	$2\lambda = u$ ou v

Agora veremos algumas consequências, bastante interessantes, do teorema 3.

COROLÁRIO 1 : Se $m > 0$, $\mathbb{K} = k(\sqrt{n})$ tem base integral sobre k $\forall n$, se e somente se, vale uma das condições abaixo:

1) $m = 2$ ou p

2) $\left[m = 2p \text{ ou } pq \text{ com } p \equiv_4 q\right]$ e $N(\varepsilon) = 1$.

DEMONSTRAÇÃO:

$\Leftarrow$: 1)Quando $m = 2$ ou p então $\lambda = 1$ ou m (logo $u = 1$ ou m), logo pelo teorema 3 temos o que queríamos provar.

2) i)Quando $m = 2p$ e $N(\varepsilon) = 1$, do Lema 2 temos:

$$\sqrt{\varepsilon} = s\sqrt{u} + t\sqrt{v} \quad \text{com} \quad mdc(u,v) = 1 \quad \text{e} \quad uv = m.$$

Logo $\begin{cases} u = 2 \quad \text{e} \quad v = p \\ \quad\quad \text{ou} \\ u = 1 \quad \text{e} \quad v = 2p \end{cases}$ ou vice-versa.

Se n é ímpar então $\lambda = 1$ ou p que implica em $2\lambda = u$ ou v. Logo pelo Teorema 3 obtemos o resultado pretendido.

Se n é par então $\lambda = 2$ ou $2p$, assim se $m_1 n_1 \equiv_4 1$ obtemos $\lambda = u$ ou v e pela parte (a) do Teorema 3, está demonstrado. Mas se $m_1 n_1 \equiv_4 3$ como $\mathbb{K} = \mathbb{Q}(\sqrt{m}\ , \sqrt{m_1 n_1})$ temos que $\lambda = m_1$ e daí $\lambda = p$ ou 1 , logo $2\lambda = u$ ou v . Pela parte (b) do Teorema 3 verifica-se o resultado.

ii)Quando $m = pq$ com $p \equiv_4 q$ e $N(\varepsilon) = 1$ então como $p \equiv_4 q$ temos que $m = pq \equiv_4 1$, e do Lema 2 temos que $\sqrt{\varepsilon} = s\sqrt{u} + t\sqrt{v}$ com $mdc(u,v) = 1$ e $uv = m$, portanto

$$\begin{cases} u = p \quad \text{e} \quad v = q \\ \quad\quad \text{ou} \\ u = 1 \quad \text{e} \quad v = pq \end{cases} \quad \text{ou vice-versa,}$$

e mais $\lambda = 1, p, q$ ou $pq \Rightarrow \lambda = 1, u, v$ ou m. Desta maneira utilizando a parte (a) do Teorema 3 obtemos o resultado.

$\Rightarrow$: Supondo que existe base integral da extensão $\mathbb{K}/k$, note que se m tem três ou mais primos ímpares como divisores, então existe para λ, pelo menos oito possibilidades dependendo da conveniente escolha para n. Mas pelo Teorema 3 somente existe quatro valores que λ pode assumir.

Se $m = 2pq$ é análogo ao anterior.

Se $m = pq$ com $p \equiv_4 q$ e $r = 1$ então quando n é par, temos pela parte (a) do Teorma 3 que não existe base integral para a extensão $\mathbb{K}/k$; o que também ocorre se $r = 2$, $\lambda = p$ e n ímpar, pois,

$$\begin{cases} n \equiv_4 1 \\ \quad \text{ou} \\ n \equiv_4 3 \end{cases} \Rightarrow m_1 n_1 \equiv_4 1$$

e portanto (a) não se verifica.

Finalmente quando $m = 2p$ ou pq com $N(\varepsilon) = -1$, se $\lambda = p$ e $n \equiv_4 1$ $\Rightarrow$ a parte (a) do Teorema não se verifica, pois não nos é possivel usar o Lema 2 ■

COROLÁRIO 2 : Se k tem número de classe ímpar então $\mathbb{K} = k(\sqrt{n})$ possui base integral sobre k, $\forall n$.

DEMONSTRAÇÃO:

Sabendo que $k = \mathbb{Q}(\sqrt{m})$ possui número de classe ímpar, se e somente se, $m = 2,\ p,\ 2p_1$ ou p_1p_2 com $p_1 \equiv_4 p_2 \equiv_4 3$.

Podemos então ver que quando m tem um divisor primo $q \equiv_4 3$ então ε tem norma positiva, pois se $\varepsilon = a + b\sqrt{m}$ e $N(\varepsilon) = -1$ temos que $a^2 - b^2m = -1$ e portanto $a^2 \equiv_q -1$, que é absurdo (lembre que $\left(\frac{-1}{q}\right) = (-1)^{q-1/2}$ e $q \equiv_4 3$). Assim imediatamente do corolário 1 obtemos o resultado proposto ■

COROLÁRIO 3 : Se k é um corpo quadrático então vale apenas uma das condições abaixo:

i)Todas as extensões de corpos, bicíclicas biquadráticas $\mathbb{K}$, possuem base integral sobre k.

ii)Existem infinitas extensões $\mathbb{K}$ que possuem (ou não possuem) uma base integral sobre k.

DEMONSTRAÇÃO:

Imediata dos Teoremas 2 e 3, e seus corolários ■

APÊNDICE

Como dissemos no capítulo 3, neste apêndice, demonstraremos o Critério de Mann e o Lema 3.1. Para isto vamos considerar sempre a seguinte situação: $\mathbb{K}/k$ extensão de corpos, $\mathbb{A}$ um subanel de k tal que $\mathbb{A}$ é algebricamente fechado com $cfr(\mathbb{A}) = k$ e $\mathbb{B}$ o fecho inteiro de $\mathbb{A}$ em $\mathbb{K}$.

TEOREMA 1(Critério de Mann): Sejam $\mathbb{K}/k$ uma extensão quadrática, com $ch(k) = 0$ [1] e $\mathcal{D}_{\mathbb{K}/k}$ o ideal discriminante da extensão. Então existe uma base integral de $\mathbb{K}/k$, se e somente se, $\mathbb{K} = k(\sqrt{d})$, onde $\mathcal{D}_{\mathbb{K}/k} = d\mathbb{A}$.

DEMONSTRAÇÃO :

$\Rightarrow$: Podemos escrever $\mathbb{K} = k(\sqrt{a})$, com $a \in k$ pois a extensão é quadrática.

---

1) vale igualmente para $ch k \neq 2$ [03].

$$\text{Seja} \begin{cases} \alpha = x_1 + x_2\sqrt{a} \\ \beta = y_1 + y_2\sqrt{a} \end{cases} \qquad \text{com} \qquad x_1,\ y_1 \in k,$$

tal que $\{\alpha,\beta\}$ seja uma base integral de $\mathbb{K}/k$.

Pelo teorema 9, do capítulo 1, temos : $\mathcal{D}_{\mathbb{K}/k} = d\mathbb{A}$ onde

$$d = D(\alpha,\beta) = \begin{vmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{vmatrix}^2 = \left[2\sqrt{a}(x_2y_1 - x_1y_2)\right]^2$$

portanto

$$\sqrt{d} = 2\sqrt{a}(x_2y_1 - x_1y_2).$$

Se $(x_2y_1 - x_1y_2) \neq 0$ então $\mathbb{K} = k(\sqrt{d})$, o que se verifica pois $\{\alpha,\beta\}$ é base.

$\Leftarrow$: Temos por hipótese que $\mathbb{K} = k(\sqrt{d})$ com $\mathcal{D}_{\mathbb{K}/k} = d\mathbb{A}$.

Note que se $\gamma = x + y\sqrt{d}$, $x,\ y \in k$ e $\gamma \in \mathbb{B}$ então $2y = \mathrm{Tr}\left(\dfrac{\gamma}{\sqrt{d}}\right) \in \mathbb{A}$. De fato pois podemos supor que $y \neq 0$ e neste caso $\{1,\gamma\} \in \mathbb{B}$ é base de $\mathbb{K}/k$ com $D(1,\gamma) = (2y)^2 d \in \mathcal{D}_{\mathbb{K}/k} = d\mathbb{A}$. Logo $(2y)^2 \in \mathbb{A}$, mas $2y \in k$ e $\mathbb{A}$ é integralmente fechado, assim $2y \in \mathbb{A}$.

Seja $\{\alpha,\beta\} \subseteq \mathbb{B}$, base de $\mathbb{K}/k$ tal que :

$$\begin{cases} \alpha = x_1 + x_2\sqrt{d} \\ \beta = y_1 + y_2\sqrt{d} \end{cases} \qquad \text{com} \quad x_1,\ y_1 \in k\ .$$

Observe que :

$$\beta\bar{\alpha} = (x_1y_1 - y_2x_2d) + (x_1y_2 - y_1x_2)\sqrt{d} \in \mathbb{A}$$

$$N(\alpha) = x_1^2 - dx_2^2 \in \mathbb{A}, \quad Tr\left(\frac{\alpha}{\sqrt{d}}\right) = 2x_2 \in \mathbb{A}$$

$$N(\beta) = y_1^2 - dy_2^2 \in \mathbb{A}, \quad Tr\left(\frac{\beta}{\sqrt{d}}\right) = 2y_2 \in \mathbb{A}$$

$$Tr(\beta\bar{\alpha}) = 2(x_1y_1 - y_2x_2d) \in \mathbb{A}$$

$$D(\alpha,\beta) = 4d(x_2y_1 - x_1y_2)^2 \in \mathbb{A}$$

Resolvendo o quadrado obtemos:

$$D(\alpha,\beta) = 4d\left[x_2^2N(\beta) + y_2^2N(\alpha) - x_2y_2Tr(\beta\bar{\alpha})\right] =$$

$$= \left[\left(Tr\left(\frac{\alpha}{\sqrt{d}}\right)^2 N(\beta) + Tr\left(\frac{\beta}{\sqrt{d}}\right)^2 N(\alpha) - Tr\left(\frac{\alpha}{\sqrt{d}}\right) Tr\left(\frac{\beta}{\sqrt{d}}\right) Tr(\beta\bar{\alpha})\right] d$$

Seja $\mathfrak{h}$ o ideal de $\mathbb{A}$ gerado pelo conjunto $\left\{Tr\left(\frac{\alpha}{\sqrt{d}}\right), \alpha \in \mathbb{B}\right\}$

AFIRMAÇÃO : $\mathfrak{h} = \mathbb{A}$.

De fato se $\{\alpha,\beta\} \subseteq \mathbb{B}$ é base de $\mathbb{K}/k$ então temos $D(\alpha,\beta) \in \mathcal{D}_{\mathbb{K}/k}$ e portanto $D(\alpha,\beta) = bd$ para algum $b \in \mathbb{A}$. Por outro lado, observando a igualdade (*) vemos que $D(\alpha,\beta) \in \mathfrak{h}^2d$,

isto é, $D(\alpha,\beta) = bd$, com $b \in \mathfrak{h}^2$. Agora, como $\mathcal{D}_{\mathbb{K}/k} = d\mathbb{A}$, temos

$d = \sum_{i=1}^{m} c_i D\left(\alpha_i , \beta_i\right)$, onde $c_i \in \mathbb{A}$, $\{\alpha_i , \beta_i\} \subseteq \mathbb{B}$ e é base de $\mathbb{K}/k$.

Mas como já vimos $D\left(\alpha_i , \beta_i\right) = b_i d$, com $b_i \in \mathfrak{h}^2$, logo

$d = \left(\sum_{i=1}^{m} c_i b_i\right) d$ e assim $\sum_{i=1}^{m} c_i b_i = 1$, com $c_i \in \mathbb{A}$ e $b_i \in \mathfrak{h}^2$, portanto

$\mathfrak{h}^2 = \mathbb{A}$, isto é, $\mathfrak{h} = \mathbb{A}$.

Portanto existem $\alpha_i \in \mathbb{B}$, $x_i \in \mathbb{A}$, para $i = 1,\ldots,m$ tal

que: $$1 = x_1 \mathrm{Tr}\left(\frac{\alpha_1}{\sqrt{d}}\right) + x_2 \mathrm{Tr}\left(\frac{\alpha_2}{\sqrt{d}}\right) + \ldots + x_m \mathrm{Tr}\left(\frac{\alpha_m}{\sqrt{d}}\right) =$$

$$= x_1\left(\frac{\alpha_1 - \bar{\alpha}_1}{\sqrt{d}}\right) + x_2\left(\frac{\alpha_2 - \bar{\alpha}_2}{\sqrt{d}}\right) + \ldots + x_m\left(\frac{\alpha_m - \bar{\alpha}_m}{\sqrt{d}}\right)$$

Assim $\sqrt{d} = \sum_{i=1}^{m} x_i \alpha_i - \sum_{i=1}^{m} x_i \bar{\alpha}_i$.

Somando e subtraindo $\sum_{i=1}^{m} x_i \alpha_i$ temos:

$$\sqrt{d} = 2\sum_{i=1}^{m} x_i \alpha_i - \sum_{i=1}^{m} x_i(\alpha_i + \bar{\alpha}_i) = 2\sum_{i=1}^{m} x_i \alpha_i - \sum_{i=1}^{m} x_i \mathrm{Tr}(\alpha_i)$$

Como $\alpha_i \in \mathbb{B}$ $\forall i$ e $\mathbb{A}$ é integralmente fechado, $Tr(\alpha_i) \in \mathbb{A}$ $\forall i$. Chamemos $b = -\sum_{i=1}^{m} a_i Tr(\alpha_i)$ então $b \in \mathbb{A}$, pois também $a_i \in \mathbb{A}$.

Portanto $\sqrt{d} - b = 2\sum_{i=1}^{m} a_i \alpha_i \in 2\mathbb{B}$, logo $\alpha = \frac{\sqrt{d} - b}{2} \in \mathbb{B}$

com $b \in \mathbb{A}$ e também,

$$\begin{vmatrix} 1 & \alpha \\ 1 & \bar{\alpha} \end{vmatrix}^2 = \begin{vmatrix} 1 & \frac{\sqrt{d} - b}{2} \\ 1 & \frac{-\sqrt{d} - b}{2} \end{vmatrix}^2 = d$$

Portanto $\left\{ 1 , \frac{\sqrt{d} - b}{2} \right\}$ é base integral de $\mathbb{K}/k$ □

Provaremos agora o Lema 1 usando as bases integrais obtidas no capítulo 2.

LEMA 1 : Sejam $\mathbb{K} = \mathbb{Q}(\sqrt{m},\sqrt{n})$, $k = \mathbb{Q}(\sqrt{m})$ e $\mathcal{D}_{\mathbb{K}/k}$ o ideal discrimimante de $\mathbb{K}/k$. Como sempre $\mathbb{A}$ é o anel de inteiros de k e $\mathbb{B}$ o anel de inteiros de $\mathbb{K}$.

i) Se $n \equiv_4 1$ ou $m_1 n_1 \equiv_4 1$ então

$$\mathcal{D}_{\mathbb{K}/k} = n_1\mathbb{A}.$$

ii) Se $n \not\equiv_4 1$ e $m \equiv_4 1$ então

$$\mathcal{D}_{\mathbb{K}/k} = 4n_1\mathbb{A}.$$

iii) Se $m \not\equiv_4 1$, $n \not\equiv_4 1$ e $m_1 n_1 \not\equiv_4 1$ então

$$\mathcal{D}_{\mathbb{K}/k} = 2n_1\mathbb{A}.$$

DEMONSTRAÇÃO:

Iniciemos observando que, tomando $m = \lambda m_1$ e $n = \lambda n_1$, temos:

a)$mdc(\lambda,m_1) = mdc(n_1,m_1) = mdc(\lambda,n_1) = mdc(m,n_1) = 1$.

b)Como $\mathbb{K} = \mathbb{Q}(\sqrt{m},\sqrt{n}) = \mathbb{Q}(\sqrt{m},\sqrt{m_1 n_1})$, podemos trocar n por $m_1 n_1$ sempre que necessário.

c)$\mathcal{D}_{\mathbb{K}/\mathbb{Q}} = \lambda^2 m_1^2 n_1^2\mathbb{Z}$ ou $16\lambda^2 m_1^2 n_1^2\mathbb{Z}$ ou $64\lambda^2 m_1^2 n_1^2\mathbb{Z}$.

d)$\mathcal{D}_{k/\mathbb{Q}} = \lambda m_1\mathbb{Z}$ ou $4\lambda m_1\mathbb{Z}$.

1) Pela observação (b) podemos supor que $n \equiv_4 1$. Tomemos $p \in \mathbb{Z}$ primo e $p|n_1$. Pelas observações (a) e (d) podemos concluir que:

1) $p\mathbb{A} = \mathbb{P}_1\mathbb{P}_2$, onde $\mathbb{P}_1 \neq \mathbb{P}_2$ são ideais primos de $\mathbb{A}$

ou

2) $p\mathbb{A} = \mathbb{P}$, sendo $\mathbb{P}$ primo de $\mathbb{A}$.

Por (c), $p \Big| \mathcal{D}_{\mathbb{K}/\mathbb{Q}}$ e portanto p se ramifica em $\mathbb{B}$, isto é,

$$1) \qquad p\mathbb{B} = \mathbb{P}_1\mathbb{P}_2\mathbb{B} = \prod_{i=1}^{g} \mathbb{Q}_i^e$$

onde $efg = 4$, $e \geq 2$, e os $\mathbb{Q}_i$ são ideais primos de $\mathbb{B}$ (ver Teorema 7, capítulo 1). Logo $e = 4$ é impossível, pois $\mathbb{P}_1\mathbb{P}_2\mathbb{B} = p\mathbb{B} = \mathbb{Q}_1^4$ implica em $\mathbb{P}_1 = \mathbb{Q}_1 \cap \mathbb{A} = \mathbb{P}_2$ que é absurdo, portanto $e = 2$ e $g = 2$, assim $p\mathbb{B} = \mathbb{P}_1\mathbb{P}_2\mathbb{B} = \mathbb{Q}_1^2\mathbb{Q}_2^2$, com $\mathbb{Q}_1 \cap \mathbb{A} = \mathbb{P}_1$ e $\mathbb{Q}_2 \cap \mathbb{A} = \mathbb{P}_2$. Disto obtemos que $\mathbb{P}_1 \Big| \mathcal{D}_{\mathbb{K}/k}$ e $\mathbb{P}_2 \Big| \mathcal{D}_{\mathbb{K}/k}$, logo $p\mathbb{A} \Big| \mathcal{D}_{\mathbb{K}/k}$. Repetindo isto para todo $p|n_1$ temos que $n_1\mathbb{A} \Big| \mathcal{D}_{\mathbb{K}/k}$, ou seja, $\mathcal{D}_{\mathbb{K}/k} \subseteq n_1\mathbb{A}$

ou

$$2) \qquad p\mathbb{B} = \mathbb{P}\mathbb{B} = \prod_{i=1}^{g} \mathbb{Q}_i^e$$

onde $efg = 4$, $e \geq 2$, e os $\mathbb{Q}_i$ são ideais primos de $\mathbb{B}$. Logo $e = 4$.

Assim $p\mathbb{B} = \mathbb{P}\mathbb{B} = \mathbb{Q}^4$, com $\mathbb{Q} \cap \mathbb{A} = \mathbb{P}$. Disto obtemos que $\mathbb{P} \Big| \mathcal{D}_{\mathbb{K}/k}$, logo $p\mathbb{A} \Big| \mathcal{D}_{\mathbb{K}/k}$. Repetindo isto para todo $p | n_1$ temos que $n_1\mathbb{A} \Big| \mathcal{D}_{\mathbb{K}/k}$, ou seja $\mathcal{D}_{\mathbb{K}/k} \subseteq n_1\mathbb{A}$.

Agora, note que, se tomarmos $\alpha = \dfrac{1 + \sqrt{n}}{2}$ (2)

e $\beta = \sqrt{m_1 n_1}$ teremos que $D(1,\alpha) = n$ e $D(1,\beta) = 4m_1n_1$. Logo $n\mathbb{A} \subseteq \mathcal{D}_{\mathbb{K}/k}$ e $4m_1n_1\mathbb{A} \subseteq \mathcal{D}_{\mathbb{K}/k}$. Porem $mdc(4m_1,n) = 1$ e portanto $4m_1\mathbb{A} + n\mathbb{A} = \mathbb{A}$.

Finalmente obtemos que :

$$n_1\mathbb{A} = 4m_1n_1\mathbb{A} + n_1n\mathbb{A} \subseteq \mathcal{D}_{\mathbb{K}/k}$$

como queríamos.

ii)Observe que este caso se resume a $(m,n) \equiv_4 (1,2)$ ou $(1,3)$.

Temos $4n = D(1,\sqrt{n}) \in \mathcal{D}_{\mathbb{K}/k}$ e $4m_1n_1 = D(1,\sqrt{m_1n_1}) \in \mathcal{D}_{\mathbb{K}/k}$. Assim da observação (a), $\lambda\mathbb{A} + m_1\mathbb{A} = \mathbb{A}$ e $4n_1\lambda\mathbb{A} + 4n_1m_1\mathbb{A} = 4n_1\mathbb{A}$, portanto $4n_1\mathbb{A} \subseteq \mathcal{D}_{\mathbb{K}/k}$.

Para provar que $\mathcal{D}_{\mathbb{K}/k} \subseteq 4n_1\mathbb{A}$, vamos primeiro considerar o caso $(m,n) \equiv_4 (1,2)$. Sabemos que neste caso,

---

2) $\alpha \in \mathbb{B}$ pois $n \equiv_4 1$.

$$\left\{ 1 , \frac{1 + \sqrt{m}}{2} , \sqrt{n} , \frac{\sqrt{n} + \sqrt{m_1 n_1}}{4} \right\}$$

é uma base integral de $\mathbb{B}/\mathbb{Z}$.

Tome agora $\alpha \in \mathbb{B}$, $\beta \in \mathbb{B}$ tal que $\{\alpha,\beta\}$ seja uma base da extensão $\mathbb{K}/k$. Logo $\alpha = z_0 + z_1\left[\frac{1 + \sqrt{m}}{2}\right] + z_2\sqrt{n} + z_3\left[\frac{\sqrt{n} + \sqrt{m_1 n_1}}{2}\right]$

com $z_0, z_1, z_2, z_3 \in \mathbb{Z}$. Mas como $\frac{\sqrt{n} + \sqrt{m_1 n_1}}{2} = \sqrt{n}\left[\frac{\lambda + \sqrt{m}}{2\lambda}\right]$ obtemos:

$\alpha = y_1 + y_2\sqrt{n}$, com $y_1 \in \mathbb{A}$ e $\lambda y_2 \in \mathbb{A}$. Analogamente temos que

$\beta = w_1 + w_2\sqrt{n}$, com $w_1 \in \mathbb{A}$ e $\lambda w_2 \in \mathbb{A}$.

Agora calculando o discriminante de $\{\alpha,\beta\}$ obtemos:

$$D(\alpha,\beta) = \left[2(y_2 w_1 - w_2 y_1)\right]^2 n = 4n\,\frac{(\lambda y_2 w_1 - \lambda y_1 w_2)^2}{\lambda^2} = \frac{4x^2}{\lambda}\, n_1 \in \mathcal{D}_{\mathbb{K}/k}$$

onde $x = \lambda y_2 w_1 - \lambda w_2 y_1 \in \mathbb{A}$.

Portanto concluimos que $\lambda\mathcal{D}_{\mathbb{K}/k} \subseteq 4n_1\mathbb{A}$; mas $\mathrm{mdc}(\lambda, 4n_1) = 1$, assim $\lambda\mathbb{A} + 4n_1\mathbb{A} = \mathbb{A}$ e $\lambda\mathcal{D}_{\mathbb{K}/k} + 4n_1\mathcal{D}_{\mathbb{K}/k} = \mathcal{D}_{\mathbb{K}/k}$.

Obtemos portanto que $\mathcal{D}_{\mathbb{K}/k} \subseteq 4n_1\mathbb{A}$.

Agora no caso $(m,n) \equiv_4 (1,3)$ temos que

$$\left\{ 1 , \frac{1 + \sqrt{m}}{2} , \sqrt{m_1 n_1} , \frac{\sqrt{n} + \sqrt{m_1 n_1}}{4} \right\}$$

é base integral de $\mathbb{B}/\mathbb{Z}$, portanto trocando n por $m_1 n_1$ podemos

repetir a prova realizada e teremos $\mathcal{D}_{\mathbb{K}/k} \subseteq 4n_1\mathbb{A}$.

iii)Observe primeiramente que se $(m,n) \equiv_4 (2,2)$ então $m_1n_1 \equiv_4 1$ ou 3, mas o caso $m_1n_1 \equiv_4 1$ está excluido. Assim trocando n por m_1n_1, se necessário, podemos supor que $(m,n) \equiv_4 (2,3)$ ou (3,2).

Mostremos que $2n_1\mathbb{A} \subseteq \mathcal{D}_{\mathbb{K}/k}$. Comecemos com o caso $(m,n) \equiv_4 (2,3)$. Aqui seja $\alpha = \dfrac{\sqrt{m} + \sqrt{m_1n_1}}{2} \in \mathbb{B}$ e assim $D(1,\alpha) = m_1n_1 \in \mathcal{D}_{\mathbb{K}/k}$. Também é sabido que $4n = 4\lambda n_1 \in \mathcal{D}_{\mathbb{K}/k}$.

Chamemos $m_1 = 2s$ com $mdc(2,s) = 1$ e portanto

$$2\mathbb{A} + s\mathbb{A} = \mathbb{A} \quad \text{e então}$$

$$2n_1\lambda\mathbb{A} = 4n_1\lambda\mathbb{A} + 2sn_1\lambda\mathbb{A} = 4n_1\lambda\mathbb{A} + m_1n_1\lambda\mathbb{A} \subseteq \mathcal{D}_{\mathbb{K}/k}.$$

Agora $\lambda\mathbb{A} + m_1\mathbb{A} = \mathbb{A}$ e $2n_1\mathbb{A} = 2n_1\lambda\mathbb{A} + 2m_1n_1\mathbb{A} \subseteq \mathcal{D}_{\mathbb{K}/k}$ e então $2n_1\mathbb{A} \subseteq \mathcal{D}_{\mathbb{K}/k}$.

Façamos agora o caso $(m,n) \equiv_4 (3,2)$.

Como $4n_1\lambda \in \mathcal{D}_{\mathbb{K}/k}$, $4m_1n_1 \in \mathcal{D}_{\mathbb{K}/k}$ e $\lambda\mathbb{A} + m_1\mathbb{A} = \mathbb{A}$, temos que $4n_1\mathbb{A} \subseteq \mathcal{D}_{\mathbb{K}/k}$. Tomemos $\alpha = \dfrac{\sqrt{n} + \sqrt{m_1n_1}}{2} \in \mathbb{B}$ e como pode ser visto :

$$D(1,\alpha) = 4\alpha^2 \in \mathcal{D}_{\mathbb{K}/k}, \text{ ou seja,}$$

$$D(1,\alpha) = n + n_1 m_1 + 2n_1\sqrt{m} = n_1(\lambda + m_1) + 2n_1\sqrt{m} ,$$

mas observe que sendo $m \equiv_4 3$ e $m = \lambda m_1$ então $\lambda \not\equiv_4 m_1$, portanto $\lambda + m_1 \equiv_4 0$ e assim $(\lambda + m_1)n_1 \in \mathcal{D}_{\mathbb{K}/k}$ e por conseguinte, $2n_1\sqrt{m} \in \mathcal{D}_{\mathbb{K}/k}$.

Agora $mdc(m,2) = 1$ e portanto $2\mathbb{A} + \sqrt{m}\mathbb{A} = \mathbb{A}$, logo $4n_1\mathbb{A} + 2n_1\sqrt{m}\mathbb{A} = 2n_1\mathbb{A}$ e desta forma obtemos que $2n_1\mathbb{A} \subseteq \mathcal{D}_{\mathbb{K}/k}$.

Mostremos para finalizar que $\mathcal{D}_{\mathbb{K}/k} \subseteq 2n_1\mathbb{A}$.

1)Caso $(m,n) \equiv_4 (2,3)$.

Neste caso temos como base integral da extensão $\mathbb{K}/\mathbb{Q}$ o conjunto:

$$\left\{ 1 , \sqrt{m} , \sqrt{n} , \frac{\sqrt{m} + \sqrt{m_1 n_1}}{2} \right\} .$$

Tomemos $\alpha, \beta \in \mathbb{B}$ tal que $\{\alpha,\beta\}$ seja base de $\mathbb{K}/k$.

Observe que $\alpha = z_0 + z_1\sqrt{m} + z_2\sqrt{n} + z_3\left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2}\right)$

$$= \frac{2z_0 + (2z_1 + z_3)\sqrt{m}}{2} + \frac{(2\lambda z_2 + z_3\sqrt{m})}{2\lambda}\sqrt{n} ,$$

$$\text{com } z_i \in \mathbb{Z} \ \forall i.$$

Disto temos:

$\alpha = y_1 + y_2\sqrt{n}$, onde $2y_1 = a_1 + b_1\sqrt{m}$ e $2\lambda y_2 = a_2 + b_2\sqrt{m}$,

sendo a_1, $a_2 \in 2\mathbb{Z}$ e $b_1, b_2 \in \mathbb{Z}$ com $b_1 \equiv_2 b_2$.

Do mesmo modo, $\beta = w_1 + w_2\sqrt{n}$, onde $2w_1 = c_1 + d_1\sqrt{m}$ e

$2\lambda w_2 = c_2 + d_2\sqrt{m}$,sendo c_1, $c_2 \in 2\mathbb{Z}$ e $d_1, d_2 \in \mathbb{Z}$ com $d_1 \equiv_2 d_2$.

Agora $D(\alpha,\beta) = \left[2(y_2w_1 - y_1w_2)\right]^2 n = \dfrac{(4\lambda y_2w_1 - 4\lambda w_2y_1)^2}{4\lambda^2}\, n$

ou seja , $D(\alpha,\beta) = \dfrac{x^2n_1}{4\lambda}$, onde $x = 4\lambda y_2w_1 - 4\lambda w_2y_1$ e

portanto $x = (a_2 + b_2\sqrt{m})(c_1 + d_1\sqrt{m}) - (a_1 + b_1\sqrt{m})(c_2 + d_2\sqrt{m})$.

Fazendo as contas temos:

$$x = a_2c_1 - c_2a_1 + (b_2d_1 - b_1d_2)m + (a_2d_1 + c_1b_2 - c_2b_1 - d_2a_1)\sqrt{m}$$

Mas como $a_1 \equiv_2 a_2 \equiv_2 c_1 \equiv_2 c_2 \equiv_2 0$, temos:

$b_1 \equiv_2 b_2$, $d_1 \equiv_2 d_2$ e $m \equiv_2 0 \quad \Rightarrow \quad x = 2(2a + b\sqrt{m})$,

com a , $b \in \mathbb{Z}$.

Portanto $x^2 = 4(4a^2 + b^2m + 4ab\sqrt{m})$ e uma vez que $m \equiv_2 0$ obtemos que: $x^2 = 8(c + d\sqrt{m})$ com c , $d \in \mathbb{Z}$. Assim

$$D(\alpha,\beta) = \frac{x^2n_1}{4\lambda} = 2n_1\frac{(c + d\sqrt{m})}{\lambda} .$$

Como $D(\alpha,\beta) \in \mathbb{A}$ e $mdc(2n_1,\lambda) = 1$ temos $2n_1\mathbb{A} + \lambda\mathbb{A} = \mathbb{A}$,

então $\left(\dfrac{c + d\sqrt{m}}{\lambda}\right)\mathbb{A} = D(\alpha,\beta)\mathbb{A} + (c + d\sqrt{m})\mathbb{A} \subseteq \mathbb{A}$ e portanto $\dfrac{c + d\sqrt{m}}{\lambda} \in \mathbb{A}$.

Assim $D(\alpha,\beta) \in 2n_1\mathbb{A}$, isto é, $\mathcal{D}_{\mathbb{K}/k} \subseteq 2n_1\mathbb{A}$.

2)Caso $(m,n) \equiv_4 (3,2)$.

Aqui o conjunto $\left\{ 1, \sqrt{m}, \sqrt{n}, \frac{\sqrt{n} + \sqrt{m_1 n_1}}{2} \right\}$ é uma base integral da extensão $\mathbb{K}/\mathbb{Q}$.

Tomemos $\alpha,\beta \in \mathbb{B}$ tal que $\{\alpha,\beta\}$ seja uma base de $\mathbb{K}/k$.

Assim $\alpha = z_0 + z_1\sqrt{m} + z_2\sqrt{n} + z_3\left(\frac{\sqrt{m} + \sqrt{m_1 n_1}}{2}\right) =$

$$= z_0 + z_1\sqrt{m} + \sqrt{n}\left(\frac{2\lambda z_2 + \lambda z_3 + z_3\sqrt{m}}{2\lambda}\right),$$

com $z_i \in \mathbb{Z}$ $\forall i$, isto é, $\alpha = y_1 + y_2\sqrt{n}$, onde $y_1 = z_0 + z_1\sqrt{m}$ e $2\lambda y_2 = a + b\sqrt{m}$, com $a, b \in \mathbb{Z}$, e $a \equiv_2 b$, pois $\lambda \equiv_2 1$.

Do mesmo modo

$\beta = w_1 + w_2\sqrt{n}$, onde $w_1 = x_0 + x_1\sqrt{m}$ e $2\lambda w_2 = c + d\sqrt{m}$,

com $c, d \in \mathbb{Z}$, e $c \equiv_2 d$.

Agora $D(\alpha,\beta) = \left[2(y_2w_1 - y_1w_2)\right]^2 n = \frac{(2\lambda y_2w_1 - 2\lambda w_1y_2)^2}{\lambda^2} n$

ou seja , $D(\alpha,\beta) = \frac{x^2 n_1}{\lambda}$, onde $x = 2\lambda y_2w_1 - 2\lambda w_2y_1$ e

portanto $x = (a + b\sqrt{m})(x_0 + x_1\sqrt{m}) - (c + d\sqrt{m})(z_0 + z_1\sqrt{m})$, isto é,

$x = ax_0 - cz_0 + (bx_1 - z_1d)m + (ax_1 + x_0b - cz_1 - dz_0)\sqrt{m} =$

$= t + s\sqrt{m}$.

Sabido que $m \equiv_2 1$, $a \equiv_2 b$, e $c \equiv_2 d$ temos :

$$t \equiv_2 a(x_0 + x_1) - c(z_0 + z_1) \equiv_2 s$$

$$\Rightarrow \qquad x^2 = t^2 + s^2m + 2ts\sqrt{m} = 2y$$

com $y \in \mathbb{A}$. portanto $D(\alpha,\beta) = \dfrac{x^2n_1}{\lambda} = \dfrac{2n_1y}{\lambda} \in \mathbb{A}$, com $y \in \mathbb{A}$.

Logo $\dfrac{y}{\lambda}\,\mathbb{A} = D(\alpha,\beta)\mathbb{A} + y\mathbb{A} \subseteq \mathbb{A}$ e assim $\dfrac{y}{\lambda} \in \mathbb{A}$, ou seja,

$D(\alpha,\beta) \in 2n_1\mathbb{A}$ e portanto concluímos que $\mathcal{D}_{\mathbb{K}/k} \subseteq 2n_1\mathbb{A}$ ■

BIBLIOGRAFIA

[01]Bird,R.H. & Parry,C.J. *Integral Bases for Bicyclic Biquadratic Fields over Quadratic Subfields.* **Pacif.Journ.Math.** 66: 29-36, 1976.

[02]Endler,O. **Teoria dos Numeros Algebricos.** IMPA, Rio de Janeiro, 1986.

[03]Mann,H.B. *On Integral Bases.* **Proc.Amer.Math.Society.** 9:167-172, 1958.

[04]Samuel,P. **Teorie Algebrique des Nombres.** Hermann, Paris, 1967.

[05]Spearman,B.K. & Williams,K.S. *Ciclic Quartic Fields with Relative Integral Bases over Quadratic Subfields.* **Proc.Amer. Math.Society.** 103 :687-694, 1988.

[06]Williams,K.S. *Integers of Biquadratic Fields.* **Canad.Math.Bull.** 13:519-526, 1970.