UNIVERSIDADE ESTADUAL DE MARINGÁ
CENTRO DE CIÊNCIAS EXATAS
DEPARTAMENTO DE MATEMÁTICA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA
(Mestrado)

GERMANO VIER ALVES

TRANSFER DE SCHARLAU PARA UMA EXTENSÃO BIQUADRÁTICA

Maringá - PR
2018

GERMANO VIER ALVES

TRANSFER DE SCHARLAU PARA UMA EXTENSÃO BIQUADRÁTICA

Dissertação submetida ao corpo docente do Programa de Pós-Graduação em Matemática da Universidade Estadual de Maringá - UEM-PR, como parte dos requisitos necessários à obtenção do grau de Mestre.

Orientador: Prof. Dr. Rosali Brusamarelo.

Maringá - PR
2018

Dedico esse trabalho aos meus pais.

Agradecimentos

Agradeço primeiramente a DEUS, por me dar força, saúde, paciência e felicidades no durante o Mestrado.

A minha família que sempre me apoiou tanto em bons momentos quantos nos ruins, mandando para mim palavras de conforto para essa caminhada.

Sou grato a minha orientadora professora Dra. Rosali que sempre me ajudou nos nuances da dissertação, pelas diversas horas dedicadas a orientações e seminários, pela sua paciência, dedicação, disposição e destreza para contribuir com sua experiência ao longo da minha formação. Também agradeço ao professor Dr. Sivatski que mesmo estando longe sempre foi paciente e me auxiliou na dissertação.

Aos colegas que estão juntos nessa caminhada chamada Mestrado, os agradeço muito por todos esses anos que passaram e toda a bagagem de conhecimento que construímos. Ao café das tardes e as discussões calorosas a respeito da Matemática.

A CAPES pelo apoio financeiro.

Resumo

Seja F um corpo de característica diferente de 2 e $a, b \in \dot{F}$, tais que $a, b, ab \neq \dot{F}^2$. Neste trabalho iremos descrever o núcleo da transfer $s_* : W(F(\sqrt{a}, \sqrt{b})) \longrightarrow W(F)$ correspondente ao F-funcional linear $s : F(\sqrt{a}, \sqrt{b}) \longrightarrow F$ determinado pelas igualdades $s(1) = s(\sqrt{a}) = s(\sqrt{b}) = 0$ e $s(\sqrt{ab}) = 1$.

Palavras-chave: formas quadráticas sobre corpos, extensões biquadráticas, transfer de Scharlau, formas de Pfister.

Abstract

Let F be a field of characteristic different from 2 and $a, b \in \dot{F}$, such that $a, b, ab \neq \dot{F}^2$. In this work we describe the kernel of the Scharlau transfer $s_* : W(F(\sqrt{a}, \sqrt{b})) \longrightarrow W(F)$ corresponding to the F-linear map $s : F(\sqrt{a}, \sqrt{b}) \longrightarrow F$ determined by the egualities $s(1) = s(\sqrt{a}) = s(\sqrt{b}) = 0$ e $s(\sqrt{ab}) = 1$.

Key words: quadratic forms over fields, biquadratic extensions, Scharlau transfer, Pfister forms.

Sumário

Introdução

Seja F um corpo de característica diferente de 2 e $K \supset F$ uma extensão de corpos finita. Dado um F-espaço quadrático (V, B, q) podemos construir um K-espaço quadrático (V_K, B_K, q_K), onde V_K é obtido de $K \otimes_F V$, e B_K é dado pela única aplicação bilinear simétrica em V_K que satisfaz

$$B_K(k \otimes v, k' \otimes v') = kk' \cdot B(v, v'), \text{ com } k, k' \in K \text{ e } v, v' \in V.$$

Neste trabalho estamos interessados em homomorfismos entre os anéis de Witt $W(F)$ e $W(K)$, mais precisamente, iremos investigar o homomorfismo conhecido como "transfer"de Scharlau. Nosso foco maior será em extensões quadráticas e biquadráticas.

Começamos, no Capítulo 1, introduzindo a teoria de formas quadráticas sobre corpos de característica diferente de 2. Enunciamos e demonstramos resultados básicos e importantes para o desenvolvimento da teoria, baseados no livro clássico de T.Y.Lam [Lam].

No Capítulo 2, definimos os anéis de Witt-Grothendieck $\widehat{W}(F)$ e de Witt $W(F)$, analisamos sua estrutura e definimos alguns invariantes dos mesmos. No final do capítulo damos condições para que estes anéis sejam Noetherianos.

O enfoque do Capítulo 3 são as álgebras de quatérnios. Inicialmente fazemos a contrução destas álgebras e depois relacionamos as mesmas com os espaços quadráticos. Das propriedades desta relação obtemos um importante teorema de classificação das álgebras de quatérnios. Ao final obtemos também uma classificação das formas binárias.

No Capítulo 4 começamos a trabalhar com extensões de corpos. Definimos o transfer de Scharlau e outros homorfismos importantes entre os anéis de Witt e os relacionamos através do resultado conhecido como "Reciprocidade de Frobenius". Analisamos o comportamento do transfer de Scharlau em extensões simples (onde provamos o Teorema de Springer), extensões quadráticas e extensões transcendentes (visando obter o Teorema de Cassels-Pfister). Finalizamos o capítulo definindo as formas de Pfister, que nos auxiliarão no estudo de alguns ideais do anel de Witt.

Por último, no Capítulo 5, vamos trabalhar com extensões biquadráticas e vamos descrever o núcleo da transfer de Scharlau para estas extensões, baseados no preprint de A.S. Sivatski [Siv]. No final do capítulo apresentamos um exemplo que dá uma resposta negativa a primeira questão em aberto deixada em [Siv].

Capítulo 1

Formas quadráticas sobre corpos

Neste capítulo introduziremos algumas noções básicas da teoria de formas quadráticas sobre corpos, ou seja, definições como o espaço quadrático e plano hiperbólico estão inclusas, bem como teoremas importantes de Witt para formas quadráticas. Nos baseamos no livro de T.Y. Lam [Lam] Ressaltamos que um corpo sempre será de característica diferente de dois, a menos que seja dito o contrário.

1.1 Formas Quadráticas e Espaço Quadrático

Definição 1.1. Uma *forma quadrática* sobre um corpo F é um polinômio f em n variáveis sobre F que é homogêneo de grau dois, isto é,

$$f(x_1, \ldots, x_n) = \sum_{i,j}^{n} a_{ij} x_i x_j \in F[x_1, \ldots, x_n] = F[X].$$

Exemplo 1.2. (i) Em $\mathbb{R}[x, y]$ o polinômio $f(x, y) = x^2 + y^2 = x^2 + 0xy + 0yx + y^2$ é uma forma quadrática sobre $\mathbb{R}$.
(ii) Em $\mathbb{R}[x_1, \ldots, x_5]$ o polinômio $f(x_1, \ldots, x_5) = x_1^2 + x_2^2 + 3x_3^2 + x_4x_5 + x_1x_5$ é uma forma quadrática sobre $\mathbb{R}$.
(iii) Se $f \in \mathbb{R}[x]$ tal que $f(x) = x^2 + x + 3$, então f não é uma forma quadrática, pois o polinômio $x^2 + x + 3$ não é homogêneo.

Os coeficientes a_{ij} de uma forma quadrática podem ser dispostos em uma matriz $n \times n$, logo a cada forma quadrática podemos associar uma matriz $[a_{ij}]_{n\times n}$, que denotaremos apenas por $[a_{ij}]_n$.

Proposição 1.3. *Seja $f(X) \in F[X] = F[x_1, \ldots, x_n]$ uma forma quadrática sobre F. Então podemos associar a $f(X)$ uma única matriz simétrica.*

Demonstração: *Existência*: Seja $f(X) = \sum_{i,j}^{n} a_{ij}x_ix_j$ uma forma quadrática sobre F. Assim para cada par (i, j) temos que

$$a_{ij}x_ix_j + a_{ji}x_jx_i = (a_{ij} + a_{ji})x_ix_j, \tag{1.1}$$

pois $x_ix_j = x_jx_i$. Podemos então reescrever a equação 1.1 da forma

$$(\frac{a_{ij} + a_{ji}}{2})x_ix_j + (\frac{a_{ij} + a_{ji}}{2})x_jx_i.$$

Assim $f(X)$ pode ser reescrita da forma

$$f(X) = \sum_{i,j}^{n} \frac{1}{2}(a_{ij} + a_{ji})x_i x_j = \sum_{i,j}^{n} a'_{ij} x_i x_j,$$

onde $a'_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$. Claramente $[a'_{ij}]_n$ é simétrica.
Unicidade: Seja $K = [k_{ij}]_n$ uma outra matriz simétrica associada a $f(X)$. Assim

$$f(X) = \sum_{i,j}^{n} k_{ij} x_i x_j = \sum_{i,j}^{n} a'_{ij} x_i x_j.$$

Como $x_i x_j = x_j x_i$, devemos ter

$$k_{ij} + k_{ji} = a'_{ij} + a'_{ji},$$

para todo $i, j = 1, \ldots, n$. Como K e $[a'_{ij}]_n$ são simétricas, $2k_{ij} = 2a'_{ij}$ e assim $k_{ij} = a'_{ij}$. Logo $K = [a'_{ij}]_n$. Portanto a matriz simétrica $[a'_{ij}]$ é única. □

Notação 1.4. Denotaremos a matriz simétrica associada a f por M_f.

Exemplo 1.5. Seja o corpo $F = \mathbb{R}$ e a forma quadrática $f(x, y, z) = x^2 + 7xy + 2y^2 + 4yx + yz + 3zy + 5z^2$. Da definição de $f(x, y, z)$, temos que

$$[a_{ij}]_3 = \begin{bmatrix} 1 & 7 & 0 \\ 4 & 2 & 1 \\ 0 & 3 & 5 \end{bmatrix}.$$

Usando o processo da proposição anterior, temos que

$$M_f = \begin{bmatrix} 1 & \frac{11}{2} & 0 \\ \frac{11}{2} & 2 & 2 \\ 0 & 2 & 5 \end{bmatrix}.$$

Proposição 1.6. *Seja $f(X) \in F[x_1, \ldots, x_n]$ uma forma quadrática e M_f sua matriz simétrica. Então $f(X) = X^t M_f X$.*

Demonstração: Seja $A = X^t M_f X$, onde $X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$. Assim,

$$A = \begin{bmatrix} x_1 & \ldots & x_n \end{bmatrix} \begin{bmatrix} a_{11} & \ldots & \frac{a_{1n}+a_{n1}}{2} \\ \vdots & \ddots & \vdots \\ \frac{a_{n1}+a_{1n}}{2} & \ldots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

Portanto,

$$A = (a_{11}x_1^2 + \frac{a_{12} + a_{21}}{2} x_1 x_2 + \cdots + a_{nn}x_n^2) = f(X).$$

□

Definição 1.7. Sejam f e g formas quadráticas sobre F. Dizemos que f *é equivalente a* g se existir uma matriz inversível $C \in GL_n(F)$ tal que $f(X) = g(CX)$. Neste caso denotaremos $f \cong g$.

Observe que $f(X) = g(CX) = (CX)^t M_g(CX) = X^t(C^t M_g C)X$, logo $M_f = C^t M_g C$. Concluímos que as matrizes de duas formas quadráticas equivalentes são congruentes.

Exemplo 1.8. Sejam F^2 o F-espaço vetorial formado pelos pares ordenados em F e $X = (x_1, x_2) \in F^2$. Sejam $f, g \in F[x_1, x_2]$ tais que $f(X) = g(CX)$, onde $g(X) = x_1x_2$, e C é a matriz da substituição linear que transformam $x_1 \to x_1 + x_2$ e $x_2 \to x_1 - x_2$. Então a matriz de C será $\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$, que é inversível. Logo $f \cong g$. Mais ainda

$$f(X) = g(CX) = g(x_1 + x_2, x_1 - x_2) = (x_1 + x_2)(x_1 - x_2) = x_1^2 - x_2^2.$$

Portanto $f(X) = x_1^2 - x_2^2$.

Vamos agora definir os espaços quadráticos utilizando o conceito de forma bilinear visto em Álgebra Linear.

Definição 1.9. Sejam V um F-espaço vetorial de dimensão finita e $B : V \times V \longrightarrow F$ uma forma bilinear simétrica. Podemos definir o par (V, B) como *espaço quadrático*, pois iremos associar a ele uma função quadrática $q = q_B : V \longrightarrow F$ dada por $q(x) = B(x, x)$, para todo $x \in V$.

Observação 1.10. A função q é chamada de quadrática pois

$$q(ax) = B(ax, ax) = a^2B(x, x) = a^2q(x), \text{ para todo } a \in F.$$

Temos ainda que

$$q(x+y)-q(x)-q(y) = B(x+y, x+y)-B(x, x)-B(y, y) = B(x, y)+B(y, x) = 2B(x, y),$$

ou seja, q admite a polarização

$$B(x, y) = \frac{q(x + y) - q(x) - q(y)}{2}.$$

Assim, q determina B e B determina q, em outras palavras o par (V, q) também representa o espaço quadrático (V, B).

Notação 1.11. Quando for conveniente, denotaremos por (V, B, q) o espaço quadrático (V, B) em conjunto com a função quadrática $q = q_B$.

Exemplo 1.12. Seja $V = \mathbb{R}^3$ o $\mathbb{R}$-espaço vetorial das triplas ordenadas. Seja $q(x_1, x_2, x_3) = 8x_1x_3 - 10x_2^2$ uma função quadrática. Podemos polarizar q para encontrar sua forma bilinear B_q associada. Assim, para $x = (x_1, x_2, x_3), y = (y_1, y_2, y_3) \in \mathbb{R}^3$, temos que

$$\begin{aligned} B_q(x, y) &= \tfrac{q(x+y)-q(x)-q(y)}{2} \\ &= \tfrac{8(x_1+y_1)(x_3+y_3)-10(x_2+y_2)^2-8x_1x_3-10x_2^2-8y_1y_3-10y_2^2}{2} \\ &= \tfrac{8x_1y_3+8x_3y_1-20x_2y_2}{2} = 4x_1y_3 - 10x_2y_2 + 4x_3y_1. \end{aligned}$$

Reciprocamente, se considerarmos $B : \mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}$ a forma bilinear simétrica dada por $B((x_1, x_2, x_3)(y_1, y_2, y_3)) := 4x_1y_3 - 10x_2y_2 + 4x_3y_1$, então q_B obtida por despolarização de B é uma função quadrática. Para obter q_B considere $x = (x_1, x_2, x_3) \in \mathbb{R}^3$, logo

$$q_B(x) = B(x, x) = 4x_1x_3 - 10x_2x_2 + 4x_3x_1 = 8x_1x_3 - 10x_2^2,$$

que claramente é a função quadrática.

Observação 1.13. Seja (V, B, q) um espaço quadrático, se colocarmos coordenadas em V, isto é, se escolhermos uma base $(e_1, \ldots, e_n)$ de V, então (V, B, q) está associado a uma forma quadrática

$$f = \sum_{i,j}^{n} B(e_i, e_j)x_ix_j, \quad \text{com } M_f = [B(e_i, e_j)]_n.$$

Proposição 1.14. *Sejam (V, B) um espaço quadrático de dimensão n e $E = (e_1, \ldots, e_n)$ uma base fixada de V tal que f é a forma quadrática associada à (V, B) nessa base. Seja $E' = (e'_1, \ldots, e'_n)$ outra base de V tal que f' é a forma quadrática associada a (V, B) na base E'. Então $f \cong f'$.*

Demonstração: De fato, como E, E' são bases de V, então $e'_i = \sum_{k=1}^{n} c_{k,i}e_k$ com $i = 1, \ldots, n$. Dados $1 \leq i, j \leq n$, temos que

$$(M_{f'})_{ij} = B(e'_i, e'_j) = B(\sum_{k=1}^{n} c_{ki}e_k, \sum_{l=1}^{n} c_{lj}e_l).$$

Como B é bilinear, então

$$(M_{f'})_{ij} = \sum_{k,l=1}^{n} c_{ki}B(e_k, e_l)c_{l,j} = (C^t M_f C)_{ij},$$

onde $C = [c_{kl}]_n$. Assim $M_{f'} = C^t M_f C$. Como C é a matriz de mudança de base de E à E', então C é invertível. Portanto $f \cong f'$. □

Observação 1.15. Pelo que foi provado na proposição anterior temos que o espaço quadrático (V, B, q) determina unicamente uma classe de equivalência de formas quadráticas, que será denotada por (f_B).

Definição 1.16. Sejam $(V, B), (V', B')$ espaços quadráticos, dizemos que eles são *isométricos* se existir um isomorfismo linear $\tau : V \longrightarrow V'$ tal que

$$B'(\tau(x), \tau(y)) = B(x, y), \text{ para todo } x, y \in V.$$

Neste caso, denotaremos por $(V, B) \cong (V', B')$ se $(V, B), (V', B')$ forem isométricos.

Proposição 1.17. *Sejam $(V, B), (V', B')$ espaços quadráticos. Então*

$$(V, B) \cong (V', B') \iff (f_B) = (f_{B'}).$$

Demonstração: Suponha que $(V, B) \cong (V', B')$. Pela definição anterior, temos que existe um isomorfismo linear $\tau : V \longrightarrow V'$ tal que $B'(\tau(x), \tau(y)) = B(x, y)$, para todo $x, y \in V$. Sejam $q_B, q_{B'}$ as funções quadráticas associadas a B e B', respectivamente. Assim, $q_B(x) = B(x, x)$, $q_{B'}(x') = B'(x', x')$ e para $x \in V$ temos

$$q_{B'}(\tau(x)) = B'(\tau(x), \tau(x)) = B(x, x) = q_B(x).$$

Como $q_B, q_{B'}$ são funções quadráticas e τ é um isomorfismo, segue que $q_B \cong q_{B'}$. Logo $(f_B) = (f_{B'})$. A recíproca é análoga. □

Iremos construir a ideia de regularidade para espaços quadráticos, algo muito útil no decorrer dessa teoria. Para isso necessitamos do seguinte teorema.

Teorema 1.18. *Sejam (V, B) um espaço quadrático, V^* o espaço dual de V e M a matriz simétrica associada a uma das formas quadráticas da classe de equivalência (f_B). Então as seguintes afirmações são equivalentes:*
(1) M é uma matriz não singular (inversível);
(2) A função

$$\begin{array}{rccccccc} \tau: & V & \longrightarrow & V^* & & & & \\ & x & \longrightarrow & B(\_, x): & V & \longrightarrow & F \\ & & & & y & \longrightarrow & B(y, x) \end{array}$$

é um isomorfismo;
(3) Se para $x \in V$, $B(x, y) = 0$ para todo $y \in V$, então $x = 0$.

Demonstração: Primeiramente, note que τ está bem definida, pois $B : V \times V \longrightarrow F$ é uma aplicação bilinear e desse modo, $B(\_, x) = B|_{V \times \{x\}}$, com $x \in V$, é um funcional linear.
(1)⇒(2) Afirmamos que τ é linear. De fato, sejam $x, y \in V$ e $\alpha \in F$, assim $\tau(x + \alpha y) = B(\_, x + \alpha y)$. Como B é uma forma bilinear, temos que $B(k, x + \alpha y) = B(k, x) + \alpha B(k, y)$, para $k \in V$. Pela escolha arbitrária de k, segue que

$$\tau(x + \alpha y) = B(\_, x + \alpha y) = B(\_, x) + \alpha B(\_, y) = \tau(x) + \alpha\tau(y).$$

Logo τ é linear. Pelo fato que $\dim V = \dim V^* < \infty$, basta provarmos que τ é injetora. Sejam $x, y \in V$ tais que $\tau(x) = \tau(y)$. Isso implica que $B(\_, x) = B(\_, y)$ e como $B(\_, x)$ é linear para todo $x \in V$, então

$$B(\_, x - y) = 0_{V^*}. \tag{1.2}$$

Seja f a forma quadrática associada a (V, B), logo $f \in (f_B)$ e sua matriz M_f é congruente a M. Como M é inversível, M_f é inversível. Por definição,

$$B(k, x - y) = k^t M_f (x - y), \qquad k \in V.$$

De (1.2), temos que

$$k^t M_f (x - y) = 0, \text{ para todo } k \in V. \tag{1.3}$$

Como M_f é inversível, fixando k, o sistema homogêneo (1.3) admite uma única solução, segue que $x - y = 0$, ou seja, $x = y$. Portanto τ é injetora, como queríamos demonstrar.

(2)⇒(3) Seja $x \in V$ tal que $B(x, y) = 0$, para todo $y \in V$. Como B é simétrica, então $B(y, x) = 0$, para todo $y \in V$. Assim $\tau(x) = B(\_, x) = 0_{V^*}$. Do fato que τ é isomorfismo, segue que $x = 0$.

(3)⇒(1) Para $x, y \in V$, temos $B(x, y) = x^t M y$. Se $x^t M y = 0$, para todo $y \in V$, então $x = 0 = x^t$ por hipótese. Assim, fixando y, temos que $x^t M y = 0$ admite solução única. Portanto M é inversível. □

Definição 1.19. Seja (V, B, q) um espaço quadrático. Dizemos que (V, B, q) é *regular* se alguma das afirmações do Teorema 1.18 for satisfeita.

Observação 1.20. Sejam (V, B, q) um espaço quadrático e $S \subseteq V$ subespaço vetorial. Então $(S, B|_{S\times S}, q|_{S\times S})$ é um espaço quadrático.

Definição 1.21. Sejam (V, B) um espaço quadrático e $S \subseteq V$ subespaço vetorial. O *complemento ortogonal* de S é definido por

$$S^{\perp} := \{x \in V \ ; \ B(x, s) = 0 \text{ para todo } s \in S\}.$$

O complemento ortogonal do espaço V será chamado de *radical* de (V, B) e denotado por $V^{\perp} := \text{rad}(V)$.

Corolário 1.22. *Seja (V, B) um espaço quadrático. Então, $\text{rad}(V) = \{0\}$ se, e somente se, (V, B) é regular.*

Demonstração: Seja $x \in V$ tal que $B(x, y) = 0$, para todo $y \in V$. Pela definição de complemento ortogonal, temos que $x \in \text{rad}(V)$. Como, por hipótese, $\text{rad}(V) = \{0\}$, então $x = 0$. Pelo Teorema 1.18 item (3), (V, B) é regular.
Reciprocamente, suponha que (V, B) é regular. Seja $x \in \text{rad}(V)$. Isso implica que $B(x, y) = 0$, para todo $y \in V$. Pelo Teorema 1.18, $x = 0$. Portanto $\text{rad}(V) = \{0\}$ □

Observação 1.23. Sejam (V, B) um espaço regular e $S \subseteq V$ subespaço. Então $(S, B|_{S\times S}, q|_{S\times S})$ não necessariamente é regular. Vamos elucidar essa afirmação com um exemplo.
Sejam $V = \mathbb{R}^4$ e $B : \mathbb{R}^4 \times \mathbb{R}^4 \longrightarrow \mathbb{R}$ tal que

$$B(x, y) = x^t M y = x^t \begin{pmatrix} 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 3 \\ 1 & 1 & 1 & 2 \\ 2 & 3 & 2 & 5 \end{pmatrix} y.$$

Como M é simétrica, então B é simétrica. Assim (V, B) é espaço quadrático. Note que M é inversível, pois $\det(M) = 1$. Pelo Teorema 1.18, (V, B) é regular. Seja

$$S = \{(x_1, x_2, 0, 0) \in \mathbb{R}^4 \ ; \ x_1, x_2 \in \mathbb{R}\}.$$

É fácil ver que S é subespaço de V. Por outro lado, tomando $x = (x_1, x_2, 0, 0)$ e $y = (y_1, y_2, 0, 0)$ em S temos que

$$B|_{S\times S}(x, y) = \begin{pmatrix} x_1 & x_2 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 & 2 \\ 0 & 0 & 1 & 3 \\ 1 & 1 & 1 & 2 \\ 2 & 3 & 2 & 5 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ 0 \\ 0 \end{pmatrix} = 0,$$

ou seja, $B|_{S\times S} = 0_{S^*}$. Logo $\text{rad}(S) \neq 0$. Portanto $(S, B|_{S\times S}, q|_{S\times S})$ não é regular.

Teorema 1.24. *Sejam (V, B) um espaço quadrático regular, $S \subseteq V$ subespaço vetorial e $S^{\perp}$ o complemento ortogonal de S. Então:*
(1) $\dim(V) = \dim(S) + \dim(S^{\perp})$;
(2) $(S^{\perp})^{\perp} = S$.

Demonstração: (1) Suponha que (V, B, q) é regular. Pelo Teorema 1.18 item (2), temos que $\tau : V \longrightarrow V^*$, dada por $\tau(x) = B(\_, x)$, é um isomorfismo. Vamos mostrar inicialmente que $\tau(S^\perp) = S^0$, onde $S^0 = \{f \in V^* : \ f(s) = 0 \text{ para todo } s \in S\}$. De fato, seja $f \in \tau(S^\perp)$, então existe $x \in S^\perp$ tal que $\tau(x) = f$. Assim, $f = B(\_, x)$. Como $x \in S^\perp$, então $B(s, x) = 0$, para todo $s \in S$. Logo $f \in S^0$, ou seja, $\tau(S^\perp) \subseteq S^0$.

Reciprocamente, seja $g \in S^0$. Assim $g(s) = 0$, para todo $s \in S$. Como $g \in V^*$ e τ é isomorfismo, então existe um único $x \in V$ tal que $g = \tau(x) = B(\_, x)$. Como $g \in S^0$, $B(s, x) = g(s) = 0$, para todo $s \in S$. Assim $x \in S^\perp$, ou seja, $g \in \tau(S^\perp)$. Logo $S^0 \subseteq \tau(S^\perp)$ e portanto $\tau(S^\perp) = S^0$. Sabemos da Álgebra Linear que $\dim(V) = \dim(S) + \dim(S^0)$. Assim

$$\dim(V) = \dim(S) + \dim(\tau(S^\perp)).$$

Como τ é isomorfismo, $\dim(S^\perp) = \dim(\tau(S^\perp))$ e obtemos

$$\dim(V) = \dim(S) + \dim(S^\perp).$$

(2) Pelo que provamos em (1), temos que

$$\dim(S^\perp) = \dim(V) - \dim(S). \tag{1.4}$$

Aplicando $S^\perp$ na Equação (1.4), obtemos

$$\dim((S^\perp)^\perp) = \dim(V) - \dim(S^\perp). \tag{1.5}$$

Substituindo (1.4) em (1.5), obtemos

$$\dim((S^\perp)^\perp) = \dim(V) - \dim(V) + \dim(S) = \dim(S).$$

Assim $\dim((S^\perp)^\perp) = \dim(S)$. Dessa forma basta provarmos que $S \subseteq (S^\perp)^\perp$. De fato, seja $x \in S$. Pela definição de complemento ortogonal, temos que

$$S^\perp = \{y \in V \text{ tal que } B(y, s) = 0 \text{ para todo } s \in S\}.$$

Como $x \in S$, então $B(y, x) = B(x, y) = 0$, para todo $y \in S^\perp$. Segue que $x \in (S^\perp)^\perp$ e portanto $S \subseteq (S^\perp)^\perp$. □

1.2 Diagonalização de Formas Quadráticas

Nesta seção iremos rever, embora de uma forma diferente, o resultado bem conhecido da Álgebra Linear de que toda forma quadrática regular é equivalente a uma forma quadrática na forma diagonal. Usaremos como ferramenta um importante teorema na teoria de formas quadráticas, o Teorema da Representação.

Denotaremos por $\dot{F}$ o grupo multiplicativo $(F^*, \cdot)$, do corpo F.

Definição 1.25. Sejam f uma forma quadrática sobre o corpo F e $d \in \dot{F}$. Dizemos que f *representa* d, se existirem $x_1, \ldots, x_n \in F$ tais que $f(x_1, \ldots, x_n) = d$. Escrevemos $D_F(f) = D(f)$ para representar o conjunto dos elementos de $\dot{F}$ representados por f. Note que na definição acima, o vetor $(x_1, \ldots, x_n)$ é não nulo.

Exemplo 1.26. Se $F = \mathbb{Q}$ e $f(x, y, z) = 2x^2 + y^2 + xy + 4z^2$, temos que o número racional $4 \in D(f)$. De fato, tomando o vetor $(1, 1, 0)$, temos que $f(1, 1, 0) = 4$.

Lema 1.27. *Seja f uma forma quadrática sobre o corpo F. O conjunto $D(f)$ depende somente da classe de equivalência de f.*

Demonstração: Em outras palavras, temos que mostrar que $D(f) = D(f')$ quando $f \cong f'$. Se $d \in D(f)$, existe $X_0 \in F^n$ tal que $f(X_0) = d$. Como $f \cong f'$, existe C inversível tal que $f(X) = f'(CX)$, para todo $X \in F^n$. Assim, $f'(CX_0) = f(X_0) = d$. Logo $d \in D(f')$, ou seja, $D(f) \subseteq D(f')$. Analogamente, $D(f') \subseteq D(f)$. Portanto $D(f') = D(f)$ □

Lema 1.28. *Sejam f uma forma quadrática sobre F e (V, B, q) é um espaço quadrático associado a f. Então*

$$D(f) = \{d \in \dot{F} \ ; \ \exists \ v \in V \ \textit{tal que} \ q = q_B(v) = d\}.$$

Demonstração: Consequência imediata do lema anterior. □

Lema 1.29. *Sejam f uma forma quadrática sobre F e $a, d \in \dot{F}$. Então $d \in D(f)$ se, e somente se, $a^2 d \in D(f)$.*

Demonstração: Considere (V, B, q) um espaço quadrático associado a f. Suponha que $d \in D(f)$. Assim, pelo lema anterior temos que existe $v \in V$ tal que $q(v) = d$. Dado $a \in \dot{F}$, pela Observação 1.10 temos que $q(a.v) = a^2 d$. Como $a, d \in \dot{F}$, então $a^2 d \neq 0$. Logo $a^2 d \in D(f)$.

Reciprocamente, suponha que $a^2 d \in D(f)$. Assim, existe um vetor $v \in V$ tal que $q_B(v) = a^2 d$. Como $a \in \dot{F}$, existe a^{-1}. Tomando o vetor $a^{-1}v$, temos que $d = a^{-2}a^2 d = q_B(a^{-1}v) \in D(f)$. Portanto $d \in D(f)$. □

Observação 1.30. (1) Pelo lema anterior, $D(f)$ é a união de algumas classes de $\dot{F}$ módulo $\dot{F}^2$. Dizemos que $\dot{F}/\dot{F}^2$ é o *grupo das classes quadradas* de F. Por abuso de notação, escreveremos $D(f)$ como subconjunto de $\dot{F}/\dot{F}^2$.

(2) Em $\dot{F}$, o subconjunto $D(f)$ é sempre fechado para inversos, pois se $d \in D(f)$, então $d^{-1} = d^{-2}d \in D(f)$. Em geral, $D(f)$ não é fechado para multiplicação. Caso $D(f)$ seja subgrupo de $\dot{F}/\dot{F}^2$, diremos que f é uma *forma de grupo* sobre F.

Para ilustrar as afirmações da observação anterior, tomemos alguns exemplos.

Exemplo 1.31. (1) Considere a forma quadrática $f(x) = 3x^2$ sobre o corpo $\mathbb{Q}$. Então $1 \notin D(f)$. De fato, suponha que exista $x \in \mathbb{Q}$ tal que $f(x) = 1$. Assim $3x^2 = 1$, implicando que $x = \pm\sqrt{\frac{1}{3}} \notin \mathbb{Q}$. Logo $1 \notin D(f)$ e neste caso f não é uma forma de grupo.

(2) Considere a forma quadrática $f(x, y, z) = x^2 + y^2 + z^2$ sobre o corpo $\mathbb{Q}$. Então $D(f)$ não é fechado para o produto. Note que $D(f)$ é o subconjunto dos racionais que são somas de três quadrados. É fácil ver que os números $1, 2, 2^{-1}, 14 \in D(f)$, mas $2^{-1}.14 = 7 \notin D(f)$. Esse fato decorre diretamente da teoria dos números, fugindo do escopo desse trabalho.

(3) Seja a forma quadrática $f(x_1, x_2, x_3, x_4) = \sum_{i=1}^{4} x_i^2$ sobre F. Então $D(f)$ é um subgrupo de $\dot{F}$. Como $1 \in D(f)$, então basta mostrar que $D(f)$ é fechado para a multiplicação. De fato, se tomarmos $a, b, c, d, w, x, y, z \in F$ temos que

$$\begin{aligned}(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2) &= (aw+bx+cy+dz)^2+\\ &\quad (ax-bw-cz+dy)^2+\\ &\quad (ay+bz-cw-dx)^2+\\ &\quad (az-by+cx-dw)^2.\end{aligned}$$

Logo o produto de dois elementos de $D(f)$ é um elemento de $D(f)$ e portanto $D(f)$ é subgrupo de $\dot{F}$. Neste caso f é uma *forma de grupo*.

No último exemplo, se $F = \mathbb{Q}$, então $D(f) = \mathbb{Q}_+$. Isso decorre do Teorema de Lagrange "*Todo inteiro positivo n pode ser escrito como soma de 4 quadrados*"(a demonstração desse teorema pode ser encontrada no capítulo 4 do livro [Mar]). Implicando que $\mathbb{Z}_+ \subseteq D(f)$ e, como $D(f)$ é subgrupo de $\dot{\mathbb{Q}}$, $\mathbb{Q}_+ \subseteq D(f)$. Claramente se $d \in D(f)$, então d é positivo. Logo $D(f) \subseteq \mathbb{Q}_+$ e portanto $D(f) = \mathbb{Q}_+$.

Vamos introduzir agora a soma ortogonal, que é uma das operações entre espaços quadráticos e formas quadráticas.

Definição 1.32. Se $(V_1, B_1), (V_2, B_2)$ são espaços quadráticos sobre o mesmo corpo F, então podemos construir (V, B), onde $V = V_1 \oplus V_2$ e $B : V \times V \longrightarrow F$ é dada por

$$B((x_1, x_2), (y_1, y_2)) = B_1(x_1, y_1) + B_2(x_2, y_2), \text{ com } x_i, y_i \in V_i.$$

É facil ver que B é simétrica e bilinear. Assim, implicando que (V, B) é um novo espaço quadrático. Temos que $B(V_1, V_2) = \{0\}$ e $B|_{(V_i,V_i)} = B_i$, com $i = 1, 2$. Denotaremos (V, B) por $V_1 \perp V_2$ e chamaremos de *soma ortogonal dos espaços quadráticos* (V_1, B_1) e (V_2, B_2).

Observação 1.33. Sejam $(V_1, B_1), (V_2, B_2)$ dois F-espaços quadráticos e $(V_1 \perp V_2, B)$ sua soma ortogonal. Então $q_B(x_1, x_2) = q_{B_1}(x_1) + q_{B_2}(x_2)$, onde $x_1 \in V_1$ e $x_2 \in V_2$. De fato, $q_B(x_1, x_2) = B((x_1, x_2)(x_1, x_2)) = B_1(x_1, x_1) + B_2(x_2, x_2) = q_{B_1}(x_1) + q_{B_2}(x_2)$. Denotaremos $q_B = q_{B_1} \perp q_{B_2}$ e chamaremos de *soma ortogonal de funções quadráticas*.

A observação anterior indica como somas ortogonais estão definidas para formas quadráticas. Vejamos alguns exemplos.

Exemplo 1.34. (1) Sejam f_1, f_2 F-formas quadráticas tais que $f_1(x_1) = x_1^2$ e $f_2(x_1) = 2x_1^2$. Sejam $(F, q_1), (F, q_2)$ os F-espaços quadráticos associados as formas f_1, f_2, respectivamente. Assim, $q_1(x_1) = x_1^2$ e $q_2(x_1) = 2x_1^2$. Daí

$$q_1 \perp q_2(x_1, x_2) = q_1(x_1) + q_2(x_2) = x_1^2 + 2x_2^2.$$

(2) Sejam q_1, q_2 F-formas quadráticas tais que $q_1(x_1, x_2) = x_1^2 + 2x_2^2$ e $q_2(x_1, x_2, x_3) = 5x_1x_2 - x_3^2$. Assim, a soma ortogonal de q_1, q_2 é dada por

$$q_1 \perp q_2(x_1, \ldots, x_5) = q_1(x_1, x_2) + q_2(x_3, x_4, x_5) = x_1^2 + 2x_2^2 + 5x_3x_4 - x_5^2.$$

Lema 1.35. *Sejam $(V_1, B_1), (V_2, B_2)$ espaços quadráticos e (V, B) dado por $V = V_1 \perp V_2$. Então $(V_1, B_1), (V_2, B_2)$ são regulares se, e somente se, (V, B) é regular.*

Demonstração: Suponha que $(V_1, B_1), (V_2, B_2)$ são regulares. Sejam $x_i \in V_i$, e $y_i \in V_i$ e $x = (x_1, x_2) \in V$ tal que $B(x, y) = 0$, para todo $y = (y_1, y_2) \in V$. Pela definição de B temos que $B(x, y) = B_1(x_1, x_2) + B_2(y_1, y_2) = 0$, para todo $(y_1, y_2) \in V$. Pelo fato que B_1, B_2 são aplicações bilineares, então existem matrizes simétricas M_{B_1}, M_{B_2} associadas a B_1, B_2, respectivamente. Implicando que

$$x_1^t M_{B_1} y_1 + x_2^t M_{B_2} y_2 = 0, \text{ para todo } (x_2, y_2) \in V.$$

O sistema homogêneo de equações anterior é equivalente a

$$[x_1 \ x_2]^t \begin{bmatrix} M_{B_1} & 0 \\ 0 & M_{B_2} \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = 0.$$

Pelo Teorema 1.18 temos que M_{B_1}, M_{B_2} são inversíveis, implicando que $\begin{bmatrix} M_{B_1} & 0 \\ 0 & M_{B_2} \end{bmatrix}$ é inversível. Assim para cada $0 \neq (y_1, y_2) \in V$ fixado, o sistema anterior tem uma única solução. Logo $(x_1, x_2) = 0$, implicando que (V, B) é regular.
Reciprocamente, suponha que (V, B) é um espaço quadrático regular. Sejam $x \in V_1$ e $y \in V_2$ tais que $B_1(x, a) = 0$, para todo $a \in V_1$ e $B_2(y, b) = 0$, para todo $b \in V_2$. Assim,

$$B((x, y), (a, b)) = B_1(x, a) + B_2(y, b) = 0, \text{ para todo } (a, b) \in V.$$

Como B é regular, segue do Teorema 1.18 que $(x, y) = (0, 0)$, implicando que $x = 0$ e $y = 0$. Portanto $(V_1, B_1), (V_2, B_2)$ são espaços regulares. □

Definição 1.36. Seja $d \in F$, escrevemos $\langle d \rangle$ para denotar a classe de isometria unidimensional correspondente a forma quadrática $f(x) = dx^2$. Note que $\langle d \rangle$ é regular se, e somente se, $d \in \dot{F}$.

Para trabalhar com formas quadráticas multidimensionais é interessante encontrar uma forma, se possível, de decompô-las como soma de formas unidimensionais. Veremos a partir do teorema a seguir que isso é possível para toda forma quadrática.

Teorema 1.37 (Critério da Representação). *Sejam (V, B) um F-espaço quadrático e $d \in \dot{F}$. Então, $d \in D(V)$ se, e somente se, existir um espaço quadrático (V', B') tal que $V \cong \langle d \rangle \perp V'$.*

Demonstração: Suponha que existe um F-espaço quadrático (V', B') tal que $V \cong \langle d \rangle \perp V'$. Afirmamos que $d \in D(\langle d \rangle \perp V')$. De fato, sejam q', q as funções quadráticas associadas a $(V', B'), (V, B)$ respectivamente. Isso implica que $(V, q) \cong (\langle d \rangle \perp V', dx^2 + q'(v))$. Tomando o vetor $(1, 0) \in \langle d \rangle \perp V'$, temos que $d \in D(\langle d \rangle \perp V') = D(V)$.

Reciprocamente, suponha que $d \in D(V)$. Teremos dois caso para ser analisados, se V é regular ou não. Caso V não seja regular, então $\text{rad}(V) \neq \{0\}$. Como V é um espaço de dimensão finita, então existe um subespaço W de V tal que $V = \text{rad}(V) \oplus W = \text{rad}(V) \perp W$. Assim $(V, B) \cong (\text{rad}(V) \oplus W, B)$. Neste caso, temos que $D(V) = D(W)$. De fato, seja $k \in D(V)$, logo existe $u \in V$ tal que $q(u) = k$, onde $q = q_B$. Como $V = \text{rad}(V) \perp W$, então $u = r + w$, com $r \in \text{rad}(V)$ e $w \in W$. Segue que

$$k = q(u) = q(r + w) = q(r) + q(w) = 0 + q(w) = q(w).$$

Implicando que $k \in D(W)$. Como $W \subseteq V$, então $D(W) \subseteq D(V)$. Logo $D(V) = D(W)$. Vamos mostrar agora que W é regular, ou seja, que $\text{rad}(W) = \{0\}$. De fato, se $w_0 \in \text{rad}(W)$, então $w_0 \in W$ e $B(w_0, w) = 0$, para todo $w \in W$. Seja $r \in \text{rad}(V)$, então $B(v, r) = 0$, para todo $v \in V$, em particular $B(w_0, r) = 0$. Como r foi escolhido arbitrariamente, então $B(w_0, r) = 0$, para todo $r \in \text{rad}(V)$. Do fato que $V = \text{rad}(V) \perp W$, temos que $B(w_0, v) = 0$, para todo $v \in V$, logo $w_0 \in \text{rad}(V)$. Implicando que $w_0 = 0$, pois $\text{rad}(V) \cap W = \{0\}$.

Pelo que já provamos até agora, basta mostrarmos o resultado para o caso em que (V, B) é regular, pois caso contrário podemos tomar W, como construído anteriormente. Suponha que (V, B) é regular. Como $d \in D(V)$, então existe $v \in V$ tal que $q(v) = d$. Vamos mostrar que $(F.v, B|_{F.v})$ é isométrico ao espaço (F, B'), onde $B'(x, y) = dxy$, $x, y \in F$. Sejam $a, b \in F.v$. Assim, $a = k_1 v$ e $b = k_2 v$, onde $k_1, k_2 \in F$. Logo $B(a, b) = k_1 k_2 d$. Tomando o isomorfismo $\phi : F \longrightarrow F.v$ dado por $k \longrightarrow k.v$, temos que $B(\phi(k_1), \phi(k_2)) = B(a, b) = k_1 k_2 d = B'(k_1, k_2)$, para todo $k_1, k_2 \in F$. Logo $(F.v, B|_{F.v}) \cong (F, B')$. Como $d \in \dot{F}$, então $(F.v, B|_{F.v}) \cong (F, B')$ é regular. Pelo fato que (V, B) ser regular por hipótese e pelo Teorema 1.24, temos que

$$\dim(F.v) + \dim(F.v)^{\perp} = \dim(V).$$

Tomando $V' = (F.v)^{\perp}$ obtemos $V \cong \langle d \rangle \perp V'$. □

A primeira consequência desse critério é a existência de uma "base ortogonal"em qualquer espaço quadrático.

Corolário 1.38. *Seja (V, B) um F-espaço quadrático, então existem escalares $d_1, \ldots, d_n \in F$ tais que $V \cong \langle d_1 \rangle \perp \cdots \perp \langle d_n \rangle$. (Em outras palavras, qualquer forma quadrática de n variáveis é equivalente a uma forma diagonal $d_1 x_1^2 + \cdots + d_n x_n^2$).*

Demonstração: Provaremos esse corolário por indução sobre $n = \dim(V)$. Suponha que $\dim(V) = 1$. Caso $D(V) = \emptyset$, então $B \equiv 0$ e $V \cong \langle 0 \rangle$. Se existir $d \in D(V)$, então pelo Critério de Representação temos que $V \cong \langle d \rangle \perp V'$. Pelo fato que $1 = \dim(V) = \dim(\langle d \rangle)$, então $V' \cong \{0\}$, implicando que $V \cong \langle d \rangle$.
Suponha que este corolário seja válido para $1 \leq k < n$. Se $\dim(V) = n$, temos dois casos para analisar. Caso $D(V) = \emptyset$ então por argumento análogo acima temos que $V \cong \langle 0, 0, \ldots, 0 \rangle$. Caso exista $d \in D(V)$, então pelo Critério de Representação temos que $V \cong \langle d \rangle \perp V'$. Como $\dim(V') = n-1$, pela hipótese de indução, $V' = \langle d_1 \rangle \perp \cdots \perp \langle d_{n-1} \rangle$ com $d_1, \ldots, d_{n-1} \in F$. Implicando que

$$V = \langle d \rangle \perp \langle d_1 \rangle \perp \cdots \perp \langle d_{n-1} \rangle.$$

Provando o corolário. □

Notação 1.39. Abreviaremos a forma diagonal $\langle d_1 \rangle \perp \cdots \perp \langle d_n \rangle$ por $\langle d_1, \ldots, d_n \rangle$. Em especial, a diagonal $\langle d, \ldots, d \rangle$ de tamanho n é abreviada em $n\langle d \rangle$. Para exemplificar, $3\langle a \rangle \perp 2\langle b \rangle$ é a abreviação de $\langle a, a, a, b, b \rangle$.

Corolário 1.40. *Seja (V, B) um F-espaço quadrático (não necessariamente regular) e $S \subseteq V$ um subespaço regular. Então:*
(1) *$V = S \perp S^{\perp}$;*
(2) *Se T é um subespaço de V tal que $V \cong S \perp T$, então $T \cong S^{\perp}$.*

Demonstração: (1) Como S é regular, então $\text{rad}(S) = S \cap S^{\perp} = \{0\}$. Assim, é suficiente se mostrarmos que V é gerado por S e $S^{\perp}$. Pelo corolário anterior, temos que S tem uma base ortogonal $\{s_1, \ldots s_n\}$ tal que $q_{B|_S}(s_i) = d_i$ e $S \cong \langle d_1, \ldots, d_n \rangle$. Pela regularidade de S temos $B(s_i, s_i) \neq 0$, para $i = 1, \ldots, n$. Dado $z \in V$, considere o vetor

$$y = z - \sum_{i=1}^{n} \frac{B(z, s_i)}{B(s_i, s_i)} \cdot s_i.$$

É fácil mostrar que $B(y, s_j) = 0$, para $j = 1, \ldots, n$. Logo

$$y \in S^{\perp} \text{ e } z = y + \sum_{i=1}^{n} \frac{B(z, s_i)}{B(s_i, s_i)} \cdot s_i \in S \perp S^{\perp}.$$

(2) Seja T um subespaço de V tal que $V \cong S \perp T$. Pelo item (1) desse corolário temos que $T \subseteq S^{\perp}$. Mas $\dim(T) = \dim(V) - \dim(S) = \dim(S^{\perp})$. Logo $T \cong S^{\perp}$. □

Corolário 1.41. *Seja (V, B) um F-espaço quadrático regular. Então, um subespaço S de V é regular se, e somente se, existe $T \subseteq V$ tal que $V \cong S \perp T$.*

Demonstração: Suponha que $S \subseteq V$ é um subespaço regular. Assim pelo corolário anterior temos que $V \cong S \perp S^{\perp}$. Tomando $T = S^{\perp}$, temos o desejado.
Reciprocamente, suponha que exista $T \subseteq V$ tal que $V \cong S \perp T$. Sejam $x \in \text{rad}(S)$ e $v \in V$. Como $V \cong S \perp T$, então $v = s + t$, com $s \in S$ e $t \in T$. Assim $B(x, s) = 0$ e $B(x, t) = 0$, pois $x \in S$ e $S \perp T$ é uma soma ortogonal. Logo $B(x, v) = B(x, s + t) = 0$. Como x, v foram tomados arbitrariamente, temos que $x \in \text{rad}(V)$, ou seja, $\text{rad}(S) \subseteq \text{rad}(V)$. Como (V, B) é regular, então $\text{rad}(S) = 0$. Logo $(S, B|_{S \times S})$ é regular. □

Definição 1.42. Definimos *determinante* de uma forma quadrática regular f por $d(f) := \det(M_f).\dot{F}^2$ (elemento de $\dot{F}/\dot{F}^2$), onde M_f é a matriz simétrica associada a f.

Exemplo 1.43. Seja a F-forma quadrática $f = 2x^2 + 3xy + y^2 + 2z^2$. Por Polarização temos a seguinte aplicação bilinear B, associada a f

$$B((x, y, z), (x', y', z')) = 2xx' + 3/2[xy' + x'y] + yy' + 2zz'.$$

Como $M_f = [B(e_i, e_j)]_3$, onde $\{e_1, e_2, e_3\}$ é a base canônica de F^3, segue que

$$M_f = \begin{bmatrix} 2 & 3/2 & 0 \\ 3/2 & 1 & 0 \\ 0 & 0 & 2 \end{bmatrix}.$$

Implicando que $d(f) = \det M_f \dot{F}^2 = 4\dot{F}^2 = 1\dot{F}^2$.

Proposição 1.44. *Sejam f e g F-formas quadráticas regulares.*
(1) *Se $f \cong g$, então $d(f) = d(g)$;*
(2) *$d(f \perp g) = d(f).d(g) \in \dot{F}/\dot{F}^2$.*

Demonstração: (1) De fato, supondo que $f \cong g$, temos que $M_f = C^t M_g C$, onde M_f, M_g são as matrizes simétricas associadas a f e g, respectivamente, e C é uma matriz inversível. Logo

$$\begin{aligned} d(f) &= \det(M_f)\dot{F}^2 = \det(C^t M_g C)\dot{F}^2 = \det(M_g) \cdot \det(C)^2 \dot{F}^2 \\ &= \det(M_g)\dot{F}^2 = d(g). \end{aligned}$$

(2) Como a soma $f \perp g$ é ortogonal temos que $M_{f\perp g} = \begin{bmatrix} M_f & 0 \\ 0 & M_g \end{bmatrix}$ e assim

$$d(f \perp g) = \det\left(\begin{bmatrix} M_f & 0 \\ 0 & M_g \end{bmatrix}\right) \cdot \dot{F}^2 = \det(M_f) \cdot \det(M_g) \cdot \dot{F}^2 = d(f) \cdot d(g).$$

□

A proposição anterior mostra que $d(f)$ é invariante da classe de equivalência de f. Se $V \cong \langle d_1, \ldots, d_n \rangle$ é uma diagonalização de V, então $d(f) = \prod_{i=1}^{n} d_i \dot{F}^2$. Muitas vezes é conveniente chamar $d(f)$ de *determinante de* V, sendo denotado por $d(V)$.

1.3 Plano Hiperbólico e Espaço Hiperbólico

Nessa seção, iremos introduzir a importante noção de espaço quadrático hiperbólico. Para começar definiremos "isotropia" e "anisotropia".

Definição 1.45. Seja v um vetor não nulo em um F-espaço quadrático (V, B). Dizemos que v é um vetor *isotrópico* se $B(v, v) = 0$ (ou equivalentemente, se $q_B(v) = 0$), e dizemos que v é *anisotrópico*, caso contrário. O F-espaço quadrático (V, B) é dito *isotrópico* se ele contém um vetor (não nulo) isotrópico, caso contrário dizemos que (V, B) é *anisotrópico*. Por último, dizemos que (V, B) é *totalmente isotrópico* se todos os vetores não nulos em V forem isotrópicos.

Observação 1.46. (1) Se (V, B) é um F-espaço quadrático anisotrópico, então podemos notar que (V, B) é regular;
(2) O F-espaço quadrático (V, B) é totalmente isotrópico se, e somente se, $B \equiv 0$.

Teorema 1.47. *Seja (V, B) um F-espaço quadrático bidimensional. Então as seguintes afirmações são equivalentes:*
(1) *(V, B) é regular e isotrópico;*
(2) *(V, B) é regular, com $d(V) = -1.\dot{F}^2$;*
(3) *$(V, B) \cong \langle 1, -1 \rangle$;*
(4) *(V, B) corresponde a classe de equivalência da F-forma quadrática $f(x_1, x_2) = x_1 x_2$.*

Demonstração: Considere $q = q_B$ a forma quadrática associada a (V, B).
(1) $\Rightarrow$ (2) Suponha que (V, B) é um espaço regular e isotrópico. Como (V, q) é um espaço quadrático bidimensional regular, então $q \cong \langle d_1, d_2 \rangle$, com $d_1, d_2 \in \dot{F}$. Seja $\{v_1, v_2\}$ uma base ortogonal de V tal que $q(v_1) = d_1$ e $q(v_2) = d_2$. Seja $v \in V$ um vetor isotrópico. Assim, $v \neq 0$ e $v = a.v_1 + b.v_2$, com $a, b \in F$. Isso implica que $0 = q(v) = a^2 d_1 + b^2 d_2$. Sem perda de generalidade, suponha que $a \neq 0$. Assim, $d_1 = -(ba^{-1})^2 d_2$, e segue que $d_1 d_2 = -(ba^{-1} d_2)^2$. Logo

$$d(V) = d_1.d_2 \dot{F}^2 = -1(ba^{-1}d_2)^2 \dot{F}^2 = -1\dot{F}^2.$$

(2) $\Rightarrow$ (3) Suponha que (V, q) é regular e $d(V) = -1.\dot{F}^2$. Como (V, q) é bidimensional, então $q \cong \langle d_1, d_2 \rangle$, com $d_1, d_2 \in F$. Pelo fato que $d(V) = -1.\dot{F}^2$, então $-d_1 d_2 = a^2$, com $a \in \dot{F}$. Assim, $d_1 = ab$ e $d_2 = -ab^{-1}$, com $b \in \dot{F}$. Segue que,

$$q \cong \langle ab, -ab^{-1} \rangle \cong \langle c, -c \rangle,$$

onde $c = ab$. Pelo Exemplo 1.8 temos que $q \cong q'$, sendo que $q'(x_1, x_2) = cx_1x_2$. Note que $D(q') = \dot{F}$, pois dado $k \in \dot{F}$, basta tomar $v = (c^{-1}k, 1)$ e teremos que $q'(v) = k$. Logo $1 \in D(q') = D(q)$. Assim, pelo Critério de Representação e do fato que $d(q) = -1\dot{F}^2$, vemos que $q \cong \langle 1, -1\rangle$.
(3) $\iff$ (4) É consequência direta do Exemplo 1.8.
(3) $\Rightarrow$ (1) Como $q \cong \langle 1, -1\rangle$, então $d(q) = -1 \cdot \dot{F}^2$, implicando na regularidade do espaço (V, q). Como $q(1, 1) = 0$ temos que (V, q) é isotrópica. □

Definição 1.48. Chamaremos de *plano hiperbólico* a classe de isometria de um espaço quadrático que satisfaça as condições do Teorema 1.47. Denotaremos o plano hiperbólico por $\mathbb{H}$. Um espaço quadrático formado unicamente por uma soma ortogonal de planos hiperbólicos será chamada de *espaço hiperbólico.*

Definição 1.49. Uma F-forma quadrática f (ou F-espaço quadrático) é chamada *universal* se ela representa todos os elementos não nulos de F ou, em outras palavras, $D(f) = \dot{F}$.

Claramente o plano hiperbólico $\mathbb{H} = \langle 1, -1\rangle$ é universal, pois $\mathbb{H}$ é equivalente a forma $f(x_1, x_2) = x_1x_2$ e dado $k \in \dot{F}$, basta tomar $v = (k, 1)$ e teremos que $f(k, 1) = k$.

Teorema 1.50. *Seja (V, B) um F-espaço quadrático regular. Então:*
(1) *Todo subespaço totalmente isotrópico $U \subset V$ tal que $\dim(U) = r$ está contido em um subespaço hiperbólico $T \subseteq V$ de dimensão $2r$;*
(2) *(V, B) é isotrópico se, e somente se, V contém um plano hiperbólico;*
(3) *Se (V, B) é isotrópico, então (V, B) é universal.*

Demonstração: (1) Provaremos por indução sobre $\dim(U) = r$. Suponha que $\dim(U) = 1$. Assim, seja $\{x\}$ uma base de U. Pelo fato que U é totalmente isotrópico, então tomando $u = \alpha x \in U$ com $\alpha \in F$, temos que $B(x, u) = \alpha B(x, x) = 0$. Implicando que $x \in U^\perp$, ou seja, $U \subset U^\perp$. Como (V, B) é regular, então $\dim(V) > \dim(U) = 1$. Pelo Teorema 1.24, temos que $\dim(U^\perp) = \dim(V) - 1$, logo $V \neq U^\perp$. Assim existe $y \in V$ tal que $y \notin U^\perp$, logo $y \notin \mathrm{Rad}(U) \subseteq U$ e $B(x, y) \neq 0$. Como $U \cap F.y = \{0\}$, tomemos o subespaço $U \oplus F.y = T$. Vamos mostrar que $(T, B|_{T\times T})$ é regular. Para tanto, considere M a matriz associada a $B|_{T\times T}$, ou seja,

$$M = \begin{bmatrix} 0 & B(x, y) \\ B(y, x) & B(y, y) \end{bmatrix}.$$

Logo, $\det(M) = -B(x, y)^2\dot{F}^2 = -1\dot{F}^2$, provando que $(T, B|_{T\times T})$ é regular. Mais ainda, pelo Teorema 1.47, $(T, B|_{T\times T})$ é um plano hiperbólico. Portanto o resultado vale para $r = 1$.
Suponha que o resultado é verdadeiro para $k \in \mathbb{N}$ tal que $1 \leq k < r$. Seja $U \subset V$ subespaço totalmente isotrópico tal que $\dim(U) = r$ e $\{x_1, \ldots, x_r\}$ uma base de U. Tomemos $S \subset U$ tal que S é gerado pelo conjunto $\{x_2, \ldots, x_r\}$. É fácil ver que $U^\perp \subset S^\perp$. Pelo Teorema 1.24 temos que

$$\dim(S^\perp) = \dim(V) - \dim(S) > \dim(V) - \dim(U) = \dim(U^\perp).$$

Logo $U^\perp \subsetneq S^\perp$ e existe $y_1 \in V$ tal que $B(y_1, x_2) = 0, \ldots, B(y_1, x_r) = 0$ e $B(y_1, x_1) \neq 0$. Queremos mostrar que $\{x_1, y_1\}$ é LI. De fato, se $\{x_1, y_1\}$ fosse LD, então $y_1 = \alpha x_1$ e $B(y_1, x_1) = \alpha B(x_1, x_1) = 0$, uma contradição. Tomemos o subespaço $H_1 = F.x_1 \oplus F.y_1$. Note que $(H_1, B|_{H_1\times H_1})$ é um plano hiperbólico, pois a matriz associada a $B|_{H_1\times H_1}$ é

$$M = \begin{bmatrix} 0 & B(x_1, y_1) \\ B(y_1, x_1) & B(y_1, y_1) \end{bmatrix}$$

e $\det(M) = -1\dot{F}^2$. Pelo Teorema 1.47 temos que $H_1 \cong \mathbb{H}$.
Como H_1 é regular, $V \cong H_1 \perp H_1^\perp$ e, disso, $\{x_2, \ldots, x_r\} \subset H_1^\perp$. Pelo Corolário 1.41 temos que $H_1^\perp$ é regular. Como $\{x_2, \ldots, x_r\} \subset H_1^\perp$, então $S \subseteq H_1^\perp$. Pelo fato que S é totalmente isotrópico em $H_1^\perp$ e $\dim(S) = r-1$. Segue, pela hipótese de indução, que existe $H_2 \subseteq H_1^\perp$ tal que H_2 é um espaço hiperbólico de dimensão $2(r-1)$. Tomando $H = H_1 \oplus H_2$, temos que $H \subseteq V$ e H é um espaço hiperbólico de dimensão $2r$.

(2) Suponha que (V, B) é isotrópico, então existe um vetor não nulo $x \in V$ tal que $B(x, x) = 0$. Tomando o subespaço $X = F.\{x\}$, temos que X é totalmente isotrópico. Assim, pelo item (1) desse teorema temos que existe $\mathbb{H} \subseteq V$ tal que $X \subset \mathbb{H}$.
A recíproca é caso direto do Teorema 1.47.

(3) Resultado imediato do item (2) desse teorema e do fato do plano hiperbólico ser universal. □

Observação 1.51. (1) Como a diagonalização de $\mathbb{H}$ é $\langle 1, -1\rangle$ e do fato de $\mathbb{H}$ ser universal, fica evidente que todo elemento não nulo de F é a diferença de dois quadrados. Pode-se verificar esse fato diretamente usando a seguinte equação:

$$a = \left(\frac{a+1}{2}\right)^2 - \left(\frac{a-1}{2}\right)^2 \text{ para todo } a \in F.$$

(2) Pode-se provar o Teorema 1.50 item (3) por um argumento direto, procedendo da seguinte maneira. Fixe um vetor isotrópico x e tome $y \in V$ tal que $B(x, y) \neq 0$. Então $B(tx + y, tx + y) = 2tB(x, y) + B(y, y)$, que assume todo os valores de F quando t varia em F. Para obter $B(tx + y, tx + y) = k$, basta tomar $t = \frac{k - B(y,y)}{2B(x,y)} \in F$.

Corolário 1.52 (**Primeiro Teorema de Representação**). *Sejam q uma forma quadrática regular e $d \in \dot{F}$. Então, $d \in D(q)$ se, e somente se, $q \perp \langle -d\rangle$ é isotrópica.*

Demonstração: Pelo Critério de Representação 1.37 podemos assumir que $q = a_1x_1^2 + \cdots + a_nx_n^2$, onde $a_i \neq 0$ para $i = 1, \ldots, n$. Suponha que $d \in D(q)$. Isso implica que existem $b_1, \ldots, b_n \in F$ (não todos nulos) tais que $d = \sum_{i=1}^n a_ib_i^2$. Logo $\sum_{i=1}^n a_ib_i^2 - d.1^2 = 0$. Como $(b_1, \ldots, b_n, 1) \neq 0$, então $q \perp \langle -d\rangle$ é isotrópica.

Reciprocamente, suponha que $q \perp \langle -d\rangle$ é isotrópica. Assim existe um vetor não nulo $(b_1, \ldots, b_{n+1})$ tal que $\sum_{i=1}^n a_ib_i^2 + (-d).b_{n+1}^2 = 0$. Se $b_{n+1} \neq 0$, então

$$d = \sum_{i=1}^n a_i \left(\frac{b_i}{b_{n+1}}\right)^2 \in D(q).$$

Se $b_{n+1} = 0$, então $(b_1, \ldots, b_n)$ é um vetor isotrópico de q. Pelo Teorema 1.50 item (3), temos que $D(q) = \dot{F}$, implicando que $d \in D(q)$. □

Corolário 1.53. *Sejam q_1 e q_2 formas quadráticas regulares de dimensão positiva. Então, $q_1 \perp q_2$ é isotrópica se, e somente se, $D(q_1) \cap -D(q_2) \neq \emptyset$.*

Demonstração: Suponha que $q := q_1 \perp q_2$ é isotrópica. Isso implica que existe um vetor não nulo (x, y) tal que $q(x, y) = q_1(x) + q_2(y) = 0$. Assim, $q_1(x) = -q_2(y)$. Se $q_1(x) \neq 0$, então $q_1(x) = a \in \dot{F}$. Segue que $a \in D(q_1)$ e $-a \in D(q_2)$, implicando que $a \in D(q_1) \cap -D(q_2)$. Se $q_1(x) = 0$, então $q_2(y) = 0$. Como (x, y) é não nulo, temos que q_1

ou q_2 é isotrópica e assim $D(q_1) = \dot{F}$ ou $D(q_2) = \dot{F}$. Sem perda de generalidade suponha que $D(q_1) = \dot{F}$, isso implica que $D(q_1) \cap -D(q_2) = -D(q_2) \neq \emptyset$.

Reciprocamente, suponha que $D(q_1) \cap -D(q_2) \neq \emptyset$. Isso implica que existe $a \in \dot{F}$ tal que $a \in D(q_1) \cap -D(q_2)$. Assim, existem vetores não nulos x, y tais que $q_1(x) = a$ e $q_2(y) = -a$. Tomando $q = q_1 \perp q_2$, temos que $q(x, y) = a - a = 0$. Logo q é isotrópica. □

Corolário 1.54. *Sejam F um corpo e r um inteiro positivo. Então as seguintes afirmações são equivalentes:*
(1) *Qualquer F-forma quadrática regular de dimensão r é universal;*
(2) *Qualquer F-forma quadrática de dimensão $r+1$ é isotrópica.*

Demonstração: (1) ⇒ (2) Suponha que as formas quadráticas regulares de dimensão r são universais. Seja q uma F-forma de dimensão $r+1$. Caso q seja isotrópica, nada temos que provar. Suponha que q é anisotrópica. Seja $d \in D(q)$. Pelo Critério de Representação 1.37 temos que $q \cong < d > \perp q'$, onde q' é uma F-forma quadrática de dimensão r. Como q é anisotrópica, então q' é anisotrópica e assim q' é regular. Pela hipótese temos que q' é universal. Em particular $-d \in D(q')$ e pelo Primeiro Teorema de Representação 1.52 temos que q é isotrópica.

(2) ⇒ (1). Suponha que qualquer forma quadrática de dimensão $r+1$ é isotrópica. Seja q uma F-forma quadrática regular de dimensão r. Por hipótese $q \perp \langle -d \rangle$ é isotrópica para qualquer $d \in \dot{F}$. Pelo Primeiro Teorema de Representação 1.52 temos que $d \in D(q)$. Logo q é universal. □

1.4 Teoremas da Decomposição e do Cancelamento de Witt

Nesta seção apresentaremos alguns dos mais importantes teoremas da teoria de formas quadráticas clássica. Para isso precisamos primeiro de alguns resultados sobre o grupo ortogonal e reflexões de hiperplano.

Definição 1.55. Seja (V, B, q) um F-espaço quadrático. Escrevemos $O_q(V) = O(V)$ para denotar o grupo de isometrias de (V, B, q), ou seja, o grupo de todos os isomorfismos $\tau : V \to V$ que preservam a forma bilinear. Esse grupo é chamado de *grupo ortogonal* e é o grupo simétrico que fundamenta a geometria de nosso espaço quadrático.

Proposição 1.56. *Seja (V, B, q) um F-espaço quadrático e $y \in V$ um vetor anisotrópico em (V, B, q). Definida a aplicação $\tau_y : V \longrightarrow V$ por*

$$\tau_y(x) := x - \frac{2B(x, y)}{q(y)} y, \text{ para todo } x \in V.$$

Então:
(1) *τ_y é um endomorfismo linear;*
(2) *$\tau_y|_{(F.\{y\})^\perp} \equiv Id$, $\tau_y(y) = -y$ e $\tau_y^2 = Id$;*
(3) *$\tau_y \in O(V)$;*
(4) *$\det(\tau_y) = -1$.*

Demonstração: (1) Primeiramente, τ_y está bem definida, pois $q(y) \neq 0$. Sejam $x, z \in V$ e $a \in F$. Assim,

$$\begin{aligned}\tau_y(x+az) &= (x+az) - \tfrac{2B(x+az,y)}{q(y)}y \\ &= x - \tfrac{2B(x,y)}{q(y)}y + a\left(z - \tfrac{B(z,y)}{q(y)}y\right) = \tau_y(x) + a\tau_y(z).\end{aligned}$$

Provando que τ_y é um endomorfismo linear.

(2) Seja $x \in (F.y)^\perp$, logo $B(x,y) = 0$. Assim, $\tau_y(x) = x - \frac{2B(x,y)}{q(y)}y = x$, ou seja, $\tau_y|_{(F.y)^\perp} \equiv Id$. Aplicando y em τ_y temos que $\tau_y(y) = y - \frac{2q(y)}{q(y)}y = -y$. E por último

$$\begin{aligned}\tau_y(\tau_y(x)) &= \tau_y(x - \tfrac{2B(x,y)}{q(y)}y) \\ &= x - \tfrac{2B(x,y)}{q(y)}y - \tfrac{2B(x,y)}{q(y)}y + \tfrac{4B(x,y)}{q(y)}y = x.\end{aligned}$$

(3) Do fato que $\tau_y^2 \equiv Id$ temos que τ_y é um isomorfismo e para provarmos que $\tau_y \in O_q(V)$, resta mostrarmos que τ_y preserva a forma bilinear B. De fato, dados $x, z \in V$ temos que

$$\begin{aligned}B(\tau_y(x), \tau_y(z)) &= B(x - \tfrac{2B(x,y)}{q(y)}y, z - \tfrac{2B(z,y)}{q(y)}y) \\ &= B(x,z) + \tfrac{4B(x,y)B(z,y)}{(q(y))^2}q(y) - \tfrac{4B(x,y)B(z,y)}{q(y)} = B(x,z).\end{aligned}$$

Logo $\tau_y \in O_q(V)$.

(4) Como y é anisotrópico, então $F.y$ é regular. Assim, $V \cong F.y \perp (F.y)^\perp$. Seja $\{y_2, \ldots, y_n\}$ uma base ortogonal de $(F.y)^\perp$. Tomemos a base de V, $\beta_V = \{y, y_2, \ldots, y_n\}$. Dado $x \in V$, temos que $x = a_1y + a_2y_2 + \cdots + a_ny_n$. Segue que $\tau_y(x) = -a_1y + a_2y_2 + \cdots + a_ny_n$, implicando que $[\tau_y]_n = \text{diag}(-1, 1, \ldots, 1)$. Portanto $\det(\tau_y) = -1$. □

Definição 1.57. Chamaremos de *reflexão de hiperplano* as isometrias definidas na Proposição 1.56.

Observação 1.58. O conjunto das reflexões de hiperplano $\{\tau_y; q(y) \neq 0\}$ é fechado pela conjugação no grupo ortogonal $O(V)$. A demonstração dessa afirmação é equivalente a provar que $\sigma\tau_y\sigma^{-1} = \tau_{\sigma(y)}$ para $\sigma \in O(V)$. De fato, para todo $x \in V$,

$$\begin{aligned}\sigma\tau_y\sigma^{-1}(x) &= \sigma[\tau_y(\sigma^{-1}(x))] \\ &= \sigma\left[\sigma^{-1}(x) - \tfrac{2B(\sigma^{-1}(x),y)}{q(y)} \cdot y\right] \\ &= x - \tfrac{2B(x,\sigma(y))}{q(\sigma(y))} \cdot \sigma(y) = \tau_{\sigma(y)}(x).\end{aligned}$$

Proposição 1.59. *Sejam (V, B, q) um F-espaço quadrático e $x, y \in V$ tais que $q(x) = q(y) \neq 0$. Então existe um elemento $\tau \in O(V)$ tal que $\tau(x) = y$.*

Demonstração: Sejam $x, y \in V$ tais que $q(x) = q(y) \neq 0$. Afirmamos que $q(x+y) + q(x-y) \neq 0$. De fato,

$$\begin{aligned}q(x+y) + q(x-y) &= B(x+y, x+y) + B(x-y, x-y) \\ &= 2q(x) + 2q(y) = 4q(x) \neq 0.\end{aligned}$$

Isso implica que $q(x+y) \neq 0$ ou $q(x-y) \neq 0$. Suponha que $q(x-y) \neq 0$. Aplicando x na reflexão de hiperplano τ_{x-y}, obtemos

$$\tau_{x-y}(x) = x - \frac{2B(x, x-y)}{q(x-y)}(x-y).$$

Mas

$$\begin{aligned} q(x-y) &= B(x-y,x-y) \\ &= B(x,x)+B(y,y)-2B(x,y) \\ &= 2[B(x,x)-B(x,y)] \\ &= 2B(x,x-y). \end{aligned}$$

Portanto, $\tau_{x-y}(x) = x-(x-y) = y$. No caso em que $q(x+y) \neq 0$, de modo análogo obtemos que $-\tau_{x+y}(x) = y$. □

Teorema 1.60 (Cancelamento de Witt). *Sejam $(V,q),(V_1,q_1),(V_2,q_2)$ F-espaços quadráticos arbitrários. Se $q \perp q_1 \cong q \perp q_2$, então $q_1 \cong q_2$.*

Demonstração: Suponha que $q \perp q_1 \cong q \perp q_2$. Dividiremos a demonstração desse teorema em três passos.
Passo 1: O cancelamento é válido quando q é totalmente isotrópica e q_1 é regular.
Demonstração do Passo 1: Sejam M, M_1, M_2 as matrizes simétricas associadas as formas quadráticas q, q_1, q_2, respectivamente. Por hipótese temos que $\begin{bmatrix} M & 0 \\ 0 & M_1 \end{bmatrix}$ é congruente a $\begin{bmatrix} M & 0 \\ 0 & M_2 \end{bmatrix}$. Isso implica que existe uma matriz inversível $E = \begin{bmatrix} A & B \\ C & D \end{bmatrix}$ tal que

$$\begin{bmatrix} M & 0 \\ 0 & M_1 \end{bmatrix} = E^t \begin{bmatrix} M & 0 \\ 0 & M_2 \end{bmatrix} E.$$

Como q é totalmente isotrópico, então $M \equiv 0$, implicando $\begin{bmatrix} 0 & 0 \\ 0 & M_1 \end{bmatrix} = E^t \begin{bmatrix} 0 & 0 \\ 0 & M_2 \end{bmatrix} E$.
Segue que

$$\begin{bmatrix} 0 & 0 \\ 0 & M_1 \end{bmatrix} = \begin{bmatrix} C^tM_2C & C^tM_2D \\ D^tM_2C & D^tM_2D \end{bmatrix}.$$

Em particular $M_1 = D^tM_2D$. Como M_1 é inversível, então D, M_2 são inversíveis. Implicando que M_1 e M_2 são congruentes. Logo $q_1 \cong q_2$.

Passo 2: O cancelamento é válido se q é totalmente isotrópico.
Demonstração do Passo 2: Diagonalizaremos q_1, q_2, assumindo que q_1 tem exatamente $r > 0$ coeficientes nulos. Assim, $q_1 \cong r\langle 0\rangle \perp q_1'$. Caso q_2 tenha r ou mais coeficientes nulos, podemos reescrever a hipótese

$$q \perp r\langle 0\rangle \perp q_1' \cong q \perp r\langle 0\rangle \perp q_2'.$$

Como q_1' é livre de coeficientes nulos, então q_1' é regular. Assim, como $q \perp r\langle 0\rangle$ é totalmente isotrópica, pelo Passo 1 dessa proposição, temos que $q_1' \cong q_2'$, portanto $q_1 \cong q_2$. Para o caso em que q_2 tenha menos do que r coeficientes nulos, tomemos q_2 no lugar de q_1 e por argumento análogo obtemos que $q_2 \cong q_1$.

Passo 3: Caso geral.
Demonstração do Passo 3: Seja $\langle a_1, \ldots, a_n\rangle$ uma diagonalização de q. Provaremos esse caso por indução sobre $n = \dim(q)$. Pelo Critério de Representação 1.52, basta provarmos para o caso em que $n = 1$, logo tomemos $q \cong \langle a_1\rangle$. Caso $a_1 = 0$, então q é totalmente isotrópica recaindo no Passo 2. Suponha que $a_1 \neq 0$. Reescrevendo as hipóteses temos que

$$g := \langle a_1\rangle \perp q_1 \cong \langle a_1\rangle \perp q_2.$$

Assim $(F \perp V_1, B, g) \cong (F \perp V_2, B, g)$. Como $a_1 \neq 0$, então existe um vetor $0 \neq v \in F$, tal que $q(v) = a_1$. Pelo fato que

$$g((v,0)) = q(v) + q_1(0) = a_1 = q(v) + q_2(o) = g((v,o)),$$

então pela Proposição 1.59 existe a isometria $-\tau_{2v} \in O(F \perp V_1)$ tal que $-\tau_{2v}(v) = v$. Afirmamos que $-\tau|_V \equiv Id$. De fato, como τ é isomorfismo e V é um espaço vetorial unidimensional em que $v \neq 0$, temos que $-\tau(\alpha v) = -(-\alpha v) = \alpha v$, com $\alpha \in V$, então $-\tau|_V \equiv Id$. Mais ainda, $-\tau(V) \perp V_1$. Queremos mostrar que $-\tau_{2v}|_{V_1}$ é uma isometria. De fato, como τ_{2v} é reflexão de hiperplano, então $\tau_{2v}|_{V_1} \equiv Id$. Assim, $-\tau_{2v}|_{V_1} \equiv -Id$.Logo $(V_1, q_1) \cong (V_2, q_2)$. □

Note que no teorema anterior (Cancelamento de Witt) e no próximo teorema não estamos assumindo que o espaço quadrático seja regular, ou seja, estes resultados valem para qualquer espaço quadrático.

Teorema 1.61 (Decomposição de Witt). *Seja (V, q) um F-espaço quadrático qualquer. Então (V, q) se fatora como uma soma soma ortogonal*

$$(V_t, q_t) \perp (V_h, q_h) \perp (V_a, q_a),$$

onde V_t é um subespaço totalmente isotrópico, V_h é um subespaço hiperbólico (ou nulo) e V_a é um subespaço anisotrópico. Além disso, a menos de isometria, V_t, V_h, V_a são unicamente determinados.

Demonstração: *Existência*: Seja $V_0 \subseteq V$ um subespaço tal que

$$V \cong (\mathrm{rad}(V)) \oplus V_0 \cong \mathrm{rad}(V) \perp V_0.$$

Tomando $V_t := \mathrm{rad}(V)$ é fácil ver que V_t é totalmente isotrópico. Afirmamos que V_0 é regular. De fato, se $x \in \mathrm{rad}(V_0)$, então $x \in V_0$ e $B(x, v_0) = 0$, para todo $v_0 \in V_0$. Como $B(x, r) = 0$, para todo $r \in \mathrm{rad}(V)$, temos que $B(x, v) = 0$, para todo $v \in V$, ou seja, $x \in \mathrm{rad}(V)$. Como $\mathrm{rad}(V) \cap V_0 = \{0\}$, temos que $x = 0$ e assim $\mathrm{rad}(V_0) = \{0\}$, implicando que V_0 é regular. Se V_0 é isotrópico, então podemos escrever $V_0 \cong \mathbb{H} \perp V_1$. Se V_1 for isotrópico, então podemos escrever $V_1 \cong \mathbb{H} \perp V_2$. Como $\dim(V_0) < \infty$, então após um número finito r de decomposições temos que

$$V_0 \cong r\mathbb{H} \perp V_a,$$

com V_a um subespaço anisotrópico. Definamos $V_h := r\mathbb{H}$. Assim, V_h é espaço hiperbólico e obtemos $V \cong V_t \perp V_h \perp V_a$, provando a existência.

Unicidade: Suponha que (V, q) tenha outra decomposição de Witt, $V \cong V_t' \perp V_h' \perp V_a'$. Afirmamos que $V_h' \perp V_a'$ é regular. De fato, como V_h' é hiperbólico e V_a' é anisotrópico, então $\det(q|_{V_h' \perp V_a'}) = (-1)^{\frac{\dim(V_h')}{2}} \cdot \det(V_a') \neq 0$. Como V_t' é totalmente isotrópico e $V_h' \perp V_a'$ é regular, então

$$\begin{aligned} \mathrm{rad}(V) &= \mathrm{rad}(V_t' \perp V_h' \perp V_a') \\ &= \mathrm{rad}(V_t') \perp \mathrm{rad}(V_h' \perp V_a') \\ &= \mathrm{rad}(V_t') \perp \{0\} = V_t'. \end{aligned}$$

Implicando que $V_t' = V_t$. Daí $V_t \perp V_h \perp V_a \cong V_t \perp V_h' \perp V_a'$. Pelo Teorema do Cancelamento de Witt 1.60 temos que $V_h \perp V_a \cong V_h' \perp V_a'$. Escrevendo $V_h \cong m\mathbb{H}$ e $V_h' \cong m'\mathbb{H}$, temos que $m\mathbb{H} \perp V_h' \cong m'\mathbb{H} \perp V_a'$. Aplicando o Teorema do Cancelamento de Witt 1.60, concluímos que $m = m'$ e assim $V_h \cong V_h'$. Aplicando novamente o Cancelamento de Witt 1.60 em $V_h \perp V_a \cong V_h \perp V_a'$, temos que $V_a \cong V_a'$ provando a unicidade. □

Definição 1.62. Seja (V, q) um F-espaço quadrático. O número inteiro $m = \frac{1}{2}\dim(V_h)$, unicamente determinado na decomposição de Witt, é chamado de *índice de Witt* do espaço quadrático (V, q). A classe de isometria V_a é chamada de *parte anisotrópica* de (V, q).

Corolário 1.63. *Se (V, q) é regular, o índice de Witt m de V é igual a dimensão de qualquer subespaço totalmente isotrópico maximal de V.*

Demonstração: Seja $U \subset V$ um subespaço totalmente isotrópico maximal com $\dim(U) = r$. Pelo Teorema 1.47 existe um espaço hiperbólico $T \supseteq U$ tal que $\dim(T) = 2r$. Como T é regular, então pelo Corolário 1.41 temos que $V \cong T \perp T^{\perp}$. Afirmamos que $T^{\perp}$ é anisotrópico. De fato, se $0 \neq v \in T^{\perp}$ é um vetor isotrópico, então $U \oplus F.v \subset V$ é totalmente isotrópico, o que contradiz a maximalidade de U. Como $T \perp T^{\perp}$ é uma decomposição de V e $T^{\perp}$ é a parte anisotrópica, então pelo Teorema da Decomposição de Witt temos que $T \cong V_h$. Assim $m = \frac{1}{2}\dim(V_h) = r = \dim(U)$. □

1.5 Teorema da Equivalência por Cadeia de Witt

O teorema descrito no título dessa seção descreve a equivalência de duas formas quadráticas diagonais em termos da equivalência de formas diagonais binárias, ou seja, formas diagonais bidimensionais. Primeiro, iremos provar um fato sobre formas binárias.

Proposição 1.64. *Sejam $q \cong \langle a, b\rangle$ e $q' = \langle c, d\rangle$ F-formas quadráticas binárias regulares. Então $q \cong q'$ se, e somente se, $d(q) = d(q')$ e q, q' representam um elemento em comum $\alpha \in \dot{F}$.*

Demonstração: Suponha que $q \cong q'$. Pela Proposição 1.44, $d(q) = d(q')$ e, pelo Lema 1.27, $D(q) = D(q')$. Como q e q' são regulares, então $D(q) \neq \emptyset$, implicando que existe $\alpha \in D(q) \cap D(q')$.

Reciprocamente, suponha que $d(q) = d(q')$ e exista $\alpha \in D(q) \cap D(q')$. Pelo Critério de Representação 1.37 temos que $q \cong \langle \alpha, \alpha'\rangle$, para algum $\alpha' \in \dot{F}$. Então $d(q) = ab\dot{F}^2 = \alpha\alpha'\dot{F}^2$. Segue que

$$\begin{array}{rcl} ab\dot{F}^2 = \alpha\alpha'\dot{F}^2 & \Leftrightarrow & \alpha^{-1}ab\dot{F}^2 = \alpha^{-1}\alpha\alpha'\dot{F}^2 \\ & \Leftrightarrow & \alpha^{-1}ab\alpha^2\dot{F}^2 = \alpha'\dot{F}^2 \\ & \Leftrightarrow & ab\alpha\dot{F}^2 = \alpha'\dot{F}^2. \end{array}$$

Assim, $q \cong \langle \alpha, ab\alpha\rangle$. De maneira análoga temos que $q' \cong \langle \alpha, cd\alpha\rangle$. Como $ab\dot{F}^2 = cd\dot{F}^2$, temos que $\langle \alpha, ab\alpha\rangle \cong \langle \alpha, cd\alpha\rangle$. Portanto $q \cong q'$, como desejado. □

Definição 1.65. Sejam $q \cong \langle a_1, \ldots, a_n\rangle$ e $q' \cong \langle b_1, \ldots, b_n\rangle$ F-formas quadráticas. Dizemos que q e q' são *simplesmente equivalentes*, se existem índices i, j tais que
(1) $\langle a_i, a_j\rangle \cong \langle b_i, b_j\rangle$, e
(2) $a_k = b_k$, sempre que $k \neq i$ ou $k \neq j$.
Note que se duas formas quadráticas f e g são simplesmente equivalentes, então f e g são isométricas. Também podemos notar que simplesmente equivalente não é uma relação de equivalência, para evidenciar isso tome $f = \langle 1, 1, 1, 1, 1, 1\rangle$, $g = \langle 1, 1, 1, 1, a, a\rangle$ e $h = \langle 1, 1, a, a, a, a\rangle$, temos que f, g e g, h são simplesmente equivalentes, mas f, h não são simplesmente equivalentes.

Definição 1.66. Dizemos que duas F-formas diagonais f e g são *equivalentes por cadeia*, se existe uma sequência de formas diagonais $\{f_0, f_1, \ldots, f_m\}$ tal que $f_0 = f$, $f_m = g$ e cada f_i é simplesmente equivalente a f_{i+1}, com $i = 1, \ldots, m-1$. É fácil mostrar que a equivalência por cadeia é uma relação de equivalência no conjunto de todas as formas diagonais de mesma dimensão. Denotaremos pelo símbolo $\approx$ a equivalência por cadeia.

Lema 1.67. *Sejam f, g F-formas quadráticas de mesma dimensão. Se $f \approx g$, então $f \cong g$.*

Demonstração: Se $f \approx g$, então existe uma sequência de F-formas quadráticas $\{f_0, f_1, \ldots, f_m\}$, tais que $f_0 = f$, $f_m = g$, $m > 1$ e f_i é simplesmente equivalente com f_{i+1}. Pela Definição 1.65 temos que $f_i \cong f_{i+1}$, para $i = 1, \ldots, m-1$. Pela transitividade de $\cong$, temos que $f \cong g$. □

Lema 1.68. *Sejam $f = \langle a_1, \ldots, a_n \rangle$, $\sigma \in S_n$ uma permutação de índices e $f^\sigma \cong \langle a_{\sigma(1)}, \ldots, a_{\sigma(n)} \rangle$. Então $f \approx f^\sigma$.*

Demonstração: Como $\sigma \in S_n$, temos que σ pode ser decomposta como o produto de transposições. Sejam $\tau_1, \ldots, \tau_m$ transposições e $\sigma = \tau_m \cdots \tau_1$. Como τ_1 é uma transposição, então f é simplesmente equivalente a f^{τ_1}, pois se $\tau_1 = (i, j)$, então

$$f^{\tau_1} = \langle a_{\tau_1(1)}, a_{\tau_1(2)}, \ldots, a_{\tau_1(i)}, \ldots, a_{\tau_1(j)}, \ldots, a_{\tau_1(n)} \rangle,$$

com $\langle a_{\tau_1(i)}, a_{\tau_1(j)} \rangle = \langle a_j, a_i \rangle \cong \langle a_i, a_j \rangle$ e $a_k = a_{\tau_1(k)}$, para $k \neq i, j$. Analogamente f^{τ_1} é simplesmente equivalente a $f^{\tau_2 \tau_1}$. Após m passos temos que $f^{\tau_{m-1} \cdots \tau_1}$ é simplesmente equivalente a f^σ. Portanto f é equivalente por cadeia a f^σ. □

Teorema 1.69 (Equivalência por Cadeia). *Sejam f, g são F-formas diagonais de mesma dimensão, então $f \cong g$ se, e somente se, $f \approx g$.*

Demonstração: Tomemos $f = \langle a_1, \ldots, a_n \rangle$ e $g = \langle b_1, \ldots, b_n \rangle$. Já provamos que $f \approx g$ implica $f \cong g$ no Lema 1.67. Assim basta provarmos a outra implicação. Como $f \cong g$, as duas formas tem o mesmo número de zeros na sua diagonalização, assim, pelo Teorema do Cancelamento de Witt 1.60, podemos assumir que f, g são regulares, isto é, $a_i, b_j \neq 0$, para todos $i, j = 1, \ldots, n$. Provaremos por indução sobre $n = \dim(f)$. Se $n = 1$, temos que $f \cong \langle a_1 \rangle$ e $g \cong \langle b_1 \rangle$. Como $\langle a_1 \rangle \cong \langle b_1 \rangle$ e não existem a_k e b_k com $k \neq 1$, então f é simplesmente equivalente a g e portanto $f \approx g$. Se $n = 2$, então $f \cong \langle a_1, a_2 \rangle$ e $g \cong \langle b_1, b_2 \rangle$. Como $f \cong g$, temos que $\langle a_1, a_2 \rangle \cong \langle b_1, b_2 \rangle$. Como não existem a_k e b_k com $k \neq 1, 2$, então f é simplesmente equivalente a g e portanto $f \approx g$.

Vamos assumir $n \geqslant 3$ e que esse teorema seja válido para $n-1$. De todas as formas diagonais equivalentes por cadeia a f, escolhemos $f' \cong \langle c_1, \ldots, c_n \rangle$ tal que $\langle c_1, \ldots, c_p \rangle$ representa b_1 e p é o menor índice possível com essa propriedade. Essa f' existe, pois como $f \cong g$, então $b_1 \in D(f)$ e, na pior das hipóteses, tomamos $f' = f$ e $p = n$. Queremos mostrar que $p = 1$. Suponha que $p \geq 2$. Como $b_1 \in D(\langle c_1, \ldots, c_p \rangle)$, então existe um vetor não nulo $(e_1, \ldots e_p, 0, \ldots, 0)$ tal que

$$b_1 = \sum_{i=1}^{p} c_i e_i^2 + \sum_{j=p+1}^{n} c_j 0^2 = \sum_{i=1}^{p} c_i e_i^2.$$

Pela minimalidade de p, nenhuma subsoma desta somatória pode ser nula. Em particular $\beta = c_1e_1^2 + c_2e_2^2 \neq 0$. Como na demonstração da Proposição 1.64 obtemos que $\langle c_1, c_2\rangle \cong \langle \beta, c_1c_2\beta\rangle$. Assim,

$$\begin{array}{rcccl} f & \approx & f' & = & \langle c_1, c_2, c_3 \ldots, c_n\rangle \\ & & & \approx & \langle \beta, c_1c_2\beta, c_3, \ldots, c_n\rangle \\ & & & \approx & \langle \beta, c_3, \ldots, c_n, c_1c_2\beta\rangle \end{array}$$

e $b_1 = \beta + c_3e_3^2 + \cdots + c_pe_p^2$. Então $b_1 \in D(\langle \beta, c_3, \ldots, c_p\rangle)$, o que é um absurdo, pois $\dim(\langle \beta, c_3, \ldots, c_p\rangle)) = p - 1$, contrariando a minimalidade de p. Logo $p = 1$ e temos que $\langle c_1\rangle \cong \langle b_1\rangle$. Segue que $f \approx \langle b_1, c_2, \ldots, c_n\rangle$ e assim $\langle b_1, c_2, \ldots, c_n\rangle \cong \langle b_1, b_2, \ldots, b_n\rangle$. Pelo Teorema do Cancelamento de Witt 1.60 temos que $\langle c_2, \ldots, c_n\rangle \cong \langle b_2, \ldots, b_n\rangle$. Pela hipótese de indução, temos que $\langle c_2, \ldots, c_n\rangle \approx \langle b_2, \ldots, b_n\rangle$. Logo, $f \approx \langle b_1, c_2, \ldots, c_n\rangle \approx \langle b_1, b_2, \ldots, b_n\rangle = g$. □

1.6 Produto de Kronecker de Espaços Quadráticos

Nessa seção iremos definir um produto entre espaços quadráticos, que terá por base o produto tensorial entre espaços vetoriais. Consideraremos conhecido o conceito de produto tensorial e indicamos [Bha] como referência.

Definição 1.70. Sejam (V_1, B_1, q_1) e (V_2, B_2, q_2) dois F-espaços quadráticos de dimensão m e n, respectivamente. Tomemos um novo espaço vetorial $V := V_1 \otimes V_2$ ($\otimes_F = \otimes$), ou seja, o produto tensorial sobre F dos espaços vetoriais V_1 e V_2. Considere $B : V \times V \longrightarrow F$ a única aplicação bilinear simétrica tal que

$$B(v_1 \otimes v_2, v_1' \otimes v_2') = B_1(v_1, v_1') \cdot B_2(v_2, v_2'), \text{ onde } v_i, v_i' \in V_i.$$

O par (V, B) é um F-espaço quadrático de dimensão $m \cdot n$, chamado de *produto de Kronecker (ou produto tensorial)* de (V_1, B_1) e (V_2, B_2). A função quadrática $q = q_B$ associada a (V, B) satisfaz, para $v_i \in V_i$,

$$q(v_1 \otimes v_2) \;\; = \;\; B(v_1 \otimes v_2, v_1 \otimes v_2) = B_1(v_1, v_1) \cdot B_2(v_2, v_2) = q_1(v_1) \cdot q_2(v_2).$$

Denotaremos q por $q_1 \otimes q_2$ ou as vezes apenas por q_1q_2.

Como espaços quadráticos são espaços vetoriais de dimensão finita, então podemos diagonaliza-los. Assim, veremos adiante o que ocorre com o produto de Kronecker entre dois espaços diagonalizados.

Sejam (V_1, B_1) e (V_2, B_2) dois F-espaços quadráticos, com $\dim(V_1) = m$ e $\dim(V_2) = n$. Sejam $\{e_1, \ldots, e_m\}$ e $\{f_1, \ldots, f_n\}$ bases ordenadas fixadas de V_1 e V_2, respectivamente. Definindo $a_{ij} := B_1(e_i, e_j)$ e $b_{ij} := B_2(f_i, f_j)$, então $M = [a_{ij}]_m$ e $N = [b_{ij}]_n$ são matrizes simétricas associadas a q_1 e q_2 nas bases fixadas, respectivamente. Tomemos o produto de Kronecker $V = V_1 \otimes V_2$ e $q = q_1 \cdot q_2$. Pela teoria de produto tensorial, temos que o conjunto

$$\beta = \{e_1 \otimes f_1, \ldots, e_1 \otimes f_n, \ldots, e_m \otimes f_1, \ldots, e_m \otimes f_n\}$$

é uma base ordenada de V. A matriz simétrica associada a q na base β é dada por

$$\begin{bmatrix} a_{11}b_{11} & a_{11}b_{12} & \cdots & a_{12}b_{11} & a_{12}b_{12} & \cdots & \cdots \\ a_{11}b_{21} & a_{11}b_{22} & \cdots & a_{12}b_{21} & a_{12}b_{22} & \cdots & \cdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \cdots \\ a_{21}b_{11} & a_{21}b_{12} & \cdots & a_{22}b_{11} & a_{22}b_{12} & \cdots & \cdots \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \end{bmatrix} = \begin{bmatrix} a_{11}\cdot N & a_{12}\cdot N & \cdots & a_{1m}\cdot N \\ a_{21}\cdot N & a_{22}\cdot N & \cdots & a_{2m}\cdot N \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}\cdot N & a_{m2}\cdot N & \cdots & a_{mm}\cdot N \end{bmatrix}$$

que é precisamente o produto de Kronecker das matrizes M e N.

Proposição 1.71. *Se $a, b \in F$, então $\langle a\rangle \otimes \langle b\rangle \cong \langle ab\rangle$.*

Demonstração: Como $\langle a\rangle$ está associada ao espaço (F, ax^2) e $\langle b\rangle$ está associada ao espaço (F, bx^2), então suas respectivas matrizes simétricas associadas são $[a]$ e $[b]$. Pelo produto de Kronecker de duas matrizes temos que $[a]\otimes[b] = [ab]$. Implicando que $[ab]$ é uma matriz simétrica associada a $\langle a\rangle \otimes \langle b\rangle$. Portanto $\langle a\rangle \otimes \langle b\rangle \cong \langle ab\rangle$. □

O produto de Kronecker visto como operação de formas quadráticas satisfaz as usuais comutatividade, associatividade, existência de elemento neutro e distributividade em relação a soma ortogonal, o que veremos no seguinte teorema.

Teorema 1.72. *Sejam q, q_1, q_2 e q_3 F-formas quadráticas. Então:*
(1) $q_1 \otimes q_2 \cong q_2 \otimes q_1$;
(2) $(q_1 \otimes q_2) \otimes q_3 \cong q_1 \otimes (q_2 \otimes q_3)$;
(3) $\langle 1\rangle \otimes q \cong q \otimes \langle 1\rangle \cong q$;
(4) $q \otimes (q_1 \perp q_2) \cong (q \otimes q_1) \perp (q \otimes q_2)$.

Demonstração: Estas propriedades seguem basicamente das propriedades do produto tensorial. Provaremos apenas o item (4), os demais casos são análogos. Seja $q\otimes(q_1 \perp q_2)$. Tomemos (V, q), (V_1, q_1), (V_2, q_2) F-espaços quadráticos associados a q, q_1, q_2, respectivamente. Da teoria de produto tensorial, temos que $V \otimes (V_1 \oplus V_2) \cong V \otimes V_1 \oplus V \otimes V_2$ (isomorfismo de espaços vetoriais) e assim $v \otimes (v_1, v_2) = (v \otimes v_1, v \otimes v_2)$. Agora, pela Definição 1.70 e pela Observação 1.33 temos que

$$\begin{aligned} q \otimes (q_1 \perp q_2)(v \otimes (v_1, v_2)) &= q(v) \cdot (q_1 \perp q_2)(v_1, v_2) \\ &= q(v)(q_1(v_1) + q_2(v_2)) \\ &= q(v) \cdot q_1(v_1) + q(v) \cdot q_2(v_2) \\ &= q \otimes q_1(v \otimes v_1) + q \otimes q_2(v \otimes v_2), \quad \text{para } v \in V \text{ e } v_i \in V_i, \end{aligned}$$

como desejado. □

Os seguintes corolários nos apresentam uma forma muito eficiente de calcular o produto de Kronecker entre duas formas quadráticas diagonais.

Corolário 1.73. *Sejam $q = \langle a_1, \ldots, a_n\rangle$ e $q' = \langle b_1, \ldots, b_m\rangle$ duas F-formas quadráticas diagonais. Então*

$$\langle a_1, \ldots, a_n\rangle \otimes \langle b_1, \ldots, b_m\rangle \cong \langle a_1b_1, \ldots, a_ib_j, \ldots, a_nb_m\rangle.$$

Demonstração: Seja $q \otimes q'$. Pelo Teorema 1.72 item (4) e pela Proposição 1.71 temos que

$$\begin{aligned} q \otimes q' &= \langle a_1, \ldots, a_n \rangle \otimes \langle b_1, \ldots, b_m \rangle \\ &\cong (\langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle) \otimes \langle b_1 \rangle \perp \cdots \perp (\langle a_1 \rangle \perp \cdots \perp \langle a_n \rangle) \otimes \langle b_m \rangle \\ &\cong \langle a_1 b_1 \rangle \perp \cdots \perp \langle a_1 b_m \rangle \perp \cdots \perp \langle a_n b_1 \rangle \perp \cdots \langle a_n b_m \rangle \\ &= \langle a_1 b_1, \ldots, a_i b_j, \ldots, a_n b_m \ldots \rangle. \end{aligned}$$

Portanto $q \otimes q' \cong \langle a_1 b_1, \ldots, a_i b_j, \ldots, a_n b_m \rangle$. □

Notação 1.74. Se $r \in \mathbb{Z}_+^*$ e q é uma F-forma quadrática, então denotaremos $r \cdot q$ (ou simplesmente rq) para a soma ortogonal de q r-vezes, ou seja, $r \cdot q = q \perp \cdots \perp q$ (r vezes).

Corolário 1.75. *Se q é uma F-forma quadrática regular, então $q \otimes \mathbb{H} \cong \dim(q) \cdot \mathbb{H}$.*

Demonstração: Pelo Corolário 1.38 temos que existem elementos $a_1, \ldots, a_n$ de F, tais que $q \cong \langle a_1, \ldots, a_n \rangle$ e $a_i \neq 0$, para $i = 1, \ldots, n$. Provaremos por indução sobre n. Se $n = 1$, então $q \cong \langle a_1 \rangle$ e assim

$$q \otimes \mathbb{H} = \langle a_1 \rangle \otimes \langle 1, -1 \rangle \cong \langle a_1 \rangle \otimes \langle 1 \rangle \perp \langle a_1 \rangle \otimes \langle -1 \rangle \cong \langle a_1, -a_1 \rangle = 1 \cdot \mathbb{H}.$$

Provando que $q \otimes \mathbb{H} \cong \dim(q) \cdot \mathbb{H}$, para o caso $n = 1$. Suponha que esse resultado é válido para $n - 1$. Seja $q = \langle a_1, \ldots, a_n \rangle$. Assim

$$q \otimes \mathbb{H} = (\langle a_1, \ldots, a_{n-1} \rangle \perp \langle a_n \rangle) \otimes \mathbb{H}.$$

Pelo Teorema 1.72 item (4) temos que $q \otimes \mathbb{H} \cong \langle a_1, \ldots, a_{n-1} \rangle \otimes \mathbb{H} \perp \langle a_n \rangle \otimes \mathbb{H}$. Pela hipótese de indução e do caso $n = 1$, temos que $q \otimes \mathbb{H} \cong (\dim(q) - 1) \cdot \mathbb{H} \perp \mathbb{H}$. Logo $q \otimes \mathbb{H} \cong \dim(q) \cdot \mathbb{H}$. □

Capítulo 2

Introdução aos Anéis de Witt

Nesse capítulo faremos uma breve introdução ao anel de Witt e anel de Witt-Grothendieck e suas propriedades. Sem dúvidas esses são uns dos mais importantes anéis na área de formas quadráticas sobre corpos.

2.1 Definição de $\widehat{W}(F)$ e $W(F)$

Nessa seção faremos a construção dos anéis de Witt-Grothendieck e Witt. Para isso, primeiramente precisamos de alguns resultados.

Definição 2.1. Definimos como $M(F)$ o conjunto de todas as classes de isometria (regulares) de formas quadráticas sobre o corpo F.

Relembramos que um semi-anel é uma estrutura algébrica semelhante à um anel, porém sem a necessidade de existir um inverso aditivo para todos os elementos dessa estrutura, analogamente um monóide é uma estrutura algébrica com uma operação que satisfaz apenas as propriedades associativa e a existência do elemento neutro. Podemos ver $\perp$ e $\otimes$ como operações em $M(F)$, e temos o seguinte resultado.

Lema 2.2. *O conjunto $M(F)$, munido das operações $\perp$ e $\otimes$, é um semi-anel comutativo, onde $\perp$ é a soma ortogonal e $\otimes$ é o produto de Kronecker de F-formas quadráticas.*

Demonstração: Sejam $f, q, g \in M(F)$. Sejam $\langle a_1, \ldots, a_n\rangle$, $\langle b_1, \ldots, b_m\rangle$ e $\langle c_1, \ldots, c_k\rangle$ as formas diagonais de f,q e g, respectivamente. Pela definição de soma ortogonal e do Teorema da Equivalência por Cadeia 1.69, é fácil mostrar que $\perp$ é uma operação associativa, comutativa e admite o elemento neutro. Pelo Cancelamento de Witt 1.60, temos que $(M(F), \perp)$ é um monóide com cancelamento. Pelo Teorema 1.72 temos que $(M(F), \otimes)$ é um monóide comutativo. Logo $(M(F), \perp, \otimes)$ é um semi-anel comutativo com cancelamento. □

Lema 2.3. *A relação $\sim$ em $M(F) \times M(F)$ dada por*

$$(f, q) \sim (f', q') \text{ se, e somente se, } f \perp q' \cong f' \perp q,$$

é uma relação de equivalência.

Demonstração: Sejam $(f, q), (f', q'), (f'', q'') \in M(F) \times M(F)$. Assim, como $f \perp q \cong f \perp q$, temos que $\sim$ é reflexiva. Se $(f, q) \sim (f', q')$, então $f \perp q' \cong f' \perp q$. Como $\cong$ é uma

relação de equivalência, então $f' \perp q \cong f \perp q'$, provando que $\sim$ é simétrica. Suponha que $(f,q) \sim (f',q')$ e $(f',q') \sim (f'',q'')$, isso implica que $f \perp q' \cong f' \perp q$ e $f' \perp q'' \cong f'' \perp q'$. Pela comutatividade de soma ortogonal, temos que $f \perp q' \perp q'' \cong f' \perp q'' \perp q$ e $f' \perp q'' \perp q \cong f'' \perp q' \perp q$. Assim, $f \perp q' \perp q'' \cong f'' \perp q' \perp q$. Pelo Cancelamento de Witt 1.60, temos que $f \perp q'' \cong f'' \perp q$. Logo $(f,q) \sim (f'',q'')$ e portanto $\sim$ é uma relação de equivalência. □

Dado o semi-anel $M(F)$ e a relação de equivalência $\sim$ podemos construir um novo conjunto Groth(M(F)) $= M(F) \times M(F)/\sim$. A classe de equivalência de (f,q) em Groth(M(F)) denotaremos também por (f,q).

Proposição 2.4. *O Conjunto* Groth(M(F)) $= M(F) \times M(F)/\sim$ *munido das operações*

$$(f,q) + (f',q') = (f \perp f', q \perp q') \text{ e}$$

$$(f,q) \cdot (f',q') = (f \otimes f' \perp q \otimes q', q \otimes f' \perp f \otimes q'),$$

é um anel comutativo.

Demonstração: Primeiramente provemos que $+$ está bem definida. De fato, se $(f,q) \sim (f',q')$ e $(f'',q'') \sim (f''',q''')$, então $f \perp q' \cong f' \perp q$ e $f'' \perp q''' \cong f''' \perp q''$. Pela comutatividade da soma ortogonal temos que

$$(f \perp f'') \perp (q' \perp q''') \cong (f' \perp f''') \perp (q \perp q'').$$

Implicando que $(f \perp f'', q \perp q'') \sim (f' \perp f''', q' \perp q''')$. Logo $(f,q) + (f'',q'') = (f',q') + (f''',q''')$, portanto $+$ está bem definida. O fato de $+$ ser comutativa e associativa decorre diretamente do comutatividade e associatividade da soma ortogonal. Tomando o elemento (g,g) com $g \in M(F)$, vemos que $(f,q) + (g,g) = (f,q)$, para todo $(f,q) \in$ Groth(M(F)). De fato, como $(f,q) + (g,g) = (f \perp g, q \perp g)$ e pelo fato que $(f \perp g) \perp q \cong f \perp (q \perp g)$, então $(f \perp g, q \perp g) \sim (f,q)$ e assim $(f,q) + (g,g) = (f,q)$, ou seja, $(g,g) = 0_{\text{Groth(M(F))}}$. Se tomarmos (f,q), note que $(f,q) + (q,f) = (f \perp q, f \perp q) = 0_{\text{Groth(M(F))}}$. Provando que (Groth(M(F)), $+$) é um grupo abeliano.

Agora provaremos que $(\cdot)$ está bem definida e satisfaz as propriedades: associatividade, comutatividade, distributiva em relação a adição e existência do elemento neutro. De fato, tomando $(f,q) \sim (f',q')$ e $(f'',q'') \sim (f''',q''')$, temos que $f \perp q' \cong f' \perp q$ e $f'' \perp q''' \cong f''' \perp q''$. Multiplicando a primeira congruência por f'', q'', f''' e q''', somando essas novas congruências e pelo Cancelamento de Witt 1.60, obtemos

$$(f \otimes f'' \perp q \otimes q'') \perp (q' \otimes f''' \perp f' \otimes q''') \cong (f' \otimes f''' \perp q' \otimes q''') \perp (q \otimes f'' \perp f \otimes q'').$$

Implicando que $(f,q) \cdot (f'',q'') = (f',q') \cdot (f''',q''')$. A associatividade e a comutatividade de $(\cdot)$ seguem do fato que $(\perp)$ e $(\otimes)$ são associativas e comutativas em $M(F)$, conforme Teorema 1.72. Para a existência do elemento neutro, considere a classe $(\langle 1\rangle, 0_{M(F)}) \in$ Groth(M(F)), assim

$$(f,q) \cdot (\langle 1\rangle, 0_{M(F)}) = (f \otimes \langle 1\rangle \perp q \otimes 0_{M(F)}, q \otimes \langle 1\rangle \perp f \otimes 0_{M(F)}) = (f,q).$$

Analogamente, $(\langle 1\rangle, 0_{M(F)}) \cdot (f,q) = (f,q)$. A propriedade distributiva de $(\cdot)$ em relação a $(+)$ em Groth(M(F)) decorre do fato da $(\otimes)$ ser distributiva em relação a $(\perp)$, conforme Teorema 1.72. Portanto (Groth(M(F)), $+, \cdot$) é um anel comutativo. □

Note que pela forma como Groth$(M(F))$ foi construído ele é único, a menos de isomorfismo.

Definição 2.5. O anel comutativo Groth(M(F)) será chamado de *anel de Witt-Grothendieck* de formas quadráticas sobre o corpo F e será denotado por $\widehat{W}(F)$.

Note que se definirmos a função $i : M(F) \longrightarrow \widehat{W}(F)$ dada por $i(q) = (q, 0_{M(F)})$, então i é um morfismo injetor e pode ser visto como a inclusão $M(F) \subseteq \widehat{W}(F)$.

Como $(f, q) = i(f) - i(q)$, então $\widehat{W}(F)$ é gerado por $M(F)$. Assim todo elemento (f, q) de $\widehat{W}(F)$ tem uma expressão formal $f-q$, onde f, q são formas quadráticas regulares, ou melhor, classes de isometrias dessas formas quadráticas. Isso segue do seguinte lema.

Lema 2.6. *Sejam f e q duas formas quadráticas regulares, então $f = q$ em $\widehat{W}(F)$ se, e somente se, $f \cong q \in M(F)$.*

Demonstração: Suponha que $f = q \in \widehat{W}(F)$. Pela construção de $\widehat{W}(F)$ temos que $(f, 0) = (q, 0)$. Implicando que $f \cong q \in M(F)$. Reciprocamente, se $f \cong q$, então $f \perp 0_{M(F)} \cong q \perp 0_{M(F)}$. Assim $(f, 0) = (q, 0)$, ou seja, $f = q$ em $\widehat{W}(F)$. □

A seguir definiremos um ideal importante de $\widehat{W}(F)$ e veremos alguns resultados envolvendo o mesmo.

Como toda forma quadrática regular em $M(F)$ tem como dimensão um n^{o} inteiro positivo, podemos definir a função $\dim : M(F) \longrightarrow \mathbb{Z}$, por $q \mapsto \dim(q)$. É fácil provar que essa função é um homomorfismo de semi-anéis. Pela propriedade universal da construção do $\widehat{W}(F)$, podemos estender este homomorfismo e obter

$$\begin{array}{rccl} \dim : & \widehat{W}(F) & \longrightarrow & \mathbb{Z} \\ & f - q & \longrightarrow & \dim(f) - \dim(q), \end{array}$$

que é um homomorfismo de anéis.

Definição 2.7. O núcleo do homomorfismo de anéis dim é um ideal de $\widehat{W}(F)$ que será denotado por $\widehat{I}F$ e chamado de *ideal fundamental de $\widehat{W}(F)$*.

Lema 2.8. *Seja $\widehat{I}F$ o ideal fundamental de $\widehat{W}(F)$. Então $\frac{\widehat{W}(F)}{\widehat{I}F} \cong \mathbb{Z}$*

Demonstração: Para mostrarmos esse resultado basta verificar que $\dim : \widehat{W}(F) \longrightarrow \mathbb{Z}$ é sobrejetora, pois o 1^{o} Teorema dos Isomorfismos nos garante o resultado. De fato, seja $z \in \mathbb{Z}$. Caso $z > 0$, basta tomar um elemento $q - 0_{M(F)} \in \widehat{W}(F)$, com $\dim(q) = z$. Implicando que $\dim(q - 0_{M(F)}) = z - 0 = z$. Para o caso em que $z < 0$, basta tomar $0_{M(F)} - q$. Por último, se $z = 0$, tomemos $\langle 1\rangle - \langle 1\rangle \in \widehat{W}(F)$, implicando em $\dim(\langle 1\rangle - \langle 1\rangle) = 1 - 1 = 0$. Portanto dim é um epimorfismo de anéis. □

Note que como $\widehat{I}F$ é o núcleo do epimorfismo dim, então $\dim(\widehat{I}F) = 0$, ou seja todo elemento de $\widehat{I}F$ tem dimensão nula. Implicando que se $f-q \in \widehat{I}F$, então $\dim(f) = \dim(q)$.

Proposição 2.9. *Seja $\widehat{W}(F)$ o anel de Witt-Grothendieck associado ao corpo F. Então o ideal $\widehat{I}F$ é gerado aditivamente por elementos da forma $\langle a\rangle - \langle 1\rangle$, onde $a \in \dot{F}$.*

Demonstração: Seja $g \in \widehat{I}F$. Como $g \in \widehat{W}(F)$, então existem $f, q \in M(F)$, tais que $g = f - q$ e $\dim(f) = \dim(q)$. Tomando as formas diagonais de f e q temos que $f = \langle a_1, \ldots, a_n\rangle$ e $q = \langle b_1, \ldots, b_n\rangle$, com $a_i, b_i \neq 0$. Então

$$\begin{aligned} f - q &= \langle a_1, \ldots, a_n\rangle - \langle b_1, \ldots, b_n\rangle \\ &= (\langle a_1\rangle + \cdots + \langle a_n\rangle) - (\langle b_1\rangle + \cdots + \langle b_n\rangle) \\ &= (\langle a_1\rangle + \cdots + \langle a_n\rangle) - (\langle b_1\rangle + \cdots + \langle b_n\rangle) + 0_{\widehat{W}(F)} \\ &= (\langle a_1\rangle + \cdots + \langle a_n\rangle - \langle 1\rangle + \cdots + \langle 1\rangle) + (\langle 1\rangle + \cdots + \langle 1\rangle - \langle b_1\rangle + \cdots + \langle b_n\rangle) \\ &= \textstyle\sum_{i=1}^{n}\langle a_i\rangle - \langle 1\rangle + \sum_{j=1}^{n}\langle 1\rangle - \langle b_j\rangle \\ &= \textstyle\sum_{i=1}^{n}\langle a_i\rangle - \langle 1\rangle - \sum_{j=1}^{n}\langle b_j\rangle - \langle 1\rangle. \end{aligned}$$

Portanto $\widehat{I}F$ é gerado aditivamente por elementos da forma $\langle a\rangle - \langle 1\rangle$, com $a \in \dot{F}$. □

Até agora provamos alguns resultados importantes sobre $\widehat{I}F$, um desses nos dá informação sobre o anel quociente de $\widehat{W}(F)$ por $\widehat{I}F$, porém não conseguimos nada expressivo no quesito da variação do corpo F, pois $\frac{\widehat{W}(F)}{\widehat{I}F} \cong \mathbb{Z}$, que é invariante pela mudança de F. Assim, nos próximos resultados buscaremos um novo ideal de Witt-Grothendieck que possamos obter mais informações de anéis quocientes de $\widehat{W}(F)$.

Definição 2.10. Seja $\widehat{W}(F)$ o anel de Witt-Grothendieck associado a F. Definimos por $\mathbb{Z}\mathbb{H}$, o subconjunto de $\widehat{W}(F)$ que consiste de todos os espaços hiperbólicos e seus "inversos aditivos".

Proposição 2.11. *$\mathbb{Z}\mathbb{H}$ é um ideal de $\widehat{W}(F)$.*

Demonstração: Sejam $m\mathbb{H}$, $n\mathbb{H} \in \mathbb{Z}\mathbb{H}$. Se $m = n$, então

$$m\mathbb{H} - n\mathbb{H} = m\mathbb{H} - m\mathbb{H} = 0_{\widehat{W}(F)} = 0\mathbb{H} \in \mathbb{Z}\mathbb{H}.$$

Suponha que $m > n$. Caso $n \geqslant 0$, então

$$m\mathbb{H} - n\mathbb{H} = (m-n)\mathbb{H} + n\mathbb{H} - n\mathbb{H} = (m-n)\mathbb{H} + 0_{\widehat{W}(F)} = (m-n)\mathbb{H} \in \mathbb{Z}\mathbb{H}.$$

Caso $m \geqslant 0$ e $n < 0$, então temos que

$$m\mathbb{H} - n\mathbb{H} = m\mathbb{H} + (-n)\mathbb{H} = (m-n)\mathbb{H} \in \mathbb{Z}\mathbb{H}.$$

Caso $m \leqslant 0$, então

$$\begin{aligned} m\mathbb{H} - n\mathbb{H} &= (-n)\mathbb{H} - (-m)\mathbb{H} = (-n+m)\mathbb{H} + (-m)\mathbb{H} - (-m)\mathbb{H} \\ &= (m-n)\mathbb{H} \in \mathbb{Z}\mathbb{H}. \end{aligned}$$

Analogamente, se $m < n$, temos que $m\mathbb{H} - n\mathbb{H} \in \mathbb{Z}\mathbb{H}$. Logo $\mathbb{Z}\mathbb{H}$ é fechado para a diferença.

Seja $m\mathbb{H} \in \mathbb{Z}\mathbb{H}$ e $f - q \in \widehat{W}(F)$ com $\dim(f) = r$ e $\dim(q) = s$. Assim,

$$\begin{aligned} (f-q)\cdot m\mathbb{H} &= f \otimes m\mathbb{H} \perp q \otimes 0 - f \otimes 0 \perp m\mathbb{H} \otimes q \\ &= (rm)\mathbb{H} - (sm)\mathbb{H} \in \mathbb{Z}\mathbb{H}, \end{aligned}$$

na penúltima igualdade foi usado o Corolário 1.75. Portanto, $\mathbb{Z}\mathbb{H}$ é ideal de $\widehat{W}(F)$. □

Definição 2.12. O anel quociente $W(F) := \frac{\widehat{W}(F)}{\mathbb{ZH}}$ é chamado de *anel de Witt* associado ao corpo F.

Notemos que como $\widehat{W}(F)$ é comutativo, então $W(F)$ é um anel comutativo. Esse anel é um dos entes mais importantes no estudo de formas quadráticas sobre corpos, que teve sua primeira aparição em 1937 em um artigo de Witt ([**?**].

Recordemos que na Decomposição de Witt 1.61 temos que qualquer forma quadrática q pode ser escrita na forma $q \cong \text{rad}(q) \perp m\mathbb{H} \perp q_a$. Como para definir $M(F)$, tomamos apenas as formas quadráticas regulares, então $q \cong m\mathbb{H} \perp q_a$. Assim, tomando q em $W(F)$, temos que $q \cong q_a$, ou seja, em $W(F)$ estamos apenas interessados na parte anisotrópica de seus elementos. Formalmente essa observação segue na seguinte proposição.

Proposição 2.13. *Seja F um corpo e $W(F)$ o anel de Witt associado a F. Então:*

(1) *Os elementos de $W(F)$ estão em correspondência biunívoca com as classes de isometria de todas as formas quadráticas anisotrópicas;*

(2) *Duas F-formas quadráticas f e q representam o mesmo elemento em $W(F)$ se, e somente se, $f_a \cong q_a$;*

(3) *Sejam f e q duas F-formas quadráticas. Se $\dim(f) = \dim(q)$, então f, q representam o mesmo elemento em $W(F)$ se, e somente se, $f \cong q$.*

Demonstração: Primeiramente, notemos que como $\mathbb{H}$ representa o elemento $0_{W(F)}$, então $\langle a\rangle + \langle -a\rangle = \langle a, -a\rangle = 0_{W(F)}$, para todo $a \in \dot{F}$. Obtendo que $-\langle a\rangle = \langle -a\rangle$ em $W(F)$.

Afirmamos que todo elemento de $W(F)$ é representado por um elemento da seguinte forma $g = (g, 0) + \mathbb{ZH}$. De fato, seja $f - q + \mathbb{ZH} \in W(F)$, onde $f = \langle a_1, \ldots, a_n\rangle$ e $q = \langle b_1, \ldots, b_m\rangle$. Pelas propriedades de $\widehat{W}(F)$ e do fato que $-\langle a\rangle = \langle -a\rangle$ temos que

$$\begin{aligned} f - q + \mathbb{ZH} &= \langle a_1, \ldots, a_n\rangle - \langle b_1, \ldots, b_m\rangle + \mathbb{ZH} \\ &= \langle a_1, \ldots, a_n\rangle + \langle -b_1, \ldots, -b_m\rangle + \mathbb{ZH} \\ &= \langle a_1, \ldots, a_n, -b_1, \ldots, -b_m\rangle + \mathbb{ZH}. \end{aligned}$$

Separando as possíveis partes hiperbólicas em $\langle a_1, \ldots, a_n, -b_1, \ldots, -b_m\rangle$ pela Decomposição de Witt 1.61 temos que

$$f - q + \mathbb{ZH} = \langle c_1, \ldots, c_k\rangle + r \cdot \mathbb{H} + \mathbb{ZH} = \langle c_1, \ldots, c_k\rangle + \mathbb{ZH}.$$

Tomando $g = \langle c_1, \ldots, c_k\rangle$, obtemos que $f - q + \mathbb{ZH} = g + \mathbb{ZH}$, provando essa afirmação. E mais, note que pela Decomposição de Witt 1.61 temos que $\langle c_1, \ldots, c_k\rangle$ é anisotrópica e é fácil ver que $g + \mathbb{ZH} = g_h + g_a + \mathbb{ZH} = g_a + \mathbb{ZH}$, para todo $g \in M(F)$.

(1) Seja $M_a(F) \subseteq M(F)$ o conjunto das classes de equivalência das F-formas quadráticas anisotrópica mais o $0_{M(F)}$. Pelo que já provamos podemos definir a seguinte função

$$\begin{aligned} \phi : \ M_a(F) &\longrightarrow W(F) \\ q_a &\longrightarrow \phi(q_a) = (q_a, 0) + \mathbb{ZH}. \end{aligned}$$

A função ϕ está bem definida, pois dados $f_a \cong q_a$, temos que $(f_a, 0) = (q_a, 0)$. Tomando $f - q + \mathbb{ZH} \in W(F)$, pelo que já provamos temos que $f - q + \mathbb{ZH} = g + \mathbb{ZH}$. Como $g + \mathbb{ZH} = g_a + \mathbb{ZH}$, então temos que $\phi(g_a) = g + \mathbb{ZH}$, provando que ϕ é sobrejetora. Sejam

$f_a, q_a \in M_a(F)$, tais que $\phi(f_a) = \phi(q_a)$. Assim $f_a + \mathbb{Z}\mathbb{H} = q_a + \mathbb{Z}\mathbb{H}$. Isso implica que $f_a - q_a \in \mathbb{Z}\mathbb{H}$, ou seja, existe $m \in \mathbb{Z}$ tal que $f_a - q_a = m \cdot \mathbb{H}$. Segue que $f_a = q_a + m \cdot \mathbb{H}$. Como f_a e q_a são anisotrópicas, então $m = 0$ e disso $f_a = q_a \in \widehat{W}(F)$, ou seja $f_a \cong q_a$, provando que ϕ é injetora e consequentemente bijetora.

(2) Decorre diretamente de (1).

(3) Sejam $f, q \in M(F)$, tais que $\dim(f) = \dim(q)$. Se f, q representam o mesmo elemento em $W(F)$, então por (2) dessa proposição temos que $f_a \cong q_a$. Segue diretamente da Decomposição de Witt 1.61 que $f \cong q$. Reciprocamente, se $f \cong q$, então $f_a \cong q_a$ e, assim por (2) dessa proposição temos que f e q representam o mesmo elemento em $W(F)$. □

Definição 2.14. A imagem do ideal $\widehat{I}F$ de $\widehat{W}(F)$ sobre a projeção natural

$$\begin{array}{rccc} i: & \widehat{W}(F) & \longrightarrow & W(F) \\ & f - q & \longrightarrow & f - q + \mathbb{Z}\mathbb{H} \end{array}$$

é denotado por $i(\widehat{I}F) := IF$ e é chamado de *ideal fundamental* de $W(F)$.

Um fato interessante que podemos abordar sobre os dois ideais de $\widehat{W}(F)$ que definimos nessa seção é que sua interseção é nula, ou seja, $\mathbb{Z}\mathbb{H} \cap \widehat{I}F = \{0_{\widehat{W}(F)}\}$. Para mostrar essa afirmação, basta tomar $f - q$ nessa intersecção, por um lado $\dim(f) = \dim(q)$ e por outro lado $f - q = m \cdot \mathbb{H}$. Segue que $0 = \dim(f - q) = \dim(m \cdot \mathbb{H}) = 2m$, implicando que $m = 0$ e consequentemente $f - q = 0_{\widehat{W}(F)}$.

A próxima proposição nos dá uma forma de descobrir se uma F-forma quadrática f em $W(F)$ pertence a IF apenas observando sua dimensão.

Proposição 2.15. *Uma F-forma quadrática f representa um elemento em $IF \subseteq W(F)$ se, e somente se,* $\dim(f)$ *é par.*

Demonstração: Suponha que f representa um elemento em IF. Então existem formas quadráticas q, g, tais que $f = q - g + m\mathbb{H}$. Como $f \in i(\widehat{I}F) = IF$, então $\dim(q) = \dim(g)$. Assim,

$$\dim(f) \;=\; \dim(q - g + m\mathbb{H}) = \dim(m\mathbb{H}) = 2m.$$

Logo $\dim(f)$ é par.

Reciprocamente, suponha que $\dim(f) = 2k$, com $k \in \mathbb{N}$. Assim, tomando a forma diagonal de f temos que $f = \langle a_1, \ldots, a_k, b_1, \ldots, b_k\rangle$, onde $a_i, b_j \in \dot{F}$. Pela Proposição 2.13 temos que $f = \langle a_1, \ldots, a_k, \rangle - \langle -b_1, \ldots, -b_k\rangle$. Como $\dim(\langle a_1, \ldots, a_k, \rangle) = \dim(\langle -b_1, \ldots, -b_k\rangle)$, então $\langle a_1, \ldots, a_k, \rangle - \langle -b_1, \ldots, -b_k\rangle \in \widehat{W}(F)$. Assim, pela projeção natural de $\widehat{W}(F)$ em $W(F)$, logo $f \in IF$. □

Observe que dado o epimorfismo de anéis $\dim : \widehat{W(F)} \longrightarrow \mathbb{Z}$, temos que $\dim(\widehat{I}F) \cong 2\mathbb{Z}$. Assim, podemos induzir um novo epimorfismo

$$\begin{array}{rccc} \dim_0: & \widehat{W}(F)/\mathbb{Z}\mathbb{H} = W(F) & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \\ & f & \longrightarrow & \dim_0(f) = \dim(f) + 2\mathbb{Z}. \end{array}$$

Pela Proposição 2.15, $\ker(\dim_0) = IF$. Vamos resumir no seguinte resultado.

Corolário 2.16. *O epimorfismo* $\dim_0$ *define um isomorfismo*

$$W(F)/IF \cong \mathbb{Z}/2\mathbb{Z}$$

Demonstração: Segue das observações acima. □

2.2 Grupo das Classes Quadradas

Na seção anterior foram construídos os anéis $\widehat{W}(F)$ e $W(F)$ e, por meio das aplicações de dimensão, conseguimos alguns resultados sobre esses anéis e ideais dos mesmos. Nessa seção iremos verificar um outro invariante nas formas quadráticas, o determinante. Assim, começamos pelo seguinte lema.

Lema 2.17. *Sejam* F *um corpo e* $(M(F), \perp)$ *o monóide formado pelas classes de isometria de* F*-formas quadráticas. Então a função*

$$\begin{array}{rccc} d: & M(F) & \longrightarrow & \dot{F}/\dot{F}^2 \\ & f & \longrightarrow & d(f) = \det(M_f) \cdot \dot{F}^2 \end{array}$$

é um homomorfismo de monóides.

Demonstração: Pela Proposição 1.44 temos que d está bem definida e $d(f \perp g) = d(f) \cdot d(g)$, para quaisquer $f, g \in M(F)$. Logo d é homomorfismo de monóides. □

Podemos estender d para a seguinte função $d' : \widehat{W}(F) \longrightarrow \dot{F}/\dot{F}^2$, dado por $d'(f - q) = d(f) \cdot d(q)^{-1} = d(f) \cdot d(q)$. Como $(\widehat{W}(F), \perp)$ é um grupo abeliano, então não é difícil provar que d' é homomorfismo de grupos.

Um fato importante de salientar é que $d'(\mathbb{H}) = -1 \cdot \dot{F}^2$ e isso nos impossibilita de estender d' para $W(F)$, pois nem sempre $-1 \in \dot{F}^2$, dependendo exclusivamente de F. Mas notemos que o problema de d' reside no sinal de $d'(\mathbb{H})$. Assim, definiremos a seguir um novo determinante.

Definição 2.18. Seja $f \in M(F)$, tal que $\dim(f) = n$. Definiremos *determinante com sinal* de q por

$$d_\pm(q) := (-1)^{\frac{n(n-1)}{2}} \cdot d(q) \in \dot{F}/\dot{F}^2.$$

Notemos que no determinante definido acima $d_\pm(\mathbb{H}) = 1$ e mais $d_\pm(n \cdot \mathbb{H}) = 1$, para $n \in \mathbb{N}$, o que possibilita uma extensão para $W(F)$. Porém, como vamos ver na observação abaixo, precisamos de algo a mais para essa extensão.

Observação 2.19. A fórmula

$$d_\pm(f \perp q) = d_\pm(f) \cdot d_\pm(q)$$

nem sempre é válida para f e q em $M(F)$. De fato, se tomarmos $f = \langle a \rangle$ e $q = \langle b \rangle$ teremos que $d_\pm(\langle a \rangle \perp \langle b \rangle) = -ab$ e $d_\pm(\langle a \rangle) \cdot d_\pm(\langle b \rangle) = ab$.

Assim, não será possível estender $d_\pm$ para $W(F)$, pois $d_\pm : M(F) \longrightarrow \dot{F}/\dot{F}^2$ não é homomorfismo de monóides. A alternativa que usaremos será a utilização do determinante com sinal junto com a $\dim_0$. Para tal tomaremos o seguinte grupo.

Definição 2.20. O conjunto $\mathbb{Z}/2\mathbb{Z} \times \dot{F}/\dot{F}^2$ munido da operação

$$(\cdot) : (e,d) \cdot (e',d') = (e+e', (-1)^{ee'}dd')$$

é um grupo abeliano, e denotaremos por $Q(F)$.

Lema 2.21. *O elemento* $(1,1) \in \frac{Q(F)}{\dot{F}/\dot{F}^2}$ *é o único elemento não identidade, tal que seu quadrado é* $(0,-1)$.

Demonstração: Em outras palavras devemos mostrar que nesse conjunto quociente $(1,1)^2 = (0,-1)$ e se $(e,d)^2 = (0,-1)$, então $(e,d) = (1,1)$. De fato, a primeira afirmação é direto da definição de $(\cdot)$ em $Q(F)$, $(1,1)^2 = (1+1, (-1)^1 1) = (0,-1)$. Para a segunda parte, seja $(e,d) \in \frac{Q(F)}{\dot{F}/\dot{F}^2}$ tal que $(e,d)^2 = (0,-1)$. Isso implica que $(2e, (-1)^{e^2}d^2) = (0,-1)$. Como $2e = 0 \in \mathbb{Z}/2\mathbb{Z}$ e $d^2 = 1 \in \dot{F}/\dot{F}^2$, então $(0,(-1)^{e^2}) = (0,-1)$, implicando que $e = 1$. Assim $(e,d) = (1,d)$. Mas $(1,d) = (1,1) \in \frac{Q(F)}{\dot{F}/\dot{F}^2}$. Logo $(1,1) \in \frac{Q(F)}{\dot{F}/\dot{F}^2}$ é a única classe que satisfaz estas propriedades. □

Recordamos que uma sequência exata curta de grupos

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

cinde se, e somente se, $B \cong C \oplus A$. Neste caso, dizemos que B é uma *extensão cindida* de A.

Proposição 2.22. $Q(F)$ *é uma extensão cindida de* $\dot{F}/\dot{F}^2$ *se, e somente se,* -1 *é um quadrado em* $\dot{F}$.

Demonstração: Considere a seguinte sequência de grupos

$$0 \longrightarrow \dot{F}/\dot{F}^2 \xrightarrow{i} Q(F) \xrightarrow{\pi} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0.$$

Como i e π são os homomorfismos inclusão e projeção, respectivamente, então essa sequência definida acima é exata. Suponha que essa sequência cinde. Isso implica que $Q(F) \cong \mathbb{Z}/2\mathbb{Z} \oplus \dot{F}/\dot{F}^2$, ou seja, $\frac{Q(F)}{\dot{F}/\dot{F}^2} \cong \mathbb{Z}/2\mathbb{Z}$. Caso $-1 \notin \dot{F}^2$, pelo Lema 2.21, temos que $(0,-1) \neq (0,1) \in \frac{Q(F)}{\dot{F}/\dot{F}^2}$ e assim $\left|\frac{Q(F)}{\dot{F}/\dot{F}^2}\right| > 2$, o que é um absurdo. Logo $-1 \in \dot{F}^2$.

Reciprocamente, suponha que $-1 \in \dot{F}^2$. Isso implica que $(e,d) \cdot (e',d') = (e+e', (-1)^{ee'}dd') = (e+e', dd')$. Que é exatamente a operação padrão de $\mathbb{Z}/2\mathbb{Z} \oplus \dot{F}/\dot{F}^2$. Logo $Q(F) \cong \mathbb{Z}/2\mathbb{Z} \oplus \dot{F}/\dot{F}^2$. Portanto a sequência anterior cinde. □

Vamos considerar agora a função $\phi : M(F) \longrightarrow Q(F)$, dada por $\phi(f) = (\dim_0(f), d_\pm(f))$.

Teorema 2.23. *A função* ϕ *define um epimorfismo de monóides de* $M(F)$ *para* $Q(F)$. *Esse epimorfismo pode ser estendido para um epimorfismo de grupos de* $\widehat{W}(F)$ *para* $Q(F)$, *que induz um isomorfismo de grupos* $\psi : W(F)/I^2F \cong Q(F)$.

Demonstração: Inicialmente, vamos mostrar que ϕ é um epimorfismo de monóides. De fato, primeiramente notemos que ϕ está bem definida, pois tomando $f, q \in M(F)$, tais que $f \cong q$, temos que $\dim(f) = \dim(q)$ e $d(f) = d(q)$. Implicando que $\dim_0(f) = \dim_0(q)$ e

$d_\pm(f) = d_\pm(q)$, ou seja, $\phi(f) = \phi(q)$. Sejam $f, q \in M(F)$, com $\dim(f) = n$ e $\dim(q) = m$. Como $\dim_0$ e d são homomorfismos de monóides, segue que

$$\begin{aligned}
\phi(f)\cdot\phi(q) &= (n, (-1)^{\frac{n(n-1)}{2}} d(f)) \cdot (m, (-1)^{\frac{m(m-1)}{2}} d(q)) \\
&= (n+m, (-1)^{nm}(-1)^{\frac{n(n-1)}{2}}(-1)^{\frac{m(m-1)}{2}} d(f)d(q)) \\
&= (n+m, (-1)^{\frac{(n+m)(n+m-1)}{2}} d(f \perp q)) \\
&= (n+m, d_\pm(f \perp q)) \\
&= \phi(f \perp q).
\end{aligned}$$

Provando que ϕ é homomorfismo de monóides. Para mostrar que ϕ é sobrejetora, seja $(e,d) \in Q(F)$. Escolhendo $f = \langle d \rangle$ se $e \notin 2\mathbb{Z}$ e $f = \langle d, 1\rangle$ se $e \in 2\mathbb{Z}$, então temos que $\phi(f) = (e,d)$.

A extensão para $\widehat{W}(F)$ é dada pela aplicação

$$\begin{aligned}
\phi' : \ \widehat{W}(F) &\longrightarrow Q(F) \\
f - q &\longrightarrow \phi'(f-q) = \phi(f)\cdot\phi(q)^{-1}.
\end{aligned}$$

Como ϕ é epimorfismo de monóides, segue que ϕ' está bem definida e

$$\begin{aligned}
\phi'((f-q)+(f'-q')) &= \phi'((f \perp f') - (q \perp q')) \\
&= \phi(f \perp f')\cdot\phi(q \perp q') \\
&= \phi(f)\cdot\phi(f')\cdot\phi(q)^{-1}\cdot\phi(q')^{-1} \\
&= \phi(f)\cdot\phi(q)^{-1}\cdot\phi(f')\cdot\phi(q')^{-1} \\
&= \phi'(f-q)\cdot\phi'(f'-q').
\end{aligned}$$

Assim, ϕ' é homomorfismo de grupos. Como ϕ é sobrejetora, então segue que ϕ' é sobrejetora e disso, segue que ϕ' é epimorfismo de grupos.

Note que $\phi'(n\cdot\mathbb{H}) = \phi'(n\cdot\mathbb{H} - 0_{M(F)}) = \phi(n\cdot\mathbb{H}) = (0,1)^n = (0,1)$, assim podemos estender ϕ' para o grupo $W(F)$ e obtemos a seguinte aplicação

$$\begin{aligned}
\phi'' : \ W(F) &\longrightarrow Q(F) \\
f &\longrightarrow \phi''(f) = \phi(f).
\end{aligned}$$

Como ϕ é homomorfismo de monóides, pela Decomposição de Witt 1.61, é fácil de provar que ϕ'' é homomorfismo de grupos. Pelo fato que $\mathrm{Im}(\phi) \subseteq \mathrm{Im}(\phi'')$, então ϕ'' é sobrejetora e portanto epimorfismo.

Por fim, considere o ideal $I^2F = IF \cdot IF$ de $W(F)$. Queremos mostrar que $I^2F \subseteq \ker(\phi'')$. De fato, pela Proposição 2.9, temos que $\widehat{I}F$ é gerado pelos elementos $\langle a\rangle - \langle 1\rangle \in \widehat{W}(F)$, então IF é gerado pelas formas quadráticas $\langle a, -1\rangle$, ou equivalentemente, IF é gerado pelas formas $\langle 1, -a\rangle$, com $a \in \dot{F}$. Assim I^2F é gerado pelas formas $\langle 1,-a\rangle \otimes \langle 1,-b\rangle$, com $a, b \in \dot{F}$. Segue que

$$\phi''(\langle 1,-a\rangle \otimes \langle 1,-b\rangle) = \phi''(\langle 1,-a,-b,ab\rangle) = (4, (-1)^{\frac{4\cdot 3}{2}}(-1)^2(ab)^2) = (0,1).$$

Implicando que $I^2F \subseteq \ker(\phi'')$. Logo ϕ'' induz o homomorfismo de grupos

$$\begin{aligned}
\psi : \ W(F)/I^2F &\longrightarrow Q(F) \\
f &\longrightarrow \psi(f) = \phi(f).
\end{aligned}$$

Como ϕ é um epimorfismo, temos que ψ é um epimorfismo.

Provaremos agora que ψ é um isomorfismo, para isso iremos construir um monomorfismo g tal que $\psi \circ g = Id_{Q(F)}$. Seja $g : Q(F) \longrightarrow W(F)/I^2F$ dada por $g((0,a)) = \langle 1, -a\rangle \pmod{I^2F}$ e $g((1,a)) = \langle a\rangle \pmod{I^2F}$. Afirmamos que g está bem definida. De fato, sejam $(e,d) = (e',d') \in Q(F)$. Isso implica que $e = e' \in \mathbb{Z}/2\mathbb{Z}$ e $d = d' \in \dot{F}/\dot{F}^2$. Assim, $\langle 1, -d\rangle \cong \langle 1, -d'\rangle$ e $\langle d\rangle \cong \langle d'\rangle$. Provaremos agora que g é homomorfismo, de fato

$$\begin{aligned}
g((0,d)\cdot(0,d')) &= g((0,dd')) = \langle 1, -dd'\rangle \pmod{I^2F} \\
&\equiv \langle 1, -dd'\rangle + \langle 1, -d, -d', dd'\rangle \pmod{I^2F} \\
&\equiv \langle 1, -d, 1, -d'\rangle \pmod{I^2F} = g((0,d)) + g((0,d')), \\
g((1,d)\cdot(1,d')) &= g((0,-dd')) = \langle 1, dd'\rangle \pmod{I^2F} \\
&\equiv \langle 1, dd'\rangle + \langle 1, d, d', dd'\rangle \equiv \langle d, d'\rangle \pmod{I^2F} \\
&= g((1,d)) + g((1,d')), \\
g((0,d)\cdot(1,d')) &= g(1,dd') = \langle dd'\rangle \pmod{I^2F} \\
&\equiv \langle dd'\rangle + \langle 1, -d, d', -dd'\rangle \pmod{I^2F} \\
&= \langle 1, -d, d'\rangle + \langle dd', -dd'\rangle \pmod{I^2F} \\
&\equiv \langle 1, -d\rangle + \langle d'\rangle \pmod{I^2F} = g((0,d)) + g((1,d')).
\end{aligned}$$

Agora, considere $(e,d),(e',d') \in Q(F)$, tais que $g((e,d)) = g((e',d'))$. Assim, ou $g((e,d)) = \langle 1, -d\rangle$, implicando que $e = e' = 0$ e $d = d'$, ou $g((e,d)) = \langle d\rangle$, implicando que $e = e' = 1$ e $d = d'$. Provando que g é injetora. Mais ainda, como $g(1,a) = \langle a\rangle$, então g é sobrejetora.

Agora basta provar que $\psi \circ g = Id_{Q(F)}$. De fato, seja $(e,d) \in Q(F)$. Se $e = 0$, então

$$\psi \circ g(0,d) = \psi(\langle 1, -d\rangle) = (2, (-1)^1(-d)) = (0,d).$$

Também, se $e = 1$, então

$$\psi \circ g(1,d) = \psi(\langle d\rangle) = (1, (-1)^0 d) = (1,d).$$

Logo ψ é um isomorfismo e portanto $W(F)/I^2F \cong Q(F)$. □

O próximo resultado nos apresenta um critério para descobrir se uma F-forma quadrática está no ideal I^2F.

Corolário 2.24 (Pfister). *Seja o ideal I^2F de $W(F)$. Se $f \in I^2F$, então* $\dim(f) = 2k$, *com $k \in \mathbb{N}$ e $d(f) = (-1)^{\frac{2k(2k-1)}{2}}$.*

Demonstração: Primeiramente, note que como $I^2F = IF \cdot IF$, então $I^2F \subseteq IF$. Assim, pela Proposição 2.15, temos que todas as formas quadráticas em I^2F tem dimensão par. Assim, dada $f \in I^2F$, temos que $\dim(f) = 2k$, onde $k \in \mathbb{N}$ e, pelo Teorema 2.23, $f \in \ker(\psi)$. Isso implica que

$$\psi(f) = (2k, (-1)^{\frac{2k(2k-1)}{2}} d(f)) = (0,1).$$

Em particular $(-1)^{\frac{2k(2k-1)}{2}} d(f) \in \dot{F}^2$. Logo $d(f) = (-1)^{\frac{2k(2k-1)}{2}}$ □

Corolário 2.25 (Pfister). *A restrição $\psi|_{IF}$ induz um isomorfismo de IF/I^2F para $\dot{F}/\dot{F}^2$.*

Demonstração: Do Teorema 2.23 temos que $\psi : W(F)/I^2F \longrightarrow Q(F)$ é um isomorfismo de grupos. Como IF é um subgrupo normal de $W(F)$ e $I^2F \subseteq IF$, então podemos restringir ψ em IF. Seja

$$\psi|_{IF} : IF/I^2F \longrightarrow Q(F)$$

esta restrição. Queremos mostrar que $\mathrm{Im}(\psi|_{IF}) \cong \dot{F}/\dot{F}^2$. De fato, seja $f \in IF$. Pela Proposição 2.15, temos que $\dim(f) = 2k$, com $k \in \mathbb{N}$. Assim

$$\psi|_{IF}(f) = \psi(f) = (2k, d_{\pm}(f)) = (0, d_{\pm}(f)) \in i(\dot{F}/\dot{F}^2) \cong \dot{F}/\dot{F}^2.$$

Reciprocamente, seja $(0, d) \in i(\dot{F}/\dot{F}^2)$. Tomando $f = \langle 1, -d\rangle$. Como $\dim(f) = 2$, então $f \in IF/I^2F$. Segue que $\psi|_{IF}(f) = \psi(f) = (0, (-1)^1(-d)) = (0, d)$. Implicando que $(0, d) \in \mathrm{Im}(\psi|_{IF})$. Pelo fato que $i(\dot{F}/\dot{F}^2) \cong \dot{F}/\dot{F}^2$, logo $IF/I^2F \cong \dot{F}/\dot{F}^2$. □

Note que, para uma F-forma quadrática f de dimensão par $n = 2r$, com $r \in \mathbb{N}$, o sinal $(-1)^{\frac{n(n-1)}{2}}$ pode ser simplificado por $(-1)^{\frac{2r(2r-1)}{2}} = (-1)^r$. Então, o critério para que uma forma $f \in IF$ pertença à I^2F é que $d(f) = 1$, no caso em que $4 | \dim(f)$, e $d(f) = -1$, no caso em que $4 \nmid \dim(f)$. Por exemplo, a F-forma de dimensão 6

$$f = \langle a, b, ab, -c, -d, -cd\rangle,$$

com $d(f) = -1$, está em I^2F. De fato, podemos reescrever essa forma quadrática como $f = \langle 1, a\rangle \cdot \langle 1, b\rangle - \langle 1, c\rangle \cdot \langle 1, d\rangle$ em $W(F)$, onde claramente cada somando está em I^2F.

Relembrando, que na Teoria de Anéis, um anel é *Noetheriano* se toda cadeia ascendente de ideais é limitada superiormente, ou equivalentemente todo ideal de um anel Noetheriano é finitamente gerado.

Corolário 2.26. *As seguintes afirmações são equivalentes:*

(1) $\widehat{W}(F)$ *é um anel Noetheriano;*

(2) $W(F)$ *é um anel Noetheriano;*

(3) $\dot{F}/\dot{F}^2$ *é um grupo finito.*

Demonstração: (1) ⇒ (2) Suponha que $\widehat{W}(F)$ é Noetheriano. Como $\widehat{W}(F)$ é um anel comutativo, então $\mathbb{Z}\mathbb{H}$ é um ideal bilateral. Como $W(F) = \widehat{W}(F)/\mathbb{Z}\mathbb{H}$ e sabemos que o quociente de um anel Noetheriano por um ideal bilateral é Noetheriano, então $W(F)$ é um anel Noetheriano.

(2) ⇒ (3) Suponha que $W(F)$ é um anel Noetheriano. Como $W(F)$ é comutativo, então IF é um ideal bilateral de $W(F)$. Assim IF é um $W(F)$-módulo finitamente gerado. Pelo mesmo argumento de (1) ⇒ (2), temos que $W(F)/IF$ é um anel comutativo Noetheriano. Isso implica que IF/I^2F é um $W(F)/IF$-submódulo finitamente gerado. Mas $W(F)/I^2F \cong \mathbb{Z}/2\mathbb{Z}$, ou seja, $W(F)/I^2F$ é um anel finito. Assim, IF/I^2F é um anel finito. Pelo corolário anterior, temos que $\dot{F}/\dot{F}^2$ é um grupo finito.

(3) ⇒ (1) Como toda forma quadrática tem uma representação diagonal, então $\widehat{W}(F)$ é gerado aditivamente por F-formas $\langle a\rangle$, onde $a \in \dot{F}$. Por hipótese temos que $\left|\dot{F}/\dot{F}^2\right| < \infty$. Assim $\widehat{W}(F)$ é finitamente gerado. Em particular todos os ideais de $\widehat{W}(F)$ são finitamente gerado. Portanto $\widehat{W}(F)$ é um anel Noetheriano. □

Note que a função $\psi : W(F)/I^2F \longrightarrow Q(F)$ definida no Teorema 2.23 é um isomorfismo de grupos, mas $W(F)/I^2F$ tem estrutura de anel comutativo. Isso sugere que $Q(F)$ possa possuir uma estrutura de anel comutativo, que transforme ψ em um isomorfismo de anéis. Uma simples conta nos leva a definir em $Q(F)$ a operação $(\circ)$ como segue: para $d, d' \in \dot{F}/\dot{F}^2$,

$$\begin{array}{rcl} (0,d)\circ(0,d') & = & (0,1), \\ (0,d)\circ(1,d') & = & (0,d), \\ (1,d)\circ(1,d') & = & (1,dd'). \end{array}$$

Note que a operação $(\circ)$ depende somente do grupo $\dot{F}/\dot{F}^2$.

Observação 2.27. O conjunto $Q(F)$ munido das operações

$$\begin{array}{rcl} (\cdot): \quad (e_1,d_1)\cdot(e_2,d_2) & = & (e_1+e_2,(-1)^{e_1e_2}d_1d_2), \\ (\circ): \quad (e_1,d_1)\circ(e_2,d_2) & = & (e_1e_2, d_1^{e_2}d_2^{e_1}) \end{array}$$

é um anel comutativo.

Note que, pelo Lema 2.21 vemos que a operação $(\cdot)$ em $Q(F)$ está relacionada com a classe $-1\dot{F}^2$ em $\dot{F}/\dot{F}^2$. Isso implica que, se F e K são dois corpos com um isomorfismo $\alpha : \dot{F}/\dot{F}^2 \longrightarrow \dot{K}/\dot{K}^2$ que preserva a classe do -1, então $Q(F) \cong Q(K)$, como anéis. De fato, pelo Corolário 2.25 e de α, temos que $IF/I^2F \cong IK/I^2K$. Como $(\circ)$ está associada a $\dot{F}/\dot{F}^2$ e $\dot{K}/\dot{K}^2$ em $Q(F)$ e $Q(K)$, respectivamente, então $(Q(F),\circ) \cong (Q(K),\circ)$. Por outro lado $-1 \in \dot{F}^2$ se, e somente se, $-1 \in \dot{K}^2$. Como $(\cdot)$ está associada a classe -1, então $(Q(F),\cdot) \cong (Q(K),\cdot)$. Portanto $(Q(F),\cdot,\circ) \cong (Q(K),\cdot,\circ)$.

Capítulo 3

Álgebras de Quatérnios e sua Forma Normal

Nesse capítulo iremos construir álgebras de quatérnios sobre corpos arbitrários com característica diferente de dois. Como uma álgebra é também um espaço vetorial, iremos utilizar formas quadráticas específicas para associar álgebras de quatérnios aos espaços quadráticos. Por último, mas não menos importante, iremos verificar algumas propriedades dessas formas quadráticas associadas as álgebras de quatérnios.

3.1 Construção das Álgebras de Quatérnios

O estudo sobre álgebras de quatérnios se inicia verificando a existência dos quatérnios sobre o corpo dos números reais. Nessa seção veremos que podemos abranger a construção de uma álgebra de quatérnios sobre um corpo arbitrário de característica distinta de dois.

Definição 3.1. Seja F um corpo, e seja A um F-espaço vetorial, onde definimos um produto $\cdot : A \times A \longrightarrow A$. Então A é chamada *álgebra sobre o corpo* F, se $(A, +, \cdot)$ é um anel, onde $+$ é a adição do F-espaço vetorial A, e se para todos x, y, $z \in A$ e $\alpha \in F$,

$(*)$ $\alpha(ab) = (\alpha a)b = a(\alpha b)$.

A dimensão da álgebra A é a dimensão de A como F-espaço vetorial.

Se A e A' são álgebras sobre um corpo F, chamaremos de *homomorfismo de álgebras* uma aplicação $\phi : A \longrightarrow A'$ que seja ao mesmo tempo uma transformação linear e um homomorfismo de anéis.

Definição 3.2. Sejam F um corpo e $a, b \in \dot{F}$. Definimos *a álgebra de quatérnios* $A = \left(\frac{a,b}{F}\right)$ pela F-álgebra sobre dois geradores i, j com as seguintes relações:

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

Tomando $k := ij \in A$, temos que $k^2 = (ij)(ij) = -i^2j^2 = -ab \in \dot{F}$,

$$ik = -ki = aj, \qquad kj = -jk = bi.$$

Então, dois a dois os elementos $\{i, j, k\}$ anticomutam.

No caso em que $F = \mathbb{R}$ e $a = b = -1$, $\left(\frac{-1,-1}{\mathbb{R}}\right)$ é o anel com divisão usual dos quatérnios sobre o corpo dos reais, que denotaremos por $\mathcal{H}$. A álgebra de quatérnios $\left(\frac{a,b}{F}\right)$ sobre F é uma generalização direta de $\mathcal{H}$.

Pelas propriedades da multiplicação em $\{1, i, j, k\}$ derivadas da definição anterior, segue que $A = \left(\frac{a,b}{F}\right)$ é gerado por $\{1, i, j, k\}$ sobre F.

Proposição 3.3. *$\{1, i, j, k\}$ forma uma F-base de $A = \left(\frac{a,b}{F}\right)$.*

Demonstração: Seja E o fecho algébrico de F. Isso implica que $x^2 + a$, $x^2 - b \in E[x]$ tem raízes em E. Sejam α, β raízes de $x^2 + a$ e $x^2 - b$, respectivamente. Considere as matrizes $i_o = \begin{bmatrix} 0 & \alpha \\ -\alpha & 0 \end{bmatrix}$, $j_o = \begin{bmatrix} 0 & \beta \\ \beta & 0 \end{bmatrix} \in \mathbb{M}_2(E)$. Assim

$$i_0^2 = \begin{bmatrix} 0 & \alpha \\ -\alpha & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & \alpha \\ -\alpha & 0 \end{bmatrix} = \begin{bmatrix} -\alpha^2 & 0 \\ 0 & -\alpha^2 \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = a\,\mathrm{Id}_2,$$

$$j_0^2 = \begin{bmatrix} 0 & \beta \\ \beta & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & \beta \\ \beta & 0 \end{bmatrix} = \begin{bmatrix} \beta^2 & 0 \\ 0 & \beta^2 \end{bmatrix} = \begin{bmatrix} b & 0 \\ 0 & b \end{bmatrix} = b\,\mathrm{Id}_2 \text{ e}$$

$$i_0 j_0 = \begin{bmatrix} 0 & \alpha \\ -\alpha & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & \beta \\ \beta & 0 \end{bmatrix} = \begin{bmatrix} \alpha\beta & 0 \\ 0 & -\alpha\beta \end{bmatrix} = \begin{bmatrix} 0 & -\beta \\ -\beta & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & \alpha \\ -\alpha & 0 \end{bmatrix} = -j_0 i_0.$$

Assim, não é difícil provar que a função $\phi : \left(\frac{a,b}{F}\right) \longrightarrow \mathbb{M}_2(E)$, expandida por $\phi(i) = i_0$ e $\phi(j) = j_0$, é um homomorfismo de álgebras sobre o corpo F.

Pela teoria de álgebra linear é suficiente provarmos que $\{\mathrm{Id}_2, i_0, j_0, k_0 = i_0 j_0\}$ é LI sobre E. De fato, sejam $c_1, \ldots, c_4 \in E$, tais que $c_1\,\mathrm{Id}_2 + c_2 i_0 + c_3 j_0 + c_4 k_0 = 0_{\mathbb{M}_2(E)}$. Isso implica no seguinte sistema

$$\begin{cases} c_1 + c_4\alpha\beta = 0_E \\ -c_2\alpha + c_3\beta = 0_E \\ c_2\alpha + c_3\beta = 0_E \\ c_1 - c_4\alpha\beta = 0_E. \end{cases}$$

Resolvendo o sistema obtemos $c_1 = c_2 = c_3 = c_4 = 0_E$. Logo $\{\mathrm{Id}_2, i_0, j_0, k_0\}$ é LI sobre E. Como $\phi^{-1}(\{\mathrm{Id}_2, i_0, j_0, k_0\}) = \{1, i, j, k\}$, então $\{1, i, j, k\}$ é LI sobre F. Portanto $\{1, i, j, k\}$ é base de A. □

Nos resultados seguintes utilizaremos o símbolo "$\cong$"para expressar o isomorfismo entre álgebras sobre um corpo fixado L, que diremos *L-isomorfismo de álgebras*. Analogamente, se ϕ é um homomorfismo de álgebras sobre um corpo L, chamaremos ϕ de *L-homomorfismo de álgebras*.

Observação 3.4. (1) A construção da álgebra generalizada de quatérnios A é simétrica em a, b, ou seja, $A = \left(\frac{a,b}{F}\right) \cong \left(\frac{b,a}{F}\right)$. Essa afirmação é de fácil demonstração utilizando a função $\phi : \left(\frac{a,b}{F}\right) \longrightarrow \left(\frac{b,a}{F}\right)$, expandida de $\phi(i) = j$ e $\phi(j) = i$, em que ϕ é um F-isomorfismo de álgebras.

(2) Seja K/F uma extensão de corpos, então $K \otimes_F \left(\frac{a,b}{F}\right) \cong \left(\frac{a,b}{K}\right)$. Tomando a função $\phi : K \otimes_F \left(\frac{a,b}{F}\right) \longrightarrow \left(\frac{a,b}{K}\right)$, dada por

$$\phi(\sum_m [l_m \otimes (c_{1m} + c_{2m} i + c_{3m} j + c_{4m} k)] = \sum_m [l_m c_{1m} + l_m c_{2m} i + l_m c_{3m} j + l_m c_{4m} k],$$

sendo as somas acima ambas finitas. É fácil de mostrar que ϕ é um K-isomorfismo de álgebras.

Recordemos que uma álgebra A é dita *simples* se A não possui ideais bilaterais distintos dos triviais.

Proposição 3.5. *Seja F um corpo ($\mathrm{char}(F) \neq 2$). Então:*

(1) $\left(\frac{a,b}{F}\right) \cong \left(\frac{ax^2,by^2}{F}\right)$, *para quaisquer* $a, b, x, y \in \dot{F}$;

(2) $\left(\frac{-1,1}{F}\right) \cong \mathbb{M}_2(F)$;

(3) $Z(\left(\frac{a,b}{F}\right)) = F \cdot 1 (\cong F)$, *para quaisquer* $a, b \in \dot{F}$;

(4) $\left(\frac{a,b}{F}\right)$ *é uma álgebra simples, para quaisquer* $a, b \in \dot{F}$.

Demonstração: (1) Seja $A = \left(\frac{a,b}{F}\right)$, munida da base natural $\{1, i, j, k = ij\}$ e seja $A' = \left(\frac{ax^2,by^2}{F}\right)$, com a base natural $\{1, i', j', k' = i'j'\}$, tal que $i'^2 = ax^2$, $j'^2 = by^2$ e $k'^2 = -ab(xy)^2$. Tomando $xi, yj \in A$, temos que $(xi)^2 = ax^2$, $(yj)^2 = bj^2$ e $(xi)(yj) = xy(ij) = -(yj)(xi)$. Assim, pela função $\phi : A' \longrightarrow A$, expandida por $\phi(i') = xi$, $\phi(j') = yj$, é fácil de mostrar que ϕ é um F-isomorfismo de álgebras, ou seja, $A \cong A'$.

(2) Note que $-1, 1$ são raízes do polinômio $x^2 - 1 \in F[x]$. Tomando $\{1, i, j, k\}$ a base natural de $\left(\frac{-1,1}{F}\right)$, por construção semelhante a da Proposição 3.3, obtemos o F-homomorfismo de álgebras $\phi : \left(\frac{-1,1}{F}\right) \longrightarrow \mathbb{M}_2(F)$, no qual

$$\phi(1) = Id_2,\ \phi(i) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix},\ \phi(j) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ e } \phi(k) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Como $\left\{\mathrm{Id}_2, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\right\}$ é uma base de $\mathbb{M}_2(F)$, ϕ leva base em base e assim ϕ é um F-isomorfismo de espaços vetoriais, e consequentemente ϕ e um F-isomorfismo de álgebras. Portanto, $\left(\frac{-1,1}{F}\right) \cong \mathbb{M}_2(F)$.

(3) Seja $A = \left(\frac{a,b}{F}\right)$, com a notação da Proposição 3.3, temos que $\phi : A \longrightarrow \mathbb{M}_2(E)$, expandida por $\phi(i) = i_0$, $\phi(j) = j_0$ é um F-homomorfismo de álgebras. Pelo 1° Teorema dos Isomorfismos, temos que $A/\ker(\phi) \cong \mathrm{Im}(\phi)$. Como

$$\left\{\mathrm{Id}_2, \begin{bmatrix} 0 & \alpha \\ -\alpha & 0 \end{bmatrix}, \begin{bmatrix} 0 & \beta \\ \beta & 0 \end{bmatrix}, \begin{bmatrix} \alpha\beta & 0 \\ 0 & -\alpha\beta \end{bmatrix}\right\} \text{ é LI,}$$

então ϕ é injetora. Implicando que $A \cong \mathrm{Im}(\phi)$. Pelo fato que

$$Z(\mathbb{M}_2(E)) \cap \mathrm{Im}(\phi) = \left\{\begin{bmatrix} x & 0 \\ 0 & x \end{bmatrix} \in \mathbb{M}_2(E) \ : \ x \in F\right\} = \{\phi(x + 0i + 0j + 0k) \ : \ x \in F\}$$

e que isomorfismos preservam o centro, logo $Z(A) = F$.

(4) No item (3) dessa proposição vimos que $A = \left(\frac{a,b}{F}\right) \cong Im(\phi) \subseteq \mathbb{M}_2(E)$, onde E é o fecho algébrico de F. Como $\mathbb{M}_2(E)$ é uma álgebra simples, se $\left(\frac{a,b}{F}\right)$ não fosse simples, então tomando $I \subset A$ um ideal não trivial, então $\phi(I)$ seria um ideal não trivial de $\mathbb{M}_2(E)$ o que é uma contradição. Logo A é álgebra simples, para quaisquer $a, b \in \dot{F}$. □

Definição 3.6. Seja a álgebra de quatérnios $A = \left(\frac{a,b}{F}\right)$, com a base natural $\{1, i, j, k\}$. Um quatérnio da forma $x = c_1 + c_2 i + c_3 j + c_4 k \in A$ é chamado de *quatérnio puro* se $c_1 = 0$. O F-subespaço dos quatérnios puros será denotado por A_0.

Proposição 3.7. *Sejam* $A = \left(\frac{a,b}{F}\right)$, *e* $v \in A$, *tal que* $v \neq 0$. *Então* $v \in A_0$ *se, e somente se,* $v \notin F$ *e* $v^2 \in F$.

Demonstração: Seja $v = c_1 + c_2 i + c_3 j + c_4 k \in A$. Por cálculo direto temos que

$$v^2 = (c_1^2 + ac_2^2 + bc_3^2 - abc_4^2) + 2c_1 \cdot (c_2 i + c_3 j + c_4 k).$$

Se $v \in A_0$, então $c_1 = 0$ implicando que $v^2 = (c_1^2 + ac_2^2 + bc_3^2 - abc_4^2) \in F$. Como $v \neq 0$ e $c_1 = 0$, então $c_i \neq 0$, para algum $i = 2, 3, 4$, consequentemente $v \notin F$.

Reciprocamente, se $v \notin F$ e $v^2 \in F$, então $c_i \neq 0$, para algum $i = 2, 3, 4$ e $2c_1 \cdot (c_2 i + c_3 j + c_4 k) = 0$. Assim, $c_1 = 0$. Logo $v \in A_0$. □

Corolário 3.8. *Sejam* $A = \left(\frac{a,b}{F}\right)$ *e* $A' = \left(\frac{a',b'}{F}\right)$, *tais que* $A \cong A'$. *Seja* $\phi : A \longrightarrow A'$ *um* F*-isomorfismo de álgebras. Então* $\phi(A_0) = A_0'$. *Em particular* A_0 *é invariante para qualquer* F*-endomorfismo de* A.

Demonstração: Note que pela Proposição 3.5 (3) temos que $Z(A) = F = Z(A')$. Como ϕ é um F-homomorfismo de álgebras, então $\phi(F) = F$. Como ϕ é F- isomorfismo, então ϕ leva base de A em base de A'. Assim ϕ leva os geradores de A_0 nos geradores de A_0', segue que $\phi(A_0) = A_0'$.

Em particular, se $\phi : A \longrightarrow A$ é um endomorfismo não nulo, então, pela Proposição 3.5 (4), temos que $\ker \phi = \{0\}$ e assim ϕ é um automorfismo. Pelo provado acima, $\phi(A_0) = A_0$. □

3.2 Álgebras de Quatérnios e Espaços Quadráticos

Nessa seção iremos associar as álgebras de quatérnios aos espaços quadráticos, para tal utilizaremos uma forma quadrática regular que existe para todas as álgebras de quatérnios.

Definição 3.9. Sejam $A = \left(\frac{a,b}{F}\right)$, na base $\{1, i, j, k\}$, e $v = c_1 + c_2 i + c_3 j + c_4 k \in A$. Definimos o *conjugado* de v como sendo o elemento $\overline{v} = c_1 - (c_2 i + c_3 j + c_4 k)$.

Lema 3.10. *Sejam* $A = \left(\frac{a,b}{F}\right)$, $x, y \in A$, $\overline{x}$ *o conjugado de* x *em* A *e* $\alpha \in F$. *Então*

$$\overline{x + y} = \overline{x} + \overline{y}, \quad \overline{x \cdot y} = \overline{y} \cdot \overline{x}, \quad \overline{\overline{x}} = x \text{ e } \overline{r \cdot x} = r \cdot \overline{x}.$$

Se $x \in A_0$, *então* $\overline{x} = -x$.

Demonstração: A demonstração é análoga para o caso dos quatérnios reais. □

Definição 3.11. A função $I : A \longrightarrow A$, definida por $x \longrightarrow \overline{x}$ é chamada de *involução barra* sobre A. Para $x \in A$, definimos a *norma de* x por $N : A \longrightarrow A$, dada por $N(x) = x \cdot \overline{x}$. Também definimos o *traço de* x por $T : A \longrightarrow A$, dado por $T(x) = x + \overline{x}$, para $x \in A$.

Note que I, N e T estão bem definidas, pois todo quatérnio de A tem um único conjugado. Observe também, que para todo $x \in A$, temos que $\overline{T(x)} = T(x)$ e $\overline{N(x)} = N(x)$. Isto implica que $T(x) \in F$ e $N(x) \in F$. Assim podemos reescrever as aplicações N e T

$$\begin{array}{rccl} T: & A & \longrightarrow & F \\ & x & \longrightarrow & T(x) = x + \overline{x} \end{array} \qquad \begin{array}{rccl} N: & A & \longrightarrow & F \\ & x & \longrightarrow & N(x) = x \cdot \overline{x}. \end{array}$$

Lema 3.12. *Seja $A = \left(\frac{a,b}{F}\right)$ uma álgebra de quatérnios sobre o corpo F. Considere a função $B : A \times A \longrightarrow F$, dada por $B(x,y) := \frac{x\overline{y}+y\overline{x}}{2} = \frac{T(x\overline{y})}{2}$, então B é uma forma bilinear simétrica.*

Demonstração: Primeiramente note que B está bem definida, pois $\frac{T(x\overline{y})}{2} \in F$. Sejam $x_1, x_2, y \in A$ e $\alpha \in F$. Assim,

$$\begin{array}{rcl} B(x_1 + \alpha x_2, y) & = & \frac{(x_1+\alpha x_2)\cdot\overline{y}+y\cdot\overline{(x_1+\alpha x_2)}}{2} \\ & = & \frac{x_1\overline{y}+\alpha x_2\overline{y}+y\overline{x_1}+y\alpha\overline{x_2}}{2} \\ & = & \frac{x_1\overline{y}+y\overline{x_1}}{2} + \frac{\alpha x_2\overline{y}+\alpha y\overline{x_2}}{2} \\ & = & B(x_1,y) + \alpha B(x_2,y). \end{array}$$

Provando que B é linear na primeira coordenada. Analogamente B é linear na segunda coordenada. Logo B é uma forma bilinear. Note que

$$T(x\overline{y}) = x\overline{y} + \overline{x\overline{y}} = x\overline{y} + y\overline{x} = y\overline{x} + x\overline{y} = T(y\overline{x}).$$

Provando que B é simétrica. Portanto B é uma forma bilinear simétrica. □

Por despolarização da forma bilinear simétrica $B(x,y) = \frac{T(x\overline{y})}{2}$ obtemos a seguinte forma quadrática

$$q_B(x) = B(x,x) = \frac{x\overline{x} + \overline{x}x}{2} = x\overline{x} = N(x).$$

Implicando que N é uma forma quadrática associada a $A = \left(\frac{a,b}{F}\right)$, para quaisquer $a, b \in \dot{F}$.

Definição 3.13. Chamaremos a forma quadrática $N : A \longrightarrow F$ de *forma normal* de A. Obtemos assim o novo espaço quadrático (A, N).

Vamos analisar agora o comportamento da ortogonalidade em (A, N) em relação aos subespaços de A. Para tanto, tomemos $x, y \in A_0$ e B a forma bilinear simétrica associada a N. Assim

$$B(x,y) \;=\; \frac{x\overline{y}+y\overline{x}}{2} = \frac{x(-y)+y(-x)}{2} = -\left(\frac{xy+yx}{2}\right).$$

Isso implica que x e y são ortogonais em (A, B, N) se, e somente se, x e y são anticomutativos, ou seja, $xy = -yx$. Em particular $\{i, j, k\}$ forma uma base ortogonal de $(A_0, N|_{A_0})$. Mais ainda, se $x \in A_0$, então

$$B(x,1) = \frac{x\overline{1} + 1\overline{x}}{2} = \frac{x - x}{2} = 0.$$

Segue que $F \cdot 1 \perp A_0$, e assim $\{1, i, j, k\}$ forma uma base ortogonal de (A, N). Implicando que $A = F \cdot 1 \perp F \cdot i \perp F \cdot j \perp F \cdot k$.

Proposição 3.14. *Sejam $A = \left(\frac{a,b}{F}\right)$ e o espaço quadrático (A, B, N) munido da base ortogonal $\{1, i, j, k\}$. Então (A, B, N) é regular e*

$$N \cong \langle 1, -a, -b, ab\rangle \cong \langle 1, -a\rangle \otimes \langle 1, -b\rangle.$$

Demonstração: Queremos provar que (A, B, N) é regular. De fato, seja $x \in \text{rad}(A)$, logo $B(x, y) = 0$, para todo $y \in A$. Em particular, $B(x, 1) = B(x, i) = B(x, j) = 0$. Como $A = F \cdot 1 \perp F \cdot i \perp F \cdot j \perp F \cdot k$, então $x \in F \cdot k$. Seja $\alpha \in F$ tal que $x = \alpha k$. Pelo fato que $0 = B(\alpha k, k) = \alpha \cdot B(k, k) = \alpha(-1)ab$, temos que $\alpha = 0$ e assim $x = 0$. Portanto $\text{rad}(A) = \{0\}$, ou seja, (A, B, N) é regular.

Agora basta mostrar que $N \cong \langle 1, -a, -b, ab\rangle$. De fato, dado $\alpha \in F$ note que

$$\begin{array}{rcccccl} N(\alpha 1) & = & \alpha 1\overline{\alpha 1} & = & = & \alpha 1\alpha 1 & = 1 \cdot \alpha^2 \\ N(\alpha i) & = & \alpha i\overline{\alpha i} & = & = & \alpha i\alpha(-i) & = -a \cdot \alpha^2 \\ N(\alpha j) & = & \alpha j\overline{\alpha j} & = & = & \alpha j\alpha(-j) & = -b \cdot \alpha^2 \\ N(\alpha k) & = & \alpha k\overline{\alpha k} & = & = & \alpha(ij)\alpha(ji) & = ab \cdot \alpha^2. \end{array}$$

Como $A = F \perp F \cdot i \perp F \cdot j \perp F \cdot k$, dado $c_1 + c_2 i + c_3 j + c_4 k \in A$ temos que $N(c_1 + c_2 i + c_3 j + c_4 k) = c_1^2 - ac_2^2 - bc_3^2 + abc_4^2$. Portanto $N \cong \langle 1, -a, -b, ab\rangle$. □

Observe que pela proposição anterior temos que $\dim((A, N)) = 4$ e $d((A, N)) = (-a)(-b)(ab) \cdot \dot{F}^2 = \dot{F}^2$.

Corolário 3.15. *Seja (A, B, N) um espaço quadrático de quatérnios, com $A = \left(\frac{a,b}{F}\right)$. Se $x = c_1 + c_2 i + c_3 j + c_4 k$, então*

$$N(x) = c_1^2 - ac_2^2 - bc_3^2 + abc_4^2.$$

Demonstração: Segue imediatamente do fato que $N \cong \langle 1, -a, -b, ab\rangle$. □

Observação 3.16. (1) Note que o corolário anterior pode ser demonstrado sem a Proposição 3.14 pelo cálculo direto de $N(x) = x \cdot \overline{x}$.

(2) Como $x \in A$ comuta com seu conjugado, então

$$N(x) = x \cdot \overline{x} = \overline{x} \cdot x = \overline{x} \cdot \overline{\overline{x}} = N(\overline{x}).$$

Implicando que $\phi : A \longrightarrow A$, dada por $\phi(x) = \overline{x}$ é uma isometria do espaço quadrático (A, N).

(3) Todo quatérnio $x \in A$ é raiz de um polinômio quadrático sobre o corpo base F. A saber, dado $x \in A$, tomando $p(y) = y^2 - T(x)y + N(x) \in F[y]$, então

$$\begin{array}{rcl} p(x) & = & x^2 - T(x)x + N(x) = x^2 - (x - \overline{x})x + x\overline{x} = x^2 - x^2 - \overline{x}x + x\overline{x} \\ & = & 0. \end{array}$$

(4) Para os quatérnios reais $\mathcal{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$, a forma quadrática N recai na norma euclidiana ao quadrado. De fato, tomando $x = c_1 + c_2 i + c_3 j + c_4 k \in \mathcal{H}$, temos

$$\begin{array}{rcl} N(x) & = & c_1^2 - ac_2^2 - bc_3^2 + abc_4^2 \\ & = & c_1^2 - (-1)c_2^2 - (-1)c_3^2 + (-1)(-1)c_4^2 \\ & = & c_1^2 + c_2^2 + c_3^2 + c_4^2 = ||x||^2. \end{array}$$

Proposição 3.17. *Seja (A, B, N) o espaço quadrático associado a álgebra de quatérnios $A = \left(\frac{a,b}{F}\right)$. Então:*

(1) *Para $x, y \in A$, $N(x \cdot y) = N(x) \cdot N(y)$;*

(2) *$x \in A$ é inversível se, e somente se, $N(x) \neq 0$.*

Demonstração: (1) Pelo Lema 3.10, temos que $\overline{xy} = \overline{y}.\overline{x}$. Como $y\overline{y} \in F$, para todo $y \in A$, então

$$N(xy) = xy\overline{xy} = x(y\overline{y})\overline{x} = x\overline{x}y\overline{y} = N(x)N(y).$$

(2) Seja $x \in \mathcal{U}(A)$ (conjunto dos inversíveis de A). Assim, existe $x^{-1} \in A$. Pelo item (1) dessa proposição temos que

$$N(x)N(x^{-1}) = N(xx^{-1}) = N(1) = 1.$$

Logo $N(x) \neq 0$.

Reciprocamente, se $N(x) \neq 0$, então $x\overline{x} \neq 0$. Tomando $x_0 = \overline{x}/N(x)$, temos que $x \cdot x_0 = \frac{x\overline{x}}{x\overline{x}} = 1$. Logo $x \in \mathcal{U}(A)$. □

Observação 3.18. Da demonstração anterior obtemos que o inverso de um elemento $x \in \mathcal{U}(A)$ é o elemento $x^{-1} = \frac{\overline{x}}{N(x)}$.

Corolário 3.19. *Seja $A = \left(\frac{a,b}{F}\right)$ uma álgebra de quatérnios sobre F. Então:*

(1) *$D_F(N)$ é um subgrupo de $\dot{F}$;*

(2) *Para qualquer $c \in \dot{F}$, temos que $c \in D_F(N)$ se, e somente se, $\langle c\rangle \cdot N \cong N$.*

Demonstração: (1) Como $N \cong \langle 1, -a, -b, ab\rangle$, então $1 \in D_F(N)$. Pela Proposição 3.17 item (1), temos que $D_F(N)$ é fechado para o produto. Por último, como $D_F(N)$ é fechado para inversos, então $D_F(N)$ é subgrupo de $\dot{F}$.

(2) Seja $c \in D_F(N)$, com $c \neq 0$. Se $c \in D_F(N)$, então existe $x \in A$, tal que $N(x) = c$. Seja $\phi : A \longrightarrow A$, definida por $\phi(y) = x \cdot y$. É fácil provar que ϕ é um F-isomorfismo de espaços vetoriais, pois pela Proposição 3.17 item (2), temos que x é inversível em A.

Queremos mostrar que ϕ é uma isometria. De fato, seja $y \in A$, temos que

$$N(\phi(y)) = N(x \cdot y) = N(x) \cdot N(y) = c \cdot N(y) = \langle c\rangle \cdot N(y).$$

Logo $(A, N) \cong (A, \langle c\rangle \cdot N)$.

Reciprocamente, se $\langle c\rangle \cdot N \cong N$, então $D_F(\langle c\rangle \cdot N) = D_F(N)$. Como $N \cong \langle 1, -a, -b, ab\rangle$, então $\langle c\rangle \cdot N \cong \langle c, -ca, -cb, cab\rangle$. Assim $c \in D_F(\langle c\rangle \cdot N)$ e portanto $c \in D_F(N)$. □

Veremos agora um importante resultado de classificação das álgebras de quatérnios.

Teorema 3.20. *Sejam $A = \left(\frac{a,b}{F}\right)$ e $A' = \left(\frac{a',b'}{F}\right)$ duas álgebras de quatérnios sobre o corpo base F. Então as seguintes afirmações são equivalentes:*

(1) *A e A' são F-álgebras isomorfas;*

(2) *A e A' são espaços quadráticos isométricos;*

(3) *A_0 e A'_0 são espaços quadráticos isométricos.*

Demonstração: (1) $\Rightarrow$ (2) Suponha que $A \cong A'$ como F-álgebras. Assim existe um F-álgebra isomorfismo $\phi : A \longrightarrow A'$. Em particular ϕ é F-isomorfismo de espaços vetoriais. Pelo Corolário 3.8 temos que $\phi(A_0) = A'_0$. Como ϕ fixa F, então se $x = \alpha + x_0 \in A$, onde

$\alpha \in F$ e $x_0 \in A_0$, então $\phi(x) = \alpha + \phi(x_0)$. Do mesmo modo, tomando $\overline{x} = \alpha - x_0$ temos que $\phi(\overline{x}) = \alpha - \phi(x_0)$. Implicando que $\overline{\phi(x)} = \phi(\overline{x})$

Sejam (A, B, N) e (A', B', N') os F-espaços quadráticos associados a A,A' e a suas formas normais, respectivamente. Tomando $x \in A$ temos que

$$N'(\phi(x)) \;=\; \phi(x) \cdot \overline{\phi(x)} = \phi(x) \cdot \phi(\overline{x}) = \phi(x \cdot \overline{x}) = \phi(N(x)) = N(x),$$

a última igualdade segue do fato que $N(x) \in F$. Como $x \in A$ foi escolhido arbitrariamente, ϕ é uma F-isometria.

(2) $\Rightarrow$ (3) Se $A \cong A'$ como F-espaços quadráticos, então

$$\langle 1, -a, -b, ab\rangle \cong \langle 1, -a', -b', a'b'\rangle.$$

Pelo Cancelamento de Witt 1.60 temos que $\langle -a, -b, ab\rangle \cong \langle -a', -b', a'b'\rangle$. Implicando que $A_0 \cong A_0'$ como F-espaços quadráticos.

(3) $\Rightarrow$ (1) Seja $\phi : A_0 \longrightarrow A_0'$ uma F-isometria. Seja $\phi' : A \longrightarrow A'$, dada por $\phi'(1) = 1$ e $\phi'(x_0) = \phi(x_0)$, para todo $x_0 \in A_0$. É fácil provar que ϕ' é uma isometria. Assim $(A, B, N) \cong (A', B', N')$.

Afirmamos que ϕ' é um F-isomorfismo de álgebras. De fato, é suficiente verificarmos se ϕ' preserva as relações de $1, i, j, k$, onde $\{1, i, j, k\}$ é a base natural de A. Para 1, temos pela construção de ϕ' que $\phi'(1) = 1$. Para i temos que por um lado

$$N'(\phi'(i)) = N(i) = i\bar{i} = -a, \text{ por outro lado,}$$

$$N'(\phi'(i)) \;=\; \phi'(i) \cdot \overline{\phi'(i)} = \phi'(i) \cdot \phi'(\bar{i}) = \phi'(i) \cdot \phi'(-i) = -\phi'(i)^2.$$

Implicando que $\phi'(i)^2 = a$. Analogamente $\phi'(j)^2 = b$. Temos também $B'(\phi'(i), \phi'(j)) = B(i, j) = 0$, implicando que $\phi'(i) \perp \phi'(j)$. E por último, $\phi'(i) \cdot \phi'(j) = -\phi'(j) \cdot \phi'(i) = \phi'(ij)$, aplicando as normas acima. Pelo que já provamos podemos concluir que $\phi'(x \cdot y) = \phi'(x) \cdot \phi'(y)$, para $x, y \in A$. Como ϕ' é F-isomorfismo de espaços vetoriais, segue que ϕ' é F-isomorfismo de álgebras. Logo $A \cong A'$ como F-álgebras. □

Teorema 3.21. *Sejam $A = \left(\frac{a,b}{F}\right)$ uma F-álgebra de quatérnios e (A, B, N) o F-espaço espaço quadrático associado a A. Então as seguintes afirmações são equivalentes:*

(1) $A \cong \left(\frac{1,-1}{F}\right)$ $(\cong \mathbb{M}_2(F))$;

(2) *A não é uma álgebra com divisão;*

(3) *(A, B, N) é F-isotrópico;*

(4) *(A, B, N) é F-hiperbólico $(N \cong 2\mathbb{H})$;*

(5) *$(A_0, N|_{A_0})$ é F-isotrópico;*

(6) $(\langle a\rangle - \langle 1\rangle) \cdot (\langle b\rangle - \langle 1\rangle) = 0$ *em* $\widehat{W}(F)$;

(7) *A forma binária $\langle a, b\rangle$ representa 1;*

Demonstração: (1) $\Rightarrow$ (2) Suponha que $A \cong \left(\frac{1,-1}{F}\right)$. Assim, $N \cong \langle 1, -1, 1, -1\rangle \cong 2\mathbb{H}$. Segue que, (A, N) é um espaço quadrático isotrópico. Seja $0 \neq x \in A$ um vetor isotrópico.

Pela Proposição 3.17 item (2), temos que x não é inversível. Logo A não é álgebra com divisão.

(2) $\Rightarrow$ (3) Como A não é álgebra com divisão, então existe $0 \neq x \in A$, tal que x não é inversível. Pela Proposição 3.17 item (2), temos que $N(x) = 0$. Logo (A, N) é um espaço quadrático isotrópico sobre o corpo F.

(3) $\Rightarrow$ (4) Suponha que (A, N) é um espaço quadrático isotrópico. Assim, $N \cong q \perp \mathbb{H}$, com $q \cong \langle e, e' \rangle$. Queremos mostrar que $q \cong \mathbb{H}$. De fato, como $d(N) = 1(-a)(-b)ab \cdot \dot{F}^2 = 1 \cdot \dot{F}^2$ e $d(q \perp \mathbb{H}) = -ee' \cdot \dot{F}^2$, então $-ee' \in \dot{F}^2$. Implicando que $-e \cdot \dot{F}^2 = e' \cdot \dot{F}^2$, pois $k \cdot \dot{F}^2 = k^{-1} \cdot \dot{F}^2$ para qualquer $k \in \dot{F}$. Assim,

$$q \cong \langle e, e' \rangle \cong \langle e, -e \rangle \cong \mathbb{H}.$$

Logo $N \cong 2 \cdot \mathbb{H}$. Portanto (A, N) é um F-espaço quadrático hiperbólico.

(4) $\Rightarrow$ (5) Se (A, N) é um espaço quadrático hiperbólico, então $N \cong \langle 1, -a, -b, ab \rangle \cong \langle 1, -1, 1, -1 \rangle$. Pelo cancelamento de Witt 1.60 temos que

$$\langle -a, -b, ab \rangle \cong \langle -1, 1, -1 \rangle \cong \mathbb{H} \perp \langle -1 \rangle.$$

Assim, $(A_0, N|_{A_0}) \cong (A_0, \mathbb{H} \perp \langle -1 \rangle)$. Logo $(A_0, N|_{A_0})$ é um espaço quadrático isotrópico.

(5) $\Rightarrow$ (3) Como $N \cong \langle 1 \rangle \perp N|_{A_0}$, então é fácil ver que, se $(A_0, N|_{A_0})$ for isotrópico, então (A, N) é isotrópico.

(4) $\Rightarrow$ (6) Se (A, N) é um F-espaço quadrático hiperbólico, então $N \cong \langle 1, -a, -b, ab \rangle \cong 2 \cdot \mathbb{H}$. Assim

$$\begin{aligned}
(\langle a \rangle - \langle 1 \rangle) \cdot (\langle b \rangle - \langle 1 \rangle) &= (\langle a \rangle, \langle 1 \rangle) \cdot (\langle b \rangle, \langle 1 \rangle) \\
&\equiv (\langle 1, ab \rangle, \langle a, b \rangle) \\
&= \langle 1, ab \rangle - \langle a, b \rangle \\
&\equiv \langle 1, ab \rangle + \langle -a, -b \rangle - \langle a, b \rangle - \langle -a, -b \rangle \\
&= \langle 1, -a, -b, ab \rangle - \langle -a, -b, a, b \rangle \\
&= 2 \cdot \mathbb{H} - 2 \cdot \mathbb{H} = 0 \in \widehat{W}(F).
\end{aligned}$$

(6) $\Rightarrow$ (7) Se $(\langle a \rangle - \langle 1 \rangle) \cdot (\langle b \rangle - \langle 1 \rangle) = \langle 1, ab \rangle - \langle a, b \rangle = 0$. Então $\langle 1, ab \rangle = \langle a, b \rangle \in \widehat{W}(F)$. Implicando que $\langle 1, ab \rangle \cong \langle a, b \rangle$. Assim, $1 \in D_F(\langle a, b \rangle)$.

(7) $\Rightarrow$ (1) Se $1 \in D_F(\langle a, b \rangle)$, então pela Proposição 1.64 temos que $\langle a, b \rangle \cong \langle 1, ab \rangle$. Assim, $\langle a, b \rangle = \langle 1, ab \rangle \in \widehat{W}(F)$. Implicando que

$$\langle 1, ab \rangle - \langle a, b \rangle = 0 \text{ em } \widehat{W}(F).$$

Adicionando $\langle -a, -b \rangle - \langle -a, -b \rangle = 0$ na igualdade acima temos que $N = 2\mathbb{H}$ em $\widehat{W}(F)$, ou seja, $N \cong 2\mathbb{H}$. Portanto, $A \cong \left(\frac{1,-1}{F}\right)$.

As afirmações são equivalentes, pois

$$(1) \Rightarrow (2) \Rightarrow (3) \Rightarrow (4) \Rightarrow (5) \Rightarrow (3) \Rightarrow (4) \Rightarrow (6) \Rightarrow (7) \Rightarrow (1).$$

□

Definição 3.22. Dizemos que uma álgebra de quatérnios A é *A se fatora em F* se A satisfaz alguma das afirmações do Teorema 3.21.

Observação 3.23. De todos os critérios de fatoração de $A = \left(\frac{a,b}{F}\right)$ em F, o critério (7) do Teorema 3.21 é especialmente importante. A equação $ax^2 + by^2 = 1$ sobre o corpo F é comumente chamada de *equação de Hilbert*. Na teoria dos números elementar, essa equação é usada para definir o símbolo de Hilbert sobre $\mathbb{Q}$.

Corolário 3.24. *Seja F um corpo. Então:*

(1) *Para qualquer $a \in \dot{F}$, $\left(\frac{1,a}{F}\right)$ e $\left(\frac{a,-a}{F}\right)$ se fatoram em F;*

(2) *Se $a \in F$ e $a \notin \{0,1\}$, então $\left(\frac{a,1-a}{F}\right)$ se fatora em F;*

(3) $\left(\frac{-1,a}{F}\right)$ *se fatora em F se, e somente se, a é soma de dois quadrados em F.*

Demonstração: (1) Como $1 \in D(\langle 1, a\rangle)$ e $1 \in D(\mathbb{H}) = D(\langle a, -a\rangle)$, pelo Teorema 3.21, ambas essas álgebras de quatérnios se fatoram em F.

(2) Seja $a \in F$, tal que $a \notin \{0,1\}$. Assim $a, 1-a \in \dot{F}$. Isso implica que $\left(\frac{a,1-a}{F}\right)$ é uma álgebra de quatérnios sobre F. Tomemos a forma quadrática $q \cong \langle a, 1-a\rangle$. Note que $q((1,1)) = a1^2 + (1-a)1^2 = 1$. Isso implica que $1 \in D(q)$. Pelo Teorema 3.21 temos que $\left(\frac{a,1-a}{F}\right)$ se fatora em F.

(3) Suponha que $\left(\frac{-1,a}{F}\right)$ se fatora em F. Assim, pelo Teorema 3.21, temos que $1 \in D(\langle -1, a\rangle)$. Assim, existem $x, y \in F$, tais que $-x^2 + ay^2 = 1$. Implicando que $ay^2 = 1 + x^2$. Caso $y \neq 0$, então $a = (y^{-1})^2 + (y^{-1}x)^2$, como desejado. Caso $y = 0$, então $x^2 = -1$. Implicando que $-1 \in \dot{F}^2$. Assim, $\langle 1, 1\rangle \cong \langle 1, -1\rangle = \mathbb{H}$, em particular $D(\langle 1,1\rangle) = D(\mathbb{H}) = \dot{F}$. Segue que $a \in D(\langle 1,1\rangle)$. Então existe $c_1, c_2 \in F$ tais que $a = c_1^2 + c_2^2$, como queríamos.

Reciprocamente, suponha que a seja soma de dois quadrados em F. Sejam $c_1, c_2 \in F$, tais que $a = c_1^2 + c_2^2$. Queremos mostrar que $\left(\frac{-1,a}{F}\right)$ se fatora em F. De fato, seja a equação de Hilbert $-x^2 + ay^2 = 1$, com x, y variáveis sobre o corpo F. Como $a = c_1^2 + c_2^2$, então $-x^2 + (c_1^2 + c_2^2)y^2 = 1$. Como $a \in \dot{F}$, devemos ter $c_1 \neq 0$ ou $c_2 \neq 0$. Suponha que $c_1 \neq 0$. Assim, $x = c_2 \cdot c_1^{-1}$ e $y = c_1^{-1}$ é uma solução da equação de Hilbert. Isso implica que $1 \in D(\langle -1, a\rangle)$. Pelo Teorema 3.21 temos que $\left(\frac{-1,a}{F}\right)$ se fatora sobre F. Analogamente para o caso em que $c_2 \neq 0$. Portanto $\left(\frac{-1,a}{F}\right)$ se fatora em F. □

Corolário 3.25 (Classificação de formas binárias). *As F-formas quadráticas (regulares) $q \cong \langle a, b\rangle$ e $q' \cong \langle a', b'\rangle$ são isométricas se, e somente se, $d(q) = d(q')$ e $\left(\frac{a,b}{F}\right) \cong \left(\frac{a,b}{F}\right)$.*

Demonstração: Assumimos que $q \cong q'$. Pela Proposição 1.64, temos que $d(q) = d(q')$, ou seja, $ab\dot{F}^2 = a'b'\dot{F}^2$. Implicando que $\langle 1, -a, -b, ab\rangle \cong \langle 1, -a', -b', a'b'\rangle$. Pelo Teorema 3.21, logo $\left(\frac{a,b}{F}\right) \cong \left(\frac{a,b}{F}\right)$.

Reciprocamente, suponha que $\left(\frac{a,b}{F}\right) \cong \left(\frac{a,b}{F}\right)$ e $d(q) = d(q')$, então

$$\langle 1, -a, -b, ab\rangle \cong \langle 1, -a', -b', a'b'\rangle.$$

Pelo Cancelamento de Witt 1.60 e $\langle ab\rangle \cong \langle a'b'\rangle$, segue que $\langle -a, -b\rangle \cong \langle -a', -b'\rangle$. Multiplicando a isometria anterior por $\langle -1\rangle$, obtemos que $q \cong q'$. □

Observação 3.26. (1) Seja $F = \mathbb{Q}$. Sejam $a, b \in \mathbb{Q}$, tais que $a, b < 0$. Então $A = \left(\frac{a,b}{\mathbb{Q}}\right)$ não se fatora em F e, consequentemente, é uma álgebra com divisão.

Para provar isso, note que dados $a, b < 0$, temos que $ax^2 + by^2 \leqslant 0$, para todos $x, y \in \mathbb{Q}$. Implicando que $ax^2 + by^2 \neq 1$, para todos $x, y \in \mathbb{Q}$. Assim, pelo Teorema 3.21 item (7) A não se fatora em F.

(2) Se $F = \mathbb{R}$, e $a, b < 0 \in \mathbb{R}$, então $A = \left(\frac{a,b}{\mathbb{R}}\right) \cong \left(\frac{-1,-1}{F}\right)$. Isso segue do fato que $\dot{\mathbb{R}}/\dot{\mathbb{R}}^2 = \{1, -1\}$ e da Proposição 3.5 (1).

Exemplo 3.27. (1) $\left(\frac{-1,-1}{\mathbb{Q}}\right) \cong \left(\frac{-2,-3}{\mathbb{Q}}\right)$.

De fato, sejam $A = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ e $A' = \left(\frac{-2,-3}{\mathbb{Q}}\right)$. Para provarmos a validade desse exemplo basta termos que $N \cong N'$, onde N, N' são as formas normais de A e A', respectivamente. Assim, $N \cong \langle 1, 1, 1, 1\rangle$ e $N' \cong \langle 1, 2, 3, 6\rangle$. Como $1 = 2(1/2^2) + 2(1/2^2)$, então $1 \in D(\langle 2, 2\rangle)$, desse modo pela Proposição 1.64 temos que $\langle 2, 2\rangle \cong \langle 1, 4\rangle \cong \langle 1, 1\rangle$. Como $1 = 3(1/3^2) + 6(1/3^2)$, então $1 \in D(\langle 3, 6\rangle)$, e desse modo $\langle 3, 6\rangle \cong \langle 1, 18\rangle \cong \langle 1, 2\rangle$. Assim,

$$N \cong \langle 1, 1, 1, 1\rangle \cong \langle 1, 1, 2, 2\rangle \cong \langle 1, 3, 6, 2\rangle \cong \langle 1, 2, 3, 6\rangle \cong N'.$$

Portanto $(A, N) \cong (A', N')$.

(2) $\left(\frac{-1,-1}{\mathbb{Q}}\right) \ncong \left(\frac{-2,-5}{\mathbb{Q}}\right)$.

De fato, sejam $A = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ e $A' = \left(\frac{-2,-5}{\mathbb{Q}}\right)$. Sejam N, N' as formas normais de A e A', respectivamente. Assim, $N \cong \langle 1, 1, 1, 1\rangle$ e $N' \cong \langle 1, 2, 5, 10\rangle$. Afirmamos que $\langle 2, 5\rangle \cong \langle 7, 70\rangle$. De fato, como $7 = 2(1)^2 + 5(1)^2$, então Pela Proposição 1.64 temos que $\langle 2, 5\rangle \cong \langle 7\rangle \otimes \langle 1, 10\rangle \cong \langle 7, 70\rangle$. Assim, $\langle 1, 2, 5, 10\rangle \cong \langle 1, 7, 70, 10\rangle$.

Se $\left(\frac{-1,-1}{\mathbb{Q}}\right) \cong \left(\frac{-2,-5}{\mathbb{Q}}\right)$, então teríamos que $\langle 1, 1, 1, 1\rangle \cong \langle 1, 7, 70, 10\rangle$. Pelo Cancelamento de Witt 1.60 temos que $\langle 1, 1, 1\rangle \cong \langle 7, 70, 10\rangle$. Em particular $7 \in D(\langle 1, 1, 1\rangle)$, o que é um absurdo, pois 7 não é soma de três quadrados de números racionais. Portanto $\left(\frac{-1,-1}{\mathbb{Q}}\right) \ncong \left(\frac{-2,-5}{\mathbb{Q}}\right)$.

(3) Seja $p \in \mathbb{Q}$ um número primo ímpar. Então $\left(\frac{-1,p}{\mathbb{Q}}\right)$ se fatora em F se, e somente se, $p \equiv 1 \pmod 4$.

De fato, se $\left(\frac{-1,p}{\mathbb{Q}}\right)$ se fatora em F, então, pelo Teorema 3.21, $1 \in D_{\mathbb{Q}}(\langle -1, p\rangle)$. Assim, existem $x, y, z \in \mathbb{Z}$, tais que $z \neq 0$, $\text{mdc}(x, y, z) = 1$ e $-x^2 + py^2 = z^2$. Afirmamos que $p \nmid x$. De fato, se $p \mid x$, então $p \mid (-x^2 + py^2) = z^2$. Como p é primo, então $p \mid z$. Assim, $z = p \cdot k$ e $x = p \cdot d$, onde $k, d \in \mathbb{Z}$. Então $-p^2d^2 + py^2 = p^2k^2$. Dividindo por p, obtemos $-pd^2 + y^2 = pk^2$, ou seja, $y^2 = p \cdot (k^2 + d^2)$.

Implicando que $p \mid y^2$ e consequentemente $p \mid y$. Assim, $\text{mdc}(x, y, z) = p$, o que é um absurdo. Logo $p \nmid x$ e assim, $-x^2 + py^2 \equiv z^2 \pmod p$, implicando $-x^2 \equiv z^2 \pmod p$. Assim, $-1 \in (\dot{\mathbb{Z}}/p\mathbb{Z})^2$. Pelo Lei de Reciprocidade Quadrática da Teoria dos Números, temos que $p \equiv 1 \pmod 4$.

Reciprocamete, se $p \equiv 1 \pmod 4$, então pelo Teorema de Fermat para quadrados da Teoria dos Números, então p é soma de dois quadrados. Pelo Corolário 3.24 (3), $\left(\frac{-1,p}{F}\right)$ se fatora em F.

(4) Encontre um inteiro positivo n, tal que $\left(\frac{5,7}{\mathbb{Q}}\right) \cong \left(\frac{13,n}{\mathbb{Q}}\right)$.

Como $-12 = -5(1)^2 - 7(1)^2$, então pela Proposição 1.64 temos que

$$\langle -5, -7\rangle \cong \langle -12, -12 \cdot (-5) \cdot (-7)\rangle \cong \langle -3, -3 \cdot 35\rangle.$$

Analogamente, como $-13 = -3(4)^2 + 35(1)^2$, então $\langle -3, 35\rangle \cong \langle -13, 3 \cdot 13 \cdot 35\rangle$.

Sejam N a forma normal de $\left(\frac{5,7}{\mathbb{Q}}\right)$ e N' a forma normal de $\left(\frac{13,3\cdot 35}{\mathbb{Q}}\right)$. Assim,

$$\begin{aligned} N &\cong \langle 1, -5, -7, 35\rangle \cong \langle 1, -3, -3 \cdot 35, 35\rangle \cong \langle 1, -3 \cdot 35, -13, 3 \cdot 13 \cdot 35\rangle \\ &\cong \langle 1, -13, -3 \cdot 35, 3 \cdot 13 \cdot \cdot 35\rangle \cong N'. \end{aligned}$$

Implicando que $N \cong N'$. Logo $\left(\frac{5,7}{\mathbb{Q}}\right) \cong \left(\frac{13,3\cdot 35}{\mathbb{Q}}\right)$. Tomando $n = 3 \cdot 35$ temos o desejado.

(5) $A = \left(\frac{5,-3}{\mathbb{Q}}\right)$ é uma álgebra com divisão e $A' = \left(\frac{5,-3}{K}\right)$ não é uma álgebra com divisão, onde $K = \mathbb{Q}(\sqrt{17})$.

Suponha que A não é uma álgebra com divisão. Pelo Teorema 3.21, temos que A se fatora em F. Pelo mesmo Teorema temos que $1 \in D(\langle 5, -3\rangle)$. Assim, existem $x, y, z \in \mathbb{Z}$, tal que $\text{mdc}(x, y, z) = 1$, $z \neq 0$ e $5x^2 - 3y^2 = z^2$. Por argumento análogo ao exemplo (3) acima temos que $3 \not| \, x$ e $5x^2 \equiv z^2 \pmod 3$. Implicando que $2x^2 \equiv z^2 \pmod 3$. Então $2 \in (\dot{\mathbb{Z}}/3\mathbb{Z})^2$ $(-1 \in\in (\dot{\mathbb{Z}}/3\mathbb{Z})^2)$, o que é um absurdo. Logo $\left(\frac{5,-3}{\mathbb{Q}}\right)$ é uma álgebra com divisão.

Para $K = \mathbb{Q}(\sqrt{17})$, temos que $5(2)^2 - 3(1)^2 = 17 = (\sqrt{17})^2$. Tomando o vetor $(2/\sqrt{17}, 1/\sqrt{17})$ temos que $1 \in D(\langle 5, -3\rangle)$. Pelo Teorema 3.21 temos que A' se fatora em F. Portanto $\left(\frac{5,-3}{\mathbb{Q}(\sqrt{17})}\right)$ não é uma álgebra com divisão.

Capítulo 4

Formas Quadráticas sobre Extensões de Corpos

Uma pergunta importante de se fazer na teoria de formas quadráticas sobre corpos é o comportamento dessas formas quadráticas sobre extensões de corpos. Quais as perdas ou ganhos ao estendermos um corpo F para uma extensão algébrica ou transcendente de F.

Nesse capítulo iremos abordar formas quadráticas sobre extensões de corpos, onde veremos diferenças nas extensões algébricas de grau ímpar, de grau par e extensões transcendentes.

4.1 Transfer de Scharlau

Seja K um corpo estendido do corpo F. Dado um F-espaço quadrático (V, B, q) podemos construir um K-espaço quadrático (V_K, B_K, q_K), onde V_K é obtido de $K \otimes_F V$, e B_K é dado pela única aplicação bilinear simétrica em V_K que satisfaz

$$B_K(k \otimes v, k' \otimes v') = kk' \cdot B(v, v'), \text{ com } k, k' \in K \text{ e } v, v' \in V.$$

Analogamente, a K-forma quadrática q_K associada com B_K é dada unicamente por

$$q_K(k \otimes v) = k^2 \cdot q(v), \text{ com } k \in K \text{ e } v \in V.$$

Observação 4.1. (1) Notemos que, dados o F-espaço quadrático (V, B, q), onde $\mathcal{B} = \{v_1, \ldots, v_n\}$ uma base de V, e K/F uma extensão de corpos. Então a matriz simétrica de q na base $\{v_1, \ldots, v_n\}$ é igual a matriz simétrica de q_K com respeito a base $\{1 \otimes v_1, \ldots, 1 \otimes v_n\}$ de V_K.

De fato, como a matriz simétrica associada a q na base $\mathcal{B}$ é dada por $[B(v_i, v_j)]_n$, e do fato que $B_K(1 \otimes v_i, 1 \otimes v_j) = 1^2 \cdot B(v_i, v_j) = B(v_i, v_j)$. Então

$$[B(v_i, v_j)]_n = [B_K(1 \otimes v_i, 1 \otimes v_j)]_n.$$

(2) Como o produto tensorial é distributivo em relação a operação $\perp$ de $M(F)$ (e também $M(K)$), é fácil mostrar que a aplicação $i : M(F) \longrightarrow M(K)$, dada por $i(q) = q_K$ é um homomorfismo de monóides.

(3) Sejam K/F uma extensão de corpos e $r : F \longrightarrow K$ a aplicação inclusão. Definimos a aplicação $\widehat{r}^* : \widehat{W}(F) \longrightarrow \widehat{W}(K)$, dada por $\widehat{r}^*(V) = V_K$. Então $\widehat{r}^*$ é um F-homomorfismo de anéis.

De fato, primeiramente se $V \cong V'$, então pelo produto tensorial temos que $K \otimes_F V \cong K \otimes_F V'$, ou seja, $\widehat{r^*}(V) = \widehat{r^*}(V')$, provando que $\widehat{r^*}$ está bem definida. Tomando $V, V' \in \widehat{W}(F)$, temos que

$$\begin{aligned} \widehat{r^*}(V+V') &= \widehat{r^*}(V \perp V') \\ &= K \otimes_F (V \perp V') \\ &= K \otimes_F V \perp K \otimes_F V' \\ &= K \otimes_F V + K \otimes_F V' \\ &= \widehat{r^*}(V) + \widehat{r^*}(V'), \end{aligned} \qquad \begin{aligned} \widehat{r^*}(V \cdot V') &= \widehat{r^*}(V \otimes V') \\ &= K \otimes_F V \otimes V' \\ &= K \otimes_F K \otimes_F V \otimes V' \\ &= K \otimes_F V \otimes K \otimes_F V' \\ &= K \otimes_F V \cdot K \otimes_F V' \\ &= \widehat{r^*}(V) \cdot \widehat{r^*}(V'). \end{aligned}$$

Provando que $\widehat{r^*}$ é um F-homomorfismo de anéis.

(4) Tomando $\widehat{r^*}$ definido na observação (3) acima, temos que $\widehat{r^*}(\mathbb{H}_F) = \mathbb{H}_K$. Assim, podemos estender $\widehat{r^*}$ para $W(F)$, ou seja, $r^* : W(F) \longrightarrow W(K)$, dada por $r^*(q) = K \otimes_F q = q_K$, é um F-homomorfismo de anéis.

(5) Em geral $\widehat{r^*}$ e r^* não são necessariamente monomorfismos de anéis.

De fato, sejam F um corpo e $a \in \dot{F}$, tal que $a \notin \dot{F}^2$. Tomando $K = F(\sqrt{a})$ e $r^* : W(F) \longrightarrow W(K)$, temos que $\langle 1, -a\rangle \neq 0$. Assim,

$$r^*(\langle 1, -a\rangle) = \langle 1, -a\rangle_K = \langle 1, -(\sqrt{a})^2\rangle_K = \mathbb{H}_K = 0_{W(K)}.$$

Implicando que r^* não é injetora. Analogamente se tomarmos $\widehat{r^*}(\langle 1, -a\rangle - 0_{\widehat{W}(F)})$, obtemos que $\widehat{r^*}$ não é injetora.

Até agora vimos que podemos "ascender"do anel de Witt $W(F)$ associado ao corpo base F para $W(K)$ associado a K, onde K/F é uma extensão de corpos. Mas uma pergunta importante é se podemos tomar o caminho contrário, sair do anel $W(K)$ e "descer"para $W(F)$. Veremos que isso é possível e para isso definiremos a *transfer de Scharlau*.

Definição 4.2. Sejam F um corpo e K/F uma extensão de corpos, tal que $[K : F] < \infty$. Seja $s : K \longrightarrow F$ um F-funcional linear não nulo (note que pelo Teorema do Núcleo e da Imagem, um funcional linear não nulo sobre uma extensão finita de corpos é automaticamente sobrejetivo). Para qualquer K-espaço quadrático (U, B), podemos compor a forma bilinear simétrica $B : U \times U \longrightarrow K$ com a funcional s, gerando a F-aplicação bilinear simétrica

$$sB : U \times U \longrightarrow F.$$

Então o K-espaço quadrático (U, B) da origem a um F-espaço quadrático (U, sB) que chamaremos de *transfer de Scharlau*, que denotaremos por $s_*((U, B))$.

Proposição 4.3. *Usando a notação da definição acima, se (U, B) é um K-espaço quadrático regular, então (U, sB) é um F-espaço quadrático regular.*

Demonstração: Suponha que (U, sB) não é regular. Isso implica que existe um $x \in \dot{U}$, tal que $sB(x, u) = 0$, para todo $u \in U$. Como (U, B) é regular, então $\mathrm{rad}(U) = \{0\}$, em particular existe $y \in U$, tal que $B(x, y) \neq 0$. Tomando $c \in K$, segue que

$$0 = sB(x, \frac{c}{B(x,y)}y) = s(\frac{c}{B(x,y)}B(x, y)) = s(c).$$

Assim, $s(c) = 0$, para qualquer $c \in K$. Implicando que $s \equiv 0$, o que é uma contradição. Logo (U, sB) é um F-espaço quadrático regular. □

Observação 4.4. Sendo K/F uma extensão de corpos finita, (U, B) um K-espaço quadrático e $s : K \longrightarrow F$ uma F-funcional linear não nula, então pelo Lema das Torres da teoria de Galois temos que

$$\dim_F(s_*(U, B)) = [K : F] \cdot \dim_K((U, B)).$$

Exemplo 4.5. (1) Seja K/F uma extensão de corpos, tal que $[K : F] < \infty$. Tomando K como K-espaço vetorial e a K-aplicação bilinear simétrica $(\cdot) : K \times K \longrightarrow K$, dada por $(\cdot)(x, y) = xy$, segue que $(K, (\cdot))$ é um K-espaço quadrático unidimensional. Pelo fato que $(\cdot)(x, x) = x^2$, temos que $\langle 1\rangle_K$ é a forma quadrática associada a $(\cdot)$ por despolarização. Escolhendo $s : K \longrightarrow F$ um F-funcional linear não nulo, então a transfer $s_*(K, (\cdot)) = s_*(K, \langle 1\rangle_K)$ é dada por $(K, s(\cdot))$, onde

$$\begin{array}{rccc} s(\cdot): & K \times K & \longrightarrow & F \\ & (x, y) & \longrightarrow & s(xy) \in F. \end{array}$$

(2) Seja K/F uma extensão de corpos, tal que $[K : F] < \infty$. Da teoria de corpos sabemos que o traço do corpo

$$\begin{array}{rccc} \mathrm{tr}_{K/F}: & K & \longrightarrow & F \\ & x & \longrightarrow & \mathrm{tr}_{K/F}(x) = \mathrm{tr}\left([m_x]\right), \end{array}$$

onde $[m_x]$ é a matriz da F-transformação definida pela lei $m_x(y) = xy$, para todo $y \in K$. Assim, $\mathrm{tr}_{K/F}$ é um F-funcional linear. Podemos utilizar $\mathrm{tr}_{K/F}$ como o F-funcional linear associado ao F-espaço quadrático $(K, \langle 1\rangle_K)$, desde que $\mathrm{tr}_{K/F} \not\equiv 0$. Pela teoria de corpos temos que $\mathrm{tr}_{K/F} \not\equiv 0$ se, e somente se, K/F é uma extensão de corpos separável.

Assim, para qualquer extensão separável de corpos ($\mathrm{char}(F) \neq 2$), K/F finita, a transfer $\mathrm{tr}_*((K, \langle 1\rangle_K))$ é a aplicação bilinear simétrica

$$\begin{array}{rccc} \mathrm{tr}(\cdot): & K \times K & \longrightarrow & F \\ & (x, y) & \longrightarrow & \mathrm{tr}(xy). \end{array}$$

Pelo fato que $\mathrm{tr}(\cdot)(x, x) = \mathrm{tr}(x^2)$, segue que $x \longrightarrow \mathrm{tr}(x^2)$ é a forma quadrática associada a $\mathrm{tr}_*((K, (\cdot)))$, conhecida como *forma traço*.

De maneira mais geral, se aplicarmos tr_* em $(K, \langle a\rangle)$, onde $a \in \dot{K}$, segue que a F-forma quadrática associada a $\mathrm{tr}_*((K, \langle a\rangle))$ é dada por $x \longrightarrow \mathrm{tr}(ax^2)$, que chamamos de *forma traço escalar*.

O próximo teorema associa $\widehat{r}^*$ com a transfer de Scharlau, em que é uma ferramenta muito importante no estudo do comportamento das formas quadráticas sobre extensões de corpos.

Teorema 4.6 (**Reciprocidade de Frobenius**). *Sejam K/F uma extensão de corpos finita, $r : F \longrightarrow K$ a inclusão de F em K e $s : K \longrightarrow F$ um F-funcional linear não nulo. Sejam (V, B) um F-espaço quadrático e (U, B') um K-espaço quadrático. Então existe uma F-isometria*

$$s_*[\widehat{r}^*((V, B)) \otimes_K (U, B')] \cong (V, B) \otimes_F s_*((U, B')).$$

Em particular, tomando $(U, B') = (K, \langle 1\rangle_K)$, temos que

$$s_*(\widehat{r}^*(V, B)) \cong (V, B) \otimes_F s_*((K, \langle 1\rangle_K)).$$

Demonstração: Primeiramente definimos a seguinte aplicação

$$\psi : s_*\left[(K \otimes_F V) \otimes_K U\right] \longrightarrow V \otimes_F s_*(U),$$

estendida de $\psi((k \otimes_F v) \otimes_K u) = v \otimes_F (ku)$, onde $k \in K$, $v \in V$, $u \in U$. Como $[K : F], \dim_F(V)$ e $\dim_K(U)$ são finitas, segue que ψ está bem definida e é fácil de provar que ψ é um F-homomorfismo de espaços vetoriais.

Afirmamos que ψ é sobrejetora. De fato, é suficiente provarmos para os elementos geradores, seja $v \otimes_F u \in (V, B) \otimes_F s_*((U, B'))$. Tomando o vetor $(1 \otimes_F v) \otimes_K u \in V_K \otimes_K U$, segue que $\psi(1 \otimes_F v) \otimes_K u) = v \otimes_F (1u) = v \otimes_F u$. Provando que ψ é sobrejetora. Como

$$\begin{aligned} \dim_F(V) \cdot \dim_F(s_*(U)) &= \dim_F(V) \cdot [K : F] \cdot \dim_K(U) \\ &= \dim_F(K) \cdot \dim_F(V) \cdot \dim_K(U), \end{aligned}$$

pelo Teorema do Núcleo e da Imagem, segue que ψ é injetora. Implicando que ψ é um F-isomorfismo de espaços vetoriais.

Agora basta provarmos que ψ é isometria. De fato, como $(V, B) \otimes_F s_*((U, B')) = (V \otimes_F s_*(U), B \cdot (sB'))$, segue que dados $k, k' \in K$, $v, v' \in V$ e $u, u' \in U$, temos

$$\begin{aligned} [B \cdot (sB')](\psi((k \otimes_F v) \otimes_K u), \psi((k' \otimes_F v') \otimes_K u')) &= [B \cdot (s \circ B')](v \otimes ku, v' \otimes k'u') \\ &= B(v, v') \cdot s[B'(ku, k'u')] \\ &= B(v, v') \cdot s[kk' \cdot B'(u, u')]. \end{aligned}$$

Por outro lado

$$\begin{aligned} s(B_K \cdot B')[(k \otimes_F v) \otimes_K u, k' \otimes_F v') \otimes_K u'] &= s[B_K(k \otimes_F v, k' \otimes_F v') \cdot B'(u, u')] \\ &= s[kk' \cdot B(v, v') \cdot B'(u, u')] \\ &= B(v, v') \cdot s[kk' \cdot B'(u, u')], \end{aligned}$$

a última igualdade segue do fato que $B(v, v') \in F$. Portanto ψ é uma isometria. Logo $s_*[\widehat{r}^*(V, B) \otimes_K (U, B')] \cong (V, B) \otimes_F s_*[(U, B')]$.

Em particular, tomando $(U, B') = (K, \langle 1 \rangle_K)$, segue que $V_K \otimes_K \langle 1 \rangle_K = V_K$ e consequentemente $s_*[\widehat{r}^*(V, B')] = s_*[V_K \otimes_K \langle 1 \rangle_K] \cong (V, B) \otimes_F s_*[\langle 1 \rangle_K]$. □

A partir de agora o corpo K será uma extensão de F, tal que $[K : F] < \infty$ a menos que se diga ao contrário.

Corolário 4.7. *Se (U, B) é um K-espaço quadrático hiperbólico, então $s_*[(U, B)]$ é um F-espaço quadrático hiperbólico.*

Demonstração: Primeiramente, note que dados K-espaços quadráticos (U_1, B_1) e (U_2, B_2), temos que $s(B_1 + B_2) = s(B_1) + s(B_2)$. Implicando que

$$s_*[(U_1, B_1) \perp (U_2, B_2)] \cong s_*[(U_1, B_1)] \perp s_*[(U_2, B_2)].$$

Assim, é suficiente provarmos esse corolário para $U \cong \mathbb{H}_K$. Pela Reciprocidade de Frobenius 4.6 e do fato que (U, B) é regular, temos que

$$s_*[(U, B)] = s_*[\mathbb{H}_K] = s_*[\widehat{r}^*(\mathbb{H}_F)] \cong \mathbb{H}_F \otimes_F s_*[\langle 1 \rangle_K] \cong \dim_F(K)\mathbb{H}_F.$$

Logo $s_*[(U, B)]$ é um F-espaço quadrático hiperbólico. □

Corolário 4.8. *Nas hipóteses da Reciprocidade de Frobenius 4.6, as seguintes afirmações são verdadeiras:*

(1) *A aplicação* $(U, B') \longmapsto s_*[(U, B')]$ *define os homomorfismos de grupos*

$$s_* : \widehat{W}(K) \longrightarrow \widehat{W}(F) \quad e \quad s_* : W(K) \longrightarrow W(F).$$

(2) *A composição*

$$\widehat{W}(F) \xrightarrow{\widehat{r}^*} \widehat{W}(K) \xrightarrow{s_*} \widehat{W}(F),$$

coincide com a multiplicação por $s_*(\langle 1\rangle_K)$ *(o mesmo ocorre para* $W(F)$ *e* $W(K)$*)*

(3) $\mathrm{Im}(s_*)$ *é um ideal de* $\widehat{W}(F)$ *(o mesmo ocorre para* $W(F)$*).*

Demonstração: (1) Seja $s_* : \widehat{W}(K) \longrightarrow \widehat{W}(F)$, dada por $(U, B') \longrightarrow s_*[(U, B')]$. Pelo fato que $s_*[(U_1, B_1) \perp (U_2, B_2)] \cong s_*[(U_1, B_1)] \perp s_*[(U_2, B_2)]$, basta provarmos que s_* está bem definida. De fato, sejam $(U, B), (U', B') \in \widehat{W}(K)$, tais que $(U, B) \cong (U', B')$. Assim, existe uma isometria $\phi : U' \longrightarrow U$, tal que $B \circ \phi = B'$. Isso implica que $s(B \circ \phi) = s(B')$. Isso é suficiente para concluirmos que $s_*[(U, B)] \cong s_*[(U', B')]$. Logo $s_*[(U, B)] = s_*[(U', B')]$ em $\widehat{W}(F)$.

(2) Segue diretamente do caso particular da Reciprocidade de Frobenius 4.6.

(3) Pelo que provamos em (1) desse corolário, temos que $\mathrm{Im}(s_*)$ é um subgrupo aditivo de $(\widehat{W}(F), +)$. Assim, basta provarmos que $\mathrm{Im}(s_*)$ é fechado para a multiplicação com $\widehat{W}(F)$. Sejam $(V, B), (V', B') \in \widehat{W}(F)$, onde $(V, B) \in \mathrm{Im}(s_*)$. Como $(V, B) \in \mathrm{Id}(s_*)$, segue que existe $(U, B_1) \in \widehat{W}(K)$, tal que $s_*[(U, B_1)] = (V, B)$. Assim, tomando $s_*[\widehat{r}(V', B') \otimes_K (U, B_1)]$, temos pela Reciprocidade de Frobenius 4.6 que

$$s_*[\widehat{r}(V', B') \otimes_K (U, B_1)] \cong (V', B') \otimes_F s_*[(U, B_1)] \cong (V', B') \otimes_F (V, B).$$

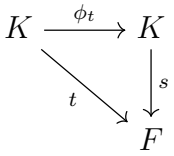
Implicando que $(V', B') \cdot (V, B) \in \mathrm{Im}(s_*)$. Logo $\mathrm{Im}(s_*)$ é ideal de $\widehat{W}(F)$. Analogamente para $W(F)$. □

Observação 4.9. Uma questão importante é se dado uma torre de extensões de corpos finita dois a dois $F \subseteq K \subseteq L$, $s : K \longrightarrow F$ e $t : L \longrightarrow K$ F-funcionais lineares não nulos, então $(s \circ t)_* = s_* \circ t_*$. Isso sai diretamente do fato que se $(V, B) \in \widehat{W}(L)$, temos que $(s \circ t)(B) = s(tB)$.

Recordemos agora um resultado sobre funcionais lineares.

Lema 4.10. *Sejam* K/F *uma extensão de corpos finita com* $\mathrm{char}(F) \neq 2$, $s : K \longrightarrow F$ *e* $t : K \longrightarrow F$ F*-funcionais lineares, tais que* s *é não nula. Então As seguintes afirmações são verdadeiras.*

(1) *Existe* $\phi_t : K \longrightarrow K$ *tal que*



é comutativo, ou seja, $t = s \circ \phi_t$.

(2) *Existe um* $k \in K$, *tal que* $t(y) = s(ky)$, *para todo* $y \in K$.

Demonstração: (1) Suponha que $[K : F] = n$. Seja $\{v_1, \ldots, v_n\}$ uma F-base de K. Segue que $s(v_i) \neq 0$, para algum $i = 1, \ldots, n$. Tomemos a aplicação

$$\begin{array}{rccc} \phi_t : & K & \longrightarrow & K \\ & y & \longrightarrow & \phi_t(y) = t(y)s(v_i)^{-1} \cdot v_i. \end{array}$$

É fácil provar que ϕ_t é F-linear. Assim,

$$s(\phi_t(y)) \;\; = \;\; s(t(y)s(v_i)^{-1} \cdot v_i) = t(y)s(v_i)^{-1} \cdot s(v_i) = t(y).$$

Portanto $t = s \circ \phi_t$.

(2) De (1), temos que $\phi_t(y) = t(y)s(v_i)^{-1}v_i$, para todo $y \in K$. Isso equivale a dizer que

$$\begin{array}{rcl} [\phi_t] \cdot y & = & s(v_i)^{-1} \cdot v_i \cdot t(y) \\ & = & s(v_i)^{-1} \cdot v_i \cdot [t] \cdot y. \end{array}$$

como $v_i \in K \cong F^n$ e $[t] \in \mathbb{M}_{1\times n}(F)$, segue que $s(v_i)^{-1} \cdot v_i \cdot [t] \in K$. Tomando $k = s(v_i)^{-1} \cdot v_i \cdot [t]$, temos que $\phi_t(y) = ky$. Assim, $t(y) = s(\phi_t(y)) = s(ky)$, para todo $y \in K$, como queríamos. □

Observação 4.11. É natural questionar até que ponto $s_* : \widehat{W}(K) \longrightarrow \widehat{W}(F)$ depende da escolha do funcional linear não nulo s. Como $s_*(\langle 1\rangle_K)$ é um F-espaço quadrático regular (pelo lema anterior e do fato que s é não nula), temos que todo F-funcional linear não nulo $K \longrightarrow F$ é da forma $z \longrightarrow s(kz)$, onde $k \in \dot{K}$. Assim, para qualquer F-funcional linear não nulo $t : K \longrightarrow F$, existe um diagrama comutativo

$$\begin{array}{ccc} \widehat{W}(K) & \xrightarrow{\langle k\rangle} & \widehat{W}(K) \\ & \searrow^{t_*} & \downarrow{\scriptstyle s_*} \\ & & \widehat{W}(F), \end{array}$$

onde $t(z) = s(kz)$, para todo $z \in K$. Dizemos que s_* e t_* são iguais a menos de automorfismos de grupos de $\widehat{W}(K)$.

Em particular, o ideal $s_*(\widehat{W}(K))$ é independente da escolha de s.

Proposição 4.12. *A transfer $s_* : \widehat{W}(K) \longrightarrow \widehat{W}(F)$ é sobrejetora se, e somente se, a forma $\langle 1\rangle_F$ está na imagem de s_*.*

Demonstração: Claramente, se s_* é sobrejetora, então $\langle 1\rangle_F \in \mathrm{Im}(s_*)$. Reciprocamente, se $\langle 1\rangle_F \in \mathrm{Im}(s_*)$, então existe $(U, B) \in \widehat{W}(K)$, tal que $s_*[(U, B)] = \langle 1\rangle_F$. Dado $a \in \dot{F}$, pela Reciprocidade de Frobenius 4.6 temos que

$$s_*[\langle a\rangle_K \otimes_K (U, B)] \;\; \cong \;\; \langle a\rangle_F \otimes_F s_*[(U, B)] \cong \langle a\rangle_F \otimes_F \langle 1\rangle_F \cong \langle a\rangle_F.$$

Assim, $\langle a\rangle \in \mathrm{Im}(s_*)$, com $a \in \dot{F}$. Como $\widehat{W}(F)$ é gerado aditivamente pelas formas $\langle a\rangle$, segue que $\widehat{W}(F) \subseteq \mathrm{Im}(s_*)$. Logo s_* é sobrejetora. □

Notação 4.13. Chamaremos o ideal $s_*(\widehat{W}(K))$ de $\widehat{W}(F)$, por *ideal transfer* relativo da extensão K/F.

Corolário 4.14. *Seja $T \subseteq W(F)$ a identificação do ideal transfer em $W(F)$ da extensão de corpos finita K/F. Seja $W(K/F)$ o núcleo do F-homomorfismo $r^* : W(F) \longrightarrow W(K)$. Então $T \cdot W(K/F) = \{0\}$.*

Demonstração: Fixando um F-funcional linear não nulo $s : K \longrightarrow F$, podemos tomar $T = \mathrm{Im}(s_*)$ em $W(F)$. Para quaisquer K-espaço quadrático (U, B') e F-espaço quadrático (V, B), pela Reciprocidade de Frobenius 4.6 temos que

$$s_*[(V_K, B_K) \otimes_K (U, B')] \cong (V, B) \otimes_F s_*[(U, B')].$$

Seja $(V_1, B_1) \otimes_F (V_2, B_2) \in T \cdot W(K/F)$. Assim, $(V_1, B_1) \in T$ e $(V_2, B_2) \in W(K/F)$. Como $(V_1, B_1) \in T$, segue que $(V_1, B_1) = s_*[(U_1, B_1')]$, com $(U_1, B_1') \in W(K)$. pelo fato que $(V_2, B_2) \in W(K/F)$, temos que $(V_{2_K}, B_{2_K}) \in \mathbb{ZH}_K$. Assim,

$$\begin{array}{rcl} s_*[(V_{2_K}, B_{2_K}) \otimes_K (U_1, B_1')] & \cong & (V_2, B_2) \otimes_F s_*[(U_1, B_1')] \\ & \cong & (V_2, B_2) \otimes_F (V_1, B_1) \\ & \cong & (V_1, B_1) \otimes_F (V_2, B_2) \end{array}$$

Como $(V_{2_K}, B_{2_K}) \in \mathbb{ZH}_K$, segue que $(V_{2_K}, B_{2_K}) \otimes_K (U_1, B_1') \in \mathbb{ZH}_K$. Pelo Corolário 4.7 segue que $(V_1, B_1) \otimes_F (V_2, B_2)$ é um F-espaço hiperbólico. Assim $(V_1, B_1) \otimes_F (V_2, B_2) = 0 \in W(F)$. Logo $T \cdot W(K/F) = \{0\}$. □

4.2 Extensões Simples e Teorema de Springer

Nosso objetivo nessa seção é olhar mais atentamente para as extensões algébricas simples $K = F(x)$ e calcular o espaço transfer $s_*(\langle 1 \rangle_K)$ com respeito a uma F-funcional linear escolhida estrategicamente. Esse calculo será extremamente útil para entendermos o homomorfismo natural $r^* : W(F) \longrightarrow W(K)$.

Definição 4.15. Seja K/F uma extensão de corpos, tal que $K = F(x)$ e $[K : F] = n$. Pela teoria de extensão de corpos, sabemos que uma F-base de K é dada por $\{1, x, \ldots, x^{n-1}\}$. Definimos o F-funcional linear $s : K \longrightarrow F$, por

$$s(1) = 1, \ s(x) = s(x^2) = \cdots = s(x^{n-1}) = 0.$$

Teorema 4.16 (Scharlau). *Com respeito a notação anterior:*

(1) *Se $n = 2m + 1$, então $s_*(\langle 1 \rangle_K) \cong m\mathbb{H}_F \perp \langle 1 \rangle_F$;*

(2) *Se $n = 2m$, então $s_*(\langle 1 \rangle_K) \cong (m-1)\mathbb{H} \perp \langle 1, -N_{K/F}(x) \rangle$.*

Demonstração: Na Seção 1 desse capítulo vimos que $s_*(\langle 1 \rangle_K)$ é dado pelo F-espaço quadrático $(K, s(\cdot))$, onde $s(\cdot)(y, z) = s(yz)$. Pela definição de s, é fácil ver que nessa estrutura quadrática os F-subespaços $F \cdot 1$ e $K_0 = \sum_{i=1}^{n-1} F \cdot x^i$ são ortogonais. Assim, $s_*[\langle 1 \rangle_K] \cong \langle 1 \rangle_F \perp K_0$. Temos dois casos para serem analisados.

Caso $n = 2m + 1$. Neste caso, $\dim_F(K_0) = n - 1 = 2m$ e K_0 é gerado pela base $\mathcal{B} = \{x, x^2, \ldots, x^m\}$. Afirmamos que K_0 é totalmente isotrópico. De fato, sejam $x^i, x^j \in \mathcal{B}$, segue que

$$s(\cdot)(x^i, x^j) = s(x^i x^j) = s(x^{i+j}) = 0,$$

pois $i+j \leqslant 2m$. Assim, pelo Teorema 1.50, temos que $m\mathbb{H}_F \subseteq K_0$. Mas pelo fato que $\dim_F(K_0) = 2m = \dim(m\mathbb{H}_F)$, segue que $K_0 \cong m\mathbb{H}_F$, implicando que $s_*(\langle 1\rangle_K) \cong \langle 1\rangle_F \perp m\mathbb{H}_F$.

Caso $n = 2m$. Agora, $\dim(K_0) = 2(m-1)+1$. Por argumento análogo ao caso anterior, temos que $K_0' \subseteq K_0$, onde K_0' é o subespaço gerado pela base $\mathcal{B} = \{x, x^2, \ldots, x^{m-1}\}$ é um subespaço totalmente isotrópico. Assim,

$$K_0 \cong (m-1)\mathbb{H} \perp K',$$

em que $\dim(K') = \dim(K_0) - 2(m-1) = 1$.

Agora vamos determinar a estrutura do espaço K' através do determinante. Se $t^n + a_{n-1}t^{n-1} + \cdot + a_0 = p(t) \in F[t]$ é o polinômio minimal de x sobre F, então a matriz simétrica associada com o F-espaço quadrático K_0 com respeito a base $\{x, x^2, \ldots, x^{n-1}\}$ é

$$M = \begin{bmatrix} 0 & 0 & \cdot & 0 & -a_0 \\ 0 & 0 & \cdot & -a_0 & * \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ -a_0 & * & \cdots & * & * \end{bmatrix} \in \mathbb{M}_{2m-1}(F).$$

De fato, como $x^n = -a_{n-1}x^{n-1} - \cdots - a_1x - a_0$, segue que

$$s(x^n) = s(-a_{n-1}x^{n-1} - \cdots - a_1x - a_0) = -a_{n-1}s(x^{n-1}) - \cdots - a_1s(x) - s(a_0) = -a_0,$$

e consequentemente,

$$s((x_i, x_j)) = s(x^{i+j}) = \begin{cases} 0 \text{ se } i+j < n \\ -a_0 \text{ se } i+j = n \\ * \text{ se } i+j > n. \end{cases}$$

Implicando que $\det(M) = (-1)^{m-1}(-a_0)^{2m-1} = (-1)^m(a_0)^{2m-1}$. Por outro lado,

$$d((m-1)\mathbb{H}_F \perp K') = (-1)^{m-1} \cdot d(K').$$

O que implica $d(K') = (-1)(a_0)^{2m-1}\dot{F}^2 = -a_0\dot{F}^2$. Assim, $K' \cong \langle -a_0\rangle_F$. Note que

$$N_{K/F}(x) = \det([m_x]) = (-1)^n a_0 = (-1)^{2m}a_0 = a_0,$$

onde $m_x(v) = xv \in K$. Então, deduzimos que

$$s_*(\langle 1\rangle_K) \cong \langle 1\rangle \perp (m-1)\mathbb{H} \perp \langle -a_0\rangle \cong \langle 1\rangle_F \perp K_0 \cong (m-1)\mathbb{H} \perp \langle 1, -N_{K/F}(x)\rangle_F.$$

□

Teorema 4.17. *Com respeito a Notação 4.15, temos:*

(1) *Se $n = 2m+1$, então $s_*(\langle x\rangle_K) \cong m\mathbb{H}_F \perp \langle N_{K/F}\rangle_F$:*

(2) *Se $n = 2m$, então $s_*(\langle x\rangle_K) \cong m\mathbb{H}_F$.*

Demonstração: (2) Se $n = 2m$, então $\{1, x, x^2, \ldots, x^{2m-1}\}$ é base do F-espaço quadrático $s_*(\langle x\rangle_K)$. Como $\{1, x, x^2, \ldots, x^{m-1}\}$ gera um subespaço $(U, (\cdot)'|_U) \subset s_*(\langle x\rangle_K)$

totalmente isotrópico e do fato que $\dim_F(U) = m$, segue pelo Teorema 1.50 que existe um espaço hiperbólico $m\mathbb{H}_F$ em $s_*(\langle x\rangle_K)$. Pelo fato que $\dim_F(m\mathbb{H}_F) = 2m = n$, logo

$$s_*[\langle x\rangle_K] \cong m\mathbb{H}_F.$$

(1) Se $n = 2m+1$, então o conjunto $\{1, x, \ldots, x^{m-1}\}$ é base de um F-subespaço totalmente isotrópico contido em K. Pelo Teorema 1.50, temos que $s_*[\langle x\rangle_K] \cong m\mathbb{H}_F \perp \langle w\rangle_F$, para algum $w \in \dot{F}$. Por um cálculo via determinante semelhante ao caso $n = 2m$ do teorema anterior, obtemos que $\langle w\rangle_F \cong \langle N_{K/F}(x)\rangle_F$. Portanto,

$$s_*(\langle x\rangle_K) \cong m\mathbb{H}_F \perp \langle N_{K/F}(x)\rangle_F.$$

□

Corolário 4.18. *Seja K/F uma extensão algébrica simples, onde $K = F(x)$. Então $s_*(\langle 1, -x\rangle_K) = \langle 1, -N_{K/F}(x)\rangle_F$ em $W(F)$.*

Demonstração:

Se $[K : F] = 2m + 1$, então pelos dois teoremas anteriores temos que

$$\begin{aligned} s_*(\langle 1, -x\rangle_K) &\cong s_*(\langle 1\rangle_K) \perp s_*(\langle -x\rangle_K) \\ &\cong m\mathbb{H}_F \perp \langle 1\rangle_F \perp m\mathbb{H}_F \perp \langle N_{K/F}(-x)\rangle_F \\ &\cong 2m\mathbb{H}_F \perp \langle 1\rangle_F \perp \langle -N_{K/F}(x)\rangle_F \\ &\cong 2m\mathbb{H}_F \perp \langle 1, -N_{K/F}(x)\rangle_F. \end{aligned}$$

A penúltima congruência acima é válida pelo fato que $2m+1$ é ímpar e assim $\det_F([m_x]) = -\det_F(m_{-x})$. Logo $s_*(\langle 1, -x\rangle_K) = \langle 1, -N_{K/F}(x)\rangle_F$ em $W(F)$.

Se $[K : F] = 2m$, o resultado segue de forma análoga utilizando os dois teoremas anteriores. □

Teorema 4.19 (Scharlau). *Seja $K = F(x)$, tal que K/F é uma extensão algébrica simples de corpos e $[K : F] = n$.*

(1) *Se $n = 2m+1$, então $r^* : W(F) \longrightarrow W(K)$ é um morfismo que se fatora na categoria dos $W(F)$-módulos, e o ideal transfer em Witt de K/F é igual a $W(F)$;*

(2) *Se $n = 2m$, então o núcleo $W(K/F)$ de $r^* : W(F) \longrightarrow W(K)$ é anulada pela forma $\langle 1, -N_{K/F}(x)\rangle_F$.*

Demonstração: Seja $s : K \longrightarrow F$ o F-funcional linear definido na Definição 4.15, seja T o ideal transfer de K/F em $W(F)$.

(1) Se $n = 2m + 1$, então pelo Corolário 4.8 temos que a composição

$$W(F) \xrightarrow{r^*} W(K) \xrightarrow{s_*} W(F)$$

coincide com a multiplicação por $s_*(\langle 1\rangle_K)$. Pelo Teorema de Scharlau 4.16 segue que $s_*(\langle 1\rangle_K) = \langle 1\rangle_F$ em $W(F)$. Implicando que

$$s_*(r^*(V, B)) \cong (V, B) \otimes_F s_*(\langle 1\rangle_K) \cong (V, B) \otimes_F \langle 1\rangle_F \cong (V, B).$$

Segue que $s_* \circ r^* = Id_{W(F)}$. Implicando que r^* fatora a sequência acima. Pelo fato que $s_* \circ r^* = Id_{W(F)}$, em particular temos que s_* é um epimorfismo de $W(F)$-módulos. Logo $T = W(F)$.

(2) Se $n = 2m$, então pelo Teorema de Scharlau 4.16 $s_*(\langle 1\rangle_K) \cong (m-1)\mathbb{H}_F \perp \langle 1, -N_{K/F}(x)\rangle$. Assim, $s_*(\langle 1\rangle_K) = \langle 1, -N_{K/F}(x)\rangle$ em $W(F)$. Isso implica que
$\langle 1, -N_{K/F}(x)\rangle \in T$. Pelo Corolário 4.14, segue que $\langle 1, -N_{K/F}(x)\rangle_F \cdot W(K/F) = \{0_{W(F)}\}$. □

Corolário 4.20. *Seja K/F uma extensão de corpos, tal que $[K : F] = 2m + 1$. Seja $r : F \longrightarrow K$ a inclusão natural de F em K. Então $r^* : W(F) \longrightarrow W(K)$ é um monomorfismo que se fatora na categoria de $W(F)$-módulos.*

Demonstração: Suponha que $[K : F] = 2m+1$. Como $[K : F] < \infty$, segue da Teoria de Extensão de Corpos que $K = F(x_1, \ldots, x_l)$, com $l \in \mathbb{Z}_+$ e $[F(x_1) : F], [F(x_1, x_2) : F(x_1)], \cdots, [K : F(x_1, \ldots, x_{l-1})] \in \mathbb{Z}_+$ são números ímpares.

Definamos $r_i : F(x_1, \ldots, x_i) \longrightarrow F(x_1, \ldots, x_i, x_{i+1})$, com $i = 1, \ldots, l-1$, a inclusão natural. Pelo Teorema de Scharlau 4.19 temos que, para cada i,

$$r_i^* : W(F(x_1, \ldots, x_i)) \longrightarrow W(F(x_1, \ldots, x_i, x_{i+1}))$$

é um monomorfismo que se fatora. Como $r = r_l \circ \cdots \circ r_1$ e $r^* = r_l^* \circ \cdots \circ r_1^*$, segue que r^* se fatora $W(K)$. □

Observação 4.21. (1) Uma consequência do corolário anterior é o fato que, se K/F é uma extensão de corpos de grau ímpar, então a aplicação natural $\phi : \dot{F}/\dot{F}^2 \longrightarrow \dot{K}/\dot{K}^2$ é injetiva.

É fácil ver que essa afirmação é verdadeira, pois se ϕ não fosse injetora, teríamos que existem $d \cdot \dot{F}^2$, $d' \cdot \dot{F}^2 \in \dot{F}/\dot{F}^2$, tais que $d \cdot \dot{F}^2 \neq d' \cdot \dot{F}^2$ e $d \cdot \dot{K}^2 = d' \cdot \dot{K}^2$. Isso implica que $dd' \in \dot{K}^2$ e $dd' \notin \dot{F}^2$. Então existe uma sub-extensão $F(\sqrt{dd'})/F$ em K/F. Pelo fato que $[F(\sqrt{dd'}) : F] = 2$, segue que $2|[K : F]$, o que é um absurdo.

(2) Em geral, para uma extensão arbitrária de corpos K/F, a injetividade de $r^* : W(F) \longrightarrow W(K)$ é uma condição mais forte do que a injetividade de $\phi : \dot{F}/\dot{F}^2 \longrightarrow \dot{K}/\dot{K}^2$.

De fato, se ϕ não for injetora, então existe $d \notin \dot{F}^2$, tal que $d \in \dot{K}^2$. Tomando o F-espaço quadrático $(F^2, \langle 1, -d\rangle_F)$, temos que $\langle 1, -d\rangle_F \ncong \mathbb{H}_F$, mas $\langle 1, -d\rangle_K \cong \mathbb{H}_K$.

Teorema 4.22 (Springer). *Seja K/F uma extensão de corpos de grau ímpar. Se q é uma F-forma quadrática anisotrópica, então q_K é uma K-forma quadrática anisotrópica.*

Demonstração: Suponha que a extensão de corpos finita de grau ímpar K/F e o F-espaço quadrático (V, q), tal que $q \cong \langle a_1, \ldots, a_l\rangle_F$, gerem um contra-exemplo com $n = [K : F]$ minimal. Pelo fato que n é minimal, podemos supor que K/F é uma extensão de corpos simples, pois caso contrário teríamos um número finito de sub-extensões simples de grau ímpar de K/F. Assim, seja x, tal que $K = F(x)$ e $p(t) \in F[t]$ o polinômio minimal de x sobre F. Como $q_K \cong \langle a_1, \ldots, a_l\rangle_K$ é K-isotrópica, segue que existe $0 \neq v = (\alpha_1, \ldots, \alpha_l) \in V_K$, tal que $q_K(v) = 0$, ou seja

$$a_1\alpha_1^2 + \cdots + a_l\alpha_l^2 = 0.$$

Pelo fato que $\alpha_j \in K$, para todo $j = 1, \ldots, l$, temos que $\alpha_j = \gamma_{0j} + \gamma_{1j}x + \cdots + \gamma_{(n-1)j}x^{n-1}$. Escolhendo $g_j(t) = \gamma_{0j} + \gamma_{1j}t + \cdots + \gamma_{(n-1)j}t^{n-1} \in F[t]$, segue que $g_j(x) = \alpha_j$, para todo $j = 1, \ldots, l$. Assim,

$$q[g_1(t), \ldots, g_l(t)](x) = q[g_1(x), \ldots, g_l(x)] = a_1\alpha_1^2 + \cdots + a_l\alpha_l^2 = 0.$$

Pela Teoria de Extensão de corpos temos que $p(t)|q[g_1(t), \ldots, g_l(t)]$, ou seja,

$$q[g_1(t), \ldots, g_l(t)] = p(t) \cdot h(t) \in F[t],$$

com $b = \max_j(\deg(g_j)) \leqslant n-1$. Note que g_j's não são todos nulos, pois $v \neq 0$.

Se existir um polinômio irredutível $f(t) \in F[t]$ que divide todos os g_j's, então $f(t)^2|g_j(t)^2$ e consequentemente,

$$f(t)^2 \left| \sum_{j=1}^{l} a_j(g_j(t))^2 \right.$$

Assim, $f(t)^2|p(t) \cdot h(t)$. Pela irredutibilidade de $p(t)$ em $F[t]$, temos que $f(t)^2|h(t)$. Então

$$q\left[\frac{g_1(t)}{f(t)^2}, \frac{g_2(t)}{f(t)^2}, \cdots, \frac{g_l(t)}{f(t)^2}\right](x) = p(x) \cdot \frac{h(x)}{f(x)^2} = 0.$$

Implicando que $q\left(g_1^*(t), g_2^*(t), \ldots, g_l^*(t)\right) = p(t) \cdot h^*(t)$, onde $g_j^*(t) = \frac{g_j(t)}{f(t)^2}$, $h^*(t) = \frac{h(t)}{f(t)^2}$ e $\deg(g_j^*(t)) \leqslant n-1$. Note que, como $g_j^*(t) = \frac{g_j(t)}{f(t)^2}$, segue que $g_j^*(t)$'s não são todos nulos. Trocando os g_j's se necessário (como mostrado acima), podemos assumir que não existe polinômio irredutível $f(t) \in K[t]$ que divide todos os g_j's.

Esta condição implica que $\sum_j F[t] \cdot g_j(t) = F[t]$. De fato, é fácil ver que $\sum_j F[t] \cdot g_j(t) \subseteq F[t]$. Para a inclusão contrária, note que $\mathrm{mdc}(g_1(t), \ldots, g_l(t)) = 1$ (retirando os $g_j(t) = 0$). Assim, tomando $z(t) \in F[t]$, temos que existe $\beta_1(t), \ldots, \beta_l(t) \in F[t]$, tal que

$$z(t) \cdot 1 = [z(t) \cdot \beta_1(t)]g_1(t) + \cdots + [z(t) \cdot \beta_l(t)]g_l(t).$$

Provando que $\sum_j F[t] \cdot g_j(t) = F[t]$.

Pelo fato que q é F-anisotrópica, segue que q não tem uma sub-forma quadrática $\langle 1, -1\rangle$, em particular, $\deg(q[g_1(t), \cdots, g_l(t)]) = 2b < 2n-2$. Como $\deg(p(t)) = n$ é ímpar, segue que $\deg(h(t))$ é ímpar e $\deg(h(t)) \leqslant n-2$. Tomando uma raiz $y \in \overline{F}$ de um fator irredutível de grau ímpar de $h(t)$ em $F[t]$. Temos que

$$q[g_1(y), \cdots, q_l(y)] = p(y) \cdot h(y) = 0.$$

Implicando que $(g_1(y), \cdots, g_l(y))$ é um vetor isotrópico de $q_{F(y)}$. Pela escolha de y, $[F(y) : F] \leqslant n-2$ e é ímpar, o que contradiz a minimalidade de n. □

Observamos que o Teorema de Springer é originalmente uma conjectura de Witt. O próximo resultado é essencialmente equivalente a esta conjectura.

Corolário 4.23. *Seja K/F como no Teorema de Springer, e seja $a \in \dot{F}$. Para qualquer F-forma quadrática q_0, $a \in D_F(q_0)$ se, e somente se, $a \in D_K(q_{0_K})$.*

Demonstração: Se $a \in D_F(q_0)$, então obviamente $a \in D_K(\langle 1\rangle_K \otimes_F q_0)$.

Reciprocamente, suponha que $a \in D_K(q_{0_K})$. Assim, tomemos $q_k := q_{0_K} \perp \langle -a\rangle_K$. Pelo 1° Teorema de Representação 1.52 temos que q_k é K-isotrópica. Tomando $q := q_0 \perp \langle -a\rangle_F$, temos pela contra-positiva do Teorema de Springer 4.22 que q é isotrópica. Logo $a \in D_F(q_0)$. □

O Teorema de Springer nos dá um bom controle sobre os espaços quadráticos sobre extensões de corpos finitas de grau ímpar. Assim, basta verificarmos o que ocorre com extensões de grau par e nas extensões transcendentais. Na próxima seção iremos verificar o que ocorre com os espaços quadráticos em extensões de grau 2.

4.3 Extensões Quadráticas

Ao considerarmos extensões de corpos de grau par, podemos observar que perdemos alguns resultados importantes, como o Teorema de Springer 4.22. Para vermos mais claramente porque esses resultados são falhos para extensões de corpos de grau par, teremos como foco o caso de extensões quadráticas.

Sejam F um corpo e $a \in \dot{F}$, tal que $a \notin \dot{F}^2$. No decorrer desta seção, denotaremos por $K = F(\sqrt{a})$, a extensão quadrática obtida pela adjunção de $\sqrt{a}$ ao corpo F. Escreveremos $\alpha := \langle 1, -a\rangle_F$, a F-forma anisotrópica que se torna um plano hiperbólico sobre K.

Teorema 4.24. *Seja q uma F-forma anisotrópica. Então q_K é F-isotrópica se, e somente se, q contém uma sub-forma binária isométrica à $\langle b\rangle \otimes \alpha$, para algum $b \in \dot{F}$.*

Demonstração: Seja $q \cong \langle b_1, \ldots, b_n\rangle$ e assuma que q_K é isotrópica. Como $\{1, \sqrt{a}\}$ é uma F-base de K, segue que existe uma equação

$$\sum_{i=1}^{n} b_i(x_i + y_i\sqrt{a})^2 = 0,$$

com $x_i, y_i \in F$ não todos nulos. Por alguns cálculos simples temos que

$$\sum_{i=1}^{n} b_i x_i^2 + a\sum_{i=1}^{n} b_i y_i^2 + 2\left(\sum_{i=1}^{n} b_i x_i y_i\right)\sqrt{a} = 0 + 0\sqrt{a}.$$

Implicando que $\sum_{i=1}^{n} b_i x_i^2 + a\sum_{i=1}^{n} b_i y_i^2 = 0$ e $\sum_{i=1}^{n} b_i x_i y_i = 0$. Como $\sum_{i=1}^{n} b_i x_i y_i = 0$, segue que os vetores $x = (x_1, \ldots, x_n)$ e $y = (y_1, \ldots, y_n)$ são ortogonais no espaço quadrático (F^n, q). Pelas equações acima temos que $q(x) = -aq(y)$. Isso implica que x e y são ambos não nulos, pois q é anisotrópica e $a \in \dot{F}$. Pelo fato que $q(x), q(y) \in D_F(q)$ e como x e y são ortogonais, pelo Critério de Representação 1.37 temos que $q \cong \langle q(x), q(y)\rangle \perp q'$. Note que

$$\langle q(x), q(y)\rangle \cong \langle -aq(y), q(y)\rangle \cong \langle q(y)\rangle \otimes_F \alpha.$$

Tomando $q(y) = b$, obtemos que $q \cong \langle b\rangle \otimes_F \alpha \perp q'$, como desejado.

Reciprocamente, suponha que $q \cong \langle b\rangle \otimes \alpha \perp q'$, com $b \in \dot{F}$. Assim,

$$\begin{aligned} q_K &\cong \langle 1\rangle_K \otimes_F \langle b\rangle \otimes \alpha \perp q' \\ &\cong \langle b\rangle_K \otimes \alpha_K \perp q'_K \\ &\cong \langle b\rangle_K \otimes \mathbb{H}_K \perp q'_K \\ &\cong \mathbb{H}_K \perp q'_K, \end{aligned}$$

pois $\alpha_K \cong \mathbb{H}_K$. Logo q_K é K-isotrópica. □

Teorema 4.25. *Uma F-forma quadrática anisotrópica, q se torna hiperbólica sobre K se, e somente se, $q \cong q' \otimes \alpha$, para alguma F-forma quadrática q'. Em particular, o núcleo $W(K/F)$ de $r^* : W(F) \longrightarrow W(K)$ é dado pelo ideal principal $W(F)\cdot\alpha$.*

Demonstração: Primeiramente, note que se $0 \neq q$ em $W(F)$, tal que $r^*(q) = 0 \in W(K)$, então $\dim_F(q) = [K : F]\dim_K(q_K)$ é par, pois $[K : F] = 2$.

Provaremos por indução sobre $m = \frac{\dim_F(q)}{2}$. Se $m = 1$, então $\dim_F(q) = 2$. Como q_K é hiperbólica, pelo Teorema 4.24, temos que $\langle b\rangle \otimes \alpha$ é uma sub-forma de q, com $b \in \dot{F}$. Mas $\dim_F(\langle b\rangle \otimes \alpha) = 2$ e $\langle b\rangle \otimes \alpha \neq 0$ em $W(F)$, logo $q \cong \langle b\rangle \otimes \alpha$.

Suponha que a implicação seja válida para $1 \leqslant i < m$, vamos mostrar que vale para m. Como q_K é K- hiperbólica, pelo Teorema 4.24, temos que, $q \cong \langle b\rangle \otimes \alpha \perp q'$, com $b \in \dot{F}$ e q' uma F-forma quadrática anisotrópica. Como $\dim_F(\langle b\rangle \otimes \alpha) = 2$, segue que $\dim_F(q') = 2m - 2$. Assim,

$$\begin{aligned} z\mathbb{H}_K = 0 = r^*(q) &= r^*(\langle b\rangle \otimes \alpha \perp q') \\ &= r^*(\langle b\rangle \otimes \alpha + q') \\ &= r^*(\langle b\rangle \otimes \alpha) + r^*(q') \\ &= \mathbb{H}_K + r^*(q'). \end{aligned}$$

Pelo Cancelamento de Witt 1.60 temos que $q'_K = r^*(q') = (z-1)\mathbb{H}_K$. Assim, podemos aplicar a hipótese de indução em q'. Implicando que $q' \cong q'' \otimes \alpha$, onde q'' é uma F-forma quadrática anisotrópica. Então

$$q \cong \langle b\rangle \otimes \alpha \perp q'' \otimes \alpha \cong (\langle b\rangle \perp q'') \otimes \alpha.$$

Provando a implicação para m. Pelo Princípio de Indução, a implicação é válida para todo $m \in \mathbb{Z}_+$.

Reciprocamente, seja q uma F-forma quadrática anisotrópica, tal que $q \cong q' \otimes \alpha$. Assim,

$$q_K = r^*(q) = r^*(q' \otimes \alpha) = q'_K \otimes \alpha_K = q'_K \otimes \mathbb{H}_K = q'_K.0_{W(K)} = 0_{W(K)}.$$

Provando que q_K é K-hiperbólica.

Em particular, $q_K = r^*(q) = 0$ em $W(F)$ se, e somente se $q = q' \otimes \alpha$, ou seja $q \in W(K/F)$ se, e somente se, $q \in W(F)\cdot\alpha$. □

Corolário 4.26. *Seja q uma F-forma quadrática, tal que $\dim_F(q) = 2m$ e q_K é K-hiperbólica, onde $K = F(\sqrt{a})$. Então:*

(1) $\langle -a\rangle_F \otimes q \cong q$;

(2) *Se q é F-anisotrópica, então $d(q) = (-a)^m$ e $d_\pm(q) = a^m$;*

(3) *Se q torna-se hiperbólica sobre $F(\sqrt{-a})$, então $2q = 0$ em $W(F)$.*

Demonstração: (1) Pela Decomposição de Witt 1.61 temos que $q \cong r\mathbb{H}_F \perp q_a$, onde q_a é uma F-forma quadrática anisotrópica. Como q_K é K-hiperbólica, pelo Teorema 4.25, segue que $q \cong r\mathbb{H}_F \perp q' \otimes \alpha$. Assim,

$$\begin{aligned}\langle -a\rangle \otimes q &\cong \langle -a\rangle \otimes (r\mathbb{H}_F \perp q' \otimes \alpha)\\ &\cong \langle -a\rangle \otimes r\mathbb{H}_F \perp \langle -a\rangle \otimes q' \otimes \alpha\\ &\cong (r\dim_F(\langle -a\rangle))\mathbb{H}_F \perp q' \otimes \langle -a\rangle \otimes \langle 1, -a\rangle\\ &\cong r\mathbb{H}_F \perp q'\langle -a, a^2\rangle\\ &\cong r\mathbb{H}_F \perp q' \otimes \alpha \cong q.\end{aligned}$$

Portanto, $\langle -a\rangle \otimes q \cong q$.

(2) Suponha que q é F-anisotrópica. Pelo Teorema 4.25 existe uma F-forma quadrática q', tal que $q \cong q' \otimes \alpha$. Como $\dim_F(\alpha) = 2$, segue que $\dim_F(q') = m$. Pelo fato que $q \cong q' \otimes \alpha \cong q' \otimes \langle 1, -a\rangle \cong q' \perp q' \otimes \langle -a\rangle$, temos que

$$d(q) = d(q' \perp q' \otimes \langle -a\rangle) = d(q')d(q')(-a)^m \cdot \dot{F}^2 = (-a)^m \cdot \dot{F}^2 \text{ e}$$

$$d_\pm(q) = (-a)^{\frac{2m(2m-1)}{2}} d(q) = [(-1)^{2m-1}]^m (-a)^m \cdot \dot{F}^2 = (a)^m \cdot \dot{F}^2.$$

(3) Suponha que $q_{F(\sqrt{-a})}$ é $F(\sqrt{-a})$-hiperbólica. Assim, pelo item (1) desse corolário no caso $K = F(\sqrt{-a})$ temos que $\langle -(-a)\rangle \otimes q \cong q$, ou seja, $\langle a\rangle \otimes q \cong q$. Do item (1) desse corolário, temos também que $\langle -a\rangle \otimes q \cong q$. Assim,

$$2q \cong q \perp q \cong \langle -a\rangle \otimes q \perp \langle a\rangle \otimes q \cong \langle a, -a\rangle \otimes q \cong \mathbb{H}_F \otimes q.$$

Tomando $2q$ em $W(F)$, temos que $2q = 0$. □

Nosso próximo passo é calcular o ideal transfer de uma extensão quadrática K/F. Para esse cálculo, o F-funcional linear mais conveniente é $s : K \longrightarrow F$, estendido de $s(1) = 0$ e $s(\sqrt{a}) = 1$.

Teorema 4.27. *Sejam K e F como anteriormente e $s : K \longrightarrow F$ o F-funcional linear definido por $s(1) = 0$ e $s(\sqrt{a}) = 1$. Então:*

(1) *Para qualquer $x \in \dot{K}$, $s_*(\langle x\rangle) \cong \langle c\rangle \otimes \langle 1, -N_{K/F}(x)\rangle$, para algum $c \in \dot{F}$. Em particular $s_*(\langle b\rangle_K) \cong \mathbb{H}_F$, para todo $b \in \dot{F}$.*

(2) *O ideal transfer T de K/F é gerado pelas formas binárias $\langle 1, -N_{K/F}(x)\rangle$, onde $x \in \dot{K}$. Em particular $T \subseteq IF$.*

(3) *$T = \text{ann}(\alpha)$, o anulador de α em $W(F)$.*

Demonstração: (1) Seja $x \in \dot{K}$. O espaço transfer $s_*(\langle x\rangle)$ é dado por $(K, s \circ (\cdot)')$, onde $(\cdot)'(y, z) = xyz$. Em relação a F-base $\{1, \sqrt{a}\}$ de K, a matriz simétrica associada a $s \circ (\cdot)'$ é

$$M = \begin{bmatrix} s(x) & s(x\sqrt{a}) \\ s(x\sqrt{a}) & s(ax) \end{bmatrix}.$$

Se $x = b + e\sqrt{a}$, com $b, e \in \dot{F}$, então

$$M = \begin{bmatrix} s(a + e\sqrt{a}) & s(ae + b\sqrt{a}) \\ s(ae + b\sqrt{a}) & s(ab + ae\sqrt{a}) \end{bmatrix} = \begin{bmatrix} e & b \\ b & ae \end{bmatrix}.$$

Implicando que $\det(M) = ae^2 - b^2 = -(b^2 - ae^2) = -N_{K/F}(x)$. Como $\dim_F(s_*(\langle x\rangle)) = \dim_F(K) = 2$, se $s(x) \neq 0$, então $s(x) \in D_F(s_*[\langle x\rangle])$ e pela Proposição 1.64 temos que

$$\begin{aligned} s_*(\langle x\rangle) &\cong \langle s(x), -N_{K/F}(x)\cdot s(x)\rangle \\ &\cong \langle s(x)\rangle \otimes \langle 1, -N_{K/F}(x)\rangle. \end{aligned}$$

Tomando $c = s(x)$, obtemos que $s_*(\langle x\rangle) \cong \langle c\rangle \otimes \langle 1, -N_{K/F}(x)\rangle$ como desejado.

Caso $s(x) = 0$, então $x = b + 0\sqrt{a}$. Pela reciprocidade de Frobenius 4.6, temos que

$$s_*(\langle x\rangle) \cong s_*(\langle x\rangle_K) \cong \langle b\rangle \otimes s_*(\langle 1\rangle_K).$$

Afirmamos que $s_*(\langle 1\rangle_K) \cong \mathbb{H}_F$. De fato, com as respectivas base $\{1, \sqrt{a}\}$ e s, temos que

$$M_{s_*[\langle 1\rangle_K]} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Implicando que $\det(s_*()\langle 1\rangle_K)) = -1$. Como $2 = s[(1+1\sqrt{a})^2] \in D_F(s_*(\langle 1\rangle_K))$, segue que

$$s_*(\langle 1\rangle_K) \cong \langle 2, -2\rangle \cong \mathbb{H}_F.$$

Provando a afirmação. Assim,

$$\begin{aligned} s_*(\langle x\rangle) &\cong \langle b\rangle \otimes \mathbb{H}_F \cong \langle b\rangle \otimes \langle 1, -1\rangle \\ &\cong \langle b\rangle \otimes \langle 1, -b^2\rangle \cong \langle b\rangle \otimes \langle 1, -N_{K/F}(x)\rangle. \end{aligned}$$

Implicando que $s_*(\langle x\rangle_K) \cong \langle b\rangle \otimes \langle 1, -N_{K/F}(x)\rangle$. Tomando $b = c$, temos o desejado.

Em particular, se $b \in \dot{F}$, então $s_*(\langle b\rangle_K) \cong \langle b\rangle \otimes \mathbb{H}_F \cong \mathbb{H}_F$.

(2) Seja T o ideal transfer de K/F em $W(F)$. Isso implica que $T = s_*(W(K))$. Seja $s_*(q') \in W(F)$, onde $q' \cong \langle a_1, \cdots, a_n\rangle = \sum_{i=1}^n \langle a_i\rangle \in W(K)$. Pelo item (1) desse teorema temos que

$$s_*(q') = \sum_{i=1}^n (s_*()\langle a_i\rangle)) = \sum_{i=1}^n \left[\langle c_i\rangle \otimes \langle 1, -N_{K/F}(a_i)\rangle\right],$$

com $c_i \in \dot{F}$. Assim, $s_*(q') = \sum_{i=1}^n \left[\langle c_i\rangle \otimes \langle 1, -N_{K/F}(a_i)\rangle\right]$ em $W(F)$. Como q' foi escolhida arbitrariamente, T é gerado por formas binárias $\langle 1, -N_{K/F}(x)\rangle$, com $x \in \dot{K}$.

(3) Pelo fato que $\alpha \in W(K/F)$, pelo Corolário 4.14, segue que $T \cdot \alpha = \{0\}$. Implicando que $T \subseteq \operatorname{ann}(\alpha)$.

Reciprocamente, seja $q \in \operatorname{ann}(\alpha)$. Isso implica que $q \otimes \alpha = 0$ em $W(F)$. Assim,

$$0 = q \otimes \alpha = q \otimes \langle 1, -a\rangle = q - \langle a\rangle \otimes q,$$

ou seja, $q = \langle a\rangle \otimes q$. Como $a \notin \dot{F}^2$ e $d(q) = a^{\dim_F(q)} \cdot d(q)$, segue que $\dim_F(q)$ é par.

Podemos mostrar que se $a \in \dot{F}$ e q uma F-forma quadrática, tal que $\dim_F(q) = 2m$, onde $m \in \mathbb{Z}_+$. Então $q \cong \langle a\rangle \otimes q$ se, e somente se, $q \cong q_1 \perp \cdots \perp q_m$, onde cada q_i é uma forma binária, tal que $q_i \cong \langle a\rangle \otimes q_i$.

Pela afirmação acima, podemos decompor q em $q_1 \perp \cdots \perp q_m$, onde q_i é uma F-forma quadrática binária, tal que $q_i \cong \langle a\rangle \otimes q_i$. Seja $c_i \in D(q_i)$. Pela Proposição 1.64 temos que $q_i \cong \langle c_i\rangle \otimes \langle 1, -d(q_i)\rangle$. Isso implica que $\langle 1, d(q_i)\rangle \cong \langle a\rangle \otimes \langle 1, d(q_i)\rangle \cong \langle a, ad(q_i)\rangle$. Assim, $\langle 1, -a\rangle = \langle -d(q_i), ad(q_i)\rangle$. Isso implica que $-d(q_i) \in D(\alpha)$. Como α é a forma

normal da extensão de corpos K/F, segue que $-d(q_i) = N_{K/F}(x_i)$, para algum $x_i \in \dot{K}$. Pelo item (1) desse teorema, temos que $q_i \cong \langle c_i\rangle \otimes \langle 1, -N_{K/F}(x_i)\rangle \in T$. Então $q = \sum_{i=1}^{m}[\langle c_i\rangle \otimes \langle 1, -N_{K/F}(x_i)\rangle] \in T$. Provando que $\text{ann}(\alpha) \subseteq T$. Logo $\text{ann}(\alpha) = T$. □

Teorema 4.28 (**Triângulo Exato**). *Seja $r : F \longrightarrow K$ a aplicação inclusão, seja $s : K \longrightarrow F$ o F-funcional linear, estendido de $s(1) = 0$ e $s(\sqrt{a}) = 1$. Se $t : W(F) \longrightarrow W(F)$ é dado por $t(q) = q \otimes \alpha$, então temos um triângulo exato*

$$\begin{array}{ccc} W(F(\sqrt{a})) & \xrightarrow{s_*} & W(F) \\ & {\scriptstyle r^*}\nwarrow & \downarrow{\scriptstyle t} \\ & & W(F) \end{array}$$

Demonstração: Primeiramente, note que r, s e t estão bem definidos e eles são homomorfismos de grupos aditivos.

Afirmamos que $\text{Im}(r^*) = \ker(s_*)$. De fato, pelo Teorema 4.27 item (1), temos que $s_*(\langle 1\rangle_K) \cong \mathbb{H}_F$. Assim, dado $q = \langle a_1, \ldots, a_n\rangle \in W(F)$, temos que

$$s_*(q_K) = \sum_{i=1}^{n}[\langle c_i\rangle \otimes s_*(\langle 1\rangle_K)] = n\mathbb{H}_F = 0,$$

em $W(F)$. Implicando que $\text{Im}(r^*) \subseteq \ker(s_*)$. Reciprocamente, seja (V, B) um K-espaço quadrático anisotrópico, tal que $s_*((V, B)) = 0_{W(F)} = r\mathbb{H}_F$. Provaremos por indução sobre $\dim_K(V) = n$ que $(V, B) \in \text{Im}(r^*)$. Suponha que $\dim_K(V) = 1$. Como $s_*[(V, B)]$ é hiperbólico, em particular, $s_*[(V, B)]$ é isotrópico. Assim, existe $v \in V$ não nulo, tal que $s_*(B(v, v)) = 0$. Pela definição de s, temos que $B(v, v) \in \dot{F}$. Seja $b = B(v, v)$. Pelo Critério de Representação 1.37 temos que $(V, B) \cong_K \langle b\rangle_K \perp V_0$. Como $\dim_K(V) = 1$, segue que $V \cong \langle b\rangle_K$. Isso implica que $(V, B) \in \text{Im}(r^*)$.

Suponha que a contingência $\ker(s_*) \subseteq \text{Im}(r^*)$ seja válida para todo K-espaço quadrático (V, B), com $1 \leqslant \dim_K(V) < n$. Seja (V', B') um K-espaço quadrático, tal que $\dim_K(V') = n$ e $(V', B') \in \ker(s_*)$. Por construção análoga a já feita, temos que

$$(V', B') \cong \langle b'\rangle_K \perp V_0',$$

com $b' \in \dot{F}$. Como $s_*[\langle b'\rangle_K] \cong \mathbb{H}_F$, segue que $s_*[(V_0', B'|_{V_0'})]$ é hiperbólico. Assim, $V_0' \in \ker(s_*)$. Pelo fato que $\dim_K(v_0') = n - 1$, pela hipótese de indução segue que $(V_0', B'|_{V_0'}) \in \text{Im}(r^*)$. Pelo fato que $\langle b'\rangle_K, (V_0', B'|_{V_0'}) \in \text{Im}(r^*)$, segue que $(V', B') \in \text{Im}(r^*)$. Provando que $\ker(s_*) \subseteq \text{Im}(r^*)$. Logo $\ker(s_*) = \text{Im}(r^*)$.

Provaremos agora que $\text{Im}(s_*) = \ker(t)$. De fato, pelo Teorema 4.27 (3), temos que $\text{Im}(s_*) = T = \text{ann}(\alpha)$. Como $\ker(t) = \{q \in W(F), \text{ tal que } q \otimes \alpha = 0\}$, segue que $\ker(t) = \text{ann}(\alpha)$. Logo $\text{Im}(s_*) = \ker(t)$.

Finalmente, a igualdade $\text{Im}(t) = \ker(r^*)$ é implicação direta do Teorema 4.25. Portanto o triângulo é exato. □

Teorema 4.29. *Sejam $g : \{\dot{F}^2, a\dot{F}^2\} \longrightarrow \dot{F}/\dot{F}^2$, a inclusão natural,*

$$\begin{array}{rccc} \phi : & \dot{F}/\dot{F}^2 & \longrightarrow & \dot{K}/\dot{K}^2 \\ & r\dot{F}^2 & \longmapsto & r\dot{K}^2 \ e \end{array}$$

$$\begin{array}{rccc} N: & \dot{K}/\dot{K}^2 & \longrightarrow & \dot{F}/\dot{F}^2 \\ & x\dot{K}^2 & \longmapsto & N_{K/F}(x)\dot{F}^2. \end{array}$$

Então a seguinte sequência é exata

$$1 \longrightarrow \{\dot{F}^2, a\dot{F}^2\} \xrightarrow{g} \dot{F}/\dot{F}^2 \xrightarrow{\phi} \dot{K}/\dot{K}^2 \xrightarrow{N} \dot{F}/\dot{F}^2.$$

Demonstração: Primeiramente, note que pelas definições de g, ϕ e N temos que essas aplicações estão bem definidas e são homomorfismos de grupos, e assim a sequência está bem definida.

Inicialmente, provaremos que $\mathrm{Im}(g) = \ker(\phi)$. Seja $c\dot{F}^2 \in \ker(\phi)$. Isso implica que $\phi(c\dot{F}^2) = 1\dot{K}^2$. Assim, $r^*(\langle 1, -c\rangle) = \langle 1, -c\rangle_K = \mathbb{H}_K = 0$. Caso $c\dot{F}^2 = 1\dot{F}^2$, segue que $c\dot{F}^2 \in \mathrm{Im}(g)$. Caso $c\dot{F}^2 \neq 1\dot{F}^2$, então $\langle 1, -c\rangle$ é F-anisotrópica. Pelo Teorema 4.25, temos que

$$\langle 1, -c\rangle \cong q' \otimes \alpha.$$

Pelo fato que $\dim_F(\langle 1, -c\rangle) = \dim_F(\alpha) = 2$, segue que $\langle 1, -c\rangle \cong \langle b\rangle \otimes \langle 1, -a\rangle$, com $b \in \dot{F}$, em particular $c\dot{F}^2 = a\dot{F}^2$. Então $\ker(\phi) \subseteq \mathrm{Im}(g)$. Reciprocamente, como $1 = 1^2 \in \dot{K}^2$ e $a = \sqrt{a}^2 \in \dot{K}^2$, temos que $\mathrm{Im}(g) \subseteq \ker(\phi)$. Logo $\mathrm{Im}(g) = \ker(\phi)$.

Provaremos agora que $\mathrm{Im}(\phi) = \ker(N)$. De fato, seja $z\dot{K}^2 \in \mathrm{Im}(\phi)$. Como $z \in \dot{F}$, segue que

$$N(z\dot{K}^2) = N_{K/F}(z)\dot{F}^2 = z^2\dot{F}^2 = 1\dot{F}^2.$$

Implicando que $z\dot{K}^2 \in \ker(N)$. Então $\mathrm{Im}(\phi) \subseteq \ker(N)$. Reciprocamente, seja $x\dot{K}^2 \in \ker(N)$. Isso implica que $N_{K/F}(x) \in \dot{F}^2$. Pelo Teorema 4.27 temos que

$$s_*(\langle x\rangle) \cong \langle c\rangle \otimes \langle 1, -N_{K/F}(x)\rangle \cong \mathbb{H}_F.$$

Implicando que $\langle x\rangle \in \ker(s_*)$. Pelo Teorema do Triângulo Exato 4.28, temos que $\langle x\rangle \in \mathrm{Im}(r^*)$. Assim, $x \in \dot{F}$. Implicando que $x\dot{K}^2 \in \mathrm{Im}(\phi)$. Então $\ker(N) \subseteq \mathrm{Im}(\phi)$, e portanto $\mathrm{Im}(\phi) = \ker(N)$. □

Corolário 4.30. *Para uma extensão quadrática K/F, temos que*

$$\left|\dot{F}/\dot{F}^2\right| < \infty \text{ se, e somente se, } \left|\dot{K}/\dot{K}^2\right| < \infty.$$

Mais precisamente, a seguinte equação é satisfeita:

$$\frac{1}{2}\left|\dot{F}/\dot{F}^2\right| \leqslant \left|\dot{K}/\dot{K}^2\right| \leqslant \frac{1}{2}\left|\dot{F}/\dot{F}^2\right|^2.$$

Demonstração: Seja K/F uma extensão quadrática. Pelo Teorema 4.29, temos que a seguinte sequência é exata

$$1 \longrightarrow \{\dot{F}^2, a\dot{F}^2\} \xrightarrow{g} \dot{F}/\dot{F}^2 \xrightarrow{\phi} \dot{K}/\dot{K}^2 \xrightarrow{N} \dot{F}/\dot{F}^2.$$

Como ϕ é um homomorfismo de grupos (abelianos), segue do 1° Teorema dos Isomorfismos que

$$\frac{\dot{F}/\dot{F}^2}{\ker(\phi)} \cong \mathrm{Im}(\phi).$$

Como $\ker(\phi) = \mathrm{Im}(g) = \{\dot{F}^2, a\dot{F}^2\}$, segue que $\frac{\dot{F}/\dot{F}^2}{\{\dot{F}^2, a\dot{F}^2\}} \cong \mathrm{Im}(\phi) \subseteq \dot{K}/\dot{K}^2$. Isso implica que

$$\frac{\left|\dot{F}/\dot{F}^2\right|}{2} = |\mathrm{Im}(\phi)| \leqslant \left|\dot{K}/\dot{K}^2\right|,$$

ou seja, $\frac{1}{2}\left|\dot{F}/\dot{F}^2\right| \leqslant \left|\dot{K}/\dot{K}^2\right|$.

Por outro lado, N é um homomorfismo de grupos (abelianos), segue do 1° Teorema dos Isomorfismos que $\frac{\dot{K}/\dot{K}^2}{\ker(N)} \cong \mathrm{Im}(N) \subseteq \dot{F}/\dot{F}^2$. Como $\ker(N) = \mathrm{Im}(\phi)$ e $\mathrm{Im}(\phi) \cong \frac{\dot{F}/\dot{F}^2}{\{\dot{F}, a\dot{F}^2\}}$, segue que

$$\frac{\left|\dot{K}/\dot{K}^2\right|}{\frac{1}{2}\cdot\left|\dot{F}/\dot{F}^2\right|} = |\mathrm{Im}(N)| \leqslant \left|\dot{F}/\dot{F}^2\right|.$$

Assim $\left|\dot{K}/\dot{K}^2\right| \leqslant \frac{1}{2}\left|\dot{F}/\dot{F}^2\right|^2$. Pelo que já provamos temos que

$$\frac{1}{2}\left|\dot{F}/\dot{F}^2\right| \leqslant \left|\dot{K}/\dot{K}^2\right| \leqslant \frac{1}{2}\left|\dot{F}/\dot{F}^2\right|^2.$$

A partir da desigualdade acima é fácil ver que,

$$\left|\dot{F}/\dot{F}^2\right| < \infty \text{ se, e somente se, } \left|\dot{K}/\dot{K}^2\right| < \infty.$$

□

Corolário 4.31. *Sejam F e K corpos, tais que $K = F(\sqrt{a})$. Então:*

(1) *$W(K)$ é finito se, e somente se, o endomorfismo $t : W(F) \longrightarrow W(F)$ definido no Teorema do Triângulo Exato 4.28 têm núcleo finito e co-núcleo finito;*

(2) *Se* $\mathrm{rank}(W(F)) < \infty$, *então* $\mathrm{rank}(W(K)) = 2\,\mathrm{rank}(\mathrm{coker(t)})$;

(3) *Se $|W(F)| < \infty$, então $|W(K)| = |\,\mathrm{coker(t)}\,|^2$.*

Demonstração: (1) Suponha que $|W(K)| < \infty$. Pelo Teorema do Triângulo Exato e pelo 1° Teorema dos Isomorfismos temos que

$$\mathrm{coker}(t) = \frac{W(F)}{\mathrm{Im}(t)} \cong \mathrm{Im}(r^*) \subseteq W(K).$$

Assim, $|\,\mathrm{coker}(t)| = |\,\mathrm{Im}(r^*)| \leqslant |W(K)| < \infty$. Como $\mathrm{Im}(s_*) = \ker(t)$ e $\frac{W(K)}{\mathrm{Im}(r^*)} \cong \mathrm{Im}(s_*)$, segue que $|\,\ker(t)| \cdot |\,\mathrm{Im}(r^*)| = |W(K)| < \infty$. Implicando que $|\,\ker(t)| < \infty$. Logo $|\,\mathrm{coker}(t)|$ e $|\,\ker(t)|$ são finitos.

Reciprocamente, suponha que $|\,\mathrm{coker}(t)|$ e $|\,\ker(t)|$ são finitos. Isso implica que $\left|\frac{W(F)}{\mathrm{Im}(t)}\right|, |\,\mathrm{Im}(s_*)|$ são finitos. Como $\mathrm{Im}(t) = \ker(r^*)$, segue que

$$\mathrm{coker}(t) = \frac{W(F)}{\ker(r^*)} \cong \mathrm{Im}(r^*) = \ker(s_*).$$

Assim, $|\,\ker(s_*)|$ e $|\,\mathrm{Im}(s_*)|$ são finitos. Então,

$$\frac{|W(K)|}{|\,\ker(s_*)|} = |\,\mathrm{Im}(s_*)| \Rightarrow |W(K)| = |\,\mathrm{Im(s*)}\,| \cdot |\,\ker(r^*)| < \infty.$$

Logo $|W(K)| < \infty$.

(2) Suponha que $\operatorname{rank}(W(F)) < \infty$. Isso implica que $W(F)$ é finitamente gerado, em particular $\frac{W(K)}{\ker(s_*)} \cong \operatorname{Im}(s_*) \subseteq W(F)$ e $\ker(s_*) = \operatorname{Im}(r^*) \cong \frac{W(F)}{\ker(t)}$ são finitamente gerados. Pelo Teorema da Correspondência da teoria de grupos, temos que $\operatorname{rank}(W(K)) < \infty$.

Dados $(W(F), +, m_F)$ e $(W(K), +, m_K)$, onde

$$\begin{array}{rccc} m_F: & F \times W(F) & \longrightarrow & W(F) \\ & (c, q) & \longrightarrow & \langle c \rangle \otimes_F q \end{array} \quad , \quad \begin{array}{rccc} m_K: & F \times W(K) & \longrightarrow & W(K) \\ & (c, q') & \longrightarrow & \langle c \rangle \otimes_K q. \end{array}$$

É fácil ver que $W(F)$ e $W(K)$ com as estruturas acima são F-espaços vetoriais. E mais, r^*, t são F-lineares e pela Reciprocidade de Frobenius 4.6, temos que s_* é F-linear. Assim, pelo Teorema do Núcleo e da Imagem, temos que

$$\begin{aligned} \operatorname{rank}(W(K)) &= \operatorname{rank}(\ker(s_*)) + \operatorname{rank}(\operatorname{Im}(s_*)) \\ \operatorname{rank}(W(F)) &= \operatorname{rank}(\ker(r^*)) + \operatorname{rank}(\operatorname{Im}(r^*)) \\ \operatorname{rank}(W(F)) &= \operatorname{rank}(\ker(t)) + \operatorname{rank}(\operatorname{Im}(t)). \end{aligned}$$

Como $\operatorname{Im}(t) = \ker(r^*)$ e $\ker(t) = \operatorname{Im}(s_*)$, segue que $0 = \operatorname{rank}(\operatorname{Im}(r^*)) - \operatorname{rank}(\operatorname{Im}(s_*))$. Assim,

$$\operatorname{rank}(W(K)) = \operatorname{rank}(\ker(s_*)) + \operatorname{rank}(\operatorname{Im}(r^*)) = 2\operatorname{rank}(\operatorname{Im}(r^*)).$$

Pelo fato que $\operatorname{coker}(t) = \frac{W(F)}{\operatorname{Im}(t)} = \frac{W(F)}{\ker(r^*)} \cong \operatorname{Im}(r^*)$, logo $\operatorname{rank}(W(K)) = 2\operatorname{rank}(\operatorname{coker}(t))$.

(3) Suponha que $|W(F)| < \infty$. Como $\ker(t), \operatorname{Im}(t) \subseteq W(F)$, segue que $|\ker(t)|$ e $|\operatorname{Im}|$ são finitos e $|\operatorname{coker}(t)| = \left|\frac{W(F)}{\operatorname{Im}(t)}\right| < \infty$. Pelo item (1) desse teorema, temos que $|W(K)| < \infty$. Assim,

$$\begin{aligned} |W(K)| &= |\ker(s_*)| \cdot |\operatorname{Im}(s_*)| = |\operatorname{Im}(r^*)| \cdot |\ker(t)| \\ &= |\tfrac{W(F)}{\ker(r^*)}| \cdot |\tfrac{W(F)}{\operatorname{Im}(t)}| = |\operatorname{coker}(t)| \cdot |\operatorname{coker}(t)| = |\operatorname{coker}|^2. \end{aligned}$$

Logo $|W(F)| = |\operatorname{coker}|^2$. Provando o resultado. □

Teorema 4.32. *Seja K/F uma extensão finita de corpos. Se $|\dot{K}/\dot{K}^2| < \infty$, então $|\dot{F}/\dot{F}^2| < \infty$. A reciproca é verdadeira se K/F é galoisiana e $[K : F] = 2^n$, com $n \in \mathbb{Z}_+$.*

Demonstração: Seja K/F uma extensão finita de corpos. Seja E/F uma sub-extensão maximal de K/F que foi obtidas por extensões quadrática a partir de F. Isso implica que K/E não tem sub-extensão quadrática.

Afirmamos que, se K/E é uma extensão finita de corpos que não têm sub-extensão quadrática, então o homomorfismo natural $\phi : \dot{E}/\dot{E}^2 \longrightarrow \dot{K}/\dot{K}^2$ é injetora. De fato, suponha que $\phi : \dot{E}/\dot{E}^2 \longrightarrow \dot{K}/\dot{K}^2$, dada por $\phi(e\dot{E}^2) = e\dot{K}^2$ não é injetora. Assim, existe $e \in \dot{E} \cap \dot{K}^2$ e $e \notin \dot{E}^2$. Como $e \in \dot{K}^2$, segue que existe $\sqrt{e} \in \dot{K}$ e $\sqrt{e} \notin \dot{E}$. Isso implica que $E(\sqrt{e})/E$ é uma sub-extensão quadrática de K/E, o que é um absurdo. Logo ϕ é injetora.

Como ϕ é injetora, segue do 1° Teorema dos Isomorfismos que $\dot{E}/\dot{E}^2 \cong \operatorname{Im}(\phi) \subseteq \dot{K}/\dot{K}^2$. Assim, se $\left|\dot{K}/\dot{K}^2\right| < \infty$, então $\left|\dot{E}/\dot{E}^2\right| < \infty$. Pelo fato que E/F foi obtida por sub-extensões quadráticas e $[E : F] < [K : F] < \infty$, temos pelo Corolário 4.30 aplicado um número finito de vezes que $\left|\dot{F}/\dot{F}^2\right| < \infty$.

Iremos provar a recíproca, seja K/F uma extensão galoisiana finita de corpos, tal que $[K:F]=2^n$, com $n\in\mathbb{Z}_+$. Como K/F é de Galois, segue da Teoria de Galois que

$$|\operatorname{Gal}(K/F)| = |\operatorname{Aut}(K/F)| = [K:F] = 2^n.$$

Assim $\operatorname{Gal}(K/F)$ é um 2-grupo de ordem 2^n. Temos pelo Primeiro Teorema de Sylow que existem subgrupos G_i's, tais que $|G_i| = 2^{n-i}$ e

$$\operatorname{Gal}(K/F) = G_0 \supset G_1 \supset \cdots \supset G_{n-1} \supset G_n = \{1\},$$

onde $[G_i : G_{i+1}] = 2$, para todo $i = 0,\ldots,n-1$. Tomando $F_i = K^{G_i}$, segue do Teorema Fundamental da Teoria de Galois que existe a seguinte sequência de corpos encaixada.

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = K,$$

onde $[F_{i+1} : F_i] = 2$, para todo $i = 0,\ldots,n-1$. Se $\left|\dot{F}/\dot{F}^2\right| < \infty$, então pelo Corolário 4.30 aplicado n vezes temos que $\left|\dot{F}_i/\dot{F}_i^{\,2}\right| < \infty$, para todo $i = 0,\ldots,n$. Logo $\left|\dot{K}/\dot{K}^2\right| < \infty$. □

4.4 Teorema de Cassels-Pfister

Nessa seção iremos observar o comportamento de formas quadráticas sobre extensões transcendentes e provaremos o importante Teorema de Cassels-Pfister.

Lema 4.33. *Seja γ uma F-forma quadrática. Se γ é F-anisotrópica, então $\gamma_{F(x)}$ é $F(x)$-anisotrópica, onde $F(x)$ é o corpo quociente de polinômios sobre F. Em particular, o núcleo de Witt $W(F(x)/F)$ é o ideal nulo em $W(F)$.*

Demonstração: Seja $\gamma \cong \langle a_1,\ldots,a_n\rangle$ uma F-forma quadrática. Suponha que γ é F-anisotrópica e assuma que $\gamma_{F(x)}$ é $F(x)$-isotrópica. Isso implica que existe um vetor não nulo $\left(\frac{g_1(x)}{h_1(x)},\cdots,\frac{g_n(x)}{h_n(x)}\right)$, tal que

$$\sum_{i=1}^{n}\left[a_i\left(\frac{g_i(x)}{h_i(x)}\right)^2\right] = 0.$$

Tomando $f_i(x) = \left[g_i(x)\cdot\prod_{j=1\ j\neq i}^{n}(h_j(x))\right]$, temos que $\sum_{i=1}^{n}\left[a_i(f_i(x))^2\right] = 0$. Pela definição de $f_i(x)$, segue que $f_i(x)\in F[x]$, para todo $i=1,\ldots,n$, e $f_i(x)\neq 0$, para algum $i = 1,\ldots,n$. Mudando os $f_i(x)$'s se necessário, podemos assumir que $\operatorname{mdc}(x, f_1(x),\ldots,f_n(x)) = 1$, onde retiramos os possíveis $f_i(x)$'s, tais que $f_i(x) = 0$. Tomando $x = 0$, temos que

$$\sum_{i=1}^{n}\left[a_i(f_i(0))^2\right] = 0.$$

Como $f_i(0)\in F$ e $f_i(0)\neq 0$, para algum $i = 1,\ldots,n$, segue tomando o vetor $(f_1(0),\cdots,f_n(0))$ que γ é F-isotrópica, o que é um absurdo. Logo $\gamma_{F(x)}$ é $F(x)$-anisotrópica. Em particular, $r^*: W(F)\longrightarrow W(K)$ é injetora, ou seja, $W(F(x)/F) = \{0_{W(F)}\}$. □

Note que o lema anterior é basicamente o Teorema de Springer 4.22 para extensões transcendentais simples.

Corolário 4.34. *Seja F um corpo, seja $F(x)$ o corpo quociente dos polinômios sobre F. Então:*

(1) *Se ϕ é uma F-forma quadrática, então $D_F(\phi) = \dot{F} \cap D_{F(x)}(\phi_{F(x)})$;*

(2) *-1 é uma soma de n quadrados em F se, e somente se, -1 é uma soma de n quadrados em $F(x)$.*

Demonstração: (1) É fácil ver que $D_F(\phi) \subseteq \dot{F} \cap D_{F(x)}(\phi_{F(x)})$. Reciprocamente, seja $d \in \dot{F} \cap D_{F(x)}(\phi_{F(x)})$ (que existe, pois ϕ é regular). Seja $\gamma := \phi \perp \langle -d \rangle$. Pelo 1° Teorema de Representação 1.52, temos que $\gamma_{F(x)}$ é $F(x)$-isotrópica. Segue pela contra-positiva do Lema 4.33 que γ é F-isotrópica. Assim, do 1° Teorema de Representação 1.52, obtemos que $d \in D_F(\phi)$. Portanto, $D_F(\phi) = \dot{F} \cap D_{F(x)}(\phi_{F(x)})$.

(2) Se $-1 = \sum_{i=1}^{n} x_i^2$, com $n \in \mathbb{Z}_+$ e $x_i \in F$. Então, em particular, -1 é soma de n quadrados em $F(x)$, pois $F \subset F(x)$.

Reciprocamente, suponha que $-1 = \sum_{i=1}^{n} y_i^2$, com $n \in \mathbb{Z}_+$ e $y_i \in F(x)$. Isso implica que $-1 \in \dot{F} \cap D_{F(X)}(n\langle 1 \rangle_{F(X)})$. Temos pelo item (1) desse corolário que $-1 \in D_F(n\langle 1 \rangle)$. Logo -1 é soma de n quadrados em F. □

Teorema 4.35 (Cassels-Pfister). *Seja γ uma F-forma quadrática, seja $p(x) \in F[x] \cap D_{F(x)}(\gamma)$. Então:*

(1) *$p(x)$ é representado por γ sobre o anel $F[x]$, e*

(2) *Se $e \in F$, tal que $p(e) \neq 0$, então $p(e) \in D_F(\gamma)$.*

Demonstração: (1) Seja $\langle a_1, \cdots, a_n \rangle$ uma diagonalização de γ sobre F. Podemos considerar γ anisotrópica sobre F. Pois, caso contrário existiria uma sub-forma $\langle 1, -1 \rangle$ em γ, ou seja, $\gamma \cong \langle 1, -1 \rangle \perp \gamma'$. Assim, temos a seguinte equação

$$p(x) = \left[\frac{p(x)+1}{2}\right]^2 - \left[\frac{p(x)-1}{2}\right]^2 \in F[x].$$

Tomando o vetor $v = \left(\frac{p(x)+1}{2}, \frac{p(x)-1}{2}, 0, \cdots, 0\right) \in F[x]^n$, temos que $p(x) = \gamma(v)$, validando (1).

Por hipótese e por construção análoga ao Lema 4.33, obtemos que

$$p(x) = a_1 \left(\frac{f_1(x)}{f_0(x)}\right)^2 + \cdots + a_n \left(\frac{f_n(x)}{f_0(x)}\right)^2, \qquad (I)$$

onde $f_0(x), f_1(x), \ldots, f_n(x) \in F[x]$ e $f_0(x) \neq 0(x)$. Mudando $f_0(x)$ se necessário, pelo Princípio da Boa Ordem podemos assumir que $\deg(f_0(x))$ é minimal.

Afirmamos que $\deg(f_0(x)) = 0$. De fato, suponha que $\deg(f_0) > 0$. Consideremos a $F(x)$-forma quadrática $\phi \cong \langle -p(x), a_1, \cdots, a_n \rangle$. Seja $B = B_\phi$ a $F(x)$-forma bilinear simétrica associada a ϕ. Seja Q o conjunto dos vetores isotrópicos de $(F[x]^n, B, \phi)$. Note que Q é uma superfície quadrática no espaço projetivo $P^n(F[x])$ n-dimensional. De fato, pela definição de Q, temos que

$$Q = \left\{ (y_0, y_1, \ldots, y_n) \in F[x]^{n+1} \ : \ -p(x)(y_0)^2 + \sum_{j=1}^{n} \left[a_j (y_j)^2\right] = 0_{F[x]} \right\}.$$

Pela equação (I), temos que o vetor $(f_0(x), f_1(x)), \cdots, f_n(x)) \in Q$, ou seja, $Q \neq \emptyset$. Da definição de superfície quadrática e do fato que formas quadráticas são polinômios quadráticos homogêneos, segue que Q é uma superfície quadrática homogênea sobre $F[x]^{n+1}$, pelos resultados da Geometria Algébrica, Q é uma superfície quadrática em $P^n(F[x])$.

Para chegarmos em uma contradição, construiremos um vetor $h(x) = (h_0(x), h_1(x), \cdots, h_n(x)) \in Q$, onde $h_i(x) \in F[x]$ e $h_0 \neq 0$, com $\deg(h_0(x)) < \deg(f_0(x))$. Para construir $h(x)$, primeiro temos que dividir todos os $f_i(x)$'s por $f_0(x)$. Como $F[x]$ é domínio euclidiano, segue que existem únicos $g_i(x), r_i(x) \in F[x]$, tais que

$$f_i(x) = f_0(x)g_i(x) + r_i(x), \text{ onde, ou } r_i(x) = 0, \text{ ou } \deg(r_i(x)) < \deg(f_0(x)).$$

Como $f_0(x) = f_0(x)1(x)+0(x)$, segue que $g_0(x) = 1(x)$ e $r_0(x) = 0$.Assim, conseguimos os vetores $f(x) = (f_0(x), \cdots, f_n(x))$, $g(x) = (g_0(x), \cdots, g_n(x))$ e $r(x) = (r_0(x), \cdots, r_n(x))$ em $F[x]^{n+1}$, relativos a equação vetorial $f(x) = f_0(x)g(x) + r(x)$. Podemos assumir que $r(x) \neq 0$, pois caso contrário $\frac{f_i(x)}{f_0(x)} \in F[x]$, para todo $i = 1, \ldots, n$, implicando que $p(x) \in F[x]$.

Afirmamos que existe $h(x) \in Q$, tal que $h(x) = c(x)f(x) + d(x)g(x)$, onde $c(x), d(x) \in F[x]$. De fato, se tomarmos $c(x) = 1$ e $d(x) = 0$, temos que $h(x) = f(x) \in Q$. Em geral, temos que

$$\begin{aligned} 0_{F[x]} = B(h,h) &= B(c(x)f(x) + d(x)g(x), c(x)f(x) + d(x)g(x)) \\ &= c(x)^2B(f(x), f(x)) + 2c(x)d(x)B(f(x), g(x)) + d(x)^2B(g(x), g(x)). \end{aligned}$$

Como $f(x) \in Q$, segue que

$$0_{F[x]} = B(h,h)) = d(x) \cdot [2c(x)B(f(x), g(x)) + d(x)B(g(x), g(x))].$$

Tomando $c_0(x) := B(g(x), g(x))$ e $d_0(x) := -2B(f(x), g(x))$, temos que $h(x) = c_0(x)f(x) + d_0(x)g(x)$ satisfaz a afirmação.

Tomamos $c(x) = B(g(x), g(x))$ e $d(x) = -2B(f(x), g(x))$. Seja $h_0(x) = c(x)f_0(x) + d(x)g_0(x)$. Como $g_0(x) = 1(x)$, segue que

$$\begin{aligned} h_0(x) &= B(g(x), g(x))f_0(x) - 2B(f(x), g(x))g_0(x) \\ &= B(g(x), g(x))f_0(x) - 2B(f(x), g(x)) \\ &= B(g(x)f_0(x) - 2f(x), g(x)) \\ &= B(f(x) - r(x) - 2f(x), g(x)) \\ &= -B(f(x) + r(x), g(x)). \end{aligned}$$

Isso implica que

$$\begin{aligned} f_0(x)h_0(x) = -f_0(x)B(f(x) + r(x), g(x)) &= -B(f(x) + r(x), f_0(x)g(x)) \\ &= B(f(x) + r(x), f(x) - r(x)) \\ &= -[B(f(x), f(x)) - B(f(x), r(x)) + \\ &\quad B(r(x), f(x)) - B(r(x), r(x))] \\ &= B(r(x), r(x)) \\ &= \textstyle\sum_{i=0}^{n}[a_i(r_i(x))^2] = \phi(r(x)) \neq 0(x). \end{aligned}$$

pois $r_0(x) = 0$ e ϕ é F-anisotrópica. Pelo fato que

$$\deg(f_0(x)) \deg(h_0(x)) = \deg(\sum_{i=1}^{n}[a_i(r_i(x))^2]) \leqslant \max(\deg(r_i))^2 < [\deg(f_0(x))]^2,$$

temos que $\deg(h_0(x)) < \deg(f_0(x))$. Assim, $\left(\frac{h_1(x)}{h_0(x)}, \frac{h_2(x)}{h_0(x)}, \cdots, \frac{h_n(x)}{h_0(x)}\right)$ é solução de (I), com $\deg(h_0(x)) < \deg(f_0(x))$, o que é um absurdo. Logo $\deg(f_0(x)) = 0$, e dessa forma $p(x) \in F[x]$.

(2) Seja $e \in F$, tal que $p(e) \neq 0$. Segue pelo item (1) desse teorema que $p(x) = \sum_{i=1}^{m}[a_i(f_i(x))^2]$, com $f_i(x) \in F[x]$. Assim,

$$p(e) = \sum_{i=1}^{m}[a_i(f_i(e))^2] = \phi(f_1(e), \cdots, f_n(e)) \neq 0.$$

Portanto $p(e) \in D_F(\gamma)$. □

4.5 Formas de Pfister

Nessa seção iremos estudar as formas quadráticas de Pfister. Essas formas são muito importantes para estudarmos os ideais de $W(F)$ da forma I^nF, com $n \in \mathbb{Z}_+$ e as álgebras de quaternios.

Definição 4.36. Seja F um corpo, chamaremos de *forma de Pfister de n camadas* sobre o corpo F a forma quadrática

$$\bigotimes_{i=1}^{n}\langle 1, a_i\rangle \cong \langle 1, a_1\rangle \otimes \cdots \otimes \langle 1, a_n\rangle,$$

com $a_i \in \dot{F}$, para todo $i = 1, \ldots, n$. Denotaremos $\bigotimes_{i=1}^{n}\langle 1, a_i\rangle$, por $\langle\langle a_1, \ldots, a_n\rangle\rangle$.

Lema 4.37. *Sobre um corpo F, qualquer forma quadrática binária $q \cong \langle 1, a\rangle$ é uma* forma de grupo*, isto é, $D_F(q)$ é subgrupo de $\dot{F}$.*

Demonstração: Claramente $1 \in D_F(q)$ e $D_F(q)$ é fechado para inversos pelo item (2) da Observação 1.30. Assim, basta provarmos que $D_F(q)$ é fechado para o produto. De fato, note que

$$(x^2 + ay^2)(z^2 + aw^2) = (xz - ayw)^2 + a(xw + yz)^2,$$

para todos $x, y, z, w \in F$. Logo $D_F(q)$ é fechado para o produto, e portanto q é uma forma de grupo. □

Uma forma quadrática de Pfister de 0 camadas é, por convenção, dada pela forma $\langle 1\rangle$. Uma forma de Pfister de 1 camada é dada por $\langle 1, a\rangle$, que coincide com a forma normal da álgebra quadrática $F[x]/(x^2 + a)$. Uma forma de Pfister de 2 camadas $\langle\langle -a, -b\rangle\rangle$ é a forma normal da álgebra de quatérnios $\left(\frac{a,b}{F}\right)$, pela Proposição 3.14.

Trabalhando com formas de Pfister é muito útil notar que, se tomarmos a forma de Pfister de n camadas $q \cong \langle\langle a_1, \ldots, a_n\rangle\rangle$, com $a_i = -1$, para algum a_i, então $q \cong 2^{n-1}\mathbb{H}_F$. De fato, basta notar que $\langle 1, a_i\rangle \cong \langle 1, -1\rangle \cong \mathbb{H}_F$. Por outro lado, se $a_1 = 1$, então

$$\langle\langle 1, a_2, \ldots, a_n\rangle\rangle \cong \langle\langle a_2, \ldots, a_n\rangle\rangle \perp \langle\langle a_2, \ldots, a_n\rangle\rangle \cong 2\langle\langle a_2, \ldots, a_n\rangle\rangle.$$

Em particular, se $a_1 = \cdots = a_n = 1$, então $\langle\langle 1, \ldots, 1\rangle\rangle \cong 2^n\langle 1\rangle$.

Proposição 4.38. *Seja IF o ideal fundamental de $W(F)$. Então I^nF é gerado aditivamente pelo conjunto de todas as formas de Pfister de n camadas.*

Demonstração: Pela Proposição 2.9 e do fato que IF é a inclusão natural de $\widehat{I}F$ em $W(F)$, segue que IF é gerado aditivamente pelas formas de Pfister $\langle 1\rangle + \langle a\rangle = \langle 1, a\rangle = \langle\langle a\rangle\rangle$ em $W(F)$. Como $I^nF = I^{n-1}F \cdot IF$, temos que I^nF é gerado aditivamente pelas formas de Pfister de n camadas. □

A seguinte proposição nos dá algumas fórmulas básicas para formas de Pfister de 2 camadas.

Proposição 4.39. *Sejam F um corpo e a, b, x, $y \in \dot{F}$. Então as seguintes afirmações são verdadeiras.*

(1) *Se $x \in D(\langle\langle a\rangle\rangle)$, então $\langle\langle a, b\rangle\rangle \cong \langle\langle a, bx\rangle\rangle$;*

(2) *Se $y \in D(\langle a, b\rangle)$, então $\langle\langle a, b\rangle\rangle \cong \langle\langle y, ab\rangle\rangle$.*

Demonstração: (1) Suponha que $x \in D(\langle\langle a\rangle\rangle) = D(\langle 1, a\rangle)$. Pela Proposição 1.64, temos que $\langle x, xa\rangle \cong \langle 1, a\rangle$. Assim,

$$\begin{aligned}\langle\langle a, b\rangle\rangle \cong \langle 1, a\rangle \otimes \langle 1, b\rangle &\cong \langle 1, a, b, ab\rangle \cong \langle 1, a\rangle \perp \langle b\rangle \otimes \langle 1, a\rangle \\ &\cong \langle 1, a\rangle \perp \langle b\rangle \otimes \langle x, xa\rangle \cong \langle\langle a, bx\rangle\rangle.\end{aligned}$$

(2) Suponha que $y \in D(\langle a, b\rangle)$. Pela Proposição 1.64, temos que $\langle a, b\rangle \cong \langle y, yab\rangle$. Assim,

$$\langle\langle a, b\rangle\rangle \cong \langle 1, ab, a, b\rangle \cong \langle 1, ab, y, yab\rangle \cong \langle\langle y, ab\rangle\rangle.$$

□

Definição 4.40. Sejam $\langle\langle a_1, \ldots, a_n\rangle\rangle$ e $\langle\langle b_1, \ldots, b_n\rangle\rangle$ duas forma de Pfister de n camadas. Dizemos que essas formas de Pfister são *simplesmente P-equivalentes*, se existem dois índices i e j, tais que

(1) $\langle\langle a_i, a_j\rangle\rangle \cong \langle\langle b_i, b_j\rangle\rangle$, e

(2) $a_k = b_k$, para qualquer $k \neq i, j$ e $k = 1, \ldots, n$.

(Note que na condição (1) da definição acima, se $i = j$, a expressão $\langle\langle a_i, a_j\rangle\rangle$ é entendida apenas por $\langle\langle a_i\rangle\rangle$.) Em geral, dizemos que duas formas de Pfister de n camadas ϕ e γ são *P-equivalentes por cadeia*, se existe uma sequência de formas de Pfister de n camadas $\phi_0, \phi_1, \ldots, \phi_m$, tal que $\phi_0 = \phi$, $\phi_m = \gamma$, e para cada ϕ_i é simplesmente P-equivalente a ϕ_{i+1} $(0 \leqslant i \leqslant m-1)$.

Não é difícil provar que a P-equivalência é uma relação de equivalência sobre todas as formas de Pfister de n camadas, que denotaremos por $\approx$.

Como toda forma de Pfister de n camadas ϕ representa 1, podemos escrever $\phi \cong \langle 1\rangle \perp \phi'$. Chamaremos a forma quadrática ϕ' de *sub-forma pura* de ϕ (em analogia com o conceito de "quaternios puros"). Essa terminologia é justificada, pois como a classe de isometria de ϕ' é determinada unicamente por ϕ de acordo com o Cancelamento de Witt 1.60.

Teorema 4.41 (Sub-forma Pura). *Seja $\phi = \langle\langle a_1, a_2, \ldots, a_n\rangle\rangle$ uma F-forma de Pfister de n-camadas, com $n \geqslant 1$, seja $b \in D_F(\phi')$. Então existem $b_2, \ldots, b_n \in \dot{F}$, tais que*

$$\phi \approx \langle\langle b, b_2, \ldots, b_n\rangle\rangle.$$

Demonstração: Provaremos por indução em n. Se $n = 1$, então $\phi = \langle 1, a_1\rangle$. Como $b \in D_F(\phi') = D_F(\langle a_1\rangle)$, segue que $\langle b\rangle \cong \langle a_1\rangle$, onde segue o resultado. Assumimos que esse teorema seja válido para as formas de Pfister de $n-1$ camadas. Seja

$$\tau := \langle\langle a_1, \ldots, a_{n-1}\rangle\rangle \cong \langle 1\rangle \perp \tau'.$$

Isso implica que $\phi \cong \tau \otimes \langle 1, a_n\rangle \cong \tau \perp \langle a_n\rangle \otimes \tau$. Assim, $\phi' \cong \tau' \perp \langle a_n\rangle \otimes \tau$. Como por hipótese $b \in D_F(\phi') = D_F(\tau' \perp \langle a_n\rangle \otimes \tau)$, temos que existem

$$x \in D_F(\tau') \cup \{0\} \quad \text{e} \quad y \in D_F(\tau) \cup \{0\},$$

tais que $b = x + a_n y$. Podemos escrever mais $y = t^2 + y_0$, onde $y_0 \in D_F(\tau') \cup \{0\}$. Como $b \in \dot{F}$, segue que $b \neq 0$. Assim, temos dois casos a se analisar.

Caso 1. Se $y = 0$, então $0 \neq b = x \in D_F(\tau')$. Pela hipótese de indução, existem $d_2, \ldots, d_{n-1} \in \dot{F}$, tais que $\tau \approx \langle\langle x, d_2, \ldots, d_{n-1}\rangle\rangle$. Assim,

$$\phi \approx \langle\langle x, d_2, \ldots, d_{n-1}\rangle\rangle \otimes \langle\langle a_n\rangle\rangle \cong \langle\langle b, d_2, \ldots, d_{n-1}, a_n\rangle\rangle,$$

como desejado.

Caso 2. Suponha que $y \neq 0$. Afirmamos que $\phi \cong \langle\langle a_1, \ldots, a_{n-1}, ya_n\rangle\rangle$. De fato, se $y_0 = 0$, então $0 \neq y = t^2$, seguindo no desejado. Se $y_0 \neq 0$, então podemos assumir que $y_0 \in D_F(\tau')$. Pela hipótese de indução novamente, $\tau \approx \langle\langle y_0, c_2, \ldots, c_{n-1}\rangle\rangle$, onde $c_i \in \dot{F}$, para todo $i = 2, \ldots, n-1$. Assim,

$$\begin{array}{rcl} \phi & \approx & \langle\langle y_0, c_2, \ldots, c_{n-1}, a_n\rangle\rangle \approx \langle\langle y_0, c_2, \ldots, c_{n-1}, a_n(t^2 + y_0)\rangle\rangle \\ & \approx & \langle\langle y_0, c_2, \ldots, c_{n-1}, ya_n\rangle\rangle, \end{array}$$

onde a segunda congruência é dada pela Proposição 4.39 item (1) em $y \in D_F(\langle\langle y_0\rangle\rangle)$. Provando nossa afirmação. Se $x = 0$, então $b = ya_n$ que pela nossa afirmação acima satisfaz o teorema. Assim, podemos supor que $x \neq 0$. Isso implica que $x \in D_F(\tau')$. Novamente, pela nossa hipótese de indução, temos que $\tau \cong \langle\langle x, d_2, \ldots, d_{n-1}\rangle\rangle$, com $d_j \in \dot{F}$, para todo $j = 2, \ldots, n-1$. Assim,

$$\begin{array}{rcl} \phi & \approx & \langle\langle x, d_2, \ldots, d_{n-1}, ya_n\rangle\rangle \approx \langle\langle x + a_n y, d_2, \ldots, d_{n-1}, a_n xy\rangle\rangle \\ & \approx & \langle\langle b, d_2, \ldots, d_{n-1}, a_n xy\rangle\rangle, \end{array}$$

onde a segunda congruência é dada pela Proposição 4.39 item (2) aplicada em $\langle\langle x, a_n y\rangle\rangle$. Provando a tese para n. □

Proposição 4.42. *Sejam $\tau \cong \langle\langle a_1, \ldots, a_{n-1}\rangle\rangle$ e $D_F(\tau)$. Então para qualquer $a_n \in \dot{F}$:*

$$\langle\langle a_1, \ldots, a_{n-1}, a_n\rangle\rangle \approx \langle\langle a_1, \ldots, a_{n-1}, a_n y\rangle\rangle.$$

Em particular, $\langle\langle a_1, \ldots, a_{n-1}, y\rangle\rangle$ é isométrica a 2τ e $\langle\langle a_1, \ldots, a_{n-1}, -y\rangle\rangle$ é hiperbólica.

Demonstração: Seja $y \in D_F(\tau)$, tal que $y = t^2 + y_0$, onde $y_0 \in D_F(\tau') \cup \{0\}$, seja $\phi \cong \langle\langle a_1, \ldots, a_{n-1}, a_n\rangle\rangle \cong \tau \otimes \langle\langle a_n\rangle\rangle$, com $a_n \in \dot{F}$. Se $y\dot{F}^2 = 1\dot{F}^2$, então a P-equivalência por cadeia acima é satisfeita. Suponha que $y\dot{F}^2 \neq 1\dot{F}^2$. Isso implica que $y_0 \neq 0$. Pelo Teorema 4.41, temos que existem $c_2, \ldots, c_{n-1}$, tais que $\tau \approx \langle\langle y_0, c_2, \ldots, c_{n-1}\rangle\rangle$. Por argumento análogo na demonstração do caso 2 do Teorema 4.41, segue que $\phi \approx \langle\langle a_1, \ldots, a_{n-1}, a_n y\rangle\rangle$. Provando nossa proposição.

Em particular se $a_n\dot{F} = 1\dot{F}$, segue que

$$2\langle\langle a_1, \ldots, a_{n-1}\rangle\rangle \cong \langle\langle a_1, \ldots, a_{n-1}, 1\rangle\rangle \approx \langle\langle a_1, \ldots, a_{n-1}, y\rangle\rangle,$$

e $\langle\langle a_1, \ldots, a_{n-1}, -y\rangle\rangle \approx \langle\langle a_1, \ldots, a_{n-1}, -1\rangle\rangle \cong \langle\langle a_1, \ldots, a_{n-1}\rangle\rangle \otimes \langle 1, -1\rangle$. □

Usando o Teorema da Sub-forma Pura 4.41, teremos acesso a duas das principais propriedades de formas de Pfister.

Teorema 4.43. *Se uma F-forma de Pfister ϕ é isotrópica, então ϕ é hiperbólica.*

Demonstração: Suponha que a forma de Pfister ϕ sobre F é isotrópica. Isso implica que $\phi \cong \mathbb{H}_F \perp \phi_0$. Assim, $\phi' \cong \langle -1\rangle \perp \phi_0$. Implicando que $-1 \in D_F(\phi')$. Pelo Teorema da Sub-forma Pura 4.41, temos que $\phi \approx \langle\langle -1, \ldots\rangle\rangle$. Como $\langle\langle -1, \ldots\rangle\rangle$ é hiperbólico e $\approx$ implica em $\cong$, logo ϕ é hiperbólica. □

Para o próximo resultado necessitamos do conceito de fatores similares de uma forma quadrática.

Definição 4.44. Seja F um corpo, seja q uma F-forma quadrática. Chamaremos de *grupo dos fatores similares* de q o conjunto

$$\begin{aligned} G(q) = G_F(q) &:= \{a \in \dot{F} \mid \langle a\rangle \otimes q \cong q\} \\ &= \{a \in \dot{F} \mid \langle a\rangle \cdot q = q \ \in W(F)\} \\ &= \{a \in \dot{F} \mid \langle 1, -a\rangle \cdot q = 0 \ \in W(F)\}. \end{aligned}$$

Note que é simples de provar que $G(q)$ é subgrupo multiplicativo de $\dot{F}$, para qualquer F-forma quadrática q. Mais ainda, como $\langle 1\rangle \cong \langle x^2\rangle$, com $x \in \dot{F}$, segue que $\dot{F}^2 \subseteq G(q)$ atua como a identidade. Assim $G(q)/\dot{F}^2$ é um subgrupo de $\dot{F}/\dot{F}^2$.

Teorema 4.45. *Seja ϕ uma F-forma de Pfister. Então $D_F(\phi) = G_F(\phi)$. Em particular, $D_F(\phi)$ é um subgrupo de $\dot{F}$.*

Demonstração: Seja $x \in G(\phi)$. Isso implica que $\langle x\rangle \otimes \phi \cong \phi$, pelo fato que ϕ é uma forma de Pfister, segue que $\phi \cong \langle 1, \ldots\rangle$. Assim, $\phi \cong \langle x, \ldots\rangle$. Implicando que $x \in D(\phi)$.

Reciprocamente, seja $y \in D(\phi)$. Queremos mostrar que $y \in G(\phi)$. De fato, escreva $y = t^2 + y'$, onde $y' \in D(\phi') \cup \{0\}$. Caso $y' = 0$, segue que $y \in \dot{F}^2$ e desse modo, $y \in G(\phi)$. Suponha que $y' \neq 0$. Então, pelo Teorema 4.41, $\phi \approx \langle\langle y', c_2, \ldots, c_n\rangle\rangle$, com $c_i \in \dot{F}$, onde $i = 2, \ldots, n$. Como $y \in D(\langle 1, y'\rangle)$, segue pela Proposição 1.64 que $\langle 1, y'\rangle \cong \langle y, yy'\rangle$. Implicando que $y \in G(\langle\langle y'\rangle\rangle)$. Assim,

$$\phi \approx \langle\langle y', c_2, \ldots, c_n\rangle\rangle \cong \langle\langle y'\rangle\rangle \otimes \langle\langle c_2, \ldots, c_n\rangle\rangle \cong \langle y\rangle \otimes \langle\langle y'\rangle\rangle \otimes \langle\langle c_2, \ldots, c_n\rangle\rangle \cong \langle y\rangle \otimes \phi.$$

Portanto $y \in G(\phi)$.

□

Capítulo 5

Transfer de Scharlau de Extensões Biquadráticas

Seja F um corpo ($\text{char}(F) \neq 2$). Nesse capítulo, $a, b \in \dot{F}$, tais que $a, b, ab \neq \dot{F}^2$ a menos que se diga ao contrário. Para qualquer extensão K/F o conjunto $W(K/F)$ é dado pelo $\ker(r^*)$, onde $r^* : W(F) \longrightarrow W(K)$ é o homomorfismo natural, definido no Capítulo 4.

Iremos calcular o núcleo da transfer $s_* : W(F(\sqrt{a}, \sqrt{b})) \longrightarrow W(F)$ correspondente ao F-funcional linear $s : F(\sqrt{a}, \sqrt{b}) \longrightarrow F$ determinado pelas igualdades $s(1) = s(\sqrt{a}) = s(\sqrt{b}) = 0$ e $s(\sqrt{ab}) = 1$. Para isso precisamos de alguns resultados auxiliares.

Lema 5.1. *O conjunto* $J := W(F(\sqrt{a})/F) \cap W(F(\sqrt{b})/F)$ *é um ideal de* $W(F)$ *e* $J \subseteq I^2F$.

Demonstração: Primeiramente notemos que pelo fato de $W(F(\sqrt{a})/F)$ e $W(F(\sqrt{b})/F)$ serem ideais não nulos de $W(F)$, então $J \neq \emptyset$ e é ideal de $W(F)$. Como $F(\sqrt{a})/F$ e $F(\sqrt{b})/F$ são extensões quadráticas de corpos, pelo Teorema 4.25, temos que

$$J = W(F) \otimes \langle\langle -a \rangle\rangle \cap W(F) \otimes \langle\langle -b \rangle\rangle.$$

Queremos mostrar que $J \subseteq I^2F$. De fato, seja $q \in J$. Se $q = 0_W(F)$, então é claro que $q \in I^2F$. Suponha que $q \neq 0_{W(F)}$. Isso implica que $q = q_1 \otimes \langle\langle -a \rangle\rangle$ e $q = q_2 \otimes \langle\langle -b \rangle\rangle$, onde q_1, $q_2 \in W(F) - \{0_{W(F)}\}$. Pelo Corolário 4.26 temos que

$$d(q) = (-a)^{\frac{\dim(q)}{2}} = (-b)^{\frac{\dim(q)}{2}}.$$

Como $a, b, ab \notin \dot{F}^2$, então $a \cdot \dot{F}^2 \neq b \cdot \dot{F}^2$. Implicando que $d(q) = 1$ e, desse modo, $4 | \dim(q)$. Assim, pelo Lema 2.24, concluímos que $q \in I^2F$. Portanto $J \subseteq I^2F$. □

Lema 5.2. *Seja* π *uma* F*-forma de Pfister de duas camadas. Então as seguintes afirmações são equivalentes:*

(1) *Existe um* $u \in F$, *tal que* $\pi \cong \langle\langle -b, -a + bu^2 \rangle\rangle$;

(2) $\pi \in J$.

Demonstração: (1) $\Rightarrow$ (2) Suponha que exista $u \in F$ tal que $\pi \cong \langle\langle -b, -a + bu^2 \rangle\rangle$. Como $\pi \cong \langle 1, -b \rangle \otimes \langle 1, -a + bu^2 \rangle$, pelo Teorema 4.25, temos que $\pi \in W(F(\sqrt{b})/F)$. Mais ainda, como $(\sqrt{a})^2 - bu^2 \in D_{F(\sqrt{a})}(\langle\langle -b \rangle\rangle)$, pela Proposição 4.39 item (1), temos que

$$\pi_{F(\sqrt{a})} \cong \langle\langle -b, -1 \rangle\rangle_{F(\sqrt{a})} \cong 2 \cdot \mathbb{H}_{F(\sqrt{a})}.$$

Implicando que $\pi \in W(F(\sqrt{a})/F)$. Portanto $\pi \in W(F(\sqrt{a})/F) \cap W(F(\sqrt{b})/F) = J$.

(2) $\Rightarrow$ (1) Seja $\pi = \langle\langle x, y\rangle\rangle$, com $x, y \in \dot{F}$, uma F-forma de Pfister de duas camadas, tal que $\pi \in J$. Como $\pi \in W(F(\sqrt{b})/F)$, pelo Teorema 4.25, temos que $\pi \cong q \otimes \langle\langle -b\rangle\rangle$, onde $q \in W(F)$. Assim, $\langle\langle x, y\rangle\rangle \cong q \otimes \langle\langle -b\rangle\rangle$. Como $\langle -b\rangle \otimes \pi \cong \pi$, pelo Teorema 4.45 temos que $-b \in D_F(\pi)$, e consequentemente $-b \in D_F(\phi')$. Pelo Teorema da Subforma Pura 4.41, temos que existe $x_0 \in \dot{F}$, tal que $\pi \cong \langle\langle -b, -x_0\rangle\rangle$. Também temos que $\pi \in W(F(\sqrt{b})/F)$ e, por argumento análogo, segue que existe $y_0 \in \dot{F}$, tal que $\pi \cong \langle\langle -a, -y_0\rangle\rangle$. Assim, π é forma normal das álgebras de quatérnios

$$A = \left(\frac{a, y_0}{F}\right), \quad A' = \left(\frac{b, x_0}{F}\right).$$

Isso implica que $A \cong A'$. Pelo Teorema 3.20, temos que $A_0 \cong A'_0$ e assim $D_F(\pi|_{A_0}) = D_F(\pi|_{A'_0})$. Logo, $-a \in D_F(\pi|_{A'_0})$, ou seja, $-a \in D_F(\langle -b, -x_0, bx_0\rangle)$. Equivalentemente, $a \in D_F(\langle b, x_0, -bx_0\rangle)$. Então

$$a = bu^2 + x_0u_1^2 - bx_0u_2^2, \quad \text{com } u, u_1, u_2 \in F.$$

Como $b \notin \dot{F}^2$ e $b \neq 0$, então $u_1^2 - bu_2^2 \neq 0$, para todos $u_1, u_2 \in F$. Implicando que $x_0 = \frac{a-bu^2}{u_1^2-bu_2^2}$. Assim, concluímos que

$$\begin{aligned} \pi &\cong \langle\langle -b, -x_0\rangle\rangle \\ &\cong \langle\langle -b, -[(a - bu^2)/(u_1^2 - bu_2^2)] \cdot (u_1^2 - bu_2^2)^2\rangle\rangle \\ &= \langle\langle -b, (-a + bu^2) \cdot (u_1^2 - bu_2^2)\rangle\rangle. \end{aligned}$$

Pelo fato que $u_1^2 - bu_2^2 \in D_F(\langle\langle -b\rangle\rangle)$ e pela Proposição 4.39 item (1), temos que $\pi \cong \langle\langle -b, -a + bu^2\rangle\rangle$, como queríamos. □

Lema 5.3. *Sejam $\phi \in J$, $c \in D_F(\phi)$ e t uma variável. Então*

$$c(t^2 - a)(t^2 - b) \in D_{F(t)}(\phi_{F(t)}).$$

Demonstração: Como $\phi \in W(F(\sqrt{a})/F)$, pelo Teorema 4.25, $\phi \cong q \otimes \langle\langle -a\rangle\rangle$, com $q \in W(F)$. Afirmamos que $\langle\langle -a\rangle\rangle_{F(t)} \cong \langle t^2 - a\rangle \otimes \langle\langle -a\rangle\rangle_{F(t)}$. De fato, como $t^2 - a \in D_{F(t)}(\langle\langle -a\rangle\rangle_{F(t)})$ e

$$d(\langle\langle -a\rangle\rangle_{F(t)}) = -a\dot{F}(t)^2 = -a(t^2 - a)\dot{F}(t)^2 = d\left(\langle t^2 - a\rangle \otimes \langle\langle -a\rangle\rangle_{F(t)}\right),$$

então obtemos a seguinte equivalência

$$\langle\langle -a\rangle\rangle_{F(t)} \cong \langle t^2 - a\rangle \otimes \langle 1, d(\langle\langle -a\rangle\rangle_{F(t)})\rangle_{F(t)} \cong \langle t^2 - a\rangle \otimes \langle\langle -a\rangle\rangle_{F(t)}.$$

Provando a afirmação.

Como $\langle\langle -a\rangle\rangle_{F(t)} \cong \langle t^2 - a\rangle \otimes \langle\langle -a\rangle\rangle_{F(t)}$, então $\phi_{F(t)} \cong \langle t^2 - a\rangle \otimes \phi_{F(t)}$. De maneira análoga temos que $\phi_{F(t)} \cong \langle t^2 - b\rangle \otimes \phi_{F(t)}$. Assim,

$$\phi_{F(t)} \cong \langle t^2 - a\rangle \otimes \phi_{F(t)} \cong \langle t^2 - a\rangle \otimes \langle t^2 - b\rangle \otimes \phi_{F(t)}.$$

Em particular, temos que $D_{F(t)}(\phi_{F(t)}) = D_{F(t)}(\langle t^2 - a\rangle \otimes \langle t^2 - b\rangle \otimes \phi_{F(t)})$. Como $c \in D_F(\phi_{F(t)})$, segue que existe $x_0 = (x_1, \ldots, x_{\dim(\phi)})$, tal que $c = \phi(x_0)$. Assim tomando o vetor $1 \otimes 1 \otimes x_0$, temos que

$$\begin{aligned} \phi_{F(t)}(x_0) &= \langle t^2 - a\rangle \otimes \langle t^2 - b\rangle \otimes \phi_{F(t)}(1 \otimes 1 \otimes x_0) \\ &= c(t^2 - a)(t^2 - b). \end{aligned}$$

Portanto, $c(t^2 - a)(t^2 - b) \in D_{F(t)}(\phi_{F(t)})$. □

Lema 5.4. *Suponha que $\phi \in J$ e ϕ seja F-anisotrópica. Então existe uma sub-forma de dimensão 3 $\phi_0 \subset \phi$, tal que as formas quadráticas $\phi_{0_{F(\sqrt{a})}}$ e $\phi_{0_{F(\sqrt{b})}}$ são isotrópicas.*

Demonstração: Seja (V, ϕ) um F-espaço quadrático anisotrópico, tal que $\phi \in J$. Como $\phi \in J$ e ϕ é anisotrópica em F, então $\dim(\phi) \geqslant 4$. Suponha que $\dim(\phi) = n$. Seja $\langle a_1, \ldots, a_n \rangle$ uma diagonalização de ϕ. Pelo fato que ϕ é F-anisotrópica, existe $c \in \dot{F}$, tal que $c \in D_F(\phi)$, segue pelo Lema 5.3 que

$$p(t) := c(t^2 - a)(t^2 - b) \in D_{F(t)}(\phi_{F(t)}).$$

Como $p(t) \in F[t] \cap D_{F(t)}(\phi_{F(t)})$, pelo teorema de Cassels-Pfister 4.35, $p(t)$ é representado por ϕ sobre $F[t]$, ou seja, $p(t) = \sum_{i=1}^{n}[a_i(f_i(t))^2]$, com $f_i(t) \in F[t]$. Pelo fato que ϕ é F-anisotrópica e $\deg(p(t)) = 4$, então $\deg(f_i(t)) \leqslant 2$, para todo $i = 1, \ldots, n$. Assim, $f_i(t) = \alpha_i t^2 + \beta_i t + \gamma_i$, com $\alpha_i, \beta_i, \gamma_i \in F$. Então

$$p(t) = \sum_{i=1}^{n}[a_i(\alpha_i t^2 + \beta_i t + \gamma_i)^2].$$

Abrindo as contas obtemos que

$$\begin{array}{rcl} p(t) & = & ct^4 - c(a+b)t^2 + abc \\ & = & \sum_{i=1}^{n}[a_i(\alpha_i)^2 t^4 + a_i(2\alpha_i\beta_i)t^3 + a_i(\beta_i^2 + 2\alpha_i\gamma_i)t^2 + a_i(2\beta_i\gamma_i)t + a_i(\gamma_i)^2]. \end{array}$$

Tomando $v_2 = (\alpha_1, \ldots, \alpha_n)$, $v_1 = (\beta_1, \ldots, \beta_n)$ e $v_0 = (\gamma_1, \ldots, \gamma_n)$ no espaço vetorial V, temos que $p(t) = \phi(v_2 t^2 + v_1 t + v_0)$. Note que em particular, $\phi(v_2) = c$ e $\phi(v_0) = abc$.

Seja $W \subset V$ o subespaço gerado por v_2, v_1 e v_0, e seja $\phi_0 = \phi|_W$. Afirmamos que $av_2 + \sqrt{a}v_1 + v_0 \neq 0$ em $W_{F(\sqrt{a})}$. De fato, suponha que $av_2 + \sqrt{a}v_1 + v_0 = 0$. Caso $v_1 \neq 0$, então $v_1 = -\sqrt{a}v_2 - (\sqrt{a})^{-1}v_0$. Assim,

$$\phi_0((t^2 - (\sqrt{a})t)v_2 + (1 - (\sqrt{a})^{-1}t)v_0) = \phi_0(v_2 t^2 + v_1 t + v_0) = ct^4 - c(a+b)t^2 + abc.$$

Seja $k = B_{\phi_0}(v_2, v_0)$, onde B_{ϕ_0} é a forma bilinear simétrica associada a ϕ_0. Desenvolvendo os dois lados da igualdade acima, temos o seguinte sistema

$$\begin{cases} a^2 = 1 \\ -ac\sqrt{a} - \sqrt{a}k = 0 \\ -\sqrt{a}k - abc\sqrt{a} = 0 \\ c(a+b) + (a+1)k = 0. \end{cases}$$

Pela resolução desse sistema em particular temos que $ab = 1$, o que é um absurdo. Logo $v_1 = 0$. Agora, se $av_2 + v_0 \neq 0$, então claramente $av_2 + \sqrt{a}v_1 + v_0 \neq 0$. Mas, se $av_2 + v_0 = 0$, então $v_0 = -av_2$ e assim,

$$c(t^2 - a)(t^2 - b) = \phi_0(av_2 + \sqrt{a}v_1 + v_0) = \phi_0((t^2 - a)v_2).$$

Como $\phi_0(v_2) = c$, então $(t^2 - a) = (t^2 - b)$. Implicando que $a = b$, o que é um absurdo. Concluímos que $av_2 + \sqrt{a}v_1 + v_0 \neq 0$ em $F(\sqrt{a})$ e como $\phi_0(av_2 + \sqrt{a}v_1 + v_0) = 0$, $\phi_{0_{F(\sqrt{a})}}$ é isotrópica. Analogamente $bv_2 + \sqrt{b}v_1 + v_0 \neq 0$ e consequentemente $\phi_{0_{F(\sqrt{b})}}$ é isotrópica.

Agora basta mostrar que $\dim(W) = 3$. De fato, como $av_2 + \sqrt{a}v_1 + v_0 \neq 0$, segue que $\dim(w) \geqslant 1$. Pelo fato que $\phi_{0_{F(\sqrt{a})}}$ é isotrópica, temos pelo Teorema 4.24 que $\phi_0 \cong$

$q \otimes \langle\langle -a \rangle\rangle \perp q'$, com $q, q' \in W(F)$ e q F-anisotrópica. Isso é suficiente para afirmarmos que $\dim(W) \geqslant 2$. Caso $\dim(W) = 2$, então $\phi_0 \cong \langle e \rangle \otimes \langle\langle -a \rangle\rangle$, com $e \in \dot{F}$. Analogamente, $\phi_0 \cong \langle e' \rangle \otimes \langle\langle -b \rangle\rangle$, com $e' \in \dot{F}$. Implicando que $-a \cdot \dot{F}^2 = d(\phi_0) = -b \cdot \dot{F}^2$. Assim, $ab \in \dot{F}^2$, o que é um absurdo. Logo $\dim(W) \leqslant 3$. Como W é gerado por v_0, v_1, v_2. Portanto $\dim(W) = 3$. □

Lema 5.5. *Seja $\phi \in J$, tal que ϕ é uma F-forma quadrática anisotrópica e ϕ_0 como no lema anterior. Se $\pi \cong \phi_0 \perp \langle d(\phi_0) \rangle$, então $\dim(\pi) = 4$, $\pi \in J$ e $\pi \cong \langle c \rangle \otimes \langle\langle -b, -a+bu^2 \rangle\rangle$, onde $c, u \in F$.*

Demonstração: Como $\dim(\phi_0) = 3$, claramente $\dim(\pi) = 4$. Agora basta provarmos que $\pi \in J$ e π é o produto de uma F-forma de Pfister de duas camadas por um escalar em $W(F)$. De fato, note que como ϕ_o é F-anisotrópica, $\dim(\phi_0) = 3$ e é $F(\sqrt{a})$-isotrópica, pelo Teorema 4.24, temos que $\phi_0 \cong \langle c \rangle \otimes \langle\langle -a \rangle\rangle \perp \langle d \rangle$, com $d \in F$ e $c \in \dot{F}$. Assim,

$$\begin{aligned} \pi &\cong \langle c \rangle \otimes \langle\langle -a \rangle\rangle \perp \langle d \rangle \perp \langle d(\phi_0) \rangle \\ &\cong \langle c \rangle \otimes \langle 1, -a, cd, (-a)cd \rangle \\ &\cong \langle c \rangle \otimes \langle\langle -a, cd \rangle\rangle \\ &\cong \langle c \rangle \otimes \langle\langle -a \rangle\rangle \otimes \langle\langle cd \rangle\rangle. \end{aligned}$$

Implicando que $\pi \in W(F(\sqrt{a})/F)$. Analogamente $\pi \cong \langle e \rangle \otimes \langle\langle -b, ke \rangle\rangle$, com $k \in F$ e $e \in \dot{F}$. Implicando que $\pi \in W(F(\sqrt{b})/F)$ e consequentemente $\pi \in J$. Como $\pi \cong \langle c \rangle \otimes \langle\langle -a \rangle\rangle \perp \langle d \rangle \in J$, então $\langle\langle -a \rangle\rangle \perp \langle d \rangle \in J$. Pelo Lema 5.2 segue que $\pi \cong \langle c \rangle \otimes \langle\langle -b, -a + bu^2 \rangle\rangle$, com $u \in F$ e $c \in \dot{F}$, provando o lema. □

Proposição 5.6. *O ideal $J \subseteq W(F)$ é gerado pelas F-formas quadráticas $\langle\langle -b, -a + bu^2 \rangle\rangle$, onde $u \in F$.*

Demonstração: Seja $\phi \in J$. Se ϕ é hiperbólica nada temos que provar. Suponha que ϕ não tenha partes hiperbólicas, ou seja ϕ é F-anisotrópica. Provaremos essa proposição por indução sobre $\dim_F(\phi)$, a seguinte igualdade

$$\phi = \sum_{i=1}^{n} \langle c_i \rangle \otimes \langle\langle -b, -a + bu_i^2 \rangle\rangle, \text{ com } c_i, u_i \in F, \text{ sendo } n = \frac{dim_F(\phi) - 2}{2}.$$

Supondo que $n = 1$, então $\dim(\phi) = 4$. Pelo Lema 5.5, temos que $\pi = \phi_o \perp \langle d(\phi_0) \in J$, sendo ϕ_0 a subforma gerada pelo Lema 5.4. Como $\dim(\phi) = 4$, então $\phi = \phi_0 \perp \langle k \rangle$, onde $k \in \dot{F}$. Afirmamos que $\pi \cong \phi$. De fato, como J é ideal de $W(F)$, então

$$\langle k, -d(\phi_0) \rangle = \phi_0 + \langle k \rangle - \phi_0 - \langle d(\phi_0) \rangle = \phi - \pi \in J.$$

Se $\langle k, -d(\phi_0) \rangle = 0_{W(F)}$, então $\phi \cong \pi$. Por outro lado, se $\langle k, -d(\phi_0) \rangle \neq 0_{W(F)}$, então $\langle k, -d(\phi_0) \rangle$ é F-anisotrópico. Como $\langle k, -d(\phi_0) \rangle \in J$, segue que $\langle k, -d(\phi_0) \rangle \cong \langle x \rangle \otimes \langle\langle -a \rangle\rangle$ e $\langle k, -d(\phi_0) \rangle \cong \langle y \rangle \otimes \langle\langle -b \rangle\rangle$, com $x, y \in \dot{F}$. Isso implica que $-b \cdot \dot{F}^2 = d(\phi - \pi) = -a \cdot \dot{F}^2$, o que é um absurdo, pois $ab \notin \dot{F}^2$. Logo $\langle k, -d(\phi_0) \rangle = 0_{W(F)}$. Portanto $\phi \cong \pi$. Pelo Lema 5.5, temos que $\phi = \langle c \rangle \otimes \langle\langle -b, -a + bu^2 \rangle\rangle$, provando a igualdade para $n = 1$.

Suponha que a igualdade seja válida para $m < \dim_F(\phi)$. Seja $\phi \in J$ uma F-forma anisotrópica, tal que $\dim(\phi) = 2n + 2$. Novamente tomando $\pi \cong \phi_0 \perp \langle d(\phi_0) \rangle$, pelo Lema

5.5 temos que $\pi \cong \langle c\rangle \otimes \langle\langle -b, -a+bu^2\rangle\rangle$. Como $\pi \in J$, segue que $\phi - \pi \in J$. Assim, pelo Teorema da Decomposição de Witt 1.61 temos que

$$\dim(\phi_a - \pi_a) \leqslant \dim(\phi_a - \phi_{0_a}) + 1 = \dim(\phi) - 2.$$

Como $\phi - \pi = \phi_a - \pi_a \perp \pi_h$, então pela hipótese de indução temos que

$$\phi - \pi = \sum_{i=1}^{n-1} \langle c_i\rangle \otimes \langle\langle -b, -a+bu_i^2\rangle\rangle.$$

Tomando $c = c_n$ e $u = u_n$, então

$$\phi = \sum_{i=1}^{n} \langle c_i\rangle \otimes \langle\langle -b, -a+bu_i^2\rangle\rangle.$$

Provando a proposição. □

Observação 5.7. Agora iremos calcular o núcleo da transfer $s_* : W(F(\sqrt{a}, \sqrt{b})) \longrightarrow W(F)$ correspondente o F-funcional linear $s : F(\sqrt{a}, \sqrt{b}) \longrightarrow F$, definido por $s(1) = s(\sqrt{a}) = s(\sqrt{b}) = 0$ e $s(\sqrt{ab}) = 1$. Para qualquer extensão quadrática de corpos $F(\sqrt{d})/F$, denotaremos por $\mathrm{cor}_{F(\sqrt{d})/F}$ a transfer $W(F(\sqrt{d})) \longrightarrow W(F)$ associada ao F-funcional linear $\mathrm{cor} : F(\sqrt{d}) \longrightarrow F$, definido por $\mathrm{cor}(1) = 0$ e $\mathrm{cor}(\sqrt{d}) = 1$.

Analogamente, tomemos $\mathrm{res}_{F(\sqrt{d})/F}$, para denotar o homomorfismo

$$r^* : W(F) \longrightarrow W(F(\sqrt{d})), \text{ dado por } q \longrightarrow q_{F(\sqrt{d})}.$$

Note que com essa notação definida anteriormente, $\mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F} = s_*$. Pela observação 4.9 , é fácil ver que $s_* = \mathrm{cor}_{F(\sqrt{a})/F} \circ \mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})}$.

Teorema 5.8. *O grupo* $\ker(s_*)$ *é gerado pelas* 1*-dimensional formas quadráticas* $\langle x + y\sqrt{a}\rangle$, $\langle x + y\sqrt{b}\rangle$ *e* $\langle x\sqrt{a} + y\sqrt{b}\rangle$, *onde* $x, y \in F$.

Demonstração: Primeiramente, note que se $F(\sqrt{d})/F$ é uma extensão quadrática e $\mathrm{cor}_{F(\sqrt{d})/F}$ é dada como nas observações acima, pelo Teorema 4.27, temos que

$$\mathrm{cor}_{F(\sqrt{d})/F}(\langle x + y\sqrt{a}\rangle) = \langle y, -y(x^2 - dy^2)\rangle, \text{ com } x \in F \text{ e } y \in D(\langle x + y\sqrt{a}\rangle).$$

Pois, $y = \mathrm{cor}_{F(\sqrt{d})/F}(\langle x + y\sqrt{a}\rangle)(1_{F(\sqrt{d})})$.

Afirmamos que $\langle x + y\sqrt{a}\rangle$, $\langle x + y\sqrt{b}\rangle$, $\langle x\sqrt{a} + y\sqrt{b}\rangle \in \ker(s_*)$, com $x, y \in F$. De fato, como $s_*(\phi) = \mathrm{cor}_{F(\sqrt{a})/F} \circ \mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})}(\phi)$, então

$$\begin{aligned} s_*(\langle x + y\sqrt{a}\rangle) &= \mathrm{cor}_{F(\sqrt{a})/F} \circ \mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})}(\langle x + y\sqrt{a}\rangle) \\ &= \mathrm{cor}_{F(\sqrt{a})/F}(\langle y, -y(x^2 - ay^2)\rangle) \\ &= \mathrm{cor}_{F(\sqrt{a})/F}(\langle y\rangle) + \mathrm{cor}_{F(\sqrt{a})/F}(\langle -y(x^2 - ay^2)\rangle) \\ &= 0_{W(F)} + 0_{W(F)} = 0_{W(F)}. \end{aligned}$$

Provando que $\langle x + y\sqrt{a}\rangle \in \ker(s_*)$, para todo $x, y \in F$. Analogamente $\langle x + y\sqrt{b}\rangle$, $\langle x\sqrt{a} + y\sqrt{b}\rangle \in \ker(s_*)$.

Note que dado uma extensão quadrática $F(\sqrt{d})/F$, se $\mathrm{cor}_{F(\sqrt{d})/F)}$ for como na Observação 5.7, pelo Teorema do Triângulo Exato 4.28, temos que

$$\begin{array}{ccc} W(F(\sqrt{a})) & \xrightarrow{\mathrm{cor}_{F(\sqrt{d})/F)}} & W(F) \\ & \nwarrow^{r^*} & \downarrow{\scriptstyle \otimes\langle\langle -d\rangle\rangle} \\ & & W(F) \end{array}$$

Agora podemos provar que o conjunto formado pelas $F(\sqrt{a},\sqrt{b})$-formas quadráticas unidimensionais $\langle x+y\sqrt{a}\rangle$, $\langle x+y\sqrt{b}\rangle$ e $\langle x\sqrt{a}+y\sqrt{b}\rangle$, com $x,y\in F$, gera $\ker(s_*)$. De fato, seja $q\in\ker(s_*)$. Isso implica que

$$s_*(q)=\mathrm{cor}_{F(\sqrt{a})/F}(\mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})}(q))=0_{W(F)}.$$

Pelo Teorema do Triângulo Exato 4.28 nas extensões quadráticas $F(\sqrt{a},\sqrt{b})/F(\sqrt{a})$ e $F(\sqrt{a})/F$ temos que $\mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})}(q)=\phi_{F(\sqrt{a})}$, com $\phi\in W(F)$. Como $\phi_{F(\sqrt{a})}\in \mathrm{Im}(\mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})})$, segue que $\phi_{F(\sqrt{a})}\in\ker(\otimes\langle\langle -b\rangle\rangle)$, ou seja, $\langle\langle -b\rangle\rangle\otimes\phi_{F(\sqrt{a})}=0_{W(F(\sqrt{a}))}$. Implicando que $\langle\langle -b\rangle\rangle\otimes\phi_{F(\sqrt{a})}\in W(F(\sqrt{a})/F)$. Então $\langle\langle -b\rangle\rangle\otimes\phi\in J$. Pela Proposição 5.6, temos que

$$\langle\langle -b\rangle\rangle\otimes\phi=\sum_{i=1}^{n}\langle c_i\rangle\otimes\langle\langle -b,-a+bu_i^2\rangle\rangle,\ \text{com } c_i\in\dot{F},\ u_i\in F \text{ e}$$

$n=\frac{\dim(\langle\langle -b\rangle\rangle\otimes\phi)-2}{2}$. Equivalentemente,

$$\langle\langle -b\rangle\rangle\otimes\left(\phi-\sum_{i=1}^{n}\langle c_i\rangle\otimes\langle\langle -a+bu_i^2\rangle\rangle\right)=0_{W(F)}.$$

Pelo Teorema do triângulo Exato 4.28 aplicado na extensão quadrática $F(\sqrt{b})/F$ temos que $\phi-\sum_{i=1}^{n}\langle c_i\rangle\otimes\langle\langle -a+bu_i^2\rangle\rangle\in\mathrm{Im}(\mathrm{cor}_{F(\sqrt{b})/F})$, ou seja,

$$\phi=\sum_{i=1}^{n}\langle c_i\rangle\otimes\langle\langle -a+bu_i^2\rangle\rangle+\mathrm{cor}_{F(\sqrt{b})/F}(\psi),\ \text{para alguma } \psi\in W(F(\sqrt{b})).$$

Notemos que

$$\mathrm{res}_{F(\sqrt{a})/F}\circ\mathrm{cor}_{F(\sqrt{b})/F}(\langle x+y\sqrt{b}\rangle)=\mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})}\circ\mathrm{res}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{b})}(\langle x+y\sqrt{b}\rangle),$$

para quaisquer $x,y\in F$. Isso é suficiente para mostrar que

$$\mathrm{res}_{F(\sqrt{a})/F}\circ\mathrm{cor}_{F(\sqrt{b})/F}=\mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})}\circ\mathrm{res}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{b})}\,.$$

Por essa igualdade acima temos que

$$\begin{aligned}
\mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})}(q) = \phi_{F(\sqrt{a})} &= \mathrm{res}_{F(\sqrt{a})/F} \circ \mathrm{cor}_{F(\sqrt{b})/F}(\phi) \\
&= \mathrm{res}_{F(\sqrt{a})/F} \left(\sum_{i=1}^{n} \langle c_i \rangle \otimes \langle\langle -a + bu_i^2 \rangle\rangle + \right. \\
&\quad \left. \mathrm{cor}_{F(\sqrt{b})/F}(\psi)\right) \\
&= \mathrm{res}_{F(\sqrt{a})/F} \left(\sum_{i=1}^{n} \langle c_i \rangle \otimes \langle\langle -a + bu_i^2 \rangle\rangle\right) + \\
&\quad \mathrm{res}_{F(\sqrt{a})/F} \circ \mathrm{cor}_{F(\sqrt{b})/F}(\psi) \\
&= \left(\sum_{i=1}^{n} \langle c_i \rangle \otimes \langle\langle -a + bu_i^2 \rangle\rangle_{F(\sqrt{a})}\right) + \\
&\quad \mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})} \circ \mathrm{res}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{b})}(\psi) \\
&= \mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})} \left(\sum_{i=1}^{n} \langle c_i \rangle \otimes \langle u_i^{-1}\sqrt{a} + \sqrt{b} \rangle\right) + \\
&\quad \mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})}(\psi_{F(\sqrt{a},\sqrt{b})}) \\
&= \mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})} \left(\sum_{i=1}^{n} \langle c_i \rangle \otimes \langle u_i^{-1}\sqrt{a} + \sqrt{b} \rangle + \right. \\
&\quad \left. \psi_{F(\sqrt{a},\sqrt{b})}\right).
\end{aligned}$$

Pois $\langle c_i \rangle \otimes \langle\langle -a + bu_i^2 \rangle\rangle = \langle c_i \rangle \otimes \langle\langle -au^{-2} + b \rangle\rangle$, para todo $i = 1, \ldots, n$. Assim,

$$\mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})} \left(q - \psi_{\sqrt{a},\sqrt{b}} - \sum_{i=1}^{n} \langle c_i \rangle \otimes \langle (u_i^{-1}\sqrt{a}) + \sqrt{b} \rangle\right) = 0_{W(F(\sqrt{a}))}.$$

Pelo Teorema do Triângulo Exato aplicado na extensão quadrática de corpos $F(\sqrt{a},\sqrt{b})/F(\sqrt{a})$ temos que

$$\left(q - \psi_{F(\sqrt{a},\sqrt{b})} - \sum_{i=1}^{n} \langle c_i \rangle \otimes \langle u_i^{-1}\sqrt{a} + \sqrt{b} \rangle\right) \in \mathrm{Im}\left(\mathrm{res}_{F(\sqrt{a},\sqrt{b})/F(\sqrt{a})}\right).$$

Implicando que $q = \psi_{F(\sqrt{a},\sqrt{b})} + \sum_{i=1}^{n} \langle c_i \rangle \otimes \langle (u_i^{-1}\sqrt{a}) + 1\sqrt{b} \rangle + \tau_{F(\sqrt{a},\sqrt{b})}$, onde $\tau \in W(F(\sqrt{a}))$. Como $W(F(\sqrt{a}))$ é gerado por somas finitas de formas quadráticas $\langle x + y\sqrt{a} \rangle$ e $W(F(\sqrt{b}))$ é gerado por somas finitas de formas quadráticas $\langle x + y\sqrt{b} \rangle$, então

$$q = \sum_{i=1}^{n} \langle c_i \rangle \otimes \langle (u_i^{-1}\sqrt{a}) + 1\sqrt{b} \rangle + \sum_{j=1}^{m} \langle x_j + y_j\sqrt{a} \rangle + \sum_{k=1}^{l} \langle x_k + y_k\sqrt{b} \rangle.$$

Provando o teorema. □

Observação 5.9. O Teorema 5.8 torna possível calcular o núcleo $\ker(s_*)$ para qualquer F-funcional linear não nulo $s : F(\sqrt{a},\sqrt{b}) \longrightarrow F$. De fato, no Capítulo 4 vimos que existe $l \in F(\sqrt{a},\sqrt{b})^*$, tal que $s(lx) = \mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F}(x)$, para qualquer $x \in F(\sqrt{a},\sqrt{b})^*$. Consequentemente $\mathrm{cor}_{(F\sqrt{a},\sqrt{b})/F} = s^* \circ l$, e então $\ker(\mathrm{cor}_{(F\sqrt{a},\sqrt{b})/F}) = \langle l \rangle \otimes \ker(s_*)$.

Uma pergunta natural que surge é se qualquer forma quadrática 1-dimensional em $\ker(\mathrm{cor}_{F(\sqrt{a},\sqrt{b})/F})$ é isométrica a um dos geradores fornecidos no Teorema 5.8. O próximo exemplo mostra que a resposta é negativa.

Exemplo 5.10. Sejam F um corpo ($charF \neq 2$) e $a, b \in \dot{F}$, tais que $a, b, ab \notin \dot{F}^2$. Então, existem uma extensão de corpos L/F e uma $L(\sqrt{a},\sqrt{b})$-forma quadrática unidimensional, tal que $\phi \in \ker(\mathrm{cor}_{L(\sqrt{a},\sqrt{b})/L})$ e $\phi \ncong < x + y\sqrt{a} >, < x + y\sqrt{b} >, < x\sqrt{a} + y\sqrt{b} >$, onde $x, y \in L$.

Demonstração: Sejam x, y, z, w variáveis distintas em F. Definamos $F_1 := F(x, y, z, w)$. Como F_1/F é uma extensão transcendental pura, segue do Lema 4.33 que $a, b, ab \notin \dot{F}_1^2$. Implicando que $F_1(\sqrt{a}, \sqrt{b})/F_1$ é uma extensão biquadrática de corpos. Seja a $F_1(\sqrt{a}, \sqrt{b})$-forma quadrática unidimensional $\phi_1 := \langle x+y\sqrt{a}+z\sqrt{b}+w\sqrt{ab}\rangle$. Pela observação 5.7, temos que $\mathrm{cor}_{F_1(\sqrt{a},\sqrt{b})/F_1} = \mathrm{cor}_{F_1(\sqrt{a})/F_1} \circ \mathrm{cor}_{F_1(\sqrt{a},\sqrt{b})/F_1(\sqrt{a})}$. Assim, tomando $\phi_1' := \mathrm{cor}_{F_1(\sqrt{a},\sqrt{b})/F_1}(\phi_1)$, segue que

$$\begin{aligned}\phi_1' &\cong \mathrm{cor}_{F_1(\sqrt{a})/F_1} \circ \mathrm{cor}_{F_1(\sqrt{a},\sqrt{b})/F_1(\sqrt{a})} \left[\langle (x+y\sqrt{a}) + (z+w\sqrt{a})\sqrt{b}\rangle\right] \\ &\cong \mathrm{cor}_{F_1(\sqrt{a})/F_1} \left[\langle z+w\sqrt{a}\rangle \otimes_{F_1(\sqrt{a})} \langle 1, -[(x+y\sqrt{a})^2 - b(z+w\sqrt{a})^2]\rangle\right].\end{aligned}$$

Pelo Teorema 4.27 e por algumas contas, obtemos que $\phi_1' \cong \langle w, -wN, K, -N'NK\rangle$, onde $N = N_{F_1(\sqrt{a})/F_1}(z+w\sqrt{a})$, $N' = N_{F_1(\sqrt{a})/F_1}[(x+y\sqrt{a})^2 - b(z+w\sqrt{a})^2]$ e K é um multinômio nas variáveis x, y, z e w, sobre F. Isso implica que $d(\phi_1') = N'\dot{F_1}^2$. Como N, N' são normas da extensão de corpos $F_1(\sqrt{a})/F_1$ e do fato que $z+w\sqrt{a}$, $(x+y\sqrt{a})^2 - b(z+w\sqrt{a})^2 \notin \dot{F}_1$, segue, pelo Teorema 4.29, que N, $N' \notin \dot{F_1}^2$.

Seja $F_2 = F_1\left(\sqrt{N'}\right)$. pelo que provamos acima, $[F_2 : F_1] = 2$. Afirmamos que $a, b, ab \notin \dot{F_2}^2$. Se $a \in \dot{F}^2$, então pelo Teorema 4.29, temos que $aN' \in \dot{F_1}^2$. Como $a = -N_{F_1(\sqrt{a})/F_1}$ e $[(x+y\sqrt{a})^2 - b(z+w\sqrt{a})]\sqrt{a} \notin \dot{F}_1$, segue, pelo Teorema 4.29, que $aN' \notin \dot{F_1}^2$. Analogamente para b e ab.

Como F_2/F_1 é uma extensão quadrática, segue que se tomarmos $\phi_2 : \phi_{1_{F_2(\sqrt{a},\sqrt{b})}}$, então

$$\begin{aligned}\phi_2' := \mathrm{cor}_{F_2(\sqrt{a},\sqrt{b})/F_2} &\cong \langle w, -wN, K, -N'NK\rangle_{F_2} \\ &\cong \langle w, -wN, K, -NK\rangle_{F_2}.\end{aligned}$$

Pelo fato que $d(\phi_2') = 1\dot{F_2}^2$, temos que

$$\begin{aligned}\phi_2' &\cong \langle w, -wN, K, -KN\rangle_{F_2} \\ &\cong \langle w, -wN, -KN, K\rangle_{F_2} \\ &\cong \langle w\rangle_{F_2} \otimes \langle 1, -N, -wKN, wK\rangle_{F_2}.\end{aligned}$$

Assim, $\phi_2' \cong \langle w\rangle_{F_2} \otimes \langle 1, -N, -wKN, wK\rangle_{F_2}$.

Seja $F_3 := F_2\left(\sqrt{N}\right)$. Afirmamos que $a, b, ab \notin \dot{F_3}^2$. De fato, se $a, b, ab \in \dot{F_3}^2$, teríamos pelo Teorema 4.29 que aN, bN e $abN \in \dot{F_2}^2$. Como $az^2 - (aw)^2, bz^2 - abw^2$ e $abz^2 - b(aw)^2 \notin \dot{F_1}^2$, segue que

$$aNN',\ bNN' \text{ e } abNN' \in \dot{F_1}^2.$$

Como $NN' = N_{F_1(\sqrt{a})/F_1}[((x+y\sqrt{a})^2 - b(z+w\sqrt{a}))(z+w\sqrt{a})]$, segue do Teorema 4.29, que aNN', bNN', $abNN' \notin \dot{F_1}^2$. O que é um absurdo. Assim, $F_3(\sqrt{a}, \sqrt{b})/F_3$ é uma extensão biquadrática.

Se definirmos $\phi_3 := \phi_{2_{F_3(\sqrt{a},\sqrt{b})}}$, então

$$\phi_3' := \mathrm{cor}_{F_3(\sqrt{a},\sqrt{b})/F_3}(\phi_3) \cong \langle w\rangle_{F_3} \otimes \langle 1, -N, -wKN, wK\rangle_{F_3} \cong \langle 1, -1, -wK, wK\rangle_{F_3}.$$

Isso implica que $\phi_3' \cong 2\mathbb{H}_{F_3}$ e dessa forma, $\phi_3' = 0$ em $W(F_3)$. Assim

$$\phi_3 \in \ker\left(\mathrm{cor}_{F_3(\sqrt{a},\sqrt{b})/F_3}\right).$$

Queremos mostrar que $\phi_3 \ncong \langle x'+y'\sqrt{a}\rangle, \langle x'+y'\sqrt{b}\rangle, \langle x'\sqrt{a}+y'\sqrt{b}\rangle$, com $x', y' \in F_3$. De fato, se $\phi_3 \cong \langle x'+y'\sqrt{a}\rangle$, com $x', y' \in F_3$, então

$$\mathrm{cor}_{F_3(\sqrt{a},\sqrt{b})/F_3(\sqrt{a})}(\phi_3) = \mathrm{cor}_{F_3(\sqrt{a},\sqrt{b})/F_3(\sqrt{a})}(\langle x'+y'\sqrt{a}\rangle) = 0 \in W(F_3(\sqrt{a})).$$

Por outro lado,

$$\begin{aligned}
\mathrm{cor}_{F_3(\sqrt{a},\sqrt{b})/F_3(\sqrt{a})}(\phi_3) &= \mathrm{cor}_{F_3(\sqrt{a},\sqrt{b})/F_3(\sqrt{a})}\left[\langle x+y\sqrt{a}+z\sqrt{b}+w\sqrt{ab}\rangle_{F_3(\sqrt{a},\sqrt{b})}\right] \\
&= \mathrm{cor}_{F_3(\sqrt{a},\sqrt{b})/F_3(\sqrt{a})}\left[\langle (x+y\sqrt{a})+(z+w\sqrt{a})\sqrt{b}\rangle_{F_3(\sqrt{a},\sqrt{b})}\right] \\
&= \langle z+w\sqrt{a}\rangle_{F_3(\sqrt{a})} \otimes \langle 1, -[(x+y\sqrt{a})^2 - b(z+w\sqrt{a})^2]\rangle_{F_3(\sqrt{a})}.
\end{aligned}$$

Isso implica que

$$N_{F_3(\sqrt{a},\sqrt{b})/F_3(\sqrt{a})}((x+y\sqrt{a})+(z+w\sqrt{a})\sqrt{b}) = [(x+y\sqrt{a})^2 - b(z+w\sqrt{a})^2] \in \dot{F}_3(\sqrt{a})^2.$$

Mostraremos que isso não pode acontecer. De fato, como $F_3(\sqrt{a},\sqrt{b})/F_3(\sqrt{a})$ é uma extensão quadrática e $[(x+y\sqrt{a})+(z+w\sqrt{a})\sqrt{b}] \notin F_3(\sqrt{a})$ (F_3 visto em $F_3(\sqrt{a},\sqrt{b})$), pelo Teorema 4.29, temos que $[(x+y\sqrt{a})^2 - b(z+w\sqrt{a})^2] \notin \dot{F}_3(\sqrt{a})^2$. O que é um absurdo. Logo $\phi_3 \ncong \langle x'+y'\sqrt{a}\rangle$.

Se $\phi_3 \cong \langle x'+y'\sqrt{b}\rangle_{F_3(\sqrt{a},\sqrt{b})}$, com $x', y' \in F_3$, então

$$\mathrm{cor}_{F_3(\sqrt{a},\sqrt{b})/F_3(\sqrt{b})}(\phi_3) = \mathrm{cor}_{F_3(\sqrt{a},\sqrt{b})/F_3}(\langle x'+y'\sqrt{b}\rangle) = 0_{W(F_3(\sqrt{a}))}.$$

Por outro lado,

$$\begin{aligned}
\mathrm{cor}_{F_3(\sqrt{a},\sqrt{b})/F_3(\sqrt{b})}(\phi_3) &= \mathrm{cor}_{F_3(\sqrt{a},\sqrt{b})/F_3(\sqrt{b})}\left[\left\langle (x+z\sqrt{b})+(y+w\sqrt{b})\sqrt{a}\right\rangle\right] \\
&= \left\langle y+w\sqrt{b}\right\rangle_{F_3(\sqrt{b})} \otimes \left\langle 1, -\left[(x+z\sqrt{b})^2 - a(y+w\sqrt{b})^2\right]\right\rangle.
\end{aligned}$$

Isso implica que

$$N_{F_3(\sqrt{a},\sqrt{b})/F_3(\sqrt{b})}\left[(x+z\sqrt{b})+(y+w\sqrt{b})\sqrt{a}\right] = [(x+z\sqrt{b})^2 - a(y+w\sqrt{b})^2] \in \dot{F}_3(\sqrt{b})^2.$$

Como $F_3(\sqrt{a},\sqrt{b})/F_3(\sqrt{b})$ é uma extensão quadrática de corpos e $(x+z\sqrt{b})+(y+w\sqrt{b})\sqrt{a} \notin F_3(\sqrt{b})$, pelo Teorema 4.29, temos que $[(x+z\sqrt{b})^2 - a(y+w\sqrt{b})^2] \notin \dot{F}_3(\sqrt{b})^2$. O que é um absurdo. Logo $\phi_3 \ncong \langle x'+y'\sqrt{b}\rangle$.

Queremos mostrar que $\phi_3 \ncong \langle x'\sqrt{a}+y'\sqrt{b}\rangle$, com $x', y' \in F_3$. Suponha que $\phi \cong \langle x'\sqrt{a}+y'\sqrt{b}\rangle$. Isso implica que $\gamma :\cong \langle\sqrt{a}\rangle \otimes \phi_3 \cong \langle x'+y'\sqrt{ab}\rangle$.

Por fim, provaremos que $\phi_3 \ncong \langle x'\sqrt{a}+y'\sqrt{b}\rangle$. Note que $F_3(\sqrt{a},\sqrt{b}) \cong F_3(\sqrt{a},\sqrt{ab})$ como F-álgebras. Assim , tomemos o corpo $F_3(\sqrt{a},\sqrt{ab})$, temos que

$$\mathrm{cor}_{F(\sqrt{a},\sqrt{ab})/F(\sqrt{ab})}(\gamma) = \mathrm{cor}_{F(\sqrt{a},\sqrt{ab})/F(\sqrt{ab})}(\langle ax'+y\sqrt{ab}\rangle) = 0_{W(F_3(\sqrt{ab}))}.$$

Por outro lado

$$\begin{aligned}
\mathrm{cor}_{F(\sqrt{a},\sqrt{ab})/F(\sqrt{ab})}(\gamma) &= \mathrm{cor}_{F(\sqrt{a},\sqrt{ab})/F(\sqrt{ab})}\left[\left\langle (ay+z\sqrt{ab})+(x+w\sqrt{ab})\sqrt{a}\right\rangle\right] \\
&= \left\langle x+w\sqrt{ab}\right\rangle_{F_3(\sqrt{ab})} \otimes \left\langle 1, -\left[(ay+z\sqrt{ab})^2 - a(x+w\sqrt{ab})^2\right]\right.
\end{aligned}$$

Implicando que $[(ay+z\sqrt{ab})^2-a(x+w\sqrt{ab})^2] \in \dot{F}_3(\sqrt{ab})^2$. Por argumento análogo ao dos casos anteriores, temos que isso é impossível de acontecer. Assim $[(ay+z\sqrt{ab})^2-a(x+w\sqrt{ab})^2] \notin \dot{F}_3(\sqrt{ab})^2$ e consequentemente,

$$\gamma \cong \langle\sqrt{a}\rangle \otimes \phi \ncong \langle ax' + y'\sqrt{ab}\rangle$$

Implicando que $\phi_3 \ncong \langle x'\sqrt{a} + y'\sqrt{b}\rangle$, com x', $y' \in F_3$.

Tomando $L = F_3$ e $\phi = \phi_3$, temos o desejado. □

Referências Bibliográficas

[Lam] LAM, Tsit-Yuen. **Introduction to quadratic forms over fields**. American Mathematical Soc., 2005.

[Siv] Sivatski, A.S. **THE KERNEL OF SCHARLAU'S TRANSFER FOR A BIQUADRATIC EXTENSION**. Preprint.

[Bha] BHATTACHARYA, Phani Bhushan; JAIN, Surender Kumar; NAGPAUL, S. R. **Basic abstract algebra**. Cambridge University Press, 1994.

[Mar] MARTINEZ, Fabio Brochero et al. **Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro**. Coleção Projeto Euclides, IMPA, 2013.