Sobre bases normais para extensões galoisianas de corpos

Thiago Castilho de Mello

Sobre bases normais para extensões galoisianas de corpos

Thiago Castilho de Mello[1]

Orientadora: *Ires Dias*

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

USP - São Carlos

Janeiro/2008

[1]O autor teve apoio financeiro da Capes.

Aos meus pais,
Ednilson e
Eliane.

Agradecimentos

Agradeço aos meus pais Ednilson e Eliane pelo amor, carinho e pelo empenho em me garantir uma educação de qualidade, mesmo em situações adversas. Aos meus irmãos Natália e Flávio pela companhia e amizade e aos meus avós Valdês, Davirce, Flávio e Haidee pelo carinho, em especial ao meu avô Flávio, pelos conselhos no início do meu curso de graduação e à minha avó Haidee por me acolher em sua casa.

Agradeço à minha namorada Marcela pelo amor, carinho e companhia nas horas boas e nas horas difíceis, aos amigos Du, Giu e Dila, com quem convivo desde a graduação, pela amizade, companhia e pelas longas conversas sobre "o que fazer da vida". Agradeço também, aos amigos de república, aos amigos da graduação e pós-graduação e aos colegas de sala e laboratório pela companhia.

Agradeço ao ICMC e aos professores da graduação e pós-graduação, que foram responsáveis pela minha formação como matemático, em especial à minha orientadora Ires, não só pela orientação acadêmica, mas também pela orientação não-acadêmica.

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

Resumo

Neste trabalho apresentamos várias demonstrações do Teorema da Base Normal para certos tipos de extensões galoisianas de corpos, algumas existenciais e outras construtivas, destacando as diferenças e dificuldades de cada situação. Apresentamos também generalizações de tal teorema e mostramos que toda extensão galoisiana de grau ímpar de corpos admite uma base normal autodual com respeito à forma bilinear traço.

Abstract

In this work we present several demonstrations of The Normal Basis Theorem for certain kinds of galoisian extensions of fields, some of them existential and others constructive, pointing the difficulties and differences in each situation. We also present generalizations of such theorem and show that every odd degree galoisian extension of fields admits a self-dual normal base with respect to the trace bilinear map.

Sumário

Introdução

Na teoria de Galois sobre corpos, ou mais precisamente, no estudo de extensões finitas de corpos $E \supseteq F$, é de fundamental importância encontrarmos bases especiais para E sobre F. Um tipo de base especial são as chamadas bases normais. Sejam $E \supseteq F$ uma extensão galoisiana de corpos com grau n e grupo de Galois $G = \{\eta_1, \eta_2, \ldots, \eta_n\}$. Uma base normal de E sobre F é uma base da forma $B = \{\eta_1(\alpha), \eta_2(\alpha), \ldots, \eta_n(\alpha)\}$, para algum $\alpha \in E$, chamado o gerador da base normal B. Assim, dizemos que a extensão galoisiana $E \supseteq F$ admite uma base normal se existe um elemento $\alpha \in E$ tal que seus conjugados formam uma base de E sobre F.

Este tipo de base é de interesse tanto para a teoria matemática quanto para aplicações práticas. Na teoria de códigos e criptografia, por exemplo, é de grande interesse a aritmética dos corpos finitos, e as bases normais desempenham um importante papel nesta teoria. De fato, sejam $F = \mathbb{F}_q$ um corpo finito com $q = p^t$ elementos, onde p é um número primo e $E = \mathbb{F}_{q^n}$ uma extensão finita de grau n e grupo de Galois G de F. Se existe $\alpha \in E$ tal que $\{\eta_1(\alpha), \eta_2(\alpha), \ldots, \eta_n(\alpha)\}$ é base de E sobre F e $x \in E$, então existem escalares $a_i \in F$ tais que $x = \sum_{i=1}^{n} a_i \eta_i(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^{q^i}$. Assim, se queremos calcular x^q, temos $x^q = \left(\sum_{i=0}^{n-1} a_i \alpha^{q^i} \right)^q = \sum_{i=0}^{n-1} a_i^q (\alpha^{q^i})^q = \sum_{i=0}^{n-1} a_i \alpha^{q^{i+1}}$, e vemos que para calcular potências q de x basta transladarmos os coeficientes de x na sua representação sobre a base normal. Tal procedimento tem custo computacional zero e, por isso, trata-se de um assunto de extrema importância e fácil aplicabilidade.

Há na literatura, diversas demonstrações do "Teorema da base normal", que garante a existência de bases normais para uma dada extensão galoisiana finita de corpos. Algumas fazendo considerações quanto a natureza dos corpos envolvidos e/ou das extensões, como por exemplo, para corpos infinitos, para extensões cíclicas, etc., mas a maioria destas não é construtiva. Em geral, a construção efetiva de geradores de bases normais para extensões galoisianas quaisquer, ainda é um problema em aberto.

Neste trabalho, fazemos um estudo detalhado destes resultados procurando, na medida do possível, destacar as diferenças e as dificuldades de cada situação e/ou as técnicas utilizadas nas demonstrações.

No capítulo 1, fazemos uma apresentação dos resultados básicos que serão necessários para o desenvolvimento dos capítulos que se seguem.

No capítulo 2, apresentaremos uma demonstração do Teorema do Elemento Primitivo e duas demonstrações do Teorema da Base Normal, destacando em cada uma delas as técnicas utilizadas e as dificuldades encontradas.

O terceiro capítulo é dedicado ao estudo de métodos para construção de bases normais. Apresentamos um método para construção de bases normais para extensões galoisianas cíclicas e, outro para extensões galoisianas abelianas de corpos.

O quarto capítulo traz uma generalização do conceito de base normal. Mostramos que extensões galoisianas de corpos infinitos e de corpos finitos de característica 2 possuem tal tipo de base e damos uma caracterização para este tipo de base em corpos finitos de característica qualquer.

Para finalizar, no capítulo 5, mostramos que toda extensão galoisiana de grau ímpar de corpos admite uma base normal auto-dual com respeito à forma bilinear traço, utilizando para isso, resultados clássicos sobre formas hermitianas e grupo de Witt, como o teorema de Springer e o Teorema do Cancelamento de Witt.

Capítulo

1

Preliminares

1.1 Preliminares

Iniciamos este trabalho com os resultados necessários para as demonstrações dos resultados contidos nos capítulos que se seguem. Alguns resultados mais básicos não serão demonstrados, e suas demonstrações podem ser encontradas em qualquer livro clássico de álgebra, salvo menção contrária, quando citaremos a referência.

Proposição 1.1.1. *Seja G um grupo abeliano. Se $r = \sup\{o(g);\ g \in G\}$ é finito, então $o(g) \mid r$, para todo $g \in G$.*

Proposição 1.1.2. *Sejam $(F, +, \cdot)$ um corpo e $(G, \cdot)$ um subgrupo finito do grupo $(\dot{F} = F - \{0\}, \cdot)$. Então G é cíclico.*

Dem.: Seja $r = \sup\{o(g);\ g \in G\}$. Como G é finito, temos que $r = \max\{o(g);\ g \in G\}$. Assim, existe $g_0 \in G$, tal que $o(g_0) = r$. Pelo Teorema de Lagrange, r divide a ordem de G. Portanto, $r \leq |G|$. Como G é abeliano, pela proposição 1.1.1, $o(g) \mid r$, para todo $g \in G$. Assim, $g^r = 1$, para todo $g \in G$, ou seja, todo $g \in G$ é raíz do polinômio $p(X) = X^r - 1 \in F[X]$. Pelo Teorema Fundamental da Álgebra $p(X)$ tem no máximo

r raízes distintas, o que mostra que $|G| \leq r$. Assim, $|G| = r$ e, conseqüentemente, $G = \langle g_0 \rangle$ é cíclico. ■

Corolário 1.1.3. *Se $(F, +, \cdot)$ é um corpo finito, então $(\dot{F}, \cdot)$ é cíclico.*

Corolário 1.1.4. *Se F é um corpo finito com q elementos, então $\alpha^q = \alpha$, para todo $\alpha \in F$.*

Definição 1.1.5. *Seja $E \supseteq F$ uma extensão de corpos. Se existe $\alpha \in E$ tal que $E = F(\alpha)$, dizemos que α é um* elemento primitivo de $E \supseteq F$, *e que a extensão $E \supseteq F$* admite um elemento primitivo.

O próximo teorema mostra que vale o Teorema do Elemento Primitivo para corpos finitos (ver capítulo 2).

Teorema 1.1.6. *Toda extensão finita de corpos finitos admite um elemento primitivo.*

Dem.: Sejam F um corpo finito e $E \supseteq F$ uma extensão finita de corpos. Como F é finito e o grau da extensão, $[E : F]$, é finito, temos que E é um corpo finito. Pelo Corolário 1.1.4, $(\dot{E}, \cdot)$ é cíclico. Portanto, existe $\alpha \in E$ tal que $\dot{E} = \langle \alpha \rangle$, de onde segue que $E = F(\alpha)$. ■

Definição 1.1.7. *Sejam G é um grupo e F um corpo. Um homomorfismo de grupos $\varphi : G \longrightarrow \dot{F}$ é chamado um* caracter *de G sobre F.*

Um importante resultado, utilizado várias vezes nos capítulos seguintes, é o Teorema da Independência dos Caracteres de Dedekind.

Teorema 1.1.8 (Dedekind - Independência dos caracteres)**.** *Sejam G um grupo, F um corpo e $\varphi_1, \varphi_2, \ldots, \varphi_n : G \longrightarrow \dot{F}$ caracteres distintos de G sobre F. Se $a_1, \ldots, a_n \in F$, então*

$$a_1\varphi_1(g) + a_2\varphi_2(g) + \ldots + a_n\varphi_n(g) = 0, \tag{1.1}$$

para todo $g \in G$ se, e somente se $a_i = 0$, para todo $i \in \{1, \ldots, n\}$, ou seja, o conjunto de caracteres $\{\varphi_1, \ldots, \varphi_n\}$ é linearmente independente sobre F.

Dem.: A demonstração será feita por indução sobre n. O caso $n = 1$ é trivial. Suponhamos o resultado válido para $n - 1$. Sejam $a_1, a_2, \ldots, a_n \in F$ satisfazendo

(1.1). Se para algum $j \in \{1, \ldots, n\}, a_j = 0$, pela hipótese de indução $a_i = 0$, para todo $i \in \{1, \ldots, n\}$. Assim, podemos supor que $a_i \neq 0$, para todo $i \in \{1 \ldots, n\}$. Como $\varphi_1 \neq \varphi_2$, existe $g_0 \in G$ tal que $\varphi_1(g_0) \neq \varphi_2(g_0)$. Trocando g por $g_0 g$ em (1.1), obtemos:

$$a_1\varphi_1(g_0)\varphi_1(g) + a_2\varphi_2(g_0)\varphi_2(g) + \ldots + a_n\varphi_n(g_0)\varphi_n(g) = 0. \tag{1.2}$$

Multiplicando (1.1) por $\varphi_1(g_0)$, obtemos:

$$a_1\varphi_1(g_0)\varphi_1(g) + a_2\varphi_1(g_0)\varphi_2(g) + \ldots + a_n\varphi_1(g_0)\varphi_n(g) = 0. \tag{1.3}$$

Subtraindo (1.3) de (1.2), temos:

$$a_2(\varphi_2(g_0) - \varphi_1(g_0))\varphi_2(g) + \ldots + a_n(\varphi_n(g_0) - \varphi_1(g_0))\varphi_n(g) = 0,$$

para todo $g \in G$. Pela hipótese de indução, segue que $a_i(\varphi_i(g_0) - \varphi_1(g_0)) = 0$, para todo $i \in \{2, \ldots, n\}$. Como $a_2 \neq 0$, temos que $\varphi_1(g_0) = \varphi_2(g_0)$, o que contradiz a escolha de g_0. Portanto, $a_i = 0$, para todo $i \in \{1, \ldots, n\}$, como queríamos. ■

Como conseqüência imediata, temos:

Corolário 1.1.9. *Sejam $\eta_1, \ldots, \eta_n : F_1 \longrightarrow F_2$ monomorfismos distintos de corpos. Então $\{\eta_1, \ldots, \eta_n\}$ é linearmente independente sobre F_2.*

Apresentamos agora, algumas definições básicas necessárias para a caracterização de corpos de fatoração de polinômios sobre um corpo F e o Teorema fundamental da Teoria de Galois.

Seja F um corpo e $f(X) \in F[X]$ um polinômio mônico. Um corpo E é chamado *um corpo de fatoração de $f(X)$ sobre F*, se $f(X) = (X - \alpha_1)(X - \alpha_2)\ldots(X - \alpha_n)$ em $E[X]$ e $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Sejam $E \supseteq F$ uma extensão de corpos. O *grupo de Galois de $E \supseteq F$*, denotado por $Gal(E/F)$, é o grupo dos automorfismos de E que fixam F, ou seja,

$$Gal(E/F) = \{\eta \in Aut(E);\ \eta(a) = a,\ \text{para todo } a \in F\}.$$

Se $\alpha \in E$, o *polinômio minimal de α sobre F*, denotado por $m_F(\alpha)$, é o polinômio mônico de menor grau em $F[X]$ que satisfaz α, ou seja, que α é raiz.

Diremos que um polinômio $f(X) \in F[X]$ é *separável sobre F*, se os fatores irredutíveis de f em $F[X]$ têm raízes distintas. Uma extensão de corpos $E \supseteq F$ é dita uma *extensão separável* se o polinômio minimal de todo elemento de E é separável sobre F. A extensão $E \supseteq F$ é dita uma *extensão normal*, se todo polinômio irredutível sobre F que tem uma raíz em E, tem todas as suas raízes em E.

O próximo resultado caracteriza uma importante classe de extensões de corpos.

Teorema 1.1.10. *Sejam $E \supseteq F$ uma extensão de corpos. As seguintes condições são equivalentes:*

(1) E é um corpo de fatoração de algum polinômio separável $f(X) \in F[X]$.

(2) $F = Fix(G) = \{a \in E;\ \eta(a) = a, \eta \in G\}$, para algum grupo finito, G, de automorfismos de E.

(3) E é normal, separável e tem dimensão finita sobre F.

(4) A aplicação $\varphi : E \otimes_F E \longrightarrow E^{|G|}$ dada por $\varphi(x \otimes_F y) = (x\eta(y))_{\eta \in G}$ é um isomorfismo de $E-$álgebras.

Mais ainda, se E e F são como em (1) e $G = Gal(E/F)$, então $F = Fix(G)$ e, se G e F são como em (2)*, então $G = Gal(E/F)$.*

Definição 1.1.11. *Se $E \supseteq F$ satisfaz as condições equivalentes do teorema anterior, diremos que $E \supseteq F$ é uma* extensão galoisiana de corpos.

Para tais extensões, vale a correspondência de Galois, dada pelo seguinte teorema:

Teorema 1.1.12 (Teorema Fundamental da Teoria de Galois)**.** *Sejam $E \supseteq F$ uma extensão galoisiana de corpos e $G = Gal(E/F)$. Sejam Γ o conjunto de todos os subgrupos de G e Σ o conjunto de todos os corpos intermediários de $E \supseteq F$. As aplicações*

$$H \mapsto Fix(H),\ H \in \Gamma \ e$$

$$K \mapsto Gal(E/K),\ K \in \Sigma$$

são inversas uma da outra e, portanto, bijeções entre os conjuntos Γ e Σ.

Mais ainda, tais aplicações revertem inclusões e valem as seguintes propriedades:

(1) $|H| = [E : Fix(H)]$ *e* $[G : H] = [Fix(H) : F]$, *para todo* $H \in \Sigma$, *onde* $[G : H]$ *denota o índice de* H *em* G.

(2) H *é um subgrupo normal de* G *se, e somente se* $Fix(H) \supseteq F$ *é uma extensão normal. Neste caso,* $Gal(Fix(H)/F) \cong G/H$.

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

Teorema 1.1.13. *Seja* $F = \mathbb{F}_q$ *um corpo com* q *elementos e* $E = \mathbb{F}_{q^n} \supseteq F$ *uma extensão de grau* n. *Então* $Gal(E/F)$ *é cíclico gerado pelo automorfismo* $x \mapsto x^q$.

Dem.: Observamos inicialmente que η é um $F-$automorfismo de E. De fato, $\eta(xy) = (xy)^q = x^q y^q = \eta(x)\eta(y)$, e $\eta(x + y) = (x + y)^q = x^q + y^q = \eta(x) + \eta(y)$, para todo $x, y \in E$, pois a característica de F divide q. Assim, η é um homomorfismo de corpos. Mas, todo homomorfismo de corpos é injetor e, como E é finito, η é uma bijeção, ou seja, um automorfismo de E. Pelo Corolário 1.1.4 temos que $\eta(x) = x$, para todo $x \in F$, o que mostra que η é um $F-$ automorfismo de E.

Agora, vamos mostrar que $G = Gal(E/F) = \langle\eta\rangle$. Seja $F' = Fix(\langle\eta\rangle)$. Pelo Teorema 1.1.10, basta mostrar que $F = F'$. O Teorema Fundamental da Teoria de Galois, nos garante que $[E : F'] = n$ e, como $\langle\eta\rangle \subseteq G$, a parte (1) nos garante que $F' \supseteq Fix(G) = F$. Assim, $n = [E : F] = [E : F'][F' : F] = n[F' : F]$, ou seja, $F = F'$, como queríamos. ■

Seja $E \supseteq F$ uma extensão de corpos. O *fêcho normal de* $E \supseteq F$ é a menor extensão K de E tal que $K \supseteq F$ é normal.

Queremos mostrar que o número de $F-$monomorfismos de E em K é igual ao grau da extensão $E \supseteq F$ e, usando tais monomorfismos, determinar quando um conjunto de elementos de E forma uma base de E sobre F. Para isso, precisamos de um resultado preliminar, cuja demonstração pode ser encontrada em qualquer livro básico de Teoria de Galois.

Teorema 1.1.14. *Sejam* $\eta : F \longrightarrow \overline{F}$ *um isomorfismo de corpos,* $f(x) \in F[X]$ *mônico não constante e* $\overline{f} \in \overline{F}[X]$ *a imagem do polinômio* f *sob a ação do isomorfismo que estende* η *a* $F[X]$ *e leva* X *em* X. *Se* E *e* $\overline{E}$ *são corpos de fatoração para* f *e* $\overline{f}$ *respectivamente, então* η *pode ser estendido a um isomorfismo de* E *em* $\overline{E}$.

Teorema 1.1.15. *Sejam $E \supseteq F$ uma extensão finita e separável de corpos e $K \supseteq F$ seu fêcho normal. Então o número de F-monomorfismos de E em K é $n = [E : F]$. Se tais monomorfismos são $\eta_1 = 1, \eta_2, \ldots, \eta_n$, então o conjunto $\{u_1, u_2, \ldots, u_n\} \subseteq E$, é uma base de E sobre F se, e somente se* $\det(\eta_i(u_j)) \neq 0$.

Dem.: Sejam $G = Gal(K/F)$ e H o subgrupo de G que fixa E, ou seja, $H = Gal(K/E)$. Então, do Teorema 1.1.12, $n = [E : F] = [G : H]$ e podemos escrever $G = (\xi_1 H) \dot{\bigcup} (\xi_2 H) \dot{\bigcup} \ldots \dot{\bigcup} (\xi_n H)$, onde os $\xi_i H$ são as classes distintas de H em G. Sejam $\eta_i = \xi_i|_E$, para cada $i \in \{1, \ldots, n\}$. Assim, cada η_i é um $F-$monomorfismo de E em K e, mais ainda, $\eta_i \neq \eta_j$, para $i \neq j$, pois caso contrário, teríamos $\xi_i^{-1}\xi_j(u) = u$, para todo $u \in E$, o que implicaria, $\xi_j^{-1}\xi_i \in H$ e, portanto, $\xi_i H = \xi_j H$, contrariando a escolha dos ξ_i. Obtemos assim n $F-$monomorfismos distintos de E em K.

Seja agora, η um $F-$monomorfismo de E em K. Como K é um corpo de fatoração sobre F de um polinômio $f(x) \in F[x]$, ele também é corpo de fatoração de $f(x)$ sobre E e sobre $\eta(E)$. Assim, pelo Teorema 1.1.14 o isomorfismo η de E em $\eta(E)$ pode ser estendido a um $F-$automorfismo ξ de K, ou seja, $\xi \in G$ e, conseqüentemente, $\xi = \xi_i\lambda$, para algum $\lambda \in H$. Mas $\eta = \xi|_E = \xi_i\lambda|_E = \xi_i|_E = \eta_i$. Assim, $\eta_1 \ldots \eta_n$ são todos os $F-$monomorfismos de E em K, o que mostra a primeira parte do teorema.

Agora, se $\{u_1, \ldots, u_n\} \subseteq E$ é um conjunto linearmente dependente sobre F, então existem $a_1, \ldots, a_n \in F$ não todos nulos tais que $\sum_{i=1}^{n} a_i u_i = 0$. Assim, para todo $j \in \{1, \ldots, n\}$, temos que $\sum_{i=1}^{n} a_i \eta_j(u_i) = 0$. Isso significa que o sistema linear homogêneo sobre K,

$$\sum_{i=1}^{n} \eta_j(u_i) x_i = 0, \quad j \in \{1, \ldots, n\}$$

admite uma solução não trivial. Portanto, $\det(\eta_i(u_j)) = 0$. Ou seja, se $\det(\eta_i(u_j)) \neq 0$ então $\{u_1, \ldots, u_n\}$ é linearmente independente sobre F, isto é, $\{u_1, \ldots, u_n\}$ é uma base de E sobre F, pois $[E : F] = n$.

Seja agora, $\{u_1, \ldots, u_n\}$ uma base de E sobre F. Suponhamos que $0 = \det(\eta_i(u_j)) = \det(\eta_j(u_i))$. Logo, existe uma solução não trivial $(a_1, \ldots, a_n) \in K^n$ para o sistema

$$\sum_{i=1}^{n} \eta_i(u_j) x_i = 0, \quad j \in \{1, \ldots, n\}.$$

Usando que o conjunto $\{u_1, \dots u_n\}$ gera E sobre F, temos que dado $u \in E$, existem $b_1, \dots, b_n \in F$, tais que $u = \sum_{i=1}^{n} b_i u_i$. Assim, $\sum_{j=1}^{n} a_j \eta_j(u) = \sum_{i=1}^{n} b_i \left(\sum_{j=1}^{n} a_j \eta_j(u_i) \right) = 0$, para todo $u \in E$, o que contradiz a independência dos caracteres. Portanto, se $\{u_1, \dots, u_n\}$ é uma base de E sobre F, então $\det(\eta_i(u_j)) \neq 0$. ■

O próximo resultado sobre o comportamento de polinômios em extensões de corpos infinitos nos será útil para mostrarmos a independência algébrica dos monomorfismos.

Teorema 1.1.16. *Sejam F um corpo infinito e E uma extensão de F. Se $f(X_1, \dots, X_n) \in E[X_1, \dots, X_n]$ é um polinômio não nulo, então existe $(a_1, \dots, a_n) \in F^n$, tal que $f(a_1, \dots, a_n) \neq 0$.*

Dem.: A demonstração será feita por indução sobre n. Se $n = 1$ como F é infinito, pelo Teorema Fundamental da Álgebra, f tem no máximo ∂f raízes em E. Como $F \subseteq E$ é infinito, existe $a \in F$ tal que $f(a) \neq 0$.

Se $n > 1$, escrevemos $f(X_1, \dots, X_n) = \sum_{i=0}^{k} g_i(X_1, \dots, X_{n-1}) X_n^i$, onde $g_i(X_1, \dots, X_{n-1}) \in E[X_1, \dots, X_{n-1}]$, e $g_k(X_1, \dots, X_{n-1}) \neq 0$. Pela hipótese de indução, existe $(a_1, \dots, a_{n-1}) \in F^{n-1}$ tal que $g_k(a_1, \dots, a_{n-1}) \neq 0$. Considere o polinômio $h(X_n) = \sum_{i=0}^{k} g_i(a_1, \dots, a_{n-1}) X_n^i \in E[X_n]$. Como $g_k(a_1, \dots, a_{n-1}) \neq 0$, segue que h é não nulo e, novamente, pelo Teorema Fundamental da Álgebra, e por F ser infinito, segue que existe $a_n \in F$ tal que $h(a_n) \neq 0$. Assim, existe $(a_1, \dots, a_n) \in F^n$ tal que $f(a_1, \dots, a_n) \neq 0$. ■

Definição 1.1.17. *Sejam $\eta_1, \dots, \eta_n$ monomorfismos de corpos de E em K. Dizemos que $\eta_1, \dots, \eta_n$ são* algebricamente independentes *sobre K, se o único polinômio $f(X_1, \dots, X_n) \in K[X_1, \dots, X_n]$, tal que $f(\eta_1(u), \dots, \eta_n(u)) = 0$, para todo $u \in E$, é o polinômio nulo.*

Teorema 1.1.18. *Sejam F um corpo infinito, $E \supseteq F$ uma extensão finita e separável de corpos de grau n, e K o fêcho normal de $E \supseteq F$. Se $\eta_1, \dots, \eta_n$ são os n $F-$monomorfismos distintos de E em K, então, $\eta_1, \dots, \eta_n$ são algebricamente independentes sobre K.*

Dem.: Seja $f(X_1,\ldots,X_n) \in K[X_1,\ldots,X_n]$ tal que $f(\eta_1(u),\ldots,\eta_n(u)) = 0$, para todo $u \in E$. Vamos mostrar que f é o polinômio nulo.

Sejam $\{u_1,\ldots,u_n\}$ uma base de E sobre F e $u = \sum_{i=1}^{n} a_i u_i$, com $a_i \in F$, um elemento genérico de E. Então

$$0 = f\left(\eta_1\left(\sum_{i=1}^{n} a_i u_i\right),\ldots,\eta_n\left(\sum_{i=1}^{n} a_i u_i\right)\right) = f\left(\sum_{i=1}^{n} a_i\eta_1(u_i),\ldots,\sum_{i=1}^{n} a_i\eta_n(u_i)\right),$$

para todo $(a_1\ldots,a_n) \in F^n$. Para $g(X_1,\ldots,X_n) \in K[X_1,\ldots,X_n]$, dado por $g(X_1,\ldots,X_n) = f\left(\sum_{i=1}^{n}\eta_1(u_i)X_i,\ldots,\sum_{i=1}^{n}\eta_n(u_i)X_i\right)$, temos que $g(a_1,\ldots,a_n) = 0$, para todo $(a_1,\ldots,a_n) \in F^n$.

Sejam $m = [K:F]$ e $\{v_1,\ldots,v_m\}$ uma base de K sobre F. Escrevendo os coeficientes de g como combinação linear dos elementos desta base, obtemos $g(X_1,\ldots,X_n) = \sum_{j=1}^{m} g_j(X_1,\ldots,X_n)v_j$, onde $g_j(X_1,\ldots,X_n) \in F[X_1,\ldots,X_n]$ e, para cada $j \in \{1,\ldots,m\}$, $g_j(a_1,\ldots,a_n) = 0$, para todo $(a_1,\ldots,a_n) \in F^n$. Como F é um corpo infinito, do Teorema 1.1.16, concluímos que $g_j(X_1,\ldots,X_n) = 0$, para todo $j \in \{1,\ldots,m\}$ e, portanto, $g(X_1,\ldots,X_n)$ é o polinômio nulo.

Como $\{u_1,\ldots,u_n\}$ é base de E sobre F, o Teorema 1.1.15 nos assegura que $\det(\eta_i(u_j)) \neq 0$. Assim, para a matriz $(w_{ij}) = (\eta_i(u_j))^{-1}$, substituindo $(X_1,\ldots,X_n)$ por $(X_1,\ldots,X_n)(w_{ij})^T$, na definição do polinômio g, obtemos $g((X_1,\ldots,X_n)(w_{ij})^T) = f(X_1,\ldots,X_n)$. Como g é o polinômio nulo, concluímos que f também é o polinômio nulo, e os n $F-$monomorfismos $\eta_1,\ldots,\eta_n : E \longrightarrow K$, são algebricamente independentes sobre o corpo K, como queríamos. ■

Finalizamos o capítulo com um resultado sobre o comportamento de matrizes em extensões de corpos. Sua demonstração pode ser encontrada em [9], Capítulo XIV, Corolário 2.2.

Definição 1.1.19. *Sejam F um corpo e $M, N \in M_n(F)$. Dizemos que M* é semelhante a *N se existe uma matriz invertível $P \in M_n(F)$ tal que $M = PNP^{-1}$.*

Teorema 1.1.20. *Sejam $E \supseteq F$ uma extensão finita de corpos e $A, B \in GL_n(F)$. Se existe $P \in GL_n(E)$ satisfazendo $PAP^{-1} = B$, então existe $Q \in GL_n(F)$ tal que*

$QAQ^{-1} = B$, ou seja, se duas matrizes com coeficientes em F são semelhantes sobre E, então elas são semelhantes sobre F.

Capítulo

2

Bases Especiais para Extensões de Corpos

Neste capítulo apresentaremos dois teoremas que tratam de bases especiais sobre extensões de corpos: o Teorema do Elemento Primitivo e o Teorema da Base Normal. Como veremos, ambos são resultado existenciais. Para demonstrá-los, usaremos apenas conceitos básicos de álgebra linear e alguns resultados do capítulo 1. Iniciamos com o Teorema do elemento primitivo, já provado para o caso de corpos finitos em 1.1.6.

2.1 O Teorema do Elemento Primitivo

O Teorema do Elemento Primitivo segue como um corolário do teorema abaixo, que dá uma caracterização equivalente de extensões finitas que admitem elemento primitivo.

Teorema 2.1.1. *Uma extensão finita de corpos admite um elemento primitivo se, e somente se ela tem uma quantidade finita de corpos intermediários.*

Dem.: Seja $E \supseteq F$ uma extensão finita de corpos. Suponhamos inicialmente que $E = F(\alpha)$, para algum $\alpha \in E$, e que K seja um corpo intermediário de $E \supseteq F$. Sejam

$f(X) \in F[X]$ o polinômio minimal de α sobre F e $g(X) \in K[X]$ o polinômio minimal de α sobre K. Assim, $g(X) \mid f(X)$ em $K[X]$ e, conseqüentemente, $\partial g \leq \partial f$.

Seja K' o corpo gerado por F e pelos coeficientes de g. É claro que $K' \subseteq K$ e que $m_K(\alpha) = g = m_{K'}(\alpha)$. Como $E = K(\alpha) = K'(\alpha)$, temos que $[E : K] = \partial g = [E : K']$, o que mostra que $K = K'$. Portanto, se K é um corpo intermediário então ele é gerado por F e por coeficientes de divisores mônicos de $f(X)$, que são em número finito. Então, existe uma quantidade finita de corpos intermediários.

Reciprocamente, suponhamos que exista uma quantidade finita de corpos intermediários de $E \supseteq F$. Pelo Teorema 1.1.6, podemos assumir que F é infinito. Como $E \supseteq F$ é uma extensão finita, existem $\alpha_1, \alpha_2, \ldots, \alpha_n \in E$, tais que $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Agora, usando indução sobre n, é suficiente mostrarmos o resultado para $n = 2$, isto é, para $E = F(\alpha_1, \alpha_2)$.

Para cada $c \in F$, consideremos o corpo intermediário $F_c = F(\alpha_1 + c\alpha_2)$. Como F é infinito e existe uma quantidade finita de corpos intermediários, temos que existem $c_1, c_2 \in F$ distintos, tais que $F_{c_1} = F_{c_2}$. Como $\alpha_2 = \dfrac{\alpha_1 + c_1\alpha_2 - (\alpha_1 + c_2\alpha_2)}{c_1 - c_2}$, temos que $\alpha_2 \in F_{c_1}$ e, conseqüentemente, $\alpha_1 \in F_{c_1}$. Assim, $F(\alpha_1, \alpha_2) = F_{c_1} = F(\alpha_1 + c_1\alpha_2)$ e $\alpha_1 + c_1\alpha_2$ é um elemento primitivo de $E \supseteq F$. ■

Corolário 2.1.2 (Teorema do Elemento Primitivo)**.** *Toda extensão finita e separável de corpos admite um elemento primitivo.*

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

Notemos que corpos intermediários de $E \supseteq F$ são também corpos intermediários de $K \supseteq F$. Como existe apenas uma quantidade finita de subgrupos do grupo $Gal(K/F)$, o Teorema fundamental da Teoria de Galois, nos garante que existe apenas uma quantidade finita de corpos intermediários de $K \supseteq F$. Conseqüentemente, $E \supseteq F$ tem somente uma quantidade finita de corpos intermediários, o que implica, de 2.1.1, que $E \supseteq F$ admite um elemento primitivo. ■

É fácil encontrar extensões de corpos que não admitam elementos primitivos, como por exemplo, $\mathbb{R} \supseteq \mathbb{Q}$. Entretanto, não é uma tarefa simples encontrar uma extensão finita de corpos que não tenha elemento primitivo. Temos que procurar, é claro, por uma extensão que não seja separável. A seguir apresentamos um exemplo onde isso ocorre.

Exemplo 2.1.3. *Sejam $F = \mathbb{F}_p(X^p, Y^p)$ e $E = \mathbb{F}_p(X, Y)$, onde X e Y são indeterminadas independentes. Observemos inicialmente que $[E : F] = p^2$, pois $\{X^i Y^j;\ 0 \leq i, j \leq p-1\}$ é uma base de E sobre F. Vamos mostrar que a extensão $E \supseteq F$, apesar de ser finita, não admite elemento primitivo. Para isso, notemos que para todo elemento $\alpha \in E$, $\alpha^p \in F$, e portanto, $\partial m_F(\alpha) \leq p$, para todo $\alpha \in E$. Assim, se existisse $\alpha \in E$ tal que $E = F(\alpha)$, teríamos que $[E : F] = \partial m_F(\alpha) = p$, o que não é verdade. Logo, a extensão $E \supseteq F$ não admite elemento primitivo.*

2.2 O Teorema da Base Normal

Comecemos com a definição formal de base normal.

Definição 2.2.1. *Sejam $E \supseteq F$ uma extensão finita de corpos e $G = Gal(E/F)$ seu grupo de Galois. Se existe um elemento $\alpha \in E$ tal que $B = \{\eta(\alpha);\ \eta \in G\}$ é uma base de E sobre F, dizemos que B é uma* base normal *de $E \supseteq F$ e que α é um* elemento normal *da extensão $E \supseteq F$. Neste caso, diremos também que $E \supseteq F$ admite uma base normal, ou que E tem base normal sobre F.*

Vejamos alguns exemplos de extensões galoisianas de corpos que admitem bases normais.

Exemplo 2.2.2. *Seja $E = \mathbb{Q}(\sqrt{2})$. É fácil ver que E é uma extensão de grau 2 de $\mathbb{Q}$ e que seu grupo de Galois é $G = \{\eta_1, \eta_2\}$, onde $\eta_1 = id$ e $\eta_2(\sqrt{2}) = -\sqrt{2}$. Assim, se $\alpha = 1 + \sqrt{2}$, temos que $\eta(\alpha) = 1 - \sqrt{2}$. Como $1 + \sqrt{2}$ e $1 - \sqrt{2}$ são linearmente independentes sobre $\mathbb{Q}$, segue que $\{\eta_1(\alpha), \eta_2(\alpha)\} = \{1+\sqrt{2}, 1-\sqrt{2}\}$ é uma base normal de E sobre $\mathbb{Q}$.*

Exemplo 2.2.3. *Sejam $F = \mathbb{F}_2$ e $p(X) = X^3 + X + 1 \in F[X]$. Como p não tem raízes em F, segue que p é irredutível. Seja β uma raiz de p. É fácil ver que β^2 e*

$\beta + \beta^2$ são as outras raízes de p. Se E é o corpo de fatoração de $p(X)$ sobre F, então $[E : F] = 3$ e $Gal(E/F) = \{\eta_1, \eta_2, \eta_3\}$, onde $\eta_1(\beta) = \beta, \eta_2(\beta) = \beta^2$ e $\eta_3(\beta) = \beta^2 + \beta$. Neste caso, tomando $\alpha = \beta + 1$, temos que $\eta_1(\beta + 1) = \beta + 1$, $\eta_2(\beta + 1) = \beta^2 + 1$ e $\eta_3(\beta + 1) = \beta^2 + \beta + 1$. Assim, através de uma simples verificação, podemos ver que $\{\eta_1(\alpha), \eta_2(\alpha), \eta_3(\alpha)\}$ é linearmente independente sobre F, ou seja, uma base normal de E sobre F.

O próximo teorema, o Teorema da Base Normal, nos garante que toda extensão galoisiana de corpos admite uma base normal.

Teorema 2.2.4 (Teorema da Base Normal)**.** *Seja $E \supseteq F$ uma extensão galoisiana de corpos. Então, $E \supseteq F$ admite uma base normal.*

Dem.: Faremos inicialmente a demonstração para o caso em que F é um corpo infinito.

Sejam $n = [E : F]$ e $G = Gal(E/F) = \{\eta_1, \ldots, \eta_n\}$. Do Teorema 1.1.15 temos que se $u \in E$, então $\{\eta_1(u), \ldots, \eta_n(u)\}$ é uma base de E sobre F se, e somente se $\det(\eta_i\eta_j(u)) \neq 0$. Escrevendo $\eta_i\eta_j = \eta_{i(j)}$, temos que $j \mapsto i(j)$ é uma permutação de $\{1, \ldots, n\}$. Assim, consideremos a matriz $X = (X_{i(j)})$ e o polinômio $d(X_1, \ldots, X_n) = \det(X) \in E[X_1, \ldots, X_n]$. Observemos que $d(1, 0, \ldots, 0) = \pm 1 \neq 0$. De fato, basta mostrarmos que o elemento 1 aparece apenas uma vez em cada coluna no cálculo do determinate $d(1, 0, \ldots, 0)$. Para isso, suponha que exista uma coluna j tal que $i(j) = k(j)$, para i e $k \in \{1, \ldots, n\}$. Então, temos que $\eta_i\eta_j = \eta_k\eta_j$, ou seja, $i = k$. Logo, $d(1, 0, \ldots, 0) \neq 0$ o que mostra que $d(X_1, \ldots, X_n)$ não é o polinômio nulo. Como, pelo Teorema 1.1.18 $\eta_1, \ldots, \eta_n$ são algebricamente independentes sobre E, concluímos que existe $u \in E$, tal que $d(\eta_1(u), \eta_2(u), \ldots, \eta_n(u)) = \det(\eta_i(\eta_j(u))) \neq 0$. Logo, $\{\eta_1(u), \ldots, \eta_n(u)\}$ é uma base normal de E sobre F.

Consideremos agora o caso em que $G = Gal(E/F)$ é um grupo cíclico. Seja $G = \langle\eta\rangle = \{1, \eta, \eta^2, \ldots, \eta^{n-1}\}$. Sendo η um $F-$automorfismo de E temos, em particular, que η é um isomorfismo de $F-$espaços vetoriais. Com isso, η induz em E uma estrutura de $F[X]-$módulo com a operação $p(X) \cdot v = p(\eta)(v)$, para todo $p(X) \in F[X]$ e $v \in E$.
Afirmação 1: E é um $F[X]-$módulo cíclico, ou seja, existe $z \in E$ tal que $E = F[X] \cdot z$.

De fato, do teorema fundamental de estrutura de módulos finitamente gerados sobre domínios de ideais principais, temos que $E = F[X] \cdot z_1 \oplus F[X] \cdot z_2 \oplus \cdots \oplus F[X] \cdot z_s$, onde $anul(z_i) = \{p \in F[X];\ p(X) \cdot z_i = 0\} = (d_i(X))$, e $d_i | d_j$, se $i \leq j$. Podemos supor que d_i é mônico, para todo $i \in \{1, \ldots, s\}$.

Afirmamos que $d_s(X)$ é o polinômio minimal da transformação linear η, ou seja, o polinômio mônico de menor grau tal que $d_s(\eta) = 0$. De fato, vamos primeiro mostrar que $d_s(X) \cdot z = d_s(\eta)(z) = 0$, para todo $z \in E$. Se $z \in E$, existem $p_1(X), \ldots, p_s(X) \in F[X]$ tais que $z = p_1(\eta)(z_1) + \cdots + p_s(\eta)(z_s)$. Assim, $d_s(\eta)(z) = d_s(\eta)p_1(\eta)(z_1) + \cdots + d_s(\eta)p_s(\eta)(z_s)$. Mas, $d_s(\eta)(z_i) = 0$, para todo $i \in \{1, \ldots, s\}$ pois, como $d_i | d_s$, temos que existem $q_i \in F[X]$ tais que $d_s(X) = q_i(X)d_i(X)$ e, então, $d_s(\eta)(z_i) = q_i(\eta)d_i(\eta)(z_i) = 0$, pois $anul(z_i) = (d_i)$. Logo, $d_s(\eta)(z) = 0$, para todo $z \in E$. Suponha agora, que exista $q(X) \in F[X]$ mônico tal que $q(\eta) = 0$. Em particular, $q(\eta)(z_s) = 0$, ou seja, $q \in anul(z_s) = (d_s(X))$. Portanto $d_s | q$, o que mostra que d_s é o polinômio minimal de η.

Afirmamos também que $\prod_{i=1}^{s} d_i(X)$ é o polinômio característico de η. Para uma demonstração, veja [9], capítulo XIV. Assim, para mostrarmos que E é um $F[X]-$módulo cíclico, é suficiente mostrarmos que os polinômios característico e minimal coincidem ou, equivalentemente, que o grau dos polinômios minimal e característico coincidem, ou ainda, como o grau do característico é a dimensão de E sobre F, que o grau do minimal é igual à dimensão de E sobre F. De fato, se o minimal e o característico coincidem, temos que $\prod_{i=1}^{s} d_i(X) = d_s(X)$. Logo, $\prod_{i=1}^{s-1} d_i(X) = 1$, ou seja, $d_i(X) = 1$, para todo $i \in \{0, \ldots, s-1\}$, pois são todos mônicos. Portanto, $anul(z_i) = F[X]$, o que implica que $z_i = 0$, para todo $i \in \{0, \ldots, s-1\}$, concluindo assim que $E = F[X] \cdot z$, onde $z = z_s$.

Mostremos agora que o grau do polinômio minimal da transformação linear η é igual à dimensão de E sobre F. Para isso, notemos que η satisfaz o polinômio $p(X) = X^n - 1 \in F[X]$, que é mônico, e que η não satisfaz nenhum polinômio de grau menor que n, pois isso contradiz o fato dos automorfismos $1, \eta, \eta^2, \ldots, \eta^{n-1}$ serem linearmente independentes sobre E. Assim, $p(X)$ é o polinômio minimal de η, e $\partial p = n = [E : F]$.

Temos então que $E = F[X] \cdot z$, onde $z = z_s$, ou seja, que E é um $F[X]-$módulo cíclico e, que o polinômio minimal da transformação linear η é $d_s(X) = p(X) = X^n - 1$. Nessas condições temos:

Afirmação 2: $\{z, \eta(z), \eta^2(z), \ldots, \eta^{n-1}(z)\}$ é uma base normal de E sobre F.

De fato, sejam $a_0, \ldots, a_{n-1} \in F$, tais que $\sum_{i=0}^{n-1} a_i \eta^i(z) = 0$. Considerando $q(X) = \sum_{i=0}^{n-1} a_i X^i \in F[X]$, temos que $q(X) \cdot z = q(\eta)(z) = 0$, ou seja, $q(X) \in anul(z) = (p(X))$. Como $\partial p = n$, temos que q é o polinômio nulo, pois $\partial q < n$. Assim, $a_i = 0$, para todo $i \in \{0, \ldots, n-1\}$, o que mostra que $\{z, \eta(z), \eta^2(z), \ldots, \eta^{n-1}(z)\}$ é linearmente independente sobre F. Como $[E : F] = n$, temos a afirmação.

Para finalizar, pelo Teorema 1.1.13, se F é finito, então G é cíclico, o que mostra que todos os casos foram considerados na demonstração e o teorema segue. ■

Observamos que, como na demonstração do Teorema do Elemento Primitivo, esta demonstração é existencial, ou seja, mostra-se que existe uma base normal, mas a demonstração não nos dá uma idéia de como encontrar um tal elemento normal, ou uma tal base.

Para o Teorema da Base Normal, podemos ver que a demonstração é dividida em duas partes, quando o corpo base é infinito e quando a extensão é cíclica.

Exibiremos agora outra demonstração para cada um dos casos. Para o caso em que F é infinito, Waterhouse exibe em [19] uma prova mais simples que a apresentada acima e, para o caso em que $E \supseteq F$ é cíclica, ou seja, quando $E \supseteq F$ é galoisiana, com $Gal(E/F)$ cíclico, Schwarz, em [16], além de exibir uma prova mais simples, exibe um método para a construção de uma base normal. Iniciemos com a demonstração apresentada por Waterhouse. Para isso, alguns resultados preliminares fazem-se necessários:

Lema 2.2.5. *Seja V um espaço vetorial de dimensão finita sobre um corpo F. Seja $B \subseteq V$ um subconjunto com a seguinte propriedade: "para todo funcional linear $f \in V^* = \{f : V \longrightarrow F;\ f \text{ é linear}\}$, existe $v \in B$, tal que $f(v) \neq 0$". Então o espaço vetorial V é gerado por B.*

Dem.: Suponhamos por absurdo que o espaço vetorial gerado por B, $[B]$, seja diferente de V. Então, $V = [B] \oplus W$, para algum subespaço $W \neq \{0\}$ de V. Seja $C_1 = \{v_1, \ldots, v_r\}$ uma base de $[B]$ e $C_2 = \{v_{r+1}, \ldots, v_n\}$ uma base de W sobre F. Então $C = \{v_1, \ldots, v_n\}$ é base de V sobre F. Seja agora o funcional linear f, definido por $f(v_i) = 0$, para $i \in \{1, \ldots, n-1\}$ e $f(v_n) = 1$. Para cada $v \in B$ temos que $v = \sum_{i=1}^{r} \alpha_i v_i$, onde $\alpha_i \in F$.

Logo, $f(v) = 0$, o que é contradiz a hipótese. Conseqüentemente, $[B] = V$. ■

O seguinte corolário é uma conseqüência do Teorema 1.1.8, da Independência dos Caracteres e do lema anterior.

Corolário 2.2.6. *Sejam $E \supseteq F$ uma extensão galoisiana de corpos com grupo de Galois $G = \{\eta_1, \ldots, \eta_n\}$. Para cada $i \in \{1, \ldots, n\}$, seja $d_i \in E$ dado. Então, existem $a_1, \ldots, a_n$, $b_1, \ldots, b_n$, elementos de E tais que $\sum_{i=1}^{n} a_i \eta_j(b_i) = d_j$, para todo $j \in \{1, \ldots, n\}$.*

Dem.: Sejam $V = E^n$, como espaço vetorial sobre E, e $B = \{(\eta_1(b), \eta_2(b), \ldots, \eta_n(b)) \in V;\ b \in E\} \subseteq V$. Dado $f \in V^* - \{0\}$, temos que existem $\alpha_1, \ldots, \alpha_n \in E$ não todos nulos tais que $f(v) = \sum_{i=1}^{n} \alpha_i v_i$, onde $v = (v_1, \ldots, v_n) \in V$.

Se $v \in B$, então $v = (\eta_1(b), \ldots, \eta_n(b))$, para algum $b \in E$ e, neste caso, $f(v) = \sum_{i=1}^{n} \alpha_i \eta_i(b)$. Pela independência dos caracteres, Teorema 1.1.8, temos que existe $v \in B$ tal que $f(v) \neq 0$. Portanto, para todo $f \in V^* - \{0\}$, existe $v \in B$ tal que $f(v) \neq 0$, o que mostra que B satisfaz a propriedade do lema anterior, o que mostra que $[B] = V$. Conseqüentemente, existem $b_1, \ldots, b_n \in E$ tais que $\{v_i = (\eta_1(b_i), \ldots, \eta_n(b_i));\ i \in \{1, \ldots, n\}\}$ é uma base de V sobre E.

Agora, dados $d_1, d_2, \ldots, d_n \in E$, considerando $v = (d_1, d_2, \ldots, d_n) \in V$, temos que existem $a_1, \ldots, a_n \in E$ tais que $v = \sum_{i=1}^{n} a_i v_i = \sum_{i=1}^{n} a_i(\eta_1(b_i), \eta_2(b_i), \ldots, \eta_n(b_i)) = \left(\sum_{i=1}^{n} a_i \eta_1(b_i), \sum_{i=1}^{n} a_i \eta_2(b_i), \ldots, \sum_{i=1}^{n} a_i \eta_n(b_i) \right)$, ou seja, para cada $j \in \{1, \ldots, n\}$, temos $d_j = \sum_{i=1}^{n} a_i \eta_j(b_i)$, como queríamos. ■

Agora, estamos aptos a apresentar a demonstração do Teorema da Base Normal para corpos infinitos, seguinte [19].

Teorema 2.2.7 (Teorema da Base Normal)**.** *Sejam F um corpo infinito e E uma extensão galoisiana de F. Então, $E \supseteq F$ admite uma base normal.*

Dem.: Seja $G = Gal(E/F) = \{\eta_1, \ldots, \eta_n\}$. Encontrar uma base normal de E sobre F é equivalente a encontrar $\alpha \in E$ tal que $\{\eta_1(\alpha), \ldots, \eta_n(\alpha)\}$ seja linearmente

independente sobre F. Pelo Corolário 2.2.6, dado $v = (1, 0, \ldots, 0) \in E^n$, existem $a_1, \ldots, a_n, b_1, \ldots, b_n \in E$ tais que $\sum_{i=1}^{n} a_i b_i = 1$ e $\sum_{i=1}^{n} a_i \eta(b_i) = 0$, para $\eta \neq id$. Considerando o polinômio

$$p(X_1, \ldots, X_n) = \det_{i,j} \left[\sum_{k=1}^{n} X_k \eta_j^{-1} \eta_i(b_k) \right] \in E[X_1, \ldots, X_n],$$

temos que $p(a_1, \ldots, a_n) = \det I_n = 1 \neq 0$. Assim, p não é o polinômio nulo. Como F é infinito, pelo Teorema 1.1.16, existem $x_1, \ldots, x_n$ elementos de F com $0 \neq \det_{i,j} \left[\sum_{k=1}^{n} x_k \eta_j^{-1} \eta_i(b_k) \right] = \det_{i,j} \left[\eta_j^{-1} \eta_i \left(\sum_{k=1}^{n} x_k b_k \right) \right]$. Tomamos $\alpha = \sum_{k=1}^{n} x_k b_k \in E$. Assim, a matriz $M = [\eta_j^{-1} \eta_i(\alpha)]$ é não singular e, pelo Teorema 1.1.15, temos que $\{\eta_1(c), \ldots, \eta_n(c)\}$ é uma base normal de E sobre F, como queríamos. ■

Observemos que nesta demonstração, o único resultado não trivial usado foi o Teorema da Independência dos caracteres de Dedekind. Na demonstração inicial usamos a independência algébrica dos caracteres.

Para extensões cíclicas finitas de corpos, veremos a demonstração que Schwarz exibe para a existência de bases normais. Para isso, um resultado preliminar de álgebra linear é necessário.

Teorema 2.2.8. *Seja $E \supseteq F$ uma extensão galoisiana cíclica de corpos. Então E admite uma base normal sobre F.*

Dem.: Seja $n = [E : F]$. Como $E \supseteq F$ é separável, temos, pelo Teorema do Elemento Primitivo, que existe $\alpha \in E$ tal que $E = F(\alpha)$. Como $G = Gal(E/F)$ é cíclico, temos que $G = \{1, \eta, \eta^2, \ldots, \eta^{n-1}\}$ para algum $F-$automorfismo η de E. Seja $f(X) \in F[X]$ o polinômio minimal de α sobre F. Então $\alpha, \eta(\alpha), \ldots, \eta^{n-1}(\alpha)$ são as raízes de $f(X)$ e, além disso, $\eta^i(\alpha) \neq \eta^j(\alpha)$, para $i \neq j$, pois a extensão $E \supseteq F$ é separável.

Sejam $\alpha_i = \eta^{i-1}(\alpha)$, para $i \in \{1, \ldots, n\}$.

Consideremos as matrizes

$$\Delta = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \dots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \dots & \alpha_n^{n-1} \end{pmatrix} \quad \text{e} \quad N = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ 1 & 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

É fácil ver que $N^{-1} = N^T$. Como $\{1, \alpha, \dots, \alpha^{n-1}\}$ é uma base de E sobre F e $\eta \in G$, temos que existe uma matiz invertível $C = (c_{ij}) \in M_n(F)$ satisfazendo o sistema linear

$$\begin{cases} \eta(1) = c_{0\,0} + c_{0\,1}\alpha + \dots + c_{0\,(n-1)}\alpha^{n-1} \\ \eta(\alpha) = c_{1\,0} + c_{1\,1}\alpha + \dots + c_{1\,(n-1)}\alpha^{n-1} \\ \qquad\qquad \vdots \\ \eta(\alpha^{n-1}) = c_{(n-1)\,0} + c_{(n-1)\,1}\alpha + \dots + c_{(n-1)\,(n-1)}\alpha^{n-1}. \end{cases}$$

Na notação matricial, temos

$$\begin{pmatrix} 1 \\ \alpha_2 \\ \alpha_2^2 \\ \vdots \\ \alpha_2^{n-1} \end{pmatrix} = C \begin{pmatrix} 1 \\ \alpha_1 \\ \alpha_1^2 \\ \vdots \\ \alpha_1^{n-1} \end{pmatrix} \tag{2.1}$$

Desde que $C \in M_n(F)$ e $E \supseteq F$ é galoisiana, para cada $i \in \{1, \dots, n\}$, aplicando η^{i+1} no sistema acima, obtemos

$$(1 \ \alpha_{i+1} \ \dots \ \alpha_{i+1}^{n-1})^T = C(1 \ \alpha_i \ \dots \ \alpha_i^{n-1})^T,$$

o que mostra que $C\Delta = \Delta N^T$.

Como $\det(\Delta) = \prod_{i>j}(\alpha_i - \alpha_j) \neq 0$, temos que $N^T = \Delta^{-1}C\Delta$, ou seja, N^T e C são matrizes semelhantes sobre E. Como $N^T, C \in M_n(F)$ o Teorema 1.1.20 nos garante

que existe $P \in GL_n(F)$ tal que $N^T = PCP^{-1}$. Agora, N e N^T são semelhantes sobre F. Assim, temos que existe uma matriz $Q \in GL_n(F)$ tal que $QCQ^{-1} = N$.

Seja $U = (u_1 \ u_2 \ \dots \ u_n)^T = Q(1 \ \alpha \ \dots \ \alpha^{n-1})^T$. Então, $Q^{-1}U = (1 \ \alpha \dots \alpha^{n-1})^T$.

Como Q é não singular, temos que Q é a matriz de algum automorfismo $F-$linear, T, do espaço vetorial E em relação à base $\{1, \alpha, \dots, \alpha^{n-1}\}$. Assim, o conjunto $U' = \{u_1, u_2, \dots, u_n\} = \{T(1), T(\alpha), \dots, T(\alpha^{n-1})\}$ também é linearmente independente sobre F, pois T é um isomorfismo de espaços vetoriais.

Vamos mostrar que U' é uma base normal de E sobre F. Para isso, como $Q \in GL_n(F)$, de (2.1) e, como $QCQ^{-1} = N$, obtemos

$$\eta(U) = Q(\eta(1) \ \eta(\alpha) \ \dots \ \eta(\alpha^{n-1}))^T = QC(1 \ \alpha \ \dots \ \alpha^{n-1})^T = NQ(1 \ \alpha \ \dots \ \alpha^{n-1})^T.$$

Como $U = Q(1 \ \alpha \ \dots \ \alpha^{n-1})^T$, temos que $\eta(U) = NU$. Explicitamente,

$$(\eta(u_1) \ \eta(u_2) \ \dots \ \eta(u_n))^T = (u_2 \ u_3 \ \dots \ u_n \ u_1)^T,$$

ou seja, $u_2 = \eta(u_1), u_3 = \eta(u_2) = \eta^2(u_1), \dots, \eta(u_n) = \eta^{n-1}(u_1)$, o que mostra que $U' = \{u_1, \eta(u_1), \eta^2(u_1), \dots, \eta^{n-1}(u_1)\}$, como queríamos. ■

Notamos nesta demonstração, que o único resultado não trivial utilizado, foi o Teorema 1.1.20. Todo o restante da demonstração utilizou-se apenas de conceitos básicos de álgebra linear e extensões de corpos.

Capítulo

3

Métodos para Construção de Bases Normais

Demonstramos de duas maneiras que se $E \supseteq F$ é uma extensão galoisiana de corpos, então $E \supseteq F$ admite uma base normal. Entretanto, para aplicações práticas, faz-se necessário encontrar efetivamente uma tal base normal. Dessa forma, exibiremos métodos para construção de tais bases. Inicialmente, apresentaremos um método, desenvolvido por Schwarz em [16], para construção de bases normais para extensões galoisianas cíclicas de corpos, e depois um método desenvolvido por Poli em [12] para construção de bases normais para extensões galoisianas abelianas de corpos, i.e., com grupo de Galois abeliano.

3.1 Construção de Bases Normais Para Extensões Cíclicas de Corpos

Seja $E \supseteq F$ uma extensão cíclica de grau n de corpos. Como na demonstração do Teorema 2.2.8, temos que $E = F(\alpha)$, para algum $\alpha \in E$, e $G = Gal(E/F) =$

$\{1, \eta, \eta^2, \ldots, \eta^{n-1}\}$. Considerando N e C como na demonstração do Teorema 2.2.8, temos:

Teorema 3.1.1. *Toda base normal* $\{w_1, \ldots, w_n\}$ *de* E *sobre* F *satisfaz* $(w_1 \ \ldots \ w_n)^T = Q(1 \ \alpha \ldots \ \alpha^{n-1})^T$, *onde* $Q \in GL_n(F)$ *é tal que* $QC = NQ$.

Dem.: Seja $Q \in GL_n(F)$ tal que $QC = NQ$. No Teorema 2.2.8 mostramos que as coordenadas do vetor coluna $Q(1 \ \alpha \ \alpha^2 \ \ldots \ \alpha^{n-1})^T$ formam uma base normal de E sobre F.

Reciprocamente, seja $\{w_1, \ldots, w_n\}$ uma base normal de E sobre F. Como $\{1, \alpha, \ldots, \alpha^{n-1}\}$ é uma base de E sobre F, temos que existe uma matriz mudança de base $Q \in GL_n(F)$, tal que $(w_1 \ \ldots \ w_n)^T = Q(1 \ \alpha \ \alpha^2 \ \ldots \ \alpha^{n-1})^T$. Mais ainda, como $G = \langle \eta \rangle$, dizer que $\{w_1, \ldots, w_n\}$ é uma base normal de E sobre F é equivalente a dizer que $\eta(U) = N(U)$, onde $U = (w_1 \ \ldots \ w_n)^T$. Como os coeficientes de Q estão em F, temos que $\eta(U) = \eta(Q(1 \ \alpha \ \ldots \ \alpha^{n-1})^T) = Q(\eta(1) \ \eta(\alpha) \ \ldots \ \eta(\alpha^{n-1}))^T = NU$, ou seja, $NU = QC(1 \ \alpha \ \ldots \ \alpha^{n-1})^T = QCQ^{-1}(w_1 \ \ldots \ w_n)^T = QCQ^{-1}U$.

Assim, $U = N^{-1}QCQ^{-1}U$, ou seja, $N^{-1}QCQ^{-1}$ é a matriz mudança da base $\{w_1, \ldots, w_n\}$ para a base $\{w_1, \ldots, w_n\}$, o que implica que $N^{-1}QCQ^{-1} = I_n$, a matriz identidade $n \times n$. Portanto, $QC = NQ$, como queríamos. ■

Com este resultado, nosso problema agora se resume a determinar que tipo de matrizes invertíveis $Q \in GL_n(F)$ satisfazem $QC = NQ$.

Primeiramente, suponhamos que $Q \in GL_n(F)$ satisfaz $QC = NQ$. Seja $v_i \in M_{1\times n}(F)$ a $i-$ésima linha de Q. Abusando da notação, escrevemos $Q = (v_1 \ v_2 \ \ldots \ v_n)^T$. De $QC = NQ$, obtemos

$$v_1C = v_2, \ v_2C = v_3, \ \ldots \ , v_{n-1}C = v_n \ \text{ e } \ v_nC = v_1.$$

De onde concluímos que $Q = (v_1 \ v_1C \ v_1C^2 \ \ldots \ v_1C^{n-1})$.

Reciprocamente, se $Q \in GL_n(F)$ é da forma $Q = (v_1 \ v_1C \ v_1C^2 \ \ldots \ v_1C^{n-1})^T$, para algum $v_1 \in M_{1\times n}(F) \cong F^n$, então é fácil ver que $QC = (v_1C \ v_1C^2 \ \ldots \ v_1C^n)^T = NQ$, pois $C^n = I_n$.

Assim, concluímos que encontrar bases normais de uma extensão cíclica $F(\alpha) \supseteq F$, com grupo de Galois $G = \langle \eta \rangle$, é equivalente a encontrar vetores $v \in F^n (\cong M_{1\times n}(F))$

tais que $Q = (v \ vC \ vC^2 \ \dots \ vC^{n-1})^T$ seja invertível, onde C é a matriz mudança da base $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ para a base $\{1, \eta(\alpha), \dots, \eta(\alpha^{n-1})\}$ de $F(\alpha)$ sobre F.

Com estas notações, temos:

Definição 3.1.2. *Um vetor linha $v \in M_{1\times n}(F)$ é dito ser* admissível com respeito a C *se a matriz $Q = (v \ vC \ vC^2 \ \dots \ vC^{n-1})^T$ for invertível, ou seja, se* $\det Q \neq 0$. *Para um dado vetor linha v, denotaremos por $\psi_v(X)$ o polinômio mônico de menor grau em $F[X]$ tal que $v\psi_v(C) = 0$. Tal polinômio será chamado de* polinômio minimal de v com respeito a C.

Observação 3.1.3. *Dado um vetor linha v, o polinômio $\psi_v(X)$ é unicamente determinado e $\psi_v(X) \mid X^n - 1$.*

De fato, a unicidade segue diretamente do algoritmo da divisão e da minimalidade do grau. Para mostrarmos que $\psi_v(X) \mid X^n - 1$, usando o algoritmo da divisão, temos que $X^n - 1 = \psi_v(X)q(X) + r(X)$, com $q, r \in F[X]$, e $\partial r < \partial\psi_v$. Como $C^n = 1$, temos que $0 = v(C^n - 1) = v\psi_v(C)q(C) + vr(C)$, o que implica que $vr(C) = 0$. Como $\partial r < \partial\psi_v$, temos que $r = 0$, pela minimalidade do grau de ψ_v. Logo, $\psi_v(X) \mid X^n - 1$, como queríamos.

Da condição $\det Q \neq 0$ temos que $\{v, vC, \dots, vC^{n-1}\} \subseteq M_{1\times n}(F)$ é linearmente independente sobre F. Assim, se v é admissível com respeito a C, temos que o polinômio minimal de v com respeito a C é $X^n - 1$. Reciprocamente, se o polinômio minimal de v com respeito a C é $X^n - 1$, suponhamos que existam $a_0, \dots, a_{n-1} \in F$ tais que $\sum_{i=0}^{n-1} a_i vC^i = 0$. Para o polinômio $p(X) = \sum_{i=0}^{n-1} a_i X^i \in F[X]$, temos, $vp(C) = 0$. Como $\partial p < n$, segue que $a_i = 0$, para todo $i \in \{0, \dots, n-1\}$. Logo, $\det Q \neq 0$.

Portanto, v é admissível com respeito a C se, e somente se o polinômio minimal de v com respeito a C é $X^n - 1$.

Vamos agora decompor o polinômio $f(X) = X^n - 1$ como produto de polinômios mônicos irredutíveis sobre F. Sabemos que um polinômio $f(X) \in F[X]$ tem raízes múltiplas se, e somente se mdc $\{f(X), f'(X)\} \neq c \in \dot{F}$, onde $f'(X)$ é a derivada formal do polinômio $f(X)$, ou seja, se e somente se $f(X)$ e $f'(X)$ tem fatores de grau maior ou igual a 1 em comum. Se $car(F) = 0$, então $f'(X) = nX^{n-1}$. Logo, $f'(X)$ e $f'(X)$ não têm raízes múltiplas. Se $car(F) = p > 0$, e mdc $\{n, p\} = 1$, então

$f'(X) = nX^{n-1} \neq 0$, e $f(X)$ e $f'(X)$ não tem fatores em comum. Se $car(F) = p$ e $n = p^c m$, onde $c \geq 1$ e mdc $\{m, p\} = 1$, então $X^n - 1 = X^{p^c m} - 1 = (X^m - 1)^{p^c}$. Assim, temos a fatoração de $X^n - 1$ dada por:

Proposição 3.1.4. *Seja F um corpo e $X^n - 1 \in F[X]$. Então*

$$X^n - 1 = [\varphi_1(X)\varphi_2(X)\dots\varphi_r(X)]^t,$$

onde $\varphi_1(X), \dots, \varphi_r(X)$ são fatores mônicos irredutíveis distintos de $X^n - 1$ em $F[X]$, e

(a) $t = 1$, se $car(F) = 0$ ou $car(F) = p$ com mdc $\{n, p\} = 1$.

(b) $t = p^c$, se $car(F) = p$ e $n = p^c m$, com mdc $\{m, p\} = 1$.

Consideremos agora os polinômios

$$\phi_1(X) = \frac{X^n - 1}{\varphi_1(X)},\ \phi_2(X) = \frac{X^n - 1}{\varphi_2(X)},\ \dots,\ \phi_r(X) = \frac{X^n - 1}{\varphi_r(X)}.$$

Para cada $i \in \{1, \dots, r\}$, seja W_i o subespaço vetorial de $M_{1\times n}(F)$ dado por $W_i = \{v \in M_{1\times n}(F);\ v\phi_i(C) = 0\}$. Temos então:

Lema 3.1.5. *O vetor linha $v \in M_{1\times n}(F)$ é admissível com respeito a C se, e somente se $v \in M_{1\times n}(F) - \bigcup_{i=1}^{r} W_i$.*

Dem.: Pelo exposto abaixo da Observação 3.1.3, basta mostrarmos que o polinômio minimal de um vetor linha $v \in M_{1\times n}(F)$, com respeito a C é $X^n - 1$ se, e somente se $v\phi_i(C) \neq 0$, para todo $i \in \{1, \dots, r\}$.

Se o polinômio minimal de v com respeito a C é $X^n - 1$, então claramente $v \notin W_1, \cup \dots \cup W_r$, pela definição do polinômio minimal.

Reciprocamente, suponhamos que $v\phi_i(C) \neq 0$, para todo $i \in \{1, \dots, r\}$. Seja $g(X)$ o polinômio minimal de v com respeito a C. Desde que $g(X) \mid X^n - 1$, temos que existe $q(X) \in F[X]$ tal que $g(X)q(X) = X^n - 1$. Suponhamos que $\partial q > 0$. Usando que $F[X]$ é um domínio de fatoração única e a fatoração de $X^n - 1$ dada pela Proposição 3.1.4, temos que $q(X) = s(X)\varphi_i(X)$, para algum $i \in \{1, \dots, r\}$, e $s(X) \in F[X]$. Podemos então, escrever $g(X)s(X) = \dfrac{X^n - 1}{\varphi_i(X)} = \phi_i(X)$. De onde temos que $0 = vg(C)s(C) = v\phi_i(C)$, o que contradiz a escolha de v. Portanto, $\partial q = 0$ e, como

$g(X)$ é mônico, temos que $g(X) = X^n - 1$, como queríamos. ■

Com este resultado, o problema de encontrar bases normais se resume a encontrar vetores $v \in M_{1\times n}(F)$ tais que $v \notin \bigcup_{i=1}^{r} W_i$. Para isso, precisamos de uma caracterização mais clara dos subespaços W_i, que será dada no próximo resultado.

Lema 3.1.6. *Para cada $i \in \{1, \ldots, r\}$, o subespaço vetorial W_i é igual ao subespaço vetorial V_i de $M_{1\times n}(F)$ gerado pelas linhas da matriz $\varphi_i(C)$.*

Dem.: Consideremos inicialmente $X^n - 1 = \varphi_1(X) \ldots \varphi_r(X)$, com os $\varphi_i(X)$ mônicos, irredutíveis e distintos.

Suponhamos que v satisfaz $v\phi_i(C) = 0$. O polinômio $\varphi_i(X)$ é um elemento irredutível no domínio de fatoração única $F[X]$ e, portanto, um primo em $F[X]$. Como $\varphi_i(X)$ não divide $\phi_i(X)$, temos que $\varphi_i(X)$ e $\phi_i(X)$ são relativamente primos em $F[X]$. Dessa forma, existem $g, h \in F[X]$ tais que $g(X)\varphi_i(X) + h(X)\phi_i(X) = 1$. Assim, $v = vg(C)\varphi_i(C) + vh(C)\phi_i(C) = vg(C)\varphi_i(C)$. Seja $v' = vg(C) \in F^n$. Assim, $v = v'\varphi_i(C)$, ou seja, v se escreve como uma combinação linear das linhas da matriz $\varphi_i(C)$ e, como queríamos, $v \in V_i$.

Reciprocamente, se $v \in V_i$, seja $\varphi_i(C) = (u_1 \ \ldots \ u_n)^T$ e $\phi_i(C) = (w_1 \ \ldots \ w_n)$, com $u_k \in M_{1\times n}(F)$ vetor linha e $w_j \in M_{n\times 1}(F)$ vetor coluna. Sabemos que $\varphi_i(C)\phi_i(C) = 0$ e, portanto, $u_k w_j = 0$, para todo $k, j \in \{1, \ldots, n\}$. Assim, se $v \in V_i$, existem $a_1, \ldots, a_n \in F$, tais que $v = \sum_{k=1}^{n} a_k u_k$ e, conseqüentemente, $v\phi_i(C) = \sum_{k=1}^{n} a_k u_k \phi_i(C) = \sum_{k=1}^{n} a_k u_k (w_1 \ \ldots \ w_n) = \sum_{k=1}^{n} a_k (u_k w_1 \ u_k w_2 \ \ldots \ u_k w_n) = 0$, o que mostra o lema para a decomposição $X^n - 1 = \varphi_1(X) \ldots \varphi_r(X)$.

Consideremos agora, $X^n - 1 = [\varphi_1(X) \ldots \varphi_r(X)]^{p^c}$, onde $car(F) = p$ e $n = mp^c$, com mdc $\{m, p\} = 1$ e $c \geq 1$.

Como acima, mostra-se que se $v \in V_i$, então $v\phi_i(C) = 0$.

Reciprocamente, seja $v \in M_{1\times n}(F)$ satisfazendo $v\phi_i(C) = 0$. Pelo Teorema 2.2.8, temos que $E \supseteq F$ admite uma base normal e, assim, pelo Teorema 3.1.1, existe $Q_0 \in GL_n(F)$ tal que $Q_0 C Q_0^{-1} = N$. Com isso, se $g(X) \in F[X]$, então, $Q_0 g(C) Q_0^{-1} = g(N)$. Como v

satisfaz $v\phi_i(C) = 0$, temos que $v\phi_i(C)Q_0^{-1} = 0$. Assim, $vQ_0^{-1}Q_0\phi_i(C)Q_0^{-1} = 0$. Como $Q_0\phi_i(C)Q_0^{-1} = \phi_i(N)$, temos que $vQ_0^{-1}\phi_i(N) = 0$. Escrevendo $v' = vQ_0^{-1}$, temos

$$v'\phi_i(N) = 0. \tag{3.1}$$

Se $v' = (r'_1 \ \ldots \ r'_n)$ satisfaz (3.1), então todas as linhas da matriz

$$\begin{pmatrix} v' \\ v'N \\ \vdots \\ v'N^{n-1} \end{pmatrix} = \begin{pmatrix} r'_1 & r'_2 & \ldots & r'_n \\ r'_n & r'_1 & \ldots & r'_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ r'_2 & r'_3 & \ldots & r'_1 \end{pmatrix}$$

também satisfazem (3.1), pois como N e $\phi_i(N)$ comutam $v'N^k\phi_i(N) = v'\phi_i(N)N^k = 0N^k = 0$, para todo k.

Considerando-se o polinômio $\psi(X) = r'_1 + r'_2X + r'_3X^2 + \ldots + r'_nX^{n-1} \in F[X]$, temos que a matriz acima pode ser escrita como

$$\psi(N) = r'_1I + r'_2N + r'_3N^2 + \ldots + r'_nN^{n-1}.$$

Assim, $\psi(N)\phi_i(N) = 0$, pois $\psi(N)\phi_i(N) = (v' \ v'N \ \ldots \ v'N^{n-1})^T\phi_i(N) =$
$= (v'\phi_i(N) \ v'N\phi_i(N) \ \ldots \ v'N^{n-1}\phi_i(N))^T = (0 \ \ldots \ 0)^T$.

Pelo algoritmo da divisão em $F[X]$, existem $\chi(X), r(X) \in F[X]$, tais que $\psi(X) = \varphi_i(X)\chi(X) + r(X)$, com $\partial r < \partial\varphi_i$. Dessa forma temos que $r = 0$ pois, caso contrário, teríamos que $0 = \psi(N)\phi_i(N) = [\varphi_i(N)\chi(N) + r(N)]\phi_i(N) = \varphi_i(N)\chi(N)\phi_i(N) + r(N)\phi_i(N) = r(N)\phi_i(N)$. Mas $\partial(r\phi_i) = \partial r + \partial\phi_i < \partial\varphi_i + \partial\phi_i = n$, e teríamos que o grau do polinômio minimal da matriz N seria menor que n, o que não é verdade. Então $\psi(X) = \varphi_i(X)\chi(X)$.

A primeira linha de $\psi(N)$ é $v' = (r'_1 \ \ldots \ r'_n)$. Então $v' = (1 \ 0 \ \ldots \ 0)\chi(N)\varphi_i(N)$. Seja $(k'_1 \ \ldots \ k'_n) = (1, 0, \ldots, 0)\chi(N)$. Temos que $v' = (k'_1 \ \ldots \ k'_n)\varphi_i(N)$. Usando que $NQ_0 = Q_0C$ e $\varphi_i(N)Q_0 = Q_0\varphi_i(C)$, temos $vQ_0^{-1} = v' = (k'_1 \ \ldots \ k'_n)\varphi_i(N)$. Logo, $v = (k'_1 \ \ldots \ k'_n)\varphi_i(N)Q_0 = (k'_1 \ \ldots \ k'_n)Q_0\varphi_i(C)$. Seja $(k_1 \ \ldots \ k_n) = (k'_1 \ \ldots \ k'_n)Q_0$. Então $v = (k_1 \ \ldots \ k_n)\varphi_i(C)$, ou seja, v é uma combinação linear das linhas de $\varphi_i(C)$, o que prova o lema. ■

Com os dois últimos lemas e o Teorema 3.1.1, provamos o seguinte teorema, que nos permite encontrar todas as bases normais de extensões cíclicas finitas de corpos.

Teorema 3.1.7. *Sejam $F(\alpha)$ uma extensão cíclica de grau n do corpo F e η um gerador do seu grupo de Galois G. Considere a matriz C definida em (2.1). Seja $X^n - 1 = [\varphi_1(X), \ldots, \varphi_n(X)]^{p^c}$ uma fatoração de $X^n - 1$ em fatores mônicos irredutíveis. Denote por V_i o espaço vetorial gerado pelas linhas da matriz $\varphi_i(C)$. Encontre um vetor $v \in F^n$, tal que $v \notin V_1 \cup \ldots \cup V_n$. Construa o vetor coluna*

$$\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = \begin{pmatrix} v \\ vC \\ \vdots \\ vC^{n-1} \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \vdots \\ \alpha^{n-1} \end{pmatrix}.$$

Então $\{w_1, \ldots, w_n\}$ é uma base normal de $F(\alpha)$ sobre F e, além disso, toda base normal de $F(\alpha)$ sobre F é obtida dessa forma.

Este teorema nos dá uma maneira simples de encontrar todas as bases normais para uma extensão cíclica de corpos. Para sua demonstração, o único resultado não trivial, além do usado na demonstração da existência na seção anterior, é a fatoração do polinômio $X^n - 1$. Em todo o resto utiliza-se apenas álgebra linear básica e manipulação com polinômios e matrizes.

Vejamos alguns exemplos para ilustrar:

Exemplo 3.1.8. *Seja $p(X) = X^3 - 3X + 1 \in \mathbb{Q}[X]$ irredutível sobre $\mathbb{Q}$. Seja α uma raiz de p e $E = \mathbb{Q}(\alpha)$. Nesta situação, temos que $[E : \mathbb{Q}] = 3$. É fácil ver que $(-2 + \alpha^2)$ e $(2 - \alpha - \alpha^2)$ são as outras raízes de p e que $Gal(E/\mathbb{Q}) = \langle \eta \rangle$, onde $\eta(\alpha) = (-2 + \alpha^2)$. Vamos agora encontrar uma base normal para esta extensão. Temos que $\eta(1) = 1, \eta(\alpha) = (-2 + \alpha^2)$ e $\eta(\alpha^2) = 4 - \alpha - \alpha^2$. Obtemos dessa forma as matrizes*

$$C = \begin{pmatrix} 1 & 0 & 0 \\ -2 & 0 & 1 \\ 4 & -1 & -1 \end{pmatrix} \text{ e } C^2 = \begin{pmatrix} 1 & 0 & 0 \\ 2 & -1 & -1 \\ 2 & 1 & 0 \end{pmatrix}.$$

Como $X^3-1=(X-1)(X^2+X+1)$, *temos que* $\varphi_1(X)=X-1$ *e* $\varphi_2(X)=X^2+X+1$. *Assim,*

$$\varphi_1(C)=\begin{pmatrix}0&0&0\\-2&-1&1\\4&-1&-2\end{pmatrix} \text{ e } \varphi_2(C)=\begin{pmatrix}3&0&0\\0&0&0\\6&0&0\end{pmatrix}.$$

Dessa forma, V_1 *é o subespaço gerado por* $(-2\ \ -1\ \ 1)$ *e* $(4\ \ -1\ \ -2)$, *que são as linhas não nulas da matriz* $\varphi_1(C)$, *e* V_2 *é o subespaço gerado por* $(3\ 0\ 0)$. *É fácil ver que* $v=(0\ 0\ 1)\notin V_1\cup V_2$. *Observamos que* $vC=(4\ \ -1\ \ -1)$ *e que* $vC^2=(2\ 1\ 0)$. *Assim, temos:*

$$\begin{pmatrix}w_1\\w_2\\w_3\end{pmatrix}=\begin{pmatrix}0&0&1\\4&-1&-1\\2&1&0\end{pmatrix}\begin{pmatrix}1\\\alpha\\\alpha^2\end{pmatrix}=\begin{pmatrix}\alpha^2\\4-\alpha-\alpha^2\\2+\alpha\end{pmatrix}$$

e observamos que $\eta(w_1)=w_2$ *e* $\eta^2(w_1)=\eta(w_2)=w_3$. *Logo,* $\{w_1,w_2,w_3\}=\{\alpha^2,4-\alpha-\alpha^2,2+\alpha\}$ *é uma base normal de* E *sobre* $\mathbb{Q}$.

Exemplo 3.1.9. *Seja* $F=\mathbb{F}_7$ *e* $P(X)=X^3+2\in F[X]$. *O polinômio* $p(X)$ *é irredutível sobre* F *pois se* $0\neq a\in F$, *então* $a^3=\pm1$. *Sejam* α *uma raiz de* p *e* $E=F(\alpha)$. *Então,* $\alpha^3=-2$ *e* $Gal(E/F)=\langle\eta\rangle$, *onde* $\eta:E\longrightarrow E$ *é dado por* $\eta(x)=x^7$. *Assim, temos que* $\eta(1)=1$, $\eta(\alpha)=\alpha^7=(\alpha^3)^2\alpha=4\alpha$ *e* $\eta(\alpha^2)=\alpha^{14}=(\alpha^3)^4\alpha^2=2\alpha^2$. *Logo,*

$$C=\begin{pmatrix}1&0&0\\0&4&0\\0&0&2\end{pmatrix} \text{ e } C^2=\begin{pmatrix}1&0&0\\0&2&0\\0&0&4\end{pmatrix}.$$

Fatorando X^3-1, *temos* $X^3-1=(X-1)(X-2)(X-4)$. *Assim,* $\varphi_1(X)=X-1,\varphi_2(X)=(X-2)$ *e* $\varphi_3(X)=X-4$ *e*

$$\varphi_1(C)=\begin{pmatrix}0&0&0\\0&3&0\\0&0&1\end{pmatrix},\varphi_2(C)=\begin{pmatrix}-1&0&0\\0&2&0\\0&0&0\end{pmatrix} \text{ e } \varphi_3(C)=\begin{pmatrix}-3&0&0\\0&0&0\\0&0&-2\end{pmatrix}.$$

Com isso, temos que $V_i=\{(x_1\ \ x_2\ \ x_3)\in F^3;\ x_i=0\}$, *para* $i=1,2,$ *ou* 3. *Assim,* $v=(x_1\ \ x_2\ \ x_3)\notin V_1\cup V_2\cup V_3$ *se, e somente se* $x_1x_2x_3\neq0$.

Tomemos então, $v = (1\ 1\ 1)$. *Assim,* $vC = (1\ 4\ 2)$, $vC^2 = (1\ 2\ 4)$ *e*

$$\begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 4 & 2 \\ 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix} = \begin{pmatrix} 1+\alpha+\alpha^2 \\ 1+4\alpha+2\alpha^2 \\ 1+2\alpha+4\alpha^2 \end{pmatrix}.$$

É fácil ver que $\eta(w_1) = w_2$ *e* $\eta(w_2) = w_3$. *Ou seja, o conjunto* $\{w_1, w_2, w_3\} = \{1+\alpha+\alpha^2, 1+4\alpha+2\alpha^2, 1+2\alpha+4\alpha^2\}$ *é uma base normal de* E *sobre* F.

3.2 Construção de Bases Normais Para Extensões Abelianas de Corpos

Nesta seção apresentaremos um método para construção de bases normais para extensões galoisianas abelianas de corpos, desenvolvido por Poli em [12].

No que segue nesta seção, $E \supseteq F$ será uma extensão galoisiana abeliana de corpos, isto é, uma extensão galoisiana com grupo de Galois abeliano de ordem $n = [E : F]$. Da decomposição dos grupos abelianos finitos, temos que $G = Gal(E/F) = \langle\eta_1\rangle \times \ldots \times \langle\eta_k\rangle$, onde $\langle\eta_i\rangle$ é o grupo cíclico gerado por η_i e $|\langle\eta_i\rangle| = e_i$, para $i \in \{1, \ldots, k\}$. Consideremos o anel de polinômios $F[X_1, \ldots, X_k]$ e seu ideal $I = (X_1^{e_1} - 1, \ldots, X_k^{e_k} - 1)$. Denotaremos por A, o anel quociente $\dfrac{F[X_1, \ldots, X_k]}{I}$.

No que segue, para cada $i \in \{1, \ldots, k\}$, usaremos as seguintes notações:

- α_i será uma raiz de $X^{e_i} - 1$.
- H_i será o conjunto de todas as raízes de $X^{e_i} - 1 \in F[X]$.
- $p_i \in F[X]$ será o polinômio minimal de α_i sobre F, e m_i a multiplicidade deste fator na decomposição de $X_i^{e_i} - 1$ em fatores irredutíveis sobre F.
- $M = m_1 + m_2 + \ldots + m_k - (k-1)$.

Observemos que pela Proposição 3.1.4, m_i não depende da escolha de p_i e, portanto, M está bem definido.

Sejam $K = F(\alpha_1, \ldots, \alpha_k)$, e $\mathcal{G} = Gal(K/F)$, A ação de $\mathcal{G}$ em $H_1 \times \ldots \times H_k$ é dada por $\eta \cdot (\alpha_1, \ldots, \alpha_k) \mapsto (\eta(\alpha_1), \ldots, \eta(\alpha_k))$, onde $\eta \in \mathcal{G}$, e $(\alpha_1, \ldots, \alpha_k) \in H_1 \times \ldots \times H_k$.

Observemos que $H_1 \times H_2 \times \ldots \times H_k$ é particionado em órbitas quando $\mathcal{G}$ age sobre ele. Denotaremos por N a quantidade de órbitas distintas.

Definição 3.2.1. *Para cada $i \in \{2, \ldots, k\}$, sejam $W_i(\alpha_1, \ldots, \alpha_{i-1}, X_i)$ o polinômio minimal de α_i sobre $F(\alpha_1, \ldots, \alpha_{i-1})$ e $\pi_i(\alpha_1, \ldots, \alpha_{i-1}, X_i) = p_i(X_i)/W_i(\alpha_1, \ldots, \alpha_{i-1}, X_i)$.*

Considerando $W_i(\alpha_1, \ldots, \alpha_{i-1}, X_i)$ e $\pi_i(\alpha_1, \ldots, \alpha_{i-1}, X_i)$ como duas expressões polinomiais em $\alpha_1, \ldots, \alpha_{i-1}$ e X_i sobre F, substituímos α_j por indeterminadas independentes X_j, para todo $j \in \{1, \ldots, i-1\}$ nestas expressões, e obtemos os polinômios $W_i(X_1, \ldots, X_i)$ e $\pi_i(X_1, \ldots, X_i) \in F[X_1, \ldots, X_i]$, que denotaremos por W_i e π_i, respectivamente.

Definição 3.2.2. *Para cada $k-$upla $(\alpha_1, \ldots \alpha_k) \in H_1 \times \ldots \times H_k$, seja:*

$$g_{\alpha_1,\ldots,\alpha_k}(X_1, \ldots, X_k) = \left(\frac{X_1^{e_1} - 1}{p_1^{m_1}}\right) \ldots \left(\frac{X_k^{e_k} - 1}{p_k^{m_k}}\right) \pi_2^{m_1+m_2-1} \ldots \pi_k^{m_1+m_2+\ldots+m_k-(k-1)}.$$

Se a $k-$upla já está especificada, usaremos a notação $g_{i_1,\ldots,i_k}$ para o polinômio

$$g_{i_1,\ldots,i_k} = \left(\frac{X_1^{e_1} - 1}{p_1^{i_1}}\right) \ldots \left(\frac{X_k^{e_k} - 1}{p_k^{i_k}}\right) \pi_2^{i_1+i_2-1} \ldots \pi_k^{i_1+i_2+\ldots+i_k-(k-1)},$$

para cada $i_j \in \{1, \ldots, m_j\}$, e $j \in \{1, \ldots, k\}$.

Observe que $\pi_i(\alpha_1, \ldots, \alpha_j) \neq 0$, para todo $i \in \{2, \ldots, k\}$, pois p_i não tem fatores irredutíveis com multiplicidade maior que 1, e $W_i(\alpha_1, \ldots, \alpha_{i-1}, X_i)$ é o polinômio minimal de α_i sobre $F(\alpha_1, \ldots, \alpha_{i-1})$. Assim, como α_i não é raiz de $\dfrac{X_i^{e_i} - 1}{p_i^{m_i}}$, para todo $i \in \{1, \ldots, k\}$, temos que $g_{\alpha_1,\ldots,\alpha_k}(\alpha_1, \ldots, \alpha_k) \neq 0$.

Observe também que $g_{\alpha_1,\ldots,\alpha_k}$ não depende da $k-$upla $(\alpha_1, \ldots, \alpha_k)$, mas apenas de sua órbita, já que os elementos de $\mathcal{G}$ levam raízes de polinômios irredutíveis em raízes de polinômios irredutíveis. Assim, o conjunto dos polinômios $g_{\alpha_1,\ldots,\alpha_k}$ tem cardinalidade N e chamá-los-emos de $g_1, \ldots, g_N$.

Sejam $(\alpha_1, \ldots, \alpha_k) \in H_1 \times \ldots \times H_k$ e g_i o polinômio associado à órbita de $(\alpha_1, \ldots, \alpha_k)$. Denotaremos por P_i o ideal em $F[X_1, \ldots, X_k]$ que é o conjunto de todos os polinômios que se anulam em $(\alpha_1, \ldots, \alpha_k)$ e por $\overline{P_i}$ a imagem de P_i pela projeção canônica de $F[X_1, \ldots, X_k]$ em A. Observe que P_i não depende de $(\alpha_1, \ldots, \alpha_k)$, mas apenas de sua órbita.

Para uma melhor caracterização de P_i, temos:

Proposição 3.2.3. *Em $F[X_1, \ldots, X_k]$ temos que $P_i = (p_1, W_2, \ldots, W_k)$.*

Dem.: Para mostrar isso, vamos mostrar que dado $p(X_1, \ldots, X_k) \in K[X_1, \ldots, X_k]$, temos que $p(\alpha_1, \ldots, \alpha_k) = 0$ se, e somente se $p \in (p_1, W_2, \ldots, W_k)$.

Aplicando o algoritmo da divisão em $F[X_2, \ldots, X_k][X_1]$, obtemos que existem $q_1, r_1 \in F[X_1, \ldots, X_k]$ tais que $p(X_1, \ldots, X_k) = p_1(X_1)q_1(X_1, \ldots, X_k) + r_1(X_1, \ldots, X_k)$, e o grau parcial de r_1 com relação a X_1, $\partial_1 r_1$, é menor que ∂p_1. Do mesmo modo, aplicamos o algoritmo da divisão para r_1 e W_2 e, assim, sucessivamente, até que obtemos $q_1, \ldots, q_k, r \in F[X_1, \ldots, X_k]$ tais que $p(X_1, \ldots, X_k) = p_1(X_1)q_1(X_1, \ldots, X_k) + W_2(X_1, X_2)q_2(X_1, \ldots, X_k) + \ldots + W_k(X_1, \ldots, X_k)q_k(X_1, \ldots, X_k) + r(X_1, \ldots, X_k)$, com $r(X_1, \ldots, X_k)$ satisfazendo $\partial_j r < \partial_j W_j$, para todo $j \in \{2, \ldots, k\}$.

Assim, como $p_1(\alpha_1) = 0$ e $W_j(\alpha_1, \ldots, \alpha_i) = 0$, para todo $j \in \{2, \ldots, k\}$, temos que $p(\alpha_1, \ldots, \alpha_k) = 0$ se, e somente se $r(\alpha_1, \ldots, \alpha_k) = 0$.

Observando-se que o polinômio $r(\alpha_1, \ldots, \alpha_{k-1}, X_k)$ tem grau menor que o grau de $W_k(\alpha_1, \ldots, \alpha_{k-1}, X_k)$, que é o polinômio minimal de α_k sobre $F(\alpha_1, \ldots, \alpha_{k-1})$ e que α_k é raiz de $r(\alpha_1, \ldots, \alpha_{k-1}, X_k)$, temos que $r(\alpha_1, \ldots, \alpha_{k-1}, X_k) = 0$, ou seja, $\partial_k r = 0$.

Repetindo o mesmo procedimento, concluímos que $\partial_j r = 0$, para todo $j \in \{1, \ldots, k\}$, ou seja, $r = 0$.

Assim, temos que $p(\alpha_1, \ldots, \alpha_k) = 0$ se, e somente se $r = 0$, ou seja, se, e somente se $p \in (p_1, W_2, \ldots, W_k)$. ■

Proposição 3.2.4. *Se P_i e $\overline{P_i}$ são definidos como acima, então P_i é um ideal maximal em $F[X_1, \ldots, X_k]$ e $\overline{P_i}$ é um ideal maximal em A.*

Dem.: Para mostrarmos que P_i é um ideal maximal em $F[X_1, \ldots, X_k]$, vamos mostrar que o anel $\dfrac{F[X_1, \ldots, X_k]}{P_i}$ é um corpo. Para isto, seja $(q(X_1, \ldots, X_k) + P_i) \in \dfrac{F[X_1, \ldots, X_k]}{P_i} - \{0\}$. Vamos mostrar que q tem inverso em $\dfrac{F[X_1, \ldots, X_k]}{P_i}$. Se $p_j(X_j) | q(X_1, \ldots, X_k)$, para todo $j \in \{1, \ldots, k\}$, então $q(\alpha_1, \ldots, \alpha_k) = 0$, o que implica que $q(X_1, \ldots, X_k) + P_i = 0 + P_i$. Assim, existe $j_0 \in \{1, \ldots, k\}$ tal que p_{j_0} não divide $q(X_1, \ldots, X_k)$. Como p_{j_0} é irredutível sobre $F[X_{j_0}]$, segue que é irredutível sobre $F[X_1, \ldots, X_k]$. Assim, existem $g, h \in F[X_1, \ldots, X_k]$ tais que $q(X_1, \ldots, X_k)g(X_1, \ldots, X_k) + p_{j_0}(X_{j_0})h(X_1, \ldots, X_k) = 1$ em $F[X_1, \ldots, X_k]$. Logo, como $p_{j_0} \in P_i$, segue que $q(X_1, \ldots, X_k)g(X_1, \ldots, X_k) + P_i = 1 + P_i$, ou seja, $g(X_1, \ldots, X_k) + P_i$

é o inverso de $q(X_1,\ldots,X_k)+P_i$ em $\dfrac{F[X_1,\ldots,X_k]}{P_i}$ e, conseqüentemente, $\dfrac{F[X_1,\ldots,X_k]}{P_i}$ é corpo, como queríamos.

Que o ideal $\overline{P_i}$ é maximal em A, segue facilmente do fato que $I \subseteq P_i$. ■

Veremos agora alguns resultados técnicos que serão necessários para a demonstração dos resultados principais desta seção. As demonstrações de alguns deles serão omitidas pois são muito técnicas e fogem aos objetivos deste trabalho. O leitor interessado, pode encontrá-las nas referências [12] e [13].

Lema 3.2.5. *Sejam $g_1 \neq g_2$ polinômios associados a $k-$uplas $(\alpha_1,\ldots,\alpha_k)$ e $(\alpha'_1,\ldots,\alpha'_k)$, respectivamente. Então, temos que $\overline{g_1 g_2} = 0$ em A.*

Dem.: Sejam p_i e $p'_i \in F[X_i]$ os polinômios minimais de α_i e α'_i sobre F, respectivamente, e W_i e $W'_i \in F(\alpha_1,\ldots,\alpha_{i-1})[X_i]$ os polinômios minimais de α_i e α'_i sobre $F(\alpha_1,\ldots,\alpha_{i-1})$ e $F(\alpha'_1,\ldots,\alpha'_{i-1})$, respectivamente. Sejam $\pi_i(\alpha_1,\ldots,\alpha_{i-1},X_i) = \dfrac{p_i}{W_i(\alpha_1,\ldots,\alpha_{i-1})}$ e $\pi'_i(\alpha'_1,\ldots,\alpha'_{i-1},X_i) = \dfrac{p'_i}{W'_i(\alpha'_1,\ldots,\alpha'_{i-1})}$.

Se existe $i \in \{1,\ldots,k\}$ tal que $p_i \neq p'_i$, então, $X_i^{e_i} - 1$ divide $g_1 g_2$ e, portanto, $\overline{g_1 g_2} = 0$ em A.

Caso contrário, como $g_1 \neq g_2$, existe $j \in \{1,\ldots,k\}$ tal que $W_j \neq W'_j$. Tome o menor j com esta propriedade. Podemos supor que $\alpha_i = \alpha'_i$, para todo $i \in \{1,\ldots,j-1\}$, pois $p_i = p'_i$, e $W_i = W'_i$, para todo $i \in \{1,\ldots,j-1\}$.

Como W_j e W'_j são irredutíveis sobre $F(\alpha_1,\ldots,\alpha_{j-1})$, segue que p_j divide $W_j W'_j$, ou seja, existe $q_j(\alpha_1,\ldots,\alpha_{j-1},X_j) \in F(\alpha_1,\ldots,\alpha_{j-1})[X_j]$, tal que $p_j(X_j) = q_j(\alpha_1,\ldots,\alpha_{j-1})W_j(\alpha_1,\ldots,\alpha_{j-1})W'_j(\alpha_1,\ldots,\alpha_{j-1})$.

Assim, $\pi_j(\alpha_1,\ldots,\alpha_{j-1},X_j)\pi'_j(\alpha_1,\ldots,\alpha_{j-1},X_j) = q_j(\alpha_1,\ldots,\alpha_{j-1},X_j)p_j(X_j)$. Da mesma maneira que fizemos quando definimos os polinômios W_i e π_i, substituímos α_i por X_i e obtemos $\pi_j(X_1,\ldots,X_j)\pi'_j(X_1,\ldots,,X_j) = q_j(X_1,\ldots,X_j)p_j(X_j)$.

Observemos que $\dfrac{X_j^{e_j}-1}{p_j^{m_j}}(\pi_j\pi'_j)^{m_1+\cdots+m_j-(j-1)}$ é um fator de $g_1 g_2$. Mas, como $m_1+\cdots+m_j-(j-1) \geq m_j$, segue que $X_j^{e_j}-1$ divide $g_1 g_2$ e, conseqüentemente, $\overline{g_1 g_2} = 0$ em A. ■

Lema 3.2.6. *Se $g_1,\ldots,g_N$ são definidos como acima, então:*
1) Para cada $i \in \{1,\ldots,N\}$, existe um elemento idempotente $\overline{E_i}$ em $(\overline{g_i})$ satisfazendo $(\overline{E_i}) = (\overline{g_i})$.

2) $A = (\overline{g_1}) \oplus \cdots \oplus (\overline{g_N}) = (\overline{E_1}) \oplus \cdots \oplus (\overline{E_N})$.

Lema 3.2.7. *para* $i \in \{1, \ldots, N\}$, *temos*
1)$\overline{P_i^M}(\overline{g_i}) = \{0\}$.
2)$\overline{P_i}(\overline{g_i})$ *é o ideal maximal em* $(\overline{g_i})$.
3)$\overline{P_i^{M-1}}(\overline{g_i})$ *é o ideal minimal de* $(\overline{g_i})$. *Este ideal é o ideal gerado pelo polinômio* $g_{1,\ldots,1}$.

Lema 3.2.8. *Em* A, *temos que* $anul(\overline{g_i}) = \overline{P_i^M} = \bigoplus_{j \neq i}(\overline{g_j})$.

Dem.: Como $A = (\overline{g_1}) \oplus \cdots \oplus (\overline{g_N})$, temos que $\overline{P_i} = \overline{P_i}(\overline{g_1}) \oplus \cdots \overline{P_i}(\overline{g_i}) \oplus \cdots \oplus \overline{P_i}(\overline{g_N})$. Mas, $(\overline{g_j}) \subseteq \overline{P_i}$, se $i \neq j$. Assim, $\overline{P_i} = (\overline{g_1}) \oplus \cdots \oplus (\overline{g_{i-1}}) \oplus \overline{P_i}(\overline{g_i}) \oplus (\overline{g_{i+1}}) \oplus \cdots \oplus (\overline{g_N})$ e $\overline{P_i}^M = (\overline{g_1}) \oplus \cdots \oplus (\overline{g_{i-1}}) \oplus \overline{P_i}^M(\overline{g_i}) \oplus (\overline{g_{i+1}}) \oplus \cdots \oplus (\overline{g_N})$. Pelo ítem 1 do Lema 3.2.7, temos que $\overline{P_i}^M(\overline{g_i}) = \{0\}$. Portanto, $\overline{P_i}^M = (\overline{g_1}) \oplus \cdots \oplus (\overline{g_{i-1}}) \oplus (\overline{g_{i+1}}) \oplus \cdots \oplus (\overline{g_N})$.

Pelo Lema 3.2.6, temos que $(\overline{g_i}) = (\overline{E_i})$, onde $\overline{E_i}$ é idempotente. Assim, temos que $anul(\overline{g_i}) = anul(\overline{E_i}) = (\overline{E_1}) \oplus \cdots \oplus (\overline{E_{i-1}}) \oplus (\overline{E_{i+1}}) \oplus \cdots \oplus (\overline{E_N}) = (\overline{g_1}) \oplus \cdots \oplus (\overline{g_{i-1}}) \oplus (\overline{g_{i+1}}) \oplus \cdots \oplus (\overline{g_N}) = \overline{P_i}^M$. ■

Depois dos resultados enunciados acima, vamos ao método de construção de bases normais para extensões abelianas de corpos, lembrando que como G é abeliano, podemos escrever $G = \langle \eta_1 \rangle \times \ldots \times \langle \eta_k \rangle$, com $\eta_i \in G$, para todo $i \in \{1 \ldots k\}$, e $|\langle \eta_i \rangle| = e_i$.

Definição 3.2.9. *Seja* $S \subseteq E$ *um subconjunto qualquer. Definimos o* $\eta-$*anulador de* S *como sendo o ideal dos polinômios* $p \in F[X_1, \ldots, X_k]$ *tais que* $p(\eta_1, \ldots, \eta_k)(v) = p(\eta)(v) = 0$, *para todo* $v \in S$. *Denotá-lo-emos por* $anul_\eta(S)$.

Lema 3.2.10. *Seja* $J = anul_\eta(E)$. *Então* $J = I$.

Dem.: Desde que $\eta_1^{e_1} = \ldots = \eta_k^{e_k} = id$, temos que $I \subseteq J$. Seja agora $p \in J$. Aplicando o algoritmo da divisão em $F[X_2, \ldots, X_k][X_1]$, obtemos polinômios $q_1, r_1 \in F[X_1, \ldots, X_k]$ tais que $p(X_1, \ldots, X_k) = q_1(X_1, \ldots, X_k)(X_1^{e_1} - 1) + r_1(X_1, \ldots, X_k)$, com $\partial_1 r_1 < e_1$. Repetindo o mesmo procedimento com o polinômio r_1 e assim, sucessivamente, obtemos polinômios $q_1, \ldots, q_k, r \in F[X_1, \ldots, X_k]$ tais que

$$p(X_1, \ldots, X_k) = (X_1^{e_1} - 1)q_1 + \ldots + (X_k^{e_k} - 1)q_k + r(X_1, \ldots, X_k),$$

com $r(X_1,\ldots,X_k)=\sum_{i=1}^{m}\alpha_i\prod_{j=1}^{k}X_j^{r_{ij}}$, onde $m\in\mathbb{N}$, $(r_{i1},\ldots,r_{ik})\neq(r_{s1},\ldots,r_{sk})$ se $s\neq i$, $r_{ij}<e_j$, para todo $i\in\{1,\ldots m\}, j\in\{1,\ldots,k\}$ e $\alpha_1,\ldots,\alpha_m\in F$. Observe que $p(\eta)=r(\eta)$. Se mostrarmos que $r=0$ então, $p\in I$.

Suponhamos que $\prod_{j=1}^{k}\eta_j^{r_{ij}}=\prod_{j=1}^{k}\eta_j^{r_{sj}}$, onde $i,s\in\{1,\ldots,m\}$. Então $\eta_1^{r_{i1}-r_{s1}}=\prod_{j=2}^{k}\eta_j^{r_{sj}-r_{ij}}$. Assim, $\eta_j^{r_{ij}-r_{sj}}=id$ e, $r_{ij}-r_{sj}\in e_j\mathbb{Z}$, para todo $j\in\{1,\ldots,k\}$. Como $r_{ij}<e_j$, para todo $i\in\{1,\ldots,m\}$, temos que $r_{ij}=r_{sj}$ e, portanto, $s=i$. Assim, $\prod_{j=1}^{k}\eta_j^{r_{ij}}\neq\prod_{j=1}^{k}\eta_j^{r_{sj}}$, sempre que $i\neq s$. Desde que $p\in J$, temos que $0=p(\eta)(v)=r(\eta)(v)$, para todo $v\in E$. Dessa forma, temos que $0=r(\eta)(v)=\sum_{i=1}^{m}\alpha_i\prod_{j=1}^{k}\eta_j^{r_{ij}}(v)$, para todo $v\in E$ e, pela independência linear dos m automorfismos distintos, $\prod_{j=1}^{k}\eta_j^{r_{ij}}, i\in\{1,\ldots,m\}$, Teorema 1.1.8, temos que $\alpha_i=0$, para todo $i\in\{1,\ldots,m\}$ e, portanto, $r=0$. O que mostra que $p\in I$ e, conseqüentemente, $J=I$, como queríamos. ■

Lema 3.2.11. *Temos uma decomposição em soma direta*

$$E=Im(g_1(\eta))\oplus\ldots\oplus Im(g_N(\eta)).$$

Dem.: Como do Lema 3.2.6, $A=(\overline{g_1})\oplus\ldots\oplus(\overline{g_N})$, temos que existem $\lambda_1,\ldots,\lambda_N\in F[X_1,\ldots,X_k]$, tais que $\overline{1}=\overline{\lambda_1}\overline{g_1}+\ldots+\overline{\lambda_N}\overline{g_N}$ em A, o que implica que $1-(\lambda_1g_1+\ldots\lambda_Ng_N)\in I$. Como $I=anul_\eta(E)$, temos que $v=id(v)=\lambda_1(\eta)g_1(\eta)(v)+\ldots+\lambda_N(\eta)g_N(\eta)(v)=g_1(\eta)\lambda_1(\eta)(v)+\ldots+g_N(\eta)\lambda_N(\eta)(v)$, para todo $v\in E$, o que mostra que $E=Img_1(\eta)+\ldots+Img_N(\eta)$.

Para mostrarmos que esta soma é direta, suponhamos que $0=y_1+\ldots+y_N$, com $y_i=g_i(\eta)(u_i)$, para algum $u_i\in E$. Como $(\overline{g_i})=(\overline{E_i})$, para cada i, temos que existe $h_i\in A$ tal que $\overline{g_i}=\overline{E_ih_i}$. Como $A=(\overline{E_1})\oplus\ldots\oplus(\overline{E_N})$ e E_j é idempotente, temos que

$$0=E_j(\eta)(0)=E_j(\eta)(y_1+\ldots+y_N)=\sum_{i=1}^{N}E_j(\eta)(y_i).$$

Afirmamos que $E_j(\eta)(y_i) = y_i\delta_{ij}$. De fato, como $A = (\overline{E_1}) \oplus \ldots \oplus (\overline{E_N})$, temos que $\overline{E_i}\,\overline{E_j} \in (\overline{E_i}) \cap (\overline{E_j}) = \{0\}$. Portanto, $E_iE_j \in I$, se $i \neq j$. Assim, $E_j(\eta)E_i(\eta)(u) = 0$, para todo $i \neq j$ e $u \in E$. Como cada E_j é idempotente, temos que $\overline{E_j}^2 - \overline{E_j} = 0$, ou seja, $E_j^2 - E_j \in I$. Como $I = anul_\eta(E)$, temos que $(E_j^2(\eta) - E_j(\eta))(u) = 0$, para todo $u \in E$. Portanto, $E_j^2(\eta)(u) = E_j(\eta)(u)$, para todo $u \in E$. Assim, $E_j(\eta)(y_i) = E_j(\eta)(g_i(\eta)(u_i)) = E_j(\eta)E_i(\eta)h_i(\eta)(u_i) = 0$, se $i \neq j$.

Para $i = j$ temos $E_j(\eta)(y_j) = E_j^2(\eta)(h_j(\eta)(u_j)) = E_j(\eta)h_j(\eta)(u_j) = g_j(\eta)(u_j) = y_j$. Logo, $E_j(\eta)(y_i) = y_i\delta_{ij}$, e

$$0 = \sum_{i=1}^{N} E_j(\eta)(y_i) = y_j,$$

para todo $j \in \{1, \ldots, N\}$, ou seja, a soma é direta. ■

Teorema 3.2.12. *Para cada $i \in \{1, \ldots, N\}$, existe pelo menos um elemento $t_i \in Im(g_i(\eta))$, tal que o $\eta-$anulador de t_i é P_i^M.*

Dem.: Notemos inicialmente, que existe pelo menos um $t_i \in Im(g_i(\eta))$ tal que $P_i^{M-1}(\eta)(t_i) \neq 0$ pois, caso contrário, $P_i^{M-1}(\eta)g_i(\eta)E = 0$ e, neste caso, teríamos que $P_i^{M-1}(g_i) \subseteq I$. Ou seja, $\overline{P_i^{M-1}}(\overline{g_i}) = 0$, o que contradiz o Lema 3.2.7.

Seja t_i um tal elemento. Então $t_i = g_i(\eta)(u_i)$, para algum $u_i \in E$. Como $P_i^{M-1}(\eta)(t_i) \neq 0$, existe $c \in P_i^{M-1}(g_i)$ tal que $c(\eta)(u_i) \neq 0$. Assim, $c \notin I$ e, portanto, $\overline{c} \in \overline{P_i^{M-1}}(\overline{g_i}) - \{0\}$.

Seja agora, $J_i = anul_\eta(\{g_i(\eta)(u_i)\})$. O ideal $\overline{J_i}(\overline{g_i})$ está contido em $(\overline{g_i})$ e, portanto, $\overline{J_i}(\overline{g_i})$ contém o ideal minimal de $(\overline{g_i})$, ou é o ideal nulo. Como $\overline{c} \in \overline{P_i^{M-1}}(\overline{g_i})$ e, pelo Lema 3.2.7 $\overline{P_i^{M-1}}(\overline{g_i})$ é o ideal minimal de $(\overline{g_i})$, se mostrarmos que $\overline{c} \notin \overline{J_i}(\overline{g_i})$, concluímos que $\overline{J_i}(\overline{g_i})$ é o ideal nulo. Suponhamos, por absurdo, que $\overline{c} \in \overline{J_i}(\overline{g_i})$. Então, podemos escrever $c = q_ig_i + h_i$, onde $q_i \in J_i$, e $h_i \in I$. Assim, temos que $c(\eta)(u_i) = q_i(\eta)(g_i(\eta)(u_i)) + h_i(\eta)(u_i) = q_i(\eta)(g_i(\eta)(u_i))$, pois $I = anul_\eta(E)$. Mas, como $q_i \in J_i = anul_\eta(\{g_i(\eta)(u_i)\})$, temos que $c(\eta)(u_i) = 0$, o que contradiz a escolha de c.

Como pelo Lema 3.2.7 $\overline{P_i^M} = anul(\overline{g_i})$, segue que $\overline{J_i} \subseteq \overline{P_i^M}$.

Se $\overline{q_i} \in \overline{P_i^M}$, então $\overline{q_i}(\overline{g_i}) = 0$. Assim, $q_i(\eta)(g_i(\eta)(u_i)) = 0$ e, $q_i \in J_i = anul_\eta(t_i)$, ou seja, $\overline{q_i} \in \overline{J_i}$, e concluímos que $\overline{P_i^M} = \overline{J_i}$. Logo, P_i^M é o $\eta-$ anulador de $\{t_i\}$. ■

Corolário 3.2.13. *Dada uma base B de E sobre F, para cada $i \in \{1, \ldots, N\}$, existe $w_i \in B$ tal que $anul_\eta(\{g_i(\eta)(w_i)\})$ é P_i^M.*

Dem.: Pela demonstração do teorema anterior, basta mostrar que existe $w_i \in B$ tal que $P_i^{M-1}(g_i(\eta)(w_i)) \neq 0$.

Para isso, suponhamos que $P_i^{M-1}(g_i(\eta)(w)) = 0$, para todo $w \in B$. Então $P_i^{M-1}(\eta)g_i(\eta)E = 0$, o que implica que $P_i^{M-1}(g_i) \subseteq I$. Conseqüentemente $\overline{P_i^{M-1}}(\overline{g_i}) = \{0\}$, o que contradiz o Lema 3.2.7. ■

Com tudo isso, podemos encontrar um elemento normal da extensão $E \supseteq F$.

Teorema 3.2.14. *Para cada $i \in \{1, \ldots N\}$, sejam w_i como no corolário anterior e $t_i = g_i(\eta)(w_i)$. Então $y = t_1 + \ldots + t_N \in E$, é um gerador de uma base normal de E sobre F.*

Dem.: Para mostrarmos que y gera uma base normal de E sobre F, temos que mostrar que o conjunto $\{\eta_1^{i_1}\eta_2^{i_2}\ldots\eta_k^{i_k}(y);\ i_j \in \{0,\ldots,e_j-1\}, j \in \{1,\ldots,k\}\} = \{\eta(y); \eta \in G\}$ é linearmente independente sobre F, ou seja, que se $\sum \alpha_{i_1,\ldots,i_k}\eta_1^{i_1}\eta_2^{i_2}\ldots\eta_k^{i_k}(y) = 0$, com $\alpha_{i_1,\ldots,i_k} \in F$ e $i_j \in \{0,\ldots,e_j-1\}$, para cada $j \in \{1,\ldots k\}$, então $\alpha_{i_1,\ldots,i_k} = 0$. Isto é equivalente a mostrar que para todo $u(X_1,\ldots,X_k) = \sum \alpha_{i_1,\ldots,i_k}X_1^{i_1}X_2^{i_2}\ldots X_k^{i_k} \in F[X_1,\ldots,X_k]$, com $i_j \in \{0,\ldots,e_j-1\}$, para todo $j \in \{1,\ldots,k\}$ satisfazendo $u(\eta)(y) = 0$, temos que $u \in I = (X_1^{e_1}-1, X_2^{e_2}-1,\ldots,X_k^{e_k}-1)$ pois, neste caso, teríamos que $u = 0$.

Seja então, $u \in F[X_1,\ldots,X_k]$ como descrito acima. Para cada $i \in \{1,\ldots,N\}$, temos que $0 = u(\eta)(y) = E_i(\eta)u(\eta)(y) = u(\eta)(E_i(\eta)(y)) = u(\eta)(t_i)$, pelo Lema 3.2.11. Assim, $u \in P_i^M$, para todo $i \in \{1,\ldots,N\}$. Ou seja, $u \in \bigcap_{i=1}^{N} P_i^M$. Note que $\bigcap_{i=1}^{N} P_i^M \subseteq I$. De fato, pelo Lema 3.2.8 temos que $\overline{P_i^M} = \oplus_{j\neq i}(\overline{g_j})$. Assim,

$$\bigcap_{i=1}^{N} \overline{P_i^M} = [\oplus_{j\neq 1}(\overline{g_j})] \bigcap [\oplus_{j\neq 2}(\overline{g_j})] \bigcap \cdots \bigcap [\oplus_{j\neq N}(\overline{g_j})] = 0,$$

o que implica que $\bigcap_{i=1}^{N} P_i^M \subseteq I$. ■

O próximo resultado nos assegura um limitante superior, para a quantidade de tentativas de encontrar o elemento y do corolário anterior. Este limitante superior é nN, como podemos ver pelo seguinte

Corolário 3.2.15. *Para cada $i \in \{1, \ldots, N\}$ e $j \in \{1, \ldots, n\}$ o elemento $g_i(\eta)(w_j)$ tem P_i^M como $\eta-$anulador se, e somente se $g_{1,\ldots,1}(\eta)(w_j) \neq 0$.*

Dem.: Como $(\overline{g_{1,\ldots,1}}) = \overline{P_i^M}(\overline{g_i})$, e I é o $\eta-$anulador de E, temos que $g_{1,\ldots,1}(\eta)(x_j) \neq 0$ se, e somente se $P_i^{M-1}(\eta)(g_i(\eta)(x_j)) \neq 0$. Mas, vimos na demonstração do Teorema 3.2.12 que $P_i^{M-1}(\eta)(g_i(\eta)(x_j)) \neq 0$ se, e somente se $P_i^M = anul_\eta(\{g_i(\eta)(x_j)\})$. Assim, temos que $g_{1,\ldots,1}(\eta)(x_j) \neq 0$ se, e somente se $P_i^M = anul_\eta(\{g_i(\eta)(x_j)\})$. ■

Com isso, podemos concluir que o resultado demonstrado por Poli é mais geral, e computacionalmente mais eficiente que o de Schwarz, já que toda extensão cíclica é abeliana. Porém, a demonstração do último é muito mais complexa e utiliza-se de resultados menos triviais, que o primeiro.

Capítulo

4

Generalizações do Teorema da Base Normal

Neste capítulo apresentaremos algumas generalizações do teorema da base normal. Caracterizaremos bases normais generalizadas para corpos finitos e mostraremos que todo corpo finito de característica 2 tem uma base normal generalizada, resultado este desenvolvido por Seroussi e Bshouty em [4]. Veremos também um resultado dado por Waterhouse em [18] que estabelece que toda extensão galoisiana de corpos infinitos, admite uma base normal generalizada.

4.1 Base Normal Generalizada

Nesta seção apresentaremos um tipo de base que generaliza a noção de base normal e caracterizamos tais bases para extensões galoisianas de corpos.

Definição 4.1.1. *Sejam $E \supseteq F$ uma extensão galoisiana de corpos com grupo de Galois $G = \{\eta_1, \ldots, \eta_n\}$ e $r_0, \ldots, r_{n-1}$ inteiros não negativos. Se existe $\alpha \in E$ tal que*

$B = \{\eta_1(\alpha)^{r_0}, \eta_2(\alpha)^{r_1}, \ldots, \eta_n(\alpha_n)^{r_{n-1}}\}$ *é uma base de* E *sobre* F*, diremos que o conjunto* B *é uma* base normal generalizada de E sobre F.

Obs.: Observemos que esta é uma generalização de base normal, pois se tomarmos $r_1 = \cdots = r_n = 1$, obtemos uma base normal. Observemos ainda que para o caso de extensões de um corpo finito, $\mathbb{F}_q$, como o grupo de Galois é cíclico e gerado pelo automorfismo $x \mapsto x^q$, a base B descrita na definição acima fica na forma $B = \{\alpha^{r_0}, \alpha^{r_1 q}, \ldots, \alpha^{r_{n-1} q^{n-1}}\}$.

Definição 4.1.2. *Sejam* $F = \mathbb{F}_q$ *um corpo finito com* $q = p^t$ *elementos, onde* p *é um número primo, e* $E = \mathbb{F}_{q^n}$ *uma extensão de grau* n *de* F*. Consideremos o polinômio*

$$\Delta(X_0, \ldots, X_{n-1}) = \det \begin{pmatrix} X_0 & X_1 & \cdots & X_{n-1} \\ X_0^q & X_1^q & \cdots & X_{n-1}^q \\ \vdots & \vdots & \ddots & \vdots \\ X_0^{q^{n-1}} & X_1^{q^{n-1}} & \cdots & X_{n-1}^{q^{n-1}} \end{pmatrix} \in F[X_0, \ldots, X_{n-1}].$$

Do Teorema 1.1.15, temos que $\{\beta_0, \ldots, \beta_{n-1}\}$ *é uma base de* E *sobre* F *se, e somente se* $\Delta(\beta_0, \ldots, \beta_{n-1}) \neq 0$*. Seja* $R = \{r_0, r_1 \ldots, r_{n-1}\}$ *um conjunto de números inteiros com* $0 \leq r_i \leq q^n - 2$*. Diremos que* $\alpha \in E$ satisfaz R *se* $\{\alpha^{r_0}, \alpha^{r_1}, \ldots, \alpha^{r_{n-1}}\}$ *é uma base de* E *sobre* F*. Diremos que* R *é* factível *se existe* $\alpha \in E$ *tal que* α *satisfaz* R*.*

Lema 4.1.3. *Sejam* $R = \{r_0, \ldots, r_{n-1}\}$ *um conjunto de inteiros como na definição anterior e* $D_R(X) = \Delta(X^{r_0}, X^{r_1}, \ldots, X^{r_{n-1}})$*. Então o conjunto* R *é factível se, e somente se* $(X^{q^n-1} - 1) \not| D_R(X)$*.*

Dem.: Suponhamos que $\alpha \in E$ satisfaz R. Então $\alpha \neq 0$ e, pelo Teorema 1.1.15, temos que $D_R(\alpha) = \Delta(\alpha^{r_0}, \ldots \alpha^{r_{n-1}}) \neq 0$, ou seja, α não é raiz de $D_R(X)$. Como α é raiz de $(X^{q^n-1} - 1)$, temos que $(X^{q^n-1} - 1)$ não divide $D_R(X)$, pois caso contrário, teríamos $D_R(X) = (X^{q^n-1} - 1)p(X)$ e $D_R(\alpha) = 0$, o que é uma contradição.

Reciprocamente, suponhamos que $(X^{q^n-1} - 1)$ não divide $D_R(X)$. Então, temos que $D_R(X) = q(X)(X^{q^n-1} - 1) + r(X)$, com $r \neq 0$ e $\partial r < q^n - 1$. Assim, $D_R(v) = r(v)$, para todo $v \in \dot{E}$. Logo, existe $\alpha \in \dot{E}$ tal que $r(\alpha) \neq 0$, pois caso contrário, r teria $q^n - 1$ raízes distintas e então $\partial r \geq q^n - 1$ o que é um absurdo. Logo, $D_R(\alpha) \neq 0$ e R é factível. ■

O próximo teorema nos dá uma condição necessária e suficiente para que o corpo finito $E = \mathbb{F}_{q^n}$ admita uma base normal generalizada sobre o corpo $F = \mathbb{F}_q$.

Teorema 4.1.4. *Sejam $R = \{r_0, \ldots, r_{n-1}\}$ um conjunto de inteiros tais que $r_i \in \{0, \ldots q^n - 2\}$ e s um inteiro arbitrário. Considere a congruência*

$$\sum_{i=0}^{n-1} r_i q^{\phi(i)} \equiv s \mod (q^n - 1), \tag{4.1}$$

onde $\phi \in S_n$, o grupo das permutações do conjunto $\{0, \ldots, n-1\}$. Sejam $N_p(s) = \sharp\{\varphi \in A_n; \varphi$ satisfaz (4.1)$\}$, onde A_n é o grupo das permutações pares de $\{0, \ldots, n-1\}$, e $N_i(s) = \sharp\{\varphi \in S_n - A_n; \varphi$ satisfaz (4.1)$\}$. Então, o conjunto R é factível se, e somente se existe um inteiro s tal que $N_p(s) \not\equiv N_i(s) \mod p$.

Dem.: Da definição de determinante temos que

$$D_R(X) = \Delta(X^{r_0}, \ldots, X^{r_{n-1}}) = \sum_{\phi \in S_n} (Sgn(\phi) \prod_{i=0}^{n-1} X^{r_i q^{\phi(i)}}) = \sum_{\phi \in S_n} Sgn(\phi) X^{(\sum_{i=0}^{n-1} r_i q^{\phi(i)})},$$

onde $sgn(\phi) = \begin{cases} 1, \text{ se } \phi \in A_n \\ -1, \text{ se } \phi \notin A_n \end{cases}$, para cada $\phi \in S_n$.

Seja $\Phi(s)$ o conjunto de todas as soluções ϕ da congruência (4.1). Consideremos

$$\overline{D_R}(X) = \sum_{s=0}^{q^n-2} D_s X^s, \tag{4.2}$$

o resto da divisão de $D_R(X)$ por $X^{q^n-1} - 1$. Observe que $D_s = \sum_{\phi \in \Phi(s)} Sgn(\phi)$.

Pelo lema anterior, temos que R é factível se, e somente se $\overline{D_R}(X) \neq 0$. Assim, R é factível se, e somente se existe um inteiro s tal que $D_s \neq 0$, ou seja, se, e somente se existe um inteiro s tal que $N_p(s) \not\equiv N_i(s) \mod p$. ■

4.2 Generalização do Teorema da Base Normal Para Corpos Finitos de Característica 2

Nesta seção, veremos que se o corpo F tem característica 2, para certas escolhas do conjunto R, o corpo E tem uma base normal generalizada sobre F. Em toda esta seção, F será um corpo com $q = 2^t$ elementos, para algum inteiro positivo t.

Iniciamos com um lema técnico que será necessário para o desenvolvimento dos resultados do restante da seção.

Lema 4.2.1. *Sejam m e n inteiros tais que $1 \leq m \leq n$ e $\lambda_0, \ldots, \lambda_{m-1}$, $k_0, \ldots, k_{m-1}$, $j_0, \ldots, j_{m-1}$ inteiros satisfazendo:*

$$0 < \lambda_i < q,$$
$$0 \leq k_i \leq n-1,$$
$$0 \leq j_0 < j_1, \ldots, < j_{m-1} \leq n-1,$$

para todo $i \in \{0, \ldots, m-1\}$. Se

$$\sum_{i=0}^{m-1} \lambda_i q^{k_i} \equiv \sum_{i=0}^{m-1} \lambda_i q^{j_i} \mod (q^n - 1), \tag{4.3}$$

então $\{k_0, k_1, \ldots, k_{m-1}\} = \{j_0, j_1, \ldots, j_{m-1}\}$.

Dem.: Considere os inteiros $l_1 = \sum_{i=0}^{m-1} \lambda_i q^{k_i}$ e $l_2 = \sum_{i=0}^{m-1} \lambda_i q^{j_i}$. Como $\lambda_i q^{j_i} > 1$, para todo $i \in \{0, \ldots, m-1\}$, temos que $m < l_2$. Mais ainda, $l_2 = \sum_{i=0}^{m-1} \lambda_i q^{j_i} \leq \sum_{i=0}^{m-1} (q-1) q^{j_i} \leq (q-1) \sum_{i=0}^{m-1} q^{n-m+i}$, pois $j_i \leq n - (m-i)$, para todo $i \in \{0, \ldots, m-1\}$. Assim, $l_2 \leq (q-1) \sum_{i=0}^{m-1} q^{n-m+i} \leq q^n - q^{n-m} \leq q^n - 1$ e l_2 é um número inteiro satisfazendo $m < l_2 \leq q^n - 1$.

Se todos os k_i são distintos, então também temos $m < l_1 \leq q^n - 1$, e a congruência (4.3) implica que $\sum_{i=0}^{m-1} \lambda_i q^{k_i} = \sum_{i=0}^{m-1} \lambda_i q^{j_i}$. Assim, $\sum_{i=0}^{m-1} \lambda_i (q^{k_i} - q^{j_i}) = 0$ e, pela unicidade da representação de um número inteiro na base q, temos que $q^{k_i} = q^{j_i}$, para todo $i \in \{0, \ldots, m-1\}$. Dessa forma, $k_i = j_i$, para todo $i \in \{0, \ldots, m-1\}$ e vale a conclusão do lema.

Suponhamos agora que nem todos os k_i sejam distintos. Vamos mostrar que a congruência (4.3) não pode ser satisfeita. Simplifiquemos a soma $l_1 = \sum_{i=0}^{m-1} \lambda_i q^{k_i}$ pelo seguinte procedimento:

Passo 1: Sejam a e b índices tais que $k_a = k_b$, para $0 \leq a < b \leq m-1$. Façamos a seguinte substituição em l_1:

Se $\lambda_a + \lambda_b < q$, troquemos $\lambda_a q^{k_a} + \lambda_b q^{k_b}$ por $\lambda'_a q^{k'_a}$, onde $\lambda'_a = \lambda_a + \lambda_b$, e $k'_a = k_a$. Isso diminui uma parcela na soma em l_1.

Se $\lambda_a + \lambda_b \geq q$, então troquemos $\lambda_a q^{k_a} + \lambda_b q^{k_b}$ na soma, por $\lambda'_a q^{k'_a} + \lambda'_b q^{k'_b}$, onde $\lambda'_a = \lambda_a + \lambda_b - q$; $\lambda'_b = 1$; $k'_a = k_a$; $k'_b = k_a + 1$ módulo n.

Note que $\lambda'_a + \lambda'_b < \lambda_a + \lambda_b$. De fato, como $q = \lambda_a + \lambda_b - \lambda'_a$, temos que $\lambda'_b = 1 < q = \lambda_a + \lambda_b - \lambda'_a$ e $\lambda'_a + \lambda'_b < \lambda_a + \lambda_b$.

Passo 2: Se o Passo 1 produziu uma soma $l'_1 = \sum_{i=0}^{m'-1} \lambda'_i q^{k'_i}$, onde m' é o número de parcelas da nova soma, cujos k'_i são distintos, então pare. Caso contrário, aplique o Passo 1 novamente.

Depois de executar o Passo 1, temos:

$$m' + \sum_{i=0}^{m'-1} \lambda'_i < m + \sum_{i=0}^{m-1} \lambda_i, \tag{4.4}$$

pois $m' \leq m$, $\sum_{i=0}^{m'-1} \lambda'_i \leq \sum_{i=0}^{m-1} \lambda_i$ e, pela observação final do Passo 1, pelo menos uma destas desigualdades é estrita.

Assim, o Passo 1 só pode ser executado um número finito de vezes e, no fim, o procedimento pára, com todos os k'_i distintos, e a nova soma satisfazendo:

$0 < \lambda'_0, \lambda'_1, \ldots, \lambda'_{m'-1} < q$;

$0 \leq k'_0, k'_1, \ldots, k'_{m'-1} \leq n-1$ e

$$\sum_{i=0}^{m'-1} \lambda'_i q^{k'_i} \equiv \sum_{i=0}^{m-1} \lambda_i q^{k_i} \mod (q^n - 1). \tag{4.5}$$

Para mostrarmos a congruência (4.5), basta mostrarmos que para os índices a e b tais que $k_a = k_b$, vale a congruência $\lambda_a q^{k_a} + \lambda_b q^{k_b} \equiv \lambda'_a q^{k'_a} + \lambda'_b q^{k'_b} \mod (q^n - 1)$.

Para os índices a e b tais que $k_a = k_b$ e $\lambda_a + \lambda_b < q$, a congruência acima é óbvia. Resta então, mostrarmos para os casos em que $k_a = k_b$ e $\lambda_a + \lambda_b \geq q$. Nesta

situação, temos que $\lambda_a q^{k_a} + \lambda_b q^{k_b} \equiv \lambda'_a q^{k'_a} + \lambda'_b q^{k'_b} \mod (q^n - 1)$ se, e somente se $\lambda_a q^{k_a} + \lambda_b q^{k_a} - \lambda'_a q^{k_a} \equiv q^{k'_b} \mod (q^n - 1)$, o que ocorre se, e somente se $(\lambda_a + \lambda_b - \lambda'_a) q^{k_a} \equiv q^{k_a+1+\gamma n} \mod (q^n - 1)$, pois $\lambda'_b = 1$, e $k'_b = k_a + 1 + \gamma n$, para algum $\gamma \in \mathbb{Z}$. Esta última congruência é equivalente a $qq^{k_a} \equiv q^{k_a+1}(q^n)^\gamma \mod (q^n - 1)$, ou seja, $q^{k_a+1} \equiv q^{k_a+1} \mod (q^n - 1)$. Portanto, $\lambda_a q^{k_a} + \lambda_b q^{k_b} \equiv \lambda'_a q^{k'_a} + \lambda'_b q^{k'_b} \mod (q^n - 1)$.

Assim, juntando (4.5), e (4.3), obtemos que $l'_1 \equiv l_2 \mod (q^n - 1)$.

Dessa forma, como todos os k'_i são distintos, pela unicidade da representação de inteiros na base q, temos que $m = m'$, $\{k'_0, k'_1, \ldots, k'_{m'-1}\} = \{j_0, j_1, \ldots, j_{m-1}\}$ e $\{\lambda'_0, \ldots, \lambda'_{m'-1}\} = \{\lambda_0, \ldots, \lambda_{m-1}\}$, o que contradiz (4.4). Logo, o passo 1 não poderia ser executado. Portanto, todos os k_i devem ser distintos, e o resultado segue. ■

No restante desta seção, as operações nos índices do conjunto $\{0, 1, \ldots, n-1\}$ serão tomadas módulo n, onde $n = 2^k m$, é o grau da extensão $E \supseteq F$, com m um inteiro ímpar e $k \geq 0$.

Seja B_n o conjunto das permutações $\Psi \in S_n$ satisfazendo as seguintes propriedades:

$$\Psi(i) = \Psi(i + m) + m, \text{para todo } i = 0, \ldots n - 1. \tag{4.6}$$

$$\{i + \Psi(i); i \in \{0, \ldots, m - 1\}\} = \{0, 2, 4, \ldots, 2(m - 1)\}. \tag{4.7}$$

Note que se a propriedade (4.6) é satisfeita, então a propriedade (4.7) é equivalente à propriedade

$$\{i + \Psi(i); i \in \{0, 1, \ldots, n - 1\}\} = \{0, 2, \ldots, 2(m - 1)\}. \tag{4.8}$$

Note também que o conjunto $\{0, 2, \ldots, 2(m - 1)\}$ tem m elementos, mesmo considerando-se congruência módulo n.

Lema 4.2.2. *Para B_n como definido acima, valem as seguintes propriedades:*
(i) Se $\Psi \in B_n$ então $\Psi^{-1} \in B_n$.
(ii) Existe uma e somente uma permutação $\Psi_0 \in B_n$ tal que $\Psi_0 = \Psi_0^{-1}$. Tal permutação é definida por:

$$\Psi_0(i) = \begin{cases} i, & \text{se } 0 \leq i \leq m - 1 \\ \Psi_0(i - m) - m, & \text{se } m \leq i \leq n - 1 \end{cases}$$

Dem.: Seja $\Psi \in B_n$. Vamos mostrar que $\Psi^{-1} \in B_n$, ou seja, que Ψ^{-1} satisfaz (4.6) e (4.8). Para isso, sejam $i \in \{0, \ldots, n-1\}$ e $j = \Psi^{-1}(i+m)$. Desde que $\Psi \in B_n$, por (4.6), temos que $\Psi(j+m) = \Psi(j) - m$. Assim, $\Psi(\Psi^{-1}(i+m)+m) = \Psi(\Psi^{-1}(i+m)) - m = i+m-m = i$. Aplicando Ψ^{-1} em ambos os lados da equação, obtemos $\Psi^{-1}(i+m)+m = \Psi^{-1}(i)$, ou seja, Ψ^{-1} satisfaz (4.6).

Como Ψ satisfaz (4.8), temos que $\{i+\Psi(i); i \in \{0, \ldots, n-1\}\} = \{0, 2, \ldots, 2(m-1)\}$. Desde que Ψ^{-1} é uma bijeção de $\{0, \ldots, n-1\}$ temos que, para cada $i \in \{0, \ldots, n-1\}$, existe um único $j \in \{0, \ldots, n-1\}$ tal que $i = \Psi^{-1}(j)$. Assim temos que $\{i + \Psi(i);\ i \in \{0, \ldots, n-1\}\} = \{\Psi^{-1}(j) + \Psi(\Psi^{-1}(j));\ j \in \{0, \ldots, n-1\}\} = \{j + \Psi^{-1}(j);\ j \in \{0, \ldots, n-1\}\}$, ou seja, Ψ^{-1} satisfaz (4.8). Portanto vale (i).

Para mostrarmos (ii), primeiramente mostremos que Ψ_0 dada acima, pertence a B_n. Desde que $n = 2^k m$, podemos escrever $\{0, \ldots, n-1\} = \bigcup_{j=0}^{2^k-1} I_j$, onde $I_j = \{jm, jm+1, \ldots, jm+m-1 = j(m+1)-1\}$. É fácil ver que se $i \in I_j$, então $\Psi_0(i) = i - 2jm$. Assim, se $i \notin I_{2^k-1}$, temos que $(i+m) \notin I_0$ e, pela definição de Ψ_0, temos que $\Psi_0(i+m) = \Psi_0(i+m-m) - m = \Psi_0(i) - m$, ou seja, $\Psi_0(i) = \Psi_0(i+m) + m$. Se $i \in I_{2^k-1}$, então $i+m \in I_0$ e $\Psi_0(i+m) = i+m$. Como $2^k m = n \equiv 0 \mod n$, temos que $i+m = i - 2^k m + m = i - 2.2^k m + 2m - m = i - (2^k-1)2m - m = \Psi_0(i) - m$, pois $\Psi_0(i) = i - 2(2^k-1)m$. Logo, $\Psi_0(i+m) = \Psi_0(i) - m$, para todo $i \in \{0, \ldots, n-1\}$ e, portanto, ψ_0 satisfaz (4.6).

Agora, para mostrar que Ψ_0 satisfaz (4.7), observemos que $i + \Psi_0(i) = i + i - 2jm = 2(i - jm)$ é par, para todo i e j. Resta então, mostrar que $i + \Psi_0(i) \in \{0, 2, \ldots, 2(m-1)\}$, para todo $i \in \{0, \ldots, n-1\}$, o que acontece se, e somente se $i - jm \leq m-1$, ou seja $i \leq m(j+1) - 1$, para algum $j \in \{0, \ldots, 2^k - 1\}$. Mas, para cada $i \in \{0, \ldots, n-1\}$, temos que $i \in \{jm, \ldots, jm+m-1\}$, para algum $j \in \{0, \ldots, 2^k - 1\}$. Assim, para este j, temos que $i \leq m(j+1) - 1$ e, conseqüentemente, $\Psi_0 \in B_n$.

Mostremos agora que $\Psi_0^{-1} = \Psi_0$. Se $i \in I_j$, então $\Psi_0(i) = i - 2jm$. Logo, $\Psi_0(\Psi_0(i)) = \Psi_0(i - 2jm)$. Mas, como $i \in I_j$, temos $mj \leq i \leq (j+1)m - 1$. Assim, $mj - 2jm \leq i - 2jm \leq mj + m - 2jm - 1$, ou seja, $-jm \leq i - 2jm \leq (-j+1)m - 1$, o que mostra que $i - 2jm \in I_{-j}$. Portanto, $\Psi_0(i - 2jm) = i - 2jm - (2(-j)m) = i$. Concluímos então que $\Psi_o^2(i) = i$, para todo $i \in \{0, \ldots, n-1\}$ o que mostra que $\Psi_0 = \Psi_0^{-1}$.

Mostremos agora, que Ψ_0 é o único com tal propriedade.

Suponhamos que $\Psi \in B_n$ satisfaz $\Psi = \Psi^{-1}$ e $\Psi \neq \Psi_0$. Pela propriedade (4.6), Ψ é determinada pelos seus valores em $\{0, \ldots, m-1\}$. Então, existe $h \in \{0, \ldots, m-1\}$, tal que $\Psi(h) \neq \Psi_0(h) = h$. Logo, $\Psi(h) = j + wm$, para algum $j \in \{0, \ldots, m-1\}$, e $w \in \{0, \ldots, 2^k - 1\}$, com $j \neq h$, ou $w > 0$.

Se $j \neq h$, como $\Psi = \Psi^{-1}$, temos que $h = \Psi(j + wm)$. Mas, por (4.6), $h = \Psi(j) - wm$ e, por (4.2), $\Psi(h) + h = \Psi(j) + j$, o que contradiz (4.7), uma vez que $0 \leq h, j \leq m-1$ e o conjunto $\{i + \Psi(i); 0 \leq i \leq m-1\}$ tem m elementos. Assim, não podemos ter $h \neq j$. Conseqüentemente, $h = j$ e $w > 0$. Como $w \leq 2^k - 1$, temos que $k > 0$ e, desde que $n = 2^k m$, temos que n é par.

Agora, $\Psi(h) = h + wm$. Somando h em ambos os lados, temos $\Psi(h) + h = 2h + wm$, onde $0 < w < 2^k$ e, de (4.7), $2h + wm \equiv 2i \mod n$, para algum $i \in \{0, \ldots, m-1\}$. Como m é ímpar e n é par, segue que w é par. Portanto, $2 \leq w \leq 2^k - 2$ e, multiplicando por m, obtemos $2m \leq wm \leq 2^k m - 2m$. Somando $2h$, temos $2m + 2h \leq wm + 2h \leq 2^k m + 2h - 2m$. Como $0 \leq h \leq m-1$, temos que $2m \leq 2m + 2h \leq wm + 2h = \Psi(h) + h \leq n + 2(h - m) < n$, ou seja, $2m \leq \Psi(h) + h < n$, o que contradiz (4.7). conseqüentemente, $\Psi = \Psi_0$, como queríamos. ■

Corolário 4.2.3. *A cardinalidade de B_n, $\sharp(B_n)$, é ímpar.*

Dem.: A demonstração segue diretamente das partes (i) e (ii) do lema anterior. ■

Definição 4.2.4. *Seja $\Lambda = (\lambda_0, \ldots, \lambda_{n-1})$ um vetor de inteiros onde $0 \leq \lambda_i < q$, com no máximo um λ_i igual a zero. Dizemos que Λ é $m-$*periódico*, com $m \in \{1, \ldots, n\}$, se $\lambda_{m+i} = \lambda_i$, para todo $i \in \{0, \ldots, n-1\}$.*

Seja Λ um vetor $m-$periódico. Para cada $\sigma \in S_m$ arbitrário, seja

$$s(\sigma) = \sum_{i=0}^{n-1} \lambda_i q^{2\sigma(i \mod m)}.$$

Consideremos o conjunto de congruências

$$\sum_{i=0}^{n-1} \lambda_i q^{i+\phi(i)} \equiv s(\sigma) \mod (q^n - 1), \tag{4.9}$$

para todo $\sigma \in S_m$ e $\phi \in S_n$. Sejam

$$\Phi_\sigma = \left\{ \phi \in S_n;\ \sum_{i=0}^{n-1} \lambda_i q^{i+\phi(i)} \equiv s(\sigma) \mod (q^n - 1) \right\} \text{ e } \Phi = \bigcup_{\sigma \in S_m} \Phi_\sigma. \tag{4.10}$$

Observe que a união acima é disjunta. De fato, se $m = 1$, não há nada a ser demonstrado, já que S_m tem apenas um elemento. Se $m > 1$, suponhamos que exista $\phi \in S_n$ tal que $\phi \in \Phi_{\sigma_1} \bigcap \Phi_{\sigma_2}$, para $\sigma_1, \sigma_2 \in S_m$. Assim, $s(\sigma_1) \equiv s(\sigma_2) \mod (q^n - 1)$. Ou seja, $\sum_{i=0}^{n-1} \lambda_i q^{2\sigma_1(i \mod m)} \equiv \sum_{i=0}^{n-1} \lambda_i q^{2\sigma_2(i \mod m)} \mod (q^n - 1)$, o que implica que $2\sigma_1(i \mod m) \equiv 2\sigma_2(i \mod m) \mod n$, para todo $i \in \{0, \ldots, n-1\}$. Como $m > 1$, temos que 2 é invertível módulo n. Assim, $\sigma_1(i \mod m) \equiv \sigma_2(i \mod m) \mod n$ e, como $n \geq m$, segue que $\sigma_1 = \sigma_2$ e, portanto, a união é disjunta.

Com estas notações, temos

Lema 4.2.5. *Seja $T : S_n \longrightarrow S_n$ dada por $(T(\phi))(i) = \phi(i+m)+m$, para todo $\phi \in S_n$ e $0 \leq i \leq n-1$. Se $\phi \in \Phi_\sigma$, para algum σ, então $T(\phi) \in \Phi_\sigma$.*

Dem.: Se $\phi \in \Phi_\sigma$, então $\sum_{i=1}^{n-1} \lambda_i q^{i+\phi(i)} = \sum_{i=1}^{n-1} \lambda_{i+m} q^{i+m+\phi(i+m)}$ pois os índices são tomados módulo n e $i \mapsto (i+m)$ é uma permutação de $\{0, \ldots, n-1\}$. Por isso, e pelo fato de Λ ser $m-$periódico, obtemos que $\sum_{i=1}^{n-1} \lambda_i q^{i+T(\phi(i))} = \sum_{i=1}^{n-1} \lambda_{i+m} q^{i+m+\phi(i+m)} \equiv S(\sigma) \mod (q^n-1)$ e, portanto, $T(\phi) \in \Phi_\sigma$. ■

Lema 4.2.6. *Para todo $\phi \in S_n$, seja $G_\phi = \{\phi, T(\phi), T^2(\phi), \ldots\}$. Então $\sharp(G_\phi) = 2^h$, para algum $0 \leq h \leq k$.*

Dem.: É fácil ver que $T^j(\phi)(i) = \phi(i + jm) + jm$, para $i \in \{0, \ldots, n-1\}$ e $j \in \{0, \ldots, 2^k - 1\}$. Assim, $T^{2^k}(\phi)(i) = \phi(i + 2^k m) + 2^k m = \phi(i)$, para todo $i \in \{0, \ldots, n-1\}$. Da definição de T, e do fato que $n = 2^k m$, segue que $T^{2^k}(\phi) = \phi$, para todo $\phi \in S_n$. Portanto, $\sharp(G_\phi)$ divide 2^k e, conseqüentemente, $\sharp(G_\phi) = 2^h$, para algum $h \in \{0, \ldots, k\}$. ■

Lema 4.2.7. *Se Φ e B_n são definidos como anteriormente, temos que $\{\phi \in \Phi;\ T(\phi) = \phi\} = B_n$.*

Dem.: Podemos, evidentemente, supor que $n > 1$ pois, se $n = 1$, o resultado é trivial. Note que se $T(\phi) = \phi$, então ϕ satisfaz (4.6). De fato, $T(\phi)(i) = \phi(i + m) + m$, para

todo $i \in \{1, \ldots, n-1\}$. Logo, $T(\phi)(i)+i = \phi(i)+i = \phi(i+m)+(i+m)$. Dessa forma, como $n = 2^k m$ e Λ é $m-$periódico, temos que

$$\sum_{i=0}^{n-1} \lambda_i q^{i+\phi(i)} = 2^k \sum_{i=0}^{m-1} \lambda_i q^{i+\phi(i)}. \tag{4.11}$$

Desde que $\phi \in \Phi$, temos que ϕ satisfaz (4.9), para algum $\sigma \in S_m$. Mas,

$$s(\sigma) = \sum_{i=0}^{n-1} \lambda_i q^{2\sigma(i \mod m)} = 2^k \sum_{i=0}^{m-1} \lambda_i q^{2\sigma(i)}. \tag{4.12}$$

Por (4.11) e (4.12), a congruência (4.9) se escreve como:

$$2^k \sum_{i=0}^{m-1} \lambda_i q^{i+\phi(i)} \equiv 2^k \sum_{i=0}^{m-1} \lambda_i q^{2\sigma(i)} \mod (q^n - 1).$$

Como $n > 1$, temos que $2 \not\equiv 0 \mod (q^n - 1)$ e

$$\sum_{i=0}^{m-1} \lambda_i q^{i+\phi(i)} = \sum_{i=0}^{m-1} \lambda_i q^{2\sigma(i)} \mod (q^n - 1). \tag{4.13}$$

Se $\lambda_i \neq 0$, para todo $i \in \{0, \ldots, m-1\}$, pelo Lema 4.2.1, (4.13) implica que

$$\{i + \phi(i);\ i \in \{0, \ldots, m-1\}\} = \{0, 2, \ldots, 2(m-1)\} \tag{4.14}$$

ou seja, ϕ satisfaz (4.7). Portanto, $\phi \in B_n$.

Se $\lambda_a = 0$, para algum índice $a \in \{0, \ldots, m-1\}$, então devemos ter que $m = n$, pois Λ é $m-$periódico e no máximo um elemento de Λ pode ser zero. Assim, temos que n é ímpar. Seja $b = 2\sigma(a) \mod n$. Segue de (4.13) e do Lema 4.2.1 que

$$\{i + \phi(i);\ i \in \{0, \ldots, n-1\} - \{a\}\} = \{0, 1, \ldots, n-1\} - \{b\} \tag{4.15}$$

Afirmamos que $\phi(a) + a = b$. De fato, como n é ímpar, $n-1$ é par. Assim, $\frac{n-1}{2} n = \sum_{i=0}^{n-1} i = \sum_{i=0}^{n-1} \phi(i) = \sum_{i=0}^{n-1} i + \phi(i) \equiv 0 \mod n$. Dessa forma, $b + \sum_{i \neq b}^{m-1} i = a + \phi(a) + \sum_{i \neq a}^{m-1} (i + \phi(i))$ e, de (4.15), temos que $b = \phi(a) + a$, o que implica que

(4.14) também é satisfeita neste caso, ou seja, $\{i+\phi(i);\ i \in \{0,\ldots,m-1\}\} = \{0,2,\ldots,2(m-1)\}$. Portanto, $\phi \in B_n$ e mostramos que $\{\phi \in \Psi;\ T(\phi)=\phi\} \subseteq B_n$.

Por outro lado, se $\Psi \in B_n$, por (4.6), temos que $T(\Psi)=\Psi$ e, por (4.7), que $\{i+\Psi(i);\ i \in \{0,\ldots,m-1\}\} = \{0,2,\ldots,2(m-1)\}$. Para $\sigma \in S_m$ definido por $\sigma(i) = \frac{i+\Psi(i)}{2}$, para $i \in \{0,\ldots,m-1\}$, temos $\Psi \in \Phi_\sigma$, pois

$$s(\sigma) = \sum_{i=0}^{n-1} \lambda_i q^{2\sigma(i \mod m)} = \sum_{i=0}^{n-1} \lambda_i q^{i+\Psi(i) \mod m} \equiv \sum_{i=0}^{n-1} \lambda_i q^{i+\Psi(i)} \mod (q^n-1).$$

O que mostra que $B_n \subseteq \{\phi \in \Psi;\ T(\phi)=\phi\}$, como queríamos. ■

Lema 4.2.8. *Para Φ como definida em* (4.10), *temos que $\sharp(\Phi)$ é ímpar.*

Dem.: Segue do Lema 4.2.5 e da demonstração do Lema 4.2.6, que T induz uma partição de Φ em órbitas disjuntas da forma $G_\phi = \{\phi, \phi T, \ldots, T(\phi)^{\sharp(G_\phi)-1}\}$. Se $T(\phi) \neq \phi$, pelo Lema 4.2.6, $\sharp(G_\phi)$ é uma potência não trivial de 2, e G_ϕ tem uma quantidade par de permutações de Φ. Pelo Lema anterior, a quantidade de permutações $\phi \in \Phi$ tais que $T(\phi)=\phi$, é igual a $\sharp(B_n)$ que, pelo Corolário 4.2.3 é ímpar. Assim, concluímos que $\sharp(\Psi)$ é ímpar. ■

O próximo resultado, é o resultado principal desta seção. Ele garante que sob certas condições, existe uma base normal generalizada para corpos de característica 2. O corolário que segue o teorema nos mostra que o resultado é mais forte quando n é ímpar.

Teorema 4.2.9. *Seja $q=2^t$ e $n=2^k m$, com m ímpar. Seja $(\lambda_0,\ldots,\lambda_{n-1})$ um vetor $m-$periódico de inteiros, com $0 \leq \lambda_i < q$, sendo no máximo um λ_i igual a zero. Então, existe um elemento $\alpha \in E = \mathbb{F}_{q^n}$ tal que $\{\alpha^{\lambda_0}, \alpha^{\lambda_1 q}, \alpha^{\lambda_2 q^2}, \ldots, \alpha^{\lambda_{n-1} q^{n-1}}\}$ é uma base de $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

Dem.: Considere o conjunto de congruências:

$$\sum_{i=0}^{n-1} \lambda_i q^{i+\phi(i)} \equiv s(\sigma) \mod (q^n-1),$$

para todo $\sigma \in S_m$, onde $s(\sigma) = \sum_{i=0}^{n-1} \lambda_i q^{2\sigma(i \mod m)}$. Pelo Lema 4.2.8, $\Phi = \bigcup_{\sigma \in S_m} \Phi_\sigma$ tem uma quantidade ímpar de elementos e, pela observação que segue a definição de Φ, equação (4.10), temos que esta união é disjunta. Logo, existe $\sigma_0 \in S_m$ tal que $\sharp(\Phi_{\sigma_0})$ é ímpar. Seja $r_i = \lambda_i q^i$, para $i \in \{0, \ldots n-1\}$. Então, o número de soluções ϕ da equação

$$\sum_{i=0}^{n-1} r_i q^{\phi(i)} \equiv s(\sigma_0) \mod (q^n - 1) \tag{4.16}$$

é ímpar. Então, $N_p(s(\sigma_0)) + N_i(s(\sigma_0)) \equiv 1 \mod 2$, onde $N_p(s(\sigma_0))$ e $N_i(s(\sigma_0))$ denotam respectivamente o número de permutações ϕ pares e ímpares, soluções da equação (4.16). Logo, $N_p(s(\sigma_0)) \not\equiv N_i(s(\sigma_0)) \mod 2$. Assim, pelo Teorema 4.1.4, o conjunto $\{\lambda_0, \lambda_1 q, \ldots, \lambda_{n-1} q^{n-1}\}$ é factível. Ou seja, existe $\alpha \in E = \mathbb{F}_{q^n}$ tal que $\{\alpha^{\lambda_0}, \alpha^{\lambda_1 q}, \ldots, \alpha^{\lambda_{n-1} q^{n-1}}\}$ é base para $E \supseteq F$. ■

Se n é ímpar, a condição "$m-$periódica" é removida e ficamos com:

Corolário 4.2.10. *Sejam $q = 2^t$, n um inteiro ímpar e $\{\lambda_0, \ldots, \lambda_{n-1}\}$ inteiros tais que $0 \leq \lambda_i < q$, com no máximo um $\lambda_i = 0$. Então existe $\alpha \in E$ tal que o conjunto $\{\alpha^{\lambda_0}, \alpha^{\lambda_1 q}, \alpha^{\lambda_2 q^2} \ldots, \alpha^{\lambda_{n-1} q^{n-1}}\}$ é uma base para $\mathbb{F}_{q^n}$ sobre $\mathbb{F}_q$.*

Agora, se $n = 2^k$, ou seja, $m = 1$, a $m-$periocidade de $(\lambda_0, \ldots, \lambda_{n-1})$ implica que $\lambda_0 = \lambda_1 = \ldots = \lambda_{n-1} < q$. Neste caso, o teorema é bem mais fraco, pois nada mais é do que o Teorema da Base Normal, com a propriedade de que o elemento normal é uma potência de λ_0, mas ainda assim, generaliza o teorema da base normal.

4.3 Generalização do Teorema da Base Normal Para Corpos Infinitos

Nesta seção apresentamos a demonstração dada por Waterhouse em [18], que mostra que toda extensão galoisiana de corpos infinitos admite uma base normal generalizada.

Lema 4.3.1. *Seja G um grupo com n elementos e (σ_i, λ_i) n pares distintos, onde $\sigma_i \in G$ e λ_i são inteiros não negativos, com no máximo um $\lambda_i = 0$. Considere a Matriz*

$$A = (X_{\eta_j\sigma_i}^{\lambda_i}) = \begin{pmatrix} X_{\eta_1\sigma_1}^{\lambda_1} & X_{\eta_2\sigma_1}^{\lambda_1} & \cdots & X_{\eta_n\sigma_1}^{\lambda_1} \\ X_{\eta_1\sigma_2}^{\lambda_2} & X_{\eta_2\sigma_2}^{\lambda_2} & \cdots & X_{\eta_n\sigma_2}^{\lambda_2} \\ \vdots & \vdots & \ddots & \vdots \\ X_{\eta_1\sigma_n}^{\lambda_n} & X_{\eta_2\sigma_n}^{\lambda_n} & \cdots & X_{\eta_n\sigma_n}^{\lambda_n} \end{pmatrix},$$

onde $X_\eta, \eta \in G$, são indeterminadas independentes indexadas por elementos de G. Então, o polinômio $p(X_{\eta_1}, \ldots, X_{\eta_n}) = det(A)$ é não nulo.

Dem.: Comecemos com considerações sobre a matriz A.

1) Suponha que duas potências não triviais de X_η ocorrem em uma mesma coluna de A, para algum $\eta \in G$. Sejam j o índice da coluna e i, k os índices das linhas. Assim, $\eta = \eta_j\sigma_i = \eta_j\sigma_k$ e então $\sigma_i = \sigma_k$. Como os pares são distintos, então $\lambda_i \neq \lambda_j$. Dessa forma, existe um único i tal que $\eta = \eta_j\sigma_i$ e $\lambda_i = \max\{\lambda_k;\ \eta = \eta_j\sigma_k\}$.

2) Numa mesma linha não ocorrem duas potências de X_η, pois dado $\sigma \in G$, temos que $G = \{\eta_1\sigma, \eta_2\sigma, \ldots, \eta_n\sigma\}$.

Visto isso, tomemos X_η aleatoriamente na matriz A, onde $\eta \in G$. Sejam $j_1, \ldots, j_s$ as colunas da matriz A em que aparecem potências de X_η. Para cada $j \in \{j_1, \ldots, j_s\}$ seja $r_j = \max\{\lambda_i;\ \eta_j\sigma_i = \eta\}$. Assim, para cada $j \in \{j_1, \ldots, j_s\}$, existe apenas um $k \in \{1, \ldots, s\}$ tal que $\lambda_{j_k} = r_j$. Tomemos $r_\eta = r_1 + r_2 + \cdots + r_s$.

Assim, $X_\eta^{r_\eta}$ é a maior potência de X_η que aparece nos monômios do polinômio p. Feito isso, tomamos X_σ nas colunas remanescentes da matriz A. Novamente, para cada coluna, existe uma única linha entre as que ainda não foram consideradas anteriormente, que contém a maior potência de X_σ. Assim como no caso de X_η, definimos r_σ, e concluímos que $X_\sigma^{r_\sigma}$ é a maior potência de X_σ que aparece nos monômios do polinômio p junto com $X_\eta^{r_\eta}$.

Repetimos o mesmo processo, até que todas as colunas da matriz sejam consideradas. Assim, obtemos um monômio que aparece uma única vez na expressão do determinante $\det(A)$. Logo, o polinômio p contém um monômio não nulo. Ou seja, p é um polinômio não nulo. ■

Terminamos com o resultado principal desta seção. Ele garante a existência de uma base normal generalizada para extensões galoisianas de corpos infinitos, utilizando-se do lema anterior e da independência algébrica dos caracteres, dada pelo Teorema 1.1.18.

Teorema 4.3.2. *Sejam F um corpo infinito e $E \supseteq F$ uma extensão galoisiana de corpos, com $[E : F] = n$ e $G = Gal(E/F) = \{\eta_1, \ldots, \eta_n\}$. Sejam (σ_i, λ_i) n pares distintos, com $\sigma_i \in G$ e λ_i inteiros não negativos, com no máximo um $\lambda_i = 0$. Então, existe $\alpha \in E$ tal que $B = \{\sigma_1(\alpha)^{\lambda_1}, \sigma_2(\alpha)^{\lambda_2}, \ldots, \sigma_n(\alpha)^{\lambda_n}\}$ é uma base de E sobre F.*

Dem.: Pelo Teorema 1.1.15 B é uma base de E sobre F se, e somente se $\det_{i,j}(\eta_j\sigma_i(\alpha)^{\lambda_i}) \neq 0$. Como o corpo F é infinito, o Teorema 1.1.18 nos garante que $\eta_1, \ldots, \eta_n$ são algebricamente independentes sobre F. Assim, se p é um polinômio não nulo, existe $\alpha \in E$ tal que $p(\eta_1(\alpha), \eta_2(\alpha), \ldots, \eta_n(\alpha)) \neq 0$. Pelo Lema anterior, o polinômio $\det(A)$ é não nulo. Assim, existe $\alpha \in E$ tal que $\det_{i,j}(\eta_j\sigma_i(\alpha)^{\lambda_i}) \neq 0$. Ou seja, existe $\alpha \in E$ tal que $\{\eta_1(\alpha), \eta_2(\alpha), \ldots, \eta_n(\alpha)\}$ é base de E sobre F. ■

Observemos que, para extensões galoisianas, este teorema generaliza não só o Torema da Base Normal, mas também o Teorema do Elemento primitivo, bastando para isso, tomar $\eta_i = id$, e $\lambda_i = i - 1$ para todo $i \in \{1, \ldots, n\}$.

Capítulo

5

Bases Normais Auto-duais

Neste capítulo mostraremos que toda extensão galoisiana de corpos de grau ímpar admite uma base normal auto-dual com respeito à forma traço. Este resultado foi demonstrado por Eva Bayer-Fluckiger e Lenstra Jr. em [1] para o caso de corpos de característica distinta de 2, e por Eva Bayer-Fluckiger em [2] para corpos de qualquer característica.

5.1 Módulos Hermitianos

Nesta seção, desenvolveremos a teoria sobre módulos hermitianos necessária para a demonstração do resultado principal. Como nosso objetivo principal é estudar bases normais e bases normais auto-duais, assumiremos que o leitor é familiarizado com os conceitos básicos de formas bilineares sobre corpos e, também, que o leitor tem conhecimento da construção dos anéis de Witt dos espaços bilineares e dos módulos hermitianos sobre um anel, pois a apresentação de tais noções foge ao objetivo da dissertação e a deixaria muito longa. Por isso, alguns resultados utilizados serão enunciados sem

demonstração. O leitor interessado em um aprofundamento nesta teoria pode consultar a referência [15].

Seja A um anel com unidade. Uma *involução* em A é uma aplicação $\bar{}\ : A \longrightarrow A$ tal que $\overline{\alpha+\beta} = \overline{\alpha}+\overline{\beta}$, $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$ e $\overline{\overline{\alpha}} = \alpha$, para todo $\alpha, \beta \in A$, isto é, é um homomorfismo de anéis de ordem 2.

Sejam M um $A-$módulo à esquerda finitamente gerado, e $\bar{}$ uma involução em A. Uma *forma sesquilinear* sobre M é uma aplicação $s : M \times M \longrightarrow A$ biaditiva, tal que $s(ax, by) = as(x, y)\bar{b}$, para todo $x, y \in M$ e $a, b \in A$. Uma *forma hermitiana sobre* M é uma forma sesquilinear $h : M \times M \longrightarrow A$ tal que $h(x, y) = \overline{h(y, x)}$, para todo $x, y \in M$. O par (M, h) é dito ser um $A-$*módulo hermitiano*. Um $A-$módulo hermitiano é dito ser *par*, se existe uma forma sesquilinear $s : M\times M \longrightarrow A$ tal que $h(x, y) = s(x, y) + \overline{s(y, x)}$, para todo $x, y \in M$.

Todos os $A-$módulos considerados serão $A-$módulos à esquerda e, a menos de necessário, escreveremos somente módulos para designá-los. Denotaremos o centro de A por $Z(A) = \{x \in A;\ xy = yx, \text{ para todo } y \in A\}$ e o conjunto dos elementos invertíveis de A por $A^{\times}$.

Os módulos hermitianos pares são de maior interesse pois para tais módulos vale o Teorema do Cancelamento de Witt. O próximo resultado dá condições necessárias sobre um anel A para que todo $A-$módulo hermitiano seja par.

Lema 5.1.1. *Se existe $\alpha \in Z(A)$ tal que $\alpha+\overline{\alpha} = 1$, então todo $A-$módulo hermitiano é par.*

Dem.: Seja (M, h) um $A-$módulo hermitiano. Tomando a forma sesquilinear $s : M\times M \longrightarrow A$, dada por $s(x, y) = \alpha h(x, y)$ e usando que h é hermitiana e que $\alpha \in Z(A)$, obtemos $h(x, y) = \alpha h(x, y) + \overline{\alpha}h(x, y) = s(x, y) + \overline{h(y, x)\alpha} = s(x, y) + \overline{\alpha h(y, x)} = s(x, y) + \overline{s(y, x)}$, ou seja, h é uma forma hermitiana par. ■

Corolário 5.1.2. *Se $2 \in A^{\times}$, então todo $A-$módulo hermitiano é par.*

Dem.: Observe que $\overline{2} = 2$, pois $\overline{2} = \overline{1+1} = \overline{1}+\overline{1} = 1+1 = 2$. Assim, basta tomar $\alpha = \dfrac{1}{2}$ e usar o lema anterior. ■

Se $a \in A$ é tal que $\overline{a} = a$, denotaremos por $\langle a\rangle$ a forma hermitiana $\langle a\rangle : A\times A \longrightarrow A$, dada por $\langle a\rangle(x, y) = xa\overline{y}$, para todo $x, y \in A$.

Para um $A-$módulo à esquerda M, definimos em $M^* = Hom_A(M, A)$ uma estrutura de $A-$módulo à esquerda, por $(a \cdot f)(x) = f(x)\bar{a}$, para todo $a \in A, f \in M^*$ e $x \in M$.

Seja (M, h) um $A-$módulo hermitiano. A aplicação $A-$linear $H : M \longrightarrow M^*$, onde para cada $x \in M$, $H(x) : M \longrightarrow A$, é dada por $H(x)(y) = h(y, x)$, é chamada de *aplicação adjunta de* h. Uma forma (ou módulo) hermitiana(o) é dita(o) ser *não singular*, se a aplicação adjunta associada é um isomorfismo.

É fácil ver que a forma hermitiana $\langle a \rangle$ é não singular se, e somente se $a \in A^\times$.

Se N um $A-$submódulo de M, então o submódulo

$$N^\perp = \{x \in M; h(x, y) = 0, \text{ para todo } y \in N\}$$

de M dito ser o *ortogonal de* N. Se $N = N^\perp$, dizemos que N é um submódulo *totalmente isotrópico* de M. Um módulo hermitiano não-singular (M, h) é dito ser *hiperbólico* se é par e contém um somando direto totalmente isotrópico.

Dois módulos hermitianos (M, h) e (M', h') são *isomorfos* se existe um isomorfismo de $A-$módulos $f : M \longrightarrow M'$ tal que $h(x, y) = h'(f(x), f(y))$, para todo $x, y \in M$. Em particular, as formas hermitianas $\langle a \rangle$ e $\langle b \rangle$ são isomorfas se, e somente se existe $c \in A^\times$ tal que $a = cb\overline{c}$.

Se (M, h) e (M', h') são dois módulos hermitianos, definimos a *soma ortogonal* como sendo o módulo hermitiano

$$(M, h) \perp (M', h') = (M \oplus M', h \perp h'),$$

onde $(h \perp h')(m + m', n + n') = h(m, n) + h'(m', n')$.

Lembramos que dois módulos hermitianos estão na mesma classe no anel de Witt, $W(A)$, se, e somente se existem módulos hermitianos hiperbólicos (N, g) e (N', g') tais que $(M, h) \perp (N, g) \cong (M', h') \perp (N', g')$.

Seja F um corpo. No que segue, A denotará uma $F-$álgebra com uma involução $\overline{\ }$. Para qualquer extensão de corpos $E \supseteq F$, consideremos a extensão de escalares $A_E = A \otimes_F E$. A extensão dos escalares induz uma aplicação $r^* : W(A) \longrightarrow W(A_E)$ dada por $r^*(M, h) = (M_E, h_E)$, onde $M_E = M \otimes_F E$ e $h_E : M_E \times M_E \longrightarrow A_E$ é dada por $h_E(m_1 \otimes v_1, m_2 \otimes v_2) = h(m_1, m_2) \otimes_F v_1\overline{v_2}$, para todo $m_1, m_2 \in M$ e $v_1, v_2 \in E$.

Os dois teoremas que se seguem são resultados clássicos da teoria algébrica das formas hermitianas, conhecidos como Teorema de Springer e Teorema do Cancelamento de Witt. Suas demonstrações fogem aos nossos objetivos e, por isso, não serão apresentadas. O leitor interessado, pode encontrar a demonstração do Teorema de Springer em [1] ou, traduzida para o português, em [3]. Já a demonstração do Teorema do Cancelamento de Witt, pode ser encontrada em [15], capítulo 7, seções 9 e 10.

Teorema 5.1.3 (Springer)**.** *Se E é uma extensão de grau ímpar de F, então o homomorfismo $r^* : W(A) \longrightarrow W(A_E)$ é injetor.*

Teorema 5.1.4 (Teorema do Cancelamento de Witt)**.** *Suponha que A tem dimensão finita sobre F. Sejam (M,h), (M',h') e (N,g) módulos hermitianos pares não singulares. Se $(M,h) \perp (N,g) \cong (M',h') \perp (N,g)$, então $(M,h) \cong (M',h')$.*

No caso em que $E \supseteq F$ é uma extensão de grau ímpar de corpos e A é uma $F-$álgebra de dimensão finita, temos:

Teorema 5.1.5. *Sejam (M,h) e (M',h') dois $A-$módulos hermitianos pares não singulares. Se $(M_E,h_E) \cong (M'_E,h'_E)$ como A_E-módulos hermitianos, então $(M,h) \cong (M',h')$ como $A-$módulos hermitianos.*

Dem.: Como $(M_E,h_E) \cong (M'_E,h'_E)$, pelo Teorema 5.1.3, temos que (M,h) e (M',h') são iguais em $W(A)$. Ou seja, existem (N,g) e (N',g'), $A-$módulos hermitianos hiperbólicos tais que $(M,h) \perp (N,g) \cong (M',h') \perp (N',g')$.

Assim, $M \oplus N \cong M' \oplus N'$. Mas, como $M_E \cong M'_E$, temos que $M \cong M'$ e, pelo Teorema de Krull Schmidt, temos que $N \cong N'$. Mas, duas formas hermitianas hiperbólicas sobre módulos isomorfos são isomorfas. Assim, $(N,g) \cong (N',g')$ e, pelo Teorema 5.1.4 temos que $(M,h) \cong (M',h')$, como queríamos ■

5.2 A Forma Traço

No que segue, neste capítulo, $E \supseteq F$ é uma extensão galoisiana de corpos e $G = Gal(E/F) = \{\eta_1, \ldots, \eta_n\}$ o seu grupo de Galois.

Para $x \in E$, definimos o *traço de x em $E \supseteq F$* por $Tr_{E/F}(x) = \sum_{i=1}^{n} \eta_i(x)$. Observemos que $Tr_{E/F}(x) \in F$, para todo $x \in E$, pois $Tr_{E/F}(x)$ é fixado pelos elementos de

G, ou seja, $Tr_{E/F}(x) \in Fix(G) = F$. Mais ainda, $Tr_{E/F} : E \longrightarrow F$ é uma aplicação $F-$linear. Assim, a partir de $Tr_{E/F}$, definimos a aplicação $T : E \times E \longrightarrow F$ por $T(x,y) = Tr_{E/F}(xy) = \sum_{i=1}^{n} \eta(x)\eta(y)$, para todo $x, y \in E$. É fácil ver que T é uma forma bilinear simétrica sobre E. Chamaremos T de *a forma bilinear traço da extensão* $E \supseteq F$.

O próximo resultado vale para $E \supseteq F$ separável e finita.

Teorema 5.2.1. *A forma bilinear T, definida acima, é não singular.*

Dem.: Temos que mostrar que a aplicação $H : E \longrightarrow E^* = Hom_F(E,F)$ dada por $H(x)(y) = T(y,x)$, para todo $x, y \in E$, é um isomorfismo de $F-$espaços vetoriais. Para isso, vamos mostrar que a matriz de T com relação a um par de bases é não-singular.

Sejam $B = \{e_1, \ldots, e_n\}$ uma base de E e $B^* = \{f_1, \ldots, f_n\}$ sua base dual. Neste caso, $f_i(e_j) = \delta_{ij}$ e, para $f \in E^*$, f se escreve de maneira única como $f = \sum_{i=j}^{n} f(e_j)f_j$. Assim, como T é simétrica e $H(e_i) \in E^*$, para todo $i \in \{1, \ldots, n\}$, temos que $H(e_i) = \sum_{j=1}^{n} H(e_i)(e_j)f_j = \sum_{i=1}^{n} T(e_i, e_j)f_j$, ou seja, a matriz de T com relação às bases B de E e B^*, de E^* é $M = (T(e_i, e_j))$. Basta então mostrarmos que $\det M \neq 0$.

Como $E \supseteq F$ é uma extensão separável, pelo Teorema do Elemento Primitivo, Corolário 2.1.2, temos que existe $\alpha \in E$ tal que $E = F(\alpha)$. Sejam $m_F(\alpha) \in F[X]$, o polinômio minimal de α sobre F e $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$, as n raízes distintas de $m_F(\alpha)$, onde $\alpha_j = \eta_j(\alpha)$, para cada $j \in \{1, \ldots, n\}$. Como a base B foi tomada arbitrariamente, para $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, ou seja, $e_i = \alpha^{i-1}$, temos $T(e_i, e_j) = T(\alpha^{i-1}, \alpha^{j-1}) = \sum_{r=1}^{n} \eta_r(\alpha^{i-1}\alpha^{j-1}) = \sum_{r=1}^{n} \alpha_r^{i-1}\alpha_r^{j-1}$ e, então

$$M = \begin{pmatrix} T(1,1) & T(1,\alpha) & \cdots & T(1,\alpha^{n-1}) \\ T(\alpha,1) & T(\alpha,\alpha) & \cdots & T(\alpha,\alpha^{n-1}) \\ \vdots & \vdots & \ddots & \vdots \\ T(\alpha^{n-1},1) & T(\alpha^{n-1},\alpha) & \cdots & T(\alpha^{n-1},\alpha^{n-1}) \end{pmatrix} =$$

$$= \begin{pmatrix} \sum_{r=1}^{n} 1.1 & \sum_{r=1}^{n} 1.\alpha_r & \cdots & \sum_{r=1}^{n} 1.\alpha_r^{n-1} \\ \sum_{r=1}^{n} \alpha_r.1 & \sum_{r=1}^{n} \alpha_r.\alpha_r & \cdots & \sum_{r=1}^{n} \alpha_r.\alpha_r^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \sum_{r=1}^{n} \alpha_r^{n-1}.1 & \sum_{r=1}^{n} \alpha_r^{n-1}.\alpha_r & \cdots & \sum_{r=1}^{n} \alpha_r^{n-1}.\alpha_r^{n-1} \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix} \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \cdots & \alpha_2^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \cdots & \alpha_n^{n-1} \end{pmatrix}.$$

Assim,

$$\det(M) = \left(\det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix} \right)^2 = \left(\prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j) \right)^2 \neq 0.$$

Portanto, T é uma forma bilinear simétrica não singular. ■

5.3 Bases Normais Auto-duais

Nesta seção estudaremos as bases normais auto-duais de $E \supseteq F$ utilizando a estrutura de $F[G]-$módulo de E, onde $F[G]$ é a álgebra de grupo de F sobre G. Iniciamos com a definição formal de bases normais auto-duais.

Definição 5.3.1. *Dada uma base $B = \{e_1, \ldots, e_n\}$ de E sobre F, dizemos que a base $B' = \{e'_1, \ldots, e'_n\}$ de E sobre F é a* base dual de B, *se $T(e_i, e'_j) = \delta_{ij}$, para todo $i, j \in \{1, \ldots, n\}$. Se a base B satisfaz $T(e_i, e_j) = \delta_{ij}$, para todo $i, j \in \{1, \ldots, n\}$, então B é dita ser uma* base auto-dual. *Finalmente, uma base normal $\{\eta_1(\alpha), \ldots, \eta_n(\alpha)\}$ de E sobre F é uma* base normal auto-dual *se $T(\eta_i(\alpha), \eta_j(\alpha)) = \delta_{ij}$, para todo $i, j \in \{1, \ldots, n\}$.*

Seja $F[G]$ a álgebra de grupo e $\bar{}: F[G] \longrightarrow F[G]$ a involução $F-$linear dada por $\bar{g} = g^{-1}$, para todo $g \in G$. Observemos que E tem uma estrutura de $F[G]-$módulo, com a ação $\left(\sum_{i=1}^{n} a_i\eta_i\right) \cdot \alpha = \sum_{i=1}^{n} a_i\eta_i(\alpha)$, para todo $\sum_{i=1}^{n} a_i\eta_i \in F[G]$ e $\alpha \in E$.

Usando esta estrutura de $F[G]-$módulo de E, associamos à forma $T : E \times E \longrightarrow F$ a $F[G]-$forma $h : E \times E \longrightarrow F[G]$, onde

$$h(x, y) = \sum_{g \in G} T(gx, y)g^{-1},$$

para todo $x, y \in E$. É fácil ver que (E, h) é um módulo hermitiano sobre $F[G]$, com a involução $\bar{}$.

O próximo resultado, nos dá uma caracterização das bases normais e das bases normais auto-duas da extensão $E \supseteq F$ em termos da estrutura de $F[G]-$módulo de E.

Lema 5.3.2. *Seja $\alpha \in E^{\times}$. Então:*
(i) α é um elemento normal de $E \supseteq F$ se, e somente se $\{\alpha\}$ é uma base de E sobre $F[G]$;
(ii) α gera uma base normal auto-dual de $E \supseteq F$ se, e somente se $\{\alpha\}$ é uma base ortonormal de E sobre $F[G]$ com respeito a h.

Dem.: Se $\alpha \in E^{\times}$ é um elemento normal de $E \supseteq F$, ou seja, $B = \{\eta_1(\alpha), \eta_2(\alpha), \ldots, \eta_n(\alpha)\}$ é uma base de $E \supseteq F$, então, para cada $x \in E$, existem $a_1, \ldots, a_n \in F$ tais que $x = \sum_{i=1}^{n} a_i\eta_i(\alpha)$. Usando a ação de $F[G]$ em E, temos que $x = \left(\sum_{i=1}^{n} a_i\eta_i\right) \cdot \alpha$, onde $\sum_{i=1}^{n} a_i\eta_i \in F[G]$, o que mostra que $\{\alpha\}$ gera E como $F[G]-$módulo. Para mostrar que $\{\alpha\}$ é linearmente independente sobre $F[G]$, suponha que exista $\sum_{i=1}^{n} a_i\eta_i \in F[G]$ tal que $\left(\sum_{i=1}^{n} a_i\eta_i\right) \cdot \alpha = \sum_{i=1}^{n} a_i\eta_i(\alpha) = 0$. Como $\{\eta_1(\alpha), \ldots, \eta_n(\alpha)\}$ é linearmente independente sobre F, segue que $a_i = 0$, para todo $i \in \{1, \ldots, n\}$ e, portanto, $\{\alpha\}$ é linearmente independente sobe $F[G]$, ou seja, uma base de E sobre $F[G]$.

Reciprocamente, se $\{\alpha\}$ é uma base de E sobre $F[G]$, sejam $a_1, \ldots, a_n \in F$, tais que $\sum_{i=1}^{n} a_i\eta_i(\alpha) = 0$. Então, $0 = \left(\sum_{i=1}^{n} a_i\eta_i\right) \cdot \alpha$ e, como $\{\alpha\}$ é linearmente independente

sobre $F[G]$, segue que $\sum_{i=1}^{n} a_i\eta_i = 0$ em $F[G]$, ou seja, $a_1 = \cdots = a_n = 0$. Portanto, $\{\eta_1(\alpha), \ldots, \eta_n(\alpha)\}$ é linearmente independente sobre F. Como $\{\alpha\}$ gera E sobre $F[G]$, segue que dado $x \in E$, existe $\sum_{i=1}^{n} a_i\eta_i \in F[G]$ tal que $x = \left(\sum_{i=1}^{n} a_i\eta_i\right) \cdot \alpha = \sum_{i=1}^{n} a_i\eta_i(\alpha)$, o que mostra que $\{\eta_1(\alpha), \ldots, \eta_n(\alpha)\}$ gera E e, ou seja, que é uma base normal de E sobre F, o que mostra (i)

Se $B = \{\eta_1(\alpha), \ldots, \eta_n(\alpha)\}$ é uma base normal auto-dual de E sobre F, então $T(\eta_i(\alpha), \eta_j(\alpha)) = \delta_{ij}$. Dessa forma, para cada $\eta \in G$, temos $T(\eta(\alpha), \alpha) = 0$, se $\eta \neq id$, e $T(\eta(\alpha), \alpha) = 1$, se $\eta = id$. Logo, $h(\alpha, \alpha) = \sum_{\eta \in G} T(\eta(\alpha), \alpha)\overline{\eta} = 1$, ou seja, $\{\alpha\}$ é uma base ortonormal de E sobre $F[G]$.

Reciprocamente, se $h(\alpha, \alpha) = 1$, para cada $\eta \in G$, temos que $T(\alpha, \alpha) = 1$, e $T(\eta(\alpha), \alpha) = 0$, se $\eta \neq id$, o que implica que $T(\eta_i(\alpha), \eta_j(\alpha)) = T(\eta_j^{-1}\eta_i(\alpha), \alpha) = \delta_{ij}$ e vale (ii). ■

Como $E \supseteq F$ é galoisiana, pelo Teorema da Base Normal, E admite uma base normal sobre F. Seja $\alpha \in E^{\times}$ um elemento normal de $E \supseteq F$. Seja $u = h(\alpha, \alpha) \in F[G]$. Considerando as formas $F[G]-$hermitianas $\langle 1\rangle$ e $\langle u\rangle \cong (E, h)$, podemos reformular a segunda parte do resultado anterior da seguinte forma.

Lema 5.3.3. *A extensão galoisiana $E \supseteq F$ admite uma base normal auto-dual se, e somente se as formas $F[G]-$hermitianas $\langle 1\rangle$ e $\langle u\rangle$ são isomorfas.*

Dem.: Se E tem uma base normal auto-dual sobre F, gerada por α, então $h(\alpha, \alpha) = 1$, ou seja, $u = 1$ e, claramente, $\langle 1\rangle \cong \langle u\rangle$, como formas $F[G]-$hermitianas.

Reciprocamente, se $\langle 1\rangle \cong \langle u\rangle$, como $F[G]-$módulos hermitianos, então existe $\varphi : F[G] \longrightarrow F[G]$ isomorfismo de $F[G]-$módulos, tal que tal que $x\overline{y} = \varphi(x)u\overline{\varphi(y)}$, para todo $x, y \in F[G]$. Como $h(\alpha, \alpha) = u$, temos $x\overline{y} = \varphi(x)h(\alpha, \alpha)\overline{\varphi(y)} = h(\varphi(x)\alpha, \varphi(y)\alpha)$. Em particular, para $x = y = 1$, temos $1 = h(\varphi(1)\alpha, \varphi(1)\alpha) = h(\alpha, \alpha)$. Logo, $h(\alpha, \alpha) = 1$ e α gera uma base normal auto-dual de $E \supseteq F$. ■

Nosso próximo objetivo é mostrarmos que as extensões por escalares das formas $F[G]-$hermitianas $\langle 1\rangle$ e $\langle u\rangle$ são isomorfas como $E[G] = E \otimes_F F[G]-$módulos hermitianos. Para tanto, necessitamos do seguinte resultado:

Lema 5.3.4. *A álgebra de Galois $E \otimes_F E$ tem base normal auto-dual sobre E.*

Dem.: Pelo Teorema 1.1.12, $E \supseteq F$ é galoisiana se, e somente se $E^{|G|} \cong E \otimes_F E$. Assim, é suficiente mostrarmos que $E^{|G|}$ admite uma base normal auto-dual sobre E.

Para cada $\eta \in G$, seja $e_\eta = (x_\rho)_{\rho \in G} \in E^{|G|}$, onde $x_\rho = 1$, se $\rho = \eta$ e $x_\rho = 0$, se $\rho \neq \eta$. Temos que $B = \{e_\eta\}_{\eta \in G}$ é uma base de $E^{|G|}$ sobre E.

Vamos mostrar que B é uma base normal auto-dual de $E^{|G|}$ sobre E. O produto em $E^{|G|}$ é induzido por $e_\eta e_\tau = \delta_{\tau\eta} e_\eta$ e $\sum_{\eta \in G} e_\eta = (1, \ldots, 1)$.

Todo elemento de $E^{|G|}$ pode ser escrito na forma $\sum_{\rho \in G} \lambda_\rho e_\rho$, com $\lambda_\rho \in E$, e a ação de G em $E^{|G|}$, é dada por $\eta \cdot \left(\sum_{\rho \in G} \lambda_\rho e_\rho \right) = \sum_{\rho \in G} \lambda_\rho e_{\eta\rho}$. Note que B é uma base normal de $E^{|G|}$ sobre E, pois $\{\tau(e_\rho)\}_{\tau \in G} = \{e_{\rho\tau}\}_{\tau \in G} = \{e_\tau\}_{\tau \in G} = B$.

Agora, os elementos da forma $(x, \ldots, x) \in E^{|G|}$ são os elementos fixados pela ação de G. Identificaremos um elemento $x \in E$ com o elemento $(x, \ldots, x) \in E^{|G|}$.

Como, $T(e_\eta, e_\tau) = \sum_{\rho \in G} \rho(e_\eta e_\tau)$ e como $\sum_{\rho \in G} \rho(e_\eta) = 1$, temos que $T(e_\eta, e_\tau) = 1$, se $\eta = \tau$ e $T(e_\eta, e_\tau) = 0$, se $\eta \neq \tau$. Portanto, como queríamos, $\{e_\eta\}_{\eta \in G}$ é uma base normal auto-dual de $E^{|G|}$ sobre E. ■

Corolário 5.3.5. *As formas hermitianas $\langle 1 \rangle$ e $\langle u \rangle$ são isomorfas sobre $E[G]$.*

Dem.: O resultado segue diretamente do Lema 5.3.3 e do Lema 5.3.4. ■

Antes do resultado principal, vejamos alguns resultados preliminares. No que segue, $s = \sum_{\eta \in G} \eta \in F[G]$, $B = sF[G]$ é a subálgebra de $F[G]$ gerado por s em $F[G]$ e $A = \dfrac{F[G]}{B}$ a álgebra quociente. Também assumiremos, no que segue, que $E \supseteq F$ é uma extensão de grau ímpar, ou seja, $n = [E : F]$ é ímpar.

Lema 5.3.6. *Se $car(F) = 2$ e A é definido como acima, temos que $F[G] \cong A \times F$.*

Dem.: Inicialmente, é fácil ver que $\overline{s} = s$ e que $s \in Z(F[G])$ pois $s\eta = s = \eta s$, para todo $\eta \in G$. Para cada $x \in B$, temos que $x = sy$, para algum $y \in F[G]$ e $\overline{x} = \overline{sy} = \overline{ys} = \overline{y}s = s\overline{y} \in B$. Logo, $\overline{B} \subseteq B$. Mais ainda, se $x = sy \in B$, com $y \in F[G]$, então $x = \overline{s\overline{y}} \in \overline{B}$, o

que mostra que $B = \overline{B}$. Portanto, a involução $\bar{}: F[G] \longrightarrow F[G]$ induz uma involução $\bar{}: A \longrightarrow A$.

Note que s é idempotente, pois $s^2 = s\left(\sum_{\eta\in G}\eta\right) = \sum_{\eta\in G} s\eta = \sum_{\eta\in G} s = |G|s = s$, pois $|G|$ é ímpar e $car(F) = 2$.

Com isso, usando que $s \in Z(F[G])$ é idempotente, temos que

$$F[G] \cong sF[G] \times (1-s)F[G].$$

De fato, é fácil ver que a aplicação $\varphi : F[G] \longrightarrow sF[G] \times (1-s)F[G]$ definida por $\varphi(x) = (sx, (1-s)x)$, para todo $x \in F[G]$ é um homomorfismo de $F-$álgebras.

Resta então mostrarmos que φ é bijetora. Se $\varphi(x) = 0$ então $sx = 0$ e $(1-s)x = 0$. Mas $(1-s)x = x - sx = x$. Logo, $x = 0$ e φ é injetora. Seja $(sx, (1-s)y) \in sF[G]\times(1-s)F[G]$. Tomando $z = y - sy + sx \in F[G]$, temos que, $\varphi(z) = (sx, (1-s)y)$. Logo φ é sobrejetora e, portanto, um isomorfismo de $F-$álgebras.

Agora, observemos que $A \cong (1-s)F[G]$ como $F-$álgebras. De fato, a aplicação $\phi : A \longrightarrow (1-s)F[G]$, definida por $\phi(\overline{x}) = (1-s)x$, para todo $\overline{x} \in A$, satisfaz $\varphi(\overline{x}+\overline{y}) = \varphi(\overline{x}) + \varphi(\overline{y})$ e $\varphi(\overline{xy}) = \varphi(\overline{x})\varphi(\overline{y})$, para todo $\overline{x}, \overline{y} \in A$, propriedade esta, que segue do fato que $s \in Z(F[G])$ e é idempotente.

Note que ϕ está bem definido, pois se $\overline{x} = \overline{y}$, então $x - y \in B$, ou seja, existe $z \in F[G]$ tal que $x - y = sz$. Mas $sz = s^2z$, o que mostra que $(x-y) = s(x-y)$ e $x - sx = y - sy$. Logo, $\phi(\overline{x})(1-s)x = (1-s)y = \phi(\overline{y})$.

É fácil ver que ϕ é bijetora. Logo, ϕ é um isomorfismo de $F-$álgebras, ou seja, $A \cong (1-s)F[G]$.

Assim, obtemos que $F[G] \cong sF[G] \times (1-s)F[G] \cong B \times A$.

Finalmente, mostraremos que $B \cong F$.

Seja $sF = \{sa;\ a \in F\} \subseteq F[G]$. Para $sx \in sF[G]$, temos $sx = s\sum_{i=1}^{n} a_i\eta_i = \sum_{i=1}^{n} a_i s\eta_i = \sum_{i=1}^{n} a_i s = s\sum_{i=1}^{n} a_i \in sF$. Logo, $sF[G] \subseteq sF$, o que mostra que $B = sF[G] = sF$.

Também é fácil ver que $\psi : sF \longrightarrow F$, definida por $\psi(sa) = a$, para todo $a \in F$, é um isomorfismo de $F-$álgebras.

Logo, $B \cong F$ e, como queríamos, $F[G] \cong A \times F$. ■

O próximo resultado, juntamente com o Lema 5.1.1, nos mostra que quando $E \supseteq F$ é uma extensão galoisiana de grau ímpar e A é definido como acima, então todo $A-$módulo hermitiano é par.

Lema 5.3.7. *Se $car(F) = 2$ e A é como acima, então existe $\alpha \in Z(A)$ tal que $\alpha + \overline{\alpha} = 1$.*

Dem.: Notemos inicialmente que o fato de $G = Gal(E/F)$ ter ordem ímpar, implica que nenhum elemento de G diferente da identidade é igual ao seu próprio inverso, ou seja, para todo $\eta \in G - \{id\}, \eta \neq \overline{\eta} = \eta^{-1}$.

Mostremos agora que existe um subconjunto S de G, estável sob a conjugação, isto é, $\eta S \eta^{-1} = S$, para todo $\eta \in G$, tal que $G = \{id\} \dot{\bigcup} S \dot{\bigcup} \overline{S}$, ou seja, todo elemento de G, diferente da identidade, está em S, ou seu inverso está em S, mas não ambos.

Para cada $\tau \in G$, seja $cl(\tau) = \{\eta\tau\eta^{-1};\ \eta \in G\}$ a classe de conjugação de τ em G. Como $cl(\tau)$ divide $|G|$ que é ímpar, temos que $|cl(\tau)|$ é um número ímpar, para todo $\tau \in G$. Mais ainda, para cada $\tau \in G - \{id\}$, temos $cl(\tau) \bigcap cl(\tau^{-1}) = \emptyset$. De fato, se $cl(\tau) \bigcap cl(\tau^{-1}) \neq \emptyset$, para algum $\tau \in G$, então existem $\sigma_1, \sigma_2 \in G$ tais que $\sigma_1\tau\sigma_1^{-1} = \sigma_2\tau^{-1}\sigma_2^{-1}$. Logo, $\sigma = \sigma_2^{-1}\sigma_1 \in G$ é tal que $\tau^{-1} = \sigma\tau\sigma^{-1}$, ou seja, $\tau^{-1} \in cl(\tau)$. Vamos mostrar que isto leva a uma contradição. Sejam $\varphi \in cl(\tau)$ e $\theta \in G$ tal que $\varphi = \theta\tau\theta^{-1}$. Assim, $\varphi^{-1} = \theta\tau^{-1}\theta^{-1} = \theta(\sigma\tau\sigma^{-1})\theta^{-1} = (\theta\sigma)\tau(\theta\sigma)^{-1} \in cl(\tau)$. Assim, se $\varphi \in cl(\tau)$ então $\varphi^{-1} \in cl(\tau)$. Mas, como $\varphi \neq \varphi^{-1}$, para todo $\varphi \in cl(\tau)$, concluímos que $cl(x)$ é par, o que é uma contradição.

Sejam $\tau_1 \in G - \{id\}$, $S_1 = cl(\tau_1)$ e $\overline{S_1} = cl(\tau^{-1})$. Como $S_1 \bigcap \overline{S_1} = \emptyset$, se $G = \{id\} \dot{\bigcup} S_1 \dot{\bigcup} \overline{S_1}$, tomamos $S = S_1$. Caso contrário, sejam $\tau_2 \in G - (\{id\} \dot{\bigcup} S_1 \dot{\bigcup} \overline{S_1})$, $S_2 = cl(\tau_2)$ e $\overline{S_2} = cl(\tau_2^{-1})$. Como as classes de conjugação formam uma partição de G, temos que $S_1 \bigcap S_2 = \emptyset$. Se $G = \{id\} \dot{\bigcup} S_1 \dot{\bigcup} S_2 \dot{\bigcup} \overline{S_1} \dot{\bigcup} \overline{S_2}$, tomamos $S = S_1 \dot{\bigcup} S_2$, caso contrário, repetimos este raciocínio um número finito de vezes, pois $|G|$ é finito, e obtemos que o conjunto $S = S_1 \dot{\bigcup} S_2 \dot{\bigcup} \cdots \dot{\bigcup} S_r$ satisfaz o requerido, onde $S_1 = cl(\tau_1)$ e $S_i = cl(\tau_i)$, com $\tau_i \in G - (\{id\} \dot{\bigcup} S_1 \dot{\bigcup} \cdots \dot{\bigcup} S_{i-1})$. Assim, tomando $\alpha = 1 + \sum_{g \in S} g$, temos que $\alpha + \overline{\alpha} = 1 + s = \overline{1} \in A$. ■

Agora estamos prontos para apresentar o resultado principal deste capítulo.

Teorema 5.3.8. *Toda extensão galoisiana de grau ímpar admite uma base normal auto-dual.*

Dem.: Sejam $E \supseteq F$ uma extensão galoisiana de grau ímpar. Mostremos o teorema com as considerações e notações dos resultados acima.

Consideremos inicialmente, o caso $car(F) \neq 2$. Neste caso, pelo corolário 5.1.2 temos que todo $F[G]-$módulo hermitiano é par. Do Corolário 5.3.5, temos que $\langle u \rangle \cong \langle 1 \rangle$ sobre $E[G]$. Como $\langle u \rangle \cong \langle 1 \rangle$ sobre $E[G] \cong E \otimes_F F[G]$, o Teorema 5.1.5, nos garante que $\langle u \rangle \cong \langle 1 \rangle$ sobre $F[G]$. Assim, pelo Lema 5.3.3, E admite uma base normal auto-dual sobre F.

Se $car(F) = 2$, pelo Corolário 5.3.5, existe $y = (y_A, y_F) \in E[G] \cong A_E \times E$, tal que $y\overline{y} = u$. Assim, $y_A\overline{y_A} = v,\ y_F\overline{y_F} = w$, onde $u = (v, w) \in A \times F$. Como a involução $\overline{\ }$ é a identidade em F, temos que sua extensão a uma involução de $E[G]$ é a identidade em E. Logo $\overline{y_F} = y_F$, o que implica que $y_F^2 = w$. Vamos mostrar que $y_F \in F$. Note que y_F é raiz do polinômio $f(x) = x^2 - w \in F[x]$. Temos então que $F \subseteq F(y_F) \subseteq E$ e, portanto, $[E : F] = [E : F(y_F)][F(y_F) : F]$. Como $[E : F]$ é ímpar, segue que $y_F \in F$.

Pelos Lemas 5.3.7 e 5.1.1, temos que toda forma hermitiana sobre A é par. Como $y_A\overline{y_A} = v \in A$, segue que $\langle 1 \rangle \cong \langle v \rangle$ sobre A_E. Assim, pelo Teorema 5.1.5, $\langle 1 \rangle$ e $\langle v \rangle$ são isomorfas sobre A. Em outras palavras, existe $x_A \in A$ tal que $x_A\overline{x_A} = v$. Tomando $x = (x_A, y_F) \in F[G]$, temos que $x\overline{x} = u$. Assim, pelo Lema 5.3.3, E admite uma base normal auto-dual sobre F, como queríamos. ■

Referências Bibliográficas

[1] Bayer-Fruckiger, E. and Lenstra Jr, H. W., *Forms in odd degree extensions and self-dual normal bases*, Amer. J. Math. 112 (1990), 359-373.

[2] Bayer-Fluckiger, E., *Self-dual normal bases*, Indag. Math. 51 (1989), 379-383.

[3] Braga, A.C., *Bases Normais Auto-Duais*, Dissertação de Mestrado, Universidade Estadual de Maringá, Maringá, 2003.

[4] Bshouty, N. H. and Seroussi, G., *Generalizations of the normal basis theorem for finite fields*, SIAM J. Disc. Math. 3 (1990), 330-337.

[5] Gao, S., *Normal Bases over Finite Fields*, Tese de Doutorado, Universidade de Waterloo, Ontário, 1993.

[6] Garcia A. and Lequain, Y., *Elementos de Álgebra*, Projeto Euclides, Rio de Janeiro, 2003.

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

[8] Lam, T.Y., *The Algebraic Theory of Quadratic Forms*, University of California, (1973).

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

[10] Paques, A., *Teoría de Galois sobre Anillos Conmutativos*, Consejo de Publicaciones Facultad de Ciencias - Mérida- Venezuela (1999).

[11] Poli, A. and Huguet, L., *Error Correcting Codes : Theory and Applications,* Prentice Hall, 1992.

[12] Poli, A., *A deterministic construction for normal bases of abelian extensions*, Comm. in Algebra 22 (1994), 4751-4757.

[13] Poli, A., *Idéaux principaux nilpotents de dimension maximale dans l'algèbre Fq[G] d'un groupe abèlien fini G*, Communications in Algebra, 12(4), pp 391-401, 1984.

[14] Rotman, J. *Galois Theory*, Universitext. Springer-Verlag, New York, 1998.

[15] Scharlau, W., *Quadratic and Hermitian Forms*, Grundlehren der Math. Wiss. 270, Springer Verlag (1985).

[16] Schwartz, S., *Construction of normal bases in cyclic extensions of field*, Czechoslovak Math. J. 38(1988), 291-312.

[17] Stewart, I., *Galois Theory*, Third Edition. Chapman & Hall/CRC Mathematics. Chapman & Hall/CRC, Boca Raton, FL, 2004.

[18] Waterhouse,W. C., *A unified version of primitive and normal basis theorems*, Comm. In Algebra 22 (1994), 2305-2308.

[19] Waterhouse, W. C., *The normal basis theorem*, Amer. Math. Month. 86 (1979), 212.