Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Construção e aplicações do caráter de Steinberg

Bruno Figueira Lourenço

Brasília
2012

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Construção e aplicações do caráter de Steinberg

Bruno Figueira Lourenço

Dissertação apresentada como requisito parcial
para conclusão do Mestrado em Matemática

Orientador
Prof. Dr. Marco Antonio Pellegrini

Brasília
2012

Universidade de Brasília
Instituto de Ciências Exatas
Departamento de Matemática

Construção e aplicações do caráter de Steinberg

Bruno Figueira Lourenço*

Dissertação apresentada como requisito parcial
para conclusão do Mestrado em Matemática

Comissão examinadora:

Prof. Dr. Marco Antonio Pellegrini (Orientador)
MAT/UnB

Prof. Dr. Noraí Romeu Rocco
MAT/UnB

Prof.ª Dr.ª Marinês Guerreiro
MAT/UFV

Brasília, 3 de setembro de 2012

*O autor foi bolsista do CNPq durante a elaboração desta dissertação.

Agradecimentos

Gostaria de agradecer ao Prof. Marco pela orientação muito divertida e interessante. Aproveito para agradecer também ao Prof. Noraí e à Prof.ª Marinês por participarem da minha defesa e pelas sugestões e comentários. Além disso, não poderia deixar agradecer aos amigos, familiares e professores pelo apoio. Por fim, agradeço à Ana por me completar e estar ao meu lado sempre.

Este trabalho contou com o apoio financeiro do CNPq, deixo aqui registrado meus agradecimentos.

Abstract

If G is a finite group with a BN-pair, it is always possible to construct a complex irreducible character called the Steinberg character. In particular, if G is a finite group of Lie type, the Steinberg character has a special place in the study of the irreducible characters of G. In this work, we discuss the construction and some applications of the Steinberg character. In particular, we show the irreducibility of the Steinberg character and, under some additional hypotheses, we calculate all its values. As examples of applications, we use the Steinberg character to show a few results about commutators and in order to count the number of unipotent elements in certain finite groups of Lie type. Moreover, we present a quick discussion of an extension of the Steinberg character introduced by Walter Feit. We tried to keep this work as self-contained as possible, therefore we included a chapter on groups with a BN-pair and another one on the theory of Linear Algebraic Groups.

Keywords: groups with a BN-pair, linear algebraic groups, finite groups of Lie type, Steinberg character.

Resumo

O caráter de Steinberg pode ser construído sempre que temos um grupo finito G equipado com um par-BN. Em particular, se G é um grupo finito do tipo Lie, o caráter de Steinberg tem um papel de destaque no estudo dos caracteres irredutíveis de G. Neste trabalho, discutimos a construção e algumas aplicações do caráter de Steinberg. Em particular, mostramos sua irredutibilidade e, sob hipóteses adicionais, determinamos todos os seus valores. Como aplicações, utilizamos o caráter de Steinberg para provar resultados sobre comutadores e para contar o número de elementos unipotentes em certos grupos finitos do tipo Lie. Além disso, apresentamos brevemente uma extensão do caráter de Steinberg proposta por Walter Feit. Para que o texto seja auto-contido, apresentamos uma discussão geral sobre grupos com par-BN e revisamos também alguns aspectos relevantes da Teoria de Grupos Algébricos Lineares.

Palavras-chave: grupos com par-BN, grupos lineares algébricos, grupos finitos do tipo Lie, caráter de Steinberg.

Lista de Símbolos

Δ	conjunto das raízes fundamentais associadas a um sistema Φ
Φ^+	conjunto das raízes positivas de Φ
Φ_J	sistema de raízes associado ao subgrupo parabólico W_J
Φ	sistema de raízes
χ^G	indução do caráter χ de um subgrupo de G ao grupo G
χ_H	restrição do caráter χ ao subgrupo H
$\mathbb{F}_p$	corpo dos inteiros módulo p
ω_χ	caráter central associado ao caráter χ
$\mathscr{K}_i$	i-ésima classe de conjugação do grupo G
$C_G(g)$	centralizador de g em G
D_J	conjunto completo de representantes das classes laterais à esquerda de W_J em W
$D_{J,K}$	conjunto completo de representantes das classes laterais duplas de W_J e W_K em W
$End_K(V)$	conjunto dos endomorfismos de V como espaço vetorial sobre K
G^0	a componente conexa que contém a identidade do grupo linear algébrico G
G'	subgrupo derivado de G
G^F	o conjunto de pontos fixos do endomorfismo $F : G \to G$, onde G é um grupo linear algébrico
$\|G\|_p$	maior potência de p que divide $\|G\|$
$\|G\|_{p'}$	a parte coprima com p de $\|G\|$, ou seja, $\frac{\|G\|}{\|G\|_p}$
G_s	conjunto de elementos semisimples de um grupo linear algébrico G
g_s	parte semisimples de um elemento g de um grupo linear algébrico G

G_u	conjunto de elementos unipotentes de um grupo linear algébrico G
g_u	parte unipotente de um elemento g de um grupo linear algébrico G
$Irr(G)$	conjunto dos caracteres complexos irredutíveis de G
$M_n(K)$	anel das matrizes $n \times n$ sobre K
$N_{J,K}$	conjunto completo de representantes das classes laterais duplas de P_J e P_K em G
$o(g)$	ordem de um elemento g de um grupo G
P_J	subgrupo parabólico padrão de G associado ao subconjunto $J \subseteq I$
$R(G)$	o radical de um grupo linear algébrico G
$R_u(G)$	o radical unipotente de um grupo linear algébrico G
St	caráter de Steinberg
St_{L_J}	caráter de Steinberg do subgrupo L_J
W_J	subgrupo parabólico padrão de W associado ao subconjunto $J \subseteq I$

Sumário

Introdução

Neste trabalho discutiremos algumas propriedades do caráter de Steinberg [34, 35] e algumas das suas aplicações. O caráter de Steinberg é um caráter irredutível que possui uma importância fundamental no estudo das representações dos grupos finitos do tipo Lie e é uma peça importante para mostrar diversos resultados sobre tais grupos. Em verdade, podemos definir tal caráter em qualquer grupo finito que possua um par-BN. Se o par-BN for *split*, podemos obter resultados ainda melhores. De toda forma, para apreciar o caráter de Steinberg, precisamos primeiro justificar a importância dos grupos finitos do tipo Lie.

Um dos resultados mais marcantes da Teoria de Grupos Finitos do século XX, sem dúvida, foi o *Teorema da Classificação dos Grupos Finitos Simples*. Podemos enunciá-lo da seguinte forma:

Teorema. *[39, Seção 1.2] Seja G um grupo finito simples, então G é isomorfo a um grupo que pertence a uma das seis famílias abaixo:*

(*i*) *Um grupo cíclico de ordem prima.*

(*ii*) *Um grupo alternado $Alt(n)$, para $n \geq 5$.*

(*iii*) *Um grupo clássico:*

- *Linear: $PSL_n(q)$, para $n \geq 2$, exceto $PSL_2(2)$ e $PSL_2(3)$.*
- *Unitário: $PSU_n(q)$, para $n \geq 3$, exceto $PSU_3(2)$.*
- *Simplético: $PSp_{2n}(q)$, para $n \geq 2$, exceto $PSp_4(2)$.*
- *Ortogonal: $P\Omega_{2n+1}(q), n \geq 3$ e q ímpar, $P\Omega^+_{2n}(q), n \geq 4$ e $P\Omega^-_{2n}(q), n \geq 4$.*

Em todos esses casos, q é uma potência de um primo p.

(*iv*) *Um grupo excepcional do tipo Lie:*

$$G_2(q), q \geq 3;\ F_4(q);\ E_6(q);\ {}^2E_6(q);\ {}^3D_4(q);\ E_7(q);\ E_8(q)$$

onde q é uma potência de um primo p, ou

$${}^2B_2(2^{2n+1});\ {}^2G_2(3^{2n+1});\ {}^2F_4(2^{2n+1})$$

para $n \geq 1$.

(*v*) *Um dos 26 grupos esporádicos.*

(*vi*) *O grupo de Tits ${}^2F_4(2)'$.*

Mais detalhes sobre o Teorema da Classificação e a notação utilizada podem ser encontrados em [39]. Alguns autores consideram o grupo de Tits como um grupo excepcional do tipo Lie. Neste trabalho, optamos por analisá-lo separadamente para tratar os outros grupos do tipo Lie de maneira uniforme.

Os grupos das famílias (iii) e (iv) podem ser obtidos a partir dos grupos do tipo Lie. Muitos desses grupos são, de fato, grupos do tipo Lie, enquanto outros são quocientes. Assim, de certa forma, a maior parte dos grupos simples são grupos finitos do tipo Lie ou estão relacionados a tais grupos de forma bem próxima. Neste trabalho, discutiremos brevemente como os grupos finitos do tipo Lie surgem a partir de um grupo linear algébrico redutivo.

Nos casos típicos em que o grupo finito do tipo Lie G possui um par-BN split em característica p, o caráter de Steinberg St possui uma série de boas propriedades. Nesses casos, temos:

$$St(g) = \begin{cases} \pm|C_G(g)|_p, & \text{se } p \text{ não divide a ordem de } g; \\ 0, & \text{caso contrário.} \end{cases}$$

Dessa forma, o caráter de Steinberg satisfaz a condição $p \nmid \frac{|G|}{St(1)}$ e é, portanto, um exemplo de caráter com p-defeito 0. Neste trabalho, discutiremos em detalhes a construção de St e como calcular os seus valores. Também veremos como o caráter de Steinberg pode ser utilizado para mostrar um Teorema de Gow [14], que é um passo importante na demonstração da Conjectura de Ore [23]. O Teorema de Gow diz que em um grupo finito simples do tipo Lie em característica p, todo elemento g tal que p não divide a ordem de g é um comutador.

Vamos agora apresentar um resumo dos capítulos. No Capítulo 1, revisaremos um pouco de Teoria de Caracteres. Em particular, na Seção 1.3.1 mostraremos alguns critérios para dizer se um elemento $g \in G$ é um comutador.

O Capítulo 2 trata de grupos que possuem um par-BN. É o caso, por exemplo, dos grupos finitos do tipo Lie. Se G é um grupo com par-BN, temos associado um grupo de Coxeter chamado de *grupo de Weyl*. Tal grupo controla fortemente a estrutura de G. Mesmos nos casos em que G é infinito, muitas vezes W é finito e podemos obter bons resultados. É o que ocorre, por exemplo, quando G é um grupo linear algébrico conexo e redutivo. Assim, uma parte substancial desse capítulo é dedicada ao estudo dos grupos de Weyl e dos sistemas de raízes associados. Na Seção 2.3 apresentamos vários exemplos de grupos finitos que possuem par-BN.

No Capítulo 3, discutiremos um pouco sobre a Teoria de Grupos Lineares Algébricos, com ênfase no caso em que a característica do corpo é positiva. Quando G é um grupo linear algébrico redutivo e F é um endomorfismo de Steinberg, então dizemos que G^F é um *grupo finito do tipo Lie*. Tais questões são discutidas na Seção 3.6.

O caráter de Steinberg é discutido no Capítulo 4. Mostraremos como ele pode ser construído em qualquer grupo com par-BN e que é sempre um caráter irredutível de G. Sob a hipótese adicional do par-BN ser *split* e satisfazer a relação dos comutadores, veremos que os valores de St podem ser completamente determinados. Na Seção 4.3 explicaremos do que se trata a Conjectura de Ore e veremos uma aplicação do caráter de Steinberg para tratar de um caso particular dessa conjectura. Na Seção 4.4 discutiremos outras aplicações do caráter de Steinberg, como um resultado que nos permite contar

elementos unipotentes.

Capítulo 1

Teoria de Caracteres

Neste capítulo, o objetivo é discutir alguns resultados de Teoria de Caracteres que serão importantes para os capítulos posteriores. A demonstração de alguns resultados será omitida e maiores detalhes podem ser vistos em [20].

1.1 Álgebras e Representações

Antes de discutir representações, precisamos relembrar a definição de álgebra.

Definição 1.1. Seja A um espaço vetorial sobre um corpo K. Dizemos que A é uma K-*álgebra* se for também um anel com unidade e, para todo $c \in K$ e para todos $x, y \in A$, valer $(cx)y = c(xy) = x(cy)$.

Com a definição de álgebra, podemos definir representações.

Definição 1.2. Seja A uma K-álgebra e V um espaço vetorial sobre K, com $n = \dim_K V$. Dizemos que ρ é uma *representação* de A (com espaço de representação V) se ρ for um homomorfismo de álgebras entre A e $End_K(V)$. O inteiro n é chamado de *grau da representação* ρ.

Se escolhermos uma base para V, podemos identificar $End_K(V)$ com $M_n(K)$, onde $M_n(K)$ denota a álgebra de matrizes $n \times n$ sobre K. Assim, podemos considerar que ρ é um homomorfismo de A para $M_n(K)$. Dizemos que duas representações ρ e σ de mesmo grau n são *equivalentes* se existe uma matriz invertível $P \in M_n(K)$ tal que $\rho(a) = P\sigma(a)P^{-1}$, para todo $a \in A$. Note que se ρ é um homomorfismo entre A e $M_n(K)$ e trocarmos a base do espaço vetorial subjacente, obteremos uma nova representação equivalente à ρ.

Seja G um grupo finito. Podemos associar ao grupo G uma álgebra que consiste de todas as somas formais finitas de elementos de G com coeficientes em K.

Definição 1.3. Seja G um grupo finito e K um corpo. O conjunto $K[G] = \{\sum_{g \in G} a_g g \mid a_g \in K\}$ é chamado de *álgebra de grupo* . As operações em $K[G]$ são definidas da seguinte forma:

$$\left(\sum_{g\in G} a_g g\right) + \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G}(a_g + b_g)g$$

$$\left(\sum_{g\in G} a_g g\right) . \left(\sum_{g\in G} b_g g\right) = \sum_{g\in G} c_g g, \quad \text{onde } c_g = \sum_{\substack{h,k\in G \\ hk=g}} a_h b_k$$

$$\lambda \left(\sum_{g\in G} a_g g\right) = \left(\sum_{g\in G}(\lambda a_g)g\right), \lambda \in K.$$

Note que $K[G]$ é, de fato, uma álgebra sobre K. Um elemento $g \in G$, pode ser visto como elemento de $K[G]$, tomando $a_g = 1$ e $a_h = 0$, para $h \neq g$. Dessa forma, o grupo G forma uma base finita para $K[G]$. Além disso, o elemento neutro é dado por $1_K 1_G$.

A cada representação ρ de $K[G]$ é possível associar um $K[G]$-módulo de forma canônica e vice-versa. Tome V um espaço vetorial de dimensão n sobre K. Assim, podemos definir o produto de um elemento $v \in V$ com $x \in K[G]$ por $xv = \rho(x)(v)$. De modo análogo, para um $x \in K[G]$ fixo, o produto xv está bem-definido para todo $v \in V$. Assim cada x induz um endomorfismo x_V tal que $x_V(v) = xv$ para todo $v \in v$, e a função ρ tal que $\rho(x) = x_V$ é uma representação de $K[G]$. Com essa identificação, temos a seguinte proposição:

Proposição 1.4. *Se V e W são $K[G]$-módulos, então eles são isomorfos se, e somente se, as representações associados a eles são equivalentes.*

Associando módulos a representações, é possível entender melhor a estrutura das representações. Dizemos que uma representação é *irredutível* se o módulo associado a representação é irredutível, isto é, não possui submódulos não triviais. Se um módulo é tal que todo submódulo admite um complemento, então dizemos que o módulo é *completamente redutível*. Com isso, podemos enunciar o Teorema de Maschke.

Teorema 1.5 (Maschke)**.** *Seja G um grupo finito e K um corpo cuja característica não divide a ordem de G. Nessas condições, todo $K[G]$-módulo é completamente redutível.*

Assim, caso as condições do Teorema de Maschke estejam satisfeitas, se uma representação não for irredutível, ela pode ser decomposta em representações de grau menor. Como esse procedimento pode ser repetido para cada uma das outras representações, temos que toda representação pode ser decomposta em representações irredutíveis. Assim, o Teorema de Maschke fornece uma forte justificativa para trabalharmos com representações sobre um corpo de característica 0. Neste trabalho, adotaremos sempre $K = \mathbb{C}$.

Se ρ é uma representação de grau n, temos que a restrição $\rho|_G$ é homomorfismo de G em $GL_n(\mathbb{C})$, pois se $\rho(g)\rho(g^{-1}) = \rho(gg^{-1}) = I$, temos $\rho(g)^{-1} = \rho(g^{-1})$. Neste caso, dizemos que $\rho|_G$ é uma representação de G de grau n. Por outro lado, se φ é uma representação de G, que é uma base para $K[G]$, é possível estender por linearidade φ para uma representação de $K[G]$.

1.2 Caracteres

Um caráter de um grupo é construído a partir de uma representação utilizando o traço das matrizes. Em um primeiro momento, parece que estamos descartando informação, mas na verdade estamos apenas nos concentrando no que é essencial.

Definição 1.6. Seja ρ uma representação de G de grau n. O *caráter associado* a ρ é a função $\chi(g) = tr(\rho(g))$.

A cada representação está associado um caráter, mas o mesmo caráter pode estar associado a diferentes representações. Note que se A e B são duas matrizes quadradas de mesmas dimensões temos $tr(AB) = tr(BA)$. Assim se ρ e σ são duas representações equivalentes, temos $tr(\rho(g)) = tr(P\sigma(g)P^{-1}) = tr(\sigma(g)P^{-1}P) = tr(\sigma(g))$. Portanto representações equivalentes induzem o mesmo caráter. Como estamos considerando $K = \mathbb{C}$, vale também uma recíproca para essa afirmação, se duas representações induzem o mesmo caráter, então elas são equivalentes.

Dizemos que um caráter é *irredutível*, se uma representação associada a ele é irredutível. Assim, pelo resultado anterior, essa definição não depende da escolha da representação pois a irredutibilidade é preservada entre representações equivalentes.

Definição 1.7. Seja $f : G \to \mathbb{C}$. Se f for constante em cada classe de conjugação, dizemos que f é uma *função de classe* de G. O espaço vetorial de todas as funções de classe complexas de G é denotado por $\mathcal{CF}(G)$.

Note que os caracteres são funções de classe, pois se $g = xhx^{-1}$ e ρ é uma representação associada ao caráter χ, temos $\rho(g) = \rho(x)\rho(h)\rho(x^{-1})$, assim $\chi(g) = tr(\rho(x)\rho(h)\rho(x^{-1})) = \chi(h)$. Além disso, $\rho(1) = I_n$, onde I_n é matriz identidade $n \times n$, e daí $\chi(1) = n$, onde n é o grau da representação. O caráter irredutível que assume o valor 1 em todas as classes de conjugação é chamado de *caráter principal* e sua representação associada é o homomorfismo $\rho : G \to GL_1(\mathbb{C})$ tal que $\rho(g) = 1$, para todo $g \in G$. Denotamos por 1_G o caráter principal de G.

Na proposição seguinte, listamos algumas boas propriedades dos caracteres.

Proposição 1.8. *Seja G um grupo finito e $Irr(G)$ o conjunto dos caracteres irredutíveis de G. Então:*

(*i*) *O número de elementos de $Irr(G)$ é igual ao número de classes de conjugação de G.*

(*ii*) $|G| = \sum_{\chi \in Irr(G)} \chi(1)^2$.

(*iii*) *Os caracteres irredutíveis formam uma base para o espaço $\mathcal{CF}(G)$. Mais ainda, se χ é um caráter qualquer, então χ é uma combinação linear de caracteres irredutíveis em que os coeficientes da base são todos inteiros não-negativos e não todos nulos.*

(*iv*) *Se $\chi \in Irr(G)$, então $\chi(1)$ divide a ordem de G.*

(*v*) *Se χ é um caráter de G, a função $\overline{\chi}$ dada por $\overline{\chi}(g) = \overline{\chi(g)}$ também é um caráter de G, chamada de "caráter conjugado" e $\overline{\chi(g)} = \chi(g^{-1})$.*

Naturalmente, nem toda função de classe é um caráter. Se f é uma função de classe em que os coeficientes dos caracteres irredutíveis são todos inteiros, dizemos que f é um *caráter generalizado.*

O espaço das funções de classe pode ser equipado com um produto interno $[\chi, \psi]_G$ da seguinte forma:

$$[\chi, \psi]_G = \frac{1}{|G|} \sum_{g \in G} \chi(g)\overline{\psi(g)}.$$

Quando ficar claro pelo contexto, escreveremos apenas $[\chi, \psi]$. Como as funções de classe são constantes nas classes de conjugação, se particionarmos G em suas r classes de conjugação $\mathscr{K}_1, \mathscr{K}_2, \ldots, \mathscr{K}_r$ e escolhermos representantes para cada classe podemos escrever:

$$[\chi, \psi] = \frac{1}{|G|} \sum_{i=1}^{r} |\mathscr{K}_i| \chi(x_i)\overline{\psi(x_i)}, \text{ onde } x_i \in \mathscr{K}_i.$$

Proposição 1.9 (Primeira Relação de Ortogonalidade)**.** *Se* $Irr(G) = \{\chi_1, \chi_2, \ldots, \chi_r\}$*, então* $[\chi_i, \chi_j] = \delta_{ij}$*, onde* δ_{ij} *é o delta de Kronecker.*

Isso significa que os caracteres irredutíveis não apenas formam uma base para as funções de classe, mas também formam uma base ortonormal. Note que se ψ é um caráter, então $\psi \in Irr(G)$ se, e somente se, $[\psi, \psi] = 1$, pois se $\psi = \sum_{i=1}^{r} a_i \chi_i$ então $[\psi, \psi] = \sum_{i=1}^{r} a_i^2$. Como os a_i são inteiros positivos, temos $[\psi, \psi] = 1$ se, e somente se, exatamente um dos a_i for 1.

Em alguns casos, o resultado abaixo também pode ser útil.

Proposição 1.10 (Segunda Relação de Ortogonalidade)**.** *Sejam* $g, h \in G$ *e* $Irr(G) = \{\chi_1, \chi_2, \ldots, \chi_r\}$*, então*

$$\sum_{\chi \in Irr(G)} \chi(g)\overline{\chi(h)} = \begin{cases} |C_G(g)| & \text{se } g \text{ e } h \text{ são conjugados} \\ 0 & \text{caso contrário} \end{cases}.$$

1.3 O centro da álgebra $\mathbb{C}[G]$

A álgebra $\mathbb{C}[G]$ está intimamente ligada com os caracteres de G. Essa ligação fica mais evidente quando analisamos o centro da álgebra $Z(\mathbb{C}[G])$. Particione G em suas r classes de conjugação $\mathscr{K}_1, \mathscr{K}_2, \ldots, \mathscr{K}_r$. Para cada $\mathscr{K}_i$, considere em $\mathbb{C}[G]$ o elemento $K_i = \sum_{g \in \mathscr{K}_i} g$.

Proposição 1.11. *O conjunto* $\{K_1, K_2, \ldots, K_r\}$ *forma uma base para* $Z(\mathbb{C}[G])$*. Assim, temos* $K_i K_j = \sum a_{ijv} K_v$ *e os* a_{ijv} *são inteiros não-negativos. Os* a_{ijv} *são chamados de* constantes de estrutura *e* $a_{ijv} = |\{(x, y) \mid x \in K_i, y \in K_j, xy = z\}|$*, para cada* $z \in K_v$ *fixado.*

Demonstração. Os K_i são linearmente indepedentes, pois estamos somando elementos de subconjuntos disjuntos de uma base para $\mathbb{C}[G]$. Note que para um elemento $z \in \mathbb{C}[G]$ pertencer ao centro é suficiente que $z = gzg^{-1}$, para todo $g \in G$. Assim ao conjugar K_i

por um elemento de $g \in G$, temos que gK_ig^{-1} é apenas uma permutação da ordem em que os elementos de $\mathscr{K}_i$ aparecem na soma K_i. Dessa forma, $gK_ig^{-1} = K_i$ e $K_i \in Z(K[G])$.

Agora se $z = \sum a_g g \in Z(\mathbb{C}[G])$, temos $z = hzh^{-1}$, para todo $h \in G$. Isso significa $\sum a_g g = \sum a_g hgh^{-1}$, para todo $h \in G$. Assim, se g e k são conjugados, existe um h tal que $hgh^{-1} = k$. Dessa forma, o coeficiente de g é igual ao coeficiente de k. Portanto, em cada classe de conjugação, o coeficiente de z é constante e z pode ser escrito como combinação linear dos K_i.

O centro da álgebra é uma subálgebra, então $K_iK_j \in Z(\mathbb{C}[G])$ e $K_iK_j = \sum a_{ijv}K_v$. Novamente, isso significa que o coeficiente a_{ijv} é o mesmo para todos os $g \in \mathscr{K}_v$. Assim, a_{ijv} é o número de vezes que um elemento g da v-ésima classe de conjugação é escrito como um produto de um elemento da i-ésima classe de conjugação com um elemento da j-ésima classe de conjugação. Portanto, a_{ijv} é um inteiro não-negativo pois é a cardinalidade de um conjunto. □

Antes de prosseguir, precisamos de um lema.

Lema 1.12 (Schur)**.** *Seja ρ uma representação irredutível de $\mathbb{C}[G]$ de grau n. Se $A \in M_n(\mathbb{C})$ é tal que $A\rho(g) = \rho(g)A$, para todo $g \in G$, então $A = \lambda I_n$, com $\lambda \in \mathbb{C}$.*

Demonstração. Tome V simultaneamente espaço vetorial sobre $\mathbb{C}$ e um $\mathbb{C}[G]$-módulo irredutível correspondendo à ρ. Denote por $\mathbb{C}[G]_V$ o conjunto $\{\rho(x) \mid x \in \mathbb{C}[G]\}$, que é um subconjunto de $End(V)$. A matriz A pode ser vista como elemento de $End(V)$, mas além disso, A também preserva a estrutura de $\mathbb{C}[G]$-módulo de V. Para verificar isso, basta observar que A é uma transformação linear e $A(\rho(x)(v)) = \rho(x)A(v)$, justamente por A comutar com os elementos de $\mathbb{C}[G]_V$. Segue que A é um endomorfismo de $\mathbb{C}[G]$-módulos.

Como $\ker A$ e ImA são submódulos de V, temos ou $\ker A = 0$ ou $\ker A = V$, pois V é irredutível. No segundo caso, temos $A = 0$. No primeiro caso, A é uma matriz invertível. Como $\mathbb{C}$ é algebricamente fechado, A tem pelo menos um autovalor λ. Agora, $A - \lambda I_n$ também comuta com os elementos de $\mathbb{C}[G]_V$. Pelo mesmo argumento, temos que $A - \lambda I_n$ é invertível ou é zero. Mas como λ é autovalor, concluímos que $A = \lambda I_n$.

□

Se ρ é uma representação associada a um caráter irredutível χ, então as imagens dos elementos de $Z(\mathbb{C}[G])$ comutam com todos os $\rho(x)$, para $x \in \mathbb{C}[G]$ e, pelo Lema 1.12 $\rho(y) = \lambda_y I_n$, para $y \in Z(\mathbb{C}[G])$. Isso motiva a nossa próxima definição.

Definição 1.13. Seja ρ uma representação associada ao caráter irredutível χ. O *caráter central associado* à χ, denotado por $\omega_\chi : Z(\mathbb{C}[G]) \to \mathbb{C}$, é o homomorfismo de álgebras tal que, para todo $x \in Z(\mathbb{C}[G])$, temos $\rho(x) = \omega_\chi(x)I_n$.

Um fato importante que deixamos registrado aqui é que os valores do caráter central são inteiros algébricos. Uma demonstração desse fato pode ser encontrada em [20, Teorema 3.7]. Se um inteiro algébrico for um número racional, então ele deve ser também um número inteiro.

Proposição 1.14. *Seja $\chi \in Irr(G)$ e K uma soma de classe de conjugação, então $\omega_\chi(K)$ é um inteiro algébrico.*

Tome ρ uma representação de grau n associada a χ e seja K_i a soma dos elementos da classe de conjugação $\mathscr{K}_i$. Temos $\rho(K_i) = \omega_\chi(K_i)I_n$ e tomando os traços das matrizes, obtemos $\chi(g)|\mathscr{K}_i| = \omega_\chi(K_i)\chi(1)$, para $g \in \mathscr{K}_i$. Assim, $\omega_\chi(K_i) = \frac{\chi(g)|\mathscr{K}_i|}{\chi(1)}$. Com o auxílio do caráter central, que pode ser obtido através da tabela de caracteres, podemos calcular as constantes de estrutura.

Proposição 1.15. *Sejam $\mathscr{K}_1, \mathscr{K}_2, \ldots, \mathscr{K}_r$ as classes de conjugação de um grupo finito G. Se K_i e K_j são as somas correspondentes às classes $\mathscr{K}_i$ e $\mathscr{K}_j$, então $K_iK_j = \sum_{v=1}^{r} a_{ijv}K_v$ e*

$$a_{ijv} = \frac{|\mathscr{K}_i||\mathscr{K}_j|}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi(x_i)\chi(x_j)\overline{\chi(x_v)}}{\chi(1)}, \tag{1.1}$$

onde x_i é um representante de $\mathscr{K}_i$.

Demonstração. Aplicando o homomorfismo ω_χ dos dois lados da equação $K_iK_j = \sum a_{ijl}K_l$, obtemos:

$$\frac{\chi(x_i)|\mathscr{K}_i|}{\chi(1)} \frac{\chi(x_j)|\mathscr{K}_j|}{\chi(1)} = \sum_{l=1}^{r} a_{ijl} \frac{\chi(x_l)|\mathscr{K}_l|}{\chi(1)}.$$

Simplificando a expressão e multiplicando por $\overline{\chi(x_v)}$ dos dois lados temos:

$$\frac{|\mathscr{K}_i||\mathscr{K}_j|\chi(x_i)\chi(x_j)\overline{\chi(x_v)}}{\chi(1)} = \sum_{l=1}^{r} a_{ijl}|\mathscr{K}_l|\chi(x_l)\overline{\chi(x_v)}.$$

Agora, a idéia é considerar essa expressão somada em relação a todos os caracteres irredutíveis de G.

$$\begin{aligned}
\sum_{\chi \in Irr(G)} \frac{|\mathscr{K}_i||\mathscr{K}_j|\chi(x_i)\chi(x_j)\overline{\chi(x_v)}}{\chi(1)} &= \sum_{\chi \in Irr(G)} \sum_{l=1}^{r} a_{ijl}|\mathscr{K}_l|\chi(x_l)\overline{\chi(x_v)} \\
&= \sum_{l=1}^{r} a_{ijl}|\mathscr{K}_l| \sum_{\chi \in Irr(G)} \chi(x_l)\overline{\chi(x_v)} \\
&= \sum_{l=1}^{r} a_{ijl}|\mathscr{K}_l||C_G(x_l)|\delta_{lv} \quad (\delta_{lv} \text{ é o delta de Kronecker}) \\
&= a_{ijv}|\mathscr{K}_v||C_G(x_v)|.
\end{aligned}$$

A penúltima igualdade segue da segunda relação de ortogonalidade. Como $|\mathscr{K}_v| = \frac{|G|}{|C_G(x_v)|}$, isolando a_{ijv} na última igualdade obtemos:

$$a_{ijv} = \frac{|\mathscr{K}_i||\mathscr{K}_j|}{|G|} \sum_{\chi \in Irr(G)} \frac{\chi(x_i)\chi(x_j)\overline{\chi(x_v)}}{\chi(1)}.$$

□

1.3.1 Resultados sobre comutadores

As constantes de estrutura a_{ijv} contam de quantas formas distintas um elemento qualquer da classe de conjugação $\mathscr{K}_v$ pode ser escrito como produto de um elemento da classe $\mathscr{K}_i$ pela classe $\mathscr{K}_j$. Esse tipo de informação nos ajuda a descobrir, por exemplo, quando um elemento em um grupo G é um comutador $[x,y] = xyx^{-1}y^{-1}$.

Proposição 1.16. *Sejam g, x elementos fixos em G. Então g é conjugado a $[x,y]$ para algum $y \in G$ se, e somente se,*

$$\sum_{\chi \in Irr(G)} \frac{|\chi(x)|^2 \overline{\chi(g)}}{\chi(1)} \neq 0.$$

Demonstração. Note que $\chi(x)\chi(x^{-1}) = \chi(x)\overline{\chi(x)} = |\chi(x)|^2$. Assim, pela Proposição 1.15, temos $\sum_{\chi \in Irr(G)} \frac{|\chi(x)|^2 \overline{\chi(g)}}{\chi(1)} \neq 0$ se, e somente se $a_{ijv} \neq 0$, onde $x \in \mathscr{K}_i$, $x^{-1} \in \mathscr{K}_j$ e $g \in \mathscr{K}_v$.

Se a_{ijv} é não-nulo, então existem $a \in \mathscr{K}_i$ e $b \in \mathscr{K}_j$ tal que $ab = g$. Porém, a é conjugado à x e b é conjugado à x^{-1}. Então, para certos $h, k \in G$, temos $a = hxh^{-1}$ e $b = kx^{-1}k^{-1}$. Assim:

$$\begin{aligned} g &= ab \\ &= hxh^{-1}kx^{-1}k^{-1} \\ &= h(xh^{-1}kx^{-1}k^{-1}h)h^{-1} \\ &= h[x, h^{-1}k]h^{-1}. \end{aligned}$$

Agora, se g é conjugado a $[x,y]$, para algum $y \in G$, temos $xyx^{-1}y^{-1} = hgh^{-1}$, para algum $h \in G$. Como $x \in \mathscr{K}_i$ e $yx^{-1}y^{-1} \in \mathscr{K}_j$, temos que a_{ijv} não pode ser 0, pois pelo menos um conjugado de g é produto de um elemento de $\mathscr{K}_i$ por um de $\mathscr{K}_j$. □

Note que para um elemento g ser um comutador é suficiente que ele seja conjugado a um comutador. Afinal, se $g = hxyx^{-1}y^{-1}h^{-1}$, temos $g = [hxh^{-1}, hyh^{-1}]$.

Denote por $\Lambda(g)$ a cardinalidade do conjunto $\{(x,y) \in G \times G \mid [x,y] = g\}$. Observe que $\Lambda(g)$ é uma função de classe, pois se g e h são conjugados, existe k tal que $kgk^{-1} = h$, dessa forma, se $g = [x,y]$, então $[kxk^{-1}, kyk^{-1}] = h$. Como a conjugação por um elemento fixo é um automorfismo de G, estabelecemos uma bijeção entre os pares (x,y) e os pares (kxk^{-1}, kyk^{-1}). Portanto $\Lambda(g) = \Lambda(h)$. Sendo uma função de classe, $\Lambda(g)$ pode ser expressa como combinação linear de caracteres irredutíveis.

Proposição 1.17. *O número $\Lambda(g)$ de pares (x,y) tais que $g = [x,y]$ é dado por:*

$$\Lambda(g) = |G| \sum_{\chi \in Irr(G)} \frac{\chi(g)}{\chi(1)}.$$

Em particular, Λ é um caráter do grupo G.

Este é um antigo resultado devido a Frobenius [11], mas como é difícil de encontrar o artigo, optamos por demonstrar este resultado aqui.

Demonstração. Tome $g, x \in G$ fixos. Se $\mathscr{K}_i$ é a classe de conjugação de x, $\mathscr{K}_{i'}$ é a classe de x^{-1} e $\mathscr{K}_v$ é a classe de g, a constante de estrutura $a_{ii'v}$ conta de quantas formas é

possível escrever um elemento fixado da classe de g como um produto de elementos das classes $\mathscr{K}_i$ e $\mathscr{K}_{i'}$.

Como observado na demonstração da Proposição 1.16, se $g = ab$ para $a = hxh^{-1} \in \mathscr{K}_i$ e e $b = kx^{-1}k^{-1} \in \mathscr{K}_i$, então g é conjugado a um comutador da forma $[x, h^{-1}k]$. Em particular g é também um comutador, porém, da forma $[hxh^{-1}, kh^{-1}] = [a, hk^{-1}]$.

Considere a função auxiliar Λ_i, onde $\Lambda_i(g)$ é a cardinalidade do conjunto $A_i = \{(x, y) \mid x \in \mathscr{K}_i, y \in G, x(yx^{-1}y^{-1}) = g\}$. Evidentemente, se tivermos r classes de conjugação temos $\Lambda(g) = \sum_{i=1}^{r} \Lambda_i(g)$. Agora, compare A_i com o conjunto $B_i = \{(hxh^{-1}, kx^{-1}k^{-1}) \mid h, k \in G, (hxh^{-1})(kx^{-1}k^{-1}) = g\}$. Note que $|B_i| = a_{ii'v}$.

A diferença entre esses dois conjuntos é que em A_i, se (x, y_1) e (x, y_2) são pares tais que $y_1x^{-1}y_1^{-1} = y_2x^{-1}y_2^{-1}$, mas y_1 é diferente de y_2, então eles são contados como elementos distintos. Já em B_i esse par seria contado apenas uma única vez, através do par $(x, y_1x^{-1}y_1^{-1})$. Assim o mesmo conjugado de x^{-1} aparece várias vezes em elementos de A_i. Para contar o tamanho do excesso, basta lembrar que existe uma bijeção entre os elementos da classe de conjugação $\mathscr{K}_{i'}$ e as classes laterais de $C_G(x^{-1})$ em G. Tome T um conjunto de representantes das classes laterais de $C_G(x^{-1})$ em G. Temos $G = \cup_{t\in T} tC_G(x^{-1})$ e $t_1x^{-1}t_1^{-1} \neq t_2x^{-1}t_2^{-1}$, se $t_1 \neq t_2$. Dessa forma, para cada x temos que cada conjugado de x^{-1} é contado $|C_G(x^{-1})|$ vezes em A_i. Além disso, o tamanho do centralizador é o mesmo para todos os elementos da classe de conjugação $\mathscr{K}_{i'}$ e, independentemente de x e x^{-1} estarem na mesma classe de conjugação ou não, é verdade que $|C_G(x^{-1})| = |C_G(x)|$. Isso nos permite concluir que $|A_i| = |B_i||C_G(x^{-1})| = a_{ii'v}|C_G(x_i)|$, onde $x_i \in \mathscr{K}_i$. Agora podemos calcular $\Lambda(g)$ por meio das constantes de estrutura. Então:

$$
\begin{aligned}
\Lambda(g) &= \sum_{i=1}^{r} \Lambda_i(g) \\
&= \sum_{i=1}^{r} a_{ii'v}|C_G(x_i)| \\
&= \sum_{i=1}^{r} \frac{|\mathscr{K}_i||\mathscr{K}_{i'}|}{|G|} \sum_{\chi\in Irr(G)} \frac{\chi(x_i)\chi(x_{i'})\overline{\chi(g)}}{\chi(1)}|C_G(x_i)| \\
&= \sum_{i=1}^{r} \frac{|\mathscr{K}_i||\mathscr{K}_i||G|}{|G||\mathscr{K}_i|} \sum_{\chi\in Irr(G)} \frac{\chi(x_i)\chi(x_{i'})\overline{\chi(g)}}{\chi(1)} \qquad (\text{pois } |C_G(x_i)| = \frac{|G|}{|\mathscr{K}_i|} \text{ e } |\mathscr{K}_i| = |\mathscr{K}_{i'}|\ ) \\
&= \sum_{i=1}^{r} \sum_{\chi\in Irr(G)} \frac{|\mathscr{K}_i||\chi(x_i)|^2\overline{\chi(g)}}{\chi(1)} \qquad (\text{pois } \chi(x_{i'}) = \chi(x^{-1}) = \overline{\chi(x)}) \\
&= \sum_{\chi\in Irr(G)} \frac{\overline{\chi(g)}}{\chi(1)} \sum_{i=1}^{r} |\mathscr{K}_i||\chi(x_i)|^2 \\
&= \sum_{\chi\in Irr(G)} \frac{\overline{\chi(g)}}{\chi(1)}|G|.
\end{aligned}
$$

A última igualdade, vem do fato de que os x_i são representantes das r classes de conjugação, portanto $[\chi, \chi] = 1 = \frac{1}{|G|}\sum_{i=1}^{r} |\mathscr{K}_i||\chi(x_i)|^2$. Agora, $\Lambda(g)$ é a cardinalidade de um conjunto, então $\Lambda(g)$ é um número inteiro não-negativo, portanto $\Lambda(g) = \overline{\Lambda(g)} =$

$\sum_{\chi\in Irr(G)} \frac{\chi(g)}{\chi(1)}|G|$, que é precisamente a fórmula que queríamos. Observe que $\Lambda(g)$ é uma combinação linear de caracteres irredutíveis em que o coeficiente de cada χ é $\frac{|G|}{\chi(1)}$, que é um inteiro positivo (veja Proposição 1.8). Portanto, $\Lambda(g)$ é um caráter de G. □

Com isso, obtemos também o seguinte corolário:

Corolário 1.18. *Um elemento $g \in G$ é um comutador $[x, y]$ para alguns $x, y \in G$, se, e somente se, $\sum_{\chi\in Irr(G)} \frac{\chi(g)}{\chi(1)} \neq 0$.*

A prova do corolário é imediata, pois $\Lambda(g) \neq 0$ se, e somente se, $\sum_{\chi\in Irr(G)} \frac{\chi(g)}{\chi(1)} \neq 0$. De toda forma, vamos apresentar uma demonstração desse fato de forma independente da Proposição 1.17.

Demonstração. Observe que se $\sum_{\chi\in Irr(G)} \frac{\chi(g)}{\chi(1)} \neq 0$ e g não é um comutador, então para cada x fixo não existe $y \in G$ tal que g seja conjugado a $[x, y]$. Pela Proposição 1.16, devemos ter, para todo $x \in G$, $\sum_{\chi\in Irr(G)} \frac{|\chi(x)|^2\overline{\chi(g)}}{\chi(1)} = 0$. Em particular, somando em todos os x, temos:

$$\begin{aligned} 0 &= \sum_{x\in G}\sum_{\chi\in Irr(G)} \frac{|\chi(x)|^2\overline{\chi(g)}}{\chi(1)} \\ &= \sum_{\chi\in Irr(G)} \frac{\overline{\chi(g)}}{\chi(1)} \sum_{x\in G} |\chi(x)|^2 \\ &= |G| \sum_{\chi\in Irr(G)} \frac{\overline{\chi(g)}}{\chi(1)}. \end{aligned}$$

A última igualdade vem da primeira relação de ortogonalidade, pois para um caráter irredutível $|G|[\chi, \chi] = |G| = \sum_{x\in G} |\chi(x)|^2$. A última equação implica $\sum_{\chi\in Irr(G)} \frac{\chi(g)}{\chi(1)} = 0$, o que é um absurdo.

Se g é um comutador da forma $[x, y]$, em particular, ele é conjugado a $[x, y]$ e temos que $\sum_{\chi\in Irr(G)} \frac{|\chi(x)|^2\overline{\chi(g)}}{\chi(1)} \neq 0$, mas mais do que isso, esse número é real e maior que 0, pois é igual a $\frac{|G|a_{ijv}}{|\mathscr{K}_i||\mathscr{K}_j|}$. Assim, se somarmos essa quantia em relação a todos os x, o resultado será maior do que 0. Manipulando de forma idêntica, obtemos:

$$\sum_{x\in G}\sum_{\chi\in Irr(G)} \frac{|\chi(x)|^2\overline{\chi(g)}}{\chi(1)} = |G| \sum_{\chi\in Irr(G)} \frac{\overline{\chi(g)}}{\chi(1)}.$$

Como o lado esquerdo da equação é diferente de 0, concluímos que $\sum_{\chi\in Irr(G)} \frac{\chi(g)}{\chi(1)}$ também tem que ser diferente de 0.

□

1.4 Indução e restrição de caracteres

Se H é um subgrupo de um grupo G e α é uma função de classe de H, denotamos por α^G a *função de classe induzida de H a G* definida por:

$$\alpha^G(g) = \frac{1}{|H|} \sum_{\substack{x \in G \\ xgx^{-1} \in H}} \alpha(xgx^{-1}).$$

Note que α^G é, de fato, uma função de classe em G. Pois se $ygy^{-1} = h$, o somatório acima não se altera se substituirmos x por xy, para y fixo. Porém, não é evidente que se χ é um caráter de H, então χ^G também será um caráter de G. Isso é verdade e será uma consequência da *reciprocidade de Frobenius*. Observe que $\alpha^G(1) = |G : H|\alpha(1)$

Se α é uma função de classe de G, denotamos por α_H a restrição de α a H. Se dois elementos de H são conjugados em H, eles também são conjugados em G. Assim, α_H é também uma função de classe. Em particular, se χ é um caráter de G, então χ_H também é um caráter de H. Afinal, se ρ é uma representação de G, a restrição de ρ à H é uma representação de H que dá origem ao caráter χ_H. Entretanto, se χ for irredutível nem sempre χ_H será irredutível também.

Proposição 1.19 (Reciprocidade de Frobenius)**.** *Se H é um subgrupo de G e α é uma função de classe de G e β uma função de classe de H, temos*

$$[\beta^G, \alpha]_G = [\alpha_H, \beta]_H.$$

Demonstração. Ver [20, Lema 5.2]. □

Agora, se ψ é um caráter de H, então para todo caráter irredutível $\chi \in Irr(G)$ temos que $[\chi, \psi^G]_G = [\chi_H, \psi]_H$ é um inteiro não-negativo. Pelo menos $\psi^G(1)$ é diferente de 0, então ψ^G não é nulo. Assim, ψ^G é um caráter de G.

Se H e K são subgrupos de um grupo G e T é um subconjunto de G tal que $G = \dot{\bigcup}_{t \in T} HtK$, então diz-se que T é um conjunto de *representantes das classes laterais duplas* em relação aos subgrupos H e K. Em geral, escolhe-se T tal que $1 \in T$. Com isso, temos o seguinte resultado:

Proposição 1.20 (Fórmula de Mackey)**.** *Seja G um grupo e K, H subgrupos de G. Se χ é um caráter de K e T é um conjunto de representantes das classes laterais duplas em relação aos subgrupos H e K, então*

$$(\chi^G)_H = \sum_{t \in T} ({}^t\chi)_{H \cap tKt^{-1}})^H,$$

onde $({}^t\chi)$ é o caráter de tKt^{-1} tal que $({}^t\chi)(tkt^{-1}) = \chi(k)$.

Demonstração. Ver [19, Teorema 17.4]. □

Como consequência, temos o seguinte corolário:

Corolário 1.21. *Se φ e χ são caracteres de subgrupos H e K de um grupo G e T é um representantes das classes laterais duplas, temos:*

$$[\varphi^G, \chi^G] = \sum_{t \in T} [\varphi, {}^t\chi]_{H \cap tKt^{-1}}.$$

Note que no lado direito da expressão acima, estamos cometendo um pequeno abuso de notação, pois escrevemos φ ao invés de $\varphi_{H \cap tKt^{-1}}$ e ${}^t\chi$ ao invés de ${}^t\chi_{H \cap tKt^{-1}}$

Demonstração.

$$\begin{aligned}
[\varphi^G, \chi^G]_G &= [\varphi, (\chi^G)_H]_H \\
&= [\varphi, \sum_{t \in T} (({}^t\chi)_{H \cap tKt^{-1}})^H]_H && \text{(pela Proposição 1.20)} \\
&= \sum_{t \in T} [\varphi, (({}^t\chi)_{H \cap tKt^{-1}})^H]_H \\
&= \sum_{t \in T} [\varphi, {}^t\chi]_{H \cap tKt^{-1}} && \text{(pela Proposição 1.20) .}
\end{aligned}$$

□

Capítulo 2

Grupos com Par-BN

O caráter de Steinberg é definido em termos de caracteres induzidos dos subgrupos parabólicos de um grupo com par-BN. Neste capítulo discutiremos precisamente esses grupos que possuem um par-BN e alguns conceitos relacionados.

Definição 2.1 (Par-BN)**.** Dois subgrupos B e N de um grupo G formam um par-BN se:

(*i*) G é gerado por B e N.

(*ii*) $B \cap N$ é normal em N.

(*iii*) O grupo $N/(B \cap N) = W$ é gerado por elementos s_i com $i \in I$ tais que $s_i^2 = 1$. W é chamado de grupo de *Weyl* e $|I|$ é chamado de *posto* do par-BN.

(*iv*) Seja $\pi : N \twoheadrightarrow W$ o homomorfismo quociente, se $n_i \in \pi^{-1}(s_i)$ então $(Bn_iB)(BnB) \subseteq Bn_inB \cup BnB$, para todo $n \in N$.

(*v*) Se $n_i \in \pi^{-1}(s_i)$, então $n_iBn_i \neq B$.

Para alguns grupos do tipo Lie, o par-BN é construído naturalmente de forma a atender as condições acima e na Seção 2.3 construíremos alguns exemplos de grupos com pares-BN.

2.1 Raízes e grupos de Weyl

Nesta seção discutiremos alguns conceitos importantes relacionados aos sistemas de raízes e o grupo de Weyl. Esta seção é um apanhado de resultados encontrados em [17, Capítulos 2 e 5], [13, Capítulos 1 e 2], [5, Capítulo 2] e [6, Capítulo 2].

Seja V um espaço vetorial real de dimensão finita equipado com um produto interno $\langle ., . \rangle$. Dado $r \in V$, denotaremos por w_r a reflexão com respeito ao hiperplano ortogonal ao vetor r. Neste caso, temos:

$$w_r(x) = x - \frac{2\langle r, x \rangle}{\langle r, r \rangle} r.$$

Note que estamos usando o termo "reflexão" num sentido mais geral, já que não necessariamente o produto interno é o produto euclideano. Com isso, temos a seguinte definição:

Definição 2.2 (Sistema de Raízes)**.** Seja V um espaço vetorial equipado com produto interno $\langle .,. \rangle$. Seja Φ um conjunto finito de vetores não-nulos de V. Dizemos que Φ é um *sistema de raízes de* V se:

(i) $\Phi \cap \mathbb{R}r = \{r, -r\}$, para todo $r \in \Phi$, isto é, para $r \in \Phi$, temos $\pm r \in \Phi$ e estes são os únicos múltiplos de r que estão em Φ.

(ii) Φ é um conjunto gerador de V.

(iii) Para todos $r, s \in \Phi$, temos $w_r(s) \in \Phi$.

(iv) (*Condição Cristalográfica*) Para todos $r, s \in \Phi$, $2\frac{\langle r,x \rangle}{\langle r,r \rangle}$ é um inteiro.

Dado um sistema de raízes Φ, *o grupo de Weyl*, denotado por W, é o grupo gerado por todas as reflexões w_r, para $r \in \Phi$. Veremos adiante que o grupo W de um grupo com um par-BN também é um grupo de Weyl neste sentido e mostraremos como associar um conjunto de raízes adequado a ele.

Observe que W age sobre Φ, pois $w \in W$ é um produto de elementos da forma w_r, para $r \in \Phi$. Assim, se $s \in \Phi$ temos $w_r(s) \in \Phi$ e, assim, $w(s) \in \Phi$. Como Φ gera todo o espaço vetorial V, se $w, w' \in W$ são elementos distintos deve existir $r \in \Phi$ tal que $w(r) \neq w'(r)$. Segue que W age de forma fiel sobre Φ. Através dessa ação W pode ser visto como um subgrupo do grupo das permutações de Φ, portanto, W é um grupo finito pois Φ é finito.

O fato de Φ gerar todo o espaço vetorial V, implica que Φ contém uma base de V. Gostaríamos, porém, de obter uma base contida em Φ que seja relativamente fácil de trabalhar. Para esse fim, introduziremos uma relação de ordem em V da seguinte forma:

1. Fixe uma base $B = \{e_1, \ldots, e_n\}$ de V.

2. Defina o conjunto V^+ como sendo o conjunto dos vetores de $v \in V$ tal que a primeira coordenada não-nula de v na base B é positiva.

3. Para $u, v \in V$ escreveremos $u \prec v$ se $v - u \in V^+$. Isso significa que se $u = \sum a_i e_i$ e $v = \sum b_j e_j$ e k é o menor índice tal que $a_k \neq b_k$, então $a_k < b_k$. Essa é a chamada *ordem lexicográfica*.

Assim, se $v \neq 0$, temos $v \in V^+$ ou $-v \in V^+$. Portanto, uma tal relação de ordem particiona Φ em exatamente duas partes iguais. Escreveremos $\Phi^+ = \Phi \cap V^+$ e diremos que os elementos de Φ^+ são as *raízes positivas*. Temos também $\Phi^- = \Phi \setminus \Phi^+$, que é o conjunto das raízes negativas de Φ.

Se B é uma base de V, podemos trocar cada elemento $v \in B$ por $\pm v$ que continuaremos tendo uma base de V. Dessa forma, fica claro que Φ^+ também tem que conter uma base de V.

Definição 2.3 (Sistema de Raízes Fundamentais)**.** Um subconjunto Δ de Φ é um dito um *sistema de raízes fundamentais* ou de *raízes simples de* V se:

(i) Δ é uma base de V.

(ii) Toda raiz de Φ pode escrita como uma combinação linear de elementos de Δ em que os coeficientes são todos não-positivos ou todos não-negativos.

Note que se existe um sistema de raízes fundamentais Δ, podemos tomá-lo como uma base para V e Φ^+ coincidirá com o conjunto $\{v \in \Phi \mid v = \sum a_i r_i,\ r_i \in \Delta, a_i \geq 0,\ \text{para todo } i\}$. Assim, Δ determina Φ^+. Não fica claro, porém, que Φ sempre contém um sistema de raízes fundamentais. Este é precisamente o objetivo da proposição seguinte.

Proposição 2.4. *Fixada uma base para V, dado $\Phi^+ = \Phi \cap V^+$ existe um único $\Delta \subseteq \Phi^+$ tal que Δ é um sistema fundamental de raízes de V.*

Demonstração. Escolha $\Delta \subseteq \Phi^+$ com as seguintes propriedades:

(i) Toda raiz em Φ^+ pode ser expressa como combinação linear com coeficientes não-negativos de raízes de Δ.

(ii) Nenhum subconjunto de Δ possui a propriedade (i).

Um tal subconjunto existe, pois o próprio Φ^+ possui a propriedade (i). Se conseguirmos mostrar que Δ é um conjunto linearmente independente, então será suficiente para mostrar que Δ é um sistema fundamental de raízes. Primeiro, vamos mostrar que se $r, s \in \Delta$, então $\langle r, s\rangle \leq 0$. Suponha $\langle r, s\rangle > 0$ e faça $\lambda = 2\frac{\langle r,s\rangle}{\langle r,r\rangle}$.

Vamos considerar o que acontece se $w_r(s) \in \Phi^+$. Neste caso, pela propriedade (i) temos $w_r(s) = \sum_{r_i \in \Delta} a_i r_i$, com $a_i \geq 0$ e, assim:

$$\sum_{r_i \in \Delta} a_i r_i = s - \lambda r.$$

Daí $\lambda r - s + \sum_{r_i \in \Delta} a_i r_i = 0$. Se a_j é o coeficiente de s no somatório da expressão anterior, podemos escrever a expressão assim:

$$(a_j - 1)s + \lambda r + \sum_{r_i \in \Delta \setminus \{s\}} a_i r_i = 0.$$

Todos os vetores de Δ estão em V^+, assim uma combinação linear positivas de vetores de Δ continua em V^+. Porém, $0 \notin V^+$ e, assim, para evitarmos cair em contradição precisamos ter $a_j - 1 \leq 0$. Passando s para o outro lado da equação, obtemos:

$$\lambda r + \sum_{r_i \in \Delta \setminus \{s\}} a_i r_i = (1 - a_j)s.$$

Assim, s pode ser escrito como uma combinação linear com coeficientes positivos de vetores de $\Delta \setminus \{s\}$ e isso viola a escolha que fizemos de Δ. Logo, devemos ter que $w_r(s) \in \Phi^-$ e portanto $-w_r(s) \in \Phi^+$. Nesse caso, $-w_r(s) = \sum_{r_i \in \Delta} a_i r_i$ e temos:

$$s - \lambda r + \sum_{r_i \in \Delta} a_i r_i = 0.$$

Denotando por a_l o coeficiente de r no somatório obtemos:

$$(a_l - 1)r + s + \sum_{r_i \in \Delta \setminus \{r\}} a_i r_i = 0.$$

De modo análogo, devemos ter $a_l - 1 \leq 0$, mas isso implica que r é uma combinação linear positiva de elementos de $\Delta \setminus \{r\}$, o que não pode ocorrer pela escolha de Δ. Todas

essas contradições surgiram por assumirmos que $\langle r, s\rangle > 0$. Então, devemos ter $\langle r, s\rangle \leq 0$. Com isso, vamos mostrar que Δ é um conjunto linearmente independente.

Suponha que $\sum_{r_i \in \Delta} a_i r_i = 0$. Podemos separar os coeficientes do somatório e deixar os coeficientes positivos do lado esquerdo e os negativos do lado direito da equação obtendo $\sum b_i r_i = \sum c_i s_i$ com $b_i \geq 0$, $c_i \geq 0$ e cada s_i distinto de cada r_i. Se tomarmos o vetor $v = \sum b_i r_i$, temos:

$$\langle v, v\rangle = \sum_i \sum_j b_i c_j \langle r_i, s_j\rangle.$$

Como cada r_i é distinto de cada s_j e $b_i c_j \geq 0$, temos $\langle v, v\rangle \leq 0$ e daí $v = 0$. Novamente, como $0 \notin V^+$, $a_i \geq 0$ e $r_i \in V^+$ devemos ter $a_i = 0$, para todo i. Isso mostra que Δ é linearmente independente.

□

Com isso, sempre podemos admitir que Φ contém um sistema fundamental de raízes. Mais ainda, os subconjuntos Φ^+ e Δ determinam um ao outro. Um fato importante é que W é gerado pelos w_r com $r \in \Delta$. Como w_r é uma involução, temos que a ordem de $w_r w_s$ para $r, s \in \Delta$ é igual à ordem de $w_s w_r = (w_r w_s)^{-1}$. Se denotarmos o conjunto dos geradores que correspondem às raízes fundamentais por $\{s_i \mid i \in I\}$, onde I é um conjunto de índices $\{1, \ldots, \ell\}$, então W satisfaz relações da forma $(s_i s_j)^{m_{ij}} = 1$, onde $m_{ii} = 1$, $m_{ij} = m_{ji}$ e $m_{ij} \geq 2$, quando $j \neq i$.

O fato é que essas relações são suficientes para determinar o grupo W todo. Assim W possui a apresentação $\langle s_i, i \in I \mid (s_i s_j)^{m_{ij}} = 1\rangle$, onde m_{ij} tem as propriedades descritas acima. Um grupo que possui uma apresentação dessa forma é chamado um*grupo de Coxeter*. Deixaremos esse fato registrado como uma proposição cuja demonstração pode ser vista em [5, Proposição 2.1.8] ou em [13, Teorema 1.2.7].

Proposição 2.5. *O grupo de Weyl é um grupo de Coxeter finito gerado pelas reflexões associadas às raízes fundamentais. Além disso, nenhum subconjunto próprio de I gera W.*

O conjunto de geradores não é necessariamente único, pois Φ pode conter vários sistemas de raízes fundamentais. Por exemplo, se Δ é um sistema de raízes fundamental, $-\Delta$ também o é. Na verdade, W também age sobre o conjunto dos sistemas fundamentais.

Proposição 2.6. *O grupo W age sobre o conjunto dos sistemas fundamentais de raízes de Φ, além disso essa ação possui as seguintes propriedades:*

(i) Se Δ_1 e Δ_2 são sistemas de raízes fundamentais existe um único $w \in W$ tal que $w(\Delta_1) = \Delta_2$.

(ii) Em particular, se $w(\Delta) = \Delta$, então $w = 1$.

Demonstração. Ver [5, Teorema 2.2.4]. □

2.1.1 A função comprimento

A partir desta seção, utilizaremos I para indicar um conjunto de índices tal que cada r_i é uma raiz fundamental distinta e w_i é o gerador w_{r_i}. Fixado um conjunto de geradores para

o grupo de Weyl W, estamos interessados em saber, para $w \in W$, qual o comprimento da menor expressão de w como um produto de geradores.

Definição 2.7. A função l que associa a cada $w \in W$ o comprimento $l(w)$ da menor expressão de w como um produto de geradores é chamada de *função comprimento*. Convenciona-se que o comprimento do elemento identidade é 0.

Se $w = w_1 w_2 \dots w_m$ e cada w_i é um gerador, dizemos que $w_1 w_2 \dots w_m$ é uma *expressão reduzida* para w se $l(w) = m$.

Proposição 2.8. *Se w_r é um gerador de W temos:*

(i) $l(w_r w) < l(w)$ *se, e somente se, existe uma expressão reduzida de w que começa com w_r.*

(ii) $l(w_r w) = l(w) \pm 1$.

Demonstração. (i) Se existe uma expressão reduzida de w que começa com w_r, então $w_r w = w_r w_{i_1} w_{i_2} \dots w_{i_{l(w)}} = w_{i_2} \dots w_{i_{l(w)}}$. Assim $w_r w$ se escreve com no máximo $l(w) - 1$ geradores. Se $l(w_r w) < l(w)$, então $w_r w = w_{i_1} w_{i_2} \dots w_{i_k}$ com $k < l(w)$, assim $w = w_r w_{i_1} w_{i_2} \dots w_{i_k}$ tem que ser uma expressão reduzida, pela minimalidade de $l(w)$.

(ii) Acabamos de ver que $l(w_r w) < l(w)$ se, e somente se, existe uma expressão reduzida de w que começa com w_r. Pela demonstração que fizemos, devemos ter que $l(w_r w) < l(w) \leq l(w_r) + 1$, o que implica $l(w_r w) = l(w) - 1$.

Se nenhuma expressão reduzida de w começa com w_r, então $l(w_r w) \geq l(w)$. Se tivéssemos $l(w_r w) = l(w)$, teríamos $w_r w = w_{i_1} w_{i_2} \dots w_{i_{l(w)}} = w_r w_{j_1} w_{j_2} \dots w_{j_{l(w)}}$, onde cada w_j é um gerador e isso é uma impossibilidade. Agora observe que W é um subgrupo de $O(V)$, o grupo das transformações ortogonais do espaço V. Em particular, sendo $w \in W$ uma transformação linear, podemos falar do determinante de w. Note que um gerador w_r fixa um hiperplano ortogonal ao vetor $r \in V$, assim, o autoespaço associado ao autovalor 1 tem dimensão $\dim V - 1$. Por outro lado, $w_r(r) = -r$. Assim, o polinômio característico possui $\dim V - 1$ raízes iguais a 1 e uma única raiz igual a -1. Portanto o determinante de w_r é -1. Isso implica $\det(w_{i_1} w_{i_2} \dots w_{i_{l(w)}}) = -\det(w_r w_{j_1} w_{j_2} \dots w_{j_{l(w)}})$ e portanto $l(w_r w) \neq l(w)$. Se $w_{i_1} w_{i_2} \dots w_{i_{l(w)}} = w$, então podemos obter uma expressão para $w_r w$ com no máximo $l(w) + 1$ geradores, como $l(w_r w) > l(w)$ temos $l(w_r w) = l(w) + 1$. □

Uma consequência da demonstração da Proposição 2.8 é que, embora um elemento possa ser escrito de diferentes formas como um produto de geradores, a paridade do número de elementos que aparece nas diferentes expressões é sempre a mesma. Essa é uma propriedade que W compartilha com os grupos de permutações.

O que faremos agora é mostrar que existe uma forma bastante conveniente de calcular o comprimento de um elemento de W. Antes de prosseguir, precisamos de alguns resultados.

Proposição 2.9. *Seja $r \in V$ e $w' \in W$, então $w' w_r w'^{-1} = w_{w'(r)}$.*

Demonstração. Para mostrar que $w' w_r w'^{-1} = w_{w'(r)}$ é suficiente mostrar que $w' w_r w'^{-1}$ e $w_{w'(r)}$ coincidem no vetor $w'(r)$ e fixam o hiperplano ortogonal à $w'(r)$. Se isso ocorrer, ambos elementos coincidem em uma base de V e o resultado estará mostrado. Primeiro, observe que $w_{w'(r)}(w'(r)) = -w'(r) = w' w_r w'^{-1}(w'(r))$.

Como w'^{-1}, w e w_r preservam o produto interno. Para $x \in V$ temos:

$$\begin{aligned}\langle x, w'(r)\rangle &= \langle w'^{-1}(x), w'^{-1}w'(r)\rangle \\ &= \langle w'^{-1}(x), r\rangle \\ &= \langle w_r w'^{-1}(x), w_r(r)\rangle \\ &= \langle w_r w'^{-1}(x), -r\rangle \\ &= \langle w' w_r w'^{-1}(x), -w'(r)\rangle.\end{aligned}$$

Assim, $\langle x, w'(r)\rangle = 0$ se, e somente se, $\langle w' w_r w'^{-1}(x), -w'(r)\rangle = 0$. Portanto, $w' w_r w'^{-1}$ fixa o hiperplano ortogonal ao vetor $w'(r)$. □

Lema 2.10. *Para $r \in \Delta$, $w_r(r) \in \Phi^-$, mas $w_r(s) \in \Phi^+$, para cada raiz positiva s diferente de r.*

Demonstração. Pela definição de w_r fica claro que $w_r(r) = -r$ e portanto $w_r(r) \in \Phi^-$. Se $s \in \Phi^+$, temos $s = \sum_i a_i r_i$, com $r_i \in \Delta$ e $a_i \geq 0$. Já que $s \neq r$, temos $a_j > 0$ para algum j, tal que $r_j \neq r$.

Agora, $w_r(s) = \sum_i a_i w_r(r_i)$. Ao escrever $w_r(s)$ na base Δ, obtemos:

$$w_r(s) = \sum_{r_i \neq r} a_i r_i - \left(a_r + \sum_{r_i \neq r} 2\frac{a_i \langle r, r_i\rangle}{\langle r, r\rangle} \right) r.$$

Como $a_j > 0$, o coeficiente de r_j de $w_r(s)$ é maior que 0 também e $w_r(s) \in \Phi^+$. □

Vamos agora introduzir a função n, que conta o número de raízes positivas que são transformadas por w em raízes negativas, isto é $n(w) = |\{w^{-1}(\Phi^-) \cap \Phi^+\}|$. Nosso objetivo é mostrar a igualdade $n(w) = l(w)$, para todo $w \in W$. Vamos primeiro mostrar algumas propriedades da função n.

Proposição 2.11. *Seja $w \in W$ e $r \in \Delta$. Então:*

(i) $n(w_r w) = n(w) + 1$, *se* $w^{-1}(r) \in \Phi^+$.

(ii) $n(w_r w) = n(w) - 1$, *se* $w^{-1}(r) \in \Phi^-$.

(iii) $n(w w_r) = n(w) + 1$, *se* $w(r) \in \Phi^+$.

(iv) $n(w w_r) = n(w) - 1$, *se* $w(r) \in \Phi^-$.

Demonstração. Pelo Lema 2.10, w_r só transforma uma única raiz positiva em negativa, o próprio r. No total, w_r troca o sinal de apenas duas raízes r e $-r$. Se $s \in \Phi^+$ é tal que $w(s) \neq \pm r$, então $w_r w(s) \in \Phi^+$ se e somente se $w(s) \in \Phi^+$. Se $w(s) = r$, então $w_r(w(s)) \in \Phi^-$ e assim $w_r w$ muda o sinal de todas as raízes positivas que w já muda e ainda troca o sinal de s, portanto, $n(w_r w) = n(w)+1$. Isso prova (i). Se $w(s) = -r$, então $w_r(w(s)) \in \Phi^+$ e $w_r w$ muda o sinal de uma raiz a menos do que w e $n(w_r w) = n(w) - 1$, o que prova (ii).

Se $s \in \Phi^+$, com $s \neq r$ e $w(s) \in \Phi^-$, então $w_r^{-1}(s) \in \Phi^+$ e $w w_r(w_r^{-1}(s)) \in \Phi^-$. Dessa forma, para cada raiz positiva $s \neq r$ que w transforma em negativa, $w w_r$ transforma

$w_r^{-1}(s)$ de positiva para negativa e, caso $w(r) \in \Phi^+$, ainda transforma r em uma raiz negativa. Portanto $n(ww_r) = n(w) + 1$. Isso prova (iii). De modo análogo, se $w(r) \in \Phi^-$ então ww_r transforma r em uma outra raiz positiva e $n(ww_r) = n(w) - 1$, o que prova (iv).

□

Proposição 2.12. *Para $w \in W$, temos $n(w) = l(w)$.*

Demonstração. Suponha $w = w_1 w_2 \dots w_{l(w)}$. Pelo Lema 2.10 w_1 só transforma uma única raiz positiva em negativa, logo $n(w_1) = 1$. Pela Proposição 2.11, $n(w_1 w_2)$ é no máximo $n(w_1) + 1$. Assim cada vez que multiplicamos por um gerador w_i, aumentamos n em no máximo 1. Como fazemos isso $l(w)$ vezes, obtemos $n(w) \leq l(w)$.

Suponha $n(w) < l(w)$. Isso significa que em algum momento, ao acrescentarmos mais um gerador w_{j+1} ao produto $w_1 w_2 \dots w_j$, o valor da função n não aumentou. Pela Proposição 2.11, n não fica constante quando multiplicamos por um gerador, logo:

$$n(w_1 w_2 \dots w_j w_{j+1}) = n(w_1 w_2 \dots w_j) - 1$$

e isso só ocorre se $w_1 w_2 \dots w_j(r_{j+1}) \in \Phi^-$ pelo item (iii). Ora, w_j não troca o sinal de r_{j+1}, assim, para que $w_1 w_2 \dots w_j(r_{j+1})$ seja uma raiz negativa deve existir um $i < j$ tal que $w_i w_{i+1} \dots w_j(r_{j+1}) \in \Phi^-$ e $w_{i+1} \dots w_j(r_{j+1}) \in \Phi^+$. Como w_i só troca o sinal de r_i e $-r_i$, temos $w_{i+1} \dots w_j(r_{j+1}) = r_i$.

Agora, podemos utilizar a Proposição 2.9 com $w' = w_{i+1} \dots w_j$ e $r = r_{j+1}$ para concluir:

$$\begin{aligned} w_i &= w_{w'(r_{j+1})} \\ &= w' w_{j+1} w'^{-1} \\ &= (w_{i+1} \dots w_j) w_{j+1} (w_j \dots w_{i+1}). \end{aligned}$$

Multiplicando por w' pela direita nos dois lados da equação, obtemos a seguinte relação:

$$w_i \dots w_j = w_{i+1} \dots w_{j+1}.$$

Isso nos permitir escrever w com menos geradores da seguinte forma:

$$\begin{aligned} w &= w_1 \dots w_{i-1}(w_i \dots w_j) w_{j+1} \dots w_{l(w)} \\ &= w_1 \dots w_{i-1}(w_{i+1} \dots w_{j+1}) w_{j+1} \dots w_{l(w)} \\ &= w_1 \dots w_{i-1} w_{i+1} \dots w_j w_{j+2} \dots w_{l(w)}. \end{aligned}$$

Conseguimos expressar w sem utilizar os geradores w_i e w_{j+1} e assim obtivemos uma expressão para w de comprimento $l(w) - 2$, o que é um absurdo. Portanto, devemos ter $n(w) = l(w)$.

□

A demonstração da Proposição 2.12 é curiosa, pois obtemos uma expressão com 2 geradores a menos, ao invés de apenas 1. Como já discutimos anteriomente, embora w possa ter várias expressões, a paridade do comprimento das diferentes expressões é sempre a mesma. Assim, ao "simplificar" uma expressão sempre eliminamos um número par de elementos para não trocar a paridade.

Corolário 2.13 (Lei do Cancelamento)**.** *Suponha $w = w_1 w_2 \dots w_k$ e $l(w) < k$, então é possível cancelar dois geradores w_i e w_j e obter uma expressão de w com $k-2$ geradores.*

Demonstração. Como $l(w) = n(w)$, temos $n(w) < k$. Como n aumenta em no máximo 1, se $n(w) < k$ existe um gerador w_{j+1} que ao ser acrescentado ao produto $w_1 w_2 \dots w_j$ diminui o valor de n. Agora, basta prosseguir exatamente como fizemos na demonstração da Proposição 2.12. □

Uma implicação da Lei do Cancelamento é que podemos obter uma expressão reduzida de w a partir de qualquer expressão para w.

2.1.2 Câmaras

Dado $v \in V$, denotaremos por H_v o hiperplano $\{x \in V \mid \langle x, v\rangle = 0\}$. Se consideramos os hiperplanos ortogonais às raízes, dividiremos V em várias regiões separadas pelos hiperplanos. Essas regiões são chamadas de *câmaras*. Mais formalmente, as câmaras são as componentes conexas de $V \setminus \bigcup_{r\in\Phi} H_r = V \setminus \bigcup_{r\in\Phi^+} H_r$.

Existe uma componente conexa que está intimamente ligada a Δ, que é a compomente formada por todos os pontos que satisfazem $\langle x, r\rangle > 0$, para $r \in \Delta$. Essa é a chamada *câmara fundamental*, que denotaremos por C_Δ.

Proposição 2.14. *O conjunto $C_\Delta = \{x \in V \mid \langle x, r\rangle > 0, \forall r \in \Delta\}$ é uma câmara.*

Demonstração. Primeiro, precisamos observar que C_Δ não é vazio. Como Δ é uma base, se escolhermos qualquer $a \in \mathbb{R}$, com $a > 0$, temos que o sistema de equações formado pelas equações $\langle x, r_1\rangle = a, \dots, \langle x, r_{|\Delta|}\rangle = a$ admite uma solução que pertence à C_Δ.

Como C_Δ é convexo, em particular é conexo. Falta verificar que C_Δ é maximal. Suponha que existe um conjunto conexo C' de $V \setminus \bigcup_{r\in\Phi} H_r$ que contenha C_Δ propriamente. Então existe $y \in C'$ tal que $y \notin C_\Delta$. Em particular, $\langle y, r_i\rangle \leq 0$ para algum $r_i \in \Delta$. Não pode ocorrer $\langle y, r_i\rangle = 0$, pois teríamos $y \in H_{r_i}$. Se $\langle y, r_i\rangle < 0$, como C_Δ não é vazio existe $x \in C'$ tal que $\langle x, r_i\rangle > 0$ e por C' ser conexo podemos aplicar o Teorema do Valor Intermediário para concluir que existe $z \in C'$ tal que $\langle z, r_i\rangle = 0$, o que é um absurdo. Assim, C_Δ é, de fato, maximal. □

Vamos agora introduzir a seguinte notação:

- $H_r^0 = \{v \in V \mid \langle v, r\rangle = 0\}$.
- $H_r^+ = \{v \in V \mid \langle v, r\rangle > 0\}$.
- $H_r^- = \{v \in V \mid \langle v, r\rangle < 0\}$.

Com essa notação temos $V \setminus \bigcup_{r\in\Phi^+} H_r = \bigcap_{r\in\Phi^+} (H_r^+ \cup H_r^-)$. Assim, fica claro que as componentes conexas são da forma $\bigcap_{r\in\Phi^+} H_r^{\epsilon_r}$, com $\epsilon_r \in \{+, -\}$. Cada elemento de w preserva o produto interno, então leva um hiperplano $H_r^{\epsilon_r}$ em $H_{w(r)}^{\epsilon_r}$. Segue que w permuta as componentes conexas e podemos considerar que W age sobre o conjunto das câmaras.

Proposição 2.15. *O grupo W age sobre o conjunto das câmaras, além disso essa ação possui as seguintes propriedades:*

(i) Se C_1 e C_2 são câmaras existe um único $w \in W$ tal que $w(C_1) = C_2$.

(ii) Em particular, se $w(C) = C$, então $w = 1$.

A Proposição 2.15 é análoga à Proposição 2.6. A razão disso é que há uma correspondência entre as câmaras e os sistemas fundamentais de raízes. Por exemplo, podemos caracterizar Δ como sendo o conjunto das raízes que são ortogonais a pelo menos uma das "paredes" da câmara fundamental e que apontam para dentro dela. Com essa mesma ideia, podemos obter sistemas fundamentais a partir das outras câmaras vendo as raízes que são ortogonais às "paredes" e que apontam para dentro da câmara. Veja [5, Proposição 2.3.1 e Corolário 2.3.2].

2.1.3 Subgrupos Parabólicos

Dado um conjunto de raízes fundamentais, temos associado um conjunto de geradores para W. Retomando a notação da Seção 2.1.1, os geradores são da forma $w_i \in W$, com $i \in I$ um conjunto de índices. Com isso, podemos definir os subgrupos parabólicos de W.

Definição 2.16. Um subgrupo parabólico de W é um subgrupo conjugado a um subgrupo da forma $W_J = \langle w_j \mid j \in J \rangle$, com $J \subseteq I$. Um subgrupo da forma W_J é chamado de *parabólico padrão*.

Com essa notação temos $W_I = W$ e $W_\emptyset = \{1\}$. Um fato importante é que que W_J também surge a partir de um sistema de raízes, e assim, também é um grupo de Weyl no sentido em que estamos discutindo nesta seção. Denotaremos por $\Delta_J = \{r_j \in \Delta \mid j \in J\}$ e $\Phi_J = \Phi \cap V_J$, onde V_J é o espaço vetorial gerado pelos vetores de Δ_J.

Proposição 2.17. *O conjunto Φ_J é um sistema de raízes e Δ_J é um sistema fundamental de raízes de Φ_J. Além disso, o grupo de Weyl correspondente a Φ_J é W_J.*

Demonstração. Como Φ_J é um subconjunto de Φ, a condição (iv) da Definição 2.1 é automaticamente satisfeita. Como Δ_J está contido em Φ_J, Φ_J gera V_J, e a condição (ii) está satisfeita. Para a condição (i), e $r \in \Phi_J$, então $-r \in \Phi$ e $-r$ é gerado pelos vetores de Δ_J, assim $-r \in \Phi_J$. Se $r, s \in \Phi_J$, então $w_r(s)$ é uma combinação linear de r e s. Como $r, s \in V_J$ e $w_r(s) \in \Phi$ temos $w_r(s) \in \Phi_J$.

Como Δ_J é um subconjunto de Δ e gera V_J, toda raiz de Φ_J pode ser escrita como combinação linear de elementos de Δ_J em que os coeficientes são todos não-negativos ou todos não-positivos. Assim, Δ_J é um sistema fundamental de raízes. O grupo de Weyl correspondente ao sistema de raízes Φ_J é gerado pelos elementos w_r com $r \in \Delta_J$ e, portanto, é precisamente W_J. □

Agora, vamos examinar o que acontece com a função comprimento nos subgrupos parabólicos. Como temos menos geradores para formar palavras, esperamos que para $w \in W_J$, tenhamos $l_W(w) \leq l_{W_J}(w)$. Na verdade, as duas funções são iguais.

Proposição 2.18. *Para $w \in W_J$, temos $l_{W_J}(w) = l_W(w)$.*

Demonstração. Como w está em W_J, é possível escrevê-lo como um produto dos geradores w_j, para $j \in J$. Pelo Corolário 2.13 é possível cancelar termos desse produto até obtermos uma expressão reduzida em W. Por construção, tal expressão reduzida contém apenas geradores de W_J. Segue que $l_{W_J}(w) = l_W(w)$. □

Com alguns outros resultados auxiliares é possível mostrar que toda expressão reduzida de $w \in W_J$ contém apenas geradores de W_J. Veja, por exemplo, [13, Proposição 1.2.10].

2.1.4 Representantes de Classes Laterais

Nesta seção vamos discutir alguns bons representantes para as classes laterais dos subgrupos parabólicos W_J em W. Antes de prosseguir, apenas uma observação sobre a notação: para tornar mais claro, nas proposições seguintes passaremos a usar s_j para denotar um gerador de W_J e w_j para denotar um elemento arbitrário de W_J.

Defina D_J como sendo os elementos $w \in W$ tais que $w(r) \in \Phi^+$ para todo $r \in \Delta_J$. Mostraremos que D_J é um transversal à esquerda de W_J em W, isto é, cada $d_J \in D_J$ está em uma classe lateral à esquerda distinta e cada classe lateral contém um elemento de D_J.

Proposição 2.19. *Dado $J \subseteq I$, cada elemento $w \in W$ pode ser escrito de forma única como $w = d_J w_j$ com $d_J \in D_J$ e $w_j \in W_J$. Além disso, temos $l(w) = l(d_J) + l(w_j)$.*

Demonstração. Primeiro mostraremos por indução que é possível fatorar w da forma $d_J w_j$, com $l(w) = l(d_J) + l(w_j)$, depois mostraremos que isso é feito de forma única.

Se $l(w) = 0$, então $w = 1$. Neste caso, basta tomar $d_J = w_j = 1$. Agora suponha que $l(w) > 0$. Se $w \in D_J$, basta tomar $w_j = 1$. Então, vamos supor $w \notin D_J$. Isso significa que existe uma raiz r com $r_j \in \Delta_J$ tal que $w(r) \in \Phi^-$. Pela Proposição 2.11, temos $n(ww_r) = n(w) - 1$. Como $n(w)$ e $l(w)$ são iguais, temos

$$l(ww_r) = l(w) - 1. \tag{2.1}$$

Por indução ww_r possui uma fatoração da forma $d'_J w'_j$ tal que

$$l(ww_r) = l(d'_J) + l(w'_J). \tag{2.2}$$

Temos $w = d'_J w'_j w_r$, com $d'_J \in D_J$ e $w'_j w_r \in W_J$. Vamos mostrar que $d_J = d'_J$ e $w_j = w'_j w_r$ tem as propriedades desejadas. Combinando as Equações (2.1) e (2.2) obtemos $l(w) = l(d'_J) + l(w'_j) + 1$. Note que $l(w_j) \leq l(w'_j) + 1$, mas se $l(w_j) < l(w'_j) + 1$, poderíamos escrever w como um produto de menos do que $l(d'_J) + l(w'_j) + 1$ geradores. Assim, devemos ter $l(w_j) = l(w'_j) + 1$ e portanto $l(w) = l(d_J) + l(w_j)$.

Falta mostrar a unicidade dessa fatoração. Se $d_J w_j = d'_J w'_j$ temos $d_J = d'_J w_j w'_j$. Considere uma raiz $r_j \in \Delta_J$. Por hipótese temos $d_J(r_j) \in \Phi^+$ e $d'_J(r_j) \in \Phi^+$. Como isso ocorre para toda raiz em Δ_J, isso também deve ocorrer com toda raiz de Φ_J^+. Portanto, dada uma raiz $r_j \in \Delta_J$, $w_j w'_j(r_j)$ tem que pertencer à Φ_J^+, pois d'_J preserva o sinal. Portanto, $n_{W_J}(w_j w'_j) = 0 = l_{W_J}(w_j w'_j)$ e $w_j w'_j = 1$ e daí $d_J = d'_J$.

□

Corolário 2.20. *O conjunto D_J é um transversal à esquerda de W_J em W. Além disso, d_J é o único elemento de comprimento mínimo de $d_J W_J$.*

Demonstração. Da Proposição 2.19 temos $W = \bigcup_{d_J \in D_J} d_J W_J$, precisamos apenas verificar que a união é disjunta. Isso é verdade, pois se ocorrer $d_J w_J = d'_J w'_j$, a unicidade da fatoração garante $d_J = d'_J$ e $w_j = w'_j$.

Para mostrar que d_J é o elemento de comprimento mínimo de $d_J W_J$ basta usar a igualdade $l(d_J w_j) = l(d_J) + l(w_j)$. Além disso, ele tem que ser único, pois $l(d_J w_J) = l(d_J)$ se, e somente, se $w_j = 1$. □

Se $s_1 s_2 \dots s_{l(w)}$ é uma expressão reduzida para $w \in W$, dizemos que $s_i \dots s_{l(w)}$ é um *sufixo* de w. Note que para $x \in W$ ser um sufixo de w é necessário e suficiente que $ux = w$, para algum $u \in W$ com $l(x) + l(u) = l(w)$. Teremos como consequência da proposição seguinte que todo sufixo de um elemento de D_J também pertence a D_J.

Proposição 2.21. *Seja $d_J \in D_J$ e $s_i \in W$, com $i \in I$. Então ou $s_i d_J \in D_J$ ou $s_i d_J = d_J s_j$, para algum $j \in J$.*

Demonstração. Suponha $s_i d_J \notin D_J$, isso significa que existe alguma raiz $\alpha_j \in \Delta_J$ que $s_i d_J$ transforma em uma raiz negativa. Pela Proposição 2.11, temos:

$$l(s_i d_J s_j) = l(s_i d_J) - 1. \tag{2.3}$$

Queremos mostrar três coisas: $l(d_J s_j) = l(d_J) + 1$, $l(s_i d_J) = l(d_J) + 1$ e $l(s_i d_J s_j) = l(d_J)$. Em seguida, mostraremos que isso implica $s_i d_J = d_J s_j$. A primeira igualdade é verdadeira, pois $d_J \in D_J$. Temos:

$$\begin{aligned} l(d_J) &= l(d_J s_j) - 1 \\ &\leq (l(s_i d_J s_j) + 1) - 1 \\ &\leq (l(s_i d_J) - 1 + 1) - 1 \qquad \text{pela Equação (2.3).} \end{aligned}$$

Isso implica $l(s_i d_J) > l(d_J)$ e $l(s_i d_J) = l(d_J) + 1$. Também pela Equação (2.3) obtemos $l(s_i d_J s_j) = l(d_J)$. Vamos mostrar agora que essas três equações implicam $s_i d_J = d_J s_j$.

Como $l(s_i d_J s_j) = l(d_J)$, temos uma expressão reduzida para $s_i d_J s_j$ da forma $s_1 s_2 \dots s_{l(d_J)}$, onde cada s_k é um gerador. Assim $s_i s_1 s_2 \dots s_{l(d_J)} s_j$ é uma expressão para d_J que *não* é reduzida. Utilizando a Lei do Cancelamento, podemos excluir dois geradores e obter uma expressão reduzida para d_J. Se não excluirmos o gerador s_i, obteríamos uma expressão reduzida para d_J que começaria com s_i assim $l(s_i d_J) < l(d_J)$, uma contradição. Da mesma forma, se não excluirmos o s_j, obteríamos uma expressão reduzida que termina em s_j e $l(d_J s_j) < l(d_j)$. Daí $d_J = s_1 s_2 \dots s_{l(d_J)} = s_i d_J s_j$ e, portanto, $s_i d_J = d_J s_j$. □

É interessante notar que o argumento final utilizado na demonstração da Proposição 2.21 não depende do fato de que $d_J \in D_J$. Deixaremos isso registrado como um corolário.

Corolário 2.22. *Se $w, s_i, s_j \in W$ são tais que s_i, s_j são geradores de W, $l(s_i w s_j) = l(w)$, $l(s_i w) > l(w)$ e $l(w s_j) > l(w)$, então $s_i w = w s_j$.*

Demonstração. Basta proceder como no último parágrafo da demonstração da Proposição 2.21, com w no lugar de d_J. □

Corolário 2.23. *Todo sufixo de $d_J \in D_J$ também está em D_J.*

Demonstração. Tome $d_J = s_1 s_2 \dots s_{l(d_J)}$. Temos $l(s_1 d_J) < l(d_J)$ e para todo $j \in J$, temos $l(d_J s_j) > l(d_J)$. Assim, nunca teremos $d_J s_j = s_1 d_J$. Pela Proposição 2.21, $s_1 d_J \in D_J$, isto é, $s_2 \dots s_{l(d_J)} \in D_J$. Fazendo $d'_J = s_2 \dots s_{l(d_J)}$, temos $l(s_2 d'_J) < l(d'_J)$ e $s_3 \dots s_{l(d_j)} \in D_J$. Prosseguindo por indução, fica claro que, para todo $i \leq l(d_J)$, temos $s_i \dots s_{l(w)} \in D_J$. □

A função que leva w em w^{-1} leva classes laterais à esquerda em classes laterais à direita. Além disso, temos $l(w) = l(w^{-1})$. Assim, D_J^{-1} é um conjunto de representantes

das classes laterais *à direita* de W_J em W e cada $d_j \in D_J^{-1}$ é o elemento de comprimento mínimo de $W_J d_j$. Dessa forma, os resultados discutidos anteriomente se aplicam de forma análoga nesta situação. O único cuidado é que a Proposição 2.23 passa a tratar de *prefixos*, isto é, todo prefixo de um elemento de D_J^{-1} também está em D_J^{-1}. Para maiores detalhes, veja [13, Proposição 2.1.1, Lema 2.1.2, Observação 2.1.6].

Agora, para $J, K \subseteq I$, defina $D_{J,K} = D_J^{-1} \cap D_K$. Vamos mostrar que $D_{J,K}$ é um conjunto de representantes para as classes laterais duplas da forma $W_J w W_K$. Para isso, precisamos de alguns resultados auxiliares.

Lema 2.24. *Se $w_j d_{J,K}(r_k) \in \Phi^-$, para $w_j \in W_J, d_{J,K} \in D_{J,K}$ e $k \in K$, então $d_{J,K}(r_k) = r_{j'}$, para algum $j' \in J$.*

Demonstração. Pelo fato de $d_{J,K}$ estar em D_K temos $d_{J,K}(r_k) \in \Phi^+$. Já que $w_j d_{J,K}(r_k)$ é uma raiz negativa, então $d_{J,K}(r_k)$ tem que estar em Φ_J^+. A razão disso é que como $l(w_j) = n_{W_J}(w_j) = n(w_j)$, pela Proposição 2.18, todas as raízes positivas que são transformadas em negativas por w_j têm que estar em Φ_J^+, caso contrário teríamos $n_{W_J}(w_j) < n(w_j)$. Assim,

$$d_{J,K}(r_k) = \sum_{r_j \in \Delta_J} a_j r_j,$$

onde cada $a_j \geq 0$. Disto temos $r_k = \sum_{r_j \in \Delta_J} a_j d_{J,K}^{-1}(r_j)$ e cada $d_{J,K}^{-1}(r_j)$ é uma raiz positiva. Observe que se $a_{j'} > 0$, ao escrevermos $d_{J,K}^{-1}(r_{j'})$ como combinação linear de raízes simples, os coeficientes das raízes diferentes de r_k têm que ser 0. Além disso, o coeficiente de r_k, deve ser $+1$ ou -1 pelo propriedade (i) da definição de sistemas de raízes. Logo $d_{J,K}^{-1}(r_{j'}) = r_k$. Como o somatório não é nulo, um tal j' com certeza existe. □

Lema 2.25. *Se $d, d' \in D_{J,K}$, então $W_J \cap dW_K d'^{-1}$ é vazio a menos que $d = d'$.*

Demonstração. Tome $w \in W_J \cap dW_K d'^{-1}$, vamos mostrar que $d = d'$, por indução sobre $l(w)$. Se $l(w) = 0$, então $w = 1$. Assim, existe $u \in W_K$ tal que $du = d'$. Segue que d e d' estão na mesma classe lateral à *esquerda* de W_K e devemos ter $d' = d$. Agora, suponha que $l(w) > 0$. Temos $x = d^{-1} w d' \in W_K$. Se ocorrer que $x = 1$, temos $d = wd'$ e isso significa que d e d' estão na mesma classe lateral à *direita* de W_J e portanto $d = d'$.

Assim, vamos supor $x \neq 1$. Como x está em W_K, tomando uma expressão reduzida para x, podemos escrever $x = x' s_k$, com $s_k \in W_K$ e $l(x) = l(x') + 1$.

Como $n(x s_k) = n(x') = n(x) - 1$, pela Proposição 2.11, temos $x(r_k) \in \Phi_K^-$. Como $d \in D_K$, temos $dx(r_k) \in \Phi_K^-$ e $wd'(r_k) \in \Phi_K^-$. Pelo Lema 2.24, $d'(r_k) = r_j$, para algum $j \in J$. Isso nos permite concluir dois fatos: $w(r_j) \in \Phi^-$ e, pela Proposição 2.9, $s_j = d' s_k d'^{-1}$.

O fato de $w(r_j)$ ser uma raiz negativa implica que alguma expressão reduzida de w termina com s_j. Em particular, podemos escrever w como $w' s_j$, com $l(w) = l(w') + 1$. Temos:

$$\begin{aligned} w' &= w s_j \\ &= w d' s_k d'^{-1} \\ &= dx s_k d'^{-1}. \end{aligned}$$

Como $x s_k$ é um elemento de W_K, então $w' \in dW_K d'^{-1}$. Assim, w' é um elemento de $W_J \cap dW_K d'^{-1}$ de comprimento menor do que $l(w)$. Por indução, temos $d = d'$. □

Proposição 2.26. *O conjunto $D_{J,K}$ é um conjunto completo de representantes das classes laterais duplas. Além disso, todo $d \in D_{J,K}$ é o único elemento de comprimento mínimo na classe lateral dupla $W_J dW_K$.*

Demonstração. Cada classe lateral dupla contém um elemento de comprimento mínimo e, em princípio, não necessariamente tal elemento é único. Vamos mostrar que um elemento de comprimento mínimo necessariamente está em $D_{J,K}$. Se $d \in W_J w W_K$ e $d = w_j d w_k$, possui comprimento mínimo, então d possui comprimento mínimo na classe lateral $W_J d w_k$, portanto $d \in D_J^{-1}$. Da mesma forma, d possui comprimento mínimo na classe lateral $w_j d W_K$ e $d \in D_K$. Assim, cada classe lateral dupla certamente contém um elemento de $D_{J,K}$. Precisamos verificar que esse elemento é único.

Se $d' = w_j d w_k$, então $w_j = d' w_k^{-1} d^{-1} \in W_J \cap dW_K d'^{-1}$ e, pelo Lema 2.25, temos $d = d'$. □

Proposição 2.27. *Todo elemento de $w \in W$ pode ser escrito da forma $w_j d w_k$, com $d \in D_{J,K}$, $w_j \in W_J$, $w_k \in W_K$ e $l(w) = l(w_j) + l(d) + l(w_k)$.*

Demonstração. Primeiro, vamos escrever w como $d_K w_k$, com $d_K \in D_K$. Agora, vamos escrever d_K como $w_j d_J$, com $d_J \in D_J^{-1}$. Essa decomposição satisfaz $l(w) = l(d_K) + l(w_k) = l(w_j) + l(d_J) + l(w_k)$. Precisamos apenas verificar que d_J^{-1} está em D_K. Isso é verdade, pois $d_K = w_j d_J$ e $l(d_K) = l(w_j) + l(d_J)$. Assim, d_J é um sufixo de d_K e, pelo Corolário 2.23, temos $d_J \in D_K$. □

Note que dessa vez, a decomposição obtida não é necessariamente única. Para um elemento w na classe lateral dupla $W_J d_{J,K} W_K$ podem haver várias formas de expressá-lo como $w_j d_{J,K} w_k$ e nem todas satisfazem $l(w) = l(w_j) + l(d_{J,K}) + l(w_k)$.

2.1.5 Complexo de Coxeter

Considerando o fecho $\overline{C}$ de uma câmara fundamental podemos particioná-la em partes de tal forma que os subgrupos parabólicos sejam os estabilizadores dessas regiões. Faremos isso introduzindo em V uma relação de equivalência.

Dados $x, y \in V$, diremos que $x \sim y$ se para cada $r \in \Phi$, tivermos $\langle r, x\rangle\langle r, y\rangle > 0$ ou $\langle r, x\rangle = \langle r, y\rangle = 0$. Isso significa que dois pontos estão numa mesma classe de equivalência se, e somente se, para cada hiperplano H_r ou ambos estão em H_r ou ambos estão do mesmo lado do hiperplano.

Definição 2.28. O conjunto das classes de equivalência da relação $\sim$ é o *complexo de Coxeter*, que denotaremos por $\mathcal{C}$.

A definição de $\mathcal{C}$ deixa claro que todos os elementos de $\mathcal{C}$ são da forma $\bigcap_{r\in\Phi^+} H_r^{\epsilon_r}$, com $\epsilon_r \in \{0, +, -\}$. Como W é composto de transformações que preservam o produto interno, para $w \in W$ temos que $H_r^{\epsilon_r}$ é levado em $H_{w(r)}^{\epsilon_r}$. Segue que w leva um elemento de $\mathcal{C}$ em outro elemento de $\mathcal{C}$ e, assim, W age sobre $\mathcal{C}$.

Agora, dado $J \subseteq I$, considere os elementos de $\mathcal{C}$ da seguinte forma:

$$C_J = \left\{ x \in V \;\middle|\; \begin{array}{ll} \langle x, r_j \rangle = 0 & \text{se } j \in J \\ \langle x, r_j \rangle > 0 & \text{se } j \in I \setminus J \end{array} \right\}$$
$$= \left\{ x \in V \;\middle|\; \begin{array}{ll} \langle x, r \rangle = 0 & \text{se } r \in \Delta_J \\ \langle x, r \rangle > 0 & \text{se } r \in \Delta \setminus \Delta_J \end{array} \right\}.$$

Lembrando que o fecho da câmara fundamental é

$$\overline{C} = \{x \in V \mid \langle x, r_i \rangle \geq 0, \forall i \in I\},$$

temos $\overline{C} = \bigcup_{J \subseteq I} C_J$. Assim, podemos utilizar alguns elementos do complexo de Coxeter para particionar $\overline{C}$ e os C_J são os únicos elementos de $\mathcal{C}$ que estão em $\overline{C}$.

Proposição 2.29. *O subgrupo W_J é o estabilizador de C_J. Mais ainda, W_J fixa C_J ponto a ponto.*

Demonstração. Para mostrar que W_J fixa C_J ponto a ponto, basta verificar essa propriedade para os geradores de W_J. Cada gerador s_j de W_J fixa o hiperplano H_{r_j} ponto a ponto. Como $C_J \subseteq \bigcap_{j \in J} H^0_{r_j}$, o resultado segue.

Suponha que w fixe C_J. Pela Proposição 2.19, temos $w = d_J w_j$, com $w_j \in W_J$. Logo $C_J = d_J(w_j(C_J)) = d_J(C_J)$. Se $d_J = 1$ não há nada a ser feito e $w \in W_J$. Caso contrário, $l(d_J) > 0$ e existe pelo menos uma raiz positiva que é levada por d_J em Φ^-. Isso implica que há pelo menos uma raiz fundamental r tal que $d_J(r) \in \Phi^-$.

Pela definição de d_J temos $r \in \Delta \setminus \Delta_J$. Agora, seja $v \in C_J$, então $\langle v, -r \rangle < 0$ e daí

$$\langle d_J(v), -d_J(r) \rangle < 0. \tag{2.4}$$

Como $-d_J(r) \in \Phi^+$, temos $-d_J(r) = \sum \lambda_i r_i$ e $\lambda_i \geq 0$. Por outro lado, como d_J fixa C_J, temos $d_J(v) \in C_J$, em particular $d_J(v)$ pertence ao fecho da câmara fundamental, o que implica $\langle d_J(v), r \rangle \geq 0$, para todo $r \in \Delta$. Assim:

$$\begin{aligned} \langle d_J(v), -d_J(r) \rangle &= \langle d_J(v), \sum \lambda_i r_i \rangle \\ &= \sum \langle d_J(v), \lambda_i r_i \rangle \\ &\geq 0, \end{aligned}$$

o que contradiz a Equação (2.4). Portanto, $d_J = 1$ e $w \in W_J$. □

Desta maneira, os subgrupos parabólicos padrões de W podem ser caracterizados como sendo os estabilizadores das classes de equivalência contidas no fecho da câmara fundamental. Agora, vamos verificar que $\overline{C}$ contém um elemento de cada órbita da ação de W sobre $\mathcal{C}$.

Proposição 2.30. *Seja $K \in \mathcal{C}$, então existe $x \in W$ e um único $J \subseteq I$ tal que $K = x(C_J)$.*

Demonstração. Dado $K \in \mathcal{C}$, fica claro que K tem que estar contido no fecho de alguma câmara C_1. Pela Proposição 2.15, existe x tal que $x(C) = C_1$, onde C é a câmara fundamental. Agora, por W agir sobre complexo de Coxeter, $x^{-1}(K)$ também é um

elemento do complexo do Coxeter, além disso, ele está contido em $\overline{C}$. Mas os únicos elementos de $\mathcal{C}$ que estão no fecho da câmara fundamental são da forma C_J, portanto, $x^{-1}(K) = C_J$, o que implica $K = x(C_J)$. □

Proposição 2.31. *Os subgrupos parabólicos de W são os estabilizadores dos elementos do complexo de Coxeter. Mais ainda, se $w \in W$ fixa um elemento do complexo de Coxeter, então w fixa esse elemento ponto a ponto.*

Demonstração. Pela Proposição 2.30, um elemento do complexo de Coxeter é sempre da forma $x(C_J)$. Assim, se w é tal que $wx(C_J) = x(C_J)$, temos $x^{-1}wx(C_J) = C_J$ e, pela Proposição 2.29, isso ocorre se, e somente se, $x^{-1}wx \in W_J$. Isto é, se e somente se $w \in xW_Jx^{-1}$. Segue que cada elemento do complexo de Coxeter é estabilizado por um subgrupo parabólico e um subgrupo parabólico xW_Jx^{-1} sempre estabiliza $x(C_J)$.

Além disso, como $x^{-1}xw(C_J) = C_J$, temos que $x^{-1}wx(C_J)$ fixa C_J ponto a ponto. Assim, dado $v \in C_J$, temos $x^{-1}wx(v) = v$ e $wx(v) = x(v)$. Isso significa que w fixa $x(C_J)$ ponto a ponto.

□

Mais detalhes sobre o complexo de Coxeter podem ser vistos em [17, Seção 1.15] ou [5, Seção 2.6].

2.1.6 Raízes para um grupo com par-BN

Até este ponto, a abordagem foi construir o grupo de Weyl a partir de um sistema de raízes. Quando temos um grupo com um par-BN não temos, em princípio, um sistema de raízes à disposição. Assim, para usar os resultados que discutimos até agora, precisamos corrigir essa falha. Temos dois objetivos aqui:

1. Construir um sistema de raízes Φ tal que o grupo de Weyl correspondente seja precisamente o W que é dado pelos axiomas de par-BN.

2. Gostaríamos que os geradores do grupo de Weyl correspondessem a um sistema de raízes fundamentais $\Delta \subseteq \Phi$.

Na verdade, só podemos atingir esses dois objetivos no caso em que W é finito, pois o grupo de Weyl associado a um sistema de raízes é sempre finito. Para o que precisamos, essa não é uma restrição severa, pois os grupos de nosso interesse são finitos. Faremos aqui apenas um esboço da construção para ter certeza de que podemos, de fato, aplicar os resultados anteriores. Maiores detalhes podem ser vistos em [17, Seção 5.3].

Dado que W possui uma apresentação da forma $\langle s_i, i \in I \mid (s_is_j)^{m_{ij}} = 1\rangle$, vamos escolher uma base $\{\alpha_1, \alpha_2, \ldots, \alpha_{|I|}\}$ para um espaço vetorial real V de dimensão $|I|$. Em V vamos introduzir a seguinte forma bilinear:

$$B(\alpha_i, \alpha_j) = -\cos\left(\frac{\pi}{m_{ij}}\right).$$

Essa forma bilinear é simétrica, pois a matriz (m_{ij}) também é simétrica. Além disso, pode-se mostrar que essa forma bilinear é positiva definida, portanto, dá origem a um

produto interno em $|I|$, que podemos denotar por $\langle ., . \rangle$. Como $m_{ii} = 2$, temos $\langle \alpha_i, \alpha_i \rangle = 1$. Para cada α_i considere a seguinte reflexão:

$$\begin{aligned} \sigma_i(x) &= x - 2\frac{\langle \alpha_i, x \rangle}{\langle \alpha_i, \alpha_i \rangle}\alpha_i \\ &= x - 2\langle \alpha_i, x \rangle \alpha_i. \end{aligned}$$

Tomando $W' \subseteq GL(V)$ como sendo o grupo gerado pelas reflexões σ_i, pode-se mostrar que $(\sigma_i\sigma_j)^{m_{ij}} = 1$ e que a função f que leva $s_i \in W$ em $\sigma_i \in W'$ é um isomorfismo. Além disso, $f(w)$ preserva a forma bilinear B, pois cada σ_i também a preserva.

Com a identificação fornecida por f, podemos tomar $\Phi = \{w(\alpha_i) \mid w \in W, i \in I\}$, que é um sistema de raízes tal que $\Delta = \{\alpha_i \mid i \in I\}$. Com isso, cumprimos nossos objetivos e podemos utilizar os resultados discutidos anteriormente.

2.2 Consequências dos axiomas de par-BN

Seja G um grupo com par-BN. Após discutir algumas propriedades do grupo de Weyl do par-BN, vamos agora discutir algumas propriedades de G. Primeiro, vamos verificar que existem subgrupos de G análogos aos subgrupos parabólicos de W. Como $B \cap N$ é normal em N, para cada subgrupo parabólico W_J, existe um N_J tal que $N_J/(B \cap N) = W_J$.

Proposição 2.32. *O conjunto $P_J = BN_JB$ é um subgrupo de G.*

Demonstração. O inverso de um elemento de P_J certamente está em P_J. Precisamos apenas verificar que P_J é fechado para a operação do grupo. Assim, seja $bnb' \in P_J$, onde $b, b' \in B$ e $n \in N_J$. W_J é gerado pelas reflexões $s_j \in W_J$, que são imagens de elementos $n_j \in N_j$ pelo homomorfismo quociente. Assim, temos:

$$n(B \cap N) = n_1 \dots n_k(B \cap N).$$

Daí $n = n_1 \dots n_k h$, com $h \in B \cap N$. Vamos verificar a inclusão $bn_1 \dots n_k hb'BN_JB \subseteq BN_JB$, isso será suficiente para mostrar que BN_JB é fechado para a operação do grupo. Temos:

$$bn_1 \dots n_k hb'BN_JB = bn_1 \dots n_kBN_JB.$$

A propriedade (iv) da Definição 2.1 para $n_i = n_k$ e $n = 1$ implica $n_kB \subseteq Bn_kB \cup B$, e como $Bn_kB \cup B \subseteq BN_JB$, obtemos $bn_1 \dots n_kBN_JB \subseteq bn_1 \dots n_{k-1}BN_JB$. Segue, por indução, $bn_1 \dots n_{k-1}BN_JB \subseteq bBN_JB$ e, portanto, $bnbBN_JB \subseteq BN_JB$. Como bnb é um elemento arbitrário de BN_JB, temos $(BN_JB)(BN_JB) \subseteq BN_JB$.

□

Com isso, podemos definir os subgrupos parabólicos de G.

Definição 2.33. Seja G um grupo com par-BN que possui um grupo de Weyl gerado por um conjunto de reflexões s_i, com $i \in I$. Os subgrupos da forma $P_J = BN_JB$, para $J \subseteq I$, são chamados de *subgrupos parabólicos padrão*. Um subgrupo parabólico de G é qualquer subgrupo que seja conjugado a um P_J.

Uma consequência imediata da Proposição 2.32 é que o próprio G é um subgrupo parabólico, pois $G = BN_IB = BNB$. Isso é verdade, pois pela propriedade (i) da Definição 2.1, G é gerado por B e N. Temos também $B = P_\emptyset$, pois $W_\emptyset = \{1\}$ e $N_\emptyset = B \cap N$.

É interessante notar que os subgrupos da forma P_J para $J \subseteq I$ também possuem um par-BN dado pelos subgrupos B e N_J. Pela Proposição 2.32, B e N_J geram P_J. Além disso $B \cap N_J = B \cap N$ e $B \cap N_J$ é normal em N_J. Isso mostra que as propriedades (i) e (ii) da Definição 2.1 são válidas. O grupo de Weyl correspondente é W_J, que é gerado por elementos de ordem 2. Tais elementos podem ser escolhidos entre os geradores de W, assim fica claro que as propriedades $(iii), (iv)$ e (v) da Definição 2.1 também são atendidas.

Outra consequência interessante da Proposição 2.32 é que podemos tomar alguns elementos de N como representantes das classes laterais duplas de B em G. Na proposição seguinte veremos que se tomarmos, para cada $w \in W$, um n tal que $\pi(n) = w$, então esses elementos formam um conjunto de representantes das classes laterais duplas de G. Nessa situação, costuma-se escrever que $G = BWB$.

Proposição 2.34 (Decomposição de Bruhat)**.** *Escolha um transversal à esquerda T de $B \cap N$ em N. Então T também é um conjunto de representantes das classes laterais duplas de B em G. Em particular, temos $BnB = Bn'B$ se e somente se $\pi(n) = \pi(n')$*

Demonstração. Suponha $BnB = Bn'B$, $w = \pi(n)$ e $w' = \pi(n')$. Podemos assumir, sem perda de generalidade, $l(w) \leq l(w')$. Mostraremos que $\pi(n') = \pi(n)$, por indução sobre $l(w)$. Se $l(w) = 0$, temos $w = 1$. Isso significa que $n \in B \cap N$ e que $Bn'B = B$. Logo $n' \in B \cap N$ e $\pi(n') = 1$ também.

Suponha agora $l(w) > 0$. Então existe um gerador $s_i \in W$ tal que $l(s_iw) = l(w) - 1$. Em particular, existe $w'' \in W$ tal que $w = s_iw''$, com $l(w'') < l(w)$. Considere elementos $n_i, n'' \in N$ tais que $\pi(n_i) = s_i$ e $\pi(n'') = w''$. Como s_i tem ordem 2, então $\pi(n_i^{-1}) = s_i$. Temos, assim:

$$\begin{aligned} n_i^{-1}n''(B \cap N) &= n(B \cap N) \\ &= n'(B \cap N). \end{aligned}$$

Isso implica $n_i^{-1}n''B = n'B$ e, em particular, $n_i^{-1}n''B \subseteq Bn'B$. Daí

$$\begin{aligned} n''B &\subseteq n_iBn'B \\ &\subseteq Bn_in'B \cup Bn'B \qquad \text{(pela propriedade } (iv) \text{ do par-BN).} \end{aligned}$$

Portanto, como as classes laterais duplas são todas disjuntas, temos $Bn''B = Bn_in'B$ ou $Bn''B = Bn'B$. Por indução, temos $w'' = s_iw'$ ou $w'' = w'$. Como $l(w'') < l(w)$ e $l(w) \leq l(w')$, não podemos ter $w'' = w'$. Assim, $w'' = s_iw'$ e $w = w'$.

Agora, se T é um transversal de $B \cap N$ em N, como $G = BNB$, então $G = \cup_{t \in T} BtB$. Além disso, só ocorre $BtB = Bt'B$ se $\pi(t) = \pi(t')$ e isso significa que t e t' estão na mesma classe lateral de $B \cap N$ em N. Por hipótese, temos $t = t'$. Portanto, T também é um transversal das classes laterais duplas de B em G.

□

A partir da decomposição de Bruhat mostraremos que há uma correspondência entre as classes laterais duplas de subgrupos parabólicos padrões de G e de subgrupos parabólicos

padrões de W. Se W_J e W_K são subgrupos parabólicos padrões de W, seja $D_{J,K}$ um conjunto de representantes das classes laterais duplas de W_J e W_K em W. Para cada $d \in D_{J,K}$ escolha $n \in N$ tal que $\pi(n) = d$. Denotaremos tal conjunto por $N_{J,K}$.

A primeira observação é que $N_{J,K}$ é um conjunto de representantes das classes laterais de N_J e N_K em N. Afinal, se $n, n' \in N_{J,K}$ são tais que $n \neq n'$ e $N_JnN_K = N_Jn'N_K$, então $\pi(N_JnN_K) = \pi(N_Jn'N_K)$. Isso implica $W_J\pi(n)W_K = W_J\pi(n')W_K$, que é um aburdo pois pela escolha dos elementos de $N_{J,K}$, $\pi(n)$ e $\pi(n')$ têm que estar em classes laterais duplas distintas. Assim, $N_JnN_K \neq N_Jn'N_K$. Agora, se n é um elemento arbitrário de N, temos $\pi(n) = w_jdw_k$, com $w_j \in W_J$, $d \in D_{J,K}$ e $w_k \in W_K$. Se tomarmos $n_j \in N_j$, $n' \in N_{J,K}$, $n_k \in N_K$ tais que $\pi(n_j) = w_j$, $\pi(n') = d$ e $\pi(n_k) = w_k$, então $n(B \cap N) = n_jn'n_k(B \cap N)$. Em particular, $n \in N_Jn'N_K(B \cap N) = N_Jn'N_K$.

Proposição 2.35. *$N_{J,K}$ é um conjunto representantes das classes laterais duplas de P_J e P_K em G.*

Demonstração. A demonstração desse resultado depende de mostrarmos que se $n \in N$, então $P_JnP_K = BN_JnN_KB$. Suponha inicialmente que esse resultado seja verdadeiro. Pela Proposição 2.34, se $n, n' \in N_{J,K}$ são tais que $BN_JnN_KB = BN_Jn'N_KB$, temos $\pi(N_JnN_K) = \pi(N_Jn'N_K)$. Em particular, $\pi(n)$ e $\pi(n')$ estão na mesma classe lateral dupla de W_J e W_K em W. Porém, pela escolha de $N_{J,K}$ isso só ocorre se $n = n'$. Dessa forma, as classes laterais duplas $BN_JnN_KB = P_JnP_K$, para $n \in N_{J,K}$, são todas distintas. Além disso, se $g \in G$, então $g = bnb'$, para $b, b' \in B$ e $n \in N$. Como os $N_{J,K}$ são representantes das classes laterais duplas de N_J e N_K em N, então $n = n_jn'n_k$, com $n' \in N_{J,K}$. Portanto, $g = bn_jn'n_kb'$.

Vamos agora verificar a igualdade $P_JnP_K = BN_JnN_KB$. Temos $P_JnP_K = BN_JBnBN_KB$, logo $BN_JnN_KB \subseteq P_JnP_K$. Precisamos mostrar a inclusão $BN_JBnBN_KB \subseteq BN_JnN_KB$.

O primeiro passo será mostrar $nBN_KB \subseteq BnN_KB$. Tome $n' \in N_K$, então $\pi(n') = \pi(n_1)\dots\pi(n_{\ell_1})$, onde $n_i \in N_K$ e cada $\pi(n_i)$ é um gerador de W_K. Pela Proposição 2.34, temos $nBn'B = nBn_1\dots n_{\ell_1}B$. Queremos mostrar que $nBn_1\dots n_{\ell_1}B \subseteq BnN_KB$. Faremos isso por indução sobre ℓ_1, que é o comprimento de $\pi(n')$ no grupo de Weyl. Se $\ell_1 = 0$, não há nada a ser feito. Considere, então, o que ocorre quando $\ell_1 = 1$. Temos a expressão nBn_1B e precisamos mudar o elemento n_1 de posição, mas ele não está na posição certa para usarmos a propriedade (iv). Para contornar isso, observe que como $\pi(n_1)$ tem ordem 2, temos $\pi(n_1^{-1}) = \pi(n_1)$. Pela propriedade (iv) do par-BN, temos $n_1^{-1}Bn^{-1} \subseteq Bn_1^{-1}n^{-1}B \cup Bn^{-1}B$ e isso implica $nBn_1 \subseteq Bnn_1B \cup BnB$. Logo $nBn_1 \subseteq BnN_KB$ e $nBn_1B \subseteq BnN_KB$.

Suponha agora $\ell_1 > 1$. Pelo que acabamos de argumentar, temos

$$(nBn_1)n_2\dots n_{\ell_1}B \subseteq (Bnn_1B)n_2\dots n_{\ell_1}B \cup (BnB)n_2\dots n_{\ell_1}B.$$

Agora, tome $n'' = n_2\dots n_{\ell_1}$, então $l(n'') = \ell_1 - 1$. Assim, podemos utilizar a hipótese de indução para obter $nn_1Bn''B \subseteq Bnn_1N_KB$ e $nBn''B \subseteq BnN_KB$. Juntando essas informações, temos:

$$\begin{aligned} nBn_1n_2\dots n_{\ell_1}B &\subseteq Bnn_1Bn_2\dots n_{\ell_1}B \cup BnBn_2\dots n_{\ell_1}B \\ &\subseteq Bnn_1N_KB \cup BnN_KB \\ &\subseteq BnN_KB \qquad \text{(pois } n_1 \in N_K\text{)}. \end{aligned}$$

Daí $nBn'B \subseteq BnN_KB$ e, como n' é um elemento arbitrário de N_K, temos $nBN_KB \subseteq BnN_KB$.

Até agora, mostramos a inclusão $BN_JBnBN_KB \subseteq BN_JBnN_KB$. O próximo passo é mostrar $BN_JBnN_KB \subseteq BN_JnN_KB$ e tal fato finalizará a demonstração. Dado $n'' \in N_J$, temos $Bn''B = Bn_1 \dots n_{\ell_2}B$, onde cada $\pi(n_i)$ é um gerador do grupo W_J e $\pi(n'') = \pi(n_1)\dots\pi(n_{\ell_2})$. Procederemos exatamente como antes, mas dessa vez, podemos utilizar diretamente a propriedade (iv) do par-BN. Se $\ell_2 = 0$, não há nada a ser feito. Quando $\ell_2 = 1$, utilizando a propriedade (iv) do par-BN, obtemos $n_{\ell_2}Bnn' \subseteq Bn_{\ell_2}nn'B \cup Bnn'B$. Isso implica $n_{\ell_2}Bnn'B \subseteq BN_JnN_KB$.

Suponha agora $\ell_2 > 0$. Temos:

$$\begin{aligned} n_1 \dots n_{\ell_2-1}(n_{\ell_2}Bnn')B &\subseteq n_1 \dots n_{\ell_2-1}(Bn_{\ell_2}nn'B) \cup n_1 \dots n_{\ell_2-1}(Bnn'B) \\ &\subseteq BN_Jn_{\ell_2}nn'B \cup BN_Jnn'B \\ &\subseteq BN_Jnn'B \qquad \text{(pois } n_{\ell_2} \in N_J\text{).} \end{aligned}$$

Note que foi utilizada hipótese de indução com elemento $n''' = n_1 \dots n_{\ell_2-1}$ para obtermos a segunda inclusão. Isso finaliza a indução. Como n' e n'' são elemento arbitrários de N_J e N_K, temos $N_JBnN_KB \subseteq BN_JnN_KB$ e $BN_JBnN_KB \subseteq BN_JnN_KB$.

□

Deixamos registradas na proposição seguinte algumas outras propriedades interessantes do par-BN. Com exceção do item (i) da proposição abaixo, os outros itens não são necessários para o desenvolvimento teórico dos capítulos seguintes.

Proposição 2.36 (Propriedades Adicionais do par-BN)**.** *Se G é um grupo com par-BN, tal que I é um conjunto de índices que correspondem aos geradores do grupo de Weyl, então:*

(i) Os únicos subgrupos de G que contêm B são os parabólicos da forma P_J, com $J \subseteq I$.

(ii) Cada subgrupo parabólico de G é igual ao seu próprio normalizador.

(iii) Se J, K são subconjuntos distintos de I, então P_J e P_K não são conjugados.

(iv) Se J, K são subconjuntos de I então $P_J \cap P_K = P_{J\cap K}$. Além disso, os subgrupos P_J formam um reticulado isomorfo ao reticulado de subconjuntos de I.

Demonstração. Veja [5, Teoremas 8.3.2, 8.3.3, 8.3.4]. □

2.3 Exemplos

Nesta seção veremos alguns exemplos de grupos com par-BN. Outros exemplos aparecerão no Capítulo 3, quando discutiremos os *Grupos Finitos do tipo Lie*. Os grupos discutidos aqui são subgrupos ou quocientes dos chamados *grupos clássicos*. Não há uma definição muito precisa do que é um grupo clássico, mas eles constitutem, em essência, os seguintes grupos de matrizes: os grupos lineares, simpléticos, unitários e as famílias de grupos ortogonais [39]. Alguns autores também incluem alguns subgrupos e quocientes desses grupos. O que tais grupos possuem em comum é que eles respeitam certas formas sesquilineares. Mais detalhes sobre os grupos clássicos podem ser vistos em [39, Capítulo 3], [37], [3, Capítulos 4,7 e 14] e [21].

2.3.1 $GL_n(q)$

Utilizamos $GL_n(q)$ para denotar o grupo das matrizes $n \times n$ invertíveis sobre o corpo $\mathbb{F}_q$ com $q = p^m$ elementos. Vamos construir um par-BN para $G = GL_n(q)$ através de uma ação de G à esquerda numa sequência de espaços vetoriais. Nesta seção dado $g \in G$, escreveremos g_{ij} para denotar a entrada (i, j) de g.

Seja V um espaço vetorial de dimensão n sobre o corpo $\mathbb{F}_q$ e fixemos uma base $\mathcal{A} = \{e_1, \ldots, e_n\}$ para V. Considere a seguinte sequência de subespaços vetoriais de V:

$$\langle e_1 \rangle \subsetneq \langle e_1, e_2 \rangle \subsetneq \ldots \subsetneq \langle e_1, \ldots, e_n \rangle = V.$$

Essa é a chamada *bandeira padrão* de V. Uma *bandeira completa* é qualquer sequência de n subespaços vetoriais de V tal que $0 \subsetneq V_1 \subsetneq V_2 \subsetneq \ldots \subsetneq V_n = V$. Já uma *bandeira* é uma sequência de k subespaços vetoriais de V tal que $V_1 \subsetneq V_2 \subsetneq \ldots \subsetneq V_k = V$. Um elemento $g \in G$ age sobre o conjunto das bandeiras levando $V_1 \subsetneq V_2 \subsetneq \ldots \subsetneq V_k$ em $gV_1 \subsetneq gV_2 \subsetneq \ldots \subsetneq gV_k$.

Se $\{v_1, v_2, \ldots, v_n\}$ é uma base para V, chamaremos de *frame* o conjunto $\{\langle v_1 \rangle, \ldots, \langle v_n \rangle\}$. Também podemos considerar que G age sobre o conjunto dos *frames* levando $\{\langle v_1 \rangle, \ldots, \langle v_n \rangle\}$ em $\{\langle g(v_1) \rangle, \ldots, \langle g(v_n) \rangle\}$.

Tomaremos B como sendo o estabilizador da bandeira padrão e N como sendo o estabilizador do *frame* associado. Se $b \in B$, temos que, para cada e_i, $b(e_i)$ é uma combinação linear de $\{e_1, e_2, \ldots, e_i\}$. Segue que na base $\mathcal{A}$, b é uma matriz triangular superior e toda matriz triangular superior (na base $\mathcal{A}$) estabiliza a bandeira padrão.

Para que n esteja em N, é preciso que cada $n(e_i)$ seja um múltiplo de algum e_j. Assim cada coluna e cada linha de n possui exatamente uma entrada não-nula. As matrizes de N são chamadas de matrizes *monomiais*.

O subgrupo $T = B \cap N$ consiste das matrizes diagonais e não é difícil verificar que T é um subgrupo normal de N. De fato, se $t \in T$, $n \in N$ e $n^{-1}(e_i) = a_i e_j$ então, para cada e_i, temos:

$$\begin{aligned} ntn^{-1}(e_i) &= nt(a_i e_j) \\ &= n(a_i t_{jj} e_j) \\ &= t_{jj} e_i. \end{aligned}$$

Assim, ntn^{-1} também é uma matriz diagonal. O grupo de Weyl $W = N/T$ é isomorfo ao grupo das matrizes de permutação, que são as matrizes monomiais em que cada entrada é 0 ou 1. Para ver isso, basta observar que em cada classe lateral nT, se $n' \in nT$, então $n'(e_i) = \lambda_i n(e_i)$, isto é, as matrizes possuem as entradas não-nulas localizadas nas mesmas posições, porém tais entradas diferem por um escalar. Por sua vez, o grupo das matrizes de permutação é isomorfo ao grupo das permutações S_n. Assim, temos $W \cong S_n$ e W é gerado por elementos de ordem 2 que correspondem às transposições $\{(1\ 2), (2\ 3), \ldots, (n-1\ n)\}$. Tomando tais elementos como geradores para W, segue que o posto do par-BN é $n - 1$.

Até agora, verificamos que as propriedades (ii) e (iii) da Definição 2.1 são satisfeitas por B e N. Para mostrar que B e N geram G, utilizaremos matrizes da forma $X_{ij}(\alpha)$, com $i \neq j$, tais que suas entradas são idênticas as da matriz identidade com exceção da entrada (i, j), que é α. As matrizes da forma X_{ij} são chamadas de *transvecções*.

As transvecções correspondem às operações elementares em matrizes. Assim, se $g \in G$, $X_{ij}(\alpha)g$ é idêntica à matriz g com exceção da i-ésima linha que é igual à i-ésima linha de g somada com α vezes a j-ésima linha de g. Notes que as transvecções que estão B são aquelas em que $i < j$.

Proposição 2.37. *$G = GL_n(q)$ é gerado por B e N.*

Demonstração. [2, Páginas 44 e 45] Dado $g \in G$, como g é invertível, a primeira coluna certamente possui uma entrada que é não-nula. Escolha k_1 tal que $g_{i1} = 0$ para $i > k_1$ e $g_{k_1 1} \neq 0$. Assim, podemos multiplicar g à esquerda por matrizes da forma $X_{ik_1}(\alpha)$ de tal forma que o único elemento não-nulo da primeira coluna seja $g_{k_1 1}$, isto é, estamos utilizando a entrada $g_{k_1 1}$ como pivô para zerar as demais entradas da primeira coluna. Além disso, pela escolha de k_1, as matrizes $X_{ik_1}(\alpha)$ que realizam o pivoteamente satisfazem $i < k_1$, logo estão em B. Denotaremos a matriz obtida ao término desse processo por $M_1 g$, onde M_1 é um produto de transvecções.

A matriz $M_1 g$ também é invertível e assim possui um elemento diferente de 0 na segunda coluna numa linha diferente de k_1. Se isso não ocorresse, as duas primeiras colunas de $M_1 g$ iriam diferir por um escalar, o que seria absurdo. Agora, escolhemos k_2 tal que $k_2 \neq k_1$, $(M_1 g)_{k_2 2} \neq 0$, $(M_1 g)_{i2} = 0$ para $i > k_2$, $i \neq k_1$. Assim, as entradas não nulas da segunda coluna estão nas linhas menores ou iguais que k_2 ou na linha k_1. Utilizaremos a entrada $(M_1 g)_{k_2 2}$ como pivô para zerar as linhas tais que $i < k_2$ e $i \neq k_1$. Isso pode ser feito por meio de transvecções da forma $X_{ik_2}(\alpha)$ e, como $i < k_2$, tais transvecções estão em B. Assim obtemos uma matriz $M_2 M_1 g$ que possui uma entrada não-nula na primeira linha e no máximo duas entradas não-nulas na segunda linha.

Continuando esse processo, obtemos uma matriz $M_n \dots M_2 M_1 g$ tal que $M_n \dots M_2 M_1 \in B$ e possui no máximo i elementos não nulos na i-ésima coluna. Chamando $M_n \dots M_2 M_1$ de b, temos que bg difere de uma matriz triangular superior apenas pela ordem das linhas. Podemos escolher em N uma matriz n que rearranja as linhas de bg de forma que $nbg \in B$. Isto é, $g = b' n^{-1} b^{-1}$. Em particular, B e N geram G.

□

Tomamos como conjunto gerador para W elementos s_i que correspondem às transposições $(i\ i+1)$. Assim, s_i troca e_i por e_{i+1} e fixa os outros vetores da base. Por sua vez, se a imagem de n_i pelo homomorfismo quociente é s_i, então n_i troca e_i por um múltiplo de e_{i+1} e leva e_j em um múltiplo de e_j, para $j \neq i$. Com isso em mente, não é muito complicado verificar a propriedade (v) da Definição 2.1. Se $g \in G$, então $n_i g$ é a matriz g, porém com a i-ésima *coluna* trocada por um múltiplo da coluna $i+1$. As outras colunas aparecem iguais a menos de um múltiplo. Agora, $n_i g n_i$ é a matriz $n_i g$, porém com a i-ésima *linha* permutada com a linha $i+1$, de forma análoga. Se tomarmos, por exemplo, uma matriz triangular tal que $b_{ij} \neq 0$ para $i \leq j$, fica claro que $n_i b n_i$ certamente não será uma matriz triangular e $n_i B n_i \neq B$.

A propriedade (iv) da Definição 2.1 é um pouco mais trabalhosa de ser verificada. Uma demonstração de que B e N satisfazem esta propriedade pode ser encontrada em [1, Seção 6.5] ou em [37, cap 5, páginas 32 e 33].

Uma vantagem dessa construção do par-BN de G através de bandeiras, é que torna fácil identificar os subgrupos parabólicos de G. Se da bandeira padrão retirarmos alguns dos espaços vetoriais obtemos uma *sub-bandeira*. Assim, o estabilizador de uma sub-bandeira com certeza contém B. Pela Proposição 2.36, os únicos subgrupos de G que

contém B são os parabólicos da forma P_J para $J \subseteq I$. A bandeira padrão possui 2^{n-1} sub-bandeiras distintas, considerando que não faz diferença se a bandeira possui o espaço V. Pode-se mostrar que os estabilizadores dessas sub-bandeiras são todos distintos e, portanto, correspondem aos subgrupos parabólicos padrões de G.

2.3.2 $SL_n(q)$, $PSL_n(q)$ e $PGL_n(q)$

A construção do par-BN para $SL_n(q)$ se dá a partir do par-BN de $GL_n(q)$. Tomaremos como par-BN para $SL_n(q)$ os grupos $B_0 = B \cap SL_n(q)$ e $N_0 = N \cap SL_n(q)$, onde B e N formam um par-BN para $GL_n(q)$ como na seção anterior. Por sua vez, o par-BN de $PSL_n(q)$ será construído a partir do par-BN de $SL_n(q)$, tomando $B_0/Z(SL_n(q))$ e $N_0/Z(SL_n(q))$. Já o par-BN de $PGL_n(q)$ será formado por $B/Z(GL_n(q))$ e $N/Z(GL_n(q))$. Vejamos primeiro o par-BN para $SL_n(q)$.

É interessante notar que boa parte dos argumentos utilizados na seção anterior dependem apenas da posição dos elementos não-nulos nas matrizes consideradas e não dos valores em si. Por exemplo, para verificar que B_0 e N_0 geram $SL_n(q)$, basta proceder como na Proposição 2.37. As transvecções $X_{ij}(\alpha)$ possuem determinante 1, de modo que se $g \in SL_n(q)$, a matriz $M_n \dots M_2 M_1 g$ também está em $SL_n(q)$. Precisamos ter cuidado, porém, na hora de escolher a matriz monomial que reordenará a matriz. Uma escolha segura é tomar uma matriz de permutação. Uma tal matriz sempre possui determinante $+1$ ou -1. Se a matriz de permutação n_0 necessária para transformar $M_n \dots M_2 M_1 g$ em uma matriz triangular superior tiver determinante -1, basta trocar o sinal de um dos elementos de n_0. Assim, $n_0 b_0 g \in B_0$, onde $b_0 = M_n \dots M_2 M_1$ e isso é suficiente para mostrar que B_0 e N_0 geram $SL_n(q)$.

O subgrupo $T_0 = B_0 \cap N_0$ é formado por matrizes diagonais com determinante 1. E utilizando o mesmo argumento de antes, que só depende da estrutura das matrizes, obtemos que T_0 é normal em N_0. Curiosamente, o grupo de Weyl correspondente também é isomorfo ao S_n, isto é, o posto do par-BN não cai. Para ver isso, observe que toda forma de trocar linhas e colunas de matrizes pode ser realizada por um elemento de N_0, desde de que não nos preocupemos se as linhas aparecem a menos de um múltiplo. Por exemplo, a matriz de permutação que troca a primeira linha com a segunda linha, dependendo da característica do corpo, não estará em $SL_n(q)$, pois o determinante da matriz será -1. Porém, se trocarmos um dos elementos não-nulos de tal matriz por -1, obtemos um elemento de N_0 que produz o mesmo efeito de trocar a primeira linha com a segunda linha. Uma das linhas aparecerá multiplicada por -1, mas isso não é problema. Quando consideramos o quociente N_0/T_0 não interessa se as linhas aparecem multiplicadas por um escalar, o que importa é quais linhas são permutadas.

A propriedade (iv) da Definição 2.1 é verificada de forma análoga. Como omitimos a demonstração da propriedade (v) para $GL_n(q)$, também omitiremos para $SL_n(q)$. De toda forma, a demonstração também é análoga. Veja, por exemplo, [8, *Remarks*, pág. 583].

Observe que $Z(SL_n(q))$ é formado por matrizes escalares com determinante 1, portanto $Z(SL_n(q)) \leq B_0 \cap N_0$. Com o que foi visto até agora, fica claro que $B_0/Z(SL_n(q))$ e $N_0/Z(SL_n(q))$ devem formar um par-BN para $PSL_n(q)$. Nesse caso, temos que

$$\frac{B_0}{Z(SL_n(q))} \bigcap \frac{N_0}{Z(SL_n(q))} = \frac{B_0 \cap N_0}{Z(SL_n(q))}.$$

e tal fato pode ser verificado observando as entradas não-nulas das matrizes. Assim, o grupo de Weyl correspondente é

$$\frac{\frac{N_0}{Z(SL_n(q))}}{\frac{B_0\cap N_0}{Z(SL_n(q))}} \cong \frac{N_0}{B_0 \cap N_0}.$$

que é exatamente o grupo de Weyl de $SL_n(q)$. Um resultado análogo vale para $PGL_n(q)$. No total, temos pelo menos 4 grupos com o mesmo grupo de Weyl: $GL_n(q), SL_n(q), PSL_n(q)$ e $PGL_n(q)$. Esse fato às vezes é mencionado dizendo que tais grupos possuem a mesma geometria.

2.3.3 $Sp_{2n}(q)$

Nesta seção discutiremos brevemente a construção do grupo simplético e de um par-BN associado a ele. Seja V um espaço vetorial de dimensão finita sobre o corpo $\mathbb{F}_q$. Vamos supor que V esteja equipado com uma forma bilinear alternada $\beta : V \times V \to \mathbb{F}_q$. Uma tal forma β satisfaz as seguintes propriedades para todos $u, v \in V$ e $\lambda \in \mathbb{F}_q$:

(i) $\beta(u + u', v) = \beta(u, v) + \beta(u', v)$.

(ii) $\beta(u, v + v') = \beta(u, v) + \beta(u, v')$.

(iii) $\beta(\lambda u, v) = \beta(u, \lambda v) = \lambda\beta(u, v)$.

(iv) $\beta(u, u) = 0$.

Uma tal forma é sempre anti-simétrica pois, $\beta(u+v, u+v) = 0$ e isso implica $\beta(u, u)+\beta(u, v)+\beta(v, u)+\beta(v, v) = 0$. Logo $\beta(u, v) = -\beta(v, u)$[1]. Dado $X \subseteq V$, escreveremos $X^\perp$ para designar o conjunto $\{v \in V \mid \beta(v, x) = 0,\ \forall x \in X\}$. Iremos exigir também que β satisfaça $V^\perp = \{0\}$, isto é, β não deve ser uma forma singular. Dizemos, então, que β é uma forma *simplética*.

Nessas circunstâncias, podemos obter uma base bastante conveniente para V. Escolha qualquer $e_1 \in V$ diferente de 0. Como β é não singular, existe $v_1 \in V$ tal que $\beta(e_1, v_1) = \lambda_1$, com $\lambda_1 \neq 0$. Tome $f_1 = \lambda^{-1}v_1$ Agora, considere a restrição de β ao subespaço $\langle e_1, f_1\rangle^\perp$. Se $V \neq \langle e_1, f_1\rangle$, podemos escolher $e_2 \in \langle e_1, f_1\rangle^\perp$, tal que $e_2 \neq 0$. Deve existir um $v_2 \in \langle e_1, f_1\rangle^\perp$ tal que $\beta(e_2, v_2) = \lambda_2$, com $\lambda_2 \neq 0$, caso contrário, teremos $e_2 \in V^\perp$. Com isso, podemos tomar $f_2 = \lambda_2^{-1}v_2$ e repetir esse processo até obtermos uma base para V. Podemos concluir desta maneira que V deve possuir dimensão par. Os pares da forma $\{e_i, f_i\}$ são chamados de *pares hiperbólicos*. Nessa base, cada vetor é ortogonal a todos os outros com a exceção do vetor que forma o seu par hiperbólico.

O grupo simplético $Sp_{2n}(q)$ é o subgrupo de $GL_{2n}(q)$ das isometrias da forma simplética β, isto é, $g \in Sp_{2n}(q)$ se, e somente se, $\beta(g(u), g(v)) = \beta(u, v)$, para todos $u, v \in V$. Na base $\mathcal{A} = \{e_1, \ldots, e_n, f_n, \ldots, f_1\}$, a matriz J da forma bilinear β assume a seguinte forma:

$$J = \begin{pmatrix} 0 & Q \\ -Q & 0 \end{pmatrix}, \text{onde } Q = \begin{pmatrix} 0 & \cdots & 1 \\ \vdots & \iddots & \vdots \\ 1 & \cdots & 0 \end{pmatrix}.$$

[1] Observe que se a característica for 2, β é simétrica.

Dessa forma $g \in Sp_{2n}(q)$ se, e somente se, $g^T J g = J$. Isso implica $\det(g)^2 = 1$ e, portanto, $\det(g) = \pm 1$. Na verdade, com um pouco mais de trabalho, pode-se mostrar que $\det(g) = 1$ e $Sp_{2n}(q) \leq SL_{2n}(q)$.

O par-BN para o grupo simplético também será construído a partir de uma bandeira completa do espaço vetorial V. Considere a seguinte bandeira:

$$\langle e_1 \rangle \subsetneq \ldots \subsetneq \langle e_1, \ldots, e_n \rangle \subsetneq \langle e_1, \ldots, e_{n-1} \rangle^{\perp} \subsetneq \ldots \subsetneq \langle e_1 \rangle^{\perp} \subsetneq V.$$

Tomaremos como B os elementos de $Sp_{2n}(q)$ que estabilizam essa bandeira completa. Note que se $g \in Sp_{2n}(q)$ e g estabiliza um espaço vetorial W, então g também estabiliza $W^{\perp}$. Dessa forma, podemos descrever B alternativamente como o estabilizador da seguinte bandeira:

$$\langle e_1 \rangle \subsetneq \ldots \subsetneq \langle e_1, \ldots, e_n \rangle.$$

Dizemos que um espaço W é *totalmente isotrópico* se $W \subseteq W^{\perp}$. Nessas condições, definimos o *índice de Witt* de V como a maior dimensão possível de um espaço totalmente isotrópico. O índice de Witt de um espaço vetorial equipado com uma forma simplética é sempre n. Assim, essa bandeira é especial pois é uma bandeira maximal com respeito a propriedade de ser composta de espaços totalmente isotrópicos.

Observe que se $W = \langle e_1, e_2, \ldots, e_i \rangle$, então $W^{\perp} = \langle e_1, e_2, \ldots, e_n, f_n, \ldots, f_{i+1} \rangle$. Portanto, na base $\mathcal{A}$, as matrizes de B também são triangulares superiores. Para o grupo N tomaremos o estabilizador do *frame* padrão:

$$\{\langle e_1 \rangle, \ldots, \langle e_n \rangle, \langle f_n \rangle, \ldots, \langle f_1 \rangle\}.$$

Assim, N é composto das matrizes monomiais que estão no grupo simplético. Isso restringe um pouco as possibilidades de permutar linhas e colunas. Dado $n \in N$, como n deve preservar a forma alternada, temos que n leva pares hiperbólicos em pares hiperbólicos. Assim, se $n(e_i) = \lambda v_j$, com $v_j \in \mathcal{A}$, temos $n(f_i) = \lambda^{-1} u_j$ e (u_j, v_j) devem formar um par hiperbólico.

Como nos casos anteriores, $B \cap N$ também é composto de matrizes diagonais e quando consideramos o grupo de Weyl $W = N/(B \cap N)$, nos preocupamos apenas em como as linhas e colunas são permutadas, desconsiderando o fato de uma linha aparecer multiplicada por uma constante, por exemplo.

Dessa vez o grupo de Weyl não será todo S_{2n}, ao invés disso, obteremos um subgrupo de S_{2n}. Um elemento $w \in W$ permuta os n pares hiperbólicos, e para cada forma de permutar os pares hiperbólicos, é permitido trocar um elemento do par pelo outro. Para exemplificar, temos que w tem que levar um par hiperbólico $\{e_i, f_i\}$ em um outro par $\{e_j, f_j\}$, mas há liberdade para escolher se $w(e_i) = e_j$ ou se $w(e_i) = f_j$. Assim, a ordem de W é $n!\, 2^n$. Para descrever de forma sucinta W, vamos discutir brevemente o produto entrelaçado de grupos. Mais informações podem ser encontradas em [31, Capítulo 7].

Definição 2.38. Sejam D e Q grupos, Ω um conjunto sobre o qual Q age e seja K o produto direto de $|\Omega|$ cópias de D. Então o *produto entrelaçado* de D por Q, denotado por $D \wr Q$ é o produto semidireto de K por Q, onde, para $q \in Q$, a ação de Q sobre K leva (d_ω) em $(d_{q\omega})$. O subgrupo K de $D \wr Q$ é chamado de *base* do produto entrelaçado.

Vamos fazer algumas observações sobre a definição e a notação utilizadas. Um elemento de K é da forma (d_ω), isso corresponde a uma escolha de um elemento de D em

cada uma das $|\Omega|$ cópias de D. Como Ω é finito, convencionamos $\omega = (\omega_1, \ldots, \omega_{|\Omega|})$ e podemos considerar um elemento (d_ω) como sendo da forma $(d_{\omega_1}, d_{\omega_2}, \ldots, d_{\omega_{|\Omega|}})$. Note que a operação em K é dada coordenada a coordenada. Agora, para $q \in Q$, a ação de Q sobre K corresponde a levar $(d_{\omega_1}, d_{\omega_2}, \ldots, d_{\omega_{|\Omega|}})$ em $(d_{q(\omega_1)}, d_{q(\omega_2)}, \ldots, d_{q(\omega_{|\Omega|})})$ e isso está bem definido pelo fato de Q agir sobre Ω.

Para descrever a operação de um grupo que é o produto semi-direto de dois grupos K e Q, precisamos conhecer como é o homomorfismo de Q em $\mathrm{Aut}(K)$. Para cada q fixo, a ação de Q sobre K define um automorfismo e isso nos dá uma expressão para a operação do grupo $D \wr Q$. Para $((d_\omega), q_1), ((d_{\omega'}), q_2) \in D \wr Q$, temos

$$((d_\omega), q_1).((d_{\omega'}), q_2) = ((d_\omega d_{q_1(\omega')}), q_1 q_2).$$

Com isso em mente, o grupo de Weyl de $Sp_{2n}(q)$ é isomorfo ao produto entrelaçado $C_2 \wr S_n$, onde C_2 é o grupo cíclico de ordem 2. O conjunto Ω é formado pelos pares hiperbólicos da base $\mathcal{A}$ e S_n age sobre eles permutando-os. Um elemento de $C_2 \wr S_n$ é da forma $((c_1, c_2, \ldots, c_n), q)$, com $q \in S_n$ e $(c_1, c_2, \ldots, c_n) \in K$, onde K é o produto direto de $|\Omega|$ cópias de C_2. Informalmente, q especifica como os pares hiperbólicos são permutados entre si e os c_i indicam se o par hiperbólico (e_i, f_i) será levado em (e_i, f_i) ou em (f_i, e_i). Dessa forma, ao menos informalmente, fica claro que $W \cong C_2 \wr S_n$. Um tal grupo, é chamado de grupo de Weyl de tipo B_n. Veja, por exemplo, [17, Capítulo 2].

A verificação de que B e N formam um par-BN de $Sp_{2n}(q)$ pode ser encontrada em [37, Teorema 8.12].

2.3.4 Grupos Simples entre os Grupos Clássicos

Para cada classe de grupos clássicos, há pelo menos uma família infinita de grupos simples. Pode-se mostrar que $PSL_n(q)$ é sempre simples, quando $n \geq 3$ ou $\mathbb{F}_q \geq 4$ [39, Seção 3.3.2]. Podemos também considerar o grupo simplético projetivo $PSp_{2n}(q) = Sp_{2n}(q)/Z(Sp_{2n}(q))$ e mostrar que $PSp_{2n}(q)$ é simples, com a exceção de $PSp_2(2), PSp_2(3)$ e $PSp_4(2)$ [37, Teorema 8.8]. Os grupos unitários e ortogonais também possuem famílias de subgrupos ou quocientes simples.

Mostrar que tais grupos são simples, em geral, envolve argumentos parecidos, mas que devem ser desenvolvidos caso a caso. O que eles têm em comum é que a simplicidade costuma vir como consequência do *Lema de Iwasawa* [39, Teorema 3.1], que fornece condições suficientes para um grupo perfeito agindo sobre um conjunto ser simples. Para finalizar este capítulo, mencionamos que é possível uma prova alternativa utilizando o seguinte resultado:

Teorema 2.39. *Seja G um grupo com par-BN satisfazendo as seguintes condições:*

(*i*) $G = G'$

(*ii*) *B é solúvel*

(*iii*) $\bigcap_{g \in G} gBg^{-1} = 1$

(*iv*) *O conjunto de índices I, ao qual correspondem os geradores do grupo de Weyl, não pode ser particionado em dois conjuntos complementares J, K tais que, para todos $w_j \in W_J$, $w_k \in W_K$, tenhamos $w_j w_k = w_k w_j$*

Então G é simples.

Demonstração. Ver [5, Teorema 11.1.1] ou [3, página 223]. □

Em [5], o autor utiliza esse resultado para provar a simplicidade dos *grupos de Chevalley* e dos grupos *twisted*. Os grupos de Chevalley contém alguns dos grupos clássicos simples, porém não todos. Os grupos clássicos restantes aparecem como subgrupos dos grupos de Chevalley, os chamados grupos *twisted* [5, Seção 13.4 e Teorema 14.4.1].

Capítulo 3

Grupos Lineares

Este capítulo apresenta alguns conceitos básicos para podermos tratar dos *Grupos Finitos do tipo Lie*. Há pelo menos duas formas distintas de obtê-los. A primeira é através de automorfismos de certas álgebras de Lie. Essa construção dá origem aos grupos de Chevalley, os grupos *twisted*, sendo que todos os grupos finitos do tipo Lie se encaixam em uma dessas duas classes. Essa abordagem pode ser vista, por exemplo, em [5].

A segunda construção envolve *Grupos Lineares Algébricos* e os grupos do tipo Lie aparecem como pontos fixos de endomorfismos de *Steinberg*. Esta é a abordagem que nós discutiremos brevemente nesse capítulo.

A Teoria dos Grupos Lineares Algébricos é vasta e depende essencialmente da *Geometria Algébrica*. Dessa forma, trataremos apenas de forma superficial os conceitos necessários. Mais informações podem ser vistas em [4, 16, 24, 33].

3.1 Um pouco de Geometria Algébrica

Esta seção trata de alguns conceitos importantes de Geometria Algébrica. Mais detalhes podem ser vistos em [25] ou [33, Capítulo 1].

Seja K um corpo algebricamente fechado de característica p. Considere a álgebra de polinômios em n variáveis $K[T_1, T_2, \ldots, T_n]$, que denotaremos por $K[T]$. A topologia de Zariski é a topologia em K^n obtida ao declarar que os conjuntos fechados são precisamente os conjuntos de zeros dos polinômios de um ideal I de $K[T]$.

Definição 3.1 (Topologia de Zariski)**.** Um subconjunto X de K^n é dito *fechado* na topologia de Zariski, se $X = \mathcal{V}(I)$, onde I é um ideal de $K[T]$ e $\mathcal{V}(I) = \{x \in K^n \mid f(x) = 0, \text{para todos } f \in I\}$. Dizemos que X é um *conjunto algébrico* .

De forma dual, se X é um subconjunto de K^n, defina $\mathcal{I}(X)$ como sendo o conjunto $\{f \in K[T] \mid f(x) = 0, \text{para todo } x \in X\}$. Nessas condições, podemos enunciar o *Nullstellensatz* de Hilbert:

Teorema 3.2 (Nullstellensatz)**.** *Se I é um ideal próprio de $K[T]$, então $\mathcal{V}(I) \neq \emptyset$. Além disso, vale $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$, onde $\sqrt{I}$ é o ideal radical de I, isto é,*

$$\sqrt{I} = \{f \in K[T] \mid f^n \in I \text{ para algum } n \text{ inteiro não-negativo}\}.$$

As funções $\mathcal{V}$ e $\mathcal{I}$ induzem bijeções que revertem as inclusões entre os fechados da topologia e os ideais radicais de $K[T]$. Agora, se X é um subconjunto fechado, podemos associar a ele uma álgebra isomorfa a $K[T]/\mathcal{I}(X)$, basta tomar os polinômios de $K[T]$ e restringir a X. De forma mais precisa, cada polinômio $f \in K[T]$ define uma função polinomial $f : K^n \to K$ que leva $(a_1, \ldots, a_n)$ em $f(a_1, \ldots, a_n)$ e podemos considerar também a restrição $f|_X : X \to K$. Assim, o núcleo do homomorfismo que leva f em $f|_X$ é precisamente o conjunto das funções polinomiais que se anulam em todo X. Costuma-se denotar a álgebra $K[T]/\mathcal{I}(X)$ por $K[X]$ e diz-se que $K[X]$ é a *álgebra afim* de X. Mostraremos a seguir que a topologia induzida em X coincide com a topologia de Zariski quando se considera os polinômios de $K[X]$.

Proposição 3.3. *Um subconjunto Y de X é fechado (na topologia induzida) se, e somente se, $Y = \mathcal{V}_X(I_X)$, onde I_X é um ideal de $K[X]$ e $\mathcal{V}_X(I_X) = \{x \in X \mid f(x) = 0, \forall f \in I_X\}$.*

Demonstração. Como X é fechado então $X = \mathcal{V}(I)$, para algum ideal radical de $K[T]$. Mostraremos primeiro que se Y é fechado, então $Y = \mathcal{V}_X(J_X)$. Se Y é fechado na topologia induzida, como X é fechado, isso significa que Y é fechado em K^n. Assim $Y = \mathcal{V}(J)$ para algum ideal radical I de $K[T]$. Como $Y \subseteq X$, então $I \subseteq J$. Como temos um homomorfismo $K[T]/I \cong K[X]$, um ideal J que contém I corresponde a um ideal J_X de $K[X]$. Temos $Y = \mathcal{V}_X(J_X)$. Afinal, dado $y \in Y$, temos $f(y) = 0$, para todo $f \in J$, como J_X é apenas a restrição dos polinômios de J a X, temos $f(y) = 0$, para tod $f \in J_X$. Reciprocamente, se y é tal que $f(y) = 0$ para todo $f \in J_X$, não podemos ter $g(y) \neq 0$, para algum $g \in J$. Assim $y \in \mathcal{V}(J)$.

Se $Y = \mathcal{V}_X(J_X)$, existe um ideal J de K^n que corresponde a J_X pelo homomorfismo dado pela restrição. O mesmo argumento utilizado nos dá $\mathcal{V}_X(J_X) = \mathcal{V}(J)$ e, assim, Y é fechado em K^n. Portanto, Y é fechado na topologia induzida. □

Note que de forma análoga, podemos definir $\mathcal{I}_X(Y)$ como o ideal radical $\{f \in K[X] \mid f(x) = 0, \text{para todo } x \in Y\}$ de $K[X]$. Como consequência do *Nullstellensatz*, há também uma bijeção entre os conjuntos fechados de X e os ideais radicais de $K[X]$. Deixaremos registrado isso como uma proposição.

Proposição 3.4. *Se X é um conjunto algébrico de K^n, as funções $\mathcal{I}_X$ e $\mathcal{V}_X$ são bijeções que revertem a inclusão entre os conjuntos fechados de X e os ideais radicais de $K[X]$. Se I é um ideal próprio de $K[X]$, então $\mathcal{V}_X(I) \neq \emptyset$.*

Na proposição seguinte, veremos que $K[X]$ e os seus ideais maximais determinam por completo não apenas a topologia de X mas também o próprio conjunto X.

Proposição 3.5. *Se X é um conjunto algébrico e para todo $x \in X$, então vale:*

(i) A topologia de Zariski é T_1, ou seja, $\{x\}$ é fechado.

(ii) O conjunto $M_x = \{f \in K[X] \mid f(x) = 0\}$ é um ideal maximal.

(iii) A correspondência que leva x em M_x é uma bijeção entre os pontos de X e os ideais maximais de $K[X]$.

(iv) Existe uma bijeção entre os homomorfismos de álgebra $K[X] \to K$ e os ideais M_x.[1]

[1]Consideramos aqui que um homomorfismo de álgebra é não-nulo e deve preservar o elemento identidade da multiplicação

Demonstração. (i) Considere o ideal $I_x = \bigoplus_{i=1}^{n}(T_i - x_i)$, onde $(T_i - x_i)$ denota o ideal gerado pelo polinômio $f(T_1, T_2, \ldots, T_i, \ldots, T_n) = T_i - x_i$. Assim, $\mathcal{V}(I_x) = \cap_{i=1}^{n}\mathcal{V}((T_i - x_i)) = \{x\}$, logo $\{x\}$ é fechado.

(ii) Note que $\mathcal{I}_X(\{x\}) = M_x$ é um ideal radical. Isso decorre do fato mais geral que se Y é qualquer subconjunto de X, então $\mathcal{I}(Y)$ é um ideal radical. De fato, se f é tal que $f^n(x) = 0$, para $x \in Y$, então como K é um corpo, temos $f(x) = 0$ e $f \in \mathcal{I}(Y)$. Agora, se M_x não for um ideal maximal, então existe um ideal próprio J de $K[X]$ que contém M_x. Como $\{x\}$ é fechado, temos $\mathcal{V}(M_x) = \{x\}$ e $\{x\} \supsetneq \mathcal{V}(J)$. A única possibilidade disso ocorrer é se $\mathcal{V}(J) = \emptyset$, mas pela Proposição 3.4 isso não poderia ocorrer, pois J é um ideal próprio. Então M_x é, de fato, um ideal maximal.

(iii) Se $x \neq y$, não podemos ter $M_x = M_y$, pois $\mathcal{V}$ é uma bijeção e temos $\mathcal{V}(M_x) = \{x\}$ e $\mathcal{V}(M_y) = \{y\}$. Se M é um ideal maximal de $K[X]$, temos que $\mathcal{V}(M)$ só pode conter um único ponto. Afinal, se tiver mais de um ponto, haveria um subconjunto fechado próprio e não-vazio de $\mathcal{V}(M)$ que seria levado por $\mathcal{I}$ em um ideal próprio de $K[X]$ que conteria M. Então $\mathcal{V}(M) = \{x\}$ e $\mathcal{I}(\mathcal{V}(M)) = M_x$.

(iv) Se φ é um homomorfismo de K-álgebras entre $K[X]$ e K, observe que ele necessariamente é sobrejetor. Pois se $c \in K$, temos $\varphi(c) = c$. Assim, $K[X]/\ker\varphi \cong K$ e $\ker\varphi$ é um ideal maximal. Agora, se M_x é um ideal maximal, o homomorfismo de álgebras φ_x que leva em $f \in K[X]$ em $f(x)$ tem M_x como núcleo. □

A Proposição 3.5 mostra que um ponto $x \in X$ pode ser visto em $K[X]$ como ideal maximal ou como o homomorfismo que avalia f no ponto x.

3.1.1 Variedades Afins

Começaremos com a definição de variedade afim.

Definição 3.6. Uma *K-variedade afim* é um par $(X, K[X])$ com X um conjunto algébrico e $K[X]$ a sua álgebra afim.

Quando não houver possibilidade de confusão, escreveremos apenas *variedade afim* ao invés de *K-variedade afim*. Além disso, escreveremos X ao invés de $(X, K[X])$. A partir do par $(X, K[X])$ é possível construir um feixe $\mathcal{O}$ de funções, de tal forma que $(X, \mathcal{O})$ é um *ringed space*. Assim, os morfismos entre duas variedades afins X e Y são definidos como os morfismos entre X e Y vistos como *ringed spaces*. Mais detalhes sobre essas definições podem ser vistos em [33, Seção 1.4]. Neste trabalho, utilizaremos uma especialização dessa definição para o caso em que X e Y são apenas variedades afins.

Definição 3.7. Se $(X, K[X])$ e $(Y, K[Y])$ são variedades afins, então uma função contínua $\varphi : X \to Y$ é um *morfismo de variedades afins* se, para todo $f \in K[Y]$, temos $f \circ \varphi \in K[X]$.

Um morfismo φ de variedades afins induz um homomorfismo de álgebra φ^* de $K[Y]$ em $K[X]$ que leva f em $f \circ \varphi$. Com isso, podemos caracterizar os morfismos de variedades afins.

Proposição 3.8. *Uma função $\varphi : X \to Y$, com $X \subseteq K^n$ e $Y \subseteq K^m$ é um morfismo de variedades afins se, e somente se, cada função coordenada de φ é um polinômio de $K[X]$.*

Demonstração. A função f_i que leva $y = (y_1, \ldots, y_i, \ldots, y_m)$ em y_i é um polinômio de $K[Y]$. Assim se φ for um morfismo de variedades afins, temos $f_i \circ \varphi \in K[X]$, isto é, a i-ésima função coordenada de φ é um polinômio de $K[X]$.

Reciprocamente, se $\varphi = (\varphi_1, \ldots, \ldots, \varphi_m)$ e cada $\varphi_i \in K[X]$, para $f \in K[Y]$ temos que $f \circ \varphi$ continua sendo um polinômio em $K[X]$. Resta mostrar que φ é contínua. Para isso, tome um conjunto A fechado em Y, então $A = \mathcal{V}(I)$, para algum ideal radical I de $K[Y]$. Podemos escrever também $A = \bigcap_{f\in I} f^{-1}(0)$. Agora, $\varphi^{-1}(A) = \varphi^{-1}(\bigcap_{f\in I} f^{-1}(0))$. Portanto, $\varphi^{-1}(A) = \bigcap_{f\in I} \varphi^{-1}(f^{-1}(0))$. Para cada $f \in I$, temos $\varphi^{-1}(f^{-1}(0)) = (f \circ \varphi)^{-1}(0)$. Logo $\varphi^{-1}(A) = \bigcap_{f\in I}(f\circ\varphi)^{-1}(0)$. Como cada $f\circ\varphi \in K[X]$, isso expressa $\varphi^{-1}(A)$ como a interseção de conjuntos de zeros de polinômios em $K[X]$, portanto, $\varphi^{-1}(A)$ é um subconjunto fechado de X.

□

Agora vamos mostrar a existência de um functor contravariante da categoria das K-variedades afins para as K-álgebras afins.

Proposição 3.9. *A correspondência $\mathcal{F}$ que leva X em $K[X]$ e φ em φ^* é um functor contravariante (isto é, $\mathcal{F}$ "inverte as setas") fiel e completo.*

Demonstração. Mostraremos que se X, Y, Z são K-variedades afins e $\varphi : X \to Y$ e $\psi : Y \to Z$ são morfismos, então

(*i*) φ^* é um morfismo entre $K[Y]$ e $K[X]$.

(*ii*) Se $\varphi = id_X$, então $id_X^* = id_{K[X]}$.

(*iii*) $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.

(*iv*) Se $\varphi^* = \psi^*$ então $\varphi = \psi$.

(*v*) Se $\gamma : K[Y] \to K[X]$ é um morfismo de K-álgebras afins, existe um único morfismo de K-variedades afins $\varphi : X \to Y$ tal que $\varphi^* = \gamma$.

Para (*i*), já vimos que φ^* é um morfismo entre $K[Y]$ e $K[X]$. Verifiquemos que se id_X é o morfismo identidade em X, então id_X^* é também o morfismo identidade em $K[X]$. Isso é evidente pois, dado $f \in K[X]$, temos $id_X^* \circ f = f$, isso prova (*ii*). Agora, se $f \in K[Z]$, temos $(\psi \circ \varphi)^* f = (f \circ \psi) \circ \varphi = (\psi^* f) \circ \varphi = \varphi^* \circ \psi^* f$ e isso prova (*iii*). Esses três itens estabelecem $\mathcal{F}$ como um functor contravariante.

(*iv*) Considere a projeção π_i na i-ésima coordenada. Se $\varphi^* = \psi^*$, temos $\pi_i \circ \varphi = \pi_i \circ \psi$, para todas as coordenadas. Como as funções coordenadas de φ e ψ são iguais, temos $\varphi = \psi$.

(*v*) Suponha $X \subseteq K^n$ e $Y \subseteq K^m$. Se $\gamma : K[Y] \to K[X]$ é um morfismo de K-álgebras afins, γ opera levando $f \in K[Y]$, em um polinômio $\gamma \circ f \in K[X]$. Agora, considere os polinômios $\tilde{y}_i$ que levam $y \in Y$ na i-ésima componente de y, que denotaremos por y_i. Pela linearidade e por ser um homomorfismo de K-álgebras, γ é completamente determinado pelos valores que assume nos polinômios $\tilde{y}_i$ e vale a seguinte relação:

$$(\gamma \circ f)(x) = f((\gamma \circ \tilde{y}_1)(x), \ldots, (\gamma \circ \tilde{y}_m)(x)). \tag{3.1}$$

Isso sugere fortemente considerar a função $\varphi : X \to K^m$ tal que as suas coordenadas sejam $(\gamma(\tilde{y}_1), \ldots, \gamma(\tilde{y}_m))$. Verifiquemos a inclusão $\varphi(X) \subseteq Y$. Se $f \in \mathcal{I}(Y)$, temos $f(\varphi(x)) = f((\gamma \circ \tilde{y}_1)(x), \ldots, (\gamma \circ \tilde{y}_m)(x))$. Pela Equação (3.1), temos:

$$f(\varphi(x)) = (\gamma \circ f)(x).$$

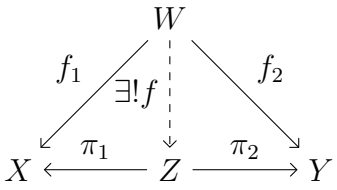
Como em $K[Y]$, f é o polinômio nulo e como γ é um homomorfismo, ele deve levar f também no polinômio nulo. Logo $f(\varphi(x)) = 0$. Assim, temos $\varphi(X) \subseteq Y$. Falta verificar que φ é um morfismo. Note que as funções coordenadas de φ são polinômios de $K[X]$ e, pela Proposição 3.8, φ é um morfismo de variedades afins. Pelo que foi exposto, fica claro que φ deve induzir o homomorfismo de álgebras γ, basta observar que o homomorfismo que leva $f \in K[Y]$ em $f \circ \varphi$ coincide com γ nos polinômios $\tilde{y}_i$.

Finalmente, note que φ deve ser o único morfismo que induz γ. De fato, se existir um outro morfismo ψ que induza γ, eles devem coincidir em suas funções coordenadas, pois caso contrário, φ^* e ψ^* não iriam coincidir nos polinômios $\tilde{y}_i$. Assim, $\varphi = \psi$.

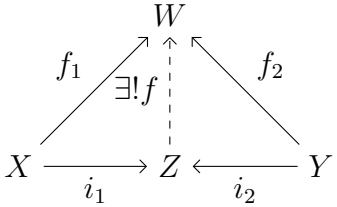
□

Se X e Y são variedades afins, podemos formar o produto $X \times Y$. O problema é que, quando falamos do "produto", estamos nos referindo ao *objeto* produto na categoria correspondente e é necessário mostrar que o objeto existe e pode ser identificado com o produto cartesiano. Esse fato é verdadeiro, porém a álgebra afim correspondente não é o produto cartesiano, mas sim o *produto tensorial* $K[X] \otimes K[Y]$. Antes de prosseguir, vamos relembrar a definição de produto e coproduto em uma categoria.

Definição 3.10. Se X e Y são objetos de uma mesma categoria, Z é chamado de *produto* entre X e Y se existem morfismos $\pi_1 : Z \to X$ e $\pi_2 : Z \to Y$ tais que, para quaisquer objeto W e pares de morfismos $f_1 : W \to X$ e $f_2 : W \to Y$, existe um único morfismo $f : W \to Z$, que faz o diagrama abaixo comutar.



Definição 3.11. Se X e Y são objetos de uma mesma categoria, Z é chamado de *coproduto* entre X e Y se existem morfismos $i_1 : X \to Z$ e $i_2 : Y \to Z$ tais que para quaisquer objeto W e pares de morfismos $f_1 : X \to W$ e $f_2 : Y \to W$, existe um único morfismo $f : Z \to W$, que faz o diagrama abaixo comutar.



As projeções canônicas π_1 e π_2 que levam $(x, y) \in X \times Y$ em x e em y, respectivamente, são morfismos de variedades afins e elas podem ser usadas para mostrar que o produto de variedades afins existe e pode ser identificado com o produto cartesiano.

Pelo fato de existir um functor contravariante da categoria $\mathcal{C}_1$ das K-variedades afins para a categoria $\mathcal{C}_2$ das K-álgebras afins, um objeto produto em $\mathcal{C}_1$ é levado num objeto que atende os requisitos para ser um *coproduto* em $\mathcal{C}_2$. Em $\mathcal{C}_2$, o coproduto de duas álgebras afins é o produto tensorial, portanto, temos $K[X \times Y] \cong K[X] \otimes K[Y]$. Uma observação importante é que a topologia em $X \times Y$ não é a topologia produto, mas sim a topologia de Zariski.

3.1.2 Alguns conceitos topológicos

Um espaço topológico X é dito *conexo* se não admite uma cisão não-trivial, isto é, se A e B são fechados em X com $A \cup B = X$ e $A \cap B = \emptyset$, então $A = X$ ou $B = X$. Quando X está equipado com a topologia de Zariski, o conceito de *irredutibilidade* também é relevante.

Definição 3.12. Um espaço topológico X é dito *irredutível* se X não é a união de dois subconjuntos fechados e próprios de X.

Assim, um espaço irredutível é sempre conexo, mas a recíproca não é verdadeira. Note que um espaço topológico que é Hausdorff e irredutível, se reduz a um único ponto. Dessa forma, o conceito de irredutibilidade não é particularmente útil nesses casos.

Proposição 3.13. (*i*) *O conjunto K^n é irredutível.*

(*ii*) *Se X é uma variedade afim irredutível, então todo subconjunto aberto de X também é irredutível.*

Demonstração. (*i*) Suponha $K^n = \mathcal{V}(I) \cup \mathcal{V}(J)$. Temos $\mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(I \cap J)$. Isso implica $I \cap J = \emptyset$. Quando I e J não são ideais vazios, temos $IJ \subseteq I \cap J$ e IJ certamente não é vazio. Assim para $I \cap J = \emptyset$, devemos ter $I = \emptyset$ ou $J = \emptyset$ e $\mathcal{V}(I) = K^n$ ou $\mathcal{V}(J) = K^n$.

(*ii*) Sejam A um subconjunto aberto de X e B, C subconjuntos fechados de X tais que $A = (B \cap A) \cup (C \cap A)$. Assim $B \cup C \subsetneq X$. Podemos escrever $X = (B \cup C) \cup A^C$. Como X é irredutível, devemos ter $B \cup C = X$ ou $A^C = X$. O segundo caso implica $A = \emptyset$, que é irredutível. O primeiro caso implica $B = X$ ou $C = X$ e temos $B \cap A = A$ ou $C \cap A = A$. Assim, A é irredutível também. □

Proposição 3.14. *Sejam X um espaço topológico e A um subconjunto de X então:*

(*i*) *A é irredutível se, e somente se, o fecho de A, denotado por $\overline{A}$, é irredutível.*

(*ii*) *Se $\varphi : X \to Y$ é uma função contínua e A é irredutível, então $\varphi(A)$ também é irredutível.*

(*iii*) *Se X é um conjunto algébrico, então X é irredutível se, e somente se, $K[X]$ é um domínio de integridade.*

(*iv*) *Se X e Y são conjuntos algébricos irredutíveis, então $X \times Y$ é irredutível.*

Demonstração. (*i*) Suponha A irredutível. Se $\overline{A}$ não for irredutível, podemos escrever $\overline{A} = B \cup C$, com B e C fechados em X, $B \subsetneq \overline{A}$ e $C \subsetneq \overline{A}$. Daí $A = (B \cap A) \cup (C \cap A)$. Como A é irredutível, isso implica $B \cap A = A$ ou $C \cap A = A$. Se ocorrer $B \cap A = A$,

então $A \subseteq B$ e, como B é fechado, temos $\overline{A} \subseteq B$. Isso é uma contradição com $B \subsetneq \overline{A}$. Portanto, devemos ter $C \cap A = A$, que leva a uma contradição análoga. Assim, $\overline{A}$ deve ser irredutível.

Agora, suponha que $\overline{A}$ seja irredutível. Se A não for irredutível, podemos escrever $A = (B \cap A) \cup (C \cap A)$, onde B e C são fechados de X, $B \cap A \subsetneq A$ e $C \cap A \subsetneq A$. Isso significa $A \subseteq B \cup C$ e, assim, $\overline{A} \subseteq B \cup C$, pois B e C são fechados. Logo $B = \overline{A}$ ou $C = \overline{A}$. Se $B = \overline{A}$, então $B \cap A = A$, que é uma contradição. Se $C = \overline{A}$ também temos uma contradição.

(*ii*) Suponha $\varphi(A) = (B \cap \varphi(A)) \cup (C \cap \varphi(A))$, com B e C fechados de Y. Como φ é uma aplicação contínua, $\varphi^{-1}(B)$ e $\varphi^{-1}(C)$ são fechados de X. Além disso, temos $A = (\varphi^{-1}(B) \cap A) \cup (\varphi^{-1}(C) \cap A)$. Como A é irredutível, isso implica $\varphi^{-1}(B) \cap A = A$ ou $\varphi^{-1}(C) \cap A = A$. No primeiro caso, temos $\varphi(A) \subseteq B$ e $B \cap \varphi(A) = A$. No segundo caso, de modo análogo, temos $C \cap \varphi(A) = A$. Portanto, $\varphi(A)$ deve ser irredutível.

(*iii*) Veja [25, Prop 2.19].

(*iv*) Pelo item (*iii*), como X e Y são irredutíveis, então $K[X]$ e $K[Y]$ são domínios de integridade. Assim, se $K[X \times Y] \cong K[X] \otimes K[Y]$ for domínio de integridade, então $X \times Y$ será irredutível. A verificação de que $K[X] \otimes K[Y]$ é domínio de integridade pode ser vista em [25, Prop 4.15(b)]. □

Em um espaço topológico podemos falar das *componentes conexas* dele, que são os subespaços maximais em relação à propriedade de ser conexo. De modo análogo, podemos discutir as *componentes irredutíveis* de um espaço topológico. Em geral, as duas coisas são distintas e uma componente conexa pode conter várias componentes irredutíveis.

Proposição 3.15. *Seja X um conjunto algébrico, então X é uma união finita de componentes irredutíveis únicas.*

Demonstração. A Proposição 2.17 de [25] estabelece X como um espaço topológico noetheriano. Já a Proposição 2.21 de [25] mostra que todo espaço topológico noetheriano é uma união finita de subconjunto irredutíveis $X_1 \cup \ldots \cup X_m$. Quando os X_i são tomados sem inclusões entre eles, obtemos as componentes irredutíveis e elas são únicas a menos da ordem em que elas aparecem na união. □

3.1.3 Dimensão

Precisamos primeiro relembrar algumas definições sobre extensões transcendentes. Mais detalhes podem ser vistos em [26, Capítulo 8]. Lembramos que se K é um corpo e L é um subcorpo de K, um subconjunto finito $A = \{\alpha_1, \ldots \alpha_n\} \subseteq K$ é dito *algebricamente independente sobre* L, se o núcleo do homomorfismo $\varphi : L[T_1, \ldots, T_n] \to K$ que leva $f \in L[T_1, \ldots, T_n]$ em $f(\alpha_1, \ldots, \alpha_n)$ é $\{0\}$. Isto é, A não satisfaz nenhum polinômio não trivial de $|A|$ variáveis sobre L. Se A for infinito, dizemos que A é *algebricamente independente sobre* L se qualquer subconjunto finito de A for algebricamente independente sobre L. Uma *base de transcendência* de K sobre L é um conjunto A algebricamente independente sobre L tal que K é uma extensão algébrica sobre $L(A)$. Nesse caso, $L(A)$ denota o corpo de frações do domínio de integridade obtido ao adicionar os elementos de A ao corpo L. Finalmente, o *grau de transcendência* de K sobre L é a cardinalidade de uma base de transcendência de K sobre L. Com isso, estamos em condições de definir dimensão.

Definição 3.16. Seja X uma variedade afim irredutível. Neste caso, $K[X]$ é um domínio de integridade e podemos considerar o seu corpo de frações $K(X)$. Definimos a *dimensão* de X como sendo o grau de transcendência de $K(X)$ em relação a K. Se X não for irredutível, definimos a *dimensão* de X como sendo o máximo entre as dimensões de suas componentes irredutíveis.

Proposição 3.17. *Seja X um variedade afim irredutível e Y é um subconjunto fechado e próprio de X, então* $\dim Y < \dim X$.

Demonstração. Veja [25, Proposição 2.26]. □

Agora precisamos de um resultado técnico sobre morfismos de variedades afins. Se $\varphi : X \to Y$ é um morfismo de variedades afins, as *fibras* de φ são as imagens inversas de elementos de Y, isto é, são conjuntos da forma $\varphi^{-1}(y)$, para $y \in Y$. Dizemos que $\varphi : X \to Y$ é um morfismo *dominante* se $\varphi(X)$ é denso em Y. Muitas vezes, não traz prejuízos substituir Y por $\overline{\varphi(X)}$. Assim, essa não é uma hipótese muito restritiva sobre um morfismo. O próximo resultado nos dá informações sobre a dimensão das fibras de um morfismo dominante.

Proposição 3.18. *Seja $\varphi : X \to Y$ um morfismo dominante entre variedades afins irredutíveis, então:*

(*i*) $\dim X \geq \dim Y$

(*ii*) *Para $y \in \varphi(X)$, temos* $\dim \varphi^{-1}(y) \geq \dim X - \dim Y$

Demonstração. Veja [25, Teorema 10.9] □

3.2 Grupos Lineares Algébricos

Um grupo linear algébrico é uma K-variedade afim em que as operações de grupo são compatíveis com a estrutura de variedade afim. Mais explicitamente, temos:

Definição 3.19. Seja G um grupo, que é também uma variedade afim. Dizemos que G é um *grupo linear algébrico*, se:

- A operação do grupo $* : G \times G \to G$ é um morfismo de K-variedades afins e
- A inversão $i : G \to G$ é um isomorfismo de K-variedades afins.

Existem homomorfismos de grupos que não são morfismos de variedades afins e vice-versa. Nesse contexto, dizemos que $\varphi : G_1 \to G_2$ é um *homomorfismo de grupos lineares algébricos* se φ é um morfismo de variedades afins e um homomorfismo de grupos.

Exemplos de grupos lineares são $GL_n(K)$, $SL_n(K)$, os grupo simpléticos, os grupos ortogonais e vários outros.

Para mostrar que $SL_n(K)$ é uma variedade afim considere o espaço vetorial $V = K^{n^2}$, em que os pontos de V são as matrizes $n \times n$. A função que leva uma matriz no seu determinante é uma função polinomial em n^2 variáveis. Assim, $SL_n(K) = \{v \in V \mid \det(v) - 1 = 0\}$ e, portanto, $SL_n(K)$ é fechado em V e isso mostra que $SL_n(K)$ é uma variedade afim.

Note que em V, $GL_n(K)$ não é um fechado e sim um conjunto aberto pois é o complementar do conjunto $\{v \in V \mid \det(v) = 0\}$. Para enxergar $GL_n(K)$ como variedade afim, precisamos considerar o espaço $W = V \times K$, assim $GL_n(K)$ é o conjunto $\{(v, \lambda) \in V \times K \mid \lambda\det(v) - 1 = 0\}$. Como a função que leva (v, λ) em $\lambda\det(v) - 1$ é uma expressão polinomial em $n^2 + 1$ variáveis, isso mostra que $GL_n(K)$ pode ser visto como uma variedade afim. Naturalmente, $SL_n(K)$ continua sendo variedade afim nessa situação, pois é a interseção de $GL_n(K)$ com os zeros do polinômio $T_{n^2+1} - 1$.

Falta ainda mostrar que as operações do grupo são morfismos de variedades afins. Para ver isso, basta considerar as matrizes como pontos de um espaço de $n^2 + 1$, a operação $*$ leva $(((a_{ij}), \lambda_1), ((b_{ij}), \lambda_2)) \in G \times G$ em $((c_{ij}), \lambda_1\lambda_2)$, onde (c_{ij}) é produto matricial entre (a_{ij}) e (b_{ij}). Dessa forma, como $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$, observa-se que as funções coordenadas de $*$ são expressões em $(n^2+1)\times(n^2+1)$ variáveis e, portanto, polinômios de $K[G]\otimes K[G]$. Assim, $*$ é um morfismo de variedades afins. Mostrar que a inversão de matrizes é um isomorfismo é feito de forma análoga. Também consiste em observar que cada elemento da matriz invertida é uma expressão polinomial em $n^2 + 1$ variáveis dos elementos da matriz original.

Vimos que, em geral, irredutibilidade e conexidade são conceitos diferentes para variedades afins. Porém, em se tratando de grupos lineares algébricos os dois conceitos coincidem.

Proposição 3.20. *Seja G um grupo linear algébrico. As componentes conexas e irredutíveis de G coincidem. Em particular, a componente conexa que contém a identidade, denotada por G^0, é um subgrupo fechado, normal e de índice finito.*

Demonstração. Suponha que X e Y sejam duas componentes irredutíveis que contenham a identidade. Pela Proposição 3.14, $X \times Y$ também é irredutível e como a operação do grupo é uma aplicação contínua, XY também é irredutível. Como X e Y ambos contêm a identidade, temos $X \subseteq XY$ e $Y \subseteq XY$. Como são ambos maximais, isso implica $XY = X = Y$.

Assim, há uma única componente irredutível que contém a identidade. Verifiquemos agora que G^0 é um subgrupo fechado. Os conjuntos $(G^0)^{-1}$ e G^0G^0 são componentes irredutíveis que contêm a identidade, então $(G^0)^{-1} = G^0$ e $G^0G^0 = G^0$. Note que G^0, sendo um componente irredutível, tem que ser fechado, pois caso contrário $\overline{G^0}$ seria um conjunto irredutível contendo propriamente G^0.

Vamos mostrar que G^0 é normal. Se $g \in G$, a função que leva x em gxg^{-1} é um automorfismo de grupos algébricos. Em particular, é um homeomorfismo de variedades afins e leva componentes conexas em componentes conexas. Assim, gG^0g^{-1} é uma outra componente conexa que contém a identidade. Portanto, devemos ter $gG^0g^{-1} = G^0$, para todo $g \in G$ e G^0 é normal.

Como G^0 é um subgrupo de G, podemos escrever $G = \cup_{g\in G} gG^0$. A função que leva $x \in G$ em gx é um homeomorfismo, então as classes laterais gG^0 devem ser componentes irredutíveis. Pela Proposição 3.15, G tem um número finito de componentes irredutíveis. Dessa forma, cada componente irredutível deve ser uma classe lateral. Além disso, como as componentes irredutíveis são todas disjuntas, elas devem ser as componentes conexas de G.

□

Assim, um grupo linear algébrico é conexo se, e somente se, $G = G^0$. Note que G^0 é "quase" um subgrupo característico. Se φ é um automorfismo de G que também é um morfismo de variedades afins, então $\varphi(G^0) = G^0$.

Com auxílio das Proposições 3.13 e 3.13 podemos verificar a conexidade de alguns grupos. Por exemplo, $GL_n(K)$ é conexo, pois é um aberto em K^{n^2}. O grupo aditivo do corpo K também é um grupo linear algébrico conexo, que denotaremos por G_a. O grupo multiplicativo de K, denotado por G_m, é isomorfo a $GL_1(K)$ e, portanto, é conexo. Denotaremos por D_n o subgrupo de GL_n formado pelas matrizes diagonais, como D_n é isomorfo ao produto cartesiano de n cópias de G_m, então D_n é conexo.

Proposição 3.21. *Sejam G um grupo linear algébrico e $(X_i, \varphi_i)_{i\in I}$ uma família de variedades afins irredutíveis tais que cada $\varphi_i : X_i \to G$ seja um morfismo de variedades afins e $G_i = \varphi(X_i)$ contenha a identidade. Nessas condições, o grupo $H = \langle G_i \mid i \in I\rangle$ gerado pelos G_i é fechado e conexo. Além disso, existem $n \in \mathbb{N}$ e $(i_1, \ldots, i_n) \in I^n$ tais que $H = G_{i_1}^{\pm 1} \ldots G_{i_n}^{\pm 1}$*

Demonstração. [33, Proposição 2.2.6]. □

Em um grupo linear algébrico, a noção de conexidade coincide com a de irredutibilidade. Assim, a Proposição 3.21 implica que um subgrupo gerado por outros subgrupos fechados e conexos também é fechado e conexo.

Proposição 3.22. *Se G é um grupo linear algébrico e $H, K \leq G$ são subgrupos fechados tais que pelo menos um deles é conexo, então $[H, K]$ é fechado e conexo.*

Demonstração. Se H é conexo, então também é irredutível. Considere a família de morfismos $\varphi_k : H \to G$, com $k \in K$, tais que $\varphi_k(h) = hkh^{-1}k^{-1}$. Cada $\varphi_k(H)$ contém a identidade e podemos utilizar a Proposição 3.21 para concluir que $\langle \varphi_k(H) \mid k \in K\rangle$ é conexo e fechado, mas esse grupo é precisamente $[H, K]$.

Se K fosse conexo, poderíamos considerar $\varphi_h : K \to G$ tal que $\varphi_h(k) = hkh^{-1}k^{-1}$ e o argumento seria análogo. □

Com auxílio das duas proposição anteriores é possível mostrar a conexidade de mais alguns grupos. O grupo $SL_n(K)$ é conexo, pois é $[GL_n(K), GL_n(K)]$. Outra forma de verificar isso é considerar os subgrupos $X_{ij} = \{X_{ij}(\alpha) \mid \alpha \in K\}$, com $i \neq j$. Um elemento $X_{ij}(\alpha) \in X_{ij}$ é uma tranvecção, que é uma matriz que difere da identidade apenas pelo fato da posição (i, j) ser α. Já utilizamos transvecções previamente na construção do par-BN de $GL_n(q)$, veja a Seção 2.3.1.

Temos $X_{ij}(\alpha)X_{ij}(\beta) = X_{ij}(\alpha + \beta)$, assim o homomorfismo que leva $X_{ij}(\alpha)$ em α estabelece um isomorfismo entre X_{ij} e G_a. Logo todos os subgrupos da forma X_{ij} são conexos. Pode-se mostrar que $SL_n(K)$ é gerado por todas as transvecções, assim usando a Proposição 3.21, $SL_n(K)$ é conexo.

Considere agora o grupo U_n das matrizes triangulares superiores em que os elementos da diagonal são todos 1. Certamente, U_n contém todas os subgrupos X_{ij} com $i < j$. Dado $u \in U_n$, suponha que o elemento da posição $(1, 2)$ seja $\alpha \neq 0$, então podemos multiplicar u à esquerda pela transvecção $X_{12}(\alpha^{-1})$ para zerar essa posição. Se na terceira coluna tiver um elemento não nulo que não esteja na diagonal, multiplicar à esquerda por transvecções $X_{23}(\beta_1^{-1})$ e $X_{13}(\beta_2^{-1})$ é o suficiente para zerar essas posições. Proseguindo dessa forma, podemos escrever $Mu = 1$, onde M é um produto de transvecções com $i < j$. Daí

$u = M^{-1}$ e, portanto, é um produto de transvecções. Assim, U_n também é um subgrupo fechado conexo. Com um pouco mais de trabalho, pode-se mostrar que U_n é um subgrupo nilpotente.

Com isso, podemos mostrar que o grupo T_n das matrizes triangulares superiores também é fechado e conexo, basta observar que $U_n \leq T_n$, $D_n \leq T_n$ e que T_n é gerado por U_n e D_n. Além disso, podemos mostrar que T_n é solúvel. Observe que $[T_n, T_n] \subseteq U_n$, pois se $t, v \in T_n$, então diagonal de tv é da forma $(t_{11}v_{11}, \dots t_{nn}v_{nn})$. Assim, a diagonal de $tvt^{-1}v^{-1}$ é da forma $(1, \dots, 1)$. Por outro lado, dado o subgrupo X_{ij} com $i < j$, temos $X_{ij} = [D_n, X_{ij}]$ e, como $[D_n, X_{ij}] \subseteq [T_n, T_n]$, segue que $[T_n, T_n]$ contém cada X_{ij} com $i < j$. Já observamos que os X_{ij} com $i < j$ são suficientes para gerar U_n, assim $[T_n, T_n] = U_n$. Isso mostra que a série derivada de T_n desce até $\{1\}$ pois U_n é nilpotente e, em particular, é solúvel.

Os exemplos vistos até agora são todos de grupos de matrizes. Em verdade, os grupos lineares algébricos sempre podem ser vistos como grupos de matrizes.

Proposição 3.23. *Se G é um grupo linear algébrico sobre K, então existe um isomorfismo de grupos algébricos ρ entre G e algum subgrupo fechado de $GL_n(K)$.*

Demonstração. Veja [16, Seção 8.6]. □

3.3 Ações sobre variedades

Seja G um grupo linear algébrico e X uma variedade afim, ambos sobre o mesmo corpo K. Dizemos que G *age morficamente* sobre X se G age sobre X como grupo abstrato e a função $\varphi : G \times X \to X$ que leva (g, x) em $g.x$ é um morfismo de variedades afins.

A ação de G sobre si mesmo que leva $(g, x) \in G \times G$ em gx é um exemplo de ação mórfica. Outro exemplo é a ação por conjugação que leva (g, x) em gxg^{-1}.

Proposição 3.24. *Se G age morficamente sobre uma variedade afim $X \neq \emptyset$, então:*

(i) Para cada $x \in X$, a função $\varphi_x(g) = g.x$ é um morfismo de variedades afins.

(ii) Toda órbita $\mathcal{O}(x)$ é aberta no seu fecho.

(iii) Existem órbitas fechadas.

Demonstração. (i) Considere a função φ que leva (g, x) em $g.x$. Por hipótese, φ é um morfismo. Considere também a imersão $i_x : G \to G \times X$ que leva g em (g, x). As funções coordenadas dessa função são claramente polinomias, assim i_x é um morfismo. Assim, $\varphi_x = \varphi \circ i_x$, portanto φ_x é, de fato, um morfismo.

(ii) Para mostrar esse item, precisamos de um resultado da Geometria Algébrica. Se $\varphi : X \to Y$ é um morfismo de variedades afins, então $\varphi(X)$ contém um subconjunto aberto não vazio do seu fecho $\overline{\varphi(X)}$, veja [25, Teorema 10.2].

Munido desse fato, temos $\varphi_x(G) = \mathcal{O}(x)$ e existe $Y \subseteq \mathcal{O}(x)$ tal que Y é aberto em $\overline{\mathcal{O}(x)}$. Agora, para cada $g \in G$, a função $\psi_g : X \to X$ que leva x em $g.x$ é um isomorfismo de variedades afins. Logo $\psi_g(Y)$ também é um subconjunto aberto de $\overline{\mathcal{O}(x)}$. Como G age transitivamente sobre a órbita $\mathcal{O}(x)$, temos $\mathcal{O}(x) = \cup_{g \in G} \psi_g(Y)$. Assim, $\mathcal{O}(x)$ também é um subconjunto aberto.

(*iii*) Primeiro, vamos observar que $\overline{\mathcal{O}(x)}$ é uma união de órbitas. Para isso, é suficiente mostrar que $g.\overline{\mathcal{O}(x)} = \overline{\mathcal{O}(x)}$, para todo $g \in G$. Agora, dado $g \in G$, temos que $g.\overline{\mathcal{O}(x)}$ é um subconjunto fechado de X que contém $\mathcal{O}(x)$, como $\overline{\mathcal{O}(x)}$ é o conjunto minimal com essa propriedade, temos $\overline{\mathcal{O}(x)} \subseteq g.\overline{\mathcal{O}(x)}$. Da mesma forma, temos $\overline{\mathcal{O}(x)} \subseteq g^{-1}.\overline{\mathcal{O}(x)}$, mas isso implica $gg^{-1}.\overline{\mathcal{O}(x)} \subseteq \overline{\mathcal{O}(x)}$. Daí $g.\overline{\mathcal{O}(x)} = \overline{\mathcal{O}(x)}$.

Suponha que não existam órbitas fechadas. Tome $X_1 = \overline{\mathcal{O}(x_1)}$, para $x_1 \in X$. Agora, $\overline{\mathcal{O}(x_1)} \setminus \mathcal{O}(x_1)$ é um conjunto fechado que também é uma união de órbitas. Por não existirem órbitas fechadas, podemos tomar $X_2 = \overline{\mathcal{O}(x_2)}$, tal que $\mathcal{O}(x_2) \subseteq \overline{\mathcal{O}(x_1)} \setminus \mathcal{O}(x_1)$. Por construção, temos $X_1 \supsetneq X_2$. Novamente, como não há órbitas fechadas, podemos escolher uma órbita $\mathcal{O}(x_3)$ que está na fronteira de $\mathcal{O}(x_2)$ para construir $X_3 = \overline{\mathcal{O}(x_3)}$. Assim, a sequência $X_1 \supsetneq X_2 \supsetneq X_3 \supsetneq \dots$ viola o fato de X ser um espaço topológico Noetheriano (veja [25, Proposição 2.17]). Portanto, devem existir órbitas fechadas. □

Se G age morficamente sobre X e $Y, Z \subseteq X$ são subconjuntos de X, definimos o *transporte* de Y em Z como sendo $Trans_G(Y, Z) = \{g \in G \mid g.Y \subseteq Z\}$.

Proposição 3.25. *Se G age morficamente sobre X, então:*

(*i*) *Se $Y, Z \subseteq X$ são tais que Z é um subconjunto fechado de X, então $Trans_G(Y, Z)$ é fechado em G.*

(*ii*) *Para $x \in X$, o estabalizador $G_x = \{g \in G \mid g.x = x\}$ é fechado.*

Demonstração. (*i*) Pela Proposição 3.24, para cada $y \in Y$, a função $\varphi_y : G \to X$, que leva g em $g.y$ é um morfismo. Assim $\varphi_y^{-1}(Z)$ é um subconjunto fechado de G. Agora, $Trans_G(Y, Z) = \bigcap_{y \in Y} \varphi_y^{-1}(Z)$, e assim $Trans_G(Y, Z)$ também é fechado.

(*ii*) Para $x \in X$, considere a função φ_x, que leva g em $g.x$. Novamente, tal função é um morfismo. Além disso, $G_x = \varphi_x^{-1}(\{x\})$. Portanto, G_x é um subconjunto fechado.

□

Proposição 3.26. *Se G é um grupo linear algébrico, então:*

(*i*) *Para $g \in G$, $C_G(g)$ é um subgrupo fechado.*

(*ii*) *O centro $Z(G)$ de G é um subgrupo fechado.*

(*iii*) *Se H é um subgrupo fechado de G, então $N_G(H)$ é um subgrupo fechado de G.*

Demonstração. (*i*) O grupo G age morficamente sobre si mesmo por conjugação. Pela Proposição 3.25, os estabalizadores são fechados. Assim, para $g \in G$, temos $G_g = C_G(g)$, que é um subgrupo fechado.

(*ii*) Basta observar a igualdade $Z(G) = \bigcap_{g \in G} C_G(g)$.

(*iii*) Consideramos novamente a ação por conjugação de G sobre si mesmo. Temos $N_G(H) = Trans_G(H, H)$, como H é fechado, segue que $N_G(H)$ é fechado, pela Proposição 3.25. □

3.4 A decomposição de Jordan

Primeiro, algumas definições.

Definição 3.27. Seja $a \in End(V)$, onde V é um espaço vetorial de dimensão finita sobre K. Dizemos que a é *nilpotente* se existe m tal que $a^m = 0$, *semisimples* se a for diagonalizável e *unipotente* se $a - 1$ for nilpotente.

Um resultado de Álgebra Linear diz que dado $a \in End(V)$, podemos escrever a de forma única como $s + n$, em que s é um endomorfismo semisimples, n é nilpotente e $sn = ns$. Essa é chamada de *Decomposição Aditiva de Jordan*. Quando $g \in GL(V)$, temos também o seguinte resultado:

Proposição 3.28 (Decomposição Multiplicativa de Jordan)**.** *Dado $g \in GL(V)$, podemos escrever g de forma única como $g_s g_u = g_u g_s$, onde g_s é semisimples e g_u é unipotente.*

Demonstração. [33, Proposição 2.4.4 e Corolário 2.4.5]. □

Pela Proposição 3.23 se G é um grupo linear algébrico qualquer, existe um isomorfismo φ de grupos algébricos entre G e um subgrupo fechado de algum $GL_n(K)$. Dessa forma, dado $g \in G$, podemos aplicar o resultado anterior para escrever g como $g_s g_u$ em $GL_n(K)$. Essa é uma forma intuitiva de ver o que acontece. Na verdade, estamos considerando a decomposição $\varphi(g) = \varphi(g)_s \varphi(g)_u$ e não é evidente que existam $g_s, g_u \in G$ tais que $g = g_s g_u$ e $\varphi(g_s) = \varphi(g)_s$ e $\varphi(g_u) = \varphi(g)_u$.

Proposição 3.29. *Seja G um grupo linear algébrico. Então:*

(*i*) *Para cada imersão φ de G em algum $GL(V)$ e, para cada $g \in G$, existem únicos $g_s, g_u \in G$ tais que $g = g_s g_u = g_u g_s$, $\varphi(g_s)$ é semisimples e $\varphi(g_u)$ é unipotente.*

(*ii*) *A decomposição $g = g_s g_u = g_u g_s$ não depende de φ.*

(*iii*) *Se $\varphi : G_1 \to G_2$ é um homomorfismo de grupos algébricos, então $\varphi(g_s) = \varphi(g)_s$ e $\varphi(g_u) = \varphi(g)_u$.*

Demonstração. Veja [24, Teorema 2.5], [16, Seção 15.3], [33, Teorema 2.4.8] ou [4, Capítulo 1, §4]. □

Se a característica de K for $p > 0$, podemos mostrar que a é unipotente se, e somente se, a tem ordem potência de p. Com efeito, se $a - 1 = n$, onde n é nilpotente, temos $n^{p^k} = 0$, para k suficientemente grande. Portanto, $a^{p^k} = (1 + n)^{p^k} = 1 + n^{p^k} = 1$. Por outro lado, se a tiver ordem p^m, $(a - 1)^{p^m} = a^{p^m} - 1 = 0$.

Nas mesmas condições, podemos mostrar que a é semisimples se, e somente se, a ordem de a é coprima com p. Se a é semisimples, existe $x \in GL(V)$ tal que xax^{-1} é uma matriz diagonal. Como K é algebricamente fechado, podemos escrever $K = \bigcup_{n>0} \mathbb{F}_{p^n}$. Assim, podemos considerar que os autovalores da matriz a estão todos em um mesmo corpo finito $\mathbb{F}_{p^m}$. Assim se λ é um autovalor de a, então $\lambda^{p^m} = \lambda$. Isso implica $(xax^{-1})^{p^m} = xax^{-1}$ e $a^{p^m} = a$. Em particular, a ordem de a é coprima com p. Utilizando a decomposição de Jordan, podemos mostrar a recíproca. Escrevendo $a = g_s g_u$, como a ordem de g_s e de g_u são coprimas e os dois elementos comutam, a ordem de a é o produto das ordens de g_s e

g_u. Se a ordem a for coprima com p, como a ordem de g_u é um potência de p devemos ter $g_u = 1$ e $a = g_s$, portanto a é semisimples.

Dessa forma, podemos olhar a decomposição de Jordan como uma versão especializada do seguinte resultado:

Proposição 3.30. *Seja G um grupo e $g \in G$ um elemento de ordem finita. Para todo primo p existem únicos $x, y \in G$ tais que $g = xy = yx$, a ordem de x é um potência de p e a ordem de y é coprima com p. Além disso $x, y \in \langle g \rangle$.*

Demonstração. Veja [20][Lema 8.18]. □

No caso de G ser um grupo linear algébrico sobre um corpo de característica prima, fica claro que g_s e g_u fazem o papel do x e y da Proposição 3.30. Escrevemos G_s e G_u para denotar os subconjuntos de G que contém os elementos semisimples e unipotentes, respectivamente. Note que, em geral, G_u e G_s não são subgrupos de G. Se $G = G_u$, dizemos que G é um grupo *unipotente*, porém um grupo com $G = G_s$ *não* é chamado de semisimples. Esse nome é reservado para um outro conceito que veremos adiante. Se G for um grupo linear algébrico abeliano, pode-se mostrar que G_s e G_u são subgrupos fechados e que G é isomorfo ao produto cartesiano $G_s \times G_u$ [16, Seção 15.5].

Um exemplo de grupo unipotente é U_n e um exemplo de grupo tal que $G = G_s$ é D_n. Na verdade, pode-se mostrar que todo grupo unipotente é isomorfo a um subgrupo de U_n [24, Proposição 2.9].

3.5 Subgrupos importantes

Dizemos que G é um *toro* se G é isomorfo ao produto direto de um número finito de cópias de G_m. O subgrupo das matrizes diagonais D_n é um exemplo de toro. Antes de prosseguir, precisamos de um lema técnico.

Lema 3.31. *Seja $\varphi : V \times G \to H$ um morfismo de variedades afins satisfazendo as seguintes hipóteses:*

(*i*) *G é um grupo linear algébrico em que o subconjunto dos elementos de ordem finita formam um conjunto denso.*

(*ii*) *H é um grupo linear algébrico tal que, para cada $m > 0$, existe um número finito de elementos de ordem m.*

(*iii*) *V é uma variedade afim conexa.*

(*iv*) *Para cada $v \in V$, o morfismo $\varphi_v : G \to H$ dado por $\varphi_v(g) = \varphi(v, g)$ é um homomorfismo de grupos algébricos.*

Então a função que leva v em φ_v é constante, isto é, φ não depende de V.

Demonstração. Denotaremos o subconjunto dos elementos de ordem finita de G por G_T. Para $g \in G$, considere o morfismo $\psi_g : V \to H$ tal que $\psi_g(v) = \varphi(v, g)$. Observe que como φ_v é um homomorfismo, temos $\varphi(v, g^m) = \varphi(v, g)^m$ e $\varphi(v, 1) = 1$. Assim, se $g \in G_T$ tiver ordem finita m, temos $\psi_g(v)^m = \varphi(v, g)^m$ e $\psi_g(v)^m = 1$. Portanto, $\psi_g(v)$ tem ordem finita.

Pela hipótese (ii), $\psi_g(V)$ é um conjunto finito. Além disso, por V ser conexo, $\psi_g(V)$ é conexo, então $\psi_g(V)$ se reduz a um único ponto, isto é, $\varphi(v,g) = \varphi(v',g)$, para todo $v, v' \in V$ e para cada $g \in G$ com ordem finita.

Pela hipótese (i), dados $v, v' \in V$, φ_v e $\varphi_{v'}$ são iguais em um subconjunto denso de G. Em um espaço topológico que é Hausdorff, isso seria suficiente para garantir $\varphi_v = \varphi_{v'}$, mas não é o caso aqui. De toda forma, podemos mostrar que isso é verdade usando o fato de que a diagonal $\Delta_H = \{(h,h) \mid h \in H\}$ é um subconjunto fechado de $H \times H$. Vamos assumir isso por enquanto. Considere a função $f : G \times H \to H$ que leva g em $(\varphi_v(h), \varphi_{v'}(h))$. Como cada função coordenada é contínua, então f é contínua. Assim, $f^{-1}(\Delta_H)$ é um subconjunto fechado de G que contém G_T. Como G_T é denso, segue $f^{-1}(\Delta_H) = G$ e $\varphi_v = \varphi_{v'}$. Em particular, a função que leva v em φ_v é constante.

Para mostrar que Δ_H é fechado, considere o ideal I em $K[X] \otimes K[X]$ gerado por $\{1 \otimes f - f \otimes 1 \mid f \in K[X]\}$. Temos $\Delta_H \subseteq \mathcal{V}(I)$. Agora, temos $(u,v) \in \mathcal{V}(I)$ se e somente $1 \otimes f(v) - f(u) \otimes 1 = 0$, isto é, se $f(v) = f(u)$ para todo $f \in K[X]$. Para cada coordenada i, considere o polinômio que leva $x \in X$ em x_i, assim para $(u,v) \in \mathcal{V}(I)$ temos $v_i = u_i$, para todo i. Portanto, $u = v$. Logo $\mathcal{V}(I) = \Delta_H$ e Δ_H é fechado. □

Com isso, pode-se mostrar o seguinte resultado:

Proposição 3.32. *Seja T um toro de um grupo linear algébrico G, então $N_G(T)^0 = C_G(T)^0$. Em particular, o índice de $C_G(T)$ em $N_G(T)$ é finito.*

Demonstração. Vamos mostrar essa proposição apenas no caso em que a característica de K é maior que 0. A demonstração do caso geral pode-se ser vista em [16, Seção 16.3]. A idéia é utilizar o Lema 3.31 considerando o morfismo $\varphi : N_G(T)^0 \times T \to T$ definido por $\varphi(x,t) = xtx^{-1}$.

A condição (i) é satisfeita, afinal todos os elementos de T tem ordem finita. Dado $l > 0$, os elementos de G_m que possuem ordem l são raízes do polinômio $x^l - 1$ e há apenas um número finito deles para cada l, portanto (ii) é satisfeita. O subgrupo $N_G(T)^0$ é conexo, então (iii) está satisfeita. Para cada $x \in N_G(T)^0$, φ_x é a restrição de um automorfismo interno de $N_G(T)$ ao subgrupo T, assim (iv) também é satisfeita.

O Lema 3.31 implica $\varphi(x,t) = \varphi(1,t)$, isto é, $xtx^{-1} = t$ e portanto cada $x \in N_G(T)^0$ centraliza T. Logo $N_G(T)^0 \subseteq C_G(T)$ e portanto $N_G(T)^0 \subseteq C_G(T)^0$. Reciprocamente como $C_G(T)$ é um subgrupo de $N_G(T)$ e $C_G(T)^0$ é uma componente conexa que contém a identidade, temos $C_G(T)^0 \subseteq N_G(T)^0$. Assim, $N_G(T)^0 = C_G(T)^0$.

Pela Proposição 3.20, $C_G(T)^0$ é um subgrupo de índice finito tanto em $C_G(T)$ quanto em $N_G(T)$. Vale a equação $|N_G(T) : C_G(T)^0| = |N_G(T) : C_G(T)||C_G(T) : C_G(T)^0|$ e o lado esquerdo da equação é finito se e somente o lado direito também é. Assim, $|N_G(T) : C_G(T)^0|$ finito implica que $|N_G(T) : C_G(T)|$ também é finito. □

O fato de $N_G(T)/C_G(T)$ ser finito e podermos utilizar o Lema 3.31 para um toro T costuma ser expresso dizendo que o toro é "rígido". Na demonstração da Proposição 3.31 foi usado o fato da característica de K ser maior que 0 para argumentar que o conjunto dos elementos de ordem finita é denso. Se a característica fosse 0, o argumento não seria muito diferente mas teríamos que levar conta que T pode ter elementos de ordem infinita.

Agora, vamos definir os subgrupos de Borel de G.

Definição 3.33. Dado G um grupo linear algébrico, dizemos que $B \leq G$ é um *subgrupo de Borel* se ele for fechado, conexo, solúvel e for um subgrupo maximal com respeito a essas três propriedades.

Se T é um toro de um grupo G, dizemos que ele é *maximal* se ele for maximal em relação à inclusão, isto é, nenhum toro próprio de G o contém propriamente. O toro é fechado, conexo e solúvel, pois é o produto direto de grupos abelianos. Assim, todo toro está em algum subgrupo de Borel de G. Naturalmente, isso também vale para os toros maximais. A recíproca também vale e um toro maximal de B também tem que ser um toro maximal de G, veja [16, Seção 21.3].

Proposição 3.34. *Seja G é um grupo linear algébrico conexo e solúvel, então:*

(*i*) *Se $G \leq GL_n(K)$, então G é conjugado a um subgrupo de T_n, o subgrupo das matrizes triangulares superiores.*

(*ii*) *G_u é um subgrupo fechado, conexo, normal e $[G, G] \subseteq G_u$.*

(*iii*) *Todos os toros maximais de G são conjugados e se T é um toro maximal, então G é o produto semidireto entre G_u e T. Além disso, $N_G(T) = C_G(T)$.*

Demonstração. Veja [16, Seção 19.3]. □

Para o grupo $GL_n(K)$, temos que T_n é um subgrupo de Borel de $GL_n(K)$. Para $SL_n(K)$, um subgrupo de Borel é obtido tomando $T_n \cap SL_n(K)$. Os subgrupo de Borel satisfazem as seguintes propriedades adicionais:

Proposição 3.35. *Seja G um grupo linear algébrico conexo, então:*

(*i*) *Todos os subgrupos de Borel de G são conjugados.*

(*ii*) *Se B é um subgrupo de Borel, vale $G = \bigcup_{g \in G} gBg^{-1}$.*

(*iii*) *$N_G(B) = B$.*

Demonstração. Veja [24, Teoremas 6.4, 6.10 e 6.12]. □

Definição 3.36. O único subgrupo de G fechado, solúvel, conexo e normal que é maximal em relação a essas propriedades é chamado de *radical de G* e é denotado por $R(G)$. A componente unipotente de $R(G)$ é chamada de *radical unipotente de G* e é denotada por $R_u(G)$. Um grupo linear algébrico que satisfaz $R_u(G) = \{1\}$ é chamado de *redutivo*. Se G for conexo e $R(G) = \{1\}$ dizemos que G é *semisimples*.

Se N e N' são dois subgrupos normais, fechados, conexos e solúveis, então NN' é outro subgrupo com as mesmas propriedades. Assim, $R(G)$ é, de fato, o único subgrupo maximal com respeito a essas propriedades. De modo análogo, podemos caracterizar $R_u(G)$ como sendo o maior subgrupo normal, fechado, conexo e unipotente de G. Primeiro, observe que $R_u(G)$ é normal em G. A razão disso é que $R(G)$ sendo normal em G, a conjugação por um elemento de G induz um automorfismo de grupos algébricos em $R(G)$. Pela Proposição 3.29, tal automorfismo deve levar elementos unipotentes em elementos

unipotentes, portanto fixa $R_u(G)$. Agora, pela Proposição 3.34, $R_u(G)$ é um subgrupo fechado e conexo. Assim, $R_u(G)$ tem todas as propriedades que mencionamos. Por outro lado, se $H \leq G$ também possui essas propriedades, então H é solúvel, pois H é isomorfo a um subgrupo de U_n. Assim $H \leq R(G)$ e por H ser unipotente, $H \leq R_u(G)$.

Os grupos lineares redutivos e semisimples são de importância fundamental e é a partir deles que construiremos certos grupos finitos. Vejamos agora algumas propriedades adicionais de $R(G)$.

Proposição 3.37. *Seja G um grupo linear algébrico, então:*

(i) $R(G) = (\cap_B B)^0$, *onde a interseção percorre todos os subgrupos de Borel de G.*

(ii) Se G for conexo redutivo, $R(G)$ é um toro e $R(G) = Z(G)^0$.

Demonstração. (i) Como o radical $R(G)$ é fechado, conexo e solúvel, certamente está em algum subgrupo de Borel B_1. Se B_2 é um outro Borel, B_1 e B_2 são conjugados e existe g tal que $gR(G)g^{-1} \leq B_2$. Como $R(G)$ é normal $gR(g)g^{-1} = R(G)$, para todo $g \in G$, e daí $R(G) \subseteq (\cap_B B)$. $R(G)$ é conexo, logo $R(G) \subseteq (\cap_B B)^0$.

Reciprocamente, $(\cap_B B)^0$ é fechado, conexo e solúvel. Se mostrarmos que também é normal, teremos $(\cap_B B)^0 \subseteq R(G)$. Sabemos que $(\cap_B B)^0$ é normal em $\cap_B B$. Observe que como todos os subgrupos de Borel são conjugados, podemos fixar $\tilde{B}$ e escrever $\cap_B B = \cap_{g \in G} g\tilde{B}g^{-1}$. Agora, $\cap_{g \in G} g\tilde{B}g^{-1}$ é um subgrupo normal de G.[2]

Em geral se H é normal em G e K é normal em H, não é verdade que K é normal em G. Mas se G é um grupo linear algébrico e H é normal em G, então H^0 também é normal em G. A razão disso é que a conjugação por um elemento de G é um automorfismo de grupos algébricos de H, pois H é normal em G. Em particular, a conjugação leva componentes conexas em componentes conexas e portanto deve levar H^0 em H^0. Portanto, $(\cap_B B)^0$ é normal em G e segue que $(\cap_B B)^0 \subseteq R(G)$.

(ii) O radical $R(G)$ satisfaz as hipóteses da Proposição 3.34, e assim é o produto semidireto de $R(G)_u$ e um toro. Como G é redutivo, temos $R(G)_u = 1$ e $R(G)$ deve ser um toro.

O centro de G é sempre um subgrupo normal e solúvel. Com a hipótese adicional de G ser grupo linear algébrico, o centro também é um subgrupo fechado, pela Proposição 3.26. Assim, temos $Z(G)^0 \leq R(G)$.

Reciprocamente, como $R(G)$ é um toro, pela Proposição 3.32, temos $N_G(R(G))^0 = C_G(R(G))^0$. Como $R(G)$ é normal em G, temos $N_G(R(G))^0 = G^0$. Daí, $C_G(R(G))$ contém a componente G^0. Como G é conexo, temos $G = G^0$ e $C_G(R(G)) = G$. Portanto $R(G) \leq Z(G)$. Como $R(G)$ é conexo, temos $R(G) \leq Z(G)^0$.

□

Como exemplo, temos que $G = GL_n(K)$ é redutivo mas não é semisimples. O centro de $GL_n(K)$ é composto por toda as matrizes escalares, portanto, $Z(GL_n(K)) \cong G_m$. Assim, o centro é um grupo conexo, solúvel, fechado e normal e $R(G)$ não pode ser trivial. O subgrupo T_n das matrizes triangulares superiores é um subgrupo de Borel e L_n, o subgrupo das matrizes triangulares inferiores também é. Pela Proposição 3.37, temos $R(G) \leq T_n \cap L_n$, mas $T_n \cap L_n$ consiste apenas de matrizes diagonais, ou seja,

[2]Se $H \leq G$, então $\bigcap_{g \in G} gHg^{-1}$ é sempre um subgrupo normal de G. Tal subgrupo normal é chamado de *core* de H em G e é o maior subgrupo normal de G contido em H.

$T_n \cap L_n = D_n$. Por sua vez, D_n é composto apenas de elementos semisimples, então $(D_n)_u = \{1\}$ e portanto, $R(G)_u = \{1\}$. Isso mostra que $GL_n(K)$ é redutivo.

Um argumento análogo mostra que $SL_n(K)$ também é redutivo. Assim, temos $R(G) = Z(G)^0$. O centro de $SL_n(K)$ é formado por matrizes escalares, mas a restrição que a matriz tenha determinante 1 implica que os elementos da matriz satisfazem $x^n = 1$. Assim, o centro de $SL_n(K)$ é um subgrupo finito e portanto $Z(G)^0 = \{1\}$. Isso mostra que $SL_n(K)$ é semisimples.

Teorema 3.38 (Par-BN para grupos redutivos)**.** *Seja G um grupo linear algébrico conexo redutivo. Tome B um subgrupo de Borel de G, T um toro maximal de B e $N = N_G(T)$. Então valem as seguintes propriedades:*

(*i*) $C_G(T) = T$.

(*ii*) $B \cap N = T$.

(*iii*) *B e N formam um par-BN para G.*

Demonstração. Veja [24, Corolário 8.13, Teorema 11.16] □

Vimos no Capítulo 2, que se G possui um par-BN, a estrutura de G é controlada fortemente pelo grupo de Weyl. Assim, o teorema anterior é bastante surpreendente. Observe que o grupo de Weyl é $N/T = N_G(T)/C_G(T)$, que pela Proposição 3.32 é *finito*. Assim, todos os resultados desenvolvidos no Capítulo 2 continuam válidos. Em particular, vale a decomposição de Bruhat $G = BWB$. Além disso, podemos falar dos subgrupos parabólicos de G da mesma forma como foi feito antes.

3.6 Endomorfismos de Frobenius

Nesta seção começaremos a ver como surgirão os grupos finitos do tipo Lie. Até este ponto, consideramos apenas grupos lineares definidos sobre corpos algebricamente fechados e, portanto, infinitos. Os grupos finitos surgirão ao considerar endomorfismos especiais dos grupos lineares e tomar os seus respectivos pontos fixos. A referência fundamental para essa abordagem é o trabalho de Steinberg [36]. Uma discussão um pouco mais recente pode ser encontrada em [24, Parte 3] ou [9, Capítulo 3]. Nessa seção sempre consideraremos que K é um corpo algebricamente fechado de característica prima.

Precisamos primeiro relembrar alguns fatos gerais sobre corpos de característica prima. Já utilizamos anteriormente que se K é um corpo algebricamente fechado em característica p, podemos escrever $K = \bigcup_{n>0} \mathbb{F}_{p^n}$. Outro fato importante é que os elementos de $\mathbb{F}_{p^n}$ são precisamente as raízes do polinômio $x^{p^n} - x$.

Considere $G = GL_n(K)$ e considere a função F_q que leva uma matriz (a_{ij}) em (a_{ij}^q), onde q é uma potência de p. A função F_q, na verdade, é um endomorfismo de grupos algébricos. Note que cada função coordenada de F_q é o polinômio x_{ij}^q, assim F_q é um morfismo de variedades afins. Precisamos verificar ainda que F_q é um endomorfismo de grupos.

Se $(a_{ij}) \in GL_n(K)$, temos $\det(a_{ij}) \neq 0$. O determinante é uma soma alternada da forma $\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{i=1}^n a_{i\sigma(i)}$, onde S_n é grupo das permutações de n elementos e $\operatorname{sgn}(\sigma)$

é o sinal da permutação σ. Assim, o determinante de (a_{ij}^q) é dado por $\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\prod_{i=1}^n a_{i\sigma(i)}^q$. Em característica p, temos a relação $(x+y)^q = x^q + y^q$, assim:

$$\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\prod_{i=1}^n a_{i\sigma(i)}^q = \left(\sum_{\sigma\in S_n}\operatorname{sgn}(\sigma)\prod_{i=1}^n a_{i\sigma(i)}\right)^q.$$

Logo o determinante de (a_{ij}^q) deve ser não-nulo também. Usando a relação $(x+y)^q = x^q+y^q$ também é possível mostrar que F_q preserva a operação do grupo. Portanto, F_q é, de fato, um endomorfismo de $GL_n(K)$. Mais ainda, F_q é uma bijeção, mas não é um automorfismo de grupos algébricos, pois as funções coordenadas de F_q^{-1} não são definidas através de polinômios em K. Um endomorfismo de um grupo linear algébrico da forma F_q é chamado de *endomorfismo de Frobenius padrão*.

Vamos olhar para o que está acontecendo do ponto de vista da Geometria Algébrica.

Se X é uma variedade afim, dizemos que X está *definida sobre* $\mathbb{F}_q$ se $K\otimes_{\mathbb{F}_q} A_0 \cong K[X]$, onde A_0 é uma F_q-álgebra (de polinômios) finitamente gerada e o isomorfismo é dado pela função que leva $\sum k\otimes f$ em $\sum kf$.

A álgebra A_0 é chamada de uma *F_q-estrutura* para X. O *endomorfismo de Frobenius geométrico com respeito a essa $\mathbb{F}_q$-estrutura* é definido pela função F^* que leva $k\otimes f$ em $k\otimes f^q$, enquanto o *endomorfismo de Frobenius aritmético* é a função Φ que leva $k\otimes f$ em $k^q\otimes f$.

O endomorfismo de Frobenius geométrico é um endomorfismo de K-álgebras, enquanto o endomorfismo de Frobenius aritmético é apenas um endomorfismo de $\mathbb{F}_q$-álgebras. De fato, para $\lambda\in K$ e $f\in A_0$, temos $\lambda(1\otimes f) = \lambda\otimes f$ e $\Phi(\lambda\otimes f) = \lambda^q\otimes f$ e isso só igual a $\lambda\phi(1\otimes f)$, se $\lambda^q = \lambda$, portanto, se $\lambda\in\mathbb{F}_q$.

Como $F^* : K[X]\to K[X]$ é um homomorfismo, ele induz um endomorfismo de variedades afins $F : X\to X$, pela Proposição 3.9 (v). Esse endomorfismo de variedades afins é o que chamaremos de *endomorfismo de Frobenius padrão* associado à $\mathbb{F}_q$-estrutura. Quando não houver possibilidade confusão, chamaremos F apenas de *endomorfismo de Frobenius*. Queremos verificar que F é o morfismo que leva $(x_1,\dots,x_n)$ em $(x_1^q,\dots,x_n^q)$ e, portanto, o endomorfismo de Frobenius padrão que discutimos anteriormente. Para isso, basta verificar que dado $h\in K[X]$ com $h = \sum k\otimes f$, temos $\sum k\otimes f^q(x_1,\dots,x_n) = \sum k\otimes f(x_1^q,\dots,x_n^q)$. Isso é verdade, pois cada f está em A_0, assim f^q é o polinômio que corresponde a elevar cada termo de f à q. Note que os coeficientes de f satisfazem $a^q = a$, então eles são fixados. Assim, fica claro [3] que $f^q(x_1,\dots,x_n) = f(x_1^q,\dots,x_n^q)$.

Proposição 3.39. *Seja X uma variedade afim definida sobre $\mathbb{F}_q$ e A_0 a sua $\mathbb{F}_q$-estrutura. Denotando por F o endomorfismo de Frobenius associado temos:*

(i) $A_0 = \{f\in K[X] \mid F(f) = f^q\}$.

(ii) Uma subvariedade fechada $Y\subseteq X$ é F-estável, isto é, $F(Y)\subseteq Y$ se, e somente se, $K[Y]\cong K\otimes I_0$, com I_0 um ideal de A_0. Nesse caso, Y está definido sobre $\mathbb{F}_q$ e seu endormofismo de Frobenius correspondente é a restrição de F à variedade Y.

[3] Por exemplo, em uma única variável, temos $f(x) = \sum a_i x^i$ e $f^q(x) = \sum (a_i x^i)^q$. Como cada $a_i\in\mathbb{F}_q$, temos $a_i^q = a_i$. Portanto, $f^q(x) = \sum a_i (x^q)^i = f(x^q)$.

Demonstração. Veja [9, Proposição 3.3]. □

Note que na Proposição 3.39 já partimos de uma variedade afim que possui uma $\mathbb{F}_q$-estrutura. Isso não é problema, pois se X é uma variedade afim sobre K, sempre podemos considerar que $X \subseteq K^n$, para algum n. A álgebra afim de K^n é a álgebra de polinômios sobre K em n variáveis $K[T_1, \ldots, T_n]$, que denotaremos por $K[T]$. Para todo subcorpo $\mathbb{F}_q$ de K temos $K[T] \cong K \otimes_{\mathbb{F}_q} \mathbb{F}_q[T]$, assim K sempre possui uma $\mathbb{F}_q$-estrutura para qualquer subcorpo de K. Assim, podemos usar a Proposição 3.39 como critério para decidir se uma variedade afim tem uma $\mathbb{F}_q$-estrutura.

Se $X \subseteq K^n$ é uma variedade afim cujo ideal $\mathcal{I}(X)$ é gerado por polinômios com coeficientes em $\mathbb{F}_q$, então X possui uma $\mathbb{F}_q$-estrutura. Isso ocorre, por exemplo, quando os polinômios que definem X possuem todos os seus coeficientes em $\mathbb{F}_q$. Para verificar isso, considere a restrição à variedade X do endomorfismo de Frobenius associado a K^n. Agora suponha que exista $S \subseteq \mathbb{F}_q[T]$ tal que $x \in X$ se, e somente se, $f(x) = 0$, para todo $f \in S$. Note que para $f \in S$, temos $f(x) = 0$ se e somente $f(x^q) = 0$. Portanto, temos $F(X) \subseteq X$, isto é, X é F-estável. Pela Proposição 3.39 isso implica que X tem uma $\mathbb{F}_q$-estrutura.

Se G é um grupo linear algébrico, dizemos que G está definido sobre $\mathbb{F}_q$ se G está definido sobre $\mathbb{F}_q$ como variedade afim e o endomorfismo de Frobenius correspondente é um endomorfismo de grupos.

Vamos, agora, voltar a discutir a situação de alguns grupos. O fato de $GL_n(K)$ possuir um endomorfismo de Frobenius implica $GL_n(K)$ ter uma $\mathbb{F}_q$-estrutura. À luz da discussão anterior poderíamos ter inferido a existência de um endomorfismo de Frobenius F usando o fato que $(g, \lambda) \in K^{n^2+1}$ está em $GL_n(K)$ se, e somente se, $\lambda \det(g) - 1 = 0$, que é uma expressão polinomial em que os coeficientes estão todos em $\mathbb{F}_q$. É claro, ainda teríamos que mostrar que F é um endomorfismo de grupos.

Agora, se $G \leq GL_n(K)$ e G está definido sobre $\mathbb{F}_q$, podemos ver o endomorfismo de Frobenius correspondente como uma restrição do endomorfismo de Frobenius da $\mathbb{F}_q$-estrutura de $GL_n(K)$. Há vários exemplos de grupos com $\mathbb{F}_q$-estruturas: $SL_n(K)$, $Sp_{2n}(K)$, T_n e outros.

A importância de se analisar o endomorfismo de Frobenius F_q de um grupo linear algébrico está no conjunto de pontos fixos de F_q. Por exemplo, os elementos $g \in GL_n(K)$ que satisfazem $F_q(g) = g$ são aqueles em que cada coordenada da matriz satisfaz $a_{ij}^q = a_{ij}$, isto é, cada coordenada de g é uma raiz de $x^q - x$ e, portanto, está em $\mathbb{F}_q$.

Se G é um grupo linear algébrico e F um endomorfismo de grupos algébricos de G, denotaremos por G^F o conjunto dos pontos fixos de F. Com essa notação, temos $GL_n(K)^{F_q} = GL_n(q)$. De modo análogo, temos $SL_n(K)^{F_q} = SL_n(q)$.

O problema é que os endomorfismos de Frobenius não são suficientes para construir todos os grupos finitos do tipo Lie e precisamos considerar endomorfimos F em que F^m é um endomorfismo de Frobenius, para algum $m \geq 1$. Seguindo [24], chamaremos tais endomorfismos de *endomorfismos de Steinberg*.

Definição 3.40. Um endomorfismo de grupos lineares algébricos $F : G \to G$ é chamado de *endomorfismo de Steinberg* se existe $m \geq 1$ tal que $F^m : G \to G$ é o endomorfismo de Frobenius com respeito a alguma $\mathbb{F}_q$-estrutura de G. Denotaremos o conjunto de pontos fixos de F por G^F.

Pelo que foi discutido até agora, fica claro que se F é um endomorfismo de Steinberg, então G^F é finito. Sob a hipótese de G ser simples, é possível mostrar que há uma certa dicotomia em relação aos endomorfismos de G. Steinberg mostrou em [36, Teorema 10.13], que se G é simples e σ é um endomorfismo qualquer de G, então ou σ é um automorfismo de G ou G^σ é finito. Note, porém, que no contexto de grupos lineares algébricos o conceito de *grupo simples* é um pouco diferente. Dizemos que um grupo linear algébrico é simples se for semisimples e não contiver nenhum subgrupo fechado normal e conexo próprio não-trivial.

3.6.1 Grupos Finitos do tipo Lie

Nesta seção finalmente definiremos o que é um grupo finito do tipo Lie.

Definição 3.41. Seja G um grupo linear algébrico redutivo sobre um corpo K de característica p e $F : G \to G$ um endomorfismo de Steinberg. O conjunto de pontos fixos G^F é chamado de *grupo finito do tipo Lie em característica p*.

Uma das vantagens de se tratar os grupos finitos do tipo Lie como grupos da forma G^F é que podemos transferir muitos resultados da teoria de grupos redutivos para G^F. Nesse sentido, o seguinte teorema é essencial.

Teorema 3.42 (Lang)**.** *Seja G um grupo linear algébrico conexo e F um endomorfismo de Steinberg. Então a função $L(g) : G \to G$ que leva g em $g^{-1}F(g)$ é sobrejetiva. A função $L(g)$ é também chamada de* função de Lang.

Em verdade, vale um resultado um pouco mais forte em que F é substituído por um endomorfismo $\sigma : G \to G$ tal que G^σ é finito. Esse resultado é o *Teorema de Lang-Steinberg*. Nos dois casos, a prova usualmente não é muito elementar e utiliza a diferencial dos endomorfismos envolvidos, que depende de resultados sobre a álgebra de Lie associada a um grupo linear algébrico. Discutiremos aqui uma prova alternativa [27] que depende apenas de alguns resultados básicos sobres grupos lineares algébricos e morfismos de variedades afins.

Antes de começar a demonstração, vamos apenas observar o fato que se G é F-estável, então G também é F^m-estável, para $m \geq 1$. Isso significa que se F é o endomorfismo de Frobenius associado a uma $\mathbb{F}_q$-estrutura, então F^m é o endomorfismo de Frobenius associado a uma $\mathbb{F}_{q^m}$-estrutura.

Demonstração. Considere a ação mórfica de G sobre si mesmo tal que, cada $g \in G$, define um morfismo que leva $x \in G$ em $g^{-1}xF(g)$. Pela Proposição 3.24, existe pelo menos uma órbita fechada Ω dessa ação. Fixe $x \in \Omega$ e considere o morfismo $\varphi : G \to \Omega$ que leva g em $g^{-1}xF(g)$. Como G é conexo, se mostrarmos que $\dim G = \dim \Omega$, teremos $G = \Omega$, pela Proposição 3.17. Nessa situação, temos $1 \in \Omega$ e portanto $\{g^{-1}F(g) \mid g \in G\} = G$.

A aplicação φ é um morfismo sobrejetor entre variedades afins, portanto é um morfismo dominante. Além disso como G é irredutível, então $\varphi(G) = \Omega$ também o é. Assim, podemos utilizar a Proposição 3.18 para concluir que as fibras do morfismo φ têm dimensão pelo menos $\dim G - \dim \Omega$. Dessa forma, se mostrarmos que existe uma fibra de dimensão 0, isso obriga $\dim G = \dim \Omega$. Considere a fibra $\varphi^{-1}(x)$. Temos $g \in \varphi^{-1}(x)$ se, e somente se, $g^{-1}xF(g) = x$. De forma equivalente, temos $g \in \varphi^{-1}(x)$ se e somente se $xF(g)x^{-1} = g$.

Vamos mostrar agora que a equação $xF(g)x^{-1} = g$ tem um número finito de soluções para $g \in G$.

Considere a função $f(g) = xF(g)x^{-1}$. Queremos mostrar que $f(g) = g$ tem um número finito de soluções. Como F é um endomorfismo de Steinberg, existe $m \geq 1$ tal que F^m é um endomorfismo de Frobenius padrão. Existe um corpo finito $\mathbb{F}_q$ tal que todos as entradas de x estão nesse corpo, logo podemos tomar m grande o suficente de tal forma que F^m seja um endomorfismo de Frobenius padrão e $F^m(x) = x$. Note que $f^n(g) = xF(x)\dots F^{n-1}(x)F^n(g)F^{n-1}(x^{-1})\dots x^{-1}$. Agora, seja r a ordem do elemento $xF(x)\dots F^{m-1}(x)$, então $f^{mr}(g) = F^{mr}(g)$. Assim, $f(g) = g$ implica $f^{mr}(g) = g$ e, pela equação anterior, $F^{mr}(g) = g$. A equação $F^{mr}(g) = g$ tem um número finito de soluções e, portanto, o mesmo vale para $f(g) = g$.

□

O Teorema de Lang-Steinberg possui muitas aplicações na teoria de grupos algébricos, veja [9, Capítulo 3], [24, Capítulos 21 e 22] ou [36, Capítulo 10]. Aqui, utilizaremos o Teorema de Lang para mostrar que existem subgrupos de Borel e toros maximais que são F-estáveis.

Proposição 3.43. *Seja G um grupo linear algébrico conexo com um endomorfismo de Steinberg $F : G \to G$. Suponha que exista uma ação de G em um certo conjunto X e uma função $\varphi : X \to X$ satisfazendo $\varphi(g.x) = F(g).\varphi(x)$, para $g \in G$, $x \in X$. Nessas condições, se Ω é uma órbita da ação de G em X tal que $\varphi(\Omega) \subseteq \Omega$, então existe $x \in \Omega$ tal que $\varphi(x) = x$.*

Demonstração. Seja Ω uma órbita da ação de G em X satisfazendo $\varphi(\Omega) \subseteq \Omega$. Dado $x \in \Omega$, existe $g \in G$ tal que $g.\varphi(x) = x$. Pelo Teorema de Lang, podemos escrever g como $h^{-1}F(h)$, para algum $h \in G$. Temos então:

$$\begin{aligned} x &= h^{-1}F(h).\varphi(x) \\ &= h^{-1}\varphi(h.x). \end{aligned}$$

Isso implica $\varphi(h.x) = h.x$ e $h.x$ é o ponto fixo desejado. □

Proposição 3.44. *Seja G um grupo linear algébrico conexo com um endomorfismo de Steinberg $F : G \to G$. Então existe um par (B, T) formado por um subgrupo de Borel B e um toro maximal T contido em B tal que ambos são F-estáveis.*

Demonstração. Considere o conjunto X das duplas da forma (B, T) em que B é um subgrupo de Borel e T é um toro maximal de B. Tomaremos a ação de G em X por conjugação, isto é, $g \in G$ leva (B, T) em (gBg^{-1}, gTg^{-1}). A idéia é utilizar a Proposição 3.43 com a função $\varphi(B, T) = (F(B), F(T))$. Como F é um endomorfismo bijetor, $F(B)$ e $F(T)$ são também subgrupo de Borel e toro maximal, respectivamente. Assim, de fato, $\varphi(X) \subseteq X$. Além disso, $\varphi(gBg^{-1}, gTg^{-1}) = (F(g)F(B)F(g^{-1}), F(g)F(T)F(g^{-1})) = F(g).\varphi(B, T)$. Portanto, todas as hipóteses da Proposição 3.43 estão atendidas. Portanto existe $(B, T) \in X$ tal que $(F(B), F(T)) = (B, T)$. □

Um toro maximal T que é F-estável e está contido em um subgrupo de Borel também F-estável é dito *maximally split* com respeito a F.

Proposição 3.45. *Seja G um grupo linear com um endomorfismo de Steinberg F e H um subgrupo de G fechado, conexo, normal e F-estável. Então $(G/H)^F$ e (G^F/H^F) são isomorfos como grupos abstratos.*

Demonstração. Considere o homomorfismo quociente $\pi : G \to G/H$ que leva g em gH. A restrição de π ao subgrupo G^F leva um elemento de G^F em um elemento gH que satisfaz $F(gH) = gH$, assim $\pi(G^F) \subseteq (G/H)^F$. O núcleo dessa restrição é H^F, portanto G^F/H^F é isomorfo a um subgrupo de $(G/H)^F$. Vamos mostrar agora que essa restrição é sobrejetora. Seja $gH \in (G/H)^F$, então $F(gH) = gH$, como H é F-estável, temos $F(g)H = gH$ e portanto $g^{-1}F(g) \in H$. Como H é conexo, podemos usar o Teorema de Lang e concluir que existe $h \in H$ tal que $h^{-1}F(h) = g^{-1}F(g)$. Rearranjando os termos, temos $gh^{-1} = F(gh^{-1})$, ou seja, $gh^{-1} \in G^F$ e $\pi(gh^{-1}) = gH$. Portanto $\pi : G^F \to (G/H)^F$ é sobrejetora e $G^F/H^F \cong (G/H)^F$. □

Quando H é um subgrupo fechado e normal de G, G/H também é um grupo linear algébrico de forma natural [24, Proposição 5.7]. Sob a hipótese adicional de H ser conexo, a proposição anterior garante que não há surpresas desagradáveis ao considerarmos os pontos fixos do quociente G/H. Quando H não é conexo, a situação pode se tornar bastante delicada. Por exemplo, há uma certa dificuldade em se obter $PSL_n(q)$ como um grupo da forma G^F, para G grupo linear algébrico.

Seja L um corpo arbitrário. Com a definição usual, temos $PSL_n(L) \cong SL_n(L)/Z(SL_n(L))$ e $PGL_n(L) \cong GL_n(L)/Z(GL_n(L))$. Quando cada elemento de L tem uma raiz n-ésima em L, $PGL_n(L)$ e $PSL_n(L)$ são iguais. No nosso caso, em que estamos considerando um corpo K algebricamente fechado, certamente essa condição é satisfeita. Considere um endomorfismo de Frobenius padrão F com respeito a uma $\mathbb{F}_q$-estrutura, então $PGL_n(K)^F \cong PSL_n(K)^F$. Agora, o centro de $GL_n(K)$ é isomorfo ao grupo G_m, em particular, ele é conexo. Portanto, pela Proposição 3.45, $PGL_n(K)^F \cong GL_n(K)^F/Z(GL_n(K))^F \cong PGL_n(q)$. Assim, $PGL_n(q)$ é de fato um grupo finito do tipo Lie. Já o centro de $SL_n(K)$ não é conexo, então não podemos utilizar a Proposição 3.45. Em princípio, ainda poderia ser o caso que mesmo assim $PSL_n(K)^F$ fosse isomorfo a $SL_n(K)^F/Z(SL_n(K))^F \cong PSL_n(q)$, porém é possível mostrar que para certas combinações de n e q isso não ocorre, veja [9, Exemplo 3.14]. De toda forma, pela discussão que fizemos até agora, temos $PSL_n(K)^F$ isomorfo a $PSL_n(q)$ se, e somente se, $PGL_n(q) \cong PSL_n(q)$.

Vamos agora exibir um par-BN para G^F.

Teorema 3.46. *Seja G um grupo conexo redutivo e F um endomorfismo de Steinberg. Tome B um subgrupo de Borel F-estável, T um toro maximal F-estável contido em B e $N = N_G(T)$. Então B^F e N^F formam um par-BN para G^F em que o grupo de Weyl correspondente é W^F.*

Demonstração. Veja [24, Teorema 24.10]. □

A hipótese de que G seja conexo não é muito restritiva. Assim, uma parte considerável dos grupos finitos do tipo Lie admite um par-BN herdado do grupo linear algébrico correspondente. Mesmo em situações em que G não é conexo, ainda podemos construir por outros meios o par-BN para G^F.

3.7 Par-BN *split*

Alguns grupos possuem um par-BN que satisfazem condições um pouco mais fortes. É o caso da maior parte dos grupos finitos do tipo Lie e dos grupos lineares algébricos conexos e redutivos. Discutiremos brevemente nesta seção o conceito de par-BN *split*. Mais detalhes podem ser vistos em [30], [6, Seção 2.5] ou [8, §69]. Em [24, Capítulos 11, 12, 24, 25, 26], não se discute explicitamente o conceito de par-BN *split*, mas mostra-se que o par-BN usual para um grupo conexo redutivo tem várias boas propriedades e que elas são herdadas por G^F. Em muitos casos, tais propriedades são consequências do fato do par-BN para G ser *split*.

Definição 3.47. Seja G um grupo linear algébrico sobre um corpo K de característica $p > 0$. Suponha também que G possua um par-BN. Dizemos que G possui um *par-BN split* se as seguintes condições são satisfeitas:

(*i*) $T = B \cap N$ é um subgrupo abeliano fechado em que todos os elementos são semisimples.

(*ii*) $B = U \rtimes T$, onde U é um subgrupo fechado normal e unipotente.

(*iii*) $\bigcap_{n \in N} nBn^{-1} = T$.

Antes de prosseguir, observe que todo grupo finito pode ser visto como um grupo linear algébrico. Pelo Teorema de Cayley, todo grupo finito G é isomorfo a um subgrupo de algum S_n, onde n é no máximo $|G|$. O grupo S_n, por sua vez, é isomorfo ao grupo das matrizes de permutação, então é um subgrupo de $GL_n(K)$. Assim, G é um subgrupo de algum $GL_n(K)$ e, por ser finito, é fechado.

O ponto importante é que faz sentido falar de um par-BN *split* quando G é finito. Quando isso ocorre, temos T um subgrupo abeliano com ordem coprima com p e U um p-grupo. Para deixar em evidência o primo p, dizemos então, que G possui um *par-BN split em característica p*.

Vamos agora observar que se G é conexo redutivo, ele possui um par-BN *split*. Pelo Teorema 3.38, G possui um par-BN em que $B \cap N$ é um toro maximal, assim a condição (*i*) é satisfeita. O B do par-BN é um subgrupo de Borel que, pela Proposição 3.34, é o produto semidireto entre B_u e T. Além disso, B_u tem todas as propriedades desejadas, logo fazendo $U = B_u$, temos a condição (*ii*) satisfeita. Como $T \leq B$, temos $nTn^{-1} \leq nBn^{-1}$, para todo $n \in N$, mas $N = N_G(T)$, portanto $nTn^{-1} = T$ e $T \subseteq \bigcap_{n \in N} nBn^{-1}$. Para obter a inclusão contrária, veja [24, Corolário 11.18], onde mostra-se que existe $n \in N$ tal que $nBn^{-1} \cap B = T$. Assim, a condição (*iii*) também é satisfeita. Aproveitamos este momento para comentar o fato de que se G é um grupo qualquer com um par-BN (B, N), não necessariamente *split*, sempre é possível obter um par-BN (B, N') em que a condição $\cap_{n \in N'} nBn^{-1} = B \cap N'$ é satisfeita e ambos os pares possuem o mesmo grupo de Weyl [30, Lema 2.1].

Quando G é conexo e redutivo, é possível mostrar que o par-BN de G^F herdado de G também é *split*. Tal fato é comentado brevemente em [6, Seção 1.18] e também pode ser deduzido a partir dos resultados discutidos em [24, Parte 3].

Proposição 3.48. *Seja G um grupo linear algébrico com um par-BN* split*, então U é um subgrupo de G que é maximal com respeito a propriedade de ser unipotente.*

Demonstração. Suponha M um subgrupo unipotente que contenha propriamente U. Se ocorrer $M \subseteq B$, isso implica $M = U(T \cap M)$. A inclusão $U(T \cap M) \subseteq M$ é clara. Agora, se $m \in M$, como $m \in B$, temos $m = ut$, com $u \in U$ e $t \in T$, daí $u^{-1}m = t$ que está em $T \cap M$. Porém, T contém apenas elementos semisimples, assim $T \cap M = \{1\}$ e $M = U$. Isso não pode ocorrer, pois M contém U propriamente. Logo M não pode estar contido em B.

Provemos que $B \cap M = U$. A inclusão $U \subseteq B \cap M$ é clara. Por outro lado, se $m \in B \cap M$, podemos escrever $m = ut$ e $t = u^{-1}m$, com $u \in U$, $t \in T$. Isso implica $t = 1$ e obtemos a inclusão $B \cap M \subseteq U$.

Considere o normalizador $P = N_G(U)$. Pode-se mostrar que todo grupo linear algébrico unipotente é isomorfo a um subgrupo de U_n. Agora, U_n é sempre nilpotente, logo todo grupo linear algébrico unipotente é nilpotente [24, Proposição 2.9 e Corolário 2.10]. No caso em que G é finito, é mais fácil verificar tal fato, pois um grupo unipotente nada mais é do que um p-grupo e todo p-grupo finito é nilpotente. Em um grupo nilpotente, todo subgrupo próprio está contido propriamente em seu normalizador. Assim, $N_M(U)$ contém propriamente U e $N_M(U)$ está contido em P. Além disso, como U é normal em B, temos que P também contém B.

A partir desses fatos, somos levados a concluir que P deve conter propriamente B. Se ocorrer $P = B$, temos $P \cap M = B \cap M$, mas $P \cap M = N_M(U)$ e $B \cap M = U$. Assim, $P = B$ implica $N_M(U) = U$, o que violaria a nilpotência de P.

Pela Proposição 2.36, os únicos subgrupos de G que contém B são os parabólicos da forma P_J, com $J \subseteq I$. Como P_J contém propriamente B, J não pode ser vazio. Isso significa que deve ser possível obter $n_j \in N_J$, tal que $\pi(n_j)$ é um gerador do grupo de Weyl W_J. Tal elemento satisfaz $n_j U n_j^{-1} = U$, pois P normaliza U. Como T é normal em N, também temos $n_j^{-1} T n_j = T$. Agora, $n_j B n_j = n_j U n_j n_j^{-1} T n_j = B$. Isso contradiz o axioma (v) do par-BN. Portanto, M não pode conter U propriamente. □

Observe que U é composto apenas de elementos que possuem ordem potência de p. Assim, no caso em que G é finito, a proposição anterior está afirmando que U é um p-subgrupo de Sylow de G.

Precisamos de um resultado técnico para prosseguir. Pela discussão da Seção 2.1.6, sempre podemos associar ao grupo de Weyl um sistema de raízes Φ. Quando G possui um par-BN *split*, podemos estabelecer uma bijeção entre Φ e uma coleção $\{U_\alpha \mid \alpha \in \Phi\}$ de subgrupos de G. Para cada $\alpha \in \Phi$, o subgrupo U_α é chamado de *subgrupo raiz*. Os subgrupos raízes podem ser escolhidos de tal forma que W aja sobre eles de forma similar à ação de W em Φ. Mais detalhes sobre os subgrupos raízes podem ser vistos em [8, §69] ou em [6, Seções 2.5 e 2.6 e Proposição 2.5.15].

Definição 3.49. Se G é um grupo com par-BN *split*, dizemos que G satisfaz as *relações dos comutadores*, se, para quaisquer raízes linearmente independentes $\alpha, \beta \in \Phi$, temos:

$$[U_\alpha, U_\beta] \subseteq \prod U_{i\alpha + j\beta},$$

onde o produtório é tomado sobre todas as raízes que podem ser expressas da forma $i\alpha + j\beta$, com $i, j > 0$.

As relações dos comutadores são essenciais para mostrar certos resultados sobre o par-BN *split*. Se G é um grupo linear algébrico conexo e redutivo, então G e G^F certamente

possuem um par-BN *split* que satisfaz as relações dos comutadores, veja os *Remarks* após o item (69.2vii) em [8] ou em [6], antes da Proposição 2.6.4.

Teorema 3.50 (Decomposição de Levi)**.** *Seja G um grupo linear algébrico com um par-BN* split *que satisfaz as relações dos comutadores. Tome P_J um subgrupo parabólico padrão de G, então:*

(*i*) *Existe U_J um subgrupo unipotente e normal em P_J tal que $P_J = U_J \rtimes L_J$, onde L_J é um complemento de U_J em P_J.*

(*ii*) *U_J é o maior subgrupo normal e unipotente de P_J.*

(*iii*) *L_J possui um par-BN* split *cujo grupo de Weyl correspondente é W_J.*

(*iv*) *Os subgrupos parabólicos padrões de L_J são da forma $P_K \cap L_J$, para $K \subseteq J$.*

Demonstração. Se G for um grupo finito, uma demonstração desses fatos pode ser encontrada em [8, Teorema 69.10]. Para o caso geral, em que assumimos apenas que G é um grupo linear algébrico com um par-BN *split*, veja [6, Seções 2.5 e 2.6]. □

A decomposição $P_J = U_J \rtimes L_J$ do teorema anterior é chamada de *decomposição de Levi*. Quando G é um grupo linear algébrico conexo e redutivo, ele sempre possui um par-BN. Nesse contexto, os dois itens (*i*) e (*ii*) são sempre verdadeiros e são resultados clássicos da teoria de grupos lineares algébricos, veja [24, Proposição 12.6], [16, Seção 30.2] ou [33, Teorema 8.4.3]. Nesse caso, temos, na verdade, que U_J é o radical unipotente de P_J.

Capítulo 4

O caráter de Steinberg e Aplicações

Neste capítulo discutiremos o caráter de Steinberg definido por Robert Steinberg em [34, 35]. Nesses dois artigos, a ênfase é na construção da representação e não no caráter propriamente dito. Assim, um dos caminhos para discutir o caráter de Steinberg é definir a representação associada, mostrar que é irredutível e que seu caráter é dado pela Equação (4.1). Uma referência moderna para essa abordagem é [8, §66c].

Neste capítulo, seguiremos [6, Capítulo 6] e primeiro definiremos o caráter de Steinberg como um caráter generalizado e, em seguida, mostraremos que é um caráter irredutível. Essa abordagem tem a desvantagem de não fornecer de forma óbvia a representação associada ao caráter, mas isso não será um problema para as aplicações discutidas aqui. Esta construção, que pode ser aplicada para todo grupo finito com par-BN, foi obtida por Curtis [7].

4.1 Definição e Irredutibilidade

O caráter de Steinberg é definido em termos de uma soma alternada dos caracteres principais induzidos a partir dos subgrupos parabólicos de um grupo com par-BN. Nesta seção, assumimos que G é um grupo finito que satisfaz as hipóteses da seguinte definição.

Definição 4.1. Seja G um grupo finito com um par-BN. Dessa forma, G possui dois grupos B e N que satisfazem a Definição 2.1. Além disso, o grupo de Weyl W é gerado por elementos indexados por um conjunto I. Nessas condições, o *caráter de Steinberg* de G é dado pela expressão

$$St = \sum_{J \subseteq I} (-1)^{|J|} 1_{P_J}^G. \tag{4.1}$$

Não é evidente, em princípio, que St seja um caráter, nem que é irredutível. Estabeleceremos a irredutibilidade de St a partir da irredutibilidade de um caráter análogo do grupo de Weyl. Defina o caráter ε de W por:

$$\varepsilon = \sum_{J \subseteq I} (-1)^{|J|} 1_{W_J}^W,$$

onde os W_J denotam os subgrupos parabólicos padrões de W (veja a Seção 2.1.3). A irredutibilidade do caráter ε será mostrada em várias etapas. A primeira delas consiste

em mostrar um resultado geral sobre decomposição de um espaço vetorial em regiões delimitadas por hiperplanos. Em seguida, dado $w \in W$, usaremos o complexo de Coxeter (Seção 2.1.5) para decompor o auto-espaço associado ao autovalor 1 e aplicaremos esse resultado para obter um expressão para o determinante de w. Isso será suficiente para mostrar que $\varepsilon(w) = \det(w)$. Note que isso implica que ε é, na verdade, o caráter que assume o valor 1 se o comprimento de w é par e -1 caso contrário. Esse resultado foi obtido originalmente por Solomon [32]. Uma demonstração alternativa recente pode ser vista em [22, Teorema 5.2].

Utilizaremos a notação da Seção 2.1.2. Seja V um espaço vetorial real de dimensão n equipado com um produto interno e $H_1, \ldots, H_m$ uma coleção de hiperplanos quaisquer. Para cada hiperplano, escolha um $r_i \in V$ tal que $H_i = \langle r_i \rangle^\perp$.

Em seguida, considere a coleção $\mathcal{K}$ de todas as possíveis interseções não-vazias da forma $\bigcap_{i=1}^m H_i^{\epsilon_i}$, com $\epsilon \in \{0, +, -\}$. Chamaremos $\mathcal{K}$ de um *complexo*. Apenas para exemplificar, se temos três hiperplanos, um elemento de $\mathcal{K}$ é da forma $H_1^{\epsilon_1} \cap H_2^{\epsilon_2} \cap H_3^{\epsilon_3}$. Neste caso, $H_1^+ \cap H_2^+ \notin \mathcal{K}$, pois H_3^ϵ não apareceu na interseção.

Para $K \in \mathcal{K}$, considere o espaço vetorial L gerado por K. Definiremos a dimensão de K como sendo a dimensão de L. Assim, se aparecerem k elementos da forma H_i^0 na definição de K, então a dimensão de K será $n - k$. Além disso, K é um subconjunto aberto de L, pois é a interseção de L com abertos de V da forma H_j^+ ou H_j^-.

Lema 4.2. *Seja n_i o número de elementos de $\mathcal{K}$ que possuem dimensão i, então*

$$\sum_i (-1)^i n_i = (-1)^n. \tag{4.2}$$

Demonstração. A prova se dá por indução no número de hiperplanos m. Se $m = 1$, temos que $\mathcal{K} = \{H_1^0, H_1^+, H_1^-\}$ e portanto:

$$\sum_i (-1)^i n_i = (-1)^{n-1} + (-1)^n \times 2 = (-1)^n.$$

Agora, suponha que tenhamos m hiperplanos e queremos adicionar um hiperplano $H = \langle v \rangle^\perp$. Para cada $K \in \mathcal{K}$ podemos escolher se vamos interceptá-lo com H^0, H^+ ou H^-, porém, só iremos criar novos elementos se as interseções forem não-vazias. Suponha que K tenha dimensão i.

Se $K \cap H = \emptyset$, não podemos ter simultaneamente $K \cap H^+ \neq \emptyset$ e $K \cap H^- \neq \emptyset$. Note que K é convexo, assim se $x \in H^+ \cap K$ e $y \in K \cap H^-$, a linha que une x e y está em K e isso implicaria na existência de um $z \in K \cap H$. Neste caso, substituiremos K ou por $K \cap H^+$ ou por $K \cap H^-$, que são elementos de mesma dimensão de K. Isso não altera o número total de elementos, então o somatório (4.2) se preserva.

Suponha agora $H \cap K \neq \emptyset$. Tome V' como o espaço vetorial gerado por todos os vetores que são ortogonais aos hiperplanos H_i^0 que aparecem na definição de K. Se $v \in V'$, então $K \cap H = K$, isso implica $K \subseteq H$, então $K \cap H^+ = K \cap H^- = \emptyset$ e não estamos adicionando nenhum elemento ao complexo.

Agora consideremos a situação em que $K \cap H \neq \emptyset$ e $v \notin V'$. Vamos mostrar que $K \cap H^+ \neq \emptyset$ e $K \cap H^- \neq \emptyset$. Note que $K \subseteq V'^\perp$ e que K é um aberto de $V'^\perp$. Dessa forma, dado $x \in H \cap K$, existe uma vizinhança U de x aberta em $V'^\perp$ toda contida em K. Como $v \notin V'$, temos $v \in V'^\perp$ e como U é aberto, podemos tomar θ pequeno de tal

forma que $x + \theta v \in U$ e $\theta > 0$. Note que $x + \theta v \in K \cap H^+$. De modo análogo, temos $x - \theta v \in K \cap H^-$. Nessa situação substituímos K por três elementos: $K \cap H^+$ e $K \cap H^-$, de dimensão i e $K \cap H^0$ de dimensão $i-1$. Assim, temos $(-1)^i(n_i+1) + (-1)^{i-1}(n_{i-1}+1) = (-1)^i n_i + (-1)^{i-1} n_{i-1} + (-1)^i + (-1)^{i-1} = (-1)^i n_i + (-1)^{i-1} n_{i-1}$. Portanto, a fórmula fica inalterada.

□

Note que o complexo de Coxeter $\mathcal{C}$ definido na Seção 2.1.5 também é um complexo no sentido definido anteriormente. Além disso, a Proposição 2.30 garante que os elementos de $\mathcal{C}$ são da forma $x(C_J)$, para algum $x \in W$ e $J \subseteq I$. Para J fixo, definiremos $n_J(w)$ como sendo o número de elementos distintos de $\mathcal{C}$ da forma $x(C_J)$ que são fixados por w. Com isso, temos o seguinte resultado:

Proposição 4.3. *Para $w \in W$, temos:*

$$\sum_{J \subseteq I} (-1)^{|J|} n_J(w) = \det(w).$$

Demonstração. Dado w considere o auto-espaço V' associado ao autovalor 1. Tome o complexo $\mathcal{K} = \{K \cap V' \mid K \in \mathcal{C}\}$. Assim, podemos utilizar o Lema 4.2:

$$\sum_i (-1)^i n_i = (-1)^{\dim V'}, \tag{4.3}$$

onde n_i é a quantidade de $K \in \mathcal{K}$ de dimensão i. Antes de prosseguir, vamos analisar com cuidado a ação de W sobre o complexo de Coxeter. Pela Proposição 2.31, se $wx(C_J) = x(C_J)$, então w fixa $x(C_J)$ ponto a ponto. Caso contrário, se $wx(C_J) \neq x(C_J)$, então $wx(C_J)$ é um outro elemento do complexo de Coxeter. Como os elementos do complexo de Coxeter são todos disjuntos, então w não pode fixar nenhum elemento de $x(C_J)$.

Assim, ao interceptarmos $x(C_J) \in \mathcal{C}$ por V' temos ou $x(C_J) \cap V' = \emptyset$ ou $K \cap V' = x(C_J)$. Dessa forma, para calcular n_i, basta levar em consideração os elementos do complexo de Coxeter fixados por w de dimensão i. Se $n = \dim V$, temos $\dim x(C_J) = n - |J|$. Então n_i é o número de $x(C_J)$ de dimensão i que são fixados por w. Portanto:

$$n_i = \sum_{\substack{J \subseteq I \\ |J| = n-i}} n_J(w).$$

Substuindo na Equação (4.3):

$$\begin{aligned}
(-1)^{\dim V'} &= \sum_i (-1)^i \sum_{\substack{J \subseteq I \\ |J| = n-i}} n_J(w) \\
&= \sum_i \sum_{\substack{J \subseteq I \\ |J| = n-i}} (-1)^{n-|J|} n_J(w) \\
&= (-1)^n \sum_{J \subseteq I} (-1)^{|J|} n_J(w).
\end{aligned}$$

A última equação implica $\sum_{J\subseteq I}(-1)^{|J|}n_J(w) = (-1)^{\dim V'-n} = (-1)^{n-\dim V'}$. Como w é uma matriz diagonalizável sobre $\mathbb{C}$, a multiplicidade algébrica e geométrica dos seus autovalores coincidem. Os autovalores de w são 1, -1 e b pares conjugados de raízes complexas cuja norma é 1. O autovalor 1 ocorre com multiplicidade $\dim V'$, portanto $\det(w) = (-1)^{n-\dim V'-2b} = (-1)^{n-\dim V'}$. □

Agora, estamos em condições de mostrar que o caráter ε é irredutível.

Teorema 4.4. *O caráter ε é irredutível. Além disso, temos :*

(i) $\varepsilon(w) = \det(w)$.

(ii) $\varepsilon(w) = (-1)^{l(w)}$, *onde $l(w)$ é a função comprimento.*

Demonstração. Pela Proposição 2.29, o grupo de Weyl age sobre o complexo de Coxeter de tal forma que o estabilizador de cada C_J é precisamente W_J. Mais ainda, se $w \in W_J$, temos $w(v) = v$, para todo $v \in C_J$. Vamos analisar agora a expressão para o caráter induzido $1_{W_J}^W$:

$$1_{W_J}^W(w) = \frac{1}{|W_J|} \sum_{\substack{x\in W \\ xwx^{-1}\in W_J}} 1. \tag{4.4}$$

Note que $x^{-1}wx \in W_J$ se, e somente, $x^{-1}wx(C_J) = C_J$, isto é, se, e somente se, w fixa $x(C_J)$. Note que se $x(C_J) = y(C_J)$, então $x^{-1}y \in W_J$ e $y = xw'$ para $w' \in W_J$. Assim, cada $x(C_J)$ distinto fixado por w é contado $|W_J|$ vezes no somatório da Equação (4.4). Lembrando que $n_J(w)$ conta o número dos $x(C_J)$ distintos fixados por w, temos:

$$1_{W_J}^W(w) = \frac{1}{|W_J|}|W_J|n_J(w) = n_J(w). \tag{4.5}$$

Utilizando a definição do caráter ε e Equação (4.5), temos:

$$\varepsilon(w) = \sum_{J\subseteq I}(-1)^{|J|}n_J(w).$$

Pela Proposição 4.3, temos $\varepsilon = \det(w)$, e isso estabelece ε como um caráter linear de W e, portanto, irredutível. Agora, dado $w \in W$, temos que w é um produto de $l(w)$ geradores, que possuem determinante -1. Assim, $\det(w) = (-1)^{l(w)}$.

□

Para mostrar a irredutibilidade de St, faremos uso da correspondência entre classes laterais duplas de subgrupos parabólicos de W e de G (veja a Seção 2.2).

Proposição 4.5. *O caráter de Steinberg satisfaz $[St, St] = 1$.*

Demonstração. Temos:

$$\begin{aligned}[St, St] &= \left[\sum_{J\subseteq I}(-1)^{|J|}1_{P_J}^G, \sum_{K\subseteq I}(-1)^{|K|}1_{P_K}^G\right] \\ &= \sum_{J\subseteq I}\sum_{K\subseteq I}(-1)^{|J|}(-1)^{|K|}[1_{P_J}^G, 1_{P_K}^G].\end{aligned}$$

Na Seção 2.1.4 discutimos o conjunto $D_{J,K}$ de representantes das classes laterais duplas de W_J e W_K em W. A partir de $D_{J,K}$, podemos construir um conjunto de representantes $N_{J,K}$ das classes laterais duplas de P_J e P_K em G. Isso foi mostrado na Proposição 2.35. O conjunto $N_{J,K}$ é construído tomando, para cada $d \in D_{J,K}$, um elemento $n \in N$ tal que $\pi(n) = d$. Com esses fatos, podemos aplicar o Corolário 1.21:

$$[St, St] = \sum_{J\subseteq I}\sum_{K\subseteq I}(-1)^{|J|}(-1)^{|K|}\sum_{n\in N_{J,K}}[1_{P_J}, {}^n(1_{P_K})]_{P_J\cap nP_Kn^{-1}}.$$

A restrição de 1_{P_J} a $P_J \cap nP_Kn^{-1}$ coincide com o caráter principal de $P_J \cap nP_Kn^{-1}$. A mesma coisa acontece com a restrição de ${}^n(1_{P_K})$. Assim, $[1_{P_J}, {}^n(1_{P_K})]_{P_J\cap nP_Kn^{-1}} = 1$. Portanto, temos:

$$[St, St] = \sum_{J\subseteq I}\sum_{K\subseteq I}(-1)^{|J|}(-1)^{|K|}|N_{J,K}|.$$

Pela construção de $N_{J,K}$, temos $|N_{J,K}| = |D_{J,K}|$. Dessa forma, obtemos:

$$[St, St] = \sum_{J\subseteq I}\sum_{K\subseteq I}(-1)^{|J|}(-1)^{|K|}|D_{J,K}|.$$

Isso nos permite trabalhar com o caráter ε definido anteriormente. Seguindo exatamente os mesmos passos de antes, porém com 1_{W_J} no lugar de 1_{P_J} e 1_{W_K} no lugar de 1_{P_K}, obtemos $[St, St] = [\varepsilon, \varepsilon]$. Como ε é irredutível, temos $[St, St] = 1$. □

Como St é uma soma alternada de caracteres de G, então os coeficientes na decomposição de St em caracteres irredutíveis certamente são números inteiros. Como $[St, St] = 1$, isso significa que $St = \pm\chi$, para $\chi \in Irr(G)$.

Proposição 4.6. *O caráter de Steinberg satisfaz* $[1_B^G, St] = 1$

Demonstração.

$$\begin{aligned}[1_B^G, St] &= \left[1_B^G, \sum_{J\subseteq I}(-1)^{|J|}1_{P_J}^G\right] \\ &= \sum_{J\subseteq I}(-1)^{|J|}[1_B^G, 1_{P_J}^G] \\ &= \sum_{J\subseteq I}(-1)^{|J|}|N_{\emptyset,J}|.\end{aligned}$$

A última igualdade segue da Proposição 1.21 e do mesmo argumento que foi utilizado na Proposição 4.5. De modo análogo, temos $|N_{\emptyset,J}| = |D_{\emptyset,J}|$ e podemos trabalhar no grupo de Weyl. Assim, $[1_B^G, St] = [1_1^W, \varepsilon]$, onde 1_1 é o caráter principal do grupo trivial. Para observar tal fato, basta substituir nas equações acima 1_B^G por 1_1^W e 1_{P_J} por 1_{W_J}.

A restrição de ε ao grupo trivial coincide com o caráter 1_1. Então, podemos utilizar a reciprocidade de Frobenius para obter $[1_1^W, \varepsilon]_W = [1_1, 1_1]_1 = 1 = [1_B^G, St]$. □

Corolário 4.7. *O caráter de Steinberg é um caráter irredutível de G.*

Demonstração. Já temos $St = \pm\chi$ para $\chi \in Irr(G)$. Se $St = -\chi$, teríamos $[1_B^G, \chi] = -1$, o que contradiz o fato de 1_B^G ser um caráter de G. Assim, temos $St = \chi$. □

É interessante notar que até este ponto, utilizamos apenas as propriedades dadas pelo par-BN para mostrar a irredutibilidade do caráter de Steinberg. Para discutir os valores do caráter de Steinberg, precisamos que o par-BN seja *split* e que G satisfaça as relações de comutadores. De toda forma, apenas com um par-BN que não seja *split* é possível calcular o grau do caráter de Steinberg.

Proposição 4.8. *Se G é um grupo finito com um par-BN, então o grau do caráter de Steinberg é dado por $|B : B \cap n_0 B n_0^{-1}|$, onde $n_0 \in N$ é tal que $\pi(n_0)$ é o elemento de comprimento máximo do grupo de Weyl.*

Demonstração. Ver [8, Teorema 67.10]. □

Este resultado não é muito fácil de utilizar na prática, pois costuma ser complicado calcular a interseção de subgrupos. Isso é um indício que precisamos de um pouco mais estrutura para obter mais informações de St.

4.2 Valores do Caráter de Steinberg

Assumiremos nessa seção que G é um grupo finito com um par-BN *split* em característica p e que satisfaz as relações dos comutadores (veja Definições 3.47 e 3.49). Nessas condições, cada subgrupo parabólico P_J tem uma decomposição de Levi, com $P_J = U_J \rtimes L_J$. Além disso, L_J possui também um par-BN. O resultado seguinte relaciona os caracteres de Steinberg dos subgrupos G e L_J. Uma demonstração desse resultado pode ser encontrada em [6, Proposição 6.3.3].

Proposição 4.9. *Se P_J é um subgrupo parabólico de G, então temos:*

$$(St_G)_{P_J} = St_{L_J}^{P_J}.$$

Uma observação sobre a notação. Neste caso, St_{L_J} denota o caráter de Steinberg de L_J e não a restrição do caráter de Steinberg de G ao grupo L_J.

Nesta seção, discutiremos alguns resultados que permitem calcular os valores do caráter de Steinberg. Isso será útil para discutirmos certas aplicações na Seção 4.3.

Proposição 4.10. *Suponha que $g \in G$ não está em nenhum subgrupo parabólico próprio de G. Então $St(g) = (-1)^{|I|}$, onde I é o conjunto de índices associados aos geradores do grupo de Weyl do par-BN.*

Demonstração. Lembramos que um subgrupo parabólico é qualquer subgrupo conjugado a um P_J, para $J \subseteq I$. Se g não está em nenhum subgrupo parabólico próprio, então nenhum conjugado de g pode estar em P_J para $J \subsetneq I$. Caso contrário, $xgx^{-1} \in P_J$ implica em $g \in x^{-1}P_J x$. Dessa forma, temos $1_{P_J}(g) = \frac{1}{|P_J|} \sum_{\substack{x \in G \\ xgx^{-1} \in P_J}} 1 = 0$, para $J \subsetneq I$. Aqui estamos cometendo um pequeno abuso de notação para indicar que o somatório é vazio. Assim, $St(g) = (-1)^{|I|}$. □

Proposição 4.11. *Se $g \in P_J$ e não é conjugado a nenhum elemento de P_K para $K \subsetneq J$ então:*

(i) $St(g) = 0$, *se g não é conjugado em P_J a algum elemento de L_J.*

(ii) $St(g) = (-1)^{|J|}|C_{U_J}(g)|$, *se $g \in L_J$.*

Demonstração. (i) Como $g \in P_J$ podemos utilizar a Proposição 4.9 para calcular $St(g)$.

$$\begin{aligned} St(g) &= St_{L_J}^{P_J}(g) \\ &= \frac{1}{|L_J|} \sum_{\substack{x \in P_J \\ xgx^{-1} \in L_J}} St_{L_J}(g). \end{aligned} \tag{4.6}$$

Por hipótese, nenhum conjugado de g está em L_J, logo o somatório é vazio e $St(g) = 0$.

(ii) Da mesma forma, como $g \in L_J$ podemos utilizar a Proposição 4.9. Consideremos agora, os $x \in P_J$ tais que $xgx^{-1} \in L_J$. Utilizando a decomposição de Levi, temos $P_J = U_J L_J$, assim se $x \in P_J$, então $x = yz$, para $y \in U_J$ e $z \in L_J$.

Vamos mostrar que $xgx^{-1} \in L_J$ se, e somente se, $y \in C_{U_J}(zgz^{-1})$. Suponha $xgx^{-1} \in L_J$. Temos $y \in C_{U_J}(zgz^{-1})$ se, e somente se, $[y, zgz^{-1}] = 1$. É o que verificaremos agora:

$$\begin{aligned} [y, zgz^{-1}] &= yzgz^{-1}y^{-1}zg^{-1}z^{-1} \\ &= xgx^{-1}zg^{-1}z^{-1}. \qquad\qquad (\text{pois } x = yz) \end{aligned}$$

Como $g, z \in L_J$, temos $(zg^{-1}z^{-1}) \in L_J$. Por hipótese, $xgx^{-1} \in L_J$, logo $[y, zgz^{-1}] \in L_J$. Temos também:

$$[y, zgz^{-1}] = y(zgz^{-1})y^{-1}(zg^{-1}z^{-1}).$$

Como U_J é normal em P_J, temos $(zgz^{-1})y^{-1}(zg^{-1}z^{-1}) \in U_J$. Assim, $[y, zgz^{-1}] \in U_J$. Como $U_J \cap L_J = \{1\}$, temos $[y, zgz^{-1}] = 1$ e $y \in C_{U_J}(zgz^{-1})$.

Reciprocamente, se $y \in C_{U_J}(zgz^{-1})$, temos:

$$\begin{aligned} xgx^{-1} &= y(zgz^{-1})y^{-1} \\ &= zgz^{-1}. \qquad\qquad (\text{pois } y \in C_{U_J}(zgz^{-1}) \ ) \end{aligned}$$

Isso implica $xgx^{-1} \in L_J$, pois $z \in L_J$. Com isso, podemos escrever a Equação (4.6) da seguinte forma:

$$\begin{aligned} St(g) &= \frac{1}{|L_J|} \sum_{z \in L_J} \sum_{y \in C_{U_J}(zgz^{-1})} St_{L_J}(zgz^{-1}) \\ &= \frac{1}{|L_J|} \sum_{z \in L_J} \sum_{y \in C_{U_J}(zgz^{-1})} St_{L_J}(g) \qquad \text{(pois } z, g \in L_J \text{ e } St_{L_J} \text{ é função de classe de } L_J\text{)} \\ &= \frac{1}{|L_J|} \sum_{z \in L_J} |C_{U_J}(zgz^{-1})| St_{L_J}(g) \\ &= |C_{U_J}(g)| St_{L_J}(g). \qquad \text{(} |C_{U_J}(h)| \text{ é função de classe de } U_J\text{)} \end{aligned}$$

Observe que g não está em nenhum subgrupo parabólico próprio de L_J. A razão disso é que os parabólicos de L_J são da forma $P_K \cap L_J$ para $K \subseteq J$ e, por hipótese, g não está em nenhum P_K, para $K \subsetneq J$. Utilizando a Proposição 4.10 obtemos:

$$St(g) = |C_{U_J}(g)|(-1)^{|J|}.$$

□

Corolário 4.12. $St(1) = |G|_p$.

Demonstração. Tomando $g = 1$ e $J = \emptyset$ na Proposição 4.11, obtemos $St(1) = |U|$. Pela Proposição 3.48, U é um p-subgrupo de Sylow de G, portanto, $St(1) = |G|_p$. □

Proposição 4.13. *Se $g \in L_J$ e g não é conjugado em G a nenhum elemento de P_K para $K \subsetneq J$ então:*

(i) $|C_{U_J}(g)| = |C_G(g)|_p$.

(ii) $St_G(g) = (-1)^{|J|}|C_G(g)|_p$.

Demonstração. Tome $\mathscr{K}$ a classe de conjugação de G que contenha g e K a correspondente soma de classe de conjugação. Pela Proposição 1.14, $\omega_{St}(K)$ é um inteiro algébrico.

$$\begin{aligned} \omega_{St}(K) &= \frac{St(g)|\mathscr{K}|}{St(1)} \\ &= \frac{St(g)}{St(1)} \frac{|G|}{|C_G(g)|}. \end{aligned}$$

Usando a Proposição 4.11 e o Corolário 4.12 obtemos:

$$\begin{aligned} \omega_{St}(K) &= \frac{(-1)^{|J|}|C_{U_J}(g)|}{|U|} \frac{|G|}{|C_G(g)|} \\ &= (-1)^{|J|} \frac{|G:U|}{|C_G(g):C_{U_J}(g)|}. \end{aligned}$$

Assim $\omega_{St}(K)$ é um número racional e como é também um inteiro algébrico, deve ser um número inteiro. Isso mostra que $|C_G(g) : C_{U_J}(g)|$ divide $|G : U|$. Como U é um p-subgrupo de Sylow de G, $|U|$ é maior potência de p que divide G assim, $|G : U| = |G|_{p'}$. Em particular, isso implica que $|C_G(g) : C_{U_J}(g)| = \frac{|C_G(g)|}{|C_{U_J}(g)|}$ é coprimo com p. Além disso, $|C_{U_J}(g)|$ é uma potência de p e portanto, $|C_{U_J}(g)| = |C_G(g)|_p$. Isso prova os itens (i) e (ii). □

Proposição 4.14. *Se $g \in G$ e não está em nenhum subgrupo parabólico próprio de G então:*

(i) $|C_G(g)|$ é coprimo com p.

(ii) A ordem de g é coprima com p.

Demonstração. Usando a Proposição 4.13 com $J = I$, temos $U_I = \{1\}$ e $|C_G(g)|_p = 1$. Isso prova o item (i). Como $g \in C_G(g)$, então p não pode dividir a ordem de g e isso prova o item (ii). □

Quando G é um grupo finito do tipo Lie em característica $p > 0$, um elemento $g \in G$ é semisimples se, e somente se, sua ordem for coprima com p. Dizemos que um elemento $g \in G$ é *semisimples regular* se g for semisimples e $|C_G(g)|$ for coprimo com p. Dessa forma, a Proposição 4.14 diz que para acharmos um elemento semisimples regular é suficiente procurar um elemento que não esteja em nenhum subgrupo parabólico próprio.

Proposição 4.15. *Suponha que $g \in P_J$ e g não é conjugado em G a nenhum elemento de P_K para $K \subsetneq J$. Então g é conjugado em P_J a um elemento de L_J se e somente se a ordem de g é coprima com p.*

Demonstração. Se g é conjugado a um elemento $x \in L_J$, então x não pode estar em um subgrupo parabólico próprio de L_J. A razão disso, novamente, é que os parabólicos de L_J são da forma $P_K \cap L_J$. Aplicando o item (ii) da Proposição 4.14 a x com L_J no lugar de G, obtemos que a ordem de x é coprima com p e portanto, a ordem de g é coprima com p.

Reciprocamente, se a ordem de g é coprima com p, devemos mostrar a existência de um $z \in P_J$ tal que $zgz^{-1} \in L_J$. Para mostrar isso, faremos uso do Teorema de Schur-Zassenhaus[1]. Considere o subgrupo $\langle U_J, g\rangle = U_J\langle g\rangle$ gerado por U_J e g. Como U_J é normal em P_J, U_J é normal em $U_J\langle g\rangle$. Além disso, a ordem de g é coprima com p, logo $U_J \cap \langle g\rangle = 1$. Dessa forma, U_J é um subgrupo normal de Hall de $U_J\langle g\rangle$, pois $|U_J|$ é uma potência de p e $|U_J\langle g\rangle : U_J| = |\langle g\rangle|$, que é coprimo com p. Como U_J é um p-grupo, em particular, é solúvel e estamos nas hipóteses do Teorema de Schur-Zassenhaus.

Pelo que foi argumentado anteriormente, fica claro que $\langle g\rangle$ é um complemento de U_J em $U_J\langle g\rangle$. Vamos verificar agora que $\langle U_J, g\rangle \cap L_J$ é um outro complemento de U_J. Como $L_J \cap U_J = 1$, temos $\langle U_J, g\rangle \cap L_J \cap U_J = 1$. Pela decomposição de Levi, $g = xy$ com $x \in L_J$ e $y \in U_J$. Assim $gy^{-1} \in \langle U_J, g\rangle \cap L_J$ e portanto $g \in (\langle U_J, g\rangle \cap L_J)U_J$. Tal fato implica $U_J(\langle U_J, g\rangle \cap L_J) = U_J\langle g\rangle$ e daí $\langle U_J, g\rangle \cap L_J$ é um complemento de U_J.

Assim, pelo Lema de Schur-Zassenhaus, os dois complementos são conjugados e existe $z \in \langle U_J, g\rangle$ tal que $zgz^{-1} \in L_J$. □

[1] *Seja K um subgrupo normal de Hall de G. Se K ou G/K for solúvel, então quaisquer dois complementos de K em G são conjugados* [31, Teorema 7.42]. Um subgrupo de Hall é um subgrupo K de um grupo finito G em que $|K|$ e $|G : K|$ são coprimos.

Utilizando as proposições anteriores podemos mostrar o seguinte teorema, que nos dá os valores do caráter de Steinberg:

Teorema 4.16. *Seja $g \in G$, então:*

(i) $St(g) = 0$, *se a ordem de g for divisível por p.*

(ii) Se a ordem de g for coprima com p, então $St(g) = (-1)^{|J|}|C_G(g)|_p$, onde J é tal que g é conjugado a um elemento de L_J mas não é conjugado a nenhum elemento de P_K para $K \subsetneq J$.

Demonstração. Dado $g \in G$, podemos tomar J tal que existe um x conjugado de g tal que $x \in P_J$ e nenhum conjugado de g está em P_K, para $K \subsetneq J$. Para um tal x temos $St(x) = St(g)$, mas a vantagem de trabalhar com x é que podemos utilizar os resultados anteriores para calcular os valores de St do seguinte modo:

(i) Se a ordem de x, e portanto, a ordem de g, for divisível por p, então x não é conjugado a um elemento de L_J pela Proposição 4.15. Utilizando a Proposição 4.11, obtemos $St(x) = 0$.

(ii) Se a ordem de x for coprima com p, então x é conjugado a um elemento y de L_J, pela Proposição 4.15. Temos $St(x) = St(y)$ e o fato de x não ser conjugado a nenhum elemento de P_K, para $K \subsetneq J$, implica que o mesmo ocorre com y. Logo $St(y) = (-1)^{|J|}|C_G(g)|_p$, pela Proposição 4.13.

□

O item (i) pode também ser obtido a partir de um resultado que surge como consequência do Teorema de Brauer [20, Capítulo 8]. Dado um número primo p, dizemos que um caráter irredutível χ tem *p-defeito zero* se p não divide $|G|/\chi(1)$. Nessas condições, se $\chi \in Irr(G)$ e possui p-defeito zero, então $\chi(g) = 0$ sempre que p divide a ordem de g [20, Teorema 8.17]. O caráter de Steinberg é um exemplo de caráter com p-defeito zero, pois $St(1) = |G|_p$.

4.3 A conjectura de Ore

Em 1951, Oystein Ore conjecturou que todo elemento em um grupo finito simples não-abeliano é um comutador [29]. Em 2010, a conjectura foi provada por Liebeck, O'Brien, Shalev e Tiep [23]. Nesta seção, vamos discutir um resultado de Gow [14] que utiliza o caráter de Steinberg para mostrar que todos os elementos semisimples de um grupo simples finito do tipo Lie em característica p são comutadores. Lembramos que, nessas condições, um elemento g é semisimples se, e somente se, p não divide a ordem de g. Antes, precisamos de algumas considerações preliminares.

4.3.1 Os Caracteres de Brauer e Blocos de Caracteres

Nesta seção faremos alguns comentários sobre os caracteres de Brauer e conceitos relacionados. Maiores detalhes podem ser vistos em [20, Capítulo 15] ou em [28]. Se G é um grupo finito, o estudo das representações sobre corpos de característica 0 é mais simples,

por conta do Teorema de Maschke. No entanto, às vezes é possível extrair informações interessantes a partir de representações sobre corpos de característica p.

Um *caráter de Brauer* é construído a partir dessas representações. Toma-se R o anel dos inteiros algébricos e escolhe-se um ideal maximal M de R tal que M contenha Rp. Assim, $F = R/M$ é um corpo de característica p que possui boas propriedades: é algebricamente fechado e é uma extensão algébrica sobre $\mathbb{F}_p$.

Considere agora o conjunto $U = \{a \in \mathbb{C} \mid \text{existe } m \text{ tal que } a^m = 1 \text{ e } p \nmid m\}$. Evidentemente, U está contido em R, mas o fato interessante é que se tomarmos o homomorfismo canônico π associado a R/M e restringirmos a U, obtemos um isomorfismo de grupos entre U e o grupo multiplicativo do corpo F, denotado por $F^\times$.

Se tomarmos uma representação de G sobre F, isto é, um homomorfismo ρ entre G e algum $GL_n(F)$, podemos considerar o caráter associado χ. Para todo g, como $\rho(g)$ é uma matriz invertível, seus autovalores pertencem a $F^\times$ e, como π restrito a U é um isomorfismo, podemos assumir que os autovalores são da forma $\pi(\xi_1), \pi(\xi_2), \ldots, \pi(\xi_n)$, para $\xi_i \in U$. O *caráter de Brauer* φ associado à ρ é uma função de que leva $g \in G$, tal que a $p \nmid o(g)$, em $\sum_{i=1}^{n} \xi_i$, onde $\pi(\xi_i)$ são os autovalores de $\rho(g)$. Note que estamos incluindo as repetições dos autovalores, de modo que $\varphi(1) = n$, onde n é o grau da representação.

Para cada primo p podemos construir os caracteres de Brauer irredutíveis de G. O problema é que o caráter depende da escolha do ideal maximal M. De todo jeito, algumas propriedades não dependem de M. Por exemplo, se p não divide a ordem de G, o conjunto de caracteres irredutíveis de Brauer $IBr(G)$ coincide com $Irr(G)$, para qualquer escolha de M.

Note que um caráter de Brauer só está definido sobre os elementos de G que são p-regulares, isto é, p não divide a ordem deles. Porém, isso é o suficiente para reconstruir o caráter χ. Mais precisamente, se G é um grupo finito e p é um primo qualquer, todo elemento g pode ser escrito como $g = g_p g_{p'} = g_{p'} g_p$, com $g_{p'}, g_p \in \langle g \rangle$, tais que a ordem de g_p é uma potência de p e p não divide a ordem de $g_{p'}$. Uma demonstração dessa proposição está em [20, Lema 8.18]. Nessas condições, temos $\chi(g) = \chi(g_{p'})$ e $\chi(g) = \pi(\varphi(g_{p'}))$, onde π é o homomorfismo canônico discutido anteriormente. Note que em grupo finito do tipo Lie em característica p, um elemento ser p-regular é a mesma coisa que ser semisimples.

Pode-se mostrar que se ψ é um caráter complexo de G, a restrição aos elementos p-regulares de G, denotada por $\hat{\psi}$, é um caráter de Brauer para qualquer escolha de ideal maximal M. Não é verdade, porém, que se ψ é irredutível, então $\hat{\psi}$ também é irredutível como caráter de Brauer. No entanto, tal qual no caso complexo, os caracteres de Brauer irredutíveis formam uma base para as funções de classe de G em $\mathbb{C}$, considerando apenas as classes de conjugação de elementos p-regulares. Assim, pode-se construir uma matriz $|Irr(G)| \times |IBr(G)|$ que indica os coeficientes da decomposição de $\hat{\psi}$ em caracteres de Brauer irredutíveis. E, a menos de permutação de linhas e colunas, essa matriz não depende da escolha de M. Costuma-se escrever $\hat{\psi} = \sum_{\varphi \in IBr(G)} d_{\psi\varphi}\varphi$ e os $d_{\psi\varphi}$ são chamados de *números de decomposição*.

Com isso, agora podemos discutir os p-blocos de G. Dados $\chi, \psi \in Irr(G)$, podemos considerar os caracteres centrais ω_χ e ω_ψ (veja a Definição 1.13). Além disso, lembremos que as somas de classes de conjugação K_i formam uma base para $Z(\mathbb{C}[G])$. Nessas

condições, podemos definir a seguinte relação de equivalência:

$$\chi \sim \psi, \text{ se, e somente se, } \pi(\omega_\chi(K_i)) = \pi(\omega_\psi(K_i)),$$

para todas as somas de classes de conjugação K_i. Nesse caso, escreveremos $\omega_\chi(K_i) \equiv \omega_\psi(K_i) \mod M$.

Dessa forma B é um *p-bloco* de G se B é um subconjunto de $Irr(G) \cup IBr(G)$ com as seguintes propriedades:

- $B \cap Irr(G)$ é uma classe de equivalência sob a relação $\sim$.
- $B \cap IBr(G) = \{\varphi \in IBr(G) \mid d_{\chi\varphi} \neq 0 \text{ para algum } \chi \in B \cap Irr(G)\}$.

Pode-se demonstrar também que relação $\sim$ não depende do ideal maximal M escolhido [20, Teorema 15.18]. Além disso, chama-se de *bloco principal* o bloco que contém o caráter principal do grupo. Com isso, podemos enunciar um importante resultado devido a Humphreys:

Teorema 4.17 (Humphreys)**.** *Se G é um grupo finito simples do tipo Lie em característica p, então G possui apenas dois p-blocos: o bloco principal e um bloco cujo único membro é o caráter de Steinberg St.*

Demonstração. Veja [18, Seções 8.3 e 8.5] ou [15]. □

4.3.2 O Teorema de Gow

Primeiro, precisamos de alguns resultados preliminares. A partir dessa seção, M é um ideal maximal contendo Rp, como definido na Seção 4.3.1, e G é um grupo finito simples do tipo Lie em característica p. Seja χ_i um caráter irredutível complexo de G, denotaremos o caráter central associado a χ_i por ω_i. Além disso, escreveremos ω_1 para o caráter central do caráter principal e ω_{St} para o caráter central do caráter de Steinberg. Note que o caráter central foi definido para as somas de classes de conjugação, mas se $g \in G$ e g está na classe de conjugação $\mathscr{K}_i$, escreveremos simplesmente $\omega_i(g)$ para indicar $\omega_i(K_i)$ (veja seção 1.3).

Vamos discutir um pouco a noção de *defeito* de um p-bloco. Seja p^e a maior potência de p que divide a ordem de G. Dizemos que um p-bloco tem defeito d se p^{e-d} é maior potência de p que divide a dimensão de todos os caracteres $\chi \in Irr(G)$ que estão no bloco. O Teorema 4.17 diz que, no caso em que G é um grupo finito simples do tipo Lie, então G tem exatamente dois blocos. Um deles contém apenas o caráter de Steinberg, que satisfaz $St(1) = |G|_p$ e assim esse bloco tem defeito 0. O outro bloco contém o caráter principal, então possui defeito máximo.

Também podemos definir uma noção de defeito para classes de conjugação de G. Dizemos que uma classe de conjugação $\mathscr{K}$ possui defeito d se p^d é maior potência de p que divide $|C_G(x)|$, para $x \in \mathscr{K}$. O interessante é que as duas noções de defeito estão ligadas e é possível mostrar que o número de blocos que possuem defeito máximo é igual ao número de classes de conjugação de elementos p-regulares que possuem defeito máximo (veja [18, Seção 8.2]).

Dessa forma, o fato de G possuir apenas um único bloco de defeito máximo implica G possuir uma única classe de conjugação com defeito máximo, que é a classe de conjugação

da identidade. Isso implica que, com a exceção da identidade, nenhum centralizador de um elemento semisimples (p-regular) contém um p-subgrupo de Sylow de G. Tal fato será utilizado na proposição seguinte.

Proposição 4.18. *Seja g um elemento semisimples diferente da identidade e seja $\mathscr{K}_i$ a classe de conjugação que contém g. Então $\omega_j(g) \equiv 0 \mod p$, para todos os $\chi_j \neq St$.*

Demonstração. Como $\omega_j(g) = \frac{\chi_j(g)|\mathscr{K}_i|}{\chi_j(1)}$, temos $\omega_1(g) = |\mathscr{K}_i|$. Além disso, para todos os caracteres centrais ω_j diferentes de ω_{St}, temos $\omega_j(g) \equiv \omega_1(g) \mod M$, pelo Teorema 4.17. Assim, $\omega_j(g) \equiv |\mathscr{K}_i| \mod M$. Se mostrarmos que p divide $|\mathscr{K}_i|$ mostraremos $\omega_j(g) \equiv 0 \mod M$, pois M contém $\mathbb{Z}p$ e, portanto, $\omega_j(g) \equiv 0 \mod p$. É isso que faremos.

Como g é semisimples, p não divide a ordem de g. Se além disso, ocorrer que p não divide $|\mathscr{K}_i|$, como $|G| = |\mathscr{K}_i||C_G(g)|$, isso força com que p divida $|C_G(g)|$. Mais ainda, todas as potências de p que dividem G, tem que dividir $|C_G(g)|$. Portanto, $|C_G(g)|$ contém um p-subgrupo de Sylow de G. Mas isso não pode ocorrer pelas observações que fizemos antes da proposição. Portanto p divide $|\mathscr{K}_i|$ e o resultado segue. □

Agora, vamos determinar uma expressão conveniente para o caráter central ω_{St}.

Proposição 4.19. *Seja g um elemento semisimples diferente da identidade, então*

$$\omega_{St}(g) = \pm|G : C_G(g)|_{p'}.$$

Demonstração. Temos $St(g) = \pm|C_G(g)|_p$ e $St(1) = |G|_p$. Assim:

$$\omega_{St}(g) = \pm\frac{|\mathscr{K}_i||C_G(g)|_p}{|G|_p} = \pm\frac{|G||C_G(g)|_p}{|C_G(g)||G|_p}.$$

Agora, como $|G|_p$ é a p-parte de $|G|$, então $\frac{|G|}{|G|_p} = |G|_{p'}$ e, de modo análogo, temos $\frac{|C_G(g)|_p}{|C_G(g)|} = \frac{1}{|C_G(g)|_{p'}}$, então $\omega_{St}(g) = \pm\frac{|G|_{p'}}{|C_G(g)|_{p'}} = \pm|G : C_G(g)|_{p'}$. □

Agora, vamos escrever o caráter Λ (introduzido na Proposição 1.17), em função dos caracteres centrais:

$$\begin{aligned}\Lambda(g) &= \sum_{\chi\in Irr(G)} \frac{|G|\chi(g)}{\chi(1)} \\ &= \sum_{\chi\in Irr(G)} \frac{|C_G(g)||\mathscr{K}_i|\chi(g)}{\chi(1)} \\ &= |C_G(g)| \sum_{\chi\in Irr(G)} \omega_\chi(g). \end{aligned} \tag{4.7}$$

Com isso, estamos em condições de demonstrar o seguinte teorema:

Teorema 4.20. *[14] Seja G um grupo finito simples do tipo Lie de característica p e seja g um elemento semisimples diferente da identidade em G. Então, vale:*

$$\frac{\Lambda(g)}{|C_G(g)|_p} \equiv \pm|G|_{p'} \mod p.$$

Em particular, $\Lambda(g)$ é não-nulo e g é um comutador em G.

Demonstração. Usando a Equação (4.7), temos $\frac{\Lambda(g)}{|C_G(g)|} = \omega_{St} + \sum_{i=1}^{r-1} \omega_i(g)$. Tomando essa expressão módulo p, como $\omega_i(g) \equiv 0 \mod p$, se $\omega_i \neq \omega_{St}$, obtemos:

$$\begin{aligned}\frac{\Lambda(g)}{|C_G(g)|} &\equiv \omega_{St}(g) \mod p \\ &\equiv |G : C_G(g)|_{p'} \mod p.\end{aligned}$$

Se multiplicarmos a congruência dos dois lados por $|C_G(g)|_{p'}$, como $|G : C_G(g)|_{p'} = \frac{|G|_{p'}}{|C_G(g)|_{p'}}$, obtemos o resultado desejado. Além disso, p não divide $|G|_{p'}$, então $\Lambda(g)$ não pode ser zero. Em particular, g é um comutador.

□

Lembremos que um elemento semisimples $h \in G$ é *regular* se $|C_G(h)|$ é coprimo com p. Nessas circunstâncias obteremos também o seguinte resultado.

Teorema 4.21. *Se g é um elemento semisimples e $\mathscr{K}_i$ e $\mathscr{K}_j$ são classes de conjugação de elementos semisimples regulares de G, então g pode ser expresso como um produto xy, com $x \in \mathscr{K}_i$ e $y \in \mathscr{K}_j$.*

Demonstração. Note que $g \in \mathscr{K}_v$ é expresso como um produto de elementos da classe $\mathscr{K}_i$ e da classe $\mathscr{K}_j$ se, e somente se, a constante de estrutura a_{ijv} é diferente de 0. Da Proposição 1.15, temos a_{ijv} diferente de 0 se, e somente se, $\sum_{\chi \in Irr(G)} \frac{\chi(x_i)\chi(x_j)\overline{\chi(g)}}{\chi(1)} \neq 0$, onde $x_i \in \mathscr{K}_i$ e $x_j \in \mathscr{K}_j$. Escrevendo essa expressão em função dos r caracteres centrais de G, temos:

$$\sum_{\chi \in Irr(G)} \frac{\chi(x_i)\chi(x_j)\overline{\chi(g)}}{\chi(1)} = \sum_{l=1}^{r} \frac{\chi_l(x_i)\chi_l(x_j)\overline{\omega_l(g)}}{|\mathscr{K}_v|}. \tag{4.8}$$

Isso implica a_{ijv} diferente de 0 se, e somente se,

$$\sum_{l=1}^{r} \chi_l(x_i)\chi_l(x_j)\overline{\omega_l(g)} \neq 0. \tag{4.9}$$

Observando que $\overline{\omega_l(g)} = \omega_l(g^{-1})$ e que g^{-1} é também um elemento semisimples, pela Proposição 4.18, temos $\overline{\omega_l(g)} \equiv 0 \mod p$, para todos os ω_l que não são ω_{St}. Então tomando módulo p a Equação (4.9), temos:

$$\sum_{i=1}^{r} \chi(x_i)\chi(x_j)\overline{\omega_i(g)} \equiv St(x_i)St(x_j)\overline{\omega_{St}(g)} \mod p.$$

Como x_i e x_j são elementos semisimples regulares, temos $St(x_i) = \pm 1$ e $St(x_j) = \pm 1$. Pela Proposição 4.19, $\omega_{St}(g) = \overline{\omega_{St}(g)} = \pm|G : C_G(g)|_{p'}$, que é coprimo com p. Então a

expressão acima não pode ser congruente a 0 módulo p. Em particular, a_{ijv} não é zero, como queríamos. □

Note que se $\mathscr{K}_i$ é uma classe de elementos semisimples regulares, então $\mathscr{K}_{i'}$, a classe de conjugação que contém os inversos de $\mathscr{K}_i$, também é composta de elementos semisimples regulares. Assim, o seguinte corolário:

Corolário 4.22. *Se G é um grupo finito simples do tipo Lie em característica p e g é um elemento semisimples, então g é um comutador da forma $[x, y]$, com $x \in \mathscr{K}_i$ e $y \in G$, onde $\mathscr{K}_i$ é uma classe de conjugação de elementos semisimples regulares.*

Demonstração. Pelo Teorema 4.21, g é um produto xy, com $x \in \mathscr{K}_i$ e $y \in \mathscr{K}_{i'}$, portanto g é um comutador da forma $[hxh^{-1}, hyh^{-1}]$, para $x \in \mathscr{K}_i$ e $y, h \in G$ (veja Proposição 1.16 e as observações seguintes). □

4.3.3 O grupo de Tits

Neste trabalho, não tratamos do grupo de Tits ${}^2F_4(2)'$. Alguns autores, consideram o grupo de Tits como sendo o 27° grupo esporádico, enquanto outros preferem tratá-lo como um grupo do tipo Lie. Para nós, é melhor considerar a primeira opção e nessa seção vamos explicar a razão para tal.

O grupo de Ree ${}^2F_4(2)$ é um grupo finito do tipo Lie excepcional que não é simples, mas possui o grupo de Tits ${}^2F_4(2)'$ como um subgrupo normal de índice 2. Ao contrário dos outros grupos finitos simples do tipo Lie, o grupo de Tits não possui um par-BN *split* que satisfaz as relações dos comutadores. Tal fato pode ser checado examinando a tabela de caracteres do grupo de Tits e verificando que ele não possui um caráter de Steinberg. Faremos isso com auxílio do programa GAP [12]. O código abaixo exibe a tabela de caracteres do grupo de Tits.

```
gap> t := CharacterTable("2F4(2)'");
CharacterTable( "2F4(2)'" )
gap> Display(t);
          1a  2a  2b 3a 4a 4b 4c 5a 6a 8a 8b 8c 8d 10a 12a 12b 13a 13b 16a 16b 16c 16d
     2P   1a  1a  1a 3a 2b 2a 2b 5a 3a 4b 4b 4c 4c  5a  6a  6a 13b 13a  8a  8b  8a  8b
     3P   1a  2a  2b 1a 4a 4b 4c 5a 2b 8b 8a 8c 8d 10a  4a  4a 13a 13b 16d 16c 16b 16a
     5P   1a  2a  2b 3a 4a 4b 4c 1a 6a 8a 8b 8c 8d  2a 12b 12a 13b 13a 16c 16d 16a 16b
    13P   1a  2a  2b 3a 4a 4b 4c 5a 6a 8a 8b 8c 8d 10a 12a 12b  1a  1a 16c 16d 16a 16b

X.1        1   1   1  1  1  1  1  1  1  1  1  1  1   1   1   1   1   1   1   1   1   1
X.2       26  -6   2 -1 -2 -2  2  1 -1  .  .  .  .  -1   1   1   .   .   D  -D  -D   D
X.3       26  -6   2 -1 -2 -2  2  1 -1  .  .  .  .  -1   1   1   .   .  -D   D   D  -D
X.4       27  -5   3  .  3 -1 -1  2  .  A /A -1 -1   .   .   .   1   1   E  -E   E  -E
X.5       27  -5   3  .  3 -1 -1  2  . /A  A -1 -1   .   .   .   1   1  -E   E  -E   E
X.6       78  14  -2 -3  2 -2  2  3  1  2  2  .  .  -1  -1  -1   .   .   .   .   .   .
X.7      300 -20  -4  3 -4  4  4  . -1  .  .  .  .   .  -1  -1   1   1   .   .   .   .
X.8      325   5 -11  1  1  5  1  .  1  1  1 -1 -1   .   1   1   .   .  -1  -1  -1  -1
X.9      351  31  15  .  3 -1  3  1  . -1 -1  1  1   1   .   .   .   .  -1  -1  -1  -1
X.10     351  -1  -9  .  3  3 -1  1  .  A /A  1  1  -1   .   .   .   .  -E   E  -E   E
X.11     351  -1  -9  .  3  3 -1  1  . /A  A  1  1  -1   .   .   .   .   E  -E   E  -E
X.12     624 -16  16  3  .  .  . -1  1  .  .  .  .  -1   B  -B   .   .   .   .   .   .
X.13     624 -16  16  3  .  .  . -1  1  .  .  .  .  -1  -B   B   .   .   .   .   .   .
X.14     650  10  10  2  6  2 -2  . -2  2  2  .  .   .   .   .   .   .   .   .   .   .
X.15     675  35   3  .  3  3  3  .  . -1 -1 -1 -1   .   .   .  -1  -1   1   1   1   1
X.16     702  30   6  . -6  2 -2  2  .  .  .  .  .   .   .   .   .   .   F   F  -F  -F
X.17     702  30   6  . -6  2 -2  2  .  .  .  .  .   .   .   .   .   .  -F  -F   F   F
X.18    1300  20 -12  4  . -4  .  .  .  .  .  2 -2   .   .   .   .   .   .   .   .   .
X.19    1300  20 -12  4  . -4  .  .  .  .  . -2  2   .   .   .   .   .   .   .   .   .
X.20    1728 -64   .  .  .  .  .  3  .  .  .  .  .   1   .   .  -1  -1   .   .   .   .
```

```
X.21    2048   .   . -4  .  .  . -2  .  .  .  .  .  .  .  .  C  *C  .  .  .  .
X.22    2048   .   . -4  .  .  . -2  .  .  .  .  .  .  .  . *C   C  .  .  .  .
```

O grupo de Tits tem ordem $2^{11}\,3^3\,5^2\,13^2$. Assim, se tivesse um caráter de Steinberg, tal caráter deveria ter grau 2048. Porém, os únicos caracteres de grau 2048 são `X.21` e `X.22`. Nenhum deles pode ser o caráter de Steinberg pois eles assumem valores complexos nas classes de conjugação `13a` e `13b`.

De todo modo, podemos verificar a conjectura de Ore para o grupo de Tits. Pelo Corolário 1.18, basta verificar se $\sum_{\chi\in Irr({}^2F_4(2)')} \frac{\chi(g)}{\chi(1)}$ é maior que 0, para todo $g \in {}^2F_4(2)'$. Isso pode ser feito da seguinte forma:

```
gap> t := CharacterTable("2F4(2)'");;
gap> ForAll( Sum(Irr(t), x -> x/DegreeOfCharacter(x)), x -> x > 0);
true
```

Naturalmente, a mesma coisa pode ser feita para os 26 grupos esporádicos e para qualquer grupo simples cuja tabela de caracteres seja conhecida pelo GAP.

4.4 Outras Aplicações

Nessa seção discutiremos outras duas aplicações do caráter de Steinberg. A primeira é uma generalização proposta por Walter Feit [10]. A segunda nos permite contar o número de elementos unipotentes do grupo G^F, onde G é um grupo linear algébrico conexo e redutivo e F é um endomorfismo de Steinberg de G.

4.4.1 Caracteres p-Steinberg

Em um grupo finito G, a existência de um caráter irredutível que se comporta como o caráter de Steinberg é uma restrição muito forte. Seja p um primo qualquer e $\chi \in Irr(G)$, dizemos que χ é um caráter p-Steinberg de G se $\chi(g) = \pm|C_G(g)|_p$, para todo $g \in G$ tal que p não divide a ordem de g. Isso implica $\chi(1) = |G|_p$. Assim, χ deve ser um caráter de p-defeito zero. Como consequência do Teorema de Brauer [20, Teorema 8.17], temos $\chi(g) = 0$, se p divide a ordem de g .

Em [10], Walter Feit questionou se todo grupo finito simples G cuja ordem é divisível por p e que possui um caráter p-Steinberg, é, em verdade, um grupo finito simples do tipo Lie em característica p. Nesse mesmo artigo, Feit sugeriu que, com a classificação dos grupos finitos simples, seria possível atacar tal questão. Feit também mostrou o seguinte resultado [10, Teorema A]:

Teorema 4.23. *Seja G um grupo finito que possua um caráter p-Steinberg χ, então:*

1. *Se $p = 2$, então χ é o único caráter p-Steinberg de G.*
2. *Se $p \neq 2$, então a função que leva λ em $\lambda\chi$ é uma bijeção entre o conjunto do caracteres lineares que assumem valores racionais em G e os caracteres p-Steinberg de G.*
3. *Se $p \neq 2$, G tem um único caráter p-Steinberg ψ que é* unimodular*, isto é, se ρ é uma representação associada a ψ, temos* $\det(\rho(g)) = 1$*, para todo $g \in G$.*

Dizemos que um $\chi \in Irr(G)$ é um *caráter p-Steinberg básico* quando χ é um caráter p-Steinberg unimodular e $p \neq 2$. Quando $p = 2$, χ é básico se for o único caráter p-Steinberg. Assim, pelo Teorema 4.23, todo grupo finito tem no máximo um único p-caráter de Steinberg básico.

Quando p não divide a ordem de G, a situação não é muito interessante, pois o caráter p-Steinberg básico de G é o caráter principal. Se p divide a ordem de G e G é simples, o resultado anterior implica que existe no máximo um único caráter p-Steinberg de G. De fato, o número de caracteres lineares em um grupo finito G é igual ao índice do subgrupo derivado G' em G. Como G é simples, temos $G' = G$ ou G abeliano. No primeiro caso, G possui um único caráter linear e, pelo item (ii) do Teorema 4.23, concluímos que G tem no máximo um único caráter p-Steinberg. No segundo caso, G não pode ter um caráter p-Steinberg, pois um tal caráter irredutível não seria linear.

Em [38], Tiep mostrou que o questionamento de Feit admite uma resposta positiva e mostrou que, de fato, todo grupo finito simples que admite um caráter p-Steinberg tal que p divide $|G|$ é um grupo finito do tipo Lie em característica p e este caráter deve ser St.

4.4.2 O número de elementos unipotentes em G^F

Para encerrar esse texto, vamos ver como o caráter de Steinberg pode ser utilizado para contar o número de elementos unipotentes de G^F sob a hipótese de G ser conexo e redutivo. Esse é um argumento desenvolvido originalmente pelo próprio Robert Steinberg em [36, Capítulo 15]. O mesmo argumento, porém, em um texto mais recente, pode ser visto em [6, Seção 6.6].

Para prosseguir, precisamos de alguns fatos técnicos.

Proposição 4.24. *Seja G um grupo linear algébrico conexo e $s \in G$ um elemento semisimples. Então todos os elementos unipotentes de $C_G(s)$ estão em $C_G(s)^0$. Se G for redutivo, então $C_G(s)^0$ também deve ser.*

Demonstração. Seja u um elemento unipotente de $C_G(s)$. Pela decomposição de Jordan e, como u comuta com s, temos que, para $x = us$, u e s são, respectivamente, as partes unipotente e semisimples de x. Como G é conexo, G é a união dos seus subgrupos de Borel e, assim, podemos considerar $x \in B$.

Como us é a decomposição de Jordan de x, isso implica $u, s \in B$. Dessa forma, $u \in C_B(s)$. Agora, B é um subgrupo linear algébrico conexo e solúvel, isso implica $C_B(s)$ conexo. Em [16, Seção 19.4], mostra-se que se G é um grupo linear algébrico conexo e solúvel e H um subgrupo que consiste apenas de elementos semisimples, então $C_G(H)$ é conexo. No nosso caso, se tomarmos H como sendo o subgrupo gerado por s, teremos $C_B(s) = C_B(H)$. Portanto, $C_B(s)$ deve estar na componente conexa $C_G(s)^0$ de $C_G(s)$. Isso mostra a primeira parte da proposição.

Para a segunda parte da proposição veja [4, Proposição 13.19]. Esse fato também é mencionado em [6], no parágrafo anterior à Seção 6.6. □

Agora, observamos que se G é conexo e redutivo de dimensão 1, então ele deve ser um toro. Isso decorre de um resultado que diz que todo grupo linear algébrico conexo de dimensão 1 é isomorfo a G_a ou G_m [16, Seções 20 e 20.5]. Como G é redutivo, G não pode ser composto apenas de elementos unipotentes, então devemos ter $G \cong G_m$.

Finalmente, se G possui um endomorfismo de Steinberg F e $g \in G^F$, então $C_G(g)$ é F-estável. De fato, se $y \in C_G(g)$, temos $F(y)gF(y)^{-1} = F(y)F(g)F(y^{-1})$, pois $F(g) = g$. Como $F(y)F(g)F(y^{-1}) = F(ygy^{-1}) = g$, temos $F(y) \in C_G(g)$.

Lembramos também que se G é um grupo linear algébrico, denotamos por G_u e G_s os subconjuntos de elementos unipotente e semisimples, respectivamente. Munido desses fatos, estamos em condições de mostrar o seguinte teorema:

Teorema 4.25. *Seja G um grupo linear algébrico conexo, redutivo e equipado com um endomorfismo de Steinberg F. Então o número de elementos unipotentes de G^F é q^2, onde q é a ordem de um p-subgrupo de Sylow de G^F.*

Demonstração. Em outras palavras, o teorema afirma a igualdade $|(G^F)_u| = (|G^F|_p)^2$. Vamos mostrar tal resultado por indução sobre a dimensão de G. Se a dimensão de G é 1, então G é um toro. Assim, o único elemento unipotente de G é o 1 e p não divide a ordem de G^F. Portanto, o resultado é válido trivialmente. Suponha, então, $\dim G > 1$.

O caráter de Steinberg de G^F satisfaz $[St, St] = 1$, isto é:

$$|G^F| = \sum_{g \in G^F} St(g)^2.$$

Se g não é semisimples, então $St(g) = 0$. Quando $s \in (G^F)_s$, temos $St(s) = \pm|C_{G^F}(s)|_p$. Para não carregar muito a notação, escreveremos apenas $C(s)$ ao invés de $C_{G^F}(s)$. Temos, então:

$$|G^F| = \sum_{s \in (G^F)_s} (|C(s)|_p)^2. \tag{4.10}$$

Uma segunda forma de calcular $|G^F|$ é considerar a decomposição de Jordan. Lembramos que se $g \in G^F$, então g pode ser escrito de forma única como $g = us = su$, onde $u, s \in G$, u é unipotente e s é semisimples. Assim, fixando um elemento semisimples $s \in (G^F)_s$ e considerando o produto su para $u \in C(s)_u$, obtemos elementos diferentes de G. Logo

$$|G^F| = \sum_{s \in (G^F)_s} |C(s)_u|. \tag{4.11}$$

Juntando as Equações (4.10) e (4.11), temos:

$$\sum_{s \in (G^F)_s} |C(s)_u| = \sum_{s \in (G^F)_s} (|C(s)|_p)^2. \tag{4.12}$$

Observe que se $s \in Z(G^F)$, então $C(s) = G^F$ e $|C(s)_u|$ é precisamente o número de elemento unipotentes de G. Então vamos analisar o que acontece quando $s \notin Z(G^F)$. Nesse caso, devemos ter $\dim C_G(s)^0 < \dim G$. Caso contrário, como G é conexo, isso implica $C_G(s) = G$ e $s \in Z(G^F)$. Agora, $C_G(s)^0$ é um subgrupo fechado, conexo, redutivo e F-estável. Pela Proposição 4.24, $C_G(s)^0$ contém todos os elementos unipotentes de $C_G(s)$.

Por indução, temos $|((C_G(s)^0)^F)_u| = (|(C_G(s)^0)^F|_p)^2$. Vamos analisar essa expressão complicada para tentar simplificá-la. Temos $((C_G(s)^0)^F)_u = C(s)_u$. Afinal, se $u \in C(s)_u$, então $u \in C_G(s)_u$. Como $C_G(s)^0$ contém todos os elementos unipotentes de $C_G(s)$, então

$u \in C_G(s)^0$ e é um elemento que é fixado por F, logo $u \in (C_G(s)^0)^F)_u$. Reciprocamente, se $u \in ((C_G(s)^0)^F)_u$, u é um elemento de $C_G(s)$ que centraliza s e é fixado por F, assim $u \in G^F$ e $u \in C(s)$.

Agora, temos ainda $|(C_G(s)^0)^F|_p = |C(s)|_p$. De fato, $C_G(s)^F = C(s)$ e $(C_G(s)^0)^F$ contém $C(s)_u$, portanto, contém um p-subgrupo de Sylow de $C(s)$.

Vamos resumir o que temos até agora. Se $s \notin Z(G^F)$, então $\dim C_G(s)^0 < \dim G$ e isso implica que podemos usar a hipótese de indução para $C_G(s)^0$. Usando os fatos discutidos, isso significa $|C(s)_u| = (|C(s)|_p)^2$, sempre que $s \notin Z(G^F)$. Dessa forma, os termos que correspondem aos elementos que não estão no centro de G^F podem ser cancelados nos dois lados da Equação (4.12):

$$\sum_{s \in Z(G^F)} |C(s)_u| = \sum_{s \in Z(G^F)} (|C(s)|_p)^2.$$

Agora, se $s \in Z(G^F)$, temos $C(s) = G^F$ e $C(s)_u = (G^F)_u$. Portanto,

$$\sum_{s \in Z(G^F)} |(G^F)_u| = \sum_{s \in Z(G^F)} (|G^F|_p)^2.$$

Dividindo os dois lados da equação por $|Z(G^F)|$, obtemos o resultado desejado.

□

É interessante notar que o teorema anterior poderia ter sido mostrado com qualquer caráter p-Steinberg de G^F, pois a única propriedade que usamos de St é o fato de $St(g) = \pm|C_{G^F}(g)|_p$, se g for semisimples. Como já discutimos anteriormente, isso é suficiente para garantir $St(g) = 0$, caso g não seja semisimples.

4.5 Considerações Finais

O objetivo deste trabalho foi estudar o caráter de Steinberg e algumas aplicações. O passo seguinte é estudar outras representações que surgem no estudo dos grupos finitos do tipo Lie. Caso o leitor esteja interessado, as referências [6, 9] são bons textos para esse assunto. Para entendê-los é preciso aprofundar um pouco mais na teoria de Grupos Lineares Algébricos. Dessa forma, vale a pena dar uma olhada em alguns aspectos que nós deixamos de lado: a classificação dos grupos semisimples, caracteres e cocaracteres de grupos lineares algébricos, a álgebra de Lie associada a um grupo linear algébrico e outros. Tais assuntos podem ser estudados, por exemplo, em [4, 16, 24, 33].

Referências

[1] Peter Abramenko and Kenneth S. Brown. *Buildings: Theory and Applications*. Springer, New York, 2008. 35

[2] Jonathan L. Alperin and Rowen B. Bell. *Groups and Representations*. Springer, New York, 1995. 35

[3] Michael Aschbacher. *Finite Group Theory*. Cambridge University Press, Cambridge, 2nd edition, 2000. 33, 40

[4] Armand Borel. *Linear Algebraic Groups*. Springer, New York, 2nd edition, 1991. 41, 53, 83, 85

[5] Roger W. Carter. *Simple Groups of Lie Type*. Wiley & Sons, New York, 1989. 15, 18, 23, 29, 33, 40, 41

[6] Roger W. Carter. *Finite groups of Lie type: conjugacy classes and complex characters*. Wiley & Sons, New York, 1993. 15, 64, 65, 66, 67, 72, 83, 85

[7] Charles W. Curtis. The Steinberg character of a finite group with a (B, N)-pair. *Journal of Algebra*, 4:433–441, 1966. 67

[8] Charles W. Curtis and Irving Reiner. *Methods of Representation Theory: With Applications to Finite Groups and Orders, Volume 2*. Wiley & Sons, New York, 1987. 36, 64, 65, 66, 67, 72

[9] François Digne and Jean Michel. *Representations of Finite Groups of Lie Type*. Cambridge University Press, Cambridge, 1991. 58, 60, 62, 63, 85

[10] Walter Feit. Extending steinberg characters. Elman, Richard S. (ed.) et al., Linear algebraic groups and their representations. Conference, March 25-28, 1992, Los Angeles, CA, USA. Providence, RI: American Mathematical Society. Contemp. Math. 153, 1-9 (1993)., 1993. 82

[11] Ferdinand G. Frobenius. Über gruppencharaktere. In *Gesammelte Abhandlungen*, volume 3, pages 1–37. Springer, 1968. Reprinted from Sitzber. Preuss. Akad. Wiss, 1896. 10

[12] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4.12*, 2008. 81

[13] Meinolf Geck and Götz Pfeiffer. *Characters of Finite Coxeter Groups and Iwahori-Hecke Algebras*. Oxford University Press, New York, 2000. 15, 18, 23, 26

[14] Rod Gow. Commutators in finite simple groups of lie type. *Bulletin of the London Mathematical Society*, 32(03):311–315, 2000. 2, 76, 79

[15] James E. Humphreys. Defect groups for finite groups of lie type. *Mathematische Zeitschrift*, 119(2):149–152, 1971. 78

[16] James E. Humphreys. *Linear Algebraic Groups*. Springer, New York, 1975. 41, 51, 53, 54, 55, 56, 66, 83, 85

[17] James E. Humphreys. *Reflection Groups and Coxeter Groups*. Cambridge University Press, Cambridge, 1992. 15, 29, 39

[18] James E. Humphreys. *Modular Representations of Finite Groups of Lie Type*. Cambridge University Press, Cambridge, 2006. 78

[19] Bertram Huppert. *Character Theory of Finite Groups*. Walter de Gruyter, Berlin, 1998. 13

[20] Irving M. Isaacs. *Character Theory of Finite Groups*. Academic Press, New York, 1976. 4, 8, 13, 54, 76, 77, 78, 82

[21] Peter B. Kleidman and Martin W. Liebeck. *The Subgroup Structure of the Finite Classical Groups*. Cambridge University Press, Cambridge, 1990. 33

[22] Matjaž Konvalinka, Götz Pfeiffer, and Claas E. Röver. A note on element centralizers in finite Coxeter groups. *Journal of Group Theory*, 14(5):727–745, 2011. 68

[23] Martin Liebeck, Eamonn A. O'Brien, Aner Shalev, and Pham H. Tiep. The Ore conjecture. *Journal of the European Mathematical Society*, pages 939–1008, 2010. 2, 76

[24] Gunter Malle and Donna Testerman. *Linear Algebraic Groups and Finite Groups of Lie Type*. Cambridge University Press, Cambridge, 2011. 41, 53, 54, 56, 58, 60, 62, 63, 64, 65, 66, 85

[25] James S. Milne. Algebraic geometry (v5.21), 2011. Disponível em www.jmilne.org/math/. 41, 47, 48, 51, 52

[26] James S. Milne. Fields and galois theory (v4.30), 2012. Disponível em www.jmilne.org/math/. 47

[27] Peter Müller. Algebraic groups over finite fields, a quick proof of lang's theorem. *Proceedings of the American Mathematical Society*, 131(02):369–370, 2002. 61

[28] Gabriel Navarro. *Characters and blocks of finite groups*. Cambridge University Press, Cambridge, 1998. 76

[29] Oystein Ore. Some remarks on commutators. *Proceedings of the American Mathematical Society*, 2(2):307–314, 1951. 76

[30] Forrest A. Richen. Modular representations of split BN pairs. *Trans. Am. Math. Soc.*, 140:435–460, 1969. 64

[31] Joseph J. Rotman. *An Introduction to the Theory of Groups*. Springer, New York, 4th edition, 1994. 38, 75

[32] Louis Solomon. The orders of the finite Chevalley groups. *Journal of Algebra*, 3(3):376 – 393, 1966. 68

[33] Tony A. Springer. *Linear Algebraic Groups*. Birkhäuser Boston, 2nd edition, 1998. 41, 43, 50, 53, 66, 85

[34] Robert Steinberg. Prime power representations of finite linear groups. *Canadian Journal of Mathematics*, 8(0):580–591, 1956. 1, 67

[35] Robert Steinberg. Prime power representations of finite linear groups. II. *Canadian Journal of Mathematics*, 9(0):347–351, 1957. 1, 67

[36] Robert Steinberg. *Endomorphisms of Linear Algebraic Groups: Number 80*. Amer Mathematical Society, 1968. 58, 61, 62, 83

[37] Donald E. Taylor. *The Geometry of the Classical Groups*. Heldermann Verlag, Berlin, 1992. 33, 35, 39

[38] Pham H. Tiep. p-Steinberg characters of finite simple groups. *Journal of Algebra*, 187(1):304–319, 1997. 83

[39] Robert Wilson. *The Finite Simple Groups*. Springer, New York, 2009. 1, 2, 33, 39

Índice Remissivo