Universidade Estadual de Campinas

INSTITUTO DE MATEMÁTICA, ESTATÍSTICA E COMPUTAÇÃO CIENTÍFICA

Departamento de Matemática

UM TEOREMA DE WITT SOBRE A IMERSÃO DE EXTENSÕES BIQUADRÁTICAS EM QUATERNIÔNICAS

por

Mauro Ribeiro de Oliveira Júnior

Mestrado em Matemática

Orientador: Prof. Dr. Antônio José Engler

Campinas, SP

Março/2006

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Maria Júlia Milani Rodrigues – CRB8a / 2116

Oliveira Júnior, Mauro Ribeiro de
OL4t Um teorema de Witt sobre a imersão de extensões biquadráticas em quaterniônicas / Mauro Ribeiro de Oliveira Júnior -- Campinas, [S.P. :s.n.], 2006.

Orientador : Antonio José Engler
Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Galois, Teoria de. 2. Formas quadráticas. 3. Brauer, Grupos de. I. Engler, Antonio José . II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: A Witt's theorem about the imersion of biquadratic extensions in quaternionics

Palavras-chave em inglês (Keywords): 1. Galois theory. 2. Quadratic forms. 3. Brauer groups

Área de concentração: Álgebra

Titulação: Mestre em Matemática

Banca examinadora: Prof. Dr. Antonio José Engler (IMECC-UNICAMP)
Profa. Dra. Ires Dias (ICMC-USP)
Profa. Dra. Dessislava Hristova Kochloukova (IMECC-UNICAMP)

Data da defesa: 17/03/2006

Resumo

Neste trabalho seguimos, nos quatro primeiros capítulos, para a construção efetiva de extensões quaterniônicas, apartir do acúmulo de informações obtidas nos capítulos iniciais 1 e 2, sobre a estrutura dos subcorpos intermediários a uma extensão deste tipo, conhecimentos quais são obtidos pela atuação forte da Teoria de Galois, uma vez que é muito bem conhecida a estrutura de subgrupos do grupos dos Quatérnios. Finalmente, em posse dos resultados e caracterizações dos capítulos precedentes, juntamente aos resultados que relacionam formas quadráticas e álgebras quaterniônicas, no capítulo 6 demonstramos o Critério de Witt, que acerta sobre a imersão de extensões biquadráticas em quaterniônicas. Deste critério obtemos um importante resultado de interesse da Teoria dos Números, uma nova caracterização dos números racionais que são somas de três quadrados.

Sumário

Introdução

O resultado fundamental dessa monografia é referente à imersão de extensões biquadráticas em extensões quarteniônicas. Tal resultado é devido ao matemático Ernst Witt $(1911 - 1991)$ e foi tratado no seguinte artigo de 1936: *Konstruktion von galoisschen Korpern der Charakteristik p zu vorgegebenerGruppe der Ordnung* p^f, Journal Reine Angew. Math. $174\ (1936)$, $237 - 245$.

Esse teorema, que ficou conhecido por *Critério de Witt*, tem atual formulação em termos do grupo de Brauer do corpo k, $Br(K)$, mais precisamente sobre relações entre elementos do grupo $Br(K)$ denominadas *obstruções*.

No sentido da definição: $L \supset k$ é quarteniônica se o seu grupo de galois for o grupo dos Quatérnios de ordem 8. Nós investigamos corpos k que admitem tais extensões quarteniônicas, e os caracterizamos segundo sua estrutura de subcorpos e elementos geradores, assim como a ação dos elementos do grupo de galois sobre esses geradores. Como resultado veremos interessante relações aritméticas sobre elementos no corpo k como somas de dois ou três quadrados.

Nossa metodologia será percorrer por caminhos construtivistas do problema em questão. Quero dizer, examinaremos a construção a partir de particulares corpos k de tais extensões quarteniônicas seguindo artigos consultados que abordaram o problema por meio de técnicas elementares do ponto de vista da Teoria dos Números.

Capítulo 1

Extensões Quaterniônicas

Diremos que uma extensão de corpos $L \supset k$ é *quaternônica* se ela for uma extensão galoisiana, isto é, normal e separável, e cujo grupo de Galois, $Gal(L|k)$, é isomorfo ao grupo de Quatérnios de ordem 8. Para nosso propósito, vamos supor que todo corpo base de uma extensão de corpos tem característica distinta de dois, e portanto toda extensão finita de grau 2^n é separável, consequentemente a condição de normalidade será equivalente a de galoisiana.

Relembrando, o grupo de Quatérnios de ordem 8, que denotaremos por $\mathbb{H}$, tem a seguinte apresentação por geradores e relações:

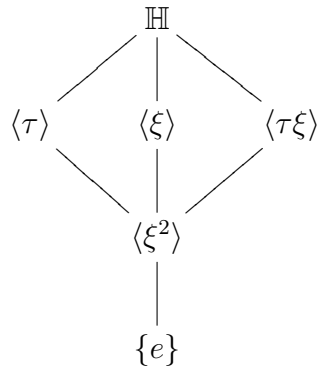
$$\begin{cases} \mathbb{H} = \langle \tau, \xi \rangle, & \mathbb{H} \text{ é gerado por dois elementos,} \\ \tau^4 = 1_{\mathbb{H}}, & \\ \tau^2 = \xi^2 \quad \text{e} & \xi\tau = \tau^3\xi \end{cases}$$

O nosso grupo não abeliano tem apenas 4 subgrupos não triviais, sendo todos subgrupos normais:

três cíclicos de ordem 4	um de ordem 2
$\langle\tau\rangle$ $\langle\xi\rangle$ $\langle\tau\xi\rangle$	$\langle\tau^2\rangle$

A saber, o subgrupo $\langle\tau^2\rangle$ é igual a $\langle\xi^2\rangle$.

A seguir apresentamos um diagrama que mostra exatamente a estrutura de subgrupos do grupo dos Quatérnios:



1.1 Recordando o Teorema Fundamental da Teoria de Galois

Dada uma extensão finita de corpos $M \supset k$ definimos o seu grupo de Galois, que denotaremos por $Gal(M|k)$, como sendo o seguinte subgrupo do grupo de automorfismo do corpo M, $Aut(M)$:

$$Gal(M|k) = \{\sigma : M \xrightarrow{\cong} M \mid \sigma(r) = r, \forall r \in k \}$$

Definição 1.1. Diremos que uma extensão finita de corpos $N \supset k$, com grupo de galois $Gal(N|k)$ é uma extensão normal se satisfaz algumas das condições equivalentes no **Teorema 1.1**, como referência temos o livro de S. Lange [8].

Teorema 1.1. *Fixado um fecho algébrico, k^a, de um corpo k, sobre uma extensão finita de corpos $N \supset k$, com $N \subset k$, as seguintes afirmações são equivalentes:*

1. *Toda imersão $\varepsilon : N \hookrightarrow k^a$ induz um automorfismo de N, isto é, $\varepsilon(N) \subset N$.*

2. *Para todo $x \in N - k$ existe $\sigma \in Gal(N|k)$ tal que $\sigma(x) \neq x$;*

3. *Todo polinômio irredutível $p(X) \in k[X]$ se $p(X)$ tem uma raiz em N então todas as outras raízes estão em N;*

4. *N é um corpo de raízes para algum polinômio $f(X) \in k[X]$;*

O Teorema Fundamental da Teoria de Galois, TFTG, apresenta uma correspondência biunívoca, denominada *correspondência galoisiana,* entre os corpos S intermediários a uma extensão galoisiana $N \supset k$ e os subgrupos H do grupo de Galois $Gal(N|k)$, fazendo corresponder:

$$S \mapsto Gal(N|S),$$

onde

$Gal(N|S) = \{\sigma \in Gal(N|k) \mid \sigma(s) = s, \forall s \in S\ \}$ - o subgrupo que fixa S,

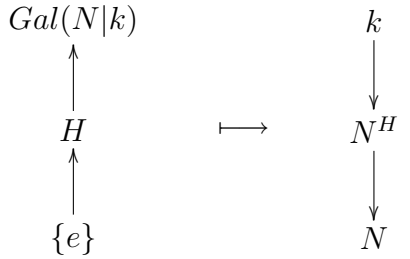
com inversa definida por

$$H \mapsto N^H,$$

onde

$N^H = \{x \in N \mid \sigma(x) = x, \forall \sigma \in H\ \}$ - o corpo fixo por H.

Representamos no diagrama a seguir o esquema de inclusões reversas decorrentes da correspondência galoisiana:



A teoria de Galois acerta que a extensão $N^H \supset k$ é normal se, e só se, H é subgrupo normal de $Gal(N|k)$, e neste caso, o grupo de Galois de $N^H \supset k$, $Gal(N^H|k)$, é isomorfo ao quociente de grupos $Gal(N|k)/H$, e portanto o seu grau de extensão é igual ao índice de H em $Gal(N|k)$, ou seja:

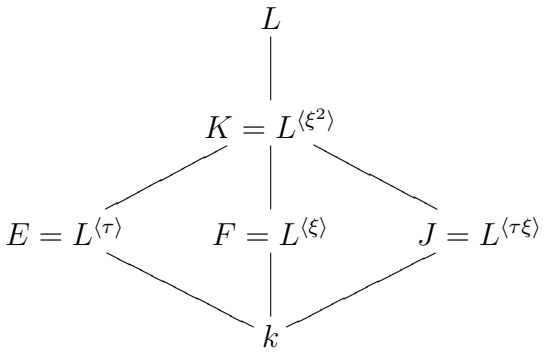
$$[N^H : k] = [Gal(N|k) : H]$$

Partindo do conhecimento da estrutura dos subgrupos do grupo $\mathbb{H}$ dos Quatérnios e da facilidade de reconhecer o quociente de $\mathbb{H}$ por seus subgrupos, pela correspondência acima podemos reconhecer detalhes da estrutura dos corpos intermediários a uma extensão quaterniônica, detalhes que serão investigados em nosso próximo capítulo no qual trataremos das extensões intermediárias e seu respectivos grupos, os quais tem ordens baixas iguais a 2 ou a 4.

Capítulo 2

Extensões Intermediárias

Pela correspondência galoisiana uma extensão quaterniônica $L \supset k$ apresenta a seguinte estrutura de subcorpos intermediários:



Como todos os subgrupos de $\mathbb{H}$ são normais pela Teoria de Galois todos os subcorpos intermediários a $L \supset k$ são extensões normais de k. A teoria de Galois nos diz que o grupo de Galois de $K \supset k$, $Gal(K|k)$, é isomorfo a $\mathbb{H}/\langle \xi^2 \rangle$. Este, que por sua vez, é isomorfo a V_4, o 4-grupo de Klein. Portanto, a extensão $K \supset k$ é dita uma **$\mathbf{V_4}$ - extensão**, ou extensão *biquadrática*.

Os grupos de Galois $Gal(L|E)$, $Gal(L|F)$ e $Gal(L|J)$ são, respectivamente, isomorfos a $\langle \tau \rangle$, $\langle \xi \rangle$ e $\langle \tau\xi \rangle$. Deste modo, ambas extensões são **cíclicas de grau**

4. Enquanto as extensões $E \supset k,\ F \supset k$ e $J \supset k$ são **quadráticas**, visto que seus grupos de Galois são, respectivamente, isomorfos a $\mathbb{H}/\langle\tau\rangle,\ \mathbb{H}/\langle\xi\rangle,\ \mathbb{H}/\langle\tau\xi\rangle$, todos grupos de ordem 2.

Vamos agora fazer uma pausa, afim de trabalhar um pouco mais detalhes destas extensões intermediárias à nossa extensão quaterniônica.

2.1 Extensões Quadráticas

Os resultados a seguir, consultados em [9], sobre extensões quadráticas foram incluidos pelo seu carácter pragmático, da simplicidade que demonstra e pela nossa necessidade de auferir proveitos do seus desdobramentos.

Um corpo quadrático é construido a partir de um corpo k (característica de k distinta de 2) pela adjuncão das raízes x_1 e x_2 de um polinômio quadrático irredutível $f \in k[X]$. Por isso, um corpo quadrático sobre k será denotado por K_f, onde o indíce f faz referência ao polinômio irredutível $f \in k[X]$.

Para determinar a irredutibilidade de um polinômio quadrático $f = aX^2 + bX + c$, $a \neq 0$, basta verificar o discriminante $D = b^2 - 4ac$. Este será redutível se, e somente se, D for um quadrado perfeito em k.

De qualquer forma sabemos, desde a época do colégio, que as raízes de f são expressões do tipo:

$$x_1 = \frac{-b+\omega}{2a},\ \ x_2 = \frac{-b-\omega}{2a},\quad \text{onde } \omega^2 = D.$$

Para nosso propósito, vamos supor daqui em diante que $\omega \notin k$, ou seja, vamos supor que f é irredutível em $k[X]$.

Assim, para obter K_f, basta adjuntar ao corpo k o elemento ω, ou seja, a raiz quadrada do discriminante de f. Resumimos isto no seguinte lema.

Lema 2.1. *$K_f = K_g$, onde $g(X) = X^2 - D \in k[X]$.*

Conseqüetemente, também podemos assumir que D é livre de fatores quadráticos em k. Sim, pois se $D = s^2 D_1$, $s \in k$, é claro que $K_f = K_{g_1}$, onde $g_1(X) = X^2 - D_1$.

Portanto o corpo quadrático K_f é igual ao corpo $k(\omega) = \{a + b\omega \mid a, b \in k\}$. Essa última igualdade justifico apenas mencionando que é uma decorrência direta da existência de divisão euclidiana no anel $k[X]$. Justifica-se agora também o adjetivo quadrático, visto que 2 é a dimensão de $k(\omega)$ como k - espaço vetorial, isto é, $[k(\omega) : k] = 2$.

Observação 1. *Por outro lado, dada uma extensão de corpos $E \supset k$, quadrática, isto é, $[E : k] = 2$, existe um polinômio irredutível de segundo grau, $f \in k[X]$, tal que E é um corpo obtido pela adjunção de suas raízes, ou seja, $E = K_f$.*

Considerando um elemento $x = a + b\omega$ do corpo quadrático $k(\omega)$, a aplicaçao:

$$\begin{array}{rccc} \sigma_c \ : & k(\omega) & \longrightarrow & k(\omega) \\ & x & \longmapsto & \overline{x} \end{array}$$

onde $\overline{x} = a - b\omega$, é um k - automorfismo de $k(\omega)$. De fato, podemos assumir sem as detalhadas demonstrações nosso próximo teorema.

Teorema 2.2. *Se x e y são dois elementos quaisquer de $k(\omega)$, então valem as seguintes propriedades:*

1. $\overline{x + y} = \overline{x} + \overline{y}$
2. $\overline{xy} = \overline{x}\,\overline{y}$
3. $\overline{\overline{x}} = x$
4. *se $x = a + b\omega$, então $x + \overline{x} = 2a$ e $x\overline{x} = a$*
5. $x = \overline{x}$ *se, e somente se,* $x \in k$

De fato σ_c é o único automorfismo de $k(\omega)$, diferente de 1_k, que fixa o subcorpo k.

Teorema 2.3. $Gal(k(\omega)|k) \cong \dfrac{\mathbb{Z}}{2\mathbb{Z}}$

Demonstração. Seja π um k - automorfismo não trivial de $k(\omega)$. Assim, $\pi(\omega) = a + b\omega \neq \omega$. De $\omega^2 = D \in k$, vem:

$$D = \pi(D) = \pi(\omega^2) = \pi(\omega)^2 = (a + b\omega)^2 = a^2 + Db^2 + 2ab\omega,$$

logo $D = a^2 + Db^2$ e $ab = 0$, consequentemente, a ou b deve ser nulo, mas não ambos, pois $\pi(\omega) \neq 0$.

Deve se ter $b \neq 0$, pois caso contrário, de $a^2 = D$, teríamos um absurdo pois D não é um quadrado em k. Portanto $Db^2 = D$. Assim $b = \pm 1$; como $\pi \neq 1_k$, concluímos que $b = -1$, isto é, $\pi(\omega) = -\omega$ e daqui resulta que $\pi = \sigma_c$. □

A fim de usar uma notação mais comumente habituada expressaremos $\omega = \sqrt{D}$. Assim nossa extensão quadrática ficará denotada do tipo $k(\sqrt{D}) \supset k$.

Citaremos nesse fim de seção, sem a devida demonstração, porém seja simples, um lema que iremos utilizar posteriormente com frequência.

Lema 2.4. *Se $a, b \notin k^2$, então $k(\sqrt{a}) = k(\sqrt{b})$ se, e somente se, $\dfrac{a}{b}$ é um quadrado em k.*

Habitualmente trabalhamos com a formulação equivalmente: se $a, b \notin k^2$ então $ab^{-1} \notin k^2$ se, e somente se, $k(\sqrt{a}) \neq k(\sqrt{b})$.

2.2 Extensões Cíclicas de grau 4

Vamos a seguir apresentar resultados, conforme leitura feita em [2], que caracterizam as extensões $C \supset k$ de grau 4 que são cíclicas, isto é, cujo grupo de Galois $Gal(C|k)$ é isomorfo a $(\mathbb{Z}_4, \oplus)$.

Sobre o grupo abeliano $\mathbb{Z}_4$, de ordem 4, ele é caracterizado por ter apenas um subgrupo de ordem 2.

Deste modo apresentamos a seguir, respectivamente, a estrutura de subgrupos de $\mathbb{Z}_4$ e de subcorpos intermediários a $C \supset k$:

$$\begin{array}{ccc} \mathbb{Z}_4 & & k = C^{\mathbb{Z}_4} \\ \uparrow & & \downarrow \\ \mathbb{Z}_2 & & E = C^{\mathbb{Z}_2} \\ \uparrow & & \downarrow \\ \{e\} & & C = C^{\{e\}} \end{array}$$

As extensões $C \supset E$ e $E \supset k$ são quadráticas. Da seção anterior, sobre extensões quadráticas, decorrem nossos dois seguintes teoremas:

Teorema 2.5. *Seja C uma extensão cíclica de grau 4 sobre um corpo k. Então existe um elemento $d \in k$, tal que d não é um quadrado em k, e existem elementos $e, f \in k$ tais que $C = k\left(\sqrt{e + f\sqrt{d}}\right)$ e além disso $d(e^2 - f^2 d)$ é um quadrado em k.*

Demonstração. De fato, como já observamos, existem $d, e, f \in k$, com $d \notin k^2$ e $e + f\sqrt{d} \notin k(\sqrt{d})^2$, tais que:

$$E = k(\sqrt{d}) \text{ e } C = E\left(\sqrt{e + f\sqrt{d}}\right) = k\left(\sqrt{e + f\sqrt{d}}\right)$$

Com isso, temos a primeira parte do teorema. Falta mostrar que $d(e^2 - f^2 d)$ é um quadrado em k.

Para isto, vamos mostrar que $e^2 - f^2 d$ **não é** um quadrado em k, pois desta forma o elemento $\sqrt{e^2 - f^2 d}$ geraria uma extensão quadrática de k, e como

$C \supset k$ admite apenas um subcorpo intermediário, teríamos então que

$$k(\sqrt{d}) = k(\sqrt{e^2 - f^2 d})$$

Por sua vez, pelo **Lema 1.4**, isto implicaria que $d(e^2 - f^2 d)$ é um quadrado em k, conforme queremos.

Denotaremos $\theta^2 := e + f\sqrt{d}$ e $\phi^2 := e - f + \sqrt{d}$, então θ e ϕ são raízes do polinômio:

$$p(X) = (X^2 - \theta^2)(X^2 - \phi^2) = X^4 - 2eX^2 + (e^2 - f^2 d) \in k[X]$$

Eis um polinômio irredutível sobre k, pois como $[C : k] = 4$, p não tem fator irredutível de grau 3 em $k[X]$. Como $C \supset k$ é normal, logo contém todas as raízes que $p(X)$, portanto $\phi \in C$.

Consideremos Δ^2, o discriminante de $p(X)$, temos:

$$\Delta^2 = (2\theta)^2(2\phi)^2(\theta - \phi)^2(\theta + \phi)^2(-\theta + \phi)^2 = 16\theta^2(e^2 - f^2 d)f^4 d^2 \qquad (2.1)$$

Como $Gal(C|k)$ é cíclico de ordem 4 , $Gal(C|k)$ não é subgrupo de $\mathbb{A}_4$, o grupo das permutações pares das permutações sobre 4 elementos. Portanto existe $\sigma \in Gal(C|k)$ tal que $\sigma(\Delta) = -\Delta$, logo $\Delta \notin k$, e então $e^2 - f^2 d$, por 2.1, não é um quadrado em k, conforme queríamos demonstrar.

□

Reciprocamente, provaremos o seguinte:

Teorema 2.6. *Suponhamos que $d \in k$ não é um quadrado em k e existem $e, f \in k$, tais que $d(e^2 - f^2 d)$ é um quadrado em k. Então $C = k\left(\sqrt{e + f\sqrt{d}}\right)$ é uma*

extensão cíclica de grau 4; e além disso, o polinômio $p(X) = X^4 - 2eX^2 + (e^2 - f^2d)$ *é o polinômio minimal de* $\sqrt{e + f\sqrt{d}}$*, isto é, o polinômio mônico irredutível o qual* $\sqrt{e + f\sqrt{d}}$ *é uma raiz.*

Demonstração. Por hipótese $d(e^2 - f^2d)$ é um quadrado em k e d não é um quadrado em k. Consequentemente $e^2 - f^2d$ não pode ser um quadrado em k.

Vamos mostrar primeiro que $e \pm f\sqrt{d}$ não é um quadrado em $k(\sqrt{d})$, afim de podermos construir as extensões quadráticas:

$$k\left(\sqrt{e + f\sqrt{d}}\right) \supset k(\sqrt{d}) \supset k \qquad \text{e} \qquad k\left(\sqrt{e - f\sqrt{d}}\right) \supset k(\sqrt{d}) \supset k$$

De fato, se

$$e \pm f\sqrt{d} = (r + s\sqrt{d})^2 = r^2 + s^2d + 2rs\sqrt{d}$$

então $e = r^2 + s^2d$ e $f = \pm 2rs$. Logo,

$$e^2 - f^2d = (r^2 + s^2d)^2 - 4r^2s^2d = (r^2 - s^2d)^2,$$

um absurdo, contrariando nossas hipóteses.

Assim como na demonstração do teorema anterior, $\theta = \sqrt{e + f\sqrt{d}}$ é uma raiz do polinômio, irredutível em $k[X]$:

$$p(X) = X^4 - 2eX^2 + (e^2 - f^2d) = (X^2 - (e + f\sqrt{d}))(X^2 - (e - f\sqrt{d}))$$

Desde que

$$\frac{e - f\sqrt{d}}{e + f\sqrt{d}} = \frac{(e - f\sqrt{d})^2}{e^2 - f^2d} = \frac{(e - f\sqrt{d})^2(\sqrt{d})^2}{(e^2 - f^2d)d},$$

temos que $\dfrac{e - f\sqrt{d}}{e + f\sqrt{d}}$ é um quadrado em $k(\sqrt{d})$. Consequentemente:

$$C \;:=\; k\left(\sqrt{e + f\sqrt{d}}\right) \;=\; k\left(\sqrt{e - f\sqrt{d}}\right)$$

Portanto C contém todas as raízes do polinômio $p(X)$, ou seja, é um corpo de raízes. Isto significa que $C \supset k$ é uma extensão normal. Pela Teoria de Galois a ordem de $Gal(C|k)$ é igual ao grau da extensão $C \supset k$, isto é:

$$|Gal(C|k) = [C : k]$$

Este últimos, como sabemos é igual a 4.

Assim o grupo de galois $Gal(C|k)$ é cíclico de ordem 4 ou é isomorfo a V_4, o 4-grupo de Klein.

Devemos examinar o discriminante de $p(X)$, para concluir sobre a natureza de $G(C|k)$, uma vez que sabemos que o 4-grupo de Klein é um grupo de permutações pares, isto é, V_4 é um subgrupo de $\mathbb{A}_4$.

Do teorema anterior:

$$\Delta^2 = 16(e^2 - f^2d)f^4d^2$$

Mas como vimos inicialmente, $e^2 - f^2d$ não é um quadrado em k, então $\Delta \notin k$. Portanto $Gal(C|k)$ é cíclico de ordem 4, conforme queríamos demonstrar.

□

Observação 2. *Nas condições acima, a extensão* $k\left(\sqrt{e + f\sqrt{d}}\right) \supset k$ *é uma* V_4*-extensão se, e somente se,* $e^2 - f^2d$ *é um quadrado em* k*. Sobre tais extensões vamos traçar mais comentários seção seguinte* **2.4**.

A condição $d(e^2 - f^2d)$ ***é um quadrado em*** k é equivalente a d ***é uma soma de dois quadrados em*** k.

De fato, se existe $r \in k$ tal que $d(e^2 - f^2d) = r^2$, então:

$$d = \left(\frac{r}{e}\right)^2 + \left(\frac{df}{e}\right)^2$$

Reciprocamente, se existem $x, y \in k$ tais que $d = x^2 + y^2$, tome $e = \frac{1}{x}$ e $f = \frac{y}{xd}$, então:

$$d\left(\frac{1}{x^2} - \frac{y^2}{x^2d^2}d\right) = 1 \text{ , que é um quadrado em } k, \text{ por outro lado,}$$

$$e^2 - f^2d = \left(\frac{1}{x^2} - \frac{y^2}{x^2d^2}d\right) = \frac{1}{d} \text{ , não é um quadrado em } k.$$

Desta forma mostramos que um corpo quadrático $k(\sqrt{d})$ pode ser imerso, estar contido, em uma extensão cíclica de grau 4 se, e somente se, d é soma de dois quadrados em k.

2.3 Extensões Cíclicas de grau 4 com raízes da unidade

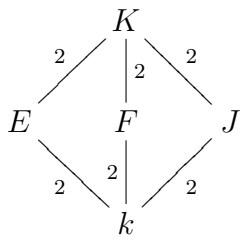
Nesta seção vamos apenas enunciar um teorema, cuja demonstração pode ser encontrada, entre outros, no livro de S. Lang [8]. Este resultado nos será util para quando formos trabalhar com corpos em que tais possuem raízes da unidade.

Teorema 2.7. *Seja $F \supset k$ uma extensão normal. Seja ξ uma raiz n- ésima da unidade. Suponhamos que $\xi \in k$. Nestas condições: $F \supset k$ é uma extensão cíclica se, e somente se, F é um corpo de raízes para um polinômio $X^n - a \in k[X]$, irredútível sobre k.*

2.4 V_4- Extensões

O 4-grupo de Klein, que denotaremos por V_4, caracteriza-se por ter ordem 4 e ter 3 subgrupos distintos não trivias.

Pela teoria de Galois, uma V_4-extensão $K \supset k$ apresenta a estrutura de subcorpos:



Portanto existem elementos $a, b, c \in k - k^2$, satisfazendo também

$$ab^{-1},\ ac^{-1},\ bc^{-1} \in k - k^2,$$

tais que:

$$E = k(\sqrt{a}) \qquad F = k(\sqrt{b}) \qquad J = k(\sqrt{c})$$

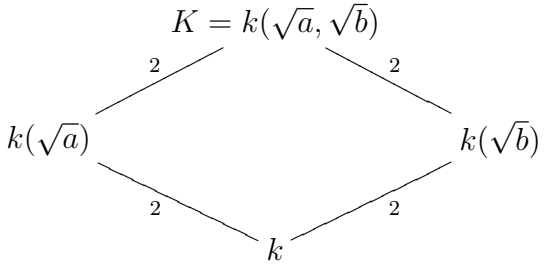
Consideremos a seguinte torre:

$$\underbrace{k(\sqrt{a}, \sqrt{b}) \supset k(\sqrt{a})}_{\text{grau } 2} \supset k$$

Temos que $K = k(\sqrt{a}, \sqrt{b})$. De fato $k(\sqrt{a}, \sqrt{b}) \supset k(\sqrt{a})$ é uma extensão quadrática. Suponhamos que $b \in k(\sqrt{a})^2$, logo existem $x, y \in k$ tais que:

$b = (x+y\sqrt{a})^2 = (x^2+y^2a)+2xy\sqrt{a} \Rightarrow xy = 0 \Rightarrow b = x^2$ ou $b = y^2a$, absurdo

Deste modo, em particular, uma V_4-extensão tem a seguinte estrutura de subcorpos:



Capítulo 3

Uma Construção elementar de Extensões Quaterniônicas

A nota de R. A. Dean, [2], nos incita a curiosidade ao mencionar que o nosso problema esta relacionado com soma de dois ou três quadrados. De fato, ao investigarmos em [4], Genjiro Fujisaki nos apresenta uma elementar construção lançando mão de hipóteses sobre elementos que são somas de quadrados.

Veremos em detalhes a contribuição de Fujisaka.

Considere um corpo k, de característica distinta de 2. Suponhamos a existência de um elemento $m \in k$ satisfazendo as seguintes condições:

1. $m \notin k^2$
2. $m = p^2 + q^2 + r^2, \quad p, q, r \in k \quad \text{e} \quad pqr \neq 0$
3. $n := p^2 + q^2 \notin k^2 \quad \text{e} \quad mn \notin k^2$

Fixando k^a, um fecho algébrio de k, seja

$$\omega = \sqrt{\sqrt{m}\sqrt{n}(\sqrt{m} + \sqrt{n})(\sqrt{n} + p)} \ \in \ k^a$$

Teorema 3.1 (Fujisaki). *$k(\omega)$ é uma extensão quaterniônica de k .*

Demonstração. Seja $K = k(\alpha, \beta)$, onde $\alpha^2 = m$ e $\beta^2 = n$. Por nossa hipóteses, esta é uma V_4- extensão de k. Denotaremos $Gal(K|k) = \{\sigma_0 = 1_K, \sigma_1, \sigma_2, \sigma_3\}$, onde como sabemos cada k - automorfismo age, sobre $\{\alpha, \beta\ \}$ conforme quadro abaixo:

	α	β
σ_0	α	β
σ_1	$-\alpha$	β
σ_2	α	$-\beta$
σ_3	$-\alpha$	$-\beta$

Seja $L = K(\omega)$. Vamos mostrar que $L \supset k$ é normal e $Gal(L|k) \cong \mathbb{H}$.

Conforme nossa definição, a normalidade de $L \supset k$ é equivalente a para toda imersão $\Sigma : L \longrightarrow k^a$, então $\Sigma(L) \subset L$.

Seja, então, Σ uma imersão de L em k^a. A restrição $\Sigma_{|_K}$ é uma imersão de K em k^a. Como $K \supset k$ é normal, $\Sigma_{|_K} \in Gal(K|k)$, isto é, existe $i \in \{0, 1, 2, 3\}$ tal que $\Sigma_{|_K} = \sigma_i$. Portanto, daqui em diante, toda imersão $\Sigma : L \longrightarrow k^a$ vai ser indexada por um indíce $i \in$, o qual é do automorfismo σ_i, o qual $\Sigma_{|_K}$ = σ_i

Então, vamos verificar que $\Sigma_i(L) \subset L$, onde $\Sigma_i : L \longrightarrow k^a$ é uma imersão. Calculando

$\Sigma_i(\omega)^2$ = $\Sigma_i(\omega^2)$, temos:

Para $i = 1$.

$$\Sigma_1(\sqrt{m}\sqrt{n}(\sqrt{m} + \sqrt{n})(\sqrt{n} + p)) =$$
$$= -\sqrt{m}\sqrt{n}(-\sqrt{m} + \sqrt{n})(\sqrt{n} + p) =$$
$$= \sqrt{m}\sqrt{n}(\sqrt{m} - \sqrt{n})(\sqrt{n} + p) =$$

$$= \sqrt{m}\sqrt{n}(\sqrt{m}+\sqrt{n})(\sqrt{n}+p)\frac{\sqrt{m}-\sqrt{n}}{\sqrt{m}+\sqrt{n}}\frac{\sqrt{m}-\sqrt{n}}{\sqrt{m}-\sqrt{n}} =$$
$$= \omega^2\frac{(\sqrt{m}-\sqrt{n})^2}{r^2}$$

Portanto, $\Sigma_1(\omega) = e_1\omega\dfrac{\sqrt{m}-\sqrt{n}}{r} \in K(\omega) = L$, onde $e_1 \in \{-1, 1\}$.

Do mesmo modo,

$$\Sigma_2(\omega)^2 = \Sigma_2(\omega^2) =$$
$$= -\sqrt{m}\sqrt{n}(\sqrt{m}-\sqrt{n})(-\sqrt{n}+p)$$
$$= \sqrt{m}\sqrt{n}(\sqrt{m}+\sqrt{n})(\sqrt{n}+p)\frac{\sqrt{m}-\sqrt{n}}{\sqrt{m}+\sqrt{n}}\frac{\sqrt{n}-p}{\sqrt{n}+p} =$$
$$= \omega^2\frac{(\sqrt{m}-\sqrt{n})^2}{r^2}\frac{(\sqrt{n}-p)^2}{q^2}$$

Portanto, $\Sigma_2(\omega) = e_2\omega\dfrac{(\sqrt{m}-\sqrt{n})}{r}\dfrac{(\sqrt{n}-p)}{q} \in K(\omega) = L$, onde $e_2 \in \{-1, 1\}$.

Finalmente,

$$\Sigma_3(\omega)^2 = \sqrt{m}\sqrt{n}(-\sqrt{m}-\sqrt{n})(-\sqrt{n}+p)$$
$$= \sqrt{m}\sqrt{n}(\sqrt{m}+\sqrt{n})(\sqrt{n}+p)\frac{-\sqrt{m}-\sqrt{n}}{\sqrt{m}+\sqrt{n}}\frac{-\sqrt{n}+p}{\sqrt{n}+p} =$$
$$= \omega^2\frac{\sqrt{n}-p}{\sqrt{n}+p} = \omega^2\frac{(\sqrt{n}-p)^2}{q^2}$$

Portanto, $\Sigma_3(\omega) = e_3\omega\dfrac{(\sqrt{n}-p)}{q} \in K(\omega) = L$, onde $e_3 \in \{-1, 1\}$.

Pelos calculos acima, verificamos que $\Sigma(\omega)$ estão todos em L, para toda imersão $\Sigma : L \longrightarrow k^a$. Uma vez que as imersões Σ estendem automorfismo de $Gal(K|k)$, podemos concluir $\Sigma(L) \subset L$. Portanto $L \supset k$ é galoisiana e Σ_i são todos k - automorfismos de L, isto é, $\Sigma_i \in Gal(L|k)$, para todo $i \in \{1, 2, 3\}$.

Para $i = 1, 2, 3$, calculando ${\Sigma_i}^2_{|_K}$, a restrição a K de ${\Sigma_i}^2$, temos:

$$\Sigma_{i|_K}^2 = {\sigma_i}^2 = 1_K \quad \text{e que} \quad {\Sigma_i}^2(\omega) = -\omega$$

Portanto, $\omega \notin K$. Assim, $L \supset K$ é uma extensão quadrática, o que implica $[L : k] = [L : K][K : k] = 2 \cdot 4 = 8$.

Deste modo, o grupo de Galois de $L \supset k$, $Gal(L|k)$, é de ordem igual a 8.

É fácil verificar que

$${\Sigma_0}^2 = 1_L \text{ e } \forall i \in \{1,2,3\} \begin{cases} {\Sigma_i}^2 \neq 1_L \\ \Sigma_i \neq {\Sigma_i}^3 \\ \Sigma_{i|_K}^3 = \sigma_i \end{cases}$$

Vamos assumir, então, que $e_i = 1$, $\forall i \in \{1,2,3\}$. Pois, caso contrário, podemos trabalhar com ${\Sigma_i}^3$ no lugar de Σ_i, uma vez que:

$$\Sigma_i^3(\omega) = \Sigma_i(\Sigma_i^2(\omega)) = \Sigma_i(-\omega) = -\Sigma_i(\omega)$$

Denotaremos por Ξ o automorfismo Σ_0, que estende $\sigma_0 = 1_k$, definido por $\Xi(\omega) = -\omega$.

Então temos o conjunto abaixo, dos 8 distintos k - automorfismo de L.

$$Gal(L|k) = \{1_L, \Xi, \Sigma_1, \Sigma_1^3, \Sigma_2, \Sigma_2^3, \Sigma_3, \Sigma_3^3\}$$

Com as seguintes relações abaixo, que verificam-se, mostramos que o grupo de Galois $Gal(L|k)$ é isomorfo ao grupo de Quatérnios.

$$\begin{cases} {\Sigma_i}^4 = 1_L \qquad i = 1,2,3 \\ {\Sigma_i}^2 = \Xi \qquad i = 1,2,3 \\ \Sigma_2\Sigma_1 = \Sigma_3, \Sigma_3\Sigma_2 = \Sigma_1, \Sigma_1\Sigma_3 = \Sigma_2 \\ \Sigma_2\Sigma_1{\Sigma_2}^3 = {\Sigma_1}^3 \end{cases}$$

Falta mostrar que $L = k(\omega)$:

$$\begin{array}{c} L = K(\omega) \\ | \\ k(\omega) \\ | \\ k \end{array}$$

De fato, como

$$\Sigma(\omega) \neq \omega, \quad \forall\, \Sigma \ \in \ Gal(L|k), \quad \Sigma \neq 1_L,$$

tem-se que $Gal(L|k(\omega)) = 1_L$, e portanto $L = k(\omega)$. □

3.1 Construção de Exemplos

Sejam $\mathbb{Q}$ e $\mathbb{Z}$, respectivamente, o corpo dos números racionais e o anel dos inteiros. Dado $m \in \mathbb{Z}$, veremos no último capítulo que se existe uma extensão quaterniônica F de $\mathbb{Q}$ tal que $\mathbb{Q} \subset \mathbb{Q}(\sqrt{m}) \subset F$, então m é soma de três quadrados em $\mathbb{Q}$, e logo $\mathbb{Q}(\sqrt{m}) \supset \mathbb{Q}$ é uma extensão quadrática real.

Seja, então, $m > 0$ um inteiro positivo livre de quadrados. Vamos mostrar, em decorrência do **Teorema de Fujisaki**, que é suficiente m ser soma de três quadrados para que exista uma extensão quaterniônica $F \supset \mathbb{Q}$ com $\mathbb{Q}(\sqrt{m}) \subset F$.

Uma outra famosa caracterização sobre somas de quadrados devida a Gauss, [5] e [11] , afirma que m é soma de três quadrados em $\mathbb{Z}$ se, e somente se,

$$m \equiv 1, 2, 3, 5, 6 \text{ mod}(8)$$

É também conhecido que m é soma de dois quadrados em $\mathbb{Z}$ se, e só se, m não é divisível por nenhum primo $p \equiv 3 \text{ mod}(4)$. Além disso, conforme [11] , m é

soma de três quadrados (ou dois quadrados) em $\mathbb{Z}$ se, e somente se, m é soma de três quadrados (ou dois quadrados) em $\mathbb{Q}$.

Consideremos então $\mathbb{Q}(\sqrt{m})$ uma extensão quadrática real de $\mathbb{Q}$, onde m é um inteiro livre de quadrados e $m \not\equiv 4, 7 \bmod(8)$.

1. Suponhamos que

$$m = p^2 + q^2 + r^2, \quad p, q, r > 0 \quad \text{em } \mathbb{Z}$$

e m não é soma de dois quadrados em $\mathbb{Z}$.

Se nós definirmos $n := p^2 + q^2$, n não é um quadrado e mn também não. De fato, se $mn = j^2$, então $m = \dfrac{(mp)^2}{j^2} + \dfrac{(mq)^2}{j^2}$ que implica m uma soma de dois quadrados em $\mathbb{Z}$, pois o é em $\mathbb{Q}$.

2. Suponha que

$$m = p^2 + q^2, \quad p, q > 0 \quad \text{em } \mathbb{Z}$$

Considere $n := m + 1 = p^2 + q^2 + 1^2$, e então de $m \equiv 1, 2, 3, 5, 6 \bmod(8)$ teremos que $n \equiv 1, 2, 3 \bmod(4)$. Claro que $n \equiv 1 \bmod(4)$ não pode ocorrer, pois implicaria em $m \equiv 0 \bmod(4)$, um absurdo supondo m livre de quadrados. Portanto n não é um quadrado em $\mathbb{Z}$, pois verifica-se que o único quadrado não nulo em $\mathbb{Z}_4$ é a classe $\bar{1}$.

O inteiro mn também não é um quadrado. Por absurdo, suponhamos que mn é uma quadrado. Logo existe um primo t tal que $t \mid m$ e $t^2 \mid mn$. Como m é livre de quadrados, então t divide n, absurdo pois $\text{mdc}(m, n) = 1$.

De acordo com o caso 1 para $\omega = \sqrt{\sqrt{m}\sqrt{n}(\sqrt{m} + \sqrt{n})(\sqrt{n} + p)}$, pelo Teorema de Fujisaki

$$K = \mathbb{Q}(\omega) \supset \mathbb{Q}(\sqrt{m}, \sqrt{n}) \supset \mathbb{Q}(\sqrt{m})$$

é uma extensão quaterniônica de $\mathbb{Q}$.

No segundo caso, com $\omega' = \sqrt{\sqrt{m}\sqrt{n}(\sqrt{m} + \sqrt{n})(\sqrt{m} + p)}$ pelo mesmo teorema $\mathbb{Q}(\omega') \supset \mathbb{Q}$ também é uma extensão quaterniônica que contém $\mathbb{Q}(\sqrt{m})$.

Capítulo 4

Extensões Quaterniônicas com raízes da unidade

Com observamos no capítulo anterior $\mathbb{Q}(\sqrt{-1})$ não pode estar contida numa extensão quaterniônica de $\mathbb{Q}$. Mas como veremos a seguir, existe extensão L, galoisiana sobre $\mathbb{Q}(\sqrt{-1})$, tal que $\mathbb{H} \cong Gal(L|\mathbb{Q}(\sqrt{-1}))$.

Então nesta seção vamos obter uma caracterização de extensões quaterniônicas de corpos $L \supset k$ assumindo que a característica do corpo base k seja distinta de 2, e que k contenha o conjunto μ_4 das raízes do polinômio $X^4 - 1 \in k[X]$, ou seja, o conjunto das raízes quarticas da unidade.

Vamos considerar a apresentação de $Gal(L|k) \cong \mathbb{H}$:

$$\begin{cases} \mathbb{H} = \langle \tau, \xi \rangle, & H \text{ é gerado por dois elementos} \\ \tau^4 = 1_{\mathbb{H}} & \\ \tau^2 = \xi^2 \quad \text{e} \quad \xi\tau = \tau^3\xi & \end{cases}$$

4.1 Estrutura

Nessas condições, $\mu_4 \subset k$, a extensão cíclica $L \supset E$, onde $E = L^{\langle \xi \rangle}$ é o corpo fixo do subgrupo cíclico $\langle \xi \rangle$, pelo **Teorema** 2.7 é da forma $L = E(\gamma) \supset E$, onde γ é raiz de um polinômio do tipo $X^4 - u \in E[X]$, com $u \in \dot{k} - k^2$ ($\dot{k} = k - \{0\}$). Já as extensões quadráticas $E \supset k$ e $F = L^{\langle \tau \rangle} \supset k$ são da forma, respectivamente, $E = k(\alpha)$ e $F = k(\beta)$, com $\alpha^2 = a \in \dot{k} - k^2$ e $\beta^2 = b \in \dot{k} - k^2$, com $\alpha\beta^{-1} \notin k^2$. Conclusão:

$$L = k(\alpha, \gamma)$$

Tendo descrito os geradores de $L \supset k$, vamos proceder agora em determinar a ação de τ e ξ sobres esse geradores. Como veremos, obtendo essas informações teremos, também, informações suficientes para proceder ao reverso, isto é, construir extensões quaterniônicas a partir de corpos k que contenham μ_4.

Com as restrições dos automorfismos τ e ξ aos corpos F e E, respectivamente, obtemos os grupos de Galois das extensões quadráticas $E = k(\alpha) \supset k, \alpha^2 \in k$ e $F = k(\beta) \supset k, \beta^2 \in k$.

$$Gal(E|k) = \langle \rho \rangle, \text{ onde } \rho = \xi_{|_E} : E \longrightarrow E$$

$$Gal(F|k) = \langle \sigma \rangle, \text{ onde } \sigma = \tau_{|_F} : F \longrightarrow F$$

Por conseguinte,

$$\begin{cases} \xi(\alpha) = \rho(\alpha) = -\alpha \\ \xi(\beta) = \beta, \quad \text{pois} \quad \beta \in F = L^{\langle \xi \rangle} \\ \tau(\alpha) = \alpha, \quad \text{pois} \quad \alpha \in E = L^{\langle \tau \rangle} \\ \xi(\beta) = \sigma(\beta) = -\beta, \quad \text{pois} \quad \beta \in F = L^{\langle \xi \rangle} \end{cases}$$

Falta, então, determinar $\tau(\gamma)$ e $\xi(\gamma)$.

As raízes de $X^4 - u$, formam o conjunto $\{\pm\gamma, \pm i\gamma\}$. Como τ é um E - automorfismo, segue que $\tau(\gamma)$ é uma raíz de $X^4 - u$, isto é, $\tau(\gamma) \in \{\pm\gamma, \pm i\gamma\}$.

$\tau(\gamma) \notin \{\pm\gamma\}$, pois caso contrário, τ^2 fixaria $k(\alpha, \gamma) = L$, um absurdo pois $\tau^2 \neq 1_L$.

Se $\tau(\gamma) = -i\gamma$, então, como $\tau^3(\alpha) = \alpha$, $\tau^3(\beta) = -\beta$ e $\tau^3(\gamma) = i\gamma$, vamos assumir, sem perda de generalidade, que $\tau(\gamma) = i\gamma$. Pois caso contrario poderíamos trabalhar com τ^3, uma vez que $\langle\tau\rangle = \langle\tau^3\rangle$.

Falta determinar $\xi(\gamma)$. Para isto, verificamos que, $\dfrac{\xi(\gamma)}{i\beta\gamma}$ é fixado por $\langle\tau\rangle$. De fato, como $\tau\xi = \xi^3\tau$ e $\tau^2 = \xi^2$:

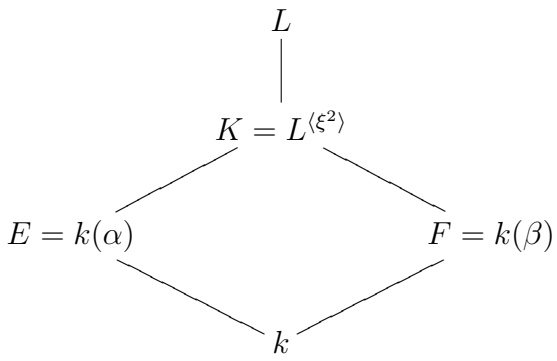
$$\tau\left(\frac{\xi(\gamma)}{i\beta\gamma}\right) = \frac{\tau\xi(\gamma)}{i\tau(\beta)\tau(\gamma)} = \frac{\tau\xi(\gamma)}{-i\beta i\gamma} = \frac{\xi^3\tau(\gamma)}{\beta\gamma}$$
$$= \frac{i\xi\tau^2(\gamma)}{\beta\gamma} = \frac{-i\xi(\gamma)}{\beta\gamma} = \frac{\xi(\gamma)}{i\beta\gamma}$$

Portanto, $\dfrac{\xi(\gamma)}{i\beta\gamma} = e \in E = L^{\langle\tau\rangle}$.

A ação de ξ e τ, sobre α, β e γ é sintetizado, finalmente, no seguinte quadro:

	α	β	γ
τ	α	$-\beta$	$i\gamma$
ξ	$-\alpha$	β	$i\beta e\gamma$

Prosseguindo, temos a torre:



Vamos olhar para a extensão quadrática $L \supset K$. É claro que $L = K(\gamma)$, pois $Gal(L|K(\gamma)) = 1_L$. Sabemos também que $Gal(L|K) = \langle \xi^2 \rangle$, mas não é direto que $\xi^2(\gamma) = -\gamma$. Isso segue se mostramos que $\gamma^2 \in K$, pois implicaria que o polinômio mininal de γ sobre K, $min(\gamma, K)$ é $X^2 - \gamma^2$, donde, por conseguinte, $\xi^2(\gamma)$ também seria uma raíz, ou seja, $\xi^2(\gamma) = -\gamma$.

Para mostrar que $\gamma^2 \in K = L^{\langle \xi^2 \rangle}$, mostraremos que $\langle \xi^2 \rangle$ fixa γ^2. De fato,

$$\xi^2(\gamma^2) = \tau^2(\gamma^2) = (\tau^2(\gamma))^2 = (-\gamma)^2 = \gamma^2$$

Por outro lado, calculando $\xi^2(\gamma)$, usando que $\xi(\gamma) = i\beta e\gamma$, $e \in E = L^{\langle \tau \rangle}$ temos:

$\xi^2(\gamma) = \xi(i\beta e\gamma) = i\xi(\beta)\xi(e)\xi(\gamma) =$

$= i\beta\xi(e)i\beta e\gamma = -\beta^2 e\xi(e)\gamma = -be\xi(e)\gamma.$

Portanto,

$$-\gamma = -be\xi(e)\gamma \Longrightarrow b = \frac{1}{e\xi(e)}, (e \neq 0)$$

Lembre-se que

$$\xi_{|_E} = \rho : E \longrightarrow E$$

Assim, $b = \dfrac{1}{e\rho(e)}$, é uma norma em $E = k(\alpha)$

Agora vamos determinar $c := \gamma^2$.
$\xi(c) = \xi(\gamma^2) = (\xi(\gamma))^2 = -\beta^2 e^2 c$.
$\xi(\alpha\beta\rho(e)) = -\alpha\beta e, \quad$ pois $\quad \rho^2 = 1_E$.
$= -\alpha\beta e\dfrac{e\rho(e)}{e\rho(e)} = -\alpha\beta e^2\rho(e)\beta^2, \quad$ pois $\quad \beta^2 = b = \dfrac{1}{e\rho(e)}$.

Portanto,

$$\xi\left(\frac{c}{\alpha\beta\rho(e)}\right) = \frac{-\beta^2 e^2 c}{-\alpha\beta e^2\rho(e)\beta^2} = \frac{c}{\alpha\beta\rho(e)} \Longrightarrow \frac{c}{\alpha\beta\rho(e)} \in L^{\xi} = F.$$

Também, como $\tau(c) = \tau(\gamma^2) = -c$, temos:

$$\tau\left(\frac{c}{\alpha\beta\rho(e)}\right) = \frac{-c}{-\alpha\beta\rho(e)} = \frac{c}{\alpha\beta\rho(e)}, \quad \text{pois} \quad \rho(e) \in E = L^{\langle\tau\rangle}$$

$$\Longrightarrow \frac{c}{\alpha\beta\rho(e)} \in E.$$

Portanto, $\dfrac{c}{\alpha\beta\rho(e)} \in E \cap F = k \Longrightarrow c = \kappa\alpha\beta\rho(e), \quad$ para algum $\kappa \in \dot{k}$.

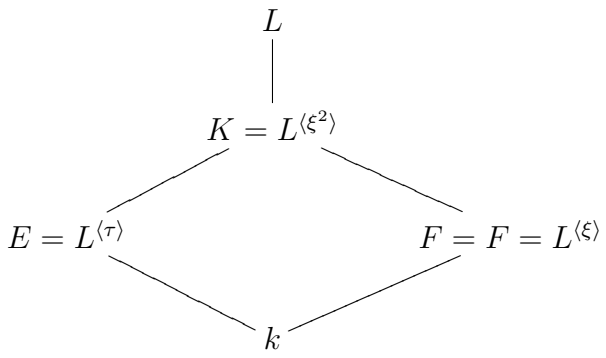
Podemos reunir nossos resultados, obtidos neste capítulo, no seguinte teorema:

Teorema 4.1. *Seja*

$$\mathbb{H} = \langle \xi, \tau |\ \xi^4 = 1, \xi^2 = \tau^2, \tau\xi = \xi^3\tau \rangle$$

e suponhamos que k é um corpo de característica diferente de 2, que contenha μ_4. Suponha também que $L \supset K$ é uma extensão Galoisiana de grau 8 com $Gal(L|k) = \mathbb{H}$. Se $K = L^{\langle\xi^2\rangle}$, $E = L^{\langle\tau\rangle}$ e $F = L^{\langle\xi\rangle}$, então temos a seguinte

estrutura de corpos intermediarios a $L \supset k$.



onde existem elementos $\alpha, \beta, \gamma \in L$*, tais que* $E = k(\alpha)$*,* $F = k(\beta)$*, e* $L = K(\gamma)$*, e tais que* $\xi(\alpha) = -\alpha$*,* $\tau(\beta) = -\beta$ *e* $\tau(\gamma) = i\gamma$*. Então* $\alpha^2 = a$*,* $\beta^2 = b$*, e* $\gamma^2 = c$*, onde* $a, b \in \dot{k}$ *e* $c \in \dot{K}$*, onde* $\alpha\beta^{-1} \notin \dot{k}^2$ *e* $c \notin \dot{K}^2$*.*

Ainda mais, se $\rho = \xi_{|_E}$ *então* $Gal(E|k) = \langle \rho \rangle$*, e existem* $\kappa \in \dot{k}$ *e* $e \in \dot{E}$*, tais que* $b = \dfrac{1}{e\rho(e)}$ *e* $c = \kappa\alpha\beta\rho(e)$ *e finalmente,* τ *e* ξ*, agem como* k *- automorfismos de* L *conforme o quadro seguinte:*

	α	β	γ
τ	α	$-\beta$	$i\gamma$
ξ	$-\alpha$	β	$i\beta e\gamma$

4.2 Construção

Suponha k um corpo de característica diferente de 2 e $\mu_4 \subset k$. Suponhamos que existam elementos a, $b \in \dot{k} - k^2$ satisfazendo:

1. $ab^{-1} \notin k^2$
2. $b \in Im(N_{E|k})$, onde $N_{E|k}$ é a função norma definida sobre $E = k(\alpha)$, $\alpha^2 = a \in k$, como sendo $N(x) = x\rho(x)$, onde $\rho \in Gal(E|k) = \langle \rho \rangle$.

Seja $F \supset k$, a extensão quadrática onde $F = k(\beta)$, e $\beta^2 = b$. Digamos que $Gal(F|k) = \langle\sigma\rangle$. A extensão $K = k(\alpha, \beta) \supset k$, como sabemos, é uma V_4 - extensão galoisiana. Abusando da notação, vamos denotar os elementos de $Gal(K|k)$ por:

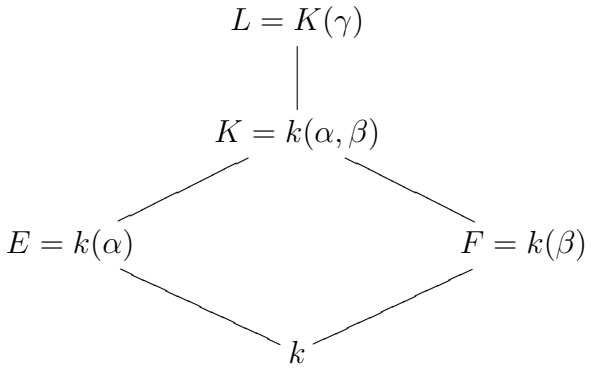
$$Gal(K|k) = \{1_K, \rho, \sigma, \rho\sigma\}$$

Tais elementos agem sobre α, β conforme abaixo:

ρ	σ	$\rho\sigma$
$\alpha \mapsto -\alpha$	$\alpha \mapsto \alpha$	$\alpha \mapsto -\alpha$
$\beta \mapsto \beta$	$\beta \mapsto -\beta$	$\beta \mapsto -\beta$

Finalmente, seja $c = \kappa\alpha\beta\rho(e)$, onde κ é supostamente escolhido de forma que $c \notin \dot{K}^2$.

Então, $L = K(\gamma)$, onde $\gamma^2 = c \in K$, é uma extensão quadrática de K. Mostramos a seguir um diagrama de subcorpos intermediários a $L \supset k$.



Nestas hipóteses, para corpos onde as escolhas de "a" , "b" e "c" podem ser feitas, provamos o seguinte

Teorema 4.2. *A extensão $L \supset k$, como acima, é uma extensão quaterniônica.*

Demonstração. $L \supset k$ é normal. De fato, seja $\xi : L \to k^a$ uma imersão de L num fecho algébrico de k. A restrição $\xi_{|_K} \in Gal(K|k)$, pois $K \supset k$ é normal. Portanto $\xi_{|_K} \in \{1_K, \rho, \sigma, \rho\sigma\}$.

Se $\xi_{|_K} = \rho$, então $(\xi(\gamma))^2 = \xi(\gamma^2) = \xi(\kappa\alpha\beta\rho(e)) = -\kappa\alpha\beta e$.

Como $b \in Im(N_{E|k})$ então $b = \dfrac{1}{e\rho(e)}$, para algum $e \in E$. Tem-se:

$\xi(\gamma^2) = -\kappa\alpha\beta e\beta^2 e\rho(e) = (i\beta e\gamma)^2$. Portanto $\xi(\gamma) = \pm i\beta e\gamma$.

Do mesmo modo, para os outros casos, temos que $\xi(\gamma) \in K(\gamma) = L$. Portanto $\xi \in Gal(L|k)$, e então $L \supset k$ é uma extensão normal.

Nesse caso, então, ξ o k - automorfismo que extende ρ a L, pertence a $Gal(L|F)$, pois $\xi(\beta) = \beta$.

Notemos que $L = E(\gamma)$. De fato, como $\dfrac{\gamma^2}{\beta} = \kappa\alpha\rho(e) \in E = k(\alpha)$, segue-se que $E(\gamma^2) = E(\beta) = K$. Portanto $L = K(\gamma) = E(\gamma^2)(\gamma) = E(\gamma)$.

Uma vez que $\mu_4 \subset E$ e $L = E(\gamma)$, onde $\gamma^4 \in E$ e $\gamma^2 \notin E$, o grupo de Galois de $L \supset E$ é cíclico de ordem 4, digamos $Gal(L|E) = \langle\tau\rangle$. Devemos ter, então $\tau(\alpha) = \alpha$ e $\tau(\beta) = -\beta$. De fato,

$$(\tau(\beta))^2 = \tau(\beta^2) = \tau\left(\frac{1}{e\rho(e)}\right) = \frac{1}{e\rho(e)} = \beta^2$$

Se $\tau(\beta) = \beta$, então $F \subset L^{\langle\tau\rangle} = E$, um absurdo. Pelo mesmo argumento da seção anterior, assumimos que $\tau(\gamma) = i\gamma$.

Seja, como acima, $\xi \in Gal(L|F)$. Portanto, $\xi(\gamma) = \pm i\beta e\gamma$. Calculando $\xi^2(\gamma) = \xi(\xi(\pm i\beta e\gamma) = \pm i\beta\xi(e)\xi(\gamma) = \pm i\beta\rho(e)(\pm i\beta e\gamma) = -\beta^2 e\rho(e)\gamma = = -\gamma = \tau^2(\gamma)$. Como τ^2 e ξ^2, coincidem seus valores também sobre α e β, e além disso, como $L = k(\alpha, \beta, \gamma)$, então $\xi^2 = \tau^2$. Portanto, ξ tem ordem 4, logo implica que $Gal(L|F) = \langle\xi\rangle$. Se $\xi(\gamma) = -i\beta e\gamma$, então $\xi^3(\gamma) = i\beta e\gamma$. Também, como $\xi^3(\alpha) = -\alpha$, $\xi^3(\beta) = \beta$ e $\langle\xi\rangle = \langle\xi^3\rangle$, vamos assumir, sem perda de generalidade, que $\xi(\gamma) = i\beta e\gamma$.

Assim, mostramos, no seguinte quadro, a ação de ξ e τ, sobre α, β e γ:

	α	β	γ
τ	α	$-\beta$	$i\gamma$
ξ	$-\alpha$	β	$i\beta e\gamma$

Para mostrar que que $Gal(L|k) \cong \mathbb{H}$, basta verificar que $\tau\xi = \xi^3\tau$.

Por um lado, $\tau\xi(\gamma) = \tau(i\beta e\gamma) = -i\beta ei\gamma = \beta e\gamma$. Por outro lado, $\xi^3\tau(\gamma) = \xi^3(i\gamma) = i\xi^2(i\beta e\gamma) = i\xi(i\beta\rho(e)i\beta e\gamma) = -i\xi(\gamma) = -ii\beta e\gamma = \beta e\gamma$. Claramente, $\tau\xi(\alpha) = \xi^3\tau(\alpha)$ e $\tau\xi(\beta) = \xi^3\tau(\beta)$.

Portanto, conforme queríamos demonstrar,

$$Gal(L|k) = \{\langle \xi, \tau |\ \ \xi^4 = 1, \xi^2 = \tau^2, \tau\xi = \xi^3\tau\rangle\} \cong \mathbb{H}$$

□

Observação 3. *De acordo com nossas contas temos que*

$$\frac{\xi(\gamma^2)}{\gamma^2} = (i\beta e\gamma)^2 \quad e \quad \frac{\tau(\gamma^2)}{\gamma^2} = (i)^2$$

Pode-se também ver que valem as relações:

$$i\beta e\xi(i\beta e) = -1, \quad i\tau(i) = -1$$

e

$$i\beta e\xi(i) = -i\tau(i\beta e)$$

Vamos mostrar a seguir, no último capítulo, que se tivermos uma V_4- extensão $M \supset k$, com $Gal(M|k) = \langle\sigma, \tau\rangle$ e existem $x, y, w \in \dot{M}$ satisfazendo as relações:

$$x\sigma(x) = -1 = y\tau(y) \quad e \quad x\sigma(y) = -y\tau(x)$$

assim como

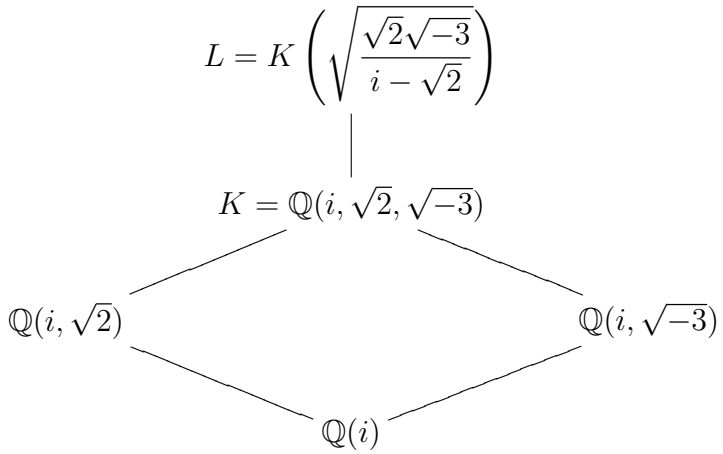
$$\frac{\sigma(w)}{w} = x^2 \quad e \quad \frac{\tau(w)}{w} = y^2$$

então $L = M(\sqrt{w}) \supset k$ é uma extensão quaterniônica.

4.3 Exemplo

Como mencionamos no início do capítulo, de fato existe uma extensão de corpos $L \supset \mathbb{Q}(i)$ quaterniônica. Tome $a = 2, \kappa = 1$ e $e = \dfrac{1}{i + \sqrt{2}}$, então $b = -3$, $c = \dfrac{\sqrt{2}\sqrt{-3}}{i - \sqrt{2}}$.

Pelo **Capítulo 4** a extensão $L(\sqrt{c}) \supset \mathbb{Q}(i)$ é galosiana e $Gal(L|\mathbb{Q}(i)) \cong \mathbb{H}$:



Como já observamos, não podemos imergir o corpo $\mathbb{Q}(\sqrt{-3})$ numa extensão $C \supset \mathbb{Q}$ cíclica de grau 4, justamente porquê -3 não é soma de dois quadrados racionais.

Mas no diagrama acima temos uma situção diferente, pois a extensão $L \supset \mathbb{Q}(i, \sqrt{2})$ é de fato cíclica de grau 4 e como podemos verificar -3 é de fato soma de quadrados em $k = \mathbb{Q}(i, \sqrt{2})$:

$$-3 = (i\sqrt{2})^2 + i^2$$

Logo não é surpresa a imersão de $k(\sqrt{-3})$ na extensão cíclica $L \supset k$.

Capítulo 5

Álgebras Quaterniônicas e Formas Quadráticas

A nossa álgebra central simples (acs) de interesse é a álgebra de Quatérnios. Vamos então neste capítulo conhecer alguns resultados sobre acs, destacando que o Teorema do Duplo Centralizador far-se-á muito útil no demonstração do critério de Witt. Utilizamos como referências os livros clássicos do Scharlau, [10], do Lam, [7], e as notas de Felzenszwalb [3].

5.1 Álgebras Centrais Simples

Uma $\mathbb{K}-$ álgebra nesta monografia será entendida como uma $\mathbb{K}-$ álgebra associativa e com unidade, ou seja, um espaço vetorial de dimensão finita sobre um corpo $\mathbb{K}$, dotado de uma operação de multiplicação associativa e distributiva em relação a soma e assumindo a existência da unidade multiplicativa 1.

Definição 5.1. Sejam A uma $\mathbb{K}-$ álgebra e S um subconjunto de A. Definimos o centralizador de S em A, denotado por $C_A(S)$ como sendo o subconjunto de A caracterizado pela propriedade $a \in C_A(S) \Leftrightarrow as = sa\ ,\ \ \forall s\ \in S$.

Definimos em particular o **centro** de A como sendo o subconjunto $C_A(A)$, simplificadamente denotado por $C(A)$.

Assim, entenderemos por uma $\mathbb{K}-$ álgebra central simples uma $\mathbb{K}-$ álgebra cujo centro é o corpo dos escalares $\mathbb{K}$, visto imerso dentro de A como $1 \cdot \mathbb{K}$. Mais ainda os únicos ideais bilaterais são os triviais, ou seja, 0 e A.

Dizemos simplesmente que uma $\mathbb{K}-$ álgebra é simples se não possui ideaís bilaterais além dos triviais. Podemos então enunciar o Teorema do Duplo Centralizador.

Teorema 5.1 (Duplo Centralizador). *Sejam A uma $\mathbb{K}-$ álgebra central simples e B uma subálgebra simples de A que contém $\mathbb{K}$. Então valem as seguintes propriedades:*

1. $C_A(B)$ *é uma* $\mathbb{K}-$ *subálgebra simples de* A
2. $dim_{\mathbb{K}} A = dim_{\mathbb{K}} B \cdot dim_{\mathbb{K}} C_A(B)$
3. $C_A(C_A(B)) = B$

Definição 5.2. Dados $a, b \in \dot{\mathbb{K}}$ definimos a **álgebra de Quatérnios** $(a, b)_{\mathbb{K}}$ como sendo a $\mathbb{K}-$ álgebra gerada por todas as combinações lineares formais dos símbolos i, j e k :

$$(a, b)_{\mathbb{K}} = \{x + yi + zj + wk \mid x, y, z, w \in \mathbb{K}\}$$

onde a multiplicação é distributivamente estendida para todos elementos via as regras abaixo:

$$i^2 = a,\ j^2 = b,\ k = ij = -ji,$$

e

$$xi = ix,\ xj = jx,\ xk = kx,\ \forall x \in \mathbb{K}$$

Como haveria de ser, toda álgebra de Quatérnios $(a,b)_{\mathbb{K}}$ é central simples. De fato, seja $q = x + yi + zj + wk$ no centro de $(a,b)_{\mathbb{K}}$. Como q comuta com todos os elementos de $(a,b)_{\mathbb{K}}$, obtemos que

$$qi = iq \Rightarrow xi + ya - zk - awj = xi + ya + zk + awj \Rightarrow$$

$$\Rightarrow zk + awj = 0 \Rightarrow z = w = 0$$

e

$$qj = jq \Rightarrow zj + yk = xj - yk \Rightarrow y = 0$$

Portanto, $q \in \mathbb{K}$.

Seja I um ideal bilateral não nulo de $(a,b)_{\mathbb{K}}$ e seja $q = x + yi + zj + wk \in I$ não nulo. Se $y = z = w = 0$, então $q \in \dot{\mathbb{K}}$ e então $1 = qq^{-1} \in I$. Sem perda de generalidade, suponhamos que $y \neq 0$.

$$iqi = (xi+ya+zk+waj)i = xa+yai-azj-wak = a(x+yi-zj-wk) \in I \Rightarrow$$

$$\Rightarrow x+yi-zj-wk \in I \Rightarrow x+yi \in I \Rightarrow j(x+yi)j = xb-byi = b(x-yi) \in I \Rightarrow$$

$$\Rightarrow x - yi \in I \Rightarrow 2yi \in I \Rightarrow y \in I \Rightarrow 1 = yy^{-1} \Rightarrow I$$

E portanto $I = (a,b)_{\mathbb{K}}$ é uma álgebra central simples.

A álgebra dos Quatérnios pode ser obtida como uma subálgebra da álgebra de matrizes $M_{4\times4}(\mathbb{K})$. Conforme veremos na demonstração do Critério de Witt esta apresentação será bastante útil.

Para cada $d \in (a,b)_{\mathbb{K}}$, a aplicação $x \mapsto dx$ é uma $\mathbb{K}-$ transformação linear sobre $(a,b)_{\mathbb{K}}$ e então podemos representa-la por uma matriz $A(d)$ relativa a base $\{1,i,j,k\}$. De fato esta aplicação é uma imersão.

Como:

$$i \mapsto I = \begin{pmatrix} 0 & a & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & a \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad j \mapsto J = \begin{pmatrix} 0 & 0 & b & 0 \\ 0 & 0 & 0 & -b \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$$

Podemos identificar $(a, b)_{\mathbb{K}}$ com a $\mathbb{K}-$ álgebra gerada por I e J em $M_{4\times4}(\mathbb{K})$, que denotaremos por $\mathbb{K}[I, J]$.

Agora vamos tratar alguns conceitos básicos sobre formas quadráticas e relacionalas com as álgebras de Quatérnios.

Uma forma quadrática φ sobre um corpo $\mathbb{K}$ é um polinômio homogêneo de grau 2 a n variáveis em $\mathbb{K}$, isto é,

$$\varphi(X) = \varphi(X_1, \ldots, X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j \in \mathbb{K}[X_1, \ldots, X_n] = \mathbb{K}[X].$$

Como $X_i X_j = X_j X_i$, podemos reescrever φ da seguinte maneira:

$$\varphi(X) = \sum_{i,j=1}^{n} \frac{1}{2}(a_{ij} + a_{ji}) X_i X_j = \sum_{i,j=1}^{n} b_{ij} X_i X_j.$$

Desta forma, $b_{ij} = b_{ji}$ e φ determina uma única matriz $n \times n$ simétrica $M_\varphi = (b_{ij})$, tal que, $\varphi(X) = X^t M_\varphi X$, olhando $X = (X_1, \ldots, X_n)$ como um vetor coluna. Uma forma quadrática φ é dita **regular** se a matriz M_φ é não singular. Além disso, definimos o **determinante** $\det(\varphi)$ como sendo o determinante da matriz simétrica M_φ e o inteiro n como a **dimensão** da forma quadrática φ, que denotamos por $\dim(\varphi)$. De agora em diante, vamos considerar apenas as formas quadráticas regulares e se φ é uma forma quadrática de dimensão n, diremos apenas que φ é uma n–forma. Em particular, se $n = 2$ dizemos também que φ é uma **forma binária**.

Duas formas quadráticas φ e ψ são ditas **isométricas** se existe uma matriz invertível C tal que $\varphi(X) = \psi(CX)$, ou ainda, $M_\varphi = C^t M_\psi C$. Esta é claramente

uma relação de equivalência e escrevemos $\varphi \cong \psi$. Note que dim(φ) é um invariante dessa relação de equivalência e que det(φ), visto como um elemento de $\dot{\mathbb{K}}/\dot{\mathbb{K}}^2$, é também um invariante da classe de equivalência de φ.

Assumindo que o corpo $\mathbb{K}$ tem sempre característica diferente de dois, toda forma quadrática pode ser diagonalizada. Sendo assim, dados $a_1, \ldots, a_n \in \dot{\mathbb{K}}$, utilizaremos a notação clássica $\langle a_1, \ldots, a_n \rangle$ para denotar a forma quadrática:

$$\varphi(X) = a_1 X_1^2 + \cdots + a_n X_n^2$$

Sejam $\varphi = \langle a_1, \ldots, a_n \rangle$ e $\psi = \langle b_1, \ldots, b_m \rangle$ duas formas quadráticas sobre $\mathbb{K}$. Definimos a **soma ortogonal** como sendo a (n+m)–forma $\varphi \perp \psi = \langle a_1, \ldots, a_n, b_1, \ldots, b_m \rangle$ e o **produto tensorial** como a (nm)–forma $\varphi \otimes \psi = \langle a_1 b_1, \ldots, a_1 b_m, \ldots, a_n b_1, \ldots, a_n b_m \rangle$. Para todo $a \in \dot{\mathbb{K}}$, escreveremos $a\varphi$ para denotar a forma $\langle a \rangle \otimes \varphi$. Dado $m \in \mathbb{N}$ escrevemos $m \times \varphi$ para representar a soma $\varphi \perp \ldots \perp \varphi$ de m cópias de φ. Se $\varphi, \psi, \tilde{\varphi}, \tilde{\psi}$ são formas quadráticas, segue das propriedades de matrizes que $\varphi \perp \psi \cong \psi \perp \varphi$, det($\varphi \perp \psi$) = det($\varphi$)det($\psi$) e se $\psi \cong \tilde{\psi}$ e $\varphi \cong \tilde{\varphi}$ então $\varphi \perp \psi \cong \tilde{\varphi} \perp \tilde{\psi}$.

Uma forma quadrática $\langle a_1, \ldots, a_n \rangle$ sobre $\mathbb{K}$ é dita **isotrópica** se existem $x_1, \ldots, x_n \in \mathbb{K}$, não todos nulos, tais que $a_1 x_1^2 + \ldots + a_n x_n^2 = 0$ e dita **anisotrópica** caso contrário. A 2–forma $\langle 1, -1 \rangle$ é a forma quadrática isotrópica de menor dimensão e é chamada de **plano hiperbólico**. Uma forma é dita **hiperbólica** se é isométrica a uma soma de planos hiperbólicos.

Se φ, ψ e γ são formas quadráticas sobre $\mathbb{K}$ e $\varphi \perp \gamma \cong \psi \perp \gamma$ então $\varphi \cong \psi$ pela **Lei do Cancelamento de Witt**.

Uma forma $\varphi \cong \langle a_1, \ldots a_n \rangle$ representa um certo elemento $a \in \dot{\mathbb{K}}$ se, e somente se, existem $x_1, \ldots, x_n \in \mathbb{K}$ tais que $a_1 x_1^2 + \ldots + a_n x_n^2 = a$ se, e somente se, $\varphi \cong \langle a \rangle \perp \psi$ para alguma forma ψ. Denotamos por $D_{\mathbb{K}}(\varphi)$ o subconjunto de $\dot{\mathbb{K}}$ formado pelos elementos que são representados por φ. Se $\phi \cong \psi$ então $D_{\mathbb{K}}(\phi) = D_{\mathbb{K}}(\psi)$.

Seja $(a,b)_{\mathbb{K}}$ uma $\mathbb{K}$–álgebra de quatérnios e $\alpha, \beta \in (a,b)_{\mathbb{K}}$. Seja $\alpha \in (a,b)_{\mathbb{K}}$:

$$\alpha = x + yi + zj + wk$$

Então definimos o **conjugado** $\overline{\alpha}$ por:

$$\overline{\alpha} = x - yi - zj - wk$$

Assumiremos sem as detalhadas demonstrações que $\overline{\alpha+\beta} = \overline{\alpha} + \overline{\beta}$, $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$, $\quad \overline{\overline{\alpha}} = \alpha$ e $\overline{\lambda\beta} = \lambda\overline{\beta}$. Além disso, $\overline{\alpha} = \alpha$ se, e somente se, $\alpha \in \mathbb{K}$. Se $\alpha = yi + zj + wk$ então dizemos que α é um **quatérnio puro**.

Podemos também definir a **norma** de α como $\mathrm{N}(\alpha) = \alpha\overline{\alpha} = \overline{\alpha}\alpha$. Se escrevermos $\alpha = x + yi + zj + wk$ podemos ver que $\mathrm{N}(\alpha) = x^2 - ay^2 - bz^2 + abw^2$. Portanto, a função norma define uma forma quadrática $\langle 1, -a, -b, ab\rangle$ em $(a,b)_{\mathbb{K}}$, que será chamada de **forma norma**.

A seguir apresentamos alguns resultados clássicos, através dos quais as álgebras de Quatérnios estão relacionadas com sua forma norma, e além do mais, esses resultados serão muito úteis na demonstração do Critério de Witt. As demonstrações conforme já mencionado foram consultadas nos livro do Scharlau [10] e do Lam [7].

Teorema 5.2. *Para $a, b, c, d \in \dot{\mathbb{K}}$ as seguintes afirmações são equivalentes:*

1. $\langle 1, -a, -b, ab\rangle \cong \langle 1, -c, -d, cd\rangle$
2. $\langle -a, -b, ab\rangle \cong \langle -c, -d, cd\rangle$
3. $(a,b)_{\mathbb{K}} \cong (c,d)_{\mathbb{K}}$

Teorema 5.3. *Sejam $q = \langle a, b\rangle$ e $q' = \langle c, d\rangle$ duas formas binárias (regulares). Então $q \cong q'$ se, e somente se, det$(q) = d(q')mod(\dot{\mathbb{K}}^2)$ e $D_{\mathbb{K}}(q) \cap D_{\mathbb{K}}(q') \neq \emptyset$.*

Teorema 5.4. *Para todo $a, b, c, d \in \dot{\mathbb{K}}$, temos que:*

1. $(a, b)_{\mathbb{K}} \cong (ac^2, bd^2)_{\mathbb{K}}$.
2. $(a, b)_{\mathbb{K}} \cong (b, a)_{\mathbb{K}}$.
3. $(1, 1)_{\mathbb{K}} \cong (1, a)_{\mathbb{K}} \cong (b, -b)_{\mathbb{K}} \cong (c, 1 - c)_{\mathbb{K}}$ *se* $c \neq 0, 1$.
4. $(a, a)_{\mathbb{K}} \cong (a, -1)_{\mathbb{K}}$.
5. $(a, b)_{\mathbb{K}} \cong (a, -ab)_{\mathbb{K}}$.
6. $[(ab, c)_{\mathbb{K}}] = [(a, c)_{\mathbb{K}}][(b, c)_{\mathbb{K}}]$ *no grupo de Brauer* $Br(\mathbb{K})$

5.2 Grupo de Brauer

Cabe agora definir o grupo de Brauer de um corpo k. Como veremos no capítulo final, as propriedades concerntes as álgebras de Quatérnios que aparecem no **Teorema 5.4** nos permitem fazer uma formulação equivalente, no que se refere a imersão de extensões biquadráticas em quaterniônicas, a original proposta no artigo de Witt [13].

O **Teorema de Wedderburn** afirma que toda álgebra central simples A é isomorfa a uma álgebra de matrizes com entradas num anel de divisão, isto é, existem $n \in \mathbb{N}$ e D, um anel de divisão, tais que $A \cong M_n(D)$, e além disso n é unicamente determinado e D é unico a menos de isomorfismos.

Deste modo podemos definir uma relação de equivalência no conjuntos das $\mathbb{K}-$ álgebras centrais simples do seguinte modo:

Se $A \cong M_n(D)$ e $B \cong M_m(D')$ então

$$A \sim B \Leftrightarrow D \cong D'$$

Se A e B são centrais simples então o resultado pelo produto tensorial também é, isto é, $A \otimes_{\mathbb{K}} B$ é central simples.

Definimos o **grupo de Brauer** de $\mathbb{K}$, que denotaremos $Br(\mathbb{K})$, como sendo o quociente do conjunto de todas as $\mathbb{K}-$ acs pela relação de equivalência definida acima. O produto entre duas classes de acs é definido por: $[A][B] = [A \otimes_{\mathbb{K}} B]$. Esta é de fato uma operação de grupo, bem definida nas classes de equivalências.

Capítulo 6

Critério de Witt

Vamos a princípio obter uma nova caracterização referente a imersão de uma V_4-extensões em extensões quaterniônicas. De fato vamos demonstrar o que ficou evidenciado pela **Observação 4** do **Capítulo 4.**

Seja $M \supset k$ uma V_4- extensão. Sejam $\sigma, \tau \in Gal(M|k)$ dados por

	σ	τ
$\sqrt{a}$	$-\sqrt{a}$	$\sqrt{a}$
$\sqrt{b}$	$\sqrt{b}$	$-\sqrt{b}$

Suponhamos que exista uma extensão quaterniônica $F \supset k$ tal que $M \subset F$, conforme o diagrama abaixo temos a seguinte estrutura de subcorpos:

$$\begin{array}{c} F = M(\sqrt{\omega}) \\ | \\ M = k(\sqrt{a}, \sqrt{b}) \\ | \\ k \end{array}$$

Sejam $\Sigma, \Psi \in Gal(F|k)$, respectivamente, as extensões de σ, τ, ou seja,

$$\Sigma_{|M} = \sigma \quad \text{e} \quad \Psi_{|M} = \tau$$

Ambas extensões tem ordem 4 em $Gal(F|k)$. De fato, caso contrário, suponhamos que $|\Sigma| = 2$, teríamos necessariamente que $F^{\langle\Sigma\rangle} = M$ pois M é a única extensão de grau 4 sobre k contida em F. Chegamos a um absurdo pois $\Sigma(\sqrt{a}) = \sigma(\sqrt{a}) = -\sqrt{a}$. De forma análogo a ordem de Ψ em $Gal(F|k)$ também é 4.

É claro que $M(\Sigma(\sqrt{\omega})) = \Sigma(M(\sqrt{\omega})) = M(\sqrt{\omega})$, e o mesmo vale para Ψ. Deste modo, pelo **Lema 2.4**, existem $x, y \in \dot{M}$ tais que

$$\frac{\Sigma(\omega)}{\omega} = x^2 \quad \text{e} \quad \frac{\Psi(\omega)}{\omega} = y^2$$

$(\Sigma(\sqrt{\omega}))^2 = \Sigma(\omega) = \omega x^2$, o que implica $\Sigma(\sqrt{\omega}) = \pm x\sqrt{\omega}$ e do mesmo modo $\Psi(\sqrt{\omega}) = \pm y\sqrt{\omega}$.

Podemos supor sem perda de generalidade que

$$\Sigma(\sqrt{\omega}) = x\sqrt{\omega} \quad \text{e} \quad \Psi(\sqrt{\omega}) = y\sqrt{\omega},$$

pois caso contrário, se por exemplo supormos que $\Sigma(\sqrt{\omega}) = -x\sqrt{\omega}$, tome então $x' = -x$. Deste modo teremos $\dfrac{\Sigma(\omega)}{\omega} = x^2 = (-x)^2 = x'^2$ e $\Sigma(\sqrt{\omega}) = x'\sqrt{\omega}$.

Uma vez que Σ e Ψ são elementos distintos de ordem 4 e $Gal(F|k)$ é o grupo dos Quatérnios, então satisfazem as relações:

$$\Sigma^2 = \Psi^2 \quad \text{e} \quad \Sigma\Psi = \Psi^3\Sigma$$

Sabendo disto, vamos calcular a ação dos elementos gerados por Σ e Ψ sobre os valores da $k-$ base do espaço F:

$$\{\ 1, \sqrt{a}, \sqrt{b}, \sqrt{w}, \sqrt{a}\sqrt{b}, \sqrt{a}\sqrt{\omega}, \sqrt{b}\sqrt{w}, \sqrt{a}\sqrt{b}\sqrt{\omega}\ \} \subset F$$

Como $\Sigma^4 = \Psi^4 = 1_F$, conforme as **Tabela 6.1** e **6.2** abaixo, concluinos que $(x\sigma(x))^2 = (y\tau(y))^2 = 1$. Como Σ^2 e Ψ^2 não são identidades, temos que

$$x\sigma(x) = y\tau(y) = -1$$

Tabela 6.1: A ação de $\Sigma^i, \quad i = 1, 2, 3.$

	Σ	Σ^2	Σ^3	Σ^4
1	1	1	1	1
$\sqrt{a}$	$-\sqrt{a}$	$\sqrt{a}$	$-\sqrt{a}$	$\sqrt{a}$
$\sqrt{b}$	$\sqrt{b}$	$\sqrt{b}$	$\sqrt{b}$	$\sqrt{b}$
$\sqrt{\omega}$	$x\sqrt{\omega}$	$x\sigma(x)\sqrt{\omega}$	$x^2\sigma(x)\sqrt{\omega}$	$(x\sigma(x))^2\sqrt{\omega}$
$\sqrt{a}\sqrt{b}$	$-\sqrt{a}\sqrt{b}$	$\sqrt{a}\sqrt{b}$	$-\sqrt{a}\sqrt{b}$	$\sqrt{a}\sqrt{b}$
$\sqrt{a}\sqrt{\omega}$	$-x\sqrt{a}\sqrt{\omega}$	$x\sigma(x)\sqrt{a}\sqrt{\omega}$	$-x^2\sigma(x)\sqrt{a}\sqrt{\omega}$	$(x\sigma(x))^2\sqrt{a}\sqrt{\omega}$
$\sqrt{b}\sqrt{\omega}$	$x\sqrt{b}\sqrt{\omega}$	$x\sigma(x)\sqrt{b}\sqrt{\omega}$	$x^2\sigma(x)\sqrt{b}\sqrt{\omega}$	$(x\sigma(x))^2\sqrt{b}\sqrt{\omega}$
$\sqrt{a}\sqrt{b}\sqrt{\omega}$	$-x\sqrt{a}\sqrt{b}\sqrt{\omega}$	$x\sigma(x)\sqrt{a}\sqrt{b}\sqrt{\omega}$	$-x^2\sigma(x)\sqrt{a}\sqrt{b}\sqrt{\omega}$	$(x\sigma(x))^2\sqrt{a}\sqrt{b}\sqrt{\omega}$

Tabela 6.2: A ação de $\Psi^i, \quad i = 1, 2, 3.$

	Ψ	Ψ^2	Ψ^3	Ψ^4
1	1	1	1	1
$\sqrt{a}$	$\sqrt{a}$	$\sqrt{a}$	$\sqrt{a}$	$\sqrt{a}$
$\sqrt{b}$	$-\sqrt{b}$	$\sqrt{b}$	$-\sqrt{b}$	$\sqrt{b}$
$\sqrt{\omega}$	$y\sqrt{\omega}$	$y\tau(y)\sqrt{\omega}$	$y^2\tau(y)\sqrt{\omega}$	$(y\tau(y))^2\sqrt{\omega}$
$\sqrt{a}\sqrt{b}$	$-\sqrt{a}\sqrt{b}$	$\sqrt{a}\sqrt{b}$	$-\sqrt{a}\sqrt{b}$	$\sqrt{a}\sqrt{b}$
$\sqrt{a}\sqrt{\omega}$	$y\sqrt{a}\sqrt{\omega}$	$y\tau(y)\sigma(x)\sqrt{a}\sqrt{\omega}$	$y^2\tau(y)\sqrt{a}\sqrt{\omega}$	$(y\tau(y))^2\sqrt{a}\sqrt{\omega}$
$\sqrt{b}\sqrt{\omega}$	$-y\sqrt{b}\sqrt{\omega}$	$y\tau(y)\sqrt{b}\sqrt{\omega}$	$-y^2\tau(y)\sqrt{b}\sqrt{\omega}$	$(y\tau(y))^2\sqrt{b}\sqrt{\omega}$
$\sqrt{a}\sqrt{b}\sqrt{\omega}$	$-y\sqrt{a}\sqrt{b}\sqrt{\omega}$	$y\tau(y)\sigma(x)\sqrt{a}\sqrt{b}\sqrt{\omega}$	$-y^2\tau(y)\sqrt{a}\sqrt{b}\sqrt{\omega}$	$(y\tau(y))^2\sqrt{a}\sqrt{b}\sqrt{\omega}$

Tabela 6.3: A ação de $\Sigma\Psi$

	Ψ	$\Sigma\Psi$
1	1	1
$\sqrt{a}$	$\sqrt{a}$	$-\sqrt{a}$
$\sqrt{b}$	$-\sqrt{b}$	$-\sqrt{b}$
$\sqrt{\omega}$	$y\sqrt{\omega}$	$x\sigma(y)\sqrt{\omega}$
$\sqrt{a}\sqrt{b}$	$-\sqrt{a}\sqrt{b}$	$\sqrt{a}\sqrt{b}$
$\sqrt{a}\sqrt{\omega}$	$y\sqrt{a}\sqrt{\omega}$	$-x\sigma(y)\sqrt{a}\sqrt{\omega}$
$\sqrt{b}\sqrt{\omega}$	$-y\sqrt{b}\sqrt{\omega}$	$-x\sigma(y)\sqrt{b}\sqrt{\omega}$
$\sqrt{a}\sqrt{b}\sqrt{\omega}$	$-y\sqrt{a}\sqrt{b}\sqrt{\omega}$	$x\sigma(y)\sqrt{a}\sqrt{b}\sqrt{\omega}$

Tabela 6.4: A ação de $\Psi^3\Sigma$

	Σ	$\Psi\Sigma$	$\Psi^2\Sigma$	$\Psi^3\Sigma$
1	1	1	1	1
$\sqrt{a}$	$-\sqrt{a}$	$-\sqrt{a}$	$-\sqrt{a}$	$-\sqrt{a}$
$\sqrt{b}$	$\sqrt{b}$	$-\sqrt{b}$	$\sqrt{b}$	$-\sqrt{b}$
$\sqrt{\omega}$	$x\sqrt{\omega}$	$y\tau(x)\sqrt{\omega}$	$xy\tau(y)\sqrt{\omega}$	$-y\tau(x)\sqrt{\omega}$
$\sqrt{a}\sqrt{b}$	$-\sqrt{a}\sqrt{b}$	$\sqrt{a}\sqrt{b}$	$-\sqrt{a}\sqrt{b}$	$\sqrt{a}\sqrt{b}$
$\sqrt{a}\sqrt{\omega}$	$-x\sqrt{a}\sqrt{\omega}$	$-y\tau(x)\sqrt{a}\sqrt{\omega}$	$-xy\tau(y)\sqrt{a}\sqrt{\omega}$	$y\tau(x)\sqrt{a}\sqrt{\omega}$
$\sqrt{b}\sqrt{\omega}$	$x\sqrt{b}\sqrt{\omega}$	$-y\tau(x)\sqrt{b}\sqrt{\omega}$	$xy\tau(y)\sqrt{b}\sqrt{\omega}$	$-y\tau(x)\sqrt{b}\sqrt{\omega}$
$\sqrt{a}\sqrt{b}\sqrt{\omega}$	$-x\sqrt{a}\sqrt{b}\sqrt{\omega}$	$y\tau(x)\sqrt{a}\sqrt{b}\sqrt{\omega}$	$-xy\tau(y)\sqrt{a}\sqrt{b}\sqrt{\omega}$	$y\tau(x)\sqrt{a}\sqrt{b}\sqrt{\omega}$

Como $\Sigma\Psi = \Psi^3\Sigma$, em conjunto as **Tabelas 6.3** e **6.4** implicam que:

$$x\sigma(y) = -y\tau(x)$$

Reciprocamente, dada uma V_4- extensão $M \supset k$ com $Gal(M|k) = \langle\sigma, \tau\rangle$ igualmente descrito como no início desse capítulo, suponhamos que existam $x, y, \omega \in \dot{M}$ satisfazendo

$$x\sigma(x) = y\tau(y) = -1 \quad \text{e} \quad x\sigma(y) = -y\tau(x)$$

e também

$$\frac{\sigma(\omega)}{\omega} = x^2 \quad \text{e} \quad \frac{\tau(\omega)}{\omega} = y^2,$$

Construindo $F = M(\sqrt{\omega})$, podemos estender os $k-$ automorfismos de M σ e τ, respectivamente, a $k-$ automorfismos de F, digamos denotados por Σ, Ψ, definindo-os conforme a tabela abaixo:

Σ	Ψ
$\sqrt{\omega} \mapsto x\sqrt{\omega}$	$\sqrt{\omega} \mapsto y\sqrt{\omega}$
$\alpha \mapsto -\alpha$	$\alpha \mapsto \alpha$
$\beta \mapsto \beta$	$\beta \mapsto -\beta$

Σ e Ψ são de fato $k-$ automorfismos de F, e de acordo com as relações e as tabelas acima, satisfazem as relações:

$$\Sigma^2 = \Psi^2, \quad \Sigma^2 = 1_F \quad \text{e} \quad \Sigma\Psi = \Psi^3\Sigma$$

E portanto $\langle\Sigma, \Psi\rangle \cong \mathbb{H}$, o grupo dos Quatérnios. Como $[F : k] = 8$ temos que $Gal(F|k) = \langle\Sigma, \Psi\rangle$, e logo a extensão $F \supset k$ é uma extensão quaterniônica.

6.1 Demonstração do Critério de Witt

Finalmente, podemos agora enunciar o *Critério de Witt*.

Teorema 6.1 (Critério de Witt). *Seja $M \supset k$ uma V_4- extensão, isto é, $M = k(\sqrt{a}, \sqrt{b})$ para algum par $a, b \in \dot{k}$. Então, existe uma extensão quaterniônica $F \supset k$ com M como subcorpo intermediário, $F \supset M \supset k$, se, e somente se, as formas quadráticas $aX^2 + bY^2 + abZ^2$ e $U^2 + V^2 + W^2$ são isométricas sobre k.*

Demonstração.

Prova da condição necessária:

Suponhamos que $F \supset k$ é uma extensão quaterniônica e $M \subset k$. Logo, existem $x, y \in \dot{M}$ com:

$$x\sigma(x) = y\tau(y) = -1 \quad \text{e} \quad x\sigma(y) = -y\tau(x)$$

Agora, para cada $t \in M$, a aplicação $x \mapsto tx$ é uma $k-$ transformação linear do espaço M. Então, fixada uma $k-$base de M, podemos representa-la por uma matriz $A(t) \in M_{4\times4}(k)$. Na verdade a aplicação

$$\begin{array}{rccc} \varphi & : & M & \longrightarrow & M_{4\times4}(k) \\ & & t & \longmapsto & A(t) \end{array}$$

é um monomorfismo injetor, isto é, M é imerso como álgebra dentro da álgebra de matrizes 4×4 com coeficiente em k.

Com respeito a $k-$ base $\beta = \{1, \sqrt{a}, \sqrt{b}, \sqrt{a}\sqrt{b}\}$ de M temos

$$\sqrt{a} \mapsto \begin{pmatrix} 0 & a & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & a \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad \sqrt{b} \mapsto \begin{pmatrix} 0 & 0 & b & 0 \\ 0 & 0 & 0 & b \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Consideremos agora a representação matricial de $\sigma, \tau \in Gal(M|k)$ em relação a base β, denotados respectivamente por U e V:

$$U := [\sigma]_\beta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \qquad V := [\tau]_\beta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

É facil ver que $U^2 = V^2 = E$, onde E é a matriz identidade 4×4; $UV = VU$ além de $U\varphi(t) = \varphi(\sigma(t))U$ e $V\varphi(t) = \varphi(\tau(t))V$, para todo $t \in M$.

De agora em diante, os cálculos serão decorrentes da suposição da validade das relações:

$$x\sigma(x) = y\tau(y) = -1 \quad \text{e} \quad x\sigma(y) = -y\tau(x)$$

Definamos $U' := \varphi(x)U$ e $V' := \varphi(y)V$.

Consideremos as subálgebras de matrizes em $M_{4\times4}(k)$:

$$\mathcal{Q}_1 = k[U', V'] \qquad \text{e} \qquad \mathcal{Q}_2 = k[U'', V''],$$

onde

$$U'' = \varphi(\sqrt{a})V' \qquad \text{e} \qquad V'' = \varphi(\sqrt{b})U'$$

Note que $U'^2 = \varphi(x)U\varphi(x)U = \varphi(x\sigma(x))U^2 = -E$ e de forma análoga $V'^2 = -E$, onde E é a matriz identidade 4×4.

Vamos ver que $U'V' = -V'U'$. De fato multiplicando as matrizes temos:

$$\begin{aligned} U'V' &= \varphi(x)U\varphi(y)V = \varphi(x\sigma(y))UV = -\varphi(y\tau(x))VU = \\ &= \quad -\varphi(y)\varphi(\tau(x))VU = -\varphi(y)V\varphi(x)U = -V'U' \end{aligned}$$

Deste modo podemos definir um isomorfismo de $k-$ álgebra de modo que:

$$\mathcal{Q}_1 \cong (-1,-1)_k$$

E de forma inteiramente análoga podemos verificar que existe um isomorfismo entre:

$$\mathcal{Q}_2 \cong (-a,-b)_k$$

As contas abaixo indicam que os centralizadores de $\mathcal{Q}_1$ e $\mathcal{Q}_2$ satisfazem:

$$C_{M_{4\times4}}(\mathcal{Q}_1) \supset \mathcal{Q}_2 \qquad \text{e} \qquad C_{M_{4\times4}}(\mathcal{Q}_2) \supset \mathcal{Q}_1$$

De fato:

$$\begin{aligned} U'U'' &= \varphi(x)U\varphi(\sqrt{a})\varphi(y)V = \varphi(x)\varphi(\sigma(\sqrt{a}))U\varphi(y)V = \\ &= \varphi(-x\sqrt{a}\sigma(y))VU = \varphi(y\sqrt{a}\tau(x))VU = \\ &= \varphi(y\sqrt{a})\varphi(\tau(x))VU = \varphi(\sqrt{a})\varphi(y)V\varphi(x)U \\ &= U''U'. \end{aligned}$$

$$\begin{aligned} U'V'' &= \varphi(x)U\varphi(\sqrt{b})\varphi(x)U = \varphi(x)\varphi(\sigma(\sqrt{b}))U\varphi(x)U = \\ &= \varphi(\sqrt{b})\varphi(x)U\varphi(x)U = \\ &= V''U'. \end{aligned}$$

$$\begin{aligned}U''V' &= \varphi(\sqrt{b})\varphi(x)U\varphi(y)V = \varphi(\sqrt{b})\varphi(x)\varphi(\sigma(y))UV = \\ &= \varphi(\sqrt{b}x\sigma(y))VU = \varphi(-y\sqrt{b}\tau(x))VU = \\ &= \varphi(y\tau(\sqrt{b}x))VU = \varphi(y)V\varphi(\sqrt{b})\varphi(x)U \\ &= V'U''.\end{aligned}$$

$$\begin{aligned}V''V' &= \varphi(\sqrt{b})\varphi(x)U\varphi(y)V = \varphi(\sqrt{b})\varphi(x)\varphi(\sigma(y))UV = \\ &= \varphi(\sqrt{b}x\sigma(y))UV = \varphi(-\sqrt{b}y\tau(x))UV \\ &\varphi(y)\varphi(\tau(\sqrt{b}x))VU = \varphi(y)V\varphi(\sqrt{b})\varphi(x)U \\ &= V'V''.\end{aligned}$$

Mas o ítem 2 do **Teorema do Duplo Centralizador** implica que a $k-$ dimensão de $C_{M_{4\times4}}(\mathcal{Q}_i)$, para $i = 1, 2,$ é igual a 4. E portanto

$$C_{M_{4\times4}}(\mathcal{Q}_1) = \mathcal{Q}_2 \qquad \text{e} \qquad C_{M_{4\times4}}(\mathcal{Q}_2) = \mathcal{Q}_1$$

Agora é a vez do Teorema do Duplo Centralizador, que no item 3 nos dirá que

$$\mathcal{Q}_1 = \mathcal{Q}_2$$

Ora, então concluimos que $(-1,-1)_k \cong (-a,-b)_k$. Logo, das equivalências do **Teorema 5.2**, temos o nosso resultado demonstrado:

$$\langle 1,1,1\rangle \cong \langle a,b,ab\rangle$$

Prova da suficiência:

Suponhamos que

$$aX^2 + bY^2 + abZ^2 \quad \overset{k}{\sim} \quad U^2 + V^2 + W^2$$

Portando existe uma matriz 3×3, $P = \begin{pmatrix} p_{11} & p_{12} & p_{13} \\ p_{21} & p_{22} & p_{23} \\ p_{31} & p_{32} & p_{33} \end{pmatrix} \in M_{3\times3}(k)$ tal que:

$$P^tAP = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{onde} \quad A = \begin{pmatrix} a & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & ab \end{pmatrix}$$

Decorrente desta equação matricial temos as relações:

$$\begin{cases} ap_{11}{}^2 + bp_{21}{}^2 + abp_{31}{}^2 = 1 \\ ap_{12}{}^2 + bp_{22}{}^2 + abp_{33}{}^2 = 1 \\ ap_{13}{}^2 + bp_{23}{}^2 + abp_{33}{}^2 = 1 \end{cases}$$

Das diagonais das equações $P^{-1} = P^tA$ e $PP^t = A^{-1}$ temos:

$$\begin{cases} p_{11} = b(p_{22}p_{33} - p_{23}p_{32}) \\ p_{22} = a(p_{11}p_{33} - p_{13}p_{31}) \\ p_{33} = p_{11}p_{22} - p_{12}p_{21} \end{cases} \quad \text{e} \quad \begin{cases} p_{11}{}^2 + p_{12}{}^2 + p_{13}{}^2 = \frac{1}{a} \\ p_{21}{}^2 + p_{22}{}^2 + p_{23}{}^2 = \frac{1}{b} \\ p_{31}{}^2 + p_{32}{}^2 + p_{33}{}^2 = \frac{1}{ab} \end{cases}$$

Seja então $\omega := 1 + p_{11}\sqrt{a} + p_{22}\sqrt{b} + p_{33}\sqrt{a}\sqrt{b}$ e

$$x = \sqrt{a}\frac{p_{31}\sqrt{b} - p_{13}}{\omega}, \quad y = \sqrt{b}\frac{p_{32}\sqrt{a} - p_{23}}{\omega}$$

Agora

$$\begin{aligned} \omega\sigma(\omega) &= (1 + p_{22}\sqrt{b})^2 - a(p_{11} + p_{33}\sqrt{b})^2 \\ &= (1 + bp_{22}{}^2 - ap_{11}{}^2 - abp_{33}{}^2) + 2(p_{22} - ap_{11}p_{33})\sqrt{b} \\ &= (bp_{21}{}^2 + abp_{31}{}^2 + bp_{22} - abp_{33}{}^2) - 2ap_{13}p_{31}\sqrt{b} \\ &= (1 - bp_{23}{}^2 + abp_{31}{}^2 - abp_{33}{}^2) - 2ap_{13}p_{31}\sqrt{b} \\ &= a(p_{13} - p_{31}\sqrt{b})^2 = x^2\omega^2 \end{aligned}$$

E analogamente

$$\omega\tau(\omega) = y^2\omega^2$$

Então segue que

$$\frac{\sigma(\omega)}{\omega} = x^2 \qquad \text{e} \qquad \frac{\tau(\omega)}{\omega} = y^2$$

Além disso

$$x\sigma(x) = y\tau(y) = -1$$

e

$$\begin{aligned}
\frac{x\sigma(y)}{y\tau(x)} &= \frac{\sqrt{a}(p_{31} - \sqrt{b} - p_{13})\omega^{-1}\sqrt{b}(-p_{32}\sqrt{a} - p_{23})\sigma(\omega^{-1})}{\sqrt{b}(p_{32} - \sqrt{a} - p_{23})\omega^{-1}\sqrt{a}(-p_{31}\sqrt{b} - p_{13})\tau(\omega^{-1})} \\
&= \frac{b(p_{32}\sqrt{a} + p_{23})(p_{32}\sqrt{a} - p_{23})}{a(p_{31}\sqrt{b} + p_{13})(p_{31}\sqrt{b} - p_{13})} \\
&= \frac{ab{p_{32}}^2 - b{p_{23}}^2}{ab{p_{31}}^2 - a{p_{13}}^2} \\
&= \frac{(1 - ab{p_{13}}^2 - ab{p_{33}}^2) - (1 - a{p_{13}}^2 - ab{p_{33}}^2)}{ab{p_{31}}^2 - a{p_{13}}^2} = -1.
\end{aligned}$$

E portanto $M(\sqrt{\omega}) \supset k$ é uma extensão quaterniônica, conforme queríamos. □

Podemos fazer uma formulação equivalente ao critério de Witt utilizando de relações entre classes de álgebras de Quatérnios no grupo de Brauer do corpo. Pois de acordo com **Teorema 5.4** temos que:

$$\langle 1, 1, 1\rangle \cong \langle a, b, ab\rangle \iff (a, b)_k(a, a)_k(b, b)_k = 1 \in Br(k)$$

De fato:
$(a,b)_k(a,a)_k(b,b)_k = (a,b)_k(a,-1)_k(b,-1)_k = (a,-b)_k(b,-1)_k =$
$= (a,-b)_k(b,-1)_k(-1,-1)_k(-1,-1)_k = (a,-b)_k(-b,-1)_k(-1,-1)_k =$
$= (-a,-b)_k(-1,-1)_k \quad$ e $\quad (-a,-b)_k(-1,-1)_k = 1 \in Br(k) \iff$
$\iff (-a,-b)_k = (-1,-1)_k \iff \langle 1,1,1\rangle \cong \langle a,b,ab\rangle$

Como vimos no **Capítulo 3** , a condição sobre soma de três quadrados é de fato necessária no caso do problema da imersão em extensões quaterniônicas, conforme enuciaremos no proximo resultado, uma decorrência imediata do teorema precedente.

Corolário 6.1. *Seja $a \in \dot{k} - k^2$. Se $k(\sqrt{a})$ pode ser imersa em uma extensão quaterniônica de k, então a é soma de três quadrados em k.*

Definição 6.1. O *level* de k, denotado por $s(k)$, é o menor número natural n para o qual -1 pode ser escrito como soma de n quadrados em k.

Corolário 6.2. *Seja k um corpo onde $-1 \notin k^2$ e $|\dot{k}/\dot{k}^2| > 2$. São equivalentes:*

1. *O level, $s(k)$, de k é dois.*
2. *Toda extensão quadratica de k pode ser imersa em uma extensão quaterniônica.*
3. *$k(\sqrt{-1})$ pode ser imersa numa extensão quaterniônica.*

Demonstração. $(1) \Rightarrow (2)$. Seja $a \notin F^2$. Pelo **Teorema** 5.3 , (1) implica que $\langle 1,1\rangle \cong \langle -1,-1\rangle$. Pelo mesmo Teorema 5.3 $\langle -1,1\rangle \cong \langle a,-a\rangle$. Então

$$\langle 1,1,1\rangle \cong \langle -1,-1,1\rangle \cong \langle -1,a,-a\rangle$$

Portanto pelo critério de Witt $k(\sqrt{-1}, \sqrt{a})$ está contida numa extensão quaterniônica.

$(3) \Rightarrow (1)$ Pelo critério de Witt , existe $a \in \dot{k}$ tal que $\langle 1,1,1\rangle \cong \langle -1, a, -a\rangle$. Mas esta última forma é isotrópica e portanto, $\langle 1,1,1\rangle$ é isotrópica, e como $-1 \notin k^2$, temos então que $s(k) = 2$. □

Já vimos que uma extensão quadrática dos racionais $\mathbb{Q}(\sqrt{d}),\ d \notin \mathbb{Q}^2$, pode ser imersa numa extensão quaterniônica se, e somente se, d é soma de três quadrados. O resultado a seguir, num contexto mais geral, trata dessa caracterização introduzindo a noção já clássica de elementos rígidos de um corpo.

Definição 6.2. Um elemento $a \in \dot{k}$ é *rígido* se $a \notin k^2 \cup ak^2$ e $D_k(\langle 1, a\rangle) = F^2 \cup aF^2$.

As formas binárias $\langle 1, a\rangle$ e $\langle b, ab\rangle$, onde $a, b \in \dot{k}$, são isométricas se $D_k(\langle 1, a\rangle) \cap D_k(\langle b, ab\rangle) \neq \emptyset$. Portanto a não é rígido se, e só se, existe $b \notin k^2 \cup ak^2$ tal que $\langle 1, a\rangle \cong \langle b, ab\rangle$.

Corolário 6.3. *Seja $a \in D_k(\langle 1,1\rangle)$, $a \notin k^2$. As seguintes condições são equivalentes:*

1. *a não é rígido.*
2. *$k(\sqrt{a})$ pode ser imerso numa extensão quaterniônica.*

Demonstração. $(1) \Rightarrow (2)$. Se a não é rígido, então existe um $b \notin k^2 \cup ak^2$ tal que $\langle 1, a\rangle \cong \langle b, ab\rangle$. Então $\langle 1,1,1\rangle \cong \langle 1, a, a\rangle \cong \langle b, ab, a\rangle$ portanto, pelo critério de Witt vale (2)

$(2) \Rightarrow (1)$ Pelo **Capítulo** 2 e o critério de Witt, existe $b \notin k^2 \cup ak^2$ tal que $\langle a, b, ab\rangle \cong \langle 1,1,1\rangle \cong \langle a, a, 1\rangle$ e do Teorema do Cancelamento de Witt $\langle b, ab\rangle \cong \langle 1, a\rangle$. Portanto a não é rígido. □

Referências Bibliográficas

[1] J. E. Carter, *Characterisation of Galois Extensions of Prime Cubed Degree*. Bull. Austral. Math. Soc. Vol. 55 1997 [99-112].

[2] R. A. Dean, *A Rational Polynomial Whose Group is the Quaternions*. American Math. Monthly, 88 1981 [42-45].

[3] B. Felzenszwalb, *Álgebras de dimensõo finitas* . 12^o Colóquio Brasileiro de Matemática, RJ : IMPA, 1979.

[4] G. Fujisaki, *An Elementary Construction of Galois Quaternion Extension*. Proc. Japan Acad., Vol. 66, Ser. A 1990 [80-83].

[5] K. Ireland, M. Rosen, *A Classical Introductin to Modern Number Theory*. Springer-Verlag, New York, 1982.

[6] C. U. Jensen, A. Ledet, N. Yui, *Generic Polynomials Constructive Aspects of Inverse Galois Problem*. Mathematical Sciences Research Institute. Cambridge University Press, 2002.

[7] T.Y. Lam, *The Algebraic Theory of Quadratics Forms*. Mathematicals Lectures Notes Series, The Benjamin/Cummings Publishing Company, Inc. Reading, Massachusetts, 1973.

[8] S. Lang, *Algebra*. Addison-Wesley, Reading, Massachusetts, 1965.

[9] L. H. J. Monteiro, *Elementos de Álgebra*. Rio de Janeiro, Ao Livro Técnico, 1971.

[10] W. Scharlau, *Quadratic and hermitian forms*. Grundlehren mat. Wiss. vol. 270, Springer-Verlag, Berlin, 1985.

[11] J. P. Serre, *A Course in Arithmetics*. Springer-Verlag, New York, 1973.

[12] R. Ware, *A note on the Quaternion Group as Galois Group*. Proceeddings of the American Mathematical Society, Vol. 108, Number 3, March 1990 [621-625].

[13] E. Witt, *Konstruktion von galoisschen Korpern der Charakteristik p zu vorgegebenerGruppe der Ordnung* p^f, Journal Reine Angew. Math. 174 (1936), [237-245].