UNIVERSIDADE FEDERAL DE SANTA MARIA
CENTRO DE CIÊNCIAS NATURAIS E EXATAS
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Mônica Piotsckowski

TÓPICOS DE ÁLGEBRA LINEAR EXPLORADOS COM O AUXÍLIO DA TEORIA DE GALOIS

Santa Maria, RS
2016

Mônica Piotsckowski

TÓPICOS DE ÁLGEBRA LINEAR EXPLORADOS COM O AUXÍLIO DA TEORIA DE GALOIS

Dissertação apresentada ao Curso de Mestrado da Pós-Graduação em Matemática, Área de Matemática Pura, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Mestre em Matemática**.

Orientador: Prof. Dr. Dirceu Bagio

Santa Maria, RS
2016

Mônica Piotsckowski

TÓPICOS DE ÁLGEBRA LINEAR EXPLORADOS COM O AUXÍLIO DA TEORIA DE GALOIS

Dissertação apresentada ao Curso de Mestrado da Pós-Graduação em Matemática, Área de Matemática Pura, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Mestre em Matemática**.

Aprovado em 10 de maio de de 2016:

Dirceu Bagio, Dr. (UFSM)
(Presidente/Orientador)

Thaisa Raupp Tamusiunas, Dra. (UFCSPA)

Gustavo Grings Machado, Dr. (UFSM)

Santa Maria, RS
2016

DEDICATÓRIA

Ao meu pai (in memoriam). Alguém a quem a matemática, mesmo em sua simplicidade, sempre encantou.

AGRADECIMENTOS

Primeiramente à Deus, que foi presença constante em minha vida neste tempo, iluminando meu caminho e reanimando minhas forças.

À minha família, por todo apoio, incentivo e suporte dado para que este trabalho pudesse ser concluído, mesmo nos momentos difíceis pelos quais passamos.

Ao meu orientador Dirceu Bagio, por ter me aceito como orientanda e por todo apoio, incentivo, paciência e conhecimento passado durante este tempo. Também aos demais professores do programa, que fizeram parte desta caminhada e contribuíram para a minha formação acadêmica. Aos professores Thaísa e Gustavo, que compuseram a banca, pelas contribuições feitas a este trabalho.

Aos meus amigos, os de perto e os que mesmo longe estavam torcendo por mim. À Marciéle, que mesmo não estando perto e às vezes não nos falando tanto, estava sempre presente. Ao Fernando, parceiro de quase tudo, uma amizade que nasceu na graduação, e se intensificou durante o mestrado. Aos amigos também de graduação: Douglas e Geovani, companheiros de mestrado, de prédio e da vida. E às novas amizades feitas neste tempo, em especial aos demais alunos da turma 2014/1 e companheiros de 1213 e 1214. Os levarei sempre em meu coração, assim como os mates, almoços no RU e brincadeiras do dia a dia. Um agradecimento especial à Silvia, um amizade que nasceu sem pretensões e tornou-se muito especial para mim. À todos estes, o meu muito obrigada pelos momentos simples e únicos que compartilhamos.

Também à Renovação Carismática Católica, especialmente ao Ministério das Universidades Renovadas de Santa Maria e aos que fazem parte dele. Obrigada pela oportunidade de fazer parte deste sonho, agradeço a Deus por ter colocado todas estas pessoas maravilhosas em minha vida. Levarei todos sempre comigo assim como os momentos que partilhamos. Sempre um só coração.

Ao PPGMAT e à UFSM pela oportunidade de cursar o mestrado. À CAPES pelo suporte financeiro.

Lâmpada para os meus pés é tua palavra,
e luz para o meu caminho.
(Bíblia Sagrada, Salmo 119, 105)

RESUMO

TÓPICOS DE ÁLGEBRA LINEAR EXPLORADOS COM O AUXÍLIO DA TEORIA DE GALOIS

AUTOR : MÔNICA PIOTSCKOWSKI
ORIENTADOR : DIRCEU BAGIO

Seja L/K uma extensão de Galois finita. Neste trabalho, exploramos o K-espaço vetorial $Alt(L)$ das formas bilineares alternadas sobre L. Em particular, apresentamos uma decomposição em soma direta de $Alt(L)$. Também estudamos a estrutura de $Alt(L)$ no caso em que a extensão de Galois L/K é cíclica. Outro aspecto de álgebra linear que é abordado nesta dissertação, são os K-endomorfismos de posto 1 de L, ou seja, os K-hiperplanos de L.

Palavras-chave: extensões de Galois, grupo de Galois, formas bilineares alternadas, posto, extensões cíclicas, endomorfismos, hiperplanos, traço Galois.

ABSTRACT

LINEAR ALGEBRA TOPICS EXPLORED WITH THE HELP OF GALOIS THEORY

AUTHOR : MÔNICA PIOTSCKOWSKI
ADVISOR : DIRCEU BAGIO

Let L/K be a finite Galois extension. In this work, we explore the K-vector space $Alt(L)$ of alternating bilinear forms over L. In particular, we present a decomposition of $Alt(L)$ in direct sum. Also, we study the structure of $Alt(L)$ in the case of cyclic Galois extension L/K. Another aspect of linear algebra that is explored in this dissertation are the K-endomorphisms over L with rank 1, that is, the K-hyperplanes of L.

Keywords: Galois extensions, Galois group, alternating bilinear forms, rank, cyclic extension, endomorphisms, hyperplane, Galois trace.

Sumário

INTRODUÇÃO

A álgebra linear é uma ferramenta extremamente útil no estudo de diversas áreas do conhecimento e hoje se encontra subjacente a quase todos os ramos da matemática, isso porque se entende que é difícil estudar qualquer problema sem a perfeita compreensão dos fenômenos lineares. Já a teoria de Galois, que surgiu no século XIX, motivou o estudo mais aprofundado da teoria de grupos e da teoria de corpos, mostrando as relações existentes entre ambas.

Dados os corpos L e K, seja L/K uma extensão de Galois finita de grau n. Então L é um K-espaço vetorial de dimensão n. Nesta situação, é natural nos perguntarmos se é possível entender melhor determinados assuntos de álgebra linear. Em outras palavras, se consideramos um K-espaço vetorial L, de tal forma que L/K é uma extensão de Galois finita, então que tipo de resultados de álgebra linear podemos obter usando as ferramentas da teoria de Galois? O objetivo deste trabalho é mostrar, em duas situações específicas, como a teoria de Galois pode ser útil em problemas de álgebra linear.

Dois artigos são estudados nesta dissertação. O primeiro, é o artigo *Galois extensions and subspaces of alternating bilinear forms with special rank properties* de Rod Gow e Rachel Quinlan [GQ1]. Os resultados deste artigo são apresentados no Capítulo 2 deste trabalho. Suponha que L/K é uma extensão de Galois finita e denote por $Alt(L)$ o K-espaço vetorial das formas bilineares alternadas sobre L. Nestas condições, provamos um teorema de decomposição em soma direta para $Alt(L)$. Os subespaços vetoriais que aparecem nesta soma direta são construídos com o auxílio da teoria de Galois. O caso em que L/K é uma extensão de Galois cíclica também é explorado.

O segundo artigo que estudamos é *Galois theory and linear algebra* de Rod Gow e Rachel Quinlan [GQ]. Os resultados deste artigo aparecem no Capítulo 3 do trabalho. Assuma novamente que L/K é uma extensão de Galois finita e denote por $End_K\ (L)$ o K-espaço vetorial dos K-endomorfismos de L. Usando a teoria de Galois, podemos descrever os elementos de $End_K\ (L)$ que possuem posto 1, isto é, os K-hiperplanos de L. Aqui, o K-endomorfismo de L obtido pelo traço da extensão L/K tem papel importante nos resultados.

Capítulo 1

PRÉ-REQUISITOS

Neste capítulo serão introduzidas algumas noções e resultados importantes que utilizaremos nos capítulos posteriores. Basicamente, os assuntos abordados aqui são: grupos simétricos, teoria de Galois e álgebra linear.

1.1 GRUPOS SIMÉTRICOS

Nesta seção, traremos de forma sucinta algumas definições e resultados sobre grupos simétricos que serão utilizados no decorrer deste trabalho.

1.1.1 Permutações

Começamos lembrando que uma *permutação* de um conjunto X é uma bijeção $\alpha : X \longrightarrow X$. O conjunto das permutações de X, que denotaremos por S_X, é um grupo com a operação de composição usual, e é chamado de *grupo simétrico*. No caso especial em que $X = \{1, 2, \ldots, n\}$ escrevemos S_n. Note que $|S_n| = n!$. A notação (1 3 5) em S_5, representa a permutação que associa $1 \longrightarrow 3$, $3 \longrightarrow 5$, $5 \longrightarrow 1$ e que deixa o 2 e o 4 fixos. O elemento identidade será representado por (1). Duas permutações α, $\beta \in S_X$ são ditas *disjuntas* se cada x movido por uma é fixo pela outra, ou seja: se $\alpha(x) \neq x$, então $\beta(x) = x$ e se $\beta(y) \neq y$, então $\alpha(y) = y$, $x, y \in X$.

Definição 1.1.1. *Sejam $i_1, i_2, \ldots, i_r$ inteiros disjuntos entre 1 e n. Se $\alpha \in S_n$ fixa os $n - r$ inteiros que não pertencem ao conjunto $i_1, i_2, \ldots, i_r$ e se*

$$\alpha(i_1) = i_2,\ \alpha(i_2) = i_3,\ \ldots,\ \alpha(i_{r-1}) = i_r,\ \alpha(i_r) = i_1,$$

então α é um r-ciclo; também chamado de ciclo de tamanho r. Além disso, o ciclo que fixa todo elemento de X é denotado por (i) e denomidado 1-ciclo.

O elemento (2 3 4) em S_7, por exemplo, é um ciclo de tamanho 3, um 3-ciclo. Um 2-ciclo, que só permuta um par de elementos, é chamado uma *transposição*, como por exemplo o elemento (2 4) em S_n, $(n \geq 4)$. Além disso, dois ciclos $(\alpha_1, \ldots, \alpha_m)$ e $(\beta_1, \ldots, \beta_k)$ com $m, k \geq 2$ são disjuntos quando nenhum dos α_i é igual a qualquer um dos β_j.

A seguir, apresentamos uma caracterização dos elementos do grupo de permutações a partir de ciclos, cuja demonstração pode ser vista em [R], no Teorema 1.1 da página 6.

Teorema 1.1.2. *Toda permutação $\alpha \in S_X$ é um ciclo ou um produto de ciclos disjuntos.*

Esse resultado é muito importante, pois nos permite decompor toda permutação em termos de ciclos, e mais do que isso, podemos fazê-lo usando apenas transposições, como nos diz o próximo teorema.

Teorema 1.1.3. *Toda permutação $\alpha \in S_X$ é um produto de transposições e um r-ciclo é um produto de $r-1$ tranposições.*

Dem.: Pelo Teorema 1.1.2 todo elemento de S_X é um produto de ciclos disjuntos. Além disso, todo r-ciclo é escrito como

$$(1\ 2\ \cdots\ r) = (1\ r)(1\ r-1)\cdots(1\ 2),$$

um produto de $r-1$ transposições. Logo, segue o resultado. □

Dada uma permutação $\alpha \in S_X$ dizemos que esta é *par* se pode ser escrita como produto de um número par de transposições, e *ímpar* se é o produto de um número ímpar de trasposições. Por exemplo, em S_6, temos que $(1\ 6\ 5\ 3\ 2) = (2\ 3)(1\ 2)(5\ 6)(1\ 5)$ é par, já $(1\ 3\ 4\ 5) = (3\ 5)(1\ 5)(1\ 4)$ é uma permutação ímpar.

Observação 1.1.4. *No Teorema 1.1.3 não temos unicidade na decomposição. Por exemplo, em S_5 temos (1 2 3)=(1 3)(1 2) e (1 2 3)=(4 5)(5 4)(1 3)(1 2). No entanto, a quantidade de tranposições em duas decomposições de um mesmo ciclo é invariante quanto a paridade, isto é, ambas possuem quantidade par ou ambas possuem quantidade ímpar. Assim, a noção de permutação par e ímpar está bem definida.*

O conjunto das permutações pares forma um grupo com características especiais.

Lema 1.1.5. *O conjunto das permutações pares, denotado por A_n, forma um subgrupo normal de S_n, de índice 2.*

Dem.: Ver o Corolário 6.10 na página 75 de [I] □

Considere uma permutação α. Uma fatoração de α como um produto de ciclos disjuntos, que contém um 1-ciclo (i) para cada i fixado por α, é dita uma *fatoração completa* de α. Em uma fatoração completa da permutação α, todo $1 \leq i \leq n$ ocorre em exatamente um dos ciclos.

Definição 1.1.6. *Se $\alpha \in S_n$ e $\alpha = \beta_1 \cdots \beta_t$ é uma fatoração completa em ciclos disjuntos, o sinal dessa permutação é definido por $\epsilon(\alpha) = (-1)^{n-t}$.*

De forma geral, como nos mostra o próximo teorema, conhecendo o sinal de uma permutação, podemos determinar se a mesma é par ou ímpar. E, reciprocamente, podemos determinar qual o sinal de uma permutação a partir da sua paridade.

Teorema 1.1.7. *Uma permutação $\alpha \in S_n$ é par se e somente $\epsilon(\alpha) = 1$ e ímpar se e somente se $\epsilon(\alpha) = -1$. Além disso, para quaisquer $\alpha,\ \beta \in S_n$ tem-se $\epsilon(\alpha\beta) = \epsilon(\alpha)\epsilon(\beta)$.*

Dem.: Ver os Teoremas 1.6 e 1.7 na página 9 de [R] □

Assim, da forma como podemos escrever cada elemento no grupo de permutações, é possível determinar o sinal e a paridade do mesmo. E, além disso, tais características nos dão informações a respeito de seus subgrupos e dos índices destes. Para o próximo resultado, considere a seguinte definição de ação de grupos.

Definição 1.1.8. *Uma ação (à esquerda) de um grupo G sobre um conjunto não vazio X é uma aplicação*

$$\begin{aligned} \cdot : G \times X &\longrightarrow X \\ (g, x) &\longmapsto g \cdot x \end{aligned}$$

que satisfaz

$$e \cdot x = x, \qquad (g.h) \cdot x = g \cdot (h \cdot x), \qquad \text{para quaisquer } g, h \in G,\ x \in X,$$

onde $e \in G$ denota o elemento neutro do grupo G. Neste caso, dizemos que G age sobre X. De maneira análoga, definimos ação (à direita) de G sobre X.

Em particular, se G é o grupo de permutações do conjunto $\Omega = \{1, 2, \ldots, n\}$, então a aplicação

$$\begin{aligned} \cdot : G \times \Omega &\longrightarrow \Omega \\ (\sigma, j) &\longmapsto \sigma \cdot j = \sigma(j) \end{aligned}$$

é uma ação (à esquerda) de G sobre Ω.

No próximo resultado, dado um grupo G usaremos a notação $A \lhd G$ para representar que A é um subgrupo normal de G.

Lema 1.1.9. *Suponha que o grupo G age em um conjunto finito Ω e assuma que algum elemento $\alpha \in G$ induz uma permutação ímpar em Ω. Então existe um subgrupo normal A de G tal que o índice de A em G é 2 e $\alpha \notin A$. Ou seja, existe $A \lhd G$ com $[G : A] = 2$ e $\alpha \notin A$.*

Dem.: Ver o Corolário 6.11 na página 75 de [I]. □

1.1.2 p-subgrupos de Sylow e p-complementos normais

Visto que para os próximos resultados necessitamos de alguns tópicos a respeito dos teoremas de Sylow, vamos relembrar algumas definições básicas e propriedades dos mesmos, assim como relacioná-los com p-complementos normais.

Definição 1.1.10. *(a) Se p é um primo, então um p-grupo é um grupo finito em que todo elemento tem como ordem uma potência de p.*

(b) Um p-subgrupo de Sylow de um grupo G é um p-subgrupo de G que é maximal (em relação à ordem).

Teorema 1.1.11. *Se G é um grupo finito de ordem $p^e m$ e $mdc(p, m) = 1$, então todo Sylow p-subgrupo de G tem ordem p^e.*

Dem.: Ver o Teorema 4.14 na página 80 de [R]. □

Seja p um número primo. Um *p-complemento normal* N de um grupo finito G é um subgrupo normal de ordem coprima com p e índice uma potência de p, ou seja, $N \lhd G$ tal que $mdc(|N|, p) = 1$ e $[G : N] = p^r$, para $r > 0$.

Também lembremos que dado H um subgrupo do grupo G, então o normalizador de H em G, denotado por $N_G(H)$, é dado por $N_G(H) = \{a \in G : aHa^{-1} = H\}$.

Sobre p-complementos normais necessitamos do seguinte resultado:

Teorema 1.1.12. *(Burnside) Sejam G um grupo finito e P um p-subgrupo de Sylow de G. Se $P \leq Z(N_G(P))$ (ou seja, P é um subgrupo do centro do normalizador de P em G), então G possui um p-complemento normal.*

Dem.: Ver o Teorema 1.13 na página 9 de [Cr]. □

No caso em que G tem um 2-subgrupo de Sylow cíclico, Cayley mostrou o seguinte resultado:

Teorema 1.1.13. *(Cayley) Seja G um grupo finito de ordem par, e seja P_2 um 2-subgrupo de Sylow de G. Se P_2 é cíclico, então G tem um 2-complemento normal.*

Dem.: Ver o Corolário 1.14 na página 10 de [Cr]. □

Lema 1.1.14. *Um grupo finito G tem no máximo um p-complemento normal.*

Dem.: Ver o Lema 15.5.1 na página 182 de [LF]. □

1.2 TEORIA DE GALOIS

A presente seção tem por objetivo familiarizar o leitor com alguns elementos principais da teoria de Galois, principalmente com a correspondência de Galois. Em toda esta seção, as extensões de corpos são finitas e as demonstrações omitidas podem ser vistas em [R1].

1.2.1 Extensões e teorema fundamental de Galois

Uma *extensão* de um corpo K é um corpo L tal que $L \supseteq K$, a qual denotaremos por L/K. Por exemplo $\mathbb{C}/\mathbb{R}$, e $\mathbb{R}/\mathbb{Q}$. O corpo L tem estrutura de K-espaço vetorial com as operações:

$$\begin{array}{ll} L \times L \longrightarrow L & K \times L \longrightarrow L \\ (x, y) \longmapsto x + y & (\lambda, x) \longmapsto \lambda x, \end{array}$$

e sua dimensão é chamada de *grau* da extensão e denotada por $[L : K]$. Para nossos propósitos, consideraremos extensões finitas, isto é, $[L : K] < \infty$. Por exemplo, $\mathbb{C}$ como $\mathbb{R}$-espaço vetorial tem base $\{1, i\}$. Então $[\mathbb{C} : \mathbb{R}] = 2$.

Observação 1.2.1. *Seja L/K uma extensão de corpos e seja F um corpo intermediário, isto é, $K \subseteq F \subseteq L$. Neste caso dizemos que $K \subseteq F \subseteq L$ é uma torre de corpos. Tanto L quanto F têm estrutura de K-espaço vetorial, mas podemos também considerar L como espaço vetorial com escalares no corpo F. E ainda vale que $[L : K] = [L : F][F : K]$.*

Seja L/K uma extensão de corpos e $u \in L$. Então o menor subcorpo de L contendo K e u (o qual existe) é denotado por $K[u]$. Dizemos que $\alpha \in L$ é *separável* sobre K se o polinômio minimal $p_{\alpha/K}(x)$ (o polinômio mônico de menor grau com coeficientes em K e que anula α) é *separável*, isto é, $p_{\alpha/K}(x)$ não possui raízes repetidas. A extensão L/K é dita *separável* se todo elemento $\alpha \in L$ é separável sobre K.

Observação 1.2.2. *Se $ch(K) = 0$ então L/K é separável.*

Uma extensão L/K é dita *normal* se cada vez que um polinômio irredutível sobre $K[x]$ tem uma raiz em L, então tem todas as suas raízes em L. Equivalentemente, L/K é normal se L é o corpo de decomposição de algum polinômio não nulo em $K[x]$, isto é, L é o menor subcorpo que contém K e todas as raízes desse polinômio. Por exemplo, $\mathbb{C}/\mathbb{R}$ é uma extensão normal porque $L = \mathbb{C}$ é o corpo de decomposição do polinômio $f(x) = x^2+1 \in \mathbb{R}[x]$. Já se considerarmos o polinômio irredutível $p(x) = x^3 - 2 \in \mathbb{Q}[x]$, vemos que $p(x)$ tem uma raiz real $a = \sqrt[3]{2} \in \mathbb{Q}[a]$. Porém este polinômio não possui todas as suas raízes em $\mathbb{Q}[a]$ e consequentemente a extensão $\mathbb{Q}[a]/\mathbb{Q}$ não é normal.

Agora podemos definir extensões de Galois.

Definição 1.2.3. *Uma extensão finita de corpos L/K é dita uma extensão de Galois se L/K é separável e normal.*

Note, por exemplo, que $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$ é Galois. O grupo de Galois, que será definido abaixo, é dado por $Gal(\mathbb{Q}[\sqrt{2}]/\mathbb{Q}) = \{id, \sigma\}$, onde σ é o automorfismo que associa $\sqrt{2}$ a $-\sqrt{2}$.

Vale também que se $L \supseteq F \supseteq K$ são extensões tais que L/K é Galois, então L/F também o é, porém F/K não é necessariamente de Galois. Tome, por exemplo, L o corpo de decomposição do polinômio $x^3 - 2$ sobre $\mathbb{Q}$, $F = \mathbb{Q}[\sqrt[3]{2}]$ e $K = \mathbb{Q}$.

Teorema 1.2.4. *(Elemento Primitivo) Seja L/K uma extensão de Galois. Então existe $u \in L$ tal que $L = K[u]$.*

Seja $Aut(L) = \{\phi : L \longrightarrow L : \phi$ é automorfismo $\}$ o grupo de todos os automorfismos de L, isto é, todas as funções bijetivas de L em L que preservam a soma e o produto de elementos de L. Considere uma extensão de Galois L/K. O *grupo de Galois* de L sobre K é o grupo de todos os automorfismos de L que deixam os elementos de K fixos, ou seja:

$$Gal(L/K) = \{\sigma \in Aut(L) : \sigma(\lambda) = \lambda, \text{ para todo } \lambda \in K\}.$$

Exemplo 1.2.5. *Seja o corpo $K = \mathbb{Q}$ e a extensão $L = \mathbb{Q}[i]$. Note que L/K é Galois e uma base de $\mathbb{Q}[i]$ é $\{1, i\}$. Evidentemente $\sigma = id \in Gal(L/K)$. Se $\sigma \in Gal(L/K)$ e $\sigma \neq id$, então $\sigma(a + bi) = \sigma(a) + \sigma(bi) = a + b\sigma(i)$, para todo $(a + bi) \in \mathbb{Q}[i]$. Mas $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$. Logo,*

$$\sigma(i) = i \text{ ou } \sigma(i) = -i$$

Dessa forma, o corpo de Galois dessa extensão é $Gal(L/K) = \{id, \sigma_1\}$, onde $\sigma_1(a + bi) = a - bi$.

Se L é uma extensão de K e H é um subgrupo de $Gal(L/K)$, o corpo fixo L^H de H sobre K é o conjunto de todos os elementos de L que são fixos por H, ou seja

$$L^H = \{a \in L : \sigma(a) = a, \text{ para todo } \sigma \in H\}.$$

É imediato verificar que L^H é um subcorpo de L e que $K \subseteq L^H \subseteq L$.

Proposição 1.2.6. *Sejam L uma extensão de Galois de K e $G = Gal(L/K)$. Se $L^G = K$, então $|Gal(L/K)| = [L : K]$.*

O próximo lema traz um resultado acerca do corpo fixo de Galois para extensões de Galois.

Lema 1.2.7. *Sejam L uma extensão de Galois de K e $G = Gal(L/K)$. Então $L^G = K$.*

A seguir, traremos o principal resultado da teoria de Galois, conhecido como o *teorema de correspondência de Galois*.

Teorema 1.2.8. *Seja L/K uma extensão de Galois e seja $Gal(L/K)$ seu grupo de Galois. Então:*

i) Existe uma correspondência biunívoca entre os subgrupos de $Gal(L/K)$ e os corpos intermediários da extensão L/K:

   (a) Se $K \subset F \subset L$, então o subgrupo de $Gal(L/K)$ que corresponde a F é $Gal(L/F)$.

   (b) Se H é um subgrupo de $Gal(L/K)$, então o corpo intermediário correspondente é L^H.

ii) $[L : L^H] = |H|$ e $[L^H : K] = [Gal(L/K) : H]$ para qualquer subgrupo H de $Gal(L/K)$.

De forma geral, a correspondência de Galois inverte as inclusões e, preserva índices e graus. Para extensões L/K de Galois, temos a seguinte correspondência ilustrada no diagrama abaixo:

$$\begin{array}{rcl} L & \longleftrightarrow & \{id\} = Gal(L/L) \\ | & & | \\ L^H = F & \longleftrightarrow & H = Gal(L/F) \\ | & & | \\ K & \longleftrightarrow & G = Gal(L/K). \end{array}$$

Exemplo 1.2.9. *Seja* $w = e^{2\pi i/5} = cos(2\pi/5) + isen(2\pi/5) \in \mathbb{C}$ *uma raiz 5-ésima primitiva da unidade, isto é,* $w^5 = 1$. *As raízes do polinômio* $x^5 - 1 = (x-1)p(x)$ *são* $1, w, w^2, w^3, w^4$, *onde* $p(x) = x^4 + x^3 + x^2 + x + 1$. *Temos que* $\mathbb{Q}[w]/\mathbb{Q}$ *é separável, pois* $ch(\mathbb{Q}) = 0$. *Além disso,* $\mathbb{Q}[w]$ *é o corpo de decomposição do polinômio* $p(x)$. *Assim,* $\mathbb{Q}[w]/\mathbb{Q}$ *é Galois e tem grau 4, visto que* $\mathbb{Q}[w]$ *como* $\mathbb{Q}$*-espaço vetorial tem base* $\{1, w, w^2, w^3\}$. *Seja* G *o grupo de automorfismos desta extensão. Cada automorfismo* $\sigma \in G$ *deve permutar as raízes de* p *e fica completamente determinada pela sua imagem* $\sigma(w)$. *Logo,* $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$ *onde* $\sigma_j(w) = w^j$. *Note que* $\sigma_1 = id$, *e aplicando sucessivamente* σ_2 *obtemos*

$$w \longmapsto w^2 \longmapsto w^4 \longmapsto w^8 = w^3 \longmapsto w^6 = w$$

e portanto σ_2 *tem ordem 4. Assim* $G \cong \mathbb{Z}_4$. *Sendo cíclico de ordem 4, o grupo* G *possui um subgrupo próprio de ordem 2, a saber* $H =< \sigma_2^2 >=< \sigma_4 >$. *Pela correspondência de Galois, a extensão* $\mathbb{Q}[w]/\mathbb{Q}$ *possui apenas um subcorpo intermediário não trivial, o corpo fixo por* H. *Para determiná-lo, tome* $u = w + w^4$. *Note que* $\sigma_4(u) = \sigma_4(w + w^4) = \sigma_4(w) + \sigma_4(w^4) = w^4 + w^{16} = w^4 + w = u$ *e portanto,* $u \in \mathbb{Q}[w]^H$. *Como* $w^4 = cos(4.2\pi/5) + isen(4.2\pi/5) = cos(2\pi/5) - isen(2\pi/5) = \overline{w}$ *é o conjugado complexo de* w, *temos que* $u \in \mathbb{R}$ *e então* $\mathbb{Q}[w]/\mathbb{Q}[u]$ *é uma extensão de grau 2, pois* $w \notin \mathbb{Q}[u]$ *e* $(x - w)(x - \overline{w}) = x^2 - ux + 1 \in \mathbb{Q}[u][x]$. $\mathbb{Q}[w]$ *como* $\mathbb{Q}[u]$*-espaço vetorial tem base* $\{1, w\}$. *A correspondência de Galois então é dada por:*

$$\begin{array}{ccc} \mathbb{Q}[w] & \longleftrightarrow & \{id\} \\ | & & | \\ \mathbb{Q}[u] & \longleftrightarrow & H \\ | & & | \\ \mathbb{Q} & \longleftrightarrow & G \end{array}$$

onde, $[\mathbb{Q}(w) : \mathbb{Q}] = 4 = 2.2 = [\mathbb{Q}(w) : \mathbb{Q}(u)].[\mathbb{Q}(u) : \mathbb{Q}]$.

Observação 1.2.10. *Em todo nosso trabalho estaremos considerando* K *um corpo,* L/K *uma extensão finita de Galois de grau* n *com grupo de Galois* $G = \{\sigma_1, \ldots, \sigma_n\}$, *e onde* $\sigma \in G$.

Por fim, utilizando as definições e resultados da Seção 1.1.2 para extensões de Galois L/K com grupo de Galois G, podemos provar os dois resultados que seguem.

Lema 1.2.11. *Sejam* L/K *uma extensão de Galois de ordem* $2^n m$ *com* m *ímpar e* G *o seu grupo de Galois. Se* G *tem um 2-subgrupo de Sylow cíclico, então existe um subgrupo normal* $H \triangleleft G$ *tal que o índice de* H *em* G *é 2, isto é,* $[G : H] = 2$.

Dem.: Sejam $G = \{\sigma_1, \ldots, \sigma_{2^n m}\}$ e P_2 o 2-subgrupo de Sylow de G. De acordo com o Teorema 1.1.11 $|P_2| = 2^n$, para $n > 0$ e temos por hipótese que $mdc(2, m) = 1$. Assim, 2^n é a maior potência de 2 que divide $|G|$, onde m é ímpar. Além disso, como P_2 é cíclico existe $\sigma \in G$ tal que P_2 é o subgrupo gerado por σ, ou seja, $P_2 =< \sigma >$. Vamos mostrar que σ induz uma permutação ímpar em G. Temos que o grupo G age em si mesmo por multiplicação regular à esquerda e ao escrevermos $\sigma\sigma_i$ para representar que $\sigma\sigma_i = \sigma_j$ então $\sigma(i) = j$, $1 \leq i, j \leq 2^n m$. Assim σ é uma permutação de $\{1, \ldots, 2^n m\}$. Dessa forma temos que G pode ser visto como um subgrupo do grupo de permutações. Além disso, note que desde que $\sigma \neq 1$, σ não tem pontos fixos nesta ação: $\sigma(\sigma_i) \neq \sigma_i$, para $i = 1, \ldots, 2^n m$.

Afirmação: Cada ciclo na decomposição de σ tem tamanho 2^n.
De fato, considere o conjunto das classes laterais à direita de P_2 em G, isto é, $P_2 \cdot G = \{P_2\sigma_1, \ldots, P_2\sigma_m\}$, onde $\sigma_1, \ldots, \sigma_m \in G$. Tais classes formam uma partição de G e todas tem ordem igual a $2^n = |P_2|$. De acordo com a estrutura de ciclo (página 72 de [I]) do elemento $\sigma \in G$, como existem m classes laterais de tamanho 2^n e $|G| = 2^n m$, σ é um produto de m ciclos de tamanho 2^n. Como os 2^n-ciclos são produtos de $2^n - 1$ transposições, aparecerão $m(2^n - 1)$ transposições na decomposição de σ, ou seja, um número ímpar de transposições. Portanto, σ induz uma permutação ímpar em G e o resultado segue do Lema 1.1.9. □

Nesse mesmo contexto, temos o seguinte lema:

Lema 1.2.12. *Sejam L/K uma extensão de Galois e G o seu grupo de Galois. Se K tem característica diferente de 2, $|G|$ é par e G tem 2-subgrupos de Sylow cíclicos, então a função sinal ϵ é não trivial.*

Dem.: Desde que $|G|$ é par, $|G| = 2^n m$, onde m é ímpar e $n \geq 1$. Então P_2, o 2-subgrupo de Sylow, tem ordem 2^n. Como este é cíclico, existe $\tau \in G$ de ordem igual a 2^n, que denotaremos por $o(\tau)$, tal que $P_2 =< \tau >$. Sabemos do Teorema 1.1.2 que toda permutação se decompõe como produto de ciclos disjuntos. Desde que $\tau\sigma_i = \sigma_j$ então τ é uma permutação dada por $\tau(i) = j$. Assim podemos escrevê-la como $\tau = c_1 \cdots c_r$, onde os c_i são ciclos disjuntos. De modo similar ao lema anterior, não temos pontos fixos nesta ação, então $\tau\sigma_i \neq \sigma_i$ e consequentemente $\tau(i) \neq i$, para $i = 1, \ldots, 2^n m$. Suponha que $c_j = (k_{1j} \cdots k_{tj})$, para todo $j = 1, \ldots, r$. Como $o(\tau) = 2^n$ temos como no resultado anterior que $o(c_j) = 2^n$, para $j = 1, \ldots, r$. Portanto, o Teorema 1.1.7 nos permite escrever $\epsilon(\tau) = \epsilon(c_1) \cdots \epsilon(c_r) = (-1)^r$. Por outro lado, $2^n m = t_1 + \ldots + t_r = r2^n$ então $r = m$, donde

$$\epsilon(\tau) = (-1)^r = (-1)^m = -1 \neq 1,$$

já que $ch(K) \neq 2$. Assim a função sinal é não trivial. □

1.2.2 Corpos finitos

Vamos relembrar alguns fatos básicos relacionados com corpos finitos os quais serão usados mais adiante.

Teorema 1.2.13. *Seja L um corpo finito de característica prima p. Então*

i) a cardinalidade de L é $|L| = p^n$, para algum primo p e algum $n \geqslant 1$ (Notação: $L = \mathbb{F}_{p^n}$).

ii) L é Galois sobre $\mathbb{F}_p$. ($\mathbb{F}_p$ significa $\mathbb{Z}_p$)

Dem.: Ver os Teoremas 20.1 e 20.3 nas páginas 227 e 228 de [St]. □

Corolário 1.2.14. *Se L é um corpo finito de característica p, então $L/\mathbb{F}_p$ é uma extensão de Galois, com grupo de Galois cíclico gerado pelo automorfismo de Frobenius σ dado por $\sigma(x) = x^p$, para qualquer $x \in L$.*

Dem.: Sabemos do teorema acima que $L/\mathbb{F}_p$ é Galois. Como $x^p = x$ para todo $x \in \mathbb{F}_p$, temos que $\mathbb{F}_p \subset L^{<\sigma>}$, isto é, $\mathbb{F}_p$ está contido no corpo fixo do subgrupo cíclico de $Aut_{\mathbb{F}_p}L$ gerado pelo automorfismo de Frobenius σ. Reciprocamente, cada elemento fixo por σ é uma raiz de $x^p - x$. Então $L^{<\sigma>}$ tem no máximo p elementos. Consequentemente, $\mathbb{F}_p = L^{<\sigma>}$ e $Gal(L/\mathbb{F}_p) =< \sigma >$. □

Esse resultado pode ser estendido ao caso em que o corpo base é "maior"que $\mathbb{F}_p$.

Corolário 1.2.15. *Seja L/F uma extensão de corpos finitos com $|L| = p^n$ e $|F| = p^m$. Então L/F é Galois e m divide n. Mais ainda, o grupo de Galois é cíclico, gerado pelo automorfismo $\tau = \sigma^m$, $\sigma^m(x) = x^{p^m}$, $x \in L$.*

Dem.: Ver o Teorema 4.26 na página 288 de [Ja]. □

1.2.3 Independência de caracteres

Nesta subseção apresentamos um resultado fundamental para o nosso trabalho.

Definição 1.2.16. *Um caracter de um grupo finito G em um corpo L é um homomorfismo $\sigma : G \to L^*$, onde $L^* = L - \{0\}$ é o grupo multiplicativo de L. Um conjunto $\{\sigma_1, \ldots, \sigma_n\}$ de caracteres de um grupo G em um corpo L é dito independente se não existem $a_1, \ldots, a_n \in L$, nem todos nulos, tal que $\sum_{i=1}^{n} a_i\sigma_i(x) = 0$, para todo $x \in G$.*

A seguir enunciamos e provamos o Lema de Dedekind.

Lema 1.2.17. *(Dedekind) Todo conjunto $\{\sigma_1, \ldots, \sigma_n\}$ de caracteres distintos de um grupo G em um corpo L é independente.*

Dem.: A prova é feita por indução sobre n:

Se $n = 1$, então $a_1\sigma_1(x) = 0$ implica que $a_1 = 0$, já que $\sigma_1(x)$ pertence a L^*.

Assuma verdadeiro para $n-1$, $n > 1$. Dado $a_1\sigma_1(x) + \ldots + a_{n-1}\sigma_1(x) = 0$, para todo $x \in G$, temos que $a_1 = \ldots = a_{n-1} = 0$. Agora suponha que

$$a_1\sigma_1(x) + \ldots + a_n\sigma_n(x) = 0, \tag{1.1}$$

para todo $x \in G$ e onde nem todos os a_i são nulos. Podemos assumir que todo $a_i \neq 0$, pois caso contrário o resultado segue da hipótese indutiva. Multiplicando por a_n^{-1}, se necessário, tomamos $a_n = 1$. Uma vez que $\sigma_n \neq \sigma_1$, existe $y \in G$ tal que $\sigma_n(y) \neq \sigma_1(y)$. Substituindo x por yx na equação (1.1), onde y é um elemento fixo temos:

$$a_1\sigma_1(y)\sigma_1(x) + \ldots + a_{n-1}\sigma_{n-1}(y)\sigma_{n-1}(x) + \sigma_n(y)\sigma_n(x) = 0.$$

Multiplicando-a por $\sigma_n(y)^{-1}$ obtemos $a_1\sigma_n(y)^{-1}\sigma_1(x) + \ldots + \sigma_n(x) = 0$, e subtraindo esta da eq. (1.1), vem que: $(a_n = 1)$

$$a_1[1 - \sigma_n(y)^{-1}\sigma_1(y)]\sigma_1(x) + \ldots + a_{n-1}[1 - \sigma_n(y)^{-1}\sigma_{n-1}(y)]\sigma_{n-1}(x) = 0,$$

uma equação de tamanho $n-1$, portanto todos os seus coeficientes são nulos. Visto que $a_1 \neq 0$, temos $\sigma_n(y)^{-1}\sigma_1(y) = 1$ e então $\sigma_n(y) = \sigma_1(y)$, uma contradição. Logo, o conjunto $\{\sigma_1, \ldots, \sigma_n\}$ é independente. □

O próximo corolário tratará especificamente dos automorfismos de um corpo, o que vem de encontro com nossos objetivos neste trabalho. Dada uma extensão de corpos L/K, denotamos por $Aut_K(L) := \{\sigma \in Aut(L) : \sigma(a) = a, \text{ para qualquer } a \in K\}$.

Corolário 1.2.18. *Seja L/K uma extensão de corpos. Então todo conjunto $\{\sigma_1, \ldots, \sigma_n\} \subseteq Aut_K(L)$ é independente.*

Dem.: Dado $\sigma \in Aut_K(L)$, notar que $\sigma\mid_{L^*}: L^* \to L^*$ é um homomorfismo do grupo $(L^*, .)$ no grupo multiplicativo de L. Como $\sigma \in Aut_K L$, temos $\sigma(0) = 0$. Dessa forma, $\sigma\mid_{L^*}$ é um caracter. Pelo Lema 1.2.17, dados $\{\sigma_1, \ldots, \sigma_n\} \subseteq Aut_K(L)$, não existem $a_1, \ldots, a_n \in L$, nem todos nulos, tais que $a_1\sigma_1(x) + \ldots + a_n\sigma_n(x) = 0$. Portanto o conjunto $\{\sigma_1, \ldots, \sigma_n\}$ é independente. □

1.2.4 Traço e norma Galois

Agora relembremos as noções de traço e norma de um extensão de Galois.

Tomando uma extensão de Galois L/K, com grupo de Galois G, definimos o *traço Galois*, $Tr : L \longrightarrow L$ por $Tr(x) = \sum_{\sigma \in G} \sigma(x)$. Observe que:

i) o traço Galois é não nulo, isto é, existe $x \in L$, $x \neq 0$ tal que $Tr(x) \neq 0$. De fato: suponha por absurdo que $Tr(x) = 0$ para todo $x \in L$, $x \neq 0$. Então $\sigma_1(x)+\ldots+\sigma_n(x) = 0$, para todo $x \in L$, $x \neq 0$ (estamos assumindo $G = \{\sigma_1, \ldots, \sigma_n\}$). Pelo Corolário 1.2.18, $1_L = 0$, o que é um absurdo.

ii) $Im\ Tr \subset K$: como L/K é Galois, temos que $K = L^G$. Dessa forma, para todo $\sigma \in G$ temos:

$$\begin{aligned} \sigma\left(Tr(x)\right) &= \sigma\left(\sum_{j=1}^{n} \sigma_j(x)\right) = \sigma\sigma_1(x) + \sigma\sigma_2(x) + \ldots + \sigma\sigma_n(x) \\ &= \sigma_1(x) + \sigma_2(x) + \ldots + \sigma_n(x) = \sum_{\sigma \in G} \sigma(x) = Tr(x). \end{aligned}$$

Portanto, $Tr(x) \in L^G = K$. Assim, $Im\ Tr \subset K$;

iii) O traço Galois é linear: é imediato verificar esta afirmação.

Por outro lado, se L/K é uma extensão de Galois e x é um elemento de L^*, definimos a *norma Galois* de x por $N(x) = \prod_{\sigma \in G} \sigma(x)$. Neste caso, temos:

i) se $x \in L^*$, então $N(x) \in K^*$: qualquer que seja $\tau \in G$,

$$\tau(N(x)) = \tau\left(\prod_{\sigma \in G} \sigma(x)\right) = \prod_{\sigma \in G} \tau\sigma(x) = \prod_{\sigma \in G} \sigma(x) = N(x).$$

Então, $N(x) \in L^G = K$.

ii) $N(xy) = N(x)N(y)$: de fato

$$N(xy) = \prod_{\sigma \in G} \sigma(xy) = \prod_{\sigma \in G} \sigma(x)\sigma(y) = \prod_{\sigma \in G} \sigma(x) \prod_{\sigma \in G} \sigma(y) = N(x)N(y),$$

para quaisquer $x,\ y \in L^*$;

iii) Se $\tau \in G$ e $x \in L^*$, então $N(\tau(x)) = N(x)$: o resultado segue de maneira análoga ao item i).

1.3 TÓPICOS DE ÁLGEBRA LINEAR

Visto que muitos de nossos objetivos neste trabalho serão relacionar ou descrever elementos da álgebra linear através da teoria de Galois, nesta seção traremos alguns tópicos desta área, bem como alguns exemplos e definições importantes.

1.3.1 Espaço dos endomorfismos

Sejam L, K corpos e L/K uma extensão de corpos. O conjunto dos K-endomorfismos $End_K(L) = \{\varphi : L \longrightarrow L : \varphi \text{ é transformação } K\text{-linear }\}$ (note que $\varphi \in End_K(L)$ se e somente se $\varphi(x+y) = \varphi(x) + \varphi(y)$ e $\varphi(\lambda x) = \lambda\varphi(x)$, para quaisquer $x, y \in L,\ \lambda \in K$) é um K-espaço vetorial com as seguintes operações: para quaisquer $\varphi, \psi \in End_K(L)$

- $(\varphi + \psi)(x) = \varphi(x) + \psi(x)$, $x \in L$
- $(\lambda\varphi)(x) = \lambda\varphi(x)$, $\lambda \in K$ e $x \in L$.

Perceba que o traço Galois, $Tr : L \longrightarrow L$, definido anteriormente é uma transformação K-linear. Portanto, um K-endomorfismo de L. Se $[L : K] = n$, então existe um isomorfismo de $End_K(L)$ com o espaço das matrizes $n \times n$ com entradas no corpo K, $M_{n\times n}(K)$. A saber,

$$\begin{array}{rcl} T : End_K(L) & \longrightarrow & M_{n\times n}(K) \\ \varphi & \mapsto & [\varphi]_\beta, \end{array}$$

onde $\beta = \{u_1, u_2, \ldots, u_n\}$ é um K-base ordenada de L,

$$[\varphi]_\beta = \begin{bmatrix} | & | & & | \\ [\varphi(u_1)]_\beta & [\varphi(u_2)]_\beta & \cdots & [\varphi(u_n)]_\beta \\ | & | & & | \end{bmatrix}$$

e $[\varphi(u_i)]_\beta = (\lambda_{1i}, \ldots, \lambda_{ni})$ se $\varphi(u_i) = \lambda_{1i}u_1 + \ldots + \lambda_{ni}u_n$. Ou seja, $[\varphi]_\beta$ é a matriz de φ na base β. Defina também,

$$\begin{array}{rcl} S : M_{n\times n}(K) & \longrightarrow & End_K(L) \\ A = (a_{ij}) & \longmapsto & S(A) : L \longrightarrow L, \end{array}$$

dada por: se $x \in L$, tome $y = A[x]_\beta = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ e $S(A)(x) = y_1u_1 + \ldots + y_nu_n \in L$. É fácil verificar que T é um isomorfismo de K-espaços vetoriais com inversa S. Além disso, $End_K(L)$ com a soma e a multiplicação (composição usual) é um anel associativo com unidade.

1.3.2 Traço de um operador linear

Sobre o espaço $M_{n\times n}(K)$ das matrizes $n \times n$ com entradas em K, considere a função traço $tr : M_{n\times n}(K) \longrightarrow K$ definida como $tr(A) = \sum_{i=1}^{n} a_{ii}$, onde $A = (a_{ij}) \in M_{n\times n}(K)$. Claramente, tr é um operador liner.

O traço tem as seguintes propriedades interessantes: dadas $A,\ B \in M_{n\times n}(K)$,

i)

$$\begin{aligned} tr(AB) &= \sum_{i=1}^{n}(ab)_{ii} = \sum_{i=1}^{n}\left(\sum_{k=1}^{n}(a_{ik})(b_{ki})\right) = \sum_{k=1}^{n}\left(\sum_{i=1}^{n}(a_{ik})(b_{ki})\right) \\ &= \sum_{k=1}^{n}\left(\sum_{i=1}^{n}(b_{ki})(a_{ik})\right) = \sum_{k=1}^{n}(ba)_{kk} = tr(BA), \end{aligned}$$

ii)

$$tr(UAU^{-1}) = tr(UU^{-1}A) = tr(A),\ U \in M_{n\times n}(K),$$

onde U é matriz inversível.

Dado um espaço vetorial V de dimensão finita e um operador linear $f : V \to V$, considere uma base β de V e defina $tr(f) = tr([f]_\beta)$. Dizemos que $tr(f)$ é o traço do operador f. Se γ é outra base de V e U é a matriz de mudança de base de γ para β então temos

$$[f]_\gamma = U[f]_\beta U^{-1}.$$

Pelo item ii) acima, segue que a definição de $tr(f)$ não depende da escolha da base de V.

No decorrer deste trabalho veremos como associar o traço definido acima com o traço Galois.

1.3.3 Formas bilineares

Sejam U e V espaços vetoriais sobre K. Uma forma bilinear é uma função $f : U \times V \longrightarrow K$ que é linear em cada uma das suas variáveis, ou seja:

i) $f(x + x', y) = f(x, y) + f(x', y)$,

ii) $f(x, y + y') = f(x, y) + f(x, y')$,

iii) $f(\lambda x, y) = \lambda f(x, y) = f(x, \lambda y)$,

para quaisquer $x,\ x' \in U,\ y,\ y' \in V$ e $\lambda \in K$.

Por exemplo, dados U e V espaços vetoriais reais, considere a função $f : U \times V \longrightarrow \mathbb{R}$, definida por: $f(u, v) = \varphi(u)\psi(v)$, onde $\varphi : U \longrightarrow \mathbb{R}$ e $\psi : V \longrightarrow \mathbb{R}$ são funcionais lineares. Tal função é uma forma bilinear chamada de *produto tensorial* das formas lineares φ e ψ, denotado por $\varphi \otimes \psi$.

Trabalharemos considerando as formas bilineares $f : L \times L \longrightarrow K$, onde L é um espaço vetorial de dimensão n sobre K. O conjunto de todas essas formas bilineares, que denotaremos por $Bil(L)$, é naturalmente um espaço vetorial sobre K, com as operações de soma e multiplicação por escalar usuais:

- $(f+g)(x,y) = f(x,y) + g(x,y)$,
- $(\lambda f)(x,y) = \lambda f(x,y)$,

para $f,\ g \in Bil(L),\ x,\ y \in L,\ \lambda \in K$.

Seja $\beta = \{u_1, u_2, \ldots, u_n\}$ uma base ordenada de L. Se $x,\ y \in L$ então $x = \alpha_1 u_1 + \ldots + \alpha_n u_n$ e $y = \delta_1 u_1 + \ldots + \delta_n u_n$. Tomando $f \in Bil(L)$, temos que

$$f(x,y) = f\left(\sum_{i=1}^{n} \alpha_i u_i, \sum_{j=1}^{n} \delta_j u_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{n} \alpha_i \delta_j (u_i, u_j).$$

Então, para cada $f \in Bil(L)$, definimos a matriz de f em relação à base ordenada β como $[f]_\beta = (a_{ij})$, onde $a_{ij} = f(u_i, u_j)$. Dessa forma, é possível definir $T : Bil(L) \to M_{n\times n}(K)$ tal que $T(f) = [f]_\beta$, para $f \in Bil(L)$. É fácil verificar que T é um isomorfismo entre espaços vetoriais. Assim, $dim_K Bil(L) = n^2$.

O conceito de matriz de uma forma bilinear em relação a uma base ordenada é semelhante ao conceito de matriz de um operador linear em relação a uma base ordenada. Dessa forma, o *posto* de uma forma bilinear sobre L pode ser definido como sendo o posto de qualquer matriz que represente a forma em relação a uma base ordenada de L. Dessa forma, o posto da forma bilinear f é igual a dimensão da imagem de f pela transformação linear T.

Lema 1.3.1. *O posto de uma forma bilinear é igual ao posto da matriz da forma bilinear em relação a qualquer base ordenada.*

Dem.: Ver o Corolário 1 na página 312 de [HK]. □

As formas bilineares podem ser classificadas em:

- *simétrica*: se $f(x,y) = f(y,x)$, para todo $x,\ y \in L$. Todo produto interno de um espaço vetorial V sobre $\mathbb{R}$ é uma forma bilinear simétrica, o que é uma consequência da própria definição de produto interno.
- *skew-simétrica* ou *antissimétrica*: se $f(x,y) = -f(y,x)$, para todo $x,\ y \in L$;
- *alternada*: se $f(x,x) = 0$, para todo $x \in L$;

Dados dois funcionais lineares $f, g : L \longrightarrow \mathbb{R}$, consideramos $(f \odot g)(x, y) = f(x)g(y) + f(y)g(x)$ e $(f \wedge g)(x, y) = f(x)g(y) - f(y)g(x)$, $x, y \in L$. Note que $f \odot g, f \wedge g : L \times L \longrightarrow \mathbb{R}$ são formas bilineares. Mais ainda $f \odot g$ é simétrica e $f \wedge g$ é antissimétrica e alternada.

Estaremos particularmente interessados em estudar as formas bilineares alternadas. Notemos que toda forma alternada é skew-simétrica. Com efeito, se $f(x + y, x + y) = 0$, temos $f(x + y, x) + f(x + y, y) = 0$. Então $f(x, x) + f(y, x) + f(x, y) + f(y, y) = 0$. Logo, $f(x, y) = -f(y, x)$, para todo $x,\ y \in L$. A recíproca é verdadeira apenas se $ch(K) \neq 2$.

Definimos ainda o conjunto $R(f) = \{x \in L : f(x, y) = 0,\ \text{para todo } y \in L\}$ como *radical* de um forma bilinear f .

De modo geral, podemos calcular o posto de uma forma bilinear observando a dimensão do radical desta forma.

Lema 1.3.2. *Se f é uma forma bilinear sobre um espaço vetorial L de dimensão finita e $R(f)$ é o radical dessa forma, então rank $f = dim\ L - dim\ R(f)$ (rank f = posto de f).*

Dem.: Ver páginas 346 e 347 de [Ja]. □

Dizemos ainda que uma forma bilinear f sobre L é *não degenerada* se $R(f) = \{0\}$.

Seja L/K um extensão de Galois e $G = Gal(L/K)$. Definimos

$$\begin{array}{rcl} f : L \times L & \longrightarrow & K \\ (x, y) & \mapsto & f(x, y) = Tr(xy), \end{array}$$

onde Tr é o traço Galois. Observe que f é uma forma bilinear não degenerada. Para verificar a não degeneração de f, basta usar o fato de que Tr é não nulo.

Teorema 1.3.3. *Seja f uma forma bilinear alternada sobre um espaço vetorial de dimensão finita L sobre K. Se L é não degenerada ($R(f) = 0$), a dimensão desse espaço é par.*

Dem.: Ver o Teorema 8.1 na página 586 de [L]. □

Capítulo 2

FORMAS BILINEARES ALTERNADAS COM PROPRIEDADES ESPECIAIS EM RELAÇÃO AO POSTO

Neste capítulo, dados um corpo K e uma extensão de Galois L/K de grau n, vamos trabalhar com as formas bilineares alternadas definidas em $L \times L$ com valores em K. Particularmente, estaremos interessados em suas propriedades com respeito ao posto. O principal resultado apresentado é uma decomposição em soma direta do espaço das formas bilineares alternadas da extensão L/K, no caso em que L/K é cíclica.

2.1 SUBESPAÇOS DE FORMAS BILINEARES ALTERNADAS

Nesta seção apresentamos algumas caracterizações das formas bilineares alternadas, bem como dos subespaços determinados pelas mesmas. Em especial, faremos um estudo acerca do posto destas formas e daremos uma decomposição do espaço que as contém.

Sejam K um corpo, L/K uma extensão de Galois de grau n e G o grupo de Galois de L sobre K. Considere K^* e L^* os grupos multiplicativos dos corpos K e L, respectivamente. Dado um elemento $b \in L^*$ e $\sigma \in G$, diferente da identidade de G, defina $f = f_{b,\sigma} : L \times L \longrightarrow K$ por

$$f(x, y) = Tr(b(x\sigma(y) - \sigma(x)y)), \tag{2.1}$$

para quaisquer $x, y \in L$. Observe que f é uma forma K-bilinear. De fato, para quaisquer

$x, x', y, y' \in L$ e $\lambda \in K$ temos:

$$\begin{aligned} f(x+x', y) &= Tr(b[(x+x')\sigma(y) - \sigma(x+x')y]) \\ &= Tr(b[x\sigma(y) + x'\sigma(y) - \sigma(x)y - \sigma(x')y]) \\ &= Tr(b[x\sigma(y) - \sigma(x)y]) + Tr(b[x'\sigma(y) - \sigma(x')y]) \\ &= f(x,y) + f(x',y), \end{aligned}$$

$$\begin{aligned} f(x, y+y') &= Tr(b[x\sigma(y+y') - \sigma(x)(y+y')]) \\ &= Tr(b[x\sigma(y) + x\sigma(y') - \sigma(x)y - \sigma(x)y']) \\ &= Tr(b[x\sigma(y) - \sigma(x)y]) + Tr(b[x\sigma(y') - \sigma(x)y']) \\ &= f(x,y) + f(x,y'), \end{aligned}$$

$$\begin{aligned} f(\lambda x, y) &= Tr(b[(\lambda x)\sigma(y) - \sigma(\lambda x)y]) \\ &= Tr(b[\lambda x\sigma(y) - \lambda\sigma(x)y]) \\ &= Tr(b[\lambda(x\sigma(y) - \sigma(x)y]) \\ &= \lambda Tr(b(x\sigma(y) - \sigma(x)y)) \\ &= \lambda f(x,y). \end{aligned}$$

De forma análoga, mostra-se que $f(x, \lambda y) = \lambda f(x,y)$. Mais ainda, para todo $x \in L$,

$$f(x,x) = Tr(b(x\sigma(x) - \sigma(x)x)) = Tr(0) = 0.$$

Portanto, f é uma forma bilinear alternada. E para $b = 0$, f é a forma nula.

No que segue, temos alguns exemplos de como são as formas bilineares alternadas f para algumas extensões de Galois.

Exemplo 2.1.1. *Seja a extensão $\mathbb{Q}[\sqrt{2}]/\mathbb{Q}$. Esta é uma extensão de Galois de grau 2 com grupo de Galois $G = \{id, \sigma\}$, onde $\sigma(\sqrt{2}) = -\sqrt{2}$. Além disso, $\beta = \{1, \sqrt{2}\}$ é base de $\mathbb{Q}[\sqrt{2}]$ como $\mathbb{Q}$-espaço vetorial. Assim, para um elemento não nulo $t = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, e para quaisquer elementos $u = x + y\sqrt{2}$ e $v = x' + y'\sqrt{2}$ também pertencentes a $\mathbb{Q}[\sqrt{2}]$, temos que as formas bilineares alternadas são:*

- $f_{t,id} \equiv 0$, *e*
- $f_{t,\sigma}(u,v) = 8b(x'y - xy')$.

Exemplo 2.1.2. *Considere* $\mathbb{Q}[\xi]/\mathbb{Q}$, *onde* $\xi = cos\left(\frac{2\pi}{3}\right) + isen\left(\frac{2\pi}{3}\right) = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$. *Esta também é uma extensão de Galois de grau 2 com grupo de Galois* $G = \{id, \sigma\}$, *onde* $\sigma(\xi) = \overline{\xi}$. *Ainda,* $\beta = \{1, \xi\}$ *é base de* $\mathbb{Q}[\xi]$ *como* $\mathbb{Q}$*-espaço vetorial. Neste caso, para um elemento não nulo* $t = a + b\xi \in \mathbb{Q}[\xi]$, *e para quaisquer* $u = x + y\xi, v = x' + y'\xi \in \mathbb{Q}[\xi]$ *obtemos:*

- $f_{t,id} \equiv 0$, *e*
- $f_{t,\sigma}(u, v) = 3b(xy' - x'y)$.

Exemplo 2.1.3. *Para a extensão de Galois de grau 4,* $L/\mathbb{Q}$, *onde* $L = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, *o grupo de Galois é dado por* $G = \{\sigma_1 = id, \sigma_2, \sigma_3, \sigma_4\}$, *onde:*

$$\begin{aligned}\sigma_2(\sqrt{2}) = -\sqrt{2} \text{ e } \sigma_2(\sqrt{3}) = \sqrt{3}\\ \sigma_3(\sqrt{2}) = \sqrt{2} \text{ e } \sigma_3(\sqrt{3}) = -\sqrt{3}\\ \sigma_4(\sqrt{2}) = -\sqrt{2} \text{ e } \sigma_4(\sqrt{3}) = -\sqrt{3}.\end{aligned}$$

Além disso, $\beta = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ *é base de* L *como* $\mathbb{Q}$*-espaço vetorial. Assim, para um elemento não nulo* $t = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in L$ *e para quaisquer* $u = x + y\sqrt{2} + z\sqrt{3} + w\sqrt{6}$ *e* $v = x' + y'\sqrt{2} + z'\sqrt{3} + w'\sqrt{6}$ *pertencentes a* L, *temos que:*

- $f_{t,id} \equiv 0$
- $f_{t,\sigma_2}(u, v) = 16[(-xy' + x'y - 3zw' + 3wz')b + (-3xw' + 3yz' - 3zy' + 3x'w)d]$,
- $f_{t,\sigma_3}(u, v) = 24[(zx' - xz' + 2wy' - 2yw')c + (2zy' + 2wx' - 2xw' - 2yz')d]$,
- $f_{t,\sigma_4}(u, v) = 8[(-2xy' + 2yx' + 6zw' - 6wz')b + (-3xz' + 6yw' + 3zx' - 6wy')c]$.

Exemplo 2.1.4. *Seja ainda* $L = \mathbb{Q}[\sqrt[3]{2}, \xi]$, *onde* $\xi = cos\left(\frac{2\pi}{3}\right) + isen\left(\frac{2\pi}{3}\right) = \frac{-1}{2} + \frac{\sqrt{3}}{2}i$ *e considere a extensão de Galois* $L/\mathbb{Q}[\xi]$. *Esta extensão tem grau 3 com grupo de Galois* $G = \{\sigma_1 = id, \sigma_2, \sigma_3 = \sigma_2^2\}$, *onde* $\sigma_2(\sqrt[3]{2}) = \sqrt[3]{2}\xi$. *E ainda* $\beta = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ *é base de* L *como* $\mathbb{Q}[\xi]$*-espaço vetorial. Assim, para um elemento não nulo* $t = a + b\sqrt[3]{2} + c\sqrt[3]{4} \in L$ *e para quaisquer* $u = x + y\sqrt[3]{2} + z\sqrt[3]{4}$ *e* $v = x' + y'\sqrt[3]{2} + z'\sqrt[3]{2}$ *também em* L, *vem que as formas bilineares alternadas são dadas por:*

- $f_{t,id} \equiv 0$,
- $f_{t,\sigma_2}(u, v) = f_{t,\sigma_3}(u, v) = 6b(zx' - xz') + 6c(yx' - xy')$.

Lema 2.1.5. *Seja $f = f_{b,\sigma}$ a forma bilinear alternada definida em* (2.1). *Então*

$$f(x,y) = Tr((\sigma^{-1}(bx) - b\sigma(x))y),$$

para quaisquer $x,\ y \in L$.

Dem.: Da linearidade do traço Galois Tr, vem que

$$f(x,y) = Tr(b(x\sigma(y) - \sigma(x)y)) = Tr(bx\sigma(y)) - Tr(b\sigma(x)y).$$

Pela forma como o traço Galois é definido, vimos na subseção 1.2.4 do Capítulo 1 que $Tr(z) = Tr(\tau(z))$ para quaisquer $z \in L$ e $\tau \in G$. Logo,

$$Tr(bx\sigma(y)) - Tr(b\sigma(x)y) = Tr(\sigma^{-1}(bx)y) - Tr(b\sigma(x)y) = Tr((\sigma^{-1}(bx) - b\sigma(x))y),$$

para quaisquer $x, y \in L$. □

Como visto na página 24 do capítulo anterior, a forma traço é não degenerada, o que implica a seguinte, e importante, consequência deste resultado.

Corolário 2.1.6. *Seja $x \in L$. Então x pertence ao radical de $f = f_{b,\sigma}$ se e somente se $\sigma^{-1}(bx) = b\sigma(x)$.*

Dem.: ($\Rightarrow$) Se x está no radical de $f = f_{b,\sigma}$, então $f(x,y) = 0$, para todo $y \in L$. Pelo Lema 2.1.5, $Tr((\sigma^{-1}(bx) - b\sigma(x))y) = 0$, para qualquer $y \in L$. Como Tr é não degenerado, devemos ter $\sigma^{-1}(bx) - b\sigma(x) = 0$. E assim, $\sigma^{-1}(bx) = b\sigma(x)$.
($\Leftarrow$) Se $\sigma^{-1}(bx) = b\sigma(x)$, temos $Tr((\sigma^{-1}(bx) - b\sigma(x))y) = 0$, para todo $y \in L$. Então, $f(x,y) = 0$ para qualquer $y \in L$. Dessa forma, x está no radical de $f = f_{b,\sigma}$. □

Agora apresentamos o primeiro resultado relacionado ao posto da forma bilinear f.

Lema 2.1.7. *Sejam $f = f_{b,\sigma}$ a forma bilinear alternada definida em* (2.1)*, com $b \neq 0$, e F o corpo fixo do automorfismo σ^2. Se $\sigma(b)b^{-1}$ é expresso na forma $\sigma^2(c)c^{-1}$ para algum $c \in L^*$, então*

$$rank\ f = n - [F:K] = n - \frac{n}{[L:F]}.$$

Caso contrário, f tem posto n e é, portanto, não degenerada.

Dem.: Seja $R = \{x \in L : f(x,y) = 0, \text{ para qualquer } y \in L\}$, isto é, R é o radical de f. Dado $x \in R$, pelo Corolário 2.1.6, temos que $\sigma^{-1}(bx) = b\sigma(x)$. Aplicando σ a essa igualdade, obtemos que $bx = \sigma(b)\sigma^2(x)$. Se x é não nulo, tomando $c = x^{-1}$, segue que $bc^{-1} = \sigma(b)\sigma^2(c^{-1})$. Assim, $\sigma(b)b^{-1} = \sigma^2(c)c^{-1}$. Portanto, se $R \neq \{0\}$ então $\sigma(b)b^{-1}$ sempre

pode ser expresso como $\sigma^2(c)c^{-1}$, para algum $c \in L^*$. Assim, se para algum $c \in L^*$, $\sigma(b)b^{-1}$ não pode ser expresso na forma $\sigma^2(c)c^{-1}$, então $R = \{0\}$. Logo $rank\ f = n$, ou seja, f é não degenerada. No restante desta demonstração, assumimos que existe $c \in L^*$ tal que $\sigma(b)b^{-1} = \sigma^2(c)c^{-1}$. Dado $x \in R$, $x \neq 0$, temos que $x\sigma(y) = \sigma(x)y$, para qualquer $y \in L$. Logo, $x^{-1}\sigma(y^{-1}) = \sigma(x^{-1})y^{-1}$, para qualquer $y \in L^*$. Desta forma, $x^{-1} \in R$. Pelos cálculos iniciais desta demonstração, trocando x por x^{-1}, obtemos $\sigma^2(c)c^{-1} = \sigma(b)b^{-1} = \sigma^2(x)x^{-1}$. Consequentemente, $x^{-1}c\sigma^2(x)\sigma^2(c)^{-1} = 1$. Então, $x = c\sigma^2(c^{-1}x)$, donde $\sigma^2(c^{-1}x) = c^{-1}x$. Assim $c^{-1}x \in F^*$. Logo, $x \in cF^*$ e portanto, $R \subseteq cF$. Observe também que $cF \subseteq R$. Se $x \in cF$, então x é escrito como $x = cy$, com $y \in F$. Para que x pertença ao radical é suficiente provar que $\sigma^{-1}(bx) = b\sigma(x)$. Note que $\sigma^{-1}(y) = \sigma(y)$ visto que $y \in F$. Também, como $c \in R$ temos pelo Corolário 2.1.6 que $\sigma^{-1}(bc) = b\sigma(c)$. Assim, $\sigma^{-1}(bx) = \sigma^{-1}(bcy) = \sigma^{-1}(bc)\sigma^{-1}(y) = b\sigma(c)\sigma(y) = b\sigma(cy) = b\sigma(x)$. Portanto, $x \in R$. Desde que $dim_K\ cF = dim_K\ F$, segue que, $dim_K\ R = dim_K\ F = [F : K]$. Dessa forma

$$rank\ f = n - [F : K] = n - \frac{n}{[L : F]},$$

visto que $[L : K] = [L : F].[F : K] = n$. □

Veremos a seguir que é possível obter uma fórmula simples para o posto de $f_{b,\sigma}$, quando σ tem ordem multiplicativa ímpar (e posteriormente quando esta é par).

Lema 2.1.8. *Nas mesmas notações do resultado anterior, suponha que* $o(\sigma) = 2r + 1 > 1$. *Se* $b \neq 0$, *então*

$$rank\ f = n - \frac{n}{2r + 1}.$$

Dem.: Seja $H =< \sigma >$. Sob a hipótese que $o(\sigma) = m = 2r+1$, vamos provar que $H =< \sigma^2 >$. De fato, se $(\sigma^2)^j = 1$ para algum $1 \leq j < m$, então $m = o(\sigma)$ divide $2j$. Logo, existe $t \in \mathbb{N}^*$ tal que $2j = mt$. Como $mdc(2, m) = 1$, segue que 2 divide t, isto é, existe $s \in \mathbb{N}^*$ tal que $t = 2s$. Assim, $j = ms$. Mas isso é um absurdo pois $j < m$. Portanto, o subgrupo gerado por σ^2 é igual ao subgrupo gerado por σ, que é o subgrupo H. Pelo Teorema 1.2.8, o corpo fixo por σ, denotado por F, também é o corpo fixo por σ^2. Seja $T_1 : L \longrightarrow F$ a forma traço da extensão L/F dada por

$$T_1(x) = \sum_{i=1}^{2r+1} \sigma_i(x),$$

para todo $x \in L$. Sejam ainda $\{\tau_1, \ldots, \tau_k\}$ um conjunto completo de representantes das classes laterais do subgrupo H em G e $T_2 : F \longrightarrow K$ a forma K-linear definida por

$$T_2(z) = \sum_{i=1}^{k} \tau_i(z),$$

para $z \in F$. Vejamos que T_2 está bem definida. Para tal note que dado $\gamma \in G$, temos que $\{\gamma\tau_1, \ldots, \gamma\tau_k\}$ também é um sistema completo de representantes das classes laterais de H em G. Segue que para qualquer $z \in F = L^H$,

$$\gamma(T_2(z)) = \sum_{i=1}^{k} \gamma\tau_i(z) = \sum_{l=1}^{k} \tau_l(z) = T_2(z).$$

Assim, $T_2(z) \in K$. E com esta notação, temos:

$$T_2(T_1(x)) = T_2\left(\sum_{h\in H} h(x)\right) = \sum_{i=1}^{k} \tau_i\left(\sum_{h\in H} h(x)\right) = \sum_{i=1}^{k}\sum_{h\in H} \tau_i h(x) = \sum_{\xi\in G} \xi(x) = Tr(x).$$

Considerando a extensão de Galois L/F, podemos definir a forma F-bilinear alternada $g : L \times L \longrightarrow F$ dada por

$$g(x, y) = T_1(b(x\sigma(y) - \sigma(x)y)),$$

para quaisquer $x,\ y \in L$. Portanto, $f(x, y) = T_2(g(x, y))$. Como L tem dimensão ímpar $2r+1$ (sobre F), sabemos do Teorema 1.3.3 que qualquer forma bilinear alternada $L \times L \longrightarrow F$ tem radical não nulo. Assim, existe $x \neq 0$ em L com $g(x, y) = 0$, para todo $y \in L$. Mas isso implica que x também está no radical de f, pois

$$f(x, y) = T_2(\underbrace{g(x, y)}_{0}) = T_2(0) = \sum_{i=1}^{k} \tau_i(0) = 0.$$

Portanto, f é degenerada. Além disso, o Lema 2.1.7 implica que

$$rank\ f = n - \frac{n}{[L : F]} = n - \frac{n}{2r + 1},$$

como queríamos demonstrar. □

Observe que no Exemplo 2.1.4, temos uma extensão $[\mathbb{Q}[\sqrt[3]{2}, \xi] : \mathbb{Q}[\xi]] = 3$ onde $o(\sigma_2) = o(\sigma_3) = 3$. As matrizes das formas bilineares definidas por estes automorfismos na base $\beta = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ para um elemento não nulo $t = a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{Q}[\sqrt[3]{2}, \xi]$ são dadas por:

$$[f_{t,\sigma_2}]_\beta = [f_{t,\sigma_3}]_\beta = 6\begin{bmatrix} 0 & -c & -b \\ c & 0 & 0 \\ b & 0 & 0 \end{bmatrix}.$$

Claramente a matriz dessas formas tem posto 2, que é o posto da forma bilinear que as define, estando portanto, de acordo com o lema anterior.

Quando σ tem ordem par também é possível obter uma fórmula para o posto de f. Neste caso, a situação descrita no lema anterior não é tão clara e nós precisaremos do seguinte resultado auxiliar.

Lema 2.1.9. *Suponha que o automorfismo σ tem ordem multiplicativa par, digamos $2r$. Então existem elementos $b \in L^*$ tal que a equação $\sigma^2(x)x^{-1} = \sigma(b)b^{-1}$ não tem solução para $x \in L^*$.*

Dem.: Considere F' o corpo fixo do automorfismo σ e suponha que K é finito. Como L/F' é uma extensão de grau par $2r$, se $|F'| = q$, então $|L| = q^{2r}$, onde q é uma potência de um número primo. Isso porque, se $|F'| = q$, $[L : F'] = 2r$ e $\{\alpha_1, \ldots, \alpha_{2r}\}$ é uma base de L sobre F', então todo $x \in L$ pode ser escrito como

$$x = x_1\alpha_1 + x_2\alpha_2 + \ldots + x_{2r}\alpha_{2r},\ x_i \in F'.$$

Como existem q escolhas para cada x_i, temos um total de q^{2r} possibilidades para os elementos de L. Além disso, de acordo com o Corolário 1.2.15 podemos assumir que $\tau : L \to L$ é dado por $\tau(x) = x^q$, uma potência do automorfismo de Frobenius. Suponha que $\sigma(b)b^{-1} = \sigma(d)d^{-1}$ para $b,\ d \in L^*$. Assim $b^q b^{-1} = d^q d^{-1}$, e então $(bd^{-1})^q = bd^{-1}$. Logo $bd^{-1} = \lambda \in F'$. Dessa forma, podemos escrever $b = \lambda d$ e como $b \neq 0$, segue que $\lambda \neq 0$. Portanto, temos que a quantidade de elementos da forma $\sigma(b)b^{-1}$ em L^* é $\dfrac{q^{2r}-1}{q-1}$. Agora considere F o corpo fixo do automorfismo σ^2 e note que $K \subseteq L^{<\sigma>} = F' \subseteq L^{<\sigma^2>} = F \subseteq L$. Além disso, como σ^2 tem ordem multiplicativa r vemos que $[L : F] = r$ e então $[F : F'] = 2$. Utilizando o mesmo argumento do início dessa demonstração concluímos que $|F| = q^2$. Assim se $\sigma^2(b)b^{-1} = \sigma^2(c)c^{-1}$ então $b^{q^2}b^{-1} = d^{q^2}d^{-1}$, donde $(bd^{-1})^{q^2} = bd^{-1}$. Logo, $bd^{-1} \in F$. Dessa forma, a quantidade de elementos na forma $\sigma^2(b)b^{-1}$ é $\dfrac{q^{2r}-1}{q^2-1}$. Desde que o número de elementos de uma forma é maior do que o número de elementos da outra, temos que existem elementos $b \in L^*$ tais que $\sigma(b)b^{-1}$ não é da forma $\sigma^2(c)c^{-1}$. Portanto, a equação $\sigma^2(x)x^{-1} = \sigma(b)b^{-1}$ não tem solução em L^*.

Suponha agora que K é infinito. Suponha também, por absurdo, que todo elemento $\sigma(b)b^{-1}$ pode ser expresso na forma $\sigma^2(c)c^{-1}$ para algum $c \in L^*$. Aplicando sucessivamente

σ^2 à essa igualdade, obtemos as seguintes equações:

$$\begin{aligned}
\sigma(b)b^{-1} &= \sigma^2(c)c^{-1} \\
\sigma^3(b)\sigma^2(b^{-1}) &= \sigma^4(c)\sigma^2(c^{-1}) \\
\sigma^5(b)\sigma^4(b^{-1}) &= \sigma^6(c)\sigma^4(c^{-1}) \\
&\vdots \\
\sigma^{2r-1}(b)\sigma^{2r-2}(b^{-1}) &= \sigma^{2r}(c)\sigma^{2r-2}(c^{-1}) = c\sigma^{2r-2}(c^{-1}).
\end{aligned}$$

Multiplicando-as lado a lado, temos $b^{-1}\sigma(b)\sigma^2(b^{-1})\sigma^3(b)\ldots\sigma^{2r-2}(b^{-1})\sigma^{2r-1}(b) = 1$. Então $\sigma(b)\sigma^3(b)\ldots\sigma^{2r-1}(b) = b\sigma^2(b)\ldots\sigma^{2r-2}(b)$. Dado $\alpha \in K$, trocando b por $\alpha - b$ nesta equação obtemos: $(\alpha-b)\sigma^2(\alpha-b)\ldots\sigma^{2r-2}(\alpha-b) = \sigma(\alpha-b)\ldots\sigma^{2r-1}(\alpha-b)$. Consequentemente, $(\alpha-b)(\alpha-\sigma^2(b))\ldots(\alpha-\sigma^{2r-2}(b)) = (\alpha-\sigma(b))\ldots(\alpha-\sigma^{2r-1}(b))$. Escolhemos um elemento $b \in L^*$ tal que os $2r$ conjugados de Galois $b, \sigma(b), \ldots, \sigma^{2r-1}(b)$ são todos distintos. Isso é possível já que segundo o Teorema da Base Normal (ver o Teorema 13.1 na página 312 de [L]) estes elementos formam uma base de L sobre K. Tome os seguintes polinômios em $L[t]$:

$$\begin{aligned}
q_1(t) &= (t-b)(t-\sigma^2(b))\ldots(t-\sigma^{2r-2}(b)) \\
q_2(t) &= (t-\sigma(b))(t-\sigma^3(b))\ldots(t-\sigma^{2r-1}(b)).
\end{aligned}$$

Assim, q_1 e q_2 não possuem raízes em comum. No entanto, mostramos que $q_1(t) = q_2(t)$ para todo $t \in K$. Como K é infinito, temos dois polinômios mônicos diferentes que coincidem em uma infinidade de pontos distintos, um absurdo. Portanto o resultado também é válido neste caso. □

Corolário 2.1.10. *Suponha que o automorfismo σ tem ordem multiplicativa par, digamos $2r > 2$. Então, como b percorre através dos elementos em L^*, a forma bilinear alternada $f_{b,\sigma}$ tem posto $n - \frac{n}{r}$ ou n. Exemplos de cada posto ocorrem para escolhas adequadas de b.*

Dem.: Do lema anterior, se σ tem ordem multiplicativa $2r$, existe $b \in L^*$ tal que $\sigma(b)b^{-1} \neq \sigma^2(c)c^{-1}$, para qualquer $c \in L^*$. Portanto, $\sigma(b)b^{-1}$ não pode ser escrito na forma $\sigma^2(c)c^{-1}$ para algum $c \in L^*$. Pelo Lema 2.1.7, $rank\ f = n$. Dessa forma, para algum $b \in L^*$ e $x = c^{-1}$, temos $\sigma^{-1}(bx) \neq b\sigma(x)$. Caso $\sigma(b)b^{-1} = \sigma^2(c)c^{-1}$, para algum $c \in L^*$, temos novamente do Lema 2.1.7 que

$$rank\ f = n - [F:K] = n - \frac{n}{[L:F]} = n - \frac{n}{r},$$

visto que $[L:F] = |<\sigma^2>| = r$. □

Observação 2.1.11. *No caso especial em que σ tem ordem 2, o Corolário 2.1.10 também é válido e implica que temos apenas duas possibilidades para os elementos $f_{b,\sigma}$: são nulos ou tem rank n. Note que no Exemplo 2.1.1 a matriz da forma $f = f_{t,\sigma}$ para um elemento não nulo $t = a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ na base $\beta = \{1, \sqrt{2}\}$ é dada por*

$$[f]_\beta = 8b \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

e no Exemplo 2.1.2 a matriz da forma $f = f_{t,\sigma}$ para um elemento não nulo $t = a + b\xi \in \mathbb{Q}[\xi]$ na base $\beta = \{1, \xi\}$ é

$$[f]_\beta = 3b \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Ambas matrizes têm posto igual a 2, que é o grau de suas respectivas extensões. Já os elementos $f = f_{t,id}$ em ambos os casos são nulos, portanto tem posto zero.

Já no caso do Exemplo 2.1.3, temos a extensão $\mathbb{Q}[\sqrt{2}, \sqrt{3}]/\mathbb{Q}$, onde os automorfismos de Galois diferentes da identidade, $\{\sigma_2, \sigma_3, \sigma_4\}$, tem todos ordem 2. Além disso, as matrizes das formas bilineares alternadas f para um elemento não nulo $t = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ na base $\beta = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ são dadas por:

$$[f_{t,\sigma_2}]_\beta = 16. \begin{bmatrix} 0 & -b & 0 & -3d \\ b & 0 & 3d & 0 \\ 0 & -3d & 0 & -3b \\ 3d & 0 & 3b & 0 \end{bmatrix}, [f_{t,\sigma_3}]_\beta = 24. \begin{bmatrix} 0 & 0 & -c & -2d \\ 0 & 0 & -2d & -2c \\ c & 2d & 0 & 0 \\ 2d & 2c & 0 & 0 \end{bmatrix} \quad e$$

$$[f_{t,\sigma_4}]_\beta = 8. \begin{bmatrix} 0 & -2b & -3c & 0 \\ 2b & 0 & 0 & 6c \\ 3c & 0 & 0 & 6b \\ 0 & -6c & -6b & 0 \end{bmatrix}.$$

Tais matrizes tem posto 0 ou 4, onde 4 é exatamente o grau dessa extensão. A forma $f_{t,\sigma_1=id}$ é a forma nula, que tem posto zero.

Definição 2.1.12. *Denote por $Alt(L)$ o conjunto de todas as formas bilineares alternadas de $L \times L$ com valores em K.*

É imediato verificar que $Alt(L)$ é um espaço vetorial sobre K com as operações usuais:

$$\begin{cases} (f+g)(x,y) &= f(x,y)+g(x,y) \\ (\lambda f)(x,y) &= \lambda f(x,y) \end{cases},$$

para quaisquer $f,\ g \in Alt(L),\ \lambda \in K$.

Vimos anteriormente na Subseção 1.3.3 do Capítulo 1 que o conjunto das formas bilineares $Bil(L)$ é um espaço vetorial de dimensão n^2 sobre K, já que o mesmo é isomorfo ao espaço $M_{n\times n}(K)$. Com isso, podemos estimar a dimensão de $Alt(L)$ (sobre K).

Lema 2.1.13. *$Alt(L)$ tem dimensão $\dfrac{n(n-1)}{2}$ como espaço vetorial sobre K.*

Dem.: Seja $\beta = \{u_1, u_2, \ldots, u_n\}$ uma base ordenada de L. E considere T' a restrição do isomorfismo T, da Subseção 1.3.3 do Capítulo 1, ao espaço $Alt(L)$. Ou seja, $T' : Alt(L) \to M_{n\times n}(K)$ tal que $T'(f) = [f]_\beta$, para $f \in Alt(L)$. É imediato verificar que T' é uma transformação linear injetora. Pelo teorema do núcleo e a da imagem temos

$$dim\ Alt(L) = dim\ Ker(T') + dim\ Im(T'),$$

e como toda forma bilinear alternada é antissimétrica segue que $dim\ Alt(L) = \dfrac{n(n-1)}{2}$. $\square$

Definição 2.1.14. *Seja σ um elemento diferente da identidade do grupo de Galois G. Considere $A^\sigma = \{f_{b,\sigma} : b \in L\}$.*

Note que A^σ é um subespaço de $Alt(L)$. De fato:

$$\begin{aligned}(f_{b,\sigma} + f_{c,\sigma})(x,y) &= f_{b,\sigma}(x,y) + f_{b,\sigma}(x,y) \\ &= Tr(b(x\sigma(y) - \sigma(x)y) + Tr(c(x\sigma(y) - \sigma(x)y) \\ &= Tr((b(x\sigma(y) - \sigma(x)y) + (c(x\sigma(y) - \sigma(x)y)) \\ &= Tr((b+c)(x\sigma(y) - \sigma(x)y) \\ &= f_{(b+c),\sigma}(x,y),\end{aligned}$$

$$\begin{aligned}\lambda f_{b,\sigma}(x,y) &= \lambda Tr(b(x\sigma(y)) - \sigma(x)y)) \\ &= Tr(\lambda b(x\sigma(y) - \sigma(x)y)) \\ &= f_{(\lambda b),\sigma}(x,y),\end{aligned}$$

para quaisquer $x,\ y,\ b,\ c \in L$ e $\lambda \in K$.

Dados $x,\ y \in L$ e $b \in L^*$, note também que:

$$\begin{aligned} f_{b,\sigma}(x,y) &= Tr(b(x\sigma(y) - \sigma(x)y)) \\ &= Tr(bx\sigma(y)) - Tr(by\sigma(x)) \\ &= Tr(\sigma^{-1}(bx)y) - Tr(\sigma^{-1}(by)x) \\ &= Tr(-\sigma^{-1}(b)(x\sigma^{-1}(y) - \sigma^{-1}(x)y) \\ &= f_{-\sigma^{-1}(b),\sigma^{-1}}(x,y). \end{aligned}$$

Portanto, $A^\sigma \subseteq A^{\sigma^{-1}}$. Analogamente, prova-se que $A^{\sigma^{-1}} \subseteq A^\sigma$. Dessa forma $A^\sigma = A^{\sigma^{-1}}$.

O próximo teorema fornece a dimensão de A^σ.

Teorema 2.1.15. *Seja σ um elemento diferente da identidade no grupo de Galois G, da extensão de Galois L/K. Então dim $A^\sigma = n$ ou dim $A^\sigma = n/2$, e este último ocorre exatamente quando a ordem de σ é 2.*

Dem.: Considere a função $\varphi : L \to A^\sigma$ dada por $\varphi(b) = f_{b,\sigma}$. Claramente φ é uma função K-linear e sobrejetora. Portanto, precisamos calcular o núcleo de φ. Suponha que $\varphi(b) = 0$. Pelo Corolário 2.1.6, $bx = \sigma(b)\sigma^2(x)$, para todo $x \in L$. Em particular, fazendo $x = 1$, obtemos $b = \sigma(b)$. Assim, se b é não nulo, devemos ter $\sigma^2(x) = x$, para todo $x \in L$. Portanto, σ tem ordem 2. Dessa forma, se σ não tem ordem 2, $f_{b,\sigma}$ é nula apenas quando b é nulo. Logo, se σ não tem ordem 2, então φ é injetora e segue que $dim\ A^\sigma = n$. Pelo que vimos acima, se $b \in Ker(\varphi)$, então $\sigma(b) = b$ e $o(\sigma) = 2$.

Reciprocamente, se σ tem ordem 2 e b é fixo por σ, então para qualquer $x \in L$ vale que $\sigma^{-1}(bx) = \sigma(bx) = \sigma(b)\sigma(x) = b\sigma(x)$. Assim qualquer $x \in L$ está no radical de f, ou seja, $f_{b,\sigma} = 0$. Logo, $b \in Ker(\varphi)$. Portanto, $b \in Ker(\varphi)$ se e somente se $\sigma(b) = b$ e $o(\sigma) = 2$. Assim, $n = dim_K\ L = dim_K\ Ker(\varphi) + dim_K\ A^\sigma = dim_K\ L^{<\sigma>} + dim_K\ A^\sigma = \dfrac{n}{2} + dim_K\ A^\sigma$. Logo, $dim_K\ A^\sigma = n - \dfrac{n}{2} = \dfrac{n}{2}$. □

Observação 2.1.16. *Quando σ tem ordem $2r+1$, os elementos não nulos de A^σ tem posto constante igual a $n - \dfrac{n}{2r+1}$. E quando σ tem ordem par $2r > 2$, os elementos não nulos de A^σ tem rank maximal n ou $n - \dfrac{n}{r}$. A^σ contém elementos de ambos os postos não nulos.*

Nosso próximo objetivo é provar que quando $[L : K]$ é ímpar, o espaço $Alt(L)$ se decompõe como uma soma direta de subespaços da forma A^σ. Primeiramente considere n um número ímpar, digamos $n = 2m + 1$, e enumere os elementos do grupo Galois G da seguinte forma: $1,\ \sigma_1,\ \sigma_1^{-1}, \ldots,\ \sigma_m,\ \sigma_m^{-1}$. Escreva A^i para representar A^{σ_i}, ou seja,

$A^i = \{f_{b,\sigma_i} : b \in L\}$. Seja L^m o conjunto das m-uplas ordenadas $(x_1, \ldots, x_m)$ de elementos de L. Claramente L^m é um espaço vetorial sobre K, com as operações usuais de adição e multiplicação por escalar, e $dim_K\ L^m = m.dim_K\ L = m.n = \left(\frac{n-1}{2}\right).n = \frac{n(n-1)}{2}$.

Teorema 2.1.17. *Suponha que $n = [L : K]$ é ímpar, $n > 1$ e $m = \frac{n-1}{2}$. Enumere os elementos de G na forma $\{1,\ \sigma_1,\ \sigma_1^{-1}, \ldots,\ \sigma_m,\ \sigma_m^{-1}\}$. Defina ainda a função K-linear $\phi : L^m \longrightarrow Alt(L)$ por $\phi(b_1, \ldots, b_m) = \sum_{i=1}^m f_{b_i,\sigma_i}$. Então ϕ é um isomorfismo de K-espaços vetoriais.*

Dem.: Como L^m e $Alt(L)$ são espaços vetoriais de mesma dimensão $\frac{n(n-1)}{2}$ sobre K, é suficiente mostrar que a função ϕ é injetiva. Ou seja, que se $\phi(b_1, \ldots, b_m) = 0$, então $b_1 = \ldots = b_m = 0$. Para tanto, suponha que $\phi(b_1, \ldots, b_m)(x, y) = \sum_{i=1}^m f_{b_i,\sigma_i}(x, y) = 0$, para quaisquer que sejam $x,\ y \in L$. Então

$$\begin{aligned}
0 &= \sum_{i=1}^m Tr(b_i(x\sigma_i(y) - \sigma_i(x)y)) = \sum_{i=1}^m Tr(b_i x\sigma_i(y)) - Tr(b_i\sigma_i(x)y) \\
&= \sum_{i=1}^m Tr(\sigma_i^{-1}(b_i x)y) - Tr(b_i\sigma_i(x)y)) = \sum_{i=1}^m Tr((\sigma_i^{-1}(b_i x) - (b_i\sigma_i(x))y) \\
&= Tr\left[\left(\sum_{i=1}^m (\sigma_i^{-1}(b_i x) - (b_i\sigma_i(x)\right)y\right],\ \text{para todo } y \in L.
\end{aligned}$$

Como o traço Galois é não degenerado, temos que $\sum_{i=1}^m \sigma_i^{-1}(b_i x) - b_i\sigma_i(x) = 0$. Dessa forma, $\sum_{i=1}^m \sigma_i^{-1}(b_i)\sigma_i^{-1} - b_i\sigma_i = 0$. Visto que tais automorfismos são todos distintos, o Corolário 1.2.18 implica que $b_1 = \ldots = b_m = 0$. □

Usando o teorema anterior obtemos uma decomposição de $Alt(L)$ como soma direta dos subespaços A^i.

Corolário 2.1.18. *Suponha que $n = [L : K]$ é ímpar e fixe $m = \frac{n-1}{2}$. Então existe uma decomposição em soma direta*

$$Alt(L) = A^1 \oplus \ldots \oplus A^m,$$

onde cada subespaço A^i tem dimensão n. Se A^i é definido pelo automorfismo σ_i ou seu inverso, e se σ_i tem ordem $2r_i + 1$, então todos os elementos não nulos de A^i tem posto igual a $n - \frac{n}{2r_i + 1}$.

Dem.: Pelo teorema anterior, os elementos de $Alt(L)$ são escritos de forma única como a soma de elementos da forma $f_{b_i,\sigma_i} \in A^i$, para $1 \leq i \leq m$. Então existe a decomposição

$Alt(L) = A^1 \oplus \ldots \oplus A^m$. Pelo Teorema 2.1.15, $dim\ A^i = n$ para todo $1 \leq i \leq m$. Se σ_i tem ordem $2r_i + 1$, então pelo Lema 2.1.8 f_{b,σ_i} tem posto $n - \dfrac{n}{2r_i + 1}$, para todo $b \in L^*$. $\square$

Estabelecemos agora um análogo ao Corolário 2.1.18 para extensões de Galois de grau par.

Teorema 2.1.19. *Suponha que $n = [L : K]$ é par e o grupo de Galois de L/K contém exatamante k elementos de ordem 2, digamos $\tau_1, \ldots, \tau_k$. Seja F_i o corpo fixo de τ_i para $1 \leq i \leq k$. Enumere os elementos restantes de G, diferentes da identidade, como $\{\sigma_1,\ \sigma_1^{-1}, \ldots,\ \sigma_m,\ \sigma_m^{-1}\}$, onde $1 + k + 2m = n$ visto que os elementos de ordem 2 são iguais ao seu inverso. E defina a função K-linear $\phi : L^{k+m} \longrightarrow Alt(L)$ por*

$$\phi(b_1, \ldots, b_k, c_1, \ldots, c_m) = \sum_{i=1}^{k} f_{b_i,\tau_i} + \sum_{j=1}^{m} f_{c_j,\sigma_j}.$$

Então ϕ leva L^{k+m} em $Alt(L)$ e o núcleo de ϕ, cuja dimensão é $\dfrac{kn}{2}$, consiste de todos os elementos da forma $(b_1, ..., b_k, 0, ..., 0)$, onde $b_i \in F_i,\ 1 \leq i \leq k$.

Dem.: Suponha que o elemento $(b_1, \ldots, b_k, c_1, \ldots, c_m)$ pertença ao núcleo de ϕ. Então $\left[\sum_{i=1}^{k} f_{b_i,\tau_i} + \sum_{j=1}^{m} f_{c_j,\sigma_j}\right](x, y) = 0$ para quaisquer $x, y \in L$. Dessa forma,

$$\begin{aligned}
0 &= \sum_{i=1}^{k} f_{b_i,\tau_i}(x, y) + \sum_{j=1}^{m} f_{c_j,\sigma_j}(x, y) \\
&= \sum_{i=1}^{k} Tr((\tau_i^{-1}(b_i x) - b_i\tau_i(x))y) + \sum_{j=1}^{m} Tr((\sigma_j^{-1}(c_j x) - c_j\sigma_j(x))y) \\
&= Tr\left[\sum_{i=1}^{k}(\tau_i^{-1}(b_i x) - b_i\tau_i(x))y + \sum_{j=1}^{m}(\sigma_j^{-1}(c_j x) - c_j\sigma_j(x))y\right] \\
&= Tr\left[\left(\sum_{i=1}^{k}\tau_i^{-1}(b_i x) - b_i\tau_i(x) + \sum_{j=1}^{m}\sigma_j^{-1}(c_j x) - c_j\sigma_j(x)\right)y\right], \text{ para todo } y \in L \\
&= \sum_{i=1}^{k}\tau_i^{-1}(b_i x) - b_i\tau_i(x) + \sum_{j=1}^{m}\sigma_j^{-1}(c_j x) - c_j\sigma_j(x) \\
&= \sum_{i=1}^{k}(\tau_i(b_i) - b_i)\tau_i(x) + \sum_{j=1}^{m}\sigma_j^{-1}(c_j)\sigma_j^{-1}(x) + \sum_{j=1}^{m} -c_j\sigma_j(x).
\end{aligned}$$

Como estes elementos são automorfismos de G, temos do Corolário 1.2.18 que $c_j = 0$ para todo $1 \leq j \leq m$. Ainda, temos que $\tau_i(b_i) = b_i$, ou seja, $b_i \in F_i$ para todo $1 \leq i \leq k$. Note que $F_i = L^{<\tau_i>}$ e como $\tau_i^2 = 1$ vem que $[L : F_i] = 2$. Portanto temos $n = [L : K] = [L :$

$F_i][F_i : K] = 2[F_i : K]$, ou seja, $[F_i : K] = \frac{n}{2}$, para qualquer $1 \leq i \leq k$. Dessa forma, temos que a dimensão do núcleo é $\frac{kn}{2}$. Além disso, visto que

$$dim\ L^{k+m} - dim\ ker\ \phi = (k+m)n - \frac{kn}{2} = \frac{2kn + 2mn - kn}{2}$$

$$= \frac{kn + (n-k-1)n}{2} = \frac{n(n-1)}{2} = dim\ Alt(L),$$

segue que ϕ é sobrejetiva. □

Como consequência dos resultados vistos temos o corolário seguinte, que descreve $Alt(L)$ mais precisamente como soma direta de subespaços B^i e A^j, o primeiro definido pela involução τ_i e o segundo pelo automorfismo σ_j.

Corolário 2.1.20. *Assuma as hipóteses e a notação do Teorema 2.1.19. Então existe uma decomposição em soma direta*

$$Alt(L) = B^1 \oplus \ldots \oplus B^k \oplus A^1 \oplus \ldots \oplus A^m,$$

onde, dim $B^i = \frac{n}{2}$, $1 \leq i \leq k$ *e dim* $A^j = n$, $1 \leq j \leq m$. *O subespaço* B^i *é definido pela involução* τ_i *e todos os seus elementos não nulos tem posto* n, *para* $1 \leq i \leq k$. A^j *é definido pelo automorfismo* σ_j *ou seu inverso, para* $1 \leq j \leq m$, *e o posto de cada elemento em* A^j *é dado de acordo com os resultados do Lema 2.1.8 e do Corolário 2.1.10.*

Note que no caso do Exemplo 2.1.3, a extensão $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ tem ordem 4, e seus elementos diferentes da identidade tem todos ordem 2. Então existe uma decomposição em soma direta $Alt(L) = B^2 \oplus B^3 \oplus B^4$, onde B^i é definido pelo automorfismo σ_i e $dim\ B^i = 2$, para $i = 2, 3, 4$. Ainda, os seus elementos não nulos tem todos posto 4.

2.2 EXTENSÕES CÍCLICAS

Nesta seção, analisaremos situações similares à seção anterior, considerando o caso em que o grupo de Galois G é cíclico. Seja L/K uma extensão de Galois cíclica cujo grau é n e suponha que σ gera o grupo de Galois G de L sobre K.

Inicialmente daremos, com o teorema que segue, uma maneira de determinar quando os elementos de L são linearmente dependentes sobre K.

Teorema 2.2.1. *Seja* L/K *uma extensão de Galois cíclica de grau* n, *e suponha que* σ *gera o grupo de Galois de* L *sobre* K. *Sejam* k *um inteiro satisfazendo* $1 \leq k \leq n$ *e*

$x_1, \ldots, x_k$ elementos de L. Então $x_1, \ldots, x_k$ é um conjunto linearmente dependente sobre K se e somente se

$$det\ S = 0,$$

onde S é a matriz $k \times k$ cuja entrada (i, j) é

$$\sigma^{i-1}(x_j), \quad 1 \leq i, j \leq k.$$

Dem.: ($\Rightarrow$) Note que:

$$S = \begin{bmatrix} x_1 & x_2 & \cdots & x_k \\ \sigma(x_1) & \sigma(x_2) & \cdots & \sigma(x_k) \\ \vdots & \vdots & & \vdots \\ \sigma^{k-1}(x_1) & \sigma^{k-1}(x_2) & \cdots & \sigma^{k-1}(x_k) \end{bmatrix}.$$

Suponha que os elementos $x_1, \ldots, x_k$ são linearmente dependentes sobre K. Então existem $a_1, \ldots, a_k \in K$, não todos nulos, tais que $a_1x_1 + \ldots + a_kx_k = 0$. Aplicando as potências de σ à esta equação, obtemos o seguinte sistema linear homogêneo:

$$\begin{cases} a_1x_1 + \ldots + a_kx_k = 0 \\ a_1\sigma(x_1) + \ldots + a_k\sigma(x_k) = 0 \\ \vdots \\ a_1\sigma^{k-1}(x_1) + \ldots + a_k\sigma^{k-1}(x_k) = 0 \end{cases}.$$

Temos assim, um sistema homogêneo de k equações lineares, com coeficientes dados exatamente pela matriz S. Este possui solução não trivial pois nem todos os $a_i's$ são nulos. Portanto, $det\ S = 0$.

($\Leftarrow$) Suponha agora que $det\ S = 0$. Faremos a prova por indução sobre k.

- Se $k = 1$ então $S = [x_1]$ e consequentemente $0 = det\ S = x_1$, onde $x_1 = 0$ é um conjunto linearmente dependente.

- Suponha $k > 1$. Podemos também supor que $x_1 \neq 0$, pois caso contrário $x_1, \ldots, x_k$ é, trivialmente, linearmente dependente. Defina os elementos $z_1, \ldots, z_k \in L$ como $z_1 = 1$ e $z_i = x_1^{-1}x_i$ para $2 \leq i \leq k$. Multiplicamos todas as entradas da i-ésima linha de S por $\sigma^{i-1}(x_1)^{-1}$, para $1 \leq i \leq k$, e obtemos a matriz:

$$T = \begin{bmatrix} 1 & x_1^{-1}x_2 & \cdots & x_1^{-1}x_k \\ 1 & \sigma(x_1^{-1}x_2) & \cdots & \sigma(x_1^{-1}x_k) \\ \vdots & \vdots & & \vdots \\ 1 & \sigma^{k-1}(x_1^{-1}x_2) & \cdots & \sigma^{k-1}(x_1^{-1}x_k) \end{bmatrix} = \begin{bmatrix} 1 & z_2 & \cdots & z_k \\ 1 & \sigma(z_2) & \cdots & \sigma(z_k) \\ \vdots & \vdots & & \vdots \\ 1 & \sigma^{k-1}(z_2) & \cdots & \sigma^{k-1}(z_k) \end{bmatrix}.$$

Note que $det\ T = x_1^{-1}\sigma(x_1)^{-1}\ldots\ \sigma^{k-1}(x_1)^{-1} det\ S = 0$. Subtraindo sucessivamente a linha $k-1$ de T da linha k, a linha $k-2$ de T da linha $k-1$, e assim por diante, obtemos a matriz:

$$U = \begin{bmatrix} 1 & z_2 & \cdots & z_k \\ 0 & \sigma(z_2) - z_2 & \cdots & \sigma(z_k) - z_k \\ \vdots & \vdots & & \vdots \\ 0 & \sigma^{k-1}(z_2) - \sigma^{k-2}(z_2) & \cdots & \sigma^{k-1}(z_k) - \sigma^{k-2}(z_k) \end{bmatrix}.$$

Claramente $det\ U = 0$, pois a matriz U é obtida através de combinações lineares das linhas da matriz T. Considere ainda a matriz $(k-1)\times(k-1)$,

$$V = \begin{bmatrix} \sigma(z_2) - z_2 & \cdots & \sigma(z_k) - z_k \\ \vdots & & \vdots \\ \sigma^{k-1}(z_2) - \sigma^{k-2}(z_2) & \cdots & \sigma^{k-1}(z_k) - \sigma^{k-2}(z_k) \end{bmatrix},$$

obtida apagando a primeira linha e a primeira coluna de U. Expandindo $det\ U$ ao longo da primeira coluna de U vemos que, $det\ V = det\ U = 0$. Note também que a entrada (i,j) de V é $\sigma^i(z_{j+1}) - \sigma^{i-1}(z_{j+1}),\ 1 \leq i,\ j \leq k-1$.

Fixemos $y_j = \sigma(z_{j+1}) - z_{j+1}$, e observe que a entrada (i,j) de V é $\sigma^{i-1}(y_j)$, pois $\sigma^i(z_{j+1}) - \sigma^{i-1}(z_{j+1}) = \sigma^{i-1}(\sigma(z_{j+1}) - z_{j+1}) = \sigma^{i-1}(y_j)$. Assim temos que

$$V = \begin{bmatrix} y_1 & y_2 & \cdots & y_{k-1} \\ \sigma^2(y_1) & \sigma^2(y_2) & \cdots & \sigma^2(y_{k-1}) \\ \vdots & \vdots & & \vdots \\ \sigma^{k-2}(y_1) & \sigma^{k-2}(y_2) & \cdots & \sigma^{k-2}(y_{k-1}) \end{bmatrix}.$$

Dado que $det\ V = 0$, aplicando a hipótese indutiva aos elementos $y_1, \ldots, y_{k-1}$, vemos que estes são linearmente dependentes sobre K. Assim, existem elementos $b_1, \ldots, b_{k-1} \in K$, não todos nulos, tais que $b_1y_1 + \ldots + b_{k-1}y_{k-1} = 0$. Trocando os elementos y_j por $\sigma(z_{j+1}) - z_{j+1}$ obtemos a equação $\sigma(b_1z_2 + \ldots + b_{k-1}z_k) = b_1z_2 + \ldots + b_{k-1}z_k$. Logo σ fixa $b_1z_2 + \ldots + b_{k-1}z_k$. Portanto, $b_1z_2 + \ldots + b_{k-1}z_k \in K$. Então existe $b_k \in K$ tal que $b_1z_2 + \ldots + b_{k-1}z_k = b_k$. Desta forma, $x_1^{-1}(-b_kx_1 + b_1x_2 + \ldots + b_{k-1}x_k) = 0$. Consequentemente temos $-b_kx_1 + b_1x_2 + \ldots + b_{k-1}x_k = 0$, onde nem todos os $b_i's$ são nulos.

Portanto, $\{x_1, \ldots, x_k\}$ é um conjunto linearmente dependente sobre K. □

Nosso próposito agora é encontrar uma decomposição para o espaço $Alt(L)$ (como soma direta de certos subespaços) no caso de extensões de Galois cíclicas. Dados $b_0, b_1, \ldots, b_k \in L$ considere o polinômio $w(t) = \sum_{i=0}^{k} b_i t^i \in L[t]$. Considere ainda $w(\sigma) : L \longrightarrow L$ dado por $w(\sigma)x = \sum_{i=0}^{k} b_i \sigma^i(x)$. Observe que $w(\sigma)$ é uma transformação K-linear e consequentemente $R = \{x \in L : \ w(\sigma)(x) = 0\}$ é um subespaço vetorial de L. A dimensão deste subespaço pode ser estimada usando o Teorema 2.2.2.

Teorema 2.2.2. *Seja L/K uma extensão de Galois cíclica de grau n e suponha que σ gera o grupo de Galois de L sobre K. Sejam k um inteiro satisfazendo $1 \leq k \leq n$ e w um polinômio de grau k em $L[t]$. Se $R = \{x \in L : \ w(\sigma)(x) = 0\}$, então dim $R \leq k$.*

Dem.: Suponha, por absurdo, que *dim* $R > k$. Tome $x_1, \ldots, x_{k+1}$ elementos de R que são linearmente independentes sobre K. Suponha ainda que $w = \sum_{i=0}^{k} b_i t^i$, com $b_0, b_1, \ldots, b_k \in L$. Como w tem grau k, vem que $b_k \neq 0$. Note que, $0 = w(\sigma)(x_i) = b_0 x_i + b_1 \sigma(x_i) + \ldots + b_k \sigma^k(x_i)$ para todo $1 \leq i \leq k+1$. Temos então um sistema linear homogêneo de $k+1$ equações lineares com coficientes dados pela matriz $A_{(k+1)\times(k+1)}$, cuja entrada (i,j) é $\sigma^{j-1}(x_i)$, para $1 \leq i, \ j \leq k+1$. Explicitamente, a matriz dos coeficientes do sistema linear é dada por:

$$A = \begin{bmatrix} x_1 & \sigma(x_1) & \cdots & \sigma^k(x_1) \\ x_2 & \sigma(x_2) & \cdots & \sigma^k(x_2) \\ \vdots & \vdots & & \vdots \\ x_{k+1} & \sigma(x_{k+1}) & \cdots & \sigma^k(x_{k+1}) \end{bmatrix}.$$

Como $b_k \neq 0$, segue que este sistema linear homogêneo possui solução não trivial. Logo *det* $A = 0$. Então *det* $A^T = 0$, onde A^T é a matriz transposta de A. Mas A^T é um matriz na forma do Teorema 2.2.1, o que implica que $x_1, \ldots, x_{k+1}$ são linearmente dependentes sobre K. Isso nos dá uma contradição. Portanto, concluímos que *dim* $R \leq k$. □

O próximo resultado mostra que qualquer subespaço R-dimensional de L é da forma descrita no Teorema 2.2.2.

Corolário 2.2.3. *Seja L/K uma extensão de Galois, cíclica e de grau n, e suponha que σ gera o grupo de Galois de L sobre K. Sejam k um inteiro satisfazendo $1 \leq k \leq n$ e U um subespaço de L de dimensão k. Então existe um polinômio w, de grau k, em $L[t]$ tal que $U = \{x \in L : \ w(\sigma)x = 0\}$.*

Dem.: Sejam $\{u_1, \ldots, u_k\}$ uma base de U sobre K e S a matriz $k \times k$ do Teorema 2.2.1, isto é, a (i,j) entrada de S é $\sigma^{i-1}(u_j)$. Pelo Teorema 2.2.1, *det* $S \neq 0$. Logo S é inversível e consequentemente S^T também o é. Seja v o vetor coluna $k \times 1$ cuja i-ésima entrada é $\sigma^k(u_i)$, $1 \leq i \leq k$. Desde que S^T é inversível, existe um único vetor coluna u tal que $S^T u = v$. Se a i-ésima entrada de u é b_i, $0 \leq i \leq k-1$, então temos

$$\begin{bmatrix} u_1 & \sigma(u_1) & \cdots & \sigma^{k-1}(u_1) \\ u_2 & \sigma(u_2) & \cdots & \sigma^{k-1}(u_2) \\ \vdots & \vdots & & \vdots \\ u_k & \sigma(u_k) & \cdots & \sigma^{k-1}(u_k) \end{bmatrix} \cdot \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{k-1} \end{bmatrix} = \begin{bmatrix} \sigma^k(u_1) \\ \sigma^k(u_2) \\ \vdots \\ \sigma^k(u_k) \end{bmatrix}.$$

.

Assim,

$$\sigma^k(u_i) = b_0u_i + b_1\sigma(u_i) + \ldots + b_{k-1}\sigma^{k-1}(u_i),$$

para todo $1 \leq i \leq k$. Tome $w \in L[t]$ dado por $w = t^k - b_{k-1}t^{k-1} - \ldots - b_1t - b_0$. Então, $w(\sigma)(u_i) = 0$ para todo $i = 1, \ldots, k$. Logo, $w(\sigma)(u) = 0$, para todo $u \in U$. Dessa forma, $U = \{u \in L : \ w(\sigma)(u) = 0\}$. □

Sigamos com a hipótese que L/K é uma extensão de Galois cíclica de grau n e que o grupo de Galois G é gerado por σ. Suponha também que $n = 2m + 1$ é um inteiro ímpar. Enumeremos os elementos do grupo de Galois G na forma: $G = \{1, \ \sigma, \ \sigma^{-1}, \ldots, \ \sigma^m, \ \sigma^{-m}\}$. Como anteriormente, os subespaços A^i de $Alt(L)$ são dados por $A^i = \{f_{b,\sigma^i} : \ b \in L\}$, para $1 \leq i \leq m$.

Teorema 2.2.4. *Seja L/K uma extensão de Galois cíclica e de grau ímpar, $n = 2m + 1$, e suponha que σ gera o grupo de Galois de L sobre K. Defina os subespaços A^i de $Alt(L)$ como acima para $1 \leq i \leq m$. Então para qualquer inteiro k satisfazendo $1 \leq k \leq m$, todos os elementos não nulos do subespaço nk-dimensional*

$$A^1 \oplus \ldots \oplus A^k$$

de $Alt(L)$ tem posto de, no mínimo, $n - 2k + 1$.

Dem.: Seja $g \in A^1 \oplus \ldots \oplus A^k$. Então existem $b_1, \ldots, b_k \in L$ tais que $g = \sum_{i=1}^k f_{b_i,\sigma i}$. Sejam R o radical de g e $x \in R$. Então temos $\sum_{i=1}^k Tr(b_i(x\sigma^i(y) - \sigma^i(x)y)) = 0$, para todo $y \in L$. Usando a mesma argumentação utilizada na demonstração do Teorema 2.1.17 obtemos $\sum_{i=1}^k \sigma^{-i}(b_ix) - b_i\sigma^i(x) = 0$. Aplicando σ^k à ambos os termos dessa igualdade, vem que $\sum_{i=1}^k \sigma^{k-i}(b_ix) - \sigma^k(b_i)\sigma^{i+k}(x) = 0$. Assim, $w(\sigma)x = 0$, onde $w \in L[t]$ é o polinômio $\sum_{i=1}^k \sigma^{k-i}(b_i)t^{k-i} - \sigma^k(b_i)t^{i+k}$. Visto que w tem grau no máximo $2k$, o Teorema 2.2.2 implica que $dim\ R \leq 2k$. Porém, não podemos ter $dim\ R = 2k$, pois L tem dimensão ímpar sobre K. Dessa forma, devemos ter $dim\ R \leq 2k - 1$, ou seja, o radical de g tem posto no máximo de $2k - 1$. Já que g tem posto $n - dim\ R$, segue que posto de g é no mínimo $n - 2k + 1$. □

No caso do Exemplo 2.1.4 temos um extensão cíclica de grau 3. Neste caso todos os elementos do subespaço 3-dimensional A^1 de $Alt(L)$ tem posto mínimo igual a 2.

Temos uma versão análoga ao Teorema 2.2.4 para extensões de grau par.

Teorema 2.2.5. *Seja L/K uma extensão de Galois cíclica e de grau par, $2m+2$, e suponha que σ gera o grupo de Galois de L sobre K. Enumerando os elementos de G como*

$$1, \sigma, \sigma^{-1}, \ldots, \sigma^m, \sigma^{-m}, \sigma^{m+1},$$

defina os subespaços A^i de $Alt(L)$ como previamente para $1 \leq i \leq m+1$. Então para qualquer inteiro k satisfazendo $1 \leq k \leq m$, todos os elementos não nulos do subespaço nk-dimensional

$$A^1 \oplus \ldots \oplus A^k$$

de $Alt(L)$ tem posto, no mínimo, $n - 2k$.

Dem.: Análoga à demonstração do Teorema 2.2.4 □

Observe que nos Exemplos 2.1.1 e 2.1.2, os elementos do grupo de Galois são apenas 1 e σ. Então teremos apenas um subespaço A^1 na decomposição de $Alt(L)$ e os elementos deste tem posto 0 ou 2, como visto na Observação 2.1.11.

Capítulo 3

ENDOMORFISMOS DE POSTO 1 PARA UMA EXTENSÃO DE GALOIS

Neste capítulo, considere L/K uma extensão de Galois de grau finito n, e seja G o grupo de Galois de L sobre K. Como já visto, podemos considerar L como um espaço vetorial de dimensão n sobre K. Nosso principal objetivo é explorar algumas consequências da identificação de $End_K(L)$ com o conjunto das combinações K-lineares de elementos de G. Em boa parte deste capítulo, consideraremos os endomorfismos de posto 1 e suas caracterizações. Além disso, trabalharemos com a função traço, determinantes associados à hiperplanos e alguns endomorfismos específicos no caso em que a extensão L/K é cíclica.

3.1 ENDOMORFISMOS DE L E AUTOMORFISMOS DE GALOIS

Nesta seção, analisaremos os automorfismos de Galois como endomorfismos K-lineares de L e traremos uma forma de expressar, de maneira única, cada elemento de $End_K(L)$. O conjunto $End_K(L)$, como já vimos no primeiro capítulo, é um espaço vetorial sobre K e um anel associativo com unidade. Além disso, $End_K(L)$ é uma álgebra com as seguintes operações:

- $(\varphi + \psi)(x) = \varphi(x) + \psi(x)$;
- $(\varphi \circ \psi)(x) = \varphi(\psi(x))$;
- $(\lambda\varphi)(x) = \lambda\varphi(x)$;

para quaisquer $\varphi, \psi \in End_K(L),\ \lambda \in K,\ x \in L$.

Como $End_K(L)$ é naturalmente um espaço vetorial de dimensão n^2 sobre K, podemos identificá-lo com a álgebra das matrizes $n \times n$ com entradas em K. Seja $G = \{\sigma_1, \ldots, \sigma_n\}$ o grupo de Galois de L sobre K e assuma que σ_1 é o elemento identidade deste grupo. Como já visto, $G = Aut_K(L) \subseteq End_K(L)$. Considere $\lambda_1, \ldots, \lambda_n \in L$. Definimos a função $\tau : L \longrightarrow L$ dada por $\tau(x) = \lambda_1\sigma_1(x) + \ldots + \lambda_n\sigma_n(x)$, para qualquer $x \in L$. Claramente $\tau \in End_K(L)$.

Mostraremos, em nosso primeiro resultado neste capítulo, que todo elemento de $End_K(L)$ é escrito (de forma única) como combinação de elementos $\sigma_1, \ldots, \sigma_n \in G$.

Teorema 3.1.1. *Seja $\tau \in End_K(L)$. Então existem únicos $\lambda_1, \ldots, \lambda_n \in L$ tais que $\tau = \lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n$.*

Dem.: Seja $E = \{\lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n : \lambda_j \in L\} \subseteq End_K(L)$ o conjunto de todos os endomorfismos escritos como "combinação linear"de elementos de G.
Afirmação 1: E é K-subespaço vetorial de $End_K(L)$. De fato, dados $\tau,\ \tau' \in E$ e $\lambda \in K$ temos que τ e τ' são escritos nas formas $\tau = \lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n$ e $\tau' = \lambda'_1\sigma_1 + \ldots + \lambda'_n\sigma_n$, para $\lambda_j,\ \lambda'_j \in L$ e $1 \leq j \leq n$. Então, $\tau+\tau' = (\lambda_1\sigma_1+\ldots+\lambda_n\sigma_n)+(\lambda'_1\sigma_1+\ldots+\lambda'_n\sigma_n) = (\lambda_1+\lambda'_1)\sigma_1+\ldots+(\lambda_n+\lambda'_n)\sigma_n \in E$. Ainda, $\lambda\tau = \lambda(\lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n) = (\lambda\lambda_1)\sigma_1 + \ldots + (\lambda\lambda_n)\sigma_n$, também pertence a E. Note que $dim_K(End_K\ L) = (dim_K\ L)^2 = n^2$, já que $End_K(L) \cong M_{n\times n}(K)$, onde $n = [L : K] = |G|$.
Afirmação 2: $dim_K\ E = n^2$. Com efeito, seja $\{u_1, \ldots, u_n\}$ base de L sobre K. Considere $C = \{u_i\sigma_j : i, j = 1, \ldots, n\} \subseteq E$. Suponha que $u_i\sigma_j = u_k\sigma_l$, então $u_i\sigma_j(x) = u_k\sigma_l(x)$ para qualquer $x \in L$. Em particular, tomando $x = 1$ temos que $u_i\sigma_j(1) = u_k\sigma_l(1)$. Daí, $u_i = u_k$ visto que σ_j e σ_l são automorfismos de corpos. Logo, $\sigma_j = \sigma_l$. Portanto, C tem n^2 elementos.Por fim, provemos que C é um conjunto K-linearmente independente. Suponha que $\sum_{i,j=1}^{n} \alpha_{ij}u_i\sigma_j = 0,\ \alpha_{ij} \in K$. Tome $\lambda_j = \sum_{i=1}^{n} \alpha_{ij}u_i$, para cada $1 \leq j \leq n$. Então

$$0 = \sum_{j=1}^{n} \left(\sum_{i=1}^{n} \alpha_{ij}u_i \right) \sigma_j = \sum_{j=1}^{n} \lambda_j\sigma_j.$$

Pelo Corolário 1.2.18 temos que $\lambda_j = 0$ para todo $j = 1, \ldots, n$. Como $\{u_1, \ldots, u_n\}$ é uma K-base de L e $0 = \lambda_j = \sum_{i=1}^{n} \alpha_{ij}u_i$, segue que $\alpha_{ij} = 0$ para todo $i = 1, \ldots, n$. Portanto C é um conjunto linearmente independente.

Das Afirmações 1 e 2 segue que cada elemento de $End_K(L)$ é uma combinação linear de elementos de G. Falta verificar a unicidade. Para isso, suponha que $\tau = \lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n$ e $\tau = \lambda'_1\sigma_1 + \ldots + \lambda'_n\sigma_n$, onde $\tau \in End_K(L)$. Então $0 = \sum_{i=1}^{n}(\lambda_i - \lambda'_i)\sigma_i$. Assim, do Corolário 1.2.18 temos $\lambda_i = \lambda'_i$ para todo $i = 1, \ldots, n$. □

3.2 ENDOMORFISMOS DE POSTO UNITÁRIO E FUNÇÕES TRAÇO

Com a intenção de relacionar o traço usual de endomorfismos com o traço Galois, nesta seção trabalharemos com K-hiperplanos, principalmente o hiperplano traço zero. Além disso, vamos caracterizar e relacionar os endomorfismos de posto 1.

Seja U um K-subespaço de L. O subconjunto, digamos W, de todos os elementos $\tau \in End_K(L)$ que satisfazem $\tau(U) = 0$ é um subespaço de $End_K(L)$. Se $dim_K\ L = n$ e $dim_K\ U = m$, então W tem dimensão $n(n - dim_K\ U)$. De fato, considere $\{u_1, \ldots, u_m\}$ base de U sobre K, complete esta base para uma base $\beta = \{u_1, \ldots, u_m, u_{m+1}, \ldots, u_n\}$ de L sobre K. Sabemos que $W = \{\tau \in End_K(L) : \tau(x) = 0, \text{ para todo } x \in U\}$. Então tome a transformação K-linear

$$\begin{array}{rcl} R : W & \longrightarrow & M_{n\times n}(K) \\ \tau & \longmapsto & R(\tau) = \begin{bmatrix} | & & | \\ [\tau(u_1)]_\beta & \cdots & [\tau(u_n)]_\beta \\ | & & | \end{bmatrix}. \end{array}$$

Claramente, R é uma transformação linear injetora. Além disso,

$$Im(R) = \left\{ \begin{bmatrix} | & | & & | & | & & | \\ 0 & 0 & \cdots & 0 & [\tau(u_{m+1})]_\beta & \cdots & [\tau(u_n)]_\beta \\ | & | & & | & | & & | \end{bmatrix} \in M_{n\times n}(K) :\ \tau \in W \right\}.$$

Assim, $dim_K\ Im(R) = n(n-m)$. Pelo teorema do núcleo e da imagem, segue que $dim_K\ W = dim_K\ Im(R) = n(n-m)$.

Seja $\varphi : L \longrightarrow L$ tal que $\varphi|_U = 0$, então pelo teorema do núcleo e da imagem

$$n = dim_K\ L = dim_K\ Ker(\varphi) + dim_K\ Im(\varphi).$$

Como $\varphi|_U = 0$, temos que $U \subseteq Ker(\varphi)$ e portanto $dim_K\ Ker(\varphi) \geq dim_K\ U$. Então $dim_K\ Im(\varphi)$ pode ser, no máximo, $n - dim_K\ U$. Assim, endomorfismos de W tem posto no máximo $n - dim_K\ U$.

Para nossos próximos resultados, lembremos que um *K-hiperplano* em L é um K-subespaço de L de dimensão $n - 1$.

Lema 3.2.1. *Seja H um K-hiperplano em L. Então todo K-hiperplano em L tem a forma $a^{-1}H$, para algum elemento não nulo $a \in L$.*

Dem.: Seja L^* o espaço dual de L, isto é, o espaço vetorial dos funcionais K-lineares de L.
Afirmação: Cada K-hiperplano é o núcleo de um elemento não nulo de L^*. De fato, seja U um K-subespaço de L tal que $dim_K\ U = n-1$. Então existe $\{u_1, \ldots, u_{n-1}\} \subseteq U$, K-base de U, e podemos completá-la para $\{u_1, \ldots, u_{n-1}, u\} \subseteq L$, uma base de L. Defina, $\varphi : L \longrightarrow L$ por $\varphi(u_i) = 0$, $i = 1, \ldots, n-1$ e $\varphi(u) = 1$. Se $z \in L$, então z é escrito de forma única como $z = \lambda_1 u_1 + \ldots + \lambda_{n-1}u_{n-1} + \lambda u$, para $\lambda,\ \lambda_1,\ \ldots,\ \lambda_{n-1} \in K$. Então $\varphi(z) = \lambda$. Logo, $z \in U$ se e somente se $z \in Ker(\varphi)$.
Pela afirmação acima, exite $g \in L^*$ tal que $H = Ker\ g$. Dado $a \in L$, definimos $g^a : L \to K$ por $g^a(x) = g(ax)$, para qualquer $x \in L$. É imediato verificar que $g^a \in L^*$. Além disso, $\alpha : L \to L^*$ dada por $\alpha(a) = g^a$ é uma transformação K-linear. Vejamos que α é uma transformação K-linear injetora. Suponha que $a \in Ker(\alpha)$. Então $\alpha(a) = 0$, isto é, $g^a(x) = 0$ para qualquer $x \in L$. Assim, $g(ax) = 0$ para qualquer $x \in L$. Logo, $aL = L \subseteq Ker(g) = H$. Portanto, $H = L$ e isso contradiz o fato que $dim_K\ H = dim_K\ L - 1$. Desde que $dim_K\ L = dim_K\ L^*$, e α é injetora, concluímos pelo teorema do núcleo e da imagem que α é um isomorfismo.

Finalmente, sabemos que $Ker(g^a) = \{x \in L :\ g^a(x) = 0\}$. Assim, se $x \in Ker(g^a)$ temos $g^a(x) = 0$, ou seja, $g(ax) = 0$ e então $ax \in Ker(g) = H$. Assim, $x = a^{-1}h$ e $x \in a^{-1}H$, o que implica $Ker(g^a) \subseteq a^{-1}H$. Por outro lado, se $x \in a^{-1}H$, temos $x = a^{-1}h$, para algum $h \in H$. Então $g^a(x) = g^a(a^{-1}h) = g(aa^{-1}h) = g(h) = 0$, já que $h \in H = Ker(g)$. Assim $a^{-1}H \subseteq Ker(g^a)$. Logo, $Ker(g^a) = a^{-1}Ker(g) = a^{-1}H$. Desde que cada K-hiperplano é o núcleo de um elemento não nulo de L^*, o resultado segue. □

Quando consideramos K-hiperplanos em L, o principal exemplo é o hiperplano *traço zero*, que é o núcleo do traço Galois $Tr = Tr_K^L \in L^*$, definido por

$$Tr(x) = \sum_{i=1}^{n} \sigma_i(x),\ x \in L.$$

Como visto no Capítulo 1, $Tr \in L^*$ e não é identicamente nulo. Assim, existe $x \in L$ tal que $Tr(x) = \alpha \in K,\ \alpha \neq 0$. Então, $Tr(\alpha^{-1}x) = \alpha^{-1}Tr(x) = \alpha^{-1}\alpha = 1$. Chamando $\alpha^{-1}x = y$ temos que para todo $\beta \in K,\ Tr(\beta y) = \beta Tr(y) = \beta$. Dessa forma, Tr é sobrejetora e pelo teorema do núcleo e imagem

$$n = dim_K\ L \ \ = \ \ dim_K\ Ker(Tr) + dim_K\ Im(Tr) = dim_K\ Ker(Tr) + 1$$

Logo, $Ker(Tr)$ é um subespaço de L de dimensão $n-1$, definindo portanto, o hiperplano traço zero que denotaremos por H_0. Ao considerarmos o elemento $\pi = \sigma_1 + \ldots + \sigma_n \in End_K(L)$,

temos que $H_0 = Ker(\pi)$.

Observação 3.2.2. *Quando nos referirmos ao funcional traço como um elemento de $End_K(L)$, usaremos a notação π ao invés de Tr.*

Suponhamos agora que H seja algum outro K-hiperplano em L. Pelo Lema 3.2.1, H é da forma $H = a^{-1}H_0$, para algum elemento não nulo $a \in L$. Nosso próximo resultado descreve quais elementos em $End_K(L)$ anulam H.

Lema 3.2.3. *Suponha que $H = a^{-1}H_0$, para algum $a \in L$. Então o elemento $\pi_a \in End_K(L)$, dado por $\pi_a = \sigma_1(a)\sigma_1 + \ldots + \sigma_n(a)\sigma_n$, anula H.*

Dem.: Se $h \in H$, então $h = a^{-1}h_0$ para algum $h_0 \in H_0$. Logo,

$$\begin{aligned} \pi_a(h) &= \pi_a(a^{-1}h_0) = \sigma_1(a)\sigma_1(a^{-1}h_0) + \ldots + \sigma_n(a)\sigma_n(a^{-1}h_0) \\ &= \sigma_1(aa^{-1}h_0) + \ldots + \sigma_n(aa^{-1}h_0) = \sigma_1(h_0) + \ldots + \sigma_n(h_0) \\ &= \pi(h_0) = 0 \end{aligned}$$

□

Seja $W = \{\varphi \in End_K(L) : \varphi(H) = 0\}$, onde $H = a^{-1}H_0$ é um K-hiperplano. Então $dim_K\ W = n(n - dim_K\ H) = n(n - (n-1)) = n$. Denote por $\widehat{W}$ o subespaço de W dado por $\widehat{W} = \{b\pi_a :\ b \in L\}$.

Afirmação: $dim(\widehat{W}) = n$. De fato, vamos verificar se $\{u_1, \ldots, u_n\}$ é uma base de L sobre K então $\{u_1\pi_a, \ldots, u_n\pi_a\}$ é uma K-base de $\widehat{W}$. Suponha que $\sum_{i=1}^{n} \lambda_i u_i \pi_a = 0$, com $\lambda_1, \ldots, \lambda_n \in K$. Note que $\pi_a \neq 0$. Com efeito, $\pi_a(1_K) = Tr(a) \neq 0$, pois $a \notin H_0$. Consequentemente, $\sum_{i=1}^{n} \lambda_i u_i = 0$. Mas $\{u_1, \ldots, u_n\}$ é K-base de L. Assim, $\lambda_1 = 0 = \ldots = \lambda_n$. Portanto, $dim\ \widehat{W} \geq n$ e $dim\ \widehat{W} \leq dim\ W = n$. Logo, $dim\ \widehat{W} = n$ e $\{u_1\pi_a, \ldots, u_n\pi_a\}$ é K-base de $\widehat{W}$. Pela afirmação acima $\widehat{W} = W$. Desta forma, $\varphi \in End_K(L)$ e $dim_K\ Im(\varphi) = 1$ (φ tem posto 1), então $Ker(\varphi) = a^{-1}H_0$ para algum $a \in L$ e $\varphi = \lambda\pi_a$ para algum $\lambda \in L$. Temos então provado o seguinte resultado.

Teorema 3.2.4. *Os elementos de posto 1 em $End_K(L)$ são precisamente aqueles da forma*

$$\lambda\pi_a = \lambda\sigma_1(a)\sigma_1 + \ldots + \lambda\sigma_n(a)\sigma_n,$$

onde λ e a são elementos não nulos de L.

Note que se $\varphi, \psi \in End_K(L)$ são endomorfismos de posto 1 então $\psi \circ \varphi = 0$ ou $\psi \circ \varphi$ tem posto 1. De fato, $Im(\psi \circ \varphi) \subseteq Im(\psi)$ e consequentemente $dim_K\ Im(\psi \circ \varphi) = 0$ ou 1. Podemos determinar uma fórmula para esse produto a partir da forma como representamos tais elementos.

Teorema 3.2.5. *Sejam λ, μ, a e b elementos não nulos de L, e $\lambda\pi_a$, $\mu\pi_b$ seus correspondentes elementos de posto unitário em $End_K(L)$. Então $(\lambda\pi_a)(\mu\pi_b) = \lambda Tr(a\mu)\pi_b$. Assim o produto é nulo se e somente se $Tr(a\mu) = 0$, e $\mu\pi_b$ é um idempotente quando $Tr(b\mu) = 1$.*

Dem.: O produto destes elementos, de acordo com a definição, é dado por

$$(\lambda\pi_a)(\mu\pi_b) = \left(\sum_{\sigma\in G} \lambda\sigma(a)\sigma\right)\left(\sum_{\tau\in G} \mu\tau(b)\tau\right) = \sum_{\sigma,\tau\in G} \lambda\sigma(a)\sigma(\mu)\sigma\tau(b)\sigma\tau.$$

Fixando um elemento ρ em G, vemos que o coeficiente de ρ no produto acima é

$$\sum_{\sigma\in G} \lambda\sigma(a)\sigma(\mu)\rho(b) = \sum_{\sigma\in G} \lambda\sigma(a\mu)\rho(b) = \lambda Tr(a\mu)\rho(b).$$

Isso nos mostra que $(\lambda\pi_a)(\mu\pi_b) = \lambda Tr(a\mu)\pi_b$. Além disso, $(\lambda\pi_a)(\mu\pi_b) = \lambda Tr(a\mu)\pi_b = 0$ se e somente se $Tr(a\mu) = 0$. Com efeito, suponha que o produto é zero. Como λ é não nulo, $Tr(a\mu) \neq 0$ então $\pi_b = 0$. Logo $\tau_1(b)\tau_1 + \ldots + \tau_n(b)\tau_n = 0$. Pelo Corolário 1.2.18, $\tau_1(b) = \ldots = \tau_n(b) = 0$. Mas como algum τ_i é a identidade, temos $b = 0$, o que é uma contradição. Portanto, devemos ter $Tr(a\mu) = 0$. A recíproca é verdadeira de forma imediata. Por fim, para que $\mu\pi_b$ seja um idempotente, devemos ter $(\mu\pi_b)(\mu\pi_b) = \mu\pi_b$, isto é, $\mu Tr(b\mu)\pi_b = \mu\pi_b$. Para tal, devemos ter $Tr(b\mu) = 1$. □

Considere τ um elemento de $End_K(L)$, e seja $tr(\tau)$ o traço usual de τ como definido no Capítulo 1. Suponha que τ tenha posto 1 e sejam, $\{u_1, \ldots, u_{n-1}\}$ e $\{u_1, \ldots, u_{n-1}, u\}$ bases de $Ker(\tau)$ e de L, respectivamente. Então, $\tau(u_i) = 0$, $i = 1, \ldots, n-1$ e $\tau(u) \neq 0$, onde $\tau(u)$ gera $Im(\tau)$. Logo, $\{\tau(u)\}$ é base de $Im(\tau)$. Note que como $\tau(u_i) = 0$ para $i = 1, \ldots, n-1$, supondo que $\tau(u) = t_1u_1 + \ldots + t_{n-1}u_{n-1} + tu$, temos que:

$$[\tau] = \begin{bmatrix} 0 & 0 & & t_1 \\ 0 & 0 & & t_2 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & & t_{n-1} \\ 0 & 0 & & t \end{bmatrix}.$$

Então $tr(\tau) = t$. Também, note que $\tau^2(u) = t.\tau(u)$. Portanto, $\tau^2(u) = tr(\tau)\tau(u)$. Dado $x = \sum_{i=1}^{n} \lambda_i u_i \in L$ $(u_n = u)$ temos que:

$$\tau(x) = \sum_{i=1}^{n} \lambda_i \tau(u_i) = \lambda_n \tau(u).$$

Se $\tau(x) \neq 0$, então $\lambda_n \neq 0$ e assim

$$\tau^2(x) = \lambda_n \tau^2(u) = \lambda_n tr(\tau)\tau(u) = \lambda_n tr(\tau)\lambda_n^{-1}\tau(x) = tr(\tau)\tau(x).$$

Se $\tau(x) = 0$, então trivialmente temos $\tau^2(x) = tr(\tau)\tau(x)$. Portanto, vale a identidade $\tau^2 = tr(\tau)\tau$ para qualquer $\tau \in End_K(L)$ que possui posto 1:

Dessa forma, tomando $\lambda\pi_a = \mu\pi_b$ no Teorema 3.2.5, obtemos o seguinte resultado sobre o traço de um endomorfismo qualquer de posto 1.

Corolário 3.2.6. *Sejam λ e a elementos não nulos de L, e $\lambda\pi_a$ o elemento correspondente de posto 1 em $End_K(L)$. Então $tr(\lambda\pi_a) = Tr(\lambda a)$.*

Dem.: Pelo que vimos acima, se $\tau = \lambda\pi_a \in End_K(L)$ então $\tau^2 = tr(\tau)\tau$. Assim, pelo Teorema 3.2.5, $\lambda Tr(a\lambda)\pi_a = (\lambda\pi_a)(\lambda\pi_a) = tr(\lambda\pi_a)\lambda\pi_a$. Consequentemente, $Tr(a\lambda) = tr(\lambda\pi_a)$. □

Este corolário é de grande importância, pois através dele estabelecemos uma relação entre o traço usual e o traço da teoria de Galois. Mais adiante complementaremos esta informação, mostrando que qualquer endormorfismo pode ser expresso como uma combinação L-linear de elementos de posto 1 da forma π_a. Mas para tal, necessitamos de mais alguns resultados.

Lema 3.2.7. *Seja $\{u_1, \ldots, u_n\}$ uma K-base de L. Então a matriz $B_{n\times n}$, cuja entrada b_{ij} é $\sigma_j(u_i)$, é inversível. Onde os σ_j são os automorfismos de Galois para $1 \leq j \leq n$.*

Dem.: Por hipótese,

$$B = \begin{bmatrix} \sigma_1(u_1) & \sigma_2(u_1) & \cdots & \sigma_n(u_1) \\ \sigma_1(u_2) & \sigma_2(u_2) & \cdots & \sigma_n(u_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(u_n) & \sigma_2(u_n) & \cdots & \sigma_n(u_n) \end{bmatrix}.$$

Suponha, por absurdo, que B não é inversível. Então existem escalares $\lambda_1, \ldots, \lambda_n$ em L, não todos nulos, de forma que

$$\lambda_1\sigma_1(u_i) + \ldots + \lambda_n\sigma_n(u_i) = 0, \tag{3.1}$$

para todo $i \in \{1, \ldots, n\}$, visto que as colunas de B são linearmente dependentes. Seja x um elemento qualquer de L. Podemos escrever $x = \mu_1 u_1 + \ldots + \mu_n u_n$, para únicos elementos $\mu_1, \ldots, \mu_n$ em K. Multiplicando a equação (3.1) por μ_i, $1 \leq i \leq n$, e somando as n equações obtidas, temos:

$$\begin{aligned} 0 &= \sum_{i=1}^{n} \mu_i\lambda_1\sigma_1(u_i) + \ldots + \mu_i\lambda_n\sigma_n(u_i) \\ &= \sum_{i=1}^{n} \lambda_1\sigma_1(\mu_i u_i) + \ldots + \lambda_n\sigma_n(\mu_i u_i) \\ &= \lambda_1\sigma_1(x) + \ldots + \lambda_n\sigma_n(x). \end{aligned}$$

Portanto $\lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n = 0$. Pelo Corolário 1.2.18 $\lambda_1 = \ldots = \lambda_n = 0$ contradizendo nossa suposição. Logo, B é inversível. □

Agora dada uma K-base $\{u_1, \ldots, u_n\}$ de L, considere $\pi_i = \sigma_1(u_i)\sigma_1 + \ldots + \sigma_n(u_i)\sigma_n$, para $1 \leq i \leq n$. Note que $\pi_i = \pi_{u_i}$.

Lema 3.2.8. *Sejam $\{u_1, \ldots, u_n\}$ uma K-base para L, π_i elementos de $End_K(L)$ como definido acima para $1 \leq i \leq n$, e τ um elemento qualquer de $End_K(L)$. Então existem únicos elementos $\mu_1, \ldots, \mu_n \in L$ tais que $\tau = \mu_1\pi_1 + \ldots + \mu_n\pi_n$.*

Dem.: Como $\tau \in End_K(L)$, pelo Teorema 3.1.1, existem únicos $\lambda_1, \ldots, \lambda_n \in L$ tais que $\tau = \lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n$. Além disso, temos por definição que, $\pi_i = \sigma_1(u_i)\sigma_1 + \ldots + \sigma_n(u_i)\sigma_n$. Queremos mostrar que existem elementos $\mu_1, \ldots, \mu_n \in L$ tais que $\tau = \mu_1\pi_1 + \ldots + \mu_n\pi_n$. Ou seja,

$$\tau = [\mu_1\sigma_1(u_1) + \ldots + \mu_n\sigma_1(u_n)]\sigma_1 + \ldots + [\mu_1\sigma_n(u_1) + \ldots + \mu_n\sigma_n(u_n)]\sigma_n.$$

Dessa forma, devemos encontrar elementos μ_i tais que $\lambda_i = \mu_1\sigma_i(u_1) + \ldots + \mu_n\sigma_i(u_n)$, para todo $1 \leq i \leq n$. Mas este é um sistema de equações lineares cuja matriz dos coeficientes é exatamente a transposta da matriz B, dada no lema anterior. Como B é inversível, tal sistema tem solução única. Assim, existem únicos $\mu_1, \ldots, \mu_n \in L$ tais que $\tau = \mu_1\pi_1 + \ldots + \mu_n\pi_n$. □

Também podemos interpretar este resultado da seguinte maneira. Seja $\{u_1, \ldots, u_n\}$ uma K-base de L. Considere o conjunto $X_i = \{\lambda\pi_i : \lambda \in L\}$. Claramente X_i é um subespaço de $End_K(L)$. Mostramos anteriormente que os múltiplos de π_a formam um K-subespaço n-dimensional de $End_K(L)$. Como $a \in L$, existem $\lambda_1, \ldots, \lambda_n \in K$ tais que $a = \lambda_1 u_1 + \ldots + \lambda_n u_n$. No caso em que $a = 1_K u_i = u_i$ temos $\pi_a = \pi_i$. Portanto, X_i também é n-dimensional. Além disso, quando não nulos, os elementos $b\pi_i = b\sigma_1(u_i)\sigma_1 + \ldots + b\sigma_n(u_i)\sigma_n$ tem posto 1, $b \in L$. Dessa maneira, visto que $X_i = \{\lambda\pi_i : \lambda \in L\}$ são subespaços de $End_K(L)$ de dimensão n cujos elementos não nulos tem posto 1 e, como já visto, (Teorema 3.1.1) todo $\tau \in End_K(L)$

é escrito na forma $\tau = \mu_1\pi_1 + \ldots + \mu_n\pi_n$ para únicos $\mu_1, \ldots, \mu_n \in L$, podemos escrever

$$End_K(L) = \bigoplus_{i=1}^{n} X_i,$$

ou seja, $End_K(L)$ é uma soma direta de n-subespaços vetoriais, cada um de dimensão n.

Finalmente, cumprindo um dos nossos própositos desta seção, podemos determinar o traço de um endomorfismo qualquer, observando apenas o coeficiente do automorfismo identidade.

Teorema 3.2.9. *Seja $\tau = \lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n$ um elemento qualquer de $End_K(L)$ e assuma $\sigma_1 = 1$. Então, $tr(\tau) = Tr(\lambda_1)$.*

Dem.: Pelo Lema 3.2.8, podemos escrever $\tau = \mu_1\pi_1 + \ldots + \mu_n\pi_n$, para únicos $\mu_1, \ldots, \mu_n \in L$. Então como o traço é linear, segue que $tr(\tau) = \sum_{i=1}^{n} tr(\mu_i\pi_i)$. Já o Corolário 3.2.6 implica que $tr(\mu_i\pi_i) = Tr(\mu_i u_i)$, então

$$tr(\tau) = \sum_{i=1}^{n} tr(\mu_i\pi_i) = \sum_{i=1}^{n} Tr(\mu_i u_i) = Tr\left(\sum_{i=1}^{n} \mu_i u_i\right),$$

visto que o traço Galois também é linear. Por um lado temos $\tau = \lambda_1\sigma_1 + \ldots + \lambda_n\sigma_n$. Por outro lado

$$\begin{aligned}
\tau = \mu_1\pi_1 + \ldots + \mu_n\pi_n &= \mu_1(\sigma_1(u_1)\sigma_1 + \ldots + \sigma_n(u_1)\sigma_n) + \ldots + \mu_n(\sigma_1(u_n)\sigma_1 + \ldots + \sigma_n(u_n)\sigma_n) \\
&= [\mu_1\sigma_1(u_1) + \ldots + \mu_n\sigma_1(u_n)]\sigma_1 + \ldots [\mu_1\sigma_n(u_1) + \ldots + \mu_n\sigma_n(u_n)]\sigma_n \\
&= [\mu_1 u_1 + \ldots + \mu_n u_n]\sigma_1 + \ldots + [\mu_1\sigma_n(u_1) + \ldots + \mu_n\sigma_n(u_n)]\sigma_n
\end{aligned}$$

Comparando o coeficiente de $\sigma_1 = 1$ em ambas as expressões para τ podemos observar que $\lambda_1 = \mu_1 u_1 + \ldots + \mu_n u_n$. Dessa forma, $Tr(\lambda_1) = Tr(\mu_1 u_1 + \ldots + \mu_n u_n) = tr(\tau)$. □

3.3 DETERMINANTES ASSOCIADOS À HIPERPLANOS

Nesta seção faremos um estudo mais detalhado da matriz B do Lema 3.2.8 e de uma matriz $(n-1) \times (n-1)$ relacionada com B. Com estes resultados poderemos dizer qual é a forma exata de um K-hiperplano qualquer em L, em relação ao K-hiperplano traço zero. Um dos fatos mais importantes, e que abordaremos desde o princípio, é que *det* B é um

elemento de K ou pertence a uma extensão quadrática de K. Nosso intuito aqui, também é estender e generalizar este fato.

Teorema 3.3.1. *Sejam L/K uma extensão de Galois de grau n com grupo de Galois $G = \{\sigma_1, \ldots, \sigma_n\}$ e $\{u_1, \ldots, u_n\}$ uma K-base de L. Então a matriz $B_{n\times n}$ cuja entrada (i, j) é $\sigma_j(u_i)$, para $1 \leq i, j \leq n$, é inversível. Além disso, $det\ B \in K$, quando K tem característica 2 ou se o 2-subgrupo de Sylow de G não é cíclico. No caso em que K tem característica diferente de 2 e G tem 2-subgrupo de Sylow cíclico, $det\ B = \mu\alpha$, onde $\mu, \alpha^2 \in K$ e $K[\alpha]$ é a única extensão quadrática de K contida em L.*

Dem.: Pelo Lema 3.2.7, a matriz B é inversível. Sejam σ um elemento qualquer de G e $\sigma(B)$ a matriz obtida de B aplicando σ em cada um das suas entradas. Como G é um grupo, vemos que as colunas de $\sigma(B)$ são obtidas permutando as colunas de B de acordo com a ação regular de σ em G. Assim se $\epsilon(\sigma)$ denota o sinal de σ (agindo em G por multiplicação à esquerda), temos $\sigma(det\ B) = det\ \sigma(B) = \epsilon(\sigma) det\ B$, pois $\sigma \in Aut_K(L)$ (por álgebra linear, a reordenação das colunas da matriz faz com que o determinante da mesma seja multiplicado por 1 ou -1, de acordo com a paridade desta troca). Lembremos que a função sinal é dada por

$$\epsilon(x) = \begin{cases} 1, & \text{se } x \text{ é uma permutação par} \\ -1, & \text{se } x \text{ é uma permutação ímpar} \end{cases},$$

para todo $x \in G$. E ainda, a função sinal é considerada trivial sempre que $\epsilon(x) = 1$ para todo $x \in G$. No caso em que K tem característica 2, temos $1 = -1$. Logo, $\epsilon(x) = 1$, para qualquer que seja $x \in G$. Neste caso a função sinal é trivial. Além disso, vimos no Lema 1.2.12 que se o 2-subgrupo de Sylow de G não é cíclico, a função sinal ϵ também é trivial. Assim,

$$\sigma(det\ B) = det\ \sigma(B) = \epsilon(\sigma) det\ B = det\ B.$$

Portanto em ambos os casos $det\ B \in L^G = K$.

Se K tem característica diferente de 2 e G tem um 2-subgrupo de Sylow cíclico, temos do 1.2.11 que existe um subgrupo normal H de G de índice 2, isto é, $H \triangleleft G$ e $[G : H] = 2$. Pelo Teorema 1.2.8 temos o diagrama:

$$\begin{array}{rcl} L & \longleftrightarrow & \{e\} \\ | & & | \\ K[\alpha] = L^H & \longleftrightarrow & H\ . \\ | & & | \\ K & \longleftrightarrow & G \end{array}$$

Mais ainda $[L^H : K] = [G : H] = 2$ e consequentemente, pelo Teorema 1.2.4, temos $L^H = K[\alpha]$ para algum $\alpha \in L$ de modo que $\alpha^2 \in K$. Note que $\{1, \alpha\}$ é base de $K[\alpha]$ sobre K. O Teorema 1.1.13 nos diz que se o 2-subgrupo de Sylow de um grupo G é cíclico, então o grupo tem um 2-complemento normal, e este é o único subgrupo desta ordem. Assim, G tem um único subgrupo de índice 2. Logo, G pode ser escrito como $G = H.T$, onde $[G : H] = 2$ e $|T| = 2$. Dado que G pode ser identificado como o grupo de permutações, e visto que o conjunto das permutações pares forma um subgrupo normal de índice 2, temos

$$G = H.T \simeq A_{|G|}.\{\pm 1\},$$

isto é, H é o subconjunto das permutações pares e $T = \{-1, 1\}$ o grupo cíclico de ordem 2. Seja ainda $a = det\ B$. Então $\sigma(a) = \pm a$ para qualquer $\sigma \in G$. Assim, $\sigma(a)^2 = a^2$ e então $\sigma(a^2) = a^2$. Desta forma, $a^2 \in L^G = H$. Como $G = H.T$, dado $\sigma \in G$ vem que $\sigma = \gamma.\delta$, com $\gamma \in H$ e $\delta \in T$. Se σ é par, então $a = \sigma(a) = \gamma\delta(a) = \gamma(a)$. Se σ é ímpar, temos $-a = \sigma(a) = \gamma\delta(a) = \gamma(-a) = -\gamma(a)$. Logo, $a \in L^H = K[\alpha]$ que tem base $\{1, \alpha\}$. Assim temos que $a = det\ B = \lambda_1 + \lambda_2\alpha$, para $\lambda_1, \lambda_2 \in K$. Então $a^2 = (det\ B)^2 = \lambda_1^2 + 2\lambda_1\lambda_2\alpha + \lambda_2^2\alpha^2 = (\lambda_1^2 + \lambda_2^2\alpha^2) + (2\lambda_1\lambda_2)\alpha \in K$ o que implica que $2\lambda_1\lambda_2 = 0$. Visto que $ch(K) \neq 2$ e $\lambda_2 \neq 0$, segue que $\lambda_1 = 0$. Portanto, $det\ B = \lambda_2\alpha$, com $\lambda_2, \alpha^2 \in K$. Note que $K[\alpha]$ é a única extensão quadrática de K contida em L. □

De posse dos resultados deste teorema, nossa intenção agora é obter informações análogas para uma matriz $(n-1) \times (n-1)$, a partir de uma base do hiperplano traço zero H_0. Para tal, considere $\{b_2, \ldots, b_n\}$ uma K-base de H_0 a qual pode ser estendida a uma base de L adicionando um elemento b_1, que não pertença à H_0. Seja $E_{n\times n}$ a matriz cuja entrada (i, j) é dada por $\sigma_j(b_i)$. Para um elemento qualquer $x \in L$, tome $E(x)$ a matriz $n \times n$ obtida substituindo a primeira linha de E por $\sigma_1(x), \ldots, \sigma_n(x)$. Ou seja,

$$E = \begin{bmatrix} \sigma_1(b_1) & \sigma_2(b_1) & \cdots & \sigma_n(b_1) \\ \sigma_1(b_2) & \sigma_2(b_2) & \cdots & \sigma_n(b_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(b_n) & \sigma_2(b_n) & \cdots & \sigma_n(b_n) \end{bmatrix} \text{ e } E(x) = \begin{bmatrix} \sigma_1(x) & \sigma_2(x) & \cdots & \sigma_n(x) \\ \sigma_1(b_2) & \sigma_2(b_2) & \cdots & \sigma_n(b_2) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_1(b_n) & \sigma_2(b_n) & \cdots & \sigma_n(b_n) \end{bmatrix}.$$

Note que, da forma como $E(x)$ foi construída, temos $E(b_1) = E$. Além disso, considere $\theta : L \longrightarrow L$ dada por $\theta(x) = det\ E(x)$, para $x \in L$. Observe que dados $x,\ y \in L,\ \lambda \in K$, temos

$$
\begin{aligned}
\theta(x+y) &= det\ E(x+y) \\
&= det \begin{bmatrix} \sigma_1(x+y) & \sigma_2(x+y) & \cdots & \sigma_n(x+y) \\ \sigma_1(b_2) & \sigma_2(b_2) & \cdots & \sigma_n(b_2) \\ \vdots & \vdots & & \vdots \\ \sigma_1(b_n) & \sigma_2(b_n) & \cdots & \sigma_n(b_n) \end{bmatrix} \\
&= det \begin{bmatrix} \sigma_1(x)+\sigma_1(y) & \sigma_2(x)+\sigma_2(y) & \cdots & \sigma_n(x)+\sigma_n(y) \\ \sigma_1(b_2) & \sigma_2(b_2) & \cdots & \sigma_n(b_2) \\ \vdots & \vdots & & \vdots \\ \sigma_1(b_n) & \sigma_2(b_n) & \cdots & \sigma_n(b_n) \end{bmatrix} \\
&= [\sigma_1(x)+\sigma_1(y)]det\ E_1 - [\sigma_2(x)+\sigma_2(y)]det\ E_2 + \ldots + \\
&\quad +(-1)^{n-1}[\sigma_n(x)+\sigma_n(y)]det\ E_n \\
&= \sigma_1(x)det\ E_1 + \sigma_1(y)det\ E_1 + \ldots + (-1)^{n-1}\sigma_n(x)det\ E_n + (-1)^{n-1}\sigma_n(y)det\ E_n \\
&= (\sigma_1(x)det\ E_1 + \ldots + (-1)^{n-1}\sigma_n(x)det\ E_n) + \\
&\quad +(\sigma_1(y)det\ E_1 + \ldots + (-1)^{n-1}\sigma_n(y)det\ E_n) \\
&= det\ E(x) + det\ E(y) = \theta(x) + \theta(y);
\end{aligned}
$$

$$
\begin{aligned}
\theta(\lambda x) &= det\ E(\lambda x) \\
&= det \begin{bmatrix} \sigma_1(\lambda x) & \sigma_2(\lambda x) & \cdots & \sigma_n(\lambda x) \\ \sigma_1(b_2) & \sigma_2(b_2) & \cdots & \sigma_n(b_2) \\ \vdots & \vdots & & \vdots \\ \sigma_1(b_n) & \sigma_2(b_n) & \cdots & \sigma_n(b_n) \end{bmatrix} \\
&= \sigma_1(\lambda x)det\ E_1 - \sigma_2(\lambda x)det\ E_2 + \ldots + (-1)^{n-1}\sigma_n(\lambda x)det\ E_n \\
&= \lambda\sigma_1(x)det\ E_1 - \lambda\sigma_2(x)det\ E_2 + \ldots + (-1)^{n-1}\lambda\sigma_n(x)det\ E_n \\
&= \lambda[\sigma_1(x)det\ E_1 - \sigma_2(x)det\ E_2 + \ldots + (-1)^{n-1}\sigma_n(x)det\ E_n] \\
&= \lambda det\ E(x) = \lambda\theta(x).
\end{aligned}
$$

Nos cálculos acima E_i representa a matriz $(n-1)\times(n-1)$ obtida omitindo a primeira linha e a i-ésima coluna de E. Dessa forma, temos que $\theta \in End_K(L)$. Além disso, o Lema 3.2.7 nos garante que θ não é identicamente nulo pois $\theta(b_1) = det\ E \neq 0$. Por outro lado, se $x \in H_0$,

então $x = \lambda_2 b_2 + \ldots + \lambda_n b_n$, para $\lambda_2, \ldots, \lambda_n \in K$. Assim

$$E(x) = \begin{bmatrix} \sigma_1(x) & \sigma_2(x) & \cdots & \sigma_n(x) \\ \sigma_1(b_2) & \sigma_2(b_2) & \cdots & \sigma_n(b_2) \\ \vdots & \vdots & & \vdots \\ \sigma_1(b_n) & \sigma_2(b_n) & \cdots & \sigma_n(b_n) \end{bmatrix}$$

$$= \begin{bmatrix} \sigma_1\left(\sum_{j=2}^n \lambda_j b_j\right) & \sigma_2\left(\sum_{j=2}^n \lambda_j b_j\right) & \cdots & \sigma_n\left(\sum_{j=2}^n \lambda_j b_j\right) \\ \sigma_1(b_2) & \sigma_2(b_2) & \cdots & \sigma_n(b_2) \\ \vdots & \vdots & & \vdots \\ \sigma_1(b_n) & \sigma_2(b_n) & \cdots & \sigma_n(b_n) \end{bmatrix}$$

$$= \begin{bmatrix} \sum_{j=2}^n \lambda_j \sigma_1(b_j) & \sum_{j=2}^n \lambda_j \sigma(b_j) & \cdots & \sum_{j=2}^n \lambda_j \sigma_n(b_j) \\ \sigma_1(b_2) & \sigma_2(b_2) & \cdots & \sigma_n(b_2) \\ \vdots & \vdots & & \vdots \\ \sigma_1(b_n) & \sigma_2(b_n) & \cdots & \sigma_n(b_n) \end{bmatrix}.$$

Assim, a primeira linha de $E(x)$ é combinação K-linear das demais. Dessa forma, $E(x)$ tem linhas linearmente dependentes, o que implica que $det\ E(x) = 0$. Logo, θ se anula em H_0 e portanto é um L-múltiplo de π. Pelo mesmo argumento visto anteriormente, para cada elemento $\sigma \in G$, temos

$$\sigma(det\ E(x)) = det\ \sigma(E(x)) = \epsilon(\sigma) det\ E(x),$$

onde ϵ é a função sinal da representação regular à esquerda de G. Observando que σ_1 é a identidade de G, $\sigma_i(E_1)$ é obtida por permutação das colunas de E_i, para $1 \leq i \leq n$. Com efeito,

$$\sigma_i(E_1) = \sigma_i \begin{bmatrix} \sigma_2(b_2) & \sigma_3(b_2) & \cdots & \sigma_n(b_2) \\ \sigma_2(b_3) & \sigma_3(b_3) & \cdots & \sigma_n(b_3) \\ \vdots & \vdots & & \vdots \\ \sigma_2(b_n) & \sigma_3(b_n) & \cdots & \sigma_n(b_n) \end{bmatrix}.$$

Note que $\sigma_1(E_1) = E_1$, já que σ_1 é a identidade. Para $i > 1$,

$$\sigma_i(E_1) = \sigma_i \begin{bmatrix} | & | & & | \\ \sigma_2 & \sigma_3 & \cdots & \sigma_n \\ | & | & & | \end{bmatrix},$$

e $\sigma_i \sigma_j \neq \sigma_i$, para quaisquer $2 \leq i, j \leq n$ (caso contrário teríamos σ_j igual a identidade de

G). Consequentemente, $\sigma_i(det\ E_1) = det\ \sigma_i(E_1) = \epsilon_i det\ E_i$, onde $\epsilon_i = \pm 1$. Isso implica que se $det\ E_1 = 0$, então $det\ E_i = 0$ para todo i. Logo $\theta \equiv 0$, o que é um absurdo. Portanto, $det\ E_1 \neq 0$.

Com vistas a obter resultados similares ao Teorema 3.3.1, porém mais abrangentes, necessitamos de algumas informações mais precisas sobre ϵ_i e $det\ E_i$.

Lema 3.3.2. *Com a notação introduzida acima, temos* $\epsilon_i = (-1)^{i-1}\epsilon(\sigma_i)$.

Dem.: Sejam i um inteiro, com $1 \leq i \leq n$, e $x \in L$. Então

$$\sigma_i(det\ E(x)) = det(\sigma_i(E(x))) = \epsilon(\sigma_i) det\ E(x).$$

Por outro lado, $\theta(x) = det(E_1)\sigma_1(x) - det(E_2)\sigma_2(x) + \ldots + (-1)^{n-1} det(E_n)\sigma_n(x)$. Então aplicando σ_i obtemos,

$$\sigma_i(det\ E(x)) = \sigma_i(\theta(x)) = \sigma_i(det\ E_1)\sigma_i\sigma_1(x) + \ldots + (-1)^{n-1}\sigma_i(det\ E_n)\sigma_i\sigma_n(x).$$

Igualando as duas expressões de $\sigma_i(det\ E(x))$ obtemos

$$\begin{aligned}
\sigma_i(det(E(x))) &= \epsilon(\sigma_i) det(E(x)) \\
&= \epsilon(\sigma_i) det\ E_1\sigma_1(x) + \ldots + \epsilon(\sigma_i)(-1)^{i-1} det\ E_i\sigma_i(x) + \ldots \\
&= \sigma_i(det\ E_1)\sigma_i\sigma_1(x) + \ldots + (-1)^{i-1}\sigma_i(det\ E_i)\sigma_i\sigma_i(x) + \ldots \\
&= \sigma_i(det\ E_1)\sigma_i(x) + \ldots + (-1)^{i-1}\sigma_i(det\ E_i)\sigma_i\sigma_i(x) + \ldots
\end{aligned}$$

pois σ_1 é a identidade. Comparando o coeficiente de σ_i vemos que $\epsilon(\sigma_i)(-1)^{i-1} det\ (E_i) = \sigma_i(det\ (E_1)) = \epsilon_i det\ (E_i)$. Desde que $det\ E_i \neq 0$, segue que $\epsilon_i = (-1)^{i-1}\epsilon(\sigma_i)$. □

De acordo com o lema anterior, como $\epsilon_i = (-1)^{i-1}\epsilon(\sigma_i)$, temos que $(-1)^{i-1} = \epsilon_i\epsilon(\sigma_i)$ para $1 \leq i \leq n$. Dessa forma, a expressão $\theta = det\ (E_1)\sigma_1 - det\ (E_2)\sigma_2 + \ldots + (-1)^{n-1} det\ (E_n)\sigma_n$ fica dada por

$$\begin{aligned}
\theta &= \epsilon_1\epsilon(\sigma_1) det\ (E_1)\sigma_1 + \ldots + \epsilon_n\epsilon(\sigma_n) det\ (E_n)\sigma_n \\
&= \epsilon(\sigma_1)\epsilon_1 det\ (E_1)\sigma_1 + \ldots + \epsilon(\sigma_n)\epsilon_n det\ (E_n)\sigma_n \\
&= \epsilon(\sigma_1)\sigma_1(det\ (E_1))\sigma_1 + \ldots + \epsilon(\sigma_n)\epsilon_n(det\ (E_1))\sigma_n.
\end{aligned}$$

Agora que temos essa forma de escrever θ, podemos relacioná-lo com π, de acordo com o que segue.

Corolário 3.3.3. *Com a notação previamente introduzida, temos* $(det\ E_1)\pi = \theta$. *Consequentemente* $det\ E_1 = \epsilon(\sigma_i)\sigma_i(det\ E_1)$, *para* $1 \leq i \leq n$.

Dem.: Observando que $(det\ (E_1))\pi = det\ (E_1)\sigma_1 + det\ (E_1)\sigma_2 + \ldots + det\ (E_1)\sigma_n$ e que $\theta = det\ (E_1)\sigma_1 - det\ (E_2)\sigma_2 + \ldots + (-1)^{n-1} det\ (E_n)\sigma_n$, vemos que $(det\ (E_1))\pi$ e θ tem o mesmo coeficiente para $\sigma_1 = 1$, o qual é dado por $det\ (E_1)$. Por outro lado, vimos anteriormente que π e θ são L-múltiplos um do outro. Dessa forma, $\theta = \lambda\pi = \lambda\sigma_1 + \ldots + \lambda\sigma_n$ para algum $\lambda \in L$. Então λ é o coeficiente que multiplica σ_1 em θ. Dessa forma, $\lambda = det\ E_1$. Logo $(det\ E_1)\pi = \theta$. Consequentemente,

$$det\ (E_1)\sigma_1 + \ldots + det\ (E_1)\sigma_n = \epsilon(\sigma_1)\sigma_1(det\ E_1)\sigma_1 + \ldots + \epsilon(\sigma_n)\sigma_n(det\ E_1)\sigma_n.$$

Assim $det\ E_1 = \epsilon(\sigma_i)\sigma_i(det\ E_1)$ para $1 \leq i \leq n$. □

Tendo isso em mente podemos enunciar o próximo teorema, análogo ao Teorema 3.3.1, mas agora em relação ao hiperplano traço zero.

Teorema 3.3.4. *Sejam L/K uma extensão de Galois de grau n, com grupo de Galois $G = \{\sigma_1, \ldots, \sigma_n\}$, onde $\sigma_1 = 1$, H_0 o K-hiperplano traço zero em L, e $\{b_2, \ldots, b_n\}$ uma K-base de H_0. Então a matriz $(n-1) \times (n-1)$, E_1, cuja entrada (i,j) é $\sigma_j(b_i)$, $2 \leq i, j \leq n$, é inversível. Além disso, $det\ E_1 \in K$, quando K tem característica 2 ou se o 2-subgrupo de Sylow de G não é cíclico. No caso em que K tem característica diferente de 2 e G tem 2-subgrupo de Sylow cíclico, $det\ E_1 = k\alpha$, onde $k, \alpha^2 \in K$ e $K[\alpha]$ é a única extensão quadrática de K contida em L.*

Dem.: Vimos anteriormente que $det\ (E_1) \neq 0$ e portanto E_1 é inversível. Já o resultado anterior nos dá a expressão $det\ (E_1) = \epsilon(\sigma_i)\sigma_i(det\ E_1)$, para $2 \leq i \leq n$. Assim a prova desse resultado segue de maneira análoga ao Teorema 3.3.1. □

Observação 3.3.5. *A matriz E_1 foi obtida omitindo o automorfismo específico $\sigma_1 = 1$. De posse de tais informações, poderíamos obter o mesmo resultado do Teorema 3.3.4 para qualquer matriz análoga E_i, formada omitindo exatamente o automorfismo $\sigma_i \in G$.*

Finalizamos esta seção com uma versão análoga ao Teorema 3.3.4, agora de forma mais generalizada, considerando um K-hiperplano qualquer em L, digamos H. Sabemos do Lema 3.2.1 que este hiperplano é da forma $H = a^{-1}H_0$ para algum elemento não nulo $a \in L$. Considerando $\{b_2, \ldots, b_n\}$ uma K-base de H_0, temos que $\{c_2, \ldots, c_n\}$, onde $c_i = a^{-1}b_i$ para $2 \leq i \leq n$, é K-base de H. Além disso, seja C_1 a matriz $(n-1) \times (n-1)$, cuja entrada (i,j) é $\sigma_j(c_i)$. Então,

$$C_1 = \begin{bmatrix} \sigma_2(c_2) & \sigma_3(c_2) & \cdots & \sigma_n(c_2) \\ \sigma_2(c_3) & \sigma_3(c_3) & \cdots & \sigma_n(c_3) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_2(c_n) & \sigma_3(c_n) & \cdots & \sigma_n(c_n) \end{bmatrix} = \begin{bmatrix} \sigma_2(a^{-1}b_2) & \sigma_3(a^{-1}b_2) & \cdots & \sigma_n(a^{-1}b_2) \\ \sigma_2(a^{-1}b_3) & \sigma_3(a^{-1}b_3) & \cdots & \sigma_n(a^{-1}b_3) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_2(a^{-1}b_n) & \sigma_3(a^{-1}b_n) & \cdots & \sigma_n(a^{-1}b_n) \end{bmatrix}$$

$$= \begin{bmatrix} | & | & & | \\ \sigma_2(a^{-1})\sigma_2(b_i) & \sigma_3(a^{-1})\sigma_3(b_i) & \cdots & \sigma_n(a^{-1})\sigma_n\sigma_n(b_i) \\ | & | & & | \end{bmatrix}.$$

Por propriedade de determinante,

$$det\ C_1 = \sigma_2(a^{-1}) \dots \sigma_n(a^{-1}) det\ E_1.$$

Porém, note que $\sigma_1(a^{-1}) = a^{-1}$ e $\sigma_1(a^{-1})\sigma_2(a^{-1}) \dots \sigma_n(a^{-1}) = \lambda \in K$. De fato, dado $\sigma_i \in G$, $\sigma_i[\sigma_1(a^{-1})\sigma_2(a^{-1}) \dots \sigma_n(a^{-1})] = \sigma_i\sigma_1(a^{-1})\sigma_i\sigma_2(a^{-1}) \dots \sigma_i\sigma_n(a^{-1})$, que a menos de reordenação tem os mesmos fatores. Dessa forma, $det\ C_1 = a\ \lambda\ det\ E_1$, para algum elemento não nulo $\lambda \in K$. Como resultado disso, temos o seguinte teorema.

Teorema 3.3.6. *Sejam L/K uma extensão de Galois de grau n, com grupo de Galois $G = \{\sigma_1, \dots, \sigma_n\}$, onde $\sigma_1 = 1$. H_0 o K-hiperplano traço zero em L e H um outro K-hiperplano em L. Considere $\{c_2, \dots, c_n\}$ uma K-base de H. Então a matriz $(n-1) \times (n-1)$, C_1, cuja entrada (i, j) é $\sigma_j(c_i)$, $2 \leq i, j \leq n$, é inversível. Além disso, $H = (det\ C_1)^{-1}H_0$, quando K tem característica 2 ou se o 2-subgrupo de Sylow de G não é cíclico. No caso em que K tem característica diferente de 2 e G tem 2-subgrupo de Sylow cíclico, $H = \alpha(det\ C_1)^{-1}(H_0)$, onde $\alpha^2 \in K$ e $K[\alpha]$ é a única extensão quadrática de K contida em L.*

3.4 EXTENSÕES CÍCLICAS E ELEMENTOS ANULADORES

Seja L/K uma extensão de Galois cíclica, isto é, o grupo de Galois G é cíclico. Nesta seção vamos investigar os endomorfismos anuladores de um K-subespaço de L e a forma como estes podem ser expressos a partir de um polinômio mônico específico.

Considere σ o gerador do grupo de Galois G. Podemos identificar os elementos de $End_K(L)$ com os polinômios na variável σ com entradas em L, já que o Teorema 3.1.1 implica

que cada elemento neste conjunto pode ser expresso na forma

$$\mu_{n-1}\sigma^{n-1} + ... + \mu_1\sigma + \mu_0 id,$$

para únicos $\mu_0,\ \mu_1, \ldots,\ \mu_{n-1} \in L$. Mais adiante asseguraremos a existência e daremos uma forma de decompor os elementos de $End_K(L)$ em fatores lineares. Iniciemos com um critério de independência dos elementos de L, um resultado similar ao visto no capítulo anterior.

Teorema 3.4.1. *Seja L/K uma extensão cíclica de Galois de grau n e suponha que σ gera o grupo de Galois de L sobre K. Sejam k um inteiro tal que $1 \leq k \leq n$ e $b_1, \ldots, b_k$ elementos de L. Então esses elementos $b_1, \ldots, b_k$ são linearmente dependentes sobre K se e somente se $det\ (S) = 0$, onde S é a matriz $k \times k$ cuja entrada (i, j) é $\sigma^{j-1}(b_i)$, para $1 \leq i, j \leq k$.*

Dem.: Tal resultado é válido já que a matriz S é exatamente a transposta da matriz do Teorema 2.2.1. □

Relembremos agora o Corolário 2.2.3, obtido no Capítulo 2, e vejamos que o polinômio w citado ali pode ser expresso usando determinantes. Sejam U um subespaço de L de dimensão k e $\{b_1, \ldots, b_k\}$ uma K-base de U. Considere x um elemento arbitrário de L e $D(x)$ a matriz $(k+1) \times (k+1)$, cuja primeira linha tem entradas $\sigma^{j-1}(x)$ para $1 \leq j \leq k+1$, e cuja i-ésima linha tem entradas $\sigma^{j-1}(b_{i-1})$ para $2 \leq i \leq k+1$ e $1 \leq j \leq k+1$. Portanto,

$$D(x) = \begin{bmatrix} x & \sigma(x) & \cdots & \sigma^k(x) \\ b_1 & \sigma(b_1) & \cdots & \sigma^k(b_1) \\ \vdots & \vdots & \ddots & \vdots \\ b_k & \sigma(b_k) & \cdots & \sigma^k(b_k) \end{bmatrix}.$$

Definimos $\phi \in End_K(L)$ por $\phi(x) = det\ D(x)$. É fácil verificar que ϕ de fato é um endomorfismo de L. Dado $x \in U$, existem $\alpha_1, \ldots, \alpha_k \in K$ tais que $x = \alpha_1 b_1 + \ldots + \alpha_k b_k$, pois $\{b_1, \ldots, b_k\}$ é K-base de U. Assim,

$$\begin{aligned} \phi(x) &= det\ D(x) \\ &= \begin{vmatrix} \alpha_1 b_1 + \ldots + \alpha_k b_k & \sigma(\alpha_1 b_1 + \ldots + \alpha_k b_k) & \cdots & \sigma^k(\alpha_1 b_1 + \ldots + \alpha_k b_k) \\ b_1 & \sigma(b_1) & \cdots & \sigma^k(b_1) \\ \vdots & \vdots & \ddots & \vdots \\ b_k & \sigma(b_k) & \cdots & \sigma^k(b_k) \end{vmatrix} = 0, \end{aligned}$$

já que a primeira linha de $D(x)$ é uma combinação K-linear das demais. Portanto, ϕ se anula

em U. Expandindo $det\ D(x)$ ao longo da primeira linha, obtemos

$$\phi = det\ (D_1)id - det\ (D_2)\sigma + \ldots + (-1)^k det\ (D_{k+1})\sigma^k,$$

onde D_i é matriz $k \times k$ obtida omitindo a primeira linha e a i-ésima coluna de $D(x)$. Pelo Teorema 3.4.1, $det\ D_{k+1} \neq 0$. Então o polinômio w dado no Corolário 2.2.3 fica caracterizado no próximo resultado.

Teorema 3.4.2. *O polinômio descrito no Corolário 2.2.3 é exatamente*

$$w = t^k - det(D_k D_{k+1}^{-1})t^{k-1} + \ldots + (-1)^k det(D_1 D_{k+1}^{-1}),$$

onde as matrizes D_i são as definidas previamente. Além disso, desde que $D_1 = \sigma(D_{k+1})$, o termo constante tem a forma $(-1)^k a\sigma(a)^{-1}$, para algum elemento $a \in L$.

Dem.: Sabemos que $w = t^k - b_{k-1}t^{k-1} - \ldots - b_1 t - b_0$ e que $\phi = (-1)^k detD_{k+1}t^k + (-1)^{k-1}detD_k t^{k-1} + \ldots - detD_2 t + detD_1$. Multiplicando por $(-1)^k det(D_{k+1}^{-1})$ obtemos que $\phi = t^k - det(D_k D_{k+1}^{-1})t^{k-1} + \ldots + (-1)^{k-1}det(D_2 D_{k+1}^{-1})t + (-1)^k det(D_1 D_{k+1}^{-1})$. Desde que ϕ é um polinômio mônico de grau k que se anula em U, temos pela unicidade de w que $w = \phi$. Assim, $w = t^k - det(D_k D_{k+1}^{-1})t^{k-1} + \ldots + (-1)^{k-1}det(D_2 D_{k+1}^{-1})t + (-1)^k det(D_1 D_{k+1}^{-1})$. Além disso, $(-1)^k det(D_1 D_{k+1}^{-1})$ pode ser escrito como $(-1)^k det(\sigma(D_{k+1})D_{k+1}^{-1})$. Chamando $det(D_{k+1}^{-1})$ de a, temos

$$\begin{aligned} (-1)^k det(D_{k+1}^{-1})det(\sigma(D_{k+1})) &= (-1)^k det(D_{k+1}^{-1})\sigma(detD_{k+1}) \\ &= (-1)^k a\sigma(a^{-1}) \\ &= (-1)^k a\sigma(a)^{-1}. \end{aligned}$$

□

Tal polinômio será utilizado nos resultados que finalizam esta seção e para tanto receberá uma nomenclatura especial.

Definição 3.4.3. *Seja U um K-subespaço vetorial de L. Denotaremos o polinômio mônico de grau $dim\ U$, descrito no Corolário 2.2.3, por $m_U(t)$.*

Para os próximos resultados, vamos utilizar a notação $*$ para a multiplicação dos termos na decomposição dos polinômios.

Lema 3.4.4. *Seja U um K-subespaço próprio de L. Cada elemento de $End_K(L)$ que anula U pode ser expresso de forma única como $f(\sigma) * m_U(\sigma)$, onde $f(t) \in L[t]$ tem grau, no máximo $n - dim\ U - 1$.*

Dem.: Suponha $dim\ U = k$. Como visto anteriormente, o subespaço W de $End_K(L)$ que anula U tem dimensão $n(n-k)$. Sejam $f(t)$ e $g(t)$ dois polinômios distintos em $L[t]$ de grau no máximo $n-k-1$. Pelo Corolário 2.2.3, $m_U(\sigma)$ anula U. Logo, $f(\sigma) * m_U(\sigma)$ e $g(\sigma) * m_U(\sigma)$ anulam U. Além disso, como $f(t)$ e $g(t)$ são polinômios diferentes, temos $(f(\sigma) - g(\sigma)) * m_U(\sigma) \neq 0$. Então $f(\sigma) * m_U(\sigma) \neq g(\sigma) * m_U(\sigma)$. Assim, de maneira similar ao que foi deduzido na seção 3.2 deste capítulo em relação à dimensão de U, temos que o conjunto dos elementos da forma $f(\sigma) * m_U(\sigma)$, onde o grau de $f(t)$ é menor ou igual a $n-k-1$, é um K-espaço vetorial de dimensão $n(n-k)$. Portanto, coincide com o subespaço W. □

Seja V um subespaço de U de dimensão $k-1$. Desde que $m_U(\sigma)$ anula V, $m_U(\sigma) = f(\sigma) * m_V(\sigma)$ para algum polinômio mônico $f(t) \in L[t]$, pelo lema anterior . Como $m_U(\sigma)$ tem grau k e $m_V(\sigma)$ tem grau $k-1$, uma comparação direta nos diz que $f(t)$ é linear, isto é, $f(t) = t - a$, para algum $a \in L$. Esse elemento a pode ser calculado da seguinte maneira.

Teorema 3.4.5. *Sejam U um K-subespaço próprio de L de dimensão k e V um subespaço de U de codimensão 1. Considere $\{b_1, \ldots, b_{k-1}\}$ uma K-base de V e b_k um elemento de U que não está em V. Sejam D_1 e D_{k+1} matrizes $k \times k$ formadas usando a base $\{b_1, \ldots, b_k\}$ de U, como descrito no Teorema 3.4.2. E sejam C_1, C_k as matrizes $(k-1) \times (k-1)$ correspondentes, formadas usando a base $\{b_1, \ldots, b_{k-1}\}$ de V. Temos assim a fatoração $m_U(\sigma) = (\sigma - a) * m_V(\sigma)$, onde $a = det(D_1 D_{k+1}^{-1}) det(C_1^{-1} C_k)$.*

Dem.: Pelo Teorema 3.4.2,

$$m_U(t) = t^k - det(D_k D_{k+1}^{-1}) t^{k-1} + \ldots + (-1)^k det(D_1 D_{k+1}^{-1}),$$

e

$$m_V(t) = t^{k-1} - det(C_{k-1} C_k^{-1}) t^{k-2} + \ldots + (-1)^{k-1} det(C_1 C_k^{-1}).$$

Como observado anteriormente $m_U(t) = f(t) * m_V(t)$, onde $f(t) = t - a$. Analisando os termos constantes em $m_U(t)$ e $m_V(t)$ obtemos $(-1)^k det(D_1 D_{k+1}^{-1}) = a(-1)^{k-1} det(C_1 C_k^{-1})$, ou seja, $a = det(D_1 D_{k+1}^{-1}) det(C_1^{-1} C_k)$. □

O último resultado que apresentaremos nos diz que $m_U(\sigma)$ pode ser expresso como um produto de k termos da forma $\sigma - a$.

Corolário 3.4.6. *Seja U um K-subespaço próprio de L de dimensão k. Então existe uma fatoração $m_U(\sigma) = (\sigma - a_1) * \ldots * (\sigma - a_k)$ em $End_K(L)$, onde cada elemento a_i tem a forma $b_i \sigma(b_i)^{-1}$ para adequados $b_i \in L$.*

Dem.: A prova deste resultado será feita por indução sobre k. Se $k = 1$, então:

$$\begin{aligned} m_U(\sigma) = &\quad \sigma - (-1)det(D_1 D_2^{-1}) \\ = &\quad \sigma + det(\sigma(D_2).D_2^{-1}). \end{aligned}$$

Tomando $a = -det(D_2^{-1}) \cdot \sigma(detD_2)$, temos que o resultado vale para $k = 1$.

Suponha que $dim\ U = k > 1$ e tome V um subespaço próprio de U tal que $dim\ V = k - 1$. Pelo Teorema 3.4.5, $m_U(\sigma) = (\sigma - a_k) * m_V(\sigma)$ com $m_V(\sigma)$ polinômio de grau $k - 1$. Então usando a hipótese indutiva obtemos

$$m_U(\sigma) = (\sigma - a_1) * \ldots * (\sigma - a_k),$$

onde $a_i = b_i \sigma(b_i)^{-1}$ e $b_i = det(D_{i+1}^{-1})$. □

Referências Bibliográficas

[Cr] D.A. Craven, *The theory of fusion systems: an algebraic aproach* (Cambridge University Press, New York, 2011).

[GQ] R. Gow and R. Quinlan. Galois theory and linear algebra, *Linear Algebra and its Applications* **430** (2009) 1778–1789.

[GQ1] R. Gow and R. Quinlan. Galois extensions and subspaces of alternating bilinear forms with especial rank properties. *Linear Algebra and its Applications* **430** (2009) 2212–2224.

[HK] K. Hoffman and R. Kunze, *Linear Algebra* (2.ed. Prentice-Hall Inc. Englewood Cliffs, N.J., 1961).

[I] I. Isaacs, *Algebra: a graduate course* (Graduate Studies in Mathematics, v.100 - AMS, 2009).

[Ja] N. Jacobson, *Basic Algebra I* (2.ed. W. H. Freeman and Company, New York, 1985).

[L] S. Lang, *Algebra* (3.ed. Graduate Texts in Mathematics, Springer, New York, 2002).

[LF] W. De Launey and D. Flannery, *Algebraic Design Theory* (Mathematical Surveys and Monographs: v. 175 - AMS, 2011).

[R] J. Rotman, *An introduction to the Theory of Groups* (4.ed. Graduate Texts in Mathematics, Springer, New York, 1994).

[R1] J. Rotman, *Galois Theory* (2.ed., Springer, New York, 1998).

[St] I. Stewart, *Galois Theory* (3.ed. Chapman & Hall/CRC, Florida 2003).

[Se] M.R. Sepanski, *Algebra* (Pure and applied undergraduate texts: v.11, AMS, 2010).