
**Sobre a existência ou não de bases normais
auto-duais para extensões galoisianas de corpos**

Sávio da Silva Coutinho

Livros Grátis

<http://www.livrosgratis.com.br>

Milhares de livros grátis para download.

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura: _____

Sobre a existência ou não de bases normais auto-duais para extensões galoisianas de corpos

*Sávio da Silva Coutinho*¹

Orientadora: Profa. Dra. Ires Dias

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação - ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Matemática

**USP – São Carlos
Janeiro/2009**

¹O autor teve apoio financeiro da CAPES.

*Aos meus pais
José e Darci,
minha irmã,
Andréia,
e minha noiva,
Priscilla.*

Agradecimentos

Agradeço primeiramente a Deus por ter dado a mim a oportunidade.

Agradeço aos meus pais, José e Darci, pelo amor incondicional e pelo apoio durante todo esse período e principalmente nos momentos mais difíceis. Agradeço a minha irmã, Andréia, pelo amor, carinho e conselhos nas horas difíceis e por estar sempre à disposição de me ajudar.

Agradeço à minha noiva, Priscilla, pelo amor, carinho, pela compreensão durante todos esses anos e por me animar em momentos difíceis. Agradeço ao Walter pela ajuda dada na digitação.

Agradeço aos professores e colegas do IME e do ICMC e a todos aqueles que foram responsáveis pela minha formação, em especial ao professor Henrique Guzzo Júnior.

Agradeço à minha orientadora, Ires, pela paciência, compreensão e pelos conselhos.

Por fim, agradeço a todos que, de alguma forma, contribuíram para a realização deste trabalho e à CAPES pelo apoio financeiro.

Resumo

Neste trabalho, apresentamos um estudo sobre a existência ou não de bases normais auto-duais para extensões galoisianas finitas de corpos, mostrando que toda extensão galoisiana finita de grau ímpar possui uma base normal auto-dual, enquanto que para extensões galoisianas de grau par, apresentamos algumas condições suficientes que garantem a não existência de bases normais auto-duais.

Abstract

In this work, we present a study about the existence or not of self-dual normal bases for finite galoisian extensions of fields, showing that all the odd degree finite galoisian extension has a self-dual normal base, whereas for even degree galoisian extensions, we present some sufficient conditions that assure the non-existence of self-dual normal bases.

Sumário

Introdução	1
1 Preliminares e o teorema da base normal	3
1.1 Extensões galoisianas de corpos	3
1.2 Formas bilineares e hermitianas	7
1.3 Independência dos caracteres e a forma traço	14
1.4 O teorema da base normal	23
2 Sobre a existência de bases normais auto-duais	29
3 Sobre a não existência de bases normais auto-duais	39
Referências Bibliográficas	55

Introdução

Na teoria de Galois sobre corpos, ou mais precisamente, no estudo de extensões finitas de corpos $L \supseteq K$, é de fundamental importância encontrarmos bases especiais para L sobre K . Um tipo de base especial são as chamadas bases normais. Sejam $L \supseteq K$ uma extensão galoisiana de corpos com grau n e grupo de Galois $G = \{\sigma_1, \sigma_2, \dots, \sigma_n\}$. Uma base normal de L sobre K é uma base da forma $\mathcal{B} = \{\sigma_1(a), \sigma_2(a), \dots, \sigma_n(a)\}$, para algum $a \in L$, chamado o gerador da base normal \mathcal{B} . Assim, dizemos que a extensão galoisiana $L \supseteq K$ admite uma base normal se existe um elemento $a \in L$ tal que seus conjugados formam uma base de L sobre K .

Também para extensões galoisianas, podemos considerar a forma bilinear traço, induzida pela aplicação traço $Tr_{L/K}$ de L sobre K e, termos a noção de ortogonalidade, ou seja, uma base $\mathcal{B}' = \{a_1, a_2, \dots, a_n\}$ de L sobre K é dita ser ortogonal se $T(a_i, a_j) = 0$, para $i \neq j$, onde $T : L \times L \rightarrow K$ é a forma bilinear traço de L sobre K .

Neste trabalho, apresentamos um estudo sobre a existência ou não de bases normais auto-duais para extensões galoisianas finitas de corpos, mostrando que toda extensão galoisiana finita de grau ímpar possui uma base normal auto-dual, enquanto que para extensões galoisianas de grau par, apresentamos algumas condições suficientes que garantem a não existência de bases normais auto-duais.

No Capítulo 1, apresentamos conceitos e propriedades básicas necessárias para o desenvolvimento e compreensão dos resultados principais do trabalho, que serão apresentados nos capítulos seguintes, finalizando com a demonstração do Teorema da Base Normal.

O Capítulo 2, baseado em [2], é dedicado a demonstrar a existência de bases normais auto-duais no caso em que o grau da extensão galoisiana de corpos é ímpar.

Por fim, no Capítulo 3, baseado em [6], mostraremos condições suficientes que garantem a não existência de bases normais auto-duais.

CAPÍTULO 1

Preliminares e o teorema da base normal

Neste primeiro capítulo apresentamos os conceitos e alguns resultados preliminares necessários para o entendimento e desenvolvimento dos dois resultados que serão apresentados nos dois próximos capítulos.

Alguns resultados básicos da teoria de Galois sobre corpos e sobre formas bilineares, serão apresentados sem demonstração que, caso seja do interesse do leitor, podem ser encontradas em [8] e/ou [9].

1.1 Extensões galoisianas de corpos

Nesta seção, para facilitar a leitura do restante deste trabalho, apresentamos alguns resultados sobre extensões de corpos e grupos de Galois que fazem parte de qualquer curso básico de teoria de Galois, cujas demonstrações podem ser encontradas, por exemplo em [5] e/ou em [9].

No que segue em todo esse trabalho, denotaremos por $L \supseteq K$ a extensão de corpos L sobre K e, por $[L : K]$ o seu grau. Todas as extensões de corpos consideradas serão assumidas serem finitas, isto é, $[L : K] < \infty$.

O conjunto dos K -automorfismos de L , isto é, dos automorfismos $\sigma : L \rightarrow L$, tais que $\sigma(x) = x$, para todo $x \in K$, com a operação de composição, forma um grupo, dito ser o *grupo de Galois de L sobre K* e denotado por $Gal(L/K)$.

Se G é um grupo finito, denotamos por $|G|$ o número de elementos de G , que é a *ordem* de G . Da mesma forma, se $\sigma \in G$, denotamos por $|\langle \sigma \rangle|$ a ordem do subgrupo cíclico $\langle \sigma \rangle$.

Seja $L \supseteq K$ uma extensão de corpos. Um elemento $a \in L$ é dito ser *separável* sobre K se o seu polinômio minimal sobre K não possuir raízes múltiplas. A extensão $L \supseteq K$ é dita ser uma *extensão separável* se cada elemento de L for separável sobre K .

A extensão $L \supseteq K$ é dita ser uma *extensão normal* se L for corpo de raízes de algum polinômio $f(X) \in K[X]$, ou seja, L for o menor corpo que contém K e todas as raízes de $f(X)$. O *fêcho normal* de $L \supseteq K$ é a menor extensão F de L tal que $F \supseteq K$ é normal.

A extensão separável $L \supseteq K$ é dita ser uma *extensão de Galois*, ou L é dita ser uma *extensão galoisiana* de K , se $[L : K] = |\text{Gal}(L/K)|$, ou seja, o grau da extensão $L \supseteq K$ é igual a ordem do grupo de Galois de L sobre K .

O próximo resultado apresenta uma caracterização das extensões galoisianas:

Teorema 1.1 *Seja $L \supseteq K$ uma extensão de corpos. As seguintes condições são equivalentes:*

- (a) $L \supseteq K$ é uma extensão galoisiana;
- (b) L é corpo de raízes de algum polinômio separável $f(X) \in K[X]$;
- (c) L é normal, separável e tem dimensão finita sobre K .

Finalizamos esta seção com a apresentação do teorema fundamental da teoria de Galois. Para tanto, considere $L \supseteq K$ uma extensão galoisiana de corpos, com grupo de Galois $G = \text{Gal}(L/K)$.

Sejam $\Delta = \{F \text{ corpo}; L \supseteq F \supseteq K\}$ o conjunto dos subcorpos intermediários de $L \supseteq K$ e, $\Sigma = \{H \subset G; H \text{ é subgrupo de } G\}$, o conjunto dos subgrupos de G .

Para cada elemento $H \in \Sigma$, associamos o elemento de Δ , $L^H = \{x \in L; \sigma(x) = x, \text{ para todo } \sigma \in H\}$, ou seja, o subcorpo dos elementos de L fixados por H . Por outro

lado, para cada $F \in \Delta$, temos que $L \supseteq F$ é uma extensão galoisiana de corpos e, associamos à F o subgrupo de G , $\text{Gal}(L/F) = \{\sigma \in G; \sigma(x) = x, \text{ para todo } x \in F\}$ o subgrupo dos elementos de G que fixam F . Com estas notações, temos:

Teorema 1.2 (Teorema Fundamental de Galois) *As aplicações $H \mapsto L^H$ e $F \mapsto \text{Gal}(L/F)$, com $H \in \Sigma$ e $F \in \Delta$, são bijeções sendo uma inversa da outra. Além disso, temos que:*

- (a) *Tais aplicações invertem inclusões;*
- (b) $|H| = [L : L^H]$ e $[G : H] = [L^H : K]$;
- (c) *H é um subgrupo normal de G se, e somente se $L^H \supseteq K$ é uma extensão normal.*

Neste último caso temos também que $\text{Gal}(L^H/K) \cong G/H$.

Seja $L \supseteq K$ uma extensão de corpos. Dizemos que $L \supseteq K$ é uma *extensão simples*, ou que L admite um *elemento primitivo* sobre K , se existir $a \in L$ tal que $L = K(a)$, ou seja, L é gerado por K e a . Neste caso, se $[L : K] = n$, então $\{1, a, a^2, \dots, a^{n-1}\}$ é uma base de L sobre K , dita ser a base gerada pelo elemento primitivo a . Sobre extensões simples temos:

Teorema 1.3 *Seja $L \supseteq K$ uma extensão de corpos. Temos que $L \supseteq K$ é uma extensão simples se, e somente se existem um número finito de corpos intermediários entre L e K .*

Demonstração: Vamos supor inicialmente que existe $a \in L$ tal que $L = K(a)$. Sejam F um subcorpo de L contendo K , $f(X) \in K[X]$ o polinômio minimal de a sobre K e $g(X) \in F[X]$ o polinômio minimal de a sobre F . Então, temos que $g(X)|f(X)$ em $F[X]$. Seja E o subcorpo de L gerado por K e pelos coeficientes de $g(X)$. Então, $E \subseteq F$ e claramente o polinômio minimal de a sobre E também é $g(X)$. Como $L = F(a) = E(a)$, temos que $[L : F] = \text{grau}(g(X)) = [L : E]$, de onde concluímos

que $F = E$. Com isso, mostramos que o número de corpos intermediários entre K e L deverá ser finito pois o número de divisores de $g(X)$ é finito.

Reciprocamente, vamos supor agora que $L \supseteq K$ possui um número finito de corpos intermediários. Se K é finito, então L também será finito, já que $|L| = |K|^{[L:K]}$. Pelo fato de L ser um corpo finito, sabemos que o grupo multiplicativo $(\dot{L} = L - \{0\}, \cdot)$ é um grupo cíclico e portanto existe $a \in \dot{L}$ tal que $\dot{L} = [a]$, logo $L = K(a)$, ou seja, a extensão $L \supseteq K$ é simples. Podemos então assumir que K é infinito. Como $[L : K] < \infty$, temos que $L = K(a_1, \dots, a_n)$, para alguns $a_1, \dots, a_n \in L$, ou seja, L é gerada por K e $\{a_1, \dots, a_n\}$. Agora, usando indução sobre n , é suficiente mostrarmos o caso em que $n = 2$, ou seja, basta mostrarmos que para dois elementos quaisquer $a, b \in L$ a extensão $K(a, b) \supseteq K$ é simples. Consideremos os subcorpos $K(a + cb) \subseteq K(a, b)$, onde $c \in K$. Por hipótese temos que existe somente um número finito de tais corpos, e, como K é infinito existem $c \neq d$ em K tais que $K(a + cb) = K(a + db)$. Logo, $b = (c - d)^{-1} \left(a + cd - (a - db) \right) \in K(a + cb)$, o que mostra que $K(a, b) = K(a + cb)$, ou seja, $a + cb$ é um elemento primitivo de $K(a, b)$, como queríamos demonstrar. ■

Como conseqüência deste teorema, temos o teorema do elemento primitivo.

Corolário 1.4 *Toda extensão finita e separável de corpos admite um elemento primitivo.*

Demonstração: Sejam $L \supseteq K$ uma extensão finita e separável e $F \supseteq K$ seu fêcho normal. Desde que $F \supseteq K$ é finita, se mostrarmos que $F \supseteq K$ é uma extensão separável, então teremos que F é uma extensão galoisiana de K . Para isso, observemos que todo elemento de F é raiz do polinômio minimal de algum elemento de L . Como $L \supseteq K$ é separável, temos que o polinômio minimal de todo elemento de L é separável sobre K . Assim, todo elemento de F é separável sobre K . Logo, $F \supseteq K$ é galoisiana.

Notemos que corpos intermediários de $L \supseteq K$ são também corpos intermediários de $F \supseteq K$. Como existe apenas uma quantidade finita de subgrupos do grupo $Gal(F/K)$,

o teorema 1.2 (teorema fundamental da teoria de Galois), nos garante que existe apenas uma quantidade finita de corpos intermediários de $F \supseteq K$. Conseqüentemente, $L \supseteq K$ tem somente uma quantidade finita de corpos intermediários, o que implica, do teorema anterior, que $L \supseteq K$ admite um elemento primitivo. ■

1.2 Formas bilineares e hermitianas

Nesta seção, começaremos apresentando, a noção de forma e/ou módulo hermitiano sobre um anel com elemento identidade. Depois, apresentaremos as noções básicas sobre formas bilineares e alguns resultados sobre anéis de Witt dos espaços bilineares sobre corpos, que serão importantes para demonstrarmos a existência de bases normais auto-duais para extensões galoisianas de grau ímpar de corpos.

No que segue, A denotará um anel com elemento unidade 1, todos os A -módulos considerados, a menos de menção contrária, serão A -módulos à esquerda unitários.

Uma *involução* sobre o anel A é uma aplicação $\bar{} : A \rightarrow A$, tal que para todo $a, b \in A$, temos:

$$(a) \quad \overline{a + b} = \bar{a} + \bar{b};$$

$$(b) \quad \overline{ab} = \bar{b}\bar{a};$$

$$(c) \quad \overline{\bar{a}} = a,$$

ou seja, uma involução sobre A é um anti-automorfismo de A de ordem 2.

Observe que uma involução $\bar{} : A \rightarrow A$ é sempre bijetora, pois de (c) temos a sobrejeção e se $\bar{a} = \bar{b}$, então $a = \overline{\bar{a}} = \overline{\bar{b}} = b$.

Sejam $\bar{} : A \rightarrow A$ uma involução e M um A -módulo. Uma *forma sesquilinear* sobre M é uma aplicação $s : M \times M \rightarrow A$ tal que

$$(a) \quad s(x + y, z) = s(x, z) + s(y, z);$$

$$(b) \quad s(x, y + z) = s(x, y) + s(x, z);$$

$$(c) \quad s(ax, by) = as(x, y)\bar{b},$$

para quaisquer que sejam $a, b \in A$ e $x, y \in M$.

Uma *forma hermitiana* sobre M é uma forma sesquilinear $h : M \times M \rightarrow A$ que satisfaz $h(x, y) = \overline{h(y, x)}$, para todo $x, y \in M$. O par (M, h) é dito ser um *módulo hermitiano* sobre A . Um módulo hermitiano (M, h) é dito ser *hermitiano par* se existir uma forma sesquilinear $s : M \times M \rightarrow A$ com $h(x, y) = s(x, y) + \overline{s(y, x)}$, para todo $x, y \in M$.

O próximo resultado mostra que sobre certas condições, todo módulo hermitiano sobre o anel A é par.

Lema 1.5 *Seja $Z(A)$ o centro do anel A . Se existe $a \in Z(A)$, tal que $a + \bar{a} = 1$, então todo módulo hermitiano sobre A é par.*

Demonstração: Sejam (M, h) um módulo hermitiano sobre A e $a \in Z(A)$, com $a + \bar{a} = 1$. Consideremos $s : M \times M \rightarrow A$, definida por $s(x, y) = ah(x, y)$, para todo $x, y \in M$. Temos que s é uma forma sesquilinear sobre M . Agora, para todo $x, y \in M$, temos $h(x, y) = 1h(x, y) = (a + \bar{a})h(x, y) = ah(x, y) + \bar{a}h(x, y) = ah(x, y) + \overline{\bar{a}h(y, x)}$.

Note que $\overline{s(y, x)} = \overline{ah(y, x)} = \bar{a}\overline{h(y, x)}$, pois $a \in Z(A)$. Conseqüentemente,

$$h(x, y) = ah(x, y) + \overline{\bar{a}h(y, x)} = s(x, y) + \overline{s(y, x)},$$

o que mostra que (M, h) é par. ■

Observação 1.6 Se K é um corpo de característica distinta de 2, $Car(K) \neq 2$, então todo módulo hermitiano sobre K é par. De fato, considerando sobre K a involução trivial, temos que $a = \frac{1}{2} \in Z(K)$ satisfaz o lema 1.5.

Dado $a \in A$, com $\bar{a} = a$, denotaremos por $\langle a \rangle : A \times A \rightarrow A$ a forma hermitiana de posto 1, definida por $(r, s) \mapsto ras$, para todo $r, s \in A$.

Sejam M um A -módulo e $M^* = Hom_R(M, A)$ o seu dual, que tem uma estrutura de A -módulo à esquerda dada por $(af)(x) = f(x)\bar{a}$, para todo $a \in A$, $f \in M^*$ e $x \in M$.

Se (M, h) é um módulo hermitiano sobre A , então a aplicação A -linear $H : M \rightarrow M^*$, dada por $H(x)(y) = h(y, x)$, para todo $x, y \in M$, é chamada a *aplicação adjunta* de h .

Dizemos que a forma hermitiana h é não-singular, ou que o módulo hermitiano (M, h) é não-singular, se a aplicação adjunta é um isomorfismo de A -módulos à esquerda. Note que a forma hermitiana $\langle a \rangle$ é não-singular se, e somente se $a \in \dot{A}$, onde \dot{A} denota o grupo dos elementos inversíveis do anel A .

Vejam agora algumas noções básicas da teoria algébrica das formas bilineares sobre corpos. A definição de formas e/ou espaços bilineares e a construção do anel de Witt dos espaços bilineares, sobre corpos, serão omitidos aqui e, podem ser encontrados em [11].

Sejam $L \supseteq K$ uma extensão de corpos, V um espaço vetorial sobre L , $s : L \rightarrow K$ uma função K -linear não nula e $b : V \times V \rightarrow L$ uma forma bilinear simétrica sobre L . Notemos que V é também um K -espaço vetorial e a composta $sb : V \times V \rightarrow K$, é uma forma bilinear simétrica sobre K . Mais ainda, se $x, y \in V$ são ortogonais no L -espaço bilinear (V, b) , ou seja, $b(x, y) = 0$, então x e y também serão ortogonais no K -espaço bilinear (V, sb) .

O K -espaço bilinear (V, sb) é chamado o *transfer* de (V, b) e denotado por $s^*(V, b)$. Pode-se mostrar que s^* leva L -espaços hiperbólicos em K -espaços hiperbólicos e que s^* induz um homomorfismo de grupos $s^* : W(L) \rightarrow W(K)$, com $(V, b) \mapsto (V, sb)$, onde $W(L)$ e $W(K)$ são os anéis de Witt dos espaços bilineares sobre L e K respectivamente e, denotamos também por (V, b) a classe do espaço bilinear (V, b) no anel de Witt.

Sejam $x \in L$ e $G = Gal(L/K) = \{\sigma_1 = id, \sigma_2, \dots, \sigma_n\}$. A *norma* de L sobre K de x é definida por $N_{L/K}(x) = \prod_{i=1}^n \sigma_i(x)$. Se $m(X) = X^r + a_{r-1}X^{r-1} + \dots + a_0$ é o polinômio minimal de x sobre K , então $N_{L/K}(x) = (-1)^r a_0$. De fato, se u_1, \dots, u_r são as raízes do polinômio minimal, então $m(X) = (X - u_1) \cdots (X - u_r) = X^r + a_{r-1}X^{r-1} + \dots + a_0$, conseqüentemente $a_0 = (-1)^r \prod_{i=1}^r u_i$. Observe que para $\sigma \in Gal(L/K)$ temos que $\sigma(m(X)) = m(X)$. Portanto $a_0 = \sigma(a_0) = \sigma\left((-1)^r \prod_{i=1}^r u_i\right) = (-1)^r \prod_{i=1}^r \sigma(u_i) = (-1)^r \prod_{i=1}^r \sigma_i(x) = (-1)^r N_{L/K}(x)$, ou seja, $N_{L/K}(x) = (-1)^r a_0$.

Para $a \in L$, denotamos por $\langle a \rangle$ o espaço bilinear $\langle a \rangle : L \times L \rightarrow L$, definido por $\langle a \rangle(x, y) = xay$, para todo $x, y \in L$. Nos próximos resultados, utilizaremos o símbolo \simeq para denotar que duas formas bilineares são isométricas.

O próximo resultado, devido à Scharlau, mostra como é a imagem do espaço $\langle 1 \rangle$ em $W(L)$ para uma extensão simples $L \supseteq K$ e um particular transfer s^* .

Teorema 1.7 *Seja $L = K(a) \supseteq K$ uma extensão simples com $[L : K] = n$ e $s : L \rightarrow K$ uma aplicação K -linear, definida por $s(1) = 1, s(a) = \dots = s(a^{n-1}) = 0$. Então,*

(a) *Se $n = 2m$, temos $s^*(\langle 1 \rangle_L) \simeq (m - 1)\mathbb{H}_K \perp \langle 1, -N_{L/K}(a) \rangle$, onde \mathbb{H}_K denota o plano hiperbólico $\langle 1, -1 \rangle$ sobre K e $\langle 1 \rangle_L$ é o espaço bilinear $\langle 1 \rangle$ sobre L ;*

(b) *Se $n = 2m + 1$, temos $s^*(\langle 1 \rangle_L) \simeq m\mathbb{H}_K \perp \langle 1 \rangle_K$, onde $\langle 1 \rangle_K$ é o espaço bilinear $\langle 1 \rangle$ sobre K .*

Demonstração: Note que $\{1, a, a^2, \dots, a^{n-1}\}$ é uma base de L sobre K e $s^*(\langle 1 \rangle_L)(x, y) = s(xy)$, para todo $x, y \in L$.

Seja $L_0 = Ka + Ka^2 + \dots + Ka^{n-1} \subseteq L$. Com relação a forma bilinear $s^*(\langle 1 \rangle_L)$, temos que os subespaços K e L_0 são ortogonais. De fato, para todo $x \in K$ e $y = y_1a + \dots + y_{n-1}a^{n-1} \in L_0$, temos

$$s^*(\langle 1 \rangle_L)(x, y) = s(xy) = y_1xs(a) + \dots + y_nxs(a^{n-1}) = 0.$$

Assim, temos que $s^*(\langle 1 \rangle_L) = \langle 1 \rangle_K \perp L_0$.

Agora, analisemos separadamente os casos em que $n = [L : K]$ é par e ímpar.

Se $n = 2m$, então $\dim_K L_0 = 2m - 1$ e $\{a, a^2, \dots, a^{m-1}\}$ gera um subespaço totalmente isotrópico de L_0 , pois $s^*(\langle 1 \rangle_L)(a^i, a^j) = s(a^{i+j}) = 0$, para todo $i, j = 1, \dots, m-1$. Por um resultado clássico sobre formas bilineares (ver teorema 4.5 em [11]), temos que L_0 contém um subespaço hiperbólico de dimensão $2(m - 1)$, que é isométrico a uma soma de $(m - 1)$ planos hiperbólicos \mathbb{H}_K , de onde obtemos que $L_0 \simeq (m - 1)\mathbb{H}_K \perp L_1$, com $\dim_K L_1 = 1$. Resta determinarmos a forma bilinear restrita ao subespaço L_1 .

Para tanto, consideremos a matriz da forma bilinear $s_*(\langle 1 \rangle_L)$ restrita a L_0 , com relação a base $\{a, a^2, \dots, a^{n-1}\}$.

$$M = \begin{bmatrix} s(a^2) & s(a^3) & \cdots & s(a^{n-1}) & s(a^n) \\ s(a^3) & s(a^4) & \cdots & s(a^n) & s(a) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ s(a^n) & s(a^{n-1}) & \cdots & s(a^{n-3}) & s(a^{n-2}) \end{bmatrix}.$$

Como $s(a^i) = 0$, para $i = 1, \dots, n-1$, resta calcularmos $s(a^n)$. Como $L = K(a)$ e $[L : K] = n$, temos que o polinômio minimal de a sobre K é da forma $X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$. De onde segue que $a^n = -c_{n-1}a^{n-1} - \cdots - c_1a - c_0$ e, como s é K -linear, obtemos $s(a^n) = -c_0$.

Calculando os determinantes, temos $\det(L_0) = \det(M) = (-1)^m c_0^{n-1} = (-1)^m c_0^{n-1}$. Por outro lado, $L_0 \simeq (m-1)\mathbb{H}_K \perp L_1$, então

$$(-1)^m c_0^{n-1} = \det(L_0) = \det((m-1)\mathbb{H}_K \perp L_1) = (-1)^{m-1} \det(L_1),$$

o que implica que $\det(L_1) = -c_0^{2m-1} = -c_0 \dot{K}^2$.

Mais ainda, como o polinômio minimal de a é $X^n + c_{n-1}X^{n-1} + \cdots + c_0$, temos que $N_{L/K}(a) = (-1)^n c_0 = c_0$. Assim, quando $n = 2m$, temos

$$s^*(\langle 1 \rangle_L) \simeq \langle 1 \rangle_K \perp L_0 \simeq (m-1)\mathbb{H}_K \perp \langle 1, -N_{L/K}(a) \rangle,$$

como queríamos.

Se n é ímpar, então $n = 2m + 1$, então $\dim L_0 = n - 1 = 2m$ e, como visto acima obtemos que $\{a, a^2, \dots, a^m\}$ gera um subespaço totalmente isotrópico de L_0 com dimensão m , o que mostra que $L_0 \cong m\mathbb{H}_K$ e, neste caso, $s^*(\langle 1 \rangle_L) \simeq \langle 1 \rangle_K \perp L_0 \simeq \langle 1 \rangle_K \perp m\mathbb{H}_K$, o que mostra o teorema. ■

No que segue, K denotará um corpo cuja característica é diferente de 2, A uma K -álgebra de dimensão finita e $\bar{}$ uma involução K -linear sobre A .

Se (M, h) é um módulo hermitiano não-singular sobre A e se (V, b) é um espaço bilinear não-singular sobre K , então o produto $b \otimes h$ é uma forma hermitiana sobre

A , definida no A -módulo $M \otimes_K V$. De fato, como $\text{Car}(K) \neq 2$, temos que toda forma bilinear simétrica sobre K é da forma $\langle a_1, \dots, a_n \rangle$, ou seja, V tem uma base $\{v_1, \dots, v_n\}$, ortogonal com respeito a forma b , isto é, com $b(v_i, v_j) = 0$ se $i \neq j$ e $b(v_i, v_i) = a_i$.

Assim, $b = \langle a_1, \dots, a_n \rangle$ e,

$$\begin{aligned} \langle a_1, \dots, a_n \rangle \otimes_K h &= (\langle a_1 \rangle \perp \dots \perp \langle a_n \rangle) \otimes_K h = \\ \langle a_1 \rangle \otimes_K h \perp \langle a_2 \rangle \otimes_K h \perp \dots \perp \langle a_n \rangle \otimes_K h &\simeq a_1 h \perp \dots \perp a_n h . \end{aligned}$$

Esta multiplicação, induz uma estrutura de $W(K)$ -módulo no anel de Witt dos espaços hermitianos sobre A , $W(A)$.

Se $L \supseteq K$ é uma extensão de corpos, então podemos estender a involução $-$ de A para uma involução $\bar{}$ de $A_L = A \otimes_K L$, com $\overline{a \otimes x}^L = \bar{a} \otimes x$, para todo $a \in A$ e $x \in L$.

Para cada módulo hermitiano (M, h) sobre A a extensão de h à $M_L = M \otimes_K L$ é o par (M_L, h_L) , onde

$$\begin{aligned} h_L : M_L \times M_L &\rightarrow A_L \\ (x \otimes c, y \otimes c') &\mapsto h(x, y) \otimes cc' . \end{aligned}$$

Esta extensão induz um homomorfismo de anéis

$$\begin{aligned} r^* : W(A) &\rightarrow W(A_L) \\ (M, h) &\mapsto (M_L, h_L) = (M, h) \otimes_K L . \end{aligned}$$

Seja $s : L \rightarrow K$ uma transformação K -linear. Estendemos s a um homomorfismo A -linear $s_A : A_L \rightarrow A$, onde $s_A(a \otimes x) = as(x)$, para todo $a \in A$ e $x \in L$ e obtemos um homomorfismo de grupos

$$\begin{aligned} s_* : W(A_L) &\rightarrow W(A) \\ (M, h) &\mapsto (M, s_A h) . \end{aligned}$$

Considerando o homomorfismo análogo $s_* : W(L) \rightarrow W(K)$, temos

$$s_*(b \otimes r^*(h)) = s_*(b) \otimes h \text{ em } W(A), \quad (\star)$$

para todo $b \in W(L)$ e $h \in W(A)$.

Para mostrarmos esta última igualdade, devemos mostrar que a aplicação K -linear

$$\begin{aligned} \Phi : V \otimes_L (M \otimes_K L) &\rightarrow V \otimes_K M \\ x \otimes_L (y \otimes c) &\mapsto cx \otimes y \end{aligned}$$

é uma isometria. De fato, para todo $x, x' \in V$, $y, y' \in M$ e $c, c' \in L$, temos

$$\begin{aligned} s_*(b \otimes_L r^*(h))(x \otimes_L (y \otimes c), x' \otimes_L (y' \otimes c')) &= \\ (s_A(b \otimes_L h_L))(x \otimes_L (y \otimes c), x' \otimes_L (y' \otimes c')) &= \\ s_A((b(x, x') \otimes_L h_L)(y \otimes c, y' \otimes c')) &= \\ s_A(b(x, x')cc'h(y, y')) = s_A(b(cx, c'x)h(y, y')) &= \\ (s_A b \otimes h)(cx \otimes y, c'x' \otimes y') &= \\ s_*(b) \otimes h(\Phi(x \otimes (y \otimes c), x' \otimes (y' \otimes c'))) & \end{aligned}$$

Com estas notações temos:

Teorema 1.8 *Sejam $L \supseteq K$ uma extensão de corpos de grau ímpar e A uma K -álgebra de dimensão finita. Então o homomorfismo $r^* : W(A) \rightarrow W(A_L)$, definido acima, é injetor.*

Demonstração: Basta mostrarmos o resultado no caso em que L é uma extensão simples de K , pois como $[L : K]$ é ímpar, temos que o grau das extensões intermediárias também são ímpares, e, o caso geral seguirá de maneira recursiva.

Desta forma, sejam $L = K(a)$ e $s : L \rightarrow K$ a aplicação K -linear, definida por $s(1) = 1$, $s(a) = s(a^2) = \dots = s(a^{n-1}) = 0$, onde $n = [L : K]$. Tomando $b = \langle 1 \rangle_L$ em (\star) , temos $s_*(\langle 1 \rangle_L \otimes r^*(h)) = s_*(\langle 1 \rangle_L) \otimes h$ em $W(A)$. Como $\langle 1 \rangle_L \otimes r^*(h) = r^*(h)$ e $[L : K]$ é ímpar, temos do teorema 1.7 que $s_*(\langle 1 \rangle_L) \otimes h = \langle 1 \rangle_L \otimes h = h$ em $W(A)$, o que mostra que $s_*(r^*(h)) = h$, para todo $h \in W(A)$ e, portanto, r^* é injetora. ■

O próximo resultado o teorema do cancelamento de Witt para formas hermitianas pares, é muito conhecido na teoria algébrica das formas hermitianas. Sua demonstração envolve conceitos que estão além dos nossos objetivos, e por essa razão deixaremos apenas sua referência.

Teorema 1.9 *Seja A uma K -álgebra de dimensão finita. Sejam (M, h) , (M', h') e (N, g) módulos hermitianos pares, não-singulares, sobre A . Se*

$$(M, h) \perp (N, g) \simeq (M', h') \perp (N, g),$$

então $(M, h) \simeq (M', h')$.

Demonstração: Ver teorema 9.1 do Capítulo 7 da referência [11]. ■

Usando o teorema do cancelamento de Witt para módulos hermitianos pares, obtemos um refinamento do teorema 1.9.

Teorema 1.10 *Sejam A uma K -álgebra de dimensão finita, e $L \supseteq K$ uma extensão de corpos de grau ímpar e (M, h) , (M', h') A -módulos hermitianos pares não-singulares. Se $(M_L, h_L) \simeq (M'_L, h'_L)$, então $(M, h) \simeq (M', h')$.*

Demonstração: Como $(M_L, h_L) \simeq (M'_L, h'_L)$, temos que eles representam o mesmo elemento em $W(A_L)$. Como r^* é injetora, temos que (M, h) e (M', h') são iguais em $W(A)$. Logo, existem A -módulos hermitianos hiperbólicos (N, g) e (N', g') tais que

$$(M, h) \perp (N, g) \simeq (M', h') \perp (N', g').$$

Assim, $M \oplus N \cong M' \oplus N'$ como A -módulos e, mais ainda, $M \cong M'$ como A -módulos, pois $M_L \cong M'_L$ como A_L -módulos. Pelo teorema de Krull-Schmidt (6.4 em [10]) obtemos que $N \cong N'$, como A -módulos.

Logo, $(N, g) \cong (N', g')$ como A -módulos hermitianos, pois módulos hermitianos hiperbólicos sobre módulos isomorfos são isomorfos (ver 4.10.1 em [1]). Agora, usando o teorema do cancelamento de Witt para módulos hermitianos pares, obtemos que $(M, h) \cong (M', h')$, como queríamos. ■

1.3 Independência dos caracteres e a forma traço

Nesta seção apresentamos o teorema de independência dos caracteres de Dedekind, um resultado sobre extensões galoisianas, a noção de forma traço de uma extensão

galoisiana de corpos e alguns resultados básicos sobre o comportamento de tais formas traços, que serão úteis no desenvolvimento dos outros capítulos.

Um *caracter* de um monóide H em um corpo F é um morfismo de H no grupo multiplicativo \dot{F} .

Teorema 1.11 (Teorema de independência de Dedeking) *Sejam F um corpo, H um monóide e $\sigma_1, \dots, \sigma_n$ caracteres distintos de H em F . Então os únicos elementos a_1, \dots, a_n em F tais que*

$$a_1\sigma_1(\phi) + a_2\sigma_2(\phi) + \dots + a_n\sigma_n(\phi) = 0,$$

para todo $\phi \in H$, são $a_1 = a_2 = \dots = a_n = 0$, ou seja, os caracteres $\sigma_1, \dots, \sigma_n$ são linearmente independentes sobre F .

Demonstração: Mostraremos este resultado por indução sobre n . Se $n = 1$, então $a_1\sigma_1(\phi) = 0$, para todo $\phi \in H$. Se $a_1 \neq 0$ teremos que $\sigma_1(\phi) = 0$, para todo $\phi \in H$, o que nos dá um absurdo, pois σ leva elemento neutro em elemento neutro, ou seja, $\sigma(1_A) = 1_F \neq 0$. Portanto, $a_1 = 0$.

Suponhamos que $n > 1$ e que o teorema é verdadeiro para $n - 1$ caracteres. Se

$$a_1\sigma_1(\phi) + a_2\sigma_2(\phi) + \dots + a_n\sigma_n(\phi) = 0, \tag{*}$$

para todo $\phi \in H$, como o teorema é válido para $n - 1$ caracteres, podemos supor que a_1, \dots, a_n são todos não nulos. Como $\sigma_1 \neq \sigma_2$, existe $\phi_0 \in H$ tal que $\sigma_1(\phi_0) \neq \sigma_2(\phi_0)$. Substituindo ϕ por $\phi_0\phi$ em (*), obtemos

$$a_1\sigma_1(\phi_0)\sigma_1(\phi) + a_2\sigma_2(\phi_0)\sigma_2(\phi) + \dots + a_n\sigma_n(\phi_0)\sigma_n(\phi) = 0.$$

Por outro lado, multiplicando os dois lados da igualdade (*) por $\sigma_1(\phi_0)$ obtemos

$$a_1\sigma_1(\phi_0)\sigma_1(\phi) + a_2\sigma_1(\phi_0)\sigma_2(\phi) + \dots + a_n\sigma_1(\phi_0)\sigma_n(\phi) = 0.$$

Subtraindo estas duas últimas igualdades temos que

$$b_2\sigma_2(\phi) + \dots + b_n\sigma_n(\phi) = 0,$$

onde $b_i = a_i(\sigma_i(\phi_0) - \sigma_1(\phi_0))$, com $2 \leq i \leq n$.

Por hipótese de indução temos que $b_i = 0$, para todo $i = 2, \dots, n$, o que contradiz o fato de que $b_2 = a_2(\sigma_1(\phi_0) - \sigma_2(\phi_0)) \neq 0$. Portanto, o resultado segue. ■

Corolário 1.12 *Sejam L e F corpos e $\sigma_1, \sigma_2, \dots, \sigma_n$ imersões distintas de L em F . Então $\sigma_1, \sigma_2, \dots, \sigma_n$ são linearmente independentes sobre F .*

Demonstração: Claramente as restrições de σ_i para \dot{L} são caracteres do grupo multiplicativo $H = \dot{L}$ em F , e o resultado segue do teorema anterior. ■

Nosso próximo objetivo é apresentarmos um resultado sobre extensão de corpos e extensões de escalares que usaremos nos próximos capítulos. Para tanto, consideremos $L \supseteq K$ uma extensão de corpos e $G = Gal(L/K)$ o seu grupo de Galois. Seja L^G o subcorpo de L fixado por G , isto é, $L^G = \{a \in L; \sigma(a) = a, \text{ para todo } \sigma \in G\}$.

Seja V um L -espaço vetorial de dimensão $|G|$ com base $\{u_\sigma; \sigma \in G\}$. Em V definimos o seguinte produto

$$\left(\sum_{\sigma \in G} a_\sigma u_\sigma \right) \left(\sum_{\tau \in G} b_\tau u_\tau \right) = \sum_{\sigma, \tau \in G} a_\sigma \sigma(b_\tau) u_{\sigma\tau},$$

para todo $a_\sigma, b_\tau \in L$ e $\sigma, \tau \in G$.

Para todo $a \in L^G$ e $x, y \in V$, temos que $(ax)y = x(ay) = a(xy)$. Com este produto e as operações de espaço vetorial de V , temos que V é uma L^G -álgebra. Como $K \subseteq L^G$, temos também que V é uma K -álgebra. Considere $End_K(L) = \{\phi : L \rightarrow L; \phi \text{ é } K\text{-linear}\}$. A aplicação $\Psi : V \rightarrow End_K(L)$, definida por

$$\Psi \left(\sum_{\sigma \in G} a_\sigma u_\sigma \right) = \sum_{\sigma \in G} a_\sigma \sigma,$$

é um homomorfismo de K -álgebras que é L -linear. Com tais nomenclaturas temos:

Teorema 1.13 *Sejam $L \supseteq K$ uma extensão galoisiana de corpos e $G = Gal(L/K)$. Então a aplicação $\varphi : L \otimes_K L \rightarrow L^{|G|}$, dada por $\varphi(x \otimes y) = (x\sigma(y))_{\sigma \in G}$, é um isomorfismo de L -álgebras.*

Demonstração: Como $L \supseteq K$ é galoisiana, temos que $[L : K] = |G|$. Utilizando o teorema 1.11 (independência de Dedekind) é fácil ver que Ψ , como definida acima, é uma aplicação injetora. Observe também que $\dim_K V = \dim_L V \cdot \dim_K L = |G| \cdot \dim_K L = (\dim_K L)^2$. Sabemos também que $\dim_K \left(\text{End}_K(L) \right) = (\dim_K L)^2$, o que mostra que, Ψ é um isomorfismo de K -álgebras.

Como V é uma K -álgebra, podemos considerar V -módulos. Mostraremos agora que para todo V -módulo à esquerda M a aplicação $\mu : L \otimes_K M^G \rightarrow M$, dada por $\mu(x \otimes m) = xm$, é um isomorfismo de L -espaços vetoriais, onde $M^G = \{y \in M; \sigma.y = y \text{ para todo } \sigma \in G\}$. Com a ação de G em M dada por $\sigma.y = u_\sigma y$, para todo $y \in M$.

De fato, seja M um V -módulo à esquerda, como V é um L -espaço vetorial, obtemos que M é também um L -espaço vetorial.

Sejam $\{x_1, \dots, x_n\} \subset L$ uma base de L sobre K e $\phi_1, \dots, \phi_n \in \text{Hom}_K(L, K)$, tais que $\phi_i(x_j) = \delta_{ij}$, a base dual. Se $\phi \in \text{Hom}_K(L, K)$, então ϕ pode ser estendida trivialmente a um K -endomorfismo de L , logo $\text{Hom}_K(L, K)$ pode ser visto como um subconjunto de $\text{End}_K(L)$. Desde que Ψ é um isomorfismo, podemos tomar $\nu_i = \Psi^{-1}(\phi_i) \in V$, para cada $i = 1, \dots, n$.

Mostraremos que a inversa de μ é a aplicação $\nu : M \rightarrow L \otimes_K M^G$, definida por $\nu(y) = \sum_{i=1}^n x_i \otimes \nu_i y$, para todo $y \in M$.

Para mostrarmos que ν é a inversa de μ , devemos mostrar inicialmente que

- (a) $\nu_i y \in M^G$, para todo $1 \leq i \leq n$ e $y \in M$.
- (b) $\sum_{i=1}^n x_i \nu_i = u_1$, onde $u_1 = u_\sigma$, com $\sigma = id \in G$.
- (c) $\nu(xy) = (\Psi(\nu)(x))y$, para todo $x \in L$, $\nu \in V$ e $y \in M^G$.

Para demonstrarmos (a), observemos que, para todo $x \in L$,

$$\Psi(u_\sigma \nu_i)(x) = \Psi(u_\sigma)(\Psi(\nu_i)(x)) = \sigma(\phi_i(x)) = \phi_i(x),$$

pois $\phi_i(x) \in K$. Logo $\Psi(u_\sigma \nu_i) = \phi_i = \Psi(\nu_i)$ e, como Ψ é um isomorfismo, obtemos $u_\sigma \nu_i = \nu_i$ para todo $\sigma \in G$ e $1 \leq i \leq n$. Assim, para todo $y \in M$ e $1 \leq i \leq n$ temos que $\sigma(\nu_i y) = u_\sigma \nu_i y = \nu_i y$, para todo $\sigma \in G$, o que mostra que $\nu_i y \in M^G$.

O item (b) segue da igualdade

$$\Psi\left(\sum_{i=1}^n x_i \nu_i\right)(x) = \sum_{i=1}^n \Psi(\nu_i)(x) = \sum_{i=1}^n x_i \phi_i(x) = x = \Psi(u_1)(x),$$

para todo $x \in L$ e do fato de Ψ ser injetor.

Para mostrarmos (c), tomemos $x \in L$, $\nu = \sum_{\sigma \in G} a_\sigma u_\sigma \in V$ e $y \in M^G$. Então

$$\nu(xy) = (\nu(xu_1))y = \left(\left(\sum_{\sigma \in G} a_\sigma u_\sigma\right)(xu_1)\right)y =$$

$$\left(\sum_{\sigma \in G} a_\sigma \sigma(x) u_\sigma\right)y = \left(\sum_{\sigma \in G} a_\sigma \sigma(x)\right)y = \Psi(\nu)(x)y.$$

Mostraremos agora que ν é a inversa de μ . Para cada $y \in M$, temos $\mu\left(\nu(y)\right) = \mu\left(\sum_{i=1}^n x_i \otimes \nu_i(y)\right) = \left(\sum_{i=1}^n x_i \nu_i\right)(y) = u_1(y) = y$. Para cada $x \in L$ e $y \in M^G$, temos $\nu\left(\mu(x \otimes y)\right) = \nu(xy) = \sum_{i=1}^n x_i \otimes \nu_i(xy) = \sum_{i=1}^n x_i \otimes \Psi(\nu_i)(x)(y) = \sum_{i=1}^n x_i \otimes \phi_i(x)(y) = \sum_{i=1}^n x_i \phi_i(x) \otimes y = x \otimes y$. Portanto μ é um isomorfismo de L -espaços vetoriais.

Seja $\varphi : L \otimes_L L \rightarrow L^{|G|}$, definida por $\varphi(x \otimes z) = (x\sigma(z))_{\sigma \in G}$. Mostremos que φ é um isomorfismo de L -álgebras. Observe que

$$L^{|G|} = L \times \cdots \times L \cong \text{Map}(G, L),$$

onde o isomorfismo é dado por

$$\begin{aligned} (a_\sigma)_{\sigma \in G} &\leftrightarrow \phi : G \rightarrow L \\ &\sigma \mapsto a_\sigma \end{aligned}$$

Logo, $\text{Map}(G, L)$ é uma L -álgebra e, G age em $\text{Map}(G, L)$ através da ação $\sigma.\phi = \sigma \circ \phi \circ \sigma^{-1}$, para cada $\phi \in \text{Map}(G, L)$ e para cada $\sigma \in G$. Essa ação induz uma estrutura de V -módulo à esquerda em $\text{Map}(G, L)$.

Tomando $M = \text{Map}(G, L)$, temos que $\mu : L \otimes_K \text{Map}(G, L)^G \rightarrow \text{Map}(G, L)$ é um isomorfismo de L -álgebras. Resta mostrarmos que $\text{Map}(G, L)^G \cong L$. Para tanto,

considere

$$\begin{aligned} \Lambda : \text{Map}(G, L)^G &\rightarrow L \\ \phi &\mapsto \phi(1). \end{aligned}$$

Claramente Λ é um homomorfismo de L -álgebras. Seja

$$\begin{aligned} \Lambda' : L &\rightarrow \text{Map}(G, L)^G \\ x &\mapsto \phi_x \end{aligned}$$

onde $\phi_x(\sigma) = \sigma(x)$, para todo $x \in L$ e $\sigma \in G$.

Assim, para cada $x \in L$ temos $\Lambda \circ \Lambda'(x) = \Lambda(\Lambda'(x)) = \Lambda(\phi_x) = \phi_x(1) = 1(x) = x$, e para cada $\phi \in \text{Map}(G, L)^G$, $(\Lambda' \circ \Lambda)(\phi) = \Lambda'(\phi(1)) = \phi_{\phi(1)}$. Mas $\phi_{\phi(1)}(\sigma) = \sigma(\phi(1)) = \sigma(\phi(\sigma^{-1}\sigma)) = (\sigma \cdot \phi)(\sigma) = \phi(\sigma)$, pois $\phi \in \text{Map}(G, L)^G$. Logo $(\Lambda' \circ \Lambda)(\phi) = \phi$ e portanto Λ é um isomorfismo.

Compondo os isomorfismos

$$L \otimes_K L \cong L \otimes_K \text{Map}(G, L)^G \cong \text{Map}(G, L) \cong L^{|G|},$$

temos

$$x \otimes z \mapsto x \otimes \phi_z \mapsto x\phi_z \mapsto (x\phi_z(\sigma))_{\sigma \in G} = (x\sigma(z))_{\sigma \in G},$$

que é o isomorfismo Φ desejado. ■

No restante desta seção, iremos introduzir a noção de forma traço e alguns resultados básicos, que são essenciais para o desenvolvimento do conteúdo do capítulo 2.

Sejam $L \supseteq K$ uma extensão galoisiana de corpos e $G = \text{Gal}(L/K) = \{\sigma_1 = \text{id}, \sigma_2, \dots, \sigma_n\}$ o seu grupo de Galois. Para $x \in L$, o elemento, $\text{Tr}_{L/K}(x) = \sum_{i=1}^n \sigma_i(x)$, é dito ser o *traço de L sobre K de x* .

Desde que $\sigma(\text{Tr}_{L/K}(x)) = \text{Tr}_{L/K}(x)$, para todo $\sigma \in G$ e $x \in L$, temos que $\text{Tr}_{L/K}(x)$ pertence a K , ou seja, $\text{Tr}_{L/K}$ é uma função de L em K , claramente K -linear.

Agora, do fato de $\text{Tr}_{L/K}$ ser K -linear e das propriedades dos elementos de G , é fácil ver que $T : L \times L \rightarrow K$, definida por $T(x, y) = \text{Tr}_{L/K}(xy) = \sum_{\sigma \in G} \sigma(xy)$, para todo $x, y \in L$, é uma forma bilinear simétrica de L sobre K dita ser a *forma traço de L sobre K* .

A seguir, apresentamos um primeiro resultado sobre a forma traço, que será usado várias vezes no que segue.

Lema 1.14 *Sejam $L \supseteq K$ uma extensão galoisiana com grupo de Galois G e $T : L \times L \rightarrow K$ a forma traço de L sobre K . Então a condição $T(\sigma_i(a), \sigma_j(a)) = \delta_{ij}$, para cada $\sigma_i, \sigma_j \in G$ e $a \in L$, é equivalente a*

$$T(a, \sigma(a)) = \begin{cases} 0, & \text{se } \sigma \neq id; \\ 1, & \text{se } \sigma = id, \end{cases}$$

para todo $\sigma \in G$.

Demonstração: Como T é G -invariante, para todo $a \in L$ e $\sigma_i, \sigma_j \in G$, temos que $T(\sigma_i(a), \sigma_j(a)) = T(a, \sigma_i^{-1}\sigma_j(a))$. Assim $T(\sigma_i(a), \sigma_j(a)) = \delta_{ij}$ se, e somente se $\sigma_i = \sigma_j$ e, o resultado segue. ■

Nosso próximo objetivo é mostrarmos que se $L \supseteq K$ é uma extensão galoisiana de corpos, então a forma traço é não-singular, ou seja, a sua adjunta $\varphi : L \rightarrow L^*$, dada por $\varphi(x)(y) = T(x, y)$, para todo $x, y \in L$, é um isomorfismo de K -espaços vetoriais.

Teorema 1.15 *Se $L \supseteq K$ é uma extensão galoisiana de corpos, então a forma traço T de L sobre K é não-singular.*

Demonstração: Basta mostrarmos que a matriz da adjunta de T , φ com relação a um par de bases B e C de L e L^* sobre K , respectivamente, é inversível. Se $\mathcal{B} = \{e_1, e_2, \dots, e_n\}$ é uma base de L sobre K , escolhamos para L^* a base dual $\mathcal{B}^* = \{f_1, \dots, f_n\}$, onde $f_i(e_j) = \delta_{ij}$, para todo $i, j \in \{1, \dots, n\}$. Com isso, temos que se $f \in L^*$, então f se escreve de modo único, como

$$f = \sum_{j=1}^n f(e_j) f_j.$$

Para cada $i = 1, \dots, n$, temos

$$\varphi(e_i) = \sum_{j=1}^n \varphi(e_i)(e_j) f_j = \sum_{j=1}^n T(e_i, e_j) f_j.$$

Logo, a matriz de φ em relação às bases \mathcal{B} e \mathcal{B}^* é $(T(e_i, e_j))_{1 \leq i, j \leq n}$. Queremos então mostrar que $\det(T(e_i, e_j)) \neq 0$.

Como $L \supseteq K$ é uma extensão finita e separável de corpos, então do corolário 1.4 temos que $L = K(a)$, para algum $a \in L$. Além disso, pelo primeiro teorema do isomorfismo, temos que $K(a) \cong \frac{K[X]}{[m(X)]}$, onde $m(X)$ é o polinômio minimal de a sobre K . Do fato de $m(a) = 0$, temos que $\sigma(m(a)) = 0$, ou seja, $m(\sigma(a)) = 0$, para cada $\sigma \in G = \text{Gal}(L/K)$. Como a extensão $L \supseteq K$ é separável, temos que $\sigma(a)$, com $\sigma \in G$, são todas as raízes distintas de $m(X)$, e portanto $m(X) = \prod_{\sigma \in G} (X - \sigma(a))$.

Mais ainda, se $a = a_1, a_2, \dots, a_n$ são as raízes de $m(X)$, temos do fato de $L \supseteq K$ ser separável, que são todas raízes distintas. Como podemos escolher \mathcal{B} uma base de L sobre K arbitrária, tomamos $\mathcal{B} = \{1, a, \dots, a^{n-1}\}$. Se $G = \{\sigma_1, \dots, \sigma_n\}$ e $a_j = \sigma_j(a)$, para todo $1 \leq j \leq n$, temos que $a_j^i = \sigma_j(a^i)$. Assim,

$$T(a^i, a^j) = \text{Tr}_{L/K}(a^{i+j}) = \sum_{r=1}^n \sigma_r(a^{i+j}).$$

Logo, escrevendo $e_i = a^{i-1}$ para cada $i = 1, \dots, n$, temos

$$\begin{aligned} \det(T(e_i, e_j)) &= \det(T(a^{i-1}, a^{j-1})) = \\ &= \det \begin{bmatrix} T(1, 1) & T(1, a) & \cdots & T(1, a^{n-1}) \\ T(a, 1) & T(a, a) & \cdots & T(a, a^{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ T(a^{n-1}, 1) & \cdots & \cdots & T(a^{n-1}, a^{n-1}) \end{bmatrix} = \\ &= \det \begin{bmatrix} \text{Tr}_{L/K}(1) & \cdots & \text{Tr}_{L/K}(a^{n-1}) \\ \vdots & \ddots & \vdots \\ \text{Tr}_{L/K}(a^{n-1}) & \cdots & \text{Tr}_{L/K}(a^{2(n-1)}) \end{bmatrix} = \\ &= \det \begin{bmatrix} \sum_{r=1}^n 1 & \cdots & \sum_{r=1}^n a_r^{n-1} \\ \vdots & \ddots & \vdots \\ \sum_{r=1}^n a_r^{n-1} & \cdots & \sum_{r=1}^n a_r^{2(n-1)} \end{bmatrix} = \end{aligned}$$

$$\begin{aligned}
 &= \det \left(\begin{bmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_n \\ \vdots & & \vdots \\ a_1^{n-1} & \cdots & a_n^{n-1} \end{bmatrix} \cdot \begin{bmatrix} 1 & a_1 & \cdots & a_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & a_n & \cdots & a_n^{n-1} \end{bmatrix} \right) = \\
 &= \left(\det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a_1 & a_2 & \cdots & a_n \\ a_1^2 & a_2^2 & \cdots & a_n^2 \\ \vdots & \vdots & & \vdots \\ a_1^{n-1} & a_2^{n-1} & \cdots & a_n^{n-1} \end{bmatrix} \right)^2 = \\
 &= \left(\prod_{1 \leq k < \ell \leq n} (a_k - a_\ell) \right)^2 \neq 0,
 \end{aligned}$$

pois $a_k \neq a_\ell$, para todo $1 \leq k < \ell \leq n$, o que mostra que a forma traço é não-singular. ■

O próximo resultado estabelece o comportamento da função traço de uma cadeia de corpos $L \supseteq F \supseteq K$.

Teorema 1.16 *Se $L \supseteq F \supseteq K$ são extensões galoisianas de corpos, então*

$$Tr_{L/K} = Tr_{F/K} \circ Tr_{L/F}.$$

Demonstração: Sejam $Gal(F/K) = \{\rho_1, \dots, \rho_m\}$ e $Gal(L/F) = \{\phi_1, \dots, \phi_r\}$. Por um resultado básico da teoria de corpos, podemos estender, de modo único, cada ρ_i , com $i = 1, \dots, m$, a um K -automorfismo $\bar{\rho}_i$ de L . Denotaremos $\bar{\rho}_i$ por ρ_i para não carregar a notação. Para todo $i = 1, \dots, r$ e $j = 1, \dots, m$, temos que $\rho_j \phi_i$ é um K -automorfismo de L , e portanto $\rho_j \phi_i \in Gal(L/K)$. Observe também que $|Gal(L/K)| = [L : K] = [L : F][F : K] = |Gal(L/F)||Gal(F/K)| = rm$ e portanto $Gal(L/K) = \{\rho_j \phi_i; 1 \leq i \leq r \text{ e } 1 \leq j \leq m\}$. Desta forma, $Tr_{F/K} \circ Tr_{L/F}(a) = Tr_{F/K} \left(\sum_{i=1}^r \phi_i(a) \right) = \sum_{j=1}^m \rho_j \left(\sum_{i=1}^r \phi_i(a) \right) = \sum_{j=1}^m \sum_{i=1}^r \rho_j \phi_i(a) = Tr_{L/K}(a)$, para cada $a \in K$. ■

1.4 O teorema da base normal

Esta seção tem por objetivo demonstrar a existência de bases normais para extensões galoisianas de corpos. Como o leitor pode notar esse resultado é o primeiro passo para garantir a existência das bases normais auto-duais no caso em que o grau da extensão é ímpar.

Sejam $L \supseteq K$ uma extensão separável de corpos com $[L : K] = n$, e seja $F \supseteq K$ o fecho normal de $L \supseteq K$.

Teorema 1.17 *Com $F \supseteq L \supseteq K$ como acima, o número de imersões de L em F é $n = [L : K]$ e, se $\sigma_1 = id, \sigma_2, \dots, \sigma_n$ são tais imersões, então a sequência de n elementos de L $\{a_1, a_2, \dots, a_n\}$ é uma base de L sobre K se, e somente se*

$$\det \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \sigma_2(a_1) & \sigma_2(a_2) & \cdots & \sigma_2(a_n) \\ \vdots & \vdots & \vdots & \vdots \\ \sigma_n(a_1) & \sigma_n(a_2) & \cdots & \sigma_n(a_n) \end{pmatrix} \neq 0.$$

Demonstração: Note que $F \supseteq K$ é uma extensão galoisiana. Seja $G = Gal(F/K)$ e H o subgrupo de G formado pelos elementos que fixam os elementos de L . Então do teorema 1.2 (teorema fundamental de Galois), temos que $n = [L : K] = [G : H]$ e, podemos escrever

$$G = \phi_1 H \dot{\cup} \phi_2 H \dot{\cup} \dots \dot{\cup} \phi_n H$$

onde $\phi_i H$, com $i = 1, \dots, n$, são as classes laterais distintas de H em G e $\phi_1 = id$.

Para cada $i = 1, \dots, n$ seja $\sigma_i = \phi_i|_L$. Então σ_i é uma imersão de L em F e, $\sigma_i \neq \sigma_j$, se $i \neq j$. De fato, se $\sigma_i = \sigma_j$, com $i \neq j$, então $\phi_i^{-1}(\phi_j(a)) = a$, para todo $a \in L$. Assim $\phi_i^{-1}\phi_j \in H$ e, conseqüentemente $\phi_i H = \phi_j H$, contrariando a hipótese.

Seja σ uma imersão de L em F . Como $F \supseteq K$ é normal e finita, temos que F é corpo de raízes de um polinômio $f(X) \in K[X]$. Como $L \subseteq F$ e $\sigma(L) \subseteq F$, temos que F é também corpo de raízes de $f(X)$ sobre L e sobre $\sigma(L)$. Assim por um resultado conhecido de extensões de corpos, o isomorfismo σ de L em $\sigma(L)$ pode ser estendido

a um automorfismo ϕ de F . Como $\phi \in Gal(F/K)$, obtemos $\phi = \phi_i \lambda$, para algum $\lambda \in H$. Mas então $\sigma = \phi|_L = \phi_i|_L = \sigma_i$, para cada $i = 1, \dots, n$. Mostramos assim que $\sigma_1, \sigma_2, \dots, \sigma_n$ formam a lista de todas as imersões de L em F .

Suponhamos agora que os elementos a_1, a_2, \dots, a_n de L são linearmente dependentes sobre K . Então existem $c_i \in K$, com $i = 1, \dots, n$, não todos nulos tais que

$$c_1 a_1 + c_2 a_2 + \dots + c_n a_n = 0.$$

Aplicando σ_j na igualdade acima, para cada $j = 1, \dots, n$, temos

$$c_1 \sigma_j(a_1) + \dots + c_n \sigma_j(a_n) = 0.$$

Com isso obtemos que o seguinte sistema linear homogêneo admite uma solução não trivial.

$$\begin{cases} \sigma_1(a_1)x_1 + \dots + \sigma_1(a_n)x_n = 0 \\ \sigma_2(a_1)x_1 + \dots + \sigma_2(a_n)x_n = 0 \\ \vdots \\ \sigma_n(a_1)x_1 + \dots + \sigma_n(a_n)x_n = 0 \end{cases}$$

Conseqüentemente, temos que $\det(\sigma_j(a_i)) \neq 0$.

Reciprocamente, suponhamos que $\det(\sigma_j(a_i)) = 0$. Então o sistema acima é indeterminado, ou seja, admite uma solução não trivial $(c_1, c_2, \dots, c_n) \in K^n$. Neste caso, $\{a_1, a_2, \dots, a_n\}$ não é uma base de L sobre K pois, caso contrário, todo elemento $a \in L$ poderia ser escrito como

$$a = d_1 a_1 + d_2 a_2 + \dots + d_n a_n,$$

com $d_i \in K$, para $1 \leq i \leq n$. Assim,

$$\sum_{j=1}^n c_j \sigma_j(a) = \sum_{1 \leq i, j \leq n} c_j d_i \sigma_j(a_i) = \sum_{i=1}^n d_i \left(\sum_{j=1}^n c_j \sigma_j(a_i) \right) = \sum_{j=1}^n d_j 0 = 0.$$

Mas isto contradiz a independência linear das imersões $\sigma_1, \dots, \sigma_n$ de L sobre K , o que mostra que $\{a_1, \dots, a_n\}$ é uma base de L sobre K . ■

O próximo resultado sobre polinômios nos será útil no que segue.

Lema 1.18 *Se F é um corpo infinito e $f(X_1, \dots, X_r)$ é um polinômio não nulo em $F[X_1, \dots, X_r]$, então existem a_1, \dots, a_r em F tais que $f(a_1, \dots, a_r) \neq 0$.*

Demonstração: Faremos a demonstração por indução sobre r . Se $r = 1$, sabemos que um polinômio $f(X)$ de grau n , tem no máximo n raízes. Como F é um corpo infinito, temos que existe $a \in F$ tal que $f(a) \neq 0$. Agora assumiremos que $r > 1$ e o resultado vale para $r - 1$. Podemos escrever

$$f(X_1, \dots, X_r) = b_0 + b_1 X_r + b_2 X_r^2 + \dots + b_n X_r^n,$$

onde $b_i \in F[X_1, \dots, X_{r-1}]$, com $b_n = b_n(X_1, \dots, X_{r-1}) \neq 0$. Pela hipótese de indução, sabemos que existem $a_1, \dots, a_{r-1} \in F$, tais que $b_n(a_1, \dots, a_{r-1}) \neq 0$. Assim,

$$\begin{aligned} f(a_1, \dots, a_{r-1}, X_r) &= b_0(a_1, \dots, a_{r-1}) + b_1(a_1, \dots, a_{r-1})X_r + \dots \\ &\quad + b_n(a_1, \dots, a_{r-1})X_r^n \in F[X_r] \end{aligned}$$

é um polinômio não nulo de grau n . Agora, basta escolher $a_r \in F$ tal que $f(a_1, \dots, a_r) \neq 0$ e o resultado segue. ■

Para o próximo resultado, necessitaremos da noção de imersões algebricamente independentes.

Sejam $L \supseteq K$ uma extensão separável de corpos, $F \supseteq K$ seu fecho normal e $\sigma_1, \dots, \sigma_n$, imersões de L em F . Dizemos que $\sigma_1, \dots, \sigma_n$ são *algebricamente independentes* sobre F se o único polinômio $f(X_1, \dots, X_n) \in F[X_1, \dots, X_n]$ satisfazendo $f(\sigma_1(a), \dots, \sigma_n(a)) = 0$, para todo $a \in L$, é o polinômio nulo. Com esta noção temos:

Teorema 1.19 *Sejam K um corpo infinito, $L \supseteq K$ uma extensão separável de corpos e $F \supseteq K$ o seu fecho normal. Se $n = [L : K]$ e $\sigma_1, \sigma_2, \dots, \sigma_n$ são as imersões distintas de L em F , então estas imersões são algebricamente independentes sobre F .*

Demonstração: Seja $f(X_1, \dots, X_n) \in F[X_1, \dots, X_n]$ satisfazendo $f(\sigma_1(a), \dots, \sigma_n(a)) = 0$, para todo $a \in L$. Temos que mostrar que f é o polinômio nulo. Seja $\{a_1, \dots, a_n\}$

uma base de L sobre K . Para quaisquer $c_i \in K$, com $1 \leq i \leq n$, temos

$$\begin{aligned} 0 &= f\left(\sigma_1\left(\sum_{i=1}^n c_i a_i\right), \dots, \sigma_n\left(\sum_{i=1}^n c_i a_i\right)\right) \\ &= f\left(\sum_{i=1}^n c_i \sigma_1(a_i), \dots, \sum_{i=1}^n c_i \sigma_n(a_i)\right). \end{aligned}$$

Consideremos o polinômio g definido por

$$g(X_1, \dots, X_n) = f\left(\sum_{i=1}^n \sigma_1(a_i) X_i, \dots, \sum_{i=1}^n \sigma_n(a_i) X_i\right).$$

Temos $g(c_1, \dots, c_n) = 0$ para quaisquer $c_i \in K$, com $1 \leq i \leq n$.

Seja $\{v_1, \dots, v_m\}$ uma base de F sobre K . Então podemos escrever

$$g(X_1, \dots, X_n) = \sum_{j=1}^m g_j(X_1, \dots, X_n) v_j,$$

onde $g_j(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$.

A condição $g(c_1, \dots, c_n) = 0$, implica que $g_j(c_1, \dots, c_n) = 0$ para cada $j = 1, \dots, m$. Como, para cada $i = 1, \dots, n$, o polinômio g se anula para todo $c_i \in K$, com $1 \leq i \leq n$, e K é infinito, concluimos, pelo lema 1.18, que $g_j(X_1, \dots, X_n) = 0$ para cada $j = 1, \dots, m$. Conseqüentemente $g(X_1, \dots, X_n) = 0$.

Agora, do teorema 1.17, temos que $\det(\sigma_j(a_i)) \neq 0$. Assim a matriz $(\sigma_j(a_i))$ possui inversa $(d_{ij}) \in M_n(F)$.

Como $g(X_1, \dots, X_n) = f\left(\sum_{i=1}^n \sigma_1(a_i) X_i, \dots, \sum_{i=1}^n \sigma_n(a_i) X_i\right)$, temos que

$$g\left(\sum_{j,k} d_{1j} \sigma_j(a_k) X_k, \dots, \sum_{j,k} d_{nj} \sigma_j(a_k) X_k\right) = f(X_1, \dots, X_n).$$

Mas como $g(X_1, \dots, X_n) = 0$, temos que $f(X_1, \dots, X_n) = 0$, provando assim a independência algébrica de $\sigma_1, \dots, \sigma_n$ sobre F . ■

O próximo resultado nos mostra que o grupo de Galois de uma extensão finita de corpos finitos é cíclica.

Proposição 1.20 *Sejam K um corpo finito com $q = p^m$ elementos e $L \supseteq K$ uma extensão de grau n . Então, $\text{Gal}(L/K)$ é cíclico gerado pelo K -automorfismo $\sigma : a \mapsto a^q$, para cada $a \in L$.*

Demonstração: Usando que $\text{Car}(K) = p$, é fácil ver que $\sigma : L \rightarrow L$ é um homomorfismo de corpos. Se $\sigma(a) = 0$, para algum $a \in L$, então $a^q = 0$ no corpo L , o que implica que $a = 0$, mostrando assim que σ é injetor. O fato de L ser finito implica que σ é também sobrejetor. Logo σ é um automorfismo de L . Agora, como $|K| = q$, temos que $a^q = a$ para todo $a \in K$, o que mostra que $\sigma \in \text{Gal}(L/K)$.

Mostramos agora que a ordem de σ é n . Como L tem q^n elementos, temos que $a^{q^n} = a$, para todo $a \in L$. Dessa forma, $\sigma^n = 1$. Se $\sigma^r = 1$ para algum $r < n$, temos $a^{q^r} = a$, para cada $a \in L$, o que contradiz o fato de que o polinômio $X^{q^r} - X$ de grau q^r tem no máximo q^r raízes distintas em L . Portanto, a ordem de σ é n . Seja $F = L^{[\sigma]}$. Pelo teorema 1.2 (teorema fundamental da teoria de Galois) temos que $[L : F] = n$ e $\text{Gal}(L/F) = [\sigma]$. Por outro lado, como $\sigma \in \text{Gal}(L/K)$, temos que $K \subseteq F$. Logo $n = [L : K] = [L : F][F : K] = n[F : K]$, o que mostra que $F = K$ e, então, $L \supseteq K$ é galoisiana com $\text{Gal}(L/K) = [\sigma]$, como queríamos. ■

Podemos agora demonstrar o principal resultado deste capítulo que é o teorema da base normal. Tal resultado garante apenas a existência de base normal.

Teorema 1.21 (Teorema da Base Normal) *Toda extensão galoisiana de corpos admite uma base normal.*

Demonstração: Seja $L \supseteq K$ uma extensão galoisiana de corpos. Dividiremos a demonstração em duas partes, uma considerando $L \supseteq K$ uma extensão cíclica, ou seja, $\text{Gal}(L/K)$ um grupo cíclico e a outra considerando K um corpo infinito. Estas duas condições englobam todos os casos pois se K é finito, então L será finito e portanto pela proposição 1.20, $L \supseteq K$ será uma extensão cíclica.

Primeiro assumiremos $L \supseteq K$ cíclica com $Gal(L/K) = [\sigma] = \{id, \sigma, \dots, \sigma^{n-1}\}$, onde $n = [L : K]$.

Observe que L é um K -espaço vetorial de dimensão finita e $\sigma : L \rightarrow L$ é um operador K -linear. Além disso, pelo fato de $|\llbracket \sigma \rrbracket| = [L : K]$, temos que o polinômio minimal de σ sobre K irá coincidir com o seu polinômio característico. Portanto, pelo teorema da decomposição racional (7.2 em [4]), existirá $a \in \dot{L}$, tal que $\{a, \sigma(a), \dots, \sigma^{n-1}(a)\}$ é uma base naturalmente normal de L sobre K .

Faremos agora o caso em que K é um corpo infinito. Pelo teorema 1.19, os K -automorfismos $\sigma_1, \dots, \sigma_n$ de L são algebricamente independentes sobre K . Temos do teorema 1.17 também que se $a \in L$, então $\{\sigma_1(a), \dots, \sigma_n(a)\}$ é base de L sobre K se, e somente se

$$\det(\sigma_i \sigma_j(a)) \neq 0.$$

Como $\sigma_1, \dots, \sigma_n$ são algebricamente independentes sobre L , temos que existe um $a \in L$ tal que $\det(\sigma_i \sigma_j(a)) \neq 0$, pois o determinante é um polinômio em n^2 variáveis. Então $\{\sigma_1(a), \sigma_2(a), \dots, \sigma_n(a)\}$ é uma base normal de L sobre K , como queríamos demonstrar. ■

CAPÍTULO 2

Sobre a existência de bases normais auto-duais

O objetivo deste capítulo é mostrarmos que toda extensão galoisiana, de grau ímpar, de corpos, admite uma base normal auto-dual. Para tanto, neste capítulo, $L \supseteq K$ é uma extensão galoisiana de corpos, $G = \text{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$, $T : L \times L \rightarrow K$ é a forma traço de L sobre K , e $K[G]$ é a K -álgebra de grupo de G .

Seja $\mathcal{B} = \{e_1, e_2, \dots, e_n\}$ uma base de L sobre K . Dizemos que $\mathcal{B} = \{e_1, e_2, \dots, e_n\}$ é uma base *auto-dual* se ela for sua própria base dual com relação a forma bilinear traço, isto é, $T(e_i, e_j) = \delta_{ij}$, para todo $1 \leq i, j \leq n$.

Dizemos que uma base normal $\{\sigma(a); \sigma \in G\}$ de L sobre K é uma base normal *auto-dual* de L sobre K se $T(\sigma_i(a), \sigma_j(a)) = \delta_{ij}$, para todo $1 \leq i, j \leq n$.

Denotamos por $\bar{\cdot} : K[G] \rightarrow K[G]$ a involução K -linear dada por $\bar{\sigma} = \sigma^{-1}$, para todo $\sigma \in G$.

O corpo L é um $K[G]$ -módulo livre de posto 1, com a multiplicação por escalar dada por

$$(c_1\sigma_1 + \dots + c_n\sigma_n).x = c_1\sigma_1(x) + \dots + c_n\sigma_n(x),$$

para todo $x \in L$ e $c_1, \dots, c_n \in K$.

Com relação a estrutura destes módulos, temos

Lema 2.1 *Se $a \in \dot{L}$, então $\mathcal{B} = \{\sigma_1(a), \dots, \sigma_n(a)\}$ é uma base normal de L sobre K se, e somente se $\{a\}$ é uma base de L sobre $K[G]$.*

Demonstração: Dado $x \in L$, existem $c_i \in K$, $i = 1, \dots, n$, tais que

$$x = c_1\sigma_1(a) + \dots + c_n\sigma_n(a) = (c_1\sigma_1 + \dots + c_n\sigma_n).a,$$

onde $c_1\sigma_1 + \dots + c_n\sigma_n \in K[G]$. Portanto, $\{a\}$ gera L sobre $K[G]$.

Além disso, se $(c_1\sigma_1 + \dots + c_n\sigma_n).a = 0$, então $c_1\sigma_1(a) + \dots + c_n\sigma_n(a) = 0$ e como \mathcal{B} é linearmente independente sobre K , temos que $c_1 = \dots = c_n = 0$ o que mostra que $\{a\}$ é linearmente independente sobre $K[G]$.

Por outro lado, se $\{a\}$ é uma base de L sobre $K[G]$, para mostrarmos que \mathcal{B} é uma base de L sobre K , basta mostrarmos que \mathcal{B} gera L , pois o número de elementos de \mathcal{B} é $|G| = [L : K]$, pois $L \supseteq K$ é galoisiana. Dado $x \in L$, temos que existe $\sum_{i=1}^n c_i\sigma_i \in K[G]$ tal que

$$x = (c_1\sigma_1 + \dots + c_n\sigma_n).a = c_1\sigma_1(a) + \dots + c_n\sigma_n(a),$$

o que mostra que \mathcal{B} gera L sobre K . ■

A forma bilinear traço $T : L \times L \rightarrow K$, induz uma aplicação $h_T : L \times L \rightarrow K[G]$ dada por

$$h_T(x, y) = T(\sigma_1(x), y)\bar{\sigma}_1 + \dots + T(\sigma_n(x), y)\bar{\sigma}_n,$$

para todo $x, y \in L$.

A aplicação h_T é uma forma hermitiana não-singular de L sobre o anel $K[G]$. De fato, mostraremos inicialmente que h_T é sesquilinear. Usando que T é bilinear e $\sigma_i \in G$, obtemos facilmente que $h_T(x + y, z) = h_T(x, z) + h_T(y, z)$ e $h_T(x, y + z) = h_T(x, y) + h_T(x, z)$, para todo $x, y, z \in L$.

Mais ainda, para todo $\sigma, \tau \in G$ e $x, y \in L$, temos:

$$h_T(\sigma.x, \tau.y) = h_T(\sigma(x), \tau(y)) = \sum_{i=1}^n T(\sigma_i(\sigma(x)), \tau(y))\bar{\sigma}_i.$$

Mas, do lema 1.14, temos $T(\sigma_i(\sigma(x)), \tau(y)) = T(\tau^{-1}\sigma_i\sigma(x), y)$. Logo,

$$h_T(\sigma.x, \tau.y) = \sum_{i=1}^n T(\tau^{-1}\sigma_i\sigma(x), y)\bar{\sigma}_i = \sum_{i=1}^n T(\psi_i(x), y)\sigma\bar{\psi}_i\bar{\tau} =$$

$$\sigma \left(\sum_{i=1}^n T(\psi_i(x), y) \overline{\psi_i} \right) \overline{\tau} = \sigma h_T(x, y) \overline{\tau},$$

de onde segue que $h_T(a.x, b.y) = ah_T(x, y)\overline{b}$, para todo $a, b \in K[G]$ e $x, y \in L$, mostrando assim que h_T é sesquilinear.

Agora, para todo $x, y \in L$, temos

$$\begin{aligned} \overline{h_T(y, x)} &= \overline{\sum_{i=1}^n T(\sigma_i(y), x) \overline{\sigma_i}} = \sum_{i=1}^n T(\sigma_i(y), x) \sigma_i = \\ &= \sum_{i=1}^n T(y, \sigma_i^{-1}(x)) \sigma_i = \sum_{i=1}^n T(\sigma_i^{-1}(x), y) \sigma_i = \sum_{i=1}^n T(\tau_i(x), y) \overline{\tau_i}, \end{aligned}$$

onde $\tau_i = \sigma_i^{-1}$, para cada i , o que mostra que $\overline{h_T(y, x)} = h_T(x, y)$, ou seja, h_T é uma forma hermitiana de L sobre $K[G]$.

Mostraremos agora que h_T é não-singular. Para tanto, note que do lema 2.1 $L = K[G].a$, onde $\{\sigma_1(a), \dots, \sigma_n(a)\}$ é uma base normal de L sobre K . Assim, para mostrar que h_T é não-singular, basta mostrar que $h_T(a, a) \neq 0$. Para isso, é suficiente mostrar que $T(\sigma(a), a) \neq 0$ para algum $\sigma \in G$. Mas se $T(\sigma(a), a) = 0$, para todo $\sigma \in G$, e a matriz de T em relação a base $\{\sigma_1(a), \dots, \sigma_n(a)\}$ é

$$\begin{aligned} &\begin{bmatrix} T(a, a) & T(a, \sigma_2(a)) & \dots & T(a, \sigma_n(a)) \\ T(\sigma_2(a), a) & T(\sigma_2(a), \sigma_2(a)) & \dots & T(\sigma_2(a), \sigma_n(a)) \\ \vdots & \vdots & \ddots & \vdots \\ T(\sigma_n(a), a) & T(\sigma_n(a), \sigma_2(a)) & \dots & T(\sigma_n(a), \sigma_n(a)) \end{bmatrix} = \\ &\begin{bmatrix} 0 & T(a, \sigma_2(a)) & \dots & T(a, \sigma_n(a)) \\ 0 & T(\sigma_2(a), \sigma_2(a)) & \dots & T(\sigma_2(a), \sigma_n(a)) \\ \vdots & \vdots & \ddots & \vdots \\ 0 & T(\sigma_n(a), \sigma_2(a)) & \dots & T(\sigma_n(a), \sigma_n(a)) \end{bmatrix} \end{aligned}$$

o que implicaria que T seria singular, o que contradiz o teorema 1.15, pois $L \supseteq K$ é separável.

O próximo resultado relaciona bases normais auto-duais de L sobre K , com bases ortonormais de L sobre $K[G]$.

Lema 2.2 *Se $a \in \dot{L}$, então $\mathcal{B} = \{\sigma_1(a), \dots, \sigma_n(a)\}$ é uma base normal auto-dual de L sobre K se, e somente se $\{a\}$ é uma base ortonormal (relativamente a h_T) de L sobre $K[G]$.*

Demonstração: Se \mathcal{B} é uma base normal auto-dual de L sobre K , então $T(\sigma_i(a), \sigma_j(a)) = \delta_{ij}$. Em particular, $T(\sigma(a), a) = 0$, para $\sigma \neq id$ e $T(\sigma(a), a) = 1$ se $\sigma = id$. Assim,

$$h_T(a, a) = T(\sigma_1(a), a)\bar{\sigma}_1 + \dots + T(\sigma_n(a), a)\bar{\sigma}_n = id = 1 \in K[G].$$

Logo, $\{a\}$ é uma base ortonormal de L sobre $K[G]$, com relação a h_T .

Por outro lado, se $h_T(a, a) = id$, então

$$T(\sigma_1(a), a)\bar{\sigma}_1 + \dots + T(\sigma_n(a), a)\bar{\sigma}_n = id,$$

ou seja,

$$(T(\sigma_1(a), a) - 1)\bar{\sigma}_1 + T(\sigma_2(a), a)\bar{\sigma}_2 + \dots + T(\sigma_n(a), a)\bar{\sigma}_n = 0.$$

Como G é uma base de $K[G]$ sobre K , obtemos que $T(\sigma(a), a) = id$ se $\sigma = id$ e $T(\sigma(a), a) = 0$ se $\sigma \neq id$. Agora, do lema 2.2 temos que a base normal $\mathcal{B} = \{\sigma_1(a), \dots, \sigma_n(a)\}$ é auto-dual. ■

Se $a \in \dot{L}$ gera uma base normal de L sobre K , seja $u = h_T(a, a)$. Considerando as formas hermitianas de posto 1, $\langle 1 \rangle$ e $\langle u \rangle \simeq (L, h_T)$ sobre $K[G]$, temos:

Lema 2.3 *A extensão galoisiana $L \supseteq K$ admite uma base normal auto-dual gerada por $a \in \dot{L}$ se, e somente se as formas hermitianas $\langle 1 \rangle$ e $\langle u \rangle$ são isométricas sobre $K[G]$.*

Demonstração: Se $a \in \dot{L}$ é um gerador da base normal auto-dual de L sobre K , então do lema anterior, temos que $h_T(a, a) = 1$. Portanto, a forma hermitiana $\langle u \rangle \simeq \langle 1 \rangle$.

Por outro lado, se $\langle u \rangle \simeq \langle 1 \rangle$, então $u = h_T(a, a) = 1$ e, portanto do item (b) do lema anterior, temos que $\{a\}$ gera uma base normal auto-dual de L sobre K . ■

Lema 2.4 *A álgebra de Galois $L \otimes_K L$ admite uma base normal auto-dual sobre L .*

Demonstração: Pelo teorema 1.13 temos que se $L \supseteq K$ é galoisiana então $L^{|G|} \cong L \otimes_K L$, como K -álgebras. Logo, basta mostrarmos que $L^{|G|}$ admite uma base normal auto-dual sobre L . Para cada $\sigma \in G$, definimos $e_\sigma = (x_\rho)_{\rho \in G} \in L^{|G|}$, onde $x_\rho = 1$, se $\rho = \sigma$, e $x_\rho = 0$, se $\rho \neq \sigma$.

Afirmamos que $\mathcal{B} = \{e_\sigma\}_{\sigma \in G}$ é uma base normal auto-dual de $L^{|G|}$ sobre L . De fato, em $L^{|G|}$ o produto é dado por $e_\rho e_\sigma = \delta_{\rho\sigma} \cdot e_{\rho\sigma}$ e note que $\sum_{\sigma \in G} e_\sigma = (1, \dots, 1)$, ou seja, os elementos de \mathcal{B} são idempotentes ortogonais de $L^{|G|}$, cuja soma é 1 em $L^{|G|}$.

Todo elemento de $L^{|G|}$ pode ser escrito na forma $\sum_{\sigma \in G} c_\sigma e_\sigma$, com $c_\sigma \in L$, e a ação de G em $L^{|G|}$ é dada por

$$\phi. \left(\sum_{\sigma \in G} c_\sigma e_\sigma \right) = \sum_{\sigma \in G} c_\sigma e_{\phi\sigma}$$

para todo $\phi \in G$. Temos que \mathcal{B} é uma base normal de $L^{|G|}$ sobre L , pois

$$\{\sigma(e_\rho)\}_{\sigma \in G} = \{e_{\sigma\rho}\}_{\sigma \in G} = \{e_\sigma\}_{\sigma \in G} = \mathcal{B}.$$

Mostremos agora que essa base é auto-dual. Para todo $\sigma, \tau \in G$, temos

$$T(e_\sigma, e_\tau) = \sum_{\rho \in G} \rho(e_\sigma e_\tau).$$

Usando que $\sum_{\rho \in G} e_\rho = 1$, temos que $\sum_{\rho \in G} \rho(e_\sigma) = 1$. Portanto, $T(e_\sigma, e_\tau) = \delta_{\sigma\tau}$, ou seja, $\{e_\sigma\}_{\sigma \in G}$ é uma base normal auto-dual de $L^{|G|}$ sobre L . ■

Como consequência dos dois últimos lemas, temos

Corolário 2.5 *As formas hermitianas $\langle 1 \rangle$ e $\langle u \rangle$ são isométricas sobre $L[G]$.*

Demonstração: No lema 2.4, mostramos que a álgebra de Galois $L \otimes_K L$ admite uma base normal auto-dual. Portanto, pelo lema 2.3, as formas hermitianas $\langle 1 \rangle$ e $\langle u \rangle$ são isométricas sobre $L[G]$. ■

Para os próximos dois resultados, assumiremos que $G = \text{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}$, $\text{Car}(K) = 2$, $s = \sum_{i=1}^n \sigma_i$, $B = sK[G]$ é a subálgebra de $K[G]$ gerada por s e $A = \frac{K[G]}{B}$ a álgebra quociente.

Observe que $s\sigma = \sigma s$, para cada $\sigma \in G$ e, conseqüentemente, $sx = xs$, para cada $x \in K[G]$. Logo, dado $b = sx \in B$, temos $\bar{b} = \overline{sx} = \overline{xs} = \overline{sx} = s\bar{x} \in B$, pois $\bar{s} = s$. Assim, $\bar{B} = B$ e a involução $-$ de $K[G]$ induz uma involução $-$ em A . Também assumiremos, no que segue, que $L \supseteq K$ é uma extensão de corpos de grau ímpar. Com as considerações acima, temos:

Lema 2.6 *Temos que $K[G] \cong A \times K$, onde A , K e G são como acima.*

Demonstração: Mostraremos inicialmente que s é idempotente. De fato,

$$s^2 = \left(\sum_{i=1}^n \sigma_i \right) \left(\sum_{i=1}^n \sigma_i \right) = \sum_{i=1}^n \sigma_i \sigma_i + \sum_{i=1}^n \sigma_2 \sigma_i + \dots + \sum_{i=1}^n \sigma_n \sigma_i = ns = s,$$

pois n é ímpar e $\text{Car}(K) = 2$. Temos também $(1-s)^2 = (1-s)$ e $s + (1-s) = 1$. Observemos também que $sK[G]$ e $(1-s)K[G]$ possuem intersecção vazia. Mostraremos agora que

$$K[G] \cong sK[G] \times (1-s)K[G] \cong B \times A.$$

Consideremos $\varphi : K[G] \rightarrow sK[G] \times (1-s)K[G]$ definida por $\varphi(x) = (sx, (1-s)x)$, para todo $x \in K[G]$. Usando que s e $(1-s)$ são idempotentes, obtemos facilmente que φ é um homomorfismo de K -álgebras. Mais ainda, φ é bijetora. De fato, se $\varphi(x) = 0$, então $sx = 0$ e $(1-s)x = 0$, logo $(1-s)x = x - sx = x = 0$ e, portanto, φ é injetora. Seja $(sx, (1-s)y) \in sK[G] \times (1-s)K[G]$. Tomando $z = y - sy + sx \in K[G]$, temos que $\varphi(z) = (sx, (1-s)y)$. Logo, φ é sobrejetora, e portanto, um isomorfismo de K -álgebras.

Mostremos agora que $A \cong (1-s)K[G]$, como K -álgebras. Para tanto, consideremos $\varphi : K[G] \rightarrow (1-s)K[G]$, o homomorfismo sobrejetor de K -álgebras obtido pela composição de φ a projeção na segunda coordenada, ou seja $\varphi(x) = (1-s)x$, para todo $x \in K[G]$. Note que $\varphi(x) = 0$ se, e somente se $x = sx$ e, usando que s é idem-

potente, obtemos que o núcleo de φ é B . Conseqüentemente, do primeiro teorema do isomorfismo, obtemos $A = \frac{K[G]}{B} \cong (1-s)K[G]$.

Resta apenas mostrarmos que $sK[G] \cong K$, como K -álgebras. Para isso, mostremos inicialmente que $sK[G] = sK$. De fato, para cada $x = c_1\sigma_1 + \cdots + c_n\sigma_n \in K[G]$, temos

$$\begin{aligned} sx &= s(c_1\sigma_1 + \cdots + c_n\sigma_n) = c_1s\sigma_1 + \cdots + c_ns\sigma_n = c_1s + \cdots + c_ns \\ &= s(c_1 + \cdots + c_n) \in sK, \end{aligned}$$

e, claramente, $sK \subseteq sK[G]$. Portanto, $sK = sK[G]$. Por fim, basta notarmos que $sK \cong K$, pois a aplicação $\psi : sK \rightarrow K$, dada por $sa \mapsto a$, é um isomorfismo de K -álgebras. Portanto, $B = sK[G] = sK \cong K$ e assim, $K[G] \cong A \times K$, como queríamos. ■

Pelo lema 1.5 e pelo próximo lema, obtemos que todos os A -módulos hermitianos são pares.

Lema 2.7 *Existe $a \in Z(A)$ que satisfazendo $a + \bar{a} = 1$.*

Demonstração: Como $|G|$ é ímpar, todo elemento de G distinto da identidade não é conjugado do seu inverso.

Vamos supor inicialmente que a afirmação acima seja verdadeira. Em particular, temos que se $\sigma \in G$ e $\sigma \neq 1$, então $\sigma \neq \sigma^{-1}$ o que é imediato pelo teorema de Lagrange. Logo, existe um subconjunto D de G invariante por conjugação, isto é, $\sigma D \sigma^{-1} = D$, para todo $\sigma \in G$, tal que todo elemento distinto da identidade está em D ou tem seu inverso em D , mas não em ambos, ou seja, $G = \{1\} \dot{\cup} D \dot{\cup} D^{-1}$, onde $D^{-1} = \{\sigma^{-1} \in G; \sigma \in D\}$.

Tomemos $a = 1 + \sum_{\sigma \in D} \sigma$. Então

$$a + \bar{a} = 1 + \sum_{\sigma \in D} \sigma + 1 + \sum_{\sigma \in D} \sigma^{-1} = 1 + \sum_{\sigma \in G} \sigma = 1 + s = 1,$$

em $A = \frac{K[G]}{B}$.

Mostremos agora que $a \in Z(A)$. Para isso, é suficiente mostrar que a comuta com os elementos de G . De fato, para $\gamma \in G$, temos

$$a\gamma = \left(1 + \sum_{\sigma \in D} \sigma\right) \gamma = \gamma + \sum_{\sigma \in D} \sigma\gamma = \gamma + \sum_{\sigma \in D} \gamma\sigma = \gamma \left(1 + \sum_{\sigma \in D} \sigma\right) = \gamma a,$$

onde usamos o fato que para cada $\sigma_k \in D$, existe $\sigma_j \in D$ tal que $\gamma\sigma_k = \sigma_j\gamma$, pois D é invariante por conjugação.

Para terminarmos a demonstração resta apenas mostrarmos que a primeira afirmação é verdadeira.

Vamos supor por absurdo que exista $\gamma \in G$, distinto da identidade, tal que $\sigma\gamma\sigma^{-1} = \gamma^{-1}$ para algum $\sigma \in G$. Seja $\bar{\gamma}$ a classe de conjugação de γ . Se $\varphi \in \bar{\gamma}$, então existe $\beta \in G$ tal que $\beta\gamma\beta^{-1} = \varphi$, logo $\varphi^{-1} = \beta^{-1}\gamma^{-1}\beta$, ou seja, $\varphi^{-1} \in \overline{\gamma^{-1}}$. Como $\overline{\gamma^{-1}} = \bar{\gamma}$, temos que $\varphi^{-1} \in \bar{\gamma}$. Como $|G|$ é ímpar, $\varphi \neq \varphi^{-1}$, para todo $\varphi \neq 1$ em G . Portanto, $\bar{\gamma}$ tem um número par de elementos, o que é um absurdo pois $|G|$ é ímpar e, a ordem de G é divisível pelo número de elementos de suas classes de conjugação. ■

Possuímos agora todas as ferramentas que nos permitirão demonstrar o teorema principal deste capítulo.

Teorema 2.8 *Se $L \supseteq K$ é uma extensão galoisiana de grau ímpar, então L admite uma base normal auto-dual sobre K .*

Demonstração: Se $\text{Car}(K) \neq 2$, da observação 1.6, temos que toda forma hermitiana sobre corpos de característica distinta de 2 é par. Pelo corolário 2.5 e o teorema 1.10 podemos concluir que $\langle 1 \rangle$ e $\langle u \rangle$ são isométricas sobre $K[G]$ e, do lema 2.3 teremos que L possui uma base normal auto-dual sobre K .

Consideremos agora que $\text{Car}(K) = 2$. Sejam $s = \sum_{\sigma \in G} \sigma$, $B = sK[G]$ e $A = \frac{K[G]}{B}$. Vimos no lema 2.6 que $K[G] \cong A \times K$. Do lema 2.5, existe $y = (y_A, y_K) \in L[G] \cong A_L \times L$ tal que $y\bar{y} = u$ em $K[G]$, com $u = (v, z) \in A \times K$. Logo, $(y_A, y_K)(\overline{y_A}, \overline{y_K}) = (v, z)$, ou seja, $y_A\overline{y_A} = v$ e $y_K\overline{y_K} = z$. Como a involução em K é a identidade, temos que

$y_K^2 = z \in K$, o que implica que $y_K \in K$. De fato, y_K é raiz do polinômio $X^2 - z \in K[X]$ e, portanto, $[K(y_K) : K] = 1$ ou 2 . Como $[K(y_K) : K]$ divide $[L : K]$ que é ímpar, temos $[K(y_K) : K] = 1$, isto é, $y_K \in K$. Pelos lemas 2.7 e 1.5, temos que toda forma hermitiana sobre A é par.

Como $y_A \overline{y_A} = v$, temos que $\langle 1 \rangle$ e $\langle v \rangle$ são isométricos sobre A_L . Do teorema 1.10, temos que $\langle 1 \rangle$ e $\langle v \rangle$ são isométricos sobre A , isto é, existe $x_A \in A$ tal que $x_A \overline{x_A} = v$. Consideremos $x = (x_A, y_K) \in A \times K \cong K[G]$. Então, $x\overline{x} = (x_A \overline{x_A}, y_K \overline{y_K}) = (v, z) = u$ em $K[G]$. Portanto, $\langle 1 \rangle$ e $\langle u \rangle$ são isométricas sobre $K[G]$ e do lema 2.3, temos que $L \supseteq K$ admite uma base normal auto-dual. ■

Finalizamos este capítulo com um exemplo:

Exemplo 2.9 Sejam $K = \mathbb{Q}$ e $f(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$. Então $L = \mathbb{Q}(a)$ com $a = X + (f(X))$ é uma extensão galoisiana de grau 3 e $Gal(L/K) = [\sigma]$, onde σ é o K -automorfismo de L é dado por $\sigma(a) = a^2 - 2$.

Seja $\alpha = -1 + \frac{a}{3} + \frac{a^2}{3} \in L$. Afirmamos que $\mathcal{B} = \{\alpha, \sigma(\alpha), \sigma^2(\alpha)\}$ é uma base normal auto-dual de L sobre K .

De fato, em L temos

$$\sigma(\alpha) = \left(\frac{a^2}{3} + \frac{a}{3} - 1 \right)^2 - 2 = \frac{a^4}{9} + \frac{2a^3}{9} - \frac{5a^2}{9} - \frac{2a}{3} - 1 = -\frac{2a^2}{9} - \frac{a}{9} - \frac{11}{9}, \text{ e}$$

$$\sigma^2(\alpha) = \left(\frac{a^2}{3} + \frac{a}{3} - 1 \right)^4 - 4 \left(\frac{a^2}{3} + \frac{a}{3} - 1 \right)^2 + 2 = \frac{19a^2}{9} + \frac{10a}{27} - \frac{5}{9}.$$

Como $[L : K] = 3$, basta mostrarmos que \mathcal{B} é linearmente independente para ser uma base de L sobre K .

Se $c_1\alpha + c_2\sigma(\alpha) + c_3\sigma^3(\alpha) = 0$, com $c_i \in K$, temos

$$c_1 \left(\frac{a^2}{3} + \frac{a}{3} - 1 \right) + c_2 \left(-\frac{2a^2}{9} - \frac{a}{9} - \frac{11}{9} \right) + c_3 \left(\frac{19a^2}{9} + \frac{10a}{27} - \frac{5}{9} \right) = 0$$

Usando que $\{1, a, a^2\}$ é uma base de L sobre K , obtemos que c_1, c_2 e c_3 satisfazem

o seguinte sistema linear homogêneo:

$$\begin{aligned} 3c_1 - 2c_2 + 19c_3 &= 0 \\ 9c_1 - 3c_2 + 10c_3 &= 0 \\ -9c_1 - 11c_2 - 5c_3 &= 0 \end{aligned}$$

cuja única solução é a trivial. Com isso, temos que \mathcal{B} é uma base normal de $\mathbb{Q}(a)$ sobre \mathbb{Q} .

Mostremos que \mathcal{B} é auto-dual. Lembremos que, neste caso, a forma traço de $\mathbb{Q}(a)$ sobre \mathbb{Q} é dada por $T(x, y) = xy + \sigma(xy) + \sigma^2(xy)$, para todo $x, y \in \mathbb{Q}(a)$. Com simples cálculos mostra-se que $T(\alpha, \alpha) = T(\sigma(\alpha), \sigma(\alpha)) = T(\sigma^2(\alpha), \sigma^2(\alpha)) = \alpha^2 + \sigma(\alpha^2) + \sigma^2(\alpha^2)$; $T(\alpha, \sigma(\alpha)) = T(\alpha, \sigma^2(\alpha)) = T(\sigma(\alpha), \sigma^2(\alpha)) = \alpha\sigma(\alpha) + \alpha\sigma^2(\alpha) + \sigma(\alpha)\sigma^2(\alpha)$.

Agora,

$$\alpha^2 = \frac{x^4}{9} + \frac{2x^3}{9} - \frac{5x^2}{9} - \frac{2x}{3} + 1,$$

$$(\sigma(\alpha))^2 = \sigma(\alpha^2) = \frac{4x^4}{81} + \frac{4x^3}{81} + \frac{45x^2}{81} + \frac{22x}{81} + \frac{121}{81},$$

$$(\sigma^2(\alpha))^2 = \sigma^2(\alpha^2) = \frac{361x^4}{81} + \frac{380x^3}{243} - \frac{1610x^2}{729} - \frac{100x}{243} + \frac{25}{81}.$$

e, conseqüentemente,

$$\begin{aligned} \alpha^2 + \sigma(\alpha^2) + \sigma^2(\alpha^2) &= \frac{374X^4}{81} + \frac{227X^3}{81} - \frac{374X^2}{27} - \frac{307X}{81} + \frac{308}{81} \\ &= \frac{374X^4}{81} + \frac{227X^3}{81} - \frac{374X^2}{27} - \frac{307X}{81} + \frac{227}{81} + \frac{81}{81} \\ &= \left(X^3 - 3X + 1 \right) \left(\frac{374X}{81} + \frac{227}{81} \right) + 1 \\ &= 1. \end{aligned}$$

Mais ainda,

$$\begin{aligned} \alpha\sigma(\alpha) + \alpha\sigma^2(\alpha) + \sigma(\alpha)\sigma^2(\alpha) &= \frac{13X^4}{81} - \frac{19X^3}{81} - \frac{780X^2}{243} - \frac{302X}{243} + \frac{199}{81} \\ &= (\alpha^3 - 3X + 1) \left(\frac{13X}{81} + \frac{199}{81} \right) = 0, \end{aligned}$$

o que mostra que \mathcal{B} é uma base normal auto-dual de $\mathbb{Q}(a)$ sobre \mathbb{Q} .

CAPÍTULO 3

Sobre a não existência de bases normais auto-duais

O principal resultado do capítulo 2 diz que toda extensão galoisiana de corpos de grau ímpar admite uma base normal auto-dual. A questão natural que surge é: As extensões galoisianas de corpos de grau par não admitem bases normais auto-duais? Neste capítulo, responderemos em parte esta pergunta, mostrando que em alguns tipos de extensões galoisianas de corpos de grau par não admitem bases normais ortogonais e conseqüentemente normais auto-duais.

O principal resultado deste capítulo é o teorema abaixo, que foi demonstrado por D. S. Kang em [6], a qual seguimos juntamente com [7], para fazermos o estudo que apresentaremos a seguir.

Teorema 3.1 *Seja G um grupo finito de ordem par.*

- (a) *Se G tem um subgrupo de índice 2, então $L \supseteq K$ não admite base normal ortogonal para qualquer extensão de corpos $L \supseteq K$ com grupo de Galois G .*
- (b) *Se um 2-subgrupo de Sylow de G é abeliano, então $L \supseteq K$ não admite uma base normal ortogonal para alguma extensão de corpos $L \supseteq K$ com grupo de Galois G .*

O restante do capítulo é dedicado a apresentação da demonstração deste teorema. Para tanto, apresentaremos algumas noções e resultados auxiliares. No que segue, os

corpos considerados serão de característica distinta de 2.

Sejam $L \supseteq K$ uma extensão galoisiana de corpos com grupo de Galois $G = \text{Gal}(L/K)$ e $T : L \times L \rightarrow K$ a forma bilinear traço de L sobre K . Associada a esta forma bilinear, temos a forma quadrática, que também chamaremos de *forma traço de L sobre K* , dada por $q_{L/K}(x) = T(x, x) = \text{Tr}_{L/K}(x^2)$, para todo $x \in L$.

Para $a \in L$, $a \neq 0$, a forma quadrática $q_{L/K}^a$, definida por $q_{L/K}^a(x) = \text{Tr}_{L/K}(ax^2)$, para todo $x \in L$, é dita ser a *forma traço escalar* de L sobre K . Note que $q_{L/K}^1 = q_{L/K}$.

O próximo lema determina a forma traço de uma extensão quadrática.

Lema 3.2 *Seja $L = K(\sqrt{b}) \supseteq K$, para algum $b \in K$, uma extensão quadrática de corpos. Então $q_{L/K} = \langle 2, 2b \rangle$.*

Demonstração: Neste caso, temos que $|G| = |\text{Gal}(L/K)| = 2$ e, portanto, $G = \{1, \sigma\}$, onde $\sigma(\sqrt{b}) = -\sqrt{b}$. Vamos mostrar que, em relação a base $\{1, \sqrt{b}\}$ de L sobre K , a forma quadrática $q_{L/K}$ tem a diagonalização $\langle 2, 2b \rangle$. De fato,

$$\begin{aligned} q_{L/K}(1) &= T(1, 1) = 1 + \sigma(1) = 2; \\ T(1, \sqrt{b}) &= T(\sqrt{b}, 1) = \sqrt{b} + \sigma(\sqrt{b}) = 0; \\ q_{L/K}(\sqrt{b}) &= T(\sqrt{b}, \sqrt{b}) = b + \rho(\sqrt{b}.\sqrt{b}) = 2b, \end{aligned}$$

o que mostra que $q_{L/K} = \langle 2, 2b \rangle$. ■

Vejamos agora, como é o comportamento da forma traço com relação à uma cadeia de corpos.

Lema 3.3 *Sejam $L \supseteq F \supseteq K$ extensões de corpos. Se $q_{L/F} = \langle a_1, a_2, \dots, a_n \rangle$, então*

(a) $q_{L/K} = q_{F/K}^{a_1} \perp q_{F/K}^{a_2} \perp \dots \perp q_{F/K}^{a_n}$;

(b) *Se $a_i \in K$, para todo $i = 1, \dots, n$, então $q_{L/K} = \langle a_1, a_2, \dots, a_n \rangle \otimes q_{F/K}$.*

Demonstração: (a) Seja $\{v_1, \dots, v_n\}$ uma base de L sobre F tal que a decomposição de $q_{L/F}$, com relação a esta base, é $q_{L/F} = \langle a_1, a_2, \dots, a_n \rangle$, com $a_1, \dots, a_n \in \dot{F}$. Então,

$L = Fv_1 \oplus Fv_2 \oplus \cdots \oplus Fv_n$ como espaço vetorial sobre K . Mais ainda, esta soma é ortogonal com respeito a $q_{L/K}$, pois se $i \neq j$ e $c_i, c_j \in F$, então $T(c_i v_i, c_j v_j) = Tr_{L/K}(c_i c_j v_i v_j) = Tr_{F/K} \circ Tr_{L/F}(c_i c_j v_i v_j)$ do teorema 1.16. Como $T_{L/F}$ é F -linear, temos $T(c_i v_i, c_j v_j) = Tr_{F/K}(c_i c_j T_{L/F}(v_i v_j)) = 0$, pois v_i e v_j são vetores de uma base ortogonal de L sobre F .

Agora, mostraremos que a restrição da forma traço $q_{L/K}$ a cada subespaço Fv_i é da forma, $q_{F/K}^{a_i}$, o que finaliza a demonstração do item (a).

Para cada $i = 1, \dots, n$, se $c \in F$, novamente usando o teorema 1.16, temos

$$\begin{aligned} q_{L/K}(cv_i) &= Tr_{L/K}(c^2 v_i^2) = Tr_{L/K}(c^2) Tr_{L/K}(v_i^2) = \\ &= (Tr_{F/K} \circ Tr_{L/F}(c^2))(Tr_{F/K} \circ Tr_{L/F}(v_i^2)) = \\ &= Tr_{F/K}(c^2) Tr_{F/K}(a_i) = Tr_{F/K}(a_i c^2) = q_{F/K}^{a_i}(c), \end{aligned}$$

como queríamos.

(b) Se $a_i \in K$, para todo $i = 1, \dots, n$, então, para cada $a \in F$, temos

$$q_{F/K}^{a_i}(a) = Tr_{F/K}(a_i a^2) = a_i Tr_{F/K}(a^2) = \langle a_i \rangle \otimes q_{F/K}(1 \otimes a).$$

Assim, do item anterior, obtemos que

$$\begin{aligned} q_{L/K} &= q_{F/K}^{a_1} \perp q_{F/K}^{a_2} \perp \cdots \perp q_{F/K}^{a_n} \\ &= (\langle a_1 \rangle \otimes q_{F/K}) \perp (\langle a_2 \rangle \otimes q_{F/K}) \perp \cdots \perp (\langle a_n \rangle \otimes q_{F/K}) \\ &= \langle a_1, a_2, \dots, a_n \rangle \otimes q_{F/K}, \end{aligned}$$

como queríamos. ■

Seja K um corpo contendo uma raiz n -ésima primitiva da unidade, para um inteiro positivo par n . Seja $L = K(\sqrt[n]{a})$, com $a \in \dot{K}$, uma extensão cíclica de K de grau n , ou seja, cujo grupo de Galois $Gal(L/K)$ é cíclico. Neste caso, temos que $Gal(L/K) = [\sigma]$, onde σ é o K -automorfismo de L que leva $x = \sqrt[n]{a}$ em ωx , com $\omega \in K$ uma raiz n -ésima

primitiva da unidade. Mais ainda, para cada $i = 1, \dots, n$, $\sigma^i(x) = \omega^i x$. Com estas considerações, apresentamos a classe de $q_{L/K}$ no anel de Witt dos espaços bilineares sobre K , $W(K)$.

Lema 3.4 *Para $L \supseteq K$ como acima, temos que $q_{L/K} = \langle n, na \rangle$ em $W(K)$.*

Demonstração: Considere a base de L sobre K , $\{1, x, x^2, \dots, x^{n-1}\}$, onde $x = \sqrt[n]{a}$. Como n é par, podemos considerar o subespaço de L gerado por $\{1, x^{n/2}\}$.

Afirmamos que a forma traço $q_{L/K}$ restrita a este subespaço é $\langle n, na \rangle$.

$$\begin{aligned} \text{De fato, } q_{L/K}(1) &= \text{Tr}_{L/K}(1^2) = \sum_{i=1}^n \sigma^i(1) = |G| = n, \quad q_{L/K}(x^{n/2}) = \text{Tr}_{L/K}(x^n) = \\ \text{Tr}_{L/K}(a) &= \sum_{i=1}^n \sigma^i(a) = \sum_{i=1}^n a \sigma^i(1) = a|G| = na, \quad \text{e } T(1, x^{n/2}) = \text{Tr}_{L/K}(x^{n/2}) = \\ &= \sum_{i=1}^n \sigma^i(x^{n/2}). \end{aligned}$$

Como $\sigma(x) = \omega x$, temos que $\sigma(x^{n/2}) = \omega^{n/2} x^{n/2}$. Mas ω é raiz n -ésima primitiva da unidade e n é par, então $\omega^{n/2} = -1$, pois $(\omega^{n/2} - 1)(\omega^{n/2} + 1) = \omega^n - 1 = 0$ e $\omega^{n/2} \neq 1$. Assim, $\sigma(x^{n/2}) = -x^{n/2}$ o que implica que $\sigma^i(x^{n/2}) = (-1)^i x^{n/2}$, para cada $i = 1, \dots, n$. Logo $T(1, x^{n/2}) = \sum_{i=1}^n \sigma^i(x^{n/2}) = \sum_{i=1}^n (-1)^i x^{n/2} = 0$, pois n é par, o que mostra a afirmação.

Agora, vamos mostrar que para $i = 1, \dots, \frac{n}{2} - 1$, a forma traço $q_{L/K}$ restrita ao subespaço $Kx^i \oplus Kx^{n-i}$ é hiperbólica. Como $q_{L/K}(x^i) = \text{Tr}_{L/K}(x^{2i}) = \sum_{j=1}^n \sigma^j(x^{2i})$ e, $\sigma(x^{2i}) = \omega^{2i} x^{2i}$, temos que $\sigma^j(x^{2i}) = \omega^{2ij} x^{2i}$, de onde segue que

$$q_{L/K}(x^i) = x^{2i}(\omega^{2i} + (\omega^{2i})^2 + \dots + (\omega^{2i})^{n-1} + (\omega^{2i})^n) = x^{2i}(1 + \omega^{2i} + (\omega^{2i})^2 + \dots + (\omega^{2i})^{n-1}).$$

Mas, $2i < n$, para cada $i = 1, \dots, \frac{n}{2} - 1$, o que implica que $\omega^{2i} \neq 1$ e, como ω^{2i} é raiz do polinômio $f(X) = X^{n-1} + X^{n-2} + \dots + 1$, obtemos que $q_{L/K}(x^i) = 0$, ou seja, x^i é um vetor isotrópico e, como $T(x^i, x^{n-i}) = \text{Tr}_{L/K}(x^n) = \text{Tr}_{L/K}(a) = na$, temos que $q_{L/K}$ restrito ao subespaço $Kx^i \oplus Kx^{n-i}$ é uma forma quadrática não-singular isotrópica. Conseqüentemente, do teorema 4.5 de [11], temos que esta restrição é isométrica ao plano hiperbólico $\langle 1, -1 \rangle$.

Assim, $q_{L/K} \simeq \langle n, na \rangle \perp \left(\frac{n-2}{2} \right) \langle 1, -1 \rangle$, o que mostra o lema. ■

Lema 3.5 *Seja $L \supseteq K$ uma extensão galoisiana de corpos, com $q_{L/K} = \langle a, a \rangle$ para algum $a \in \dot{K}$. Então $q_{L/K}$ é hiperbólica se, e somente se K contém uma raiz quarta da unidade.*

Demonstração: Desde que uma forma quadrática de dimensão 2 é hiperbólica se, e somente se o seu determinante é menos um quadrado, temos que $q_{L/K} = \langle a, a \rangle$ é hiperbólica se, e somente se $a^2 = \det(q_{L/K}) = -1$ em \dot{K}/\dot{K}^2 . Mas $a^2 = -1$ em \dot{K}/\dot{K}^2 se, e somente se K contém uma raiz quarta primitiva da unidade, o que mostra o lema. ■

Nosso próximo objetivo é relacionarmos a existência de base normal ortogonal com o fato da forma traço $q_{L/K}$ ser hiperbólica. Para isso, se $L \supseteq K$ é uma extensão galoisiana de corpos com grupo de Galois G , dizemos que uma base normal $\{\sigma(a); \sigma \in G\}$ de L sobre K é uma *base normal ortogonal* se ela for ortogonal em relação a forma traço, ou seja,

$$T(\sigma_i(a), \sigma_j(a)) = Tr_{L/K}(\sigma_i(a)\sigma_j(a)) = 0,$$

para todo $\sigma_i \neq \sigma_j$ em G .

Teorema 3.6 *Sejam K um corpo contendo uma raiz quarta primitiva da unidade, $L \supseteq K$ uma extensão galoisiana com $G = Gal(L/K)$ de ordem par. Se $L \supseteq K$ admite uma base normal ortogonal, então $q_{L/K}$ é hiperbólica.*

Demonstração: Sejam $\mathcal{B} = \{\sigma_1(a), \sigma_2(a), \dots, \sigma_n(a)\}$ uma base normal ortogonal de L sobre K , onde $a \in \dot{L}$ e $n = [L : K]$ é par. Como a forma traço é uma aplicação G -invariante, isto é, $T(x, y) = T(\sigma(x), \sigma(y))$, para todo $x, y \in L$ e $\sigma \in G$, temos que existe $c = Tr_{L/K}(a^2) \in \dot{K}$ tal que

$$T(\sigma(a), \sigma(a)) = Tr_{L/K}(\sigma(a)\sigma(a)) = Tr_{L/K}(\sigma(a^2)) = Tr_{L/K}(a^2) = c,$$

para cada $\sigma \in G$.

Assim, a decomposição de $q_{L/K}$ com relação a base \mathcal{B} é $q_{L/K} = \langle c, c, \dots, c \rangle = \langle c, c \rangle \perp \langle c, c \rangle \perp \dots \perp \langle c, c \rangle = \frac{n}{2} \langle c, c \rangle$.

Como K contém uma raiz quarta primitiva da unidade, teremos pelo lema anterior que a forma $\langle c, c \rangle$ é hiperbólica e, conseqüentemente, $q_{L/K}$ é hiperbólica. ■

Como conseqüência imediata temos

Corolário 3.7 *Seja $L \supseteq K$ uma extensão galoisiana de corpos. Se L sobre K admitir uma base normal ortogonal, então $\det(q_{L/K})$ é um quadrado em \dot{K} .*

Demonstração: Como a forma traço é uma aplicação G -invariante, como na demonstração do teorema acima, temos que existe $c \in \dot{K}$ tal que $q_{L/K} = \langle c, c, \dots, c \rangle$ e $\det(q_{L/K}) = c^n$. Se $n = [L : K]$ é par, então $\det(q_{L/K})$ é um quadrado em K . Se n é ímpar, então do teorema 2.8, temos que $L \supseteq K$ admite uma base normal auto-dual. Neste caso, $c = \text{Tr}_{L/K}(a^2) = q_{L/K}(a) = 1$ e, portanto, $\det(q_{L/K}) = 1$, que é um quadrado em K . ■

O próximo resultado nos mostra a não existência de base normal auto-dual para extensões galoisianas de corpos de grau 2.

Lema 3.8 *Seja $L \supseteq K$ uma extensão galoisiana de grau 2. Então L não admite base normal ortogonal sobre K .*

Demonstração: Suponhamos que $L \supseteq K$ admite uma base normal ortogonal. Como $L \supseteq K$ é uma extensão quadrática e galoisiana, do lema 3.2 temos que, $q_{L/K} = \langle 2, 2b \rangle$, onde $b \in \dot{K}$, não é um quadrado e $L = K(\sqrt{b})$. Assim, $\det(q_{L/K}) = 4b$ que não é um quadrado em K , o que contradiz o corolário 3.7. ■

Nos próximos três resultados, estaremos apresentando as relações entre a existência de bases normais ortogonais e/ou auto-duais, de extensões galoisianas de corpos $L \supseteq K$,

com a existência de tais bases para extensões $F \supseteq K$, onde F é um corpo intermediário. Recordemos que se H é um subgrupo normal de $Gal(L/K)$, então L^H denota o subcorpo de L fixado por H , ou seja $L^H = \{x \in L; \sigma(x) = x, \text{ para todo } \sigma \in H\}$.

Lema 3.9 *Seja $L \supseteq K$ uma extensão galoisiana de corpos com grupo de Galois G . Para H subgrupo normal de G tal que, $Car(K)$ não divide $[G : H]$, $F = L^H$ e $y \in F$, temos:*

(a) *Existe $y' \in L$, tal que $y = \sum_{\phi \in H} \phi(y')$.*

(b) *Para $y' \in L$, como no item anterior, temos que $T'(x, y) = T(x, y')$ onde $T'(x, y) = Tr_{F/K}(xy)$ e $T(x, y') = Tr_{L/K}(xy')$, para todo $x \in F$.*

Demonstração: Se $y \in F$, basta considerarmos $y' = \frac{y}{m}$, onde $m = [G : H]$. De fato,

$$\begin{aligned} & \phi_1(y') + \phi_2(y') + \dots + \phi_m(y') = \\ & \phi_1\left(\frac{y}{m}\right) + \phi_2\left(\frac{y}{m}\right) + \dots + \phi_m\left(\frac{y}{m}\right) = \\ & \frac{y}{m} + \dots + \frac{y}{m} = y, \end{aligned}$$

mostrando assim o item (a).

Para mostrarmos (b) consideremos $G = Gal(L/K) = \{\sigma_1, \dots, \sigma_n\}$, e $G/H \cong \{\rho_1, \dots, \rho_m\} \cong Gal(F/K)$ o grupo quociente. Assim para todo $x, y \in F$, temos que

$$\begin{aligned} T'(x, y) &= Tr_{F/K}(xy) = Tr_{F/K}\left(x \sum_{\phi \in H} \phi(y')\right) = \\ & \sum_{\rho \in G/H} \rho(x) \rho\left(\sum_{\phi \in H} \phi(y')\right) = \sum_{\rho \in G/H} \sum_{\phi \in H} (\rho\phi)(x)(\rho\phi)(y') = \\ & \sum_{\sigma \in G} \sigma(x)\sigma(y') = Tr_{L/K}(xy') = T(x, y'). \quad \blacksquare \end{aligned}$$

Lema 3.10 *Se $L \supseteq K$ é uma extensão galoisiana que possui uma base normal auto-dual sobre K e H é um subgrupo normal de $G = Gal(L/K)$, tal que, $Car(K)$ não divide $[G : H]$, então:*

- (a) A forma traço $q_{F/K}$, de $F = L^H$ sobre K é isométrica a forma $\langle 1, 1, \dots, 1 \rangle$, $[F : K]$ -vezes.
- (b) A extensão galoisiana $L^H = F \supseteq K$ admite uma base normal auto-dual.

Demonstração: Sejam $a \in L$ um gerador da base normal de L sobre K e $G/H \cong \{\rho_1, \dots, \rho_m\}$ o grupo quociente. Para cada $\rho \in G/H$, definimos

$$a_\rho = \sum_{\phi \in H} \phi \rho(a). \quad (\star)$$

Agora o resultado do item (a) segue imediatamente do fato que a família $(a_\rho)_{\rho \in G/H}$ é uma base auto-dual de F sobre K com relação a forma traço T' de F sobre K , pois, para cada $\rho, \rho' \in G/H$, usando o lema anterior, obtemos que

$$T'(a_\rho, a_{\rho'}) = T(a_\rho, \rho'(a)) \stackrel{(\star)}{=} \sum_{\phi \in H} T(\phi \rho(a), \rho'(a)) = \sum_{\phi \in H} \delta_{\phi \rho, \rho'} = \delta_{\rho, \rho'}.$$

Finalmente, o resultado do item (b) segue do fato que o elemento $a_1 = \sum_{\phi \in H} \phi(a)$ é um gerador de uma base normal auto-dual de F sobre K , ou seja, $\{\rho(a_1); \rho \in G/H\}$ é uma base auto-dual de F sobre K .

Do fato de H ser normal em G , temos que para cada $\rho \in G/H$, $\rho(a_1) = \sum_{\phi \in H} \rho \phi(a) = \sum_{\phi \in H} \phi \rho'(a)$, para algum $\rho' \in G/H$. De (\star) , temos que $\rho(a_1) = a_{\rho'}$, mostrando assim que $\{\rho(a_1); \rho \in G/H\} = (a_\rho)_{\rho \in G/H}$. Agora o resultado segue da demonstração do item (a). ■

Demonstração do Teorema 3.1, item (a)

Queremos mostrar que se G é um grupo finito de ordem par que possui um subgrupo H de índice 2, então $L \supseteq K$ não admite base normal ortogonal para qualquer extensão de corpos $L \supseteq K$ com grupo de Galois G . Faremos o caso mais geral, substituindo base normal ortogonal, por base normal auto-dual.

Suponhamos que existe uma extensão galoisiana de corpos $L \supseteq K$ com $G = \text{Gal}(L/K)$ tal que L admite uma base normal auto-dual sobre K . Desde que H é em subgrupo de G de índice 2, temos que H é um subgrupo normal de G e, conseqüentemente $H = \text{Gal}(L^H/K)$, ou seja, $L^H \supseteq K$ é uma extensão galoisiana de grau 2.

Temos então as extensões galoisianas de corpos $L \supseteq L^H \supseteq K$ com $L \supseteq K$ admitindo uma base normal auto-dual. Desde que $\text{Car}(K) \neq 2$, temos que esta não divide $[G : H]$, do lema 3.10 temos que $L^H \supseteq K$ admite uma base normal auto-dual, o que contradiz o lema 3.8, pois $[L^H : K] = 2$, mostrando assim o item (a).

Demonstração do Teorema 3.1, item (b)

No que segue, nos dedicaremos a demonstração do item (b) do teorema 3.1, ou seja, mostrar que se G é um grupo de ordem par e seu 2 subgrupo de Sylow é abeliano, então existe uma extensão galoisiana de corpos $L \supseteq K$ com grupo de Galois G tal que L não admite uma base normal ortogonal sobre K .

Dizemos que G é um 2-grupo se sua ordem for uma potência de 2. O *expoente* de um grupo finito G é o menor inteiro positivo n tal que $\sigma^n = 1$, para todo $\sigma \in G$. Observe que o expoente de um 2-grupo é obrigatoriamente uma potência de 2.

Vamos mostrar agora que nenhuma extensão de corpos $L \supseteq K$ com grupo de Galois G , sendo G um 2-grupo abeliano e com expoente d , e K contendo uma d -ésima raiz primitiva da unidade, possui a forma traço $q_{L/K}$ hiperbólica.

De fato, seja G um 2-grupo abeliano. Da decomposição dos grupos abelianos finitos, temos que $G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ onde $n_{i+1} | n_i$, para cada $i = 1, \dots, r-1$ e $|G| = n_1 n_2 \cdots n_r$. Observe que cada n_i é uma potência de 2. Consideremos o caso $r = 2$. Para obtermos o caso geral, basta aplicarmos o processo de indução finita sobre r .

Sejam K_1 um corpo contendo as raízes n_i -ésimas primitivas da unidade, para $i =$

1, 2, $K = K_1(a_1, a_2)$ e $L = K_1(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2})$, onde a_1 e a_2 são variáveis algebricamente independentes sobre K_1 .

Para $F = K(\sqrt[n_1]{a_1})$, temos $K \subseteq F \subseteq L$. Do lema 3.4 temos que $q_{F/K} = \langle n_1, n_1 a_1 \rangle$ e $q_{L/F} = \langle n_2, n_2 a_2 \rangle$. Mais ainda, do teorema 1.16, temos que $q_{L/K} = \langle n_1, n_1 a_1 \rangle \otimes \langle n_2, n_2 a_2 \rangle = \langle n_1 n_2 \rangle \otimes (\langle 1, a_1 \rangle \otimes \langle 1, a_2 \rangle) = \langle |G| \rangle \otimes (\langle 1, a_1 \rangle \otimes \langle 1, a_2 \rangle)$. Esta forma é anisotrópica e conseqüentemente não-hiperbólica sobre $K_1(a_1, a_2)$.

Mostraremos que de fato $q_{L/K}$ é anisotrópica. Note que

$$\langle 1, a_1 \rangle \otimes \langle 1, a_2 \rangle = (\langle 1 \rangle \otimes \langle 1, a_1 \rangle) \perp (\langle a_2 \rangle \otimes \langle 1, a_1 \rangle) = \langle 1, a_1 \rangle \otimes \langle a_2 \rangle \langle 1, a_1 \rangle.$$

Se $q_{L/K}$ for isotrópica, existirá $x \in \dot{L}$, tal que $q_{L/K}(x) = 0$. Assim, $\langle 1, a_1 \rangle(x) \perp \langle a_2 \rangle \langle 1, a_1 \rangle(x) = 0$ e, conseqüentemente, $\langle 1, a_1 \rangle(x) = -\langle a_2 \rangle \langle 1, a_1 \rangle(x)$.

Note que do lado esquerdo da última igualdade temos um polinômio $p(a_2)$ com grau digamos m . Do lado direito da igualdade temos um outro polinômio $q(a_2)$ com grau $m + 1$, o que leva a uma contradição. Usando isso e um processo indutivo, obtemos

Lema 3.11 *Sejam $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ um 2-grupo abeliano, $K = K_1(a_1, \dots, a_r)$ e $L = K_1(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r})$ onde K_1 é um corpo contendo as n_i -ésimas raízes primitivas da unidade, com $i = 1, 2, \dots, r$, e a_1, a_2, \dots, a_n são variáveis algebricamente independentes sobre K_1 . Então $q_{L/K}$ não é hiperbólica sobre K .*

Sejam H um 2-subgrupo de Sylow de G abeliano, $m = [G : H]$ e $|G| = 2^r m$, para algum $r \in \mathbb{N}$.

Lema 3.12 *Existe uma única forma quadrática q' , de dimensão 2^r , tal que $q_{L/K} \simeq \langle m \rangle \otimes q'$, isto é, $q_{L/K}$ é isométrica à soma direta ortogonal de m cópias de q' . Esta forma é única a menos de isometria.*

Demonstração: A existência segue do resultado 6.1 em [3]. Mostraremos a unicidade. Se $q_{L/K} \simeq \langle m \rangle \otimes q''$, então $\langle m \rangle \otimes (q' - q'') = 0$ em $W(K)$, o que implica que $q' \simeq q''$, pois $W(K)$ não possui divisores de zero de dimensão ímpar, ver corolário 2.6.5 em [11]. ■

Iremos utilizar o seguinte resultado sobre o comportamento de formas quadráticas sobre extensões transcendentais.

Lema 3.13 *Sejam F um corpo e q uma forma quadrática sobre F . Se q é anisotrópica sobre F , então q também será anisotrópica sobre $F(X)$, o corpo de frações do anel de polinômios em uma variável X , sobre F .*

Demonstração: Como $\text{Car}(F) \neq 2$, temos que q é da forma $\langle a_1, a_2, \dots, a_n \rangle$, com $a_i \in F$, para todo $i = 1, 2, \dots, n$. Se q é isotrópica sobre $F(X)$, então, multiplicando por um polinômio conveniente, se necessário, temos que existem polinômios $f_i(X) \in F(X)$, não todos nulos, tais que $\sum_{i=1}^n a_i f_i(X)^2 = 0$. Mais ainda, podemos assumir, sem perda de generalidade, que X não divide todos os polinômios $f_i(X)$. Em particular, tomando $X = 0$, obtemos $\sum_{i=1}^n a_i f_i(0)^2 = 0$, onde $f_i(0) \in F$ são não todos nulos. Portanto, q é isotrópica sobre F , o que contradiz a hipótese. ■

Para atingirmos o nosso objetivo final, iremos relacionar formas quadráticas hiperbólicas com representações lineares fiéis de um grupo finito G .

Uma *representação de um grupo* G em um espaço vetorial V sobre um corpo K é um homomorfismo de grupos $\Phi : G \rightarrow GL(V) = \{f : V \rightarrow V; f \text{ é } K\text{-automorfismo}\}$, isto é, uma representação é uma aplicação $\Phi : G \rightarrow GL(V)$ tal que $\Phi(\sigma_1\sigma_2) = \Phi(\sigma_1)\Phi(\sigma_2)$, para todo $\sigma_1, \sigma_2 \in G$.

Neste caso, V é chamado o *espaço de representação* e a dimensão de V é chamada a *dimensão da representação*. Uma representação de grupo é dita ser uma *representação fiel* se ela for injetora. Observe que para falarmos de uma representação de um grupo, devemos exibir o espaço vetorial V e o homomorfismo. Algumas vezes, neste trabalho, por abuso de notação, denotaremos a representação de um grupo, apenas por V .

Denotaremos também $K(V) \supseteq K$ como uma extensão de corpos, onde $K(V) = K(\Psi(\sigma_1), \dots, \Psi(\sigma_n))$ e Ψ é a representação do grupo $G = \{\sigma_1, \dots, \sigma_n\}$ sobre o K -espaço vetorial V .

Iremos agora relacionar representações lineares fiéis com as extensões de corpos e suas respectivas formas traços. No próximo resultado, mostraremos que o fato da forma traço ser hiperbólica não depende da escolha de uma representação fiel.

Lema 3.14 *Sejam V e V' duas representações lineares fiéis de um grupo finito G sobre um corpo K , e consideremos $L = K(V)$, $K_1 = L^G$, $L' = K(V')$ e $K'_1 = L'^G$. Se q_{L/K_1} é hiperbólica, então q_{L'/K'_1} também será.*

Demonstração: Sejam $n = \dim_K(V)$, $n' = \dim_K(V')$, $s = (s_1, s_2, \dots, s_n)$ e $t = (t_1, \dots, t_{n'})$ úplas de variáveis independentes sobre K e K' , respectivamente. Pelo lema sem nome no apêndice 3 de [12], temos que $L(t) \cong L'(s)$ como $K[G]$ álgebras, onde G age trivialmente nas variáveis.

Assim, desde que q_{L/K_1} é hiperbólica, temos que $q_{L(t)/K_1(t)} \simeq q_{L'(s)/K'_1(s)}$ é hiperbólica sobre $K_1(t) \cong K'_1(s)$. Agora, o resultado segue do fato que a aplicação natural $W(K'_1) \rightarrow W(K'_1(s))$ é injetiva. A injetividade segue do lema anterior. ■

Vamos agora mostrar que sob certas condições, a extensão galoisiana L sobre K não admite uma base normal ortogonal. Feito isso, poderemos enfim, concluir a demonstração do item (b) do teorema 3.1.

Proposição 3.15 *Seja V uma representação linear fiel de um grupo G sobre um corpo K_1 , $L = K_1(V)$, $K = L^G$, e seja $G_2 \leq G$ um 2-subgrupo de Sylow abeliano de G . Suponha que n é o expoente de G_2 e que K contém uma raiz n -ésima primitiva da unidade. Então a extensão galoisiana L sobre K não admite uma base normal ortogonal.*

Demonstração: Se mostrarmos que $q_{K_1(V)/K_1(V)^{G_2}} = q_{L/L^{G_2}}$ não é hiperbólica, então pelo lema 3.12 teremos que $q_{L/K}$ não será hiperbólica, e portanto pelo teorema 3.6 teremos que L sobre K não possui base normal ortogonal e, conseqüentemente, não possui base normal auto-dual.

Mostraremos então que q_{L/LG_2} não é hiperbólica.

Seja $G_2 \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_r}$ um 2-grupo abeliano com expoente n . Note que se $\sigma \in G_2$ então podemos associar σ a uma r -upla $(\overline{m_1}, \dots, \overline{m_r})$ onde $\overline{m_i} \in \mathbb{Z}_{n_i}$ e $1 < m_i < n_i$, para cada $i = 1, \dots, r$. O subgrupo G_2 possui uma representação fiel Φ de dimensão r sobre $K_1 \times \cdots \times K_1 = K_1^r = S$ dada por

$$\sigma \mapsto \Phi(\sigma)(x_i) = (\omega_{n_i})^{m_i} x_i,$$

onde ω_{n_i} é uma raiz n_i -ésima primitiva da unidade e $x = (x_1, \dots, x_r) \in S$. Mostremos que de fato Φ é uma representação de G_2 . Note que para $x = (x_1, \dots, x_r) \in S$ e $\sigma, \rho \in G_2$, com σ associado a $(\overline{m_1}, \dots, \overline{m_r})$ e ρ associado a $(\overline{l_1}, \dots, \overline{l_r})$, temos

$$\begin{aligned} \Phi(\sigma\rho)(x) &= (\sigma\rho)(x_1, x_2, \dots, x_r) = (\omega_{n_1}^{m_1+l_1} x_1, \dots, \omega_{n_r}^{m_r+l_r} x_r) = \\ &= (\omega_{n_1}^{m_1} x_1, \dots, \omega_{n_r}^{m_r} x_r)(\omega_{n_1}^{l_1} x_1, \dots, \omega_{n_r}^{l_r} x_r) = \Phi(\sigma)(x)\Phi(\rho)(x). \end{aligned}$$

A representação Φ é de fato fiel, pois se $\Phi(\sigma) = \Phi(\rho)$, então $(\omega_{n_i})^{m_i} x_i = (\omega_{n_i})^{l_i} x_i$, para cada $i = 1, 2, \dots, r$. Conseqüentemente $(\omega_{n_i})^{m_i} = (\omega_{n_i})^{l_i}$, para cada $i = 1, 2, \dots, r$. Como $0 \leq m_i, l_i \leq n_i$ e ω_{n_i} é uma n_i -ésima raiz primitiva da unidade, temos que $m_i = l_i$ para cada $i = 1, 2, \dots, r$, e portanto Φ é injetora.

Observe que

$$K_1(S) = K_1(\sqrt[n_1]{a_1}, \dots, \sqrt[n_r]{a_r}) \quad \text{e} \quad K_1(V)^{G_2} = K_1(a_1, \dots, a_r),$$

onde a_1, a_2, \dots, a_n são variáveis algebricamente independentes sobre K_1 , e $a_i = x_i^{n_i}$, com $i = 1, \dots, r$. De fato, considere $\sigma \in G_2$ associado ao elemento $(\overline{1}, \dots, \overline{1})$, então $\Psi(\sigma)(x_i) = \omega_{n_i} x_i$, para cada $i = 1, \dots, r$. Portanto, $K_1(S) = K_1(\omega_{n_1} x_1, \dots, \omega_{n_r} x_r)$. Além disso, para cada $i = 1, \dots, r$, temos que $\omega_{n_i} x_i = \sqrt[n_i]{x_i^{n_i}} = \sqrt[n_i]{a_i}$, pois $a_i = x_i^{n_i}$, portanto a igualdade segue. Pelo lema 3.11, temos que $q_{K_1(S)/K_1(S)G_2}$ não é hiperbólica e conseqüentemente pelo lema 3.14 teremos que q_{L/LG_2} também não será hiperbólica. ■

A proposição demonstrada acima é uma versão mais fraca do teorema 3.1 item (b), pois neste teorema, não garantimos que o corpo K tenha a n -ésima raiz primitiva da

unidade. Logo, para fecharmos a demonstração do item (b) vamos supor agora que K não contenha uma raiz n -ésima primitiva da unidade. Seja ω uma raiz n -ésima primitiva da unidade. Consideremos então a extensão de corpos $L(\omega) \supseteq K(\omega)$. Basta mostrarmos que esta extensão é galoisiana pois, feito isso, as hipóteses da proposição 3.15 estarão satisfeitas e portanto o teorema 3.1, item (b), estará provado.

Como a extensão $L \supseteq K$ é galoisiana, temos que L é o corpo de raízes de um polinômio separável $p(X) \in K[X]$. Se $\omega \in L$, então ainda teremos que L será corpo de raízes do polinômio separável $p(X) \in K(\omega)[X]$. Conseqüentemente, a extensão $L = L(\omega)$ sobre $K(\omega)$ é uma extensão galoisiana.

Se $\omega \notin L$, então consideremos $q(X) = p(X)(X^n - 1)$. Claramente, temos que $q(X)$ é um polinômio separável em $K(\omega)[X]$ e $L(\omega)$ é o corpo de raízes de $q(X)$ sobre $K(\omega)[X]$. Seja $G = Gal(L/K) = \{\sigma_1, \dots, \sigma_n\}$. Temos que $\sigma_i(x) = x$, para todo $x \in K$, com $i = 1, \dots, n$.

Consideremos $G' = Gal(L(\omega)/K(\omega))$. Desde que cada elemento de G' deixa ω fixo, temos que $G' \cong G$. Temos então que $L(\omega)/K(\omega)$ satisfaz as hipóteses da proposição 3.15, e portanto o teorema 3.1 (b) está provado. ■

Para compreender melhor esse resultado, vamos apresentar um exemplo.

Exemplo 3.16 Consideremos a extensão de corpos $L \supseteq K$ dada por $L = \mathbb{Z}_3(i)$, $K = \mathbb{Z}_3$ com i a unidade imaginária. Mostraremos que o teorema 3.1 se aplica neste exemplo, ou seja, a extensão L sobre K não possui base normal ortogonal. Na verdade, mostraremos que todas as possíveis bases normais desta extensão não são ortogonais.

Primeiro, note que o polinômio minimal de i sobre \mathbb{Z}_3 é o polinômio $p(X) = X^2 + \bar{1}$. Esse polinômio é irredutível sobre \mathbb{Z}_3 , pois não possui raízes em \mathbb{Z}_3 . Claramente i é a raiz de $p(X)$. Concluímos então que $[\mathbb{Z}_3(i) : \mathbb{Z}_3] = 2$, logo $|G| = |Gal(L/K)| = 2$, então $G = \{1, \sigma\}$ com $\sigma(i) = \bar{2}i$. Temos também que $\mathbb{Z}_3(i) = \{\bar{0}, \bar{1}, \bar{2}, i, \bar{2}i, \bar{1} + i, \bar{2} + i, \bar{1} + \bar{2}i, \bar{2} + \bar{2}i\}$.

Analisando todos os possíveis casos, obtemos que as únicas bases normais de $\mathbb{Z}_3(i)$ sobre \mathbb{Z}_3 são $\mathcal{B}_1 = \{\bar{1} + i, \bar{1} + \bar{2}i\} = \{\bar{1} + i, \sigma(\bar{1} + i)\}$ e $\mathcal{B}_2 = \{\bar{2} + \bar{2}i, \bar{2} + i\} = \{\bar{2} + \bar{2}i, \sigma(\bar{2} + \bar{2}i)\}$.

Com relação a \mathcal{B}_1 , temos que

$$\begin{aligned} T(\bar{1} + i, \bar{1} + i) &= Tr_{L/K}(\bar{2}i) = \bar{2}i + \sigma(\bar{2}i) \\ &= \bar{2}i + (-\bar{2}i) = \bar{0}, \end{aligned}$$

$$\begin{aligned} T(\bar{1} + i, \bar{1} + \bar{2}i) &= T(\bar{1} + \bar{2}i, \bar{1} + i) \\ &= Tr_{L/K}(\bar{2}) = \bar{2} + \sigma(\bar{2}) = 1, \end{aligned}$$

$$T(\bar{1} + \bar{2}i, \bar{1} + \bar{2}i) = Tr_{L/K}(i) = i + \sigma(i) = i + \bar{2}i = \bar{0},$$

ou seja, \mathcal{B}_1 é uma base normal não ortogonal.

Com relação a \mathcal{B}_2 , temos

$$T(\bar{2} + \bar{2}i, \bar{2} + \bar{2}i) = Tr_{L/K}(\bar{2}i) = \bar{0},$$

$$T(\bar{2} + \bar{2}i, \bar{2} + i) = T(\bar{2} + i, \bar{2} + \bar{2}i) = Tr_{L/K}(\bar{2}) = \bar{1},$$

$$T(\bar{2} + i, \bar{2} + i) = Tr_{L/K}(i) = \bar{0},$$

ou seja, \mathcal{B}_2 também é uma base normal não ortogonal.

Referências Bibliográficas

- [1] Bass, H., Unitary algebraic K -theory. *Lecture Notes in Mathematics*, **343** (1973), 57–265.
- [2] Bayer-Fluckiger, E., Self-dual normal bases, Nedel, Akad. Wetensch, *Indag. Math.*, **51** (1989), no. 4, 379–383.
- [3] Bayer-Fluckiger, E., Serre, J. P., Torsions Quadratiques et Bases Normales Auto-duales, *Amer. J. Math.*, **116** (1994), 1–64.
- [4] Hoffman, K., Kunze, R., *Linear Algebra*, Prentice-Hall, New Jersey, 2.ed.,(1971).
- [5] Jacobson, N., *Basic Algebra I*, W. H. Freeman and Company, New York (1985).
- [6] Kang, D. S., Nonexistence of self-dual normal bases, *Comm. in Algebra*, **32**, no. 1 (2004), 125–132.
- [7] Kang, D. S., Reichstein, Z., Trace forms of Galois field extensions in the presence of roots of unity, *J. Reine Angew Math.*, **549** (2002), 79–89.
- [8] Lam, T. Y., *The Algebraic Theory of Quadratic Forms*, University of California (1973).
- [9] Lang, S., *Algebra*, Addison-Wesley, Reading (1965).
- [10] Milies, C. P., *Anéis e Módulos*, IME-USP, Publicações do Instituto de Matemática e Estatística da Universidade de São Paulo (1972).
- [11] Scharlau, W., *Quadratic and Hermitian Forms*, Grundlehren der Math. Wiss. 270, Springer-Verlag (1985).
- [12] Shafarevich, I. R., *Basic Algebraic Geometry*, vol. 1, 2.ed., Springer-Verlag (1994).

Livros Grátis

(<http://www.livrosgratis.com.br>)

Milhares de Livros para Download:

[Baixar livros de Administração](#)

[Baixar livros de Agronomia](#)

[Baixar livros de Arquitetura](#)

[Baixar livros de Artes](#)

[Baixar livros de Astronomia](#)

[Baixar livros de Biologia Geral](#)

[Baixar livros de Ciência da Computação](#)

[Baixar livros de Ciência da Informação](#)

[Baixar livros de Ciência Política](#)

[Baixar livros de Ciências da Saúde](#)

[Baixar livros de Comunicação](#)

[Baixar livros do Conselho Nacional de Educação - CNE](#)

[Baixar livros de Defesa civil](#)

[Baixar livros de Direito](#)

[Baixar livros de Direitos humanos](#)

[Baixar livros de Economia](#)

[Baixar livros de Economia Doméstica](#)

[Baixar livros de Educação](#)

[Baixar livros de Educação - Trânsito](#)

[Baixar livros de Educação Física](#)

[Baixar livros de Engenharia Aeroespacial](#)

[Baixar livros de Farmácia](#)

[Baixar livros de Filosofia](#)

[Baixar livros de Física](#)

[Baixar livros de Geociências](#)

[Baixar livros de Geografia](#)

[Baixar livros de História](#)

[Baixar livros de Línguas](#)

[Baixar livros de Literatura](#)
[Baixar livros de Literatura de Cordel](#)
[Baixar livros de Literatura Infantil](#)
[Baixar livros de Matemática](#)
[Baixar livros de Medicina](#)
[Baixar livros de Medicina Veterinária](#)
[Baixar livros de Meio Ambiente](#)
[Baixar livros de Meteorologia](#)
[Baixar Monografias e TCC](#)
[Baixar livros Multidisciplinar](#)
[Baixar livros de Música](#)
[Baixar livros de Psicologia](#)
[Baixar livros de Química](#)
[Baixar livros de Saúde Coletiva](#)
[Baixar livros de Serviço Social](#)
[Baixar livros de Sociologia](#)
[Baixar livros de Teologia](#)
[Baixar livros de Trabalho](#)
[Baixar livros de Turismo](#)