Problema de Noether não-comutativo
CPG para a dissertação

João Fernando Schwarz

Dissertação apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Mestre em Matemática

Programa: Mestrado em Matemática
Orientador: Prof. Dr. Vyacheslav Futorny

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro do CNPq

São Paulo, fevereiro de 2015

Problema de Noether não-comutativo

Esta versão da dissertação contém as correções e alterações sugeridas pela Comissão Julgadora durante a defesa da versão original do trabalho, realizada em 12/02/2015. Uma cópia da versão original está disponível no Instituto de Matemática e Estatística da Universidade de São Paulo.

Comissão Julgadora:

- Prof. Dr. Vyacheslav Futorny (orientadora) - IME-USP
- Prof. Dr. Hugo Luiz Mariano - IME-USP
- Prof. Dr. Plamen Emilov Kochloukov - IMECC-Unicamp

Resumo

SCHWARZ, J. F. **Problema de Noether não-comutativo**. 2014. 120 f. Dissertação (Mestrado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2015.
Neste trabalho, temos o objetivo de introduzir o Problema de Noether Clássico e sua versão não-comutativa introduzida por J. Alev e F. Dumas em [AD06]. Discutiremos os principais casos conhecidos nos quais os problemas têm solução positiva, observando um forte paralelo entre os casos comutativo e não-comutativo. Cobriremos os tópicos preliminares necessários para entendimento dos enunciados: álgebras de Weyl, anéis de operadores diferenciais, extensões de Ore, localização em domínios não-comutativos, e corpos de Weyl. No Capítulo 5 deste trabalho, o aluno apresenta duas contribuições originais, obtidas em colaboração com seu orientador V. Futorny e F. Eshmatov: o Teorema 5.5, que é um resultado folclórico sobre invariantes de ações livres de grupos finitos no anel de operadores diferenciais de variedades afins; e o Teorema 5.6, que até onde sabemos é inédito, sobre invariantes dos Corpos de Weyl sob a ação de grupos de pseudo-reflexão. Todo material algébrico preliminar para a demonstração destes dois teoremas é incluído no texto da dissertação: um básico de teoria de invariantes, vários resultados da teoria de grupos de pseudo-reflexão, alguns conceitos básicos de geometria algébrica e álgebra comutativa, e uma discussão detalhada do quociente de variedades afins sob ação de grupos finitos.

Palavras-chave: Problema de Noether, Teoria de Invariantes Não-Comutativa, Anéis de Operadores Diferenciais, Grupos de Pseudo-Reflexão.

Abstract

Schwarz, J. F. **Noncommutative Noether's problem**. 2010. 120 f. Dissertação (Mestrado) - Instituto de Matemática e Estatística, Universidade de São Paulo, São Paulo, 2010.

In this work we aim to introduce the Classical Noether's Problem, and its noncommutative version introduced by J. Alev and F. Dumas in [AD06]. We discuss the most well known cases of positive solution of these problems, pointing out a strong similarity between the cases of positive solution for the classical and noncommutative versions of the Problem. We cover the preliminary topics to understand the statement and solutions of these problems: Weyl algebras, differential operators rings, Ore extensions, noncommutative localization, and Weyl Skew-Fields. In the Chapter 5 of this dissertation, the student shows two original contributions, obtained in collaboration with his advisor V. Futorny and F. Eshmatov: Theorem 5.5, a result belonging to the folklore of the area of differential operators, describing its invariants under the free action of a finite group on an affine variety; and Theorem 5.6, about the invariants of the Weyl skew-fields under the action of pseudo-reflection groups. As far as we know, this result is new. All preliminary algebraic facts to prove these two facts are included in the body of this text. It includes some basic facts on invariant theory, many results about pseudo-reflection groups, some basic concepts of algebraic geometry and commutative algebra, and a detailed discussion of the quotient of an affine variety under the action of a finite group.
Keywords: Noether's Problem, Noncommutative Invariant Theory, Rings of Differential Operators, Pseudo-Reflection Groups.

Sumário

Capítulo 0

Introdução

O propósito dessa dissertação será introduzir casos conhecidos e alguns novos de solução positiva para o Problema de Noether Não-Comutativo ([AD06], 1.2.2): Seja k um corpo de característica 0, e V um espaço vetorial de dimensão finita n sobre k. Sendo G um subgrupo finito de $GL(V)$, podemos estender sua ação para a álgebra polinomial de V, $S(V^*)$ que, após uma escolha de base, é identificada com a álgebra de polinômios em n variáveis. Esta ação pode ser extendida para o anel de operadores diferenciais em $S(V^*)$, que é a n-ésima álgebra de Weyl $A_n(k)$; e finalmente esta ação pode ser extendida para o corpo de frações, $D_n(k)$. A questão levantada pelo Problema de Noether Não-Comutativo é a seguinte: quando temos $D_n(k)^G$, o subcorpo de invariantes, isomórfico a $D_n(k)$?

Além da discussão dos resultados conhecidos sobre o assunto, duas novas demonstrações obtidas pelo aluno, em colaboração com V. Futorny e F. Eshmatov serão apresentadas:

Teorema 0.1. (Teorema 5.5 da dissertação) *Suponha k algebricamente fechado, e seja X uma variedade algébrica afim, irredutível e normal sobre k. Seja G um grupo finito de k-automorfismos que age sobre X de maneira livre. Chamando $R = O(X)$, o anel das funções regulares, temos que G age sobre R como automorfismos de k-álgebra. Assim, $D(R)^G \cong D(R^G)$, onde $D(A)$, A qualquer k-álgebra, é seu anel de operadores diferenciais.*

Este resultado é bem conhecido, e faz parte do folclore da área. No nosso entendimento, é difícil encontrar na literatura uma demonstração explícita deste fato. Por isso, o trabalho em reproduzir nesta dissertação uma demonstração completa.

Teorema 0.2. (Teorema 5.6 da dissertação) *Seja k algebricamente fechado, V um espaço vetorial de dimensão finita n, e W um grupo finito de pseudo-reflexões de V. Estendendo a ação de W para $D_n(k)$, temos $D_n(k)^W \cong D_n(k)$.*

Este resultado, até onde sabemos, é novo.

0.1 Organização

A estrutura da dissertação será a seguinte:

No Capítulo 1, é introduzido o Problema de Noether Clássico, com algumas considerações históricas sobre a sua origem. Ele é enunciado, tanto de maneira puramente algébrica, quanto em linguagem geométrica - a equivalência birracional entre certas variedades afins. Essas considerações geométricas serão relevantes para os capítulos que se seguem. Na Seção 2, fazemos um apanhado dos principais casos de solução positiva para o Problema de Noether. A maior parte deles é provada ao longo da dissertação, ou então a demonstração é indicada a partir de resultados bem conhecidos, como o Teorema de Lüroth. Indicamos nesta seção, também, contra-exemplos, nos quais o Problema tem solução negativa. Na seção 3, introduzimos o Teorema de Miyata, cuja versão não-comutativa será o cerne da demonstração de vários casos de solução positiva para o Problema Não-Comutativo.

Usando o Teorema de Miyata, demonstrações simples dos resultados positivos obtidos por Fischer e Burnside são exibidas.

No Capítulo 2, discutimos as Álgebras de Weyl, suas localizações e corpos de frações. A maior parte do material deste Capítulo é bem conhecida: propriedades básicas da Álgebra de Weyl, Extensões de Ore e localização não-comutativa de conjuntos multiplicativamente fechados que satisfazem a condição de Ore. O material menos usual se encontra na Seção 5; o resultado mais importante deste Capítulo, para o que se segue, é a Proposição 2.10.

Na Seção 1, introduzimos, primeiramente, a Álgebra de Weyl como o anel de operadores diferenciais na álgebra de polinômios. Usamos duas noções de operadores diferenciais: a primeira mais simples (definição 2.2), a segunda com escopo mais geral (definição 2.4). É indicada a classe de álgebras na qual as duas noções coincidem (finitamente geradas e regulares), e exibimos a prova da equivalência para a álgebra de polinômios de maneira direta. Finalmente, introduzimos a Álgebra de Weyl por meio de geradores e relações.

Na Seção 2, fazemos uma discussão geral sobre extensões de Ore: uma generalização natural do conceito de extensões polinomiais. Extensões de Ore serão usadas continuamente ao longo deste trabalho, e nesta seção, em particular, este conceito nos dá mais uma definição da Álgebra de Weyl. Seguimos provando algumas propriedades de anel de extensões de Ore. Elas são totalmente análogas a propriedades de extensões polinomiais usuais - por exemplo, temos a extensão do Teorema da Base de Hilbert. Juntamos tudo isto para concluir as principais propriedades de anel da álgebra de Weyl: um domínio noetheriano, simples, e cujas unidades se limitam aos escalares.

Na Seção 3, fazemos uma discussão geral sobre localizações no contexto não-comutativo, uma vez que o procedimento de localizar por um conjunto multiplicativamente fechado não é direto como no caso comutativo. A última proposição da Seção 3 é fundamental (proposição 2.10), e será usada diversas vezes ao longo do trabalho; sua demonstração está na seção 3 do Capítulo 3. Na Seção 4, fazemos uma breve discussão sobre características indesejadas da Álgebra de Weyl que surgem se o corpo base tiver característica prima.

Na Seção 5, fazemos algumas observações sobre corpos de frações de extensões de Ore que serão utilizadas com frequência no restante do trabalho. Em particular, tal qual no caso comutativo, onde podemos mergulhar o corpo de funções racionais em uma variável no anél de séries de Laurent, exatamente o mesmo procedimento pode ser feito para corpo de frações de extensões de Ore (que são análogos não-comutativos de funções racionais). Por fim, discutimos algumas apresentações equivalentes dos corpos de Weyl, e calculamos seu centro.

No Capítulo 3, fazemos um apanhado de várias áreas de Álgebra que serão utilizadas no decorrer do trabalho. As seções 1 e 3 têm material bastante canônico (com exceção, talvez, da proposição 3.11 e a prova da proposição 2.10). Na Seção 1 falamos de teoria clássica de invariantes. Os assuntos abordados por esta área são inúmeros, mas nos concentramos na questão da geração finita da subálgebra de invariantes. Mostramos duas provas do Teorema de Hilbert-Noether, que diz que a subálgebra é finitamente gerada quando o grupo é finito. A primeira é para álgebras finitamente geradas arbitrárias, e para qualquer corpo. A segunda, baseada nos operadores de Reynolds, é para característica 0, e para o caso específico da álgebra de polinômios. Esta segunda demonstração é oferecida devido a sua simplicidade, e porque iremos utilizá-la posteriormente como etapa na demonstração do Teorema de Chevalley-Shephard-Todd.

Na Seção 2, discutimos grupos de pseudo-reflexão, em particular, grupos de Weyl, grupos de reflexão ortogonais, e grupos de reflexão unitários. Tudo é feito para corpos arbitrários de característica 0. Mostramos um exemplo de grupo de pseudo-reflexão que não é de reflexão. Depois, mostramos que, tal qual no caso bem conhecido de grupos de Weyl, sempre podemos decompor a análise de grupos de pseudo-reflexão em suas componentes irredutíveis. Usando a classificação de Shephard-Todd para os grupos de reflexão unitários, indicamos como é possível obter uma classificação de todos os grupos de pseudo-reflexão para qualquer corpo de característica 0. Em seguida, apresentamos uma demonstração do Teorema de Chevalley-Shephard-Todd, um resultado surpreendente e que será crucial para o restante do trabalho. Por fim, incluímos, sem demonstração, um resultado sobre semi-invariantes sob a ação de um grupo de pseudo-reflexão, e um resultado de

Steinberg sobre grupos de isotropia - ambos resultados que usaremos posteriormente.

A Seção 3 faz um apanhado de resultados de álgebra comutativa que serão utilizados no trabalho. A maior parte dos fatos são enunciados sem demonstração, e podem ser facilmente encontrados em qualquer livro sobre o assunto. Por usar técnicas de álgebra comutativa, a demonstração da proposição 2.10 foi deixada para o final desta seção. A Seção 4 resume as partes relevantes de geometria algébrica que serão utilizadas no restante do trabalho. Aqui, devido à complexidade do assunto, temos que ser bastante breves - assumimos conhecidas várias definições prévias, e os resultados citados têm as demonstrações apenas referenciadas. A perfeição técnica em geometria algébrica é um feito extraordinário - por isso, a ênfase aqui é em explicar intuitivamente os conceitos da maneira mais clara possível. É abordado com mais detalhes, contudo, o assunto de quocientes por ações de grupos finitos. Discutimos duas definições naturais do que gostaríamos de considerar um quociente: o categorial e o geométrico, e provamos, de maneira direta, que as duas noções coincidem e têm uma interpretação extremamente natural quando temos uma variedade afim e um grupo finito: se $X = Spec\, A$, e o grupo finito é G, então $X/G = Spec\, A^G$.

No Capítulo 4, introduzimos o Problema de Noether Não-Comutativo. Na primeira seção, baseados na ideia introduzida por Duflo de "almost comutative algebra", e na célebre Conjectura de Gelfand-Kirillov, argumentamos que os Corpos de Weyl (mais precisamente, são anéis de divisão) constituem um análogo correspondente não-comutativo para os corpos de funções racionais. Na Seção 2, introduzimos o Problema de Noether Não-Comutativo: para que grupos finitos G agindo linearmente, temos $D_n(k)^G \cong D_n(k)$? Na verdade, inicialmente consideramos uma versão ligeiramente modificada desse problema, para quando G não é necessariamente finito, mas provamos que quando G é finito, essa modificação não é necessária. Provamos nesta seção dois casos de solução positiva para o Problema: quando $n = 1$, e quando a representação natural de G se decompõe em soma direta de representações de dimensão 1. Estes resultados foram obtidos por J. Alev e F. Dumas. Ao longo disto, destacamos alguns resultados que serão utilizados de maneira essencial nas provas dos casos positivos: o Lema de Artin Não-Comutativo, e a extensão não-comutativa do Teorema de Miyata.

Na Seção 3, separamos a prova do seguinte Teorema, também de Alev e Dumas: $D_2(k)^G \cong D_2(k)$, para qualquer $G \subset GL_2(k)$ grupo finito. Esta demonstração é basta extensa, porém, é elementar. Consiste basicamente em manipulações inteligentes que permitem aplicar os Teoremas Clássico e Não-Comutativo de Miyata de maneira iterada. Essa demonstração só havia sido publicada em francês. Nesta dissertação, a traduzimos, e conseguimos fazer significativas simplificações assumindo G finito (a demonstração original permitia G ser infinito).

Na seção 4, provamos o resultado obtido por Futorny, Molev e Ovsienko, de que $D_n(k)^{S_n} \cong D_n(k)$, onde S_n age da maneira natural. O material desta seção inspira o que será desenvolvido no Capítulo 6. Usamos nesta seção o resultado bem conhecido de que se R é um anel simples e G é um grupo finito de automorfismos externos de G, então R^G também é simples. Na seção 5, exibimos a demonstração da extensão não-comutativa do Teorema de Miyata. Neste processo, obtemos também o resultado interessante de que $Frac\, A^G = (Frac\, A)^G$, onde A é um domínio não-comutativo e G um grupo finito de automorfismos - isto é uma generalização, não-trivial, do caso comutativo bem conhecido. Finalmente, na seção 6, explicitamos o interessante paralelo entre os casos de solução positiva para as versões comutativa e não-comutativa do Problema de Noether.

No Capítulo 5, usando o material que foi desenvolvido previamente, obtemos os resultados originais deste trabalho. A Seção 1 é uma coletânea do material relevante do artigo "Graded Cofinite Rings of Differential Operators", de F. Knop, que é usado de maneira essencial no que se segue. Na Seção 2, discutimos um análogo não-comutativo do Teorema de Hilbert-Noether sobre geração finita de subálgebra de invariantes sob a ação de grupos finitos, instanciado no caso particular da álgebra de Weyl. A existência de um conjunto finito de geradores é uma resposta possível para a questão: qual a estrutura do anel $A_n(k)^G$? São indicados alguns resultados que permitem encontrar tais geradores de maneira explícita. Contudo, tais geradores podem ter relações bastante complicadas entre si. Mencionamos um resultado de Levasseur que diz, de maneira precisa, qual a estrutura de $A_n(k)^G$ quando G é um grupo finito agindo linearmente, sem pseudo-reflexões diferentes da identidade. Mostramos uma demonstração do Teorema 0.1, que descreve de maneira precisa a estrutura de $D(X)^G$, onde X é uma variedade afim, quando a ação de G tem uma propriedade geométrica bastante forte: é livre. Na Seção 5.3, usando o material das seções anteriores, mostramos um resultado que é uma extensão do resultado obtido anteriormente para o grupo simétrico: o Teorema 0.2.

No Capítulo 6, mostramos demonstrações alternativas de que $D_n(k)^W \cong D_n(k)$, onde $W = B_n, D_n$. As demonstrações destes fatos são puramente algébricas, sem levar em conta argumentos geométricos e, portanto, são válidas para qualquer corpo de caractéristica 0, não necessariamente algébricamente fechado. As demonstrações são obtidas por meio de um argumento similar àquele da seção 4.4 para o grupo simétrico. Acreditamos que, por meio de assistência computacional, o isomorfismo $D_n(k)^W \cong D_n(k)$ pode ser obtido para W o grupo de Weyl F_4, E_6, E_7, E_8 usando a mesma estratégia. Por fim, ao final do capítulo 6, uma outra demonstração de que $D_n(k)^{B_n} \cong D_n(k)$, diferente das anteriores, é exibida. Todas as demonstrações desta seção foram concebidas pelo aluno.

0.2 Definições e Notações

Vamos reunir aqui, por comodidade, algumas convenções sobre definições e notações. Algumas delas foram assumidas bem conhecidas ao longo da dissertação; outras estamos repetindo aqui por comodidade de leitura. Usaremos o termo “domínio"tanto para anéis comutativos quanto não-comutativos; idem para o termo “corpo"e corpo de frações: a localização pelos elementos não-nulos em um domínio. k sempre será usado para denotar o corpo base. Usamos a notação $A_n(k)$ para denotar a n-ésima álgebra de Weyl, e denotaremos seus geradores usuais por $x_1, \dots, x_n, y_1, \dots, y_n$ ou então $x_1, \dots, x_n, \partial_1, \dots, \partial_n$. $Frac\, A$ sempre denotará o corpo de frações de um domínio A, sendo comutativo ou não. Localização por um conjunto multiplicativamente fechado X será denotada por $X^{-1}A$, AX^{-1}, ou simplesmente A_X se localização à direita e esquerda coincidirem. $D_n(k) = Frac\, A_n(k)$ são os Corpos de Weyl. $D_{m,t}(k)$ é $D_m(k(z_1, \dots, z_t))$ se $m > 0$, e $k(z_1, \dots, z_t)$ se $m = 0$. Dada uma álgebra comutativa A, $D(A)$ indica o seu anel de operadores diferenciais.

Denotaremos por *Specm* o espectro maximal de um anel comutativo, comumente identificando-o com um subconjunto de pontos de um espaço afim k^n, como em geometria algébrica clássica, no caso de k algebricamente fechado (pelo Nullstellensatz de Hilbert). *Spec* denota o espectro total. Se X é um esquema, denotamos por O_X o seu esquema estrutural, e dado um aberto $U \subset X$, por $O_X(U)$ o anel de funções regulares em U. Denotaremos $O_X(X)$ por $O(X)$ também. $D(X)$ é definido como $D(O(X))$, o anel de operadores diferenciais em X. Dado um ponto $x \in X$, o anel de germes de funções do feixe O_X é denotado por $O_{X,x}$, com único ideal maximal denotado por m_x. Denotamos por $ht(p)$, onde p é um ideal primo de um anel A, a sua altura. Dado um morfismo $f : X \to Y$, denotamos por $f^{\#}$ o morfismo canônico $Y \to f_*X$. f_* é a imagem direta, e f^* a imagem inversa. A fibra de um ponto $y \in Y$ é denotada por X_y. Demais noções de geometria algébrica têm a notação usual - seguimos principalmente [Har77], e também [Liu02].

Capítulo 1

Problema de Noether Clássico

Neste Capítulo, será introduzido o Problema de Noether Clássico. Suas origens serão brevemente discutidas. Após isto, serão discutidos os principais casos onde há uma solução positiva, e serão indicados também alguns contra-exemplos. Utilizando um teorema de Miyata Teorema 1.4 ([Miy71]), serão provados alguns casos de solução positiva - casos que admitem versões análogas para a versão não-comutativa do Problema, e que admitem uma demonstração semelhante utilizando uma extensão do Teorema de Myiata para extensões de Ore ([AD06], Teorema 1.4) - que será discutida no Capítulo 4 dessa dissertação (Teorema 4.4).

1.1 Origens

Seja k um corpo, que por simplicidade se assumirá ter característica 0. Seja $X = \{x_1, \ldots, x_n\}$ um conjunto finito de símbolos e seja G um grupo finito que os permuta, transitivamente. Seja $K = k(x_1, \ldots, x_n)$ o corpo das funções racionais em tais símbolos. G age em K por automorfismos de corpos de maneira natural, fixando k e com cada elemento $g \in G$ levando x_i em $g.x_i$, $i = 1, \ldots, n$.

A questão inicialmente levantada por Emmy Noether ([Noe13]) é a seguinte: na situação acima, quando temos o subcorpo de invariantes $k(x_1, \ldots, x_n)^G \cong k(x_1, \ldots, x_n)$?

Observação. *Dado um grupo qualquer G agindo num conjunto E, denotamos $E^G = \{e \in E | ge = e, \forall g \in G\}$.*

O interesse inicial nesta questão se deve à sua relação com o Problema Inverso da Teoria de Galois: seja G um grupo finito. Quando $k = \mathbb{Q}$ admite uma extensão de Galois L, tal que o grupo $Gal(L/\mathbb{Q}) = G$? Noether mostrou ([Noe13]) que, se o seu Problema apresenta solução positiva para um grupo G, visto como um grupo de permutações, então o Problema Inverso também apresenta solução positiva; e que podemos parametrizar tais extensões de Galois ([Sal85]).

Será considerada, ao longo deste trabalho, a seguinte versão um pouco mais geral do Problema de Noether, considerada por vários matemáticos há um bom tempo (e.g., Burnside, [Bur14]).

Seja V um espaço vetorial de dimensão finita n, e seja $G \subset GL(V)$ um subgrupo finito. A ação de G se extende para $S(V^*)$, a álgebra simétrica em V^*, da seguinte maneira: $g.f(v) = f(g^{-1}v)$, $g \in G, f \in S(V^*), v \in V$ - lembrando que cada $f \in S(V^*)$ pode ser visto como uma função em V. Dessa maneira, G se identifica a um grupo finito de automorfismos de k-álgebra de $S(V^*)$. Por meio da escolha de uma base de V, tem-se um isomorfismo $S(V^*) \cong k[x_1, \ldots, x_n]$, onde os x_i são os duais da base escolhida. Desta forma, $S(V^*)$ é identificada à álgebra de polinômios em n variáveis.

Definição 1.1. *Grupos de k-automorfismos de $k[x_1, \ldots, x_n]$ obtidos como acima são chamados de grupos de* automorfismos lineares.

Dado qualquer domínio comutativo A e um grupo H de automorfismos (de anel) de A, a ação de H se extende de maneira natural de forma a se obter um grupo de automorfismos de $Frac\, A$, naturalmente isomórfico à H: $g(ab^{-1}) = g(a)g(b)^{-1}$, $a, b \in A, g \in H$.

Seja G um grupo finito de automorfismos lineares de $k[x_1, \ldots, x_n]$, e considere a extensão de sua ação para o corpo de funções racionais. A versão estendida do Problema de Noether (chamada aqui simplesmente de Problema de Noether, com ou sem o adjetivo comutativo/clássico) faz a seguinte pergunta:

Problema. (Problema de Noether) *Quando, nas condições acima, $k(x_1, \ldots, x_n)^G \cong k(x_1, \ldots, x_n)$?*

O Problema de Noether também permite uma interpretação geométrica - este ponto de vista será particularmente útil quando discutirmos sua versão não comutativa.

No contexto da geometria algébrica clássica - isto é, com k algebricamente fechado e variedades quasi-projetivas - é fundamental a noção de equivalência birracional ([Har77], Cap. 1). No contexto restrito de variedades algébricas afins (e irredutíveis), temos que $Specm\, A$ e $Specm\, B$, onde A e B são k-álgebras finitamente geradas sem divisores de 0, são birracionalmente equivalentes, se e somente se, $Frac\, A \cong Frac\, B$.

Se nós temos um grupo finito G de k-automorfismos agindo em $Specm\, A$, é natural procurar entender o que seria um quociente desta variedade pela ação do grupo. Para grupos algébricos gerais, e variedades algébricas em geral, entender o quociente de ações é algo altamente não trivial, e é estudado pela área de Teoria Geométrica de Invariantes (cuja principal referência é [MFK94]). Em nosso caso restrito, com G finito agindo em $Specm\, A$, contudo, a resposta é simples. A ação de G na variedade é induzida por uma ação de G em A por automorfismos de k-álgebra. Pelo teorema de Noether sobre invariantes de grupos finitos (Teorema 3.1), temos que A^G é uma álgebra finitamente gerada, e evidentemente é um domínio. Logo, $Specm\, A^G$ é uma variedade algébrica afim irredutível, e a projeção $Specm\, A \to Specm\, A^G$ induzida pela inclusão das álgebras constitui o quociente (Seção 3.4).

Neste contexto que foi desenvolvido acima, o Problema de Noether pode ser expresso de maneira geométrica: sendo $A = k[x_1, \ldots, x_n]$, e G um grupo finito de automorfismos lineares, quando a projeção $SpecmA \to SpecmA^G$ constitui uma equivalência birracional?

1.2 Resultados Positivos e Contra-Exemplos

Nesta seção, serão apresentados alguns dos principais casos de solução positiva do Problema de Noether, e contra-exemplos. Antes de mais nada, algumas observações preliminares são pertinentes.

Proposição 1.1. *Seja A um domínio e G um grupo finito de automorfismos de A. Considerando a ação estendida de G em $Frac\, A$, tem-se que $Frac\, A^G = (Frac\, A)^G$.*

Demonstração. A inclusão $Frac\, A^G \subseteq (Frac\, A)^G$ é clara. No outro sentido: seja $r = a/b$ um elemento invariante de $Frac\, A$. Chamando $b' = \prod_{g \in G, g \neq id} g.b$, tem-se $r = ab'/bb'$; donde $ab' = rbb'$. Como r, bb' são invariantes, ab' também o é; então, pode-se escrever r como razão de dois elementos invariantes, e a proposição está demonstrada. □

Vamos fixar a notação: seja $K = k(x_1, \ldots, x_n)$ e G um grupo finito de automorfismos lineares agindo em K. Pelo Lema de Artin, K é uma extensão algébrica de K^G, com $[K : K^G] = |G|$. Dados três corpos $E \subseteq F \subseteq L$, tem-se que $trdeg_E L = trdeg_F L + trdeg_E F$. Portanto, $trdeg_k K^G = trdeg_k K = n$. Em particular, não se pode ter $K^G = k$. Este fato, na verdade, é válido para qualquer grupo finito de automorfismos de K, não apenas os lineares. Vamos anotar isso:

Lema 1.1. *K^G nunca se restringe a k, para qualquer grupo finito de automorfismos G de K; $trdeg_k\, K^G = trdeg_k\, K$.*

Observação. *Este último fato é definitivamente falso se G não for finito. Por exemplo, se $G = GL(V)$, com $dim\, V = n$, $k[x_1, \ldots, x_n]^G$ é constituído apenas pelas funções constantes ([Dol03], pág. 2).*

Eis os principais casos onde se têm uma solução positiva para o Problema de Noether.

- Quando $K = k(x)$ e G é arbitrário. Isto é consequência imediata do Teorema de Lüroth ([Jac89], Sec. 8.14):

  Teorema 1.1. *Seja k um corpo arbitrário, e L um subcorpo de $k(x)$ diferente de k. Então, existe uma função racional $y(x)$ tal que L é o corpo de funções racionais em y.*

- Quando $K = k(x, y)$, e G arbitrário. Isto é consequência imediata do Teorema de Zariski-Castelnuovo ([Jac89], Sec. 8.14), quando k é algebricamente fechado:

  Teorema 1.2. *Seja k um corpo algebricamente fechado, e L um subcorpo de $k(x, y)$, diferente de k, e com $[k(x, y) : L]$ finito. Então existem funções racionais u, v tais que $L = k(u, v)$ (extensão puramente transcendental, com grau de transcendência 2).*

  Observação. *A notação $L = E(u)$, onde L é um corpo, E um subcorpo e $u \in L$ indica que L é uma extensão puramente transcendental de E, com $\{u\}$ base de transcendência.*

  Quando o corpo não é algebricamente fechado, este resultado segue do Teorema de Lüroth usando o Teorema de Miyata (Teorema 1.4). O argumento é o mesmo que o usado para provar o seguinte caso positivo:

- Quando $K = k(x, y, z)$, k é algebricamente fechado, e G é arbitrário (Burnside, [Bur14]).

  Isto será demonstrado na próxima seção.

- Quando k contém uma e-ésima raiz primitiva da unidade, onde e é o expoente de G, e o grupo é abeliano (Fischer, [Fis16]).

  Isto também será demonstrado na próxima seção. Lembramos que o expoente de um grupo finito é o mínimo múltiplo comum das ordens de seus elementos.

- Quando G é gerado pelas pseudo-reflexões que contém:

  Definição 1.2. *Um isomorfismo linear s de um espaço vetorial V é chamado de* pseudo-reflexão *se ele fixa um hiperplano e $s^n = I$ para algum natural n. Quando $n = 2$, s é chamado de uma* reflexão.

  Grupos finitos de (pseudo)reflexões são subgrupos gerados pelas (pseudo)reflexões que contêm. Quando $k = \mathbb{Q}$, tais grupos correspondem aos grupos de Weyl; quando $k = \mathbb{R}$ tais grupos correspondem aos grupos de reflexão usuais; e quando $k = \mathbb{C}$ temos os grupos de reflexão unitários.

  Neste caso, o Problema de Noether possui uma solução positiva em função do célebre teorema de Chevalley-Shephard-Todd ([Spr77], Sec. 4.2):

  Teorema 1.3. *Seja V um espaço vetorial de dimensão finita e $G \subseteq GL(V)$ um grupo finito. Então $S(V^*)^G$ é isomórfico a uma álgebra de polinômios em n variáveis, se e somente se, G é um grupo de pseudo-reflexões.*

  Com este resultado, fica simples demonstrar a solução positiva do Problema de Noether. De fato, usando a proposição 1.1, $K^G = Frack[x_1, \ldots, x_n]^G \cong Frack[x_1, \ldots, x_n]$.

  Note que o caso clássico de invariantes do grupo simétrico é recuperado desta forma: afinal, ele é um grupo finito de reflexões ([Hum90]).

  Observação. *Mais precisamente, para qualquer domínio comutativo como escalares, os invariantes da álgebra de polinômios pela ação do grupo simétrico são isomórficos à algebra de polinômios, nos polinômios simétricos elementares.*

  O tópico de grupos finitos de pseudo-reflexão, e o Teorema de Chevalley-Shephard-Todd, serão discutidos com mais detalhes no Capítulo 2.

- Quando $K = k(x_1, x_2, x_3)$, e $G = A_3$, permutando as variáveis da forma usual; quando $K = k(x_1, \ldots, x_4)$ e $G = A_4$, da mesma maneira; e quando $k = \mathbb{Q}$ e $K = k(x_1, \ldots, x_5)$, e $G = A_5$, agindo também da forma usual ([Jac89], sec. 8.14, [Mae89]).

O problema de Noether é aberto para todos os demais grupos alternantes ([JLY02], Capítulo 0). Parte da dificuldade é que, ao contrário de S_n, A_n não é um grupo de pseudo-reflexões ([For84], seção 5). Isto nos dá um exemplo interessante de duas variadades afins que não são isomórficas mas são birracionalmente equivalentes: $Specm\, k[x_1, \ldots, x_i]$ e $Specm\, k[x_1, \ldots, x_i]^{A_i}$, $i = 3, 4$ e k algebricamente fechado.

Alguns contra-exemplos para o Problema de Noether são conhecidos. Por exemplo, quando $k = \mathbb{Q}$, $n = 47$ e G é o subgrupo cíclico de ordem 47 de S_{47} - Teorema 9 em [For84]; este contra-exemplo foi descoberto por Swan e Vorenskii. Os primeiros contra-exemplos para corpos algebricamente fechados foram descobertos por Saltman ([Sal84]), onde G é um grupo de ordem p^9, p um primo.

1.3 Teorema de Miyata e Aplicações

Segue-se um Teorema de Miyata ([Miy71]) que permite demonstrar de maneira simples alguns dos casos particulares de solução positiva do Problema de Noether.

Teorema 1.4. (Miyata, [Miy71]) *Seja K um corpo comutativo, $S = K[x]$ o anel de polinômios em uma variável sobre K, e $F = K(x)$ seu corpo de frações. Seja G um subgrupo de automorfismos de S, não necessariamente finito, tal que $g(K) \subseteq K$ para todo $g \in G$. Duas coisas podem acontecer:*

- *$S^G \subseteq K$, e no caso $F^G = S^G = K^G$.*
- *S^G não está contido em K. Sendo qualquer $u \in S^G$, $u \notin K$, e de grau $m = min\{deg_x y | y \in S^G, y \notin K\}$, temos $S^G = K[u]$ e $F^G = K^G(u)$.*

Uma demonstração de uma versão mais geral deste teorema será apresentada no Capítulo 4, Seção 5.

Vamos ver agora uma demonstração para as soluções positivas obtidas por Burnside e Fischer.

Demonstração. (Burnside) Seja $K' = k(y/x, z/x)$ e $S = K'[x]$. $Frac\, S = k(x, y, z)$, e $G(K') \subseteq K'$: de fato, se $g \in G$,

$$gx = ax + by + cz,\ gy = a'x + b'y + c'z \,\text{e}\, gz = a''x + b''y + c''z,$$

e então

$$g(y/x) = \frac{a' + b'(y/x) + c'(z/x)}{a + b(y/x) + c(y/x)} \in K';$$

e similarmente $g(z/x) \in K'$ $(a, b, c, a', b', c', a'', b'', c'' \in K)$. Portanto podemos aplicar o Teorema de Miyata. Note que $[FracS : FracS^G]$ é finito (e igual a $|G|$), e assim não podemos ter $S^G \subseteq K'$. Desta maneira, $FracS^G = K'^G(t)$ para algum $t \in S^G$. Pelo Teorema de Zariski-Castelnuovo, $K'^G = k(u, v)$ para alguns $u, v \in K'$; Portanto, $Frac\, S^G = k(u, v, t)$. □

Demonstração. (Fischer) Como k contém a raiz e-ésima da unidade, onde e é o expoente do grupo, todo elemento de G é diagonalizável. Como todos os elementos de G comutam, eles são simultaneamente diagonalizáveis, isto é, existe uma base dual $x_1, \ldots, x_n$ e $\xi_i : G \to k^*$, $i = 1, ..., n$ homomorfismos de grupo tal que $gx_i = \xi_i(g)x_i$, $i = 1, \ldots, n$. Em particular, G age em $S_1 = k(x_2, \ldots, x_n)[x_1]$ estabilizando $K_1 = k(x_2, \ldots, x_n)$. Logo $k(x_1, \ldots, x_n)^G = K_1^G(u_1)$ para algum $u_1 \in S_1^G$. Aplicando indutivamente o Teorema de Miyata, e sabendo que o caso base quando $n = 1$ já é coberto pelo Teorema de Lüroth, a demonstração se encerra. □

Veremos posteriormente, no Capítulo 4, que utilizando uma versão não-comutativa deste teorema de Miyata, demonstrações análogas para casos análogos são possíveis no Problema de Noether Não-Comutativo.

1.4 Referências

A exposição nesta seção foi baseada em [Dum06], Seção 3. Aqui foi apresentada uma breve introdução ao problema de Noether. Para mais informações, ver [For84], [Sal85], [Sal84], [Jr.74], [Dum06], e as referências neles. Para generalizações para grupos algébricos além de grupos finitos, [PSV94].

Capítulo 2

Álgebras de Weyl e Localizações

Neste capítulo, serão introduzidas as Álgebras de Weyl e suas principais propriedades. Para aplicações neste caso e uso posterior também são introduzidas extensões de Ore no caso geral. Posteriormente estaremos interessados em tomar localizações e formar corpo de frações da Álgebra de Weyl, e tais procedimentos não são diretos como no caso comutativo. Portanto, localizações em domínios não comutativos são discutidas em certo detalhe, instanciadas no caso particular da Álgebra de Weyl; também são feitas algumas discussões específicas deste caso.

2.1 Introduzindo a Álgebra de Weyl

Será necessário supor que o corpo base possui característica 0. Depois, faremos algumas indicações sobre o porquê desta necessidade.

Vamos definir as n-ésimas Álgebras de Weyl sobre k, $A_n(k)$, de várias maneiras diferentes. No final, todas as definições serão equivalentes.

Dado A uma k-álgebra comutativa, gostaríamos de introduzir o conceito de operadores diferenciais em A. Todo elemento $a \in A$ dá origem a uma transformação linear em A, a multiplicação à esquerda por a. Isto nos dá um homomorfismo de anéis $A \to End_k(A)$, que claramente é injetivo: desta forma, podemos considerar A como uma subálgebra de $End_k(A)$.

Definição 2.1. *Uma k-derivação de A é uma função $\delta \in End_k(A)$ que satisfaz $\delta(ab) = \delta(a)b + a\delta(b)$, para todos $a, b \in A$. O conjunto das k-derivações formam um A-módulo, denotado por $Der_k A$, com a seguinte ação de A: $(a\delta)(b) = a\delta(b), a, b, \in A, \delta \in Der_k A$; ele também carrega a estrutura de álgebra de Lie sobre k, por meio do comutador de duas derivações.*

Observação. *Relembrando, numa álgebra associativa, o comutador $[a, b]$ entre dois elementos é dado por $ab - ba$.*

Proposição 2.1. *$Der_k(k[x_1, \ldots, x_n])$ é o módulo livre gerado pelas derivadas parciais $\partial_1, \ldots, \partial_n$ (∂_i é a derivada parcial em relação a x_i).*

Demonstração. É evidente que as derivadas parciais são derivações. Seja δ uma derivação arbitrária, e f um polinômio. É fácil ver que $\delta(f) = \sum_{i=1}^n \partial_i f \delta(x_i)$. Logo, $\delta = \sum_{i=1}^n \delta(x_i)\partial_i$, e portanto as derivadas parciais geram o módulo de derivações. Se temos uma relação $0 = \sum_{i=1}^n a_i\partial_i$, aplicando sucessivamente a derivação a $x_1, \ldots, x_n$, vê-se que todos os a_i são 0. Logo, o módulo é livremente gerado por $\partial_1, \ldots, \partial_n$. □

Quando a álgebra A é finitamente gerada e é regular (Definição 3.12), como no caso de $k[x_1, \ldots, x_n]$, definimos o anel de operadores diferenciais da seguinte maneira.

Definição 2.2. (Primeira definição de operadores diferenciais) *$D(A)$, o* anel de operadores diferenciais *em A, é a subálgebra de $End_k(A)$ gerada por A e $Der_k(A)$.*

Definição 2.3. (Álgebra de Weyl) $A_n(k) = D(k[x_1, \ldots, x_n])$.

Uma questão que surge nauralmente após essa definição é: se $A_n(k) \cong A_m(k)$, isso implica que $m = n$? Isso foi respondido de maneira afirmativa por Gelfand e Kirillov [GK66], usando o conceito introduzido neste trabalho de dimensão de Gelfand-Kirillov: um invariante, cujo valor é $2n$ para $A_n(k)$, provando o não-isomorfismo quando $n \neq m$. Para maiores detalhes sobre a teoria de dimensão de Gelfand-Kirillov, a referência canônica é o livro de Krause e Lenegan, [KL00].

Na Álgebra de Weyl, temos a seguinte relação fundamental: $[\delta, f] = \delta(f)$, para δ uma k-derivação e f um polinômio. De fato, aplicando $[\delta, f]$ em um polinômio arbitrário g nós temos: $\delta(fg) - g\delta(f) = \delta(f)g$. Em particular, $[\partial_i, x_j] = \delta_{ij}$, $1 \leq i, j \leq n$.

Vamos introduzir algumas notações. Seja $\alpha = (\alpha_1, \ldots, \alpha_n)$ uma n-upla de inteiros não-negativos. Definimos $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, e similarmente $\partial^\alpha = \partial_1^{\alpha_1} \ldots \partial_n^{\alpha_n}$. Definimos $|\alpha| = \alpha_1 + \ldots + \alpha_n$ (módulo de α), $\alpha! = \alpha_1! \ldots \alpha_n!$.

Lema 2.1. *Sejam $\alpha, \beta \in \mathbb{N}^n$, com $|\alpha| \leq |\beta|$. Então $\partial^\beta(x^\alpha) = \beta!$ se $\alpha = \beta$, e 0 caso contrário.*

É claro que, como k espaço vetorial, $A_n(k)$ é gerada por todos os monômios em $x's$ e $\partial's$; isto é, elementos da forma $\mu_1 \ldots \mu_s$, onde $\mu_i \in \{x_1, \ldots, x_n, \partial_1, \ldots, \partial_n\}$. Usando a relação de comutação $[\partial_i, x_j] = \delta_{ij}$, podemos escrever cada monômio como uma soma de monômios com todos os $x's$ agrupados na esquerda e os $\partial's$ agrupados na direita. De fato, mais ainda vale:

Proposição 2.2. *Os monômios $x^\alpha \partial^\beta$, onde α, β percorrem todas as n-uplas de inteiros não-negativos, formam uma base de $A_n(k)$ como k-espaço vetorial.*

Demonstração. Já vimos que tais monômios geram $A_n(k)$. Resta ver que eles são linearmente independentes. Suponha que tenhamos uma relação não-trivial da forma

$$\sum c_{\alpha\beta} x^\alpha \partial^\beta = 0,$$

com α, β n-uplas de inteiros não-negativos e os $c's$ escalares. Seja σ uma n-upla de módulo mínimo entre todas aquelas com algum $c_{\alpha\sigma} \neq 0$ para algum α. Então, usando o Lema 2.1, tem-se que

$$\sum c_{\alpha\beta} x^\alpha \partial^\beta (x^\sigma) = \sigma! \sum_\alpha c_{\alpha\sigma} x^\alpha.$$

Por hipótese, este polinômio não é nulo, pois algum dos seus coeficientes é diferente de 0. Portanto, $\sum c_{\alpha\beta} x^\alpha \partial^\beta = 0$ não pode ser 0. □

Existe uma segunda definição de operadores diferenciais, que se aplica para k-álgebras comutativas A arbitrárias:

Definição 2.4. (Segunda definição de operadores diferenciais) *Defina indutivamente $D(A)_0 = \{d \in End_k(A) | [d, a] = 0, \forall a \in A\}$, e para todo $i > 0$, $D(A)_i = \{d \in End_k(A) | [d, a] \in D(A)_{i-1}, \forall a \in A\}$. Claramente temos $D(A)_i \subseteq D(A)_j$ se $i < j$ e $D(A)_i D(A)_j \subseteq D(A)_{i+j}$. Chamando $D(A) = \bigcup_{i=0}^\infty D(A)_i$, obtemos desta forma uma álgebra associativa, chamada de* anel de operadores diferenciais *em A.*

Talvez uma afirmação acima mereça alguma justificação. Se $D \in D(A)_i, E \in D(A)_j$, vamos mostrar que $DE \in D(A)_{i+j}$ por indução em $i + j$. O caso $i + j = 0$ é claro pela proposição abaixo. $[DE, a] = D[E, a] + [D, a]E, \forall a \in A$. $[E, a] \in D(A)_{j-1}, [D, a] \in D(A)_{i-1}$, logo por indução $[DE, a]$ pertence a $D(A)_{i+j-1}$ para todo a, o que é equivalente a $DE \in D(A)_{i+j}$. Para todo elemento $D \in D(A)$, o menor i tal que $D \in D(A)_i$ é definido como a *ordem* do operador diferenciail.

Proposição 2.3. *$D(A)_0 = A$ e $D(A)_1 = A \oplus Der_k A$.*

Demonstração. Se $T \in D(A)_0$, então $[T, a](1) = T(a) - aT(1) = 0, \forall a \in A$. Portanto, T é multiplicação por $T(1)$. Se $T \in D(A)_1$, seja $U = T - T(1)$. Então, para todos $a, b \in A$, $[b, [U, a]](1) = b(U(a) - aU(1)) - U(ab) + aU(b) = 0$. $U(1) = 0$, e, portanto, $U(ab) = aU(b) + bU(a)$, ou seja, U é uma derivação. Finalmente, é claro que $A \cap Der_k A = \{0\}$. □

Esta proposição mostra que o anel de operadores diferenciais em A, no segundo sentido, contém o anel de operadores diferenciais em A, no primeiro sentido. As duas definições coincidem quando A é finitamente gerada e regular,[MR01], sec. 15.4. Contudo, em geral, elas diferem. Por exemplo, quando A é um domínio de integridade e k é algebricamente fechado, $D(A)$ é noetheriano à esquerda e à direita e finitamente gerado como k-álgebra, [SS88]. Contudo, em [BGG72], é mostrado que $D(A)$, quando $k = \mathbb{C}$ e $A = \mathbb{C}[x_1, x_2, x_3]/(x_1^3 + x_2^3 + x_3^3)$, que tem uma singularidade na origem, não é nem noetheriano nem finitamente gerado.

Vamos mostrar a equivalência das duas definições de maneira direta para o caso $A = k[x_1, \dots, x_n]$. Usaremos $A_n(k)$ para indicar a álgebra de operadores diferenciais no primeiro sentido, e $D(k[x_1, \dots, x_n])$ para indicar tal álgebra no segundo sentido. Usaremos e_i para indicar a n-upla de inteiros não negativos com 0 em todas as posições menos na i-ésima, que contém 1. Usaremos também dois fatos frequentemente: o colchete é uma derivação, em qualquer álgebra associativa A, isto é, $[a, bc] = [a, b]c + b[a, c]$, $\forall a, b, c \in A$. Além disso, usaremos a identidade de Jacobi: $[a, [b, c]] + [b[c, a]] + [c[a, b]] = 0, \forall a, b, c, \in A$.

Lema 2.2. *Seja $P \in D(k[x_1, \dots, x_n])$, no segundo sentido de operadores diferenciais. Se $[P, x_i] = 0$ para $i = 1, \dots, n$ então $P \in k[x_1, \dots, x_n]$.*

Demonstração. Tendo em vista a proposição 2.3, basta provar que $P \in D_0(k[x_1, \dots, x_n])$, ou seja, que $[P, f] = 0$ para todo polinômio. Como o comutador é linear na segunda entrada, basta provar isto para quando f é um monômio. Seja então $f = x^\alpha$ para algum $\alpha \in \mathbb{N}^n$, com $\alpha_i \neq 0$. Então $[P, x^\alpha] = [P, x_i]x^{\alpha - e_i} + x_i[P, x^{\alpha - e_i}]$. Por indução no grau dos monômios, temos que $[P, x_i] = [P, x^{\alpha - e_i}] = 0$. Logo, $[P, f] = 0$ como queríamos. □

O próximo lema é o análogo formal do fato que todo campo vetorial $F = (F_1, \dots, F_n)$ em $\mathbb{R}^n$ que satisfaz $\partial_i F_j = \partial_j F_i$, $1 \leq i, j \leq n$ admite uma função potencial. Seja C_r o conjunto de operadores diferenciais (no segundo sentido) que podem ser escritos da forma $\sum_\alpha f_\alpha \partial^\alpha$, com $|\alpha| \leq r$. É imediato que $C_r = C_{r+1} \cap D_r(k[x_1, \dots, x_n])$.

Pela proposição 2.3 nós temos que $C_0 = k[x_1, \dots, x_n]$ e $C_1 = Der_k k[x_1, \dots, x_n] \oplus k[x_1, \dots, x_n]$. Usaremos no próximo lema a convenção de que se $k < n$ então $\mathbb{N}^k$ é identificado com o subconjunto de $\mathbb{N}^n$ com as últimas $n - k$ coordenadas 0.

Lema 2.3. *Sejam $P_1, \dots, P_n \in C_{r-1}$ tais que $[P_i, x_j] = [P_j, x_i]$ para $1 \leq i, j \leq n$. Então, existe $Q \in C_r$, tal que $P_i = [Q, x_i]$, para $i = 1, \dots, n$.*

Demonstração. Se $P_n = \sum f_\alpha \partial^\alpha$, definindo $Q' = \sum(\alpha_n + 1)^{-1} f_\alpha \partial^{\alpha + e_n}$, temos $[Q', x_n] = P_n$. Suponha, por indução, que determinamos um $Q' \in C_r$, tal que $[Q', x_i] = P_i$ para $k + 1 \leq i \leq n$. Desta maneira $[[Q', x_i], x_k] = [P_k, x_i]$. Seja $G = [Q', x_k] - P_k$. Então, $[G, x_i] = 0$ para $k + 1 \leq i \leq n$. Temos que $[\partial^\beta, x_i] = \beta_i \partial^{\beta - e_i}$, e, portanto, se $[\partial^\beta, x_i] = 0$ então $\beta_i = 0$. Assim, como $[G, x_i] = 0$ para $k + 1 \leq i \leq n$ nós temos, usando esse argumento, que $G = \sum_{\alpha \in A} f_\alpha \partial^\alpha$, onde $A \subseteq \mathbb{N}^k$. Seja

$$Q'' = \sum_{\alpha \in A} (\alpha_k + 1)^{-1} f_\alpha \partial^{\alpha + e_k}.$$

$Q' \in C_r \subseteq D_r(k[x_1, \dots, x_n])$ implica que $[Q', x_k] \in C_r \cap D_{r-1}(k[x_1, \dots, x_n]) = C_{r-1}$. Como P_k pertence a C_{r-1}, G também pertence. Logo $Q'' \in C_r$. $[Q'', x_i] = 0$ para $k+1 \leq i \leq n$, por construção. Assim, $[Q' - Q'', x_i] = P_i$. Além disso, $[Q'', x_k] = G$, e portanto $[Q' - Q'', x_k] = [Q', x_k] - G = P_k$. Portanto, $[Q' - Q'', x_i] = P_i$ para $k \leq i \leq n$, e a indução está completa. □

Teorema 2.1. *O anel de operadores diferenciais, no segundo sentido, em $k[x_1, \dots, x_n]$, é igual à $A_n(k)$. Além disso, $D_k(k[x_1, \dots, x_n]) = C_k$.*

Demonstração. Basta provar que $D_k(k[x_1, \dots, x_n]) \subseteq C_k$ - a inclusão oposta é clara. Claramente $C_0 = D_0(k[x_1, \dots, x_n])$. Seja $P \in D(k[x_1, \dots, x_n])$. Se $P \in D_1(k[x_1, \dots, x_n])$ então, pela proposição 2.3, $P \in Der_k k[x_1, \dots, x_n] \oplus k[x_1, \dots, x_n]$. Portanto, $P \in C_1$ pela proposição 2.1. Suponha, por indução, que $D_k(k[x_1, \ldots, x_n]) = C_k$ para todo $k < m$ (acabamos de mostrar o caso base m=1). Seja $P \in D_m(k[x_1, \ldots, x_n])$. Defina $P_i = [P, x_i]$; como P_i tem ordem $k \leq m-1$, $P_i \in C_{m-1}$. Para todos $1 \leq i, j \leq n$, $[P_i, x_j] = [[P, x_i], x_j] = [[P, x_j], x_i] = [P_j, x_i]$; portanto, usando o lema 2.3 existe $Q \in C_m$ tal que $[Q, x_i] = P_i$, $1 \leq i \leq n$. Portanto, $[Q-P, x_i] = 0$ em $D(k[x_1, \ldots, x_n])$, e usando o lema 2.2 temos que $Q - P \in C_0$, e assim $P \in C_m$. Logo $D_m(k[x_1, \ldots, x_n]) \subseteq C_m$, como queríamos. □

Uma maneira mais direta e explícita de introduzir a Álgebra de Weyl é por geradores e relações:

Definição 2.5. *Seja $k\langle x_1, \ldots, x_n, y_1, \ldots, y_n\rangle$ a álgebra associativa livre nas variáveis $x_1, \ldots, x_n, y_1, \ldots, y_n$. Seja I o seu ideal gerado pelos elementos $[x_i, x_j], [y_i, y_j], i, j = 1, \ldots, n$, e $[y_i, x_j] - \delta_{ij}$, $i, j = 1, \ldots, n$. Seja $A_n^*(k)$ o quociente da álgebra livre pelo ideal I.*

Proposição 2.4. *A função k-linear $A_n^*(k) \to A_n(k)$ que manda x_i em x_i e y_i em ∂_i é um isomorfismo de k-álgebras.*

Demonstração. Temos um homomorfismo da álgebra livre para $A_n(k)$ com x_i indo para x_i e y_i indo para ∂_i. Tendo em vista que os $x's$ e $\partial's$ satisfazem em $A_n(k)$ as relações que definem I, esse homomorfismo se fatora num homomorfismo de $A_n^*(k)$ para $A_n(k)$. De maneira análoga a $A_n(k)$, temos que $A_n^*(k)$ é gerada por monômios da forma $x^\alpha y^\beta$. Eles são enviados para a base de $A_n(k)$, como vimos. Portanto, eles são linearmente independentes em $A_n^*(k)$. Assim, esse homomorfismo é um isomorfismo de espaços vetoriais, e, portanto, de álgebras. □

Desta forma, já obtemos duas caracterizações distintas da álgebra de Weyl. Vamos para a terceira.

2.2 Extensões de Ore

Seja R um anel não necessariamente comutativo, e α um automorfismo de R. Por uma α-derivação δ de R, queremos dizer um mapa $\delta : R \to R$ tal que $\delta(a+b) = \delta(a) + \delta(b)$ e $\delta(ab) = \alpha(a)\delta(b) + \delta(a)b$, para todos $a, b \in R$. Ou seja, quando $\alpha = id$, temos apenas uma derivação usual. Note que, em todo caso, necessariamente $\delta(1) = 0$.

Definição 2.6. *Um anel S, contendo R como subanel, livremente gerado como R-módulo à esquerda por uma base $\{1, x, \ldots, x^n, \ldots\}$, onde x é um elemento de S, e tal que $xr = \alpha(r)x + \delta(r)$, denota-se $S = R[x; \alpha, \delta]$, e diz-se que S é uma extensão de Ore de R.*

Quando $\alpha = id$, costuma-se escrever $S = R[x; \delta]$, e quando $\delta = 0$, $S = R[x; \alpha]$. Quando $\alpha = id, \delta = 0$, temos simplesmente extensões polinomiais.

A rigor, é necessário provar que tais extensões realmente existem, e que são únicas à menos de um isomorfismo que se restringe à identidade em R. Da mesma forma que extensões polinomiais usuais, a existência pode ser mostrada de maneira direita, introduzindo o R-módulo à esquerda livre em símbolos $1, x, \ldots, x^n, \ldots$, e definindo a multiplicação como acima. Isto é completamente elementar, mas bastante laborioso. Um caminho alternativo e conceitual é o seguinte:

Teorema 2.2. *Dado um anel R, um automorfismo α de R e uma α-derivação δ de R, existe uma extensão de Ore $S = R[x; \alpha, \delta]$.*

Demonstração. Seja $E = End(R[z])$ o anel de endomorfismos de $R[z]$ visto como grupo abeliano; vamos construir S como um subanel de E. Como $R[z]$ é um R-módulo à esquerda, existe um homomorfismo de anéis $\lambda : R \to E$ que manda $r \in R$ na multiplicação à esquerda por r. λ é injetivo: de fato $\lambda(r)(1) = r$, para $r \in R$. Dessa forma, podemos identificar R com um subanel de E. Agora, definimos $x \in E$ da seguinte forma (usando que E é livre como R-módulo):

$$x(\sum_i r_i z^i) = \sum_i (\alpha(r_i) z^{i+1} + \delta(r_i) z^i).$$

Seja S o subanel de E gerado por $\{x\} \cup R$. Para todo $r \in R$ e $p = \sum_i r_i z^i \in R[z]$, temos:

$$(xr)(p) = x(\sum_i rr_i z^i) = \sum_i (\alpha(rr_i)z^{i+1} + \delta(rr_i)z^i) = \sum_i \alpha(r)\alpha(r_i)z^{i+1} + \sum_i (\alpha(r)\delta(r_i) + \delta(r)r_i)z^i$$

$$= \alpha(r)\sum_i (\alpha(r_i)z^{i+1} + \delta(r_i)z^i) + \delta(r)\sum_i r_i z^i = (\alpha(r)x + \delta(r))p.$$

Portanto, $xr = \alpha(r)x + \delta(r)$ para todo $r \in R$. Em particular, $xR \subseteq Rx + R$. Por indução, $x^i R \subseteq Rx^i + \ldots + Rx + R$ para todo $i > 0$, e portanto $Rx^i Rx^j \subseteq Rx^{i+j} + \ldots + Rx + R$. Portanto, o subgrupo $\sum_{i=0}^{\infty} Rx^i$ é um subanel de E, e, portanto, $S = \sum_{i=0}^{\infty} Rx^i$. Tudo que resta é mostrar que os x^i, $i \geq 0$ são linearmente independentes. Se tivéssemos $\sum_i r_i x^i = 0$ em S par alguns $r_i \in R$, aplicando tal operador em 1, nos daria $\sum_i r_i z^i = 0$ em $R[z]$; portanto, todos os coeficientes devem ser 0, o que mostra que temos independência linear. □

Além disso, uma extensão de Ore $S = R[x; \alpha, \delta]$ satisfaz uma propriedade universal semelhante a extensões polinomiais usuais - o que mostra que tais extensões são únicas à menos de um único isomorfismo que se restringe a identidade em R.

Proposição 2.5. *Seja $S = R[x; \alpha, \delta]$ uma extensão de Ore. Dado um homomorfismo $\phi : R \to T$ para um anel T, e um elemento $y \in T$ satisfazendo $y\phi(r) = \phi\alpha(r)y + \phi\delta(r)$ para todo $r \in R$, existe uma única extensão de ϕ para S que envia x para y.*

Demonstração. Defina $\psi : S \to T$ dado por $\psi(\sum_i r_i x^i) = \sum_i \phi(r_i)y^i$. É claro que qualquer extensão de ϕ, se existir, deverá ser igual a ψ. Portanto, resta provar que ψ é bem definida e um homomorfismo de anéis. ψ é bem definida, pois S é livremente gerado sobre R pela base $\{1, x, x^2, \ldots\}$, e claramente preserva a estrutura aditiva. Se $t = \sum_j b_j x^j$ é um elemento arbitrário de S, então

$$\psi(xt) = \psi(\sum_j \alpha(b_j)x^{j+1} + \sum_j \delta(b_j)x^j) = \sum_j \phi\alpha(b_j)y^{j+1} + \sum_j \phi\delta(b_j)y^j$$

$$= \sum_j (\phi\alpha(b_j)y + \phi\delta(b_j))y^j = \sum_j y\phi(b_j)y^j = y\psi(t).$$

Segue por indução que $\psi(x^i t) = y^i\psi(t)$ para todos $i > 0, t \in S$. Além disso, se $a \in R$,

$$\psi(at) = \sum_j \phi(ab_j)y^j = \sum_j \phi(a)\phi(b_j)y^j = \phi(a)\psi(t).$$

Logo, dado qualquer $s = \sum_i a_i x^i \in S$, temos:

$$\psi(st) = \sum_i \psi(a_i x^i t) = \sum_i \phi(a_i)\psi(x^i t) = \sum_i \phi(a_i)y^i\psi(t) = \psi(s)\psi(t).$$

Portanto, ψ é um homomorfismo de anéis.

□

Mostrada a existência e unicidade de extensões de Ore, podemos dar alguns exemplos.

Exemplo. *Vamos introduzir o plano quântico:*

Definição 2.7. *Uma matriz multiplicativamente anti-simétrica sobre k é uma matriz $n \times n$ $q = (q_{ij})$ com entradas em k^* e tal que $q_{ii} = 1, q_{ij} = q_{ji}^{-1}$ para todos i, j. Dada tal matriz, o espaço afim de dimensão n quantizado é a álgebra $O_q(k^n)$ dada por geradores $x_i x_j = q_{ij} x_j x_i$, para todos i, j.*

Esta álgebra também pode ser escrita como uma extensão de Ore iterada $k[x_1][x_2; \alpha_2] \ldots [x_n; \alpha_n]$, onde α_i é o automorfismo de $k[x_1] \ldots [x_{i-1}; \alpha_{i-1}]$ que fixa k e manda x_j para $q_{ij} x_j$, $j < i$ (Exerc. 1K, [GJ04]).

Exemplo. *Álgebras universais envolventes de álgebras de Lie também aparecem como exemplos de Extensões de Ore. Considere, por exemplo,* $sl_2(k)$ *com a base usual* e, f, h*, satisfazendo as relações* $[ef] = h$, $[he] = 2e$, $[hf] = -2f$. *Então,* $U(sl_2(k))$ *é a* k*-álgebra associativa com geradores* e, h, f *e relações*

$$ef - fe = h,\ he - eh = 2e,\ hf - fh = -2f.$$

A subálgebra R *dessa álgebra gerada por* e, h *é uma extensão de Ore da forma* $k[e][h; \delta_1]$*, onde* $\delta_1 = 2e\partial_e$. $U(sl_2(k))$ *por sua vez será* $R[f; \alpha_2, \delta_2]$*, onde* $\alpha_2(e) = e$ *e* $\alpha(h) = h + 2$*, e* $\delta_2(e) = -h$ *e* $\delta_2(h) = 0$*. Este exemplo é fundamental, uma vez que as representações de* $sl_2(k)$ *ocupam um lugar central na classificação das álgebras de Lie semissimples (sobre um corpo algebricamente fechado), e também na teoria de representação de tais álgebras ([Hum90]). Contudo, não é o caso que* $sl_n(k)$ *podem ser escritos como extensões iteradas de Ore quando* $n \geq 3$ *([GJ04], pág. xx). Mas uma grande classe de álgebras de Lie pode: se L é uma álgebra de Lie solúvel de dimensão finita (sobre um corpo algebricamente fechado), então* $U(L)$ *é realizável por uma série de extensões* $T_0 = k \subset T_1 \ldots \subset T_m = U(L)$*, onde cada* T_i *é da forma* $T_{i-1}[x; \delta_i]$ *para alguma* T_{i-i}*-derivação* δ_i *([GJ04], pág. xx).*

Como terceiro exemplo:

Definição 2.8. *Seja* $R = k[x_1, \ldots, x_n]$ *e* $S = R[y_1; \partial_1] \ldots [y_n; \partial_n]$*, onde* ∂_j *é simplesmente derivação com relação a* x_j*, e manda* y_i *para 0 quando i<j. Essa extensão de Ore iterada é isomórfica à* $A_n(k)$*, pela propriedade universal acima, que mostra que temos exatamente a álgebra livre quocientada pelas relações como na Definição 2.5.*

Encerramos assim nossas descrições equivalentes da Álgebra de Weyl. Para nos referir aos seus geradores usuais, usaremos tanto a notação $x_1, \ldots, x_n, y_1, \ldots, y_n$, quanto $x_1, \ldots, x_n, \partial_1, \ldots, \partial_n$.

Vamos reunir agora alguns fatos relevantes sobre extensões de Ore. Em vários sentidos, como fica claro pela definição, e como veremos em breve em alguns resultados, elas são uma generalização não comutativa de polinômios usuais. Se $S = R[x; \alpha, \delta]$, e $s \in S$ é $r_n x^n + \ldots + r_1 x + r_0$, $r_i \in R, r_n \neq 0$, lembrando que tal representação é única, definimos o *grau* de s por n, e o denotamos por $deg\, s$. O *coeficiente líder* (*à esquerda*) de s é definido como sendo r_n.

A rigor pode-se dizer que se definiu acima apenas o conceito de grau à esquerda, uma vez que s também pode ser escrito da forma $x^m q^m + \ldots x q_1 + q_0$, $q_i \in R$. Contudo, temos o seguinte Lema simples:

Lema 2.4. $x^n r = \alpha^n(r) x^n + \ldots + \delta^n(r), r \in R.$

Como α é um automorfismo, isto mostra que o conceito simétrico de grau à direita coincide com o de grau à esquerda. Mostra, também, que $R[x; \alpha, \delta]$ é um módulo livre à direita sobre R. Além disso, fica claro que $deg\, ss' = deg\, s + deg\, s', \forall s, s' \in S$ não nulos. Portanto, as mesmas considerações sobre grau, como no caso de polinômios usuais, nos dão:

Proposição 2.6. *Se* S *é uma extensão de Ore de* R*, e* R *é um domínio, então* S *também o é. As unidades de* S *são as unidades de* R*.*

Corolário 2.1. *As unidades da Álgebra de Weyl* $A_n(k)$ *são* k*.*

Demonstração. Note que, para qualquer domínio R, podemos fazer uma construção idêntica à da álgebra de Weyl: definimos $A_1(R) = R[x][y; \partial]$, onde ∂ é a derivação que anula R e manda x em 1. As unidades de $A_1(R)$ são, portanto, as unidades de R. Podemos definir as álgebras de Weyl indutivamente: $A_1(k)$ é o que já conhecemos, e $A_n(k) = A_1(A_{n-1}(k))$. As unidades de $A_n(k)$ são, portanto, as unidades de $A_{n-1}(k)$. Por indução, temos que as unidades se limitam a k. □

Proposição 2.7. *Se* R *é um anel de divisão e* S *é uma extensão de Ore de* R*, então dados quaisquer* $a, b \in S$ *existem únicos* $q, r \in S$*, tal que* $a = qb + r$ *e* $deg\, r < deg\, b$*. Um resultado análogo para divisão com resto à direita também vale. Em particular,* S *é um domínio de ideais principais à direita e à esquerda.*

Demonstração. Igual ao caso de extensões polinomiais. □

O Teorema da Base de Hilbert também admite uma generalização para o caso de extensões de Ore.

Teorema 2.3. (Teorema da Base de Hilbert Estendido) *Se R é noetheriano à esquerda ou à direita e S é uma extensão de Ore de R, então S também o é.*

Demonstração. Suponha, inicialmente, que R é noetheriano à direita. Seja I um ideal à direita de S e J o conjunto dos coeficientes líderes (à esquerda) dos elementos de I, mais 0. J é claramente um subgrupo aditivo, e é um ideal à direita de R. De fato, se $r \in J$, então I contém um elemento da forma $rx^n + \ldots$ (termos de menor grau). Multiplicando à direita por $\alpha^{-n}(r'), \forall r' \in R$, temos que $rr' \in J$, em função do Lema 2.4.

Sejam $\{r_1, \ldots, r_m\}$ um conjunto finito de geradores de J (R é noetheriano à direita). Sejam polinômios $p_1, \ldots, p_n \in I$ tendo os respectivos $r_i's$ como coeficientes líderes à esquerda. Multiplicando à direita por potências apropriadas de x, podemos supor todos os $p_i's$ de mesmo grau, digamos, n_0. Seja N o conjunto dos elementos de S de grau menor que n_0. Sendo um módulo finitamente gerado sobre R, ele é noetheriano à direita, e, portanto, da mesma forma, o é o seu submódulo $N \cap I$. Sejam $q_1, \ldots, q_k$ geradores de $N \cap I$ como R-módulo à direita.

Teremos então, finalmente, que $p_1, \ldots, p_m, q_1, \ldots, q_k$ determinam um conjunto finito de geradores para I. Se $p \in I$ tem grau menor que n_0, isto é claro. Se ele tem grau maior que n_0, então p é da forma $rx^M + \ldots$, $r \in J$, e portanto $r = r_1a_1 + \ldots + r_ma_m$ para alguns $a_i \in R$. Chamando $a_i' = \alpha^{-n_0}(a_i)$, temos que $p - (p_1a_1' + \ldots p_ma_m')x^{M-n_0} \in I$ e é de grau menor que p. Usando um argumento indutivo no grau, temos que p é expresso por meio dos geradores $p_1, \ldots, p_m, q_1, \ldots, q_k$.

Supondo agora R noetheriano à esquerda, temos que S é noetheriano à esquerda pelo resultado parcial acima e o lema seguinte. □

Lema 2.5. *Seja α um automorfismo de um anel R, e δ uma α-derivação. Então α^{-1} é um automorfismo de R^{op}, $-\delta\alpha^{-1}$ é uma α^{-1}-derivação de R^{op}, e $R[x; \alpha, \delta]^{op} = R^{op}[x; \alpha^{-1}, -\delta\alpha^{-1}]$.*

Observação. *Relembrando, R^{op} denota o anel oposto de R: igual a R como conjunto, com a mesma soma, mas com multiplicação $a * b = ba$.*

Podemos aplicar os últimos resultados acima para $A_n(k)$ e obter vários resultados sobre sua estrutura de anel.

Teorema 2.4. *$A_n(k)$ é uma k-álgebra simples, noetheriana à direita e à esquerda, e não possui divisores de 0.*

Demonstração. Resta apenas mostrar a simplicidade. Vamos provar isto por indução em n, usando por conveniência durante a prova a notação $A_0(k) = k$. O caso base é claro. Para o passo indutivo, seja J um ideal não nulo de $A_n(k)$. Basta provar que $J \cap A_{n-1}(k)$ é não nulo, e por hipótese indutiva teremos $J \cap A_{n-1}(k) = A_{n-1}(k)$; portanto, J contém unidade e é igual a $A_n(k)$.

$D \in J, D \neq 0$ pode ser escrito da forma $a_0 + a_1\partial_n + \ldots + a_s\partial_n^s$ com os $a_i \in A_{n-1}(k)[x_n]$ e $a_s \neq 0$. Se $s \geq 1$, então temos $D_1 = [D, x_n] = a_1 + 2a_2\partial_n + \ldots + sa_s\partial_n^{s-1}$ em J. Se $s \geq 2$, repetimos o processo de tomar comutadores, e obtemos $D_2 = [D_1, x_n] \in J$. Continuando assim, obtém-se um elemento não nulo de $J \cap A_{n-1}(k)[x_n]$ igual a $s!a_s$ após s passos (isso é imediato se $s = 0$). Chamando este elemento de E, temos que ele é igual a $b_0 + b_1x_n + \ldots + b_tx_n^t$, onde $b_i's \in A_{n-1}(k)$, $b_t \neq 0$. Procedendo de maneira análoga, tomando agora comutadores com $-\partial_n$, temos que $t!b_t \in J \cap A_{n-1}(k)$, que é o que queríamos. □

2.3 Localização

Seja R um domínio não comutativo, e X um conjunto multiplicativamente fechado ($x, y \in X$ implica $xy \in X$). Assumiremos sempre que tais conjuntos contêm 1. Se possível, gostaríamos de definir a localização à direita e à esquerda de R por X, de forma que o anel resultante satisfizesse a mesma propriedade universal esperada que no caso comutativo.

Definição 2.9. *Seja R um domínio e X um conjunto multiplicativamente fechado. Uma localização (posteriormente justificaremos que é válido usar o artigo "a") à direita de R por X é um anel S contendo R, e tal que todo elemento de X seja invertível, e todo elemento de S possa ser escrito da forma ax^{-1} para alguns $a \in R, x \in X$. Localização à esquerda pode ser introduzida de maneira totalmente simétrica.*

Mais para frente, mostraremos que, caso uma localização à direita (ou à esquerda) exista, ela satisfaz a propriedade universal desejada:

Proposição 2.8. *Seja R um domínio e X um conjunto multiplicativamente fechado. Se uma localização à direita S existe, e se $\phi : R \to T$ é qualquer homomorfismo de anéis, tal que X é levado em unidades de T, então ϕ admite uma extensão única para um homomorfismo de S para T. O mesmo vale para localização à esquerda.*

Por satisfazer essa propriedade universal, é claro que se a localização à direita (esquerda) existir, ela é única a menos de um único isomorfismo que é a identidade em R.

Contudo, não necessariamente tal localização existe. Vamos ver condições necessárias e suficientes para ela existir.

Definição 2.10. *Seja X um conjunto multiplicativamente fechado de um anel R. Então X é dito um* conjunto de Ore à direita *(*à esquerda*) se, dados quaisquer $x \in X, r \in R$, $xR \cap rX \neq \{\}$ ($Rx \cap Xr \neq \{\}$).*

Lema 2.6. *Seja X um conjunto de Ore à direita num anel R. Dados quaisquer elementos $x_1, \ldots, x_n \in X$, existem $s_1, \ldots, s_n \in R$, tal que $x_1 s_1 = \ldots x_n s_n \in X$.*

Demonstração. Por indução, basta considerar o caso $n = 2$. Neste caso, como X é um conjunto de Ore à direita, $x_1 y = x_2 s$ para alguns $y \in X, s \in R$, e $x_1 y \in X$ pois X é multiplicativamente fechado. □

Lema 2.7. *Seja R um domínio e X um conjunto multiplicativamente fechado. Se uma localização à direita de R por X, digamos S, existe, então:*

1. *X é um conjunto de Ore à direita.*
2. *Dados quaisquer $s_1, \ldots, s_n$ em S, existem $a_1, \ldots, a_n \in R$ e $x \in X$, tal que cada $s_i = a_i x^{-1}$. Ou seja, podemos colocar as frações com um denominador comum.*
3. *Dados $a, b \in R$ e $x, y \in X$, $ax^{-1} = by^{-1}$ em S, se e somente se, existem $c, d \in R$, tais que $ac = bd$ e $xc = yd \in X$ (em R).*

Demonstração.

1. Dados $b \in R, x \in X$, devem existir $c \in R, z \in X$ tal que $x^{-1}b = cz^{-1}$ em S, pela definição de localização à direita. Isto nada mais é do que $bz = xc$ (em R), ou seja, X é de Ore à direita.
2. Cada $s_i = b_i x_i^{-1}$ para alguns $b_i \in R, x_i \in X$. Pelo Lema 2.6, existem $x \in X$, $c_1, \ldots, c_n \in R$ tais que $x = x_i c_i$ para todo i. Como x e x_i são invertíveis em S, também o é c_i, e $x^{-1} = c_i^{-1} x_i^{-1}$. Portanto $s_i = b_i c_i x^{-1}$ para todo i.

3. Suponha, primeiramente, que existem $c, d \in R$ com $ac = bd$ e $xc = yd \in X$. Então, $ax^{-1} = ac(xc)^{-1} = bd(yd)^{-1} = by^{-1}$. Reciprocamente, suponha que $ax^{-1} = by^{-1}$. Pelo Lema 2.6, existem $c, d \in R$ com $xc = yd \in X$. Portanto, $ac(xc)^{-1} = ax^{-1} = by^{-1} = bd(yd)^{-1} = bd(xc)^{-1}$, e assim $ac = bd$.

□

Esse Lema nos dá condições de definir uma localização procedendo de maneira análoga ao caso comutativo. Suponha, então, X um conjunto de Ore à direita num domínio R. Defina uma relação de equivalência em $R \times X$, $\equiv$, com $(a, x) \equiv (b, y)$, se e somente se, existem $c, d \in R$ com $ac = bd$ e $xc = yd \in X$. $[a, x]$ denotará a classe de equivalência de (a, x). Sendo S o conjunto de tais classes de equivalência, podemos definir soma e produto. Dados $[a, x], [b, y] \in S$, e escolhendo $c, d \in R$ com $xc = yd \in X$, define-se $[a, x] + [b, y] = [ac + bd, xc]$; escolhendo $c \in R, z \in X$ com $bz = xc$, define-se $[a, x][b, y] = [ac, yz]$. Tal soma e produto estão bem definidos. Desta forma, S se torna um anel, e a função $r \to [r, 1]$ define um isomorfismo de R com um subanel de S, identificando R com um subanel de S, e fazendo S uma localização à direita de R por X.

A verificação em detalhes da construção indicada acima, apesar de elementar, é bastante laboriosa. Para uma construção alternativa, [GJ04], Teorema 6.2.

Estamos em condições agora de provar a propriedade universal enunciada na Proposição 2.8.

Demonstração. Recapitulando: começamos com um homomorfismo $\phi : R \to T$, tal que $\phi(X)$ consista de unidades, e queremos estendê-lo de maneira única para $S \supseteq R$ uma localização à direita. Se tal ψ existe, ele só pode ser da seguinte forma: $\psi(ax^{-1}) = \phi(a)\phi(x)^{-1}$, para $a \in R, x \in X$. Sabendo disto, vamos definir ψ exatamente dessa maneira, mostrar que é bem-definido, que é um homomorfismo de anéis, e que estende ϕ. Suponha que $a, b \in R$ e $x, y \in X$ com $ax^{-1} = by^{-1}$ sejam dados. Pelo Lema 2.7, existem $c, d \in R$ com $ac = bd$, $xc = yd \in X$. Assim, $\phi(x), \phi(y), \phi(xc), \phi(yd)$ são invertíveis em T e, portanto, $\phi(c), \phi(d)$ também são invertíveis. Sendo assim, $\phi(a)\phi(x)^{-1} = \phi(ac)\phi(xc)^{-1} = \phi(bd)\phi(yd)^{-1} = \phi(b)\phi(y)^{-1}$. Então ψ realmente é uma função bem definida. Tem-se também que $\psi(a) = \psi(a1^{-1}) = \phi(a)$ para todo $a \in R$ e, portanto, ψ é uma extensão de ϕ.

Sejam agora $a, b \in R$, $x, y \in X$. Existem $c, d \in R$ com $xc = yd \in X$, e assim

$$\psi((ax^{-1}) + (by^{-1})) = \psi((ac + bd)(xc)^{-1}) = \phi(ac + bd)\phi(xc)^{-1} =$$

$$\phi(ac)\phi(xc)^{-1} + \phi(bd)\phi(yd)^{-1} = \psi(ax^{-1}) + \psi(by^{-1}).$$

Existem também $e \in R, z \in X$, tal que $bz = xe$ e, portanto,

$$\psi((ax^{-1})(by^{-1})) = \psi((ae)(yz)^{-1}) = \phi(ae)\phi(yz)^{-1} = \phi(a)\phi(e)\phi(z)^{-1}\phi(y)^{-1}.$$

Como $\phi(b)\phi(z) = \phi(x)\phi(e)$, nós temos que $\phi(e)\phi(z)^{-1} = \phi(x)^{-1}\phi(b)$, e portanto $\psi((ax^{-1})(by^{-1})) = \phi(a)\phi(x)^{-1}\phi(b)\phi(y)^{-1} = \psi(ax^{-1})\psi(by^{-1})$.

Logo ψ é um homomorfismo de anéis. □

Observação. *Tudo que foi feito acima pode ser feito de maneira totalmente simétrica para localizações à esquerda. Denotaremos por $X^{-1}R$ a localização à esquerda e RX^{-1} a localização à direita.*

Proposição 2.9. *Seja R um anel e X um conjunto de Ore à direita e à esquerda. Então $RX^{-1} = X^{-1}R$.*

Demonstração. Seja $S = RX^{-1}$. Todo elemento de X é invertível em S. Dado $s \in S$, $s = ax^{-1}$ para alguns $a \in R, x \in X$. Como X é Ore à esquerda, existem $b \in R, y \in X$ com $ya = bx$; portanto $s = y^{-1}b$. Logo $S = X^{-1}R$. □

Exemplo. *Seja $S = R[x; \alpha]$ uma extensão de Ore, com α um automorfismo de R. A localização de S pelo conjunto $\{1, x, x^2, \ldots\}$ existe (tanto à direita quanto esquerda), e constitui o anel de polinômios de Laurent torcidos, $T = R[x^{\pm 1}; \alpha]$. É o módulo livre à esquerda sobre R com base $\{x^k | k \in \mathbb{Z}\}$, e* *relações* $x^k r = \alpha^k(r)x^k$, $k \in \mathbb{Z}$. *Temos que se* R *for noetheriano à direita ou à esquerda,* T *também será noetheriano à direita ou à esquerda ([GJ04] Teo. 1.14).*

Temos dois casos interessantes da construção acima. Seja $q = (q_{ij})$ *uma matriz* $n \times n$ *multiplicativa antissimétrica, como na definição 2.7. O* toro quântico *multiparâmetro é a* k*-álgebra* $O_q((k^*)^n)$ *dada por geradores* $x_1^{\pm 1}, \dots, x_n^{\pm 1}$, *e relações* $x_i x_i^{-1} = x_i^{-1} x_i = 1$, $i = 1, \dots, n$, *e* $x_i x_j = q_{ij} x_j x_i$. *Tal como o plano quântico multiparâmetro é uma extensão de Ore iterada, o toro quântico é da forma* $k[x_1^{\pm 1}; \alpha_1] \dots [x_n^{\pm 1}; \alpha_n]$, *onde* $\alpha_i(x_j) = q_{ij} x_j$ *para* $j < i$.

Outro caso interessante vem da teoria de anéis de grupos.

Definição 2.11. *Um grupo* G *é chamado de* policíclico-por-finito *se existem subgrupos.*

$$G_0 = \{id\} \subset G_1 \subset \dots \subset G_n \subseteq G_{n+1} = G,$$

tais que cada G_{i-1} *é normal em* G_i, *e* G_i/G_{i-1} *é infinito cíclico para* $i = 1, \dots, n$, *enquanto* G/G_n *é finito.*

É claro que se G *é finito, então* $k[G]$ *é um anel noetheriano (de fato, ele também é artiniano). É uma questão em aberto determinar que outras condições sobre* G *fazem* $k[G]$ *ser um anel noetheriano. A única condição conhecida é exatamente quando* G *é policíclico-por-finito (note que grupos finitos estão contidos neste caso), [GJ04], pág. xvi. De fato, temos nesta situação*

$$k[G_0] = k \subset k[G_1] \subset \dots \subset k[G_n] \subseteq k[G_{n+1}] = k[G],$$

com cada extensão nesta cadeia da forma $R_{i+1} = R_i[x^{\pm 1}; \alpha_i]$, *para* $i = 0, \dots, n-1$, *e a última extensão sendo um módulo finitamente gerado sobre a anterior. De forma iterativa, temos que cada anel da cadeia, inclusive o último, é noetheriano. Para mais detalhes, [GJ04], Teo. 1.16.*

Definição 2.12. *No caso particular de* $X = R - \{0\}$ *ser o conjunto multiplicativo no domínio* R, *dizemos que* RX^{-1} $(X^{-1}R)$ *é um corpo de frações à esquerda (à direita) de* R. *Quando ambos coincidem, dizemos apenas corpo de frações.*

Temos o seguinte resultado muito importante:

Teorema 2.5. *Seja* R *um domínio noetheriano à esquerda e à direita. Então ele admite um corpo de frações.*

Demonstração. Vamos mostrar que se R é noetheriano à direita, então $X = R - \{0\}$ é um conjunto de Ore à direita; o caso à esquerda é simétrico. Dados $a, b \in X$, precisamos mostrar que $aR \cap bR \neq (0)$. Considere a seguinte cadeia ascendente de ideias à direita: aR, $baR + aR$, $b^2aR + baR + aR, \dots$, $b^k aR + \dots + baR + aR, \dots$. Ela eventualmente estabiliza. Portanto, para algum n, $b^{n+1}a = b^n a x_n + \dots + bax_1 + ax_0$, para alguns $x_i \in R$. Seja k o menor i tal que $x_i \neq 0$ (nem todos os x_i são 0 pois R é um domínio). Cancelando por b^k nos dá $0 \neq ax_k = b^{n+1-k}a - bax_{k+1} - \dots - b^{n-k}ax_n \in aR \cap bR$. □

Em particular, $A_n(k)$ admite um corpo de frações: ele será denotado por $D_n(k)$. São chamados de *Corpos de Weyl*.

Introduzimos agora um resultado que será fundamental para o restante do trabalho. Sua demonstração será exibida ao final da seção 3 do Capítulo 3.

Proposição 2.10. *Seja* S *um conjunto multiplicativamente fechado de* $\Lambda = k[x_1, \dots, x_n]$. *Então,* $S^{-1}A_n(k)$ *e* $A_n(k)S^{-1}$ *existem e são iguais à* $D(\Lambda_S)$. *Aqui podemos usar a segunda descrição de anéis de operadores diferenciais, uma vez que toda localização de um anel regular é regular, Proposição 3.12.*

Encerramos essa seção com a seguinte observação. Neste capítulos discutimos apenas localizações em domínios. Isto é apenas por simplicidade, não por necessidade. Localizações em anéis com divisores de 0, com divisores de 0 no conjunto X que será localizado, também existem, e admitem propriedades totalmente similares ao que foi desenvolvido aqui. Este assunto é coberto em [GJ04], Cap. 10, e [MR01], Cap. 2.

2.4 Problemas em Característica prima

Como foi observado no começo deste capítulo, é crucial que o corpo base seja de característica 0 - caso contrário, várias coisas indesejáveis acontecem. Por exemplo, podemos definir a álgebra de Weyl como anel de operadores diferenciais em $k[x_1, \ldots, x_n]$, $A_n(k)$ (em qualquer um dos dois sentidos), ou como quociente de uma álgebra livre, $A_n^*(k)$ da mesma forma que na primeira seção. As duas definições não são equivalentes quando $char\, k \neq 0$. Vejamos, por exemplo, o que ocorre quando o corpo tem característica p. Considere o elemento em $A_n(k)$ dado por ∂_1^p. Ele atua como 0 em $x_2, \ldots, x_n$, manda x_1^k para 0 se $k < p$, e manda x_1^k para $Cx_1^s = 0$, pois C é um múltiplo de p, se $k \geq p$. Portanto, $\partial_1^p = 0$, e $A_n(k)$ contém elementos nilpotentes.

$A_n^*(k)$, por outro lado, continua sendo um domínio: essa definição continua sendo equivalente a uma extensão iterada de Ore, como na seção 2, e a prova de que assim obtemos um domínio não usou a característica do corpo. Portanto, $A_n(k)$ e $A_n^*(k)$ não são isomórficas.

Além disso, $A_n^*(k)$ apresenta propriedades indesejadas: não é um anel simples. De fato, $[y_1, x_1^p] = px_1^{p-1} = 0$. Logo, x_1^p está no centro de $A_n^*(k)$, e portanto, gera um ideal bilateral não-trivial.

Estes breves comentários já indicam que existe uma grande diferença entre os casos de característica 0 e prima. Álgebras de Weyl em característica prima são discutidas, por exemplo, em [Smi85].

2.5 Corpos de Weyl

Aqui faremos algumas observações sobre os corpos de Weyl para uso posterior.

Primeiramente, seja R um domínio noetheriano à esquerda e à direita. Seja $A = R[x; \alpha, \delta]$ uma extensão de Ore. Como vimos, A também é um domínio noetheriano à esquerda e à direita e, portanto, $Frac\, A$ existe. Seja $K = Frac\, R$. α se estende de maneira única para um automorfismo de K: $\alpha(xy^{-1}) = \alpha(x)(\alpha(y))^{-1}$, $x, y \in R$, e δ se estende de maneira única a uma α-derivação de K, usando que: $\delta(s^{-1}) = -\alpha(s)^{-1}\delta(s)s^{-1}$, para $s \neq 0 \in R$. Podemos formar assim a extensão de Ore $K[x; \alpha, \delta]$, e então:

Proposição 2.11. *$Frac\, A = Frac\, K[x; \alpha, \delta]$.*

Demonstração. A inclusão $Frac\, A \subseteq Frac\, K[x; \alpha, \delta]$ é clara. No sentido contrário, qualquer elemento de $K[x; \alpha, \delta]$, após tomar denominadores comuns, pode ser escrito da forma $s^{-1}a$, onde $a \in A, s \in R$. Assim, se $x, y \in K[x; \alpha, \delta]$, $xy^{-1} = s^{-1}ab^{-1}t$ para alguns $s, t \in R, a, b \in A$. Logo, $FracK[x; \alpha, \delta] \subseteq Frac\, A$. $\square$

O valor comum de $Frac\, A$ e $Frac\, K[x; \alpha, \delta]$ será denotado por $K(x; \alpha, \delta)$. Se $\alpha = id$ ou $\delta = 0$ usa-se a notação $K(x; \delta)$ ou $K(x; \alpha)$, respectivamente.

Da mesma forma que no caso comutativo, ao discutir funções racionais, é interessante considerar séries de potência.

Seja K um anel de divisão, α um automorfismo de K e δ uma α-derivação. O corpo $K(x; \alpha, \delta)$ pode ser visto como subcorpo do anel de séries de Laurent torcidas $K((x, \alpha^{-1}, -\delta\alpha^{-1}))$. Seus elementos são séries de Laurent da forma $\sum_{i \geq m}^{\infty} a_i x^{-i}$, onde $m \in \mathbb{Z}, a_i \in K$, e $a_m \neq 0$, com a multiplicação dada por:

$$x^{-1}a = \sum_{n \geq 1} \alpha^{-1}(-\delta\alpha^{-1})^{n-1}(a)x^{-n} = \alpha^{-1}(a)x^{-1} - x^{-1}\delta\alpha^{-1}(a)x^{-1}.$$

De fato, multiplicando à esquerda e à direita por x, se obtém as mesmas relações que em $K[x; \alpha, \delta]$. $K[x; \alpha, \delta]$ portanto aparece como subanel de $K((x; \alpha^{-1}, -\delta\alpha^{-1}))$, e assim $K(x; \alpha, \delta)$ é um subcorpo. Quando $\alpha = id$ usamos a notação $K((x; \delta))$, e usa-se a nomenclatura de anel de operadores pseudo-diferenciais.

Lema 2.8. *Seja K um anel de divisão com centro $Z(K)$. Seja σ um automorfismo de K, tal que σ^n não é interno para nenhum $n \geq 1$ (um automorfismo interno é da forma $x \to yxy^{-1}$, para algum*

$y \in K$). Então o centro $Z(D)$ de $D = K(x;\sigma)$ é o subcorpo $Z(K) \cap K^\sigma$, onde $K^\sigma = \{a \in K; \sigma(a) = a\}$.

Demonstração. No mergulho de D em $K((x^{-1};\sigma^{-1}))$, todo elemento $f \in D$ pode ser escrito da forma $\sum_{j \geq m} a_j x^{-j}$, onde $m \in \mathbb{Z}, a_j \in K$. Neste caso, como $\delta = 0$, a multiplicação é dada simplesmente por $x^j a = \sigma^j(a)x^j$, $a \in K, j \in \mathbb{Z}$. Se f está em $Z(K)$, então $xf = fx$ e $af = fa$ para todo $a \in K$. Como $xa_j = \sigma(a)a_j$, a primeira igualdade implica $a_j \in K^\sigma$; a segunda implica $aa_j = a_j\sigma^{-j}(a)$ para todo $j \geq m$; como σ^j não é interno, necessariamente se tem $a_j = 0$ para $j \neq 0$. □

Vamos especificar a discussão para a Álgebra de Weyl. Considere primeiramente $A_1(k)$. Chame $w = yx$.

Temos que $wx = xw + x$ e, portanto, a subálgebra de $A_1(k)$ gerada por x, w é $k[x][w;d]$, onde d é a derivação $x\partial_x$. Temos $yw = (w+1)y$, e assim a subálgebra de $A_1(k)$ gerada por y, w é $k[w][y;\theta]$, onde θ é o automorfismo de $k[w]$ definido por $w \to w + 1$.

É claro que o corpo de frações dessas duas subáglebras corresponde à totalidade do corpo de frações de $A_1(k)$, portanto temos:

$D_1(k) \cong k(x)(w;d) \cong k(w)(y;\theta)$.

De maneira indutiva, temos no caso de $A_n(k)$, definindo $w_i = y_i x_i$:

Proposição 2.12. *$D_n(k) \cong k(x_1, \ldots, x_n)(w_1;d_1)\ldots(w_n;d_n)$, onde $d_i = x_i\partial_{x_i}$.*

$D_n(k) \cong k(w_1, \ldots, w_n)(y_1;\theta_1)\ldots(y_n;\theta_n)$, onde $\theta_i(w_j) = w_j + \delta_{ij}$ e fixa os y_j com $j < i$.

Finalmente:

Proposição 2.13. *O centro de $D_n(k)$ é k.*

Demonstração. Aplicação direta do Lema nessa seção, pois os θ_i não são automorfismos internos. □

Como $k \subset A_n(k) \subset D_n(k)$, isto também nos dá que o centro de $A_n(k)$ é k.

2.6 Referências

Boa parte da seção 1 foi baseada em [Cou95]. Seções 2 e 3 foram baseadas em [GJ04], capítulos 2 e 6. O Teorema 2.4 teve sua demonstração baseada em [Bjo79], Capítulo 1, e o Teorema 2.5 teve sua demonstração baseada em [Jac62], Capítulo V. A Seção 4 foi baseada em [Cou95], e a Seção 5 em [Dum06], 3.2 e [Coh85], Capítulo 8.7.

Capítulo 3

Preliminares Algébricos

Neste Capítulo iremos coletar conceitos, definições e resultados de álgebra que serão utilizados em outras partes deste trabalho. Temos um seção em Teoria de Invariantes, discutindo alguns resultados básicos da área; uma seção sobre grupos de pseudo-reflexão, introduzindo alguns resultados muito importantes, como o Teorema de Chevalley-Shepard-Todd; uma seção com alguns conceitos e proposições de álgebra comutativa; e uma seção fazendo um apanhado da geometria algébrica que será utilizada no trabalho: em especial, o conceito de variedades normais e não-singulares, divisores, morfismos étale e quociente pela ação de grupos finitos.

3.1 Teoria Clássica de Invariantes

Seja inicialmente k um corpo arbitrário.

A Teoria Clássica de Invariantes estuda o que pode ser dito sobre anéis comutativos de invariantes sob ações de grupos. Existem várias questões naturais que aparecem, e disso nasce uma teoria bastante rica (para uma introdução, [Dol03], [Spr77]). Estaremos interessados em uma das primeiras e mais importantes questões levantadas sobre o assunto: sendo R uma k-álgebra finitamente gerada, quando R^G também é?

Existe uma vasta gama de resultados neste sentido. O resultado positivo mais importante é devido a Nagata (exposto, por exemplo, em [Dol03], Sec. 3.4), que diz que para todo grupo algébrico linear geometricamente redutivo G (para a definição, ver [Spr77]), R^G é finitamente gerada quando G age racionalmente numa variedade afim $\mathit{Specm}\, R$ (não necessariamente irredutível). Contra-exemplos para grupos lineares algébricos não-redutivos existem, trabalho também de Nagata ([Dol03], sec 4.3).

Para grupos finitos G, a questão da geração finita é particularmente simples:

Teorema 3.1. (Noether) *Seja R uma k-álgebra finitamente gerada, e G um grupo finito de k-automorfismos de R. Então R^G é finitamente gerada sobre k, e R é integral sobre R^G. Além disso, R é finitamente gerada como R^G módulo.*

Demonstração. Seja $a \in R$ arbitrário e considere o polinômio $\prod_{g \in G}(t - g.a)$. Seus coeficientes claramente pertencem a R^G, e este polinômio anula a. Portanto R é integral sobre R^G. Seja S a k-subálgebra de R^G gerada pelos coeficientes dos polinômios mônicos de $R^G[t]$ que anulam um conjunto finito de geradores de R. S é finitamente gerada e, portanto, noetheriana. R é integral sobre S, e finitamente gerada sobre S: logo R é um módulo finitamente gerado sobre S, pela Proposição 3.6. Como S é noetheriana, R^G também é um S-módulo finitamente gerado. Isso claramente implica que R^G é uma k-álgebra finitamente gerada. R é integral sobre R^G e finitamente gerada sobre este subanel (pois é sobre k) - portanto R é um R^G módulo finitamente gerado, (proposição 3.6). □

Observação. *No caso de R ser um domínio, R^G também é um domínio. Logo, pelo teorema Going-Up (Teorema 3.7), a função $\mathit{Spec}\, R \to \mathit{Spec}\, R^G$ é sobrejetor.*

Vamos apresentar, agora, outra prova desse teorema, no caso $R = k[x_1, \ldots, x_n]$, quando $char\, k = 0$, que usaremos posteriormente para provar o Teorema de Chevalley-Shephard-Todd. Seja G um grupo agindo linearmente em R, a priori não necessariamente finito.

Definição 3.1. *Seja $\theta : R \to R^G$ uma transformação k-linear que: (i) se restrinja à identidade em R^G e (ii) seja um homomorfismo de R^G-módulos. θ é um* operador de Reynolds.

Quando G é um grupo redutivo, o operador de Reynolds existe ([Stu93]). Isto é suficiente para a demonstração da geração finita de R^G que iremos exibir. Quando G é finito, a existência de tal operador é uma questão simples: basta definir

$$\theta(f) = \frac{1}{|G|} \sum_{g \in G} g(f),\ f \in R.$$

Temos que R é uma álgebra graduada (pelo grau dos polinômios), e que a ação de cada elemento de G preserva o grau. Dessa forma, R^G herda a graduação de R. Seja I o ideal de R gerado pelos elementos de R^G com termo constante 0. I é claramente um ideal graduado e, portanto, admite um conjunto finito de geradores homogêneos.

Teorema 3.2. *Sejam $f_1, \ldots, f_r$ geradores homogêneos de I. Então eles, juntamente com 1, geram R^G como k-álgebra.*

Demonstração. Seja f um polinômio em R^G. Queremos expressar f como polinômio em $f_1, \ldots, f_r$. Vamos fazer isso por indução em $deg\, f$. Basta considerarmos f um polinômio homogêneo. Se $deg\, f = 0$, isto é claro. Se $deg\, f > 0$, podemos escrever

$$f = s_1 f_1 + \ldots + s_r f_r,\ s_i \in R.$$

Como $f, f_1, \ldots, f_r$ são homogêneos, depois de possivelmente remover termos redundantes dos s_i, podemos supor cada s_i homogêneo e de grau $deg\, f - deg, f_i$. Aplicando o operador de Reynolds, temos

$$f = \theta(s_1) f_1 + \ldots \theta(s_r) f_r.$$

Como $\theta(s_i)$ são elementos homogêneos de R^G de grau menor do que f, por indução eles são polinômios em $f_1, \ldots, f_r$ e, portanto, também o é f. $\square$

Note que, apesar de nossas duas demonstrações mostrarem que $k[x_1, \ldots, x_n]^G$ é finitamente gerado, elas não nos dão procedimentos para encontrar os geradores de forma explícita. Essa questão em geral pode ser bastante complicada.

Para encerrar essa seção, anotemos o seguinte resultado simples:

Proposição 3.1. *Se R é um domínio integralmente fechado, R^G também o é.*

Demonstração. Denotemos $L = Frac\, R^G = (Frac\, R)^G$. É claro que $R^G = L \cap R$. Se $x \in L$ satisfaz um polinômio mônico com coeficientes em R^G, e portanto em R, $x \in R$ pois R é integralmente fechado. Portanto $x \in R^G$ $\square$

3.2 Grupos de Pseudo-Reflexão

Vamos relembrar alguns igredientes do Capítulo 1.

Definição 3.2. *Seja V um espaço vetorial de dimensão finita sobre os reais, com produto interno. Dado um hiperplano H de V, uma reflexão ortogonal com respeito à H é uma transformação $g \in GL(V)$ que fixa H ponto a ponto e manda os vetores do seu complemento ortogonal para os seus opostos aditivos. Um elemento $g \in GL(V)$ é chamado de uma* reflexão *se ele é reflexão com relação a algum hiperplano. Um subgrupo finito de $GL(V)$ é chamado de* grupo de reflexões ortogonais *se ele é gerado pelas reflexões que contém.*

Exemplo. *O exemplo mais simples são os grupos dihedrais, I_n, com $2n$ elementos. Eles são constituídos pelas transformações ortogonais que fixam um n-ágono regular centrado na origem. Ele é constituído por n rotações, múltiplas de $2\pi/n$ radianos, e n reflexões: se n é par, as reflexões são em relação às retas que ligam vértices opostos do polígono, ou pontos médios de arestas opostas; se n é ímpar, as reflexões são em relação aos eixos que ligam cada vértice ao ponto médio da aresta oposta. I_n é de fato um grupo de reflexões ortogonais, pois a rotação por $2\pi/n$ pode ser obtida pelo produto de duas reflexões em relação a retas que fazem um ângulo de π/n entre si.*

Exemplo. *S_n também é um grupo de reflexões. Ele age num espaço de dimensão n permutando os elementos da base canônica: $e_1, \ldots, e_n$. A transposição (ij) é obtida por meio da reflexão que manda $e_i - e_j$ para o seu negativo e fixa seu complemento ortogonal. Como S_n é gerado pelas transposições, ele é um grupo de reflexões ortogonais. Nessa ação, S_n fixa o vetor $e_1 + \ldots + e_n$, e estabiliza seu complemento ortogonal, que é o subespaço de dimensão $n-1$ constituído pelos vetores cuja soma das coordenadas é 0. Dessa forma, S_n também é um grupo de reflexões ortogonais de um espaço de dimensão $n-1$, e nesse caso é denotado por A_{n-1}.*

Exemplo. *Num espaço de dimensão n, temos também as reflexões $s_1, \ldots, s_n$: $s_i(e_j) = (-1)^{\delta_{ij}} e_j$. Essas trocas de sinal geram um grupo isomórfico a $\mathbb{Z}_2^n$, o qual tem intersecção trivial com S_n (com a ação igual à acima), e é conjugado por ele. O produto semidireto de S_n com $\mathbb{Z}_2^n$ gera um grupo de reflexões ortogonais, chamado de B_n. Podemos considerar também o produto semidireto de S_n com o grupo que muda um número* par *de sinais (mudanças pares de sinais são geradas pelas reflexões $(e_i + e_j) \to -(e_i + e_j), i \neq j$, e resultam em um grupo isomórfico a $\mathbb{Z}_2^{n-1}$); tal grupo é denotado por D_n. B_n tem ordem $2^n n!$, e D_n $2^{n-1} n!$.*

Grupos de reflexão são bastante estudados, pois além da sua beleza intrínseca, eles têm vastas aplicações em Teoria de Lie, por meio dos grupos de Weyl, [Hum72], Cap. III. Além disso, eles correspondem exatamente aos grupos de Coxeter finitos, [Hum90].

Um conceito ligeiramente mais amplo, mas que compartilha muitos dos resultados relacionados aos grupos de reflexão, é o seguinte.

A partir de agora, k é um corpo arbitrário de característica 0.

Definição 3.3. *Seja V um espaço vetorial de dimensão finita. Um elemento $g \in GL(V)$ é chamado de* pseudo-reflexão *se ele fixa um hiperplano ponto a ponto, e tem ordem finita. Se a ordem é 2, temos uma* reflexão. *Um subgrupo finito de $GL(V)$ é chamado de* grupo de pseudo-reflexões *se ele é gerado pelas pseudo-reflexões que contém. Similarmente, se for gerado pelas reflexões, temos um* grupo de reflexões.

Uma diferença significativa do caso de grupos de reflexões é que grupos de pseudo-reflexões não são grupos de Coxeter de uma maneira natural ([Hum90], pág. 66). É importante notar que a noção de grupo de pseudo-reflexões não depende apenas do grupo finito em consideração - ela envolve simultaneamente o grupo e sua representação fiel no espaço vetorial.

Quando $k = \mathbb{Q}$, os grupos de pseudo-reflexão são exatamente os grupos de Weyl, e quando $k = \mathbb{R}$ obtemos precisamente os grupos de reflexão reais. Quando $k = \mathbb{C}$ temos os chamados *grupos de reflexão unitários*, pois eles sempre são invariantes a uma forma hermitiana definida positiva.

De fato, sendo $(.,.)$ uma forma hermitiana definida positiva em V, arbitrária, definindo para todo par $v, w \in V$: $\langle v, w\rangle = \sum_{g \in G}(gv, gw)$, para G um grupo finito de automorfismos lineares agindo em V, temos uma forma hermitiana definida positiva tal que $\langle gv, gw\rangle = \langle v, w\rangle, \forall v, w \in V, \forall g \in G$. O mesmo procedimento se aplica claramente a produtos internos em espaços reais.

Vamos dar um exemplo de grupo de pseudo-reflexão que não é, em geral, de reflexão.

Definição 3.4. *Seja $\Omega = \{1, \ldots, n\}$ e G um grupo que age em Ω. Seja H um grupo e $B = H \times \ldots \times H$ n vezes. Existe uma ação de G em B dada por $g.(h_1, \ldots, h_n) = (h_{g(1)}, \ldots, h_{g(n)})$, $g \in G, h_i \in H$. O produto wreath, $H \wr_n G$, é o produto semi-direto de B por G. Seus elementos são da forma (h, g), com produto $(h, g)(h', g') = (hg.h', gg')$.*

Seja V um espaço vetorial de dimensão n sobre $\mathbb{C}$, e H o grupo cíclico gerado por uma raiz m-primitiva da unidade. $B = H \times \ldots \times H$, n vezes, age em V, que tem base $e_1, \ldots, e_n$, da seguinte forma $b.e_i = h_i e_i$, onde $b = (h_1, \ldots, h_n)$. Seja p um divisor de m, e $A(m,p,n)$ o subgrupo de B constituído pelos elementos b tais que $b^{m/p} = id$. A ação de S_n em B descrita na definição acima evidentemente se restringe a uma ação em $A(m,p,n)$, e denotamos $G(m,p,n)$ produto semidireto de $A(m,p,n)$ por S_n.

Proposição 3.2. *$G(m,p,n)$ é um grupo de pseudo-reflexões, gerado por pseudo-reflexões da forma $se_i = \lambda e_i$, $se_j = e_j$ $(j \neq i)$, onde λ é uma raiz m-ésima da unidade; ou da forma $se_i = \lambda e_i$, $se_j = \lambda^{-1} e_j$, $se_h = e_h$, $i \neq j$, $h \neq i, j$.*

Demonstração. [Spr77], Exercício 4.2.16. □

Para alguns valores de m, p, n recuperamos grupos conhecidos ([LT09], pág. 27): $G(m,p,1)$ é o grupo cíclico de ordem m/p; $G(1,1,n)$ é S_n; $G(2,1,n)$ é o grupo de Weyl B_n e $G(2,2,n)$ é o grupo de Weyl D_n; $G(m,m,2)$ é o grupo dihedral com 2m elementos.

Vamos desenvolver agora um pouco da teoria geral de grupos de pseudo-reflexões, para mostrar que eles podem ser de forma natural decompostos em componentes mais simples, os componentes essenciais irredutíveis, que possuem uma classificação completa; e para mostrar o Teorema de Chevalley-Shephard-Todd.

Definição 3.5. *Dada uma transformação linear g num espaço V de dimensão finita, denotamos $Fix\, g = \{v \in V | gv = v\} = Ker\,(Id - g)$, e $[V, g] = Im(Id - g)$.*

Se g é uma pseudo-reflexão diferente da identidade, $Fix\, g$ é um hiperplano e $[V, g]$ é um espaço de dimensão 1. Neste caso, se $a \in V$ gera $[V, g]$, então para todo elemento v de V existe $\phi(a) \in k$ tal que $v - gv = \phi(v)a$. ϕ é claramente um funcional linear, e $ker\, \phi = Fix\, g$.

Lema 3.1. *Se $g, h \in GL(V)$, então $Fix(ghg^{-1}) = gFix\, h$. Em particular, se h é uma pseudo-reflexão diferente da unidade, que fixa um hiperplano H, ghg^{-1} é uma pseudo-reflexão que fixa o hiperplano gH.*

Lema 3.2. *Seja g uma pseudo-reflexão diferente da unidade, de ordem m, $H = Fix\, g$, e L_H qualquer funcional linear com $H = kerL_H$ (note que L_H é determinado a menos de escalar). Suponha que a gera $[V, g]$. Então existe uma raiz m-ésima primitiva da unidade μ tal que $rv = v - (1-\mu)\frac{L_H(v)}{L_H(a)}a$, para todo $v \in V$.*

Demonstração. Como vimos acima, existe um funcional linear ϕ tal que $gv = v - \phi(v)a$ e $H = ker\, \phi$. Portanto $ga = \mu a$ para alguma raiz primitiva da unidade de ordem m μ, e assim $\phi(a) = 1 - \mu$. Temos que $\phi = \lambda L_H$ para algum $\lambda \neq 0 \in k$, e isso nos dá imediatamente que $\lambda = (1-\mu)/L_H(a)$, o que completa a prova. □

Lema 3.3. *Sejam r, s pseudo-reflexões diferentes da identidade, $H = Fix\, r$, $J = Fix\, s$, a um gerador de $[V, r]$ e b um gerador de $[V, s]$. Se $a \in J$ e $b \in H$, então $rs = sr$.*

Demonstração. Usando o lema acima temos escalares $\mu, \nu \in k$, tais que, para todo $v \in V$.

$$rs(v) = v - (1-\mu)\frac{L_H(v)}{L_H(a)}a - (1-\nu)\frac{L_J(v)}{L_J(b)}b + (1-\mu)(1-\nu)\frac{L_H(b)L_J(v)}{(L_H(a)L_J(b))}a.$$

Se $b \in H$, $L_H(b) = 0$, e portanto o último termo acima desaparece. Por simetria, o último termo da expressão $sr(v)$ desaparece, e o que resta é igual. Logo $rs = sr$. □

Proposição 3.3. *Um subespaço V' de V é invariante com respeito a uma pseudo-reflexão $r \neq id$ se e somente se $V' \subseteq Fix\, r$ ou $[V, r] \subseteq W$.*

Demonstração. Se $V' \subseteq Fix\, r$, então obviamente V' é invariante. Se $[V, r] \subseteq V'$, então a fórmula do lema 3.2 mostra que V' é invariante. Reciprocamente, se V' é invariante e não está contido em $Fix\, r$, então $[V', r] \neq 0$ e, portanto, $[V, r] = [V', r] \subseteq V'$. □

Definição 3.6. *Seja W um grupo finito de pseudo-reflexões. Dizemos que ele é irredutível se a sua representação natural é irredutível.*

Proposição 3.4. *Seja W um grupo finito de pseudo-reflexões num espaço vetorial V. Seja $V_1 \oplus \ldots \oplus V_m$ uma decomposição de V em subespaços invariantes por W e irredutíveis (isso é possível pelo Lema de Maschke, lembrando que char $k = 0$). Seja W_i a restrição de W para V_i, $i = 1, \ldots, m$. Então W_i é um grupo de pseudo-reflexão irredutível, e $W \cong W_1 \times \ldots \times W_m$.*

Demonstração. Pelo lema acima, se r é uma pseudo-reflexão $\neq id$, então $[V, r] \subseteq V_i$ para algum i. Seja W_i o subgrupo de W gerado pelas pseudo-reflexões tais que isso ocorre. W_i fixa todo elemento de V_j, para $i \neq j$, e pelo lema 3.3, os elementos de W_i comutam com os elementos de W_j. Portanto, W é o produto direito dos W_i, e cada W_i por sua vez evidentemente é um grupo de pseudo-reflexões em V_i. □

Usando a última proposição, é fácil ver que cada grupo de pseudo-reflexões pode ser decomposto em componentes irredutíveis. A classificação dos grupos de Weyl e grupos de reflexão irredutíveis é bem conhecida, [Hum90], usando diagramas de Dynkin. Uma classificação dos grupos de reflexão unitários também existe: ela foi realizada por Shephard e Todd, [ST54]. É um caso muito mais complexo do que os anteriores; os grupos $G(m, p, n)$ são exemplos de grupos irredutíveis, exceto para $G(2, 2, 2)$ e $G(1, 1, n)$ ([LT09], pág. 27). Uma exposição moderna da classificação pode ser encontrada em [LT09].

É um fato notável que, tendo a classificação dos grupos de pseudo-reflexão irredutíveis para $\mathbb{C}$ nos permite obter uma classificação para *todos* os corpos de característica 0.

Dado um grupo irredutível de reflexões unitárias $W \subset GL_n(\mathbb{C})$, com representação natural ρ, seja $\chi : W \to \mathbb{C}^*$ o seu caráter. Seja $\mathbb{Q}(\chi)$ a extensão de $\mathbb{Q}$ gerada pelos valores possíveis de χ.

Teorema 3.3. (Clark-Ewing) *Seja G um grupo finito e k um corpo arbitrário de característica* 0. *Então G tem uma representação sobre k como grupo de pseudo-reflexões irredutível, se e somente se, ele tiver uma representação como grupo de reflexão unitário irredutível, com caráter χ, e $\mathbb{Q}(\chi) \subseteq k$.*

Demonstração. Teorema 15-2 em [Kan01]. □

Observação. *Para grupos finitos arbitrários, não é o caso que $\mathbb{Q}(\chi) \subseteq k$ implique que a representação é realizável sobre k. Uma medida do quão longe isto é de ser verdade é dada pelo índice de Schur, [Jac89], 5.14.*

Este resultado nos remete ao clássico teorema que diz que todas as representações irredutíveis de S_n são realizáveis sobre $\mathbb{Q}$ - isto é, que suas representações são absolutamente irredutíveis. Usando a classificação de Shephard-Todd dos grupos complexos unitários irredutíveis, para classificar os grupos de pseudo-reflexão irredutíveis em k, basta ver para quais grupos da lista $\mathbb{Q}(\chi)$ está contido em k. Checando a lista, vemos que $\mathbb{Q}(\chi)$ envolve apenas os elementos $\epsilon_n = e^{2\pi i/n}(n \geq 1), \epsilon_n + \epsilon_n^{-1}, \sqrt{\pm 2}, \sqrt{5}, \sqrt{7}$ ([Kan01], pág. 175).

Um resultado impressionante, o qual demonstra a posição de destaque dos grupos de pseudo-reflexão dentre os grupos finitos, é o seguinte:

Teorema 3.4. (Chevalley-Shephard-Todd) *Seja V um espaço vetorial de dimensão finita e $G \subset GL(V)$ um grupo finito. $S(V^*)^G$ é isomórfico a uma álgebra polinomial (necessariamente em dim$V$ variáveis), se e somente se, G é um grupo de pseudo-reflexões.*

Este resultado também tem uma aplicação muito importante: seja L uma álgebra de Lie semisimples de dimensão finita sobre um corpo algebricamente fechado de caractrística 0. Temos o isomorfismo de Harish-Chandra de $Z(U(L))$ para $S(H)^W$, onde H é uma subálgebra de Cartan e W

é o grupo de Weyl ([Car05], Teorema 11.30). Pelo Teorema de Chevalley-Shephard-Todd, concluímos que o centro da álgebra universal envolvente é uma álgebra polinomial em $dim\, H$ variáveis.

Vamos provar a implicação de que se G é grupo de pseudo-reflexão, então $S(V^*)$ é a álgebra polinomial - utilizaremos apenas esse sentido da equivalência. Uma prova completa (com outras equivalências) pode ser encontrada em [Spr77], Capítulo 4.

Denotaremos por $S = S(V^*) \cong k[x_1, \ldots, x_n]$ e $R = S^G$ no que se segue.

Lema 3.4. *Se $r \neq id$ é uma pseudo-reflexão em V e $H = Fix\, r$, então para todo $P \in S$ existe um $Q \in S$ com $rP = P + L_H Q$, onde L_H é qualquer forma linear tendo H como conjunto de zeros.*

Demonstração. Vamos mostrar isto primeiramente para $P = \phi \in V^*$ um funcional linear. r^{-1} também é uma pseudo-reflexão, e $H = Fix\, r^{-1}$. Seja a um gerador de $[V, r^{-1}]$. Do Lema 3.2 existe $\mu \in k$, tal que $r^{-1}v = v + \mu L_H(v)a$ para todo $v \in V$. Portanto, para todo $\phi \in V^*$ nós temos $r\phi(v) = \phi(v) + \mu L_H(v)\phi(a)$; isto é, $r\phi - \phi = \mu L_H$. Suponha agora que para polinômios $P_1, P_2 \in S$ existam $Q_1, Q_2 \in S$, tal que $rP_1 = P_1 + L_H Q_1$ e $rP_2 = P_2 + L_H Q_2$. Então

$$r(P_1P_2) - P_1P_2 = r(P_1)(r(P_2) - P_2) + (r(P_1) - P_1)P_2 = r(P_1)L_H Q_2 + L_H Q_1 P_2 = L_H(r(P_1)Q_2 + Q_1P_2),$$

e o resultado vale para P_1P_2. Como S é gerado pelos funcionais lineares, temos o que queríamos. □

Vamos relembrar algumas notações introduzidas na seção anterior. Seja I o ideal homogêneo de S gerado pelos elementos de R com termo constante 0, e seja θ o operador de Reynolds.

Lema 3.5. *Sejam $f_1, \ldots, f_r \in R$, com f_1 não pertencente ao ideal de R gerado por $f_2, \ldots, f_r$. Suponha que $g_1, \ldots, g_r$ são elementos homogêneos de S satisfazendo (*)$f_1g_1 + \ldots f_rg_r = 0$. Então $g_1 \in I$.*

Demonstração. Note que f_1 não pode pertencer ao ideal de S gerado por $f_2, \ldots, f_r$. Caso contrário, teríamos, para alguns $h_i \in S$ homogêneos, $f_1 = f_2h_2 + \ldots f_rh_r$. Aplicando o operador de Reynolds, nos daria $f_1 = f_2\theta(h_2) + \ldots f_r\theta(h_r)$. Isto implicaria que f_1 está no ideal de R gerado pelos outros f_i, contrariando a hipótese. Para provar que $g_1 \in I$, procederemos por indução em $deg\, g_1$. Se g_1 tem grau 0, então ele deve ser 0, caso contrário, f_1 pertenceria ao ideal de S gerado pelos outros f_i, o que acabamos de ver ser impossível. Suponha então $deg\, g_1 > 0$. Seja $s \neq id$ uma pseudo-reflexão em W, e l um funcional linear que tem $Fix\, s$ como seu conjunto de zeros. Pelo lema acima, existem $h_i \in S$, $i = 1, \ldots, r$, tal que $sg_i - g_i = lh_i$. Como sg_i, g_i são homogêneos de mesmo grau, isso implica que h_i também é homogêneo, de grau menor que g_i. Aplicando s na equação (*) e subtraindo (*) temos portanto:

$$l(f_1h_1 + \ldots + f_rh_r) = 0.$$

Como l não é identicamente nulo, isso nos dá $f_1h_1 + \ldots + f_rh_r = 0$ (note que o corpo é infinito). Por indução, como $deg\, h_1 < deg\, g_1$, temos que $h_1 \in I$. Portanto, $sg_1 \equiv g_1 (mod\, I)$. Como W estabiliza I, ele age de maneira natural no anel S/I. Acabamos de ver que cada pseudo-reflexão atua de maneira trivial na imagem de g_1 em S/I; como essas pseudo-reflexões geram W, temos que $wg_1 \equiv g_1 (mod\, I)$ para todo $w \in W$. Isso implica que $\theta(g_1) \equiv g_1 (mod\, I)$. Isso nos dá $g_1 \in I$, pois $\theta(g_1) \in I$. □

Podemos agora provar o Teorema de Chevalley-Shephard-Todd.

Demonstração. Sejam $f_1, \ldots, f_r$ um conjunto de geradores de I, com o menor número possível de elementos. Sabemos, pelo Teorema 3.2, que eles e a unidade geram R. Portanto, resta provar que eles são algebricamente independentes e que $r = n$. Primeiramente, a independência algébrica. Suponha que exista um polinômio $h(y_1, \ldots, y_r)$, tal que $h(f_1, \ldots, f_r) = 0$. Sendo $\alpha y_1^{e_1} \ldots y_r^{e_r}$ um dos monômios de h, e chamando $d_i = deg\, f_i$, $i = 1, \ldots, n$ (grau em $x_1, \ldots, x_n$), temos chamando $d = \sum_i e_i d_i$ que o grau de $\alpha f_1^{e_1} \ldots f_r^{e_r}$ é d (nas variáveis x_i). Sendo $h*$ a soma de todos os monômios de h com a propriedade que a substituição de y_i por f_i resulta em polinômio de grau d, evidentemente temos que $h * (f_1, \ldots, f_r) = 0$. Portanto, sem perda de generalidade, podemos supor que h é constituído apenas de monômios com essa propriedade. Fixando k, e derivando $h(f_1, \ldots, f_r)$ por x_k, temos: (*) $\sum_{i=1}^{r} h_i \partial_{x_k} f_i = 0$, onde $h_i = \partial_{y_i} h$. Cada h_i é homogêneo de grau $d - d_i$, e cada $\partial_{x_k} f_i$ é homogêneo. Renumeremos, se necessário, os h_i de forma que $h_1, \ldots, h_m$ seja um conjunto minimal de geradores do ideal de R gerado por $h_1, \ldots, h_r$, $m \leq r$.

Se $i > m$, podemos escrever

$$h_i = \sum_{j=1}^{m} g_{ij} h_j,\ g_{ij} \in R.$$

h_i é um polinômio homogêneo de grau $d - d_i$ nas variáveis $x_1, \ldots, x_n$, portanto, descartando termos redundantes, podemos supor g_{ij} homogêneo de grau $d_j - d_i$. Substituindo essas equações acima em (*), temos para cada k:

$$\sum_{i=1}^{m} h_i (\partial_{x_k} f_i + \sum_{j=m+1}^{r} g_{ji} \partial_{x_k} f_j) = 0.$$

Abreviando as expressões em parênteses por p_i, temos que são polinômios homogêneos de grau $d_i - 1$. Aplicando o lema acima, temos que $p_1 \in I$ e, portanto, para cada k:

$$\partial_{x_k} f_1 + \sum_{j=m+1}^{r} g_{j1} \partial_{x_k} f_j = \sum_{i=1}^{r} f_i q_i,$$

para alguns $q_i \in S$.

Multiplicando essa identidade por x_k e somando sobre k, podemos usar a identidade e Euler: se f é um polinômio homogêneo em $x_1, \ldots, x_n$,

$$\sum_{i=1}^{n} x_i \partial_{x_i} f = (deg\, f) f.$$

Obtemos assim:

$$d_1 f_1 + \sum_{j=m+1}^{r} d_j g_{j1} f_j = \sum_{i=1}^{r} f_i r_i,$$

com os $r_i \in S$ de grau maior que 0.

Os termos do lado esquerdo são homogêneos de grau d_i e, portanto, do lado direito $f_i r_i$ deve se cancelar com outros termos de grau diferente de d_i. Após descartar todos os termos, menos os de grau d_i, escrevemos f_1 como elemento do ideal de S gerado por $f_2, \ldots, f_r$, contrariando a hipótese inicial. Assim temos a independência algébrica.

Finalmente, temos pela proposição 1.1 e lema 1.1 que $trdeg_k Frac\, R = n$; portanto $r = n$. □

Seja W um grupo de pseudo-reflexões. Seja $f_1, \ldots, f_n$ um conjunto de geradores algebricamente independentes de $S(V^*)^G \cong k[x_1, \ldots, x_n]^W$ ($n = dim\, V$). Vamos relacioná-los com aspectos geométricos do grupo de pseudo-reflexões. Seja (*) M a matriz $n \times n$ cuja entrada ij é $\partial_{x_j} f_i$, e seja J seu determinante.

Cada pseudo-reflexão diferente da identidade em W fixa um hiperplano. Seja $\mathbb{S}$ o conjunto das pseudo-reflexões em W, e para cada $s \in \mathbb{S}$ seja L_s uma forma linear cujo conjunto de zeros é $Fix\, s$.

Teorema 3.5. *Um elemento h de $k[x_1, \ldots, x_n]$ é chamado de semi-invariante se $w.h = det(w)h$ para todo $w \in W$. J é semi-invariante, e todo elemento semi-invariante se escreve como produto de J por um elemento invariante. $J = a \prod_{s \in \mathbb{S}} L_s$, onde a é um escalar que varia de acordo com a escolha de geradores algebricamente independentes e das formas lineares L_s. Finalmente, $J \neq 0$.*

Demonstração. [Kan01], 20-2, Proposição A e B, 21-1, Proposição A e B. □

Seja X um subconjunto qualquer de V. Denotamos por $isp(X) = \{w \in W | w.x = x, \forall x \in X\}$ o grupo de isotropia de X. Temos o seguinte resultado de Steinberg:

Teorema 3.6. (Steinberg) *Dado qualquer subconjunto X de V, $isp(X)$ é gerado pelas pseudo-reflexões que contém.*

Demonstração. [Kan01], Corolário 26-1. □

3.3 Álgebra Comutativa

Nesta seção, iremos relembrar alguns fatos bem conhecidos de álgebra comutativa. As demonstrações podem ser encontradas em [AM69] e [Mat89]. Por economia de espaço, assumiremos o equivalente a aproximadamente os Capítulos 1,2,3 de [AM69] - em particular, as propriedades de localização.

Definição 3.7. *Sejam $A \subseteq B$ dois anéis. Um elemento $b \in B$ é dito* integral *sobre A se ele é anulado por um polinômio mônico com coeficientes em A: isto é, se $b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0 = 0$ para alguns $a_i \in A$, $n \geq 1$. Se todo elemento de B é integral sobre A, então diz-se que B é integral sobre A.*

Proposição 3.5. *Sejam $A \subseteq B$ dois anéis, $x \in B$. x é integral sobre A, se e somente se, o anel $A[x]$ gerado por A, x é um A-módulo finitamente gerado.*

Proposição 3.6. *Se $A \subseteq B$, e B é uma A-álgebra finitamente gerada e integral sobre A, então B é um A-módulo finitamente gerado.*

Proposição 3.7. *Sejam $A \subseteq B$ dois anéis. O conjunto dos elementos de B integrais sobre A constitui um anel C, chamado de* fecho integral *de A.*

Proposição 3.8. *Sejam $A \subseteq B$, e S um conjunto multiplicativamente fechado de A. Se B é integral sobre A, B_S é integral sobre A_S. Se C é o fecho integral de A em B, C_S é o fecho integral de A_S em B_S.*

Definição 3.8. *Seja A um domínio. A é chamado de* integralmente fechado *se A é o seu fecho integral em $Frac\, A$.*

Proposição 3.9. *Todo domínio de fatoração única é integralmente fechado. Em particular, $k[x_1, \ldots, x_n]$ é integralmente fechado. A localização de um domínio integralmente fechado sempre é integralmente fechada, tendo em vista a proposição 3.8.*

Teorema 3.7. (Going-Up) *Sejam $A \subseteq B$ anéis, B integral sobre A. Dados ideais primos $p_1 \subsetneq p_2$ de A e um ideal primo q_1 de B, tal que $p_1 = q_1 \cap A$, existe um ideal primo de B, $q_2 \supsetneq q_1$, tal que $p_2 = q_2 \cap A$. Se q_2' é outro ideal primo com $q_2' \cap A = p_2$ e $q_2 \subseteq q_2'$, então $q_2 = q_2'$.*

Proposição 3.10. *Seja A um domínio, S um conjunto multiplicativamente fechado de A, e G um grupo finito de automorfismos de A com $G(S) \subseteq S$. Então $(A_S)^G = A^G_{S^G}$, vistos como subanéis de $Frac\, A$.*

Demonstração. Idêntica à prova da Proposição 1.1. □

Proposição 3.11. *Seja A um anel e G um grupo finito de automorfismos de A. Seja p um ideal primo de A^G. O conjunto dos ideais primos P de A tais que $P \cap A^G = p$ é permutado por G transitivamente; em particular, ele é finito.*

Demonstração. Sejam P_1, P_2 ideais primos de A com $P_i \cap A^G = p$, $i = 1, 2$. Seja $x \in P_1$. $\prod_{g \in G} g(x) \in P_1 \cap A^G = p \subseteq P_2$ e, portanto, $h(x) \in P_2$ para algum $h \in G$. Dessa forma, $P_1 \subseteq \bigcup_{g \in G} g(P_2)$. Por "prime avoidance"([Mat89], exercício 1.6) e o Teorema Going-Up, isso implica que $P_1 = h(P_2)$ para algum $h \in G$. □

Definição 3.9. *Seja A um anel comutativo. Dada uma cadeia de ideais primos $p_0 \subsetneq p_1 \subsetneq \ldots \subsetneq p_n$, dizemos que ela tem comprimento n. A dimensão de Krull do anel A, $\dim A$ é o supremo do comprimento de tais cadeias.*

Definição 3.10. *Seja A um anel Noetheriano local, com ideal maximal m, de dimensão d, e corpo residual $k = A/m$. A é um* anel regular local *se $\dim_k m/m^2 = d$, ou de maneira equivalente, m pode ser gerado por d elementos.*

Em geral se tem $\dim A \leq \dim_k m/m^2$. O conceito de anel regular local é a tradução puramente algébrica do conceito de suavidade em um ponto. Isto fica claro em virtude das seguintes definição e teorema:

Definição 3.11. *Seja $Y \subseteq k^n$ uma variedade afim, com $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$ um conjunto de geradores do ideal de Y. Y é não-singular em um ponto $P \in Y$ se o posto da matriz M, $r \times n$, de entrada ij correspondendo a $\partial_j f_i(P)$ é $n - r$, onde r é a dimensão de Y.*

Teorema 3.8. (Critério Jacobiano) *Seja $Y \subseteq k^n$ uma variedade afim, $P \in Y$. Y é não-singular em P se e somente se $O_{Y,P}$ é um anel regular local.*

Demonstração. [Har77], Capítulo I, Teorema 5.1. □

Definição 3.12. *Um anel A, Noetheriano, é* regular *se todas as suas localizações A_p, para todos os seus ideais primos p, são anéis regulares locais.*

No caso de A ser o anel de funções regulares numa variedade afim, isso se traduz no fato dela ser suave em todos os seus pontos (ver definição 3.16 na seção seguinte).

Teorema 3.9. *Dado um corpo k, o anel de polinômios $k[x_1, \ldots, x_n]$ é regular. Isto é correspondente algébrico ao fato "óbvio"de que o espaço afim é suave.*

Proposição 3.12. *Se A é um anel regular e S um conjunto multiplicativamente fechado, então A_S também é regular.*

Demonstração. A localização de um anel Noetheriano é sempre Noetheriana. Os ideias primos de A_S são da forma pA_S, onde p é um ideal primo de A que tem interseção disjunta com S. $(A_S)_{pA_S} \cong A_p$, dado que localização é transitiva. Logo, todas as localizações de A_S em ideias primos são anéis regulares locais. □

Encerraremos essa seção introduzindo o conceito de diferenciais de Kähler.

Definição 3.13. *Sejam $A \subset B$ dois anéis. Uma A-derivação de B em um B-módulo M é um mapa $d : B \to M$, tal que d é um homomorfismo de grupos abelianos, $d(bb') = bd(b') + b'd(b), \forall b, b' \in B$, e $d(a) = 0$ para todo $a \in A$. O conjunto de todas A-derivações de B para B é denotado por $Der_A B$, e é claramente um B módulo: $(b\delta)(b') = b\delta(b'), \delta \in Der_A(B), b, b' \in B$.*

Definição 3.14. *Definimos o* módulo de formas diferenciais relativas *de B sobre A como o B-módulo $\Omega_{B/A}$ junto com uma A-derivação $d : B \to \Omega_{B/A}$ com a seguinte propriedade universal: para todo B-módulo M e $d' : B \to M$ uma A-derivação, existe um único homomorfismo de B-módulos $f : \Omega_{B/A} \to M$ tal que $d' = fd$.*

Tal módulo $\Omega_{B/A}$ é claramente único a menos de isomorfismo, pela proriedade universal. Ele pode ser construído de maneira simples, como quociente do módulo livre gerado por símbolos da forma $db, b \in B$, pelas relações $d(b+b') - db - db'$, $d(bb') - bd(b') - b'd(b)$ e da, $b, b' \in B$, $s \in A$. A derivação $d : B \to \Omega_{B/A}$ é definida enviando $b \to db$. Pela definição, é claro que $Der_A B = Hom_B(\Omega_{B/A}, B)$.

Teorema 3.10. (Primeira Sequência Exata) *Sejam $A \subset B \subset C$ anéis comutativos. Então existe uma sequência exata de C-módulos:*

$$\Omega_{B/A} \otimes_B C \to \Omega_{C/A} \to \Omega_{C/B} \to 0.$$

Demonstração. [Liu02], Capítulo 6, Proposição 1.8. □

Proposição 3.13. *Seja B uma A-álgebra e S um conjunto multiplicativamente fechado de B. Então,* $(\Omega_{B/A})_S \cong \Omega_{B_S/A}$.

Demonstração. [Liu02], Capítulo 6, Proposição 1.8. □

Encerrando esta seção, vamos demonstrar a Proposição 2.10

Lema 3.6. *Seja $\Lambda = k[x_1, \ldots, x_n]$, e S um subconjunto multiplicativamente fechado deste anel. Então $Der_k(\Lambda)_S \cong Der_k(\Lambda_S)$.*

Demonstração. Procedendo de maneira análoga à demonstração da proposição 2.1, se mostra que $\Omega_{\Lambda/k}$ é livre de dimensão n (para detalhes, [MR01], 5.1.11). Λ_S é um módulo plano, uma vez que localização é um funtor exato. Logo, $Der_k(\Lambda)_S \cong \Lambda_S \otimes Hom_\Lambda(\Omega_{\Lambda/k}, \Lambda) \cong Hom_{\Lambda_S}(\Omega_{\Lambda_S/k}, \Lambda_S) \cong Der_k(\Lambda_S)$. Nesta cadeia de isomorfismos usamos a proposição acima e um homomorfismo bem conhecido, no segundo isomorfismo: [Mat89], Teorema 7.11. □

Finalmente, a prova da Proposição 2.10:

Demonstração. O lema acima mostra que $D(\Lambda_S)$ é gerado, sobre Λ_S, por elementos de $Der_k\Lambda$. Usando as relações de comutação $\delta a - a\delta = \delta(a)$, podemos escrever cada elemento de $D(\Lambda_S)$ da forma $s^{-1}r$ ou rs^{-1}, onde $s \in S, r \in D(\Lambda)$. Portanto, como a localização é única à menos de isomorfismo, $D(\Lambda)_S \cong D(\Lambda_S)$. □

3.4 Geometria Algébrica

Devido à complexidade mesmo das definições mais básicas (por exemplo, a mera definição do que é um esquema requer um conhecimento mínimo prévio de feixes) e das proposições mais básicas (por exemplo, a demonstração de que $Spec\,A$ é um espaço localmente anelado é extremamente técnica), e pela economia de espaço, assumiremos uma quantidade razoável de pré-requisitos nesta seção: aproximadamente, o equivalente aos Capítulo I, Seção 1-5, Capítulo II, Seção 1-5, de [Har77], relembrando apenas as coisas cruciais para o restante do trabalho.

Uma dessas coisas é o conceito de variedade abstrata. Por simplicidade, consideraremos apenas corpos algebricamente fechados.

Definição 3.15. *Uma variedade abstrata é um esquema integral separado de tipo finito sobre um corpo algebricamente fechado k.*

Nesta seção, por simplicidade, iremos na maior parte dos casos assumir que nossos esquemas são variedades sobre k. Sempre que discutirmos morfismos de esquemas sobre k, assumiremos que o morfismo em questão é um k-morfismo.

Outra coisa que merece uma atenção especial é a ponte de geometria algébrica clássica para geometria algébrica moderna - dita em outras palavras, a relação entre $Specm\,A$, o conjunto de ideais maximais, e $Spec\,A$, o conjunto de ideais primos. Em geral, propriedades de pontos fechados numa variedade são suficientes para entender propriedades em todos os pontos - veremos alguns exemplos disso. Vale a pena destacar dois resultados:

Teorema 3.11. *Seja k um corpo algebricamente fechado. Existe um funtor F fiel e pleno da categoria de variedades quasi-projetivas para a categoria de esquemas. Para toda variedade quasi-projetiva V, ela é homeomorfa ao conjunto de pontos fechados de $F(V)$, e seu feixe de funções regulares é obtido a partir da restrição do feixe de funções regulares de $F(V)$ via esse homeomorfismo. A imagem do funtor F é o conjunto de esquemas quasi-projetivos sobre k e integrais.*

Demonstração. [Har77], Proposição 2.6 e 4.10 do Capítulo II. □

Proposição 3.14. *O conjunto de pontos fechados numa variedade abstrata X é denso. De fato, mais ainda vale: seja U um aberto de X. Se $p \in U$ é um ponto fechado em U, então ele também é fechado em X.*

Demonstração. [Liu02], Capítulo 2, Lema 4.3 □

Passados esses preliminares, vamos introduzir os conceitos de variedades não-singulares e normais.

Definição 3.16. *Uma variedade X é não-singular se os anéis de germes em todos os seus pontos são anéis regulares locais.*

Este é um exemplo de propriedade que precisa ser checada apenas nos pontos fechados. De fato, dado qualquer ponto $p \in X$, seja $Spec\, A$ um aberto afim que o contém. Este aberto contém um ponto fechado, m, que corresponde a um ideal maximal de A contendo p (identificado com um ideal primo de A). O anel de germes de X em p é $A_m \cong (A_m)_p$. Agora, A_m é um anel regular local, e por um célebre resultado de Serre, toda localização de um anel regular local é um anel regular local ([Mat89], Teorema 19.3). No caso de variedades afins, os pontos fechados correspodem a pontos num espaço afim k^n (Nullstellensatz de Hilbert, [Mat89], Teorema 5.4), onde a variedade está imersa e, para checar sua regularidade basta usar o critério Jacobiano, Teorema 3.8.

Exemplo. *Quando A é um domínio regular finitamente gerado como k-álgebra, $Spec\, A$ é uma variedade não-singular.*

O próximo exemplo requer duas definições fundamentais:

Definição 3.17. *Seja X uma variedade e $p \in X$ um ponto fechado, com anel de germes em p $O_{X,p}$ e ideal maximal m_p. $m_p/(m_p)^2$ tem naturalmente uma estrutura de $k(p)$-espaço vetorial, onde $k(p)$ é o corpo residual $O_{X,p}/m_p$. Pelo Teorema Nullstellensatz de Hilbert ([Mat89], Teorema 5.4), $k(p)$ é apenas k. O* plano tangente *em p, denotado por T_p, é o dual $Hom_k(m_p/(m_p)^2, k)$ com a estrutura de k-espaço vetorial. Seja $f : X \to Y$ um morfismo entre variedades que leva o ponto fechado $p \in X$ no ponto fechado $q = f(p) \in Y$. f induz uma função $m_q/(m_q)^2 \to m_p/(m_p)^2$, que tomando o dual induz uma função $df : T_p \to T_q$, uma k-transformação linear, que é a* diferencial *de f.*

Se X for uma variedade afim, usando sua imersão em k^n para algum espaço afim, temos que T_p é naturalmente isomorfo ao subespaço de k^n definido por $\{(t_1, \dots, t_n) \in k^n | \sum_{j=1}^{n} \partial_j F_i(p) t_j = 0; i = 1, \dots, m\}$, onde $F_1, \dots, F_m$ geram o ideal que define X ([Liu02], Proposição 2.5). Desta forma, o critério Jacobiano (Teorema 3.8) diz que X é não-singular em p, se e somente se, $dim_k T_p = dim X$.

Definição 3.18. *Seja G uma variedade afim irredutível, com estrutura de grupo. Então G é um* grupo algébrico linear *se a multiplicação $G \times G \to G$ e a inversa $G \to G$ são mapas regulares. Note que a topologia de $G \times G$ é a topologia de Zariski, que não coincide em geral com a topologia produto. Uma definição equivalente é: G é um grupo algébrico se, e somente se, ele for um subgrupo e subconjunto fechado de $GL_n(k) = Spec\, k[x_{ij}]_{det}$, $1 \leq i, j \leq n$, [Fog69].*

Exemplo. *Seja G um grupo algébrico linear. As translações por g, para todo elemento de G, mostram que os planos tangentes dos pontos fechados são todos isomórficos: $dg : T_h \to T_{gh}$ é um isomorfismo, de inversa dg^{-1}. Um ponto fechado g é não-singular, se e somente, se $dim_k T_g = dim\, G$. Sabemos que o conjunto de pontos fechados não-singulares é não-vazio (na verdade, é um aberto denso no subespaço de pontos fechados, [Har77], Teorema 1.5.3). Portanto, todos os pontos fechados são não-singulares e, dessa forma, G é não-singular.*

Definição 3.19. *Uma variedade é normal quando os anéis de germes de todos os seus pontos são domínios integralmente fechados.*

Esta propriedade precisa ser checada apenas nos pontos fechados. O argumento é igual ao caso de não-singularidade, usando o fato de que a localização de um domínio integralmente fechado é integralmente fechada, Proposição 3.11.

Exemplo. *Seja A um domínio finitamente gerado como k-álgebra. Ser integralmente fechado é uma propriedade local ([AM69], Proposição 5.13). Então $Spec\, A$ é uma variedade normal, se e somente se, A for integralmente fechado.*

Estendendo o exemplo acima, temos o seguinte resultado:

Proposição 3.15. *Uma variedade X é normal, se e somente se, $O_X(U)$ for um domínio integralmente fechado para todo aberto U de X.*

Demonstração. [Liu02], Capítulo 4, Proposição 1.5. □

Exemplo. *Toda variedade não-singular é normal. Isto segue de um célebre teorema de Auslander e Buchsbaum ([Mat89], Teorema 20.3), o qual diz que todo anel regular local é um domínio de fatoração única.*

Para nós, o principal fato a respeito de variedades normais é o seguinte:

Teorema 3.12. *Sejam X uma variedade normal e F um subesquema fechado de codimensão maior ou igual a dois. Então a restrição $O_X(X) \to O_X(X - F)$ é um isomorfismo.*

Demonstração. [Liu02], Teorema 1.14, Capítulo 4. □

Esse fato é essencialmente uma tradução geométrica do seguinte fato bem conhecido de álgebra comutativa, uma vez que para uma variedade $O_X(U) = \bigcap_{p \in U} O_{X,p}$, onde todos os anéis envolvidos são vistos como subanéis do corpo $K(X) = Frac\, O_X(X)$ ([Liu02], Capítulo 2, Proposição 4.18).

Teorema 3.13. *Seja A um anel Noetheriano integralmente fechado de dimensão maior ou igual a 1. Então $A = \bigcap_{p \in Spec\, A, ht(p)=1} A_p$.*

Demonstração. [Mat89], Teorema 11.4 □

Vamos introduzir agora os conceitos de morfismos planos, suaves e étale.

Definição 3.20. *Seja $f : X \to Y$ um morfismo entre duas variedades.*

- *Dizemos que f é um morfismo plano, se o anel de germes $O_{X,p}$ é um $O_{Y,f(p)}$-módulo plano, para todo $p \in X$.*
- *Dizemos que f é suave de dimensão relativa n se f é plano, $dim\, X = dim\, Y + n$ e para qualquer $x \in X$, $dim_{k(x)} \Omega_{X/Y} x \otimes k(x) = n$.*
- *Dizemos que f é étale se ela é suave de dimensão relativa 0.*

Observação. *Note que, como variedades são conexas, a dimensão relativa é constante.*

Aqui, $\Omega_{X/Y}$ é o feixe obtido colando o módulo de diferenciais de Kähler $\Omega_{B/A}$ (definição 3.14), cobrindo Y por abertos afins $V = Spec\, A$ e X por abertos afins $U = Spec\, B$ com $f(U) \subseteq V$ (detalhes desta construção podem ser vistos em [Har77], Capítulo II, Seção 8).

Vamos explicar intuitivamente o que significa cada conceito. O conceito de morfismos planos serve para definir uma noção adequada de uma família algébrica de variedades. Dado um morfismo $X \to Y$, podemos considerar as fibras X_y como uma família algébrica de esquemas parametrizada por Y. Contudo, esta definição é insatisfatória. A exigência de que o morfismo seja plano, apesar de parecer técnica e pouco justificada geometricamente, nos dá uma noção muito boa de variedades parametrizadas algebricamente. Por exemplo, as fibras X_y têm dimensão bem comportada, e vários invariantes, como o genus artimético, são constantes ([Har77], Capítulo 3, Seção 9).

Para trabalhar mais a intuição, utilizaremos a correspondência funtorial entre esquemas de tipo finito sobre $\mathbb{C}$ e espaços complexos analíticos, desenvolvida por Serre no famoso artigo GAGA ([Ser56]). Um tal esquema X é localmente da forma $Spec\, \mathbb{C}[x_1, \dots, x_n]/(f_1, \dots, f_n)$, onde os f_i são polinômios. Da mesma forma que o esquema X é obtido colando esses abertos afins, estes abertos nos dão espaços complexos analíticos (os f_i são considerados funções holomorfas), e colando-os da mesma forma, obtemos um espaço complexo analítico X_h ([Har77], Apêndice B).

A não-singularidade de uma variedade X é equivalente (quando k é algebricamente fechado), a ela ser suave sobre k ([Har77], Capítulo III, Seção 10), e quando estamos considerando $\mathbb{C}$ como corpo base, variedades não-singulares são exatamente aquelas cujo espaço analítico complexo correspondente é uma variedade complexa suave ([Har77], Apêndice B). Um morfismo étale entre duas variedades X e Y, por sua vez, corresponde precisamente a um isomorfismo local entre os espaços analíticos X_h, Y_h correspondentes ([Mum99], Capítulo 3, Seção 5).

Em geometria complexa, considerando variedades complexas M, temos uma correspondência entre fibrados vetoriais e feixes localmente livres de $H(M)$-módulos ($H(M)$ é o feixe de funções holomorfas em M) ([Voi08]). Temos que uma variedade X é suave sobre k, se e somente se, $\Omega_{X/k}$ é um O_X-módulo localmente livre de posto $dim\, X$ ([Har77], Capítulo III, Proposição 10.4). Intuitivamente, $\Omega_{X/k}$ é o correspondente algébrico da ideia de fibrado cotangente de geometria diferencial. Seguindo a filosofia de Grothendieck de que todos os conceitos de geometria algébrica devem ser relativos e não absolutos, consideramos $\Omega_{X/Y}$ para variedades Y quaisquer.

Nesta dissertação, estaremos pouco interessados em morfismos suaves em geral - o interesse é no caso específico de morfismos étale. Vamos mostrar duas outras definições equivalentes deste conceito. A primeira é bastante prática, e a segunda esclarece mais um pouco o sentido intuitivo do conceito.

Teorema 3.14. *Seja $f : X \to Y$ um morfismo de tipo finito entre duas variedades. Seja $x \in X$ e $y = f(x) \in Y$. Dizemos que f é não-ramificada em x se o homomorfismo $O_{Y,y} \to O_{X,x}$ verifica $m_y O_{X,x} = m_x$, onde m_x, m_y são os ideais maximais de $O_{X,x}, O_{Y,y}$, e se o homomorfismo induzido no corpo de resíduos $k(y) \to k(x)$ é separável. Um morfismo é étale, se e somente se, ele for plano e não-ramificado em todos os pontos de X.*

Demonstração. [Har77], Exercício 3, Seção 10 do Capítulo 3. □

Teorema 3.15. *Um morfismo $f : X \to Y$ é étale, se e somente se, todo ponto $x \in X$ está contido em um aberto afim $Spec\, C$, tal que $y = f(x)$ esteja contido num aberto afim $Spec\, A$, tal que $C = A[T_1, \ldots, T_n]/(F_1, \ldots, F_n)$ e o determinante da matriz $(\partial_j F_i)$ é uma unidade em C.*

Demonstração. [Mil80], Capítulo 1, Corolário 3.16 □

Este último teorema deixa claro que morfismos étale correspondem a isomorfismos locais. É evidente que imersões abertas são planas e étale. Temos também a seguinte proposição:

Proposição 3.16. *Seja $f : X \to Y$ um morfismo dominante entre duas variedades, e suponha que $char\, k = 0$. Então existe um aberto não vazio $U \subseteq X$, tal que $f : U \to Y$ é um morfismo suave.*

Demonstração. [Har77], Capítulo 3, Lema 10.5. □

Precisamos esclarecer o que é um morfismo dominante. A referência é [Liu02], Capítulo 2, Exercício 4.12.

Definição 3.21. *Dadas duas variedades irredutíveis X, Y, um morfismo $f : X \to Y$ é dito dominante se qualquer uma das seguintes propriedades equivalentes é satisfeita:*

- *O mapa de feixes $f^{\#} : O_Y \to f_* O_X$ é injetivo.*
- *Para todo aberto V de Y e todo aberto U de X com $U \subseteq f^{-1}(V)$, o mapa $O_Y(V) \to O_X(U)$ é injetivo.*
- *O ponto genérico de X é enviado para o ponto genérico de Y.*
- *$f(X)$ é um subconjunto denso de Y.*

Finalmente, vamos introduzir a noção de divisores, de três maneiras distintas: divisores de Weil, de Cartier, e feixes invertíveis.

Os divisores de Weil são os de conteúdo geométrico mais palpável, mas eles necessitam certas hipóteses sobre a variedade X para serem definidos.

Definição 3.22. *Dizemos que um esquema é regular em codimensão 1 se todo anel local $O_{X,x}$ de X, de dimensão 1, é regular.*

Os dois exemplos mais importantes de variedades regulares em codimensão 1 são variedades não-singulares, e variedades normais, em função do seguinte teorema bem conhecido de álgebra comutativa:

Teorema 3.16. *Um domínio noetheriano, local, de dimensão 1, é regular local, se e somente se, ele é integralmente fechado.*

Demonstração. [AM69], Proposição 9.2 □

Definição 3.23. (Divisores de Weil) *Seja X um variedade regular em codimensão 1. Um divisor primo em X é um subesquema Y fechado e integral em codimensão 1. Um divisor de Weil é um elemento de $Div\, X$, o grupo abeliano livre, livremente gerado pelos divisores primos.*

Se Y é um divisor primo em X, e ϵ é seu ponto genérico, então $O_{X,\epsilon}$ é um anel de valorização discreta cujo corpo de frações é $K(X)$, o corpo de funções racionais em X. Seja v_Y a valorização discreta correspondente. Para cada $f \in K(X)$ diferente de 0, podemos considerar $v_Y(f)$: se tal número é positivo, dizemos que f tem um zero de ordem $v_Y(f)$, e se tal número é negativo, dizemos que f tem um polo de ordem $|v_Y(f)|$. Essa nomenclatura, e o próprio conceito de divisores, têm origem em superfícies de Riemann. Divisores primos correspondem simplesmente a pontos, e cada função meromórfica pode ser escrita localmente como série de Laurent, uma vez que a superfície de Riemmann é localmente biholomorfa a um aberto de $\mathbb{C}$: os conceitos de ordem de zeros e polos são exatamente os mesmos que em análise de uma variável complexa.

Lema 3.7. *Se X é uma variedade regular em codimensão 1 e $f \neq 0 \in K(X)$, então $v_Y(f) = 0$ exceto para uma quantidade finita de divisores primos Y.*

Definição 3.24. *Se X é uma variedade regular em codimensão 1 e $f \neq 0 \in K(X)$, usando o lema acima, definimos o divisor de f, denotado por (f), como:*

$$(f) = \sum v_Y(f)Y,$$

onde a soma percorre todos os divisores primos.

Pelas propriedades de valorização, temos que $v_Y(f/g) = v_Y(f) - v_Y(g)$ para cada Y divisor primo, $f, g \neq 0 \in K(X)$. Portanto, a função que manda cada $f \neq 0 \in K(X)$ para (f) é um homomorfismo de grupos. A imagem desse homomorfismo, que denotaremos por $Pr(X)$, é constituída pelos chamados divisores *principais*.

Definição 3.25. *Seja X uma variedade regular em codimensão 1. Dizemos que dois divisores D, D' são* linearmente equivalentes *se $D - D' \in Pr(X)$. Definimos o* grupo de classes de divisores *de X como o quociente $Div\, X/Pr(X)$, e o denotamos por $Cl\, X$.*

Exemplo. *Seja $Spec\, A$ uma variedade afim. Então A é um domínio de fatoração única, se e somente, $Cl\, Spec\, A = 0$.*

Exemplo. *Seja X o espaço projetivo P^n_k. Para cada divisor $D = \sum n_i Y_i$ defina $deg\, D = \sum n_i deg\, Y_i$, onde $deg\, Y_i$ é o grau da hiperfície. Denotando por H a hiperfície definida por $x_0 = 0$, temos que D é linearmente equivalente a $(deg\, D)H$ para todo divisor D, $deg(D) = 0$ para todo divisor principal, e que $deg : Cl\, X \to \mathbb{Z}$ é um isomorfismo de grupos.*

Existe uma outra noção de divisores, que pode ser definida para esquemas arbitrários: divisores de Cartier. Seja X um esquema, e para cada aberto afim $U = Spec\,A$ seja $K(U)$ a localização de A por todos os seus elementos que não são divisores de 0. Essa associação nos dá um pré-feixe, cuja feixificação nos dá um feixe, K_X, o *feixe de anéis quocientes totais*. Note que, se X é integral, K_X é apenas o feixe constante igual a $K(X)$. Associados a K_X e O_X temos dois feixes: K_X^* é o feixe de grupos dado pelos elementos invertíveis em K_X, e o O_X^* é o feixe de grupos dado pelos elementos invertíveis em O_X. Por [Liu02], lemma 1.12, Capítulo 7, O_X pode ser visto como um subfeixe de K_X (e, portanto, O_X^* de K_X^*).

Definição 3.26. (Divisor de Cartier) *Um* divisor de Cartier *em um esquema X é uma seção global do feixe K_X^*/O_X^*, e o grupo de tais divisores é denotado $CDiv\,X$. A imagem de $K_X^*(X)$ pelo mapa natural $K_X^*(X) \to K_X^*/O_X^*(X)$ constitui o subgrupo dos* divisores de Cartier principais. *Dois divisores $D, D' \in CDiv\,X$ são linearmente equivalentes se a sua diferença $D - D'$ for um divisor principal (a operação de grupo original em $CDiv\,X$ é a multiplicação, mas usamos a notação aditiva para ficar consistente com o uso de divisores de Weil). Denotamos $CCl\,X$ o quociente de $CDiv\,X$ pelo subgrupo de divisores de Cartier principais.*

Expandindo o que foi dito acima: um divisor de Cartier é dado por uma cobertura $\{U_i\}_i$ de X por abertos, e um elemento $f_i \in K_X^*(U_i)$ dado pela razão de dois elementos regulares em $O_X(U_i)$ para cada i, tal que $f_i/f_j \in O_X^*(U_i \cap U_j)$ para cada i, j. Duas escolhas $\{U_i\}_i, \{f_i\}_i$ e $\{V_j\}_j, \{g_j\}_j$ dão o mesmo divisor de Cartier se as restrições de f_i, g_j para $U_i \cap V_j$ diferem por um fator multiplicativo de $O_X^*(U_i \cap V_j)$, para todos i, j. A soma de dois divisores de Cartier $\{U_i\}_i, \{f_i\}_i$ e $\{V_j\}_j, \{g_j\}_j$ é dada pela cobertura $\{U_i \cap V_j\}_{i,j}$ e o produto da restrição de f_i, g_j para $U_i \cap V_j$, para todo i, j. Finalmente, um divisor é principal se ele pode ser representado pela cobertura $\{X\}$ e um elemento $f \in K_X^*(X)$.

As duas noções de divisores coincidem numa classe importante de variedades:

Teorema 3.17. *Seja X uma variedade, cujos anéis de germes em todos os pontos são domínios de fatoração única (por exemplo, se X é não-singular ou normal). O grupo $Div\,X$ de divisores de Weyl (note que a hipótese sobre X implica que ele é regular em codimensão 1) é isomórfico ao grupo $CDiv\,X$ de divisores de Cartier, e esse isomorfismo identifica os divisores de Weil principais com os divisores de Cartier principais. Portanto, também temos $Cl\,X \cong CCl\,X$.*

Finalmente, temos uma terceira noção possível de divisores. Lembramos que um feixe invertível num esquema X é um O_X-módulo localmente livre de posto 1. Eles recebem esse nome, porque dado qualquer feixe invertível L, existe um feixe invertível L', tal que $L \otimes L' \cong O_X$. Além disso, se L e M são feixes invertíveis, também o é $L \otimes M$ ([Har77], Capítulo II, Proposição 1.2, para esses dois fatos). Portanto, para um esquema X, podemos fazer a seguinte definição:

Definição 3.27. *Para um esquema X, o* grupo de Picard *de X, $Pic\,X$, é o grupo de classes de isomorfismo de feixes invertíveis em X, com a operação $\otimes$.*

Proposição 3.17. *Seja X uma variedade. Então existe um mapa θ que manda cada $D \in CDiv\,X$ em um feixe invertível $\theta(D)$ de X. Este mapa entre divisores de Cartier e feixes invertíveis é bijetivo, e temos que $D, D' \in CDiv$ são linearmente equivalentes, se e somente se, $\theta(D) \cong \theta(D')$. Além disso, $\theta(D + D') = \theta(D) \otimes \theta(D')$.*

Demonstração. [Har77], Capítulo II, Proposições 6.13 e 6.15. □

Finalmente, juntando Teorema 3.17 e a proposição 3.17:

Teorema 3.18. *Se X é uma variedade normal, então $Cl\,X \cong CCl\,X \cong Pic\,X$.*

Para uso no Capítulo 5, introduzimos a noção de imagens inversas de divisores.

Lema 3.8. *Seja $f : X \to Y$ um morfismo de variedades. Se f é plano, ou se f é dominante, então o morfismo canônico $O_Y \to f_*O_X$ se estende para um morfismo $K_Y \to f_*K_X$.*

Demonstração. [Liu02], Capítulo 7, Lema 1.33. □

Definição 3.28. *Sob as hipóteses do lema acima, existe um morfismo $K_Y^*/O_Y^* \to f_*(K_X^*/O_X^*)$. Para divisor de Cartier D em Y, denotamos por $f^{-1}(D)$ sua imagem em $CDiv\, X$ via esse morfismo.*

Vendo divisores como feixes invertíveis, temos uma definição equivalente à acima:

Proposição 3.18. *Seja $f : X \to Y$ um morfismo de variedades. Se L é um feixe invertível em Y, f^*L é um feixe invertível em X. Se f é dominante ou plano, então usando a correspondência entre divisores de Cartier e feixes invertíveis, temos que f^*L corresponde à imagem inversa do divisor associado a L. Em outras palavras, o mapa da proposição 3.17 é natural.*

Demonstração. Seja $V = Spec\, A$ um aberto afim de Y, tal que $L|_V \cong (A)^\sim$, e $U = Spec\, B$ um aberto afim de X com $f(U) \subseteq V$. Então $f^*L|_U \cong (A \otimes_A B)^\sim \cong (B)^\sim$. Logo, $f^*(L)$ é localmente livre de posto 1. A proposição 3.17 mostra a correspondência desejada. □

Finalmente, tendo definido imagem inversa de divisores via divisores de Cartier e feixes invertíveis, podemos citar que a definição pode ser feita de maneira direta para divisores de Weil, quando $f : X \to Y$ é um morfismo plano ou finito e sobrejetivo. Contudo, esta definição é muito complicada, por isso, apenas a citamos: [Liu02], Seção 7.2, exercício 2.3.

O resto desta seção irá lidar com a seguinte questão: seja X um k-esquema e G um grupo finito de k-automorfismos de X. Gostaríamos de definir um objeto quociente para essa ação. Uma definição natural seria a seguinte:

Definição 3.29. (Quociente Categorial) *Dado um k-esquema X e um grupo G de k-automorfismos de X, o* quociente *$X//G$ é um esquema com um morfismo $\pi : X \to X//G$ G-invariante (isto é, tal que $\pi(g(x)) = \pi(x), \forall x \in X, \forall g \in G$), satisfazendo a seguinte propriedade universal: dado qualquer k-esquema Z e um morfismo $\phi : X \to Z$ que seja G-invariante, temos uma fatoração única $\phi = \phi'\pi$, onde $\phi' : X//G \to Z$ é um k-morfismo.*

Essa definição é extremamente razoável, e identifica o quociente de maneira única a menos de isomorfismo. A definição análoga na categoria de espaços topológicos nos dá exatamente o resultado esperado: $X//G$ é o espaço das órbitas com a topologia quociente. Vamos ver o que essa definição nos dá no caso de esquemas afins.

Sejam então A uma k-álgebra e G um grupo de automorfismos de $Spec\, A$. Isto é a mesma coisa que um grupo de automorfismos k-álgebra em A. Temos a inclusão $A^G \to A$, que induz um morfismo $\pi : Spec\, A \to Spec\, A^G$. Vamos mostrar que isso nos dá o quociente categorial. Seja $\phi : Spec\, A \to Spec\, B$ um morfismo G-invariante de esquemas induzido por um homomorfismo $\psi : B \to A$. A G-invariância de ϕ se traduz simplesmente em $g(\psi(b)) = \psi(b)$, $\forall g \in G, b \in B$. Logo, ψ se fatora em $\psi' : B \to A^G$ e a inclusão $A^G \to A$. Voltando para a categoria de esquemas, isso nos dá a desejada fatoração de ϕ. Dado um mapa $\phi : Spec\, A \to Y$, onde Y é um k-esquema arbitrário, temos a fatoração desejada de ϕ escrevendo Y como uma união de esquemas afins e colando. Portanto, $A//G = Spec\, A^G$.

Observação. *Como o funtor contravariante Spec da categoria de k-álgebras para esquemas sobre k é pleno e fiel ([Har77], capítulo II, Proposição 2.3), o argumento acima mostra que a fatoração de ϕ também é única.*

Em contextos geométricos, também é razoável esperar que o quociente seja, como conjunto, dado pelas órbitas da ação. Isto ocorre, como é bem conhecido, na categoria de espaços topológicos. Contudo, isso não funciona para esquemas. Por exemplo, como vimos na observação 1.2, quando $A = k[x_1, \ldots, x_n]$ e $G = GL_n(k)$, $A^G = k$. Portanto, $A//G = Spec\, k$ consiste de apenas um ponto. Entretanto, em $Specm\, A \cong k^n$ $GL_n(k)$ tem duas órbitas: $\{0\}$ e o seu complemento. Logo, $A//G$ não pode ser constituído pelas órbitas.

Um outro exemplo, um pouco mais interessante: seja $A = k[x_{ij}]_{1 \le i,j \le n}$, $M_n(k) = Specm\, A$. $GL_n(k)$ age em $M_n(k)$ por conjugação: $g.m = gmg^{-1}$, $m \in M_n(k), g \in GL_n(k)$. Sendo $\lambda_1, \ldots, \lambda_n$

os coeficientes do polinômio característico de uma matriz $n \times n$, temos que $A^{GL_n(k)} = k[\lambda_1, \ldots, \lambda_n]$, e os λ_i são algebricamente independentes. Logo, o quociente categorial, nos pontos fechados, é uma função $M_n(k) \to k^n$. A fibra do ponto $(0, \ldots, 0)$ é o conjunto das matrizes M de polinômio característico $det(M - tI) = t^n$. Este conjunto não consiste numa órbita: qualquer matriz de Jordan com apenas zeros na diagonal pertence a essa fibra ([Dol03], Exemplo 1.2, Cap. 1).

Em vista disso, uma segunda definição de quociente é possível.

Definição 3.30. (Quociente Geométrico Bom) *O quociente geométrico bom de uma variedade sobre k, X, é um morfismo $p : X \to Y$, G-invariante, tal que:*

1. *p é sobrejetivo.*

2. *Dado um subconjunto U de Y, ele é aberto, se e somente se, $p^{-1}(U)$ for aberto (ou seja, Y tem a topologia quociente).*

3. *Para qualquer aberto U de Y, o homomorfismo natural $O(U) \to O(p^{-1}(U))$ resulta em um isomorfismo de $O(U)$ sobre o subanel $O(p^{-1}(U))^G$.*

4. *As fibras de p são órbitas.*

Usamos X/G para denotar o quociente geométrico bom. Como poderia se esperar, essa noção é mais forte do que a primeira. Note que a proposição abaixo justifica o uso do artigo “o"na definição de quociente geométrico bom - ele é único a menos de isomorfismos.

Proposição 3.19. *Um quociente geométrico bom é um quociente categorial.*

Demonstração. Seja $q : X \to Z$ um morfismo G-invariante, e $p : X \to X/G$ o quociente geométrico bom. Podemos recobrir Z como uma família de subespaços abertos afim, $\{V_i\}_{i \in I}$. Para cada V_i, $q^{-1}(V_i)$ será um aberto G-invariante de X, e definindo $U_i = p(q^{-1}V_i)$, temos $q^{-1}(V_i) \subseteq p^{-1}(U_i)$. Como as fibras de pontos de X/G são órbitas, e como $q^{-1}(V_i)$ é G-invariante, isso nos dá que, na verdade, temos uma igualdade $q^{-1}(V_i) = p^{-1}(U_i)$. Como p é sobrejetivo e X/G tem a topologia quociente, os U_i formam uma cobertura aberta de X/G. O mapa $q : q^{-1}(V_i) \to V_i$ é definido por um homomorfismo de anéis $\alpha_i : O(V_i) \to O(q^{-1}(V_i)) = O(p^{-1}(U_i))$. Como q é G-invariante, a imagem de α_i está contida em $O(p^{-1}(U_i))^G$ e, portanto, temos um único homomorfismo $O(V_i) \to O(U_i)$, que nos dá um único morfismo $\psi_i : U_i \to V_i$, uma vez que V_i é afim. Colando os ψ_i, uma vez que é fácil ver que $\psi_i = \psi_j$ em $U_i \cap U_j$, obtemos o mapa $\psi : X/G \to Z$ satisfazendo $q = \psi p$ desejado. □

Lema 3.9. *Seja $p : X \to Y$ um morfismo G-invariante de esquemas irredutíveis com as seguintes propriedades:*

1. *Para qualquer aberto U de Y, o homomorfismo natural $O(U) \to O(p^{-1}(U))$ resulta em um isomorfismo de $O(U)$ sobre o subanel $O(p^{-1}(U))^G$.*

2. *Se W é um sunconjunto fechado e G-invariante de X, então $p(W)$ é um conjunto fechado de Y.*

3. *Se W_1, W_2 são dois fechados G-invariantes e disjuntos de X, então $p(W_1)$ e $p(W_2)$ também são disjuntos.*

4. *As fibras de p são órbitas.*

Então, p é um quociente geométrico bom.

Demonstração. Os pontos 1 e 2 implicam, respectivamente, que p é dominante e $p(X)$ é fechado em Y. Logo, p é sobrejetiva. A propriedade 2 implica que Y tem a topologia quociente. De fato, se $U \subseteq Y$ e $p^{-1}(U)$ é aberto, então $X - p^{-1}(U)$ é fechado e G-invariante. O ponto 2 implica que, uma vez que p é sobrejetiva, $Y - U$ é fechado e, portanto, U aberto. □

Com isso, podemos mostrar que, apesar das complicações no caso geral, quando X é uma variedade afim e G é finito, então X/G existe e é igual a $Spec\, O(X)^G$- e portanto o quociente se comporta da maneira mais natural possível.

Teorema 3.19. *Sejam $X = Spec\, A$ uma variedade afim, e G um grupo finito de k-morfismos de X - simultaneamente, G é um grupo de isomorfismos de k-álgebra de A. Então a inclusão $A^G \to A$ induz um morfismo $\pi : X \to Y = Spec\, A^G$ que é um quociente geométrico bom.*

Demonstração. Note que, pelo teorema Teorema 3.1 Y é uma variedade afim. Vamos mostrar que todas as hipóteses do lema acima são satisfeitas. Os abertos básicos de Y são da forma $Spec\, A_f^G$, onde $f \in A^G$. A imagem inversa por π desses abertos básicos é $Spec\, A_f$. Como vimos na proposição 3.10, $(A_f)^G \cong A_f^G$. Portanto, o ponto 1 do lema acima se aplica aos abertos básicos e, dessa forma, se aplica a todos os abertos. Seja $V(P)$ um fechado irredutível de X (P é ideal primo), e $p = P \cap A^G$. É claro que $\pi(V(P)) \subseteq V(p)$. Vamos mostrar a inclusão contrária: se p' é ideal primo de A^G contendo p, pelo Teorema Going-Up, existe ideal primo P' contendo P, tal que $P' \cap A^G = p'$. Portanto, $\pi(V(P)) = V(p)$ é um fechado de Y. No caso geral, seja $V(I)$ um fechado de X, I um ideal qualquer. Temos $V(I) = \bigcup_{i=1}^s V_i$, onde os V_i são suas componentes irredutíveis. Logo $\pi(V(I)) = \bigcup_{i=1}^s \pi(V_i)$, sendo uma união finita de fechados, é fechado. Para provar o item 3 do lema, basta considerar $W_1 = V(P_1), W_2 = V(P_2)$ irredutíveis. Se $\pi(W_1) \cap \pi(W_2)$ contém um ponto p, existem ideais primos $Q_1 \in W_1, Q_2 \in W_2$, tal que $p = Q_1 \cap A^G = Q_2 \cap A^G$. Mas, pela proposição 3.11, existe um $g \in G$, tal que $g(Q_1) = Q_2$. Como W_1 e W_2 são G-invariantes, isto implicaria que a interseção deles é não nula, contrariando a hipótese. Finalmente, para provar o item 4, basta observar que, pela proposição 3.11 a fibra de $\pi(P) = P \cap A^G$ é a órbita de P pela ação de G. □

3.5 Referências

A seção 1 usou material de [Dol03] e [Hum90], Capítulo 3. A seção 2 foi baseada em material em [LT09], [Hum90] e [Kan01]. A seção 3 contém, em sua maioria, resultados e definições básicos de álgebra comutativa, que podem ser encontrados em [AM69] e [Mat89]. A demonstração da proposição 2.10 seguiu [MR01], Capítulo 15. A seção 4 baseou-se fortemente em material de [Har77] e [Liu02], e a parte específica sobre quocientes sob ação de grupos em [Dol03], Capítulo 6.

Capítulo 4

Problema de Noether Não-Comutativo

Este Capítulo introduz a questão que é o interesse principal deste trabalho: o Problema de Noether Não-Comutativo. Ele é colocado em contexto na primeira seção, onde se argumenta que corpos de frações de álgebras universais envolventes de álgebras de Lie de dimensão finita são bons análogos não-comutativos de corpos de funções racionais. Nas três seções seguintes são introduzidos e provados os casos de solução positiva para o problema, obtidos por J. Alev, F. Dumas, A. Molev, S. Ovsienko e V. Futorny. Um ingrediente essencial nessas provas é a extensão não-comutativa do Teorema de Miyata (Teorema 4.4), obtida por Alev e Dumas. Ela será demonstrada na última seção deste capítulo; o resultado provado tem, como caso particular, a versão clássica do Teorema de Miyata utilizada no Capítulo 1 (Teorema 1.4).

4.1 "Almost Commutative Algebras"e Conjectura de Gelfand-Kirillov

É um tópico importante de teoria de anéis encontrar classes naturais de anéis não-comutativos onde técnicas de álgebra comutativa possam ser transferidas. Uma vasta área de estudos neste sentido são os anéis e álgebras com identidades polinomiais ([Row80], Introdução). Outra classe de anéis cuja experiência mostra estar nesta categoria são as álgebras universais envolventes de álgebras de Lie de dimensão finita, e as Álgebras de Weyl. Nesta seção, abordaremos um dos aspectos disso: a existência de uma filtração adequada para qual a álgebra graduada associada é comutativa (na verdade, nesses dois casos, se obtêm a álgebra de polinômios, como veremos).

Vamos relembrar as definições de álgebras graduadas, filtradas, e como passar de uma filtração numa álgebra para uma graduação.

Definição 4.1. *Seja A uma k-álgebra. Dizemos que ela é* graduada *se $A = \bigoplus_{i=0}^{\infty} A_i$, onde cada A_i é um subespaço, e $A_iA_j \subseteq A_{i+j}$. Poderíamos usar outros monóides (ou mesmo semigrupos) para fazer a graduação da álgebra, mas neste trabalho será suficiente graduação por $\mathbb{N}$. Agora, dizemos que A é uma k-álgebra* filtrada *se existe uma cadeia de subespaços $A_0 \subseteq A_1 \subseteq \ldots \subseteq A_n \subseteq \ldots$, tal que $A = \bigcup_{i=0}^{\infty} A_i$ e $A_iA_j \subseteq A_{i+j}$.*

Definição 4.2. *Dada uma k-álgebra A com uma filtração $\{A_i\}_{i=0}^{\infty}$, definimos $gr\, A = \bigoplus_{i=0}^{\infty} A_i/A_{i-1}$, como espaço vetorial, com $A_{-1} = 0$. A multiplicação é dada da seguinte maneira: se $u \in A_i/A_{i-1}$ e $v \in A_j/A_{j-1}$, então uv é a classe lateral de $u'v' \in A_{i+j}$ em A_{i+j-1}, onde u' e v' são representantes das classes laterais de u e v, respectivamente. É fácil ver que esse produto está bem definido. O produto de elementos arbitrários de $gr\, A$ é extensão por linearidade do caso definido acima. $gr\, A$ tem a graduação dada pela sua soma direta em subespaços vetoriais.*

As propriedades importantes das filtrações das álgebras universais envolventes (de álgebras de Lie de dimensão finita) e da álgebra de Weyl foram axiomatizadas por Duflo ([Duf73]), que o introduziu o conceito de "almost commutative algebra". Por simplicidade, assuma $char\, k = 0$.

Definição 4.3. *Uma k-álgebra A é chamada de "almost commutative"se ela possui uma filtração A_i, $i \geq 0$, tal que: $A_0 = k$, A_1 é de dimensão finita, $A_i = A_1^i$ para todo $i > 0$, e a álgebra graduada associada a esta filtração é comutativa.*

Exemplo. *Este é o caso para as álgebras universais envolventes de álgebras de Lie de dimensão finita. De fato, se L é uma álgebra de Lie de dimensão finita com uma base ordenada $e_1, \dots, e_n$, então, pelo Teorema PBW (Poincaré-Birkhoff-Witt), $U(L)$ tem uma base $\{e_{j_1} \dots e_{j_s} | 1 \leq j_1 \leq \dots \leq j_s \leq n\} \cup \{1\}$ ([Jac62], Teorema 4, Cap. V); ou seja, a base é dada por 1 e os monômios com elementos da base em ordem não-decrescente. Seja $U(L)_i$ o subespaço gerado pelos monômios de comprimento i ou menos ($e_{j_1} \dots e_{j_s}$ com $s \leq i$). Eles formam uma filtração, com $U(L)_i = U(L)_1^i$; $U(L)_1$ tem dimensão finita (igual a $\dim L$, [Jac62], Corolário 1, Cap. V), e a álgebra graduada associada é a álgebra de polinômios em n variáveis ([Jac62], texto imediatamente antes do Teorema 6, Cap. V).*

Exemplo. *Este também é o caso para as Álgebras de Weyl, utilizando a filtração de Bernstein, que introduziremos agora. Como vimos, $A_n(k)$ tem como base monômios $x^\alpha \partial^\beta$, onde α, β são n-uplas de inteiros não negativos. Definamos a ordem de tal monômio como $|\alpha| + |\beta|$. Seja $A_n(k)_i$ o subespaço gerado pelos monômios de ordem menor ou igual a i. Usando combinatória simples, é fácil ver que todos possuem dimensão finita. Além disso, $A_n(k)_i = A_n(k)_1^i$. E, finalmente, a álgebra graduada associada é a álgebra de polinômios em $2n$ variáveis:*

Teorema 4.1. *Seja $S = gr\, A_n(k)$ a álgebra graduada associada a $A_n(k)$ com a filtração de Bernstein. Então $S \cong k[z_1, \dots, z_{2n}]$.*

Demonstração. Sejam $t_1, \dots, t_n$ as classes de $x_1, \dots, x_n$ em $A_n(k)_1/k$, e $t_{n+1}, \dots, t_{2n}$, as classes $\partial_1, \dots, \partial_n$. Note que cada t_i é um elemento homogêneo de grau 1 em S. $[t_i, t_{n+j}]$ é a imagem em $A_n(k)_2/A_n(k)_1$ de $[x_i, \partial_j]$; portanto, essas variáveis comutam. Os outros pares possíveis de t_i, t_j já comutam, porque os x_i, ∂_j correspondentes comutam em $A_n(k)$. Como $A_n(k)$ é gerada pelos $x_i's$ e $\partial_i's$, S é gerada por $t_1, \dots, t_{2n}$ e, portanto, é uma álgebra comutativa.

Seja $\phi : k[z_1, \dots, z_{2n}] \to S$ o k-homomorfismo que manda z_i em t_i. Ele é sobrejetivo, e como os z_i tem grau 1, ele é um homomorfismo graduado (um homomorfismo graduado entre dois espaços vetoriais graduados manda os elementos homogêneos de grau n em elementos homogêneos de mesmo grau).

Resta provar que ϕ é injetivo. Seja F um polinômio, tal que $\phi(F) = 0$. Como ϕ é graduado, podemos assumir F homogêneo de grau K, e igual a

$$\sum_{c_{\alpha\beta}} c_{\alpha\beta} z_1^{\alpha_1} \dots z_n^{\alpha_n} z_{n+1}^{\beta_1} \dots z_{2n}^{\beta_n},$$

com todos os α, β envolvidos satisfazendo $|\alpha| + |\beta| = K$. Seja $\sigma \in A_n(k)$ igual a

$$\sum_{c_{\alpha\beta}} c_{\alpha\beta} x_1^{\alpha_1} \dots x_n^{\alpha_n} \partial_1^{\beta_1} \dots \partial_n^{\beta_n}.$$

A imagem de σ em S é igual a $\phi(F) = 0$. Portanto, a imagem de σ em $A_n(k)_K/A_n(k)_{K-1}$ é 0, isto é, σ pode ser expresso como combinação linear de elementos de $A_n(k)_{K-1}$. Isso é impossível dada a base conhecida da Álgebra de Weyl (proposição 2.2) como espaço vetorial, a menos que todos os coeficientes de F sejam 0. Portanto, ϕ é injetiva.

□

Observação. *A Álgebra de Weyl possui outra filtração importante, por ordem dos operadores diferenciais - mais genericamente, essa filtração é definida em toda álgebra de operadores diferenciais. A álgebra graduada correspondente é sempre comutativa, como é fácil ver por indução, e novamente coincide com a álgebra de polinômios em $2n$ variáveis no caso de A_n ([Cou95], Cap. 7, Exercício 6.5). O problema é que os subespaços da filtração não têm dimensão finita.*

“Almost commutative algebras"imediatamente têm muitas propriedades importantes. Por exemplo, elas são noetherianas à esquerda e à direita, porque suas álgebras graduadas correspondentes são ([KL00], Prop. 7.1); isso nos dá uma prova diferente da apresentada no Capítulo 2 de que as Álgebras de Weyl são noetherianas). Além disso, é possível desenvolver para elas uma teoria de dimensão, de Gelfand-Kirillov, de maneira totalmente análoga à dimensão de Krull no caso comutativo, utilizando polinômios de Hilbert ([KL00], Cap. 7).

Apesar disso, a definição de tal classe de álgebras pode parecer um tanto artificial. Entretanto, tal impressão é ilusória: essas álgebras correspondem a uma classe de álgebras extremamente natural:

Teorema 4.2. *"Almost commutative"k-algebras correspondem exatamente à classe de imagens homomórficas de álgebras universais envolventes de álgebras de Lie de dimensão finita sobre k.*

Demonstração. Suponha que A seja uma "almost commutative algebra"com respeito a uma filtração A_i. Sejam x, y elementos de A_1, com imagens $\overline{x}, \overline{y}$ em A_1/A_0. Como $gr\,A$ é comutativo, $0 = [\overline{x}, \overline{y}] = [x, y] + A_1 \in A_2/A_1$ e, portanto, $[x, y] \in A_1$, e A_1 assim tem uma estrutura de álgebra de Lie. Denotemos essa álgebra de Lie por L. A inclusão de L em A se estende, pela propriedade universal de $U(L)$, para um homomorfismo de álgebras associativas de $U(L) \to A$. Como A é gerada por L, esse homomorfismo é sobrejetivo. Reciprocamente, suponha que A seja uma imagem homomórfica de um k-homomorfismo ϕ de $U(L)$, onde L é uma álgebra de Lie de dimensão finita. Definindo $A_n = \phi U(L)_n$, temos uma filtração de A. Como ϕ é um k-homomorfismo, $A_0 = k$, e A_1 tem dimensão finita, uma vez que $U(L)_1$ o tem. Além disso, como $U(L)_n = U(L)_1^n$, $A_n = A_1^n$.

Para cada n, a função ϕ induz uma função de k-espaços vetoriais de $U(L)_n/U(L)_{n-1}$ para A_n/A_{n-1}, e essas funções se combinam para um homomorfismo graduado de espaços vetoriais $gr(\phi) : gr\,U(L) \to gr\,A$. Este homomorfismo é sobrejetivo. Como sabemos, $gr\,U(L)$ é comutativa e, portanto, obtemos o que queremos se mostrarmos que $gr(\phi)$ é um homomorfismo de anéis.

Para tanto, sejam $\overline{u} = u + U(L)_{m-1}$ e $\overline{v} = v + U(L)_{n-1}$ elementos homogêneos de $gr\,U(L)$ de graus m, n, respectivamente. Então $\overline{uv} = uv + U(L)_{m+n-1}$, e

$$gr(\phi)(\overline{uv}) = \phi(uv) + A_{m+n-1} = \phi(u)\phi(v) + A_{m+n-1}$$

$$= (\phi(u) + A_{m-1})(\phi(v) + A_{n-1}) = gr(\phi)(\overline{u})gr(\phi)(\overline{v}).$$

□

Exemplo. *$A_n(k)$ é imagem homomórfica de $U(H_n)$, onde H_n, a n-ésima álgebra de Heisenberg, é dada por geradores $x_1, \ldots, x_n, y_1, \ldots, y_n, z$ e relações $[x_i, x_j] = [y_i, y_j] = 0, [y_i, x_j] = \delta_{ij} z$, $i, j = 1, ..., n$ e z está no centro. $A_n(k)$ é o quociente de $U(H_n)$ pelo ideal gerado por $z - 1$.*

Portanto, as "almost commutative k-algebras"são imagens homomórficas de álgebras universais envolventes de álgebras de Lie de dimensão finita. De maneira similar, k-álgebras comutativas finitamente geradas são imagens homomórficas de álgebras de polinômios num número finito de variáveis.

Dessa forma, corpos de frações de álgebras $U(L)$, com L álgebra de Lie de dimensão finita, funcionam como correspondentes de corpos de funções racionais ($U(L)$ admite corpo de frações porque é um domínio noetheriano à esquerda e à direita, Teo. 6, Cap. 5 [Jac62]). Assim, os corpos de Weyl ganham proeminência, em função da célebre Conjectura de Gelfand-Kirillov ([GK66]):

Conjectura. (Gelfand-Kirillov) *Se L é uma álgebra de Lie de dimensão finita, $Frac\,U(L)$ é isomórfico a $D_n(K)$, para algum n e K uma extensão puramente transcendental de k, de grau de transcendência finito.*

A Conjectura é sabida ter resposta positiva para várias álgebras: todas as de dimensão menor ou igual a 8, sl_n, gl_n, álgebras de Lie solúveis etc. Porém, contra-exemplos também são conhecidos. Uma discussão mais detalhada de casos positivos e negativos de solução da Conjectura encontra-se na introdução de [Pre10].

De todo modo, tais considerações justificam a escolha dos corpos de Weyl como correspondentes não-comutativos naturais para os corpos de funções racionais, e isto motiva a introdução do Problema de Noether Não-Comutativo.

4.2 Problema de Noether Não-Comutativo

Aqui, e durante o resto do capítulo, supor-se-á $char\, k = 0$.

Seja A uma k-álgebra, e G um grupo (não-necessariamente finito) de k-automorfismos de A. A ação de G pode ser estendida para $End_k(A)$: $(g.T)(a) = g(T(g^{-1}a)), g \in G, T \in End_k(A), a \in A$. Não importa qual das duas definições de $D(A)$ se utilize, é fácil ver que tal ação de G se restringe a uma ação em $D(A)$.

De fato, usando a primeira definição de operadores diferenciais, sendo λ_a multiplicação por um escalar $a \in A$ e ∂ uma derivação em $Der_k(A)$, temos que $g(\lambda_a) = \lambda_{g(a)}$, e para todos $x, y \in A$,

$$g(\partial)(xy) = g(g^{-1}(x)\partial(g^{-1}(y)) + g^{-1}(y)\partial(g^{-1}(x))) = yg(\partial)(x) + xg(\partial)(y).$$

Ou seja, $g(\partial)$ também é uma derivação. Usando a segunda definição, isto é claro uma vez que

$$g([\ldots[[D, a_0], a_1], \ldots, a_n]) = [\ldots[[g(D), g(a_0)], g(a_1)], \ldots, g(a_n)].$$

Seja $A = S(V^*) \cong k[x_1, \ldots, x_n]$, onde V é um espaço de dimensão n. Seja G um subgrupo qualquer de $GL(V)$. Como sabemos, sua ação se estende para k-automorfismos de $k[x_1, \ldots, x_n]$, e como vimos acima, para k-automorfismos de seus operadores diferenciais: $A_n(k)$. Sempre que tivermos um grupo G agindo em $A_n(k)$, com a ação de origem como acima, se dirá que G é um grupo de *automorfismos lineares*, como no caso comutativo.

Dado $g \in G$, se M_g for a matriz da restrição de g ao subespaço $kx_1 \oplus \ldots \oplus kx_n$, usando a base $x_1, \ldots, x_n$, a matriz da restrição de g ao subespaço $ky_1 \oplus \ldots \oplus ky_n$, com relação à base $y_1, \ldots, y_n$, é $(M_g^t)^{-1}$. Isto ocorre porque, das relações $y_i(x_j) = \delta_{ij}$, podemos considerar $ky_1 \oplus \ldots \oplus ky_n$ como o espaço dual de $kx_1 \oplus \ldots \oplus kx_n$, e a base $\{y_i\}$ como dual da base $\{x_i\}$. Isto nos dá o seguinte resultado.

Proposição 4.1. *O elemento $w = x_1y_1 + \ldots + x_ny_n$, de $A_n(k)$ é G-invariante para* qualquer *subgrupo, finito ou não, de $GL_n(k)$.*

Isso mostra uma diferença interessante entre $k[x_1, \ldots, x_n]$ e $A_n(k)$. Para grupos infinitos de $GL_n(k)$, a álgebra de invariantes dos polinômios pode se restringir a k (Observação 1.2); isto nunca é o caso para $A_n(k)^G$, pois ela sempre contém w.

Seja $D_{m,t}(k) = Frac\, A_m(K)$, onde $K = k(z_1, \ldots, z_t)$, se $m > 0$; se $m = 0$, $D_{0,t}(k) = K$.

Problema. (Problema de Noether Não-Comutativo) *Seja G um grupo de automorfismos lineares agindo, por extensão, em $D_n(k)$. Quando $D_n(k) \cong D_{m,t}(k)$, para alguns m, t não-negativos?*

Essa questão foi introduzida por Jacques Alev e François Dumas, c.f. [AD06]. Uma questão imediata que ocorre é: quando $D_{m,t}(k) \cong D_{n,u}(k)$? Pelo último resultado do Capítulo 2, sabemos que tomando o centro e depois calculando o grau de transcendência sobre k, obrigatoriamente devemos ter $t = u$. Portanto, a dúvida restante é: quando $D_n(k) \cong D_m(k)$, para k um corpo arbitrário de característica 0. Gelfand e Kirillov, [GK66], desenvolveram neste artigo uma noção não-comutativa de grau de transcendência, o qual denotaremos por $GK - trdeg_k$, e mostraram que $GK - trdeg_k(D_n(k)) = 2n$; portanto, este invariante distingue $D_n(k)$ de $D_m(k)$, se $m \neq n$.

Nosso interesse será para grupos G finitos, apesar de resultados interessantes existirem para G arbitrários ([AD06]). Neste caso, existe uma precisão importante para a resposta possível:

Teorema 4.3. *Se G é um grupo de automorfismos linears finito agindo em $D_n(k)$, e o Problema de Noether Não-Comutativo tem uma solução positiva, então $n = m$, $t = 0$.*

Demonstração. É um fato conhecido ([MR01], corolário 6.6.18) que nenhum subcorpo comutativo de $D_n(k)$ pode ter um grau de transcendência sobre k maior do que n. $D_{m,t}(k)$ contém um subcorpo de grau de transcendência $m+t$ (gerado por $z_1, \ldots, z_t, x_1, \ldots, x_m$) e, portanto, devemos ter $(*) m + t \leq n$. Se G é finito, pelo análogo não-comutativo do Lema de Artin (lema 4.1 abaixo), $[D_n(k) : D_n(k)^G] \leq |G|$. No caso comutativo, isso nos daria a igualdade dos graus de transcendência. No caso não-comutativo, utilizando o grau de transcendência de GK, é uma questão em aberto se $[D : Q] < \infty$ implica que $GK - trdeg_k D = GK - trdeg_k Q$, onde D, Q são álgebras de divisão sobre k. J. Zhang [Zha98] introduziu uma variante de grau de transcendência não-comutativo, o "lower transcendence degree", denotado por Ld_k, e mostrou que se $[D : Q] < \infty$, $Ld_k\, Q = Ld_k\, D$. Esta noção coincide com $GK - trdeg_k$ no caso dos corpos de Weyl. $GK - trdeg_k D_n(k) = 2n$, $GK - trdeg_k D_{m,t}(k) = 2m + t$. Portanto, se $D_n(k)^G \cong D_{m,t}(k)$, $2n = 2m + t$. Isto, juntamente com $(*)$, implica $m = n$, $t = 0$. □

Uma discussão detalhada sobre diferentes versões de graus de transcendência não-comutativos pode ser encontrada em [KL00], Sec. 12.8. O análogo não-comutativo do Lema de Artin citado acima será utilizado em várias oportunidades, portanto destacamos seu enunciado:

Lema 4.1. (Lema de Artin Não-Comutativo) *Seja D um anel de divisão e G qualquer grupo finito de automorfismos de D. Então $[D : D^G] \leq |G|$; isto é, D é um D^G-espaço vetorial de dimensão finita.*

Demonstração. [Mon80], lema 2.18. □

Vamos analisar agora os casos onde uma solução positiva do Problema de Noether Não-Comutativo é conhecida. Como ficará claro em breve, existe uma similaridade notável com o Problema Noether Clássico.

No caso comutativo, utilizamos o Teorema de Miyata. No caso não-comutativo, usaremos a seguinte generalização para extensões de Ore, obtida por J. Alev e F. Dumas em [AD97].

Teorema 4.4. (Versão Não-Comutativa do Teorema de Miyata) *Seja K um corpo não necessariamente comutativo, σ um automorfismo e δ uma σ-derivação de K. Seja $S = K[x; \sigma, \delta]$ e $D = Frac\, S = K(x; \sigma, \delta)$. Seja G um grupo de automorfismos (não necessariamente finito) do anel S, tal que $g(K) \subseteq K$ para todo $g \in G$. Duas coisas podem acontecer:*

1. *$S^G \subseteq K$. Neste caso, $S^G = D^G = K^G$.*
2. *S^G não está contido em K. Neste caso, para todo $u \in S^G$ de grau maior que 0 em x, e de grau mínimo dentre todos os elementos de S^G de grau maior que 0, existe um automorfismo de K^G, σ', e uma σ'-derivação δ' de K^G, tal que $S^G = K^G[u; \sigma', \delta']$ e $D^G = Frac\, S^G = K^G(u; \sigma', \delta')$.*

Iremos apresentar uma demonstração desse Teorema na Seção 4.4.

Vamos assinalar um fato que será constantemente usado.

Lema 4.2. *Seja K um anel de divisão e $S = [x; \alpha, \delta]$ uma extensão de Ore. Seja G um grupo de automorfismos de S, não necessariamente finito, tal que $G(K) \subseteq K$. Se, para todo $i > 1$, e todo $g \in G$, $g(x^i) = \lambda_i^g x^i$ para algum $\lambda_i^g \in K^*$, então, se tivermos um elemento $y \in S$ invariante por G da forma $y = u_n x^n + \ldots u_1 x + u_0$, com $u_i \in K, u_n \neq 0$, $u_n x^n$ também é G-invariante.*

Demonstração. $y = g(y)$ implica, igualando os coeficientes em K de x^n nos dois lados, que $g(u_n)\lambda_n^g = u_n$ para todo $g \in G$. Logo, $u_n x_n$ é invariante por G. □

Teorema 4.5. *Seja G um subgrupo finito de $GL_1(k) \cong k^*$. Então $D_1(k)^G \cong D_1(k)$.*

Demonstração. Seja $A_1(k) = k[x][y; \partial_x]$. Existe um caráter $\chi : G \to k^*$, tal que $g.x = \chi(g)x, g.y = \chi(g)^{-1}y$. Seja $w = yx$. Como vimos na Proposição 2.12, $D_1(k) = Frac\, S$, onde $S = k(w)[y; \sigma]$. G fixa w e manda y para $\chi(g)^{-1}y$. Logo, estamos na condição de usar a versão não comutativa do Teorema de Miyata, o Teorema 4.4. S^G não pode estar contido em $k(w)$ - se isso ocorresse, se teria, pelo item 1 daquele teorema, $D_1(k)^G = k(w)$; mas pela versão não-comutativa do Lema de Artin, $[D_1(k) : D_1^G(k)] < \infty$. Por consequência, estamos no item 2 do Teorema. Isto é, $S^G = k(w)[u; \sigma', \delta']$ para alguns σ', δ'. Pela forma da ação de G nos monômios y^k, pelo lema 4.2, temos que u é da forma y^a para algum inteiro $a \geq 1$. Então $\sigma' = \sigma^a$, e $\delta' = 0$. Sendo assim, $D_1(k)^G = k(w)(y^a; \sigma^a)$. Este corpo de frações também é gerado por $X = y^a$ e $Y = a^{-1}wy^{-a}$, que satisfazem $[X, Y] = 1$. Logo, $D_1(k)^G \cong D_1(k)$. □

Teorema 4.6. *Seja G um subgrupo finito de $GL_n(k)$, cuja representação natural em k^n é soma direta de representações de dimensão 1. Então, $D_n(k)^G \cong D_n(k)$.*

Demonstração. Provaremos por indução em n, o caso $n = 1$ sendo o teorema acima. Escolhendo uma base adequada, a ação de G em $A_n(k)$ é da forma $g.x_i = \chi_i(g)x_i$, $g.y_i = \chi_i^{-1}(g)y_i$, onde para $i = 1, \ldots, n$ χ_i é um caráter de G. Definimos $w_i = y_i x_i$ para todo i. Todos os w_i são invariantes pela ação de G. Novamente vamos usar a descrição dos corpos de Weyl da Proposição 2.12. Usando a notação desta Proposição, $D_n(k) = k(w_1, \ldots, w_n)(y_1; \sigma_1) \ldots (y_n; \sigma_n)$. Vamos introduzir os subcorpos

$$L = k(w_n),\ K = k(w_1, \ldots, w_n)(y_1; \sigma_1) \ldots (y_{n-1}; \sigma_{n-1}) = D_{n-1}(L).$$

Seja $S = K[y_n; \sigma_n]$; $Frac\, S = D_n(k)$. Usando a hipótese indutiva na restrição da ação de G em K (note que K é estabilizado por G), temos que $K^G = D_{n-1}(L)^G = D_{n-1}(L)$. Estamos em condição de aplicar a versão não-comutativa do Teorema de Miyata. Temos dois casos possíveis.

Se $S^G \subseteq K^G$, então $D_n(k)^G = D_{n-1}(L)^G \cong D_{n-1}(L) = D_{n-1,1}(k)$, o que não pode ocorrer, tendo em vista o Teorema 4.3.

Portanto, estamos no segundo caso do Teorema de Miyata não-comutativo. Seja $u \in S^G$ um elemento invariante de grau minimal em y_n. $S^G = K^G[u; \sigma', \delta']$ para algum automorfismo σ' e σ'-derivação δ' de K^G. u pode ser escrito como

$$f_m y_n^m + \ldots + f_1 y_n + f_0,$$

onde os $f_i \in K^G$, e $m \geq 1$. Tendo em vista a ação de G em y_n (lema 4.2), temos que $u = f_m y_n^m$. Podemos usar o mergulho no anel das séries de Laurent torcidas, como na Seção 2.5, com a ação de G extendida diagonalmente nos y_i e fixando os w_i. Portanto, sem perda de generalidade, podemos supor que $u = y_1^{a_1} \ldots y_n^{a_n}$, onde $(a_1, \ldots, a_n) \in \mathbb{Z}^n$, e $a_n \geq 1$.

Para $1 \leq j \leq n$ se tem $uw_j = (w_j + a_j)u$. Introduzimos os elementos

$$w_i' = w_i - a_n^{-1} a_i w_n$$

para $i = 1, \ldots, n-1$. Temos $w_j' u = u w_j'$ para $1 \leq j \leq n-1$. Como $\sigma_i(w_j') = w_j' + \delta_{ij}$ para $1 \leq i, j \leq n-1$, o corpo $F = k(w_1', \ldots, w_{n-1}')(y_1; \sigma_1) \ldots (y_n; \sigma_{n-1})$ é isomórfico a $D_{n-1}(k)$. Aplicando a hipótese indutiva, $F^G \cong D_{n-1}(k)$. Por definição, é claro que $k(w_n)(w_1', \ldots, w_{n-1}') = k(w_n)(w_1, \ldots, w_n)$. Como w_n comuta com todos os elementos de F, $K = F(w_n)$. A álgebra S^G, então, pode ser escrita como $S^G = F^G(w_n)[u; \sigma', \delta']$.

u comuta com cada um dos w_j', $j = 1, \ldots, n-1$, como vimos, e comuta com todos os y_i por definição, e satisfaz com w_n a relação $uw_n = (w_n + a_n)u$. Portanto, mudando de variáveis: $u' = a_n^{-1} u$ implica que $S^G = F^G(w_n)[u'; \sigma'']$, onde σ'' é a identidade em F^G e satisfaz $\sigma''(w_n) = w_n + 1$. Portanto, $Frac\, S^G = F^G(w_n)(u'; \sigma'') = k(w_1', \ldots, w_{n-1}', w_n)(y_1; \sigma_1) \ldots (y_{n-1}; \sigma_{n-1})(u; \sigma'')$, cuja descrição é a mesma de $D_n(k)$, de acordo com a Proposição 2.12. Portanto, $Frac\, S^G \cong D_n(k)$. □

Corolário 4.1. *Seja G um subgrupo abeliano finito de $GL_n(k)$. Se k contém uma raiz e-ésima da unidade, onde e é o expoente do grupo, então $D_n(k)^G \cong D_n(k)$.*

Os dois últimos Teoremas e Corolário foram obtidos por J. Alev e F. Dumas, [AD06]. Neste trabalho, eles também obtiveram o resultado seguinte:

Teorema 4.7. *Seja G qualquer subgrupo finito de $GL_2(k)$. Então $D_2(k)^G \cong D_2(k)$.*

A demonstração deste teorema é bastante extensa e, portanto, reservaremos uma seção para ela.

4.3 Prova do Teorema 4.7

Nesta seção, usaremos a notação q_1, q_2, p_1, p_2 para denotar os geradores usuais x_1, x_2, ∂_1 (ou y_1),∂_2 (ou y_2) de $A_2(k)$, respectivamente.

Seja G um subgrupo finito de $GL_2(k)$. Para todo $g \in G$,

$$g(q_1) = \alpha_g q_1 + \beta_g q_2,\ g(q_2) = \gamma_g q_1 + \delta_g q_2,$$
$$g(p_1) = \frac{1}{\Delta_g}(\sigma_g p_1 - \gamma_g p_2),\ g(p_2) = \frac{1}{\Delta_g}(-\beta_g p_1 + \alpha_g p_2),$$

onde $\alpha_g, \beta_g, \gamma_g, \delta_g \in k$, e $\Delta_g = \alpha_g\delta_g - \beta_g\gamma_g \neq 0$.

Seja $w = q_1p_1 + q_2p_2$, e $v = q_1q_2^{-1}$. Temos w invariante (proposição 4.1), e com a notação acima:

$$g(v) = \frac{\alpha_g v + \beta_g}{\gamma_g v + \delta_g},\ g(q_2) = (\gamma_g v + \delta_g)q_2.$$

Como na proposição 2.12, podemos expressar $D_2(k)$ da seguinte maneira: $D_2(k) = k(q_1, q_2)(w_1; d_1)(w_2; d_2)$, onde $w_1 = q_1p_1$, $w_2 = q_2p_2$, $d_1 = q_1\partial_1$, $d_2 = q_2\partial_2$. Temos que $[w, w1] = 0$ e $[w, q_1] = q_1$, $[w, q_2] = q_2$. Assim, denotando por d a derivação de $k(q_1, q_2)(w_1; d_1)$, tal que $d(q_1) = q_1$, $d(q_2) = q_2$ e $d(w_1) = 0$, temos $D_2(k) = k(q_1, q_2)(w_1; d_1)(w; d)$, donde $D_2(k) = k(v, q_2)(w_1; d_1)(w; d)$, com $d_1(v) = v$ e $d(v) = d(w_1) = 0$ (de fato, $d(v) = q_1q_2^{-1} - q_1q_2^{-2}q_2 = 0$). Usando esses fatos, vemos que os geradores v, q_2, w, w_1 do corpo $D_2(k)$ satisfazem as relações:

$$[v, q_2] = [w_1, q_2] = [w, v] = [w, w_1] = 0,\ [w_1, v] = v,\ [w, q_2] = q_2.$$

A ação de G em v, q_2, w já foi descrita acima. Para w_1 temos:

$$g(w_1) = \frac{1}{\Delta_g}(\alpha_g q_1 + \beta_g q_2)(\delta_g p_1 - \gamma_g p_2)$$
$$= \frac{1}{\Delta_g}(\alpha_g\delta_g q_1p_1 - \beta_g\gamma_g q_2p_2 - \alpha_g\gamma_g q_1p_2 + \beta_g\delta_g q_2p_1)$$
$$= \frac{1}{\Delta_g}(\alpha_g\delta_g w_1 - \beta_g\gamma_g(w - w_1) - \alpha_g\gamma_g v(w - w_1) + \beta_g\delta_g v^{-1}w_1)$$
$$= \frac{1}{\Delta_g}(\alpha_g + \beta_g v^{-1})(\gamma_g v + \delta_g)w_1 - \frac{1}{\Delta_g}\gamma_g(\beta_g + \alpha_g v)w.$$

Para simplificar a forma da ação, definimos $x = (q_1q_2)^{-1}w_1 = v^{-1}q_2^{-2}w_1 = q_2^{-1}p_1$, de forma que $g(x) = \frac{1}{\Delta_g}x - \frac{1}{\Delta_g}\gamma_g q_2^{-2}(\gamma_g v + \delta_g)^{-1}w$ para todo $g \in G$. $D_2(k)$ é gerado sobre k por v, q_2, w, x, e calculamos: $[x, v] = q_2^{-2}, [x, q_2] = 0, [x, w] = 2x$.

Podemos resumir o que foi feito acima no seguinte lema:

Lema 4.3. *1. Os elementos $w = q_1p_1 + q_2p_2$, $v = q_1q_2^{-1}$ e $x = q_2^{-1}p_1$ verificam as relações:*

$$[q_2, v] = 0;\ [w, v] = 0,\ [w, q_2] = q_2;\ [x, v] = q_2^{-2},\ [x, q_2] = 0,\ [x, w] = 2x.$$

2. *Denotando d a derivação de $k(v, q_2)$, tal que $d(v) = 0$ e $d(q_2) = q_2$; K o corpo $k(v, q_2)(w; d)$; σ' o automorfismo de K fixando v, q_2 e tal que $\sigma'(w) = w + 2$; d' a σ'-derivação de K, tal que $d'(v) = q_2^{-2}$, $d'(q_2) = 0$, $d'(w) = 0$; e S a k-álgebra $K[x; \sigma', d']$, tem-se:*

$$D_2(k) = Frac\, S = K(x; \sigma', d') = k(v, q_2)(w; d)(x; \sigma', d').$$

3. *A ação sobre $D_2(k)$ de um automorfismo $g \in G$ é dada pela seguinte ação nos geradores: $g(v) = \frac{\alpha_g v + \beta_g}{\gamma_g v + \delta_g}$, $g(q_2) = (\gamma_g v + \delta_g)q_2$, $g(w) = w$ e*

$$g(x) = \frac{1}{\Delta_g}x - \frac{1}{\Delta_g}\gamma_g q_2^{-2}(\gamma_g v + \delta_g)^{-1}w.$$

4. *Em particular, a cadeia de subcorpos $k(v) \subset k(v, q_2) \subset K$ é estabilizada por G.*

Essa cadeia de subcorpos estabilizada por G é o cerne da demonstração. O objetivo é utilizar os Teoremas Clássicos e a Extensão para Extensões de Ore dos Teoremas de Miyata (Teorema 1.4, Teorema 4.4), reduzindo a questão de invariantes de cada subcorpo para o subcorpo que o precede na cadeia. Pelo Lema de Artin Não-Comutativo 4.1, não podemos ter $S^G \subseteq K^G$. Mostraremos que podemos substituir o gerador x por um elemento y adequado que é autovetor de todos os elementos de G.

Lema 4.4. *Mantendo a notação do Lema anterior:*

1. *Existe uma função racional $b(v) \in k(v)$, tal que*

$$g(b) = \frac{1}{\Delta_g}(\gamma_g v + \delta_g)^2 b + \frac{1}{\Delta_g}\gamma_g(\gamma_g v + \delta_g),\ \forall g \in G.$$

2. *Definindo $y = x + b(v)q_2^{-2}w = q_2^{-1}p_1 + b(v)q_2^{-2}w \in S$, temos as relações:*

$$[q_2, v] = 0;\ [w, v] = 0,\ [w, q_2] = q_2;\ [y, v] = q_2^{-2},\ [y, q_2] = b(v)q_2^{-1},\ [y, w] = 2y.$$

3. *Denotando: d a derivação de $k(v, q_2)$, tal que $d(v) = 0$ e $d(q_2) = q_2$; σ' o k-automorfismo de K que fixa v, q_2 e manda w para $w + 2$; d'' a σ'-derivação de K, tal que $d''(v) = q_2^{-2}$, $d''(q_2) = b(v)q_2^{-1}$, $d''(w) = 0$, temos $S = K[y; \sigma', d''] = k(v, q_2)(w; d)[y; \sigma', d'']$.*

4. *A ação sobre $D_2(k)$ de um automorfismo $g \in G$ é dada pela seguinte ação nos geradores: $g(v) = \frac{\alpha_g v + \beta_g}{\gamma_g v + \delta_g}$, $g(q_2) = (\gamma_g v + \delta_g)q_2$, $g(w) = w$ e $g(y) = \frac{1}{\Delta_g}y$.*

Demonstração. Seja n o inteiro ≥ 1 que é o grau mínimo em x dos elementos G-invariantes de S que não estão em K. Seja $u = u_n x^n + \ldots + u_1 x + u_0$, $u_i \in K, u_n \neq 0$, um elemento de S^G com grau n em x. Do segundo ponto do último lema temos, definindo $r_g = -\gamma_g(\gamma_g v + \delta_g)^{-1}q_2^{-2}w$, que $g(x) = \frac{1}{\Delta_g}(x + r_g)$, para todo $g \in G$. Sendo assim,

$$g(u) = \left(\frac{1}{\Delta_g}\right)^n g(u_n)(x + r_g)^n + g(u_{n-1})\left(\frac{1}{\Delta_g}\right)^{n-1}(x + r_g)^{n-1} + \ldots$$

Uma vez que K é estabilizado pela ação de G, explicitando os coeficientes em K dos termos de grau n e $n-1$ em x:

$$g(u) = g(u_n)\left(\frac{1}{\Delta_g}\right)^n x^n + \left[g(u_n)\left(\frac{1}{\Delta_g}\right)^n \sum_{i=0}^{n-1}\sigma'^i(r_g) + g(u_{n-1})\left(\frac{1}{\Delta_g}\right)^{n-1}\right]x^{n-1} + \ldots$$

A igualdade $g(u) = u$ implica, para todo $g \in G$, as seguintes igualdades em K:

$$g(u_n) = (\Delta_g)^n u_n.$$

$$g(u_{n-1}) = (\Delta_g)^{n-1}u_{n-1} + (\Delta_g)^{n-1}u_n \sum_{i=0}^{n-1}\gamma_g(\gamma_g v + \delta_g)^{-1}q_2^{-2}(w + 2i).$$

Multiplicando os dois membros da segunda igualdade pelos inversos dos dois membros da primeira, e usando que $\sum_{i=0}^{n-1}(w + 2i) = nw + n(n-1)$, tem-se:

$$g(u_n^{-1}u_{n-1}) = \left[\frac{1}{\Delta_g}u_n^{-1}u_{n-1} + \frac{1}{\Delta_g}n(n-1)\gamma_g(\gamma_g v + \delta_g)^{-1}q_2^{-2}\right] + \left[\frac{1}{\Delta_g}n\gamma_g(\gamma_g v + \delta_g)^{-1}q_2^{-2}\right]w.$$

O elemento $u_n^{-1}u_{n-1}$ de $K = k(v, q_2)(w; d)$ se expressa no corpo de operadores pseudo-diferenciais formais $k(v, q_2)((w^{-1}; -d))$ em uma série de Laurent $u_n^{-1}u_{n-1} = \sum_{j > j_0}\phi_j w^{-j}$ com $\phi_j \in k(v, q_2)$

para todo j. Como w é G-invariante, $g(u_n^{-1}u_{n-1}) = \sum_{j>j_0} g(\phi_j)w^{-j}$, de forma que identificando os coeficientes de w nas igualdades acima temos:

$$g(\phi_{-1}) = \frac{1}{\Delta_g}\phi_{-1} + \frac{1}{\Delta_g}n\gamma_g(\gamma_g v + \delta_g)^{-1}q_2^{-2},\ \forall g \in G.$$

O elemento ϕ_{-1} de $k(v, q_2)$ se desenvolve em $k(v)((q_2^{-1}))$ como uma série de Laurent $\phi_{-1} = \sum_{l>l_0} a_l q_2^{-l}$ com $a_l \in k(v)$ para todo l. Dessa forma, identificando os coeficientes dos termos em q_2^{-2} na igualdade acima nos dá:

$$(\gamma_g v + \delta_g)^{-2}g(a_2) = \frac{1}{\Delta_g}a_2 + \frac{1}{\Delta_g}n\gamma_g(\gamma_g v + \delta_g)^{-1},\ \forall g \in G.$$

Dessa maneira, encontramos um elemento $b = n^{-1}a_2$ de $k(v)$ que satisfaz:

$$g(b) = \frac{1}{\Delta_g}(\gamma_g v + \delta_g)^2 b + \frac{1}{\Delta_g}\gamma_g(\gamma_g v + \delta_g),\ \forall g \in G.$$

Definindo $y = x + bq_2^{-2}w$, para todo $g \in G$:

$$g(y) = g(x) + \left[\frac{1}{\Delta_g}(\gamma_g v + \delta_g)^2 b + \frac{1}{\Delta_g}\gamma_g(\gamma_g v + \delta_g)\right](\gamma_g v + \delta_g)^{-2}q_2^{-2}w$$

$$= \frac{1}{\Delta_g}x - \frac{1}{\Delta_g}\gamma_g q_2^{-2}(\gamma_g v + \delta_g)^{-1}w + \frac{1}{\Delta_g}bq_2^{-2}w + \frac{1}{\Delta_g}\gamma_g(\gamma_g v + \delta_g)^{-1}q_2^{-2}w = \frac{1}{\Delta_g}y.$$

É claro que y gera S sobre K, e a partir das relações entre v, q_2, w e x, as relações seguintes são claras: $[y, v] = q_2^{-1}$, $[y, q_2] = bq_2^{-1}$, $[y, w] = 2y$. Portanto, o lema está demonstrado. □

Lema 4.5. *Na notação do Lema anterior, seja n o grau mínimo em x de elementos de S^G que não pertencem a K.*

1. *$K^G = k(v, q_2)^G(w; d)$, onde d foi restringida a $k(v, q_2)^G$.*

2. *Existe um inteiro m e uma função racional $f_m \in k(v)$, tal que $f = f_m q_2^m$ verifica $g(f) = (\Delta_g)^n f$ para todo $g \in G$.*

3. *Definindo $z = fy^n$, temos que z é invariante pela ação de G.*

4. *Denotando τ o automorfismo de $K^G = k(v, q_2)^G(w; d)$ que se restringe à identidade em $k(v, q_2)^G$ e manda w para $w + 2n - m$, existe uma τ-derivação D de K^G, tal que:*

$$S^G = k(v, q_2)(w; d)[z; \tau, D],\ D_2(k)^G = k(v, q_2)(w; d)(z; \tau, D).$$

Se $n \geq 2$, a restrição de D em $k(v, q_2)^G$ é 0.

Demonstração. Na notação do Lema anterior, temos que $u_n \in K$ satisfaz $g(u_n) = (\Delta_g)^n u_n$ para todo $g \in G$. Desenvolvendo u_n em série de Laurent em $K(v, q_2)((w^{-1}; -d))$, temos que $u_n = \sum_{j \geq j_0} \psi_j$, $\psi_j \in k(v, q_2)$ para todo j, e $\psi_{j_0} \neq 0$. Como w é G-invariante, isso nos dá $g(\psi_{j_0}) = (\Delta_g)^n \psi_{j_0} w^{-j}$ para todo $g \in G$. Desenvolvendo agora ψ_{j_0} em série de Laurent em $k(v)((q_2))$, temos $\psi_{j_0} = \sum_{i \geq m} f_i q_2^i$, $f_i \in k(v), f_m \neq 0$. Isso nos dá $g(f_m)(\gamma_g v + \delta_g)^m = (\Delta_g)^n f_m$ para todo $g \in G$. Definindo $f = f_m q_2^m$, temos que $g(f) = (\Delta_g)^n f$ para todo $g \in G$ e, dessa forma, definindo $z = fy^n$, temos que z é G-invariante. Como y tem grau 1 em x, temos que o grau de z em x é igual a n e, portanto, pelo Teorema 4.4, temos que $S^G = K^G[z; \tau, D]$ para um automorfismo τ de K^G e uma τ-derivação D. Aplicando novamente o Teorema 4.4 em $S_0 = k(v, q_2)[w; d]$, cujo corpo de frações é K, uma vez que w é G-invariante, temos que $K^G = k(v, q_2)^G(w; d)$ e portanto:

$$D_2(k)^G = Frac\, S^G = k(v, q_2)^G(w; d)(z; \tau, D).$$

Podemos calcular a relação de comutação entre z e w. $yw = (w+2)y$; portanto, $y^n w = (w + 2n)y^n$; e então $fy^n w = (fw + 2nf)y^n = (wf - d(f))y^n + 2nz = wz + (2n - d(f)f^{-1})z$. Como $d(v) = 0$ e $d(q_2) = q_2$, $d(f) = d(f_m q_2^m) = mf_m q_2^m = mf$. Assim:

$$zw - wz = (2n - m)z.$$

Podemos também fazer algumas precisões sobre os valores de τ e D em $k(v, q_2)^G$. Relembrando a notação do Lema anterior, item 3, temos que para todo $a \in k(v, q_2)$, $ya = ay + d''(a)$, e por indução $y^n a = ay^n + nd''(a)y^{n-1} + \dots$ (termos de grau $\leq n-2$ em y). Multiplicando à esquerda por f:

$$za = az + nd''(a)fy^{n-1} + \dots, \forall a \in k(v, q_2).$$

Se $a \in k(v, q_2)^G$, então por outro lado $za = \tau(a)z + D(a)$. Juntando isto com a equação acima, temos

$$(\tau(a) - a)z + D(a) = nd''(a)fy^{n-1} + \dots$$

Da igualdade dos coeficientes, em $k(v, q_2)$, de y^i nessa equação, temos que τ se restringe à identidade em $k(v, q_2)^G$, de forma que D se restringe a uma derivação. Se $n \geq 2$, o coeficiente de y^{n-1} é 0, isto é, $d''(a) = 0$, e isto mostra que $D(a) = 0$ para todo $a \in k(v, q_2)^G$. A prova assim se encerra. $\square$

Vamos ver agora que, na notação do lema acima, $n \geq 2$ não pode ocorrer. Caso contrário, teríamos $D_2(k)^G = k(v, q_2)^G(w; d)(z; t)$. Em $k(v, q_2)$, d'' age como $q_2^{-2}\partial_v + b(v)q_2^{-1}\partial_{q_2}$, e do lema acima sabemos que em $k(v)^G$, d'' age como 0. Portanto, a única possibilidade é $k(v)^G = k$. Mas em função do lema 1.1, isso não pode ocorrer. Dessa maneira, $n = 1$.

Finalmente, podemos encerrar a demonstração do Teorema 4.7.

Demonstração. Relembrando o último lema, temos que $z = yf$ e $f = f_m q_2^m$ para algum inteiro m e $f_m \neq 0 \in k(v)$. Usando a sua última conclusão, podemos reescrever $D_2(k)^G$ como a seguinte extensão de Ore iterada:

$$k(v, q_2)^G(z; D)(w; d),$$

onde $D = fd''$, com d'' a derivação introduzida no lema 4.4. Ou seja, D é a restrição a $k(v, q_2)^G$ da derivação de $k(v, q_2)$ definida por $D(v) = f_m q_2^{m-2}$ e $D(q_2) = f_m b q_2^{m-1}$. d é a derivação de $k(v, q_2)^G(z; D)$, tal que $d(z) = (m-2)z$, e em $k(v, q_2)^G$ é a restrição da derivação de $k(v, q_2)$ definida por $d(v) = 0$, $d(q_2) = q_2$.

Como de praxe, definimos $B = k(v)[q_2]$. Pelo Lema de Artin, não podemos ter $B^G \subseteq k(v)^G$. Seja então q um elemento de B^G de grau não-nulo e minimal em q_2; denotamos tal grau de e. Pelo formato da ação de G em q_2 (lema 4.2), temos $q = sq_2^e$, como $s \neq 0 \in k(v)$. Então, $Frac\, B^G = k(v, q_2)^G = k(v)^G(q)$. Como $d(q_2) = q_2$, $d(v) = 0$, temos $d(q) = eq$. Calculamos:

$$D(q) = D(s)q_2^e + seD(q_2)q_2^{e-1} = \partial_v(s)D(v)q_2^e + sef_m b q_2^{e+m-2} = (\partial_v(s) + esb)f_m q_2^{e+m-2}.$$

$D(q) \in k(v)^G(q)$ se desenvolve em $k(v)^G((q))$ como uma série de Laurent $\sum_{j>j_0} h_j q^j$ com $h_j \in k(v)^G$. Como $q^j = s^j q_2^{ej}$, a partir da igualdade obtida acima para $D(q)$, temos que $D(q)$ é um monômio $h_r q^r$, onde o inteiro r satisfaz $e + m - 2 = er$, e $h_r = s^{-r}(\partial_v(s) + esb)f_m$; vamos denotar tal elemento simplesmente por c. Resumindo:

$$D_2(k)^G = k(v)^G(q)(z; D)(w; D),$$

com $D(q) = cq^r$ e $d(q) = eq$, $c \in k(v)^G$ e $er = e + m - 2$. Novamente, pelo lema 1.1, temos que $k(v)^G = k(t)$ para alguma função racional $t(v)$. Como d é 0 em $k(v)^G$, $d(t) = 0$. $D(t) = \partial_v(t)D(v) = \partial_v(r)f_m q_2^{m-2}$. Como $q = sq_2^e$ e $m - 2 = e(r-1)$, temos $q_2^{m-2} = s^{1-r}q^{r-1}$ e, portanto, $D(t) = \partial_v(t)f_m s^{1-r}q^{r-1}$. Simplificando a notação, definimos $a = \partial_v(t)f_m s^{1-r}$. Note que $a \neq 0 \in k(v)$, pois $f_m, s \neq 0$ e $t \notin k$. Além disso, $a = D(t)q^{1-r} = [z, t]q^{1-r}$ é invariante sobre G e, portanto, pertence a $k(t)$. Assim, $D_2(k)^G = k(t, q)(z; D)(w; d)$, com :

$[z,t] = D(t) = aq^{r-1}$, $[z,q] = D(q) = cq^r$, $[w,t] = d(t) = 0$, $[w,q] = d(q) = eq$, $[w,z] = d(z) = (m-2)z$.

Introduzindo $z' = q^{1-r}z$, $d(z') = (m-2)q^{1-r}z + (1-r)eq^{1-r}z = 0$. Denotando $D' = q^{1-r}D$: $D_2(k)^G = k(t,q)(z';D')(w;d)$, com:

$[q,t] = 0$, $[z',t] = D'(t) = a$, $[z',q] = D'(q) = cq$, $[w,t] = d(t) = 0$, $[w,q] = d(q) = eq$, $[w,z'] = d(z') = 0$.

Os 4 elementos $t, q, w'' = \frac{1}{eq}w$ e $z'' = -\frac{c}{ea}w + \frac{1}{a}z'$ geram $D_2(k)^G$ e verificam:

$$[q,t] = 0,\ [z'',t] = 1,\ [z',q] = 0,\ [w'',t] = 0,\ [w'',q] = 1,\ [w'',z''] = 0.$$

Isso exibe de maneira explícita um isomorfismo $D_2(k)^G \cong D_2(k)$. E encerra a prova. $\square$

A natureza elementar desta demonstração permite elaborar um procedimento mais ou menos direto para exibir explicitamente o isomorfismo $D_2(k)^G \cong D_2(k)$. Para um caso interessante, podemos de fato obter esse isomorfismo de maneira uniforme e algorítmica. Quando $k = \mathbb{C}$, temos o clássico resultado da classificação dos subgrupos finitos de $SL_2(\mathbb{C})$: os grupos cíclicos, dihedrais, binário tetraédrico, binário octaédrico, e binário icosaédrico ([Spr77], por exemplo). Também temos que $k[q_1,q_2]$ tem uma estrutura natural de álgebra de Poisson, cujo colchete é invariante pela ação induzida de $SL_2(\mathbb{C})$. Usando isso e o resultado bem conhecido dos invariantes dos subgrupos finitos de $SL_2(\mathbb{C})$ ([Spr77]), na seção 3.2 de [AD06] é exibido o isomorfismo explícito $D_2(\mathbb{C})^G \cong D_2(\mathbb{C})$. Por exemplo, quando G é grupo cíclico de ordem ímpar $2p+1$ os elementos de $D_2(\mathbb{C})^G$ que realizam o isomorfismo são: $Q_1 = q_1^p q_2^{-p}$, $Q_2 = q_1q_2$,

$$P_2 = \frac{1}{2}(q_2^{-1}p_1 + q_1^{-1}p_2),$$

$$P_1 = \frac{1}{2p}(q_1^{1-p}q_2^p p_1 - q_1^{-p}q_2^{p+1}p_2).$$

4.4 Invariantes do Grupo Simétrico

O resultado discutido nesta seção foi obtido por S. Ovsienko e V. Futorny [FO06], usando métodos elementares, e A. Molev, S. Ovsienko e V. Futorny usando um argumento geométrico [FMO10]. Com ele, é possível obter uma demonstração nova da Conjectura de Gelfand-Kirillov para $gl_n(k)$, [FMO10]. Apresentaremos uma versão adaptada daquela em [FO06], substituindo certos cálculos envolvidos por um argumento conceitual, usando anéis de grupos torcidos. Essa modificação será utilizada no Capítulo 6.

Seja k um corpo arbitrário de característica 0. Seja $\Lambda = k[x_1,\ldots,x_n]$. Temos uma ação conhecida do grupo simétrico S_n em Λ: $\pi \in S_n$ manda $x_i \to x_{\pi(i)}$, para todo i. Esta ação se estende para $A_n(k) = D(\Lambda)$. Aqui usaremos a primeira noção de operadores diferenciais (lembrando que ambas são equivalentes, pois Λ é finitamente gerado regular). Segue a descrição explícita dessa ação:

Seja $\pi \in S_n$. Vamos calcular $\pi.x_i$ (visto agora como elemento de $D(\Lambda)$). Seja $f \in \Lambda$. Então $\pi.x_i(f) = \pi(x_i\pi^{-1}(f)) = \pi(x_i)f = x_{\pi(i)}f$. Logo, $\pi.x_i = x_{\pi(i)}$. De fato, já havíamos visto este fato na discussão no começo da Seção 4.2.

Para calcular $\pi.(\partial_i)$, temos: $\pi(\partial_i(\pi^{-1}(x_j))) = 1$ se $j = \pi(i)$, e 0 caso contrário. Logo, $\pi(\partial_i) = \partial_{\pi(i)}$. Resumindo, S_n apenas permuta os x_i, ∂_i simultaneamente.

Vamos relembrar a demonstração de que $(Frac\,\Lambda)^{S_n} \cong Frac\,\Lambda$. $(Frac\,\Lambda)^{S_n} \cong Frac\,\Lambda^{S_n} \cong Frac\,\Lambda$. Idealmente, gostaríamos que a demonstração para os corpos de Weyl seguisse os mesmos passos. Contudo, não é o caso $A_n(k)^{S_n} \cong A_n(k)$, e então o procedimento não funcionará do mesmo modo. Contudo, ele funcionará se tomarmos uma etapa intermediária: localizar por um elemento adequadamente escolhido.

Vamos aplicar ideias desenvolvidas na Seção 2.2 - lembrando que S_n é um grupo de reflexão sobre qualquer corpo de característica 0. Seja $\Lambda^{S_n} = k[e_1, \ldots, e_n]$, onde e_i é o i-ésimo polinômio simétrico elementar em n variáveis. Seja M a matriz $n \times n$ cuja entrada ij é $\partial_j e_i$, e seja J seu determinante. Sabemos pelo Teorema 3.5 que $\pi J = det(\pi) J$ para todo $\pi \in S_n$ e, portanto, $\Delta = J^2$ é invariante por S_n (de fato, $\det(\pi) = \pm 1$, para qualquer $\pi \in S_n$, pois os elementos do grupo simétrico correspondem a transformações ortogonais). J, na verdade, é um polinômio bastante conhecido:

Proposição 4.2. $J = \prod_{i<j}(x_i - x_j)$.

Demonstração. De fato, J é um polinômio de grau $n(n-1)/2$. Substituindo x_i por x_j, $j \neq i$ em J, claramente obtemos 0. Portanto, $\prod_{i<j}(x_i - x_j)$ divide J, e como ambos têm o mesmo grau, $J = a \prod_{i<j}(x_i - x_j)$ para algum escalar a. Observando que, em ambos os polinômios, o monômio $x_1^n x_2^{n-1} \ldots x_n$ aparece com coeficiente 1, tem-se que $a = 1$. □

Considere os anéis Λ_Δ e $\Lambda_\Delta^{S_n}$. O segundo é um subanel do primeiro. Seja $d \in D(\Lambda_\Delta)^{S_n}$, e $f \in \Lambda_\Delta^{S_n}$. Para todo $\pi \in S_n$, $\pi(d(f)) = (\pi.d)(\pi f) = d(f)$ - ou seja, $d(f)$ também está em $\Lambda_\Delta^{S_n}$. Desta forma, restringindo o domínio, obtém-se um homomorfismo de anéis $\phi : D(\Lambda_\Delta)^{S_n} \to D(\Lambda_\Delta^{S_n})$.

Teorema 4.8. *ϕ é um isomorfismo.*

Vamos por partes. Primeiro vamos mostrar a sobrejetividade. Seja

$$E_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix},$$

o vetor de tamanho n, com 1 na posição i e 0 nas demais, e seja

$$F_i = \begin{pmatrix} f_{i1} \\ \vdots \\ f_{in} \end{pmatrix}$$

uma solução do sistema $MF_i = E_i$. Pela Regra de Cramer, é claro que $f_{ij} \in \Lambda_\Delta$, $1 \leq i, j \leq n$.

Seja $d_i = \sum_{k=1}^n f_{ik} \partial_k$. Temos que $d_i(e_j) = \delta_{ij}$, e que cada $d_i \in D(\Lambda_\Delta) = D(\Lambda)_\Delta$ (proposição 2.10). Se d_i for S_n invariante, então os d_i, e_i são enviados por ϕ para os geradores de $D(\Lambda_\Delta^{S_n})$. Portanto, resta provar que cada d_i é S_n invariante.

Lema 4.6. *d_i é invariante pela ação de S_n.*

Demonstração. É suficiente mostrar que $\pi f_{ij} = f_{i\pi(j)}$ para $1 \leq i, j \leq n$, poris $\pi(\partial_i) = \partial_{\pi(i)}$. Vamos usar a regra de Cramer. Seja v_i o vetor

$$\begin{pmatrix} \partial_i e_1 \\ \vdots \\ \partial_i e_n \end{pmatrix}.$$

É claro que $\pi(v_i) = v_{\pi(i)}$.

$$f_{ij} = \frac{det(v_1, \ldots, E_i, \ldots, v_n)}{det(v_1, \ldots, v_n)},$$

com E_i na posição j.

Então,

$$\pi f_{ij} = \frac{det(v_{\pi(1)}, \ldots, E_i, \ldots, v_{\pi(n)})}{det(v_{\pi(1)}, \ldots, v_{\pi(n)})}$$

$$= sign(\pi)det(v_1, \ldots, E_i, \ldots, v_n)/sign(\pi)det(v_1, \ldots, v_n),$$

com agora E_i na posição $\pi(j)$.

E, isso é igual a $f_{i\pi(j)}$. □

Portanto, temos que a função ϕ é sobrejetiva.

Da mesma forma em que ϕ foi obtida restringindo, para cada $d \in D(\Lambda_\Delta)^{S_n}$, o domínio para $\Lambda_\Delta^{S_n}$, obtemos por restrição de domínio um homomorfismo $\phi' : D(\Lambda)^{S_n} \to D(\Lambda^{S_n}) \subseteq D(\Lambda_\Delta^{S_n})$.

Lema 4.7. *Se ϕ' é injetiva, então ϕ é injetiva.*

Demonstração. Seja $d \neq 0 \in D(\Lambda_\Delta)$. Pela proposição 2.10, $D(\Lambda_\Delta)$ é a localização à esquerda por Δ de $D(\Lambda)$. Portanto, d pode ser escrito da forma $\Delta^k D$, com $k \in \mathbb{Z}, D \neq 0 \in D(\Lambda)$. Se d é S_n invariante, como Δ é S_n invariante, D também é S_n invariante. Então, $\phi(d) = \phi(\Delta)^k \phi'(D)$. O primeiro termo é não nulo, e se ϕ' é injetivo, o segundo também não. Como $D(\Lambda_\Delta^{S_n})$ é domínio, tal produto não é nulo e, portanto, ϕ é injetiva (esse anel é realmente um domínio, pois é isomórfico a uma localização de uma álgebra de Weyl, como é claro usando a proposição 2.10 e o fato que $\Lambda^{S_n} \cong \Lambda$). □

Vamos demonstrar que ϕ' é injetiva, mostrando que $A_n(k)^{S_n}$ é simples. Introduziremos, para uso agora e no Capítulo 5, o conceito de anel de grupo torcido.

Definição 4.4. *Seja R um anel e G um subgrupo finito de $Aut\, R$. O anel de grupo torcido $R\#G$ é, como R-módulo à esquerda, livremente gerado pelos elementos de G, e a multiplicação é estendida por linearidade, a partir do seguinte produto: $rgsh = rg^{-1}(s)gh$, $r, s \in R, g, h \in G$.*

Sendo finitamente gerado como R-módulo à esquerda, $R\#G$ é noetheriano à esquerda. R é canonicamente identificado a um subanel de $R\#G$: $R\, id$.

Definição 4.5. *Dado R um anel e $g \in Aut\, R$, dizemos que g é um automorfismo interno se ele é da forma $g : r \to xrx^{-1}$, para um certo x unidade em R. Se g não é interno, ele é dito* externo. *Um subgrupo G de $Aut\, R$ é de automorfismos externos se ele não possui automorfismos internos além da unidade.*

Proposição 4.3. *Dado um anel R simples e um subgrupo finito de automorfismos externos G de $Aut\, R$, então $R\#G$ é simples.*

Demonstração. Seja I um ideal não nulo de $R\#G$. Defina como comprimento, para $x \in R\#G$, a cardinalidade do conjunto $\{x_g \neq 0\}$, onde x_g são os coeficientes de $x : x = \sum_{g \in G} x_g g$. Seja $y \in I$ um elemento diferente de 0 de comprimento mínimo. Multiplicando à esquerda por um elemento adequado de G, podemos supor que $y_{id} \neq 0$. Além disso, como R é simples, $Ry_{id}R = R$ e, portanto, existem elementos $j, k \in R$, tal que $jy_{id}k = 1$. Multiplicando y à esquerda por j e à direita por k, podemos supor $y_{id} = 1$. Seja, portanto,

$$y = id + \sum_{g \neq id \in G} y_g g.$$

Se $y = id$, então $I = R\#G$ e estamos feitos. Caso contrário, seja $h \neq id \in G$ com $y_h \neq 0$. $ry - yr \in I$ para todo $r \in R$ e é igual a $\sum_{g \neq id \in G}(ry_g - y_d g^{-1}(r))g$, que tem comprimento menor y. Portanto isto resulta em 0, e assim para todo $r \in R$ $(*) ry_h = y_h h^{-1}(r)$. Isso implica $Ry_h = y_h R$ é um ideal bilateral, que pela simplicidade de R deve ser o próprio R. Portanto, y_h é uma unidade, e sendo assim por (*), $h^{-1}(r) = (y_h)^{-1} r y_h$, e h é um automorfismo interno. Isso contraria as hipóteses, pois $h \neq id$. Portanto, y necessariamente é id, e $I = R\#G$. □

Vamos relembrar o seguinte resultado de equivalência de Morita.

Observação. *Dois anéis S e T são equivalentes por Morita quando existem funtores aditivos entre as categorias de módulos à esquerda de S e T, que nos dão uma equivalência de categorias (é claro que o mesmo conceito existe para módulos à direita). Várias propriedades de anéis são preservadas por equivalência de Morita. [MR01] é uma boa referência para este assunto.*

Proposição 4.4. *Dois anéis T e S são equivalentes por Morita, se e somente se, existe $n \geq 1$ e um idempotente $e \in M_n(S)$, tal que $T \cong eM_n(S)e$ e $M_n(S)eM_n(S) = M_n(S)$.*

Demonstração. [MR01], proposição 3.5.6. □

Teorema 4.9. *Se R é um anel simples, G é um subgrupo finito externo de $Aut\, R$, e $|G|$ é invertível em R, então R^G é simples.*

Demonstração. Simplicidade é invariante por Morita, portanto basta provar que R^G é equivalente por Morita a $S = R\#G$. Usamos o critério acima com $n = 1$ (ou seja $M_n(S)$ é apenas S). Seja $e = 1/|G| \sum_{g \in G} g$. $e^2 = e$, $eSe \cong R^G$ (lema 5.1) e $SeS = S$ pois, como acabamos de ver, S é simples. □

As unidades de $A_n(k)$ são apenas os elementos de k, como vimos no corolário 2.1 e, portanto, $A_n(k)$ não têm automorfismos internos não triviais; além disso $A_n(k)$ é simples e *char* $k = 0$. Logo, usando o teorema acima:

Teorema 4.10. *Sendo G qualquer grupo finito de automorfismos de $A_n(k)$, $A_n(k)^G$ é simples.*

Se k é um corpo algebricamente fechado, temos o seguinte resultado mais preciso para a álgebra de Weyl, de Levasseur [Lev80], Teo. 5, pág. 170:

Teorema 4.11. *Seja G um grupo finito de automorfismos lineares de Λ (e portanto, por extensão, de $A_n(k)$). Por restrição de domínio, tal como acima, obtemos um homomorfismo $\theta : A_n(k)^G \to D(\Lambda^G)$. Este homomorfismo é sempre injetivo, e é um isomorfismo, se e somente se, G não contém nenhuma pseudo-reflexão além da identidade.*

Isso explica a necessidade da etapa intermediária de localizar por Δ: S_n é um grupo de reflexões.

Estamos prontos agora para concluir a demonstração de que $D_n(k)^{S_n} \cong D_n(k)$. Vamos enumerar alguns fatos:

1. Seja S um conjunto mulitplicativo de Λ. $D(\Lambda_S) = D(\Lambda)_S$.
2. Seja G um grupo finito agindo em Λ e Ξ um elemento G-invariante. $(D(\Lambda)_\Xi)^G \cong (D(\Lambda)^G)_\Xi$.
3. Nas mesmas condições acima, $\Lambda_\Xi^G = (\Lambda^G)_\Xi$.
4. $D(\Lambda_\Delta)^{S_n} \cong D(\Lambda_\Delta^{S_n})$, com $\Delta = \prod_{i<j}(x_i - x_j)^2$.

Acabamos de provar o item 4. O item 1 é a proposição 2.10, o item 3 é a proposição 3.10. Vamos provar o item 2. Todo elemento de $(D(\Lambda)_\Xi)^G$ é, em particular, um elemento de $D(\Lambda)_\Xi$, e portanto pode ser escrito da forma $D\Xi^k$ (em função do item 1), com $D \in D(\Lambda), k \in \mathbb{Z}$. Como o produto é invariante, e Ξ é invariante, D também é invariante.

Considere a seguinte cadeia de isomorfismos:
$((D(\Lambda))^{S_n})_\Delta \cong ((D(\Lambda))_\Delta)^{S_n} \cong D(\Lambda_\Delta^{S_n}) \cong D(k[e_1, \ldots, e_n]_\Delta) \cong (D(k[e_1, \ldots, e_n]))_\Delta$.

O primeiro isomorfismo é o item 2 acima. O segundo é o ponto 1, seguido do ponto 4. O terceiro é o resultado clássico da geração dos polinômios simétricos pelos simétricos elementares. O quarto é o item 1.

Localizar antes de tomar corpo de frações, quando estamos num domínio, não muda nada. Portanto, tomando o corpo de frações do primeiro e do último anel nessa cadeia de isomorfismos, temos $Frac\, A_n^{S_n} \cong D_n(k)^{S_n} \cong D_n(k)$. No primeiro isomorfismo, usamos a proposição 4.5, a primeira da próxima seção.

Note, finalmente, que o isomorfismo obtido pode ser escrito de maneira explícita. Por exemplo, quando consideramos S_3, o isomorfismo é dado por: $D_3(k)^{S_3} \to D_3(k)$:

$$x_1 + x_2 + x_3 \to X_1,\; x_1x_2 + x_2x_3 + x_1x_3 \to X_2,\; x_1x_2x_3 \to X_3;$$

$$\frac{x_1^2(x_2-x_3)}{J}\partial_1 + \frac{x_2^2(x_3-x_1)}{J}\partial_2 + \frac{x_3^2(x_1-x_2)}{J}\partial_3 \to Y_1;$$
$$\frac{x_1(x_3-x_2)}{J}\partial_1 + \frac{x_2(x_1-x_3)}{J}\partial_2 + \frac{x_3(x_2-x_1)}{J}\partial_3 \to Y_2;$$
$$\frac{(x_2-x_3)}{J}\partial_1 + \frac{(x_3-x_1)}{J}\partial_2 + \frac{(x_1-x_2)}{J}\partial_3 \to Y_3.$$

Denotamos por $X_1, X_2, X_3, Y_1, Y_2, Y_3$ os geradores canônicos de $D_3(k)$.

4.5 Prova da Extensão Não-Comutativa do Teorema de Miyata

Proposição 4.5. *Seja R um domínio com $X = R - \{0\}$ um conjunto de Ore à direita e à esquerda, com corpo de frações F. Seja G um grupo finito de automorfismos de R, com $|G|$ invertível em R. Então R^G também admite corpo de frações, isto é, $R^G - \{0\}$ é um conjunto de Ore à direita e à esquerda. Além disso, $Frac\, R^G = F^G$.*

Demonstração. Inicialmente note que, se I, J são dois ideais à esquerda não nulos de R, $I \cap J \neq (0)$. De fato, se $i \in I, j \in J$ são elementos não nulos, pela condição de Ore à esquerda $Ri \cap Rj \neq (0)$. Indutivamente, a interseção de qualquer família finita de ideais à esquerda é não nula. Seja $x \in F^G$, diferente de 0. Ele é da forma $t^{-1}b$. Seja $N = \bigcap_{g \in G} g(Rt)$. Ele é um ideal à esquerda não nulo, e $G(N) \subseteq N$ e, portanto, em função de um Teorema de Isaac e Bergson (corol. 1.5, [Mon80]) existe $v = dt \in N$ não nulo e G-invariante. Então, $x = t^{-1}b = t^{-1}d^{-1}db = v^{-1}u$, onde $u = db$. Como x, v são G invariantes, u também o é. Portanto, temos o seguinte: (*) todo elemento de F^G diferente de 0 é da forma $v^{-1}u$, com $u, v \neq 0 \in R^G$.

Sejam agora $a, b \in R^G$ não nulos. $ab^{-1} \in F^G$ é da forma $v^{-1}u$ para alguns $u, v \neq 0 \in R^G$, por (*). Isto implica que $va = ub$, que é exatamente a condição de Ore à esquerda para R^G. Similarmente temos a condição de Ore à direita. Finalmente, (*) deixa claro que $Frac\, R^G = F^G$. □

Lema 4.8. *Seja K um corpo não necessariamente comutativo, e $S = K[x; \sigma, \delta]$ uma extensão de Ore. Seja $u \in S$ de grau maior que 0.*

1. *Para qualquer subcorpo (comutativo ou não) L de K, a família $U = \{u^i; i \geq 0\}$ é linearmente independente à esquerda e à direita sobre L.*

2. *Se os módulos à esquerda e à direita gerados por U sobre L são iguais, a T digamos, e T é um anel, então $T = L[u; \sigma', \delta']$ para algum automorfismo σ' de L, e uma σ'-derivação de L.*

3. *Se K é comutativo, então $\sigma' = \sigma^m$, onde m é o grau de u.*

Demonstração. O ponto 1 é imediato levando em consideração os termos de maior grau nos polinômios em U, uma vez que S é livre sobre K (e portanto sobre L), tanto à esquerda quanto à direita.

Agora, para provar 2: $deg\, ua = deg\, u$, para todo $a \in L$. Portanto, existem $a_1, a_0 \in L$ unicamente determinados com $ua = a_1u + a_0$. Definimos mapas $L \to L$ assim: $\sigma' : a \to a_1$, $\delta' : a \to a_0$ satisfazendo $ua = \sigma'(a)u + \delta'(a)$ para todo $a \in L$. Denotando $u = \lambda_m x^m + \ldots + \lambda_0$, com $m \geq 1$, $\lambda_i \in L$, $\lambda_m \neq 0$, temos que $\lambda_m \sigma^m(a) = \sigma'(a)\lambda_m$ para todo $a \in L$. Isso implica que σ' é um automorfismo interno de L, e implica, também, o ponto 3. A associatividade e distributividade no anel T implicam que δ' é uma σ'-derivação, como em [GJ04], pág. 33. Então, temos o ponto 2. □

Demonstração. (Extensão Não-Comutativa do Teorema de Miyata)

Seja $g \in G$ arbitrário, $s \in S$ arbitrário, e considere $n = deg\, g(x)$. Como $G(K) \subseteq K$, $deg\, g(s)$ é um múltiplo de n; portanto $n = 1$, pois g é sobrejetiva. Dessa forma, $deg\, g(s) = deg\, s$, para todos $g \in G, s \in S$.

Se $S^G \subseteq K$, $S^G = K^G$. Caso contrário, seja $u \in S^G$ de grau mínimo possível em x sem pertencer a K. Seja $m = deg\, u$. Para aplicar o lema acima, com $L = K^G$, precisamos mostrar que o K^G-módulo à esquerda gerado pelas potências de u, que chamaremos T, é igual a S^G. Evidentemente $T \subseteq S^G$. Vamos provar a inclusão reversa: seja $s \in S^G$. Então temos, pela Proposição 2.7 que $s = q_1 u + r_1$ para $q_1, r_1 \in S$ únicos, com $deg\, r_1 < deg\, u$. Para todo $g \in G$, $s = gs = g(q_1)u + g(r_1)$. Pela unicidade do quociente e resto, $g(q_1) = q_1$ e $g(r_1) = r_1$ para todo $g \in G$. Ou seja, eles são invariantes. Como ou $r_1 = 0$ ou $deg\, r_1 < deg\, u$ e u foi escolhido de grau mínimo, $r_1 \in K^G$.

Resumindo, conseguimos escrever $s \in S^G$ arbitrário da forma $q_1 u + r_1$, com $q_1 \in S^G$ de grau menor que s (uma vez que o grau de u é maior que 0) e $r_1 \in K^G$. Repetindo o processo com q_1 no lugar de s, iterativamente, obtemos que s é combinação linear com coeficientes em K^G das potências de u, como módulo à esquerda. Usando divisão euclidiana à direita, obtemos o mesmo resultado como módulo à direita. Usando o resultado 2 do lema acima, temos que existem um K^G automorfismo σ' e uma σ'-derivação δ' com $S^G = K[u; \sigma', \delta']$.

Quando G é finito, podemos usar a Proposição 4.5 e proposição 2.11 para concluir a prova da versão não-comutativa do Teorema de Miyata. Usamos esse Teorema apenas neste caso, nesta dissertação. Para o caso de G não necessariamente finito, [AD97] ou [Dum06]. □

4.6 Semelhanças entre as versões Clássica e Não-Comutativa

Resumiremos aqui os resultados que estudamos.

Vimos no Capítulo 1 que, quando a representação de G em V é de dimensão 1 ou 2; quando G é abeliano e o corpo base tem uma e-ésima raiz primitiva da identidade; e quando G é um grupo de pseudo-reflexões, o Problema de Noether Clássico tem solução positiva. Neste Capítulo, vimos que todos esses casos, com exceção do último, também apresentam solução positiva para o Problema de Noether Não-Comutativo. Vimos que $D_n(k)^G \cong D_n(k)$ para um caso específico de grupo de reflexão: S_n. No próximo Capítulo, mostraremos uma generalização grande deste fato, que aumenta a lista de semelhança de casos positivos de solução para os Problemas Clássico e Não-Comutativo: mostraremos que $D_n(k)^W \cong D_n(k)$ para todos os grupos de pseudo-reflexão W, quando k é algebricamente fechado.

4.7 Referências

A seção 1 se baseou em material de [KL00], Capítulo 7. O Teorema 4.1 tem a demonstração baseada em [Cou95]. O primeiro resultado presente na literatura semelhante ao Problema de Noether não-comutativo, do tipo $D_n(k)^G \cong D_n(k)$, se deve a J. Alev e F. Dumas [AD98], no caso k algebricamente fechado e G abeliano, com uma demonstração independente da apresentada neste capítulo. O material da seção 2 é originário, principalmente, de [AD06]. A prova do Teorema 4.7 na Seção 3 seguiu de perto a encontrada nesta referência, com algumas simplificações, pois G é finito, e no artigo original eles trabalhavam sem essa hipótese. A seção 4 é baseada em [FO06], com algumas simplificações. A seção 5 foi baseada em [Dum06].

Capítulo 5

Novos Resultados

O objetivo deste Capítulo é provar os Teoremas 5.5 e 5.6 - usando todo o material desenvolvido previamente na dissertação. O Teorema 5.5 é bastante conhecido, mas de acordo com nosso conhecimento, não havia uma prova explícita na literatura. O Teorema 5.6 é novo, e a versão no caso não-comutativo da solução positiva do Problema de Noether para grupos de pseudo-reflexão. O Teorema 5.6 foi obtido pelo aluno, desenvolvendo ideias no artigo [FMO10], em colaboração com Vyacheslav Futorny e Farkhod Eshmatov. Além de resultados da teoria de grupos de pseudo-reflexão, desenvolvidos no Capítulo 3, usamos de maneira essencial resultados do artigo “Graded Cofinite Rings of Differential Operators", de Friedrich Knop [Kno06].

5.1 Material preliminar

O material desenvolvido aqui se baseia fortemente na seção 3 do artigo [Kno06]. Em todo o Capítulo, k é algebricamente fechado de característica 0, e todos os morfismos são k-morfismos.

Sejam X e Y duas variedades algébricas, e seja $\phi : X \to Y$ um morfismo dominante. Isto implica que $O(Y) \subseteq O(X)$ (definição 3.21).

Definição 5.1. ([Kno06], (3.1)) $D(X,Y) = \{d \in D(X) | d(O(Y)) \subseteq D(Y)\}$. *Ou seja, temos os operadores diferenciais em X que se restringem para operadores diferenciais em Y.*

Suponha que a extensão de corpos $k(X)/k(Y)$ seja finita. Isso implica que ϕ é étale sobre os pontos genéricos (Teorema 3.14); logo, existe um aberto de X, X_0, tal que a restrição de ϕ para X_0 é étale (proposição 3.16). Sendo assim, todo operador diferencial em Y se levanta para um operador diferencial em X_0 de maneira única - isto é, $D(Y)$ é identificado com uma subálgebra de $D(X_0)$ ([Kno06], (2.5)).

Seja Z uma variedade algébrica afim e W um grupo finito de k-automorfismos de Z. Sabemos o que constitui o quociente Z/W neste caso, como vimos na Seção 3.4; em particular, $O(Z/W) = O(Z)^W$ e, portanto, $[k(Z) : k(Z/W)] = [k(Z) : k(Z)^W] = |W|$ (Lema de Artin), e estamos na situação acima com $X = Z$, $Y = Z/W$.

Temos o seguinte resultado:

Teorema 5.1. $D(Z, Z/W) = D(Z)^W$. ([Kno06], Teorema 3.1)

Demonstração. Claramente $D(Z)^W \subseteq D(Z, Z/W)$. Se $D \in D(Z, Z/W)$, seja $D' = 1/|W| \sum_{w \in W} wD$ - $D' \in D(Z)^W$. Se $f \in O(Z)^W$, então $(wD)(f) = w(D(w^{-1}f)) = w(Df) = Df$. Da mesma forma $D'f = Df$. Portanto, $D - D'$ é um operador diferencial que é zero em $O(Z)^W$, e como $O(Z)$ é um módulo finitamente gerado sobre $O(Z)^W$ (Teorema 3.1), isso implica que $D - D' = 0$ em $D(Z)$, ou seja, $D = D' \in D(Z)^W$. □

Vamos dar um exemplo do que foi discutido acima (exemplo na seção 3 de [Kno06]). Seja $X = Spec\, k[x]$ a linha afim, e seja W o grupo cíclico gerado por ϵ_n, onde ϵ_n é uma n-raiz primitiva da unidade, agindo em $k[x]$ multiplicando x. $Y = X/W = Spec\, k[x]^W = Spec\, k[t]$, onde $t = x^n$.

Usando a regra da cadeia, temos $\partial_x = nx^{n-1}\partial_t = nt^{1-1/n}\partial_t$. Seja $X_0 = Speck[x, x^{-1}]$ o subesquema aberto de X, obtido ao remover a origem (isto é, localizando $k[x]$ por x). A restrição da projeção $\pi : X \to Y$ para X_0 é étale. Temos $D(X) = A_1(k)$, $D(X, Y)$ é a subálgebra de $D(X)$ gerada por $x^n, x\partial_x, \partial_x^n$, que coincide com $A_1(k)^W$ (ver o exemplo Teorema 5.2 na próxima seção), concordando com o teorema acima. $D(X_0) = D(k[x]_x) = D(k[x])_x$ e, portanto, $D(X_0)$ é a k-álgebra gerada por x, x^{-1}, ∂_x (vista como subálgebra de $End_k(O(X_0))$). Vendo $k[t]$ como subanel de $k[x, x^{-1}]$, $D(Y)$ é a k-álgebra gerada por $x^n, x^{1-n}\partial_x$ e, portanto, um subanel de $D(X_0)$

A seguir, vem o conceito fundamental para o restante do trabalho.

Definição 5.2. ([Kno06], Definição na Seção 3) *Sejam X e Y variedades normais e $\phi : X \to Y$ um morfismo finito e sobrejetivo. Seja D um divisor primo de Y e considere $\phi^{-1}(D) = r_1E_1 + \ldots r_sE_s$, onde os E_i são distintos e os r_i são inteiros positivos. Dizemos que ϕ é* uniformemente ramificada *sobre D se $r_1 = \ldots = r_s$. Dizemos que ϕ é* uniformemente ramificada *se ela é uniformemente ramificada sobre todo divisor primo de Y. Se todos os r_i são r, dizemos que r é o grau de ramificação. Se todos os r_i são 1 para todo divisor primo, então se diz que ϕ é* não-ramificada em codimensão 1*. Isso é equivalente à existência de um subconjunto aberto $X_0 \subseteq X$ com $codim_X(X - X_0) \geq 2$, onde ϕ é étale.*

Teorema 5.2. ([Kno06], Proposição 3.2) *Seja $\phi : X \to Y$ um morfismo finito e sobrejetivo entre variedades normais afins que é não-ramificado em codimensão 1. Então $D(X, Y) = D(Y)$.*

Demonstração. Seja $D \in D(Y)$. Então D pode ser unicamente levantado para um operador D_0 num aberto X_0 onde ϕ é étale. Como $codim_X(X - X_0) \geq 2$ e X é normal, $O(X) = O(X_0)$. Portanto, D_0 se estende de maneira única a um operador em $D(X)$. Isso mostra que $D(X, Y) = D(Y)$. □

Proposição 5.1. ([Kno06], Seção 3) *Seja W um grupo finito de k-automorfismos agindo numa variedade normal X. Dado um divisor primo Z de X, seja W_Z o subgrupo de W que fixa todos os pontos de Z. Esse grupo é sempre cíclico, e sua ordem é o grau de ramificação de $X \to X/W$.*

5.2 Resultado Principal

Dado G um grupo finito de k-automorfismos de $A_n(k)$, existe um interesse natural em saber como será o anel $A_n(k)^G$. Uma solução possível para esse problema é encontrar geradores para essa subálgebra. Tal qual no caso de teoria clássica de invariantes, é imediata a pergunta: o número de geradores pode ser escolhido como sendo finito?

O seguinte teorema, obtido por S. Montgomery e L. W. Small [MS81], pode ser visto como uma generalização do teorema clássico de Noether (Teorema 3.1).

Teorema 5.3. *Seja A um anel noetheriano comutativo, R um anel não necessariamente comutativo, tal que A é um subanel central de R e R é uma A-álgebra finitamente gerada. Seja G um grupo finito de automorfismos de A-álgebra de R, tal que $|G|$ seja invertível em R. Então, se R é noetheriano à esquerda (ou à direita), R^G é uma A-álgebra finitamente gerada.*

Vamos provar esse teorema. Usaremos o conceito de anel de grupo torcido, Definição 4.4.

Lema 5.1. *Seja R um anel noetheriano à esquerda, G um subgrupo finito de $Aut\, R$, e $S = R\#G$. Suponha que $|G|$ seja invertível em R, e seja $e = 1/|G| \sum_{g \in G} g$. Então:*

1. $e^2 = e$
2. $eS = eR$
3. $eSe = eR^G \cong R^G$

Demonstração. O item 1 é direto. A inclusão $eR \subseteq eS$ é clara. Pela definição da multiplicação em S, $rg = gg(r)$, para todo $r \in R, g \in G$. Portanto, para todo $x = \sum_{g\in G} r_g g \in S$, nós temos $ex = \sum_{g\in G} er_g g = \sum_{g\in G} egg(r_g)$. Como $eg = e$, segue que $ex = \sum_{g\in G} eg(r_g) = e\sum_{g\in G} g(r_g) \in eR$. Isso nos dá $eS \subseteq eR$. Assim, temos o item 2. Segue-se dele que $eSe = eRe$. Para $r \in R$, calculamos:

$$\begin{aligned} ere &= e/|G|\sum_{g\in G} rg = e/|G|\sum_{g\in G} gg(r) = 1/|G|\sum_{g\in G} egg(r) \\ &= 1/|G|\sum_{g\in G} eg(r) = e/|G|\sum_{g\in G} g(r) = e/|G|\tau(r) = e\tau(r/|G|), \end{aligned}$$

onde $\tau : R \to R^G$ é definido por $\tau(r) = \sum_{g\in R} g(r)$, $r \in R$. Isso prova que $eSe = e\tau(R)$. A hipótese de que $|G|$ é invertível em R implica que todo $r \in R^G$ pode ser escrito da forma $r = \tau(1/|G|r)$, de tal forma que $R^G \subseteq \tau(R)$, e finalmente $R^G = \tau(R)$. Portanto, $eSe = eR^G$. Como $er = re$ para qualquer $r \in R^G$, o mapa $r \to er$ define um isomorfismo de anéis $R^G \to eR^G$. □

Com esse lema preliminar, podemos terminar a prova do teorema.

Demonstração. Vamos introduzir $S = R\#G$. S é noetheriano à esquerda. Da hipótese de que A é um subanel central de S é fácil ver que S é finitamente gerado como A-álgebra: se $\{q_1, \ldots, q_m\}$ geram R sobre A e $G = \{g_1, \ldots, g_d\}$, então a união desses dois conjuntos gera S sobre A. Considere, novamente, o elemento $e = 1/|G|\sum_{g\in G} g$ de S, que satisfaz $e^2 = e$. Em particular, eSe é um subanel de S, eS é um eSe-módulo à esquerda, e SeS é um ideal bilateral de S.

Vamos mostrar que eS é um eSe-módulo à esquerda finitamente gerado. Como S é noetheriano à esquerda, SeS é finitamente gerado como ideal à esquerda de S. Seja então $SeS = \sum_i Sx_i$, e escreva $x_i = \sum_j v_{ij}ew_{ij}$, com $v_{ij}, w_{ij} \in S$ para todos i, j. Seja $r \in S$ arbitrário. Então $er = eeer \in e(SeS)$ e, portanto,

$$er = e(\sum_i s_i x_i) = \sum es_i v_{ij} ew_{ij} = \sum es_i v_{ij} e^2 w_{ij}.$$

Assim, o conjunto finito $\{ew_{ij}\}$ gera eS como eSe-módulo à esquerda.

Feito isto, seja portanto $eS = \sum_{i=1}^n eSex_i$ como $x_i \in S$, e sejam $t_1, \ldots, t_m$ geradores de S como A-álgebra. Agora, escrevamos $et_j = \sum_{i=1}^n ey_{ij}ex_i$ e $ex_k t_j = \sum_{i=1}^n ez_{ijk}ex_i$ com $y_{ij}, z_{ijk} \in S$ para todos $1 \leq j \leq m$, $1 \leq k \leq n$. Considere o conjunto finito $E = \{ex_i e, ey_{ij}e, ez_{ijk}e\}$, com $1 \leq i, k \leq n$, $1 \leq j \leq m$. Calculamos:

$$\begin{aligned} et_1t_2e &= (\sum_{i=1}^n ey_{i1}ex_i)t_2e = \sum_{i=1}^n ey_{i1}e(ex_it_2)e \\ &= \sum_{i=1}^n ey_{i1}e(\sum_{l=1}^n ez_{l2i}ex_l)e = \sum_{i=1}^n ey_{i1}e(\sum_{l=1}^n ez_{l2i}eex_le), \end{aligned}$$

e assim provamos indutivamente que todo monômio $et_{j_1}\ldots t_{j_k}e$ com $1 \leq j_1, \ldots, , j_k \leq m$ pode ser expresso como uma soma finita de produtos de elementos de E. Todo elemento de eSe é uma combinação linear de tais monômios com coeficientes em A e, portanto, concluímos que eSe é finitamente gerado como A-álgebra por E. Pelo lema acima, isso mostra que R^G é finitamente gerado como A-álgebra. □

Isso resolve positivamente a questão da geração finita da subálgebra de invariantes no caso da Álgebra de Weyl. Note que aqui não é necessário supor k algebricamente fechado.

Como encontrar de maneira efetiva tais geradores?

Um resultado notável de Levasseur e Stafford permite resolver essa questão, a reduzindo para teoria clássica de invariantes.

Teorema 5.4. [LS95] *Seja G um grupo finito de automorfismos lineares de $A_n(k)$. $A_n(k)$ contém duas subálgebras isomórficas à álgebra de polinômios em n variáveis: $k[x_1, \ldots, x_n]$ e $k[y_1, \ldots, y_n]$ -*

a segunda é constituída pelos operadores diferenciais a coeficientes constantes. $A_n(k)^G$ *é gerada por* $k[x_1,\ldots,x_n]^G$ *e* $k[y_1,\ldots,y_n]^G$.

Outros resultados nesse sentido, de reduzir o cálculo de invariantes de $A_n(k)$ para invariantes de polinômios, existem. Temos, por exemplo, o artigo [CCK99], no qual computações explícitas para os geradores de $A_1(\mathbb{C})^G$ são exibidas para G um subgrupo finito de $SL_2(\mathbb{C})$.

Exemplo. *Usando o resultado do artigo acima, pode-se obter que* $A_1(k)^G$ *é gerada por* x^n, xy, y^n, *quando* G *é o grupo cíclico em* n *elementos (*k *é arbitrário de* $char\, k = 0$*).*

Outra pergunta no sentido de entender $A_n(k)^G$ é descobrir qual a sua estrutura precisa como anel - o que nem sempre é claro encontrando apenas os geradores, uma vez que as relações entre eles podem ser extremamente complicadas.

Um resultado importante nesse sentido foi obtido por Levasseur, e foi discutido no capítulo 4: Teorema 4.11.

Estamos interessados aqui em $D(X)^G$, onde X é uma variedade afim normal (se $X = Speck[x_1,\ldots,x_n]$ recuperamos o caso da Álgebra de Weyl), e G é um grupo finito de k-automorfismos com uma propriedade geométrica bastante forte: a ação é livre. Na verdade, como veremos, para os nossos interesses bastará que G tenha uma ação livre nos pontos fechados da variedade.

Neste caso, $X = Spec\, A$, onde A é uma k-álgebra finitamente gerada, e um domínio integralmente fechado. Neste caso $X/G = Spec\, A^G$, e a projeção $\pi : X \to X/G$ é induzida pela inclusão $A^G \to A$. Podemos reunir vários fatos. A^G também será um domínio integralmente fechado pela proposição 3.1, e finitamente gerado como álgebra pelo Teorema 3.1 e, portanto, X/G é uma variedade afim normal. Além disso, A é um módulo finitamente gerado sobre A^G (Teorema 3.1), e o morfismo $\pi : X \to X/G$ é finito e sobrejetivo, pela Observação na seção 3.1. Além disso, como a ação de G é livre, o estabilizador de qualquer subconjunto de X, e em particular de qualquer divisor primo, é o grupo trivial. Supondo que a ação de G seja livre apenas em $Specm\, A$, obtemos o mesmo resultado, pois todo divisor primo contém pontos fechados. Portanto, o morfismo é não-ramificado em codimensão 1, usando a proposição 5.1. Usando o Teorema 5.1 e o Teorema 5.2, obtemos que:

Teorema 5.5. *Seja* $X = Spec\, A$ *uma variedade afim normal, e* G *um grupo finito de k-automorfismos que age em* X *(ou então em* $Specm\, A$*) de maneira livre. Então* $D(X)^G = D(X/G)$ *- ou, de maneira equivalente,* $D(A)^G = D(A^G)$.

Este resultado já é interessante por si só. Aparentemente, ele já pertencia ao folclore da área, mas uma demonstração explícita é difícil de ser encontrada. Ele será a peça principal para o trabalho da próxima seção.

5.3 Resultado Novo

Seja W um grupo finito de pseudo-reflexões agindo num espaço vetorial V de dimensão finita n. Seja o polinômio J introduzido no Capítulo 3, seção 2. Considere o conjunto V' dado da seguinte forma: $\{v \in V | J(v) \neq 0\}$. Este é um aberto na topologia de Zariski em V, e é isomórfico a $Specm\, k[x_1,\ldots,x_n]_J = Specm\, k[x_1,\ldots,x_n]_{J^N}$, onde $N = |W|$, de forma que J^N é W-invariante. V' corresponde ao subconjunto de V obtido removendo os hiperplanos fixados pelas pseudo-reflexões. Todos esses fatos mencionados decorrem do Teorema 3.5.

Lema 5.2. *A ação de* W *se restringe numa ação em* V' *e tal ação é livre.*

Demonstração. Seja $w \in W, v \in V'$. Para mostra que temos uma ação em V', precisamos mostrar que $w.v \in V'$. Se esse não fosse o caso, então $w.v$ pertence a algum hiperplano fixo de uma pseudo-reflexão s diferente da identidade. Dessa forma, $(sw).v = w.v$ e, portanto, $(w^{-1}sw).v = v$. Logo, $w^{-1}sw \in isp(v)$, o grupo de isotropia de v (seção 2, capítulo 3). Sabemos que $isp(v)$ é gerado pelas pseudo-reflexões que cont Em, pelo Teorema de Steinberg (Teorema 3.6). Mas como v não pertence a nenhum dos hiperplanos fixos por uma pseudo-reflexão, tal grupo é trivial. Sendo assim,

$w^{-1}sw = id$, $s = id$, contrariando a hipótese. Dessa forma, temos uma ação de W em V', e tal ação é livre pois, como acabamos de ver, o grupo de isotropia de todo vetor em V' é trivial. □

Vamos usar a notação $\Lambda = k[x_1, \ldots, x_n]$, $\Delta = J^N$. (Λ_Δ) é um anel integralmente fechado, sendo a localização de um anel integralmente fechado (proposição 3.8). Logo, $X = Spec\,\Lambda_\Delta$ é uma variedade afim normal. Pelo Lema acima, W age em X, e a ação correspondente em Λ_Δ é a extensão natural da ação de W na álgebra de polinômios. Além disso, a ação é livre nos pontos fechados. Portanto, podemos aplicar o Teorema 5.5 da seção anterior e obter: $D(\Lambda_\Delta)^W = D(\Lambda_\Delta^W)$.

Agora, a demonstração segue exatamente os mesmos passos que a demonstração de que $D_n(k)^{S_n} \cong D_n(k)$ (Capítulo 4, Seção 4). De fato, vamos repetir o que fizemos lá. Temos os seguintes fatos:

1. Seja S um conjunto multiplicativo de Λ. $D(\Lambda_S) = D(\Lambda)_S$.
2. Seja G um grupo finito agindo em Λ e Ξ um elemento G-invariante. $(D(\Lambda)_\Xi)^G \cong (D(\Lambda)^G)_\Xi$.
3. Nas mesmas condições acima, $\Lambda_\Xi^G = (\Lambda^G)_\Xi$.
4. $D(\Lambda_\Delta)^W \cong D(\Lambda_\Delta^W)$, com $\Delta = J^N$.

O último item foi o que acabamos de demonstrar. Seguindo a mesma cadeia de isomorfismos que no caso do grupo simétrico, temos:

$((D(\Lambda))^W)_\Delta \cong ((D(\Lambda))_\Delta)^W \cong D(\Lambda_\Delta^W) \cong D(k[f_1, \ldots, f_n]_\Delta) \cong (D(k[f_1, \ldots, f_n]))_\Delta$.

Os f_i são os geradores algebricamente independentes de Λ^W. Finalmente, tomando o corpo de frações dos dois anéis nas extremidades, temos:

Teorema 5.6. *Seja W um grupo de pseudo-reflexões agindo num espaço vetorial V de dimensão n. Tomando a ação induzida de W em $D_n(k)$, temos que $D_n(k)^W \cong D_n(k)$.*

O argumento geométrico utilizado para provar que $D(\Lambda_\Delta)^W \cong D(\Lambda_\Delta^W)$ tem uma tradução precisa no contexto algébrico utilizado na seção 4.4 na discussão do caso do grupo simétrico. Seja, usando a mesma notação que lá, M a matriz $n \times n$ cuja entrada ij é $\partial_j f_i$, seja E_i a matriz $n \times 1$ com 0 em todas as entradas, menos a i-ésima, que contém 1, e seja

$$T_i = \begin{pmatrix} t_{i1} \\ \vdots \\ t_{in} \end{pmatrix}$$

a solução do sistema $MT_i = E_i$. Definindo, para $i = 1, \ldots, n$, $d_i = \sum_{k=1}^n t_{ik}\partial_k$, temos que $f_1, \ldots, f_n, d_1, \ldots, d_n$ geram $D_n(k)^W$ e o isomorfismo $D_n(k)^W \to D_n(k)$ é dado por: $f_i \to X_i$, $d_i \to Y_i$, onde X_i, Y_i denotam os geradores canônicos de $D_n(k)$. Em particular, quando os geradores $f_1, \ldots, f_n$ são conhecidos, os d_i podem ser calculados de maneira explícita.

5.4 Referências

A seção 1 se baseou em [Kno06], particularmente a seção 3. A demonstração do Teorema 5.3 seguiu [Dum06]. O Teorema 5.5 é um resultado bem conhecido no folclore da área. Contudo, desconhecemos algum lugar onde uma demonstração explícita e suficientemente detalhada deste fato esteja publicada. Por isso, tivemos o interesse em apresentar uma demonstração completa do Teorema 5.5.

Capítulo 6

Provas Alternativas

Nesta seção, apresentaremos demonstrações de que $D_n(k)^W \cong D_n(k)$ quando $W = B_n, D_n$, seguindo as ideias da seção 4.4. Depois, apresentaremos uma segunda prova para B_n de que $D_n(k)^{B_n} \cong D_n(k)$, usando o fato correspondente para S_n. Essas provas são inteiramente algébricas; não fazemos recurso de argumentos geométricos. O corpo base, portanto, não precisa ser algebricamente fechado.

Denote $\Lambda = k[x_1, \ldots, x_n]$. Quando k é de característica 0, os geradores algebricamente independentes de Λ^{B_n} podem ser escolhidos como $f_i = \sum_{j=1}^n x_j^{2i}, i = 1, \ldots, n$, e os de Λ^{D_n} como $h_i = \sum_{j=1}^n x_j^{2i}, i = 1, \ldots, n-1$, $h_n = x_1 \ldots x_n$ (ver, por exemplo, [Hum90], 3.12). Tal qual procedemos na seção 4.4, seja M a matriz $n \times n$ com entrada ij igual a $\partial_j f_i$, e N a matriz $n \times n$ a matriz com entrada ij igual a $\partial_j h_i$. Como na seção 2.4, pelo Teorema 3.5, temos que $\Delta = det(M)^2$ é B_n-invariante, e $\Gamma = det(N)^2$ é D_n invariante. O intuito é provar que $D(\Lambda_\Delta)^{B_n} \cong D(\Lambda_\Delta^{B_n})$ e $D(\Lambda_\Gamma)^{D_n} \cong D(\Lambda_\Gamma^{D_n})$, e então a prova de que $D_n(k)^W \cong D_n(k)$, $W = B_n, D_n$ seguirá os mesmos passos que para S_n. A injetividade dos mapas obtidos por restrição de domínio $D(\Lambda_\Gamma)^{D_n} \to D(\Lambda_\Gamma^{D_n})$ e $D(\Lambda_\Delta)^{B_n} \to D(\Lambda_\Delta^{B_n})$, segue dos Teorema 4.10 e lema 2.7, assim como no caso do grupo simétrico. Resta provar a sobrejetividade de tais mapas.

Teorema 6.1. *O homomorfismo $D(\Lambda_\Delta)^{B_n} \to D(\Lambda_\Delta^{B_n})$ obtido por restrição de domínio é sobrejetivo.*

Demonstração. Igual ao caso do grupo simétrico, seja E_i, $i = 1, \ldots, n$ a matriz $n \times 1$ com 0 em todas as posições, menos na i-ésima, que contém 1, e seja:

$$T_i = \begin{pmatrix} t_{i1} \\ \vdots \\ t_{in} \end{pmatrix}$$

a solução do sistema $MT_i = E_i$. Pela regra de Cramer, cada $t_{ij} \in \Lambda_\Delta$. Sejam $s_1, \ldots, s_n$ os elementos de B_n, tais que $s_i(x_j) = (-1)^{\delta_{ij}} x_j$. Eles também satisfazem $s_i(\partial_j) = (-1)^{\delta_{ij}} \partial_j$. Seja, para $i = 1, \ldots, n$, $d_i = \sum_{k=1}^n t_{ik} \partial_k$; $d_i(f_j) = \delta_{ij}$. B_n é gerador por $s_1, \ldots, s_n$ e S_n. Como no caso do grupo simétrico, basta provar que d_i é invariante por B_n, para todo i, para termos a sobrejetividade. A invariância por S_n repete o argumento da seção 4.4 - resta provar que d_i é invariante por $s_1, \ldots, s_n$. Para tanto, é suficiente mostrar que $s_l(t_{ij}) = (-1)^{\delta_{jl}} t_{ij}$, $1 \leq i, j, l \leq n$. Seja v_i o vetor

$$\begin{pmatrix} \partial_i f_1 \\ \vdots \\ \partial_i f_n \end{pmatrix}.$$

v_i contém apenas polinômios de grau ímpar em x_i e, portanto, $s_l(v_i) = (-1)^{\delta_{il}} v_i$. Pela regra de Cramer,

$$t_{ij} = \frac{det(v_1, \ldots, E_i, \ldots, v_n)}{det(v_1, \ldots, v_n)},$$

com E_i na posição j.

$$s_l(t_{ij}) = \frac{(-1)^{1-\delta_{jl}} det(v_1, \ldots, E_i, \ldots, v_n)}{(-1) det(v_1, \ldots, v_n)} = (-1)^{\delta_{jl}} t_{ij},$$

como queríamos.

□

Teorema 6.2. *O homomorfismo obtido por restrição de domínio $D(\Lambda_\Gamma)^{D_n} \to D(\Lambda_\Gamma^{D_n})$ é sobrejetivo.*

Demonstração. Usando a mesma notação da prova acima, consideramos as soluções do sistema $NT_i = E_i$, e definimos $d_i = \sum_{k=1}^n t_{ik}\partial_k$; $d_i(h_j) = \delta_{ij}$. D_n é gerado por S_n e s_i, $i = 1, \ldots, n-1$, onde $s_i(x_i) = -x_i$, $s_i(x_{i+1}) = -x_{i+1}$ e $s_i(x_j) = x_j$ para todos os outros valores de j. s_i atua da mesma maneira nos ∂_j. Precisamos mostrar que, para todo $i = 1, \ldots, n$, d_i é D_n invariante. Isso é claro para S_n; resta provar para os demais geradores. Para isso, basta provar que $s_l(f_{ij}) = -f_{ij}$ quando $j = l, l+1$, e igual a f_{ij} para todos os outros valores de j.

Fixe l. A n-ésima componente de v_l é um monômio, o produto de todas as variáveis, menos x_l. As demais componentes de v_l são monômios que envolvem apenas x_l, com grau ímpar. Logo, $s_l(v_l) = -v_l$. Um raciocínio análogo mostra que $s_l(v_{l+1}) = -v_{l+1}$. Se j não é nem l, nem $l+1$, então a n-ésima componente de v_j envolve um número par de variáveis cujo sinal é alterado; as demais componentes não envolvem nenhum. Dessa forma, $s_l(v_j) = v_j$.

Se $j = l$ então

$$s_l(f_{il}) = \frac{-det(v_1, \ldots, E_i, \ldots, v_n)}{det(v_1, \ldots, v_n)},$$

com E_i na j-ésima coluna. De fato, apenas uma coluna tem o sinal alterado no numerador (v_{l+1}), e duas no denominador (v_l, v_{l+1}). Dessa forma, $s_l(f_{il}) = -f_{il}$. De maneira análoga, $s_l(f_{il+1}) = -f_{il+1}$.

Se j não é l, nem $l+1$, então

$$s_l(f_{ij}) = \frac{det(v_1, \ldots, E_i, \ldots, v_n)}{det(v_1, \ldots, v_n)}.$$

De fato, duas colunas têm o sinal trocado tanto no numerador quanto no denominador (v_l, v_{l+1}). Portanto, $s_l(f_{ij}) = f_{ij}$. temos o que queríamos. □

A sobrejetividade desses mapas mostra, uma vez que já temos a injetividade, que são isomorfismos. Isto nos dá $D_n(k)^W \cong D_n(k)$, $W = B_n, D_n$, seguindo os mesmos passos que no caso do grupo simétrico.

Quando W é um dos grupos de Weyl F_4, E_6, E_7, E_8 (o caso G_2 já é coberto pelo Teorema 4.7) temos uma descrição explícita da ação de tais grupos no espaço vetorial, assim como temos uma descrição explícita dos geradores algebricamente independentes da subálgebra de invariantes - e eles têm coeficientes racionais. Em cada um dos casos, denotando por $\{f_i\}$ um conjunto de geradores de $S(V^*)^W$ (V é o espaço vetorial onde os grupos agem naturalmente), podemos introduzir a matriz M com entrada $ij = \partial_j f_i$, e de maneira análoga ao que foi feito acima, podemos considerar soluções do sistema $MT_i = E_i$, e definir $d_i = \sum t_{ik}\partial_k$. Dada a ação explícita desses grupos finitos no espaço vetorial, a questão da W-invariância dos d_i pode ser resolvida computacionalmente. Isto, como nos casos anteriores, nos daria a sobrejetividade do mapa $D(\Lambda_\Delta)^W \to D(\Lambda_\Delta^W)$. A injetividade já temos. Portanto, teríamos o isomorfismo $D(\Lambda_\Delta)^W \cong D(\Lambda_\Delta^W)$ e, como acima, isto nos daria o isomorfismo $D_n(k)^W \cong D_n(k)$. Sendo assim, a solução positiva do Problema de Noether Não-Comutativo para os grupos de Weyl excepcionais provavelmente é acessível via a implementação de um programa que chegue a invariância dos d_i usando a descrição explícita de tais grupos e suas ações. Desta forma, restaria apenas checar o caso $W = A_n$ para termos a solução positiva, para k um corpo arbitrário de característica 0, para o Problema de Noether Não-Comutativo para todos os grupos de Weyl.

Vamos agora apresentar uma segunda prova de que $D_n(k)^{B_n} \cong D_n(k)$, válida para qualquer k de característica 0.

Teorema 6.3. $D_n(k)^{B_n} \cong D_n(k)$.

Demonstração. Dado qualquer anel R e um grupo G de automorfismos de R, com um subgrupo normal H, temos: $R^G \cong (R^H)^{G/H}$. $\mathbb{Z}_2^n$ é normal em B_n, e $B_n/\mathbb{Z}_2^n \cong S_n$. Vamos calcular portanto $D_n(k)^{\mathbb{Z}_2^n}$. Isto é igual a $Frac\, A_n^{\mathbb{Z}_2^n}$. $A_n^{\mathbb{Z}_2^n}$ é gerado, como subálgebra de $A_n(k)$, por $x_i^2, \partial_i^2, x_i\partial_i$, como é fácil ver usando Teorema 5.4. No corpo de frações de $A_n^{\mathbb{Z}_2^n}$, precisamos apenas dos geradores $x_i^2, x_i\partial_i$, pois $x_i^2\partial_i^2 = x_ix_i\partial_i\partial_i = -x_i\partial_i + x_i\partial_ix_i\partial_i$; portanto, dividindo à esquerda por x_i^2, expressamos ∂_i^2 em função dos demais geradores. Chamando $w_i = x_i\partial_i/2$ e $q_i = x_i^2$, temos a relação de comutação $[w_i, q_i] = q_i$. Portanto, a descrição obtida para $Frac\, A_n^{\mathbb{Z}_2^n} = D_n(k)^{\mathbb{Z}_2^n}$ é exatamente a mesma que a primeira descrição da proposição 2.12. Sendo assim, $D_n(k)^{\mathbb{Z}_2^n} \cong D_n(k)$. A ação de $B_n/\mathbb{Z}_2^n \cong S_n$ em $D_n(k)^{\mathbb{Z}_2^n}$ é exatamente a permutação de variáveis, portanto, usando este último isomorfismo, temos que $D_n(k)^{B_n} \cong D_n(k)^{S_n} \cong D_n(k)$, o que encerra a prova. $\square$

Referências Bibliográficas

[AD97] J. Alev e F. Dumas. Invariants du corpos de Weyl sous l'action de grupes finis. *Communications in Algebra*, 25:1655–1672, 1997. 45, 56

[AD98] J. Alev e F. Dumas. Sur les invarians des algebres de weyl de leus corps de fractions. *Lecutre Notes in Pure and Applied Mathematics*, 197:1–10, 1998. 56

[AD06] J. Alev e F. Dumas. Opérateurs différentiels invariants et problème de Noether. Em J. Bernstein, V. Hinich e A. Melnikov, editors, *Studies in Lie Theory*, páginas 21–50. Birkhäuser, 2006. i, iii, 1, 5, 44, 46, 51, 56

[AM69] M. F. Atiyah e I. G. MacDonald. *Introduction to Commutative Algebra.* Addison-Wesley, 1969. 30, 34, 36, 40

[BGG72] J. N. Bernstein, I. M. Gelfand e S. I. Gelfand. Differential operators on the cubic cone. *Russian Mathematical Surveys*, 27:169–174, 1972. 13

[Bjo79] J. E. Bjork. *Rings of Differential Operators.* North-Holland, 1979. 22

[Bur14] W. Burnside. *Theory of Groups of Finite Order.* Cambridge University Press, 1914. 5, 7

[Car05] R. Carter. *Lie Algebras of Finite and Affine Type*, volume 96 of *Cambridge Studies in Advanced Mathematics.* Cambridge University Press, 2005. 28

[CCK99] L. Chiang, H. Chu e M. Kang. Generation of Invariants. *Journal of Algebra*, 221:232–241, 1999. 60

[Coh85] P. M. Cohn. *Free Rings and Their Relations.* Academic Press, second edição, 1985. 22

[Cou95] S. C. Coutinho. *A primer of algebraic D-modules.* London Mathematical Society Student Texts 33. Cambridge University Press, 1995. 22, 42, 56

[Dol03] I. Dolgachev. *Lectures on Invariant Theory.* London Mathematical Society Lecture Note Series 296. Cambridge University Press, 2003. 6, 23, 39, 40

[Duf73] M. Duflo. Certaines algebres de type fini sont de algebres de Jacbson. *Journal of Algebra*, 27:358–365, 1973. 41

[Dum06] F. Dumas. An introduction to noncommutative polynomial invariants, March 2006. Homological Methods and representations of non-commutative algebras, Mar del Plata, Argentina, http://math.univ-bpclermont.fr/~fdumas/fichiers/CIMPA.pdf. 9, 22, 56, 61

[Fis16] E. Fischer. Zur theorie der endlichen abelschen gruppe. *Mathematische Annalen*, 77:81–88, 1916. 7

[FMO10] V. Futorny, A. Molev e S. Ovsienko. The Gelfand-Kirillov conjecture and Gelfand-Tsetlin modules for finite W-algebras. *Advances in Mathematics*, 223:773–796, 2010. 51, 57

[FO06] V. Futorny e S. Ovsienko. Galois Algebras I: Structure Theory. *Trabalhos do Departamento de Matemática*, (13), 2006. 51, 56

[Fog69] J. Fogartry. *Invariant Theory.* Lecture Notes in Mathematics. W. A. Benjamin, 1969. 33

[For84] E. Formanek. Rational Function Fields. Noether's Problem and Related Questions. *Journal of Pure and Applied Algebra*, 31:28–36, 1984. 8, 9

[GJ04] K. R. Goodearl e R. B. Warfield Jr. *An introduction to noncommutative Noetherian Rings.* London Mathematical Society Students Texts 61. Cambridge University Press, segunda edição, 2004. 15, 16, 19, 20, 22, 55

[GK66] I. M. Gelfand e K. K. Kirillov. *Sur les corps liés aux algèbres envoloppantes des algèbres de Lie*, volume 31 of *Institut des Hautes Ãtudes Scientifiques. Publications MathÃ©matiques*, páginas 5–19. 1966. 12, 43, 44

[Har77] R. Hartshorne. *Algebraic Geometry.* Springer-Verlag, 1977. 4, 6, 31, 32, 33, 34, 35, 37, 38, 40

[Hum72] J. Humphreys. *Introduction to Lie Algebras and Representation Theory.* Springer, 1972. 25

[Hum90] J. E. Humphreys. *Reflection Groups and Coxeter Groups.* Cambridge Studies in Advanced Mathematics 29. Cambridge University Press, 1990. 7, 16, 25, 27, 40, 63

[Jac62] N. Jacobson. *Lie Algebras.* Wiley Interscience, 1962. 22, 42, 43

[Jac89] N. Jacobson. *Basic Algebra II.* W. H. Freeman, segunda edição, 1989. 7, 8, 27

[JLY02] C. U. Jensen, A. Ledet e N. Yui. *Generico Polynomials: Constructive Aspects of the Inverse Galois Problem*, volume 45 of *Mathematical Sciences Research Institute Publications.* Cambridge University Press, 2002. 8

[Jr.74] H. W. Lenstra Jr. Rational functions invariant under a finite abelian group. *Inventiones Mathematicae*, páginas 299–325, 1974. 9

[Kan01] R. Kane. *Reflection Groups and Invariant Theory.* CMS Books in Mathematics. Springer, 2001. 27, 29, 30, 40

[KL00] G. R. Krause e T. H. Lenegan. *Growth of Algebras and Gelfand-Kirillov Dimension.* Graduates Studies in Mathematics 22. American Mathematical Society, revisada edição, 2000. 12, 42, 43, 45, 56

[Kno06] F. Knop. Graded cofinite rings of differential operators. *Michigan Mathematical Journal*, 54, 2006. 57, 58, 61

[Lev80] T. Levasseur. Anneaus d'operateurs differentiels. Em *Séminaire d'Algebre Paul Dubreil et Marie-Pau le Malliavin*, Lecture Notes in Mathematics 867, páginas 157–173, Paris, 1980. Springer-Verlag. 54

[Liu02] Q. Liu. *Algebraic Geometry and Arithmetic Curves*, volume 6 of *Oxford Graduate Texts in Mathematics.* Oxford University Press, 2002. 4, 32, 33, 34, 35, 37, 38, 40

[LS95] T. Levasseur e J. Stafford. Invariant differential operators and an homomophism of Harish-Chandra. *Journal of the American Mathematical Society*, 8:365–372, 1995. 59

[LT09] G. I. Lehrer e D. E. Taylor. *Unitary Reflection Groups*, volume 20 of *Australian Mathematical Society Lecture Series.* Cambridge University Press, 2009. 26, 27, 40

[Mae89] T. Maeda. Noether's problem for A5. *Journal of Algebra*, 125:418–430, 1989. 8

[Mat89] H. Matsumara. *Commutative Ring Theory.* Cambridge Studies in Advanced Mathematics 8. Cambridge University Press, 1989. 30, 32, 33, 34, 40

[MFK94] D. Mumford, J. Fogarty e F. Kirwan. *Geometric Invariant Theory*. Springer-Verlag, 3 edição, 1994. 6

[Mil80] J. S. Milne. *Étale Cohomoly*, volume 33 of *Princeton Mathematical Series*. Princeton University Press, 1980. 35

[Miy71] T. Miyata. Invariants of certain groups I. *Nagoya Mathematical Journal*, 42:68–73, 1971. 5, 8

[Mon80] S. Montgomery. *Fixed Rings of Finite Automorphism Groups of Associative Rings*. Lecture Notes in Mathematics 818. Springer-Verlag, 1980. 45, 55

[MR01] J. C. McConnell e J. C. Robson. *Noncommutative noetherian rings*. Graduate Studies in Mathematics 30. American Mathematical Society, revisada edição, 2001. 13, 20, 32, 40, 44, 54

[MS81] S. Montgomery e L. W. Small. Fixed rings of noetherian rings. *The Bulletin of the London Mathematical Society*, 13:33–38, 1981. 58

[Mum99] D. Mumford. *The Red Book of Varieties and Schemes*. Lecture Notes in Mathematics 1358. Springer, 1999. 35

[Noe13] E. Noether. Rational Funktionenkörper. *Jahrericht Deutsch. Math.-Varein.*, 22:316–319, 1913. 5

[Pre10] A. Premet. Modular Lie Algebras and the Gelfand-Kirillov Conjecture. *Inventiones Mathematicae*, 181:395–420, 2010. 43

[PSV94] V. L. Popov, T. A. Springer e E. B. Vinberg. Algebraic Geometry IV. Springer-Verlag, 1994. 9

[Row80] L. H. Rowen. *Polynomial Identities in Ring Theory*. Academic Press, 1980. 41

[Sal84] D. Saltman. Noether's problem over an algebraically closed field. *Inventiones Mathematicae*, 77:71–84, 1984. 8, 9

[Sal85] D. Saltman. Groups acting on fields: Noether's problem. Em *Groups Actions on Rings*, Contemporary Mathematics 43, páginas 267–277. American Mathematical Society, 1985. 5, 9

[Ser56] J-P. Serre. Géométrie algébrique et géometrie analytique. *Annales de l'Institut Fourier*, 6:1–42, 1956. 34

[Smi85] S. P. Smith. Differential Operators in A1 and P1 in char p >0. Em *Séminaire d'Algèbre Paul Dubreil et Marie-Pau le Malliavin*, Lecture Notes in Mathematics 1220, páginas 157–177. Springer-Verlag, 1985. 21

[Spr77] T. A. Springer. *Invariant Theory*. Lecture Notes in Mathematics 585. Springer-Verlag, 1977. 7, 23, 26, 28, 51

[SS88] S. P. Smith e J. T. Stafford. Differential Operators on an affine curve. *Proceedings of the London Mathematical Society*, 56:229–259, 1988. 13

[ST54] G. C. Shephard e J. A. Todd. Finite unitary reflection groups. *Canadian Journal of Mathematics*, 6:274–304, 1954. 27

[Stu93] B. Sturmfels. *Algorithms in Invariant Theory*. Springer-Verlag, 1993. 24

[Voi08] C. Voisin. *Hodge Theory and Complex Algebraic Geometry I*, volume 76 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, 2008. 35

[Zha98] J. J. Zhang. On Lower Transcendene Degree. *Advances in Mathematics*, páginas 157–193, 1998. 45