Universidade Federal do Rio Grande do Sul

Instituto de Matemática

Programa de Pós-Graduação em Matemática

Estrutura de Módulo de Extensões Finitas de Corpos

Dissertação de Mestrado

GLAUBER RODRIGUES DE QUADROS

Porto Alegre, 30 de Março de 2012

Dissertação submetida por Glauber Rodrigues de Quadros* **, como requisito parcial para a obtenção do grau de Mestre em Ciência Matemática, pelo Programa de Pós-Graduação em Matemática, do Instituto de Matemática da Universidade Federal do Rio Grande do Sul.**

Professor Orientador:

Prof. Dr. Antonio Paques

Banca examinadora:

Prof. Dr. Antonio Paques (IM - UFRGS, ORIENTADOR)

Profª. Drª. Cydara Cavedon Ripoll (IM - UFRGS)

Profª. Drª. Daiana Aparecida da Silva Flôres (UFSM)

Prof. Dr. Dirceu Bagio (UFSM)

*Bolsista do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq)

Agradecimentos

À minha esposa pelo apoio psicológico, companheirismo e compreensão nos momentos difíceis.

À minha família, com a qual sei que sempre posso contar.

Ao meu orientador por toda a ajuda, paciência e boas idéias.

A todos os membros da banca pelas excelentes sugestões e correções feitas.

Agradeço também à Universidade Federal do Rio Grande do Sul, pela oportunidade de realização deste curso e ao CNPq pelo apoio financeiro.

Resumo

Mostraremos de duas maneiras diferentes (uma delas usando o Teorema da Base Normal e a outra não) que se um corpo L é uma extensão finita um corpo K e G é um subgrupo dos K-automorfismos de L, então L é um $K[G]$-módulo à esquerda livre com exatamente $[L^G : K]$ geradores. Mais ainda, se $c(K) \neq 2$ e N é o fecho normal de L/K com $[N : K]$ ímpar, então conseguimos dar uma interessante estrutura de espaço quadrático a L.

Esta dissertação foi elaborada com base no artigo de P. Lundström: "Galois Module Structure Of Fields Extensions", International Eletronic Journal Of Algebra, 2007.

Abstract

We will show in two different ways (one using the Normal Basis Theorem and the other not) that if a field L is a finite extension of a field K and G is a subgroup of K-automorfisms of L, then L is a free left $K[G]$-module with exactly $[L^G : K]$ generators. Moreover, if $c(K) \neq 2$ and N is the normal closure of L/K with $[N : K]$ odd, then we can give an interesting structure of quadratic space to L.

The subject of this dissertation is based on P. Lundström's paper: "Galois Module Structure Of Fields Extensions", International Eletronic Journal Of Algebra, 2007.

Índice

Introdução **1**

1 Preliminares **3**

1.1 Um pouco da Teoria de Galois 3

1.2 O Traço 26

1.3 Krull-Schmidt 30

1.4 Formas quadráticas 38

2 O Teorema da Base Normal **53**

3 Estruturas de Módulos **71**

3.1 Estrutura de $K[G]$-módulo de uma extensão finita de corpos 71

3.2 Outro olhar sobre o Teorema 3.1.1 73

4 Estrutura de Espaço Quadrático **89**

Referências Bibliográficas **93**

Introdução

Neste trabalho mostraremos por dois métodos independentes que se L/K é uma extensão finita de corpos e G é um subgrupo dos K-automorfismos de L, então L é um $K[G]$-módulo à esquerda livre com exatamente $[L^G : K]$ geradores.

No primeiro método, feito na Seção 3.1, usamos uma demonstração relativamente simples, que pode ser facilmente entendida por qualquer um que conheça o Teorema da Base Normal, abordado no Capítulo 2. Este teorema é de vital importância para o método e é pouco abordado na literatura, sendo quase sempre remetido ao caso em que o corpo é infinito. Aqui, faremos ambos os casos e este capítulo depende apenas da Seção 1.1 e de um pequeno conhecimento sobre álgebra linear.

No segundo método usamos uma demonstração mais elaborada, construída ao longo de toda a Seção 3.2. Este método é totalmente independente do Teorema da Base Normal, podendo-se entendê-lo apenas usando as Seções 1.1 e 1.3 e resultados básicos sobre o produto tensorial entre módulos. Para resultados importantes sobre o produto tensorial de módulos, recomendamos a leitura de [11] ou [1].

Em decorrência desta segunda demonstração, no Capítulo 4 conseguimos dar a L uma interessante estutura de K-espaço quadrático, usando a forma traço descrita na Seção 1.2. É de grande importância que o leitor compreenda o tema abordado

na Seção 1.4 que, juntamente com as Seções 1.2 e 3.2 são os alicerces para um total entendimento do resultado final.

Optamos por colocar vários resultados da teoria de Galois para que o leitor se familiarize com os conceitos, que serão usados ao longo de todo este trabalho.

As preliminares incluem resultados, com e sem demonstrações, que são necessários para os capítulos seguintes. No intuito de não tornar o texto excessivamente volumoso, optamos por apresentar apenas aquelas demonstrações que não exigissem uma quantidade muito grande de pré-requisitos. Para as demonstrações omitidas, o leitor é remetido à bibliografia.

Capítulo 1

Preliminares

Neste capítulo falaremos um pouco sobre Teoria de Galois, Teoria de Módulos e Formas Quadráticas. Isto nos dará um embasamento para entendermos mais facilmente os capítulos seguintes.

1.1 Um pouco da Teoria de Galois

A teoria de Galois será de fundamental importância para o contexto geral deste trabalho. Tentamos encaixar os resultados da melhor forma possível para que o leitor se familiarize com a teoria.

Dizemos que um corpo L é extensão de um corpo K (ou que L estende K) se K for um subcorpo de L. Vamos denotar essa extensão por L/K.

Vamos chamar de grau da extensão L/K à dimensão de L como K-espaço vetorial. Denotaremos este grau por $[L : K]$.

Teorema 1.1.1. *Se L é uma extensão de K e F é uma extensão de L, então $[F : K] = [F : L][L : K]$, mesmo quando alguma destas dimensões é infinita.*

Demonstração. Sejam $a_1, ..., a_m$ elementos de F linearmente independentes sobre L e $b_1, ..., b_n$ elementos de L linearmente independentes sobre K.

Suponha $\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}a_ib_j = 0$ com $c_{ij} \in K$, para todo $i = 1, ..., m$ e $j = 1, ..., n$.

Repare que $\sum_{j=1}^{n} c_{ij}b_j \in L$, logo como $\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}a_ib_j = \sum_{i=1}^{m}(\sum_{j=1}^{n} c_{ij}b_j)a_i = 0$ e $a_1, ..., a_m$ são linearmente independentes sobre L, então $\sum_{j=1}^{n} c_{ij}b_j = 0$, para todo $i \in \{1, ..., m\}$.

Como $b_1, ..., b_n$ são linearmente independentes sobre K e $\sum_{j=1}^{n} c_{ij}b_j = 0$, para todo i em $\{1, ..., m\}$, então $c_{ij} = 0$ para todo $i = 1, ..., m$ e $j = 1, ..., n$.

Concluímos então que o conjunto $\{a_ib_j | 1 \leq i \leq n \text{ e } 1 \leq j \leq m\}$ é linearmente independente.

Isto nos diz que o teorema é válido mesmo quando $[L : K]$ ou $[F : L]$ são infinitos.

Suponha agora que $[F : L] = m$ e $[L : K] = n$, $\{a_1, ..., a_m\}$ é uma base de F sobre L e $\{b_1, ..., b_n\}$ é uma base de L sobre K.

Se $d \in F$, então $d = \sum_{i=1}^{m} c_ia_i$ com $c_i \in L$ para todo $i \in \{1, ..., m\}$. Para qualquer $i \in \{1, ..., m\}$, $c_i = \sum_{j=1}^{n} d_{ij}b_j$ com $d_{ij} \in K$, para todo $i \in \{1, ..., m\}$ e $j \in \{1, ..., n\}$. Logo $d = \sum_{i=1}^{m}\sum_{j=1}^{n} d_{ij}a_ib_j$.

Assim o conjunto $\{a_ib_j \mid i = 1, ..., m \text{ e } j = 1, ..., n\}$ é base de F sobre K, ou seja, $[F : K] = [F : L][L : K]$ □

Definição 1.1.2. *Uma extensão L/K é dita finita se $[L : K]$ é finito.*

Considere L/K uma extensão de corpos.

Se U for um subconjunto de L, denotaremos por $K(U)$ o menor corpo que estende K e contém U. Se U for um conjunto finito, digamos $U = \{a_1, ..., a_n\}$,

vamos denotar $K(U)$ por $K(a_1, ..., a_n)$.

Veja que $K(a)$ é exatamente o corpo $\{\frac{f(a)}{g(a)} \mid f(X), g(X) \in K[X] \text{ e } g(a) \neq 0\}$.

Ainda, denotaremos por $K[a]$ o anel $\{f(a) \mid f(X) \in K[X]\}$.

Se L/K é uma extensão finita, então existe uma base $\{a_1, ..., a_n\}$ de L sobre K. Logo $L = K(a_1, ..., a_n)$.

Definição 1.1.3. *Se $a \in L$ e existe um polinômio $p(X)$ em $K[X]$ tal que $p(a) = 0$, dizemos que a é algébrico sobre K. L/K é dita extensão algébrica se todo elemento de L for algébrico sobre K.*

Veja que toda extensão finita é algébrica pois, se L/K é uma extensão de grau n e $a \in L$, então $\{1, a^1, ..., a^{n-1}, a^n\}$ é um conjunto linearmente dependente sobre K. Desta forma, existem $\{c_0, ..., c_n\}$ não todos nulos em K tais que $\sum_{i=0}^{n} c_i a^i = 0$. Logo, $p(X) = \sum_{i=0}^{n} c_i X^i \in K[X]$ e $p(a) = 0$, ou seja, L/K é uma extensão algébrica.

Teorema 1.1.4. *Sejam L/K uma extensão de corpos e $a \in L$ algébrico sobre K. Valem:*

(i) Existe um único polinômio mônico irredutível $p(X) \in K[X]$ tal que $p(a) = 0$.

(ii) Se $g(x)$ é um polinômio em $K[X]$ tal que $g(a) = 0$, então $p(X)$ divide $g(X)$.

(iii) $K(a) = K[a]$.

(iv) Todo elemento de $K(a)$ é escrito unicamente na forma $r(a)$ onde $r(X) \in K[X]$ e $r(X) = 0$ ou $deg(r(X)) < deg(p(X))$.

(v) $K(a)/K$ é uma extensão algébrica.

(vi) $[K(a) : K] = deg(p(X))$.

Demonstração.

(i) Defina $\psi : K[X] \longrightarrow K[a]$ por $\psi(f(X)) = f(a)$. É claro que ψ é um homomorfismo bem definido de anéis. Repare que ψ é sobrejetor.

Como a é algébrico sobre K, então $ker(\psi) \neq 0$. Desta forma $ker(\psi)$ é um ideal de $K[X]$. Como todo ideal em $K[X]$ é principal, existe $p(X) \in K[X]$ tal que $ker(\psi) =< p(X) >$. Vamos supor sem perda de generalidade que $p(X)$ seja mônico.

Pelo Teorema do Isomorfismo, $\frac{K[X]}{<p(X)>} \simeq K[a]$ que é um domínio de integridade. Logo $< p(X) >$ é um ideal primo.

Desta maneira $p(X)$ é irredutível em $K[X]$, pois se $p(X) = g(X)h(X)$, então $g(X) \in< p(X) >$ ou $h(X) \in< p(X) >$ ou seja, $g(X) = p(X)$ ou $h(X) = p(X)$.

Se $g(X) \in K[X]$ é tal que $g(a) = 0$, então $g(X) \in ker(\psi) =< p(X) >$. Logo $g(X) = p(X)h(X)$, para algum $h(X) \in K[X]$.

Assim, $p(X)$ é o único polinômio mônico irredutível que anula a.

(ii) Imediato da demonstração do ítem (i).

(iii) Como em um anel de polinômios sobre um corpo todo ideal primo não nulo é maximal, temos que $\frac{K[X]}{<p(X)>}$ é um corpo. Logo $K[a]$ é um corpo e assim $K(a) \subseteq K[a]$. A inclusão contrária é imediata.

(iv) Se $\alpha \in K(a) = K[a]$, então existe $h(X) \in K[X]$ tal que $\alpha = h(a)$.

Veja que dado $h(X) \in K[X]$ existem polinômios $q(X)$ e $r(X)$ em $K[X]$ tais que $h(X) = q(X)p(X) + r(X)$ e $r(X) = 0$ ou $deg(r(X)) < deg(p(X))$.

Logo $\alpha = h(a) = q(a)p(a) + r(a) = r(a)$.

Mais ainda, se $\alpha = r'(a)$ para algum $r'(X) \in K[X]$ e $deg(r'(X)) < deg(p(X))$, então $g(X) = r(X) - r'(X) \in K[X]$ tem grau menor do que $p(X)$ e $g(a) = 0$, ou seja, como $g(X) \in< p(X) >$ devemos ter $g(X) = 0$.

Desta forma temos que $r(X)$ é o único polinômio em $K[X]$ tal que $\alpha = r(a)$ e

$deg(r(X)) < deg(p(X))$ ou $r(X) = 0$.

(v) e (vi) Pelo ítem (iv) temos claramente que $\{1, a, a^2..., a^{n-1}\}$ é uma base de $K(a)$ sobre K com $n = deg(p(X))$. Logo $K(a)$ é extensão finita (e portanto algébrica) de K e $[K(a) : K] = n$.

□

Desta maneira, se $p(X)$ for o polinômio mônico irredutível em $K[X]$ que anula a, diremos que $p(X)$ é o minimal de a em $K[X]$.

Corolário 1.1.5. *Se $a_1, ..., a_r$ são algébricos sobre K, então $K(a_1, ..., a_r)$ é uma extensão algébrica de K.*

Demonstração. Basta ver que, se a_i é algébrico sobre K, então a_i é algébrico sobre $K(a_1, ..., a_{i-1})$. Desta forma, a extensão $K(a_1, ..., a_i)/K(a_1, ..., a_{i-1})$ é finita para todo $i = 2, ..., r$ e $K(a_1)/K$ é finita. Denote $K(a_1, ..., a_i)$ por K_i.

Então, como $[K_r : K] = [K_r : K_{r-1}]...[K_2 : K_1][K_1 : K]$, $K(a_1, ..., a_r)/K$ é finita e portanto algébrica. □

A partir de agora sempre que nos referirmos a uma extensão estaremos subentendendo extensão algébrica de corpos, salvo menção em contrário.

Teorema 1.1.6. ***(Dedekind)****Sejam K e L corpos e $\sigma_1, \sigma_2, ..., \sigma_n$ homomorfismos de K em L distintos dois a dois. Suponha que exista $\{\lambda_1, \lambda_2, ..., \lambda_n\} \subset L$ tal que $\sum_{i=1}^{n} \lambda_i \sigma_i = 0$. Então $\lambda_i = 0$, para todo $i = 1, 2, ..., n$.*

Demonstração. Usaremos indução sobre o número de homomorfismos n.

Se $n = 1$ e temos $\lambda_1 \sigma_1 = 0$, em particular $0 = \lambda_1 \sigma_1(1_K) = \lambda_1$.

Suponha agora que $n > 1$ e que o resultado seja válido para todo $1 \leq m < n$.

Agora mostraremos que não podemos ter que $\lambda_i \neq 0$ para todo $i = 1, ..., n$.

Vamos então considerar $\lambda_i \neq 0$ para todo $i \in \{1, 2, ..., n\}$. Como os homomorfismos são distintos, existe $x_0 \in K$ tal que $\sigma_1(x_0) \neq \sigma_n(x_0)$.

Por hipótese, $\sum_{i=1}^{n} \lambda_i \sigma_i = 0$. Em particular, $\sum_{i=1}^{n} \lambda_i \sigma_i(xx_0) = 0$ e $\sum_{i=1}^{n} \lambda_i \sigma_i(x) = 0$, para todo $x \in K$.

Multiplicando o segundo por $\sigma_n(x_0)$ e fazendo a diferença com o primeiro temos

$$\sum_{i=1}^{n} \lambda_i \sigma_i(xx_0) - \sigma_n(x_0) \sum_{i=1}^{n} \lambda_i \sigma_i(x) = 0 \ \forall \ x \in K$$

Assim,

$$\sum_{i=1}^{n-1} \lambda_i (\sigma_i(x_0) - \sigma_n(x_0)) \sigma_i(x) = 0 \ \forall \ x \in K$$

e logo

$$\sum_{i=1}^{n-1} \lambda_i (\sigma_i(x_0) - \sigma_n(x_0)) \sigma_i = 0$$

Pela hipótese de indução temos $\lambda_i(\sigma_i(x_0) - \sigma_n(x_0)) = 0$ para $1 \leq i \leq n-1$.

Em particular, para $i = 1$ temos $\lambda_1(\sigma_1(x_0) - \sigma_n(x_0)) = 0$. Como $\sigma_1(x_0) \neq \sigma_n(x_0)$, deve ser $\lambda_1 = 0$, o que é absurdo pois supomos $\lambda_i \neq 0$ para todo $i \in \{1, 2, ..., n\}$.

Logo não pode ocorrer o caso $\lambda_i \neq 0$ para todo $i \in \{1, 2, ..., n\}$.

Desta forma, $\lambda_j = 0$ para algum $j \in \{1, ..., n\}$ e, pela hipótese de indução, vale o resultado.

□

Teorema 1.1.7. *Sejam F e L corpos e $\{\sigma_1, \sigma_2, ..., \sigma_n\}$ homomorfismos de F em L distintos dois a dois. Seja, ainda, $K = \{a \in F | \sigma_1(a) = ... = \sigma_n(a)\}$. Então $[F : K] \geq n$.*

Demonstração. Seja $r = [F : K]$. Vamos supor por absurdo que $r < n$.

Tome $\beta = \{a_1, ..., a_r\}$ base de F sobre K e considere o sistema linear homogêneo

$$\begin{cases} \sigma_1(a_1)x_1 + \sigma_2(a_1)x_2 + ... + \sigma_n(a_1)x_n &= 0 \\ \sigma_1(a_2)x_1 + \sigma_2(a_2)x_2 + ... + \sigma_n(a_2)x_n &= 0 \\ \vdots & \vdots \\ \sigma_1(a_r)x_1 + \sigma_2(a_r)x_2 + ... + \sigma_n(a_r)x_n &= 0 \end{cases}$$

Como $r < n$ e o sistema tem r equações e n variáveis, existe solução não trivial, digamos $\{b_1, ..., b_n\} \subset L$.

Desta forma, $\sum_{j=1}^{n} b_j\sigma_j(a_i) = 0$ para todo $i = 1, ..., r$. Se $a \in F$, $a = \sum_{i=1}^{r} \lambda_i a_i$ com $\lambda_i \in K$, ou seja, $\sigma_1(\lambda_i) = \sigma_2(\lambda_i) = ... = \sigma_n(\lambda_i)$ para todo $i = 1, ..., r$.

Assim, $\sum_{j=1}^{n} b_j\sigma_j(a) = \sum_{j=1}^{n} b_j\sigma_j(\sum_{i=1}^{r} \lambda_i a_i) = \sum_{i=1}^{r} \sigma_1(\lambda_i) \sum_{j=1}^{n} b_j\sigma_j(a_i) = 0$ para todo $a \in F$.

Ou seja, $\sum_{j=1}^{n} b_j\sigma_j = 0$. Isto é absurdo pois, pelo Teorema 1.1.6, cada b_i deveria ser zero, contrariando o fato de $\{b_1, ..., b_r\}$ ser solução não trivial.

Logo $[F : K] \geq n$

□

Considere L/K extensão de corpos e G subgrupo do grupo dos K-automorfismos de L. Vamos definir $L^G = \{x \in L \mid \sigma(x) = x \ \forall \sigma \in G\}$.

Repare que esta definição é um caso particular da hipótese do Teorema 1.1.7 pois $Id_L \in G$.

Teorema 1.1.8. *Sejam L/K extensão de corpos e G subgrupo finito de $Aut_K(L)$. Então $[L : L^G] = |G|$.*

Demonstração. Suponha $G = \{\sigma_1 = Id_L, \sigma_2, ..., \sigma_n\}$ com $n = |G|$.

Temos do Teorema 1.1.7 que $[L : L^G] \geq |G|$. Vamos supor por absurdo que seja estritamente maior. Desta forma existe um conjunto $\{a_1, a_2, ..., a_n, a_{n+1}\} \subset L$

linearmente independente sobre L^G.

O sistema

$$\begin{cases} \sigma_1(a_1)x_1 + \sigma_1(a_2)x_2 + ... + \sigma_1(a_n)x_n + \sigma_1(a_{n+1})x_{n+1} &= 0 \\ \sigma_2(a_1)x_1 + \sigma_2(a_2)x_2 + ... + \sigma_2(a_n)x_n + \sigma_2(a_{n+1})x_{n+1} &= 0 \\ \vdots & \vdots \\ \sigma_n(a_1)x_1 + \sigma_n(a_2)x_2 + ... + \sigma_n(a_n)x_n + \sigma_n(a_{n+1})x_{n+1} &= 0 \end{cases}$$

tem $n+1$ variáveis e n equações. Desta forma possui uma solução $\{b_1, ..., b_{n+1}\} \subset L$ não trivial.

Dentre todas as soluções possíveis, escolha a que tem o menor número de termos não-nulos, o qual denotaremos por r. Para facilitar , vamos supor $b_1, b_2, ..., b_r$ não-nulos e $b_{r+1} = b_{r+2} = ... = b_{n+1} = 0$, reordenando o sistema se necessário. Suponha ainda $b_r = 1$, multiplicando cada termo da solução por b_r^{-1} se necessário.

Note que $\{b_1, b_2, ..., b_r\} \not\subset L^G$ pois caso o fosse, para $\sigma_1 = Id_L$, $\sum_{j=1}^{n+1} a_j b_j = 0$ e, como $\{a_1, a_2, ..., a_n, a_{n+1}\}$ é linearmente independente sobre L^G, seria todo $b_j = 0$ o que é absurdo.

Desta forma existe $1 \leq m \leq r$ tal que $b_m \notin L^G$ e logo existe $1 \leq l \leq n$ tal que $\sigma_l(b_m) \neq b_m$.

Repare ainda que $r > 1$ pois se $r = 1$ deveria ser $0 = \sigma_1(a_1)b_1 = a_1 b_1$ e logo $a_1 = 0$ o que é absurdo.

Como $\sum_{j=1}^{r} b_j \sigma_i(a_j) = 0$, então $0 = \sigma_l(\sum_{j=1}^{r} b_j \sigma_i(a_j)) = \sum_{j=1}^{r} \sigma_l(b_j)\sigma_l(\sigma_i(a_j))$ para todo $i = 1, 2, ..., n$.

Mas G é grupo, então $\sigma_l \sigma_i$ varia em todo G quando i varia de 1 a n, ou seja, $\sum_{j=1}^{r} \sigma_l(b_j)\sigma_k(a_j) = 0$ para todo $k = 1, 2, ..., n$.

Desta forma, como $b_r = 1$ e $\sigma_l(1) = 1$,

$$\sum_{j=1}^{r-1} (\sigma_l(b_j) - b_j)\sigma_i(a_j) = \sum_{j=1}^{r} \sigma_l(b_j)\sigma_i(a_j) - \sum_{j=1}^{r} b_j \sigma_i(a_j) = 0$$

para todo $i = 1, 2, ..., n$.

Defina agora $c_j = \sigma_l(b_j) - b_j$. Obtemos desta forma $c_m \neq 0$, ou seja, temos $\{c_1, ..., c_m, ..., c_{r-1}, 0, 0, ..., 0\}$ uma solução não trivial com no máximo $r-1$ elementos não nulos, o que é absurdo pois contraria a minimalidade de r.

Logo $[L : L^G] = |G|$. □

Suponhamos que $\sigma : F \longrightarrow L$ seja isomorfismo de corpos. Vamos definir por σ^* o isomorfismo de anéis entre $F[X]$ e $L[X]$ dado por $\sigma^*(\sum_{i=1}^{n} a_i X^i) = \sum_{i=1}^{n} \sigma(a_i) X^i$. Denotaremos por $\sigma^*(f)(\alpha)$ o polinômio $\sigma^*(f(X))$ aplicado a $\alpha \in L$.

Vamos dizer que um homomorfismo $\sigma : K_1 \to K_2$ pode ser prolongado a um homomorfismo $\rho : L_1 \to L_2$ se $K_1 \subset L_1$, $K_2 \subset L_2$ e $\rho|_{K_1} = \sigma$.

Teorema 1.1.9. *Sejam $\sigma : K_1 \longrightarrow K_2$ isomorfismo de corpos e L_1 e L_2 extensões de K_1 e K_2 respectivamente. Seja, ainda, $\theta \in L_1$ elemento algébrico sobre K_1 com $m_{\theta,K_1}(X) \in K_1[X]$ seu minimal. Então σ pode ser prolongado a um homomorfismo injetor $\rho : K_1(\theta) \longrightarrow L_2$ se, e somente se, $\sigma^*(m_{\theta,K_1}(X))$ tem uma raiz em L_2. Ainda, o número de prolongamentos é igual ao número de raízes distintas de $\sigma^*(m_{\theta,K_1}(X))$ em L_2.*

Demonstração.

($\Rightarrow$) Suponha $m_{\theta,K_1}(X) = \sum_{i=0}^{n} a_i X^i \in K_1[X]$. Se $\rho : K_1(\theta) \longrightarrow L_2$ é um prolongamento de σ, então $\rho(\theta)$ é raiz de $\sigma^*(m_{\theta,K_1}(X))$.

De fato, $\sigma^*(m_{\theta,K_1}(\rho(\theta))) = \sum_{i=0}^{n} \sigma(a_i)\rho(\theta)^i$.

Mas $\rho|_{K_1} = \sigma$ e $a_i \in K_1$, temos

$$\begin{aligned} \sigma^*(m_{\theta,K_1}(\rho(\theta))) &= \sum_{i=0}^{n} \sigma(a_i)\rho(\theta)^i = \sum_{i=0}^{n} \rho(a_i)\rho(\theta)^i \\ &= \rho(\sum_{i=0}^{n} a_i\theta^i) = \rho(m_{\theta,K_1}(\theta)) \\ &= \rho(0) = 0 \end{aligned}$$

Como $\rho(\theta) \in L_2$, $\sigma^*(m_{\theta,K_1}(X))$ tem uma raiz em L_2.

($\Leftarrow$) Repare que $\sigma^*(m_{\theta,K_1}(X))$ é irredutível em $K_2[X]$ pois $m_{\theta,K_1}(X)$ é irredutível em $K_1[X]$ e σ é isomorfismo de corpos. Suponha que $\lambda \in L_2$ seja raiz de $\sigma^*(m_{\theta,K_1}(X))$. Temos então que $\sigma^*(m_{\theta,K_1}(X))$ é o minimal de λ em $K_2[X]$.

Mas $K_1(\theta) = \frac{K_1[X]}{<m_{\theta,K_1}(X)>}$ e $K_2(\lambda) = \frac{K_2[X]}{<\sigma^*(m_{\theta,K_1}(X))>}$.

Podemos definir

$$\begin{array}{rccc} \tilde{\rho}: & K_1[X] & \longrightarrow & K_2(\lambda) \\ & f(X) & \longmapsto & \sigma^*(f)(\lambda) \end{array}$$

que é claramente um homomorfismo bem definido de anéis.

Vamos supor que $f(X) \in ker(\tilde{\rho})$, ou seja, $\sigma^*(f)(\lambda) = 0$. Como $\sigma^*(m_{\theta,K_1}(X))$ é o minimal de λ em K_2, temos que $\sigma^*(f(X)) = \sigma^*(m_{\theta,K_1}(X))g^*(X)$ com $g^*(X) \in K_2[X]$.

Como σ^* é isomorfismo de anéis, $g^*(X) = \sigma^*(g(X))$ para algum $g(X) \in K_1[X]$ e logo, pelo mesmo motivo, $f(X) = m_{\theta,K_1}(X)g(X)$.

Desta forma, $ker(\tilde{\rho}) \subseteq < m_{\theta,K_1}(X) >$.

Se $f(X) \in < m_{\theta,K_1}(X) >$, então $f(X) = m_{\theta,K_1}(X)g(X)$ e consequentemente temos que $\sigma^*(f(X)) = \sigma^*(m_{\theta,K_1}(X)g(X))$. Por conseguinte, $\sigma^*(f)(\lambda) = 0$, obtendo-se assim que $ker(\tilde{\rho}) \supseteq < m_{\theta,K_1}(X) >$.

Concluímos então que $ker(\tilde{\rho}) = < m_{\theta,K_1}(X) >$.

Pelo Teorema do Isomorfismo, existe um isomorfismo ρ entre $K_1(\theta) = \frac{K_1[X]}{<m_{\theta,K_1}(X)>}$ e $K_2(\lambda) \subset L_2$. Este isomorfismo claramente prolonga σ.

A última parte é imediata. □

A partir de agora, sempre que falarmos que um polinômio $p(X)$ se decompõe sobre $L[X]$, com L corpo, entenderemos que a decomposição é em fatores lineares,

ou seja, $p(X)$ tem todas as suas raízes em L.

Sejam K um corpo e $p(X) \in K[X]$. Dizemos que um corpo L é corpo de decomposição ou de raízes de $p(X)$ se existirem $\alpha_1, ..., \alpha_n$ em L tais que $L = K(\alpha_1, ..., \alpha_n)$ e $p(X) = \prod_{i=1}^{n} (X - \alpha_i)^{r_i}$ em $L[X]$, com $r_i \neq 0$ para todo $i = 1, ..., n$.

Para assegurar a existência de um corpo de raízes de $p(X) \in K[X]$, é suficiente que se mostre a existência de um corpo que estenda K e contenha uma raiz de $p(X)$, pois $p(X)$ tem grau finito. Suponha $p(X)$ irredutível (caso $p(X)$ seja redutível, faça a construção para um de seus fatores irredutíveis) e considere $\frac{K[X]}{<p(X)>}$ que é um corpo. Podemos fazer $K \subset \frac{K[X]}{<p(X)>}$ identificando $a \in K$ com $a+ < p(X) > \in \frac{K[X]}{<p(X)>}$. Veja que $X+ < p(X) >$ é raiz de $p(X)$. Neste corpo $p(X)$ pode ser reduzido a um polinômio de grau menor e assim repetir o processo finitas vezes.

Definição 1.1.10. *Um polinômio $p(x)$ é dito separável sobre um corpo K se todos os seus fatores irredutíveis em $K[X]$ só tiverem raízes simples em qualquer corpo de raízes.*

Teorema 1.1.11. *Sejam $\sigma : K_1 \longrightarrow K_2$ isomorfismo de corpos, $f(X) \in K_1[X]$ não-constante, L_1 corpo de raízes de $f(X)$ sobre K_1, L_2 corpo de raízes de $\sigma^*(f(X))$ sobre K_2. Então valem:*

(i) Existe um isomorfismo $\rho : L_1 \longrightarrow L_2$ que prolonga σ.

(ii) Se $f(X)$ for um polinômio separável, então existem exatamente $[L_1 : K_1]$ isomorfismos de L_1 em L_2 que prolongam σ

Demonstração. Em ambos os casos usaremos indução sobre $[L_1 : K_1]$.

(*i*) De fato, se $[L_1 : K_1] = 1$, então $f(X)$ se decompõe em $K_1[X] = L_1[X]$, ou seja, $f(X) = a_r \prod_{i=1}^{r} (X - \theta_i)$ com $\theta_i \in K_1$. Assim, $\sigma^*(f(X)) = \sigma(a_r) \prod_{i=1}^{r} (X - \sigma(\theta_i))$ com $\sigma(\theta_i) \in K_2$. Ora, $\sigma^*(f(X))$ se decompõe em K_2 e então $K_2 = L_2$.

Suponha agora que $[L_1 : K_1] = n > 1$ e que o resultado seja válido para todo $m \in \mathbb{N}$ tal que $1 \leq m < n$.

Desta forma, $f(X)$ não se decompõe em K_1, ou seja, existe $q(X)$ fator irredutível de $f(X)$ com $deg(q(X)) > 1$. Considere θ raiz de $q(X)$ em L_1. Note que $\theta \notin K_1$ pois teríamos $q(X)$ redutível.

Temos, pelo Teorema 1.1.9, que σ pode ser prolongado a um homomorfismo injetor $\rho' : K_1(\theta) \longrightarrow L_2$. Podemos restringir a imagem de ρ' para o corpo $\rho'(K_1(\theta)) \subset L_2$ e assim considerar $\rho' : K_1(\theta) \longrightarrow \rho'(K_1(\theta))$ isomorfismo.

Ora, L_1 é corpo de raízes de $f(X)$ sobre $K_1(\theta)$ e L_2 é corpo de raízes de $\sigma^*(f(X))$ sobre $\rho'(K_1(\theta))$.

Mas $n = [L_1 : K_1] = [L_1 : K_1(\theta)][K_1(\theta) : K_1]$ e $[K_1(\theta) : K_1] > 1$ pois $\theta \notin K_1$. Logo $n > [L_1 : K_1(\theta)]$. Pela hipótese de indução, existe $\rho : L_1 \longrightarrow L_2$ isomorfismo que prolonga ρ' e logo σ.

(ii) Se $[L_1 : K_1] = 1$, então $f(X)$ se decompõe em $K_1[X]$ e logo $\sigma^*(f(X))$ se decompõe em $K_2[X]$, ou seja, $L_1 = K_1$ e $L_2 = K_2$, valendo o resultado.

Seja, agora, $[L_1 : K_1] = n > 1$ e que o resultado seja válido para todo $m \in \mathbb{N}$ tal que $1 \leq m < n$.

Tome $p(X)$ fator irredutível de $f(X)$ com $deg(p(X)) = d > 1$ pois $f(X)$ não se decompõe em K_1.

Desta forma, como $f(X)$ é separável, $p(X)$ tem exatamente d raízes distintas em L_1, digamos $\alpha_1, ..., \alpha_d$. Sejam $\beta_1, ..., \beta_d$ raízes de $\sigma^*(p(X))$ em L_2 (note que também são distintas). Ora, existem d isomorfismos $\sigma_i : K_1(\alpha_1) \longrightarrow K_2(\beta_i)$ com $\sigma_i(\alpha_1) = \beta_i$ e que prolongam σ.

Encare L_1 e L_2 como corpos de raízes sobre $K_1(\alpha_1)$ e, $\forall i$, $K_2(\beta_i)$ respectivamente.

Logo $l = [L_1 : K_1(\alpha_1)] = \frac{[L_1:K_1]}{[K_1(\alpha_1):K_1]} = \frac{[L_1:K_1]}{d} < [L_1 : K_1] = n$.

Pela hipótese de indução, existem exatamente $l = \frac{[L_1:K_1]}{d}$ isomorfismos que prolongam σ_i para cada i. Como os σ_i são distintos, temos $d\frac{[L_1:K_1]}{d} = [L_1 : K_1]$ isomorfismos de L_1 em L_2 que prolongam σ.

□

Desta forma temos o seguinte corolário:

Corolário 1.1.12. *Quaisquer dois corpos de raízes de um mesmo polinômio sobre um corpo K são isomorfos.*

Demonstração. Basta tomar $K_1 = K = K_2$ no Teorema 1.1.11. □

Teorema 1.1.13. *Sejam K um corpo, $f(X) \in K[X]$ um polinômio não-constante e F corpo de raízes de $f(X)$. Então se $g(X)$ é um polinômio irredutível em $K[X]$ e $g(X)$ tem uma raiz em F, então $g(X)$ se decompõe em $F[X]$.*

Demonstração. Sendo F corpo de raízes de $f(X)$ sobre K, então $F = K(\alpha_1, ..., \alpha_m)$, onde $\alpha_1, ..., \alpha_m$ são todas as raízes de $f(X)$ em F.

Considere $\beta \in F$ raiz de $g(X)$. Como $g(X) \in K[X] \subset F[X]$, tome L corpo de raízes de $g(X)$ sobre F.

Temos $L = F(\beta_1, ..., \beta_n)$ com $\beta_1, ..., \beta_n$ todas as raízes de $g(X)$ em L. Seja $\beta' \in L$ tal que $\beta' \neq \beta$ e $g(\beta') = 0$. Assim existe um K-isomorfismo τ de $K(\beta)$ em $K(\beta')$, com $\tau(\beta) = \beta'$, por uma simples aplicação do Teorema 1.1.9.

Ora, podemos olhar F como corpo de raízes de $f(X)$ sobre $K(\beta)$ pois $\beta \in F$ e $F(\beta')$ como corpo de raízes de $f(X)$ sobre $K(\beta')$.

Além disso, $\tau^*(f(X)) = f(X)$. Pelo Teorema 1.1.11 existe um isomorfismo ρ de F em $F(\beta')$ que prolonga τ. Note ainda que $\rho(\alpha_i)$ são raízes de $f(X)$, logo $\rho(\alpha_i) \in F$ para todo $i = 1, 2, ..., m$.

Mas $\rho(\beta) = \tau(\beta) = \beta'$. Ainda, $\beta \in F = K(\alpha_1, ..., \alpha_m)$, então existe um polinômio $h(X_1, ..., X_m) \in K[X_1, ..., X_m]$ tal que $h(\alpha_1, ..., \alpha_m) = \beta$.

Logo, $\beta' = \rho(\beta) = (\rho^* h)(\rho(\alpha_1), ..., \rho(\alpha_m)) = h(\rho(\alpha_1), ..., \rho(\alpha_m)) \in F$.

Assim $g(X)$ se decompõe em F.

□

Definição 1.1.14. *Uma extensão L/K é dita normal se todo polinômio irredutível em K que tem uma raiz em L se decompõe em L.*

Proposição 1.1.15. *Uma extensão L/K é normal e finita se, e somente se, L é corpo de raízes de algum polinômio em $K[X]$.*

Demonstração.

($\Rightarrow$) Como L/K é finita, $L = K(\alpha_1, ..., \alpha_n)$. Tome $p(X) = \prod_{i=1}^{n} m_{\alpha_i,K}(X)$, com $m_{\alpha_i,K}(X)$ o minimal de α_i em $K[X]$ para todo $i = 1, ..., n$. Claramente L é corpo de raízes de $p(X)$.

($\Leftarrow$) Imediato do Teorema 1.1.13. □

Definição 1.1.16. *Sejam L/K uma extensão e $a \in L$. Dizemos que a é separável sobre K se a é raiz simples de seu minimal em $K[X]$. A extensão L/K é dita separável se todo elemento de L for separável sobre K.*

Observe que toda extensão de um corpo K de característica 0 é separável pois, se $a \in L$, caso $m_{a,K}(X)$ tenha a como raiz múltipla, a derivada usual de $m_{a,K}(X)$ será tal que $m'_{a,K}(a) = 0$, contrariando o fato de $m_{a,K}(X)$ ser o minimal.

Definição 1.1.17. *Sejam L/K uma extensão e $a \in L$. Dizemos que a é puramente inseparável sobre K se o minimal de a tiver a forma $(X - a)^m$ para algum $m \in \mathbb{N}$. A extensão L/K é dita puramente inseparável se for finita e todo elemento de L for puramente inseparável sobre K.*

Usaremos $c(K)$ para indicar a característica de um corpo K.

Teorema 1.1.18. *Sejam K um corpo com $c(K) = p$, L/K uma extensão finita e $a \in L$ puramente inseparável sobre K. Se $m_{a,K}(X)$ é o minimal de a em K, então existe $r \geq 0$ tal que o grau de $m_{a,K}(X)$ é p^r. Ainda, $a^{p^r} \in K$ mas $a^{p^s} \notin K$ para todo $0 \leq s < r$.*

Demonstração. Suponha que $deg(m_{a,K}(X)) = np^r$ tal que p não divide n.

Temos $m_{a,K}(X) = (X - a)^{np^r} = (X^{p^r} - a^{p^r})^n$.

Assim, $(-1)^{n-1}na^{p^r}$ é o coeficiente do termo $(X^{p^r})^{n-1}$ de $m_{a,K}(X) \in K[X]$.

Ora, $na^{p^r} \in K$. Desde que p não divide n, temos que $a^{p^r} \in K$.

Como $m_{a,K}(X)$ é irredutível, devemos ter $n = 1$. Logo $deg(m_{a,K}(X)) = p^r$.

Mais ainda, se para algum s tal que $0 \leq s < r$ tivéssemos $a^{p^s} \in K$, o polinômio $f(X) = X^{p^s} - a^{p^s}$ estaria em $K[X]$, anularia a e teria grau menor do que o minimal, o que é absurdo. □

Corolário 1.1.19. *Se $c(K) = p$ e L/K é uma extensão finita e puramente inseparável, então $[L : K] = p^r$ para algum $r \geq 0$.*

Demonstração. Temos que $L = K(a_1, ..., a_n)$. Note que a_i é puramente inseparável sobre $K(a_1, ..., a_{i-1}) = K_{i-1}$ para todo $i = 1, ..., n$. Assim, pelo Teorema 1.1.18, $[K_i : K_{i-1}] = p^{r_i}$. O resultado se segue imediato. □

Teorema 1.1.20. *Sejam K um corpo com $c(K) = p$, $K^p = \{a^p \mid a \in K\}$ e $a \in K \backslash K^p$. Então, para todo inteiro não-negativo n, temos que $f(X) = X^{p^n} - a$ é irredutível em $K[X]$.*

Demonstração. Seja $g(X)$ um fator mônico, não constante e irredutível em $K[X]$ de $f(X)$. Considere $L = K(b)$ tal que $g(b) = 0$. Desta forma temos $f(b) = 0$, sendo assim $a = b^{p^n}$. Logo $f(X) = (X - b)^{p^n} \in L[X]$.

Se $q(X)$ é outro fator irredutível, mônico e não constante de $f(X)$ em $K[X]$, então, em $L[X]$, $g(X)$ é uma potência de $(X-b)$. Temos assim $q(b)=0$.

Mas pela nossa construção, $g(X)$ é minimal de b em $K[X]$, logo $g(X)$ divide $q(X)$. Como $q(X)$ é irredutível e mônico, $g(X)=q(X)$.

Assim, $f(X)=g(X)^m$. Mas $deg(f(X))=p^n$, logo $deg(g(X))=p^s$ e $m=p^r$, com $r+s=n$.

Resta-nos mostrar que $m=1$.

Seja c o termo constante de $g(X)$. Então $a=(c)^{p^r}\in K^{p^r}$.

Note que se $r\neq 0$, $a=(c)^{p^r}=(c^{p^{r-1}})^p$ com $c\in K$. Logo $a\in K^p$, o que é absurdo.

Logo $r=0$. Temos então $m=1$ e $f(X)=g(X)$ irredutível em $K[X]$. □

Corolário 1.1.21. *Sejam K um corpo com $c(K)=p$, L/K uma extensão de corpos e $a\in L$. Se existe $n\geq 0$ tal que $a^{p^n}\in K$, então a é puramente inseparável sobre K.*

Demonstração. Suponha que n seja o menor inteiro não negativo com essa propriedade. Caso $n=0$ nada se tem a fazer.

Se $n>0$, caso $a^{p^n}\in K^p$, temos $a^{p^n}=b^p$ para algum $b\in K$. Logo $a^{p^{n-1}}=b\in K$, contrariando o fato de n ser o menor inteiro não negativo com essa propriedade.

Logo $a^{p^n}\notin K^p$. Pelo teorema acima temos que $X^{p^n}-a^{p^n}=(X-a)^{p^n}$ é irredutível, logo mínimo de $a\in L$.

Temos então que a é puramente inseparável sobre K. □

Corolário 1.1.22. *Seja K um corpo de característica p. Se a é puramente inseparável sobre K e a é separável sobre K, então $a\in K$.*

Demonstração. Seja n o menor inteiro tal que $a^{p^n} \in K$. Veja que $a^{p^n} \notin K^p$. Logo, $X^{p^n} - a^{p^n} = (X-a)^{p^n}$ é irredutível, ou seja, é mínimo de a em $K[X]$. Como a é separável, $p^n = 1$. Logo $a \in K$. □

Teorema 1.1.23. *Se L/K é separável e $c(K) = p$, então $KL^p = L$. Reciprocamente, se L/K é finita e $KL^p = L$, então L/K é separável.*

Demonstração. Suponhamos primeiramente que L/K seja separável. Note que $L^p \subseteq KL^p$. Assim, se $a \in L$, então $a^p \in L^p \subseteq KL^p$. Logo a é puramente inseparável sobre KL^p.

Temos então que L/KL^p é puramente inseparável, por outro lado, como L/K é separável e $K \subseteq KL^p \subseteq L$, temos que L/KL^p é separável. Desta forma temos $L = KL^p$.

Reciprocamente, suponhamos que L/K é finita e $KL^p = L$. Tome $a \in L$ e considere $m_{a,K}(X)$ o minimal de a em $K[X]$. Suponhamos por absurdo que a não é separável sobre K. Temos então o polinômio $m'_{a,K}(X)$ derivado de $m_{a,K}(X)$ tal que $m'_{a,K}(a) = 0$. Desta forma $m_{a,K}(X)$ divide $m'_{a,K}(X)$. Como o grau do polinômio derivado é estritamente menor do que o grau de $m_{a,K}(X)$, temos que $m'_{a,K}(X) = 0$.

Assim, se bX^n é um dos termos de $m_{a,K}(X)$, então nbX^{n-1} é um dos termos de $m'_{a,K}(X) = 0$. Logo $b = 0$ ou p divide n.

Decorre que $m_{a,K}(X) = \sum_{t=0}^{l} a_t X^{pt}$, com $a_t \in K$ para todo $t = 1, ..., l$.

Suponhamos sem perda de generalidade que $a_l \neq 0$ (logo $a_l = 1$). Como $m_{a,K}(a) = 0$, temos $\sum_{t=0}^{l} a_t a^{pt} = 0$ e $a_l \neq 0$. Ou seja, o conjunto $\{1, a^p, ..., a^{pl}\}$ é um conjunto linearmente dependente sobre K.

Entretanto, o conjunto $\{1, a, ..., a^l\}$ é linearmente independente sobre K pois, caso fosse linearmente dependente, existiriam $b_0, ..., b_l$ em K, não simultaneamente nulos, tais que $\sum_{i=0}^{l} b_i a^i = 0$. Assim o polinômio $q(X) = \sum_{i=0}^{l} b_i X^i \in K[X]$ seria tal

que $q(a) = 0$ e $deg(q(X)) = l < lp = deg(m_{a,K}(X))$, o que é absurdo.

Complete o conjunto $\{1, a, ..., a^l\}$ a uma base de L/K, a qual chamaremos de $\{b_0, ..., b_l, ..., b_{l+s}\}$, com $b_i = a^i$ para $i = 0, ..., l$. Repare que assim estamos supondo que $dim_K(L) = l + s + 1$.

Assim, se $c \in L$, $c = \sum_{i=0}^{l+s} c_i b_i$. Então, $c^p = \sum_{i=0}^{l+s} c_i^p b_i^p$.

Desta forma, temos que $\{b_0^p, ..., b_{l+s}^p\}$ gera L^p sobre K^p.

Mas por hipótese $L = KL^p$ e, como visto acima, $KL^p = K(\sum_{i=0}^{l+s} Kb_i^p) = \sum_{i=0}^{l+s} Kb_i^p$.

Ora, $L = \sum_{i=0}^{l+s} Kb_i^p$, ou seja, $\{b_0^p, ..., b_{l+s}^p\}$ gera L sobre K. Este conjunto tem $l + s + 1$ geradores em um espaço de dimensão $l + s + 1$, logo deve ser uma base de L sobre K e, assim, linearmente independente.

Em particular $\{b_0^p, b_1^p, ..., b_l^p\}$ é um conjunto linearmente independente sobre K. Mas este conjunto é exatamente o conjunto $\{1, a^p, ..., a^{pl}\}$, o qual sabíamos ser linearmente dependente sobre K. Temos então um absurdo, proveniente do fato de supormos que a não fosse separável sobre K.

Logo L/K é separável. □

Corolário 1.1.24. *Se K é um corpo com $c(K) = p$ e a é separável sobre K, então $K(a) = K(a^p)$ e $K(a)$ é separável sobre K. Por outro lado, se $K(a) = K(a^p)$, então a é separável sobre K.*

Demonstração. Suponha primeiramente que a seja separável sobre K. Então a é separável sobre $K(a^p)$.

Mas a é puramente inseparável sobre $K(a^p)$ pois $a^p \in K(a^p)$.

Logo $a \in K(a^p)$. Ou seja, $K(a) \subseteq K(a^p)$. A inclusão contrária é imediata.

Por outro lado, se $K(a) = K(a^p)$ temos $K[K(a)^p] = KK^p(a^p) = K(a^p) = K(a)$. Logo, pelo Teorema 1.1.23, $K(a)$ é separável sobre K. □

Corolário 1.1.25. *Se L/F e F/K são extensões finitas separáveis, então L/K é uma extensão finita separável.*

Demonstração. Se $c(K) = p$, $KF^p = F$ e $FL^p = L$, então $L = KF^pL^p \subseteq KL^p$. Trivialmente temos $KL^p \subseteq L$.

Logo $L = KL^p$, ou seja, L/K é separável.

Se $c(K) = 0$, então é imediato que L/K é separável, pois toda extensão finita de um corpo de característica 0 é separável. □

Corolário 1.1.26. *Se $a_1, ..., a_n$ são separáveis sobre K, então $K(a_1, ..., a_n)$ é separável sobre K.*

Demonstração. Seja $K_0 = K$ e $K_i = K_{i-1}(a_i)$

Note que a_i é separável sobre K_{i-1} para todo $i = 1, ..., n$.

O caso $n = 1$ já foi demonstrado no Corolário 1.1.24. Seja $n > 1$ e suponha o resultado válido para $n - 1$.

Ora, a_n é separável sobre K_{n-1}, logo K_n é separável sobre K_{n-1}. Mas, pela hipótese de indução, K_{n-1} é separável sobre K. Logo $K_n = K(a_1, ..., a_n)$ é separável sobre K. □

Teorema 1.1.27. *Sejam L/K extensão finita e $G = Aut_K(L)$. As seguintes afirmações são equivalentes:*

(i) $[L : K] = |G|$

(ii) $L^G = K$

(iii) *L é corpo de decomposição de algum $f(X) \in K[X]$ separável.*

(iv) *L/K é normal e separável.*

Demonstração. Inicialmente observe que L/K finito implica G finito.

$(i) \Rightarrow (ii)$ Do Teorema 1.1.8 $[L : L^G] = |G|$ e, por hipótese, $|G| = [L : K]$. Logo $[L : L^G][L^G : K] = [L : K] = |G| = [L : L^G]$. Ora, $[L^G : K] = 1$ e assim $L^G = K$.

$(ii) \Rightarrow (i)$ Direto do Teorema 1.1.8.

$(iii) \Rightarrow (iv)$ Se $\{a_1, ..., a_n\}$ são as raízes de f, então $L = L(a_1, .., a_n)$ e, como $f(X)$ é separável, cada fator irredutível de $f(X)$ em $K[X]$ só tem raízes simples. Assim cada a_i é separável sobre L pois é raiz de algum destes polinômios. Logo L/K é separável pelo Corolário 1.1.26.

Ainda, desde que L é corpo de decomposição de um polinômio em $K[X]$, L/K é normal pela Proposição 1.1.15.

$(iv) \Rightarrow (iii)$ Temos L/K finita, digamos $L = K(a_1, ...a_n)$. Sendo $m_{a_i,K}(X)$ minimal de a_i em $K[X]$, escolha $f(X) = \prod_{i=1}^{n} m_{a_i,K}(X)$. Como L/K é normal, $f(X)$ se decompõe em L e logo, como L/K é separável cada $m_{a_i,K}(X)$ só tem raízes simples, ou seja, $f(X)$ é separável. Claramente L é corpo de raízes de $f(X)$.

$(iii) \Rightarrow (i)$ Imediato do Teorema 1.1.11 item (ii)

$(ii) \Rightarrow (iv)$ Seja $\alpha \in L$. Se $\alpha \in K$, então é claro que α é separável sobre K. Assim, só nos é interessante o caso $\alpha \notin K$.

Seja $m_{\alpha,K}(X)$ o minimal de α em $K[X]$. Temos $\sigma^*(m_{\alpha,K}(X)) = m_{\alpha,K}(X)$ para qualquer $\sigma \in G$. Logo, $m_{\alpha,K}(\sigma(\alpha)) = \sigma^*(m_{\alpha,K}(\alpha)) = 0$. Ou seja, como $m_{\alpha,K}(X)$ tem finitas raízes, o conjunto $\{\sigma(\alpha)|\sigma \in G\}$ é finito.

Sendo assim, considere $\alpha_1, ..., \alpha_r$ todos os elementos, dois a dois distintos, do conjunto $\{\sigma(\alpha)|\sigma \in G\}$. Defina $f(X) = \prod_{i=1}^{r} (X - \alpha_i)$.

Veja que, se $\sigma \in G$, $\sigma(\alpha_i) = \sigma(\alpha_j) \Leftrightarrow \alpha_i = \alpha_j \Leftrightarrow i = j$. Ainda, $\sigma(\alpha_i) = \alpha_j$ para algum $1 \leq j \leq r$.

Logo $\sigma^*(f(X)) = \prod_{i=1}^{r}(X - \sigma(\alpha_i)) = \prod_{i=1}^{r}(X - \alpha_i) = f(X)$, ou seja, os coeficientes de $f(X)$ são fixos por G e estão em L. Assim $f(X) \in L^G[X] = K[X]$.

Considere $g(X)$ um fator irredutível de $f(X)$ em $K[X]$ e suponha α_k raiz de $g(X)$. Para facilitar escreveremos $\alpha_i = \sigma_i(\alpha)$ para todo $i \in \{1, ..., r\}$.

Logo, $g(\alpha_i) = g(\sigma_i(\alpha)) = g(\sigma_i\sigma_k^{-1}(\alpha_k))$.

Como $g(X) \in K[X]$, temos $g(\sigma_i\sigma_k^{-1}(\alpha_k)) = (\sigma_i\sigma_k^{-1})^*(g(\alpha_k)) = 0$. Desta forma toda raiz de $f(X)$ é raiz de $g(X)$, ou seja, $g(X) = f(X)$. Logo $f(X)$ é irredutível, ou seja, $f(X)$ é o minimal de todo $\sigma_i(\alpha)$, em particular de α, quando tomamos $\sigma_1 = Id_L$.

Como $f(X)$ só tem raízes simples, α é separável sobre K. Desta forma mostramos que L é extensão separável de K. Ainda, qualquer polinômio irredutível em $K[X]$ que tiver uma raiz em L precisa ter todas as raízes em L, pois mostramos que este polinômio precisa ter a forma $\prod_{i=1}^{s}(X - a_i)$ com $a_i \in L$.

Logo a extensão é normal e separável.

□

Definição 1.1.28. *Uma extensão L/K finita é de Galois se é normal e separável.*

Proposição 1.1.29. *Considere L/K extensão finita e H subgrupo de $Aut_K(L)$. Nestas condições $H = Aut_{L^H}(L)$.*

Demonstração. Claramente $H \subseteq Aut_{L^H}(L)$.

Sejam $\sigma \in Aut_{L^H}(L)$ e $H' = H \cup \{\sigma\}$.

Ora, $L^H = L^{H'}$ pois $L^H \supseteq L^{H'}$ e se $\alpha \in L^H$ temos que $\tau(\alpha) = \alpha \ \forall \tau \in H$ e $\sigma(\alpha) = \alpha$. Logo $\omega(\alpha) = \alpha$ para todo $\omega \in H'$. Então $\alpha \in L^{H'}$ e assim $L^H = L^{H'}$.

Logo, pelo Teorema 1.1.8, $|H| = [L : L^H] = [L : L^{H'}] = |H'|$ e como $H \subseteq H'$, temos $H = H'$ e assim $\sigma \in H$, valendo $H \supseteq Aut_{L^H}(L)$. Logo $H = Aut_{L^H}(L)$. □

Veja que na proposição anterior bastaria que H fosse subgrupo finito, sem exigir que L/K fosse finita.

Teorema 1.1.30. *Considere L/K uma extensão de Galois. Seja L' corpo tal que $K \subseteq L' \subseteq L$. Então L/L' é extensão de Galois.*

Demonstração. Trivialmente L/L' é separável. Ainda, L/L' é normal pois L é corpo de raízes de algum $f(X) \in K[X] \subset L'[X]$. □

Teorema 1.1.31. ***(Teorema Fundamental da Teoria de Galois)*** *Sejam L/K extensão de Galois finita e $G = Aut_K(L)$. Então existe uma bijeção entre os subgrupos de G e os subcorpos de L que contém K dada por:*

$$\begin{array}{ccc} \{H \mid H \text{ é subgrupo de } G\} & \longleftrightarrow & \{F \mid K \subset F \subset L\} \\ H & \xrightarrow{\varphi} & L^H \\ Aut_F(L) & \xleftarrow{\psi} & F \end{array}$$

Demonstração.

(i) φ é injetiva:

De fato, se $L^H = L^{H'}$, então $H = Aut_{L^H}(L) = Aut_{L^{H'}}(L) = H'$.

(ii) φ é sobrejetiva:

Ora, só precisamos mostrar que $\varphi \circ \psi = Id$.

Considere $F \subset L$ corpo que contém K.

Temos $\varphi \circ \psi(F) = \varphi(Aut_F(L)) = L^{Aut_F(L)}$.

Mas L/F é Galois pois L/K o é. Logo, pelo Teorema 1.1.27, $L^{Aut_F(L)} = F$.

□

Definição 1.1.32. *Se L/K é uma extensão, definiremos a parte separável de L como $L_{sep} = \{\alpha \in L \mid \alpha$ é separável sobre $K\}$.*

Note que $K \subseteq L_{sep}$ e, se a e b são elementos de L_{sep}, então $K(a,b)$ é uma extensão separável de K. Assim, $a+b$, ab e a^{-1} são separáveis sobre K. Então L_{sep} é um corpo e estende K.

Teorema 1.1.33. *Seja L/K extensão algébrica. Então L/L_{sep} é puramente inseparável.*

Demonstração. De fato, se a característica de K é zero, temos $L = L_{sep}$ e nada temos a fazer.

Suponha que a característica de K é um p primo. Se $\alpha \in L \backslash L_{sep}$, então α não é raiz simples de seu minimal $q(X)$, ou seja, $q(X) = (X-\alpha)^s q(X)$ em $L[X]$ com $s > 1$. Assim $q'(\alpha) = 0$ e como $gr(q'(X)) < gr(q(X))$ devemos ter $q'(X) = 0$. Temos então $q(X) \in K[X^p]$. Podemos dizer $q(X) = q_1(X^p)$. Note que $q_1(X)$ é irredutível em $K[X]$ pois caso não o fosse, teríamos $q_1(X) = q(X)r(X)$ ($q(X)$ e $r(X) \in K[X]$) e logo $q(X) = q(X^p)r(X^p) = q_1(X)r_1(X^p)$, contrariando o fato de $q(X)$ ser irredutível em $K[X]$. Repare ainda que $q_1(X)$ é o minimal de α^p.

Agora, ou α^p é separável sobre K ou $q_1(X) = q_2(X^p)$ e $q_2(X)$ será o minimal de α^{p^2}. Vamos supor o segundo caso.

Desde que o minimal tem finitas raízes, continuando o processo acima obteremos e inteiro não negativo tal que $q(X) = q_e(X^{p^e})$, com $q_e(X)$ o minimal de α^{p^e} e $q_e(X) \notin K[X^p]$, ou seja, α^{p^e} é separável sobre K e assim $\alpha^{p^e} \in L_{sep}$.

Assim, α é puramente inseparável sobre L_{sep} e sendo assim L/L_{sep} é puramente inseparável. □

1.2 O Traço

Nesta seção, bem como na Seção 1.4, trataremos de elementos que nos ajudarão a dar uma interessante estrutura ao K-espaço vetorial L quando L/K é uma extensão separável finita de corpos e tivermos certas condições estabelecidas futuramente.

Definição 1.2.1. *Seja L/K uma extensão finita. Definimos $[L:K]_s = [L_{sep}:K]$ e $[L:K]_i = [L:L_{sep}]$.*

Note que $[L:K] = [L:K]_i[L:K]_s$.

Teorema 1.2.2. *Sejam L/K finita, N/K normal finita tal que $K \subseteq L \subseteq N$ e $n_0 = [L:K]_s$. Então existem exatamente n_0 K-isomorfismos de L em subcorpos de N (ou seja, n_0 K-imersões de L em N).*

A demonstração deste resultado se encontra em [8], página 18.

Definição 1.2.3. *Dada uma extensão finita L/K, vamos chamar de fecho normal de L/K a menor extensão normal (a menos de isomorfismo) de K que contém L.*

Note que se $L = K(a_1, ..., a_n)$, N é exatamente o corpo de raízes do polinômio $f(X) = \prod_{i=1}^{n}(m_{a_i,K}(X))$, onde $m_{a_i,K}(X)$ é o polinômio minimal de a_i sobre K para todo $i = 1, ..., n$. Mais ainda, se L/K for separável, então cada $m_{a_i,K}(X)$ é um polinômio separável. Ora, N é corpo de decomposição de um polinômio separável. Logo N/K é extensão de Galois.

Definição 1.2.4. *Sejam L/K extensão finita e N o fecho normal de L/K. Considere $S = \{s : L \longrightarrow N | s \text{ é } K\text{-imersão }\}$. Defina*

$$\begin{aligned} tr_{L/K}: \ L &\longrightarrow N \\ x &\longrightarrow [L:K]_i \sum_{s\in S} s(x) \end{aligned}$$

$tr_{L/K}(x)$ é dito traço de x.

Proposição 1.2.5. *Sejam L/K extensão finita, $a \in L$ e N/K normal finita tal que $K \subseteq K(a) \subseteq N$. Sejam $S = \{\sigma_1, \ldots, \sigma_r\}$ as $r = [K(a) : K]_s$ K-imersões de $K(a)$ em N. Seja $m_{a,K}(X) \in K[X]$ o polinômio minimal de a. Então $\sigma_1(a), \ldots, \sigma_r(a)$ são todas as raízes de $m_{a,K}(X)$, cada uma com multiplicidade $[K(a) : K]_i$.*

Demonstração. Suponha $m_{a,K}(X) = X^n + c_{n-1}X^{n-1} + \ldots + c_0$. Logo, se $\sigma \in S$

$$m_{a,K}(\sigma(a)) = \sigma(a)^n + c_{n-1}\sigma(a)^{n-1} \ldots + c_0$$

E como σ é K-imersão

$$m_{a,K}(\sigma(a)) = \sigma(a^n + c_{n-1}a^{n-1} \ldots + c_0) = \sigma(0) = 0$$

Logo $\sigma(a)$ é raiz de $m_{a,K}(X)$ $\forall \sigma \in S$.

Agora, seja b raiz de $m_{a,K}(X)$. Então existe um K-isomorfismo

$$\rho : K(a) \longrightarrow K(b)$$

tal que $\rho(a) = b$. Podemos ver ρ como K-imersão de $K(a)$ em N, visto que $K(b)$ é subcorpo de N.

Como $\rho \in S$, temos $\rho = \sigma_j$ para algum $j \in \{1, ..., r\}$. Assim $b = \sigma_j(a)$. Logo $\sigma_1(a), \ldots, \sigma_r(a)$ são todas as raízes de $m_{a,K}(X)$.

Desta forma

$$m_{a,K}(X) = \prod_{i=1}^{r} (X - \sigma_i(a))^{m_i}$$

Suponhamos sem perda de generalidade que σ_1 é a K-imersão trivial de $K(a)$ em N, ou seja, $\sigma_1(a) = a$.

Ora,existe um K-isomorfismo $\tilde{\sigma} : K(a) \longrightarrow K(\sigma_j(a))$ com $\tilde{\sigma}(a) = \sigma_j(a)$ para algum $1 \leq j \leq r$ fixo. Como N é normal, e logo é corpo de raizes de algum polinomio $p(X) \in K[X]$, e $\tilde{\sigma}^*(p(X)) = p(X)$, N é corpo de raízes tanto de $p(X) \in K(a)[X]$

quanto de $p(X) \in K(\sigma_j(a))[X]$. Pelo teorema 1.1.11, $\tilde{\sigma}$ pode ser estendido a um K-automorfismo de N, digamos $\tau : N \longrightarrow N$.

Claramente temos $\tau^*(m_{a,K}(X)) = m_{a,K}(X)$ e, assim,

$$\tau^*(m_{a,K}(X)) = \prod_{i=1}^{r} (X - \tau(\sigma_i(a)))^{m_i}$$

E, como $\tau(\sigma_1(a)) = \sigma_j(a)$, pela fatoração única do polinômio, $m_1 = m_j$. Como j é qualquer, $m = m_1 = m_2 = ... = m_r$.

Assim,

$$m_{a,K}(X) = \prod_{i=1}^{r} (X - \sigma_i(a))^{m}$$

Logo,

$$mr = gr(m_{a,K}(X)) = [K(a) : K] = [K(a) : K]_i[K(a) : K]_S = r[K(a) : K]_i$$

Então $m = [K(a) : K]_i$ e

$$m_{a,K}(X) = \prod_{i=1}^{r} (X - \sigma_i(a))^{[K(a):K]_i}$$

ficando assim demostrado o resultado. □

Observação 1.2.6. *Repare que se L/K é uma extensão finita, $a \in L$ e o polinômio minimal de a é dado por $m_{a,K}(X) = X^n + c_{n-1}X^{n-1} + \ldots + c_1X^1 + c_0$, temos que $c_{n-1} = -[K(a) : K]_i \sum_{i=1}^{r} \sigma_i(a)$. Logo:*

$$tr_{K(a)/K}(a) = [K(a) : K]_i \sum_{i=1}^{r} \sigma_i(a) \in K$$

Proposição 1.2.7. *Sejam L/K uma extensão finita e $a \in L$. Então temos que $[L : K]_s = [L : K(a)]_s[K(a) : K]_s$ e $[L : K]_i = [L : K(a)]_i[K(a) : K]_i$.*

Demonstração. Suponha N fecho normal de L/K.

Pelo Teorema 1.2.2 existem $[K(a) : K]_s = r_0$ K-imersões de $K(a)$ no fecho normal de L/K N. Sejam $\{\sigma_1, \ldots, \sigma_{r_0}\}$ essas imersões.

Veja que para qualquer $i = 1, ..., r_0$, $\sigma_i : K(a) \longrightarrow \sigma_i(K(a))$ é um K-isomorfismo de corpos e, pelo Teorema 1.1.9, σ_i pode ser estendido a um K-automorfismo de N, o qual denotaremos por σ_i^N. Note que não estamos exigindo que a extensão de σ_i seja única, mas sim fixando uma das possíveis extensões.

Sejam $\{\tau_1, \ldots, \tau_{s_0}\}$ as $s_0 = [L : K(a)]_s$ $K(a)$-imersões de L em N.

Devemos mostrar que o conjunto $\{\sigma_i^N \tau_j \mid i = 1, ..., r_0,\ j = 1, ..., s_0\}$ possui todas as K-imersões de L em N.

Primeiramente repare que, se η é uma K-imersão de L em N, a restrição de η a $K(a)$ é uma K-imersão de $K(a)$ em N, ou seja, para algum $i \in \{1, ..., r_0\}$ temos $\eta|_{K(a)} = \sigma_i$. Repare ainda que, $(\sigma_I^N)^{-1}\eta$ é uma $K(a)$-imersão de L em N. Logo, para algum $j \in \{1, ..., s_0\}$ temos $(\sigma_I^N)^{-1}\eta = \tau_j$. Assim $\eta = (\sigma_I^N)\tau_j$, ou seja, toda K-imersão de L em N está no conjunto $\{\sigma_i^N \tau_j \mid i = 1, ..., r_0,\ j = 1, ..., s_0\}$.

Agora, se

$$\sigma_{i_1}^N \tau_{j_1} = \sigma_{i_2}^N \tau_{j_2}$$

então

$$\sigma_{i_1}^N \tau_{j_1}|_{K(a)} = \sigma_{i_2}^N \tau_{j_2}|_{K(a)}$$

Mas desde que τ_j é uma $K(a)$-imersão,

$$\sigma_{i_1}^N|_{K(a)} = \sigma_{i_2}^N|_{K(a)}$$

Logo, como $\sigma_i^N|_{K(a)} = \sigma_i$ temos $\sigma_{i_1} = \sigma_{i_2}$ e assim $i_1 = i_2$. E, desde que σ_i^N é um isomorfismo para todo i, $j_1 = j_2$.

Assim, $\{\sigma_i^N \tau_j \mid i = 1, ..., r_0,\ j = 1, ..., s_0\}$ é o conjunto das K-imersões de L em N, e possui exatamente $r_0 s_0$ elementos. Como pelo Teorema 1.2.2 existem $[L : K]_s$

K-imersões de L em N, $[L : K]_s = [L : K(a)]_s[K(a) : K]_s$ e, consequentemente $[L : K]_i = [L : K(a)]_i[K(a) : K]_i$. □

Proposição 1.2.8. *Seja L/K extensão finita, então $tr_{L/K}(L) \subseteq K$.*

Demonstração. Sejam $a \in L$ e N fecho normal de L/K.

Considere $\{\sigma_i^N\tau_j \mid i = 1, ..., r_0,\ j = 1, ..., s_0\}$ o conjunto das K-imersões de L em N exatamente como construído na Proposição 1.2.7.

Temos

$$tr_{L/K}(a) = [L : K]_i \sum_{i=1}^{r_0} \sum_{j=1}^{s_0} \sigma_i^N \tau_j(a)$$

E como τ_j é uma $K(a)$-imersão

$$tr_{L/K}(a) = [L : K]_i \sum_{i=1}^{r_0} \sum_{j=1}^{s_0} \sigma_i^N(a) = s_0[L : K]_i \sum_{i=1}^{r_0} \sigma_i(a)$$

Mas $[L : K]_i = [L : K(a)]_i[K(a) : K]_i$, então

$$tr_{L/K}(a) = s_0[L : K(a)]_i([K(a) : K]_i \sum_{i=1}^{r_0} \sigma_i(a))$$

Pela Proposição 1.2.5, $\sigma_1(a), \ldots, \sigma_{r_0}(a)$ são todas as raizes do minimal de a $m_{a,K}(X)$, cada uma com multiplicidade $[K(a) : K]_i$. Desta forma, temos pela Observação 1.2.6 que $[K(a) : K]_i \sum_{i=1}^{r_0} \sigma_i(a) \in K$. Logo $tr_{L/K}(a) \in K\ \forall a \in L$.

□

1.3 Krull-Schmidt

Aqui faremos uma construção do Teorema de Krull-Schmidt, que nos ajudará a demonstrar o Teorema 3.1.1, de uma forma a evitar o Teorema da Base Normal.

Definição 1.3.1. *Considere M um A-módulo. Vamos dizer que uma sequência $M = M_0 \supset M_1 \supset ... \supset M_r = \{0\}$ de A-submódulos de M é uma sequência de*

composição se as inclusões são próprias e não existe nenhum submódulo de M entre cada M_i e M_{i+1}. Neste caso, diremos que esta sequência tem comprimento r.

Note que nesta definição não exigimos que M possua uma sequência de composição.

Definição 1.3.2. *Seja M um A-módulo. Uma sequência $M'_0 \supset M'_1 \supset ... \supset M'_s$ de M é dita refinamento de uma outra sequência $M_0 \supset M_1 \supset ... \supset M_r$ de M se para todo $i = 1, ..., s$ existe $j \in 1, ..., r$ tal que $M'_i = M_j$.*

O Teorema de Jordan-Hölder (ver [9]) nos diz que, se M tem uma sequência de composição, então qualquer outra sequência de composição terá o mesmo comprimento. Mais do que isso, qualquer sequência estrita de submódulos pode ser refinada a uma sequência de composição de M.

Assim, diremos que M tem comprimento finito r se M admite uma sequência de composição de comprimento r.

Definição 1.3.3. *Um A-módulo M é dito Artiniano se toda sequência infinita decrescente de submódulos é estacionária, ou seja, se $M_1 \supseteq M_2 \supseteq M_3 \supseteq ...$ é uma sequência infinita de submódulos, então existe $n \in \mathbb{N}$ tal que $M_n = M_{n+i}$ para todo $i \in \mathbb{N}$.*

Definição 1.3.4. *Um A-módulo M é dito Noetheriano se toda sequência infinita crescente de submódulos é estacionária, ou seja, se $M_1 \subseteq M_2 \subseteq M_3 \subseteq ...$ é uma sequência infinita de submódulos, então existe $n \in \mathbb{N}$ tal que $M_n = M_{n+i}$ para todo $i \in \mathbb{N}$.*

Proposição 1.3.5. *Um A-módulo M admite uma sequência de composição se e somente se M é Artiniano e Noetheriano.*

Demonstração. ($\Rightarrow$) Imediato, visto que se negarmos que M seja Artiniano ou Noetheriano conseguimos uma sequência de comprimento maior do que a sequência de composição.

($\Leftarrow$) Basta tomarmos M_1 submódulo maximal de $M = M_0$, o qual existe pois M é Noetheriano. Podemos seguir com essa operação obtendo M_i maximal de M_{i-1} se $M_{i-1} \neq \{0\}$. Como M é Artiniano, esta cadeia é estacionária (e logo algum $M_n = \{0\}$). Desta forma temos uma sequência de composição.

□

Lema 1.3.6. *Seja M um A-módulo, $\varphi : M \longrightarrow M$ um homomorfismo e $n > 0$ inteiro. Chame $I_n = Im(\varphi^n)$ e $N_n = Ker(\varphi^n)$. Valem:*

(i) Se $I_1 = I_2$, então $I_1 + N_1 = M$ e se $N_1 = N_2$, $I_1 \cap M_1 = \{0\}$.

(ii) Se M é Artiniano, existe $n_0 \in \mathbb{N}$ tal que para todo $n \geq n_0$ tem-se $I_n + N_n = M$. Se M é Noetheriano, existe $n_0' \in \mathbb{N}$ tal que para todo $n \geq n_0'$ $I_n \cap N_n = \{0\}$.

Demonstração.

(*i*) Se $I_1 = I_2$, dado $x \in M$, existe $y \in M$ com $\varphi(x) = \varphi^2(y)$. Temos $\varphi(x - \varphi(y)) = 0$ e, assim, $x - \varphi(y) \in Ker\varphi = N_1$.

Ora,

$$x = \underbrace{\varphi(y)}_{\in I_1} + \underbrace{x - \varphi(y)}_{\in N_1}$$

Ou seja, $M = I_1 + N_1$.

Agora, suponhamos $N_1 = N_2$ e tome $x \in I_1 \cap N_1$. Ora, $\varphi(x) = 0$ pois $x \in N_1$ e existe $y \in M$ tal que $\varphi(y) = x$ pois $x \in I_1$.

Como $\varphi^2(y) = \varphi(x) = 0$, temos $y \in N_2 = N_1$. Desta forma $x = \varphi(y) = 0$

(*ii*) Se M é Artiniano, a cadeia descendente

$$I_1 \supset I_2 \supset ... \supset I_n \supset ...$$

é estacionária, ou seja, existe n_0 tal que $I_n = I_{n_0}\ \forall n \geq n_0$.

Em particular, $I_{2n} = I_{n_0} = I_n\ \forall n \geq n_0$.

Seja $\psi = \varphi^n$ para algum $n \geq n_0$. Vamos indicar I_j e N_j por $I_{j,\psi}$ e $N_{j,\psi}$ quando nos referirmos a este homomorfismo.

Desta forma, $I_{1,\psi} = Im(\psi) = Im(\varphi^n) = I_n = I_{2n} = Im(\varphi^{2n}) = Im(\psi^2) = I_{2,\psi}$

Pela primeira parte do Lema, $M = I_{1,\psi} + N_{1,\psi} = I_n + N_n$.

Agora, se M é Noetheriano, a cadeia ascendente

$$N_1 \subset N_2 \subset ... \subset N_n \subset ...$$

é estacionária, ou seja, existe n_0' tal que $N_n = N_{n_0'}\ \forall n \geq n_0'$.

Defina $\psi = \varphi^n$ para algum $n \geq n_0'$. Ora, $N_{1,\psi} = N_n = N_{2n} = N_{2,\psi}$. Pela primeira parte, $\{0\} = I_{1,\psi} \cap N_{1,\psi} = I_n \cap N_n$.

□

Particularmente, se M é um módulo Artiniano e Noetheriano, existe n_0 tal que $M = I_n \oplus N_n$, $\forall\ n \geq n_0$.

Lema 1.3.7. *Sejam M um A-módulo e $\varphi : M \longrightarrow M$ homomorfismo de A-módulos.*

(*i*) *Se M é Artiniano e φ é monomorfismo, então φ é epimorfismo.*

(*ii*) *Se M é Noetheriano e φ é epimorfismo, então φ é monomorfismo.*

Demonstração.

(i) Se M é Artiniano, pelo lema anterior temos que existe n_0 tal que $M = I_n + N_n$ para $n \geq n_0$, com $I_n = Im(\varphi^n)$ e $N_n = Ker(\varphi^n)$.

Mas φ é monomorfismo, logo temos $N_1 = N_n = \{0\}$. Assim, $M = I_n$.

Note que $M \supset I_1 \supset I_2 \supset ... \supset I_n = M$. Desta forma, $M = I_1$. Logo φ é epimorfismo.

(ii) Se M é Noetheriano, pelo lema anterior temos que existe n_0' tal que $I_n \cap N_n = \{0\}$ para $n \geq n_0$, com $I_n = Im(\varphi^n)$ e $N_n = Ker(\varphi^n)$.

Por hipótese, $M = I_1 = I_n$. Logo devemos ter $N_n = \{0\}$.

Note que $\{0\} \subset N_1 \subset ... \subset N_n = \{0\}$ e assim $N_1 = \{0\}$. Logo φ é monomorfismo.

□

Definição 1.3.8. *Seja M um A-módulo. Se existem submódulos próprios M_1 e M_2 de M tais que $M = M_1 \oplus M_2$, dizemos que M é decomponível. M é dito indecomponível se não é decomponível.*

Repare que se M é indecomponível e $M = M_1 \oplus M_2$, então $M_1 = 0$ ou $M_2 = 0$.

Definição 1.3.9. *Um homomorfismo de A-modulos é dito nilpotente se existe $n \in \mathbb{N}$ tal que $\varphi^n = 0$.*

Lema 1.3.10. ***(Fitting)*** *Sejam M um A-módulo e $Hom_A(M, M)$ o conjunto dos endomorfismos de M. Se M é indecomponível de comprimento finito, então todo elemento não invertível de $Hom_A(M, M)$ é nilpotente. Ainda, $Hom_A(M, M)$ tem um único ideal bilateral maximal dado por $I = \{\varphi \in Hom_A(M, M) \mid \varphi$ não é invertível $\}$.*

Demonstração. Seja $\varphi \in Hom_A(M,M)$ não invertível. Como M tem comprimento finito, M é Artiniano e Noetheriano. Assim podemos encontrar $n > 1$ tal que $I_n \oplus N_n = M$ com $I_n = Im(\varphi^n)$ e $N_n = Ker(\varphi^n)$.

Como M é indecomponível, $I_n = \{0\}$ ou $N_n = \{0\}$.

Caso $N_n = \{0\}$, φ é epimorfismo e logo, pelo Lema 1.3.7, φ é monomorfismo. Desta forma temos φ invertível, o que é absurdo.

Temos assim $I_n = \{0\}$. Ora, $\varphi^n = 0$, ou seja, φ é nilpotente.

Seja, agora, $\varphi \in I$ e $\psi \in Hom_A(M,M)$. Caso $\varphi\psi$ seja invertível, teremos $(\varphi\psi)(\varphi\psi)^{-1} = Id_M$ e então $\psi(\varphi\psi)^{-1}$ será inversa à direita de φ, fazendo com que φ seja epimorfismo. Pelo Lema 1.3.7, φ também será monomorfismo e assim invertível, o que é absurdo. Logo $\varphi\psi$ não é invertível.

Com raciocínio análogo provamos que $\psi\varphi$ não é invertível.

Ora, $Hom_A(M,M)I \subset I$ e $IHom_A(M,M) \subset I$ com a operação composição.

Nos resta mostrar que I é fechado para a soma.

Considere, então, φ e $\psi \in I$. Vamos supor que $\omega = \varphi + \psi$ é invertível. Com isso, defina $\varphi_1 = \omega^{-1}\varphi$ e $\psi_1 = \omega^{-1}\psi$. Assim, $Id_M = \omega^{-1}\omega = \omega^{-1}(\varphi+\psi) = \varphi_1 + \psi_1$.

Mostremos inicialmente que φ_1 e ψ_1 comutam:

$$\begin{aligned}
\varphi_1\psi_1 &= \omega^{-1}\varphi\omega^{-1}\psi \\
&= \omega^{-1}(\omega-\psi)\omega^{-1}(\omega-\varphi) \\
&= (\omega^{-1}\omega - \omega^{-1}\psi)(\omega^{-1}\omega - \omega^{-1}\varphi) \\
&= (Id_M - \omega^{-1}\psi)(Id_M - \omega^{-1}\varphi) \\
&= Id_M - \omega^{-1}\psi - \omega^{-1}\varphi + \omega^{-1}\psi\omega^{-1}\varphi \\
&= Id_M - \omega^{-1}(\psi+\varphi) + \omega^{-1}\psi\omega^{-1}\varphi \\
&= \omega^{-1}\psi\omega^{-1}\varphi \\
&= \psi_1\varphi_1
\end{aligned}$$

Veja que φ e ψ estão em I e, assim, como mostramos anteriormente, φ_1 e ψ_1 também estão, ou seja, são não-invertíveis. Logo, φ_1 e ψ_1 são nilpotentes. Suponha $\varphi_1^n = 0 = \psi_1^n$ para algum n.

Como ψ_1 e φ_1 comutam, podemos aplicar o teorema do binômio:

$$Id_M = Id_M^{2n} = (\varphi_1 + \psi_1)^{2n} = \sum_{i=1}^{2n} \frac{2n!}{(2n-i)!i!} \varphi_1^i \psi_1^{2n-i} = 0$$

o que é absurdo.

Logo, $\varphi + \psi$ não é invertível. Assim, I é ideal bilateral.

Claramente I é o único ideal bilateral maximal pois, se J é ideal bilateral e $f \in J \backslash I$, então f é invertível. Assim, $ff^{-1} \in J$ e temos $J = Hom_A(M, M)$

□

Teorema 1.3.11. ***(Krull-Schmidt)*** *Seja M um A-módulo de comprimento finito. Então:*

(i) *M é soma direta de módulos indecomponíveis.*

(ii) *Se $M \simeq \bigoplus_{i=1}^{m} M_i$ e $M \simeq \bigoplus_{j=1}^{m'} M'_j$ com M_i e M'_j todos indecomponíveis e não nulos para todo $i = 1, ..., m$ e $j = 1, ...m'$, então $m = m'$ e existe uma permutação σ tal que $M_i = M'_{\sigma(i)}$.*

Demonstração.

(i) Se M tem comprimento 1, então M não tem submódulos próprios, pois se M_1 o fosse, seria $M = M_0 \supset M_1 \supset M_2 = \{0\}$ inclusões estritas e o comprimento de M seria maior que 1. Logo M é indecomponível.

Vamos, então, usar indução sobre o comprimento n de M. Suponha $n > 1$ e que o resultado seja válido para módulos com comprimento menor do que n.

Ora, se M for indecomponível não há nada a se fazer. Se M é decomponível, escreva $M = M_1 \oplus M_2$.

Veja que, se $M_1 \supset N_1 \supset ... \supset N_l = \{0\}$ é uma sequência de composição de M_1 submódulo próprio de M, então $M \supset M_1 \supset N_1 \supset ... \supset N_l = \{0\}$ é uma sequência de M, que pode ser refinada a uma sequência de composição de M, ou seja, $l + 1 \leq n$. Assim o comprimento de M_1 deve ser estritamente menor do que o comprimento de M. Análogo para M_2.

Desta forma aplicamos a hipótese de indução para M_1 e M_2 e o resultado segue trivialmente.

(ii) Considere $p_i : M \longrightarrow M_i$ e $p'_j : M \longrightarrow M'_j$ projeções associadas às decomposições.

Assim, se $x \in M$, $x = \sum_{i=1}^{m} p_i(x) = \sum_{j=1}^{m'} p'_j(x)$.

Ora, $Id_M = \sum_{i=1}^{m} p_i$ e então $p'_1 = \sum_{i=1}^{m} p'_1 p_i$. Ainda, $p'_1|_{M'_1} = Id_{M'_1} = Id_M|_{M_1}$ e temos $Id_{M'_1} = \sum_{i=1}^{m} p'_1 p_i|_{M'_1}$. Note que I descrito no Lema de Fitting é ideal e $Id_{M'_1} \notin I$. Assim, se todas as parcelas da soma estivessem em I, $Id_{M'_1}$ estaria em I, o que é absurdo. Logo existe $k \in \{1, ..., m\}$ tal que $p'_1 p_k|_{M'_1} \notin I$, ou seja, $p'_1 p_k|_{M'_1}$ é invertível.

Vamos mostrar que $M'_1 \simeq M_k$.

Seja $\varphi_1 := Id_M - p'_1 - p_k p'_1 \in Hom_A(M, M)$. Devemos mostrar que φ_1 é isomorfismo.

Temos que φ_1 é monomorfismo pois, se $\varphi_1(x) = 0$, então $0 = p'_1(\varphi_1(x)) = p'_1(x) - p'_1 p'_1(x) - p'_1 p_k p'_1(x)$. Desde que p'_1 é projeção, $p'_1 p'_1(x) = p'_1(x)$ e , sendo assim, $p'_1 p_k p'_1(x) = 0$. Como $p'_1 p_k$ restrito a M'_1 é bijeção, $p'_1(x) = 0$. Logo $0 = \varphi_1(x) = Id_M(x) - p'_1(x) - p_k p'_1(x) = Id_M(x) = x$, ou seja, φ_1 é injetora.

Como M tem comprimento finito, ou seja, é Artiniano e Noetheriano, pelo Lema

1.3.7, φ_1 é isomorfismo.

Repare que para $j \neq 1$, $p'_1 p'_j = 0$. Logo $\varphi_1 p'_j = p'_j - p'_1 p'_j - p_k p'_1 p'_j = p'_j$. Desta forma, $\varphi_1|_{M'_j} = Id_{M'_j}$ para $j \neq 1$.

Afirmação: $\varphi_1(M'_1) = M_k$:

Se $x \in M'_1$, $\varphi_1(x) = x - p'_1(x) - p_k p'_1(x) = x - x - p_k(x) = -p_k(x) \in M_k$. Desta forma $\varphi_1(M'_1) \subseteq M_k$

Mas $M = \varphi_1(M) = \bigoplus_{j=1}^{m'} \varphi_1(M'_j) = \varphi_1(M'_1) \oplus (\bigoplus_{j=2}^{m'} M'_j)$.

E, $M_k = M_k \cap M = M_k \cap [\varphi_1(M'_1) \oplus (\bigoplus_{j=2}^{m'} M'_j)] = [M_k \cap \varphi_1(M'_1)] \oplus [M_k \cap \bigoplus_{j=2}^{m'} M'_j]$.

Mas M_k é indecomponível e $\varphi_1(M'_1) \subset M_k$.

Observe que φ_1 é injetora e $M'_1 \neq \{0\}$, logo $M_k \cap \varphi_1(M'_1) = \varphi_1(M'_1) \neq \{0\}$

Logo $M_k \cap \bigoplus_{j=2}^{m'} M'_j = \{0\}$ e assim $M_k = \varphi_1(M'_1)$.

Assim a restrição de φ_1 a M'_1 é isomorfismo de M'_1 em M_k, como queríamos.

Desta forma, $\bigoplus_{j=2}^{m} M_j \simeq \frac{\bigoplus_{j=1}^{m} M_j}{M_1} \simeq \frac{\varphi_1(\bigoplus_{j=1}^{m} M_j)}{\varphi_1(M_1)} \simeq \frac{\bigoplus_{j=1}^{m'} M'_j}{M'_k} \simeq \bigoplus_{i=1, i\neq k}^{m'} M'_i$.

O resultado segue facilmente por indução. □

1.4 Formas quadráticas

Ao longo desta seção estaremos supondo sempre que a característica de qualquer corpo é distinta de 2. Todos os espaços vetoriais serão de dimensão finita. Para uma melhor compreensão dos conceitos e demonstrações contidos nesta seção, são recomendados os capítulos 1 e 2 de [6].

Definição 1.4.1. *Seja F um corpo. Uma forma quadrática (n-ária) f sobre F é um polinômio $f(X_1, ..., X_n) \in F[X_1, ..., X_n]$ homogêneo de grau 2. Em outras palavras,* $f(X_1, ..., X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j$ *com $a_{ij} \in F$ para todo $i = 1, ..., n$ e $j = 1, ..., n$.*

Repare que $X_i X_j = X_j X_i$ para $i \in \{1, ..., n\}$ e $j = \{1, ..., n\}$. Assim, podemos reescrever a forma $f(X_1, ..., X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j$ como $f(X_1, ..., X_n) = \sum_{i,j=1}^{n} a'_{ij} X_i X_j$ com coeficientes simétricos onde $a'_{ij} = \frac{1}{2}(a_{ij} + a_{ji})$.

Note que $f(X_1, ..., X_n)$ determina unicamente uma matriz simétrica, denotada por M_f, tal que, $f(X) = X^t M_f X$, onde X é o vetor coluna com entradas $X_1, .., X_n$, X^t representa X como um vetor linha e a multiplicação é a usual de matrizes por vetores.

Para facilitar a notação, escreveremos uma forma quadrática n-ária f como $f(X_1, ..., X_n) = f(X)$.

Definição 1.4.2. *Se f e g são duas formas quadráticas n-árias sobre F, diremos que f é equivalente a g se existir um matriz invertível $C \in M_n(F)$ tal que $f(X) = g(CX)$. Denotaremos a equivalência de f e g por $f \simeq g$. Equivalentemente, podemos dizer que $f \simeq g$ se $M_f = C^t M_g C$, pois $g(CX) = (CX)^t M_g CX = X^t (C^t M_g C) X$.*

Dada uma forma quadrática n-ária f, vamos denotar por (f) a classe de todas as formas quadráticas n-árias sobre F que são equivalentes a f

Considere V um F-espaço vetorial de dimensão n e $q : V \times V \longrightarrow F$ uma aplicação F-bilinear. Suponha, ainda, que q seja simétrica, ou seja, $q(u, v) = q(v, u)$ $\forall\ u, v \in V$. Ao espaço (V, q) damos o nome de espaço quadrático. Veja que, se $\{v_1, ..., v_n\}$ é uma base de V, então temos a forma quadrática $f_q = \sum_{i,j=1}^{n} q(v_i, v_j) X_i X_j$ sobre F. Mais ainda, $(M_{f_q})_{ij} = q(v_i, v_j)$ com $i, j \in \{1, ..., n\}$.

Note qua f_q foi definida a partir de uma base de V, ou seja, ao mudarmos a

base, mudamos a forma f_q.

Entretanto, se supormos uma outra base $\{v'_1, ..., v'_n\}$ de V, então obteremos uma forma $f'_q = \sum_{i,j=1}^{n} q(v'_i, v'_j)X_iX_j$.

Seja $v'_i = \sum_{k=1}^{n} c_{ki}v_k$ para todo $i = 1, ..., n$. Tome $C = (c_{ij})$.

Temos

$$\begin{aligned}(M_{f'_q})_{ij} &= q(v'_i, v'_j) = q(\sum_{k=1}^{n} c_{ki}v_k, \sum_{l=1}^{n} c_{lj}v_l) \\ &= \sum_{k,l=1}^{n} c_{ki}q(v_k, v_l)c_{lj} = (C^t M_{f_q} C)_{ij}\end{aligned}$$

ou seja, $f'_q \simeq f_q$.

Logo, (V, q) determina unicamente uma classe de equivalência (f_q). Observe que, dada qualquer forma $g \in (f_q)$, tomando a matriz C tal que $f_q(X) = g(CX)$ e fazendo-se $\{Cv_1, ..., Cv_n\}$, obtemos uma base de V que determina g.

Mais ainda, se f é uma forma quadrática n-ária qualquer, podemos considerar o espaço vetorial F^n com a aplicação bilinear simétrica $q((x_1, ..., x_n), (y_1, ..., y_n)) = (x_1, ..., x_n)^t M_f(y_1, ..., y_n)$. Ora, na base canônica de F^n, $f = f_q$.

Definição 1.4.3. *Sejam (V, q) e (V', q') dois espaços quadráticos. Diremos que (V, q) e (V', q') são isométricos ($\simeq$) se existir um isomorfismo $\tau : V \longrightarrow V'$ tal que $q'(\tau(x), \tau(y)) = q(x, y)$ para todo $x, y \in V$.*

Proposição 1.4.4. *Sejam (V, q) e (V', q') dois espaços quadráticos de dimensão n. Então $(V, q) \simeq (V', q') \Leftrightarrow (f_q) = (f_{q'})$.*

Demonstração. ($\Rightarrow$) Suponha que existe um isomorfismo $\tau : V \longrightarrow V'$ tal que $q'(\tau(x), \tau(y)) = q(x, y)\ \forall\ x, y \in V$. Considere $\{v_1, ..., v_n\}$ uma base de V. Então, para f_q definida a partir desta base, $M_{f_q} = (q(v_i, v_j))$. Como τ é um isomorfismo, então $\{\tau(v_1), ..., \tau(v_n)\}$ é uma base para V'. E, para $f_{q'}$ definida a partir desta base, $M_{f_{q'}} = (q(\tau(v_i), \tau(v_j)))$. Logo $M_{f_q} = M_{f_{q'}} = Id_n^t M_{f_{q'}} Id_n$ e, assim, $f_q \simeq f_{q'}$.

($\Leftarrow$) Sejam $\{v_1, ..., v_n\}$ base de V e $\{w_1, ..., w_n\}$ base de V'. Considere g e h formas quadráticas definidas a partir destas bases e das aplicações bilineares q e q'. Ora $g \in (f_q)$ e $h \in (f_{q'})$. Como $(f_{q'}) = (f_q)$, $g \simeq h$. Assim existe $C = (c_{ij}) \in M_n(F)$ invertível tal que $M_{f_q} = C^t M_{f_{q'}} C$.

Considere o conjunto $\{v'_1, ..., v'_n\}$ tal que $v'_i = \sum_{k=1}^{n} c_{ki} w_k$ para todo $i = 1, ..., n$.

Veja que $0 = \sum_{l=1}^{n} a_l v'_l = \sum_{l,k=1}^{n} a_l c_{lk} w_k \Leftrightarrow \sum_{l=1}^{n} a_l c_{li} = 0 \ \forall \ i \in \{1, ..., n\} \Leftrightarrow (a_1, ..., a_n)$ é solução de $CX = 0 \overset{det(C)\neq 0}{\Leftrightarrow} a_i = 0 \ \forall \ i \in \{1, ..., n\}$. Logo $\{v'_1, ..., v'_n\}$ é base de V'.

Defina $\tau : V \longrightarrow V'$ por $\tau(v_i) = v'_i \ \forall \ i \in \{1, ..., n\}$. Veja que τ é isomorfismo.

Mais ainda,

$$\begin{aligned} q(v_i, v_j) &= (M_g)_{ij} = (C^t M_h C)_{ij} \\ &= \sum_{k,l=1}^{n} c_{ki} q'(w_i, w_j) c_{lj} = q'(\sum_{k=1}^{n} c_{ki} w_k, \sum_{l=1}^{n} c_{lj} w_l) \\ &= q'(v_i, v_j) = q'(\tau(v_i), \tau(v_j)) \end{aligned}$$

Ora, se x e y são elementos de V, escreva $x = \sum_{i=1}^{n} x_i v_i$ e $y = \sum_{j=1}^{n} y_j v_j$.

Temos

$$\begin{aligned} q'(\tau(x), \tau(y)) &= q'(\tau(\sum_{i=1}^{n} x_i v_i), \tau(\sum_{j=1}^{n} y_j v_j)) = \sum_{i,j=1}^{n} x_i y_j q'(\tau(v_i), \tau(v_j)) \\ &= \sum_{i,j=1}^{n} x_i y_j q(v_i, v_j) = q(x, y) \end{aligned}$$

Assim, $(V, q) \simeq (V', q')$.

□

Logo, temos uma correspondência $1 - 1$ entre as classes de isometria de espaços quadráticos sobre F e as classes de formas quadráticas sobre F.

Proposição 1.4.5. *Sejam (V, q) um espaço quadrático (V não-nulo) e M uma matriz associada a uma das formas na classe (f_q). As seguintes afirmações são equivalentes:*

(i) *M é uma matriz não-singular, ou seja, $det(M) \neq 0$.*

(ii) *$x \mapsto q(\cdot, x)$ define um isomorfismo $V \to V^*$, onde V^* é o espaço dual de V.*

(iii) *Se $x \in V$ e $q(x, y) = 0 \ \forall \ y \in V$, então $x = 0$.*

A demonstração deste resultado decorre da álgebra linear básica e não será feita neste trabalho.

Definição 1.4.6. *Um espaço quadrático (V, q) será dito regular se qualquer uma das condições acima se verificar. Uma forma quadrática é dita regular se um espaço quadrático associado à sua classe for regular.*

Note que o espaço nulo satisfaz (ii) e (iii), mas não satisfaz (i). Mesmo assim o entenderemos como regular.

Chamaremos de $M(F)$ o conjunto das classes de equivalência de todas as formas quadráticas regulares sobre F.

Tentaremos agora definir uma soma em $M(F)$. Para isso, introduziremos uma soma no conjunto dos espaços quadráticos.

Sejam (V_1, q_1), (V_2, q_2) espaços quadráticos sobre um corpo F. Definiremos a soma ortogonal entre estes espaços por $(V_1, q_1) \perp (V_2, q_2) = (V, q)$ de forma que $V = V_1 \oplus V_2$ e $q((x_1, x_2), (y_1, y_2)) = q_1(x_1, y_1) + q_2(x_2, y_2)$. Note que (V, q) é trivialmente um espaço quadrático.

Repare que, se $(V_1, q_1) \simeq (V_2, q_2)$ e $(V_3, q_3) \simeq (V_4, q_4)$ são espaços quadráticos, então $(V_1, q_1) \perp (V_3, q_3) \simeq (V_2, q_2) \perp (V_4, q_4)$. Ou seja, esta soma é bem definida no conjunto das classes de isometria de espaços quadráticos sobre F.

Se f e g são formas quadráticas associadas a espaços (V, q) e (V', q') em relação às bases $\{v_1, ..., v_n\}$ e $\{v'_1, ..., v'_m\}$ respectivamente, obteremos uma forma quadrática

em relação à base $\{v_1, ..., v_n, v'_1, ..., v'_m\}$ de $V \oplus V'$. Esta forma será denotada por $f \perp g$.

Isto induz uma soma em $M(F)$ por $(f) \perp (g) = (f \perp g)$.

Observação 1.4.7. *O conjunto $M(F)$ com a soma ortogonal é um semigrupo comutativo, ou seja, a soma $\perp$ é associativa e comutativa.*

Observação 1.4.8. *Repare que, se $f = \sum_{i,j=1}^{n} a_{ij} X_i X_j$ e $g = \sum_{i,j=1}^{m} b_{ij} X_i X_j$ são duas formas quadráticas, então $f \perp g = \sum_{i,j=1}^{n} a_{ij} X^i X^j + \sum_{i,j=n+1}^{n+m} b_{ij} X^i X^j$.*

Isto pois

$$M_{f \perp g} = \left[\begin{array}{c|c} M_f & 0_{n \times m} \\ \hline 0_{m \times n} & M_g \end{array}\right]$$

nas bases acima referidas.

Para $d \in F$, denotaremos por $< d >_F$ a classe de isometria dos espaços quadráticos associados à forma quadrática dX^2. Quando não houver dúvidas quanto ao corpo, escreveremos $< d >_F$ simplesmente como $< d >$. Veja que $< d >$ é regular se $d \neq 0$. Abreviaremos a soma $< d_1 > \perp ... \perp < d_n >$ por $< d_1, ..., d_n >$.

Definição 1.4.9. *Seja (V, q) um espaço quadrático. Dizemos que $v \in V$ é isotrópico se $q(v, v) = 0$. O espaço (V, q) (ou simplesmente V) é dito isotrópico se existe um vetor $v \in V$ que é isotrópico. Um espaço em que todo vetor é isotrópico é dito totalmente isotrópico.*

Observe que em um espaço totalmente isotrópico (V, q) temos $q = 0$ pois, como a característica do corpo é distinta de 2,

$$q(u, v) = \frac{1}{2} q(u, u) + q(u, v) + \frac{1}{2} q(v, v) = \frac{1}{2} q(u + v, u + v) = 0$$

para quaisquer $u, v \in V$.

Teorema 1.4.10. *Seja (V, q) um espaço quadrático de dimensão 2 ($dim_F V = 2$). São equivalentes:*

(i) V é regular e isotrópico.

(ii) V é isométrico a $< 1, -1 >$.

A demonstração deste resultado e outras equivalências, podem ser vistas em [6] página 12.

Definição 1.4.11. *Se (V, q) cumpre alguma das condições acima, então a classe de isometria de (V, q) é chamada de plano hiperbólico sobre F. Denotaremos um plano hiperbólico sobre F por $\mathbb{H}_F$, bem como a classe de formas associadas a (V, q).*

A uma soma de n planos hiperbólicos (denotado por $n\mathbb{H}_F$) damos o nome de espaço hiperbólico.

Teorema 1.4.12. ***(Lei do cancelamento de Witt)*** *Sejam (V, q), (V_1, q_1) e (V_2, q_2) espaços quadráticos. Então, se $(V, q) \perp (V_1, q_1) \simeq (V, q) \perp (V_2, q_2)$, então $(V_1, q_1) \simeq (V_2, q_2)$.*

Para esta demonstração, consulte [6], página 15.

Caso o corpo F seja estendido a um corpo K, estudaremos a forma como podemos estender um espaço quadrático (V, q) sobre F a um espaço quadrático sobre K.

Seja K/F extensão de corpos e (V, q) espaço quadrático sobre F. Note que espaço $V_K = K \otimes_F V$ torna-se um K-espaço vetorial de dimensão $dim_F V$, com K agindo no primeiro fator.

Assim, podemos construir o espaço quadrático (V_K, q_K) sobre K com $q_K(k \otimes_F v, k' \otimes_F v') = kk'q(v, v')$.

Note ainda que, se (V,q) é regular, (V_K, q_K) também o é. Para isso, basta observar que a matriz de f_q em relação a uma base $\{v_1, ..., v_n\}$ de V sobre F é igual a matriz de f_{q_K} na base $\{1 \otimes v_1, ..., 1 \otimes v_n\}$ de V_K sobre K e, sendo (V,q) regular, ambas têm o determinante não-nulo.

A partir de agora, sempre que nos referirmos a espaços quadráticos ou a formas quadráticas estaremos nos referindo a espaços quadráticos e formas quadráticas regulares.

Veja que a aplicação $(V,q) \mapsto (V_K, q_K)$ induz um homomorfismo de semigrupos

$$\begin{array}{rccc} r: & M(F) & \longrightarrow & M(K) \\ & (f_q) & \longrightarrow & (f_{q_k}) \end{array}$$

De fato, r é um homomorfismo de semigrupos pois:

(i) Se temos $(f_q) = (f_{q'})$ em $M(F)$, então $(V,q) \simeq (V',q')$. Claramente temos $(V_K, q_K) \simeq (V'_K, q'_K)$. Assim $(f_{q_K}) = (f_{q'_K})$ e logo r é bem definido.

(ii) Sejam (f_q) correspondente a (V,q) e $(f_{q'})$ correspondente a (V',q'). Note que, como já vimos, $(f_q) \perp (f_{q'}) = (f_{q \perp q'})$. Assim, temos que $r((f_q) \perp (f_{q'}))$ corresponde ao K-espaço quadrático $(K \otimes_F (V \oplus V'), (q \perp q')_K) \simeq (K \otimes_F V, q_K) \perp (K \otimes_F V', q'_K)$. Ora, $r((f_q) \perp (f_{q'})) = (f_{q_K}) \perp (f_{q'_K}) = r((f_q)) \perp r((f_{q'}))$.

Observação 1.4.13. *Podemos ainda definir um produto entre espaços quadráticos. De fato, considere (V_1, q_1) e (V_2, q_2) espaços quadráticos sobre F. Definiremos $(V_1, q_1) \otimes_F (V_2, q_2) = (V_1 \otimes_F V_2, q_1 \otimes q_2)$, onde $V_1 \otimes_F V_2$ é o produto tensorial sobre F de V_1 por V_2 e $(q_1 \otimes q_2)(v_1 \otimes v_2, v'_1 \otimes v'_2) = q_1(v_1, v'_1) q_1(v_2, v'_2)$.*

Repare que $(V_1 \otimes_F V_2, q_1 \otimes q_2)$ é um espaço quadrático e que tem dimensão $dim_F V_1 dim_F V_2$. Note ainda que, se $(V_1, q_1) \simeq (V_2, q_2)$ e $(V_3, q_3) \simeq (V_4, q_4)$ são espaços quadráticos, então $(V_1, q_1) \otimes_F (V_3, q_3) \simeq (V_2, q_2) \otimes_F (V_4, q_4)$. Desta forma, temos um produto bem definido em $M(F)$ por $(f_q) \otimes_F (f_{q'}) = (f_q \otimes_F f_{q'})$, onde f_q

e $f_{q'}$ são formas associadas a espaços (V,q) e (V',q') e $f_q \otimes_F f_{q'}$ é forma associada a $(V \otimes V', q \otimes q')$.

Proposição 1.4.14. *Se f é uma forma quadrática n-ária regular sobre F, então* $(f \otimes_F \mathbb{H}_F) = (n\mathbb{H}_F)$

Ver [6], página 24.

Como $M(F)$ é um semigrupo comutativo com a operação $\perp$ e temos em $M(F)$ definido um produto comutativo, é natural tentarmos construir um anel a partir de $M(F)$.

Para isso, usaremos a construção conhecida como Construção de Grothendieck.

Defina em $M(F) \times M(F)$ a seguinte relação:

$$((f_1),(f_2)) \sim ((g_1),(g_2)) \Leftrightarrow (f_1) \perp (g_2) = (g_1) \perp (f_2)$$

Repare que é imediato o fato de $((f_1),(f_2)) \sim ((f_1),(f_2))$ e $((f_1),(f_2)) \sim ((f_2),(f_1))$.

Ainda, se $((f_1),(f_2)) \sim ((g_1),(g_2))$ e $((g_1),(g_2)) \sim ((h_1),(h_2))$, então $(f_1) \perp (g_2) = (g_1) \perp (f_2)$ e $(g_1) \perp (h_2) = (h_1) \perp (g_2)$. Logo $(f_1) \perp (f_2) \perp (g_1) \perp (h_2) = (f_1) \perp (f_2) \perp (h_1) \perp (g_2) = (f_2) \perp (h_1) \perp (f_2) \perp (h_2)$. Pela Lei do Cancelamento de Witt, $(f_1) \perp (h_2) = (h_1) \perp (f_2)$.

Assim $\sim$ é uma relação de equivalência. Denotaremos por $\hat{W}(F)$ o conjunto $\frac{M(F)\times M(F)}{\sim}$ e uma classe será simplesmente denotada por $((f),(g))$. Mais ainda, em $\hat{W}(F)$ induzimos uma soma $((f),(g)) + ((f'),(g')) = ((f) \perp (f'),(g) \perp (g'))$.

Note que as classes $((f),(g))$ e $((g),(f))$ são inversas aditivas uma da outra. Assim, $\hat{W}(F)$ se torna um grupo abeliano.

A aplicação $i : M(F) \to \hat{W}(F)$ definida por $i((f)) = ((f),0)$ é uma imersão de $M(F)$ em $\hat{W}(F)$ que será vista como uma inclusão, onde 0 é a classe de formas que

representa o espaço nulo. Ou seja, $(f) = ((f), 0)$.

Veja que $((f), (g))$ pode ser visto como $i((f)) - i((g))$ pois $-((g), 0) = (0, (g))$. Logo, todo elemento $((f), (g))$ de $\hat{W}(F)$ pode ser escrito como $(f) - (g)$, onde f e g são formas quadráticas regulares.

Se G é um grupo abeliano, todo homomorfismo de semigrupos $\rho : M(F) \to G$ pode ser estendido unicamente a um homomorfismo de grupos $\rho : \hat{W}(F) \to G$ através da regra $\rho((f) - (g)) = \rho((f)) - \rho((g))$. Esta propriedade é chamada de Propriedade Universal de $M(F)$.

Podemos ainda induzir uma multiplicação comutativa em $\hat{W}(F)$. De fato, se $((f), (g))$ e $((f'), (g'))$ pertencem a $\hat{W}(F)$, então definiremos

$$((f), (g))((f'), (g')) = ([(f) \otimes_F (f')] \perp [(g) \otimes_F (g')], [(f') \otimes_F (g)] \perp [(f) \otimes_F (g')])$$

o que torna $\hat{W}(F)$ um anel comutativo.

A princípio, este produto parece complicado. Entretanto, olhando-se cada par $((f), (g))$ como $(f) - (g)$, temos simplesmente a distributividade da multiplicação.

Definição 1.4.15. *$\hat{W}(F)$ é chamado de Anel de Witt-Grothendieck de formas quadráticas sobre F.*

Podemos, então, estender a aplicação $r : M(F) \longrightarrow \hat{W}(K) \supset M(K)$ a $\hat{r}^* : \hat{W}(F) \to \hat{W}(K)$ homomorfismo de grupos de forma que $\hat{r}^*((f) - (g)) = r((f)) - r((g))$ pois $\hat{W}(K)$ é grupo abeliano.

Mais ainda, é fácil ver que $\hat{r}^*$ é um homomorfismo de anéis.

Repare que se $\mathbb{H}_F$ é um plano hiperbólico sobre F e $\mathbb{H}_K$ é um plano hiperbólico sobre K, $\hat{r}^*(\mathbb{H}_F) = \mathbb{H}_K$ pois a $\mathbb{H}_F$ está associado um F-espaço quadrático (V, q) regular e isotrópico. Ora, (V_K, q_K) é regular e, se v é vetor isotrópico em (V, q), então $q(v, v) = 0$ e $q_K(1_K \otimes_F v, 1_K \otimes_F v) = 1_K q(v, v) = 0$. Logo (V_K, q_K) é regular e isotrópico, ou seja, $\hat{r}^*(\mathbb{H}_F)$ é o plano hiperbólico sobre K.

Observação 1.4.16. *$\hat{r}^*$ não é necessariamente monomorfismo. Como exemplo cito [6], página 190.*

Agora vamos construir a aplicação transfer.

Seja K/F extensão finita e $s : K \longrightarrow F$ um homomorfismo F-linear não-nulo. Repare que s é trivialmente sobrejetor.

Então, se (U, q) é um K-espaço quadrático, fazendo-se $sq : U \times U \to F$ definido por $sq(u, u') = s(q(u, u'))$, temos o F-espaço quadrático (U, sq), pois sq é F-bilinear.

Proposição 1.4.17. *Se (U, q) é K-espaço quadrático regular, então (U, sq) é F-espaço quadrático regular.*

Demonstração. Suponha que exista $x_0 \in U$ não nulo tal que $sq(x_0, y) = 0\ \forall y \in U$. Como (U, q) é regular, existe $y_0 \in U$ tal que $q(x_0, y_0) \neq 0$.

Ora, $\forall c \in K$, $q(x_0, \frac{c}{q(x_0,y_0)}y_0) = \frac{c}{q(x_0,y_0)}q(x_0, y_0) = c$

Assim $s(c) = s(q(x_0, \frac{c}{q(x_0,y_0)}y_0)) = 0$ para todo c em K. Temos $s = 0$, o que é absurdo, uma vez que s é sobrejetor.

Logo não pode existir $x_0 \in U$ não nulo tal que $sq(x_0, y) = 0\ \forall y \in U$, ou seja, (U, sq) é um espaço regular. □

Vamos denotar o espaço (U, sq) descrito acima por $s_*(U)$, o qual é chamado de "transfer" de U.

Veja que $dim_F s_*(U) = [K : F] dim_K U$.

Até o final desta seção, salvo menção em contrário, s sempre representará um homomorfismo F-linear de K em F.

Lembre-se que $r : M(F) \to M(K)$ foi construído a partir da aplicação $(V, q) \mapsto (V_K, q_K)$ estendida às classes de isometria de formas quadráticas. Desta forma, abusaremos da notação e faremos $\hat{r}^*$ agir tanto em $\hat{W}(F)$ como em espaços quadráticos,

ou seja, $\hat{r}^*((V,q)) = \hat{r}^*((f_q))$. Para não sobrecarregar a demonstração, denotaremos $r^*((V,q))$ simplesmente por $r^*(V)$.

Teorema 1.4.18. *Sejam (V,q) um espaço quadrático sobre F e (U,p) um espaço quadrático sobre K. Então existe uma F-isometria*

$$s_*(\hat{r}^*(V) \otimes_K U) \simeq V \otimes_F s_*(U)$$

Em particular, se $U =< 1 >_K$, então $s_*(\hat{r}^*(V)) \simeq V \otimes_F s_*(< 1 >_K)$.

Demonstração. Devido ao grande número de aplicações bilineares simétricas envolvidas na demonstração, vamos denotar de forma geral estas aplicações por $<,>$ tendo o espaço onde é definida como índice, por exemplo, $q(v,v') =< v, v' >_V$ $\forall\ v, v' \in V$.

Defina

$$\begin{array}{rccc} \rho: & s_*((K \otimes_F V) \otimes_K U) & \longrightarrow & V \otimes_F s_*(U) \\ & (k \otimes_F v) \otimes_K u & \longrightarrow & v \otimes_F ku \end{array}$$

(i) ρ é um isomorfismo:

Para isso apresentaremos uma inversa para ρ.

Defina

$$\begin{array}{rccc} \varphi: & V \otimes_F s_*(U) & \longrightarrow & s_*((K \otimes_F V) \otimes_K U) \\ & v \otimes_F u & \longrightarrow & (1 \otimes_F v) \otimes_K u \end{array}$$

Temos

$$\rho\varphi(v \otimes_F u) = \rho((1 \otimes_F v) \otimes_K u) = v \otimes_F u$$

E

$$\varphi\rho((k \otimes_F v) \otimes_K u) = \varphi(v \otimes_F ku) = (1 \otimes_F v) \otimes_K ku = (k \otimes_F v) \otimes_K u$$

Logo φ é inversa de ρ e assim ρ é isomorfismo.

(ii) ρ é uma isometria:

Sejam $k, k' \in K$; $vv' \in V$ e $uu' \in U$. Sejam $a = (k \otimes_F v) \otimes_K u$ e $a' = (k' \otimes_F v') \otimes_K u'$.

$$\begin{aligned}
< \rho(a), \rho(a') >_{V \otimes_F s_*(U)} &= < v \otimes_F ku, v' \otimes_F k'u' >_{V \otimes_F s_*(U)} \\
&= < v, v' >_V < ku, k'u' >_{s_*(U)} \\
&= < v, v' >_V s(< ku, k'u' >_U) \\
&= < v, v' >_V s(kk' < u, u' >_U) \\
&= s(< v, v' >_V kk' < u, u' >_U) \\
&= s(kk' < v, v' >_V < u, u' >_U) \\
&= s(< k \otimes_F v, k' \otimes_F v' >_{K \otimes_F V} < u, u' >_U) \\
&= s(< (k \otimes_F v) \otimes_K u, (k' \otimes_F v') \otimes_K u' >_{(K \otimes_F V) \otimes_K U}) \\
&= < (k \otimes_F v) \otimes_K u, (k' \otimes_F v') \otimes_K u' >_{s_*((K \otimes_F V) \otimes_K U)} \\
&= < a, a' >_{s_*((K \otimes_F V) \otimes_K U)}
\end{aligned}$$

Ou seja , ρ é isometria de F-espaços vetoriais (ou F-isometria).

□

Corolário 1.4.19. *Se U é um espaço hiperbólico sobre K, então $s_*(U)$ é um espaço hiperbólico sobre F.*

Demonstração. Note que, como observamos anteriormente, $\hat{r}^*(\mathbb{H}_F) = \mathbb{H}_K$.

Como um espaço hiperbólico em F é escrito na forma $m\mathbb{H}_F$ com $m \in \mathbb{N}$, podemos supor sem perda de generalidade que $U = \mathbb{H}_K$ pois, da definição de soma ortogonal, $s_*(U_1 \perp U_2) = s_*(U_1) \perp s_*(U_2)$ e soma de espaços hiperbólicos é um espaço hiperbólico.

Logo,

$$\begin{aligned} s_*(U) &= s_*(\mathbb{H}_K) = s_*(\hat{r}^*(\mathbb{H}_F)) \\ &= s_*(\hat{r}^*(\mathbb{H}_F) \otimes_K < 1 >_K) \simeq \mathbb{H}_F \otimes_F s_*(< 1 >_K) \\ &\overset{1.4.14}{\simeq} dim_F(s_*(< 1 >_K))\ \mathbb{H}_F = [K : F]\ \mathbb{H}_F \end{aligned}$$

Assim $s_*(U)$ é hiperbólico.

□

Corolário 1.4.20. *Valem:*

(1) $U \mapsto s_*(U)$ *induz um homomorfismo de grupos* $s_* : \hat{W}(K) \longrightarrow \hat{W}(F)$.

(2) *A composição* $\hat{W}(F) \xrightarrow{\hat{r}^*} \hat{W}(K) \xrightarrow{s_*} \hat{W}(F)$ *coincide com a multiplicação por* $s_*(< 1 >_K)$.

(3) *A imagem de* $s_* : \hat{W}(K) \longrightarrow \hat{W}(F)$ *é ideal em* $\hat{W}(F)$.

Repare que em momento algum demos "cara" a s. Na verdade podemos mostrar que, para qualquer homomorfismo t, s_* e t_* são iguais a menos de um automorfismo de $\hat{W}(K)$, ou seja, $s_*(\hat{W}(K)) = t_*(\hat{W}(K))$. Veja [6], página 194.

Então, podemos escolher um s conveniente.

Teorema 1.4.21. ***(Scharlau)*** *Seja K/F extensão simples finita com $[K : F] = n$ ímpar. Suponha $K = F(\alpha)$ e $s : K \to F$ homomorfismo F-linear definido por $s(1) = 1$ e $s(\alpha^i) = 0\ \forall\ 1 \leq i \leq n-1$. Então $s_*(< 1 >_K) \simeq m\mathbb{H}_F \perp < 1 >_F$.*

Demonstração. Suponha que $n = 2m + 1$. Pensaremos em $s_*(< 1 >_K)$ como o F-espaço K com a forma $(y, z) \longrightarrow s(yz)$ F-bilinear.

Temos os espaços $F \cdot 1$ e $\sum_{i=1}^{n-1} F\alpha^i = K_0$ ortogonais pois, se $y_0 \in F$ e $z_0 \in K_0$, $s(y_0 z_0) = y_0 s(z_0) = y_0 s(\sum_{i=1}^{n-1} x_i \alpha^i) = y_0 \sum_{i=1}^{n-1} x_i s(\alpha^i) = 0$

Desta forma, como $F \cdot 1 \simeq < 1 >_F$, temos $s_*(< 1 >_K) \simeq < 1 >_F \perp K_0$.

Note que o subespaço gerado por $\{\alpha^1, ..., \alpha^m\}$ é totalmente isotrópico, assim deve estar contido em um subespaço hiperbólico de K_0 de dimensão $2m$. Como $dim K_0 = 2m$, temos K_0 hiperbólico e, assim, K_0 isométrico a $m\mathbb{H}_F$.

Logo, $s_*(< 1 >)_K) = < 1 >_F \perp m\mathbb{H}_F$.

□

Proposição 1.4.22. *Seja $K = F(\alpha)$ extensão finita de grau ímpar. Então $\hat{r}^* : \hat{W}(F) \longrightarrow \hat{W}(K)$ é um monomorfismo.*

Demonstração. Suponhamos $n = 2m + 1$. Aqui, a dimensão de uma forma é a demensão do espaço quadrático ao qual ela é associada. Veja que, pela propriedade universal de $M(F)$, o homomorfismo $dim : M(F) \to \mathbb{Z}$ definido por $dim((f)) = dim_F(V)$, onde (V, q) é o F-espaço quadrático associado a (f), pode ser estendido a um homomorfismo $dim : \hat{W}(F) \to \mathbb{Z}$.

Seja $z \in \hat{W}(F)$ tal que $\hat{r}^*(z) = 0$. Temos $z = (f_1) - (f_2)$.

Ora, $z \otimes (m\mathbb{H}_F \perp < 1 >_F) = s_*\hat{r}^*(z) = 0$ em $\hat{W}(F)$

Logo $0 = dim(z \otimes (m\mathbb{H}_F \perp < 1 >_F)) = dim(z)dim(m\mathbb{H}_F \perp < 1 >_F)$.

Desde que $dim(m\mathbb{H}_F \perp < 1 >_F) = 2m + 1 \neq 0$, $dim(z) = 0$. Assim $dim((f_1)) = dim((f_2)) = t$.

Temos $(f_1) \otimes (m\mathbb{H}_F \perp < 1 >_F) = (f_2) \otimes (m\mathbb{H}_F \perp < 1 >_F) \Rightarrow tm\mathbb{H}_F \perp (f_1) = tm\mathbb{H}_F \perp (f_2) \Rightarrow (f_1) = (f_2)$. Logo $z = 0$ e, assim, $\hat{r}^*$ é injetora.

□

Corolário 1.4.23. *Seja K/F extensão de grau ímpar. Então $\hat{r}^*$ é um monomorfismo.*

Demonstração. Como $K = F(\alpha_1, ..., \alpha_l)$, basta aplicar o resultado l vezes. □

Capítulo 2

O Teorema da Base Normal

Este capítulo nos dá um resultado fundamental para obtermos uma demonstração simples do Teorema 3.1.1.

Desejamos demonstrar o seguinte teorema:

Teorema 2.1.1. *Toda extensão L/K Galoisiana finita possui base normal.*

Ao longo de todo o capítulo apresentaremos resultados necessários para alcançarmos nosso objetivo. Este teorema é pouco abordado na literatura usual, sendo quase sempre remetido ao caso em que o corpo K é infinito. Ao final deste capítulo será apresentado ao leitor a demonstração em sua totalidade, ou seja, tanto para K infinito como para K finito.

Começaremos com o seguinte lema:

Lema 2.1.2. *Uma matriz $P \in M_n(K[X])$ é invertível se e somente se $det(P)$ é um escalar não nulo em K.*

Demonstração. ($\Rightarrow$) Se P é invertível, $det(P)det(P^{-1}) = det(PP^{-1}) = det(I_n) = 1$, ou seja, $det(P)$ é invertível em $K[X]$. Como os únicos elementos invertíveis em $K[X]$ são elementos de $K\backslash\{0\}$, então $det(P) \in K\backslash\{0\}$.

($\Leftarrow$) Lembre que a matriz adjunta a P, dada por $P' = ((-1)^{i+j} det(P(j|i)))$, onde $P(j|i)$ é a matriz $(n-1) \times (n-1)$ obtida de P tirando-se a j-ésima linha e a i-ésima coluna, é tal que $PP' = det(P)I$. Ora, se $det(P) \in K\backslash\{0\}$, então $P^{-1} = det(P)^{-1}P'$ é a inversa de P. □

O lema seguinte é de vital importância para a nossa construção. Entretanto optamos por omitir sua demonstração a fim de não tornarmos o texto excessivamente volumoso. Sua demonstração pode ser vista em [4], página 257, Teorema 9.

Lema 2.1.3. *Seja $M \in M_n(K[X])$. Então existem $d_1(X), d_2(X), ..., d_s(X)$ não nulos em $K[X]$, com $d_i(X)|d_j(X)$ para $1 \leq i \leq j \leq s$ tais que M é equivalente a $diag\{1, ..., 1, d_1(X), d_2(X), ..., d_s(X)\}$. Ou seja, existem P e Q invertíveis em $M_n(K[X])$ tais que $PMQ = diag\{1, ..., 1, d_1(X), d_2(X), ..., d_s(X)\}$*

Repare que, como K é corpo, os polinômios $d_1(X), d_2(X), ..., d_s(X)$ podem ser tomados mônicos sem perda de generalidade.

Definição 2.1.4. *Seja A um anel. Um A-módulo livre é um módulo que possui uma base, ou seja, um conjunto gerador linearmente independente sobre A.*

Sejam K um corpo e V um K-espaço vetorial. Considere $End_K(V)$ a K - álgebra de todos os operadores lineares $T : V \longrightarrow V$.

Teorema 2.1.5. *Se V tem dimensão finita, então todo operador linear $T : V \longrightarrow V$ determina uma estrutura de $K[X]$ - módulo sobre V e polinômios mônicos $d_1(X)$ ... $d_s(X)$ tais que:*

(i) $V \simeq \frac{K[X]}{<d_1(X)>} \oplus ... \oplus \frac{K[X]}{<d_s(X)>}$ *como $K[X]$-módulos.*

(ii) $d_i(X)|d_j(X)$ *para* $1 \leq i \leq j \leq s$.

(iii) $d_1(X)d_2(X)\ldots d_s(X)$ *é o polinômio característico de T.*

(iv) $d_s(X)$ *é o polinômio minimal de* T.

Demonstração. Seja

$$\begin{array}{rccc} \varphi: & K[X] & \longrightarrow & End_K(V) \\ & f(X) & \longrightarrow & f(T) \qquad (T \text{ fixo}) \\ & \sum_{i=0}^{m} a_i X^i & \longrightarrow & a_0 I + \sum_{i=1}^{m} a_i T^i \end{array}$$

trivialmente homomorfismo de K-álgebras.

Assim, T determina em V uma estrutura de $K[X]$-módulo da seguinte forma:

$$f(X)v = \varphi(f(X))(v) = a_0 v + \sum_{i=1}^{m} a_i T^i(v) \in V,$$

com $f(X) \in K[X]$ e $v \in V$.

Vamos denotar por $A = [T]$ a matriz quadrada que representa o operador T e supor $n = dim_K(V)$.

Usando o Lema 2.1.3, existem $d_1(X), ..., d_s(X) \in K[X]$ tais que

$$XI_n - A \sim diag\{1, ..., 1, d_1(X), ...d_s(X)\}$$

Desta forma, obtemos matrizes P e Q com determinantes em K tais que

$$P(XI_n - A)Q = diag\{1, ..., 1, d_1(X), ...d_s(X)\} \tag{2.1}$$

Logo $det(P)det(XI_n - A)det(Q) = det(diag\{1, ..., 1, d_1(X), ...d_s(X)\})$ e como os polinômios $det(XI_n - A)$ e $det(diag\{1, ..., 1, d_1(X), ...d_s(X)\})$ são mônicos, devemos ter $det(P)det(Q) = 1$. Assim

$$det(XI_n - A) = \prod_{i=1}^{s} d_i(X)$$

valendo assim os ítens (ii) pelo Lema 2.1.3 e (iii). □

Antes de prosseguirmos na demonstração, precisamos de alguns resultados. Considere, então, $\{v_1, ..., v_n\}$ base de V sobre K.

Logo

$$V = Kv_1 \oplus ... \oplus Kv_n \subset K[X]v_1 + ... + K[X]v_n \subset V$$

Desta forma $V = K[X]v_1 + ... + K[X]v_n$ e logo $\{v_1, ..., v_n\}$ gera V como $K[X]$-módulo.

Fixemos para o que segue $T(v_i) = \sum_{j=1}^{n} a_{ij}v_j$ de modo que a matriz de T nesta base é dada por $A = (a_{ij})$.

Defina $K[X]^n = K[X] \times K[X] \times ... \times K[X]$ e

$$\psi : \quad K[X]^n \quad \longrightarrow \quad V$$

aplicação $K[X]$ - linear (V com a estrutura de $K[X]$-módulo determinada por T) induzida por :

$$e_i \longrightarrow v_i \forall\ i = 1, ..., n$$

com e_i o vetor em $K[X]^n$ que tem 1 na posição i e zero em todas as outras. Em outras palavras, se $z \in K[X]^n$, digamos $z = \sum_{i=1}^{n} g_i(X)e_i$, então $\psi(z) = \sum_{i=1}^{n} g_i(X)v_i$.

Lema 2.1.6. *O conjunto* $\beta = \{f_i \in K[X]^n \mid i = 1, ..., n\}$ *com* $f_i = Xe_i - \sum_{j=1}^{n} a_{ij}e_j$ *é uma base para* $N = ker(\psi)$ *sobre* $K[X]$.

Demonstração.

(I) $f_i \in N$ para todo $i \in \{1, ..., n\}$:

$\psi(f_i) = \psi(Xe_i - \sum_{j=1}^{n} a_{ij}e_j) = Xv_i - \sum_{j=1}^{n} a_{ij}v_j = T(v_i) - T(v_i) = 0.$

Ou seja, $f_i \in N$ para todo $i = 1, ..., n$, como queríamos.

(II) β gera N sobre $K[X]$:

Seja $z \in N$. Digamos $z = \sum_{i=1}^{n} g_i(X)e_i$ e $\psi(z) = 0$.

Mas $Xe_i = f_i + \sum_{j=1}^{n} a_{ij}e_j$, então existem $h_i(X) \in K[X]$ e $b_i \in K$ tais que

$$z = \sum_{i=1}^{n} g_i(X)e_i = \sum_{i=1}^{n} h_i(X)f_i + \sum_{i=1}^{n} b_i e_i$$

Assim $0 = \psi(z) = \sum_{i=1}^{n} h_i(X)\psi(f_i) + \psi(\sum_{i=1}^{n} b_i e_i) = \sum_{i=1}^{n} b_i v_i$

Mas, como $\{v_1, ..., v_n\}$ é base de V sobre K, $b_i = 0 \ \forall \ i = 1, ...n$ e assim temos $z = \sum_{i=1}^{n} h_i(X)f_i$, valendo (II).

(III) β é um conjunto linearmente independente:

Se $\sum_{i=1}^{n} g_i(X)f_i = 0$, então $\sum_{i=1}^{n} g_i(X)Xe_i = \sum_{i=1}^{n} (\sum_{j=1}^{n} g_i(X)a_{ij})e_j = \sum_{i=1}^{n} (\sum_{j=1}^{n} g_j(X)a_{ji})e_i$.

Pela independencia linear dos e_i, $g_i(X)X = \sum_{j=1}^{n} g_j(X)a_{ji}$ para todo $i = 1, ..., n$.

Suponha que exista $g_i(X) \neq 0$ e considere r inteiro tal que $1 \leq r \leq n$ e $deg(g_r(X)) \geq deg(g_i(X)) \ \forall \ i = 1, ..., n$.

Mas $g_r(X)X = \sum_{j=1}^{n} g_j(X)a_{jr}$, logo

$$\begin{aligned} deg(g_r(X)) + 1 &= deg(g_r(X)X) \\ &= deg(\sum_{j=1}^{n} g_j(X)a_{jr}) \\ &\leq max_{i=1,...,n}(deg(g_i(X))) \\ &= deg(g_r(X)) \end{aligned}$$

o que é absurdo.

Logo $g_i(X) = 0$ para todo $i = 1, ..., n$ e consequentemente β é base de $ker(\psi)$ sobre $K[X]$. □

Agora podemos voltar ao Teorema 2.1.5.

Demonstração. Considere P e Q matrizes associadas a um operador T como em 2.1 e chame $Q^{-1} = [q_{ij}]$ e $P = [p_{ij}]$ as matrizes em $M_n(K[X])$.

Defina para todo $i = 1, ..., n$

$$\begin{aligned} v'_i &= \sum_{j=1}^{n} q_{ij} v_j \\ e'_i &= \sum_{j=1}^{n} q_{ij} e_j \\ f'_i &= \sum_{j=1}^{n} p_{ij} f_j \end{aligned}$$

Ora, temos

$$\begin{pmatrix} f'_1 \\ \vdots \\ f'_n \end{pmatrix} = P \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = P(XI_n - A) \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = P(XI_n - A)Q \begin{pmatrix} e'_1 \\ \vdots \\ e'_n \end{pmatrix}$$

$$= diag\{1, ..., 1, d_1(X), ..., d_s(X)\} \begin{pmatrix} e'_1 \\ \vdots \\ e'_n \end{pmatrix}$$

Logo

$$\begin{aligned} f'_1 &= e'_1 \\ f'_2 &= e'_2 \\ &\vdots \\ f'_{n-s} &= e'_{n-s} \\ f'_{n-s+1} &= d_1(X) e'_{n-s+1} \\ &\vdots \\ f'_n &= d_s(X) e'_n \end{aligned} \tag{2.2}$$

E,

$$\psi(e'_i) = \psi(\sum_{j=1}^{n} q_{ij} e_j) = \sum_{j=1}^{n} q_{ij} v_j = v'_i \tag{2.3}$$

E assim concluímos que

$$\begin{aligned} 0 &= \psi(f_i') = \psi(e_i') = v_i' \ \forall\ 1 \leq i \leq n-s \\ 0 &= \psi(f_{n-s+i}') = \psi(d_i(X)e_{n-s+i}') = d_i(X)v_{n-s+i}' \ \forall\ 1 \leq i \leq s \end{aligned} \tag{2.4}$$

Mas $\begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = Q \begin{pmatrix} v_1' \\ \vdots \\ v_n' \end{pmatrix}$ implica $V = K[X]v_1' + ... + K[X]v_n'$.

Como $v_1' = ... = v_{n-s}' = 0$, temos $V = K[X]v_{n-s+1}' + ... + K[X]v_n'$. Para facilitar escreva $u_i = v_{n-s+i}'$ para $1 \leq i \leq s$.

Mostremos que essa soma é direta.

Seja $\sum_{i=1}^{s} h_i(X)u_i = 0$.

Temos $0 = \sum_{i=1}^{s} h_i(X)v_{n-s+i}' \overset{2.3}{=} \sum_{i=1}^{s} h_i(X)\psi(e_{n-s+i}') = \psi(\sum_{i=1}^{s} h_i(X)e_{n-s+i}')$.

Logo $\sum_{i=1}^{s} h_i(X)e_{n-s+i}' \in N$ e, assim,

$$\sum_{i=1}^{s} h_i(X)e_{n-s+i}' = \sum_{i=1}^{n} g_i(X)f_i' \overset{2.2}{=} \sum_{i=1}^{n-s} g_i(X)e_i' + \sum_{i=1}^{s} g_{n-s+i}(X)d_i(X)e_{n-s+i}'$$

Claramente o conjunto $\{e_i' | 1 \leq i \leq n\}$ é linearmente independente sobre $K[X]$ pois $\{e_i | 1 \leq i \leq n\}$ o é e Q é invertível.

Desta forma

$$\begin{aligned} g_i(X) &= 0 && \forall\ 1 \leq i \leq n-s \\ g_{n-s+i}(X)d_i(X) &= h_{n-s+i}(X) && \forall\ 1 \leq i \leq s \end{aligned}$$

Assim, para $1 \leq i \leq s$

$$h_{n-s+i}(X)u_i = g_{n-s+i}(X)d_i(X)u_i = g_{n-s+i}(X)d_i(X)v_{n-s+i}' \overset{2.4}{=} 0$$

Logo $V = K[X]u_1 \oplus ... \oplus K[X]u_s$

Repare agora que, para cada i, a aplicação

$$\begin{aligned} \rho_i : \quad K[X] &\longrightarrow K[X]u_i \\ f(X) &\longrightarrow f(X)u_i = f(T)u_i \end{aligned}$$

é um $K[X]$ - homomorfismo sobrejetor de anéis que tem como núcleo o conjunto $ker\rho_i = \{f(X)|f(T)u_i = 0\}$.

Pelo Teorema do Isomorfismo, $\frac{K[X]}{ker\rho_i} \simeq K[X]u_i$.

Afirmação: $ker\rho_i =< d_i(X) >$, onde $< d_i(X) >$ é o gerado por $d_i(X)$ sobre $K[X]$.

De fato: Por 2.4, $0 = d_i(X)v'_{n-s+i} = d_i(X)u_i$, temos que $\rho_i(g(X)d_i(X)) = g(X)d_i(X)u_i = 0$ com $g_i(X) \in K[X]$.

Assim, $ker\rho_i \supset< d_i(X) >$

Reciprocamente, seja $h(X) \in ker\rho_i$

Então $0 = \rho_i h(X) = h(X)u_i = h(X)v'_{n-s+i} = \psi(h(X)e'_{n-s+i})$.

Segue que

$$h(X)e'_{n-s+i} \overset{2.1.6}{=} \sum_{j=1}^{n} g_j(X)f_j \overset{2.2}{=} \sum_{j=1}^{n-s} g_j(X)e'_j + \sum_{j=1}^{s} g_{n-s+j}(X)d_j(X)e'_{n-s+j}$$

Pela independência linear do conjunto $\{e'_j|1 \leq j \leq n\}$,

$$h(X) = g_{n-s+i}(X)d_i(X) \in< d_i(X) >$$

Logo $ker\rho_i \subset< d_i(X) >$, valendo então a igualdade.

Desta forma temos $\frac{K[X]}{<d_i(X)>} \simeq K[X]u_i$ para todo inteiro i tal que $1 \leq i \leq s$.

Ou seja,

$$V \simeq \frac{K[X]}{< d_1(X) >} \oplus \frac{K[X]}{< d_2(X) >} \oplus ... \oplus \frac{K[X]}{< d_s(X) >}$$

ficando assim demonstrado o ítem (i) do Teorema 2.1.5.

Resta-nos somente mostar o ítem (iv).

Primeiramente mostremos que $d_s(T) = 0$.

Como $d_i(X)|d_s(X)$, então $d_s(X) = h_i(X)d_i(X)$ com $h_i(X) \in K[X]$.

Logo $d_s(X)u_i = h_i(X)d_i(X)u_i = h_i(T)d_i(T)u_i = 0$ pois $< d_i(X) >= ker\rho_i$.

E como $u_1, ..., u_n$ é base de V sobre $K[X]$, $d_s(X)v = 0$ para todo $v \in V$, sendo assim $d_s(T) = 0$.

Seja, agora, $g(X) \in K[X]$ mônico tal que $g(T) = 0$. Temos $g(T)v = 0$ para todo $v \in V$, em particular $g(T)u_s = 0$.

Assim $g(X) \in ker\rho_s =< d_s(X) >$. Desta forma existe $h(X) \in K[X]$ tal que $g(X) = d_s(X)h(X)$, o que nos diz que $deg(g(X)) \geq deg(d_s(X))$.

Se vale a desigualdade estrita nada se tem a fazer.

Se vale a igualdade, então $h(X)$ é constante igual a 1 pois $g(X)$ e $d_s(X)$ são mônicos.

Logo $g(X) = d_s(X)$.

Ficando assim provado na íntegra o Teorema 2.1.5.

□

Antes de introduzirmos o próximo teorema, faremos uma breve observação.

Observação 2.1.7. *A aplicação*

$$\begin{array}{rccc} \varphi: & \mathbb{Z} & \longrightarrow & K \\ & n & \longmapsto & n \cdot 1_K \end{array}$$

é claramente um homomorfismo de anéis.

Logo, como K é corpo, $ker\varphi$ é um ideal maximal em $\mathbb{Z}$, ou seja, $ker(\varphi) = 0$ ou $ker(\varphi) = p\mathbb{Z}$ para algum p primo. Então, se a característica de K for zero,

$ker(\varphi) = 0$ e K contém uma cópia de $\mathbb{Q}$ pois φ é injetora. Se a característica de K for p, $ker(\varphi) = p$ e K contém uma cópia de $\mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$.

Agora podemos passar ao seguinte teorema:

Teorema 2.1.8. *Seja K corpo finito, com $c(K) = p$ e $\#K = p^n$. Então K é corpo de raízes de $X^{p^n} - X$ sobre $\mathbb{F}_p$.*

Demonstração. Sejam $a_0 = 0, ..., a_{p^n-1}$ todos os elementos de K. Então K^* tem ordem $p^n - 1$, ou seja, $a_i^{p^n-1} = 1$ implica $a_i^{p^n} = a_i$ para todo $i = 1, ..., p^n - 1$. Claramente $a_0^{p^n-1} = 0 = a_0$.

Assim temos p^n raízes distintas de $X^{p^n} - X$, o qual tem, no máximo, p^n raízes.

Ora, todo elemento de K é raiz de $X^{p^n} - X$ e toda raiz de $X^{p^n} - X$ é elemento de K. Em outras palavras, K é a menor extensão de $\mathbb{F}_p$ que contém todas as raízes de $X^{p^n} - X$.

□

Temos então que $K/\mathbb{F}_p$ é extensão de Galois.

Definição 2.1.9. *Uma extensão Galoisiana K/F é dita cíclica se o grupo $Aut_F(K)$ é cíclico.*

Teorema 2.1.10. *Seja K um corpo finito de característica p. Então $K/\mathbb{F}_p$ é uma extensão cíclica com $Aut_{\mathbb{F}_p}(K) =< \sigma >$, sendo*

$$\begin{array}{rccc} \sigma : & K & \longrightarrow & K \\ & x & \longrightarrow & x^p \end{array}$$

Demonstração. Estamos supondo $c(K) = p$. Repare que o polinômio $X^{p^n} - X$ é separável. Como K é corpo de raízes deste, temos $K/\mathbb{F}_p$ extensão Galoisiana. Desta forma $|Aut_{\mathbb{F}_p}(K)| = [K : \mathbb{F}_p] = n$.

(I) $\sigma : K \longrightarrow K$ é $\mathbb{F}_p$ - homomorfismo:

Veja que, pelo Teorema Binomial,

$$(x+y)^p = x^p + y^p + \sum_{i=1}^{p-1} \binom{p}{i} x^i y^{p-i}$$

Mostremos, então, que p divide $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ para $1 < i < p$.

De fato, $\binom{p}{i} = \frac{p!}{i!(p-i)!} = p\frac{(p-1)!}{i!(p-i!)} = \frac{p}{p-i}\frac{(p-1)!}{i!(p-1-i!)} = \frac{p}{p-i}\binom{p-1}{i}$. Como $\binom{p}{i}$ é inteiro (pois os coeficiente binomiais são inteiros) e p é primo, $p-i$ divide $\binom{p-1}{i}$.

Logo $\binom{p}{i} = pm$, para algum $m \in \mathbb{N}$ e $1 < i < p$.

Assim ficamos com $(x+y)^p = x^p + y^p$, pois $c(K) = p$.

Repare que $1^p = 1$ e $(xy)^p = x^p y^p$ trivialmente.

Desta forma fica demonstrado que σ é homomorfismo.

Como $\mathbb{F}_p$ tem p elementos, $x^p = x$ para todo $x \in \mathbb{F}_p$.

Logo σ é $\mathbb{F}_p$ -homomorfismo.

(II) σ é isomorfismo:

Basta mostrar a injetividade pois K é um conjunto finito.

Se $x^p = y^p$, então $(x-y)^p = x^p - y^p = 0$. Logo $x - y = 0$ e assim $x = y$.

Desta forma $\sigma \in Aut_{\mathbb{F}_p}(K)$.

(III) $Aut_{\mathbb{F}_p}(K) =< \sigma >$:

Para isto basta mostrar que a ordem de σ é n, pois $Aut_{\mathbb{F}_p}(K) \supseteq < \sigma >$.

Suponha então que m seja o menor inteiro tal que $\sigma^m = Id_K$. Observe que m existe pois, como $Aut_{\mathbb{F}_p}(K)$ é grupo finito, $\sigma^{n+1} = \sigma^l$ para algum l entre 1 e n. Logo $\sigma^{n+1-l} = Id_K$.

Mas $\sigma^n(x) = x^{p^n} = x$, ou seja, $\sigma^n = Id_K$. Como estamos supondo m a ordem de σ, então $m \leq n$.

Veja que $x = \sigma^m(x) = x^{p^m}$ para todo x em K. Sendo assim, todo elemento de K é raiz do polinômio $X^{p^m} - X$.

Assim $X^{p^m} - X$ tem no mínimo $\#(K) = p^n$ raízes, ou seja, $deg(X^{p^m} - X) \geq p^n$.

Então $p^m = deg(X^{p^m} - X) \geq p^n$. Logo $m \geq n$, valendo assim a igualdade.

Assim $|Aut_{\mathbb{F}_p}(K)| = | < \sigma > |$ e portanto $Aut_{\mathbb{F}_p}(K) =< \sigma >$.

□

Para não sobrecarregar a escrita, no próximo teorema vamos entender uma imersão de L em N como um K - homomorfismo injetor de L em N.

Teorema 2.1.11. *Seja L/K extensão separável finita e N o fecho normal de L sobre K. Então,*

(i) O número de imersões de L em N é $n = [L : K]$

(ii) Sendo $\sigma_1 = Id_L, \sigma_2, ..., \sigma_n$ as n imersões, o conjunto $\{u_1, ..., u_n\} \subset L$ é base para L/K se, e somente se, $\begin{vmatrix} u_1 & u_2 & ... & u_n \\ \sigma_2(u_1) & \sigma_2(u_2) & ... & \sigma_2(u_n) \\ \vdots & \vdots & & \vdots \\ \sigma_n(u_1) & \sigma_n(u_2) & ... & \sigma_n(u_n) \end{vmatrix} \neq 0$.

Demonstração.

(i) Veja que N/K é Galois pois N é corpo de raízes de um polinômio separável. Como L/K é separável, $[L : K]_s = [L : K]$. Do Teorema 1.2.2 temos que o número de imersões de L em N é exatamente $[L : K]_s = [L : K]$.

(ii) ($\Leftarrow$) Suponha que $\{u_1, ..., u_n\}$ não seja base de L/K. Como $n = [L : K]$, então

o conjunto é linearmente dependente.

Assim existem $a_1, ...a_n \in K$ não todos nulos tais que $\sum_{i=1}^{n} a_i u_i = 0$.

Logo $\sum_{i=1}^{n} a_i \sigma_j(u_i) = \sigma_j(\sum_{i=1}^{n} a_i u_i) = \sigma_j(0) = 0 \ \forall \ j = 1, ..., n$.

Desta forma, o sistema

$$\begin{cases} \sum_{i=1}^{n} x_i u_i & = & 0 \\ \sum_{i=1}^{n} x_i \sigma_2(u_i) & = & 0 \\ & \vdots & \\ \sum_{i=1}^{n} x_i \sigma_n(u_i) & = & 0 \end{cases}$$

tem a solução $\{a_1, ..., a_n\}$ não trivial.

Logo $det((\sigma_j(u_i))_{i,j}) = 0$. Por contraposição vale o resultado.

($\Rightarrow$) Se $det((\sigma_j(u_i))_{i,j}) = 0$, então $det((\sigma_i(u_j))_{i,j}) = 0$.

Logo o sistema

$$\begin{cases} \sum_{i=1}^{n} x_i \sigma_i(u_1) & = & 0 \\ \sum_{i=1}^{n} x_i \sigma_i(u_2) & = & 0 \\ & \vdots & \\ \sum_{i=1}^{n} x_i \sigma_i(u_n) & = & 0 \end{cases}$$

tem solução não trivial, digamos $\{a_1, ..., a_n\}$. Ou seja, $\sum_{i=1}^{n} a_i \sigma_i(u_j) = 0 \ \forall \ j = 1, ..., n$.

Se $\{u_1, ..., u_n\}$ fosse base de L/K, dado $u \in L$ teríamos $u = \sum_{i=1}^{n} c_i u_i$, com $c_i \in K$.

Logo $\sum_{j=1}^{n} a_j \sigma_j(u) = \sum_{i=1}^{n} \sum_{j=1}^{n} a_j c_i \sigma_j(u_i) = \sum_{i=1}^{n} c_i \sum_{j=1}^{n} a_j \sigma_j(u_i) = \sum_{i=1}^{n} c_i 0 = 0$

Assim $\sum_{i=1}^{n} a_i \sigma_i = 0$ com $a_1, ..., a_n$ não todos nulos, o que contradiz o Teorema 1.1.6.

Logo $\{u_1, ..., u_n\}$ não pode ser base de L/K. Por contraposição obtemos o

resultado.

□

Teorema 2.1.12. *Se K é um corpo infinito e $p(X_1, ..., X_r)$ é um polinômio não nulo em $K[X_1, ..., X_r]$, então existem $a_1, ..., a_r$ em K tais que $p(a_1, ..., a_r) \neq 0$.*

Demonstração. Usaremos indução sobre r.

Se $r = 1$, $p(X)$ possui $deg(p(X)) < \infty$ raízes. Desde que K é corpo infinito, existe $a \in K$ tal que $p(a) \neq 0$.

Suponha $r > 1$ e que o resultado seja válido para $r - 1$.

Vamos escrever $p(X_1, ..., X_r) = \sum_{i=0}^{n} p_i(X_1, ..., X_{r-1}) X_r^i$.

Como $p(X_1, ..., X_r)$ é um polinômio não-nulo, algum $p_j(X_1, ..., X_{r-1})$ é não nulo.

Segundo nossa hipótese de indução, existem $a_1, ..., a_{r-1} \in K$ de forma que $p_j(a_1, ..., a_{r-1}) \neq 0$.

Defina $g(X_r) = \sum_{i=0}^{n} p_i(a_1, ..., a_{r-1}) X_r^i \in K[X_r]$. Veja que $g(X_r) \neq 0$ pois temos $p_j(a_1, ..., a_{r-1}) \neq 0$.

Como $g(X_r)$ é em uma variável, existe $a_r \in K$ tal que $g(a_r) \neq 0$.

Assim, $p(a_1, ..., a_r) = g(a_r) \neq 0$, valendo o resultado.

□

Observação 2.1.13. *Repare que, apesar da aparente trivialidade do teorema anterior, o fato de K ser infinito é fundamental. Por exemplo, se K for um corpo finito tal que $c(K) = p$ e $\#K = p^e$, o polinômio $f(X) = X^{p^e} - X$ é um polinômio não-nulo em $K[X]$ com $f(a) = 0$ para todo $a \in K$.*

Definição 2.1.14. *Sejam K e L corpos e $\sigma_1, ..., \sigma_n$ imersões de K em L. Dizemos que essas imersões são algebricamente independentes sobre L se $p(X_1, ..., X_n) = 0$*

é o único polinômio em $L[X_1, ..., X_n]$ *que satisfaz* $p(\sigma_1(u), ..., \sigma_n(u)) = 0$ *para todo* $u \in K$.

Teorema 2.1.15. *Seja* K *corpo infinito,* L/K *extensão separável finita e* N *fecho normal de* L/K. *Se* $\sigma_1, \sigma_2, ..., \sigma_n$ *são as* $[L : K] = n$ K*-imersões de* L *em* N, *então os* σ_i*'s são algebricamente independentes sobre* N.

Demonstração. Considere o polinômio $p(X_1, ..., X_n) \in N[X_1, ..., X_n]$ de forma que $p(\sigma_1(u), ..., \sigma_n(u)) = 0$ para todo $u \in L$.

Tome $\{u_1, ..., u_n\}$ base de L/K.

Então para todo $a_1, ..., a_n \in K$,

$$0 = p(\sigma_1(\sum_{i=1}^{n} a_i u_i), ..., \sigma_n(\sum_{i=1}^{n} a_i u_i)) = p(\sum_{i=1}^{n} a_i \sigma_1(u_i), ..., \sum_{i=1}^{n} a_i \sigma_n(u_i))$$

Defina $g(X_1, ..., X_n) \in N[X_1, ..., X_n]$ da seguinte forma:

$$g(X_1, ..., X_n) = p(\sum_{i=1}^{n} X_i \sigma_1(u_i), ..., \sum_{i=1}^{n} X_i \sigma_n(u_i))$$

Ora, para todo $a_1, ..., a_n \in K$, $g(a_1, ..., a_n) = 0$.

Seja $\{v_1, ..., v_m\}$ base de N/K. Temos $g(X_1, ..., X_n) = \sum_{j=1}^{m} g_j(X_1, ..., X_n) v_j$ com $g_j(X_1, ..., X_n) \in K$.

Assim, $g_j(a_1, ..., a_n) = 0$ para todo $1 \leq j \leq m$ e para todo $a_1, ..., a_n \in K$ pois $\{v_1, ..., v_m\}$ é base de N/K.

Mas K é infinito. Então, pelo Teorema 2.1.12, só podemos ter $g_j(X_1, ..., X_n) = 0 \ \forall \ 1 \leq j \leq m$.

Logo $g(X_1, ..., X_n) = 0$.

Pelo Teorema 2.1.11 (ii), $det([\sigma_j(u_i)_{ij}]) \neq 0$ pois $\{u_1, ..., u_n\}$ é base de L/K.

Considere, então, A a matriz inversa de $[\sigma_j(u_i)_{ij}]$.

$$\text{Logo } 0 = g(A\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}) = p([\sigma_j(u_i)_{i,j}]A\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix}) = p(X_1, ..., X_n).$$

Assim, $\sigma_1, ..., \sigma_n$ são algebricamente independentes sobre N.

□

Definição 2.1.16. *Seja K um corpo. Dizemos que uma extensão finita L/K possui base normal se existe $u \in L$ tal que $\{\sigma(u)|\sigma \in Aut_K(L)\}$ é base de L sobre K.*

Agora temos ferramentas suficientes para demonstrar o Teorema 2.1.1, ou seja, demonstraremos que toda extensão Galoisiana L/K finita tem base normal.

Demonstração. Vamos analisar separadamente os casos K finito e K infinito.

(I) Caso K finito:

Temos L corpo finito de mesma característica de K, digamos p.

Observe que as extensões $L/\mathbb{F}_p$ e $K/\mathbb{F}_p$ são Galois, como visto no Teorema 2.1.10.

Pelo mesmo Teorema, $Aut_{\mathbb{F}_p}(L)$ é um grupo cíclico.

Desde que $\mathbb{F}_p \subset K \subset L$, temos claramente $Aut_K(L) \subset Aut_{\mathbb{F}_p}(L)$. Desta forma temos $Aut_K(L)$ grupo cíclico, suponha $Aut_K(L) =< \sigma >$.

Repare que da mesma forma como construimos a estrutura de $K[X]$ - módulo para K usando T, podemos construir uma estrutura de $K[X]$ - módulo para L usando σ.

Note que a ordem de σ é $[L : K]$ que chamaremos de n.

Como $\sigma^n = Id_L$, o polinômio $g(X) = X^n - 1 \in \mathbb{F}_p(X)$ é tal que $g(\sigma) = 0$.

Seja $m_\sigma(X)$ o polinômio minimal de σ. Chame $s = deg(m_\sigma(X))$. Queremos mostrar que $s = m$.

Pela definição de polinômio minimal, $s = deg(m_\sigma(X)) \leq deg(g(X)) = n$.

Suponha por absurdo que $s < n$. Escreva $m_\sigma(X) = X^s + a_{s-1}X^{s-1} + ... + a_1X + a_0$ e, assim, $\sigma^s + a_{s-1}\sigma^{s-1} + ... + a_1\sigma^1 + a_0\sigma^0 = 0$. Repare que $\sigma^i \neq \sigma^j$ para $i \neq j$ com $1 \leq i, j < n$ pois a ordem de σ é n.

Como o coeficiente de σ^s é não-nulo, conseguimos uma combinação linear nula de automorfismos distintos, contrariando o Teorema 1.1.6. Logo $s = n$.

De modo análogo ao feito no Teorema 2.1.5 ítem (iv), temos $m_\sigma(X)|g(X)$.

Como são ambos mônicos e de mesmo grau, $m_\sigma(X) = g(X) = X^n - 1$.

Seja $h(X) \in K[X]$ o polinômio característico de σ, então $m_\sigma(X)|h(X)$ e o grau $deg(h(X)) = [L : K] = n = deg(m_\sigma(X))$.

Logo $h(X) = m_\sigma(X) = X^n - 1$.

Pelo ítem (iii) do Teorema 2.1.5, $h(X) = d_1(X)d_2(X)....d_{s-1}(X)m_\sigma(X)$, fazendo com que $d_i(X) = 1$. Como $< 1 >= K[X]$, $\frac{K[X]}{<d_i(X)>} = 0$. Pelo ítem (i), $L \simeq \frac{K[X]}{<X^n-1>}$ como $K[X]$ - módulos. Chamaremos este isomorfismo de φ.

Assim $\overline{1} = 1 + < X^n - 1 >$. Desta forma todo elemento de $\frac{K[X]}{<X^n-1>}$ é da forma $f(X)\overline{1} = \overline{f(X)}$ com $deg(f(X)) < n$. Observe que se $deg(f(X)) \geq n$ podemos dividir $f(X)$ por $X^n - 1$ e obter a mesma classe com o polinômio resto.

Se $x \in L \Rightarrow \varphi(x) \in \frac{K[X]}{<X^n-1>} \Rightarrow \varphi(x) = \overline{f(X)}$ para algum $f(X) \in K[X]$.

Defina $\alpha = \varphi^{-1}((\overline{1}))$.

Ora, $\varphi(x) = f(X)\overline{1} = f(X)\varphi(\alpha) = \varphi(f(X)\alpha)$. Logo $x = f(X)\alpha = f(\sigma)\alpha$.

Como supomos $deg(f(X)) < n$, escreva $f(X) = \sum_{i=1}^{n-1} a_iX^i$.

Assim, $x = f(\sigma)\alpha = \sum_{i=1}^{n-1} a_i\sigma^i(\alpha)$

Ou seja, dado $x \in L$, existem $a_0, ..., a_{n-1} \in K$ tais que $x = \sum_{i=1}^{n-1} a_i\sigma^i(\alpha)$. Ora,

$\{\sigma^0(\alpha), \sigma^1(\alpha), ..., \sigma^{n-1}(\alpha)\}$ gera L/K e tem $[L : K]$ elementos, logo é uma base. Como $\{\sigma^0, ..., \sigma^{n-1}\}$ são todos os elementos de $Aut_K(L)$, a base acima é normal.

(II) Caso K infinito:

Seja $Aut_K(L) = \{\sigma_1, ..., \sigma_n\}$. Como L/K é normal, L é seu próprio fecho normal e, assim, pelo Teorema 2.1.15, $\sigma_1, ..., \sigma_n$ são algebricamente independentes sobre L.

Agora, para algum $u \in L$, $\{\sigma_1(u), ..., \sigma_n(u)\}$ é base de L/K se, e somente se, $det([\sigma_i\sigma_j(u)]_{i,j}) \neq 0$ pelo Teorema 2.1.11 parte (ii).

Mostremos, então, que existe $u \in L$ com $det([\sigma_i\sigma_j(u)]_{i,j}) \neq 0$.

Fixando-se i e variando j, temos que $\sigma_i\sigma_j$ percorre $Aut_K(L)$.

Assim, obtemos uma permutação $j \mapsto i(j)$ para todo i fixo com $1 \leq i \leq n$.

Considere a matriz $A = [X_{i(j)}]_{i,j}$ e o polinômio $d(X_1, ..., X_n) := det(A)$. Observe que $A \in M_n(L[X_1, ..., X_n])$.

Note que $d(X_1, ..., X_n) \neq 0$ pois, como cada X_j aparece uma única vez em cada linha de A, $d(1, 0, ..., 0) = \pm 1$.

Ora, $\sigma_1, ..., \sigma_n$ são algebricamente independentes e $d(X_1, ..., X_n) \neq 0$, existe u em L tal que

$$d(\sigma_1(u), ..., \sigma_n(u)) \neq 0$$

Logo $det([\sigma_i\sigma_j(u)]_{i,j}) = det([\sigma_{i(j)}(u)]_{i,j}) = d(\sigma_1(u), ..., \sigma_n(u)) \neq 0$.

Assim $\{\sigma_1(u), ..., \sigma_n(u)\}$ é base normal de L/K.

□

Capítulo 3

Estruturas de Módulos

Neste capítulo aplicamos grande parte do tema abordado ao longo dos capítulos anteriores.

3.1 Estrutura de $K[G]$-módulo de uma extensão finita de corpos

Seja L/K uma extensão finita e G um subgrupo finito de $Aut_K(L)$. Considere o conjunto $K[G] = \{\sum_{\sigma \in G} a_\sigma \sigma | a_\sigma \in K\}$. Observe que $K[G]$ é um K-espaço vetorial com base G. $K[G]$ também é um anel com a multiplicação dada por $(a\sigma)(b\tau) = (ab)(\sigma\tau)$ e possui a unidade Id_L. Note ainda que L tem uma estrutura de $K[G]$-módulo à esquerda via a seguinte ação: se $a\sigma \in K[G]$ e $l \in L$, $a\sigma \cdot l = a\sigma(l) \in L$. A partir de agora, quando falarmos em um A-módulo para algum anel A, estaremos nos referindo a um A-módulo à esquerda.

Recorde que se $G = Aut_K(L)$ e $|G| = [L : K] = n$, do Teorema 1.1.27 temos que L/K é extensão de Galois. Pelo Teorema da Base Normal (2.1.1), existe $w \in L$ tal que $\{\sigma_1(w), ..., \sigma_n(w)\}$ é base de L sobre K e por conseguinte L é um $K[G]$-módulo

livre com o gerador $\{w\}$.

Assim, se L/K é extensão Galoisiana finita e $G = Aut_K(L)$, então L é um $K[G]$-módulo livre com 1 gerador.

Mais geralmente temos o seguinte teorema:

Teorema 3.1.1. *Se L/K é uma extensão finita e G é subgrupo de $Aut_K(L)$, então L é um $K[G]$-módulo livre com $[L^G : K]$ geradores.*

Demonstração. Veja que $G = Aut_{L^G}(L)$ pois $G \subset Aut_{L^G}(L)$ e, como $L^G = L^{Aut_{L^G}(L)}$ então $|G| = [L : L^G] = [L : L^{Aut_{L^G}(L)}] = |Aut_{L^G}(L)|$. Assim L/L^G é Galois.

Como vimos, L é um $L^G[G]$-módulo livre com um gerador, digamos w.

Sejam $\beta = \{b_1, ..., b_r\}$ base de L^G/K como espaço vetorial ($r = [L^G : K]$) e $\beta_w = \{b_{i,w} = b_i w | i = 1, ..., r\}$ conjunto em L. Vamos mostrar que β_w é base de L sobre $K[G]$. De fato, mostremos primeiro que β_w gera L sobre $K[G]$:

Como $\beta \subset L^G$, temos que $\sigma(b_j) = b_j$ para todo $\sigma \in G$ e para todo $j = 1, ..., r$.

Seja $x \in L$. Ora, $x = gw$ para algum $g \in L^G[G]$.

Suponha $g = \sum_{i=1}^{m=|G|} a_{\sigma_i}\sigma_i$ com $a_{\sigma_i} \in L^G$ e $\sigma_i \in G$. Escreva $a_{\sigma_i} = \sum_{j=1}^{r} \alpha_{ij} b_j$, com $\alpha_{ij} \in K$.

Assim:

$$x = gw = \sum_{i=1}^{m} a_{\sigma_i}\sigma_i(w) = \sum_{i=1}^{m}\sum_{j=1}^{r} \alpha_{ij} b_j \sigma_i(w) = \sum_{j=1}^{r}\sum_{i=1}^{m} \alpha_{ij}\sigma_i(b_j w)$$

Defina $g_j = \sum_{i=1}^{m} \alpha_{ij}\sigma_i \in K[G]$. Logo $x = \sum_{j=1}^{r} (\sum_{i=1}^{m} \alpha_{ij}\sigma_i) b_{j,w} = \sum_{j=1}^{r} g_j b_{j,w}$.

Desde que $x \in L$ é qualquer, β_w gera L sobre $K[G]$.

Agora mostremos que β_w é um conjunto linearmente independente sobre $K[G]$:

De fato, suponhamos $\sum_{j=1}^{r} g_j b_{j,w} = 0$ com $g_j = \sum_{i=1}^{m} a_{ij}\sigma_i \in K[G]$. Então,

$$\sum_{j=1}^{r} g_j b_{j,w} = 0 \Leftrightarrow \sum_{i=1}^{m}\sum_{j=1}^{r} a_{ij}\sigma_i(b_j w) = 0 \Leftrightarrow \sum_{i=1}^{m}\sum_{j=1}^{r} a_{ij} b_j \sigma_i(w) = 0$$

Como $\{w\}$ é base de L sobre $L^G[G]$ e $a_{ij}b_j \in L^G$ para todo $i = 1, ..., m$ e $j = 1, ...r$, então

$$\sum_{i=i}^{m}\sum_{j=1}^{r} a_{ij} b_j \sigma_i = 0$$

Pelo Teorema 1.1.6,

$$\sum_{j=1}^{r} a_{ij} b_j = 0$$

para todo $i = 1, ..., m$.

Uma vez que $\{b_j | j = 1, ..., r\}$ é base de L^G sobre K, temos que $a_{ij} = 0$ para todo $i = 1, ..., m$ e $j = 1, ..., r$.

Assim $g_j = 0$ para todo $j = 1, ...m$. Ou seja, β_w é linearmente independente sobre $K[G]$ e consequentemente base.

Como β_w tem $r = [L^G : K]$ elementos, vale o teorema.

□

3.2 Outro olhar sobre o Teorema 3.1.1

Note que na demonstração do Teorema 3.1.1 foi de fundamental importância o Teorema da Base Normal. Nesta seção daremos uma nova demonstração para este mesmo teorema que será totalmente independente do Teorema da Base Normal.

Ao longo desta seção serão apresentados resultados que nos darão base tanto para redemonstrarmos o Teorema 3.1.1 como para fundamentarmos os resultados contidos no Capítulo 4.

Seja L/K uma extensão finita e consideremos K_1 a maior extensão separável de K contida em L, ou seja, $K_1 = L_{sep}$.

Proposição 3.2.1. *Os grupos $Aut_K(K_1)$ e $Aut_K(L)$ são isomorfos.*

Demonstração. Defina

$$\begin{array}{rccc} f: & Aut_K(L) & \longrightarrow & Aut_K(K_1) \\ & \sigma & \longmapsto & \sigma|_{K_1} \end{array}$$

que é claramente um homomorfismo de grupos.

Veja que se $C(K) = 0$, então L/K é separável e assim $L = K_1$. Vamos supor, então, $C(K) = p$.

(I) Mostremos que f é injetiva. De fato, se $f(\sigma) = f(\tau)$, então $\sigma|_{K_1} = \tau|_{K_1}$. Seja $\alpha \in L$, como L/K_1 é puramente inseparável, temos que existe e inteiro não negativo tal que $\alpha^{p^e} \in K_1$.

Logo $\sigma(\alpha)^{p^e} = \sigma(\alpha^{p^e}) = \tau(\alpha^{p^e}) = \tau(\alpha)^{p^e}$

Assim, $(\sigma(\alpha) - \tau(\alpha))^{p^e} = \sigma(\alpha)^{p^e} - \tau(\alpha)^{p^e} = 0$ o que implica $\sigma(\alpha) = \tau(\alpha)$ e, desde que α é qualquer, $\sigma = \tau$.

(II) Mostremos que f é sobrejetiva. De fato, seja $\rho \in Aut_K(K_1)$. Mostraremos que ρ é a restrição de um K-automorfismo de L

Veja que $L = K_1(\alpha_1, ..., \alpha_n)$ e que, para algum $n_1 \in \mathbb{N}$, $\{1, \alpha_1, ..., \alpha_1^{n_1}\}$ é base de $K_1(\alpha_1)/K_1$

Defina

$$\begin{array}{rccc} \sigma_1: & K_1(\alpha_1) & \longrightarrow & K_1(\alpha_1) \\ & \sum_{i=1}^{n_1} x_i \alpha_1^i & \longrightarrow & \sum_{i=1}^{n_1} \rho(x_i)\alpha_1^i \end{array}$$

Claramente $\sigma_1(x + y) = \sigma_1(x) + \sigma_1(y)$ para todo $x, y \in K_1(\alpha_1)$.

Ainda, para todo $x, y \in K_1(\alpha_1)$

$$\begin{aligned}\sigma_1(xy) &= \sigma_1((\sum_{i=1}^{n_1} x_i\alpha_1^i)(\sum_{j=1}^{n_1} y_j\alpha_1^j)) = \sigma_1(\sum_{i=1}^{n_1}\sum_{j=1}^{n_1} x_iy_j\alpha_1^{i+j}) \\ &= \sum_{i=1}^{n_1}\sum_{j=1}^{n_1}\rho(x_iy_j)\alpha_1^{i+j} = \sum_{i=1}^{n_1}\sum_{j=1}^{n_1}\rho(x_i)\rho(y_j)\alpha_1^{i+j} \\ &= \sum_{i=1}^{n_1}\rho(x_i)\alpha_1^i\sum_{j=1}^{n_1}\rho(y_j)\alpha_1^j = \sigma_1(x)\sigma_1(y)\end{aligned}$$

Ou seja, σ_1 preserva as operações do corpo $K_1(\alpha_1)$.

Desde que $\{1, \alpha_1, ..., \alpha_1^{n_1}\}$ é base, σ_1 é injetora e, como ρ é automorfismo de K_1, σ_1 é sobrejetora.

Assim $\sigma_1 \in Aut_K(K_1(\alpha_1))$ e $\sigma_1|_{K_1} = \rho$.

Tome $\{1, \alpha_2, ..., \alpha_2^{n_2}\}$ base de $K_1(\alpha_1, \alpha_2)/K_1(\alpha_1)$ e defina

$$\begin{array}{rccc}\sigma_2: & K_1(\alpha_1,\alpha_2) & \longrightarrow & K_1(\alpha_1,\alpha_2) \\ & \sum_{i=1}^{n_2} x_i\alpha_2^i & \longrightarrow & \sum_{i=1}^{n_2}\sigma_1(x_i)\alpha_2^i\end{array}$$

com $x_i \in K(\alpha_1)$.

De maneira análoga $\sigma_2 \in Aut_K(K_1(\alpha_1, \alpha_2))$ e $\sigma_2|_{K_1} = \rho$.

Podemos repetir esse processo e obter $\sigma_n : L \longrightarrow L$ automorfismo com $\sigma_n|_{K_1} = \rho$.

Ora, $f(\sigma_n) = \sigma_n|_{K_1} = \rho$ e, assim f é sobrejetora.

Logo f é isomorfismo entre $Aut_K(K_1)$ e $Aut_K(L)$.

□

Em face da Proposição 3.2.1 podemos abusar da notação e escrever G do Teorema 3.1.1 como subgrupo tanto de $Aut_K(K_1)$ quanto de $Aut_K(L)$.

Lema 3.2.2. *Sejam L/K extensão finita e G um subgrupo finito de $Aut_K(L)$. Existe uma base $\beta = \{\alpha_1, ..., \alpha_n\}$ para L/K_1 tal que $\alpha_i \in L^G$ para todo $i = 1, ..., n$.*

Demonstração. Primeiramente repare que, se uma extensão de corpos F''/F é puramente inseparável e existe um corpo F' tal que $F \subset F' \subset F''$, então F''/F' é puramente inseparável.

De fato, se $\alpha \in F''$, como F''/F é puramente inseparável, $m_{\alpha,F}(X) = (X-\alpha)^n$ é o minimal de α em F para algum n.

Então, o minimal de α em F', $m_{\alpha,F'}(X)$, divide $m_{\alpha,F}(X)$. Assim temos que $(X-\alpha)^n = m_{\alpha,F'}(X)p(X)$ para algum $p(X) \in F'[X]$.

Logo $m_{\alpha,F'}(X) = (X-\alpha)^m$ para algum m e, assim, como α é qualquer, F''/F' é puramente inseparável.

Com uma demonstração semelhante se conclui que se F''/F é uma extensão separável e $F \subset F' \subset F''$, então F''/F' é separável.

Mostremos, então, que $L = K_1L^G$

Repare que $L^G \subset K_1L^G \subset L$. Como L/L^G é Galois, logo separável, então L/K_1L^G é separável.

Ainda, $K_1 \subset K_1L^G \subset L$. Como L/K_1 é puramente inseparável, L/K_1L^G é puramente inseparável.

Então L/K_1L^G é puramente inseparável e separável, ou seja, pelo Corolário 1.1.22 temos $L = K_1L^G$.

Seja $\{\alpha_1, ..., \alpha_m\}$ base de L^G/K. Assim,

$$x \in L \Leftrightarrow x = \sum_{i=1}^{r} k_i l_i = \sum_{i=1}^{r} k_i (\sum_{j=1}^{m} l_{ij}\alpha_j) = \sum_{j=1}^{m} (\sum_{i=1}^{r} k_i l_{ij})\alpha_j$$

com $k_i \in K_1; l_i \in L^G; l_{ij} \in K \ \forall i = 1, ..., r; j = 1, ..., m$.

Como $c_j = \sum_{i=1}^{r} k_i l_{ij} \in K_1$ para todo $j = 1, ..., m$, temos que $x \in L \Leftrightarrow x = \sum_{j=1}^{m} c_j\alpha_j$, ou seja, $\{\alpha_1, ..., \alpha_m\}$ gera L sobre K_1

Desde que $\{\alpha_1, ..., \alpha_m\} \subset L^G$, basta reduzirmos este conjunto a uma base de

L/K_1.

□

Proposição 3.2.3. *É suficiente mostrar o Teorema 3.1.1 para extensões separáveis.*

Demonstração. Suponha que o Teorema 3.1.1 seja válido para extensões separáveis.

Considere uma extensão finita qualquer L/K e $K_1 = L_{sep}$.

Como K_1/K é separável, existe $\tilde{\beta} = \{v_1, ..., v_{s_0}\}$ base para K_1 como $K[G]$-módulo livre com exatamente $s_0 = [K_1^G : K]$ elementos.

Seja $\beta = \{b_1, ..., b_{r_0}\}$ base de L/K_1 como no Lema 3.2.2.

Vamos mostrar que o conjunto $B = \{bv | b \in \beta;\ v \in \tilde{\beta}\}$ é base para o $K[G]$-módulo L e que tem exatamente $[L^G : K]$ elementos.

(I) B é linearmente independente sobre $K[G]$:

Suponha

$$\sum_{b\in\beta}\sum_{v\in\tilde{\beta}}(\sum_{\sigma\in G} l_{\sigma bv}\sigma)bv = 0$$

com $l_{\sigma bv} \in K$ para todo $\sigma \in G$, $b \in \beta$ e $v \in \tilde{\beta}$.

Temos

$$\begin{aligned}
\sum_{b\in\beta}\sum_{v\in\tilde{\beta}}(\sum_{\sigma\in G} l_{\sigma bv}\sigma)bv = 0 \quad &\Leftrightarrow \quad \sum_{b\in\beta}\sum_{v\in\tilde{\beta}}(\sum_{\sigma\in G} l_{\sigma bv}\sigma(bv)) = 0 \\
&\Leftrightarrow \quad \sum_{b\in\beta}\sum_{v\in\tilde{\beta}}(\sum_{\sigma\in G} l_{\sigma bv}\sigma(b)\sigma(v)) = 0 \\
&\overset{b\in L^G}{\Leftrightarrow} \quad \sum_{b\in\beta}\sum_{v\in\tilde{\beta}}(\sum_{\sigma\in G} l_{\sigma bv} b\sigma(v)) = 0 \\
&\Leftrightarrow \quad \sum_{b\in\beta}(\sum_{v\in\tilde{\beta}}\sum_{\sigma\in G} l_{\sigma bv}\sigma(v))b = 0 \\
&\overset{\beta \text{ base de } L/K_1}{\Leftrightarrow} \quad \sum_{v\in\tilde{\beta}}\sum_{\sigma\in G} l_{\sigma bv}\sigma v = 0\ \forall b \in \beta \\
&\overset{\tilde{\beta} \text{ base de } K_1/K[G]}{\Leftrightarrow} \quad \sum_{\sigma\in G} l_{\sigma bv}\sigma = 0\ \forall b \in \beta; v \in \tilde{\beta} \\
&\overset{1.1.6}{\Leftrightarrow} \quad l_{\sigma bv} = 0\ \forall b \in \beta; v \in \tilde{\beta}; \sigma \in G
\end{aligned}$$

Observe que, usamos acima que $l_{\sigma bvg(v)} \in K_1$ pois, como mostramos na Proposição 3.2.1, σ pode ser visto tanto como automorfismo de L quanto de K_1 e, como $v \in K_1$, $\sigma(v) \in K_1$.

Logo $\sum_{\sigma \in G} l_{\sigma bv}\sigma = 0$ e portanto B é linearmente independente sobre $K[G]$.

(II) B gera L sobre $K[G]$:

Seja $x \in L$. Temos $x = \sum_{b \in \beta} \alpha_b b$ com $\alpha_b \in K_1$ para todo $b \in \beta$.

Ainda, $\alpha_b = \sum_{v \in \tilde{\beta}} (\sum_{\sigma \in G} l_{\sigma vb}\sigma)v$ com $l_{\sigma vb} \in K$, pois $\tilde{\beta}$ é base de K_1 como $K[G]$-módulo.

Desde que $\sigma(b) = b \ \forall b \in \beta$, temos:

$$\begin{aligned} x &= \sum_{b \in \beta} (\sum_{v \in \tilde{\beta}} (\sum_{\sigma \in G} l_{\sigma vb}\sigma)v)b \\ &= \sum_{b \in \beta} \sum_{v \in \tilde{\beta}} \sum_{\sigma \in G} l_{\sigma vb}\sigma(v)\sigma(b) \\ &= \sum_{b \in \beta} \sum_{v \in \tilde{\beta}} \sum_{\sigma \in G} l_{\sigma vb}\sigma(bv) \\ &= \sum_{b \in \beta} \sum_{v \in \tilde{\beta}} (\sum_{\sigma \in G} l_{\sigma vb}\sigma)bv \end{aligned}$$

Ou seja, B gera L sobre $K[G]$.

Assim, como B tem $[L : K_1][K_1^G : K]$ elementos, L é um $K[G]$-módulo livre com $[L : K_1][K_1 : K_1^G]$ geradores.

E,

$$\begin{aligned} [L : K_1][K_1^G : K] &= \frac{[L:K_1][K_1:K_1^G][K_1^G:K]}{[K_1:K_1^G]} \\ &= \frac{[L:K]}{|G|} \\ &= \frac{[L:L^G][L^G:K]}{|G|} \\ &= \frac{|G|[L^G:K]}{|G|} \\ &= [L^G : K] \end{aligned}$$

Logo L é um $K[G]$-módulo livre com $[L^G : K]$ geradores, ou seja, se o Teorema

3.1.1 é válido para extensões finitas separáveis, então é válido para extensões finitas quaisquer.

□

Observação 3.2.4. *Note que* $\sum_{b\in\beta}(\sum_{v\in\tilde{\beta}}(\sum_{g\in G} l_{gvb}g)v)b$ *não é simplesmente aplicar* g *em* vb*, pois o que temos é um escalar em* K_1*, a saber* $\sum_{g\in G} l_{gvb}gv$ *, e não em* $K[G]$*. Por isso o fato de* $g(b) = b$ *é fundamental para garantir que* B *seja um conjunto gerador.*

A partir de agora, salvo menção em contrário, L/K é uma extensão finita separável e N o fecho normal de L sobre K.

Observação 3.2.5. *Se* X *é um conjunto finito, definimos* $N[X]$ *como o conjunto das somas formais* $\sum_{x\in X} n_x x$ *com* $n_x \in N$*.*

Ainda, se algum conjunto G *age em* X*, então* $N[X]$ *torna-se um* $N[G]$*-módulo à esquerda através da seguinte ação:* $m_\sigma\sigma \cdot n_x x = (m_\sigma n_x)(\sigma \cdot x)$

Considere o conjunto $S = \{s : L \longrightarrow N \mid s \text{ é } K\text{-imersão}\}$. Vamos definir o conjunto $S^{-1} = \{s^{-1} | s \in S\}$.

Observe que S^{-1} não é o conjunto das inversas dos elementos de S, mas sim um conjunto que está em bijeção com S via $s \mapsto s^{-1}$. Entretanto, para $\sigma \in G$, σ^{-1} é a aplicação inversa de σ, ainda em G.

Vamos fazer $\sigma \in G = Aut_K(L)$ agir em S^{-1} da seguinte forma:

$$\sigma \cdot s^{-1} := (s\sigma^{-1})^{-1}$$

Note que a ação de G em S^{-1} é bem definida pois como σ é K-automorfismo de L, σ^{-1} também o é, assim $s\sigma^{-1}$ é uma K-imersão de L em N. Desta forma $(s\sigma^{-1})^{-1} \in S^{-1}$. Vamos denotar a ação de σ em s^{-1} simplesmente por σs^{-1}.

Como G age em L, podemos induzir em $L \otimes_K N$ uma estrutura de $N[G]$-módulo considerando $\sum_{\sigma \in G} n_\sigma \sigma \in N[G]$ e definindo

$$(\sum_{\sigma \in G} n_\sigma \sigma)(a \otimes_K b) = \sum_{\sigma \in G} \sigma(a) \otimes_K n_\sigma b$$

Observação 3.2.6. *Repare que definimos a ação de $N[G]$ em $L \otimes_K N$ para um elemento básico, entretanto deve-se entender esta ação como linear em um elemento qualquer $\sum_i a_i \otimes_K b_i$ de $L \otimes_K N$, ou seja:*

$$(\sum_{\sigma \in G} n_\sigma \sigma)(\sum_i a_i \otimes_K b_i) = \sum_{\sigma \in G} \sum_i (\sigma(a_i) \otimes_K n_\sigma b_i)$$

Com isso todas as propriedades de módulos se satisfazem trivialmente.

Lema 3.2.7. *Os $N[G]$-módulos à esquerda $L \otimes_K N$ e $N[S^{-1}]$ são isomorfos.*

Demonstração. Defina

$$\begin{array}{rccc} \varphi: & L \otimes_K N & \longrightarrow & N[S^{-1}] \\ & \sum_i a_i \otimes_K b_i & \longrightarrow & \sum_{s \in S} \sum_i s(a_i) b_i s^{-1} \end{array}$$

Veja que é imediato o fato de que φ é bem definida pela propriedade universal do produto tensorial. Entretanto a propriedade universal não garante que φ é N-linear mas sim K-linear.

(I) φ é N-linear:

Claro pois se $n \in N$,

$$\begin{aligned} \varphi(n \sum_i a_i \otimes_K b_i) &= \varphi(\sum_i a_i \otimes_K n b_i) \\ &= \sum_{s \in S} \sum_i s(a_i) n b_i s^{-1} \\ &= n \sum_{s \in S} \sum_i s(a_i) b_i s^{-1} \\ &= n\varphi(\sum_i a_i \otimes_K b_i) \end{aligned}$$

(II) φ respeita a ação de G:

Primeiramente repare que, ao variarmos s, para cada $\sigma \in G$ fixo $s\sigma$ percorre S, ou seja, $S = S\sigma = \{s\sigma | s \in S\}$.

De fato, $s_1\sigma = s_2\sigma \Rightarrow s_1 = s_2$ pois σ é automorfismo, assim $\#S\sigma = \#S$. Como $S\sigma \subset S$, temos $S\sigma = S$.

Se $\sigma \in G$, podemos olhar σ como elemento de $N[G]$. Ora

$$\varphi(\sigma(\sum_i a_i \otimes_K b_i)) = \varphi \sum_i \sigma(a_i) \otimes_K b_i = \sum_{s\in S} \sum_i s(\sigma(a_i))b_i s^{-1}$$

Seja $t := s\sigma \in S$, logo $\sigma t^{-1} = (t\sigma^{-1})^{-1} = (s\sigma\sigma^{-1})^{-1} = s^{-1}$. Logo, como $S\sigma = S$, $s\sigma = t$ percorre S. Desta forma temos:

$$\varphi(\sigma(\sum_i a_i \otimes_K b_i)) = \sum_{t\in S} \sum_i t(a_i)b_i \sigma t^{-1}$$

Por outro lado, como σ age em S^{-1}:

$$\sigma(\varphi(\sum_i a_i \otimes_K b_i)) = \sigma(\sum_{s\in S} \sum_i \underbrace{s(a_i)b_i}_{\in N} s^{-1}) = \sum_{s\in S} \sum_i s(a_i)b_i \sigma s^{-1}$$

Logo $\varphi(\sigma(\sum_i a_i \otimes_K b_i)) = \sigma(\varphi(\sum_i a_i \otimes_K b_i))$ como queríamos.

Em outra palavras, (I) e (II) nos dizem que φ é homomorfismo de $N[G]$-módulos.

(III) φ é bijeção:

Repare que, olhando $L \otimes_K N$ como N espaço vetorial, $dim_N L \otimes_K N = dim_K L$.

Mas $dim_K L = [L : K] = [L : K]_s = \#S = dim_N N[S^{-1}]$.

Assim $dim_N L \otimes_K N = dim_N N[S^{-1}]$. Portanto basta mostrar φ injetiva.

Suponha, então, $\varphi(x) = 0$ para algum $x \in L \otimes_K N$.

Tome uma base $\{a_t \in L \mid t \in S\}$ de L/K.

Relembre que, do Teorema 1.2.2 temos que $\#S = [L:K]_S = [L:K] = dim_K L$.

Assim existe um conjunto $\{n_t \in N \mid t \in S\}$ de forma que $x = \sum_{t\in S} a_t \otimes_K n_t$.

De fato, como $x \in L \otimes_K N$ então

$$\begin{aligned} x &= \sum_i a_i \otimes_K b_i = \sum_i (\sum_{t\in S} \alpha_{it} a_t) \otimes_K b_i \quad (\alpha_{it} \in K) \\ &= \sum_i \sum_{t\in S} (\alpha_{it} a_t \otimes_K b_i) = \sum_i \sum_{t\in S} (a_t \otimes_K \alpha_{it} b_i) \\ &= \sum_{t\in S} a_t \otimes_K \underbrace{\sum_i \alpha_{it} b_i}_{n_t} = \sum_{t\in S} a_t \otimes_K n_t \end{aligned}$$

Logo $0 = \varphi(x) = \varphi(\sum_{t\in S} a_t \otimes_K n_t) = \sum_{s\in S}\sum_{t\in S} s(a_t) n_t s^{-1}$.

Desde que S^{-1} é base de $N[S^{-1}]$ sobre N, temos $\sum_{t\in S} s(a_t) n_t = 0$ para todo $s \in S$.

Mas pelo Teorema 2.1.11, a matriz $(s(a_t))_{s,t}$ é não singular. Logo o sistema $\sum_{t\in S} s(a_t) X_t = 0$, $s \in S$ tem única solução $X_t = 0$ para todo $t \in S$. Como $X_t = n_t$ para todo $t \in S$ é solução, devemos ter $n_t = 0$ para todo $t \in S$.

Logo $x = \sum_{t\in S} a_t \otimes_K 0 = 0_{L\otimes_K N}$, ficando assim provado o lema.

□

Note que podemos dar uma estrutura de $K[G]$-módulo para $L^{\oplus m} = \bigoplus_{i=1}^{m} L = L \times L \times ... \times L$ e $K[S^{-1}]^m$ simplesmente fazendo os escalares agirem em cada coordenada.

Vamos ver mais alguns isomorfismos que nos ajudarão na demonstração do Teorema 3.1.1.

Proposição 3.2.8.

(i) $L \otimes_K N \simeq L^{\oplus [N:K]}$ *como* $K[G]$*-módulos*

(ii) $N[S^{-1}] \simeq K[S^{-1}]^{[N:K]}$ *como* $K[G]$*-módulos*

Demonstração. Considere $n = [N : K]$ e $\{v_1, ..., v_n\}$ base de N/K

(i) Seja $\{w_1, ..., w_m\}$ base de L/K.

Defina:

$$\begin{array}{rccc} \varphi : & L \otimes_K N & \longrightarrow & L^{\oplus[N:K]} \\ & \sum_{i=1}^{n} (\sum_{j=1}^{m} \alpha_{ij} w_j) \otimes_K v_i & \longrightarrow & (\sum_{j=1}^{m} \alpha_{ij} w_j)_{i=1}^{n} \end{array}$$

Note que φ é claramente homomorfismo bem definido K-espaços vetoriais pela propriedade universal do produto tensorial.

Primeiramente, vejamos que φ é injetora:

Suponha $\varphi(\sum_{i=1}^{n} (\sum_{j=1}^{m} \alpha_{ij} w_j) \otimes_K v_i) = \varphi(\sum_{i=1}^{n} (\sum_{j=1}^{m} \beta_{ij} w_j) \otimes_K v_i)$. Assim temos que

$$(\sum_{j=1}^{m} \alpha_{ij} w_j)_{i=1}^{n} = (\sum_{j=1}^{m} \beta_{ij} w_j)_{i=1}^{n}$$

para todo $i = 1, ..., n$.

Logo

$$\sum_{j=1}^{m} (\alpha_{ij} - \beta_{ij}) w_j = 0$$

para todo $i = 1, ..., n$.

Como $\{w_j \mid 1 \leq j \leq m\}$ é base de L sobre K, para todo i temos que $\alpha_{ij} = \beta_{ij}$. Assim, φ é injetora.

Mostraremos que φ é sobrejetora:

Seja $x = (a_i)_{i=1}^{n} \in L^{\oplus[N:K]}$. Escreva $a_i = \sum_{j=1}^{m} \alpha'_{ij} w_j$.

Logo $\varphi(\sum_{i=1}^{n} (\sum_{j=1}^{m} \alpha'_{ij} w_j) \otimes_K v_i) = (\sum_{j=1}^{m} \alpha'_{ij} w_j)_{i=1}^{n} = (a_i)_{i=1}^{n} = x$, ou seja, φ é sobrejetora.

Ainda, φ respeita a ação de G.

De fato, se $\sigma \in G$,

$$\begin{aligned}
\varphi(\sigma(\sum_{i=1}^{n}(\sum_{j=1}^{m}\alpha_{ij}w_j)\otimes_K v_i)) &= \varphi(\sum_{i=1}^{n}(\sum_{j=1}^{m}\alpha_{ij}\sigma(w_j)\otimes_K v_i)) \\
&= (\sum_{j=1}^{m}\alpha_{ij}\sigma(w_j))_{i=1}^{n} \\
&= \sigma((\sum_{j=1}^{m}\alpha_{ij}w_j)_{i=1}^{n}) \\
&= \sigma(\varphi(\sum_{i=1}^{n}(\sum_{j=1}^{m}\alpha_{ij}w_j)\otimes_K v_i))
\end{aligned}$$

Desta forma φ respeita claramente a ação de $K[G]$, ou seja, φ é isomorfismo de $K[G]$-módulos.

(ii) Defina

$$\begin{array}{rccl}
\varphi: & N[S^{-1}] & \longrightarrow & K[S^{-1}]^{[N:K]} \\
& \sum_{s\in S}\sum_{i=1}^{n}\alpha_{is}v_i s^{-1} & \longrightarrow & (\sum_{s\in S}\alpha_{is}s^{-1})_{i=1}^{n} \qquad \alpha_{is}\in K
\end{array}$$

φ é claramente um homomorfismo bem definido de grupos.

Temos φ injetora pois se $\varphi(\sum_{s\in S}\sum_{i=1}^{n}\alpha_{is}v_i s^{-1}) = \varphi(\sum_{s\in S}\sum_{i=1}^{n}\beta_{is}v_i s^{-1})$, temos para todo i entre 1 e n

$$\sum_{s\in S}\alpha_{is}s^{-1} = \sum_{s\in S}\beta_{is}s^{-1}$$

Desta forma, pela definição de $K[S^{-1}]$, temos que $\alpha_{is} = \beta_{is}$ para todo $s \in S$ e $1 \leq i \leq n$. Logo φ é injetora.

Ainda, tomando $x = (\sum_{s\in S}\alpha'_{is}s^{-1})_{i=1}^{n} \in K[S^{-1}]^{[N:K]}$, então

$$\varphi(\sum_{s\in S}\sum_{i=1}^{n}\alpha'_{is}v_i s^{-1}) = x$$

ou seja, φ é sobrejetora.

Mais que isso, φ respeita a ação de G.

De fato, se $\sigma \in G$,

$$\begin{aligned}
\varphi(\sigma(\sum_{s\in S}\sum_{i=1}^{n}\alpha_{is}v_i s^{-1})) &= \varphi(\sum_{s\in S}\sum_{i=1}^{n}\alpha_{is}v_i\sigma s^{-1}) \\
&= \varphi(\sum_{s\in S}\sum_{i=1}^{n}\alpha_{is}v_i(s\sigma^{-1})^{-1}) \\
&= (\sum_{s\in S}\alpha_{is}(s\sigma^{-1})^{-1})_{i=1}^{n} \\
&= (\sum_{s\in S}\alpha_{is}\sigma s^{-1})_{i=1}^{n} \\
&= \sigma((\sum_{s\in S}\alpha_{is}s^{-1})_{i=1}^{n}) \\
&= \sigma(\varphi(\sum_{s\in S}\sum_{i=1}^{n}\alpha_{is}v_i s^{-1}))
\end{aligned}$$

E assim claramente φ é um isomorfismo de $K[G]$-módulos.

□

Assim, os isomorfismos acima, juntamente com o Lema 3.2.7, nos dizem que $L^{\oplus[N:K]} \simeq K[S^{-1}]^{[N:K]}$ como $K[G]$-módulos.

Definição 3.2.9. *Uma ação de G em X é dita fiel se $\sigma_1 \cdot x = \sigma_2 \cdot x$ implicar $\sigma_1 = \sigma_2$ para todo $x \in X$.*

Proposição 3.2.10. *A ação de G em S^{-1} é fiel. Ainda, as órbitas de S^{-1}, definidas por $o(s^{-1}) = \{\sigma s^{-1} \mid \sigma \in G\}$, são iguais ou disjuntas.*

Demonstração. Suponha $\sigma_1 s^{-1} = \sigma_2 s^{-1}$. Temos que $(s\sigma_1^{-1})^{-1} = (s\sigma_2^{-1})^{-1}$ e, como cada elemento de S^{-1} é associado a um único elemento de S, $s\sigma_1^{-1} = s\sigma_2^{-1}$.

Assim, para qualquer $x \in L$, $s\sigma_1^{-1}(x) = s\sigma_2^{-1}(x)$. Como s é imersão, e portanto injetora, temos $\sigma_1^{-1}(x) = \sigma_2^{-1}(x)\ \forall\ x \in L$.

Mas σ_1 e σ_2 são automorfismos, logo $\sigma_1(x) = \sigma_2(x)$ para todo $x \in L$. Desta forma $\sigma_1 = \sigma_2$ e portanto a ação é fiel.

Mostraremos agora que as órbitas são disjuntas:

Considere agora $s^{-1} \in o(s_1^{-1}) \cap o(s_2^{-1})$ com s_1^{-1}, $s_2^{-1} \in S^{-1}$.

Temos $s^{-1} = \sigma_1 s_1^{-1}$ para algum $\sigma_1 \in G$ e $s^{-1} = \sigma_2 s_2^{-1}$ para algum $\sigma_2 \in G$.

Por conseguinte $s_1^{-1} = \sigma_1^{-1}\sigma_2 s_2^{-1}$ e logo $s_1^{-1} \in o(s_2^{-1})$. Veja que desta maneira obtemos $o(s_1^{-1}) \subset o(s_2^{-1})$.

Analogamente $s_2^{-1} \in o(s_1^{-1})$ e portanto $o(s_1^{-1}) = o(s_2^{-1})$.

Logo duas órbitas são iguais ou disjuntas.

□

Como a ação é fiel, cada órbita tem exatamente $|G|$ elementos, desta forma, o número de órbitas de S^{-1} é $\#o(S^{-1}) = \frac{\#S}{|G|}$.

Vamos escolher um elemento em cada uma das $m = \#o(S^{-1})$ órbitas de S^{-1} e nomeá-los $s_1^{-1}, ..., s_m^{-1}$.

Repare que, independentemente da escolha dos elementos das órbitas, $\sigma_1(s_i^{-1})$ percorre $o(s_i^{-1})$ quando σ_1 percorre G pois $\sigma_1\sigma_2$ percorre G para σ_2 fixo.

Proposição 3.2.11. *$K[S^{-1}] \simeq K[G]^m$ como $K[G]$-módulos.*

Demonstração. Primeiramente note que podemos reescrever qualquer elemento da forma $\sum_{s^{-1} \in S^{-1}} \lambda_{s^{-1}} s^{-1} \in K[S^{-1}]$ como $\sum_{i=1}^{m} \sum_{\sigma_1 \in G} \lambda_{\sigma_1 s_i^{-1}} \sigma_1 s_i^{-1}$.

Defina então

$$\begin{array}{rccc} \varphi : & K[S^{-1}] & \longrightarrow & K[G]^m \\ & \sum_{i=1}^{m} \sum_{\sigma_1 \in G} \lambda_{\sigma_1 s_i^{-1}} \sigma_1 s_i^{-1} & \longrightarrow & (\sum_{\sigma_1 \in G} \lambda_{\sigma_1 s_i^{-1}} \sigma_1)_{i=1}^{m} \end{array}$$

É imediato o fato de que φ é bem definido. Mostremos que φ é um isomorfismo de grupos:

(I) φ é injetora:

Suponha $\varphi(\sum_{i=i}^{m}\sum_{\sigma_1\in G}\lambda_{\sigma_1 s_i^{-1}\sigma_1 s_i^{-1}}) = \varphi(\sum_{i=i}^{m}\sum_{\sigma_1\in G}\alpha_{\sigma_1 s_i^{-1}\sigma_1 s_i^{-1}})$.

Temos $\sum_{\sigma_1\in G}\lambda_{\sigma_1 s_i^{-1}\sigma_1} = \sum_{\sigma_1\in G}\alpha_{\sigma_1 s_i^{-1}\sigma_1}\ \forall\ i = 1, ..., m$.

Mas pelo Teorema 1.1.6 G é um conjunto linearmente independente sobre K, logo $\lambda_{\sigma_1 s_i^{-1}} = \alpha_{\sigma_1 s_i^{-1}}\ \forall\ i = 1, ..., m;\ \sigma_1 \in G$.

(II) φ é sobrejetora:

Considere $\beta \in K[G]^m$. Ora, $\beta = (\sum_{\sigma_1\in G}\alpha_{\sigma_1,i}\sigma_1)_{i=1}^{m}$.

Defina $\alpha = \sum_{i=1}^{m}\sum_{\sigma_1\in G}\alpha_{\sigma_1,i}\sigma_1 s_i^{-1} \in K[S^{-1}]$. Claramente $\varphi(\alpha) = \beta$.

(III) φ preserva a ação de G:

Seja $\sigma_2 \in G$. Pensando σ_2 como elemento de $K[G]$ temos

$$\begin{aligned}
\varphi(\sigma_2\sum_{i=1}^{m}\sum_{\sigma_1\in G}\lambda_{\sigma_1 s_i^{-1}\sigma_1 s_i^{-1}}) &= \varphi(\sum_{i=1}^{m}\sum_{\sigma_1\in G}\lambda_{\sigma_1 s_i^{-1}\sigma_2\sigma_1 s_i^{-1}}) \\
&= (\sum_{\sigma_1\in G}\lambda_{\sigma_1 s_i^{-1}\sigma_2\sigma_1})_{i=1}^{m} \\
&= \sigma_2(\sum_{\sigma_1\in G}\lambda_{\sigma_1 s_i^{-1}\sigma_1})_{i=1}^{m} \\
&= \sigma_2(\varphi(\sum_{i=1}^{m}\sum_{\sigma_1\in G}\lambda_{\sigma_1 s_i^{-1}\sigma_1 s_i^{-1}}))
\end{aligned}$$

Assim claramente φ respeita a ação de $K[G]$. Logo φ é um isomorfismo de $K[G]$-módulos.

□

Podemos, agora, voltar à prova do Teorema 3.1.1

Demonstração. De 3.2.7 e 3.2.8 temos que $L^{\oplus[N:K]} \simeq K[S^{-1}]^{[N:K]}$ como $K[G]$-módulos

Então, pelo Teorema 1.3.11 temos $L \simeq K[S^{-1}]$ como $K[G]$-módulos.

Ainda, pela proposição 3.2.11, temos que $K[S^{-1}] \simeq K[G]^m$ como $K[G]$-módulos com $m = \#o(S^{-1})$. Logo $L \simeq K[G]^m$ como $K[G]$-módulos.

Mas $m = \#o(S^{-1}) = \frac{\#S}{|G|} = \frac{[L:K]_s}{[L:L^G]} \overset{L/Ksep}{=} \frac{[L:K]}{[L:L^G]} = \frac{[L:L^G][L^G:K]}{[L:L^G]} = [L^G : K]$.

Claramente $K[G]^{[L^G:K]}$ é $K[G]$-módulo livre com $[L^G : K]$ geradores.

Desde que $L \simeq K[G]^{[L^G:K]}$ como $K[G]$-módulos, vale o resultado.

□

Capítulo 4

Estrutura de Espaço Quadrático

Neste capítulo ainda estamos supondo L/K uma extensão separável finita.

Toda maquinaria construída ao longo deste trabalho induz um resultado que nos dá uma estrutura de K-espaço quadrático a L usando o traço, descrito na Seção 2.2, quando o fecho normal N de L/K é tal que $[N : K]$ é ímpar.

Veja que, como estamos supondo L/K separável, então $[L : K]_i = 1$ e o traço de $x \in L$ é dado por $tr_{L/K}(x) = \sum_{s \in S} s(x)$ com S o conjunto das K-imersões de L em seu fecho normal N.

Lembre-se que pelo Teorema 1.2.8, $tr_{L/K}(L) \subset K$. Desta forma, o traço induz uma aplicação K-bilinear simétrica q_L em L, quando este é visto como espaço vetorial sobre K. Basta definir:

$$q_L(x, y) = tr_{L/K}(xy)$$

Veja que se $x \in L\backslash\{0\}$, então x tem inverso em L. Temos que $q_L(x, x^{-1}) = tr_{L/K}(xx^{-1}) = tr_{L/K}(1) = \sum_{s \in S} s(1) = [L : K]$ pois L/K é separável e, pelo Teorema 1.2.2, temos que S tem $[L : K]$ elementos. Logo, se $x \neq 0$ então $q_L(x, x^{-1}) \neq 0$, ou seja, $x = 0$ é o único elemento de L tal que $q_L(x, y) = 0$ para todo $y \in L$. Por 1.4.5

(iii), (V, q_L) é regular. Em outra palavras, $(f_{q_L}) \in M(F)$.

Para simplificarmos a escrita, a partir de agora quando (V, q) for um espaço quadrático, q representará tanto a aplicação bilinear quanto a classe de formas quadráticas (f_q) associada a (V, q).

Vimos que, se N é uma extensão de K, então o K-espaço quadrático (L, q_L) pode ser estendido a um N-espaço quadrático $(L \otimes_K N, q_N)$, onde $q_N(l \otimes_K n, l' \otimes_K n') = nn' q_L(l, l')$.

Vamos definir uma aplicação bilinear p_N em $N[S^{-1}]$ por

$$\begin{cases} p_N(s^{-1}, s^{-1}) = 1 \\ p_N(s^{-1}, s'^{-1}) = 0 \ se \ s \neq s' \end{cases}$$

e estender cada variável por linearidade em N.

Lema 4.1.1. *Os espaços quadráticos $(L \otimes_K N, q_N)$ e $(N[S^{-1}], p_N)$ são isométricos.*

Demonstração. Já sabemos que $L \otimes_K N$ e $N[S^{-1}]$ são isomorfos como $N[G]$-módulos pelo Lema 3.2.7. Vamos usar a mesma aplicação e mostrar que ela é isometria.

Relembrando, tínhamos a aplicação

$$\begin{array}{rccc} \varphi: & L \otimes_K N & \longrightarrow & N[S^{-1}] \\ & \sum_i a_i \otimes_K b_i & \longrightarrow & \sum_{s \in S} \sum_i s(a_i) b_i s^{-1} \end{array}$$

É suficiente mostrarmos que $q_N(a \otimes_K b, a' \otimes_K b') = p_N(\varphi(a \otimes_K b), \varphi(a' \otimes_K b'))$ pois as aplicações são bilineares e φ é homomorfismo.

Ora,

$$\begin{aligned} q_N(a \otimes_K b, a' \otimes_K b') &= q_L(a, a') bb' \\ &= \sum_{s \in S} s(aa') bb' \\ &= \sum_{s \in S} s(a) s(a') bb' \\ &= \sum_{s \in S} \sum_{s' \in S} s(a) s'(a') bb' p_N(s, s') \end{aligned}$$

$$
\begin{aligned}
&= p_N(\sum_{s\in S} s(a)bs, \sum_{s'\in S} s'(a')b's') \\
&= p_N(\varphi(a\otimes_K b), \varphi(a'\otimes_K b'))
\end{aligned}
$$

□

Teorema 4.1.2. *Seja L/K extensão separável finita e N fecho normal de L/K tal que $[N:K]$ tem grau ímpar e $c(K)\neq 2$. Considere p aplicação bilinear em $K[S^{-1}]$ definida por $p(s,s)=1$ e $p(s,s')=0$ se $s\neq s'$. Seja q_L a aplicação bilinear induzida pelo traço. Então $(L,q_L)\simeq(K[S^{-1}],p)$.*

Demonstração. Note que claramente $(K[S^{-1}],p)$ é um espaço regular.

Repare que a aplicação bilinear p_N definida em $K[S^{-1}]\otimes_K N$ por:

$$p_N(s\otimes_K n, s'\otimes_K n') = nn'p(s,s')$$

é exatamente a imagem de p pela aplicação $r: M(K)\longrightarrow M(N)$ descrita na Seção 1.4.

Claramente podemos ver que os espaços $(K[S^{-1}]\otimes_K N, p_N)$ e $(N[S^{-1}], p_N)$ são isométricos, com $\tau: K[S^{-1}]\otimes_K N\to N[S^{-1}]$ definida por $\tau(s^{-1}\otimes_K n)=ns^{-1}$ e p_N trivialmente induzido para agir em $N[S^{-1}]$, ou seja, $p_N(ns^{-1}, n's'^{-1}) = nn'p(s,s'^{-1})$.

Veja que p_N é a mesma aplicação usada no Lema 4.1.1. Por este mesmo lema, $(L\otimes_K N, q_N)\simeq(N[S^{-1}],p_N)$. Assim, em $M(N)\subset\hat{W}(N)$, $q_N=p_N$.

Agora, $\hat{r}^*: W(K)\longrightarrow\hat{W}(N)$ é tal que $\hat{r}^*(q_L)=q_N=p_N=\hat{r}^*(p)$ em $\hat{W}(N)$.

Mas mostramos que $\hat{r}^*$ é injetiva se $[N:K]$ for ímpar. Desta forma temos que $q_L=p$ em $M(K)\subset\hat{W}(K)$.

Assim, pela Proposição 1.4.4, temos que $(L,q_L)\simeq(K[S^{-1}],p)$. □

Defina a aplicação q_0 em $K[G]$ por $q_0(g,g)=1$ e $q_0(g,g')=0$ se $g\neq g'$. Repare que esta aplicação é bilinear simétrica e que o espaço $(K[G],q_0)$ é regular.

Teorema 4.1.3. *Sejam L/K extensão finita separável e G subgrupo de $Aut_K(L)$. Suponha que $c(K) \neq 2$ e L tem fecho normal N tal que $[N : K]$ é ímpar, então (L, q_L) é isomorfo a uma soma ortogonal de $[L^G : K]$ cópias de $(K[G], q_0)$.*

Demonstração. Tome $m = [L^G : K]$. Denotaremos a soma ortogonal de m cópias de $(K[G], q_0)$ por $(K[G], q_0)^m$.

Defina:

$$\begin{array}{rccc} \sigma : & K[S^{-1}] & \longrightarrow & K[G]^m \\ & \sum_{i=1}^{m} \sum_{g\in G} \lambda_{gs_i^{-1}} g s_i^{-1} & \longrightarrow & (\sum_{g\in G} \lambda_{gs_i^{-1}} g)_{i=1}^m \end{array}$$

Com p a forma em $K[S^{-1}]$ definida acima e q a soma ortogonal de m vezes q_0.

Já mostramos anteriormente que σ é um isomorfismo. Só precisamos mostrar que σ é isometria, ou seja, $q(\sigma(a), \sigma(b)) = p(a, b)$, com $a, b \in K[S^{-1}]$.

De fato, sejam $a = \sum_{i=1}^{m} \sum_{g\in G} \lambda_{gs_i^{-1}} g s_i^{-1}$ e $b = \sum_{i=1}^{m} \sum_{g\in G} \alpha_{gs_i^{-1}} g s_i^{-1}$.

$$\begin{aligned} q(\sigma(a), \sigma(b)) &= q(\sigma(\sum_{i=1}^{m} \sum_{g\in G} \lambda_{gs_i^{-1}} g s_i^{-1}), \sigma(\sum_{i=1}^{m} \sum_{g\in G} \alpha_{gs_i^{-1}} g s_i^{-1})) \\ &= q((\sum_{g\in G} \lambda_{gs_i^{-1}} g)_{i=1}^m, (\sum_{g\in G} \alpha_{gs_i^{-1}} g)_{i=1}^m) \\ &= \sum_{i=1}^{m} q_0(\sum_{g\in G} \lambda_{gs_i^{-1}} g, \sum_{g\in G} \alpha_{gs_i^{-1}} g) \\ &= \sum_{i=1}^{m} \sum_{g\in G} q_0(\lambda_{gs_i^{-1}} g, \alpha_{gs_i^{-1}} g) \\ &= \sum_{i=1}^{m} \sum_{g\in G} p(\lambda_{gs_i^{-1}} g s_i^{-1}, \alpha_{gs_i^{-1}} g s_i^{-1}) \\ &= p(\sum_{i=1}^{m} \sum_{g\in G} \lambda_{gs_i^{-1}} g s_i^{-1}, \sum_{i=1}^{m} \sum_{g\in G} \alpha_{gs_i^{-1}} g s_i^{-1}) \\ &= p(a, b) \end{aligned}$$

Logo $(K[G], q_0)^m \simeq (K[S^{-1}], p)$ e, pelo Teorema 4.1.2, $(K[S^{-1}], p) \simeq (L, q_L)$. Ou seja, $(L, q_L) \simeq (K[G], q_0)^m$.

□

Referências Bibliográficas

[1] Atiyah, M. F.; Macdonald, I. G., *"Introduction to Commutative Algebra"*, Addison - Wesley Publishing Company, Massachusetts, 1969.

[2] Bayer-Fluckiger, E. ; *"Self-dual Normal Bases"*, Nedel, Akad. Wetensch, Indag. Math. **51** (1989), no. 4, 379-383.

[3] Braga, A.C. ; *"Bases Normais Auto-Duais"*, Dissertação de Mestrado , UEM (2003).

[4] Hoffmann, K. e Kunze, R.; *"Linear Algebra - Second Edition"*, Prentice-Hall, Englewood Cliffs (1971).

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

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

[7] Lundström, P. ; *"Galois Module Structure Of Fields Extensions"*, International Eletronic Journal Of Algebra (2007), Volume 2 , 100-105.

[8] McCarthy, P. J. ; *"Algebraic Extension Of Fields"*, Blaisdell Publishing Company, London (1966).

[9] Milies, F.C.P ; *"Anéis e Módulos"*, USP, São Paulo (1972).

[10] Picado, J. ; *"Corpos e Equações Algébricas"*, Universidade de Coimbra (2007).

[11] Saldanha, D.Z. ; *"Funtores Separáveis Aplicados a Anéis Graduados "*, Dissertação de Mestrado, UFRGS (2010).