Universidade Federal do Espírito Santo
Centro de Ciências Exatas
Programa de Pós-Graduação em Matemática

Dissertação de Mestrado em Matemática

Álgebra Diferencial e Equações Diferenciais Polinomiais

Flávio da Silva

Agosto/2015

Universidade Federal do Espírito Santo
Centro de Ciências Exatas
Programa de Pós-Graduação em Matemática

Álgebra Diferencial e Equações Diferenciais Polinomiais

Flávio da Silva

Dissertação apresentada ao Programa de Pós-Graduação em Matemática da Universidade Federal do Espírito Santo como requisito parcial à obtenção do grau de Mestre em Matemática.

Orientador: Valmecir A. dos S. Bayer

Agosto/2015

Agradecimentos

Ao término deste trabalho, cumpro meu dever em deixar aqui registrado meus sinceros agradecimentos a todos aqueles que foram de importância fundamental para que eu chegasse até aqui. Não podendo mencionar cada um deles, agradeço aos professores da graduação e do mestrado por toda a minha formação. Em particular, ao coordenador do mestrado, o professor Gilvan, a quem devo uma das cartas de recomendação ao programa de mestrado e os ensinamentos de cada encontro. A elegância e competência em que ministra suas aulas é um exemplo a ser seguido. Aos professores da banca, Magno e Leandro, pela gentileza de engrandecer este trabalho com uma leitura crítica do texto final. Com o apoio direto ou indireto de várias pessoas fui capaz de escrever esta redação, porém sou incapaz de juntar algumas palavras que expressem o quão grande é a minha gratidão por meu orientador, o professor Valmecir Bayer. Por causa de seus valiosos ensinamentos, grande parte da Matemática que sei deve a ele. Este trabalho não seria possível sem o seu apoio, crédito e confiança depositados em mim, da graduação até hoje. Obrigado professor e amigo Valmecir por tudo. Aos amigos Fidélis, Flavione, Geovane e João (e sua mãe Albina) que tanto me ajudaram antes mesmo de meu ingresso a universidade. Também, aos amigos Fernando, Maicon, Telau e Tiago pela presença em tantos bons momentos e pela imprescindível ajuda noutros difíceis. De igual modo sou grato aos amigos Aaron, Ramon (e familiares), sempre dispostos a uma boa prosa, nunca mediram esforços a me ajudar nos momentos em que precisei. A minha amiga Loyde, do bacharelado, obrigado por todas as vezes que compartilhou comigo as minhas dificuldades. Aprendi muito com você e, sem dúvida alguma, é uma daquelas raras pessoas que passam por nossas vidas. A minha família que sempre me concedeu apoio incondicional, a minha base de sustentação. Em especial, as minhas tias (mães) Ideni, Idilene e Irlene, e meu pai, Silvio, que me acompanham desde sempre. Se sou o que sou, devo a eles. A meu irmão Thadeu por todo carinho, respeito e amizade por todos esses anos. A minha querida amada esposa, Sabrina, por seu amor e incentivo, e por sua paciência e compreensão pelas horas em que estive ausente. Aos familiares de minha esposa, agradeço pelas orações e carinho que sempre tiveram comigo, em especial, ao seu pai Firmino e sua esposa Vera. Agradeço também à Capes pelo auxílio financeiro. A todos vocês, o meu muito obrigado, por todo carinho e atenção dispensada. Por fim, agradeço à Deus por motivos que dispensam comentários!

.

In Memoria

Minha mãe Maria Gusmão (avó).

Sumário

Resumo

O objetivo deste trabalho é estudar sistemas de equações diferenciais polinomiais paramétricas, cujo resultado principal é a determinação de uma expressão explícita para uma equação implícita.

Palavras-chave: Álgebra Diferencial, equações diferenciais polinomiais, implicitização, Bases de Gröbner.

Abstract

In this dissertation we study systems of parametric differential polynomial equations. The main result is the determination of an explicit expression for an implicit such equation.

Keywords: Differential algebra, polynomial differential equations, implicitization, Gröbner bases.

Introdução

Em 1930, o matemático americano *Joseph Fels Ritt* (1893-1951) criou a *Teoria das Equações Diferenciais Algébricas* modelados sobre a nova álgebra desenvolvida pela matemática alemã *Amalie Emmy Noether* (1882-1935) e seu pupilo, o matemático holandês *Bartel Leendert van der Waerden* (1903-1996), que inspirado por Emmy Noether publicou, em 1931, um tratado de dois volumes intitulado *Moderne Algebra*.

No início desta década de 30, quase ao mesmo tempo que *Gröbner*, Ritt começa a pensar sobre *Computação Simbólica* na *Teoria Algébrica da Eliminação*, desenvolvendo métodos construtivos na *Teoria da Eliminação de Equações Diferenciais Algébricas*. Ritt assim cria a *Teoria dos Conjuntos Característicos*, que juntamente com a *Teoria Algébrica da Eliminação*, leva de fato ao desenvolvimento de computadores digitais de alta velocidade, seguido de poderosos sistemas computacionais simbólicos, revivendo o seu interesse em *Álgebra Algorítmica*.

Em 1932, Ritt publicou no colóquio da Sociedade Americana de Matemática o livro *Differential Equations from the algebraic standpoint* com o propósito de dar, a teoria clássica das equações diferenciais não lineares, uma rigorosa fundamentação algébrica via polinômios diferenciais e variedades diferenciais algébricas (Emmy Noether e sua escola fizeram a mesma coisa para a *Teoria das Equações Algébricas* e *Variedades Algébricas*). No prefácio deste trabalho de 1932, Ritt escreve:

"*As contribuições de Mertens, Hilbert, Koenig, Lasker, Macaulay, Henzelt, Emmy Noether, vander Waerden...trouxeram para a Teoria Algébrica da Eliminação e a Teoria Geral Algébrica de Variedades um alto grau de perfeição*."

Posteriormente, esta nova teoria criada por Ritt passou a ser chamada de *Álgebra Diferencial*, nome sugerido pelo seu aluno, o americano *Ellis Robert Kolchin* (1916-1991), que sob a sua supervisão, obteve o doutorado em

matemática pela Universidade de Columbia, em 1941, com a dissertação *On the Exponents of Differential Ideals*.

Em sua monografia de 1950 intitulada *Differential Algebra*, Ritt dá uma nova exposição a *Teoria dos Conjuntos Característicos*, incluindo o que hoje é chamado de *Álgebra Computacional do Processo de Pseudo Redução*. Ele escreve:

"*...a Teoria das Equações Algébricas pode ser desenvolvida a partir do ponto de vista algorítmico, de modo que cada entidade cuja existência é estabelecida é construído com um número finito de operações*".

Neste, ele ecoa as palavras de Hensel no prefácio de *Palestras de Kronecker* na Teoria dos Números:

"*Kroenecker acreditava que se podia, e isso deve-se, nestas partes da Matemática, enquadrar cada definição de tal maneira que se pode testar num número finito de passos que se aplique a qualquer quantidade dada*"([25]).

Com as fundamentações de Ritt e, profundamente influenciado pelos matemáticos franceses *André Weil* (1906-1998) e *Claude Chevalley* (1909-1984) (membros fundadores do *Grupo Bourbaki*), Kolchin escreveu artigos fundamentais no que tange a *Teoria dos Corpos de Galois Diferenciais*, e publicou os livros *Differential Algebra and Algebraic Groups* (1973) e *Differential Algebraic Groups* (1985). A Teoria de Galois Diferencial foi iniciada no século XIX pelos matemáticos franceses *Charles Émile Picard* (1856-1941) e *Ernest Vessiot* (1865-1952). Os conceitos básicos da álgebra comutativa diferencial são baseados naqueles da álgebra comutativa comum. Um excelente estudo sobre este assunto pode ser encontrado em *Selected Works of Ellis Kolchin, with Commentary* ([3]). Muito da álgebra diferencial ([27], [31]) ou da geometria algébrica diferencial ([4], [35]) pode ser tida como a generalização da teoria da geometria algébrica de maneira análoga à teoria de equações diferenciais algébricas. Entretanto, partes consideráveis dos resultados de geometria algébrica ainda precisam ser extendidos aos casos diferenciais. Em particular, não há um análogo direto para o *Teorema da Base de Hilbert* no caso diferencial, no entanto, há um análogo "enfraquecido", a saber, o *Teorema de Ritt-Raudenbush* (para uma demonstração, veja por exemplo [19], capítulo III) A bem da verdade é que, para muitas propriedades em geometria algébrica, seus homólogos diferenciais são muito mais difíceis de provar e, alguns deles, ainda são problemas em aberto. Por exemplo, muitas das 16 questões propostas por Ritt em seu clássico livro de álgebra diferencial ([29], p.177) ainda não estão resolvidos.

A álgebra diferencial nos fornece poderosas ferramentas, por exemplo, os métodos de *Wu* (Wu Wen-Tsun: matemático chinês nascido em 1919) que permitem automatizar algumas provas de teoremas da geoemtria elementar, tal como o elegante *Teorema dos Nove Pontos no Círculo*, difícil de ser provado sinteticamente (veja [12]).

Recentemente, o trabalho de Kolchin em geometria algébrica diferencial e grupos algébricos diferenciais foi combinada com a chamada *Teoria da Deformação de Variedades Algébricas* para responder a perguntas em Geometria Diofantina, que por sua vez, tem por objetivo estudar conjuntos de pontos racionais de variedades algébricas. É bom ressaltar o artigo [4] que busca explorar a evolução da álgebra diferencial de equações diferenciais algébricas para os problemas de aritmética. Hoje em dia, a álgebra diferencial encontra importantes aplicações em campos como computação simbólica, robótica, sistemas dinâmicos e teoria do controle, para citar algumas, fornecendo algoritmos computacionais para trabalhar de forma simples com equações diferenciais algébricas.

Resumimndo, a álgebra diferencial ou a geometria algébrica diferencial, iniciadas por Ritt e Kolchin, tem como objetivo estudar equações diferenciais algébricas de uma forma semelhante em que equações polinomiais são estudadas, respectivamente, em álgebra comutativa ou geometria algébrica ([29], [19]).

O estudo de variedades algébricas uniracionais e as equações paramétricas racionais correspondentes é um objeto de estudo clássico na geometria algébrica. O recente estudo extensivo desse problema está focado em achar, de forma efetiva, algoritmos que possam transformar a representação implícita e a paramétrica de variedades uniracionais, devido ao fato desses algoritmos terem aplicações em modelagem sólida ([15], [27]). Variedades diferenciais com representações paramétricas são chamadas uniracionais. Claramente essa variedade diferencial uniracional é um dos tipos mais simples de variedades, e a representação paramétrica é a solução geral das equações diferenciais algébricas correspondentes.

O estudo das equações diferenciais racionais paramétricas teve início no artigo *Implicitization of differential rational parametric equations* do matemático chinês *Xiao-Shan Gao*, nascido em 1963, professor e diretor do Instituto de Ciência de Sistemas da Academia Chinesa de Ciências. Utilizando a teoria da álgebra diferencial desenvolvida por Ritt e Kolchin, em especial, com o uso dos denominados conjuntos característicos, X. S. Gao estabelece, entre outras coisas, a base para a generalização ao caso diferencial dos resultados

em geometria algébrica sobre as representações implícitas e paramétricas de variedades uniracionais. Em particular, os problemas relacionados a implicitização de equações diferenciais polinomiais paramétricas lineares são muito bem tratados por métodos de resultantes diferenciais ([31]).

Ao longo desta dissertação, um anel será suposto comutativo com unidade e característica zero, a menos que seja dito explicitamente o contrário.

Capítulo 1

Preliminares Algébrico Diferenciais

Neste capítulo será introduzido a linguagem necessária da álgebra diferencial usada em toda a dissertação. Como resultado principal, iremos determinar um algoritmo de divisão (processo de redução) para polinômios diferenciais.

1.1 Derivações em Anéis

Definição 1.1 *Uma derivação δ num anel A é um mapa linear (homomorfismo aditivo) $\delta : A \longrightarrow A$ que satisfaz a regra do produto de Leibniz, isto é,*

$$\delta(xy) = \delta(x)y + x\delta(y), \text{ para todos } x, y \in A.$$

A diferenciação é comumente indicada por $x' = \delta(x)$, para todo $x \in A$. Assim, por vezes, denotaremos $x'', x''', \ldots, x^{(n)}$ para indicar as derivadas sucessivas $\delta^2(x), \delta^3(x), \ldots, \delta^{(n)}(x) = \delta(\underbrace{\delta(\cdots(x)\cdots)}_{(n-1) \text{ vezes}})$, para todo $x \in A$.

É fácil provar por indução a seguinte regra de derivação

$$(x^n)' = nx^{n-1}x'$$

e a regra do produto de Leibniz para a n-ésima derivação:

$$(xy)^{(n)} = x^{(n)}y + \cdots + \left(\begin{array}{c} n \\ k \end{array} \right) x^{(n-k)}y^{(k)} + \cdots + xy^{(n)}.$$

Em particular, dados um anel A e δ uma derivação em A, tem-se as seguintes implicações imediatas da definição de δ:

i) $0'_A = 0_A$

ii) $1'_A = 0_A$

De fato, uma vez que δ é um homomorfismo aditivo, tomando $y = 0$ obtemos,

$$(x+y)' = x' + y', \text{ e portanto, } x' = x' + 0'_A. \text{ Segue que } 0'_A = 0_A.$$

Para a segunda propriedade, observe que da regra do produto aplicado a $x \neq 0$ e $y = 1$, temos que,

$$(xy)' = x'y + xy' \text{ e então } x' = x' + 1'_A. \text{ Daí segue que } 1'_A = 0_A.$$

Como consequência, vê-se que se $x, y \in A$, com y inversível em A, então para qualquer derivação δ em A temos a regra do quociente:

$$0 = \delta(1) = \delta(y \cdot y^{-1}) = \delta(y)y^{-1} + y\delta(y^{-1}) \text{ então } \delta(y^{-1}) = -\frac{\delta(y)}{y^2}.$$

Utilizando a notação de frações, segue que,

$$\delta\left(\frac{x}{y}\right) = \delta\left(x \cdot \frac{1}{y}\right) = \delta(x)\frac{1}{y} + x\delta\left(\frac{1}{y}\right) = \delta(x)\frac{1}{y} - x\frac{\delta(y)}{y^2} = \frac{y\delta(x) - x\delta(y)}{y^2}.$$

Exemplo 1.2

A única derivação em $\mathbb{Z}$ é a derivação nula. De fato, seja $\delta : \mathbb{Z} \longrightarrow \mathbb{Z}$ uma derivação. Da regra de Leibniz, tem-se que $\delta(1) = \delta(-1) = 0$. Por indução, segue que $\delta(z) = 0$ para todo $z \in \mathbb{Z}$. Mais geralmente, devido a regra do quociente, a única derivação em $\mathbb{Q}$ é também a derivação nula.

Exemplo 1.3

Seja $E \mid K$ uma extensão algébrica de característica zero. Suponha que $\delta : K \to K$ seja uma derivação. Então existe uma única derivação $\hat{\delta} : E \to E$ tal que $\hat{\delta}(x) = \delta(x)$ para todo $x \in K$. Com efeito, suponha que $\hat{\delta}$ seja uma tal derivação e tome $\alpha \in E$. Seja $p(X)$ o polinômio minimal de α sobre K, digamos,

$$p(X) = a_n X^n + \cdots + a_1 X + a_0,$$

com $a_i \in K$ para cada $i = 0, 1, \ldots, n$. Assim,

$$a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0.$$

Aplicando a derivação $\hat{\delta}$, tem-se que

$$a_n n\alpha^{n-1}\hat{\delta}(\alpha) + \hat{\delta}(a_n)\alpha^n + \cdots + a_1\hat{\delta}(\alpha) + \hat{\delta}(a_1)\alpha + \hat{\delta}(a_0) = 0.$$

Como $\hat{\delta}(x) = \delta(x)$ para $x \in K$, tem-se,

$$a_n n\alpha^{n-1}\hat{\delta}(\alpha) + \delta(a_n)\alpha^n + \cdots + a_1\hat{\delta}(\alpha) + \delta(a_1)\alpha + \delta(a_0) = 0.$$

Assim,

$$\hat{\delta}(\alpha)\left(na_n\alpha^{n-1} + \cdots + a_1\right) = -\left(\delta(a_n)\alpha^n + \cdots + \delta(a_1)\alpha + \delta(a_0)\right).$$

Pela definição do polinômio minimal de α tem-se que $na_n\alpha^{n-1} + \cdots + a_1 \neq 0$. Portanto,

$$\hat{\delta}(\alpha) = -\frac{\delta(a_n)\alpha^n + \cdots + \delta(a_1)\alpha + \delta(a_0)}{na_n\alpha^{n-1} + \cdots + a_1}.$$

Logo, a derivaçâo $\hat{\delta}$ fica definida e o resultado segue.

Segue dos dois exemplos acima que a única derivação num corpo de números algébricos (extensão algébrica de $\mathbb{Q}$) é a derivação nula.

Exemplo 1.4

Em extensões transcendentes de $\mathbb{Q}$ há derivações não nulas, por exemplo, a derivação usual do corpo de funções racionais $\mathbb{Q}(X)$. Segue que, se α é um número complexo transcendente sobre $\mathbb{Q}$ então há derivações não nulas em $\mathbb{Q}(\alpha)$, uma vez que, neste caso, $\mathbb{Q}(X)$ é isomorfo (como corpo) a $\mathbb{Q}(\alpha)$.

Definição 1.5 *Um anel A, munido de um conjunto finito $\Delta = \{\delta_1, \delta_2, \ldots, \delta_n\}$ de derivações, é um anel diferencial ou um Δ-anel se $\delta_j\delta_k = \delta_k\delta_j$, para todos $j, k \in \{1, \ldots, n\}$.*

Corpos diferenciais e álgebras diferenciais são corpos e álgebras equipadas com um número finito de derivações que comutam aos pares.

No caso em que $n = 1$, dizemos que A é um *anel diferencial ordinário*. No caso em que $n \geq 2$ dizemos que A é um *anel diferencial parcial*. É bom salientar que no caso $n = 0$, a noção de anel diferencial se reduz ao de anel.

Um elemento a de um Δ-anel é chamado *constante* se $\delta(a) = 0$ para todo $\delta \in \Delta$. Assim, no caso de $\mathbb{R}(X)$ e $\mathbb{C}(X)$ com as derivações usuais, o conjunto de constantes são respectivamente $\mathbb{R}$ e $\mathbb{C}$. Já no caso do corpo $\mathbb{Q}(\alpha)$ do exemplo 1.4, o conjunto de constantes é $\mathbb{Q}$. Neste caso α não é constante.

Seja $\Delta = \{\delta_1, \ldots, \delta_n\}$ o conjunto de derivações do anel diferencial A. Podemos considerar o anel de constantes $A^{\Delta} := \{c \in A \mid \delta_i c = 0, i = 1, \ldots, n\}$, que também é um Δ-anel. Em particular, tem-se que $1_A \in A^{\Delta}$ visto que $1'_A = 0_A$. O conjunto de constantes de um Δ-anel A é precisamente a intersecção dos núcleos das derivações δ_i para $i = 1, 2, , \ldots, n$.

Observe que um anel pode ter diversas estruturas de anel diferencial, dependendo do conjunto de derivações que se toma.

Exemplo 1.6

Seja $A = K[X_1, X_2, \ldots, X_n]$ o anel de polinômios em n indeterminadas sobre um corpo K. O conjunto das derivadas parciais

$$\Delta = \left\{ \frac{\partial}{\partial X_1}, \frac{\partial}{\partial X_2}, \ldots, \frac{\partial}{\partial X_n} \right\}$$

mune A de uma estrutura de anel diferencial parcial.

Exemplo 1.7

O anel das funções reais de uma variável real infinitamente diferenciáveis, com derivação usual, é um anel diferencial.

Considere A um Δ-anel, onde $\Delta = \{\delta_1, \delta_2, \ldots, \delta_n\}$. O conjunto

$$\Theta := \left\{ \delta_1^{i_1} \cdots \delta_n^{i_n} \mid \delta_j \in \Delta \text{ e } i_j \geq 0 \right\}$$

é chamado de conjunto de *operadores derivação* em A. Cada $\theta \in \Theta$ tem a forma $\theta = \delta_1^{i_1} \cdots \delta_n^{i_n}$, e define-se $ord(\theta) = i_1 + \cdots + i_n$. Observe que o conjunto Θ é um monóide livre comutativo, a saber, um conjunto munido de uma operação que possui um elemento neutro.

Neste texto, o foco é o caso de anéis diferenciais ordinários. Para um estudo dos anéis diferenciais parciais, sugerimos ([29]) e ([18]).

1.2 A Estrutura Diferencial num Anel

Para que se conheça por completo um anel diferencial, é necessário conhecer uma classe especial de subconjuntos deste anel, a saber, seus *ideais diferenciais*, que são definidos a seguir.

Definição 1.8 *Seja I um subconjunto de um Δ-anel A. Diz-se que I é um Δ-ideal de A se*

i) I for um ideal do anel A.

ii) $\delta(I) \subset A$ para cada $\delta \in \Delta$.

Em outras palavras, um ideal I de A é um Δ-ideal se for δ-invariante (ou δ-estável) para todo $\delta \in \Delta$, isto é, se $x \in I$ implicar que $\delta(x) \in I$ para todo $\delta \in \Delta$.

É imediato verificar que interseções, somas e produtos de ideais diferenciais são ainda ideais diferenciais. De fato, vamos provar por exemplo, que a intersecção de uma família qualquer de Δ-ideais é um Δ-ideal. Seja $(I_\lambda)_{\lambda\in\Lambda}$ uma família de Δ-ideais de A e $I = \bigcap_{\lambda\in\Lambda} I_\lambda$. Naturalmente I é um ideal de A. Para verificar a segunda condição, seja $\delta \in \Delta$ um derivação de A. Se $x \in I$, então $x \in I_\lambda$ para todo $\lambda \in \Lambda$. Assim $\delta(x) \in I_\lambda$ para todo $\lambda \in \Lambda$, uma vez que cada I_λ é um Δ-ideal. Logo $\delta(x) \in I$. Portanto I é um Δ-ideal de A.

Observe que dizer que I é δ-estável é o mesmo que dizer que é fechado em relação à derivação δ. A fim de que uma derivação δ preserve o ideal I, é necessário e suficiente que preserve os seus geradores.

Exemplo 1.9

Como ilustração, considere o anel $\mathbb{R}[X, Y, Z]$ e o ideal $I = \langle XY, YZ\rangle$, vamos encontrar uma derivação δ que torne I um ideal δ-estável. Uma vez que toda derivação em anéis de polinômios sobre um corpo são combinações lineares de suas derivadas parcias, podemos escrever

$$\delta := a\frac{\partial}{\partial X} + b\frac{\partial}{\partial Y} + c\frac{\partial}{\partial Z}.$$

Assim, a fim de que uma derivação δ preserve o ideal I, é necessário que $\delta(XY), \delta(YZ) \in I$, em outras palavras, é preciso que:

$$\begin{cases} \delta(XY) &= X\delta(Y) + Y\delta(X) = bX + aY \in I \\ \delta(YZ) &= Y\delta(Z) + Z\delta(Y) = cY + bZ \in I \end{cases}$$

De acordo com isso, para que I seja δ-estável, é necessário que $a, c \in \langle X, Z\rangle$ e $b \in \langle Y\rangle$. Reciprocamente, tem-se que a família

$$\Delta := \langle X, Z\rangle \frac{\partial}{\partial X} + \langle Y\rangle \frac{\partial}{\partial Y} + \langle X, Z\rangle \frac{\partial}{\partial Z}$$

de derivações δ preserva o ideal I. Portanto, Δ é um conjunto de derivações que faz de I um ideal δ-estável.

Exemplo 1.10

Sejam δ uma derivação de um corpo diferencial F e $p(X)$ um polinômio irredutível no anel $F[X]$. Pode-se estender a derivação δ de F para $F[X]$ de tal forma que o ideal $\langle p\rangle$, gerado por p, seja um ideal diferencial. Com efeito, escreva $p = p(X) = p_nX^n + \cdots + p_0$, onde n é o grau de p. Defina $\delta(X) := -hp^\delta$, onde $p^\delta := \delta(p_n)X^n + \cdots + \delta(p_0)$ e $hp' \equiv 1\ (mod\ p)$, sendo $p' = np_nX^{n-1} + \cdots + p_1$ a derivada usual do anel de polinômios $F[X]$. Com estas considerações, escrevendo $hp' = 1 - kp$ e aplicando as propriedades operatórias de δ, segue que:

$$\begin{aligned} \delta(p) &= \underbrace{\delta(p_n)X^n + \cdots + \delta(p_0)}_{=p^\delta} + p_n\delta(X^n) + \cdots + p_1\delta(X) \\ &= p^\delta + np_nX^{n-1}\delta(X) + \cdots + p_1\delta(X) \\ &= p^\delta + \left(\underbrace{np_nX^{n-1} + \cdots + p_1}_{=p'}\right)\underbrace{\delta(X)}_{=-hp^\delta} = p^\delta + p'\left(-hp^\delta\right) \\ &= p^\delta\left(1 - \underbrace{hp'}_{=1-kp}\right) = p^\delta(1 - (1 - kp)) = p^\delta kp \end{aligned}$$

Assim, $\delta(p) \in \langle p\rangle$. Portanto $\langle p\rangle$ é um ideal diferencial.

Os conceitos de *ideais diferenciais primos* e *ideais diferenciais radicais* são uma extensão natural dos conceitos análogos em álgebra não diferencial.

Seja S um subconjunto de um Δ-anel A. A interseção de todos os ideais diferenciais que contém S será chamado o *ideal diferencial gerado por* S, e o denotamos por $[S]$. Em especial, dizemos que um subconjunto S de um anel diferencial A é *trivial* se o ideal diferencial $[S]$ é igual a A.

É fácil verificar que dado um Δ-anel A e um Δ-ideal I de A, o anel quociente A/I também tem uma estrutura de Δ-anel.

Definição 1.11 *Um homomorfismo de anéis diferenciais de A em B, ou um Δ-homomorfismo, é um homomorfismo $\varphi : A \longrightarrow B$ tal que,*

$$\delta\left(\varphi(x)\right) = \varphi\left(\delta(x)\right), \text{ para todo } \delta \in \Delta \text{ e para todo } x \in A.$$

Aqui, dizemos também que B é uma Δ-A-álgebra.

Esta definição carrega consigo, é claro, as correspondentes (no contexto diferencial) definições de Δ-isomorfismo, Δ-automorfismo, etc.

1.3 Polinômios Diferenciais

Na sequência do texto, vamos considerar apenas anéis diferenciais ordinários, salvo menção ao contrário, e vamos denotar a derivação por δ. Na construção de polinômios diferenciais (originalmente chamado de *formas* por Ritt), usaremos os símbolos $y, y', y'', \ldots, y^{(p)}$ (num número finito deles) e chamaremos y e $y^{(p)}$, respectivamente, de *indeterminada diferencial* e *p-ésima derivada de y*. Além disso, para os naturais p e q, com $q > 0$, denotaremos por $y^{(p+q)}$ a *q-ésima derivada de $y^{(p)}$* (precisamente, o que estamos fazendo é $y^{(p+q)} := \left(y^{(p)}\right)^{(q)}$). Ressaltamos que apenas y é uma indeterminada, sendo $y^{(p)}$ a p-ésima derivada da indeterminada y, para todo p natural.

Nossos problemas vão lidar com um número finito de indeterminadas diferenciais $y_1, \ldots, y_n$. Doravante, vamos também denotar por y_{ij} a j-ésima derivada de y_i, para todo $i = 1, \ldots, n$, com j natural. Vamos chamar y_i de sua própia derivada de ordem 0, e escrevemos $y_i := y_{i0}$. Por vezes, usaremos $u, v, \ldots, w$ como indeterminadas diferenciais. Neste caso, as derivadas serão subescritas e não sobrescritas. Por exemplo, a j-ésima derivada de u é u_j. Feitas essas considerações, fixe um corpo diferencial ordinário K de característica 0.

Definição 1.12 *Guardando as notações acima, por um polinômio diferencial ordinário nas indeterminadas diferenciais $y_1, \ldots, y_n$ sobre K, entenderemos um polinômio em y_{ij} com coeficientes no corpo K, e o chamaremos de polinômio diferencial ordinário ou, por simplicidade, um polinômio diferencial.*

O conjunto de todos os polinômios diferenciais sobre K será denotado por $K\{y_1, \ldots, y_n\}$. Mais especificamente, dado o conjunto de indeterminadas diferenciais $Y = \{y_1, \ldots, y_n\}$ e denotando por

$$\{Y\} = \left\{\delta^k y \mid y \in Y,\ k \in \mathbb{N}\right\} = \{y_{ij} \mid i = 1, \ldots, n,\ j \in \mathbb{N}\} = \{y_{ij}\}_{1 \leq i \leq n,\ j \in \mathbb{N}}$$

o conjunto das derivadas de elementos de Y, o conjunto $K\{y_1, \ldots, y_n\}$ se torna um anel diferencial ordinário estendendo a derivação δ em K para todos naturais i e j, como segue:

$$\delta(y_{ij}) = y_{i(j+1)}.$$

O anel $K\{y_1, \ldots, y_n\}$ é chamado *anel de polinômios diferenciais ordinários* e podemos representá-lo por:

$$K\{Y\} = K[\{y_{ij}\}] = K[y_{ij} \mid i = 1, \ldots, n,\ j \in \mathbb{N}]$$

Um *derivativo* é um elemnto de $K\{Y\}$ escrito na forma $\delta(y_i)$ para algum $i \in \{1, 2, \ldots, n\}$.

Como no caso de anéis de polinômios comum, um polinômio diferencial é uma combinação linear finita de monômios diferenciais ordinários, que por sua vez, são monômios nas derivadas com coeficientes em K. Cada monômio diferencial M é um produto (formal)

$$M = \prod_{1 \leq i \leq n,\ j \in \mathbb{N}} y_{ij}^{e_{ij}},\ \text{onde } e_{ij} \in \mathbb{N}$$

onde apenas um número finito desses fatores comparecem no produto. Além disso, se M envolve l derivativos, digamos

$$v_1 = y_{i_1 j_1}, \quad v_2 = y_{i_2 j_2}, \quad \ldots, \quad v_l = y_{i_l j_l},$$

onde os pares (i_k, j_k) são distintos, então podemos escrever

$$M = v_1^{e_1} \cdots v_l^{e_l} = y_{i_1 j_1}^{e_1} \cdots y_{i_l j_l}^{e_l} = \left(\delta^{j_1} y_{i_1}\right)^{e_1} \cdots \left(\delta^{j_l} y_{i_l}\right)^{e_l}.$$

Esta notação carregada sugere a conveniência de suprimir a grande quantidade de detalhes e podemos escrever um polinômio diferencial P simplesmente sob a forma

$$P = u_1 M_1 + \cdots + u_t M_t, \text{ com } u_1, \ldots, u_t \in K,$$

onde cada M_s é um monômio diferencial.

Dois polinômios diferenciais são idênticos se os coeficientes em y_{ij} são iguais. Dado um polinômio diferencial P, por derivada de P entenderemos o polinômio diferencial P' obtido de P via utilização das operações de derivação.

Exemplo 1.13

Seja $K = \mathbb{Q}(x)$ o corpo das funções racionais na indeterminada x e considere $F = K\{y\}$, onde y é uma indeterminada diferencial. Para o polinômio diferencial dado por

$$P = xy_1^2 + x^2 y_{21},$$

obtemos:

$$\begin{aligned} P' &= (xy_1^2 + x^2 y_{21})' = (xy_1^2)' + (x^2 y_{21})' \\ &= \left(x' y_1^2 + x\,(y_1^2)'\right) + \left((x^2)'\, y_{21} + x^2\,(y_{21})'\right) \\ &= (y_1^2 + 2xy_1 y_{11}) + (2xy_{21} + x^2 y_{22}) \end{aligned}$$

Exemplo 1.14

Seja $K = \mathbb{Q}(x)$ o corpo das funções racionais na indeterminada x e considere $F = K\{y\}$, onde y é uma indeterminada diferencial. Podemos associar à equação diferencial ordinária

$$\frac{d^2y}{dx^2} + xy\frac{dy}{dx} + x^2 = 0$$

o polinômio diferencial $p = y_2 + xy_0 y_1 + x^2$, com coeficientes em K.

1.4 Ordenação de Polinômios Diferenciais

Daqui por diante, vamos às vezes nos referir sobre um determinado polinômio diferencial P como sendo o que envolve um certo y_i efetivamente, ou seja, no sentido que ao menos um y_{ij} aparece como um termo (com coeficiente $\neq 0$) na expressão de P, para algum $j \in \mathbb{Z}_{>0}$.

Mais adiante, vamos aplicar um algoritmo de divisão para polinômios diferenciais. Para isso, vamos precisar de um modo de ordená-los, a saber, a noção de *posicionamento de derivadas*. De antemão, deixamos registrado que existe um posicionamento específico e cada classificação é uma boa ordenação do conjunto das derivadas θy_i (isto resulta do Lema 15, pg 49 em [19]). Comecemos com as noções de *classe* e *ordem* de um polinômio diferencial.

Se um polinômio diferencial P não for um elemento do corpo K, por *classe* de P entenderemos como o maior $i \in \mathbb{Z}_{>0}$ tal que, algum y_{ij} aparece efetivamente em P, e a denotamos por $clas(P)$. Caso $P \in K$, escrevemos $clas(P) = 0$. Para cada natural i em que o P envolve y_i efetivamente, entenderemos por sua *ordem* com respeito a y_i como o maior $j \in \mathbb{Z}_{>0}$ tal que, y_{ij} aparece efetivamente em P, e a denotamos $ord(P, y_i)$. Em particular, se $clas(P) = p > 0$, dizemos que $ord(P, y_p)$ é a ordem de P, e escrevemos $ord(P)$. Além disso, se P não envolve y_i efetivamente, denotamos $ord(P, y_i) = -\infty$. Podemos também dizer que a ordem de um polinômio diferencial $P \in K\{y_1, \ldots, y_n\}$, onde $P \notin K$, é o menor inteiro j tal que, $P \in K\left[y_1, \ldots, y_n, \ldots, y_1^{(j)}, \ldots, y_n^{(j)}\right]$. Explicitamente, se $P \in K\{Y\} \setminus K$ tem ordem j, podemos escrever

$$P(y) = \sum_{i=0}^{m} P_i(y, y', y'', \ldots, y^{(j-1)})(y^{(j)})^i,$$

onde $P_i \in K\left[y, y', y'', \ldots, y^{(j-1)}\right]$. Se $P_m \neq 0$, dizemos que P tem *grau* m, e o denotamos $gr(P) = m$. Mais geralmente, designamos por $gr(P, y_i)$ o grau de P em relação a y_i. Agora, sejam P_1 e P_2 dois polinômios diferenciais tais que, y_p aparece efetivamente em ambos. Se P_1 e P_2 são de mesma classe $p > 0$ e de mesma ordem em y_p, dizemos que P_1 e P_2 tem a mesma posição em y_p. Segue que todos os polinômios diferenciais de classe 0 são de mesma posição. Dizemos que P_2 possui uma posição maior do que P_1 em y_p e que P_1 possui uma posição menor do que P_2 em y_p, e denotamos respectivamente $posto_{y_p}(P_2) > posto_{y_p}(P_1)$ e $posto_{y_p}(P_1) < posto_{y_p}(P_2)$, caso uma das condições seguintes for satisfeita:

i) $0 \leq clas(P_1) < clas(P_2) = p$.

ii) $clas(P_1) = clas(P_2) = p > 0$, mas $ord(P_1, y_p) < ord(P_2, y_p)$.

iii) $clas(P_1) = clas(P_2) = p > 0$ e $ord(P_1, y_p) = ord(P_2, y_p)$, mas $gr(P_1) < gr(P_2)$.

Neste caso, dizemos que P_1 e P_2 são *comparáveis*, caso contrário são ditos *incomparáveis*, isto é, quando nem $posto_{y_p}(P_1) > posto_{y_p}(P_2)$ nem $posto_{y_p}(P_2) > posto_{y_p}(P_1)$. Quando P_1 e P_2 são incomparáveis, é usual chamá-los de *polinômios diferenciais equivalentes* e denota-se $P_1 \equiv P_2$ ou $P_1 \sim_{\prec} P_2$ ($\prec$ indica ordenação considerada).

Exemplo 1.15 *:*

Seja $K = \mathbb{Q}(x)$ o corpo das funções racionais na indeterminada x e considere $F = K\{y\}$, onde y é uma indeterminada diferencial.

(a) Suponha que $P_1 = xy_1^2 + x^2y_{24}^2$, com $p = 2$ e $P_2 = xy_{13}^2 + x^2y_{23}^2 + y_3$, com $p = 3$. Então,

$$posto_{y_3}(P_2) > posto_{y_3}(P_1)$$

(b) Se $P_1 = y_{3,6}^7 + y_{2,6} + 1$ e $P_2 = y_{4,0\leq j<6}^6 + y_{3,0\leq j<6}^2 + 5$ então,

$$posto_{y_4}(P_2) > posto_{y_4}(P_1).$$

(c) Sejam $P_1 = xy_{13}^2 + x^2y_{21}$, com $p = 2$ e $P_2 = xy_1^2 + x^2y_{22}$, com $p = 2$. Então,

$$posto_{y_2}(P_2) > posto_{y_2}(P_1)$$

(d) Sejam $P_1 = xy_{13}^2 + x^2y_{24}^2$, com $p = 2$ e $P_2 = xy_1^2 + x^2y_{24}^3$, com $p = 2$. Então,

$$posto_{y_2}(P_2) > posto_{y_2}(P_1).$$

(e) Se desejarmos, podemos "refinar" o posicionamento ainda mais como segue:

(f) Se $clas(P_1) = clas(P_2) = p > 0$ e $clas_{p-m}(P_1) < clas_{p-m}(P_2)$, para algum inteiro $m > 0$, então,

$$posto_{p-m}(P_2) > posto_{p-m}(P_1).$$

(g) Se $P_1 = xy_1^2 + x^2y_{24}^2 + y_4$ e $P_2 = x + y_1 + xy_2^2 + y_3 + y_4$ então,

$$posto_{y_3}(P_2) > posto_{y_3}(P_1).$$

Definição 1.16 *Seja K um corpo diferencial ordinário com derivação δ. Uma ordem no conjunto $Y = \{y_1, \ldots, y_n\}$ das indeterminadas diferenciais sobre K induz uma ordenação total no conjunto das derivadas de $\{Y\}$, tal que:*

(I) $v < \delta(v)$, *para todos* $v \in \{Y\}$.

(II) Se $u < v$ *então* $\delta^r(u) < \delta^s(v)$ *para todos* $u, v \in \{Y\}$ *e para todos* $r, s \in \mathbb{N}$.

As condições de posição dadas em (i), (ii) e (iii) são induzidas pela *ordem lexicográfica* nos pares $(i := classe, j := ordem)$, de modo que:

$$\left.\begin{array}{c} \text{Se} \quad i < l \\ \text{ou} \\ i = l \text{ e } j < k \end{array}\right\} \text{ então } y_{ij} < y_{lk} \tag{1.1}$$

Chamamos a condição (1.1) de *posicionamento puro.*

Temos a seguinte ordenação de posições para $n = 2$:

$$y_1 < y_1' < y_1'' < \cdots < y_2 < y_2' < y_2'' < \cdots$$

1.5 O Processo de Redução

1.5.1 Caso Não Diferencial

Como sabemos, o algoritmo da divisão em $K[X]$ generaliza o algoritmo de divisão dos números inteiros para o caso da divisão de polinômios, conforme descrito a seguir em pseudocódigo, para únicos $q, r \in K[X]$ e $f, g \in K[X]$ dados arbitrariamente. Em outras palavras, queremos dividir f por g e obter o quociente q e resto r. No algoritmo, vamos usar tl para abreviar termo líder.

Algoritmo: Sejam g, $f \in K[X]$, com $g \neq 0$
Entrada: g, f
Saída: q, r
$q := 0$, $r := f$
Enquanto $r \neq 0$ e $tl(g)$ divide $tl(r)$ faça

$$q := q + \frac{tl(r)}{tl(g)} \quad r := r - \frac{tl(r)}{tl(g)} g$$

Note que no início de cada passo, verificamos se $r \neq 0$ e comparamos os termos líderes. Caso tivermos ainda que $r \neq 0$ e $tl(g)$ divide $tl(r)$, então

prosseguimos através da divisão novamente. Repomos os valores de r e q, voltando ao início. Em geral, se temos dois polinômos

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

e

$$g(X) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0$$

em $K[X]$, com graus, digamos, $n = gr(f) \geq gr(g) = m$, então o primeiro passo para a divisão de f por g é subtratir de f o produto $\frac{a_n}{b_m} x^{n-m} g$. Notamos que o fator de g deste produto é $\frac{tl(f)}{tl(g)}$, e temos assim $h = f - \frac{tl(f)}{tl(g)} g$ como o primeiro resto. Chamamos h de uma *redução* de f por g e denotamos o processo de computação de h por $f \xrightarrow{g} h$. Todo o processo de redução, em que figura todas as suas etapas, denota-se por $f \xrightarrow{g}_+ r$.

Como consequência, da relação $f = qg + r$, o *Teorema do Resto* nos diz que um zero de g será um zero de f se, e somente se, é um zero de r.

Comecemos por analisar o caso em que K não é um corpo, mas apenas um domínio, digamos $K = \mathbb{Z}$.

Exemplo 1.17

Suponha que desejamos dividir $f = 6X^4 + 4X^2 + 3X$ por $g = 4X^2 + 1$. Como sabemos, precisamos inicialmente multiplicar o dividendo por 4 antes de se dividir, e daí, aplicando duas vezes o passo de redução temos:

1) Pré multiplicação:

$$4f = 24X^4 + 16X^2 + 12X$$

2) Passo de redução:

$$4f = 6X^2 g + \left(10X^2 + 12X\right)$$

3) falso resto:

$$h = 10X^2 + 12X$$

4) Pré multiplicação:

$$4h = 40X^2 + 48X$$

5) Passo de redução:

$$4h = 10g + (48X - 10)$$

6) falso resto:

$$r = 48X - 10$$

Todo o processo de redução é denominado *falsa divisão* e o coeficiente do termo líder do divisor g (4 no exemplo) é chamado o *inicial* de g. Designando por s o inicial do divisor g, tem-se

$$s^e f = qg + r, \tag{1.2}$$

onde e é um número natural chamado um *falso expoente*, q é um *falso quociente* e r é um *falso resto*. Salientamos que, para cada falso expoente fixado, são únicos o falso quociente e o falso resto. Observamos também que podemos sempre escolher $e := max\{gr(f) - gr(g) + 1\}$, não necessitando ser minimal (por exemplo, quando $f = g$). E mais, caso $r = 0$, não sabemos a priori se $f \in \langle g \rangle$, mas sim, que $s^e f \in \langle g \rangle$, para algum natural e.

Vamos supor agora que K seja um corpo, digamos $K = \mathbb{Q}$, e seja $K[X, Y]$.

Exemplo 1.18

Vamos fazer uso da ordem lexicográfica, abreviadamente, *ordem lex*, (para a definição veja, por exemplo, a referência [21]). Tomando $X > Y$, suponha que seja requerido dividir $f = 5X^3Y^2 - 10XY^3$ por $g = 2X^2Y + X^2 + XY^3$. Na falsa divisão que segue, em cada passo de redução, destacam-se em negrito os maiores termos que podem ser reduzidos, a qual chamaremos cada um de *termo líder secundário*. Este nome que estamos dando a tal termo é bem sugestivo, uma vez que o mesmo não precisa ser o termo líder do polinômio em questão, visto que isto depende do divisor g.

Passo 1:

$$f = \left(\tfrac{5}{2}XY\right) g + h_1, \text{ onde } h_1 = -\tfrac{5}{2}\mathbf{X^3Y} - \tfrac{5}{2}X^2Y^4 - 10XY^3$$

Passo 2:

$$h_1 = \left(-\tfrac{5}{4}X\right) g + h_2, \text{ onde } h_2 = \tfrac{5}{4}X^3 - \tfrac{5}{2}\mathbf{X^2Y^4} + \tfrac{5}{4}X^2Y^3 - 10XY^3$$

Passo 3:

$$h_2 = \left(-\tfrac{5}{4}Y^3\right) g + h_3, \text{ onde } h_3 = \tfrac{5}{4}X^3 + \tfrac{5}{2}\mathbf{X^2Y^3} + \tfrac{5}{4}XY^6 - 10XY^3$$

Passo 4:

$$h_3 = \left(\tfrac{5}{4}Y^2\right) g + h_4, \text{ onde } h_4 = \tfrac{5}{4}X^3 - \tfrac{5}{4}\mathbf{X^2Y^2} + \tfrac{5}{4}XY^6 - \tfrac{5}{4}XY^5 - 10XY^3$$

Passo 5:

$$h_4 = \left(-\tfrac{5}{8}Y\right) g + h_5, \text{ onde } h_5 = \tfrac{5}{4}X^3 + \tfrac{5}{8}\mathbf{X^2Y} + \tfrac{5}{4}XY^6 - \tfrac{5}{4}XY^5 + \tfrac{5}{8}XY^4 - 10XY^3$$

Passo 6:

$$h_5 = \left(-\tfrac{5}{16}\right) g + r, \text{ onde } r = \tfrac{5}{4}X^3 - \tfrac{5}{16}X^2 + \tfrac{5}{4}XY^6 - \tfrac{5}{4}XY^5 + \tfrac{5}{8}XY^4 - \tfrac{165}{16}XY^3$$

Note que $r := h_6$ não é constituído de monômio algum que seja divisível pelo monômio líder de g. Além disso, visto que a seqüência de termos líderes secundários dos restos $h_1, \ldots, h_6$ é estritamente decrescente, segue que o processo se encerra.

Exemplo 1.19

Ainda no exemplo exemplo anterior, novamente supondo por um momento que $K = \mathbb{Z}$, recorremos à falsa divisão (aqui, e em cada etapa, o falso resto será pré multiplicado pelo inicial 2 sempre que necessário) e obtemos:

Passo 1:

$$2f = (5XY)\, g + h_1, \text{ onde } h_1 = -5\mathbf{X^3Y} - 5X^2Y^4 - 20XY^3$$

Passo 2:

$$2h_1 = (-5X)\, g + h_2, \text{ onde } h_2 = 5X^3 - 10\mathbf{X^2Y^4} + 5X^2Y^3 - 40XY^3$$

Passo 3:

$$h_2 = \left(-5Y^3\right) g + h_3, \text{ onde } h_3 = 5X^3 + 10\mathbf{X^2Y^3} + 5XY^6 - 40XY^3$$

Passo 4:

$$h_3 = \left(5Y^2\right) g + h_4, \text{ onde } h_4 = 5X^3 - 5\mathbf{X^2Y^2} + 5XY^6 - 5XY^5 - 40XY^3$$

Passo 5

$$2h_4 = (-5Y)\, g + h_5, \text{ onde } h_5 = 10X^3 + \mathbf{5X^2Y} + 10XY^6 - 10XY^5 + 5XY^4 - 80XY^3$$

Passo 6:

$$2h_5 = (-5)\, g + r, \text{ onde } r = 20X^3 - 5X^2 + 20XY^6 - 20XY^5 + 10XY^4 - 165XY^3$$

Observe que dividindo $r := h_6$ por $2^4 = 16$ reobtemos o resto quando $K = \mathbb{Q}$. Assim, é mais eficiente realizar a falsa divisão em $\mathbb{Z}$ e depois colocar de volta os devidos denominadores, caso necessário. De acordo com isso, teoricamente, é melhor lidar com corpos, mas computacionalmente, é mais fácil trabalhar em domínios. Salientamos que o cálculo do resto vai depender da ordenação imposta sobre os termos. De fato, neste mesmo exemplo, se tomarmos a ordenação via *grau-lex* (veja a referência [21] para definição), com $X > Y$, temos $f = 5X^3Y^2 - 10XY^3$ e $g = XY^3 + 2X^2Y + X^2$ para esta ordenação, realizamos a redução com um único passo, veja:

Passo único:

$$f = (-10)\, g + r, \text{ onde } r = 5X^3Y^2 + 20X^2Y - 10X^2$$

Neste caso, note que o termo de f que é reduzido é $-10XY^3$ e não o seu termo líder $5X^3Y^2$. Novamente, note que r não é constituído de monômio algum que seja divisível pelo monômio líder de g. Um tal polinômio é dito ser *Gröbner reduzido em relação a* g.

Não custa lembrar que podemos considerar polinômios em várias variáveis como polinômios em uma variável, dita *variável principal*. Mais especificamente, como um polinômio diferencial $P \in K\{Y\} \setminus K$ de ordem j pode ser escrito como

$$P(y) = \sum_{i=0}^{m} P_i \cdot (y^{(j)})^i$$

sendo que $P_i \in K\{Y \setminus y\}$ e y é a maior variável em $\{y_1, \ldots, y_n\}$ em que $gr_y(P) \neq 0$. Para um polinômio diferencial $P \in K\{y_1, \ldots, y_n\} - K$, assumindo esta variável como variável principal y_i, vamos considerar P como um polinômio univariado em $K\{y_1, \ldots, y_{i-1}\}\{y_i\}$, dado por $P = cy_i^e + r$, onde $gr(P, y_i) = e$, $c \in K\{y_1, \ldots, y_{i-1}\}$ e $r \in K\{y_1, \ldots, y_n\}$, com $0 \leq gr(r, y_i) < e$ (comumente, e é chamado de o *grau principal* de P).

Exemplo 1.20

Considerando ainda os mesmos exemplos anteriores, só que agora com $K[X, Y]$ visto como $K[Y][X]$, onde X é a variável principal, tem-se que

$$f = (5Y)\, X^3 + \left(-10Y^3\right) X \quad \text{e} \quad g = (2Y + 1)X^2 + \left(Y^3\right) X.$$

Aqui, o inicial de g é $2Y + 1$ e a redução é feita pela falsa divisão tomando coeficientes no domínio $K[Y]$. Claramente, o resto será de menor grau na variável principal com respeito ao divisor g, veja:

Passo 1:

$$(2Y+1)\,f = [\left(5Y^2\right)X]g + h_1, \text{ onde } h_1 = \left(-5Y^5\right)X^2 + \left(-20Y^4 - 10Y^3\right)X$$

Passo 2:

$$(2Y+1)\,h_1 = \left(5Y^5\right)g + r, \text{ onde } r = \left(5Y^8X^3 - 40Y^5 - 40Y^4 - 10Y^3\right)X$$

Tal resto dizemos ser *algebricamente reduzido* em relação a g e sua variável principal.

1.5.2 Caso Diferencial

Paralelamente ao caso não diferencial, vamos tratar o processo de redução no caso diferencial. Seja K um corpo diferencial ordinário e um conjunto Y de indeterminadas diferenciais. Comecemos com um exemplo com duas indeterminadas diferenciais. Considere inicialmente um posicionamento ordenado tal que y_2 possua uma posição maior do que y_1, em $K\{y_1, y_2\}$. Suponha que se deseje dividir o polinômio diferencial

$$F = 5\left(y_1'\right)^2\left(y_2''\right)^3 - 10\left(y_1'\right)^3 y_2'' \text{ por } G = \left(y_1'\right)^3 y_2'' + 2y_1'\left(y_2''\right)^2 + \left(y_2''\right)^2.$$

Note que F e G envolvem apenas duas derivadas, a saber, y_1' e y_2'', sendo que y_2'' possui uma posição maior do que y_1' devido ao posicionamento ordenado. Agora, substituindo y_2'' por X e y_1' por Y, concluímos que

$$F = 5X^3Y^2 - 10XY^3 \quad \text{e} \quad G = XY^3 + 2X^2Y + X^2.$$

Ora, mas estes polinômios diferenciais são exatamente os mesmos polinômios f e g dados anteriormente, aos quais aplicamos um processo de divisão! Isto nos sugere que seja, de fato, possível realizar divisões no *"mundo dos polinômios diferenciais"*.

Façamos neste momento uma reflexão: e se um dos y_2'' em F fosse na verdade y_2'''? Antes de mais nada, devemos ser capazes de diferenciar o polinômio diferencial G para reduzir F. Mais geralmente e precisamente, devemos ser capazes de diferenciar um polinômio diferencial.

Já conhecemos a estrutura da derivada de um polinômio diferencial. Para um melhor entendimento no que se segue, vamos partir do ponto de vista univariado (polinômio diferencial em uma variável).

Primeiramente, dado um polinômio diferencial $P \in K\{y_1, \ldots, y_n\}$, onde $P \notin K$, vamos escolher a derivada $\delta(y_i)$ de maior posição que aparece em P

como a variável principal. A esta variável, dá-se o nome de *líder de* P, e a denotamos por u_P. Do ponto de vista de uma variável principal, podemos escrever P como um polinômio diferencial na variável u_P com coeficientes I_d, onde $d \in \{0, \ldots, d\}$, em $K\{Y \backslash u_P\}$ como segue:

$$P = \sum_{0 \leq i \leq d} I_i u_P^i = I_d u_P^d + I_{d-1} u_P^{d-1} + \cdots + I_1 u_P + I_0$$

Assim, nesta representação, todos os coeficientes $I_d \neq 0$ (únicos) são menores do que P. Mais especificamente, cada derivada $\delta(y_k)$ presente em I_i é menor do que u_P. O polinômio diferencial I_d é chamado de o *inicial de* P, e denotamos I_P. De forma resumida, podemos escrever

$$P = I_P \left(u_P\right)^{gr_{u_P}(P)} + P_0, \text{ onde } P_0 < P.$$

Segue das regras de derivação que:

$$\begin{aligned} \delta(P) &= P' = \left(dI_d u_P^{d-1} + (d-1) I_{d-1} u_P^{d-2} + \cdots + I_1\right) \delta u_P + \\ &\quad + \delta(I_d)\, u_P^d + \delta\left(I_{d-1}\right) u_P^{d-1} + \cdots + \delta\left(I_1\right) u_P + \delta\left(I_0\right). \end{aligned}$$

O líder de $\delta(P)$ é δu_P, desde que, se $v < u_P$ então $\delta v < \delta u_P$, para qualquer derivada v que aparece em I_j. Uma vez que $\delta(P)$ é linear em δu_P, tem-se que o inicial de $\delta(P)$ é

$$I_{\delta(P)} = dI_d u_P^{d-1} + (d-1) I_{d-1} u_P^{d-2} + \cdots + I_1 = \sum i I_i u_P^{i-1} = \frac{\partial P}{\partial u_P}.$$

A este polinômio diferencial inicial, dá-se o nome de o *separante de* P, e é designado por S_P. De forma resumida, podemos escrever

$$\delta(P) = S_P \delta u_P + (\text{termos envolvendo derivadas} < \delta u_P).$$

Para qualquer polinômio diferencial $P \in K\{y_1, \ldots, y_n\}$, onde $P \notin K$, tem-se que P é maior do que o inicial I_P e o separante S_P. Claramente, a escolha de ordenações diferentes pode resultar em líder e separante diferente.

Vamos agora a uma resposta ao nosso dito momento de reflexão. Suponha que nosso polinômio diferencial F seja

$$F = 5\left(y_1'\right)^2 \left(y_2'''\right)^3 - 10\left(y_1'\right)^3 y_2'', \tag{1.3}$$

e vamos manter a nossa G original, dada por

$$G = \left(y_1'\right)^3 y_2'' + 2y_1' \left(y_2''\right)^2 + \left(y_2''\right)^2. \tag{1.4}$$

Derivando G obtemos:

$$\begin{aligned}\delta(G) &= G' = (y_1')^3 y_2''' + 3(y_1')^2 y_1'' y_2'' + 4y_1' y_2'' y_2''' + 2y_1''(y_2'')^2 + 2y_2'' y_2''' \\ &= \left((y_1')^3 + 4y_1' y_2'' + 2y_2''\right) y_2''' + 3(y_1')^2 y_1'' y_2'' + 2y_1''(y_2'')^2 = S_G y_2''' + T\end{aligned}$$

Aqui, T é uma soma de termos envolvendo derivadas de ordem < 3. Daí, uma vez que G' é linear em $y_2''' = u_{G'}$, eliminamos y_2''' em F da seguinte forma:

$\delta(G) = S_G y_2''' + T$ ou seja $y_2''' = \dfrac{\delta(G) - T}{S_G}$. Substituindo em (1.3), obtemos,

$F = 5(y_1')^2 \left(\dfrac{\delta(G) - T}{S_G}\right)^3 - 10(y_1')^3 y_2''$. E, portanto teremos,

$$\begin{aligned}(S_G)^3 F &= 5(y_1')^2 (\delta(G) - T)^3 - 10(y_1')^3 y_2''(S_G)^3 \\ &= 5(y_1')^2 (\delta(G))^3 + 5(y_1')^2 (-T)^3 - 10(y_1')^3 y_2''(S_G)^3 \\ &= Q\delta(G) + 5(y_1')^2 (-T)^3 - 10(y_1')^3 y_2''(S_G)^3,\end{aligned}$$

onde $Q = 5(y_1')^2 (\delta(G))^2$.

Esta redução é chamada de *redução parcial*. Quando reduzimos parcialmente F por G, supondo que $\delta^j u_G$ esteja em F, onde $j \geq 1$ é o máximo possível, diferenciamos G até a ordem j, obtendo:

$$\begin{aligned}\delta(G) &= S_G \delta u_G + T_1 \\ \delta^2(G) &= S_G \delta^2 u_G + T_2 \\ &\vdots \\ a\delta^j(G) &= S_G \delta^j u_G + T_j\end{aligned}$$

Aqui, cada T_k é uma soma de termos envolvendo derivadas de posição menores do que $\delta^k u_G$. Em seguida, fazendo as devidas substituições e "limpando" os denominadores como feito anteriormente, obtemos:

$$(S_G)^s F = Q_1\delta(G) + Q_2\delta^2(G) + \cdots + Q_j\delta^j(G) + \widetilde{F}, \text{ com } \widetilde{F} < G \text{ (em } u_G)$$

Chamamos $\widetilde{F}$ de *resto parcial* de F com respeito a G.

Definição 1.21 *Seja K um corpo diferencial ordinário e Y um conjunto de indeterminadas diferenciais. Um polinômio diferencial q é parcialmente reduzido em relação a p se nenhuma derivada da variável principal u_p, de ordem positiva, comparece em q. Além disso, q é reduzido em relação p se q é parcialmente reduzido em relação a p e o $grau_{u_p}(q) < grau_{u_p}(p)$. Um subconjunto A de $K\{Y\} - K$ é chamado um conjunto autoreduzido se cada um de seus elementos é reduzido em relação a todos os outros.*

Salientamos que podemos continuar (algebricamente) o processo de redução, reduzindo $\widetilde{F}$, usando a falsa divisão univariada por G de modo que, aparecendo no resto o líder u_G de G, o mesmo será de menor grau do que o grau de u_G em G. De acordo disso, obtemos uma completa redução de F por G, resultando na seguinte expressão:

$$I_G^i S_G^s F = Q_0 G + I_G^i Q_1 \delta(G) + I_G^i Q_2 \delta^2(G) + \cdots + I_G^i Q_j \delta^j(G) + R \quad (1.5)$$

O resto R assim obtido é chamado de *resto Ritt-Kolchin*, e tem a propriedade de ser parcialmente reduzido e algebricamente reduzido em relação a G.

Existe um algoritmo ([19], p.77) que reduz, um dado polinômio diferencial F com respeito a um conjunto autoreduzido $A = A_1, \ldots, A_n$, para um polinômio diferencial R que é reduzido com respeito a A e que satisfaz

$$I_{A_1}^{i_1} \cdots I_{A_n}^{i_n} S_{A_1}^{i_1} \cdots S_{A_n}^{i_n} F \equiv R \, (mod \, [A_1, \ldots, A_n])$$

(veja também [5] e [29]).

Dados um subconjunto S e um ideal diferencial J, ambos em $K\{Y\}$, e denotando por S^∞ o monóide livre multiplicativo garado por 1 e os fatores irredutíveis dos elementos de S, definimos a *saturação* de J por um conjunto S como sendo

$$J : S^\infty = \{f \in K\{Y\} \mid gf \in J \text{ para algum } g \in S^\infty\}.$$

O conjunto $J : S^\infty$ é também um ideal, e temos $J \subset J : S^\infty$. Assim, em particular, definimos o *ideal de saturação* de um ideal J por um elemento s em um anel A como sendo

$$J : s^\infty = \{f \in K\{Y\} \mid s^e f \in J \text{ para algum } e \in \mathbb{N}\}.$$

Quando o ideal J é principal, digamos $J = \langle g \rangle$, o terno (e, q, r), na relação (1.2), é único, para qualquer $f \in \langle g \rangle : s^\infty$, desde que a escolha de e seja minimal. Além disso, sendo e minimal ou não, tem-se que $r = 0$ se e só se $f \in \langle g \rangle : s^\infty$. Em particular, quando $e = 1$, para $h \in K\{Y\}$ temos o *ideal quociente* de $\langle g \rangle$ por h, definido por $\langle g \rangle : h = \{p \in K\{Y\} \mid ph \in \langle g \rangle\}$.

Capítulo 2

Equações Diferenciais Racionais Paramétricas

Ao longo deste capítulo vamos considerar alguns problemas computacionais relacionados à implicitização de equações diferenciais racionais paramétricas ($EDRP's$). Por exemplo, o conjunto de equações paramétricas formado por

$$\begin{cases} x &= u \\ y &= au + b \end{cases}$$

onde x e y são indeterminadas, u é um parâmetro, e a e b constantes ($a' = b' = 0$), é a representação paramétrica para a variedade diferencial (definição na seção 1) definida pela seguinte equação algébrica diferencial:

$$x'y'' - x''y' = 0$$

Vamos propor algoritmos para os seguintes problemas relacionados a um conjunto de $EDRP's$.:

(1) Encontrar um conjunto característico para o *ideal primo implícito* (definição na seção *2*) de um conjunto de EDRP's.

(2) Encontrar uma *representação canônica* para a *imagem* (definição na seção *3*) de um conjunto de EDRP's.

(3) Decidir se os *parâmetros* de um conjunto de EDRP's são *independentes*, e se não, reparametrizar as EDRP's para que novas as EDRP's possuam *parâmetros independentes*.

(4) Calcular os *mapas inversos* de um conjunto de EDRP's, e como consequência, decidir quando um conjunto de EDRP's é *próprio*. No

caso da variedade implícita ser de dimensão diferencial 1 e o conjunto de EDRP's não *próprio*, achar uma reparametrização própria para as dadas EDRP's. Isso é baseado na prova construtiva da versão diferencial do teorema de *Lüroth* ([29]). O cálculo é baseado principalmente no método do conjunto característico para equações diferenciais algébricas ([9], [29]).

Na seção 2, mostraremos como calcular o conjunto característico para um ideal implícito de um conjunto de $EDRP's$.

2.1 Preliminares da Álgebra Diferencial

Seja K um corpo diferencial de característica zero. Chamamos de E uma *extensão universal do corpo* K quando para qualquer extensão finitamente gerada $K_1 \supset K$, com $K_1 \subseteq E$, tem-se que, se E_0 é uma extensão finitamente gerada de K_1, não necessariamente em E, então existe um K_1-isomorfismo de E_0 em E (isto é, existe um isomorfismo σ de E_0 em E tal que $\sigma a = a$, para cada $a \in K_1$) (veja Capítulo III seção 7 de [19]). Tal extensão universal de K sempre existe ([19]) p.133), mas não é única. Todavia, se E e F são duas extensões universais de K, então existem extensões universais $\widehat{E}$ e $\widehat{F}$ de E e F, respectivamente, tais que, $\widehat{E}$ é isomorfo a $\widehat{F}$ sobre K (o fato de um corpo diferencial K ter uma extensão universal é um bom exercício do *Lema de Zorn*, ([19], p.135, Exerc. 7); veja também a referência [4], p.771). Como observa Ritt, não existe um conjunto de todas extensões de corpos diferenciais finitamente gerados (do ponto de vista diferencial) de um corpo diferencial F. Dentro deste contexto, primeiramente Kolchin introduz um corpo universal em analogia ao corpo universal de *Weil* (veja [34]). Kolchin escreve:

"*O uso de uma extensão universal, que segue agora bem conhecida da Geometria Algébrica Moderna, torna possível evitar certas dificuldades lógicas conectada com frases como o conjunto de todas as extensões.*"(Veja [4] p.577).

Utilizando a relação (1.5) do capítulo anterior, dados dois polinômios diferenciais P e Q, designando por $R := f_r(P, Q)$ o falso resto de P em relação à Q, temos a seguinte *fórmula do resto* para R

$$JP = \sum_i B_i Q^{(i)} + R,$$

onde J é um produto de certas potências do inicial e separante (*SI-produto*) de Q, cada $Q^{(i)}$ é a i-ésima derivada de Q e os B_i são polinômios diferenciais.

Podemos definir o falso resto $f_r(P, \mathcal{A})$ do polinômio P em relação a um conjunto autoreduzido $\mathcal{A} = \{A_1, \ldots, A_m\}$, recursivamente, como

$$f_r(P, \mathcal{A}) := f_r\left(f_r(P, A_m), A_1, \ldots, A_{m-1}\right), \text{ com } f_r(P, \varnothing) = P.$$

Para o que segue, definiremos um particular conjunto de polinômios diferenciais, chamado conjunto triangular. Tais conjuntos foram introduzidos por Ritt em 1932 como conjuntos característicos e estão profundamente envolvidos na resolução de sistemas polinomiais. Por exemplo, em métodos como os encontrados em [35] e [5], considera-se um subconjunto particular de uma dada variedade afim associado a um conjunto triangular (em um fecho algébrico de K), ou seja, o conjunto de zeros regulares. Vamos agora a definição de conjuntos triangulares.

Definição 2.1 *Dizemos que um subconjunto $T \subset K\{x_1, \ldots, x_n\}$ é um conjunto triangular se nenhum elemento de T está em K e se P e Q em T são distintos então eles têm variáveis principais distintas. Quando existe $P \in T$ tal que v é sua variável principal dizemos que v é algébrico em relação a T e as demais variáveis são ditas transcendentes.*

Qualquer conjunto triangular T em $K\{x_1, \ldots, x_n\}$ pode ser escrito sob a forma

$$T = \left[T_1\left(x_1, \ldots, x_{p_1}\right), \ldots, T_r\left(x_1, \ldots, x_{p_r}\right)\right], \text{ onde } 0 < p_1 < \cdots < p_r \leq n,$$

com x_{p_i} a variável líder de T_i, para cada $i = 1, \ldots, r$. As demais variáveis de $x_{p_1}, \ldots, x_{p_r}$ são chamadas de *parâmetros* de T.

Por exemplo, considerando os subconjuntos de variáveis algébricas x_2, x_3, x_4

$$T_1 = \left\{x_2^2 + x_1, x_1x_3^2 + 2x_2x_3 - 7, \left(x_2x_3 + 7\right)x_4 - x_2^2\right\}$$

e

$$T_2 = \left\{x_1^2x_2 - 5, x_1x_2^2 + 5\right\}$$

em $K\{x_1, \ldots, x_n\}$, com $n \geq 4$, tem-se que T_1 é um conjunto triangular, enquanto que T_2 não é.

Para um conjunto triangular $\mathcal{A}$, temos que

$$\mathbf{SAT}(\mathcal{A}) = \{P \in K\{X\} \mid JP \in [\mathcal{A}] \text{ para algum } J\},$$

onde J é um SI-produto de polinômios diferenciais em $\mathcal{A}$ e $[\mathcal{A}]$ é o ideal diferencial gerado por $\mathcal{A}$.

Definição 2.2 *Um conjunto autoreduzido $\mathcal{A}$ é dito irredutível se não existirem polinômios diferenciais P e Q, reduzidos pelos polinômios diferencias em $\mathcal{A}$, tais que ambos $f_r(P,\mathcal{A})$ e $f_r(Q,\mathcal{A})$ são não nulos e $f_r(PQ,\mathcal{A})=0$.*

O próximo resultado fornece uma condição necessária e suficiente para que um conjunto $\mathcal{A}$ seja um conjunto característico de um ideal primo I, e sua prova pode ser encontrada em [29] (p.107) ou em [19] (p.167).

As definições de grau de transcendência e dimensão de ideais no caso diferencial são feitas de maneira análogas ao caso não diferencial (veja, por exemplo, [17], página 4581). Nesse trabalho, entenderemos dimensão sempre como a dimensão diferencial.

Proposição 2.3 *Se $\mathcal{A} \subset K\{X\}$ é um conjunto autoreduzido irredutível, então $\mathbf{SAT}(\mathcal{A})$ é um ideal primo de dimensão diferencial $n-|\mathcal{A}|$. Reciprocamente, para qualquer ideal primo $\mathcal{I}$, existe um conjunto autoreduzido irredutível $\mathcal{A}$ tal que, $\mathcal{I}=\mathbf{SAT}(\mathcal{A})$.*

Definição 2.4 *Na situação da proposição acima, o conjunto autoreduzido $\mathcal{A}$ é chamado conjunto característico de $\mathbf{SAT}(\mathcal{A})$ e o ideal diferencial I é dito caracterizável. Mais especificamente, um ideal I de $K\{X\}$ é caracterizável se para um conjunto característico $\mathcal{A}$ de $\mathcal{I}$ temos $\mathcal{I}=\mathbf{SAT}(\mathcal{A})$. Neste caso, dizemos que $\mathcal{A}$ caracteriza $\mathcal{I}$.*

Caracterização do anulamento de $f_r(P,\mathcal{A})$:

Se $\mathcal{A}$ é um conjunto característico de

$$\mathbf{SAT}(\mathcal{A})=[\mathcal{A}]:H_{\mathcal{A}}^{\infty}=\{P\in K\{X\}\mid HP\in[\mathcal{A}] \text{ para algum } H\in H_{\mathcal{A}}^{\infty}\}$$

então,

$$P\in\mathbf{SAT}(\mathcal{A})=[\mathcal{A}]:H_{\mathcal{A}}^{\infty}\Longleftrightarrow f_r(P,\mathcal{A})=0$$

Demonstração. Sejam $\mathcal{I}$ um ideal diferencial saturado definido por $\mathcal{A}$ e P um polinômio diferencial em $K\{X\}$. É claro que se $\mathcal{A}$ é um conjunto característico de $\mathcal{I}$ e P um polinômio diferencial de $\mathcal{I}$, então $f_r(P,\mathcal{A})=0$. Reciprocamente, se $f_r(P,\mathcal{A})=0$, então $P\in\mathbf{SAT}(\mathcal{A})=[\mathcal{A}]:H_{\mathcal{A}}^{\infty}$, onde $[\mathcal{A}]$ é o ideal diferencial gerado por $\mathcal{A}$ e $H_{\mathcal{A}}=I_{\mathcal{A}}S_{\mathcal{A}}$ um $SI-produto$ de polinômios diferenciais em $\mathcal{A}$. Desde que $\mathcal{I}$ seja saturado, tem-se que $[\mathcal{A}]:H_{\mathcal{A}}^{\infty}=\mathcal{I}$ é o ideal de saturação de $\mathcal{A}$ e vem que $P\in\mathcal{I}$. ■

Para um conjunto $\mathcal{S}$ de polinômios diferenciais definimos

$$Z(\mathcal{S})=\{\eta=(\eta_1,\ldots,\eta_n)\in E^n\mid P(\eta)=0, \text{ para todo } P\in\mathcal{S}\}$$

que é chamado de *variedade diferencial* definida por $\mathcal{S}$.

Para dois conjuntos $\mathcal{S}$ e $\mathcal{D}$ de polinômios diferenciais, definimos a *quasi variedade diferencial* como sendo

$$Z\left(\mathcal{S}/\mathcal{D}\right) = Z\left(\mathcal{S}\right) - \bigcup_{d\in\mathcal{D}} Z\left(d\right)$$

Seja $\mathcal{I}$ um ideal diferencial primo em $K\left\{X\right\}$. Um *zero genérico* de $\mathcal{I}$ é um ponto $\eta \in Z\left(\mathcal{I}\right)$ tal que, cada polinômio diferencial em $K\left\{X\right\}$ anulado por η está contido em $\mathcal{I}$.

Seja $\mathcal{A}$ um conjunto autoreduzido irredutível. As variáveis que não são variáveis líderes de polinômios diferenciais em $\mathcal{A}$ são chamadas de *variáveis paramétricas* de $\mathcal{A}$. A *ordem* de um conjunto autoreduzido irredutível $\mathcal{A}$ é a soma das ordens dos polinômios diferenciais em $\mathcal{A}$. Para um ideal primo $\mathcal{I} = \mathbf{SAT}\left(\mathcal{A}\right)$, a *ordem* de $\mathcal{A}$ é chamada *ordem* de $\mathcal{I}$ (ou $Z\left(\mathcal{I}\right)$) em relação às variáveis paramétricas de $\mathcal{A}$. A ordem de um ideal primo não depende da escolha de conjuntos autoreduzidos com as mesmas variáveis paramétricas ([29]).

Precisaremos das seguintes formas do *Teorema de Decomposição dos Zeros de Wu-Ritt* (veja [11], página 588):

Teorema 2.5 *Para dois conjuntos $\mathcal{S}$ e $\mathcal{D}$ de polinômios diferenciais, temos um método para encontrar conjuntos autoreduzidos ascendentes irredutíveis $\mathcal{A}_i$ tais que*

$$Z\left(\mathcal{S}/\mathcal{D}\right) = \bigcup_i Z\left(\mathcal{A}_i/\mathcal{D} \cup \left\{J_i\right\}\right),$$

onde J_i é um SI-produto de polinômios diferenciais em $\mathcal{A}_i$.

Teorema 2.6 *Para dois conjuntos $\mathcal{S}$ e $\mathcal{D}$ de polinômios diferenciais, temos um método para encontrar conjuntos autoreduzidos ascendentes irredutíveis $\mathcal{A}_i$ tal que*

$$Z\left(\mathcal{S}/\mathcal{D}\right) = \bigcup_i Z\left(\mathbf{SAT}\left(\mathcal{A}_i\right)/\mathcal{D}\right).$$

A grande maioria dos trabalhos tem sido feito com o uso desses teoremas. Alguns podem ser achados em [5].

2.2 Ideal Implícito de um conjunto de EDRP's

Dado um conjunto de indeterminadas diferenciais $U = \{u_1, \ldots, u_m\}$, para polinômios diferenciais não nulos $P_1, \ldots, P_n, Q_1, \ldots, Q_n$ em $K\{U\}$, chamamos

$$x_1 = \frac{P_1(U)}{Q_1(U)}, \ldots, x_n = \frac{P_n(U)}{Q_n(U)}$$

de um conjunto de *equações diferenciais racionais paramétricas* (EDRP's). Vamos assumir que algum dos $P_i(U)$ ou algum dos $Q_i(U)$ não estão em K e que o $MDC(P_i(U), Q_i(U)) = 1$. Por simplicidade, as EDPR's envolvendo constantes arbitrárias, como no exemplo dado na introdução, não serão consideradas. Todavia, não há dificuldade alguma em extender os resultados para este caso.

Definição 2.7 *O ideal implícito do conjunto de EDPR's é definido como*

$$\boldsymbol{ID}(P, Q) = \left\{ P \in K\{x_1, \ldots, x_n\} \mid P\left(\frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n}\right) \equiv 0 \right\}.$$

A variedade diferencial $Z(\mathbf{ID}(P, Q))$ é chamada de *variedade implícita* do conjunto de EDRP's. Dada uma variedade diferencial $\mathcal{V}$, se existe um conjunto de EDRP's (como o definido) tal que, $\mathcal{V}$ seja a variedade implícita para tal conjunto de EDRP's, dizemos que $\mathcal{V}$ é uma *variedade diferencial uniracional* e o conjunto de EDRP's é a *representação paramétrica* para $\mathcal{V}$.

Para o desenvolvimento das próximas seções, precisaremos dos lemas que seguem.

Lema 2.8 *O ideal implícito* $\boldsymbol{ID}(P, Q)$ *é um ideal diferencial primo, com zero genérico* $\eta = \left(\frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n}\right)$.

Demonstração. Seja $\mathbf{ID}(P, Q)$ o ideal implícito do conjunto de EDRP's

$$x_1 = \frac{P_1(U)}{Q_1(U)}, \ldots, x_n = \frac{P_n(U)}{Q_n(U)}.$$

É claro que $\mathbf{ID}(P, Q)$ é um ideal diferencial. Vamos mostrar que $\mathbf{ID}(P, Q)$ é também primo. Suponha então que $PQ \in \mathbf{ID}(P, Q)$ e seja $\eta = \left(\frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n}\right)$. Então, por definição de $\mathbf{ID}(P, Q)$, segue que $P(\eta)Q(\eta) = 0$ o que implica que $P(\eta) = 0$ ou $Q(\eta) = 0$. Novamente, pela definição de $\mathbf{ID}(P, Q)$, segue que $P \in \mathbf{ID}(P, Q)$ ou $Q \in \mathbf{ID}(P, Q)$. Assim, o ideal implícito $\mathbf{ID}(P, Q)$ é um

ideal diferencial primo. Além disso, uma vez que a extensão E contém cada u_i de $P_i(U)$ e $Q_i(U)$, e portanto de $\frac{P_i(U)}{Q_i(U)}$, segue da definição de variedade implícita que $\eta \in Z(\mathbf{ID}(P,Q))$. E mais, visto que $\mathbf{ID}(P,Q)$ é um ideal diferencial primo, tem-se por definição que η é um zero genérico de $\mathbf{ID}(P,Q)$. ■

Utilizando as mesmas notações introduzidas acima, sejam

$$\mathbf{PS} = \{F_1 = P_1 - x_1Q_1, \ldots, F_n = P_n - x_nQ_n\} \text{ e } \mathbf{DS} = \{Q_1, \ldots, Q_n\}.$$

Como $\mathbf{PS} = \{P_i(U) - x_iQ_i(U),\ i = 1, \ldots, n\}$, em $K\{U, X\}$, é um conjunto autoreduzido ascendente nas variáveis ordenadas

$$u_1 < \cdots < u_m < x_1 < \cdots < x_n,$$

podemos definir $\mathbf{SAT}(\mathbf{PS})$.

Lema 2.9 *: $\mathbf{SAT}(\mathbf{PS})$ é um ideal diferencial primo de dimensão m e $\mathbf{SAT}(\mathbf{PS}) \cap K\{X\}$ é o ideal implícito do conjunto de EDRP's.*

$$x_1 = \frac{P_1(U)}{Q_1(U)}, \ldots, x_n = \frac{P_n(U)}{Q_n(U)}.$$

Demonstração. Seja $\mathbf{SAT}(\mathbf{PS})$, onde

$$\mathbf{PS} = \{F_1 = P_1 - x_1Q_1, \ldots, F_n = P_n - x_nQ_n\}$$

é um conjunto autoreduzido ascendente nas variáveis ordenadas

$$u_1 < \cdots < u_m < x_1 < \cdots < x_n.$$

Sob esta ordenação, tem-se que as variáveis líderes são de grau 1. Portanto, $\mathbf{PS}$ é um conjunto autoreduzido ascedente irredutível e temos, pela proposição 2.3, que $\mathbf{SAT}(\mathbf{PS})$ é um ideal primo, com zero genérico da forma

$$\eta = \left(U, \frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n}\right)$$

([29], [35]). A dimensão de $\mathbf{SAT}(\mathbf{PS})$ é o grau de transcendência diferencial de η sobre K, que é m. Agora, como η é um zero genérico de $\mathbf{SAT}(\mathbf{PS})$, tem-se que

$$\eta_0 = \left(\frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n}\right)$$

é um zero genérico de $\mathbf{SAT}(\mathbf{PS}) \cap K\{X\}$. Ora, mas pelo Lema 2.8, η_0 também é um zero genérico de $\mathbf{ID}(P,Q)$. Assim, $\mathbf{SAT}(\mathbf{PS}) \cap K\{X\}$ e $\mathbf{ID}(P,Q)$ possuem o mesmo zero genérico, e portanto,

$$\mathbf{SAT}(\mathbf{PS}) \cap K\{X\} = \mathbf{ID}(P,Q).$$

De acordo com isso, segue que $\mathbf{SAT}(\mathbf{PS}) \cap K\{X\}$ é o ideal implícito do conjunto de EDRP's $x_1 = \dfrac{P_1(U)}{Q_1(U)}, \ldots, x_n = \dfrac{P_n(U)}{Q_n(U)}$. ■

Lema 2.10 *:* $Z(\mathbf{PS}/\mathbf{DS}) = Z(\mathbf{SAT}(\mathbf{PS})/\mathbf{DS})$.

Demonstração. Dadas as variedades diferenciais

$$Z(\mathbf{PS}/\mathbf{DS}) \text{ e } Z(\mathbf{SAT}(\mathbf{PS})/\mathbf{DS}),$$

como por definição $\mathbf{PS} \subset \mathbf{SAT}(\mathbf{PS})$, onde $\mathbf{PS}, \mathbf{SAT}(\mathbf{PS}) \subset K\{U,X\}$, segue que

$$Z(\mathbf{SAT}(\mathbf{PS})/\mathbf{DS}) \subset Z(\mathbf{PS}/\mathbf{DS}).$$

Vamos mostrar que $Z(\mathbf{PS}/\mathbf{DS}) \subset Z(\mathbf{SAT}(\mathbf{PS})/\mathbf{DS})$. Tome arbitrariamente $\eta \in Z(\mathbf{PS}/\mathbf{DS})$. Da definição de **PS** e **DS**, segue que $F_i(\eta) = 0$ e $Q_i(\eta) \neq 0$, para $i = 1, \ldots, n$. Agora, dado $H \in \mathbf{SAT}(\mathbf{PS})$, pela definição de $\mathbf{SAT}(\mathbf{PS})$, existe um SI-produto J de polinômios diferenciais em **PS** tal que, $JH \in [PS]$. Ora, mas na verdade, pela definição de **PS** e visto que $F_i(\eta) = 0$ e $Q_i(\eta) \neq 0$, para $i = 1, \ldots, n$, existe então é um produto J de potências de Q_i tal que, $JH \in [PS]$. Note agora que sendo $J(\eta)H(\eta) = 0$, tem-se que $\eta \in Z(\mathbf{SAT}(\mathbf{PS}))$. De fato, pois por definição de SI-produto temos que $J \neq \{0\}$, e portanto $J(\eta) \neq 0$. Daí, $H(\eta) = 0$ e segue que $\eta \in Z(\mathbf{SAT}(\mathbf{PS}))$, visto que $\mathbf{SAT}(\mathbf{PS})$ é um ideal diferencial primo (*Lema* 2.9), e assim, η é um seu zero genérico. Como η foi tomado qualquer, tem-se que $Z(\mathbf{PS}/\mathbf{DS}) \subset Z(\mathbf{SAT}(\mathbf{PS})/\mathbf{DS})$, e concluímos que $Z(\mathbf{PS}/\mathbf{DS}) = Z(\mathbf{SAT}(\mathbf{PS})/\mathbf{DS})$. ■

Observação 2.11

Do Lema 2.9, para acharmos o conjunto característico do ideal implícito, precisamos achar o conjunto característico para o ideal primo $\mathbf{SAT}(\mathbf{PS})$ nas variáveis ordenadas

$$x_1 < \cdots < x_n < u_1 < \cdots < u_m.$$

Com o Lema 2.10, esse problema é reduzido a acharmos a decomposição dos zeros $Z(\mathbf{PS}/\mathbf{DS})$. Aplicando o Teorema 2.6 nas variáveis ordenadas $x_1 < \cdots < x_n < u_1 < \cdots < u_m$, teremos:

$$Z(\mathbf{PS}/\mathbf{DS}) = \bigcup_i Z(\mathbf{SAT}(\mathcal{A}_i)/\mathbf{DS}),$$

onde os $\mathcal{A}_i$ são conjuntos autoreduzidos ascedentes irredutíveis.

Lema 2.12 *Existe um $\mathcal{A}_k$ na decomposição*

$$Z(\mathbf{PS}/\mathbf{DS}) = \bigcup_i Z(\mathbf{SAT}(\mathcal{A}_i)/\mathbf{DS})$$

tal que, substituindo x_i por $\dfrac{P_i}{Q_i}$, todo polinômio diferencial em $\mathcal{A}_k$ se anula, e temos

$$\mathbf{SAT}(\mathcal{A}_k) = \mathbf{SAT}(\mathbf{PS}).$$

Demonstração. Primeiramente note que, de fato, existe um $\mathcal{A}_k$ na decomposição

$$Z(\mathbf{PS}/\mathbf{DS}) = \bigcup_i Z(\mathbf{SAT}(\mathcal{A}_i)/\mathbf{DS})$$

tal que, substituindo x_i por $\frac{P_i}{Q_i}$, todo *polinômio diferencial* em $\mathcal{A}_k$ se anula. Com efeito, tendo em vista a observação anterior, como $\eta = \left(U, \frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n}\right)$ é um zero genérico do ideal primo $\mathbf{SAT}(\mathbf{PS})$ (Lema 2.8), e por conseguinte, $\eta \in Z(\mathbf{PS}/\mathbf{DS})$ (Lema 2.10), um tal k existe. Assim, resta-nos mostrar que $\mathbf{SAT}(\mathcal{A}_k) = \mathbf{SAT}(\mathbf{PS})$. Pela decomposição dada e do (Lema 2.10), tem-se que

$$Z(\mathbf{SAT}(\mathbf{PS})/\mathbf{DS}) = \bigcup_i Z(\mathbf{SAT}(\mathcal{A}_i)/\mathbf{DS}).$$

Assim, já temos que $\mathbf{SAT}(\mathbf{PS}) \subset \mathbf{SAT}(\mathcal{A}_k)$. Basta então mostrar que $\mathbf{SAT}(\mathcal{A}_k) \subset \mathbf{SAT}(\mathbf{PS})$. Como η é um zero de $\mathcal{A}_k$ (η anula todo polinômio diferencial em $\mathcal{A}_k$ como dito inicialmente) e também um zero genérico de $\mathbf{SAT}(\mathbf{PS})$, tem-se que $\mathcal{A}_k \subset \mathbf{SAT}(\mathbf{PS})$. Agora, note que para um SI-produto J qualquer de $\mathcal{A}_k$, digamos $J = I_{\mathcal{A}_k} S_{\mathcal{A}_k}$, tem-se que $J \notin \mathbf{SAT}(\mathbf{PS})$. Com efeito, caso contrário temos que $J \in \mathbf{SAT}(\mathbf{PS}) \subset \mathbf{SAT}(\mathcal{A}_k)$, e assim, $J \in \mathbf{SAT}(\mathcal{A}_k)$. Ora, mas isso é uma contradição, pois sendo $\mathcal{A}_k$ um conjunto autoreduzido irredutível, por definição, não podem existir polinômios diferenciais $I_{\mathcal{A}_k}$ e $S_{\mathcal{A}_k}$, reduzidos pelos polinômios diferenciais em $\mathcal{A}_k$, tais que ambos $f_r(I_{\mathcal{A}_k}, \mathcal{A}_k)$ e $f_r(S_{\mathcal{A}_k}, \mathcal{A}_k)$ são não nulos e $f_r(I_{\mathcal{A}_k} S_{\mathcal{A}_k}, \mathcal{A}) = 0$ (o

produto $I_{\mathcal{A}_k} S_{\mathcal{A}_k}$, e portanto J, não está em $\mathcal{A}_k$, isto é, $f_r(I_{\mathcal{A}_k} S_{\mathcal{A}_k}, \mathcal{A}) \neq 0$). De acordo disso, dado arbitrariamente $H \in \mathbf{SAT}(\mathcal{A}_k)$, mostremos então que $H \in \mathbf{SAT}(\mathbf{PS})$. Uma vez que $H \in \mathbf{SAT}(\mathcal{A}_k)$, por definição, existe um polinômio diferencial L que é um SI-produto dos polinômios diferenciais em $\mathcal{A}_k$ tal que, $LH \in [A_k] \subset \mathbf{SAT}(\mathbf{PS})$ (por definição, $[A_k]$ é o menor ideal contendo o seu gerador $\mathcal{A}_k$). Como, em particular, o SI-produto L não está em $\mathbf{SAT}(\mathbf{PS})$, e sendo $\mathbf{SAT}(\mathbf{PS})$ um ideal primo, tem-se que $H \in \mathbf{SAT}(\mathbf{PS})$. Uma vez que H foi tomado qualquer, segue que

$$\mathbf{SAT}(\mathcal{A}_k) \subset \mathbf{SAT}(\mathbf{PS}),$$

e portanto, concluímos que $\mathbf{SAT}(\mathcal{A}_k) = \mathbf{SAT}(\mathbf{PS})$. ■

Depois de mudarmos os nomes das variáveis, podemos escrever $\mathcal{A}_k$ como segue:

$$A_1(x_1, \ldots, x_{d+1}), \ldots, A_{n-d}(x_1, \ldots, x_n), \ldots$$

$$\ldots, B_1(x_1, \ldots, x_n, u_1, \ldots, u_{s+1}), \ldots, B_{m-s}(x_1, \ldots, x_n, u_1, \ldots, u_m).$$

Pelo Lema 2.10, tem-se que $\mathbf{SAT}(\mathbf{PS}) = \mathbf{SAT}(\mathcal{A}_k)$ tem dimensão m. Assim, o conjunto de variáveis paramétricas de $\mathcal{A}_k$, a saber $\{x_1, \ldots, x_d, u_1, \ldots, u_s\}$, deve conter m elementos ([29] p.44). Temos então que $d + s = m$. De acordo com isso e de posse do próximo teorema, seremos capazes (seção 4) de impormos uma condição necessária e suficiente sobre o *grau de transcendência diferencial* do corpo $K\left\langle \frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n} \right\rangle$, sobre K, em respeito aos parâmetros dados acima.

Teorema 2.13 *O ideal implícito do conjunto de EDRP's*

$$x_1 = \frac{P_1(U)}{Q_1(U)}, \ldots, x_n = \frac{P_n(U)}{Q_n(U)}$$

é $\boldsymbol{ID}(P, Q) = \mathbf{SAT}(A_1, \ldots, A_{n-d})$.

Demonstração. Pelo processo de computação acima, $\mathcal{A}_k$ escrito como

$$A_1(x_1, \ldots, x_{d+1}), \ldots, A_{n-d}(x_1, \ldots, x_n), \ldots$$

$$\ldots, B_1(x_1, \ldots, x_n, u_1, \ldots, u_{s+1}), \ldots, B_{m-s}(x_1, \ldots, x_n, u_1, \ldots, u_m),$$

é o conjunto característico de $\mathbf{SAT}(\mathbf{PS})$. Agora, o resultado é consequência dos Lemas 2.9 e 2.10. ■

Ressaltamos que o problema de como se calcular a base para o ideal primo implícito está em aberto. Por sorte, usando o *Teorema da Baixa Potência* ([29], p.65), conseguimos obter uma base para o ideal implícito do exemplo que segue.

Exemplo 2.14

Consideremos as seguintes EDRP's:

$$\begin{cases} x &= u^2 \\ y &= u' \end{cases}$$

Considerando o conjunto de polinômios diferenciais

$$S = \left\{F_1 = x - u^2, F_2 = y - u'\right\},$$

sob a ordem $x < y < u$ nas variáveis, seja o conjunto autoreduzido $A = \{A_1, A_2\}$ obtido por derivação sobre S:

$$A = \left\{4xy^2 - (x')^2, 2yu - x'\right\}$$

Pelo *Teorema de Decomposição* dos Zeros de Wu-Ritt (Teorema 2.5), tem-se que os zeros de S é

$$Z\left(\left\{4xy^2 - (x')^2, 2yu - x'\right\}/xy\right) \cup Z\left(\left\{x', y, u^2 - x\right\}/u\right) \cup Z\left(\{x, y, u\}\right)$$

Note que apenas $A_1 = 4xy^2 - (x')^2$ se anula para as EDRP's dadas. Pelo processo de obtenção de $\mathcal{A}_k$ dado anteriormente, vem que o ideal implícito é $\mathbf{SAT}\left(4xy^2 - (x')^2\right)$. Pelo Teorema da Baixa Potência, segue que

$$\mathbf{SAT}\left(4xy^2 - (x')^2\right) = \left[4xy^2 - (x')^2\right].$$

2.3 A Imagem de um conjunto de EDRP's

Definição 2.15 *O conjunto imagem de um conjunto de EDRP's em E^n é*

$$\boldsymbol{IM}(P, Q) = \left\{(\eta_1, \ldots, \eta_n) \in E^n \mid \textit{existe } \tau \in E^m \textit{ onde } \eta_i = \frac{P_i(\tau)}{Q_i(\tau)}\right\}.$$

Para calcularmos essa imagem, precisamos do seguinte conceito. Para dois conjuntos $\mathcal{S}$ e $\mathcal{D}$ de polinômios diferenciais em $K\{U, X\}$, definimos a *projeção* em X como segue:

$$Proj_{x_1,\ldots,x_n} Z(\mathcal{S}/\mathcal{D}) = \{e \in E^m \mid \text{existe } a \in E^n \text{tal que } (e,a) \in Z(\mathcal{S}/\mathcal{D})\}$$

O próximo teorema descreve a relação entre a imagem e a variedade implícita de um conjunto de EDRP's e nos dá uma *representação canônica* para a imagem. Mas antes, precisamos de um lema que será útil na demonstração do teorema.

Lema 2.16 *Podemos encontrar conjuntos de polinômios diferenciais $\mathcal{S}_i$ e polinômios diferenciais d_i, para $i = 1, \ldots, t$, tais que*

$$\boldsymbol{IM}(P,Q) = \bigcup_{1 \le i \le t} Z(\mathcal{S}_i / \{d_i\})$$

Demonstração. Primeiramente, escrevendo $x = (x_1, x_2, \ldots, x_n) \in E^n$, veja que podemos escrever a imagem como segue:

$$\mathbf{IM}(P,Q) = \left\{ x \in E^n \mid \text{existe } \tau \in E^m \text{ onde } x_i = \frac{P_i(\tau)}{Q_i(\tau)} \right\}$$

$$= \{x \in E^n \mid \text{existe } \tau \in E^m \text{ onde } Q_i(\tau)\, x_i - P_i(\tau) = 0 \text{ e } Q_i(\tau) \neq 0\}$$

$$= Proj_x Z(\mathbf{PS}/\mathbf{DS}) = \{e \in E^m \mid \exists\, a \in E^n \text{ tal que } (e,a) \in Z(\mathbf{PS}/\mathbf{DS})\}$$

Com o algoritmo para o cálculo de projeção apresentado em [9], podemos achar conjuntos de polinômios diferenciais $\mathcal{S}_i$ e polinômios diferenciais d_i, para $i = 1, \ldots, t$, tais que

$$\mathbf{IM}(P,Q) = \bigcup_{1 \le i \le t} Z(\mathcal{S}_i / \{d_i\})$$

seja válido. ■

Teorema 2.17 *Se $\mathcal{V}$ é uma variedade implícita do conjunto de EDRP's*

$$x_1 = \frac{P_1(U)}{Q_1(U)}, \ldots, x_n = \frac{P_n(U)}{Q_n(U)}$$

e de dimensão d, então:

(1) $\boldsymbol{IM}(P,Q) \subset \mathcal{V}$.

(2) A variedade $\mathcal{V}-\boldsymbol{IM}(P,Q)$ é uma quasi-variedade diferencial com dimensão menor do que ou igual a d, mas com ordem menor do que a ordem de $\mathcal{V}$.

(3) Podemos achar conjuntos autoreduzidos ascendentes irredutíveis $\mathcal{A}$ e $\mathcal{A}_i$ tais que

$$\boldsymbol{IM}(P,Q) = Z(\mathbf{SAT}(\mathcal{A})) - \bigcup_{i=1}^{k} Z(\mathcal{A}_i/J_iD_i)$$

onde $\mathbf{SAT}(\mathcal{A})$ é o ideal implícito do conjunto de EDRP's, os J_i são SI-produtos de $\mathcal{A}_i$ e os D_i são polinômios diferenciais. Em outras palavras, $\mathcal{V}$ é o fecho de $\boldsymbol{IM}(P,Q)$ (em relação à topologia de Zariski diferencial) em $\mathbb{A}_E^n$.

Demonstração. Seja $\mathcal{V}$ a variedade implícita (uniracional) do conjunto de EDRP's de dimensão d

$$x_1 = \frac{P_1(U)}{Q_1(U)}, \ldots, x_n = \frac{P_n(U)}{Q_n(U)} \text{ (representação paramétrica de } \mathcal{V})$$

A condição (1) é uma consequência do Lema 2.9 e a condição (2) segue de (3) e do Teorema da Dimensão Diferencial ([29], p.49). De acordo com isso, precisamos provar somente (3). Pelo Lema 2.16, podemos encontrar conjuntos $\mathcal{S}_k$ de polinômios diferenciais e polinômios diferenciais d_k, para $i = 1, \ldots, k$, em $K\{X\}$ tais que

$$\mathbf{IM}(P,Q) = \bigcup_{1 \le i \le k} Z(\mathcal{S}_k/\{d_k\}).$$

Pelo Teorema 2.5, podemos assumir ainda que

$$\mathbf{IM}(P,Q) = \bigcup_{k} Z(\mathcal{A}_k/\{d_kJ_k\}),$$

onde $\mathcal{A}_k$ são conjuntos autoreduzidos ascendentes irredutíveis e J_k são SI-produtos de $\mathcal{A}_k$. Se $\eta = \left(\frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n}\right)$, então $\eta \in \mathbf{IM}(P,Q)$. Como

$$\mathbf{IM}(P,Q) = \bigcup_{k} Z(\mathcal{A}_k/\{d_kJ_k\}),$$

obtemos $\eta \in Z(\mathcal{A}_k/\{d_kJ_k\})$, para algum k. Temos ainda que $\eta \in Z(\mathbf{SAT}(\mathcal{A}_k))$, pois $Z(\mathcal{A}_k/\{d_kJ_k\}) \subset Z(\mathbf{SAT}(\mathcal{A}_k)/\{d_kJ_k\})$ pelo Lema 2.10. Vamos mostrar

que a variedade implícita $\mathcal{V}$ do conjunto de $EDRP's$ é $Z(\mathbf{SAT}(\mathcal{A}_k))$. Por um lado, como do Lema 2.8 temos que η é um zero genérico de $\mathcal{V}$, segue que $\mathcal{V} \subset Z(\mathbf{SAT}(\mathcal{A}_k))$. Temos também que:

$$Z(\mathbf{SAT}(\mathcal{A}_k)/\{d_kJ_k\}) \overset{Lema\ 2.10}{=} Z(\mathcal{A}_k/\{d_kJ_k\}) \overset{Teo.\ 2.5}{\subset} \mathbf{IM}(P,Q) \overset{(1)}{\subset} \mathcal{V}$$

Por outro lado, tomando arbitrariamente um zero genérico ς de $\mathbf{SAT}(\mathcal{A}_k)$, uma vez que d_kJ_k não está no ideal diferencial primo $\mathbf{SAT}(\mathcal{A}_k)$, e portanto $d_k(\varsigma)J_k(\varsigma) \neq 0$, tem-se que $\varsigma \in \mathcal{V}$. Como ς foi tomado arbitrário, segue que $Z(\mathbf{SAT}(\mathcal{A}_k)) \subset \mathcal{V}$. Portanto, $\mathcal{V} = Z(\mathbf{SAT}(\mathcal{A}_k))$, e assim, por definição, $\mathbf{SAT}(\mathcal{A}_k)$ é o ideal implícito do conjunto de EDRP's. Por fim, vamos considerar as duas propriedades seguintes correlatas (ao caso diferencial) sobre variedades.

(i). Se $\{I_\alpha\}_{\alpha\in\Lambda}$ é qualquer coleção de ideais em $K[X_1,\ldots,X_n]$, então

$$\mathcal{Z}_K\left(\bigcup_{\alpha\in\Lambda} I_\alpha\right) = \bigcap_{\alpha\in\Lambda} \mathcal{Z}_K(I_\alpha).$$

Em particular, a intersecção de qualquer coleção de conjuntos algébricos é um conjunto algébrico.

Aqui, dados dois conjuntos $\mathcal{S}_1$ e $\mathcal{S}_2$ de polinômios diferenciais e $\mathcal{D}_1$ e $\mathcal{D}_2$ dois polinômios diferenciais, tem-se que:

$$Z(P\mathcal{S}_1 \cup P\mathcal{S}_2/\{\mathcal{D}_1\mathcal{D}_2\}) = Z(\mathcal{S}_1/\{\mathcal{D}_1\}) \cap Z(P\mathcal{S}_2/\{\mathcal{D}_2\}).$$

(ii). $Z(\mathcal{S}_1/\{\mathcal{D}_1\}) - Z(\mathcal{S}_2/\{\mathcal{D}_2\}) = \bigcup_{P\in\mathcal{S}_2} Z(\mathcal{S}_1/\{\mathcal{D}_1P\}) \cup Z(\mathcal{S}_1 \cup \{\mathcal{D}_2\}/\{\mathcal{D}_1\})$.

De acordo com estas considerações temos:

$$\begin{aligned}
\mathbf{IM}(P,Q) &= Z(\mathbf{SAT}(\mathcal{A}_k)/\{d_kJ_k\}) \bigcup \cup_{i\neq k} Z(\mathcal{A}_i/\{d_iJ_i\}) \\
&= [Z(\mathbf{SAT}(\mathcal{A}_k)) - Z(\{d_kJ_k\})] \bigcup \cup_{i\neq k} Z(\mathcal{A}_i/\{d_iJ_i\}) \\
&= Z(\mathbf{SAT}(\mathcal{A}_k)) - Z(\{d_kJ_k\}) - \cup_{i\neq k} Z(\mathcal{A}_i/\{d_iJ_i\}) \\
&= Z(\mathbf{SAT}(\mathcal{A}_k)) - [Z(\{d_kJ_k\}) - \cup_{i\neq k} Z(\mathcal{A}_i/\{d_iJ_i\})] \\
&\overset{\star}{=} Z(\mathbf{SAT}(\mathcal{A})) - \bigcup_{i=1}^{k} Z(\mathcal{A}_i/J_iD_i).
\end{aligned}$$

Portanto,

$$\mathbf{IM}(P,Q) = Z(\mathbf{SAT}(\mathcal{A})) - \bigcup_{i=1}^{k} Z(\mathcal{A}_i/J_iD_i)$$

A igualdade identificada por uma estrela (★) foi obtida fazendo uso das propriedades refereridas anteriormente, e assim, viabilizando mudança de

$$Z\left(\{d_k J_k\}\right) - \bigcup_{i \neq k} Z\left(\mathcal{A}_i / \{d_i J_i\}\right)$$

para a forma desejada $\bigcup_{i=1}^{k} Z\left(\mathcal{A}_i / J_i D_i\right)$. ■

Exemplo 2.18

Vamos calcular a imagem de EDRP's do exemplo 2.14 dadas por

$$\left\{ \begin{array}{rcl} x & = & u^2 \\ y & = & u' \end{array} \right.$$

Agora, usando o *método da projeção* em *Gao* e *Chou* temos:

$$\begin{aligned} \mathbf{IM}\left(P, Q\right) &= Z\left(\left\{4xy^2 - \left(x'\right)^2\right\} / \{xy\}\right) \cup Z\left(\{x', y\} / x\right) \cup Z\left(\{xy\}\right) \\ &= Z\left(\left\{4xy^2 - \left(x'\right)^2\right\} / \{xy\}\right) \cup Z\left(\{x', y\}\right) \end{aligned}$$

Então, pelo Teorema 2.17, podemos achar as seguintes representações canônicas:

$$\begin{aligned} \mathbf{IM}\left(P, Q\right) &= Z\left(\left\{4xy^2 - \left(x'\right)^2\right\} / \{xy\}\right) \cup Z\left(\{x', y\}\right) \\ &= Z\left(\left\{4xy^2 - \left(x'\right)^2\right\}\right) - \left[Z\left(\{xy\}\right) - Z\left(\{x', y\}\right)\right] \\ &= Z\left(\left\{4xy^2 - \left(x'\right)^2\right\}\right) - \left\{\left[Z\left(\{x\}\right) \cup Z\left(\{y\}\right)\right] - Z\left(\{x', y\}\right)\right\} \\ &= Z\left(\left\{4xy^2 - \left(x'\right)^2\right\}\right) - \left\{\left[Z\left(\{x\}\right) \cup Z\left(\{x'y\}\right)\right] - Z\left(\{x', y\}\right)\right\} \\ &= Z\left(\left\{4xy^2 - \left(x'\right)^2\right\}\right) - \left[Z\left(\{x\}\right) - Z\left(\{x', y\}\right)\right] \\ &= Z\left(\left\{4xy^2 - \left(x'\right)^2\right\}\right) - Z\left(\{x\} / \{y\}\right) \end{aligned}$$

Acima, usamos o fato $Z\left(\{y\}\right) = Z\left(\{x', y\}\right)$, que é válido sob a condição $4xy^2 - \left(x'\right)^2 = 0$.

Do exemplo acima, vemos que a imagem geralmente não é igual à variedade implícita.

2.4 Parâmetros Independentes

Os parâmetros $u_1, \ldots, u_m$ do conjunto de EDRP's são chamados *independentes* se o ideal implícito deste conjunto de EDRP's for de dimensão m ou, equivalentemente, o grau diferencial transcendente do corpo $K\left\langle \frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n} \right\rangle$ sobre K é m.

O próximo resultado nos fornece um meio de checarmos se determinados parâmetros são ou não independentes. Para tanto, vamos considerar a construção feita na secção 2 para $\mathcal{A}_k$, a saber,

$$A_1\left(x_1, \ldots, x_{d+1}\right), \ldots, A_{n-d}\left(x_1, \ldots, x_n\right),$$

$$B_1\left(x_1, \ldots, x_n, u_1, \ldots, u_{s+1}\right), \ldots, B_{m-s}\left(x_1, \ldots, x_n, u_1, \ldots, u_m\right),$$

e vamos designá-la por Ψ.

Lema 2.19 *Suponha que tenhamos construído Ψ. Então a dimensão de $\boldsymbol{ID}(P, Q)$ é $d = m - s > 0$, e portanto, os parâmetros são independentes se, e somente se, $s = 0$.*

Demonstração. A dimensão de um ideal primo é igual ao número de parâmetros de seu conjunto característico ([29]). Pelo Teorema 2.13, a dimensão do ideal implícito é $\mathbf{ID}(P, Q) = d = m - s$. ■

As vezes é desejável, ou mesmo necessário, que determinados parâmetros de um conjunto de EDRP's sejam *independentes*, mas nem sempre os são. O resultado que segue, nos assegura que podemos reparametrizar as EDRP's para que novas EDRP's possuam parâmetros independentes.

Teorema 2.20 *Se os parâmetros do conjunto de EDRP's*

$$x_1 = \frac{P_1\left(U\right)}{Q_1\left(U\right)}, \ldots, x_n = \frac{P_n\left(U\right)}{Q_n\left(U\right)}$$

não são independentes e $K = \mathbb{Q}(t)$ é o corpo de frações, então podemos achar o conjunto

$$x_1 = \frac{\overline{P_1}}{\overline{Q_1}}, \ldots, x_n = \frac{\overline{P_n}}{\overline{Q_n}}$$

de novas EDRP's que possui a mesma variedade implícita deste conjunto de EDRP's, porém com parâmetros independentes.

Demonstração. Suponha que o conjunto de EDRP's

$$x_1 = \frac{P_1\,(U)}{Q_1\,(U)}, \ldots, x_n = \frac{P_n\,(U)}{Q_n\,(U)}$$

tenha parâmetros não independentes e seja $K = \mathbb{Q}(t)$ o corpo de frações. Primeiramente, vamos mostrar que a partir deste conjunto de EDRP's com parâmetros não independentes, podemos achar um novo conjunto de EDRP's

$$x_1 = \frac{\overline{P_1}}{\overline{Q_1}}, \ldots, x_n = \frac{\overline{P_n}}{\overline{Q_n}}$$

mas agora com parâmetros independentes. Para isso, considere inicialmente o SI-produto $J = I_\Psi S_\Psi$ de Ψ designado anteriormente. Como Ψ é irredutível, por definição, tem-se que $f_r(I_\Psi S_\Psi, \Psi) \neq 0$. Pelo Lema 4 ([36], p.175), podemos achar um polinômio diferencial F não nulo, reduzido com Ψ e livre dos líderes dos polinômios diferenciais em Ψ tal que,

$$F \in [A_1, \ldots, A_{n-d}, B_1, \ldots, B_{m-s}, J].$$

Analogamente, uma vez que $f_r(Q_i, \Psi) \neq 0$, podemos encontrar um polinômio diferencial não nulo q_i, reduzido com Ψ e livre dos líderes dos polinômios diferenciais em Ψ tal que, $q_i \in [A_1, \ldots, A_{n-d}, B_1, \ldots, B_{m-s}, Q_i]$. Defina

$$M := F \prod_{j=1}^{n} q_j.$$

É claro que M assim definido é um polinômio diferencial livre dos líderes dos polinômios diferenciais em Ψ, pois F e q_i os são. Segue então que $M \notin \mathbf{SAT}\,(\Psi)$. Com efeito, pois pela definição de $\mathbf{SAT}\,(\Psi)$, a fim de que $P \in \mathbf{SAT}\,(\Psi)$, deve-se cumprir $JP \in [\Psi]$, sendo J um SI-produto. Mas tal J não pode ocorrer (devido sua definição), pois não há líderes em M. Agora, substituindo x_i por P_i/Q_i em M, obtemos uma *função diferencial racional* não nula N em u_i. Como $K = \mathbb{Q}(t)$, existem $h_1, \ldots, h_s$ em K tais que, quando substituirmos u_i por h_s, para cada $i = 1, \ldots, s$, tem-se que N torna-se um polinômio diferencial não-nulo $\overline{N}$ ([29], p.35). Sejam os polinômios diferenciais $\overline{P_i}$, $\overline{Q_i}$ e $\overline{B_i}$ obtidos de P_i, Q_i e B_i a partir da substituição de u_i por h_s, para cada $i = 1, \ldots, s$. Note que $\overline{P_i}$, $\overline{Q_i}$ e $\overline{B_i}$ envolvem somente $u_{s+1}, \ldots, u_m$. Assim, agora obtivemos o novo conjunto de EDRP's

$$x_1 = \frac{\overline{P_1}}{\overline{Q_1}}, \ldots, x_n = \frac{\overline{P_n}}{\overline{Q_n}}$$

e com parâmetros independentes. Como $\overline{N} \neq 0$, depois da substituição, Ψ ainda permanece sendo um conjunto autoreduzido ascendente, que é denotado por Ψ'. Finalmente, vamos mostrar que o conjunto com as novas EDPR's obtidas possui a mesma variedade implícita do conjunto de EDRP's inicial. Considerando então que W e V sejam as variedades implícitas definidas, respectivamente, por

$$x_1 = \frac{P_1(U)}{Q_1(U)}, \ldots, x_n = \frac{P_n(U)}{Q_n(U)} \text{ e } x_1 = \frac{\overline{P_1}}{\overline{Q_1}}, \ldots, x_n = \frac{\overline{P_n}}{\overline{Q_n}},$$

devemos provar que $W = V$. Por um lado, pela seleção feita de h_i, é claro que $W \subset V$. Por outro lado, tome $\phi = (\alpha_1, \ldots, \alpha_n)$ um zero genérico de V. Como feito acima, substituindo-se x_i por α_i em $\overline{B_i}$ obtemos $\widehat{B_i}$. Pela seleção de h_i, os SI-produtos de $\widehat{B_i}$ são não nulos. Daí, pelo Teorema da Projeção ([11], Lema 3.5), existem soluções h_i para u_i, com $i = s+1, \ldots, m$, de $\widehat{B_i} = 0$, que não anula M, e então, nem Q_i e nem os inicial e separante de B_i. Seja agora $\xi = (\alpha_1, \ldots, \alpha_n, h_1, \ldots, h_m)$. Temos que $M(\xi) \neq 0$ e isto implica que $Q(\xi) \neq 0$ e $J(\xi) \neq 0$. Como $F_i = P_i - x_i Q_i \in \mathbf{SAT}(\Psi)$, existe por definição um SI-produto L de Ψ tal que, $LF_i \in [\Psi]$. Então $L(\xi) F_i(\xi) = 0$. Ora, mas de $J(\xi) \neq 0$ temos que $L(\xi) \neq 0$, e assim, segue que $P_i(\xi) - \alpha_i Q_i(\xi) = F_i(\xi) = 0$. Daí, tem-se que $\alpha_i = \frac{P_i(\xi)}{Q_i(\xi)}$ e $\phi \in W$. Portanto, $W = V$. ■

Exemplo 2.21

Consideremos as seguintes EDRP's

$$\begin{cases} x &= u^2 + 2uv^2 + v^4 \\ y &= u' + 2vv' \end{cases}$$

Seja $\mathcal{S} = \{x - u^2 - 2uv^2 - v^4, y - u' - 2vv'\}$. Com a ordenação

$$y < x < v < u$$

nas variáveis, pelo Teorema de Decomposição dos Zeros de Wu-Ritt (Teorema 2.5), tem-se que

$$\begin{aligned} Z(S) &= Z\left(\left\{(x')^2 - 4xy^2, 2y(u - v^2) - x'\right\} / \{x'y\}\right) \cup \\ &\quad \cup Z\left(\left\{y, x', (u - v^2)^2 - x\right\} / \{u - v^2\}\right) \cup Z\left(\{y, x, u - v^2\}\right). \end{aligned}$$

Usando o Lema 2.12, podemos checar que

$$(x')^2 - 4xy^2 \qquad \text{e} \qquad 2y\left(u - v^2\right) - x'$$

é um conjunto autoreduzido correspondente à Ψ (designação do conjunto autoreduzido $\mathcal{A}_k$ feita anteriormente). Pelo Lema 2.19, podemos checar que os paraâmetros u e v não são independentes. O SI-produto para conjunto autoreduzido acima é $J = x'y$. Para elimanarmos x' de J com $(x')^2 - 4xy^2$ temos que $F = 4xy^4$. Para acharmos o conjunto de parâmetros independentes, precisamos somente escolher um valor para v tal que o seguinte não seja zero:

$$F = 4xy^4 = 4\left(\underbrace{u^2 + 2uv^2 + v^4}_{=x}\right)\left(\underbrace{u' + 2vv'}_{=y}\right)^4$$

Escolhamos $v = 0$. Assim, as EDRP's

$$\begin{cases} x &= u^2 + 2uv^2 + v^4 \\ y &= u' + 2vv' \end{cases}$$

dadas inicialmente tornam-se as EDRP's

$$\begin{cases} x &= u^2 \\ y &= u' \end{cases}$$

do exemplo anterior, com parâmetro independente.

2.5 Inversão de Mapas e Equações Paramétricas Próprias

Dado um conjunto de EDRP's, nossa preocupação agora é a de responder o *problema da inversão*, isto é, obter um meio de calcular os *mapas inversos* de um dado conjunto de EDRP's.

O problema da inversão é o seguinte. Dado um ponto $(a_1, \ldots, a_n)$ na imagem do conjunto de EDRP's, devemos encontrar o conjunto de valores $(\tau_1, \ldots, \tau_m)$ para u tais que, para $i = 1, \ldots, n$,

$$a_i = \frac{P_i(\tau_1, \ldots, \tau_m)}{Q_i(\tau_1, \ldots, \tau_m)}$$

Esse problema pode ser reduzido à resolução de um problema de uma equação diferencial. A seguir, mostramos que em certos casos, podemos achar uma solução de forma fechada para o problema da inversão.

Os *mapas inversos* para EDRP's são funções dos x_i e suas derivadas

$$u_1 = f_1(x_1, \ldots, x_n), \ldots, u_m = f_m(x_1, \ldots, x_n),$$

tais que o que segue torna-se uma identidade quando substituindo x_i por $\frac{P_i}{Q_i}$:

$$x_i \equiv \frac{P_i\left(f_1,\ldots,f_m\right)}{Q_i\left(f_1,\ldots,f_m\right)}$$

O problema da inversão está fortemente ligado ao fato das equações paramétricas serem próprias.

Definição 2.22 *Dizemos que as equações diferenciais racionais paramétricas de um conjunto de EDRP's são próprias (ou que um conjunto de EDRP's é próprio), se para um zero genérico $(a_1,\ldots,a_n)$ (e assim a maioria dos pontos) da variedade implícita, existe somente um $(\tau_1,\ldots,\tau_m)$ em E^m tal que, para $i=1,\ldots,n$,*

$$a_i = \frac{P_i\left(\tau_1,\ldots,\tau_m\right)}{Q_i\left(\tau_1,\ldots,\tau_m\right)}$$

Pelo Teorema 2.20, podemos assumir que os parâmetros $u_1,\ldots,u_m$ do conjunto de EDRP's sejam idependentes, isto é, $s=0$. Então Ψ (definido na seção anterior) torna-se (fazendo $d=m$ em Ψ, pois $s=0$)

$$A_1\left(x_1,\ldots,x_{m+1}\right),\ldots,A_{n-m}\left(x_1,\ldots,x_n\right),$$

$$B_1\left(x_1,\ldots,x_n,u_1\right),\ldots,B_m\left(x_1,\ldots,x_n,u_1,\ldots,u_m\right),$$

que representaremos por Υ. As equações $B_1=0,\ldots,B_m=0$ são equações diferenciais em u_i, respectivamente. Uma vez que este "novo" Ψ é um conjunto característico de **SAT** (**PS**), uma solução de $B_i=0$ que não anula o SI-produto de nosso "novo" Ψ é uma solução de u_i em termos de x_i, e pode ser tratado como um conjunto de mapas inversos.

Usando as notações acima, o resultado que segue nos mostra que podemos obter, em certos casos, uma representação explícita para os mapas inversos.

Teorema 2.23 *O conjunto de EDRP's é próprio se, e somente se, $B_i = I_iu_i - U_i$ são lineares em u_i, para $i=1,\ldots,m$, e se este for o caso, os mapas inversos são*

$$u_1 = \frac{U_1}{I_1},\ldots,u_m = \frac{U_m}{I_m}$$

onde I_i e U_i são polinômios diferenciais em $K\{X\}$.

Demonstração. Primeiramente note que os B_i são as relações entre x e $u_1,\ldots,u_i$ que possuem a menor ordem e grau em u_i. Como Υ é um conjunto

autoreduzido ascendente irredutível, para um zero genérico η da variedade implícita $\mathcal{V}$, $B_i(\eta, u_1, \ldots, u_i)$ para $i = 1, \ldots, m$, sempre possui raízes múltiplas para os u_i se B_i não for linear em u_i. Portanto, um ponto $x \in \mathbf{IM}(P, Q)$ corresponde a um conjunto de valores para u_i se, e somente se, os B_i forem lineares em u_i, para $i = 1, \ldots, m$. Seja $B_i = I_i u_i - U_i$ onde I_i e U_i estão em $K\{X\}$ então as mapas inversos são $u_i = \dfrac{U_i}{I_i}$, para $i = 1, \ldots, m$. ■

Se um conjunto de EDRP's com parâmetros independentes for próprio, estas EDRP's e seus mapas inversos geram um *isomorfismo diferencial biracional* entre a variedade implícita e o *espaço diferencial afim* $\mathbb{A}^m_K$. Neste caso, a variedade implícita é chamada *racional*. O teorema clássico de Lüroth no caso algébrico diz que aquelas variedades uniracionais de dimensão 1 são sempre racionais ([33]). Ritt provou a seguinte versão do Teorema de Lüroth no caso diferencial ([29], página 52).

Lema 2.24 *Se u é uma indeterminada e F um corpo diferencial tal que, $K \subset F \subset K\langle u \rangle$, então existe $v \in K\langle u \rangle$ tal que, $F = K\langle v \rangle$. Mais ainda, u é um zero genérico de um ideal primo $\mathcal{I} \subset F[y]$. Além disso, se $\mathcal{I} = \mathbf{SAT}(\{f(y)\})$, para algum polinômio difrerencial irredutível*

$$f(y) = a_r D_1 + \cdots + a_1 D_r + a_0$$

onde $a_i \in F \subset K\langle u \rangle$ e com os D_i como produtos de derivadas de y, então um dos elementos $\dfrac{a_s}{a_r}$ não está em K e temos que $F = K\left\langle \dfrac{a_s}{a_r} \right\rangle$.

De posse deste lema, vamos ao teorema final que nos fornece um método para encontrar uma reparametrização própria para EDRP's impróprias.

Teorema 2.25 *Se $m = 1$ e o conjunto de $EDRP_s$ não é próprio, podemos achar um novo parâmetro $s = \dfrac{f(u_1)}{g(u_1)}$, onde f e g estão em $K\{u_1\}$ e tais que, a reparametrização do conjunto de EDRP's em termos de s,*

$$x_1 = \frac{F_1(s)}{G_1(s)}, \ldots, x_n = \frac{F_n(s)}{G_n(s)}$$

sejam próprias.

Demonstração. Defina o corpo diferencial

$$K_0 := K\left\langle \frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n} \right\rangle$$

adicionando a K os elementos $\frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n}$ (veja [29]). Ou seja, K_0 é o conjunto de todas as funções racionais em $\frac{P_i}{Q_i}$ e as suas derivadas, com coeficientes em K. Como $P_1(u_1) - Q_1(u_1)\, l = 0$, onde $l = \frac{P_1(u_1)}{Q_1(u_1)} \in K_0$, temos que u_1 satisfaz uma equação diferencial algébrica sobre K_0. Seja I um ideal primo em $K_0\{w\}$, com u_1 um zero genérico e $\{f\}$ o conjunto característico para I. Escreva f na forma

$$f(w) = a_r D_1 + \cdots + a_1 D_r + a_0,$$

onde $a_i \in K_0$ e os D_i sendo produtos de derivadas de w. Pelo Lema 2.24, ao menos um dos $\frac{a_i}{a_r}$, digamos $\eta = \frac{a_s}{a_r}$, não está em K e $K_0 = K(\eta)$. Isto significa que $x_i = \frac{P_i}{Q_i}$ pode ser expresso como funções racionais em η e suas derivadas, e com η também podendo ser expresso como uma função racional de $\frac{P_i}{Q_i}$ e suas derivadas. Em outras palavras, existe uma correspondência biunívoca entre os valores de $x_i = \frac{P_i}{Q_i}$ e η. Portanto, η é o novo parâmetro que procuramos. Para calcularmos η, basta tomarmos $B_i(x_1, \ldots, x_n, u_1) = 0$ como sendo o polinômio diferencial de Υ. Então,

$$\overline{B_1}(w) = B_1\left(\frac{P_1}{Q_1}, \ldots, \frac{P_n}{Q_n}, w\right) = 0$$

é um polinômio diferencial em $K_0\{w\}$ de menor ordem e grau em w tal que, $B_1(u_1) = 0$, isto é, $B_1(w)$ pode ser tomado como $f(w)$. De acordo com isso, s pode ser obtido como segue. Se B_1 for linear em u_1, não há nada a ser feito. Caso contrário, suponha que

$$B_1 = b_r D_1 + \cdots + b_1 D_r + b_0,$$

onde b_i está em $K\{X\}$ e os $D_i's$ sendo produtos das derivadas de u_1. Substituindo x_i por $\frac{P_i}{Q_i}$, vem que b_i torna-se um elemento $a_i(u_1)$ em K_0. Pelo menos um dos $\frac{a_i}{a_r}$, digamos $\frac{a_0}{a_r}$, não está em K. Seja $s = \frac{a_0}{a_r}$. Novamente pelo Lema 2.24 temos que $x_i = \frac{P_i}{Q_i}$ pode ser expresso como funções racionais em s e suas derivadas. Eliminando-se u_1 das EDRP's

$$x_1 = \frac{P_1(U)}{Q_1(U)}, \ldots, x_n = \frac{P_n(U)}{Q_n(U)}$$

$a_r s - a_0$, obtemos $R_i = Q_i' x_i - P_i'$ que deve ser linear em x_i. Portanto, obtemos a reparametrização do conjunto de $EDRP_s$ em termos de s,

$$x_1 = \frac{F_1(s)}{G_1(s)}, \ldots, x_n = \frac{F_n(s)}{G_n(s)}.$$

Note que a_i surge de b_i substituindo-se x_j por $\dfrac{P_j}{Q_j}$, com $j = 1, \ldots, n$, e então $s = \dfrac{b_0}{b_r}$ é um mapa inverso de

$$x_1 = \frac{F_1(s)}{G_1(s)}, \ldots, x_n = \frac{F_n(s)}{G_n(s)}.$$

■

Exemplo 2.26

Consideremos as seguintes EDRP's

$$\begin{cases} x &= u^4 \\ y &= 2uu' \end{cases}$$

Seja $\mathcal{S} = \{x - u^4, y - 2uu'\}$. Sob a ordenação $x < y < u$ nas variáveis, pelo Teorema de Decomposição dos Zeros de Wu-Ritt (Teorema 2.5), tem-se que

$$\begin{aligned} Z(\mathcal{S}) &= Z\left(\left\{4xy^2 - (x')^2, 2yu^2 - x'\right\} / \{xy\}\right) \cup \\ &\quad \cup Z(\{x', y, u^4 - x\} / \{u\}) \cup Z(\{x, y, u\}) \end{aligned}$$

Como $2yu^2 - x'$ não é linear em u, pelo Teorema 2.23 as EDRP's

$$\begin{cases} x &= u^4 \\ y &= 2uu' \end{cases}$$

não são próprias. Um mapa inverso poderia ser $u = \sqrt{\dfrac{x'}{2y}}$. Para acharmos EDRP's próprias, pelo Teorema 2.25 temos que

$$\overline{B_1} = 2yw^2 - x' = 4uu'w^2 - 4u^3u'.$$

Podemos selecionar novos parâmetros $s = \dfrac{4u^3u'}{4uu'} = u^2$. Eliminando-se u de $s = u^2$ e das EDRP's consideradas no início, obtemos um novo conjunto de equações paramétricas, a saber,

$$\begin{cases} x &= s^2 \\ y &= s' \end{cases}$$

possuindo o mesmo ideal implícito que das referidas EDRP's consideradas no início e é próprio. O que são na verdade as EDRP's

$$\begin{cases} x &= u^2 \\ y &= u' \end{cases}$$

do exemplo dado a pouco. O mapa inverso para este conjunto de equações paramétricas próprias é $s = \dfrac{x'}{2y}$, que tem um significado para aqueles pontos da imagem satisfazendo $y \neq 0$.

Capítulo 3

Implicitização de Sistemas de EQDP's Paramétricas

Vamos agora estudar a implicitização de equações diferenciais polinomiais paramétricas lineares via resultantes diferenciais. Assim, os métodos de resolução dos problemas presentes neste capítulo serão realizados com uma abordagem diferente ao feito no capítulo precedente, em que os métodos algorítmicos empregados para resolver os problemas propostos foram abordados via conjuntos característicos. É neste capítulo que se encontra o resultado principal desta dissertação, a saber, a determinação de uma fórmula explícita da resultante diferencial em termos da resultante diferencial homogênea.

3.1 Parametrizações e Implicitizações de Variedades

A Álgebra Computacional é um assunto da ciência da computação dedicada a métodos de resolução de problemas utilizando algoritmos simbólicos formulados matematicamente, bem como à execução destes algoritmos através de softwares e hardwares.

Conjuntos algébricos podem ser apresentados de duas formas, a saber, através de equações paramétricas ou, de maneira implícita como um conjunto de soluções de equações cartesianas. Cada maneira tem suas vantagens. A implicitização é o processo de passar da primeira forma à segunda, sendo de certo modo, complementar à teoria de eliminação. Vamos olhar para as duas representações de um conjunto algébrico mencionadas, a saber, a parametrização e a implicitização. Comecemos pela parametrização.

Uma das preocupações da geometria algébrica é a de descrever os pontos

de uma variedade afim $\mathcal{V}$. Isso reduz a perguntar se existe uma maneira de "escrever"as soluções do sistema de equações polinomiais $f_1 = \cdots = f_s = 0$. Quando há um número finito de soluções, o objetivo é simplesmente enumerá-las. Mas o que fazer quando há uma infinidade delas? Como veremos, esta questão leva à noção de parametrizar uma variedade afim.

Para começar, vamos olhar para um exemplo de álgebra linear. Considere o seguinte sistema de equações com coeficientes reais:

$$S_1 := \begin{cases} x + y + z = 1 \\ x + 2y - z = 3 \end{cases}$$

Geometricamente, o sistema S_1 representa uma reta em $\mathbb{R}^3$, que é a intersecção dos planos

$$\Pi_1 : x + y + z = 1 \quad \text{e} \quad \Pi_2 : x + 2y - z = 3.$$

O sistema possui infinitas soluções. Para descrevê-las, uma das técnicas é usarmos operações nas linhas da matriz do sistema para obter as equações equivalentes $x + 3z = -1$ e $y - 2z = 2$. Assim, podemos utilizar z como parâmetro. Fazendo $z = t$, obtemos todas as soluções de S_1 quando fazemos t variar em $\mathbb{R}$, a saber,

$$S_2 := \begin{cases} x &= -1 - 3t \\ y &= 2 + 2t \\ z &= t \end{cases}$$

O sistema S_2 é, uma *parametrização* das soluções de S_1.

É bom destacar que uma parametrização pode não descrever toda a variedade $\mathcal{V}$, em outras palavras, pode não cobrir todos os pontos de $\mathcal{V}$. Com efeito, por exemplo, considere o círculo unitário

$$C : x^2 + y^2 = 1.$$

Uma maneira algébrica de parametrizá-la (veja [13] capítulo 1, § 3) é

$$T_C := \begin{cases} x = \dfrac{1 - t^2}{1 + t^2} \\ \\ y = \dfrac{2t}{1 + t^2} \end{cases}$$

Note que esta parametrização, de fato, não descreve todo o círculo, pois desde que $x = \dfrac{1-t^2}{1+t^2}$ não pode assumir valor -1, o ponto $(-1, 0)$ (que está em C) não é coberto.

Observe que as equações de T_C envolvem quocientes de polinômios. Estes são exemplos de funções racionais.

Lembremos que uma *função racional* nas variáveis $t_1, \ldots, t_m$, com coeficientes em K, é um quociente $\dfrac{P}{Q}$ de dois polinômios $P, Q \in K[t_1, \ldots, t_m]$, onde Q é não nulo. Naturalmente o conjunto das funções racionais em $t_1, \ldots, t_m$ com coeficientes em K é um corpo, denominado *corpo das funções racionais*, e o denotamos por $K(t_1, \ldots, t_m)$.

Dada uma variedade algébrica $\mathcal{V}$ em K^n, uma *representação paramétrica racional* de $\mathcal{V}$ consiste de funções racionais $\dfrac{f_1}{g_1}, \ldots, \dfrac{f_n}{g_n} \in K(t_1, \ldots, t_m)$ tais que, os pontos dados por

$$\begin{cases} x_1 &= \dfrac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \\ &\vdots \\ x_n &= \dfrac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)}, \end{cases} \tag{3.1}$$

onde $f_1, g_1, \ldots, f_n, g_n$ são polinômios em $K[t_1, \ldots, t_m]$, com $g_i \neq 0$, estão em $\mathcal{V}$. Geometricamente, uma representação paramétrica racional de $\mathcal{V}$ pode ser vista como um mapa $F : K^m \longrightarrow K^n$, definido por (3.1). É claro que os pontos em (3.1) podem não estar definidos em todo K^m devido aos denominadores. Mas, se temos $\mathcal{W} = \mathcal{Z}_K(g_1 g_2 \cdots g_n) \subset K^m$, então é claro que

$$F(t_1, \ldots, t_m) = \left(\frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)}, \ldots, \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)} \right)$$

define um mapa $F : K^m - \mathcal{W} \longrightarrow K^n$. Assim, para resolvermos o problema da implicitização, devemos determinar a menor variedade de K^n contendo $F(K^m - \mathcal{W})$. Em particular, quando $r_1 := \dfrac{f_1}{g_1}, \ldots, r_n := \dfrac{f_n}{g_n}$ são polinômios, temos uma *representação paramétrica polinomial* de $\mathcal{V}$

$$\begin{cases} x_1 &= r_1(t_1, \ldots, t_m), \\ &\vdots \\ x_n &= r_n(t_1, \ldots, t_m) \end{cases} \tag{3.2}$$

onde $r_1, \ldots, r_s$ são polinômios em $K[t_1, \ldots, t_m]$. Novamente, podemos pensar geometricamente em um mapa $F : K^m \longrightarrow K^n$, definido por

$$F(t_1, \ldots, t_m) = (r_1(t_1, \ldots, t_m), \ldots, r_n(t_1, \ldots, t_m)).$$

Assim, temos que $F(K^m) \subset K^n$ é o subconjunto de K^n parametrizado pelas equações de (3.2). Como $F(K^m)$ pode não ser uma variedade afim (veja exercícios da página 135 em [13]), uma solução do problema da implicitização significa então encontrar a menor variedade afim que contém $F(K^m)$.

Visto que uma parametrização pode não cobrir todos os pontos de $\mathcal{V}$ (como bem mostra o exemplo do círculo), salientamos a exigência de que $\mathcal{V}$ seja a "menor"variedade que contém esses pontos.

Uma das principais virtudes de uma representação paramétrica de uma curva ou superfície é a de ser fácil de se representar graficamente em um computador. Com efeito, dadas as equações da parametrização, usando meios computacionais, avalia-se os pontos para vários valores do parâmetro. Por exemplo, a variedade afim $\mathcal{V} = \mathcal{Z}_{\mathbb{R}}(x^2 - y^2z^2 + z^3) \subset \mathbb{R}^3$ que se auto-intercecta ao longo do eixo y, pode ser plotada fazendo uso da seguinte representação paramétrica:

$$T := \begin{cases} x &= t(u^2 - t^2) \\ y &= u \\ z &= u^2 - t^2 \end{cases}$$

Por outro lado, às vezes é útil ter efetivamente as equações cartesianas $f_1 = \cdots = f_s = 0$ que definem a variedade $\mathcal{V}$. Estas são denominadas *representação implícita* de $\mathcal{V}$. Por exemplo, suponha que desejamos saber se o ponto $P := P(1, 2, -1)$ é coberto pela superfície $\mathcal{V} = \mathcal{Z}_{\mathbb{R}}(x^2 - y^2z^2 + z^3)$. Neste caso, se temos apenas a parametrização T, é necessário resolver, em t e u, as equações

$$\begin{aligned} 1 &= t(u^2 - t^2), \\ 2 &= u, \\ -1 &= u^2 - t^2. \end{aligned}$$

Ora, se temos a representação implícita $x^2 - y^2z^2 + z^3 = 0$, o trabalho é simplesmente uma avaliação desta equação no ponto P. Assim, uma vez que

$$1^2 - 2^2(-1)^2 + (-1)^3 = 1 - 4 - 1 = -4 \neq 0,$$

segue que P não está na superfície.

O desejo de termos os dois tipos de representações leva às seguintes duas perguntas:

1. *Parametrização*: Será que toda variedade afim tem uma representação paramétrica racional?

2. *Implicitização*: Dada uma representação paramétrica de uma variedade afim, podemos sempre encontrar as suas equações de definição (ou seja, podemos encontrar uma representação implícita)?

A resposta à primeira pergunta é não. Na verdade, a maioria das variedades afins não podem ser parametrizadas no sentido descrito aqui. As que podem, são chamadas de *uniracionais*. Em geral, é difícil decidir se uma determinada variedade é uniracional ou não. A situação para a segunda questão é muito mais agradável, ou seja, dada uma representação paramétrica, podemos sempre encontrar as suas equações de definição. Com efeito, o conjunto de superfícies racionais é um subconjunto do conjunto das superfícies algébricas. Assim, cada superfície racional paramétrica tem uma representação correspondente implícita e, por definição, o processo de conversão de paramétrico para implícita é conhecido como implicitização.

Agora, antes de tratarmos da implicitização, vamos fazer alguns comentários sobre a *Teoria de Eliminação*.

A teoria de eliminação estuda métodos sistemáticos para eliminar variáveis de sistemas de equações polinomiais. Em particular, a estratégia básica desta teoria concentra-se em torno de dois teoremas, a saber, o *Teorema de Eliminação* e o *Teorema de Extensão*. Em especial, o problema de implicitização é uma das muitas aplicações da teoria de eliminação. Fazendo uso da linguagem desta teoria, podemos ver que a eliminação das variáveis $X_1, \ldots, X_l$ significa encontrar polinômios não nulos no *l-ésimo ideal de eliminação* I_l, conforme definição que segue:

Definição 3.1 *Dado* $I = \langle f_1, \ldots, f_s \rangle \subset K[X_1, \ldots, X_n]$*, o l-ésimo ideal de eliminação é o ideal de* $K[X_{l+1}, \ldots, X_n]$*, definido por*

$$I_l = I \cap K[X_{l+1}, \ldots, X_n].$$

Teorema 3.1 (*Teorema de Eliminação*) *Se* $I \subset K[X_1, \ldots, X_n]$ *é um ideal e* G *uma base de Gröbner de* I *em relação à ordem lex, onde*

$$X_1 > X_2 > \cdots > X_n,$$

então, para cada $0 \leq l \leq n$*, o conjunto*

$$G_l = G \cap K[X_{l+1}, \ldots, X_n]$$

é uma base de Gröbner do l-ésimo ideal de eliminação I_l*.*

Para uma demonstração deste teorema, veja a referência [13], pg 116.

Este teorema mostra que uma base de Gröbner (veja a definição em [21]) para a ordem lex, não elimina apenas a primeira variável, mas também as duas primeiras variáveis, as três primeiras variáveis, ...

Em alguns casos (como no problema da implicitização) temos apenas que eliminar certas variáveis, sem nos preocupar com as demais. Agora, fixado algum l entre 1 e n, obtemos um ideal de eliminação I_l e chamamos uma solução $(a_{l+1}, \ldots, a_n) \in \mathcal{Z}_K(I_l)$ de uma *solução parcial* do sistema original de equações. Para estender $(a_{l+1}, \ldots, a_n)$ a uma solução completa em $\mathcal{Z}_K(I)$, primeiramente precisamos adicionar mais uma coordenada para a solução. Em outras palavras, isto significa encontrar a_l de modo que pertença a variedade $\mathcal{Z}_K(I_{l-1})$ do próximo ideal de eliminação. Mais especificamente, se $I_{l-1} = \langle g_1, \ldots, g_r \rangle$ em $K[X_l, X_{l+1}, \ldots, X_n]$, então buscamos encontrar as soluções $X_l := a_l$ das equações

$$g_1(X_l, a_{l+1}, \ldots, a_n) = \cdots = g_r(X_l, a_{l+1}, \ldots, a_n) = 0.$$

Se restringirmos nossa atenção para o caso em que eliminamos apenas a primeira variável X_1, então buscaremos determinar se uma solução parcial $(a_2, \ldots, a_n) \in \mathcal{Z}_K(I_1)$ pode ser estendida a uma solução $(a_1, a_2, \ldots, a_n) \in \mathcal{Z}_K(I)$. O teorema que segue nos diz quando isso pode ser feito (sua demonstração pode ser encontrada em [13], página 118).

Teorema 3.2 (*Teorema de Extensão*) *Dado* $I = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[X_1, \ldots, X_n]$*, seja* I_1 *o primeiro ideal de eliminação de* I*. Para cada* $1 \leq i \leq s$*, escreva* f_i *sob a forma*

$$f_i = g_i(X_2, \ldots, X_n) X_1^{N_i} + (\textit{termos em que } gr(X_1) < N_i),$$

onde $N_i \geq 0$ *e* $g_i \in \mathbb{C}[X_2, \ldots, X_n]$ *não nulo. Suponha que tenhamos uma solução parcial* $(a_2, \ldots, a_n) \in \mathcal{Z}_K(I_1)$*. Se* $(a_2, \ldots, a_n) \notin \mathcal{Z}_K(g_1, \ldots, g_s)$*, então existe* $a_1 \in \mathbb{C}$ *tal que,* $(a_1, a_2, \ldots, a_n) \in \mathcal{Z}_K(I)$*.*

Feitas estas considerações em relação à teoria de eliminação, vamos agora à implicitização. A idéia básica do problema da implicitização é converter a parametrização para obter equações que definem uma variedade $\mathcal{V}$. O nome

"implicitização"vem das equações que definem a variedade $\mathcal{V}$, que foram chamadas de representação implícita de $\mathcal{V}$. Como foi observado, uma parametrização não precisa de encher toda a variedade $\mathcal{V}$ (veja em [13] o exemplo da parametrização do círculo). É devido a isto que, para o problema da implicitização, pede-se as equações que definem a menor variedade $\mathcal{V}$ contendo a parametrização.

Teorema 3.3. (*Implicitização Polinomial*) *Suponha que K seja um corpo infinito e considere $F : K^m \longrightarrow K^n$ uma função determinada pela parametrização polinomial. Considere o ideal*

$$I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle \subset K[t_1, \ldots, t_m, x_1, \ldots, x_n]. \tag{3.3}$$

Se $I_m = I \cap K[x_1, \ldots, x_n]$ é o m-ésimo ideal de eliminação, então $\mathcal{V} = \mathcal{Z}_K(I_m)$ é a menor variedade em K^n contendo $F(K^m)$.

Para uma demonstração, veja [13], página 130.

Este teorema, que faz uso da teoria da eliminação para encontrar a menor variedade contendo $F(K^m)$, nos fornece o seguinte algoritmo:

Algoritmo de Implicitização para Parametrizações Polinomiais

Se temos $x_i = f_i(t_1, \ldots, t_m)$ para polinômios $f_1, \ldots, f_n \in K[t_1, \ldots, t_m]$, considere o ideal $I = \langle x_1 - f_1, \ldots, x_n - f_n \rangle$ e calcule uma *base Gröbner* com respeito a uma ordenação lexicográfica, onde cada t_i é superior a todos os x_i. Pelo *Teorema da Eliminação*, os elementos da base de Gröbner não envolvendo t_i formam uma base de I_m, e pelo teorema precedente, definem a menor variedade em K^n contendo a parametrização.

O próximo passo é, mais geralmente, ver o que acontece quando temos uma parametrização por funções racionais não polinomiais. Assim, como no caso polinomial, podemos agora usar a teoria da eliminação para resolver o problema da implicitização.

Teorema 3.4 (*Implicitização Racional*) Seja K um corpo infinito e considere $F : K^m - \mathcal{W} \longrightarrow K^n$, uma função determinada pela parametrização racional. Considerando o ideal

$$J = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy \rangle \subset K[y, t_1, \ldots, t_m, x_1, \ldots, x_n],$$

onde $g = g_1 g_2 \cdots g_n$, se $J_{m+1} = J \cap K[x_1, \ldots, x_n]$ é o $(m+1) - ésimo$ ideal de eliminação, então $\mathcal{V} = \mathcal{Z}_K(J_{m+1})$ é a menor variedade em K^n contendo $F(K^m - \mathcal{W})$.

Para uma demonstração desse teorema veja [13] página 134.

Este teorema nos fornece o seguinte algoritmo:

Algoritmo de Implicitização para Parametrizações Racionais

Se temos $x_i = f_i/g_i$ para polinômios $f_1, g_1, \ldots, f_n, g_n \in K[t_1, \ldots, t_m]$, considere a nova variável y e o ideal $J = \langle g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy \rangle$, onde $g = g_1 g_2 \cdots g_n$. Calculando uma base Gröbner em relação a uma ordenação lexicográfica, onde y e cada t_i é superior a todos os x_i, então os elementos da base de Gröbner não envolvendo y e qualquer t_i definem a menor variedade em K^n contendo a parametrização.

3.2 Equação Implícita de um Sistema Linear de EDPP's

Vamos iniciar o nosso estudo definindo o que é uma equação implícita de um sistema $(n-1)$-dimensional de equações diferenciais polinomiais paramétricas (EDPP's). Para ilustrar comecemos com um exemplo.

Exemplo 3.1

Considere os sistemas

$$\mathcal{S}_1 := \left\{ \begin{array}{rcl} x_1 & = & u_1 + u_{11} + u_2 + u_{21} \\ x_2 & = & t(u_{11} + u_{12}) + u_{22} \\ x_3 & = & u_1 + u_{11} + u_{21} \end{array} \right. \quad \mathcal{S}_2 := \left\{ \begin{array}{rcl} x_1 & = & u_1 + u_2 + u_{21} \\ x_2 & = & tu_{11} + u_{22} \\ x_3 & = & u_1 + u_{21} \end{array} \right. ,$$

onde $u_{jk} = \dfrac{\partial^k u_j}{\partial t^k}$, para $j \in \{1, 2\}$ e $k \in \mathbb{N}$, iremos buscar responder se são sistemas próprio, qual é a resultante diferencial, quem é a equação implícita e bem como se há alguma relação entre estes sistemas. Em particular, o sistema $\mathcal{S}_1$ não é próprio, mas sua equação implícita, dada por

$$(t-1)x_{12} - tx_{31} - (t-1)x_{32} + x_2 = 0,$$

onde $x_{ik} = \dfrac{\partial^k x_i}{\partial t^k}$, para $i \in \{1, 2, 3\}$ e $k \in \mathbb{N}$, é igual a equação implícita do sistema $\mathcal{S}_2$, e a resultante diferencial das equações $\{F_1, F_2, F_3\}$ é nula, onde

$$\begin{array}{rcl} F_1 & = & x_1 - u_1 - u_{11} - u_2 - u_{21} \\ F_2 & = & x_2 - t(u_{11} + u_{12}) - u_{22} \\ F_3 & = & x_3 - u_1 - u_{11} - u_{21} \end{array}$$

Dado um conjunto de indeterminadas diferenciais $U = \{u_1, \ldots, u_m\}$, para polinômios diferencias não nulos $P_1, \ldots, P_n, Q_1, \ldots, Q_n$ em $K\{U\}$, conforme definido no capítulo precedente, chamamos

$$x_1 = \frac{P_1(U)}{Q_1(U)}, \ldots, x_n = \frac{P_n(U)}{Q_n(U)}$$

de um conjunto de equações diferenciais racionais paramétricas (EDRP's). Além disso, assumimos que nem todos $P_i(U)$ e $Q_i(U)$ estão em K e que $MDC(P_i(U), Q_i(U)) = 1$.

Definição 3.2 *Um sistema da forma*

$$\mathcal{R}(X,U) := \begin{cases} x_1 &= \frac{P_1(U)}{Q_1(U)} \\ &\vdots \\ x_n &= \frac{P_n(U)}{Q_n(U)} \end{cases}$$

onde $P_1, \ldots, P_n, Q_1, \ldots, Q_n$ são polinômios diferencias em $K\{U\}$, com todos os Q_i não nulos e nem todos P_i e Q_i em K, para $i = 1, \ldots, n$, é chamado de um sistema de equações diferenciais racionais paramétricas, ou simplesmente e abreviadamente, um sistema de EDRP's.

Assumiremos que o conjunto U de indeterminadas, chamado *conjunto de parâmetros diferenciais* de $\mathcal{R}(X,U)$, não é necessariamente independente. Quando todos os P_i e Q_i são de grau no máximo 1, dizemos que $\mathcal{R}(X,U)$ é um *sistema linear*. Além disso, se todos os Q_i estão em K, dizemos que $\mathcal{R}(X,U)$ é um *sistema de equações diferenciais polinomiais paramétricas*, ou simplesmente e abrevidamente, um *sistema de EDPP's*, e denotamos $\mathcal{P}(X,U)$. Em particular, se $Q_i = 1$, para todo $i = 1, \ldots, n$, e nem todos os P_i estão em K, tem-se o seguinte sistema de EDPP's:

$$\mathcal{P}(X,U) := \begin{cases} x_1 &= P_1(U) \\ &\vdots \\ x_n &= P_n(U) \end{cases}$$

Associado com o sistema $\mathcal{R}(X,U)$, consideramos o ideal diferencial

$$\mathbf{ID} = \left\{ f \in K\{X\} \mid f\left(\frac{P_1(U)}{Q_1(U)}, \ldots, \frac{P_n(U)}{Q_n(U)}\right) = 0 \right\},$$

denominado *ideal implícito* de $\mathcal{R}(X,U)$. Pelo Lema 2.8 do capítulo anterior, tem-se que **ID** é um ideal diferencial primo. Também, consideramos a *variedade implícita* (diferencial) de $\mathcal{R}(X,U)$, definida por

$$Z(\mathbf{ID}) = \{\eta \in E^n \mid f(\eta) = 0, \text{ para todo } f \in \mathbf{ID}\}.$$

Da secção 4 do capítulo anterior, vem que os parâmetros de U são independentes se $dim\left(\mathcal{R}\left(X,U\right)\right)=|U|$ (a dimensão de um sistema de EDRP's entendemos como sendo a dimensão de seu ideal implícito). Além disso, se $\mathcal{C}$ é um conjunto característico de **ID**, então $n-|\mathcal{C}|$ é a dimensão (diferencial) de **ID**. E mais, em particular, se $dim\left(\mathbf{ID}\right)=n-1$, então $\mathcal{C}=\{A\left(X\right)\}$ para algum polinômio diferencial irredutível $A\in K\{X\}$. A este polinômio A, dá-se o nome de *polinômio característico* de **ID**. Além disso, se B é outro polinômio característico de **ID**, então $A=bB$, para algum $b\in K$.

Dado um conjunto $X=\{x_1,\ldots,x_n\}$ de indeterminadas diferenciais, vamos introduzir o conceito principal desta seção, a saber, a noção de equação implícita.

Definição 3.3 *A equação implícita de um sistema $(n-1)$-dimensional de EDRP's, em n indeterminadas diferenciais $x_1,\ldots,x_n$, é uma equação do tipo $A\left(X\right)=0$, em que A é qualquer polinômio característico do ideal implícito* **ID** *do sistema de EDRP's.*

Seja $K\left[\partial\right]$ o *anel de operadores diferenciais* com coeficientes em K. Considerando o sistema de EDPP's

$$\mathcal{P}\left(X,U\right):=\left\{\begin{array}{rcl} x_1 & = & P_1\left(U\right) \\ & \vdots & \\ x_n & = & P_n\left(U\right) \end{array}\right. ,$$

em que todos os P_i são de grau no máximo 1, sendo que nem todos estão em K, para todo $i=1,\ldots,n$, existem operadores diferenciais $\mathcal{L}_{ij}\in K\left[\partial\right]$, com $j=1,\ldots,n-1$, e constantes $a_i\in K$ tais que,

$$P_i\left(U\right)=a_i-\sum_{j=1}^{n-1}\mathcal{L}_{ij}\left(u_j\right).$$

A partir daí, para cada $x_i=P_i\left(U\right)$, com $i=1,\ldots,n$, chamando

$$T_i\left(X\right):=x_i-a_i \text{ e } H_i\left(U\right):=\sum_{j=1}^{n-1}\mathcal{L}_{ij}\left(u_j\right),$$

definimos o *polinômio diferencial ordinário linear*

$$F_i\left(X,U\right):=T_i\left(X\right)+H_i\left(U\right)$$

de ordem o_i, para $i=1,\ldots,n$. Salientamos que, para garantir que o número de parâmetros seja $n-1$, assume-se que para cada $j\in\{1,\ldots,n-1\}$, existem $i\in\{1,\ldots,n\}$ tais que $\mathcal{L}_{ij}\neq 0$. Mais especificamente, para cada elemento $j\in\{1,\ldots,n-1\}$, existem $i\in\{1,\ldots,n\}$, tais que $ord\left(F_i,u_j\right)\geq 0$.

3.3 Resultantes Diferenciais

Sejam f_i polinômios diferenciais em $D\{U\}$ de ordem o_i, para $i = 1, \ldots, n$, onde D é um domínio diferencial. Uma *resultante diferencial* de n polinômios diferenciais $f_1, \ldots, f_n$ em $n-1$ variáveis diferenciais $u_1, \ldots, u_{n-1}$, designada por $\partial Res(f_1, \ldots, f_n)$, foi introduzida por *Carra-Ferro* em [8]. Tal noção coincide com a *resultante algébrica de Macaulay* de um conjunto de polinômios diferenciais

$$PS(f_1, \ldots, f_n) := \left\{ \partial^{N-o_i} f_i, \ldots, \partial f_i, f_i \mid i = 1, \ldots, n, \text{ com } N = \sum_{i=1}^{n} o_i \right\}.$$

Agora, para cada $i = 1, \ldots, n$, seja $h_i \in D\{U\}$ um polinômio diferencial homogêneo de ordem o_i. Definimos a *resultante diferencial homogênea* de n polinômios diferenciais $h_1, \ldots, h_n$ em $n-1$ variáveis diferenciais $u_1, \ldots, u_{n-1}$, designada por $\partial Res^h(f_1, \ldots, f_n)$, como a *resultante algébrica de Macaulay* do conjunto de polinômios diferenciais

$$PS^h(f_1, \ldots, f_n) := \left\{ \partial^{N-o_i-1} h_i, \ldots, \partial h_i, h_i \mid i = 1, \ldots, n, \text{ com } N = \sum_{i=1}^{n} o_i \right\}.$$

Ressaltamos que a noção de resultantes diferenciais de polinômios diferenciais foram introduzidas em uma situação mais geral, dadas em dois trabalhos de *G. Carra-Ferro*, em [7] (para dois polinômios) e em [8] (para n polinômios). Definições anteriores da resultante diferencial, para operadores diferenciais, foram dadas por *L. M. Berkovich e V. G. Tsirulik* em [6] e *M. Chardin* em [10]. Salientamos que, para $n = 2$, quando os polinômios diferenciais homogêneos possuem grau 1, a resultante diferencial homogênea coincide com a resultante diferencial de dois operadores diferenciais, conforme definida por Berkovitch-Tsirulik e também estudada por Chardin. Uma vez que resultantes diferenciais algébricas são resultantes de Macaulay, a implementação das resultantes diferenciais, segue de alguns cálculos anteriores da resultante algébrica de Macaulay (*Disponível em Minimair, M., 2005. MR: Macaulay Resultant Package for Maple*).

Agora, para o que segue, dado o polinômio diferencial

$$F_i(X, U) = T_i(X) + H_i(U)$$

introduzido na seção anterior, para $i = 1, \ldots, n$, consideremos cada F_i como um polinômio em $n-1$ variáveis diferenciais $u_1, \ldots, u_{n-1}$ e com coeficientes no domínio diferencial $D = K\{X\}$. Recordemos que $F_1, \ldots, F_n$ são de ordens

o_i, para cada $i = 1, \ldots, n$, e de grau 1. Recordemos também que uma ordem no conjunto $Y = \{y_1, \ldots, y_n\}$ das indeterminadas diferenciais sobre K induz uma ordenação total no conjunto das derivadas $\{Y\}$, tal que:

(I) $v < \delta(v)$, para todos $v \in \{Y\}$.

(II) Se $u < v$ então $\delta^r(u) < \delta^s(v)$ para todos $u, v \in \{Y\}$ e para todos $r, s \in \mathbb{N}$.

Seja A o posicionamento em $X \cup U$ induzido por

$$u_1 < \cdots < u_{n-1} < x_1 < \cdots < x_n.$$

Agora, o conjunto $PS := PS(F_1, \ldots, F_n)$ é ordenado por A e, da particular estrutura de F_i, tem-se que:

$$F_1 < \partial F_1 < \cdots < \partial^{N-o_1} F_1 < F_2 < \partial F_2 < \cdots < F_n < \cdots < \partial^{N-o_n} F_n$$

Em outras palavras, da definição de conjunto autoreduzido, segue que PS é um conjunto autoreduzido de polinômios diferenciais $\{B_1, \ldots, B_L\}$, com $L = (n-1)N + n$, visto que para cada $i = 1, \ldots, n$ dos F_i no conjunto autoreduzido $F_1 < \cdots < \partial^{N-o_n} F_n$, encontramos $N, -o_i$ e 1, que somando obtemos:

$$\begin{aligned} L &= \sum_{i=1}^{n} (N - o_i + 1) \\ &= (N - o_1 + 1) + (N - o_2 + 1) + \cdots + (N - o_n + 1) \\ &= \left(\underbrace{N + N + \cdots + N}_{\text{n parcelas}} \right) - \left(\underbrace{o_1 + o_2 + \cdots + o_n}_{=N} \right) + \left(\underbrace{1 + 1 + \cdots + 1}_{\text{n parcelas}} \right) \\ &= nN - N + n = (n-1)N + n. \end{aligned}$$

Portanto,

$$L = \sum_{i=1}^{n} \left(\left(\sum_{k=1}^{n} o_k \right) - o_i + 1 \right)$$

Vamos ainda considerar em U o posicionamento A^*, induzido pela ordenação

$$1 < u_1 < \cdots < u_{n-1}.$$

Feitas estas considerações, seja $M(L)$ a matriz $L \times L$ cuja k-ésima linha é formada pelos coeficientes do k-ésimo polinômio em PS, visto como um polinômio em $D\{U\}$, e de coeficientes escritos em ordem decrescente com respeito a A^*. Assim, $M(L)$ é uma matriz sobre $D = K\{X\}$.

Definição 3.4 *Utilizando as notações acima, a matriz $M(L)$ é denominada matriz resultante diferencial de $F_1, \ldots, F_n$ e o seu determinante*

$$\partial Res(F_1, \ldots, F_n) = det(M(L))$$

é a resultante diferencial de $F_1, \ldots, F_n$.

Podemos fazer definições análogas para o caso homogêneo e obter a resultante diferencial homogênea $\partial Res^h(H_1, \ldots, H_n)$. Com efeito, recordemos a princípio que os polinômios diferenciais homogêneos $H_i \in K\{U\}$ são de ordens o_i, para cada $i = 1, \ldots, n$, e de grau 1. Seja $L^h = L - n$ e considere $PS^h := PS^h(H_1, \ldots, H_n)$ como sendo o conjunto polinomial obtido, a partir de PS, subtraindo de cada polinômio seu monômio em D (isto é, $T_i(X) := x_i - a_i$), e assim, mantendo em PS^h a ordem herdada de PS.

Feitas estas considerações, seja então $M\left(L^h\right)$ a matriz $L^h \times L^h$ cuja k-ésima linha é formada pelos coeficientes do k-ésimo polinômio em PS^h, visto como um polinômio em $D\{U\}$, e de coeficientes escritos em ordem decrescente com respeito a A^*.

Definição 3.5 *Usando as notações acima, a matriz $M\left(L^h\right)$, com entradas em K, é denominada matriz resultante diferencial homogênea de $H_1, \ldots, H_n$. O seu determiante*

$$\partial Res^h(H_1, \ldots, H_n) = det\left(M\left(L^h\right)\right)$$

é a resultante diferencial homogênea de $H_1, \ldots, H_n$.

Algumas propriedades das resultantes ∂Res e ∂Res^h estão a seguir.

Proposição 3.6 *Se o sistema $\{H_1 = 0, \ldots, H_n = 0\}$ tem uma solução não nula, então $\partial Res^h(H_1, \ldots, H_n) = 0$.*

Demonstração. Considere F como extensão diferencial do corpo K. Se o sistema $\{H_1 = 0, \ldots, H_n = 0\}$ tem uma solução não nula então a afirmação $\partial Res^h(H_1, \ldots, H_n) = 0$ segue dos dois fatos básicos seguintes:

Fato 1: Cada solução não nula do sistema $\{H_1 = 0, \ldots, H_n = 0\}$ em F^{n-1} é uma solução não nula do sistema

$$\left\{ \partial^{N-o_i-1} H_i, \ldots, \partial H_i, H_i \mid \text{com } i = 1, \ldots, n, \text{ onde } N = \sum_{i=1}^{n} o_i \right\}.$$

Fato 2: Se uma tal solução existe, então as colunas da matriz $M\left(L^h\right)$ são linearmente independentes em F. ■

Em relação a esta proposição, cabe a seguinte pergunta: Vale a recíproca? Mais especificamente, a condição $\partial Res^h(H_1,\ldots,H_n)=0$ é suficiente para a existência de alguma solução não nula do sistema $\{H_1=0,\ldots,H_n=0\}$?

Em geral (para $n>3$), infelizmente a resposta é não. Salvo o particularíssimo caso, para $n=2$, em que $\{H_1=0,H_2=0\}$ tem uma solução não nula se, e somente se, $\partial Res^h(H_1,H_2)=0$ ([6], Teorema 3.1).

Exemplo 3.7

Seja $n=3$ e considere os três seguintes polinômios diferenciais:

$$H_1(U)=u_{11}+u_{21},\quad H_2(U)=u_1+u_2\ \text{ e }\ H_3(U)=u_1+u_{11}+u_{21}$$

Temos $\partial Res^h(H_1,H_2,H_3)=0$, pois as duas primeiras colunas da matriz $M\left(L^h\right)$ são iguais, e o sistema $\{H_1=0,H_2=0,H_3=0\}$ tem apenas a solução nula.

Vamos agora introduzir algumas matrizes que serão utilizadas na prova do próximo resultado e que aparecerão em enunciados futuros.

Seja S a matriz $n\times(n-1)$ cuja i-ésima linha L_i é definida por:

$$L_i:=\begin{cases}\text{coeficientes dos termos de ordem } o_i \text{ em } F_i, \text{ caso existam}\\ \\ 0, \text{ caso não exista termo de ordem } o_i \text{ em } F_i\end{cases}$$

Seja S_i a matriz obtida por remoção da i-ésima linha de S.

Observação 3.8

Note que as linhas diferentes de zero das colunas de $M(L)$ (respectivamente $M\left(L^h\right)$) correspondentes aos coeficientes de u_{jN} (respectivamente u_{jN-1}), para $j=1,\ldots,n-1$, são as linhas de S. De acordo com isso, em particular, se a matriz S tem uma coluna nula, então $\partial Res^h(H_1,H_2,H_3)=0$.

Seja M_{L-1} a *submatriz principal* $L\times(L-1)$ de $M(L)$. Defina o conjunto

$$XS:=\left\{x_i,\partial x_i,\ldots,\partial^{N-o_i}x_i\mid i=1,\ldots,n\right\}.$$

Dado $x\in XS$, digamos $x:=x_{ik}$, com $k\in\{0,1,\ldots,N-o_i\}$, seja M_x a submatriz de $M(L)$ obtida por remoção da linha correspondente aos coeficientes de $\partial^k F_i=x_{ik}+\partial^k(H_i(U)-a_i)$. Desenvolvendo o determinante de $M(L)$, pela última coluna, utilizando o desenvolvimento de Laplace, obtemos

$$\partial Res(F_1,\ldots,F_n)=\sum_{i=1}^{n}\left(\sum_{k=0}^{N-o_i}b_{ik}\cdot det\left(M_{x_{ik}}\right)\left(x_{ik}-\partial^k a_i\right)\right)\tag{3.4}$$

onde $b_{ik} \cdot det\left(M_{x_{ik}}\right)$ é o complemento algébrico (ou cofator) de $x_{ik} - \partial^k a_i$, com $b_{ik} = \pm 1$ de acordo com o índice da linha de $x_{ik} - \partial^k a_i$ na matriz $M\left(L\right)$. Além disso, para cada $i \in \{1, \ldots, n\}$, existe $\lambda \in \mathbb{N}$ tal que

$$det\left(M_{x_{iN-o_i}}\right) = (-1)^{\lambda} \partial Res^h\left(H_1, \ldots, H_n\right) det\left(S_i\right) \tag{3.5}$$

Um fato útil é que, se $\partial Res^h\left(H_1, \ldots, H_n\right) \neq 0$, então pelo exposto acima, existe $k \in \{1, \ldots, n\}$ tal que $det\left(S_k\right) \neq 0$. E mais, uma vez que se tem $\partial Res^h\left(H_1, \ldots, H_n\right) \neq 0$, segue que são verdadeiras as seguintes afirmações:

A1 - Para cada $i \in \{1, \ldots, n\}$, tem-se que $det\left(M_{x_{iN-o_i}}\right) = 0$ se e só se $det\left(S_i\right) = 0$.

A2 - Existe $k \in \{1, \ldots, n\}$ tal que $det\left(M_{x_{kN-o_k}}\right) \neq 0$.

Proposição 3.9 *Seja M_{L-1} a submatriz principal $L \times (L-1)$ de $M\left(L\right)$. As seguintes afirmações são equivalentes:*

(1) . $\partial Res\left(F_1, \ldots, F_n\right) \neq 0$;

(2) . $\partial Res^h\left(H_1, \ldots, H_n\right) \neq 0$;

(3) . $posto\left(M_{L-1}\right) = L - 1$.

Demonstração. Seja M_{L-1} a submatriz principal $L \times (L-1)$ de $M\left(L\right)$. Considere ainda a submatriz M_x de $M\left(L\right)$.

Vamos verificar que (1) implica (2). Seja $\Delta = \partial Res\left(F_1, \ldots, F_n\right)$ e suponha que $\Delta \neq 0$. Assim, tem-se que $ord\left(\Delta, x_i\right) \leq N - o_i$, para $i = 1, \ldots, n$. Pela proposição 12 em [8], tem-se que $\Delta \in \mathbf{ID}$, onde $\mathbf{ID}$ é o ideal implícito de $\mathcal{P}\left(X, U\right)$. Segue do Lema 2.9 (capítulo anterior) que, se $[PS]$ é o ideal diferencial gerado por PS, então $\mathbf{ID} = [PS] \cap K\left\{X\right\}$. Assim, Δ é um polinômio diferencial linear em $[PS] \cap K\left\{X\right\}$, e temos que

$$\Delta = \sum_{i=1}^{n} \left(\sum_{k=0}^{ord(\Delta, x_i)} c_{ik} \cdot \partial^k F_i \right),$$

com $c_{ik} \in K$. Definindo o inteiro positivo

$$\xi := min\left\{N - o_i - ord\left(\Delta, x_i\right) \mid i \in \{1, \ldots, n\}\right\},$$

temos que $\xi = N - o_t - ord(\Delta, x_t)$, para algum $t \in \{1, \ldots, n\}$, e segue que $P = \partial^{\xi}\Delta$ verifica ser de ordem $ord(P, x_t) = N - o_t$ e $P \in [PS] \cap K\{X\}$. Daí, pelo Teorema 3.12 (próxima seção), segue que $\partial Res^h(H_1, \ldots, H_n) \neq 0$.

Vejamos que (2) implica (3). Seja $\Delta^h = \partial Res^h(H_1, \ldots, H_n)$ e suponha que $\Delta^h \neq 0$. Pela afirmação A2, existe $k \in \{1, \ldots, n\}$ tal que $det\left(M_{x_{kN-o_k}}\right) \neq 0$, e portanto, tem-se que $posto(M_{L-1}) = L - 1$.

Finalmente, basta verificar que (3) implica (1): Se $posto(M_{L-1}) = L - 1$ então existe $x \in XS$ tal que, $det(M_x) \neq 0$. Assim, pela observação 3.8, segue que $\partial Res(F_1, \ldots, F_n) \neq 0$. ■

3.4 Computando a Equação Implícita

Nesta seção, vamos tratar dos principais resultados deste capítulo, a saber, a equação implícita de $\mathcal{P}(X, U)$ é $\partial Res(F_1, \ldots, F_n)(X) = 0$, desde que $\partial Res(F_1, \ldots, F_n) \neq 0$, e dar uma fórmula explícita da resultante diferencial em termos da resultante diferencial homogênea.

Seja **ID** o ideal implícito de $\mathcal{P}(X, U)$. Pela Proposição 12 em [8], tem-se que $\partial Res(F_1, \ldots, F_n) \in \mathbf{ID}$. Segue do Lema 2.9 (capítulo anterior) que, se $[PS]$ é o ideal diferencial gerado por PS, então $\mathbf{ID} = [PS] \cap K\{X\}$. Se $\mathcal{A}$ é um conjunto característico de $[PS]$, então pelo Teorema 2.13 (capítulo anterior) temos que $\mathbf{ID} = [\mathcal{A}_0]$, onde $\mathcal{A}_0 = \mathcal{A} \cap K\{X\}$.

Seja $A^{\#}$ o posicionamento em $X \cup U$, induzido por

$$x_1 < \cdots < x_n < u_1 < \cdots < u_{n-1}.$$

Para polinômios $P, Q \in K\{X \cup U\}$, sejam $ord(P, y), ld(P)$ e $f_r(P, Q)$, respectivamente, a ordem de P na variável $y \in X \cup U$, o líder de P (com relação a $A^{\#}$) e o falso resto de P com respeito a Q. Considere $\mathcal{A} = \{A_1, \ldots, A_t\}$ um conjunto autoreduzido de elementos de $K\{X \cup U\}$. Considere ainda

$$[PS] \subseteq K[x_i, \ldots, x_{iN-o_i}, u_j, \ldots, u_{jN} \mid i = 1, \ldots, n, j = 1, \ldots, n-1]$$

o ideal gerado por PS. Daqui por diante, quando se fizer necessário, usaremos a base de Gröbner reduzida β de $[PS]$ com respeito a $A^{\#}$ para computar um conjunto característico de **ID**. Além disso, para calcularmos um conjunto característico de $[PS]$, aplicaremos o algoritmo do Teorema 6 descrito em [5]. Salientamos que, dado o conjunto de polinômios de PS, o algoritmo que segue retorna um conjunto característico de $[PS]$.

1. Calcula-se a base de Gröbner reduzida β de $[PS]$ com respeito a $A^{\#}$.

2. Assume-se que os elementos de β são arranjados em ordem crescente $\beta_1 < \cdots < \beta_m$ em relação a $A^{\#}$. Sendo $\mathcal{A} = \{\beta_i\}$, para $i = 2, \ldots, m$, se $ld(\beta_i) \neq ld(\beta_{i-1})$, então $\mathcal{A} := \mathcal{A} \cup \{f_r(\beta_i, \mathcal{A})\}$.

No que segue, apresentaremos os dois principais resultados deste capítulo. Mas antes, passamos a um lema que será útil na demonstração do primeiro destes resultados.

Lema 3.10 *O conjunto $\beta_0 = \beta \cap K\{X\}$ é não vazio e tem cardinalidade 1 se, e somente se, a resultante $\partial Res^h(H_1, \ldots, H_n)$ é não nula.*

Demonstração. Seja β uma Base de Gröbner reduzida de $[PS]$ que pode ser calculada realizando a eliminação gaussiana nas linhas de M_{2L-1}, conforme descrito em ([13], Exercício 10; Seção 7). Considere M_{2L-1} como sendo a matriz $L \times (2L-1)$, cuja k-ésima linha é constituída dos coeficientes do k-ésimo polinômio em PS, vistos como polinômios em $K\{X \cup U\}$, e de modo que os coeficientes estejam escritos em ordem decrescente em relação a $A^{\#}$.

$$M_{2L-1} = \begin{bmatrix} & 1 & & & & & \partial^{N-o_1}a_1 \\ & & \ddots & & & & \vdots \\ & & & 1 & & & a_1 \\ M_{L-1} & & & & \ddots & & \vdots \\ & & & & & 1 & \partial^{N-o_n}a_n \\ & & & & & & \vdots \\ & & & & & 1 & a_n \end{bmatrix}$$

De modo mais preciso, uma vez que $posto(M_{2L-1}) = L$, logo β contém L elementos $b_0 < b_1 < \cdots < b_{L-1}$, e M_{L-1} é a submatriz de M_{2L-1} formada pelas primeiras $L-1$ colunas de M_{2L-1}, com $posto(M_{L-1}) \leq L-1$. Portanto, $\beta_0 = \beta \cap K\{X\}$ é não vazio, com pelo menos $b_0 \in \beta_0$. Note que, considerando E_{2L-1} como sendo a forma escalonada reduzida por linhas da matriz M_{2L-1} ($det(M_{2L-1}) = b \cdot det(E_{2L-1})$, para algum $b \in K$), tem-se que os polinômios correspondentes às linhas de E_{2L-1} são exatamente os elementos da base β. Assim, de fato, o conjunto $\beta_0 = \beta \cap K\{X\}$ é não vazio, uma vez que $posto(M_{2L-1}) = L$. Quanto à cardinalidade de β_0, observe que é igual a 1 quando a última coluna de E_{2L-1} tem as primeiras $L-1$ entradas iguais a zero, equivalentemente, $posto(M_{L-1}) = L-1$. Da proposição 3.9, segue que $\partial Res^h(H_1, \ldots, H_n) \neq 0$, como queríamos. ■

Teorema 3.11 *Seja $\mathcal{P}(X,U)$ um sistema de equaçõ̃es diferenciais polinomiais. Suponha que $\partial Res^h(H_1,\ldots,H_n) \neq 0$. Então $dim(\mathbf{ID}) = n-1$ e $\partial Res(F_1,\ldots,F_n)(X) = 0$ é a equação implícita de $\mathcal{P}(X,U)$.*

Demonstração. Considere o sistema $\mathcal{P}(X,U)$ e seja β uma base de Gröbner reduzida de $[PS]$. Pelo Lema 3.10 o conjunto $\beta_0 = \beta \cap K\{X\}$ é não vazio, e assim, existe um conjunto característico $\mathcal{A}$ de $[PS]$ tal que, $\mathcal{A}_0 = \{b_1\}$. Logo, $dim(\mathbf{ID}) = n-1$. Considerando a forma escalonada reduzida por linhas E_{2L-1} da matriz M_{2L-1} dada no Lema 3.10, defina $E(L)$ como sendo a matriz $L \times L$ cujas primeiras $L-1$ colunas são as primeiras $L-1$ colunas de E_{2L-1}, e com última coluna igual à soma das últimas L colunas da mesma. Note que a matriz $E(L)$ assim definida contém b_1 como L-ésimo elemento de sua diagonal. Como, por definição, temos que

$$\partial Res(F_1,\ldots,F_n)(X) = det(M(L)) = (-1)^{\lambda} det(E(L)),$$

para algum $\lambda \in \mathbb{N}$, logo $\partial Res(F_1,\ldots,F_n)(X) = cb_1$, com $c \in K$ constante. Isto prova que $\partial Res(F_1,\ldots,F_n)$ é um conjunto característico de **ID**, e portanto, a equação implícita de $\mathcal{P}(X,U)$ de é $\partial Res(F_1,\ldots,F_n)(X) = 0$. ■

No próximo teorema vamos exibir uma fórmula explícita da resultante diferencial em termos da resultante diferencial homogênea. Aqui, a matriz S_k é a mesma definida na página 62.

Teorema 3.12 *Existe P no ideal implícito* **ID** *do sistema $\mathcal{P}(X,U)$ tal que:*

(i) $ord(P,x_i) \leq N - o_i$ *e* $ord(P,x_k) \leq N - o_k$, *para* $i = 1,\ldots,n$ *e algum* $k \in \{1,\ldots,n\}$.

(ii) $\partial Res(F_1,\ldots,F_n) = \frac{1}{\mu} det(S_k)\, \partial Res^h(H_1,\ldots,H_n)\, P(X)$,
onde $\mu = (-1)^{\lambda} \dfrac{\partial P}{\partial x_{kN-o_k}}$, *com* $\lambda \in \mathbb{N}$.

Demonstração. Para verificar *(i)*, seja **ID** o ideal implícito do sistema $\mathcal{P}(X,U)$. Dada a base de Gröbner reduzida β de $[PS]$ em relação a $A^{\#}$, tomemos um polinômio Q em $\beta_0 = \beta \cap K\{X\}$. A fim de que sejam verificadas, para algum P de **ID**, as condições $ord(P,x_i) \leq N - o_i$ e $ord(P,x_k) \leq N - o_k$, para $i = 1,\ldots,n$ e algum $k \in \{1,\ldots,n\}$, basta definir o inteiro positivo

$$\gamma := min\{N - o_i - ord(Q_i,x_i) \mid i \in \{1,\ldots,n\}\}$$

e tomar o polinômio $P = Q^{(\gamma)}$ que o resultado segue.

Vamos provar *(ii)*. Uma vez que $P \in \mathbf{ID} = [PS] \cap K\ \{X\}$, existem operadores diferenciais $\mathcal{F}_1 \ldots, \mathcal{F}_n \in K[\partial]$, com $gr(\mathcal{F}_i) \leq N - o_i$, tais que

$$\begin{aligned} P(X) &= \mathcal{F}_1(F_1(X,U)) + \cdots + \mathcal{F}_n(F_n(X,U)) \\ &= \mathcal{F}_1(T_1(X) + H_1(U)) + \cdots + \mathcal{F}_n(T_n(X) + H_n(U)) \\ &= \mathcal{F}_1(T_1(X)) + \cdots + \mathcal{F}_n(T_n(X)) + \\ &\qquad + \underbrace{\mathcal{F}_1(H_1(U)) + \cdots + \mathcal{F}_n(H_n(U))}_{=0} \\ &= \mathcal{F}_1(T_1(X)) + \cdots + \mathcal{F}_n(T_n(X)). \end{aligned}$$

Como uma consequência, podemos realizar operações de linha em $M(L)$ para se obter uma matriz do tipo

$$\begin{bmatrix} 0 & \cdots & 0 & 0 & \cdots & 0 & P(X) \\ & & & * & \cdots & * & * \\ & S_k & & & \ddots & & \vdots \\ & & & * & \cdots & * & * \\ 0 & \cdots & 0 & & & & * \\ & \ddots & & & M\left(L^h\right) & & \vdots \\ 0 & \cdots & 0 & & & & * \end{bmatrix}.$$

Para ser mais preciso, reordenamos as linhas de $M(L)$ de modo que os coeficientes de $\partial^{N-o_k} F_k$ estejam na primeira linha, as linhas 2 a n são as linhas que contêm as entradas da matriz S_k, obtida de S e de ordem $(n-1) \times (n-1)$, e as linhas $n+1$ até L são as linhas que contêm as entradas de $M\left(L^h\right)$, de ordem $L^h = L - n = (n-1)N$. Lembre-se que, as linhas diferentes de zero das colunas de $M(L)$ (respectivamente $M\left(L^h\right)$) correspondentes aos coeficientes de u_{jN} (respectivamente u_{jN-1}), para $j = 1, \ldots, n-1$, são as linhas de S. Em seguida, multiplique a primeira linha da matriz obtida por $\frac{\partial P}{\partial x_{kN-o_k}} \neq 0$. Finalmente, substitua a primeira linha pelos coeficientes de $P(X)$ como um polinômio em $D\{U\}$ escrito em ordem decrescente com respeito ao posicionamento em U, ou seja, todas entradas nulas exceto da última entrada igual a $P(X)$ (note que, por definição, esta última entrada é a soma $\mathcal{F}_1(F_1(X,U)) + \cdots + \mathcal{F}_n(F_n(X,U))$). Definindo $\mu := (-1)^{\lambda} \dfrac{\partial P}{\partial x_{kN-o_k}}$, para algum $\lambda \in \mathbb{N}$, tem-se que

$$\mu \cdot det(M(L)) = det(S_k)\, det\left(M\left(L^h\right)\right) P(X),$$

e portanto, $\partial Res\left(F_1,\ldots,F_n\right)=\frac{1}{\mu}det\left(S_k\right)\partial Res^h\left(H_1,\ldots,H_n\right)P\left(X\right).$ ■

Como aplicação, vamos explicitar uma expressão polinomial, em termos de operadores diferenciais que definem EDPP's, que verifique o Teorema 3.12 nos casos $n=2$ e $n=3$.

1. Caso $n=2$

Dados operadores diferenciais $\mathcal{L}_1,\mathcal{L}_2\in K\left[\partial\right]$, vamos considerar o seguinte sistema de EDPP's:

$$\mathcal{P}_2\left(x_1,x_2,u\right):=\left\{\begin{array}{l} x_1=a_1-\mathcal{L}_1\left(u\right)\\ x_2=a_2-\mathcal{L}_2\left(u\right)\end{array}\right.$$

Fixado $u=u_1$, pomos $H_1\left(u\right)=\mathcal{L}_1\left(u\right)$ e $H_2\left(u\right)=\mathcal{L}_2\left(u\right)$, e escrevemos $F_1\left(x_1,x_2,u\right)=x_1-a_1+H_1\left(u\right)$ e $F_2\left(x_1,x_2,u\right)=x_2-a_2+H_2\left(u\right)$.

Observamos que o anel $K\left[\partial\right]$ é *euclidiano à direita* (e também *euclidiano à esquerda*). Isto significa que dados $\mathcal{L}_1,\mathcal{L}_2\in K\left[\partial\right]$, obtemos $q,r\in K\left[\partial\right]$ tais que

$$\mathcal{L}_2=q\mathcal{L}_1+r,\ \ \text{com}\ \ gr\left(r\right)<gr\left(\mathcal{L}_1\right).$$

Também podemos encontrar $\mathcal{L}:=MDC_d\left(\mathcal{L}_1,\mathcal{L}_2\right)$ o *máximo divisor comum à direita* de $\mathcal{L}_1$ e $\mathcal{L}_2$, onde $\mathcal{L}\in K\left[\partial\right]$. Neste caso, existem $\widehat{\mathcal{L}}_1,\widehat{\mathcal{L}}_2\in K\left[\partial\right]$ tais que $\mathcal{L}_i=\widehat{\mathcal{L}}_i\mathcal{L}$, para $i=1,2$. Os operadores diferenciais $\mathcal{L}_1$ e $\mathcal{L}_2$ são *coprimos* se eles têm um máximo divisor comum à direita constante, e escrevemos $\left(\mathcal{L}_1,\mathcal{L}_2\right)=1$. Neste caso, o máximo divisor comum é dito *trivial*.

Se K é um corpo de constantes em relação a ∂, isto é, $\partial\left(k\right)=0$ para todo $k\in K$ (por exemplo $\partial=\frac{\partial}{\partial t}$ para $K=\mathbb{C}$) então $\mathcal{L}_1\mathcal{L}_2-\mathcal{L}_2\mathcal{L}_1=0$, ou seja, os operadores diferenciais comutam. Se K não é um corpo de constantes em relação a ∂, então o anel $K\left[\partial\right]$ não é comutativo e temos $\partial k-k\partial=\partial\left(k\right)$, para todo $k\in K$.

A propriedade seguinte sobre a comutatividade será usado na demonstração da próxima proposição onde vamos exibir a expressão polinomial explícita mencionada.

Lema 3.13 *Suponha que* $\mathcal{L}_1,\mathcal{L}_2\in K\left[\partial\right]$ *sejam coprimos. Então existem* $\mathcal{D}_1,\mathcal{D}_2\in K\left[\partial\right]$ *com* $gr\left(\mathcal{D}_i\right)\leq gr\left(\mathcal{L}_i\right)-1$, *para* $i=1,2$, *tais que*

$$\left(\mathcal{L}_2-\mathcal{D}_2\right)\mathcal{L}_1-\left(\mathcal{L}_1-\mathcal{D}_1\right)\mathcal{L}_2=0.$$

Demonstração. Dados os operadores diferenciais $\mathcal{L}_1,\mathcal{L}_2\in K\left[\partial\right]$, seja $\mathcal{L}:=MDC_d\left(\mathcal{L}_1,\mathcal{L}_2\right)$ o máximo divisor comum à direita de $\mathcal{L}_1$ e $\mathcal{L}_2$. Logo existem

$\widehat{\mathcal{L}}_1, \widehat{\mathcal{L}}_2 \in K[\partial]$ tais que $\mathcal{L}_i = \widehat{\mathcal{L}}_i \mathcal{L}$, para $i = 1, 2$. Suponha que os operadores diferenciais $\mathcal{L}_1$ e $\mathcal{L}_2$ sejam coprimos. Vamos mostrar que, independente da comutatividade de $\mathcal{L}_1$ e $\mathcal{L}_2$, existem $\mathcal{D}_1, \mathcal{D}_2 \in K[\partial]$ com $gr(\mathcal{D}_i) \leq gr(\mathcal{L}_i) - 1$, para $i = 1, 2$, tais que $(\mathcal{L}_2 - \mathcal{D}_2)\mathcal{L}_1 - (\mathcal{L}_1 - \mathcal{D}_1)\mathcal{L}_2 = 0$. De fato, suponha então por um instante que $\mathcal{L}_1$ e $\mathcal{L}_2$ comutam. Daí:

$$\begin{aligned} 0 &= \mathcal{L}_1\mathcal{L}_2 - \mathcal{L}_2\mathcal{L}_1 = \left(\widehat{\mathcal{L}}_1\mathcal{L}\right)\mathcal{L}_2 - \left(\widehat{\mathcal{L}}_2\mathcal{L}\right)\mathcal{L}_1 = \left(\widehat{\mathcal{L}}_1 1\right)\mathcal{L}_2 - \left(\widehat{\mathcal{L}}_2 1\right)\mathcal{L}_1 \\ &= \widehat{\mathcal{L}}_1\mathcal{L}_2 - \widehat{\mathcal{L}}_2\mathcal{L}_1 = \widehat{\mathcal{L}}_1\mathcal{L}_2 - \widehat{\mathcal{L}}_2\mathcal{L}_1 + 0 = \widehat{\mathcal{L}}_1\mathcal{L}_2 - \widehat{\mathcal{L}}_2\mathcal{L}_1 + (\mathcal{L}_2\mathcal{L}_1 - \mathcal{L}_1\mathcal{L}_2) \\ &= \left(\mathcal{L}_2 - \widehat{\mathcal{L}}_2\right)\mathcal{L}_1 - \left(\mathcal{L}_1 - \widehat{\mathcal{L}}_1\right)\mathcal{L}_2 \end{aligned}$$

Assim, existem operadores diferenciais, a saber $\widehat{\mathcal{L}}_1, \widehat{\mathcal{L}}_2 \in K[\partial]$, que cumprem o requerido e, visto que $\mathcal{L}_1$ e $\mathcal{L}_2$ são comutativos, tome $\widehat{\mathcal{L}}_i := \mathcal{D}_i = 0$, para $i = 1, 2$, e o resultado segue. Suponha agora que $\mathcal{L}_1$ e $\mathcal{L}_2$ não comutem, ou seja, $\mathcal{L}_1\mathcal{L}_2 - \mathcal{L}_2\mathcal{L}_1 \neq 0$, e sejam $\mathcal{L}_1 = \sum_{0 \leq i \leq o_1} A_i \partial^i$ e $\mathcal{L}_2 = \sum_{0 \leq j \leq o_2} B_j \partial^j$ suas expressões. Pela equação 1.2 em [6], podemos escrever

$$\mathcal{L}_1\mathcal{L}_2 - \mathcal{L}_2\mathcal{L}_1 = \sum_{k=0}^{o_1+o_2} (c_k - \overline{c}_k)\partial^k,$$

onde c_k e $\overline{c}_k$ são dados, respectivamente, por

$$\begin{aligned} c_k &= \sum_{s:=max\{0,k-o_2\}}^{s:=min\{o_1,k\}} \sum_{i=s}^{o_1} A_i \partial^{(i-s)}(B_{k-s}) \\ \overline{c}_k &= \sum_{s:=max\{0,k-o_1\}}^{s:=min\{o_2,k\}} \sum_{j=s}^{o_2} B_j \partial^{(j-s)}(A_{k-s}), \end{aligned}$$

e daí, segue que $c_{o_1+o_2} = \overline{c}_{o_1+o_2} = A_{o_1}B_{o_2}$. Portanto, segue que

$$gr(\mathcal{L}_1\mathcal{L}_2 - \mathcal{L}_2\mathcal{L}_1) \leq o_1 + o_2 - 1.$$

Agora, precisamos encontrar operadores diferenciais $\mathcal{D}_1 = \sum_{0 \leq i \leq o_1 - 1} \alpha_i \partial^i$ e $\mathcal{D}_2 = \sum_{0 \leq j \leq o_2 - 1} \beta_j \partial^j$, com $\alpha_i, \beta_j \in K$, tais que,

$$\mathcal{D}_1\mathcal{L}_2 - \mathcal{D}_2\mathcal{L}_1 = \mathcal{L}_1\mathcal{L}_2 - \mathcal{L}_2\mathcal{L}_1.$$

Novamente, podemos escrever

$$\mathcal{D}_1\mathcal{L}_2 - \mathcal{D}_2\mathcal{L}_1 = \sum_{k=0}^{o_1+o_2-1} (\gamma_k - \overline{\gamma}_k)\,\partial^k,$$

onde γ_k e $\overline{\gamma}_k$ dados, respectivamente, por

$$\gamma_k = \sum_{s:=max\{0,k-o_2\}}^{s:=min\{o_1-1,k\}} \sum_{i=s}^{o_1-1} A_i \partial^{(i-s)}\left(B_{k-s}\right)$$

$$\overline{\gamma}_k = \sum_{s:=max\{0,k-o_1\}}^{s:=min\{o_2-1,k\}} \sum_{j=s}^{o_2-1} B_j \partial^{(j-s)}\left(A_{k-s}\right).$$

Vamos considerar o sistema de $N := o_1 + o_2$ equações $\gamma_k - \overline{\gamma}_k = c_k - \overline{c}_k$, para $k = 0, \ldots, o_1 + o_2 - 1$, nas N incógnitas α_i e β_j, para $i = 0, \ldots, o_1$ e $j = 0, \ldots, o_2$. A matriz dos coeficientes deste sistema é a matriz $M(N)$, onde $N := L^h$, que define a resultante diferencial homogênea $\partial Res^h(H_1, H_2)$. De acordo com isso, segue que o sistema tem uma única solução, uma vez que $det(M(N)) = \partial Res^h(H_1, H_2) \neq 0$ (pelo Teorema 2 de [10], tem-se que $MDC_d(\mathcal{L}_1, \mathcal{L}_2)$ é não trivial se e só se $\partial Res^h(H_1, H_2) = 0$). ■

Proposição 3.14 *Seja K um corpo de funções em uma variável real t e $\frac{\partial}{\partial t}$. Se $(\mathcal{L}_1, \mathcal{L}_2) = 1$ então existem $\mathcal{D}_1, \mathcal{D}_2 \in K[\partial]$ tais que*

$$\begin{aligned}\partial Res(F_1, F_2)(x_1, x_2) &= (-1)^{\lambda}\,\partial Res^h(H_1, H_2)(\mathcal{L}_2 - \mathcal{D}_2)(x_1 - \alpha_1) \\ &\quad - (-1)^{\lambda}\,\partial Res^h(H_1, H_2)(\mathcal{L}_1 - \mathcal{D}_1)(x_2 - \alpha_2),\end{aligned}$$

para algum $\lambda \in \mathbb{N}$.

Demonstração. Seja K um corpo de funções em uma variável real t e $\frac{\partial}{\partial t}$. Fixado $u = u_1$, pomos $H_1(u) = \mathcal{L}_1(u)$ e $H_2(u) = \mathcal{L}_2(u)$, para operadores diferenciais $\mathcal{L}_1, \mathcal{L}_2 \in K[\partial]$. Se $(\mathcal{L}_1, \mathcal{L}_2) = 1$, segue do lema anterior que existem $\mathcal{D}_1, \mathcal{D}_2 \in K[\partial]$ tais que $(\mathcal{L}_2 - \mathcal{D}_2)\mathcal{L}_1(u) - (\mathcal{L}_1 - \mathcal{D}_1)\mathcal{L}_2(u) = 0$. Pelo teorema anterior, temos que:

$$\partial Res(F_1, \ldots, F_n) = \frac{1}{\mu} det(S_k)\,\partial Res^h(H_1, \ldots, H_n)\,P(X),$$

onde $\mu = (-1)^{\lambda}\frac{\partial P}{\partial x_{kN-o_k}}$, com $\lambda \in \mathbb{N}$. Assim, aplicando o teorema ao polinômio definido por

$$P(x_1, x_2) := (\mathcal{L}_2 - \mathcal{D}_2)(x_1 - \alpha_1) - (\mathcal{L}_1 - \mathcal{D}_1)(x_2 - \alpha_2),$$

e visto que se $\partial Res^h(H_1, H_2) \neq 0$, então existe $k \in \{1, 2\}$ tal que

$$det(S_k) = \frac{\partial P}{\partial x_{kN-o_k}} \neq 0,$$

obtemos explicitamente a seguinte expressão polinomial, para $n = 2$,

$$\partial Res(F_1, F_2)(x_1, x_2) = \frac{1}{(-1)^\lambda \frac{\partial P}{\partial x_{kN-o_k}}} \frac{\partial P}{\partial x_{kN-o_k}} \partial Res^h(H_1, H_2) P(x_1, x_2)$$

$$= (-1)^\lambda \partial Res^h(H_1, H_2) [(\mathcal{L}_2 - \mathcal{D}_2)(x_1 - \alpha_1) - (\mathcal{L}_1 - \mathcal{D}_1)(x_2 - \alpha_2)]$$

observando que $ord(P, x_k) \leq N - o_k$, para $k \in \{1, 2\}$, e novamente que $det(S_k) = \frac{\partial P}{\partial x_{kN-o_k}}$. ■

2. Caso $n = 3$.

Aqui neste caso, para $K = \mathbb{C}$, com $\mathcal{L}_{ij} \in \mathbb{C}[\partial]$, vamos considerar o seguinte sistema de EDPP's.

$$\mathcal{P}_3(X, U) := \begin{cases} x_1 &= a_1 - \mathcal{L}_{11}(u_1) - \mathcal{L}_{12}(u_2) \\ x_2 &= a_2 - \mathcal{L}_{21}(u_1) - \mathcal{L}_{22}(u_2) \\ x_3 &= a_3 - \mathcal{L}_{31}(u_1) - \mathcal{L}_{32}(u_2) \end{cases},$$

onde $X = \{x_1, x_2, x_3\}$ e $U = \{u_1, u_2\}$. Por definição, estes operadores diferenciais comutam. Assim, por conseguinte, o polinômio $P(X)$ dado por

$$P(X) : = \mathcal{L}_{21}\mathcal{L}_{32}(x_1 - a_1) - \mathcal{L}_{22}\mathcal{L}_{31}(x_1 - a_1) - \mathcal{L}_{11}\mathcal{L}_{32}(x_2 - a_2)$$

$$+ \mathcal{L}_{12}\mathcal{L}_{31}(x_2 - a_2) + \mathcal{L}_{11}\mathcal{L}_{22}(x_3 - a_3) - \mathcal{L}_{12}\mathcal{L}_{21}(x_3 - a_3),$$

pertence ao ideal implícito de $\mathcal{P}_3(X, U)$. Para $i = 1, 2, 3$, temos que

$$F_i(X, U) = x_i - a_i + H_i(U) \quad \text{e} \quad H_i(U) = \mathcal{L}_{i1}(u_1) + \mathcal{L}_{i2}(u_2)$$

de ordem o_i. Além disso, se $det(S_i) \neq 0$, para algum $i = 1, 2, 3$, resulta do Teorema 3.12 que

$$\partial Res(F_1, F_2, F_3)(X) = (-1)^\lambda \partial Res^h(H_1, H_2, H_3) P(X),$$

sendo $\lambda \in \mathbb{N}$. Salientamos que $det(S_i)$ é o coeficiente de $x_{i,N-o_i}$ em $P(X)$.

3.5 Resultantes Diferenciais Generalizados

De acordo com a Observação 3.8, se a matriz S tem uma coluna nula, então $\partial Res^h(H_1,\ldots,H_n) = 0$. Com efeito, a razão disto é que os polinômios $H_1,\ldots,H_n$ não são completos em todas as suas variáveis, isto é, existe $j \in \{1,\ldots,n-1\}$ tal que, nenhum F_i tem um termo em u_{jo_i}, para todo $i \in \{1,\ldots,n\}$. Assim, se para algum $j \in \{1,\ldots,n-1\}$ a variável diferencial u_j tem ordem menor do que o_i em F_i, para todo $i \in \{1,\ldots,n\}$, então a matriz $M(L)$ tem uma ou mais colunas de zeros (o exemplo dado no início da secção 3.2 ilustra bem isto, uma vez que a ordem de u_1 em todo polinômio de $\{F_1(X,U), F_2(X,U), F_3(X,U)\}$ é menor do que o_i em $F_i(X,U)$, para todo $i \in \{1,2,3\}$). Nesta seção, vamos estender a definição de resultante diferencial de modo a que ela seja aplicável a esse tipo de sistema de EDPP's. Para isso, naturalmente, vamos precisar introduzir algumas notações.

Dada a matriz S, comecemos definindo o conjunto

$$J := \{j \in \{1,\ldots,n-1\} \mid \text{a } j-\textit{ésima} \text{ coluna de } S \text{ é nula}\}.$$

Devido ao motivo de que se $ord(F_i,u_j) < o_i$, então a matriz $M(L)$ tem uma ou mais colunas de zeros, para cada $j \in J$, definamos os seguintes inteiros positivos

$$\gamma_j := \gamma_j(F_1,\ldots,F_n) = min\{o_i - ord(F_i,u_j) \mid i \in \{1,\ldots,n\}\}$$

e

$$\gamma := \gamma(F_1,\ldots,F_n) = \sum_{i=1}^{n} \gamma_i(F_1,\ldots,F_n)$$

Observe que $1 \leq \gamma_j \leq o_i$ e $0 \leq \gamma \leq N - o_i$, para todo $i \in \{1,\ldots,n\}$. Além disso, note que se $J \neq \varnothing$, então $PS(F_1,\ldots,F_n)$ é um conjunto de L polinômios em $L-\gamma$ variáveis diferenciais. Agora, considere M_J a matriz $L \times (L-\gamma)$ obtida por remoção das colunas nulas de $M(L)$ que corresponde aos monômios no conjunto dado por

$$m_J := \{u_{jk} \mid k = N-\gamma_j,\ldots,N, \text{ com } j \in J\}.$$

De modo análogo, definimos também M_J^h como sendo a matriz $L^h \times \left(L^h - \gamma\right)$ obtida por remoção das colunas nulas de $M\left(L^h\right)$ que correspondem aos monômios no conjunto dado por

$$m_J^h := \{u_{jk} \mid k = N-\gamma_j-1,\ldots,N-1, \text{ com } j \in J\}.$$

Para um dado $i \in \{1,\ldots,n\}$, seja Γ_i a submatriz de M_J cujas linhas contém os coeficientes dos polinômios em $\left\{\partial^{N-o_i}F_i,\ldots,\partial F_i, F_i\right\}$. Analogamente,

para um certo $i \in \{1, \ldots, n\}$, seja Γi^h a submatriz de M_J^h cujas linhas contém os coeficientes dos polinômios em $\left\{\partial^{N-o_i-1} H_i, \ldots, \partial H_i, H_i\right\}$. Seja agora M_{J_i} a submatriz de M_J obtida por remoção das últimas γ linhas do bloco Γ_i. De igual modo, seja agora $M_{J_i}^h$ a submatriz de M_J^h obtida por remoção das últimas γ linhas do bloco Γ_i^h. Vamos também considerar o seguinte subconjunto de $K\{X\}$, de polinômios de grau 1:

$$\mathcal{M} := \{\text{determinantes não nulos de menores de } M_J \text{ de ordem } L - \gamma\}$$

De forma análoga, consideremos também o seguinte subconjunto de K:

$$\mathcal{M}^h := \left\{\text{determinantes não nulos de menores de } M_J^h \text{ de ordem } L^h - \gamma\right\}$$

Salientamos que os conjuntos $\mathcal{M}$ e $\mathcal{M}^h$ estão contidos, respectivamente, nos espaços vetoriais

$$K\left\langle det\left(M_{J_i}\right) \mid i \in \{1, \ldots, n\}\right\rangle \text{ e } K\left\langle det\left(M_{J_i}^h\right) \mid i \in \{1, \ldots, n\}\right\rangle.$$

Definição 3.15 *A resultante diferencial generalizada de $\{F_1, \ldots, F_n\}$, denotada por $\partial Res_J(F_1, \ldots, F_n)$, é definida como segue:*

$$\partial Res_J(F_1, \ldots, F_n) := \begin{cases} 0, & \text{se } \mathcal{M} = \varnothing \\ A \text{ ou } 1, & \text{se existe } A \in \mathcal{M} \text{ talque } \mathcal{M} \subseteq [A] \end{cases}$$

Observação 3.16

A definição dada aqui de resultante diferencial generalizada se aplica apenas aos polinômios de grau 1, visto que esta definição para polinômios de qualquer grau não é o objetivo deste trabalho.

Dados $F_1, \ldots, F_n$, o seguinte algoritmo retorna $\partial Res_J(F_1, \ldots, F_n)$.

1. Se $det\left(M_{J_i}\right) = 0$, para todo $i \in \{1, \ldots, n\}$, então retorna 0.
2. Se $\Delta = \{k \in \{1, \ldots, n\} \mid det\left(M_{J_k}\right) \neq 0\}$, então $\Delta = \{i_1, \ldots, i_t\} \subseteq \{1, \ldots, n\}$ é tal que $det\left(M_{J_{i_1}}\right) < \cdots < det\left(M_{J_{i_t}}\right)$, em relação a A.
3. Seja $A = det\left(M_{J_{i_1}}\right)$. Se $det\left(M_{J_i}\right) \in [A]$, para todo i, então retorna A senão retorna 1.

Definição 3.17 *A resultante diferencial homogênea generalizada do conjunto $\{H_1, \ldots, H_n\}$, denotada por $\partial Res_J^h(H_1, \ldots, H_n)$, é definida como segue:*

$$\partial Res_J^h(H_1, \ldots, H_n) := \begin{cases} 0, & \text{se } \mathcal{M}^h = \varnothing \\ MDC\left(\mathcal{M}^h\right), & \text{caso contrário} \end{cases}$$

Note que, se $\partial Res_J^h(H_1,\ldots,H_n) \neq 0$, então

$$\partial Res_J^h(H_1,\ldots,H_n) = MDC\left\{det\left(M_{J_i}^h\right) \mid i \in \{1,\ldots,n\}\right\}.$$

Proposição 3.18 *Dado o sistema $S := \{H_1 = 0,\ldots,H_n = 0\}$, tem-se que:*

1. *Se S tem uma solução não nula, então $\partial Res_J^h(H_1,\ldots,H_n) = 0$.*
2. *$\partial Res_J^h(H_1,\ldots,H_n) = 0$ se, e somente se, $\partial Res_J(F_1,\ldots,F_n) = 0$.*

A demonstração deste resultado encontra-se em [31].

Vamos usar o próximo resultado para provar o principal resultado desta seção, a saber, se $J \neq \varnothing$ e $\partial Res_J(F_1,\ldots,F_n)$ é não constante (isto é, $\partial Res_J(F_1,\ldots,F_n) \notin K$), então $\partial Res_J(F_1,\ldots,F_n)(X) = 0$ é a equação implícita de $\mathcal{P}(X,U)$.

Lema 3.19 *Se $P(X) = det(M_{j_i}) \in K\{X\}$, com $i \in \{1,\ldots,n\}$, então $ord(P,x_j) \leq N - o_j - \gamma$, para todo $j \in \{1,\ldots,n\}$.*

Demonstração. A demonstração segue da definição de ordem apresentada anteriormente. ■

Teorema 3.20 *Seja $\mathcal{P}(X,U)$ um sistema de equações, $J \neq \varnothing$ e suponha $\partial Res_J(F_1,\ldots,F_n) \notin K$. Então,*

1. *$dim(\mathbf{ID}) = n - 1$.*
2. *$\partial Res_J(F_1,\ldots,F_n)(X) = 0$ é a equação implícita de $\mathcal{P}(X,U)$.*

Demonstração. Dado um sistema $\mathcal{P}(X,U)$, suponha que $J \neq \varnothing$ e que $\partial Res_J(F_1,\ldots,F_n)$ seja não constante. Assim, em particular, tem-se que $\partial Res_J(F_1,\ldots,F_n) \neq 0$. Daí, pela definição de $\partial Res_J(F_1,\ldots,F_n)$, vem que $\mathcal{M} \subset K\langle det(M_{J_i}) \mid i \in \{1,\ldots,n\}\rangle$ é um subconjunto não vazio de $K\{X\}$, e portanto, segue que o conjunto Δ descrito no algoritmo a pouco é não vazio, por definição. De acordo disso, definindo $A := det\left(M_{J_{i_1}}\right)$, segue do lema anterior que $ord(A,x_k) \leq N - o_k - \gamma$, para todo $k \in \Delta$. Novamente, do lema anterior temos que $A^{(\gamma)} \in [PS]$ e podemos realizar operações nas linhas de M_J obtendo a matriz

$$E_k = \begin{bmatrix} M_{Jk} & \cdots \\ 0 & A^{(\gamma)} \\ & \\ 0 & \vdots \\ 0 & A^{(1)} \end{bmatrix}.$$

Agora, realizamos operações nas linhas de E_k para obter a forma escalonada reduzida de M_{Jk}. Assim, as linhas da matriz obtida são uma base de Gröbner β de $[PS]$, com $\beta \cap K\{X\} = \left\{A, A^{(1)}, \ldots, A^{(\gamma)}\right\}$. Logo, por definição, tem-se que A é um polinômio característico de **ID**, e portanto, $dim\,(\mathbf{ID}) = n-1$, o que prova ser $\partial Res_J\,(F_1, \ldots, F_n)\,(X) = A\,(X) = 0$ a equação implícita de $\mathcal{P}\,(X, U)$. ■

Observação 3.21

Observe que $\partial Res_J\,(F_1, \ldots, F_n) = 1$ implica que a dimensão de **ID** é menor do que $n-1$ e, por conseguinte, a equação implícita não existe. Resta determinar a razão para a qual $\partial Res_J\,(F_1, \ldots, F_n) = 0$.

Exemplo 3.22

Considere o sistema linear de equações polinomiais paramétricas

$$\mathcal{S}_2 := \begin{cases} x_1 &= u_1 + u_2 + u_{21} \\ x_2 &= tu_{11} + u_{22} \\ x_3 &= u_1 + u_{21} \end{cases}$$

dado no exemplo, onde $u_{jk} = \frac{\partial^k u_j}{\partial t^k}$, para $j \in \{1, 2\}$ e $k \in \mathbb{N}$, e $x_{ik} = \frac{\partial^k x_i}{\partial t^k}$, para $i \in \{1, 2, 3\}$ e $k \in \mathbb{N}$. A matriz $M\,(11)$ definindo a resultante diferencial $\{x_1 - u_1 - u_2 - u_{21}, x_2 - tu_{11} - u_{22}, x_3 - u_1 - u_{21}\}$ tem uma coluna nula. Assim, a equação implícita de $\mathcal{S}_2$ coincide com o determinante das submatrizes 10×10 de $M\,(11)$, obtida removendo a coluna nula e qualquer outra linha.

3.6 Operadores Diferenciais Próprios

Nesta seção, daremos alguns resultados relacionados com o problema de inversão. Para ser mais preciso, vamos estudar certas condições nos operadores diferenciais $\mathcal{L}_{ij}$ que faz de $\mathcal{P}\,(X, U)$ um conjunto próprio de EDPP's. Reuniremos a seguir algumas definições que serão necessários nesta seção e que foram usados na seção 5 do capítulo anterior, para estudar o problema de inversão em termos de conjuntos característicos.

A imagem de $\mathcal{P}\,(X, U)$ em E^n é o conjunto **IM** definido por

$$\left\{(\eta_1, \ldots, \eta_n) \in E^n \mid \text{existe } (\tau_1, \ldots, \tau_{n-1}) \in E^{n-1} \text{ onde } \eta_i = P_i\,(\tau_1, \ldots, \tau_{n-1})\right\}.$$

O problema de inversão diz é o seguinte: dado $(\eta_1, \ldots, \eta_n) \in \mathbf{IM}$, determine $(\tau_1, \ldots, \tau_{n-1}) \in E^{n-1}$ tal que, $\eta_i = P_i(\tau_1, \ldots, \tau_{n-1})$.

Chamamos de *mapas inversos* para $\mathcal{P}(X, U)$ a um conjunto de funções $v_1, \ldots, v_{n-1}$ em $\{X\}$ tais que $u_j = v_j(x_1, \ldots, x_n)$, para $j = 1, \ldots, n-1$. Temos que $(P_1(U), \ldots, P_n(U))$ é um zero genérico de **ID** e, por definição, a *variedade implícita* de $\mathcal{P}(X, U)$ é

$$\mathcal{V}(\mathbf{ID}) = \{\eta \in E^n \mid f(\eta) = 0, \text{ para todo } f \in \mathbf{ID}\}.$$

Um conjunto de EDPP's é *próprio* se para um zero genérico $(a_1, \ldots, a_n)$ (e assim a maioria dos pontos) da variedade implícita, existe somente um $(\tau_1, \ldots, \tau_{n-1})$ em E^{n-1} tal que $a_i = P_i(\tau_1, \ldots, \tau_{n-1})$, para $i = 1, \ldots, n$.

Proposição 3.23 *Suponha que $\partial Res_J(F_1, \ldots, F_n) \notin K$. Então o conjunto $\mathcal{P}$ de EDPP's é próprio. Além disso, existem mapas inversos $B_j(X, U) = c_j u_j + U_j(X)$, com $c_j \in K$ e $U_j \in K\{X\}$, para todo $j \in \{1, \ldots, n-1\}$.*

Demonstração. Dado o conjunto $\mathcal{P} : \mathcal{P}(X, U)$ de EDPP's, suponha que $\partial Res_J(F_1, \ldots, F_n)$ seja não constante. Se a matriz S, definida na seção anterior, tem uma coluna nula, então temos que $\partial Res^h(H_1, \ldots, H_n) = 0$. Neste caso, o conjunto J também definido na seção anterior é não vazio. Deste modo, se $J = \varnothing$, então $\partial Res^h(H_1, \ldots, H_n) \neq 0$, e assim, a forma escalonada reduzida $E(L)$ de $M(L)$ da prova do Teorema 3.11 é uma matriz triangular. Caso $J \neq \varnothing$, tem-se que o conjunto $\mathcal{M}$ contido no espaço vetorial $K\langle det(M_{J_i}) \mid i \in \{1, \ldots, n\}\rangle$ é vazio, e então $\partial Res_J(F_1, \ldots, F_n) = 0$, por definição. Uma vez que $\partial Res_J(F_1, \ldots, F_n) \notin K$, tem-se então também que $\partial Res_J(F_1, \ldots, F_n) \neq 1$. De acordo com isso, existe $k \in \{1, \ldots, n\}$ tal que, $det(M_{Jk}) \neq 0$ é a equação implícita de $\mathcal{P}$. Portanto, a forma escalonada reduzida de M_{Jk} é uma matriz triangular. Em ambos os casos, a base de Gröbner obtida a partir da forma escalonada reduzida contém polinômios B_i lineares em u_i. Além disso, os parâmetros u_j são independentes. Segue que o conjunto $\mathcal{P}$ de EDPP's é próprio, e neste caso, existem mapas inversos $B_j(X, U) = c_j u_j + U_j(X)$, com $c_j \in K$ e $U_j \in K\{X\}$, para todo $j \in \{1, \ldots, n-1\}$. ■

O próximo resultado nos fornece uma condição necessária para que um conjunto $\mathcal{P}(X, U)$ de $EDPP$ seja próprio.

Teorema 3.24 *Se o conjunto $\mathcal{P}(X, U)$ de EDPP's é próprio, então temos que $\{\mathcal{L}_{1j}, \ldots, \mathcal{L}_{nj}\}$ é um conjunto de operadores diferenciais coprimos, para $j = 1, \ldots, n-1$.*

Demonstração. Fixada a extensão universal E do corpo diferencial K, seja $\mathcal{P}(X,U)$ um conjunto de EDPP's. Suponha que $\mathcal{P}(X,U)$ seja próprio e considere um conjunto de operadores diferenciais, digamos $\{\mathcal{L}_{1j},\ldots,\mathcal{L}_{nj}\}$. Agora, suponha por absurdo que exista $k \in \{1,\ldots,n-1\}$ de modo que $\mathcal{L}_j = MDC_d(\mathcal{L}_{1j},\ldots,\mathcal{L}_{nj}) \in K[\partial]$ e não trivial. Então existe um elemento $\eta \in E$ diferente de zero tal que, $\mathcal{L}_{ik}(\eta) = 0$, para $i = 1,\ldots,n$. Definindo o elemento $U+\eta := \{u_1,\ldots,u_k+\eta,\ldots,u_{n-1}\} \in E^{n-1}$ e, lembrando que $P_i(U) = a_i - \sum_{j=1}^{n-1} \mathcal{L}_{ij}(u_j)$, tem-se então que

$$(P_1(U+\eta),\ldots,P_n(U+\eta)) = (P_1(U),\ldots,P_n(U)),$$

e assim, segue que $\mathcal{P}(X,U)$ não é próprio, por definição, absurdo. Portanto, $\mathcal{L}_j = MDC_d(\mathcal{L}_{1j},\ldots,\mathcal{L}_{nj}) \in K[\partial]$ é trivial, ou seja, os elementos do conjunto $\{\mathcal{L}_{1j},\ldots,\mathcal{L}_{nj}\}$ sã o coprimos, para $j = 1,\ldots,n-1$. ■

Observação 3.25

Para $n = 2$, a condição no teorema anterior é também suficiente, mas para $n \geq 3$ não é verdade. De fato, tomando $K = \mathbb{C}(t)$ e $\partial = \frac{\partial}{\partial t}$, considere o sistema linear de EDPP's dado por

$$\mathcal{S}: \begin{cases} x_1 &= 2u_1 + u_{11} + u_2 + u_{22} \\ x_2 &= u_1 + u_{11} + u_{12} + u_2 + u_{22} \\ x_3 &= u_1 + 2u_{11} + u_2 + u_{21} \end{cases},$$

onde:

$$\begin{array}{lll} \mathcal{L}_{11} = 2+\partial & \mathcal{L}_{12} = 1+\partial^2 & \mathcal{L}_{21} = 1+\partial+\partial^2 \\ \mathcal{L}_{22} = 1+\partial^2 & \mathcal{L}_{31} = 1+2\partial & \mathcal{L}_{32} = 1+\partial \end{array}$$

Podemos mostrar que, apesar de $MDC_d(\mathcal{L}_{1j},\mathcal{L}_{2j},\mathcal{L}_{3j}) = 1$, o sistema $\mathcal{S}$ não é próprio (veja [31]).

Dado o sistema de $\mathcal{P}_2(x_1,x_2,u)$ de EDPP's, o algoritmo que segue retorna a sua equação implícita $A(X)$:

1. $\mathcal{L} := MDC_d(\mathcal{L}_1,\mathcal{L}_2)$.
2. Se $\mathcal{L} \notin K$ então calcula-se $\widetilde{\mathcal{L}}_i$ tal que $\mathcal{L}_i = \widetilde{\mathcal{L}}_i\mathcal{L}$ e $\mathcal{L}_i := \widetilde{\mathcal{L}}_i$, $i = 1,2$.
3. Calcula-se $\mathcal{D}_1$ e $\mathcal{D}_2$.
4. $A(X) := (\mathcal{L}_2 - \mathcal{D}_2)(x_1-\alpha_1) - (\mathcal{L}_1 - \mathcal{D}_1)(x_2-\alpha_2)$

Observação 3.26

O Maple packages OreTools, DEtools e Ore-algebra podem ser usados para calcular $MDC_d(\mathcal{L}_1, \mathcal{L}_2)$ ([1]).

Uma vez definido $\mathcal{L}_j := MDC_d(\mathcal{L}_{1j}, \ldots, \mathcal{L}_{nj})$, com $j = 1, \ldots, n-1$, existem $\widetilde{\mathcal{L}}_{ij} \in K[\partial]$ tais que $\mathcal{L}_{ij} = \widetilde{\mathcal{L}}_{ij}\mathcal{L}_j$, para $i = 1, \ldots, n$. Se $\mathcal{L}_j \in K$, então $\widetilde{\mathcal{L}}_{ij} = \mathcal{L}_{ij}$, para $j \in \{1, \ldots, n-1\}$. A partir daí, podemos definir um novo conjunto de EDPP's

$$\widetilde{\mathcal{P}}(X, U) := \begin{cases} x_1 &= \widetilde{P}_1(U) = a_1 - \widetilde{H}_i(U) \\ &\vdots \\ x_n &= \widetilde{P}_n(U) = a_n - \widetilde{H}_n(U) \end{cases},$$

onde $\widetilde{H}_i(U) = \sum_{j=1}^{n-1} \widetilde{\mathcal{L}}_{ij}(u_j)$ e $\widetilde{F}_i(U) = T_i(X) + \widetilde{H}_i(U)$.

Proposição 3.27 *Se* $\widetilde{\mathbf{ID}}$ *é o ideal implícito do conjunto* $\widetilde{\mathcal{P}}(X, U)$ *de EDPP's, então* $\mathbf{ID} = \widetilde{\mathbf{ID}}$.

Demonstração. Seja $\widetilde{\mathbf{ID}}$ o ideal implícito do conjunto $\widetilde{\mathcal{P}}(X, U)$ de EDPP's. Vamos mostrar que $\mathbf{ID} = \widetilde{\mathbf{ID}}$. De fato, por um lado, suponha que $f \in \widetilde{\mathbf{ID}}$. Logo, $f\left(\widetilde{P}_1(U), \ldots, \widetilde{P}_n(U)\right) = 0$. Em particular, para

$$\eta = (\mathcal{L}_1(u_1), \ldots, \mathcal{L}_{n-1}(u_{n-1})),$$

tem-se que $0 = f\left(\widetilde{P}_1(\eta), \ldots, \widetilde{P}_n(\eta)\right) = f(P_1(U), \ldots, P_n(U))$, e assim, $f \in \mathbf{ID}$. Portanto, $\widetilde{\mathbf{ID}} \subseteq \mathbf{ID}$. Por outro lado, seja $f \in \mathbf{ID} = [PS] \cap K[X]$. Logo existem $\mathcal{F}_i \in K[\partial]$, para $i = 1, \ldots, n$, tais que

$$f(X) = \mathcal{F}_1(F_1(X, U)) + \cdots + \mathcal{F}_n(F_n(X, U)).$$

Assim, vem que $\mathcal{F}_1(H_1(U)) + \cdots + \mathcal{F}_n(H_n(U)) = 0$ e

$$f(X) = \mathcal{F}_1(T_1(X)) + \cdots + \mathcal{F}_n(T_n(X)),$$

consequentemente, tem-se que $\mathcal{F}_1(\mathcal{L}_{1j}(u_j)) + \cdots + \mathcal{F}_n(\mathcal{L}_{nj}(u_j)) = 0$, para todo $j \in \{1, \ldots, n-1\}$. Por conseguinte, segue que

$$\left(\mathcal{F}_1\widetilde{\mathcal{L}}_{1j} + \cdots + \mathcal{F}_n\widetilde{\mathcal{L}}_{nj}\right)\mathcal{L}_j = 0,$$

e daí, uma vez observado que $\mathcal{L}_{ij} \neq 0$ (final da seção 2), tem-se que o operador diferencial $\mathcal{F}_1\widetilde{\mathcal{L}}_{1j} + \cdots + \mathcal{F}_n\widetilde{\mathcal{L}}_{nj}$ é nulo. Concluímos então que

$$\mathcal{F}_1\left(\widetilde{H}_1(U)\right) + \cdots + \mathcal{F}_n\left(\widetilde{H}_n(U)\right) = 0,$$

o que implica que $f\left(\widetilde{P}_1(U), \ldots, \widetilde{P}_n(U)\right) = 0$, e portanto, tem-se que $f \in \widetilde{\mathbf{ID}}$, ou seja, $\mathbf{ID} \subseteq \widetilde{\mathbf{ID}}$ e o resultado segue. ■

O corolário seguinte decorre diretamente do Teorema 3.11 e proposição 3.27.

Corolário 3.28 *Dado um sistema $\mathcal{P}(X,U)$, se $\partial Res^h\left(\widetilde{H}_1, \ldots, \widetilde{H}_n\right) \neq 0$, então $dim(\mathbf{ID}) = n-1$ e $\partial Res\left(\widetilde{F}_1, \ldots, \widetilde{F}_n\right)(X) = 0$ é a equação implícita de $\mathcal{P}(X,U)$.*

Revisitanto o sistema dado no início da secção 3.2, o método para calcular a sua equação implícita seria a seguinte: calcula-se o sistema $\widetilde{\mathcal{S}}_1$, e em seguida, determina-se a equação implícita de $\mathcal{S}_1$ que é

$$\partial Res\left(\widetilde{F}_1, \widetilde{F}_2, \widetilde{F}_3\right)(X) = (t-1)x_{12} - tx_{31} - (t-1)x_{32} + x_2 = 0.$$

Corolário 3.29 *Fixado $u = u_1$, colocamos $H_1(u) = \mathcal{L}_1(u)$ e $H_2(u) = \mathcal{L}_2(u)$, para operadores diferenciais $\mathcal{L}_1, \mathcal{L}_2 \in K[\partial]$. Assim, se $n = 2$, são equivalentes as seguintes afirmações:*

1. *$\mathcal{P}(X,U)$ é próprio;*
2. *$(\mathcal{L}_1, \mathcal{L}_2) = 1$;*
3. *$\partial Res(F_1, F_2) = 0$.*

Demonstração. O corolário segue da proposição 3.23, do teorema 3.24 e do teorema 2 de [10]. ■

3.7 Trabalhos Futuros

Definir e estudar a resultante diferencial generalizada para polinômios de qualquer grau.

Referências Bibliográficas

[1] S.A. Abramov, H.Q. Le, Z Li, *Univariate Ore polynomial rings in computer algebra*, Journal of Math. Sci. 131 , 5, 5885-5903,(2005).

[2] M.F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra*, AddisonWesley Publishing Co., Reading, Mass.-London-Don Mills, (1969).

[3] H. Bass, A. Buium, P. J. Cassidy, *Selected Works of Ellis Kolchin with commentary*, American Mathematical Society (1999).

[4] A. Buium, and P. J. A. Cassidy, *Differential algebraic geometry and differential algebraic groups: from algebraic differential equations to Diophantine geometry*, In: Bass, H. et al. (Eds.), Selected Works of Ellis Kolchin, with Commentary. American Mathematical Society, Providence, RI, pp. 567-636,(1998).

[5] F. Boulier, D. Lazard, F. Ollivier and M. Petitot *Representation for the radical of a finitely generated differential ideal*, Proceedings of the ISSAC'95 , 158-166,(1995).

[6] L.M. Berkovich and V.G. Tsirulik, *Differential resultants and some of their applications*, Differential Equations, Plenum Publ. Corp., 22,750-757,(1986).

[7] G. Carra'Ferro *A resultant theory for systems of two ordinary algebraic differential equations*, Applicable Algebra in Engineering, Communication and Computing , 8, 539-560,(1997).

[8] G. Carra'Ferro, *A resultant theory for ordinary algebraic differential equations*, Lecture Notes in Computer Science, 1255. Applied Algebra, Algebraic Algorithms and Error-Correcting Codes. Proceedings, (1997).

[9] S.C. Chou and X.S. Gao, *Automated reasoning in differential geometry and mechanics: part I. An improved version of Ritt–Wu's decomposition algorithm*, Automat. Reason. 10, 161-172, (1993).

[10] M. Chardin *Differential Resultants and Subresultants*, Proc. FCT'91, Lecture Notes in Computer Science 529, Springer-Verlag (1991)

[11] Chou S.C. A. and X.S. Gao, *A zero structure theorem for differential parametric systems*, J. Symbolic Comput. 16, 585-595, (1994).

[12] S. C. Chou, X. S. Gao, J. Z Zhang *Machine Proofs in Geometry: Automated Production of Readable Proofs for Geometry Theoremas*, (Series on Applied Mathematics), World Scientific Pub. Co. Inc. 400 pp (1994).

[13] D. Cox, J. Little, D. O'Shea *Ideals, Varieties and Algorithms*,2nd edn.,Springer, New York, (1997).

[14] W. Fulton, *Algebraic Curves*, W. A. Benjamin, Inc., New York, (1969).

[15] A. Galligo, *Self-intersection of bicubic surfaces*, preprint presented at ACA'2002. Volos. Greece.

[16] X.S. Gao, *Implicitization of differential rational parametric equations*, Journal of Symbolic Computation, 36 (2003), 811-824, (2003).

[17] X.S. Gao, W. Li and C. M. Yuan, *Intersection Theory in Differential Algebraic Geometry: Generic Intersection and the Differential Chow Form*, Transactions of the AMS, V. 365, N. 9, September 2013, pp. 4575-4632, (2013).

[18] L. Guangwei, *Implicitization of partial differential rational parametric equations*, Journal System Science and Complexity, 19 256-265 (2006).

[19] E.R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, London, (1973).

[20] M. Kreuzer and L. Robbiano, *Computational Commutative Algebra 1*, Springer-Verlag (1991).

[21] P. Loustaunau and A. William, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics, Vol. 3. Providence, Rhode Island: American Mathematical Society, (1994).

[22] F.S. Macaulay *The Algebraic Theory of Modular Systems*, Proc. Cambridge Univ. Press., Cambridge, (1916).

[23] A. Magid, *Lectures on Differential Galois Theory*, University Lecture Series, vol. 7, American Mathematical Society, Providence, RI, (1994).

[24] J.S. Milne, *Commutative Algebra*, v4.01, (2014).

[25] , B. Mishra, *Algorithmic Algebra*, Texts Monog. Comput. Sei., Springer-Verlag, New York, Berlin, Heidelberg (1993).

[26] G. Matera and A. Sedoglavic, *The differential Hilbert function of a differential rational mapping can be computed in polynomial time*, In: Proc. ISSAC'2002. ACM Press, New York, pp. 184-191, (2002).

[27] F. Orecchia, *Implicitization of a general union of parametric varieties*, J. Symbolic Comput. 31, 343-356, (2001).

[28] S. Perez-Diaz, J.R. Sendra, F. Winkler, *Rational Algebraic Curves: A Computer Algebra Approach*, Series: Algorithms and Computation in Mathematics, Vol. 22. Springer Verlag (2007).

[29] J.F. Ritt *Differential Algebra*, Amer. Math. Soc. Colloquium, New York, (1950).

[30] A. Rosenfeld, *Specialization in differential algebra*, Trans. Amer. Math. Soc. 90, 394-407, (1959).

[31] S. L. Rueda and J. R. Sendra *Implicitization of Linear DPPEs by Differential Resultants*, Journal of Symbolic Computation, Vol. 45, pg 324-341, (2010).

[32] V.G. Tsirulik, *Differential Equations*, (in Russian), RGPI, Pedagogical Institutes RSFSR, Rayzan, 133-140,(1981).

[33] R. Walker, *Algebraic Curves*, Springer Verlag, New York, (1978).

[34] A. Weil, *Foundations of algebraic geometry*, A.M.S. Colloquium Publ. 29, New-York, 1946.

[35] W.T. Wu, *A constructive theory of differential algebraic geometry*, LNM, vol. 1255. Springer, Berlin,Heidelberg, pp. 173-189, (1987).

[36] W.T. Wu, *Basic Principles of Mechanical Theorem Proving in Geometries*, Springer-Verlag, Berlin (original work published 1984,Science Press. Beijing(in Chinese)), (1994).