UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
INSTITUTO DE MATEMÁTICA

Cláudio Cesar Saccomori Júnior

Famílias de variedades involutivas mínimas em $\mathbb{P}^3$

Rio de Janeiro
Novembro de 2014

Cláudio Cesar Saccomori Júnior

Famílias de variedades involutivas mínimas em $\mathbb{P}^3$

Tese apresentada para obtenção do Título de Doutor em Matemática

Universidade Federal do Rio de Janeiro
Instituto de Matemática

Orientador: Severino Collier Coutinho

2014

Cláudio Cesar Saccomori Júnior

Famílias de variedades involutivas mínimas em $\mathbb{P}^3$

Tese submetida ao corpo docente do Instituto de Matemática da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requesitos necessários à obtenção do grau de Doutor em Ciências.

Área de concentração: Matemática

Aprovado, em 11 de novembro de 2014, por:

Prof. Dr. Severino Collier Coutinho (Presidente), UFRJ

Prof. Dr. Daniel Levcovitz, USP-São Carlos

Prof. Dr. Gabriel Calsamiglia, UFF

Prof. Dr. Guilherme Leal, UFRJ

Prof. Dr. Marco Pacini, UFF

Aos meus pais.

Agradecimentos

Agradeço primeiramente ao Severino Collier Coutinho por sua paciência e dedicação. Além de matemática, adquiri com o Collier, através de seu comportamento, valores que levarei comigo por toda a vida.

Agradeço aos meus pais pelo apoio incondicional e à minha esposa Priscila pela compreensão dos esforços necessários à realização deste trabalho.

Agradeço aos professores do IM/UFRJ. Em especial, agradeço ao Guilherme Leal.

Agradeço aos meus colegas do DEMAT/UFRRJ que permitiram minha dedicação exclusiva ao doutorado durante 4 anos.

Agradeço aos membros da banca por suas críticas e sugestões que enriqueceram este trabalho.

Finalmente, agradeço a Deus.

Resumo

Em 1989, Valery Lunts [15] mostrou que um polinômio homogêneo genérico define uma hipersuperfície involutiva mínima. No entanto, até o presente momento, um único exemplo concreto de uma tal variedade é conhecido; veja [2].

Neste trabalho, apresentaremos dois critérios para determinar se uma superfície em $\mathbb{P}^3$ é involutiva mínima. A partir do primeiro critério, construiremos exemplos explícitos de famílias infinitas de superfícies involutivas mínimas de graus 3 e 4. Enquanto o primeiro critério se restringe a variedades de grau 3 ou 4, o segundo se aplica a variedades de grau maior ou igual a 5, mas requer que a variedade possua número de Picard igual a 1. Usando este segundo critério, mostraremos que as variedades de Shioda

$$\mathcal{Z}(u^k + x(x+y)^{k-1} + (x+y)z^{k-1} + zx^{k-1})$$

são involutivas mínimas para $k = 5$ e $k = 7$.

Palavras-chave: Geometria algébrica; Geometria projetiva; Variedades.

Abstract

In 1989, Valery Lunts [15] proved that a generic homogeneous polynomial defines a minimal involutive hypersurface. However, up to now, only one concrete example of this variety is known; see [2].

In this work, we present two criteria to determine if a surface in $\mathbb{P}^3$ is minimal involutive. The first criterion is used to construct explicit examples of an infinite family of minimal involutive surfaces of degree 3 and 4. While the first criterion is restricted to varieties of degree 3 or 4, the second one applies to varieties of degree higher or equal to 5, but only applies to surfaces of Picard number equal to 1. Using this second criterion, we prove that Shioda's varieties

$$\mathcal{Z}(u^k + x(x+y)^{k-1} + (x+y)z^{k-1} + zx^{k-1})$$

are minimal involutive if $k = 5$ or $k = 7$.

Keywords: Algebraic geometry; Projective geometry; Varieties.

Sumário

Introdução

Seja $\mathcal{A}_n$ a n-ésima álgebra de Weyl, ou seja, a $\mathbb{C}$-subálgebra de $End_{\mathbb{C}}(\mathbb{C}[x_1, \ldots, x_n])$ gerada pelos operadores $\hat{x}_1, \ldots, \hat{x}_n$ e $\partial_1, \ldots, \partial_n$, definidos por $\hat{x}_i(f) = x_i f$ e por $\partial_i(f) = \partial f / \partial x_i$. Considerando a filtração de Bernstein $\mathcal{B} = \{B_k\}$, em que B_k é o espaço vetorial de base $\{x^\alpha \partial^\beta : |\alpha| + |\beta| \leq k\}$ e $B_{-1} = \{0\}$, temos a álgebra graduada:

$$gr\mathcal{A}_n = \bigoplus_{k \geq 0} B_k / B_{k-1} = \bigoplus_{k \geq 0} \Sigma_k$$

e as aplicações símbolos $\sigma_k : B_k \to \Sigma_k = B_k / B_{k-1}$. Denotando $x_i = \sigma_1(\hat{x}_i)$ e $x_{n+i} = \sigma_1(\partial_i)$, podemos verificar que $x_1, \ldots, x_{2n}$ geram $gr\mathcal{A}_n$ como uma $\mathbb{C}$-álgebra comutativa livre [7, Theorem 7.3.1, pg. 58]. Logo, $gr\mathcal{A}_n \simeq \mathbb{C}[x_1, \ldots, x_{2n}]$.

1. $\mathcal{A}_n$-módulos não holônomos.

A um $\mathcal{A}_n$-módulo à esquerda finitamente gerado M, podemos associar seu ideal característico $\mathcal{I}(M) \subset \mathbb{C}[x_1, \ldots, x_{2n}]$ e, portanto, sua variedade característica $Ch(M)$; veja [7, Chapter 11 §1]. No caso particular em que $d \in B_k$ e $M = \mathcal{A}_n / \mathcal{A}_n d$, temos que $\mathcal{I}(M)$ é o radical de $\mathbb{C}[x_1, \ldots, x_{2n}] \cdot \sigma_k(d)$ e, portanto, $Ch(M) = \mathcal{Z}(\sigma_k(d))$ é uma hipersuperfície em $\mathbb{C}^{2n}$.

Até 1985, acreditava-se que se um $\mathcal{A}_n$-módulo M era irredutível, então M era holônomo; isto é, $\dim(Ch(M)) = n$. Contudo, J. T. Stafford [23] construiu um contra-exemplo concreto de um módulo irredutível não holônomo. Especificamente, supondo que $d \in B_k$ gera um ideal máximo à esquerda $I = \mathcal{A}_n d$, então, por um lado, $M = \mathcal{A}_n/I$ é irredutível. Por outro, $\mathcal{I}(M)$ é gerado por $\sigma_k(d)$. Em particular, $\dim(Ch(M)) = 2n-1$. Dessa forma, se $n > 1$, segue-se que M é irredutível e não é holônomo. Stafford mostrou que se

$$d = \partial_1 + \sum_{i=2}^{n}(\lambda_i x_i x_1 + 1)\partial_i + \sum_{i=2}^{n} 2x_i,$$

em que $\lambda_2, \ldots, \lambda_n \in \mathbb{C}$ são linearmente independentes sobre $\mathbb{Q}$, então $\mathcal{A}_n d$ é um ideal máximo à esquerda.

Em 1988, J. Bernstein e V. Lunts [5] mostraram que se $n = 2, k \geq 4$ e $F \in \Sigma_k$ é um polinômio genérico, então, para cada operador $d \in B_k$, tal que $\sigma_k(d) = F$, temos que o ideal $\mathcal{A}_n d$ é máximo à esquerda. Na verdade, eles mostraram um resultado um pouco mais forte usando geometria simplética.

2. Geometria simplética.

Seja $\mathbb{C}^{2n}$ munido da 2-forma simplética

$$\omega = \sum_{i=1}^{n} dx_{i+n} \wedge dx_i.$$

A cada polinômio $F \in \mathbb{C}[x_1, \ldots, x_{2n}]$, podemos associar um campo de vetores h_F através da equação $\omega(\cdot, h_F) = dF$. Em termos algébricos, este campo corresponde à derivação $\delta_F \in Der_{\mathbb{C}}(\mathbb{C}[x_1, \ldots, x_{2n}])$ definida por

$$\delta_F = \sum_{i=1}^{n} \left(\frac{\partial F}{\partial x_{i+n}} \frac{\partial}{\partial x_i} - \frac{\partial F}{\partial x_i} \frac{\partial}{\partial x_{i+n}} \right).$$

Uma variedade V é involutiva, se seu ideal é fechado para o colchete de Poisson. Em outras palavras, se para todo $F \in \mathcal{I}(V)$, verifica-se que $\delta_F(\mathcal{I}(V)) \subset \mathcal{I}(V)$. Se V é involutiva e não admite subvariedade involutiva própria, então V é involutiva mínima.

Variedades involutivas mínimas têm uma estreita relação com módulos não holônomos. Especificamente, se $\sigma_k(d)$ é irredutível e $\mathcal{Z}(\sigma_k(d))$ é mínima, então d gera um ideal à esquerda máximo [7, Proposition 11.3.1, pg. 105]. Em particular, $\mathcal{A}_n/\mathcal{A}_n d$ é irredutível e não holônomo, se $n > 1$. O interessante é que a maioria das superfícies em $\mathbb{C}^{2n}$ são mínimas. De maneira mais precisa: em 1989, Lunts [15] generalizou o resultado obtido em [5], provando o seguinte teorema.

Teorema *Sejam $n \geq 2$, $k \geq 4$ e $F \in \Sigma_k$ um polinômio genérico. Então (F) é o único ideal homogêneo não trivial de dimensão positiva que é preservado por δ_F.*

Vejamos o que significa um polinômio ser genérico. Seja $\mathscr{S}(2n, k)$ o conjunto dos polinômios homogêneos de grau k em $2n$ variáveis. De forma natural, $\mathscr{S}(2n, k)$ está identificado com o espaço afim de dimensão $\binom{2n+k-1}{k}$. Agora, tome N o conjunto dos polinômios F's para os quais δ_F preserva algum ideal não trivial de dimensão positiva além de (F). O teorema afirma que N está contido em uma união enumerável de hipersuperfícies de $\mathscr{S}(2n, k)$.

Como consequência deste teorema, um polinômio homogêneo genérico define uma variedade involutiva mínima. Apesar disto, só há na literatura um exemplo explícito de variedade mínima; exibido por L. C. Almeida e S. C. Coutinho em [2]. O objetivo deste trabalho é construir exemplos concretos de famílias de superfícies involutivas mínimas em $\mathbb{P}^3$. Para tanto, apresentamos dois critérios que determinam se uma superfície em $\mathbb{P}^3$ é involutiva mínima.

No capítulo 1, fazemos um breve estudo sobre bases de Gröbner. Além disso, reunimos alguns resultados sobre derivações, campos e a relação entre eles. No capítulo 2, exibimos um critério para determinar se um polinômio $F \in \mathbb{Q}[u, x, y, z]$ de grau 3 ou 4 define uma variedade mínima. Ao polinômio F, podemos associar um campo de retas ρ_F a partir da desomogenização do hamiltoniano de F. Uma das condições do critério apresentado é que as singularidades de ρ_F estejam todas na parte afim $D_+(u)$, que sejam em número finito e estejam em posição u-normal. Para verificar essas duas últimas condições, precisamos calcular uma base de Gröbner para o ideal das singularidades de θ_u, em que θ_u é um campo vetorial que representa

ρ_F em $D_+(u)$. Para o cálculo desta base, usamos o sistema de computação algébrica Singular. Contudo, duas outras condições do critério não são, de maneira imediata, verificáveis computacionalmente. Para contornar esta questão, determinamos, na seção §2.3, condições equivalentes às do critério e que podem ser verificadas pelo Singular. Aplicando o critério, temos, por exemplo, que

$$y^3 + u^2x + 2x^2u + 3z^3$$

define uma variedade involutiva mínima.

Nas seções seguintes, a partir de um número primo q, definimos uma relação de equivalência entre polinômios com coeficientes inteiros, cujas bases para os ideais das singularidades apresentam certas características. Usando esta relação de equivalência, estendemos o critério apresentado inicialmente e exibimos condições para determinar toda uma família de variedades involutivas mínimas. Mostramos, por exemplo, que

$$\{y^3 + u^2x + 2x^2u + (3 + 7n)z^3 : n \in \mathbb{Z}\} \quad \text{e}$$
$$\{y^4 + u^3x + 2x^3u + (3 + 61n)z^4 + x^2y^2 + u^3y : n \in \mathbb{Z}\}$$

determinam famílias infinitas de variedades involutivas mínimas.

No capítulo 3, apresentamos um critério que se aplica a polinômios de grau maior ou igual a 5. Porém, este segundo critério requer que $\mathcal{Z}(F)$ possua número de Picard igual a 1. Através deste critério, concluímos que, se $k = 5$ ou $k = 7$, então a variedade de Shioda

$$\mathcal{Z}(u^k + x(x + y)^{k-1} + (x + y)z^{k-1} + zx^{k-1}) \tag{1}$$

é involutiva mínima.

T. Shioda [20] mostrou que as variedades como em (1) têm número de Picard igual a 1, sempre que k for primo. No entanto, por limitações computacionais no cálculo da base de Gröbner do ideal das singularidades, não pudemos verificar as condições do nosso critério, para $k \geq 11$. Esperamos, no futuro, otimizar o critério, de forma que as limitações computacionais possam ser contornadas.

Como observação final, lembre-se que se $\sigma_k(d)$ é irredutível e $\mathcal{Z}(\sigma_k(d))$ é involutiva mínima, então d induz um módulo irredutível e não holônomo. Assim, as famílias de variedades involutivas mínimas citadas anteriormente nos dizem que, se $d \in \mathcal{A}_2$ é da forma:

$$\partial_1^3+\hat{x}_1^2\hat{x}_2+2\hat{x}_2^2\hat{x}_1+(3+7n)\partial_2^3+P \quad \text{ou} \quad \partial_1^4+\hat{x}_1^3\hat{x}_2+2\hat{x}_2^3\hat{x}_1+(3+61n)\partial_2^4+\hat{x}_2^2\partial_1^2+\hat{x}_1^3\partial_1+Q,$$

em que $n \in \mathbb{Z}$ e P e Q são operadores em B_2 e B_3, respectivamente, então $\mathcal{A}_2/\mathcal{A}_2 d$ é um $\mathcal{A}_2$-módulo irredutível e não holônomo.

Capítulo 1

Preliminares

Nesta capítulo, reunimos alguns resultados sobre bases de Gröbner, campos e derivações que serão úteis ao longo de todo o texto.

1.1 Base de Gröbner

Nesta seção, faremos um breve estudo sobre um tipo especial de sistema de geradores de um ideal.

Sejam $A = \mathbb{Q}[x_1, \ldots, x_m]$ e $f \in A$. Considerando a ordem lexicográfica para a qual $x_1 > x_2 > \ldots > x_m$, denote por $\mathrm{lt}(f)$ o termo líder de f. No caso em que I é um ideal de A, definimos $\mathrm{lt}(I)$ como o ideal gerado por $\{\mathrm{lt}(f) : f \in I\}$. Seja, agora, $G = \{g_1, \ldots, g_n\} \subset I$. Dizemos que G é uma *base de Gröbner* para I, se $\mathrm{lt}(I)$ é gerado por $\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_n)\}$. Neste caso, $I = (G)$; veja [8, Corolário 5.2, pg. 144].

Bases de Gröbner têm uma estreita relação com divisão de polinômios em várias variáveis. Para entendermos essa relação, começamos com o seguinte resultado:

Teorema 1.1.1 *Sejam $\varphi, g_1, \ldots, g_n \in \mathbb{Q}[x_1, \ldots, x_m]$. Então existem polinômios $q_1, \ldots, q_n, r$, tais que*

$$\varphi = q_1 g_1 + \cdots + q_n g_n + r, \tag{1.1}$$

em que:

a) nenhum termo de r pertence ao ideal gerado por $\operatorname{lt}(g_1), \ldots, \operatorname{lt}(g_n)$*;*

b) $\operatorname{lt}(\varphi) = \max\{\operatorname{lt}(q_1 g_1), \ldots, \operatorname{lt}(q_n g_n), \operatorname{lt}(r)\}$.

Demonstração. [8, Teorema 4.5, pg. 135]. ∎

O teorema acima generaliza a divisão de polinômios em uma única variável. No entanto, no caso de várias variáveis, não há unicidade em (1.1). Porém, se $G = \{g_1, \ldots, g_n\}$ é uma base de Gröbner para $I = (G)$, então temos a unicidade do resto r; [8, Corolário 5.4, pg. 147]. De forma equivalente, $\varphi \in I$ se, e somente se, $r = 0$. De agora em diante, uma decomposição de φ, como no teorema, será chamada de uma *divisão* de φ por $g_1, \ldots, g_n$.

Entre as bases de Gröbner de um ideal, destacamos a base reduzida. Especificamente, dizemos que uma base de Gröbner $G = (g_1, \ldots, g_n)$ é *reduzida*, se g_i é mônico, qualquer que seja i, e se $\operatorname{lt}(g_i)$ não divide nenhum termo de g_j, sempre que $i \neq j$. É importante destacar que todo ideal de $\mathbb{Q}[x_1, \ldots, x_m]$ admite uma única base de Gröbner reduzida; veja [8, Proposição 5.9, pg. 163].

Bruno Buchberger descobriu, em sua tese de doutoramento [6], um algoritmo que nos fornece uma base de Gröbner para o ideal I usando, como ponto de partida, um conjunto gerador de I. Se $I = (g_1, \ldots, g_n)$, definimos o S-polinômio de g_i e g_j como sendo

$$S(g_i, g_j) = \frac{\operatorname{lt}(g_j)}{\delta} g_i - \frac{\operatorname{lt}(g_i)}{\delta} g_j, \ \text{ em que } \ \delta = \operatorname{mdc}\big(\operatorname{lt}(g_i), \operatorname{lt}(g_j)\big).$$

O algoritmo de Buchberger, baseia-se no seguinte critério.

Critério de Buchberger. $G = \{g_1, \ldots, g_n\}$ *é uma base de Gröbner para* $I = (G)$ *se, e somente se, para toda divisão de* $S(g_i, g_j)$ *por* G*, temos que* $r = 0$*, quaisquer que sejam* $i, j \in \{1, \ldots, n\}$.

Demonstração. [8, pg. 154]. ■

Não faremos aqui um estudo do algoritmo de Buchberger, mas usaremos o seu critério para exibir uma base de Gröbner que terá um papel central no decorrer do texto.

Exemplo 1.1.2 Sejam $f, g, h \in \mathbb{Q}[y]$ polinômios em uma única variável y. Considerando a ordem lexicográfica em que $x > z > y$, temos que $G = \{f, x - g, z - h\}$ é uma base de Gröbner para o ideal $I = (G)$ de $\mathbb{Q}[x, y, z]$. De fato, seja $c = \mathrm{lt}(f)$ e suponha que

$$x \cdot f - c \cdot (x - g) = q_1 \cdot f + q_2 \cdot (x - g) + q_3 \cdot (z - h) + r \tag{1.2}$$

é uma divisão de $S(f, x - g) = x \cdot f - c \cdot (x - g)$ por G. Pelo item (a) do teorema 1.1.1, nem x, nem z, dividem algum termo de r, ou seja, $r \in \mathbb{Q}[y]$. Além disso, $\deg r < \deg f$, pois $c = \mathrm{lt}(f)$ também não divide nenhum termo de r. Agora, tomando $x = g$ e $z = h$ em (1.2), segue-se que $x \cdot f = q_1(g, y, h) \cdot f + r$. Portanto, f divide r. Assim, de $\deg r < \deg f$, obtemos que $r = 0$.

No caso de uma divisão por G do S-polinômio $S(f, z - h)$, temos que a demonstração de que $r = 0$ é inteiramente análoga ao caso $S(f, x - g)$, pois não usamos em nenhum momento a relação $x > z$. Usamos apenas que $x > y$ e que $z > y$. Quanto a $S(x - g, z - h) = z \cdot (x - g) - x \cdot (z - h)$, suponha que

$$z \cdot (x - g) - x \cdot (z - h) = q_1 \cdot f + q_2 \cdot (x - g) + q_3 \cdot (z - h) + r \tag{1.3}$$

é uma divisão. Como antes, $r \in \mathbb{Q}[y]$ e $\deg r < \deg f$. Tomando $x = g$ e $z = h$ em (1.3), segue-se que $0 = q_1(g, y, h) \cdot f + r$. Se $q_1(g, y, h) = 0$, então $r = 0$. Se $q_1(g, y, h) \neq 0$, então f divide r, de modo que $r = 0$. Em qualquer dos casos, temos que r é nulo. Dessa forma, todos os S-polinômios têm resto zero, quaisquer que sejam as divisões por G. Aplicando o critério de Buchberger, obtemos que G é uma base de Gröbner para $I = (G)$. □

No exemplo acima, temos que $(G) \cap \mathbb{Q}[y]$ é gerado por f. Isto pode ser demonstrado diretamente ou como consequência do seguinte resultado mais geral.

Proposição 1.1.3 *Seja I um ideal de $\mathbb{Q}[y_1, \ldots, y_m, x_1, \ldots, x_n]$. Se G é uma base de Gröbner para I, com respeito à ordem lexicográfica em que $y_1 < \cdots < y_m < x_1 < \cdots < x_n$, então $G \cap \mathbb{Q}[y_1, \ldots, y_m]$ é uma base de Gröbner para $I \cap \mathbb{Q}[y_1, \ldots, y_m]$.*

Demonstração. [8, Proposição 6.13, pg. 210]. ∎

1.2 Derivações e Campos

Sejam A uma K-álgebra, M um A-módulo e $\delta : A \to M$ uma aplicação K-linear. Dizemos que δ é uma *K-derivação* de A em M se satisfaz a regra de Leibniz, ou seja,

$$\delta(ab) = a\delta(b) + b\delta(a), \forall a, b \in A.$$

O conjunto das K-derivações de A em A será denotado por $\mathrm{Der}_K(A)$. Sejam I ideal de A e $\delta \in \mathrm{Der}_K(A)$. Dizemos que I é *invariante* por δ se $\delta(I) \subset I$.

Proposição 1.2.1 *Sejam A uma K-álgebra e $\delta \in Der_K(A)$. Se I é um ideal de A invariante por δ, então seu radical $\sqrt{I}$ também é invariante.*

Demonstração. Sejam $a, b \in A$. Se $k \in \mathbb{N}$, então $\delta(a^{k+1}) = (k+1)a^k\delta(a)$ e

$$\delta^k(a^{k+1}b) = \delta^{k-1}\big(\delta(a^{k+1}b)\big) = \delta^{k-1}\big((k+1)a^k\delta(a)b + a^{k+1}\delta(b)\big).$$

Em particular, $\delta^k(a^{k+1}b)$ é da forma $\delta^{k-1}(a^k b_1)$, para algum $b_1 \in A$. Aplicando recursivamente este argumento, $\delta^k(a^{k+1}b) = \delta(a^2 b_{k-1}) = a^2\delta(b_{k-1}) + b_{k-1}a\delta(a)$ e concluímos que a divide $\delta^k(a^{k+1}b)$. Suponha, agora, que $a \in \sqrt{I}$. Tome $n \in \mathbb{N}^*$, tal que $a^n \in I$. Se $0 \leq i < n$, então

$$\begin{aligned}
\delta^{n-i}\big(a^{n-i}\delta(a)^i\big) &= \delta^{n-i-1}\big(\delta(a^{n-i}\delta(a)^i)\big)\\
&= \delta^{(n-i)-1}\big((n-i)a^{(n-i)-1}\delta(a)^{i+1} + a^{n-i}\delta(\delta(a)^i)\big)\\
&\equiv (n-i)\delta^{(n-i)-1}\big(a^{(n-i)-1}\delta(a)^{i+1}\big) \mod \sqrt{I},
\end{aligned}$$

pois $\delta^{(n-i)-1}$ é K-linear e a divide $\delta^{(n-i)-1}\big(a^{n-i}\delta(\delta(a)^i)\big)$. Com isso, em $A/\sqrt{I}$,

$$\delta^n(a^n) = n\delta^{n-1}(a^{n-1}\delta(a)) = \ldots = \frac{n!}{(n-i)!}\delta^{n-i}(a^{n-i}\delta(a)^i) = \ldots = n!\delta(a)^n.$$

Contudo, pela invariância de I, temos que $\delta^n(a^n) \in I$. Logo, $n!\delta(a)^n \in \sqrt{I}$. Assim, $\delta(a) \in \sqrt{I}$ e provamos a invariância de $\sqrt{I}$ por δ. ■

Proposição 1.2.2 *Sejam A uma K-álgebra, $\delta \in Der_K(A)$ e $I = \cap_{\lambda\in\Lambda}\mathfrak{p}_\lambda$ um ideal de A, dado por uma interseção de ideais primos. Se, para cada $\lambda \in \Lambda$, vale $I \subsetneq \cap_{k\neq\lambda}\mathfrak{p}_k$, então δ preserva I se, e somente se, preserva cada $\mathfrak{p}_\lambda$.*

Demonstração. Se δ preserva I e $a \in \mathfrak{p}_\lambda$, então, tomando $b \in \cap_{k\neq\lambda}\mathfrak{p}_k \setminus I$, segue-se que $ab \in I$. Portanto, $\delta(ab) \in I \subset \mathfrak{p}_\lambda$ e

$$b\delta(a) = \delta(ab) - a\delta(b) \in \mathfrak{p}_\lambda.$$

Como $b \notin \mathfrak{p}_\lambda$, temos que $\delta(a) \in \mathfrak{p}_\lambda$ e $\mathfrak{p}_\lambda$ é invariante. Reciprocamente, se $\delta(\mathfrak{p}_\lambda) \subset \mathfrak{p}_\lambda$, para todo $\lambda \in \Lambda$, então $\delta(I) \subset \cap_{\lambda\in\Lambda}\mathfrak{p}_\lambda = I$. ■

Se I é um ideal de A invariante por δ, temos uma derivação $\bar{\delta}$ induzida no quociente $B = A/I$,

$$B \ni \bar{a} \mapsto \overline{\delta(a)} \in B.$$

Além disso, se $\mathfrak{m}$ é um ideal primo de B, então, é de fácil verificação, que $\bar{\delta}$ passa à localização,

$$\begin{aligned}
\delta_\mathfrak{m} : B_\mathfrak{m} &\to B_\mathfrak{m}\\
\frac{b}{s} &\mapsto \frac{s\bar{\delta}(b) - b\bar{\delta}(s)}{s^2}
\end{aligned}$$

e temos $\delta_{\mathfrak{m}} \in \mathrm{Der}_K(B_{\mathfrak{m}})$. Suponha, agora, que a imagem de $\delta_{\mathfrak{m}}$ esteja contida no ideal máximo $\underline{\mathfrak{m}} := \mathfrak{m}B_{\mathfrak{m}}$ de $B_{\mathfrak{m}}$. Então, $\delta_{\mathfrak{m}}$ induz uma K-derivação Δ de $B_{\mathfrak{m}}$ em $\underline{\mathfrak{m}}/\underline{\mathfrak{m}}^2$. Especificamente,

$$\begin{aligned} \Delta : B_{\mathfrak{m}} \to \; & \underline{\mathfrak{m}}/\underline{\mathfrak{m}}^2 \\ f \mapsto \; & \overline{\delta_{\mathfrak{m}}(f)}. \end{aligned} \tag{1.4}$$

Exemplo 1.2.3 Sejam $A = \mathbb{C}[x_1, \ldots, x_m]$ e $\theta = \sum_{i=1}^m h_i \frac{\partial}{\partial x_i}$ um campo vetorial em $\mathbb{C}^m$. De maneira natural, identificamos θ com a derivação

$$\begin{aligned} \theta : A \; & \to A \\ f \; & \mapsto \sum_{i=1}^{m} h_i \frac{\partial f}{\partial x_i}. \end{aligned}$$

Se I é um ideal invariante por θ, tome $X = \mathcal{Z}(I)$ e $B = A/\sqrt{I}$. Por 1.2.1, $\sqrt{I}$ é invariante por θ. Além disso, se $p \in X$ é tal que $h_i(p) = 0$, para todo $i = 1, \ldots, m$, então, tomando $\mathfrak{m}$ como sendo o ideal de B associado a p, temos que $\mathrm{im}\,(\bar{\theta}) \subset \mathfrak{m}$. Portanto, $\mathrm{im}\,(\theta_{\mathfrak{m}}) \subset \underline{\mathfrak{m}}$. Tomando Δ como em (1.4), temos uma derivação

$$\begin{aligned} \Delta : B_{\mathfrak{m}} \to \; & \underline{\mathfrak{m}}/\underline{\mathfrak{m}}^2 \\ f \mapsto \; & \overline{\sum_{i=1}^{m} h_i \frac{\partial f}{\partial x_i}} \end{aligned} \tag{1.5}$$

do anel local de p no dual de seu espaço tangente. $\square$

Sejam $\theta = \sum_{i=1}^m h_i \frac{\partial}{\partial x_i}$ um campo em $\mathbb{C}^m$ e $p \in \mathbb{C}^m$. Dizemos que p é uma *singularidade* de θ, ou um ponto *singular* de θ, se $h_i(p) = 0$, para todo $i = 1, \ldots, m$. O conjunto de todas as singularidades de θ será denotado por $\mathrm{Sing}(\theta)$. Além disso, dada uma subvariedade X de $\mathbb{C}^m$, dizemos que θ *preserva* X se θ é tangente a X em todo ponto não singular de X.

Proposição 1.2.4 *Sejam $\theta = \sum_{i=1}^m h_i \frac{\partial}{\partial x_i}$ um campo vetorial em $\mathbb{C}^m$, I um ideal de $A = \mathbb{C}[x_1, \ldots, x_m]$ invariante por θ e $X = \mathcal{Z}(I)$. Se $p \in \mathrm{Sing}(\theta) \cap X$, então T_pX é subespaço vetorial de $\mathbb{C}^m$ invariante pelo jacobiano $J_p(\theta)$ do campo no ponto p.*

Demonstração. Sejam $f \in I$ e $\xi \in T_pX$. Tomando $B = A/\sqrt{I}$ e $\mathfrak{m}$ o ideal máximo que corresponde a p, defina Δ como em (1.5). Por um lado, $\Delta(f) = 0$, pois $f = 0$ em $B_{\mathfrak{m}}$. Por outro, denotando por $d_p(g) = \sum_{j=1}^{m} \frac{\partial g}{\partial x_j}(p)dx_j$ a diferencial de g no ponto p e considerando a identificação $\bar{g} \mapsto d_pg$ entre $\underline{\mathfrak{m}}/\underline{\mathfrak{m}}^2$ e $(T_pX)^*$, temos que $\Delta(f)$ agindo em ξ se dá por:

$$\begin{aligned}
\Delta(f)(\xi) &= d_p\left(\sum_{i=1}^{m} h_i \frac{\partial f}{\partial x_i}\right)(\xi) \\
&= \sum_{i=1}^{m}\left(\sum_{j=1}^{m} \frac{\partial h_i}{\partial x_j}(p)\frac{\partial f}{\partial x_i}(p)dx_j + h_i(p)\frac{\partial^2 f}{\partial x_i \partial x_j}(p)dx_j\right)(\xi) \\
&= \sum_{i=1}^{m}\left(\sum_{j=1}^{m} \frac{\partial h_i}{\partial x_j}(p)\frac{\partial f}{\partial x_i}(p)\right) dx_j(\xi),
\end{aligned}$$

pois p é ponto singular do campo. Assim,

$$0 = \sum_{i=1}^{m} \frac{\partial f}{\partial x_i}(p)\left(\sum_{j=1}^{m} \frac{\partial h_i}{\partial x_j}(p)dx_j(\xi)\right) = \sum_{i=1}^{m} \frac{\partial f}{\partial x_i}(p)dx_i\big(J_p(\theta)\xi\big) = d_pf\big(J_p(\theta)\xi\big).$$

Sendo f e ξ arbitrários, $J_p(\theta)(T_pX) \subset T_pX$. ■

Proposição 1.2.5 *Sejam $A = \mathbb{C}[x_1, \ldots, x_m]$ e $\theta = \sum_{i=1}^{m} h_i \frac{\partial}{\partial x_i}$ um campo vetorial em $\mathbb{C}^m$. Se $X \subset \mathbb{C}^m$ é subvariedade, então θ preserva X se, e somente se, $\mathcal{I}(X)$ é invariante por θ.*

Demonstração. Seja $X = \cup_{i=1}^{n} X_i$ a decomposição de X em irredutíveis. Para cada i, tome o aberto $\mathfrak{a}_i = X_i \setminus (\mathrm{Sing}(X) \cap X_i)$ não vazio de X_i. Pela irredutibilidade dos X_i's, temos, para todo i, que $\mathfrak{a}_i$ é denso em X_i. Assim,

$$X \setminus \mathrm{Sing}(X) = (\cup_{i=1}^{n} X_i) \setminus \mathrm{Sing}(X) = \cup_{i=1}^{n} \mathfrak{a}_i$$

é denso em X. Consequentemente, uma função regular se anula em X se, e somente se, se anula em $X \setminus \mathrm{Sing}(X)$. Portanto,

$$\theta(\mathcal{I}(X)) \not\subset \mathcal{I}(X) \iff \exists f \in \mathcal{I}(X) \text{ e } p \in X \setminus \mathrm{Sing}(X), \text{ tais que } \theta(f)(p) \neq 0.$$

Por outro lado,

$$\theta(f)(p) = \sum_{i=1}^{m} h_i(p)\frac{\partial f}{\partial x_i}(p) = \sum_{i=1}^{m} \frac{\partial f}{\partial x_i}(p)dx_i\big(\theta(p)\big) = d_p(f)\big(\theta(p)\big).$$

Logo, $\mathcal{I}(X)$ não é invariante por θ se, e somente se, existe um ponto p não singular de X, em que $\theta(p) \notin T_pX$. E o resultado segue. ■

Corolário 1.2.6 *Sejam $\theta = \sum_{i=1}^{m} h_i \frac{\partial}{\partial x_i}$ um campo vetorial em $\mathbb{C}^m$ e X uma subvariedade de $\mathbb{C}^m$. Então, θ preserva X se, e somente se, preserva cada um dos componentes irredutíveis de X.*

Demonstração. Seja $X = X_1 \cup \ldots \cup X_n$ a decomposição de X em irredutíveis. Denotando $\mathfrak{p}_i = \mathcal{I}(X_i)$, com $i = 1, \ldots, n$, temos que $\mathcal{I}(X) = \cap_{i=1}^{n}\mathfrak{p}_i$ satisfaz as condições da proposição 1.2.2. Portanto, $\mathcal{I}(X)$ é invariante por θ se, e somente se, cada $\mathcal{I}(X_i)$ também é invariante, que por sua vez, equivale a θ preservar cada componente de X. ■

1.3 Campo de Retas

Passemos agora ao caso projetivo. Um campo vetorial $\theta = \sum_{i=0}^{m} h_i \frac{\partial}{\partial x_i}$ em $\mathbb{C}^{m+1}$ é *homogêneo de grau d*, se todos os h_i's são homogêneos de grau d. Neste caso, θ induz naturalmente um campo de retas ρ em $\mathbb{P}^m$ de *grau d*. Especificamente, dado um aberto $D_+(x_j) \subset \mathbb{P}^m$, defina a *desomogenização* de θ em relação a $D_+(x_j)$ como o campo de vetores

$$\theta_j = \sum_{\substack{i=0,\ldots,m \\ i\neq j}} (h_i - h_j x_i)_{|x_j=1} \frac{\partial}{\partial x_i}$$

em $D_+(x_j)$, que está identificado, da maneira usual, com $\mathbb{C}^m$. E tome ρ a colagem dos θ_j's, cujas mudanças de coordenadas são dadas por $\theta_j = (x_j/x_k)^{-d+1}\theta_k$. Dizemos que $p \in D_+(x_j)$ é uma *singularidade* de ρ se p é uma singularidade de θ_j, para algum j. De forma equivalente, se $\theta(\check{p})$ é proporcional a $E(\check{p})$, em que $E = \sum_{i=0}^m x_i \frac{\partial}{\partial x_i}$ é o campo vetorial de Euler e $\check{p} \in \mathbb{C}^{m+1}$ é um representante de p. O conjunto das singularidades de ρ será denotado por $\mathrm{Sing}(\rho)$. Uma singularidade $p \in D_+(x_j)$ de ρ é *não degenerada*, se o determinante de $J_p(\theta_j)$ é não nulo. Se toda singularidade de ρ é não degenerada, então dizemos que ρ é *não degenerado*.

Dada uma subvariedade $X \subset \mathbb{P}^m$, dizemos que ρ *preserva* X se ρ é tangente a X em todo ponto não singular de X. Observe que, se $p \in D_+(x_j)$, então ρ é tangente a X em p se, e somente se, θ_j é tangente a $X \cap D_+(x_j)$ em p, pois ρ é justamente a colagem do θ_j's. Para futuras referências, vamos destacar esta observação:

Proposição 1.3.1 *Sejam $X \subset \mathbb{P}^m$ uma variedade projetiva, θ um campo vetorial homogêneo em $\mathbb{C}^{m+1}$ e ρ o campo de retas induzido por θ. Então ρ preserva X se, e somente se, θ_j preserva $X \cap D_+(x_j)$, para cada $j = 0, \ldots, m$.*

Proposição 1.3.2 *Sejam $X \subset \mathbb{P}^m$ uma variedade projetiva e $\theta = \sum_{i=0}^m h_i \frac{\partial}{\partial x_i}$ um campo vetorial homogêneo em $\mathbb{C}^{m+1}$. Se ρ é o campo de retas induzido por θ, então ρ preserva X se, e somente se, $\mathcal{I}(X)$ é invariante por θ.*

Demonstração. Pela proposição anterior e por 1.2.5, ρ preserva X se, e somente se, para cada $j = 0, \ldots, m$, o ideal I_j de $X \cap D_+(x_j)$, como subvariedade de $\mathbb{C}^m$, é invariante por θ_j. Assim, é suficiente mostrarmos que esta última condição é equivalente a $\theta(\mathcal{I}(X)) \subset \mathcal{I}(X)$. Dado $f \in I_j$, denote por $f^\sharp$ sua homogenização em relação a x_j. Antes de provarmos a equivalência propriamente dita, calculemos a derivação θ em $x_j f^\sharp$:

$$\theta(x_j f^\sharp) = \sum_{i=0}^m h_i \left(x_j \frac{\partial f^\sharp}{\partial x_i} + f^\sharp \frac{\partial x_j}{\partial x_i} \right) = \left[\sum_{\substack{i=0 \\ i \neq j}}^m h_i x_j \frac{\partial f^\sharp}{\partial x_i} \right] + h_j x_j \frac{\partial f^\sharp}{\partial x_j} + h_j f^\sharp.$$

Usando a igualdade $\sum_{i=0}^m x_i \frac{\partial f^\sharp}{\partial x_i} = f^\sharp \cdot \deg f^\sharp$, obtemos que

$$\theta(x_j f^\sharp) = \sum_{\substack{i=0\\ i\neq j}}^{m} h_i x_j \frac{\partial f^\sharp}{\partial x_i} + h_j \left(f^\sharp \cdot \deg f^\sharp - \sum_{\substack{i=0\\ i\neq j}} x_i \frac{\partial f^\sharp}{\partial x_i} \right) + h_j f^\sharp.$$

Assim, desomogenizando a expressão acima em relação a x_j, segue-se que

$$\begin{aligned} \theta(x_j f^\sharp)_{x_j=1} &= \textstyle\sum_{\substack{i=0\\ i\neq j}}^{m} (h_i - h_j x_i)_{|x_j=1} \frac{\partial f}{\partial x_i} + h_{j|x_j=1} \cdot f \cdot (\deg f^\sharp + 1) \\ &= \theta_j(f) + h_{j|x_j=1} \cdot f \cdot (\deg f^\sharp + 1). \end{aligned} \tag{1.6}$$

Para provarmos a equivalência

$$\theta(\mathcal{I}(X)) \subset \mathcal{I}(X) \iff \theta_j(I_j) \subset I_j, \forall j,$$

comece supondo que $\theta(\mathcal{I}(X)) \subset \mathcal{I}(X)$. Dado $f \in I_j$, tome $F \in \mathcal{I}(X)$, tal que a desomogenização $F_\flat$ de F, em relação a x_j, é igual a f. Se $F = x_j^k H$, em que x_j não divide H, então $(x_j H)_\flat = f$. Além disso, $x_j H \in \mathcal{I}(X)$, pois $\mathcal{I}(X)$ é radical. Assim, sem perda de generalidade, podemos supor que $k = 1$. Como $f^\sharp = H$, temos que $x_j f^\sharp = F$. Mas, $\theta(F) \in \mathcal{I}(X)$. Assim, $\theta(x_j f^\sharp)_\flat \in I_j$ e (1.6) nos diz $\theta_j(f) \in I_j$.

Reciprocamente, suponha que $\mathcal{I}(X)$ não é invariante por θ. Tome $F \in \mathcal{I}(X)$ e $\bar{p} \in X$, tais que $\theta(F)(p) \neq 0$. Fixe j, tal que $p \in D_+(x_j)$ e considere a j-ésima coordenada de p igual a 1. Escreva F na forma $F = x_j^k H$, em que x_j não divide H. Mostraremos que $\theta_j(F_\flat) \notin I_j$. Denote $f = F_\flat$. Como $F \in \mathcal{I}(X)$, então $f \in I_j$ e (1.6) nos diz que

$$\theta(x_j f^\sharp)_\flat(p) = \theta_j(f)(p).$$

Por outro lado, de $F(p) = 0$, segue-se que $H(p) = 0$ e

$$\theta(F)(p) = \big(x_j^k \cdot \theta(H)\big)(p) + \big(H \cdot \theta(x_j^k)\big)(p) = \theta(H)(p).$$

Contudo, $f^\sharp = H$. Logo,

$$\theta(x_j f^\sharp)_\flat(p) = \theta(H)_\flat(p) + H_\flat(p)\theta(x_j)_\flat(p) = \theta(H)(p) = \theta(F)(p) \neq 0.$$

Dessa forma, $\theta_j(f)(p) \neq 0$ e I_j não é invariante por θ_j. O que conclui a demonstração da recíproca. ■

Corolário 1.3.3 *Sejam $X \subset \mathbb{P}^m$ uma variedade projetiva e θ um campo vetorial homogêneo em $\mathbb{C}^{m+1}$. Se ρ é o campo de retas induzido por θ, então ρ preserva X se, e somente se, preserva cada componente irredutível de X.*

Demonstração. Decompondo $X = \cup_{i=1}^{m} X_i$ em irredutíveis e tomando $\mathfrak{p}_i = \mathcal{I}(X_i)$, temos, repetindo exatamente os mesmos argumentos do corolário 1.2.6, que ρ preserva X se, e somente se, cada $\mathfrak{p}_i$ é invariante por θ. Mas, de acordo com a proposição 1.3.2, esta última condição é equivalente a ρ preservar cada componente X_i. Com isto, obtemos a equivalência desejada. ■

Capítulo 2

Variedade Involutiva

Neste capítulo, exibimos, através do teorema 2.2.15, um critério para determinar se um polinômio homogêneo $F \in \mathbb{Q}[u,x,y,z]$ de grau igual a 3 ou 4 define uma variedade involutiva mínima. Na seção §2.3, determinamos condições equivalentes às do critério, de forma a podermos verificá-las no sistema de computação algébrica Singular. Posteriormente, estendemos este critério e exibimos exemplos de famílias infinitas de variedades involutivas mínimas.

2.1 Variedades Involutivas

Seja $\omega : \mathbb{C}^{2n} \times \mathbb{C}^{2n} \to \mathbb{C}$ a *forma simplética canônica* de $\mathbb{C}^{2n}$. Especificamente,

$$\omega(u,v) = u\Omega v^t, \text{ em que } \Omega = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}, \tag{2.1}$$

com I_n sendo a matriz identidade $n \times n$. É de fácil verificação que ω é bilinear, anti-simétrica e não degenerada.

Dado V um subespaço vetorial de $\mathbb{C}^{2n}$, definimos seu *complemento ω-ortogonal* por:

$$V^{\perp} = \{u \in \mathbb{C}^{2n} : \omega(v,u) = 0, \forall v \in V\}.$$

Não é verdade que $\mathbb{C}^{2n}$ é a soma direta de V e $V^{\perp}$. No entanto, as dimensões de V e $V^{\perp}$ são complementares. Antes de provarmos esta afirmação, fixemos um isomorfismo entre $\mathbb{C}^{2n}$ e seu espaço dual. Seja $\Phi : \mathbb{C}^{2n} \to (\mathbb{C}^{2n})^*$ a aplicação $\mathbb{C}$-linear definida por

$$\Phi(u)(v) = \omega(v, u). \tag{2.2}$$

Como ω é não degenerada, Φ é injetiva. Sendo $\dim \mathbb{C}^{2n} = \dim(\mathbb{C}^{2n})^*$, segue-se que Φ é um isomorfismo.

Proposição 2.1.1 *Se V é um subespaço vetorial de $\mathbb{C}^{2n}$, então*

$$\dim V^{\perp} + \dim V = 2n.$$

Demonstração. Seja $\Upsilon : \mathbb{C}^{2n} \to V^*$ definida por $\Upsilon(u) = \Phi(u)_{|V}$. Como Φ é sobrejetiva e todo funcional em V^* se estende a um funcional em $(\mathbb{C}^{2n})^*$, temos que Υ é sobrejetiva. Por outro lado, $\ker \Upsilon = V^{\perp}$. Assim,

$$2n = \dim(\ker \Upsilon) + \dim(\operatorname{im} \Upsilon) = \dim V^{\perp} + \dim V^* = \dim V^{\perp} + \dim V.$$

Como queríamos demonstrar. ∎

Se $V^{\perp} \subset V$, então dizemos que V é *involutivo.* Uma subvariedade X de $\mathbb{C}^m$ é *involutiva* se T_pX é involutivo, para todo p não singular em X.

Corolário 2.1.2 *Se $X \subset \mathbb{C}^{2n}$ é involutiva, então* $\dim X \geq n$.

Demonstração. Seja $p \in X$ um ponto não singular. Sendo X involutiva, temos que $(T_pX)^{\perp} \subset T_pX$. Assim, pela proposição anterior,

$$2n = \dim(T_pX)^{\perp} + \dim T_pX \leq 2 \dim T_pX = 2 \dim X.$$

Logo, $n \leq \dim X$. ∎

Seja agora a *2-forma simplética canônica* de $\mathbb{C}^{2n}$

$$\tilde{\omega} = \sum_{i=1}^{n} dx_{i+n} \wedge dx_i$$

e note que, se $p \in \mathbb{C}^{2n}$, então, identificando-se $T_p\mathbb{C}^{2n}$ com $\mathbb{C}^{2n}$, segue-se que $\omega = \tilde{\omega}_p$.

A cada polinômio F, temos associado um campo de vetores através da equação $\tilde{\omega}(\cdot, h_F) = dF$. Especificamente, dado $F \in \mathbb{C}[x_1, \ldots, x_{2n}]$, definimos o *hamiltoniano* de F como o campo vetorial:

$$h_F = \sum_{i=1}^{n} \left(\frac{\partial F}{\partial x_{i+n}} \frac{\partial}{\partial x_i} - \frac{\partial F}{\partial x_i} \frac{\partial}{\partial x_{i+n}} \right).$$

Observação 2.1.3 Sejam $p \in \mathbb{C}^{2n}$ e $u \overset{\Phi}{\mapsto} \omega(\cdot, u)$ o isomorfismo entre $\mathbb{C}^{2n}$ e seu dual. Então $\tilde{\omega}_p(\cdot, h_F(p)) = d_pF$ nos diz que $\Phi(h_F(p)) = d_pF$, ou seja, $h_F(p) = \Phi^{-1}(d_pF)$.

Proposição 2.1.4 *Seja $F \in \mathbb{C}[x_1, \ldots, x_{2n}]$ um polinômio homogêneo. Se ρ_F é o campo de retas associado a h_F, então*

$$\mathrm{Sing}(\rho_F) \subset \mathcal{Z}(F).$$

Demonstração. Seja $p \in \mathrm{Sing}(\rho_F)$. Se $h_F(p) = (0, 0, 0, 0)$, então da identidade $F \cdot \deg F = \sum_i^{2n} \frac{\partial F}{\partial x_i}$, obtemos que $F(p) = 0$ e, portanto, $p \in \mathcal{Z}(F)$. Considere, então, $h_F(p) \neq (0, 0, 0, 0)$. Por definição, existe $\lambda \in \mathbb{C}^*$, tal que $h_F(p) = \lambda E(p)$, com $E = \sum_{i=0}^{m} x_i \frac{\partial}{\partial x_i}$. Por um lado, $d_pF\big(E(p)\big) = F(p) \cdot \deg F$. Por outro, sendo $\tilde{\omega}_p$ anti-simétrica, $\tilde{\omega}_p\big(\lambda E(p), h_F(p)\big) = 0$. Assim,

$$0 = \lambda \tilde{\omega}_p\big(E(p), h_F(p)\big) = \lambda d_pF\big(E(p)\big) = \lambda F(p) \cdot \deg F.$$

Logo, $F(p) = 0$ e $\mathrm{Sing}(\rho_F) \subset \mathcal{Z}(F)$. ■

Sejam, agora, $F, G \in \mathbb{C}[x_1, \ldots, x_n]$. Definimos o *colchete de Poisson* de F e G por:

$$\{F, G\} = \tilde{\omega}(h_F, h_G).$$

Mostraremos que uma variedade é involutiva se, e somente se, seu ideal é fechado para o colchete de Poisson. Comecemos com um resultado auxiliar:

Lema 2.1.5 *Sejam $X \subset \mathbb{C}^{2n}$ uma subvariedade e $p \in X$. Se $\varphi \in (\mathbb{C}^{2n})^*$ com $\varphi_{|T_pX} = 0$, então existe $F \in \mathcal{I}(X)$ tal que $\varphi = d_pF$.*

Demonstração. Sejam $F_1, \ldots, F_m$ geradores de $\mathcal{I}(X)$ e $\Psi : (\mathbb{C}^{2n})^* \to (T_pX)^*$ induzida pela inclusão $T_pX \to \mathbb{C}^{2n}$. Se d_pF_m é combinação linear de $d_pF_1, \ldots, d_pF_{m-1}$, então $T_pX = \mathcal{Z}(d_pF_1, \ldots, d_pF_m) = \mathcal{Z}(d_pF_1, \ldots, d_pF_{m-1})$. Portanto, reordenando os geradores, podemos supor que $T_pX = \mathcal{Z}(d_pF_1, \ldots, d_pF_s)$, com $d_pF_1, \ldots, d_pF_s$ linearmente independentes.

Afirmação. $d_pF_1, \ldots, d_pF_s$ geram $\ker \Psi$.

Demonstração da Afirmação. Seja $\gamma : \mathbb{C}^{2n} \to \mathbb{C}^s$ a aplicação linear definida por $\gamma(\xi) = \big(d_pF_1(\xi), \ldots, d_PF_s(\xi)\big)$. Aplicando o teorema do núcleo e da imagem à γ, temos que $2n - \dim_{\mathbb{C}}(\ker \gamma) = \dim_{\mathbb{C}}(\operatorname{im} \gamma) \leq s$. Logo, $\dim_{\mathbb{C}}(T_pX) = \dim_{\mathbb{C}}(\ker \gamma) \geq 2n - s$. Por outro lado, como todo funcional linear em T_pX se estende a $\mathbb{C}^{2n}$, então Ψ é sobrejetiva. Assim, $\dim_{\mathbb{C}}(\operatorname{im} \Psi) = \dim_{\mathbb{C}}(T_pX)^* = \dim_{\mathbb{C}}(T_pX) \geq 2n - s$. Logo, $\dim_{\mathbb{C}}(\ker \Psi) \leq s$. No entanto, $d_pF_1, \ldots, d_pF_s$ são L.I. e pertencem ao $\ker \Psi$. Dessa forma, $\dim_{\mathbb{C}}(\ker \Psi) = s$ e $d_pF_1, \ldots, d_pF_s$ geram $\ker \Psi$. O que prova a afirmação.

Voltando à demonstração do lema, como $\varphi_{|T_pX} = 0$, então $\varphi \in \ker \Psi$. Assim, pela afirmação acima, existem $a_1, \ldots, a_s \in \mathbb{C}$, tais que $\varphi = \sum a_i d_pF_i$. Tomando $F = \sum a_iF_i$, segue-se que $\varphi = d_pF$, com $F \in \mathcal{I}(X)$. ■

Proposição 2.1.6 *Seja $X \subset \mathbb{C}^{2n}$ uma subvariedade. Então X é involutiva se, e somente se, $\mathcal{I}(X)$ é fechado para o colchete de Poisson.*

Demonstração. Suponha X involutiva e tome $p \in X$ um ponto não singular. Se $F \in \mathcal{I}(X)$, então

$$\tilde{\omega}_p(\cdot, h_F(p))_{|T_pX} = d_pF_{|T_pX} = 0.$$

Ou seja, $h_F(p) \in T_pX^\perp$. Como X é involutiva, $T_pX^\perp \subset T_pX$ e $h_F(p) \in T_pX$. Portanto, se $G \in \mathcal{I}(X)$, então

$$\{F,G\}(p) = \tilde{\omega}_p\big(h_F(p), h_G(p)\big) = d_pG\big(h_F(p)\big) = 0.$$

Sendo $p \in X$ um ponto não singular arbitrário, obtemos que $\{F,G\} \in \mathcal{I}(X)$. Logo, $\mathcal{I}(X)$ é fechado para o colchete de Poisson.

Reciprocamente, suponha $\mathcal{I}(X)$ fechado para o colchete de Poisson. Se $p \in X$ e $u \in (T_pX)^\perp$, então $\Phi(u)_{|T_pX} = 0$. Aplicando o lema anterior, $\Phi(u) = d_pF$, para algum $F \in \mathcal{I}(X)$. Assim, pela observação 2.1.3, $u = \Phi^{-1}(d_pF) = h_F(p)$. Dessa forma, se $G \in \mathcal{I}(X)$, então

$$d_pG(u) = d_pG\big(h_F(p)\big) = \{F,G\}(p) = 0,$$

pois $\{F,G\} \in \mathcal{I}(X)$. Portanto, $u \in T_pX$ e temos que $(T_pX)^\perp \subset T_pX$. Sendo p arbitrário, concluímos que X é involutiva. ■

Como exemplo inicial, afirmamos que toda hipersuperfície em $\mathbb{C}^{2n}$ é involutiva. Antes de verificarmos esta afirmação, observe que, se $F, G \in \mathbb{C}[x_1, \ldots, x_n]$, então

$$\{F,G\} = dG(h_F) = \sum_{i=1}^{2n} \frac{\partial G}{\partial x_i} dx_i(h_F) = \sum_{i=1}^{n} \left(\frac{\partial G}{\partial x_i}\frac{\partial F}{\partial x_{i+n}} - \frac{\partial G}{\partial x_{i+n}}\frac{\partial F}{\partial x_i} \right) = h_F(G).$$

Em particular, $\{F, GH\} = h_F(GH) = Gh_F(H) + Hh_F(G) = G\{F,H\} + H\{F,G\}$.

Exemplo 2.1.7 Se $X \subset \mathbb{C}^{2n}$ é uma hipersuperfície, então X é involutiva. De fato, se $\mathcal{I}(X) = (F)$ e $G_1, G_2 \in \mathcal{I}(X)$, com $G_i = FH_i, i = 1, 2$, então

$$\{G_1, G_2\} = F\{H_1, FH_2\} + H_1\big(F\{F, H_2\} + H_2\{F,F\}\big) \in (F),$$

pois $\{F,F\} = h_F(F) = 0$. Assim, $\mathcal{I}(X)$ é fechado para o colchete de Poisson. □

Uma variedade involutiva é *mínima* se não contém subvariedade própria involutiva. Note que se $Y \subset \mathcal{Z}(F)$ é involutiva, então, para todo $G \in \mathcal{I}(Y)$, temos

$h_F(G) = \{F, G\} \in \mathcal{I}(Y)$. Ou seja, Y é invariante por h_F. Assim, para mostrar que $\mathcal{Z}(F)$ é involutiva mínima, é suficiente provar que $\mathcal{Z}(F)$ não contém subvariedade invariante pelo hamiltoniano. Esta é justamente a estratégia que usaremos na próxima seção, no contexto projetivo, para obtermos o principal resultado deste capítulo. Dizemos que uma variedade projetiva $X \subset \mathbb{P}^{2n-1}$ é *involutiva* se seu ideal é fechado para o colchete de Poisson; isto é, se seu cone é involutivo no sentido afim. De agora em diante, se F for homogêneo, denotaremos por ρ_F, tanto a derivação h_F, quanto seu campo de retas associado. De forma análoga ao caso afim, dizemos que uma variedade projetiva involutiva é *mínima* se não contém subvariedade projetiva própria involutiva. Como antes, se $\mathcal{Z}(F) \subset \mathbb{P}^{2n-1}$ não contém subvariedade projetiva própria, invariante por ρ_F, então $\mathcal{Z}(F)$ é mínima.

Tanto no caso afim como no caso projetivo, dizemos que uma curva C é uma *solução algébrica* de um campo se C é preservada por este campo. No caso em que C é irredutível e $\mathcal{I}(C)$ é gerado por polinômios com coeficientes em $\mathbb{Q}$, dizemos então que C é uma *solução definida sobre* $\mathbb{Q}$, ou simplesmente, uma *solução sobre* $\mathbb{Q}$.

2.2 Variedade Involutiva Mínima

O objetivo desta seção é demonstrar o teorema 2.2.15 que determina condições sobre F que garantem que $\mathcal{Z}(F) \subset \mathbb{P}^3$ seja uma variedade involutiva mínima. Nossa estratégia será supor que ρ_F admite uma solução algébrica C e estudar propriedades relacionadas às singularidades de ρ_F. Antes de passarmos efetivamente a $\mathbb{P}^3$, temos o seguinte resultado em $\mathbb{P}^n$.

Proposição 2.2.1 *Seja $F \in \mathbb{Q}[x_0, \ldots, x_n]$ um polinômio homogêneo. Se $\mathcal{Z}(F) \subset \mathbb{P}^n$ contém uma subvariedade de dimensão $d \geq 1$ invariante por ρ_F, então $\mathcal{Z}(F)$ contém uma subvariedade irredutível definida sobre $\mathbb{Q}$, invariante por ρ_F e de mesma dimensão d.*

Demonstração. Seja $\mathcal{Z}(J)$ uma subvariedade de $\mathcal{Z}(F)$ invariante por ρ_F de dimensão d, em que $J = (F, g_1, \ldots, g_r)$ é um ideal radical de $\mathbb{C}[x_0, \ldots, x_n]$. Tome L a extensão de $\mathbb{Q}$ por adjunção dos coeficientes dos g_i's. Como $L/\mathbb{Q}$ é finitamente gerada, existe uma extensão $K = \mathbb{Q}(a_1, \ldots, a_m)$ puramente transcendente, tal que L/K é algébrica. Sem perda de generalidade, considere $a_1, \ldots, a_m$ algebricamente independentes. Se $I = J \cap K[\mathtt{x}]$, onde $\mathtt{x}$ representa $x_0, \ldots, x_n$, então $\dim I = \dim(J \cap L[\mathtt{x}])$; veja [13, Corolary 2.13 (b), pg. 47]. Além disso, $\rho_F(I) \subset I$, pois $\rho_F(J) \subset J$ e ρ_F contém apenas coeficientes em $\mathbb{Q} \subset K$. Como $F \in I$ e a dimensão de uma variedade independe do corpo de definição de seu ideal, então

$$\dim I_{K[\mathtt{x}]} = \dim(J \cap L[\mathtt{x}])_{L[\mathtt{x}]} = \dim \mathcal{Z}(J) = d$$

e ainda temos um subvariedade $\mathcal{Z}(I) \subset \mathcal{Z}(F)$ invariante e de dimensão d, com a vantagem de estarmos trabalhando sobre uma extensão K puramente transcendente. Se $I = (F, f_1, \ldots, f_s)$, então, eliminando os denominadores, podemos supor que $f_1, \ldots, f_s \in \mathbb{Q}[a_1, \ldots, a_m][\mathtt{x}]$.

Seja, agora, $\mathbb{Q}[T_1, \ldots, T_m][\mathtt{x}]$ o anel dos polinômios em $m + n$ variáveis. Para cada $b = (b_1, \ldots, b_m) \in \mathbb{C}^m$, defina

$$\varphi_b : \mathbb{Q}[T_1, \ldots, T_m][\mathtt{x}] \to \mathbb{Q}[b_1, \ldots, b_m][\mathtt{x}],$$

o homomorfismo sobrejetivo dado por $\varphi_b(T_i) = b_i$. No caso particular em que $a = (a_1, \ldots, a_m)$, temos que φ_a é isomorfismo, pois os a_i's são algebricamente independentes. Podemos então definir, $M = \{\varphi_a^{-1}(f_1), \ldots, \varphi_a^{-1}(f_s)\}$.

Afirmação 1. $I_b := \varphi_b(M) \cdot \mathbb{C}[\mathtt{x}]$ é um ideal de $\mathbb{C}[\mathtt{x}]$ invariante por ρ_F, qualquer que seja $b \in \mathbb{C}^m$.

Demonstração da Afirmação. Sendo φ_a um isomorfismo, ρ_F induz naturalmente uma derivação δ em $\mathbb{Q}[T_1, \ldots, T_m][\mathtt{x}]$, especificamente $\delta = \varphi_a^{-1} \rho_F \varphi_a$. Como ρ_F tem apenas coeficientes em $\mathbb{Q}$, então $\rho_F(x_i) \in \mathbb{Q}[\mathtt{x}]$, para todo i. Sendo $\mathbb{Q}[\mathtt{x}]$ fixado tanto por φ_a quanto por φ_b, segue-se que $\varphi_b\big(\delta(x_i)\big) = \rho_F(x_i)$, para todo i. Usando a regra de Leibniz, temos $\varphi_b\big(\delta(\mathtt{x}^{\mathtt{j}})\big) = \rho_F(\mathtt{x}^{\mathtt{j}})$, para qualquer multi-índice j. Portanto, dado $g = \varphi_a^{-1}(f_i) \in M$, com $g = \sum \alpha_j(T)\mathtt{x}^{\mathtt{j}}$, obtemos:

$$\rho_F\big(\varphi_b(g)\big) = \rho_F\left(\sum \alpha_j(b)\mathtt{x}^{\mathtt{j}}\right) = \sum \alpha_j(b)\rho_F\left(\mathtt{x}^{\mathtt{j}}\right) = \sum \alpha_j(b)\varphi_b\big((\delta(\mathtt{x}^{\mathtt{j}})\big) = \varphi_b\big(\delta(g)\big).$$

Contudo, $\delta(g) = \varphi_a^{-1}\rho_F\varphi_a(g) = \varphi_a^{-1}\rho_F(f_i) \in \varphi_a^{-1}(I) = (M)$. Consequentemente, $\rho_F\big(\varphi_b(g)\big) \in \varphi_b\big((M)\big) \subset I_b$. Sendo I_b gerado por $\varphi_b(M)$, concluímos que $\rho_F(I_b) \subset I_b$ e temos a invariância por ρ_F.

Segue da afirmação, que é suficiente encontrarmos $b_1, \ldots, b_m \in \mathbb{Q}$, tais que $\dim\big(\mathcal{Z}(I_b)\big) = d$. Comecemos com um caso mais simples.

Afirmação 2. Se $b_1, \ldots, b_m$ são algebricamente independentes, então

$$\dim \mathcal{Z}(I_b) = d.$$

Demonstração da Afirmação. Segue da hipótese, que φ_b induz naturalmente um isomorfismo $\tilde{\varphi}_b : \mathbb{Q}(T_1, \ldots, T_m)[\mathtt{x}] \to \mathbb{Q}(b_1, \ldots, b_m)[\mathtt{x}]$, tal que $\tilde{\varphi}_b(M) = \varphi_b(M)$. Assim,

$$\frac{\mathbb{Q}(T_1, \ldots, T_m)[\mathtt{x}]}{(M)} \simeq \frac{\mathbb{Q}(b_1, \ldots, b_m)[\mathtt{x}]}{\big(\varphi_b(M)\big)}.$$

Como os a_i's também são algebricamente independentes, vale o mesmo resultado. Dessa forma, de $\big(\varphi_a(M)\big) = I$, segue-se que

$$\frac{\mathbb{Q}(a_1, \ldots, a_m)[\mathtt{x}]}{I} \simeq \frac{\mathbb{Q}(T_1, \ldots, T_m)[\mathtt{x}]}{(M)} \simeq \frac{\mathbb{Q}(b_1, \ldots, b_m)[\mathtt{x}]}{\big(\varphi_b(M)\big)}.$$

Portanto, $d = \dim I = \dim\big(\varphi_b(M)\big) = \dim \mathcal{Z}(I_b)$. O que prova a afirmação.

A partir da afirmação 2, mostraremos que existem $b_1, \ldots, b_m \in \mathbb{Q}$ satisfazendo o desejado. Seja

$$\Psi : \mathcal{Z}(M) \subset \mathbb{C}^{m+n} \to \mathbb{C}^m$$

homomorfismo dado por $\Psi\big((b, \mathtt{x})\big) = b$. Se $b_1, \ldots, b_m$ são algebricamente independentes, então $\Psi^{-1}(b) \simeq \mathcal{Z}(I_b)$ tem dimensão positiva, em particular, $b \in \operatorname{im}\Psi$.

Além disso, como a topologia usual de $\mathbb{C}$ é mais fina que a de Zariski, segue-se que todo aberto (de Zariski) em $\mathbb{C}^m$ possui elemento $b = (b_1, \ldots, b_m)$ com $b_1, \ldots, b_m$ algebricamente independentes. Dessa forma, Ψ é um morfismo dominante entre variedades quasiprojetivas. Por [19, Theorem 6, §5, pg. 63], existe um aberto U de $\mathbb{C}^m$ contido na imagem de Ψ. Aplicando o teorema da dimensão das fibras a $\Psi_{|\Psi^{-1}(U)} : \Psi^{-1}(U) \twoheadrightarrow U$, obtemos um aberto $V \subset U$, tal que $\dim \Psi^{-1}(v) = d$, para todo $v \in V$. Finalmente, pela densidade de $\mathbb{Q}$ em $\mathbb{C}$, existe $q = (q_1, \ldots, q_m) \in V$ com $q_1, \ldots, q_m \in \mathbb{Q}$. Assim, $\dim \mathcal{Z}(I_q) = \dim \Psi^{-1}(q) = d$. Como I_q é gerado pelos polinômios com coeficientes racionais $F, \varphi_q(f_1), \ldots, \varphi_q(f_s)$, concluímos, com o auxílio da afirmação 1, que $\mathcal{Z}(I_q)$ é uma subvariedade de $\mathcal{Z}(F)$ definida sobre $\mathbb{Q}$, invariante por ρ_F e de dimensão d. Dessa forma, pelo corolário 1.3.3, qualquer ideal primo P de $\mathbb{Q}[\mathtt{x}]$, mínimo sobre I_q, define uma subvariedade irredutível satisfazendo o desejado. ■

Passemos agora a $\mathbb{P}^3$. Com o intuito de não sobrecarregarmos a notação, trabalharemos sobre o anel $\mathbb{C}[u, x, y, z]$ ao invés de $\mathbb{C}[x_1, x_2, x_3, x_4]$. Nesta notação, se $F \in \mathbb{C}[u, x, y, z]$ é um polinômio homogêneo, seu hamiltoniano tem a forma:

$$h_F = \frac{\partial F}{\partial y}\frac{\partial}{\partial u} + \frac{\partial F}{\partial z}\frac{\partial}{\partial x} - \frac{\partial F}{\partial u}\frac{\partial}{\partial y} - \frac{\partial F}{\partial x}\frac{\partial}{\partial z}.$$

Ainda com F como acima, denotamos por $\theta_{u,F}$ a desomogenização de h_F em relação a $D_+(u) \subset \mathbb{P}^3$. Ou seja,

$$\theta_{u,F} = \left(\left(\frac{\partial F}{\partial z} - \frac{\partial F}{\partial y} x \right)_{|u=1}, - \left(\frac{\partial F}{\partial u} + \frac{\partial F}{\partial y} y \right)_{|u=1}, - \left(\frac{\partial F}{\partial x} + \frac{\partial F}{\partial y} z \right)_{|u=1} \right).$$

Quando não houver ambiguidade quanto a F, denotaremos $\theta_{u,F}$ por θ_u. Sendo θ_u um campo de vetores em $D_+(u)$, temos, em particular, que $\mathrm{Sing}(\theta_u) \subset D_+(u) \simeq \mathbb{C}^3$.

Proposição 2.2.2 *Sejam $F \in \mathbb{Q}[u, x, y, z]$ um polinômio homogêneo, C uma solução sobre $\mathbb{Q}$ de ρ_F em $\mathcal{Z}(F)$ e $p = [1 : \alpha : \beta : \gamma] \in \mathrm{Sing}(\theta_u)$ um ponto não singular* *de $\mathcal{Z}(F)$. Se p é ponto não singular de C, então $T_p\mathcal{Z}(F)$ é subespaço invariante pelo jacobiano $J_p(\theta_u)$ do campo em p e, se λ_1, λ_2 são os autovalores de $J_p(\theta_u)_{|T_p\mathcal{Z}(F)}$, então λ_1, λ_2 pertencem a $K_p = \mathbb{Q}(\alpha, \beta, \gamma)$.*

Demonstração. Por 1.3.1, as desomogenizações de C e de $\mathcal{Z}(F)$ em relação a u são invariantes por θ_u. Assim, por 1.2.4,

$$J_p(\theta_u)(T_pC) \subset T_pC \text{ e } J_p(\theta_u)(T_p\mathcal{Z}(F)) \subset T_p\mathcal{Z}(F).$$

Quanto aos autovalores, começamos afirmando que existe $v \in T_pC$, cujas coordenadas pertencem a K_p. De fato, tome $v = (v_1, v_2, v_3) \in T_pC$ não nulo. Suponha, para fixar as ideias, $v_3 \neq 0$. Multiplicando v por v_3^{-1}, podemos considerar $v_3 = 1$. Sejam, agora, f a desomogenização de F em relação a u e $g \in K_p[x, y, z]$, tal que $\mathcal{I}(C) = (g)$ em $\mathcal{O}_{X,p}$. Como v é ortogonal tanto a $\nabla f(p)$ quanto a $\nabla g(p)$, temos que (v_1, v_2) satisfaz o sistema

$$\begin{bmatrix} \partial_x f(p) & \partial_y f(p) \\ \partial_x g(p) & \partial_y g(p) \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -\partial_z f(p) \\ -\partial_z g(p) \end{bmatrix}. \tag{2.3}$$

Denotemos por A a matriz 2×2 à esquerda da igualdade. Como $\dim T_pC = 1$, segue-se que (v_1, v_2) é a única solução de (2.3). Logo, $\det A \neq 0$ e, como f e g têm coeficientes em K_p, o mesmo vale para as suas derivadas parciais. Assim, resolvendo o sistema, verificamos que

$$v_1 = \frac{1}{\det A}(\partial_y f \cdot \partial_z g - \partial_y g \cdot \partial_z f)(p) \quad \text{ e } \quad v_2 = \frac{1}{\det A}(\partial_x g \cdot \partial_z f - \partial_x f \cdot \partial_z g)(p)$$

pertencem a K_p. O que prova nossa afirmação.

Seja, agora, $w = (w_1, w_2, w_3) \in T_p\mathcal{Z}(F)$ ortogonal a v, em que pelo menos uma de suas coordenadas é igual a 1. Para fixar as ideias, suponha $w_3 = 1$. De maneira semelhante a (2.3), (w_1, w_2) satisfaz o sistema

$$\begin{bmatrix} \partial_x f(p) & \partial_y f(p) \\ v_1 & v_2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} -\partial_z f(p) \\ -v_3 \end{bmatrix}. \tag{2.4}$$

Como o espaço ortogonal a v em $T_p\mathcal{Z}(F)$ tem dimensão 1, então (w_1, w_2) é a única solução de (2.4) e, pelos mesmos argumentos expostos anteriormente, concluímos que $w_1, w_2 \in K_p$. Com isso, no novo sistema de coordenadas $\{v, w, \nabla f(p)\}$, a matriz M associada a $J_p(\theta_u)$ tem todas as entradas em K_p, pois a matriz de mudança de base tem esta propriedade. Por outro lado, sendo $\langle v\rangle = T_pC$ e $\langle v, w\rangle = T_p\mathcal{Z}(F)$ invariantes por $J_p(\theta_u)$, temos que M é da forma

$$M = \begin{bmatrix} \lambda_1 & * & * \\ 0 & \lambda_2 & * \\ 0 & 0 & * \end{bmatrix}.$$

Portanto, $\lambda_1, \lambda_2 \in K_p$. ■

Nosso próximo passo será estabelecer condições sobre F, de forma que se C é uma solução sobre $\mathbb{Q}$ em $\mathcal{Z}(F)$, então C contém todas as singularidades de ρ_F. Seja $F \in \mathbb{C}[u, x, y, z]$ um polinômio homogêneo de grau k. Nossa primeira exigência é que a quantidade de singularidades de ρ_F seja finita. Nesta situação, o número de singularidades de ρ_F é dado pela fórmula clássica de Baum-Bott [17, Theorem 1, pg. 70],

$$\sum_{p\in \mathrm{Sing}(\rho_F)} n_p = (k-1)^3 + (k-1)^2 + (k-1) + 1, \tag{2.5}$$

em que $n_p = \dim_{\mathbb{C}} \left(\mathcal{O}_p/(f_1, \ldots, f_n)\right)$ e $\sum_{i=1}^n f_i\partial_{x_i}$ representa ρ_F em um aberto afim contendo p. De agora em diante, denotaremos esta quantidade por $m(k)$, ou seja,

$$m(k) = (k-1)^3 + (k-1)^2 + (k-1) + 1. \tag{2.6}$$

Para fixar a notação, se $F \in \mathbb{Q}[u, x, y, z]$, então denotamos por $\mathcal{S}(\theta_u)$ o ideal de $\mathbb{Q}[x, y, z]$ gerado pelos menores da matriz

$$\begin{bmatrix} \frac{\partial F}{\partial y} & \frac{\partial F}{\partial z} & -\frac{\partial F}{\partial u} & -\frac{\partial F}{\partial x} \\ 1 & x & y & z \end{bmatrix}_{|u=1}. \tag{2.7}$$

Como as singularidades de θ_u são os pontos $[1 : x_0 : y_0 : z_0] \in D_+(u)$, em que o $h_F\big((1, x_0, y_0, z_0)\big)$ é proporcional a $(1, x_0, y_0, z_0)$, então $\mathrm{Sing}(\theta_u) = \mathcal{Z}(\mathcal{S}(\theta_u))$.

Lema 2.2.3 *Sejam X uma variedade algébrica afim irredutível com anel de coordenadas R e I um ideal de R. Se $\mathcal{Z}(I)$ é finito, então*

$$R/I = \prod_{x \in \mathcal{Z}(I)} \mathcal{O}_{X,x}/I\mathcal{O}_{X,x}.$$

Demonstração. [16, Proposition-Definition VI.1.6, pg. 103]. ■

Lema 2.2.4 *Se $F \in \mathbb{Q}[u, x, y, z]$ é um polinômio de grau k, tal que* $\mathrm{Sing}(\rho_F)$ *é finito, então*

$$\dim_{\mathbb{C}} \frac{\mathbb{C}[x, y, z]}{\mathcal{S}(\theta_u)\mathbb{C}[x, y, z]} = \dim_{\mathbb{Q}} \frac{\mathbb{Q}[x, y, z]}{\mathcal{S}(\theta_u)} \leq m(k).$$

Demonstração. Para cada $p \in \mathrm{Sing}(\theta_u)$, tome $\mathfrak{m}_p$ seu ideal máximo associado em $\mathbb{C}[x, y, z]$. Por 2.2.3,

$$\dim_{\mathbb{C}} \frac{\mathbb{C}[x, y, z]}{\mathcal{S}(\theta_u)\mathbb{C}[x, y, z]} = \sum_{p \in \mathcal{Z}(\mathcal{S}(\theta_u))} \dim_{\mathbb{C}} \left(\frac{\mathbb{C}[x, y, z]}{\mathcal{S}(\theta_u)\mathbb{C}[x, y, z]} \right)_{\mathfrak{m}_p} = \sum_{p \in \mathrm{Sing}(\theta_u)} n_p \leq m(k).$$

Logo, o resultado segue da igualdade $\dim_{\mathbb{Q}} \frac{\mathbb{Q}[x,y,z]}{\mathcal{S}(\theta_u)} = \dim_{\mathbb{C}} \frac{\mathbb{C}[x,y,z]}{\mathcal{S}(\theta_u)\mathbb{C}[x,y,z]}$; veja apêndice B. ■

Proposição 2.2.5 *Seja $F \in \mathbb{Q}[u, x, y, z]$ um polinômio homogêneo de grau k, tal que* $\mathrm{Sing}(\rho_F)$ *é finito. Se $\mathcal{S}(\theta_u) \cap \mathbb{Q}[y]$ é gerado por um polinômio f de grau $m(k)$, então existem $f_1, f_3 \in \mathbb{Q}[y]$, tais que*

$$\mathcal{S}(\theta_u) = (f, x - f_1, z - f_3).$$

Em particular, $\mathrm{Sing}(\theta_u) = \{\big(f_1(\beta), \beta, f_3(\beta)\big) : \beta \in \mathbb{C}$ *e* $f(\beta) = 0\}$ *e, se f é reduzido, então* $\#\mathrm{Sing}(\theta_u) = m(k)$.

Demonstração. Começamos afirmando que $\mathbb{Q}[y] \hookrightarrow \mathbb{Q}[x,y,z]$ induz um isomorfismo de $\mathbb{Q}[y]/(f)$ em $\mathbb{Q}[x,y,z]/\mathcal{S}(\theta_u)$. De fato, seja $\varphi : \mathbb{Q}[y] \to \mathbb{Q}[x,y,z]/\mathcal{S}(\theta_u)$ o homomorfismo canônico de $\mathbb{Q}$-álgebras. Se $g \in \ker\varphi$, então $\varphi(g) \in \mathcal{S}(\theta_u) \cap \mathbb{Q}[y]$ e $g \in (f)$. Portanto, φ induz um homomorfismo injetivo

$$\Psi : \frac{\mathbb{Q}[y]}{(f)} \to \frac{\mathbb{Q}[x,y,z]}{\mathcal{S}(\theta_u)}.$$

Analisando as dimensões como $\mathbb{Q}$-espaços vetoriais,

$$m(k) = \deg f = \dim_{\mathbb{Q}} \mathbb{Q}[y]/(f) \leq \dim_{\mathbb{Q}} \mathbb{Q}[x,y,z]/\mathcal{S}(\theta_u).$$

Mas, por 2.2.4, $\dim_{\mathbb{Q}} \mathbb{Q}[x,y,z]/\mathcal{S}(\theta_u) \leq m(k)$. Dessa forma, as dimensões são iguais e Ψ, sendo uma aplicação $\mathbb{Q}$-linear injetiva, é sobrejetiva. Logo, Ψ é um isomorfismo (de álgebras) e a afirmação segue. Tomando $f_1, f_3 \in \mathbb{Q}[y]$, tais que $\Psi(\overline{f_1}) = \overline{x}$ e $\Psi(\overline{f_3}) = \overline{z}$, temos, em $\mathbb{Q}[x,y,z]$, que $x - f_1, z - f_3 \in \mathcal{S}(\theta_u)$. Portanto, $\mathcal{S}(\theta_u)$ contém o ideal $(f, x - f_1, z - f_3)$. Mostraremos que também vale a recíproca. Seja $h \in \mathcal{S}(\theta_u)$. Definindo $\tilde{h}$ como o polinômio obtido, a partir de h, substituindo-se x e z por f_1 e f_3, respectivamente, segue-se que $(f, x - f_1, z - f_3, h) = (f, x - f_1, z - f_3, \tilde{h})$. Como $\tilde{h} \in \mathcal{S}(\theta_u) \cap \mathbb{Q}[y] = (f)$, concluímos que $(f, x - f_1, z - f_3, h) = (f, x - f_1, z - f_3)$. Assim,

$$\mathcal{S}(\theta_u) = (f, x - f_1, z - f_3).$$

Como queríamos demonstrar. ∎

Na proposição anterior, a condição $\mathcal{S}(\theta_u) \cap \mathbb{Q}[y] = (f)$, em que f é reduzido, implica que se $p, q \in \mathrm{Sing}(\theta_u)$, tais que $p \neq q$, então a primeira coordenada de p é distinta da primeira coordenada de q.

Proposição 2.2.6 *Seja $G \in \mathbb{Q}[u,x,y,z]$ um polinômio homogêneo de grau k, tal que $\mathrm{Sing}(\rho_G)$ é finito. Se $\mathcal{S}(\theta_u) = (g, x - g_1, z - g_3)$, com $g, g_1, g_3 \in \mathbb{Q}[y]$, então $\deg g \leq m(k)$.*

Demonstração. Definindo $\varphi : \mathbb{C}[x,y,z] \to \mathbb{C}[y]/(g)$ por $\varphi(y) = y, \varphi(x) = g_1$ e $\varphi(z) = g_3$, temos que φ é sobrejetivo com $\mathcal{S}(\theta_u) \subset \ker\varphi$. Afirmamos que $\ker\varphi$ é $\mathcal{S}(\theta_u)$. De fato, seja $h = \sum a_{i,j,k}x^iy^jz^k \in \mathbb{C}[x,y,z]$. Tome $s \in \mathcal{S}(\theta_u)$, tal que $h = \sum a_{i,j,k}g_1^iy^jg_3^k + s$. Se $\varphi(h) = 0$, então, de $\mathcal{S}(\theta_u) \subset \ker\varphi$, segue-se que $\sum a_{i,j,k}g_1^iy^jg_3^k \in (g)$. Portanto, $h \in (g,s) \subset \mathcal{S}(\theta_u)\mathbb{C}[x,y,z]$. O que prova nossa afirmação. Assim, por 2.2.4, obtemos

$$m(k) \geq \dim_{\mathbb{C}} \frac{\mathbb{C}[x,y,z]}{\mathcal{S}(\theta_u)\mathbb{C}[x,y,z]} = \dim_{\mathbb{C}} \frac{\mathbb{C}[x,y,z]}{\ker\varphi} = \dim_{\mathbb{C}} \frac{\mathbb{C}[y]}{(g)} = \deg g.$$

Como queríamos demonstrar. ■

Nossa próxima exigência sobre F é que $\mathcal{S}(\theta_u) \cap \mathbb{Q}[y]$ seja gerado por um polinômio irredutível de grau $m(k)$. Comecemos com um lema:

Lema 2.2.7 *Seja $F \in \mathbb{C}[u,x,y,z]$ um polinômio homogêneo de grau $k \geq 2$, tal que $\mathcal{Z}(F)$ é não singular. Se C é uma solução algébrica irredutível de ρ_F em $\mathcal{Z}(F)$, então $C \cap \operatorname{Sing}(\rho_F) \neq \emptyset$.*

Demonstração. [2, Lemma 3.2, pg. 305]. ■

Proposição 2.2.8 *Seja $F \in \mathbb{Q}[u,x,y,z]$ um polinômio homogêneo de grau k, tal que $\operatorname{Sing}(\rho_F)$ é finito e $\mathcal{Z}(F)$ é não singular. Seja ainda $C \subset \mathcal{Z}(F)$ uma solução sobre $\mathbb{Q}$ do campo ρ_F. Se $\mathcal{S}(\theta_u) \cap \mathbb{Q}[y]$ é gerado por um polinômio irredutível f de grau $m(k)$, então $\operatorname{Sing}(\rho_F) \subset C \cap D_+(u)$.*

Demonstração. Por (2.5), ρ_F contém no máximo $m(k)$ singularidades. Mas, por 2.2.5, $\operatorname{Sing}(\theta_u)$ contém exatamente $m(k)$ pontos. Dessa forma, $\operatorname{Sing}(\rho_F) \subset D_+(u)$. Resta mostrar que se C é solução sobre $\mathbb{Q}$, então C contém todas as singularidades de ρ_F. Primeiramente, por 2.2.7, $C \cap \operatorname{Sing}(\rho_F) \neq \emptyset$ e podemos fixar $p \in C \cap \operatorname{Sing}(\theta_u)$. A partir de uma ação de grupo em $\operatorname{Sing}(\theta_u)$, mostraremos que todas as outras singularidades também pertencem à curva. Tome L o corpo de decomposição de f e sejam $f_1, f_3 \in \mathbb{Q}[y]$, tais que $\mathcal{S}(\theta_u) = (f, x - f_1, z - f_3)$. Se G é o grupo de Galois de $L/\mathbb{Q}$, então sua ação em L induz naturalmente uma ação de G em $\mathrm{Sing}(\theta_u)$. Especificamente, se $\sigma \in G$ e β é uma raiz de f, então

$$\sigma\big((f_1(\beta), \beta, f_3(\beta))\big) := \big(\sigma(f_1(\beta)), \sigma(\beta), \sigma(f_3(\beta))\big) = \big(f_1(\sigma(\beta)), \sigma(\beta), f_3(\sigma(\beta))\big),$$

em que a última igualdade segue de f_1, f_3 serem polinômios com coeficientes em $\mathbb{Q}$, que é o corpo fixo de G. Sejam, agora, $g_1, \ldots, g_m \in \mathbb{Q}[u, x, y, z]$ geradores de $\mathcal{I}(C)$ e $\beta_p \in L$, tal que $p = \big(f_1(\beta_p), \beta_p, f_3(\beta_p)\big)$. Se $q = \big(f_1(\beta_q), \beta_q, f_3(\beta_q)\big) \in \mathrm{Sing}(\theta_u)$, então, pela transitividade de G, existe $\sigma \in G$, tal que $\sigma(\beta_p) = \beta_q$. Logo, $\sigma(p) = q$ e

$$g_i(q) = g_i(\sigma(p)) = \sigma(g_i(p)) = \sigma(0) = 0, \forall i = 1, \ldots m.$$

Portanto, $q \in C$. Sendo q uma singularidade arbitrária, segue o resultado. ■

A proposição acima, nos dá condições que garantem que uma solução C sobre $\mathbb{Q}$ de ρ_F contenha todas as singularidades do campo. No entanto, para podermos fazer uso da proposição 2.2.2, precisamos garantir que pelo menos uma das singularidades de $\theta_{u,F}$ seja um ponto não singular de C. Comecemos com um resultado que M. G. Soares provou em [22, Lema 5.1, pg. 156], cuja demonstração reproduzimos a seguir.

Proposição 2.2.9 *Seja ρ o germe em $0 \in \mathbb{C}^2$ de um campo vetorial holomorfo, em que $0 \in \mathbb{C}^2$ é uma singularidade isolada de ρ. Sejam ainda, λ_1 e λ_2 os autovalores de $J_0(\rho)$. Se $\lambda_1/\lambda_2 \notin \mathbb{Q}$, então nenhum germe em 0 de uma curva analítica, irredutível e singular pode ser invariante por ρ.*

Demonstração. Como $\lambda_1/\lambda_2 \notin \mathbb{Q}$, temos que os autovalores são não-ressonantes, ou seja, se $i = 1$ ou $i = 2$, então não existe solução para $\lambda_i = a\lambda_1 + b\lambda_2$, com

$a, b \in \mathbb{N}, a + b \geq 2$. Assim, pelo teorema de Poincaré [3, Theorem, §22.B, pg. 178], temos, através de uma mudança formal de coordenadas, que

$$\rho = \lambda_1 x \frac{\partial}{\partial x} + \lambda_2 y \frac{\partial}{\partial y}.$$

Agora, suponha, por absurdo, que Γ é o germe em $0 \in \mathbb{C}^2$ de uma curva analítica, irredutível, singular e invariante por ρ. Tome $\gamma : D_\varepsilon \to \mathbb{C}^2$ uma parametrização de Γ, em que $D_\varepsilon = \{z \in \mathbb{C} : |z| < \varepsilon\}$. Se γ^* corresponde a γ pela mudança formal de coordenadas, então podemos supor, sem perda de generalidade, que γ^* é da forma $\gamma^*(t) = (t^{l_1}, at^{l_2} + \cdots)$, em que $1 < l_1 \leq l_2$. Sendo Γ invariante por ρ, segue-se que $d\gamma^*/dt = \nu(t)\rho(\gamma^*(t))$, em que $\nu(t)$ não é identicamente zero. Com isso,

$$l_1 t^{l_1 - 1} = \nu(t)\lambda_1 t^{l_1} \quad \text{e} \quad al_2 t^{l_2 - 1} + \cdots = \nu(t)(\lambda_2 a t^{l_2} + \cdots).$$

Eliminando-se ν, obtemos:

$$\frac{l_1 t^{l_1 - 1}}{\lambda_1 t^{l_1}} = \frac{al_2 t^{l_2 - 1} + \cdots}{\lambda_2 a t^{l_2} + \cdots}.$$

Portanto, $l_1 \lambda_2 a t^{l_1 - 1 + l_2} + \cdots = \lambda_1 a l_2 t^{l_1 + l_2 - 1} + \cdots$. Logo, $l_1 \lambda_2 = \lambda_1 l_2$ e

$$\frac{\lambda_2}{\lambda_1} = \frac{l_2}{l_1} \in \mathbb{Q}.$$

Contradizendo as hipóteses. ■

Corolário 2.2.10 *Seja $F \in \mathbb{Q}[u, x, y, z]$ um polinômio homogêneo, tal que* $\mathrm{Sing}(\rho_F)$ *é finito e $\mathcal{Z}(F)$ é não singular. Sejam ainda $p \in \mathrm{Sing}(\theta_u)$ e λ_1, λ_2 os autovalores de $J_p(\theta_u)_{|T_p\mathcal{Z}(F)}$. Se $\lambda_1/\lambda_2 \notin \mathbb{Q}$ e C é solução algébrica de ρ_F singular em p, então p é um nó de C.*

Demonstração. Como $\mathcal{Z}(F)$ é não singular, então existe vizinhança aberta de p em $\mathcal{Z}(F)$ analiticamente isomorfa a um aberto de $\mathbb{C}^2$. Além disso, p é singularidade isolada, pois a quantidade de pontos singulares é finita. Assim, se C é solução algébrica de ρ_F, então, por 2.2.9, C é analiticamente redutível em p, pois, por hipótese, C é singular em p. Por outro lado, pelo teorema de Poincaré, podemos supor que o germe de ρ_F é dado por $\rho = \lambda_1 x\frac{\partial}{\partial x} + \lambda_2 y\frac{\partial}{\partial y}$. Sendo o germe Γ de C uma solução de ρ, segue-se que Γ é definida por uma das seguintes equações: $x = 0, y = 0$ ou $xy = 0$; veja proposição C.3. Como C é analiticamente redutível em p, então C é dada localmente por $\mathcal{Z}(xy)$. Portanto, p é um nó. ∎

Sejam F nas condições do corolário anterior e C uma solução de ρ_F. Usando teoria de índices, T. Suwa [24, Theorem 2.1, pg. 2994] mostrou que

$$\sum_{p\in \mathrm{Sing}(\rho_F)\cap C} \mathrm{ind}_p(\rho_F, C) = C^2. \tag{2.8}$$

Além disso, se $p \in \mathrm{Sing}(\rho_F)$ também está nas condições do corolário, então podemos considerar o germe do campo como sendo igual a $\lambda_1 x\frac{\partial}{\partial x} + \lambda_2 y\frac{\partial}{\partial y}$ e, aplicando [24, Example 1.6, pg. 2992], obtemos que

$$\mathrm{ind}_p(\rho_F, C) = (\lambda_1 + \lambda_2)^2/\lambda_1\lambda_2. \tag{2.9}$$

Usaremos esta última igualdade juntamente com (2.8) para exibir as condições que garantem que $\mathrm{Sing}(C)$ está propriamente contido em $\mathrm{Sing}(\rho_F)$.

Lema 2.2.11 *Seja $F \in \mathbb{C}[u, x, y, z]$ um polinômio homogêneo, tal que $\mathcal{Z}(F)$ é não singular. Se* $\mathrm{Sing}(\rho_F)$ *é finito e C é uma solução algébrica de ρ_F, então*

$$\mathrm{Sing}(C) \subset \mathrm{Sing}(\rho_F).$$

Demonstração. Seja $p \in C$, tal que $p \notin \mathrm{Sing}(\rho_F)$. Tome U um aberto afim de $\mathcal{Z}(F)$ contendo p e Θ um campo vetorial que define ρ_F em U. Como $\mathrm{Sing}(\rho_F)$ é finito, podemos supor que Θ nunca se anula em U. Sendo $\mathcal{Z}(F)$ não singular, então U é localmente difeomorfo a um disco D aberto em $\mathbb{C}^2$. Identificando U com D e usando coordenadas u e v em $\mathbb{C}^2$, podemos supor, pelo teorema da vizinhança tubular, que

$p = (0,0)$ e $\Theta = \partial/\partial u$. Com isso, C é localmente definida por $\mathcal{Z}(v)$. Logo, C é não singular em p e concluímos que $\mathrm{Sing}(C) \subset \mathrm{Sing}(\rho_F)$. ■

O próximo lema e sua demonstração encontram-se essencialmente em [2]. A única diferença é uma sutil adaptação das hipóteses.

Lema 2.2.12 *Seja $F \in \mathbb{Q}[u,x,y,z]$ um polinômio homogêneo de grau k, tal que $\mathrm{Sing}(\rho_F)$ é finito, $\mathcal{Z}(F)$ é não singular, ρ_F é não degenerado e $\mathcal{S}(\theta_u) \cap \mathbb{Q}[y]$ é gerado por um polinômio irredutível de grau $m(k)$. Além disso, suponha que, para todo $p \in \mathrm{Sing}(\theta_u)$, os autovalores $\lambda_1^{(p)}, \lambda_2^{(p)}$ de $J_p(\theta_u)_{|T_p\mathcal{Z}(F)}$ satisfazem $\lambda_1^{(p)}/\lambda_2^{(p)} \notin \mathbb{Q}$. Se C é uma solução algébrica de ρ_F em $\mathcal{Z}(F)$, tal que $\mathrm{Sing}(C) = \mathrm{Sing}(\rho_F)$, então*

$$2g + (4-k)d = -2k^3 + 4k^2 + 2,$$

em que $d = \deg(C)$ e g é o gênero da normalização de C.

Demonstração. Pelo corolário 2.2.10 e por (2.8) e (2.9)

$$C^2 = \sum_{p \in \mathrm{Sing}(\rho_F) \cap C} \frac{(\lambda_1^{(p)} + \lambda_2^{(p)})^2}{\lambda_1^{(p)} \lambda_2^{(p)}}. \tag{2.10}$$

Agora, por [4, I.15, pg. 8], $C^2 = 2p_a - 2 - C \cdot K$, em que p_a é o gênero aritmético de C e K é o divisor canônico de $\mathcal{Z}(F)$. Por [19, III, §6.4, pg. 210], $K = (k-4)L$, em que L é seção hiperplana de $\mathcal{Z}(F)$. Portanto, $C \cdot K = d(k-4)$. Além disso, 2.2.10 nos diz que toda singularidade de C é um nó, enquanto de 2.2.5 e de Baum-Bott (2.5), segue-se que $\#\mathrm{Sing}(C) = m(k)$. Assim, aplicando [12, Exercise 1.8, pg. 298], temos que $p_a = g + m(k)$, em que g é o gênero da normalização de C. Portanto, $C^2 = 2g + 2m(k) - 2 - d(k-4)$. Por outro lado, [2, Theorem 3.4, pg. 305] nos diz que o lado direito de (2.10) é igual a $4k$. Logo,

$$\begin{aligned} 2g + (4-k)d &= 4k - 2m(k) + 2 \\ &= -2k^3 + 4k^2 + 2. \end{aligned}$$

E isto conclui a demonstração do lema. ■

Corolário 2.2.13 *Seja $F \in \mathbb{Q}[u, x, y, z]$, tal que F e ρ_F satisfazem todas as condições do lema anterior. Se F tem grau k igual a 3 ou a 4, então*

$$\operatorname{Sing}(C) \subsetneq \operatorname{Sing}(\rho_F),$$

qualquer que seja $C \subset \mathcal{Z}(F)$ solução algébrica de ρ_F.

Demonstração. Suponha, por absurdo, que $\operatorname{Sing}(C) = \operatorname{Sing}(\rho_F)$. Pelo lema anterior, $2g + (4-k)d = -2k^3 + 4k^2 + 2$. Agora, se k igual a 3 ou a 4, então $2g + (4-k)d \geq 0$, enquanto que $-2k^3 + 4k^2 + 2 < 0$. E temos uma contradição. ■

Observação 2.2.14 Se $\operatorname{Sing}(\rho_F)$ é finito, então F é irredutível. De fato, se $F = GH$, em que G e H não são constantes, então $\partial_u F = G \cdot \partial_u H + H \cdot \partial_u G$ se anula em $\mathcal{Z}(G, H)$. Procedendo de maneira análoga com as outras variáveis x, y e z, concluímos que o hamiltoniano de F se anula em $\mathcal{Z}(G, H)$. Em particular, $\mathcal{Z}(G, H) \subset \operatorname{Sing}(\rho_F)$. Mas isto contradiz a finitude de $\operatorname{Sing}(\rho_F)$, pois $\dim \mathcal{Z}(G, H) \geq 1$.

Como consequência das proposições acima, temos:

Teorema 2.2.15 *Seja $F \in \mathbb{Q}[u, x, y, z]$ um polinômio homogêneo de grau $k = 3$ ou $k = 4$, tal que $\operatorname{Sing}(\rho_F)$ é finito, $\mathcal{Z}(F)$ é não singular e ρ_F é não degenerado. Se $\mathcal{S}(\theta_u) \cap \mathbb{Q}[y]$ é gerado por um polinômio irredutível de grau $m(k)$ e, para todo $p \in \operatorname{Sing}(\theta_u)$, os autovalores λ_1, λ_2 de $J_p(\theta_u)_{|T_p\mathcal{Z}(F)}$ satisfazem $\lambda_1/\lambda_2 \notin K_p$, então $\mathcal{Z}(F)$ é involutiva mínima.*

Demonstração. Suponha, por absurdo, que $X = \mathcal{Z}(F)$ contém uma subvariedade involutiva própria Y. Como $\rho_F(G) = \{F, G\} \in \mathcal{I}(Y)$, para todo $G \in \mathcal{I}(Y)$, segue-se que Y é invariante por ρ_F. Além disso, sendo F irredutível, $\dim X > \dim Y$. Por outro lado, como o cone $\mathcal{C}(Y)$ de Y é uma variedade afim involutiva em $\mathbb{C}^4$, temos, por 2.1.2, que $\dim \mathcal{C}(Y) \geq 2$. Com isso,

$$2 = \dim X > \dim Y = \dim \mathcal{C}(Y) - 1 \geq 2 - 1 = 1.$$

Logo, $\dim Y = 1$ e Y é uma solução algébrica de ρ_F. Aplicando a proposição 2.2.1, podemos tomar uma solução C sobre $\mathbb{Q}$ contida em X. Por um lado, 2.2.8 nos diz que $\mathrm{Sing}(\rho_F) \subset C \cap D_+(u)$. Por outro, por 2.2.13, $\mathrm{Sing}(C) \subsetneq \mathrm{Sing}\big(\rho_F\big)$. Assim, $\mathrm{Sing}(C) \cap D_+(u) \subsetneq \mathrm{Sing}(\theta_u) \subset C \cap D_+(u)$ e podemos tomar $p \in \mathrm{Sing}(\theta_u)$ um ponto não singular de C. Por 2.2.2, se λ_1 e λ_2 são os autovalores de $J_p(\theta_u)_{|T_p\mathcal{Z}(F)}$, então λ_1 e λ_2 pertencem a K_p. Em particular, $\lambda_1/\lambda_2 \in K_p$, contradizendo a hipótese. Com isso, $\mathcal{Z}(F)$ é involutiva mínima. ■

De agora em diante, se $p \in \mathrm{Sing}(\theta_{u,F})$ e λ_1, λ_2 são os autovalores de $J_p(\theta_u)_{|T_p\mathcal{Z}(F)}$, então iremos nos referir a λ_1 e λ_2, simplesmente como os *autovalores associados* a p.

2.3 Um Critério Prático para a Minimalidade

Nesta seção, veremos como substituir as condições do teorema 2.2.15 por critérios verificáveis computacionalmente. Para tanto, investigaremos condições equivalentes ao campo ser não degenerado e às exigências do teorema quanto aos autovalores associados aos pontos singulares. De acordo com a proposição 2.3.3, estas condições podem ser verificadas através de dois polinômios η e μ em uma única variável que serão definidos nesta seção.

Seja $F \in \mathbb{Q}[u, x, y, z]$ um polinômio homogêneo de grau k, tal que $\mathcal{Z}(F)$ é não singular. Seja ainda $p = [1 : \alpha : \beta : \gamma]$ uma singularidade de ρ_F. V. Lunts mostrou, em [15, §2.3.4, pg. 536], que a matriz $J_p(\theta_u)$ assume uma forma bastante prática quando o ponto singular se encontra em $[1 : 0 : 0 : 0]$. Assim, começaremos nossa investigação fazendo a seguinte mudança de coordenadas: tomando as matrizes

$$M_p = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \alpha & 0 & 0 & 1 \\ \beta & \alpha & 1 & \gamma \\ \gamma & -1 & 0 & 0 \end{pmatrix}, \Omega = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \text{ e } M_p^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ \gamma & 0 & 0 & -1 \\ -\beta & -\gamma & 1 & \alpha \\ -\alpha & 1 & 0 & 0 \end{pmatrix},$$

temos que $M_p^T \Omega M_p = \Omega$ e $M_p^{-1}(p) = [1 : 0 : 0 : 0] = q$. Com isso, se M_p é a matriz de passagem para um novo sistema de coordenadas, então, neste novo sistema, F se escreve como

$$P = F\big(M_p(u', x', y', z')\big) = F(u', \alpha u' + z', \beta u' + \alpha x' + y' + \gamma z', \gamma u' - x').$$

Note que P depende da singularidade p e, caso seja necessário enfatizar a singularidade, usaremos a notação P_p.

Inicialmente, verificaremos que q é uma singularidade do campo $\theta_{u',P}$ e que os autovalores associados a p não se alteram pela mudança de coordenadas. Seja $\varphi : \mathbb{C}^4 \to \mathbb{C}^4$ o isomorfismo linear cuja matriz associada é M_p^{-1}. Se h_F e h_P são os hamiltonianos de F e P, respectivamente, então, pelo teorema de Jacobi [1, Theorem 3.3.19, pg. 194], o diagrama

$$\begin{array}{ccc} \mathbb{C}^4 & \xrightarrow{h_F} & T\mathbb{C}^4 \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle d\varphi} \\ \mathbb{C}^4 & \xrightarrow{h_P} & T\mathbb{C}^4 \end{array} \tag{2.11}$$

comuta. Seja, agora, $\breve{p} \in \mathbb{C}^4$ pertencente à fibra de p em relação a aplicação canônica de $\mathbb{C}^4$ em $\mathbb{P}^3$. Sendo p um ponto singular de ρ_F, existe $\lambda \in \mathbb{C}^*$, tal que $h_F(\breve{p}) = \lambda E(\breve{p})$, em que E denota o campo de Euler. Além disso, $d_{\breve{p}}\varphi = \varphi$, pois φ é linear. Assim,

$$h_P(\breve{q}) = d_{\breve{p}}\varphi\big(h_F(\breve{p})\big) = d_{\breve{p}}\varphi\big(\lambda E(\breve{p})\big) = \lambda\varphi\big(E(\breve{p})\big) = \lambda E(\breve{q}),$$

e q é uma singularidade de ρ_P.

Lema 2.3.1 *O campo ρ_P é não degenerado em q se, e somente se, ρ_F é não degenerado em p. Além disso, os autovalores de $J_q(\theta_{u',P})_{|T_q\mathcal{Z}(P)}$ coincidem com os de $J_p(\theta_{u,F})_{|T_p\mathcal{Z}(F)}$.*

Demonstração. Sejam $\pi : \mathbb{C}^4 \to \mathbb{P}^3$ a projeção canônica e $\breve{p} \in \pi^{-1}(p)$. Sendo p um ponto singular de ρ_F, temos que $h_F(\breve{p})$ é proporcional à $E(\breve{p})$, em particular, $(\partial F/\partial y)(\breve{p}) \neq 0$. Dessa forma, podemos tomar uma vizinhança aberta V de p, tal que $V \subset D_+(u) \cap \mathcal{Z}(\partial F/\partial y) \subset \mathbb{P}^3$. Seja, agora, $E = V \times \mathbb{C}^4$ o fibrado vetorial trivial. Nosso primeiro passo será construir um morfismo de E no fibrado tangente TV de V. Em função do isomorfismo $[1 : x : y : z] \mapsto (x, y, z)$ entre V e um aberto de $\mathbb{C}^3$, podemos supor que $TV = V \times \mathbb{C}^3$. Se $v = [1 : x : y : z] \in V$ e $\xi = (\xi_0, \xi_1, \xi_2, \xi_3)$ pertence à fibra E_v de v, denote

$$\xi^\sharp = (\xi_1 - \xi_0 x, \xi_2 - \xi_0 y, \xi_3 - \xi_0 z)\,.$$

Defina, então,

$$\begin{aligned} \Psi : E &\to TV \\ (v, \xi) &\mapsto (v, \xi^\sharp). \end{aligned}$$

Defina ainda,

$$\begin{aligned} \bar{h}_F : V &\to E \\ [1 : x : y : z] &\mapsto \big([1 : x : y : z], h_F((1, x, y, z))\big) \end{aligned}$$

e note que, se $v \in V$, então $\theta_{u,F}(v) = \Psi(\bar{h}_F(v))$. Portanto, $\theta_{u,F|V} = \Psi \circ \bar{h}_F$. Repetindo a mesma construção para o polinômio P, tomamos $W \subset D_+(u)$ vizinhança aberta de q, definimos $Q = W \times \mathbb{C}^4$ e construímos um morfismo

$$\Phi : Q \to TW,$$

tal que $\theta_{u',P|W} = \Phi \circ \bar{h}_P$. Reduzindo as vizinhanças V e W, podemos supor que $\varphi(\pi^{-1}(V)) = \pi^{-1}(W)$. Agora, se $\breve{v}_1, \breve{v}_2 \in \pi^{-1}(v)$, então, pela linearidade de φ, segue-se que $\varphi(\breve{v}_1)$ e $\varphi(\breve{v}_2)$ são proporcionais. Portanto, $\pi\big(\varphi(\breve{v}_1)\big) = \pi\big(\varphi(\breve{v}_2)\big)$ e podemos definir

$$\begin{aligned} \bar{\varphi} : V &\to W \\ v &\mapsto \pi\big(\varphi(\breve{v})\big) \end{aligned} \qquad \text{e} \qquad \begin{aligned} \bar{d} : E &\to Q \\ (v, \xi) &\mapsto \big(\bar{\varphi}(v), \varphi(\xi)\big) \end{aligned}$$

morfismos induzidos por φ e $d\varphi$, em que $\breve{v} \in \pi^{-1}(v)$. Por (2.11), obtemos que o lado esquerdo do diagrama

$$\begin{tikzcd} V \arrow[r, "\bar{h}_F"] \arrow[d, "\bar{\varphi}"'] \arrow[rr, bend left, "\theta_{u,F|V}"] & E \arrow[r, "\Psi"] \arrow[d, "\bar{d}"'] & TV \arrow[d, dashed, "\Gamma"'] \\ W \arrow[r, "\bar{h}_P"] \arrow[rr, bend right, "\theta_{u',P|W}"'] & Q \arrow[r, "\Phi"] & TW \end{tikzcd} \tag{2.12}$$

comuta. Definiremos um morfismo de fibrados vetoriais $\Gamma : TV \to TW$, de forma que $\Gamma \circ \theta_{u,F|V} = \theta_{u',P} \circ \bar{\varphi}$. Seja $\tau : \mathbb{C}^3 \to \mathbb{C}^4$ a inclusão dada por $\tau(\zeta_1, \zeta_2, \zeta_3) = (0, \zeta_1, \zeta_2, \zeta_3)$. Se $v = [1 : x, y, z] \in V$, denote $\breve{v} = (1, x, y, z)$ e tome

$$\begin{aligned} \imath : TV &\to E \\ (v, \zeta) &\mapsto \left(v, \tau(\zeta) + \tfrac{\partial F}{\partial y}(\breve{v}) \cdot \breve{v}\right). \end{aligned}$$

Defina $\Gamma = \Phi \circ \bar{d} \circ \imath$. É de fácil verificação que, se $w \in W$, então $\pi^{-1}(w) \subset \ker \Phi_w$. Assim, se $\zeta \in T_v V$, temos que

$$\Gamma_v(\zeta) = \Phi_{\bar{\varphi}(v)} \left(\varphi(\tau(\zeta)) + \frac{\partial F}{\partial y}(\breve{v})\varphi(\breve{v}) \right) = \Phi_{\bar{\varphi}(v)} \circ \varphi \circ \tau(\zeta),$$

pois $\varphi(\breve{v}) \in \pi^{-1}(\bar{\varphi}(v))$. Logo, Γ_v é uma composição de aplicações lineares e Γ é linear nas fibras. Para mostrarmos que $\Gamma \circ \theta_{u,F|V} = \theta_{u',P} \circ \bar{\varphi}$, note que se $v = [1 : x : y : z]$ e $\bar{h}_F(v) = (\xi_0, \xi_1, \xi_2, \xi_3)$, então $\frac{\partial F}{\partial y}(\breve{v}) = \xi_0$ e

$$\imath_v \circ \Psi(\bar{h}_F(v)) = \imath_v(\xi^\sharp) = (0, \xi_1 - \xi_0 x, \xi_2 - \xi_0 y, \xi_3 - \xi_0 z) + \xi_0(1, x, y, z) = \bar{h}_F(v).$$

Assim, $\imath \circ \Psi \circ \bar{h}_F = \bar{h}_F$ e

$$\Gamma \circ \theta_{u,F|V} = (\Phi \circ \bar{d} \circ \imath) \circ (\Psi \circ \bar{h}_F) = \Phi \circ \bar{d} \circ \bar{h}_F = \Phi \circ \bar{h}_P \circ \bar{\varphi} = \theta_{u',P} \circ \bar{\varphi}.$$

Ou seja, o diagrama

$$\begin{tikzcd} V \arrow[r, "\theta_{u,F|V}"] \arrow[d, "\bar{\varphi}"'] & TV \arrow[d, "\Gamma"'] \\ W \arrow[r, "\theta_{u',P|W}"] & TW \end{tikzcd}$$

comuta. Com isso,

$$J_v(\Gamma) \circ J_v(\theta_{u,F}) = J_{\bar{\varphi}(v)}(\theta_{u',P}) \circ J_v(\bar{\varphi}), \forall v \in V. \tag{2.13}$$

Para determinar $d_v\bar{\varphi}$, considere o isomorfismo canônico entre $\mathbb{C}^3$ e $D_+(u)$ e tome $V_a \subset \mathbb{C}^3$ identificado com V. De maneira análoga, tome $W_a \subset \mathbb{C}^3$ identificado com W.

$$\begin{tikzcd}
(1,x,y,z) & \mathbb{C}^4_{|\pi^{-1}(V)} \arrow[r, "\varphi"] & \mathbb{C}^4_{|\pi^{-1}(W)} \arrow[d, "\pi"] & \varphi((1,x,y,z)) \arrow[d, mapsto] \\
{[1:x,y,z]} \arrow[u, mapsto] & V \arrow[u] \arrow[r, "\bar{\varphi}"] \arrow[d, equal] & W \arrow[d, equal] & \pi\big(\varphi((1,x,y,z))\big) \arrow[d, mapsto] \\
(x,y,z) \arrow[u, mapsto] & V_a \arrow[r, dashed] & W_a & \left(\frac{\varphi_1}{\varphi_0}, \frac{\varphi_2}{\varphi_0}, \frac{\varphi_3}{\varphi_0}\right)(1,x,y,z)
\end{tikzcd}$$

Se $\varphi = (\varphi_0, \varphi_1, \varphi_2, \varphi_3)$, então

$$\begin{aligned}
\bar{\varphi} : V_a &\to W_a \\
(x,y,z) &\mapsto \left(\tfrac{\varphi_1}{\varphi_0} \circ \tau, \tfrac{\varphi_2}{\varphi_0} \circ \tau, \tfrac{\varphi_3}{\varphi_0} \circ \tau\right).
\end{aligned}$$

Logo, $d\bar{\varphi} = M \circ d\tau$, em que

$$M = \left(\begin{bmatrix} \varphi_0 \cdot \nabla\varphi_1 \\ \varphi_0 \cdot \nabla\varphi_2 \\ \varphi_0 \cdot \nabla\varphi_3 \end{bmatrix} - \begin{bmatrix} \varphi_1 \cdot \nabla\varphi_0 \\ \varphi_2 \cdot \nabla\varphi_0 \\ \varphi_3 \cdot \nabla\varphi_0 \end{bmatrix} \right) \cdot \frac{1}{\varphi_0^2}.$$

Como $\varphi_0(\tau(v)) = 1$, para todo $v \in V_a$, temos que a primeira coordenada de $d_v\bar{\varphi}(\zeta)$ é dada por

$$(\varphi_1 \circ \tau)(\zeta) - \varphi_1(\tau(v)) \cdot (\varphi_0 \circ \tau)(\zeta).$$

Note que, se $w = \bar{\varphi}(v)$, ou mais precisamente, se $w = \pi(\varphi(\tau(v)))$, então $\Gamma_v(\zeta) = \Phi_w\big((\varphi \circ \tau)(\zeta)\big)$, cuja primeira coordenada é igual à primeira coordenada de $d_v\bar{\varphi}(\zeta)$. Repetindo a análise para as outras coordenadas, concluímos que $\Gamma_v = d_v\bar{\varphi}$. Assim, (2.13) nos diz que $J_v(\theta_{u,F})$ e $J_{\bar{\varphi}(v)}(\theta_{u',P})$ são conjugadas. Em particular, tomando

$v = p$, segue-se que zero é um autovalor de $J_p(\theta_{u,F})$ se, e somente se, é um autovalor de $J_q(\theta_{u',P})$. Ou seja, ρ_F é não degenerado em p se, e somente se, ρ_P é não degenerado em q.

Agora, como $F = P \circ \varphi$, então $\bar{\varphi}$ se restringe a $V \cap \mathcal{Z}(F) \to W \cap \mathcal{Z}(P)$. Em particular, $d_v\bar{\varphi}(T_v\mathcal{Z}(F)) = T_{\bar{\varphi}(v)}\mathcal{Z}(P)$ e

$$d_v\bar{\varphi}_{|T_v\mathcal{Z}(F)} : T_v\mathcal{Z}(F) \to T_{\bar{\varphi}(v)}\mathcal{Z}(P)$$

é um isomorfismo. Além disso, no caso em que $p = v$, a proposição 1.2.4 nos diz que $T_p\mathcal{Z}(F)$ é invariante por $J_p(\theta_{u,F})$. Dessa forma,

$$d_v\bar{\varphi}_{|T_p\mathcal{Z}(F)} \circ J_p(\theta_{u,F})_{|T_p\mathcal{Z}(F)} \circ (d_v\bar{\varphi})^{-1}_{|T_q\mathcal{Z}(P)} = J_q(\theta_{u',P})_{|T_q\mathcal{Z}(P)}.$$

Sendo $J_p(\theta_{u,F})_{|T_p\mathcal{Z}(F)}$ e $J_q(\theta_{u',P})_{|T_q\mathcal{Z}(P)}$ conjugadas, temos que seus autovalores coincidem. ∎

Em vista do lema anterior, é suficiente estudarmos os autovalores de $J_q(\theta_{u',P})$ e, para facilitar a notação, usaremos as variáveis u, x, y, z ao invés de u', x', y', z'. Além disso, $P_\flat$ representa a desomogenização de P, ou seja, $P_\flat(x, y, z) = P(1, x, y, z)$. Lembre-se que $q = [1 : 0 : 0 : 0]$ e, considerando ainda a desomogenização em u, se $G \in \mathbb{C}[u, x, y, z]$, então $G_\flat(q) = G(1, 0, 0, 0)$. Nesta notação, temos que

$$\theta_{u,P} = \left(\left(\frac{\partial P}{\partial z} - \frac{\partial P}{\partial y}x \right)_\flat, -\left(\frac{\partial P}{\partial u} + \frac{\partial P}{\partial y}y \right)_\flat, -\left(\frac{\partial P}{\partial x} + \frac{\partial P}{\partial y}z \right)_\flat \right).$$

Note que

$$\begin{aligned} \nabla \left(\left(-\frac{\partial P}{\partial y}x \right)_\flat \right)(q) &= -\left(\frac{\partial P_\flat}{\partial y}(q), 0, 0 \right) \\ -\nabla \left(\left(\frac{\partial P}{\partial y}y \right)_\flat \right)(q) &= -\left(0, \frac{\partial P_\flat}{\partial y}(q), 0 \right) \\ -\nabla \left(\left(\frac{\partial P}{\partial y}z \right)_\flat \right)(q) &= -\left(0, 0, \frac{\partial P_\flat}{\partial y}(q) \right). \end{aligned}$$

Assim,

$$J_q(\theta_{u,P}) = J_q \left(\left(\frac{\partial P}{\partial z}, -\frac{\partial P}{\partial u}, -\frac{\partial P}{\partial x} \right)_\flat \right) - \frac{\partial P_\flat}{\partial y}(q) \cdot \mathrm{Id}_{3\times 3}. \tag{2.14}$$

Lema 2.3.2 *Nas condições acima,* $\frac{\partial P_\flat}{\partial y}(q) \neq 0$ *e*

$$\nabla(P_\flat)(q) = \left(0, \frac{\partial P_\flat}{\partial y}(q), 0\right) \quad e \quad \nabla\left(\left(\frac{\partial P}{\partial u}\right)_\flat\right)(q) = \left(0, (k-1)\frac{\partial P_\flat}{\partial y}(q), 0\right).$$

Demonstração. Denote $\breve{q} = (1, 0, 0, 0)$ e escrevendo P como polinômio em u, temos:

$$P = \zeta u^k + (ax + by + cz)u^{k-1} + (\text{termos de menor grau em } u),$$

em que $\zeta, a, b, c \in K_p$. Como $\theta_{u,P}$ singular em q, então $\theta_{u,P}(q) = 0$ e

$$\frac{\partial P_\flat}{\partial z}(q) = \left(\frac{\partial P}{\partial u}\right)_\flat(q) = \frac{\partial P_\flat}{\partial x}(q) = 0. \tag{2.15}$$

Sendo $a = \frac{\partial P}{\partial x}(\breve{q}) = \frac{\partial P_\flat}{\partial x}(q)$ e $c = \frac{\partial P}{\partial z}(\breve{q})$, segue-se que $a = c = 0$. Com isso,

$$\frac{\partial^2 P}{\partial u \partial x}(\breve{q}) = \frac{\partial^2\left((ax + by + cz)u^{k-1}\right)}{\partial u \partial x}(\breve{q}) = (k-1)a = 0.$$

De maneira análoga, $\frac{\partial^2 P}{\partial u \partial z}(\breve{q}) = (k-1)c = 0$. No caso da variável y, (2.15) nos diz que

$$\frac{\partial^2 P}{\partial u \partial y}(\breve{q}) = (k-1)b = (k-1)\frac{\partial P}{\partial y}(\breve{q}) \neq 0, \tag{2.16}$$

pois, sendo q um ponto não singular de $\mathcal{Z}(P)$, temos $\nabla P(\breve{q}) \neq 0$. Consequentemente, $\nabla\left(\left(\frac{\partial P}{\partial u}\right)_\flat\right)(q) = \left(0, (k-1)b, 0\right)$ e, por (2.15), $\nabla(P_\flat)(q) = (0, b, 0)$. ∎

Seja $b = \frac{\partial P_\flat}{\partial y}(q)$. Se $J_q\left(\left(\frac{\partial P}{\partial z}, -\frac{\partial P}{\partial u}, -\frac{\partial P}{\partial x}\right)_\flat\right) = (b_{i,j})$, então, por (2.14) e 2.3.2,

$$J_q(\theta_{u,P}) = \begin{pmatrix} b_{1,1} - b & b_{1,2} & b_{1,3} \\ 0 & -kb & 0 \\ b_{3,1} & b_{3,2} & b_{3,3} - b \end{pmatrix}, \tag{2.17}$$

com $b \neq 0$. Ainda por 2.3.2, temos que $T_q\mathcal{Z}(P)$ é gerado por $\partial/\partial x$ e $\partial/\partial z$. Assim, finalmente, obtemos

$$J_q(\theta_{u,P})_{|T_q\mathcal{Z}(P)} = \begin{pmatrix} \frac{\partial^2 P}{\partial z \partial x}(\breve{q}) - b & \frac{\partial^2 P}{\partial z^2}(\breve{q}) \\ -\frac{\partial^2 P}{\partial x^2}(\breve{q}) & -\frac{\partial^2 P}{\partial x \partial z}(\breve{q}) - b \end{pmatrix}. \tag{2.18}$$

Para reescrever $J_q(\theta_{u,P})_{|T_q\mathcal{Z}(P)}$ diretamente em função dos coeficientes de P, denote por $a_{2,2}, a_{2,4}, a_{4,4}$ os coeficientes de $x^2u^{k-2}, xzu^{k-2}, z^2u^{k-2}$, respectivamente, e observe que

$$\frac{\partial^2 P}{\partial x^2}(\breve{q}) = 2a_{2,2}\,, \quad \frac{\partial^2 P}{\partial z \partial x}(\breve{q}) = a_{2,4} \quad \text{e} \quad \frac{\partial^2 P}{\partial z^2}(q) = 2a_{4,4}.$$

Portanto,

$$J_q(\theta_{u,P})_{|T_q\mathcal{Z}(P)} = \begin{pmatrix} a_{2,4} - b & 2a_{4,4} \\ -2a_{2,2} & -a_{2,4} - b \end{pmatrix}, \tag{2.19}$$

cujo determinante é igual a $-a_{2,4}^2 + b^2 + 4a_{2,2}a_{4,4}$. Por razões que ficarão claras a seguir, preferimos escrever o determinante na forma:

$$\det\left(J_q(\theta_{u,P})_{|T_q\mathcal{Z}(P)}\right) = b^2 - (a_{2,4}^2 - 4a_{2,2}a_{4,4}).$$

Proposição 2.3.3 *Seja $F \in \mathbb{Q}[u,x,y,z]$ um polinômio homogêneo de grau k, tal que* $\operatorname{Sing}(\rho_F) = \operatorname{Sing}(\theta_u)$ *e $\mathcal{Z}(F)$ é não singular. Seja ainda $\mathcal{G}$ a base de Gröbner reduzida de $\mathcal{S}(\theta_u)$, com respeito à ordem lexicográfica em que $x > z > y$. Se $\mathcal{G}$ é da forma $\{f, x - f_1, z - f_3\}$, em que $f, f_1, f_3 \in \mathbb{Q}[y]$ e f é irredutível de grau $m(k)$, então existe um polinômio $\eta \in \mathbb{Q}[y]$, tal que*

$$\rho_F \text{ é não degenerado} \iff \eta \not\equiv 0 \mod (f). \tag{2.20}$$

Além disso, se ρ_F é não degenerado, então existe $\mu \in \mathbb{Q}[y]$, tal que são equivalentes:

1. *para todo $p \in \operatorname{Sing}(\theta_u)$, os autovalores λ_1, λ_2 de $J_p(\theta_u)_{|T_p\mathcal{Z}(F)}$ satisfazem a condição $\lambda_1/\lambda_2 \notin K_p$.*
2. *$h^2 \not\equiv \mu \mod (f)$, para todo $h \in \mathbb{Q}[y]$.*

Demonstração. Faremos a demonstração em três etapas.

Passo 1 - Construção de η e μ. Considere α, β e γ como variáveis independentes e defina

$$P = F(u, \alpha u + z, \beta u + \alpha x + y + \gamma z, \gamma u - x) \in \mathbb{Q}[\alpha,\beta,\gamma][u,x,y,z]. \tag{2.21}$$

Considerando P como polinômio em u, x, y, z, com coeficientes em $\mathbb{Q}[\alpha, \beta, \gamma]$, tome $B \in \mathbb{Q}[\alpha, \beta, \gamma]$ o coeficiente de yu^{k-1} e, $A_{2,2}, A_{2,4}, A_{4,4} \in \mathbb{Q}[\alpha, \beta, \gamma]$ os coeficientes de x^2u^{k-2}, xzu^{k-2} e z^2u^{k-2}, respectivamente. Se

$$\Delta = A_{2,4}^2 - 4A_{2,2}A_{4,4} \quad \text{e} \quad \Phi = B^2 - \Delta, \tag{2.22}$$

então definimos $\eta, \mu \in \mathbb{Q}[y]$ por:

$$\mu = \Delta\big(f_1(y), y, f_3(y)\big) \quad \text{e} \quad \eta = \Phi\big(f_1(y), y, f_3(y)\big). \tag{2.23}$$

Passo 2 - Equivalência em (2.20)**.** Por hipótese, $\mathcal{S}(\theta_u) = (f, x - f_1, z - f_3)$. Em particular,

$$\operatorname{Sing}(\theta_u) = \{\big(f_1(\xi), \xi, f_3(\xi)\big) : \xi \in \mathbb{C} \text{ e } f(\xi) = 0\}.$$

Assim, dado $p \in \operatorname{Sing}(\theta_{u,F})$, tome β_p a raiz de f associada a p e note que os números $b, a_{2,2}, a_{2,4}, a_{4,4}$ em (2.19) correspondem aos valores dos polinômios $B, A_{2,2}, A_{2,4}, A_{4,4}$ avaliados em $\big(f_1(\beta_p), \beta_p, f_3(\beta_p)\big)$. Dessa forma, se $q = [1 : 0 : 0 : 0]$, então, por (2.17) e (2.18),

$$\eta(\beta_p) = \Phi\big(f_1(\beta_p), \beta_p, f_3(\beta_p)\big) = \det\left(J_q(\theta_{u,P_p})_{|T_q\mathcal{Z}(P_p)}\right) = \frac{\det\big(J_q(\theta_{u,P_p})\big)}{-kb}. \tag{2.24}$$

Por outro lado, como $f_1, f_3 \in \mathbb{Q}[y]$, então $f_1(\beta_p), f_3(\beta_p) \in \mathbb{Q}(\beta_p)$ e $K_p = \mathbb{Q}(\beta_p)$. Com isso, $\varphi_p : \mathbb{Q}[y]/(f) \to K_p$, definido por $\varphi_p(\bar{h}) = h(\beta_p)$, é um isomorfismo. Sendo $\varphi_p(\bar{\eta}) = \eta(\beta_p)$, temos, por (2.24) e 2.3.1, que ρ_F é não degenerado em p se, e somente se, $\varphi_p(\bar{\eta}) \neq 0$, que por sua vez, equivale a $\bar{\eta} \neq 0$. Sendo p um ponto singular arbitrário em $\operatorname{Sing}(\theta_{u,F}) = \operatorname{Sing}(\rho_F)$, segue a equivalência em (2.20).

Passo 3 - Equivalência entre (1) **e** (2)**.** Suponha ρ_F não degenerado. Dado

$$p = [1 : f_1(\beta_p) : \beta_p : f_3(\beta_p)] \in \operatorname{Sing}(\theta_{u,F}),$$

tome $b, a_{2,2}, a_{2,4}, a_{4,4}$ as avaliações de $B, A_{2,2}, A_{2,4}, A_{4,4}$ em $\big(f_1(\beta_p), \beta_p, f_3(\beta_p)\big)$ respectivamente. Assim, de acordo com 2.3.1 e (2.19), os autovalores λ_1, λ_2 associados a p são as raízes de

$$(a_{2,4} - b - \lambda) \cdot (-a_{2,4} - b - \lambda) + 2a_{4,4} \cdot 2a_{2,2} = \lambda^2 + 2b\lambda + (b^2 - a_{2,4}^2 + 4a_{2,2}a_{4,4}).$$

Tomando $\Delta_p = a_{2,4}^2 - 4a_{2,2}a_{4,4}$ e $\sqrt{\Delta_p}$ uma das raízes de $x^2 = \Delta_p$, temos, por Bhaskara, que a razão entre os autovalores é:

$$\frac{\lambda_1}{\lambda_2} = \frac{-2b + \sqrt{4\Delta_p}}{-2b - \sqrt{4\Delta_p}} = \frac{-b + \sqrt{\Delta_p}}{-b - \sqrt{\Delta_p}} = \frac{b^2 - 2b\sqrt{\Delta_p} + \Delta_p}{b^2 - \Delta_p}.$$

Como $\Delta_p \in K_p$ e $b \in K_p^*$, segue-se que

$$\lambda_1/\lambda_2 \in K_p \iff \sqrt{\Delta_p} \in K_p. \tag{2.25}$$

Por outro lado, $\varphi_p(\bar{\mu}) = \mu(\beta_p) = \Delta\big(f_1(\beta_p), \beta_p, f_3(\beta_p)\big) = \Delta_p$. Assim, $\lambda_1/\lambda_2 \in K_p$ se, e somente se, $\Delta_p = \xi^2$, para algum $\xi \in K_p$ que, por φ_p, equivale à existência de $h \in \mathbb{Q}[y]$ satisfazendo $\overline{\mu} = \overline{h}^2$ em $\mathbb{Q}[y]/(f)$. Sendo p uma singularidade arbitrária, temos a equivalência entre (1) e (2). ∎

Para futuras referências, destacaremos duas observações. Antes contudo, fixemos a notação: se f é um polinômio em $\mathbb{C}[u, x, y, z]$, então $\mathrm{lc}(f)$ denota o coeficiente líder de f com respeito à ordem lexicográfica para a qual $u > x > z > y$.

Observação 2.3.4 Na demonstração acima, Δ e Φ são polinômios em $\mathbb{Q}[\alpha, \beta, \gamma]$ cujos coeficientes pertencem ao subanel de $\mathbb{Q}$ gerado pelos coeficientes de F. Portanto, os coeficientes de μ e η pertencem ao subanel de $\mathbb{Q}$ gerado pelos coeficientes de F, f_1 e f_3.

Observação 2.3.5 Seja F um polinômio com coeficientes inteiros satisfazendo as condições da proposição anterior. Se $\{\tilde{f}, nx - \tilde{f}_1, mz - \tilde{f}_3\}$, com $\tilde{f}, \tilde{f}_1, \tilde{f}_3 \in \mathbb{Z}[y]$ e $n, m \in \mathbb{Z}$, também é base de Gröbner para $\mathcal{S}(\theta_u)$, em que $\deg \tilde{f}_1, \deg \tilde{f}_3 < \deg \tilde{f}$, então $\{\tilde{f}/\mathrm{lc}(\tilde{f}), x - \tilde{f}_1/n, z - \tilde{f}_3/m\}$ é a base reduzida de $\mathcal{S}(\theta_u)$. Portanto,

$$\mu = \Delta\left(\frac{\tilde{f}_1}{n}, y, \frac{\tilde{f}_3}{m}\right) \quad \text{e} \quad \eta = \Phi\left(\frac{\tilde{f}_1}{n}, y, \frac{\tilde{f}_3}{m}\right). \tag{2.26}$$

Além disso, pela observação acima, se q é um número primo que não divide n nem m, então μ e η tem seus coeficientes em $\mathbb{Z}$ localizado em $q\mathbb{Z}$.

A proposição 2.3.3 é peça fundamental na construção de exemplos de variedades involutivas mínimas, pois, juntamente com o teorema 2.2.15, nos fornece um critério que pode ser implementado em sistemas de computação algébrica. De agora em diante, denotaremos por η_F e μ_F os polinômios construídos na demonstração da proposição, e além disso, em vista dos isomorfismos φ_p's, escreveremos $\sqrt{\mu} \notin \mathbb{Q}[y]/(f)$ para representar a afirmação: $h^2 \not\equiv \mu \mod (f)$, para todo $h \in \mathbb{Q}[y]$. Como aplicação inicial de 2.3.3, temos:

Exemplo 2.3.6 $F = y^3 + u^2x + 2x^2u + 3z^3$ define uma variedade involutiva mínima. Mostraremos que F satisfaz as hipóteses de 2.2.15. Comecemos verificando que $\mathcal{Z}(F)$ é não singular e que $\mathrm{Sing}(\rho_{F_d})$ é finito. Como este exemplo será útil mais adiante, mostraremos que F, em uma forma um pouco mais geral, satisfaz duas condições.

Afirmação 1. Se $F_d = y^3 + u^2x + 2x^2u + dz^3$, então $\mathcal{Z}(F_d)$ é não singular, qualquer que seja $d \in \mathbb{Z}^*$.

Demonstração da Afirmação. Suponha, por absurdo, que $p = [u_0 : x_0 : y_0 : z_0]$ é um ponto singular de $\mathcal{Z}(F_d)$. De maneira imediata, $y_0 = z_0 = 0$. Multiplicando por u a derivada parcial em relação a u e aplicando em p, temos que

$$0 = u\frac{\partial F}{\partial u}(p) = 2u_0^2x_0 + 2x_0^2u_0 = u_0^2x_0 + (u_0^2x_0 + 2x_0^2u_0).$$

Como $p \in \mathcal{Z}(F_d)$, $u_0^2x_0 + 2x_0^2u_0 = 0$. Assim, $u_0^2x_0 = 0$ e $u_0 = 0$ ou $x_0 = 0$. Se $u_0 = 0$, então $2x_0^2 = \frac{\partial F_d}{\partial u}(p) = 0$ nos diz que $x_0 = 0$. Analogamente, se $x_0 = 0$, então $u_0 = 0$, pois $\frac{\partial F_d}{\partial x}(p) = 0$. Dessa forma, $u_0 = x_0 = y_0 = z_0 = 0$, que é uma contradição. Portanto, F_d é não singular e a afirmação segue.

Afirmação 2. $\mathrm{Sing}(\theta_{u,F_d}) \subset D_+(u)$, para todo $d \in \mathbb{Z}^*$.

Demonstração da Afirmação. Suponha, por absurdo, que $p = [0 : x_0 : y_0 : z_0]$ é uma singularidade de ρ_{F_d}. Tome $\breve{p} = (0, x_0, y_0, z_0) \in \mathbb{C}^4$. Sendo $h_{F_d}(\breve{p})$ proporcional a $E(\breve{p}) = (0, x_0, y_0, z_0)$, segue-se que $3y^2(\breve{p}) = \partial_y F_d(\breve{p}) = 0$. Logo, $y_0 = 0$. Por 2.1.4, $p \in \mathcal{Z}(F)$ e $z_0 = 0$. Novamente pela proporcionalidade entre $h_F(\breve{p})$ e $E(\breve{p})$, temos, de $\partial_z F_d(\breve{p}) = 3dz^2(\breve{p}) = 0$, que $x_0 = 0$. Com isso, $x_0 = y_0 = z_0 = 0$, o que não é possível. Dessa forma, $\mathrm{Sing}(\theta_{u,F_d}) \subset D_+(u)$.

Voltemos a F. Com a ajuda do sistema de computação algébrica Singular, calculamos a base de Gröbner de $\mathcal{S}(\theta_u)$ com respeito à ordem lexicográfica para a qual $u > x > z > y$, obtendo:

$$\mathcal{S}(\theta_u) = \big(9y^{15} + 386y^6 - 96y^3 + 6, x - f_1, z - f_3\big), \tag{2.27}$$

em que $f_1 = (-216y^{12} - 9y^9 + 576y^6 - 9240y^3 + 382)/3074$ e

$$f_3 = (6903y^{13} + 864y^{10} + 36y^7 + 293758y^4 - 36672y)/9222.$$

Pelo critério de Eisenstein, para o primo $p = 2$, $f = 9y^{15} + 386y^6 - 96y^3 + 6$ é irredutível de grau $15 = m(3)$. Como $\mathcal{S}(\theta_u) \cap \mathbb{Q}[y] = (f)$, então $\mathcal{S}(\theta_u)$ satisfaz uma das condições do teorema 2.2.15. Além disso, pela afirmação (1), $\mathcal{Z}(F)$ é não singular e, pela afirmação (2), $\mathrm{Sing}(\rho_F) = \mathrm{Sing}(\theta_{u,F})$ que, por (2.27), é finito. Resta mostrar que ρ_F é não degenerado e que a condição sobre os autovalores é satisfeita. Para isto, usaremos as equivalências em 2.3.3. Definindo P como em (2.21), e calculando η_F e μ_F como em (2.23), obtemos:

$$\eta_F \equiv (81540y^{13} + 10314y^{10} + 3888y^7 + 3538821y^4 - 437772y)/1537 \mod (f) \text{ e}$$
$$\mu_F \equiv (-81540y^{13} - 10314y^{10} - 3888y^7 - 3524988y^4 + 437772y)/1537 \mod (f).$$

Sendo $\eta_F \not\equiv 0 \mod (f)$, segue-se que ρ_F é não degenerado. Quanto à μ_F, denote $\mathbb{Q}[y]/(f)$ por L e note que a condição $\sqrt{\overline{\mu_F}} \notin L$ é equivalente a $T^2 - \overline{\mu_F}$ ser irredutível em $L[T]$. Mas, usando o Singular para fatorar $T^2 - \overline{\mu_F}$ em $L[T]$, temos como saída que $T^2 - \overline{\mu_F}$ já é irredutível. Assim, $\sqrt{\overline{\mu_F}} \notin L$ e a condição sobre os autovalores é satisfeita. Com isso, concluímos a verificação de todas as hipóteses de 2.2.15 e temos que $\mathcal{Z}(F)$ é de fato uma variedade involutiva mínima. $\square$

2.4 Polinômios q-equivalentes

Nesta seção, fixado um número primo q, definiremos uma relação de equivalência entre polinômios em $\mathbb{Z}[u, x, y, z]$. Veremos no corolário 2.4.3 que, sob certas condições, se $\mathcal{Z}(F)$ é involutiva mínima e G é equivalente a F, então $\mathcal{Z}(G)$ também é involutiva mínima. Com isso, a partir de uma única variedade involutiva mínima, poderemos, na próxima seção, exibir toda uma família de variedades mínimas.

Seja $F \in \mathbb{Z}[u, x, y, z]$ um polinômio homogêneo. Se $\{h_i \in \mathbb{Q}[x, y, z] : i \in I\}$ é a base de Gröbner reduzida de $\mathcal{S}(\theta_u)$, tome, para cada $i \in I$, o inteiro positivo z_i, tal que $z_i h_i \in \mathbb{Z}[x, y, z]$ tem conteúdo igual a 1. Dizemos que $\{z_i h_i : i \in I\}$ é a base *$\mathbb{Z}$-reduzida* de $\mathcal{S}(\theta_u)$. Note que esta base é uma base de Gröbner e está univocamente determinada, pois a base reduzida, de $\mathcal{S}(\theta_u)$ em $\mathbb{Q}[x, y, z]$, é única; veja [8, Proposição 5.9, pg. 163]. De agora em diante, a menos de menção em contrário, toda base de Gröbner refere-se à ordem lexicográfica para a qual $u > x > z > y$, que, na ausência da variável u, restringe-se a $x > z > y$.

Sejam, agora, $q \in \mathbb{N}$ um número primo e $F \in \mathbb{Z}[u, x, y, z]$ um polinômio homogêneo de grau k, tal que $\mathcal{Z}(F)$ é não singular e $\mathrm{Sing}(\rho_F)$ é finito. Dizemos que F é *q-compatível* se a base $\mathbb{Z}$-reduzida de $\mathcal{S}(\theta_{u,F})$, em relação à ordem lexicográfica para a qual $x > z > y$, é da forma

$$\{f, nx - f_1, mz - f_3\}, \tag{2.28}$$

em que $f, f_1, f_3 \in \mathbb{Z}[y]$ são polinômios com coeficientes inteiros em uma única variável y, tais que:

1. f é irredutível de grau $m(k)$;

2. q não divide $n \cdot m \cdot \mathrm{lc}(f)$.

Note que, pela unicidade da base $\mathbb{Z}$-reduzida, os coeficientes n, m e $\mathrm{lc}(f)$ estão univocamente determinados.

Ainda com $q \in \mathbb{N}$ primo, sejam $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$, $\mathfrak{q} = q\mathbb{Z}$ e $\mathbb{Z}_\mathfrak{q}$ a localização de $\mathbb{Z}$ em seu ideal primo $\mathfrak{q}$. Tomando $\varphi : \mathbb{Z} \to \mathbb{F}_q$ a aplicação canônica, temos que $\varphi(z)$ tem inverso para todo $z \notin \mathfrak{q}$. Assim, φ induz uma aplicação de $\mathbb{Z}_\mathfrak{q}$ em $\mathbb{F}_q$, que por sua vez, induz

$$\pi : \mathbb{Z}_\mathfrak{q}[y] \to \mathbb{F}_q[y]. \tag{2.29}$$

A aplicação acima será ingrediente chave na definição da relação de equivalência. Sejam $F, G \in \mathbb{Z}[u, x, y, z]$ polinômios homogêneos q-compatíveis, tais que as bases $\mathbb{Z}$-reduzidas de $\mathcal{S}(\theta_{u,F})$ e $\mathcal{S}(\theta_{u,G})$ sejam

$$\{f, n_F x - f_1, m_F z - f_3\} \quad \text{e} \quad \{g, n_G x - g_1, m_G z - g_3\},$$

respectivamente. Dizemos que F e G são *q-equivalentes* se as seguintes condições se verificam:

1. $F \equiv G \bmod q$ e $\deg F = \deg G$;

2. $\pi(f)$ e $\pi(g)$ são associados (em $\mathbb{F}_q[y]$);

3. $\pi(f_1/n_F) = \pi(g_1/n_G)$ e $\pi(f_3/m_F) = \pi(g_3/m_G)$.

Neste caso, escrevemos $F \sim_q G$. Vale ressaltar que nosso interesse reside exclusivamente sobre os polinômios F's, com coeficientes inteiros, cujos ideais $\mathcal{S}(\theta_{u,F})$'s apresentam uma boa base de Gröbner em relação a q, ou seja, estamos interessados apenas nos polinômios q-compatíveis. E é somente neste universo de polinômios q-compatíveis que a relação de equivalência acima está definida.

A partir de uma variedade mínima $\mathcal{Z}(F)$, queremos mostrar, sob certas condições, que se $F \sim_q G$, então $\mathcal{Z}(G)$ também é mínima. Assim, as equivalências na proposição 2.3.3 motivam nossa próxima definição. Seja $F \in \mathbb{Z}[u,x,y,z]$ um polinômio homogêneo q-compatível, com $\{f, nx - f_1, mz - f_3\}$ sendo a base $\mathbb{Z}$-reduzida de $\mathcal{S}(\theta_u)$. Pela observação 2.3.5, μ_F e η_F têm seus coeficientes em $\mathbb{Z}_{\mathfrak{q}}$. Logo, μ_F e η_F pertencem ao domínio de π. Dizemos então, que F é *q-mínimo* se:

1. $\pi(f)$ é irredutível de grau $m(k)$;

2. $\pi(\eta_F) \not\equiv 0 \bmod \pi(f)$;

3. $\overline{\pi(\mu_F)}^{1/2} \notin \mathbb{F}_q[y]/(\pi(f))$.

Lema 2.4.1 *Sejam q um número primo e $F, G \in \mathbb{Z}[u,x,y,z]$ polinômios homogêneos q-compatíveis. Se $F \sim_q G$, então*

$$\pi(\mu_F) = \pi(\mu_G) \quad e \quad \pi(\eta_F) = \pi(\eta_G).$$

Demonstração. Sendo F e G polinômios q-compatíveis, tome

$$\{f, n_F x - f_1, m_F z - f_3\} \quad \text{e} \quad \{g, n_G x - g_1, m_G z - g_3\},$$

as bases $\mathbb{Z}$-reduzidas de $\mathcal{S}(\theta_{u,F})$ e $\mathcal{S}(\theta_{u,G})$, respectivamente. Tome ainda,

$$\begin{aligned} P_F &= F(u, \alpha u + z, \beta u + \alpha x + y + \gamma z, \gamma u - x) \quad \text{e} \\ P_G &= G(u, \alpha u + z, \beta u + \alpha x + y + \gamma z, \gamma u - x), \end{aligned}$$

polinômios em $\mathbb{Z}[\alpha,\beta,\gamma][u,x,y,z]$. Como $F \equiv G \bmod q$, temos que $P_F \equiv P_G \bmod q$. Em particular, considerando-se P_F e P_G como polinômios em u, x, y, z, temos que seus coeficientes são polinômios em $\mathbb{Z}[\alpha,\beta,\gamma]$ congruentes módulo q. Portanto, se $\Delta_F, \Delta_G, \Phi_F$ e Φ_G são obtidos de acordo com as construções em (2.22), então

$$\Delta_F \equiv \Delta_G \bmod q \quad \text{e} \quad \Phi_F \equiv \Phi_G \bmod q. \tag{2.30}$$

Por outro lado, de acordo com (2.26),

$$\mu_F = \Delta_F\left(\frac{f_1}{n_F}, y, \frac{f_3}{m_F}\right) \quad \text{e} \quad \mu_G = \Delta_G\left(\frac{g_1}{n_G}, y, \frac{g_3}{m_G}\right).$$

Assim, calculando $\pi(\mu_F)$ e usando a congruência em (2.30), segue-se que

$$\pi(\mu_F) = \pi\left(\Delta_F\left(\frac{f_1}{n_F}, y, \frac{f_3}{m_F}\right)\right) = \pi\left(\Delta_G\left(\frac{f_1}{n_F}, y, \frac{f_3}{m_F}\right)\right).$$

Sendo $F \sim_q G$, temos que $\pi(f_1/n_F) = \pi(g_1/n_G)$ e $\pi(f_3/m_F) = \pi(g_3/m_G)$. Logo,

$$\pi(\mu_F) = \Delta_G\left(\pi\left(\frac{f_1}{n_F}\right), y, \pi\left(\frac{f_3}{m_F}\right)\right) = \Delta_G\left(\pi\left(\frac{g_1}{n_G}\right), y, \pi\left(\frac{g_3}{m_G}\right)\right) = \pi(\mu_G).$$

E provamos a primeira igualdade $\pi(\mu_F) = \pi(\mu_G)$. Aplicando o mesmo raciocínio aos η's, temos, por (2.26), que

$$\eta_F = \Phi_F\left(\frac{f_1}{n_F}, y, \frac{f_3}{m_F}\right) \quad \text{e} \quad \eta_G = \Phi_G\left(\frac{g_1}{n_G}, y, \frac{g_3}{m_G}\right).$$

Novamente, por (2.30) e pela relação $F \sim_q G$, segue-se que

$$\pi(\eta_F) = \pi\left(\Phi_G\left(\frac{f_1}{n_F}, y, \frac{f_3}{m_F}\right)\right) = \Phi_G\left(\pi\left(\frac{g_1}{n_G}\right), y, \pi\left(\frac{g_3}{m_G}\right)\right) = \pi(\eta_G).$$

Dessa forma, a segunda igualdade também se verifica. ■

Proposição 2.4.2 *Sejam q um número primo e $F, G \in \mathbb{Z}[u,x,y,z]$ polinômios homogêneos q-compatíveis de mesmo grau k. Seja, ainda, $\{g, n_G x - g_1, m_G z - g_3\}$ a base $\mathbb{Z}$-reduzida de $\mathcal{S}(\theta_{u,G})$. Se $F \sim_q G$ e F é q-mínimo, então $\sqrt{\mu_G} \notin \mathbb{Q}[y]/(g)$ e $\eta_G \not\equiv 0 \mod g$.*

Demonstração. Tome

$$\{f, n_F x - f_1, m_F z - f_3\}$$

a base $\mathbb{Z}$-reduzida de $\mathcal{S}(\theta_{u,F})$. Mostraremos inicialmente que $\sqrt{\mu_G} \notin \mathbb{Q}[y]/(g)$. De $F \sim_q G$, obtemos, por definição, que $\pi(f)$ é associado a $\pi(g)$. Logo, a aplicação identidade de $\mathbb{F}_q[y]$ em $\mathbb{F}_q[y]$ induz um isomorfismo $\varphi : \mathbb{F}_q[y]/(\pi(f)) \to \mathbb{F}_q[y]/(\pi(g))$, tal que o diagrama

$$\begin{tikzcd} \mathbb{F}_q[y] \arrow[r] \arrow[dr] & \mathbb{F}_q[y]/(\pi(f)) \arrow[d, "\varphi"] \\ & \mathbb{F}_q[y]/(\pi(g)) \end{tikzcd} \tag{2.31}$$

comuta. Além disso, como F é q-mínimo, temos que $\overline{\pi(\mu_F)}^{1/2} \notin \mathbb{F}_q[y]/(\pi(f))$; isto é, o polinômio $T^2 - \overline{\pi(\mu_F)}$ é irredutível em $\frac{\mathbb{F}_q[y]}{(\pi(f))}[T]$. Contudo, pelo lema anterior, $\pi(\mu_F) = \pi(\mu_G)$. Portanto, $T^2 - \overline{\pi(\mu_G)}$ é irredutível em $\frac{\mathbb{F}_q[y]}{(\pi(g))}[T]$. Dessa forma, o homomorfismo

$$\frac{\mathbb{Z}_{\mathfrak{q}}[y]}{(g)}[T] \to \frac{\mathbb{F}_q[y]}{(\pi(g))}[T],$$

induzido por π, nos diz que $T^2 - \overline{\mu_G}$ é irredutível em $\frac{\mathbb{Z}_{\mathfrak{q}}[y]}{(g)}[T]$. Agora, por A.3, $\mathbb{Z}_{\mathfrak{q}}[y]/(g)$ é um domínio fatorial, cujo corpo de frações é $\mathbb{Q}[y]/(g)$. Assim, pelo Lema de Gauss, $T^2 - \overline{\mu_G}$ é irredutível sobre $\mathbb{Q}[y]/(g)$, ou seja,

$$\sqrt{\overline{\mu_G}} \notin \mathbb{Q}[y]/(g).$$

Resta mostrar que $\eta_G \not\equiv 0 \mod g$. Como F é q-mínimo, $\overline{\pi(\eta_F)} \neq 0$ em $\mathbb{F}_q[y]/(\pi(f))$. Pelo lema anterior, $\pi(\eta_F) = \pi(\eta_G)$ e, usando a identificação em (2.31), temos que $\overline{\pi(\eta_G)} \neq 0$ em $\mathbb{F}_q[y]/(\pi(g))$. Ou seja, $\tilde{\pi}(\overline{\eta_G}) \neq 0$. Em particular, $\overline{\eta_G} \neq 0$ em $\mathbb{Z}_{\mathfrak{q}}[y]/(g)$. Portanto,

$$\overline{\eta_G} \neq 0 \text{ em } \mathbb{Q}[y]/(g);$$

veja observação A.4. ■

Corolário 2.4.3 *Sejam q um número primo e $F, G \in \mathbb{Z}[u, x, y, z]$ polinômios homogêneos q-compatíveis de grau k igual 3 ou 4, tais que $F \sim_q G$. Se F é q-mínimo, então $\mathcal{Z}(G)$ é involutiva mínima.*

Demonstração. Para provar que $\mathcal{Z}(G)$ é involutiva mínima, é suficiente verificarmos as hipóteses do teorema 2.2.15. Como G é q-compatível, então, por definição, $\mathcal{Z}(G)$ é não singular e ρ_F contém apenas uma quantidade finita de singularidades. Além disso, a base $\mathbb{Z}$-reduzida de $\mathcal{S}(\theta_{u,G})$ é da forma:

$$\mathcal{G} = \{g, n_G x - g_1, m_G z - g_3\},$$

em que $g \in \mathbb{Z}[y]$ é irredutível de grau $m(k)$. Como $g \in \mathcal{S}(\theta_{u,G}) \cap \mathbb{Q}[y]$ e $\mathbb{Q}[y]$ é um domínio de ideais principais, segue da irredutibilidade de g que

$$\mathcal{S}(\theta_{u,G}) \cap \mathbb{Q}[y] = (g).$$

Assim, verificamos três das hipóteses do teorema 2.2.15. Resta provar que o campo ρ_G é não degenerado e que vale a condição sobre os autovalores associados às singularidades de ρ_G. Contudo, pela proposição 2.3.3, estas duas hipóteses são equivalentes a $\overline{\eta_G} \neq 0$ em $\mathbb{Q}[y]/(g)$ e $\sqrt{\mu_G} \notin \mathbb{Q}[y]/(g)$. Portanto, pela proposição anterior, $\mathcal{Z}(G)$ é variedade involutiva mínima. ■

Exemplo 2.4.4 Seja

$$\begin{aligned} F = u^3 + u^2x + u^2y + u^2z + 2ux^2 + 2uy^2 + 2uz^2 + 8x^3 \\ + x^2y + x^2z + 2xy^2 + 2xz^2 + y^3 + y^2z + 2yz^2 + 8z^3. \end{aligned}$$

Em [2], L. C. O. Almeida e S. C. Coutinho mostraram que F define uma variedade involutiva mínima. Este é o primeiro, e até o momento, o único exemplo concreto de uma variedade involutiva mínima encontrado na literatura. Vejamos que F é 29-mínimo. De fato, calculando a base de Gröbner para $\mathcal{S}(\theta_u)$ no Singular, obtemos que $\mathcal{S}(\theta_u)$ é gerado por $\{f, nx - f_1, mz - f_3\}$ com $f, f_1, f_3 \in \mathbb{Z}[y]$, em que

$$\begin{aligned} f = 8008437601600y^{15} + 78249430071040y^{14} + 366986878364864y^{13} \\ +1101180576025792y^{12} + 2385157428197184y^{11} + 3988752594636448y^{10} \\ + 5362037277684144y^9 + 5930160900133088y^8 + 5468751014770636y^7 \\ + 4229126908379472y^6 + 2737402505413244y^5 + 1472646978689336y^4 \\ + 642752946860013y^3 + 222497314188384y^2 + 54676874408130y + 9051833473125 \end{aligned}$$

é irredutível. Não exibiremos f_1 nem f_3, pois seus coeficientes contêm muitos dígitos. Pelo mesmo motivo, não explicitaremos n nem m. Contudo, verificamos computacionalmente que $8008437601600 \cdot n \cdot m \equiv 24 \cdot 26 \cdot 14 \mod 29$. Assim, F é 29-compatível. Além disso,

$$\pi(f) = -5y^{15}+6y^{14}+11y^{12}+12y^{11}+6y^{10}+6y^{9}-y^{8}+13y^{7}-5y^{6}+8y^{4}-6y^{3}-6y^{2}+9y+13$$

é irredutível em $\mathbb{F}_{29}[y]$ e

$$\begin{aligned}\pi(\eta) \equiv -7y^{14} - 11y^{13} + 6y^{12} + 12y^{11} + 3y^{10} - 11y^{9} + 7y^{8} - 14y^{7} \\ - 11y^{6} - y^{5} + 5y^{4} + 7y^{3} - 5y^{2} + 3 \not\equiv 0 \mod \pi(f).\end{aligned}$$

Como $T^2 - \overline{\pi(\mu)}$ é irredutível sobre $\mathbb{F}_{29}[y]/\big(\pi(f)\big)$, em que

$$\begin{aligned}\overline{\pi(\mu)} = -y^{13} - 12y^{12} - 4y^{11} + 13y^{10} + 4y^{9} + 12y^{8} - 10y^{7} - 9y^{6} \\ + 3y^{5} + 7y^{4} + 5y^{3} + 14y^{2} + 4y - 13,\end{aligned}$$

então F é 29-mínimo. Dessa forma, provamos, através do corolário 2.4.3, o resultado obtido em [2], sem utilizar as aproximações necessárias ao enfoque adotado naquele artigo. $\square$

2.5 Famílias Involutivas Mínimas

De acordo com o corolário 2.4.3, para construirmos uma família de variedades involutivas mínimas, precisamos, a partir de um polinômio q-mínimo F, construir uma família de polinômios q-equivalentes a F. Para tanto, usaremos parâmetros $t_1, \ldots, t_l$ e estudaremos condições sobre um polinômio $H \in \mathbb{Z}[t_1, \ldots, t_l][u, x, y, z]$, de tal maneira que, atribuindo valores aos $t_i's$, produziremos, conforme o teorema 2.5.2, uma família de polinômios q-equivalentes a F. Para facilitar a notação, $\mathbf{t}$ representará o conjunto de parâmetros $t_1, \ldots, t_l$.

Dado $d = (d_1, \ldots, d_l) \in \mathbb{Z}^l$, tome o homomorfismo de anéis

$$\Psi_d : \mathbb{Q}[\mathbf{t}][x, y, z] \to \mathbb{Q}[x, y, z]$$

definido por $\Psi_d(t_i) = d_i, 1 \leq i \leq l$, e que fixa x, y e z. Tome ainda

$$\tilde{\Psi}_d : \mathbb{Q}[\mathbf{t}][u, x, y, z] \to \mathbb{Q}[u, x, y, z]$$

estendendo Ψ_d com $\tilde{\Psi}_d(u) = u$. Seja, agora, $H \in \mathbb{Z}[\mathbf{t}][u, x, y, z]$ um polinômio homogêneo em u, x, y, z, com coeficientes em $\mathbb{Z}[\mathbf{t}]$. Sob certas condições, mostraremos que, se $\tilde{\Psi}_{d_0}(H)$ é q-mínimo e $d \equiv d_0 \mod q$, então $\mathcal{Z}\big(\tilde{\Psi}_d(H)\big)$ é involutiva mínima, em que a notação $d \equiv d_0 \mod q$ significa que a i-ésima coordenada de d é congruente, módulo q, a i-ésima coordenada de d_0, para todo $i \in \{1, \ldots, l\}$. Comecemos fixando a notação. Sejam M_H e L_H os ideais gerados pelos menores 2×2 da matriz

$$\begin{bmatrix} \frac{\partial H}{\partial y} & \frac{\partial H}{\partial z} & -\frac{\partial H}{\partial u} & -\frac{\partial H}{\partial x} \\ 1 & x & y & z \end{bmatrix}_{|u=1}, \tag{2.32}$$

em $\mathbb{Q}(\mathbf{t})[x, y, z]$ e $\mathbb{Q}[\mathbf{t}][x, y, z]$, respectivamente. Observe que M_H é um ideal do anel de polinômios em x, y e z, com coeficientes no corpo $\mathbb{Q}(\mathbf{t})$, enquanto o anel de polinômios referente a L_H tem seus coeficientes apenas em um anel, a saber $\mathbb{Q}[\mathbf{t}]$. Estamos interessados no caso em que M_H admite uma base de Gröbner da forma

$$\mathcal{G} = \{h, rx - h_1, sz - h_3\}, \text{ com } h, h_1, h_3 \in \mathbb{Z}[\mathbf{t}][y] \text{ e } 0 \neq r, s \in \mathbb{Z}[\mathbf{t}], \tag{2.33}$$

em que $\deg h_1, \deg h_3 < \deg h$, como polinômios em y com coeficientes em $\mathbb{Z}[\mathbf{t}]$. Neste caso, se $c(\mathbf{t}) \in \mathbb{Z}[\mathbf{t}]$ é o coeficiente líder de h, tome a subvariedade $B = \mathcal{Z}(rsc)$ de $\mathbb{C}^l$.

Lema 2.5.1 *Seja $H \in \mathbb{Z}[\mathbf{t}][u, x, y, z]$ um polinômio homogêneo em u, x, y, z, tal que M_H admite uma base de Gröbner $\mathcal{G}$ como em* (2.33). *Se $\mathcal{G} \subset L_H$, então*

$$\mathcal{S}(\theta_{u, \tilde{\Psi}_d(H)}) = \big(\Psi_d(h), \Psi_d(rx - h_1), \Psi_d(sz - h_3)\big),$$

para todo $d \in \mathbb{Z}^l \setminus B$.

Demonstração. Sejam $d \in \mathbb{Z}^l$ e $P_1, \dots, P_6$ os menores da matriz em (2.32). Para cada $i = 1, \dots, 6$, defina $p_i = \Psi_d(P_i)$. Como $h \in L_H$, existem $g_1, \dots, g_6 \in \mathbb{Q}[\mathbf{t}][x, y, z]$, tais que $h = \sum g_i P_i$. Em particular, $\Psi_d(h) = \sum \Psi_d(g_i) p_i \in \mathcal{S}(\theta_{u, \tilde{\Psi}_d(H)})$, pois $p_1, \dots, p_6$ são justamente os polinômios que definem $\mathcal{S}(\theta_{u, \tilde{\Psi}_d(H)})$ como ideal de $\mathbb{Q}[x, y, z]$; veja (2.7). Aplicando os mesmos argumentos a $rx - h_1$ e $sz - h_3$, concluímos que

$$\big(\Psi_d(h), \Psi_d(rx - h_1), \Psi_d(sz - h_3)\big) \subset \mathcal{S}(\theta_{u, \tilde{\Psi}_d(H)}).$$

Note que não há restrições a $d \in \mathbb{Z}^l$ para a relação de inclusão acima.

Vejamos a reciproca. Seja P um dos menores da matriz em (2.32). Nosso primeiro passo será determinar um polinômio $\xi \in \mathbb{Q}[\mathbf{t}]$, tal que ξP pertence ao ideal gerado por $\mathcal{G}$ em $\mathbb{Q}[\mathbf{t}][x, y, z]$. Comecemos tomando $a_{i,j} \in \mathbb{Z}[\mathbf{t}][y]$, com $0 \le i, j \le m$, tais que

$$P(\mathbf{t}, x, y, z) = \sum_{0 \le i, j \le m} a_{i,j} x^i z^j.$$

Multiplicando por $r^m s^m$, temos, em $\mathbb{Z}[\mathbf{t}][x, y, z]$, que

$$\begin{aligned} r^m s^m P &= \sum a_{i,j} \cdot r^{m-i} \cdot (rx)^i \cdot s^{m-j} \cdot (sz)^j \\ &= \sum a_{i,j} \cdot r^{m-i} \cdot \big((rx - h_1) + h_1\big)^i \cdot s^{m-j} \cdot \big((sz - h_3) + h_3\big)^j. \end{aligned}$$

Definindo $\phi = \sum a_{i,j} \cdot r^{m-i} \cdot h_1^i \cdot s^{m-j} \cdot h_3^j$, podemos escrever $r^m s^m P$ na forma:

$$r^m s^m P = \phi + \Phi_1 \cdot (rx - h_1) + \Phi_2 \cdot (sz - h_3), \tag{2.34}$$

com $\phi \in \mathbb{Z}[\mathbf{t}][y]$ e $\Phi_1, \Phi_2 \in \mathbb{Z}[\mathbf{t}][x, y, z]$. Lembrando que $P, (rx - h_1), (sz - h_3) \in M_H$, segue-se que $\phi \in M_H \cap \mathbb{Q}(t)[y]$. Contudo, $\mathcal{G}$ é uma base de Gröbner para M_H com relação à ordem lexicográfica em que $x > z > y$. Assim, $M_H \cap \mathbb{Q}(\mathbf{t})[y]$ é gerado por h e existem $a = \sum_{i=1}^n \alpha_i(t) y^i \in \mathbb{Q}[\mathbf{t}][y]$ e $b \in \mathbb{Q}[\mathbf{t}]$, tais que $\phi = (a/b)h$. Sem perda de generalidade, podemos supor que m.d.c.$\{a, b\} = 1$. Tomando $\xi = b r^m s^m$, temos, por (2.34), que

$$b r^m s^m P = ah + b\Phi_1 \cdot (rx - h_1) + b\Phi_2 \cdot (sz - h_3) \in \mathcal{G} \cdot \mathbb{Q}[\mathbf{t}][x, y, z]. \tag{2.35}$$

E concluímos nosso primeiro passo.

Afirmação. $\mathcal{Z}(b) \subset \mathcal{Z}(\mathrm{lc}(h))$.

Demonstração da afirmação. Denote $c = \mathrm{lc}(h)$ e suponha, por absurdo, que $\mathcal{Z}(b) \not\subset \mathcal{Z}(c)$. Com isso, b não divide c e podemos tomar w um fator irredutível de b que não divide c. Por outro lado, fixado $i \in \{1, \ldots, n\}$, a equação (2.35) nos diz que $\mathcal{Z}(b) \subset \mathcal{Z}(\alpha_i c)$. Assim, pelo Nullstellensatz, $\alpha_i c$ pertence ao radical de $b \cdot \mathbb{C}[\mathbf{t}]$. Como $b, \alpha_i, c \in \mathbb{Q}[\mathbf{t}]$, temos, na verdade, que $\alpha_i c$ pertence ao radical de (b) como ideal de $\mathbb{Q}[\mathbf{t}]$. Dessa forma, w divide $\alpha_i c$, para todo i. Como w não divide c, segue-se que w divide o m.d.c.$\{a, b\}$ que é igual a 1. Absurdo. E isto conclui a demonstração da afirmação.

Seja agora $d \in \mathbb{Z}^l \setminus B$. Sendo $\Psi_d(br^m s^m)$ diferente de zero, obtemos

$$\Psi_d(P) = \frac{1}{\Psi_d(br^m s^m)} \Psi_d\big(ah + b\Phi_1 \cdot (rx - h_1) + b\Phi_2 \cdot (sz - h_3)\big).$$

Com isso, $\Psi_d(P)$ pertence ao ideal de $\mathbb{Q}[x, y, z]$ gerado por $\Psi_d(h), \Psi_d(rx - h_1)$ e $\Psi_d(sz - h_3)$. Sendo P um menor arbitrário de (2.32), segue-se que

$$\mathcal{S}(\theta_{u,\tilde{\Psi}_d(H)}) = (\Psi_d(P_1), \ldots, \Psi_d(P_6)) \subset \big(\Psi_d(h), \Psi_d(rx - h_1), \Psi_d(sz - h_3)\big),$$

para todo $d \in \mathbb{Z}^l \setminus B$. O que conclui a demonstração do lema. ∎

Se H satisfaz as condições do lema anterior e $d \in \mathbb{Z}^l \setminus B$, então podemos explicitar a base $\mathbb{Z}$-reduzida de $\mathcal{S}(\theta_{u,\tilde{\Psi}_d(H)})$. De fato, pelo lema,

$$\mathcal{G}_0 = \{\Psi_d(h), r(d)x - \Psi_d(h_1), s(d)z - \Psi_d(h_3)\}$$

gera o ideal $\mathcal{S}(\theta_{u,\tilde{\Psi}_d(H)})$. Como $\Psi_d(h), \Psi_d(h_1)$ e $\Psi_d(h_3)$ são polinômios apenas em y, então $\mathcal{G}_0$ é uma base de Gröbner, em que

$$\deg \Psi_d(h_1) \le \deg h_1 < \deg h = \deg \Psi_d(h) \quad \text{e} \quad \deg \Psi_d(h_3) < \deg \Psi_d(h).$$

No entanto, $\mathcal{G}_0$ não é necessariamente $\mathbb{Z}$-reduzida, porque os polinômios podem não ter conteúdos iguais a 1. Assim, denotando os conteúdos por:

$$c = \mathrm{cont}\big(\Psi_d(h)\big), \quad c_1 = \mathrm{cont}\big(r(d)x - \Psi_d(h_1)\big) \quad \text{e} \quad c_3 = \mathrm{cont}\big(s(d)z - \Psi_d(h_3)\big),$$

e definindo $f = \Psi_d(h)/c$, $f_1 = \Psi_d(h_1)/c_1$ e $f_3 = \Psi_d(h_3)/c_3$, temos que

$$\mathcal{G}_{\tilde{\Psi}_d(H)} = \{f, nx - f_1, mz - f_3\} \tag{2.36}$$

é a base $\mathbb{Z}$-reduzida de $\mathcal{S}(\theta_{u,\tilde{\Psi}_d(H)})$, em que $n = r(d)/c_1$ e $m = s(d)/c_3$.

Para o próximo teorema, usaremos a seguinte notação: se $d_0 = (d_1, \ldots, d_l) \in \mathbb{Z}^l$ e $q \in \mathbb{N}$ é um número primo, então

$$d_0 + q\mathbb{Z}^l = \{(d_1 + qn_1, \ldots, d_l + qn_l) : n_1, \ldots, n_l \in \mathbb{Z}\}.$$

Além disso, se $d \in d_0 + q\mathbb{Z}^l$, então escreveremos $d \equiv d_0 \mod q$.

Teorema 2.5.2 *Seja $H \in \mathbb{Z}[\mathbf{t}][u, x, y, z]$ um polinômio homogêneo em u, x, y, z de grau k igual a 3 ou 4, tal que M_H admite uma base $\mathcal{G} = \{h, rx - h_1, sz - h_3\}$ como em* (2.33)*, de forma que $\mathcal{G} \subset L_H$. Se $d_0 \in \mathbb{Z}^l$ é tal que*

1. *q não divide $r(d_0) \cdot s(d_0) \cdot \Psi_{d_0}(lc(h))$;*

2. *$\tilde{\Psi}_{d_0}(H)$ é q-mínimo.*

Então,

$$\mathcal{F} = \{\mathcal{Z}\big(\tilde{\Psi}_d(H)\big) : d \in (d_0 + q\mathbb{Z}^l) \text{ com } \mathcal{Z}\big(\tilde{\Psi}_d(H)\big) \text{ não singular e } \operatorname{Sing}(\rho_{\tilde{\Psi}_d(H)}) \text{ finito}\}$$

é uma família de variedades involutivas mínimas.

Demonstração. Tome $F = \tilde{\Psi}_{d_0}(H)$ e seja $n \in \mathbb{Z}^l$, tal que $\mathcal{Z}\big(\tilde{\Psi}_{d_0+qn}(H)\big) \in \mathcal{F}$. Denote $G = \tilde{\Psi}_{d_0+qn}(H)$. De acordo com o corolário 2.4.3, para mostrarmos que $\mathcal{Z}(G)$ é involutiva mínima, basta provarmos que $F \sim_q G$, pois, por hipótese, F é q-mínimo. Como o polinômio $rs \cdot lc(h)$ avaliado em d_0 é congruente módulo q a $rs \cdot lc(h)$ avaliado em $d_0 + qn$, temos, pela hipótese (1) do teorema, que $d_0, d_0 + qn \notin \mathcal{Z}\big(rs \cdot lc(h)\big)$. Portanto, pelo lema 2.5.1,

$$\begin{aligned}
\mathcal{S}(\theta_{u,F}) &= \big(\Psi_{d_0}(h), r(d_0)x - \Psi_{d_0}(h_1), s(d_0)z - \Psi_{d_0}(h_3)\big) \text{ e} \\
\mathcal{S}(\theta_{u,G}) &= \big(\Psi_{d_0+qn}(h), r(d_0+qn)x - \Psi_{d_0+qn}(h_1), s(d_0+qn)z - \Psi_{d_0+qn}(h_3)\big).
\end{aligned}$$

E, como visto em (2.36), dividindo cada gerador pelo seu conteúdo, obtemos as bases $\mathbb{Z}$-reduzidas

$$\mathcal{G}_F = \{f, n_F x - f_1, m_F z - f_3\} \quad \text{e} \quad \mathcal{G}_G = \{g, n_G x - g_1, m_G z - g_3\} \tag{2.37}$$

de $S(\theta_{u,F})$ e $S(\theta_{u,G})$, respectivamente. Verificaremos, agora, cada uma das condições para termos $F \sim_q G$. Comecemos mostrando que G é q-compatível. Sendo $\mathcal{Z}(G)$ um membro de $\mathcal{F}$, temos que $\mathcal{Z}(G)$ é não singular e $\operatorname{Sing}(\rho_G)$ é finito. Seja, agora, $\pi : \mathbb{Z}_{\mathfrak{q}}[y] \to \mathbb{F}_q[y]$ como em (2.29). Sendo $\Psi_{d_0+qn}(h)$ da forma $\Psi_{d_0}(h) + qR$, para algum $R \in \mathbb{Z}[x, y, z]$, temos que

$$\pi\big(\Psi_{d_0+qn}(h)\big) = \pi\big(\Psi_{d_0}(h)\big). \tag{2.38}$$

Além disso, por hipótese, q não divide $\Psi_{d_0}(\operatorname{lc}(h))$. Logo, $\pi(\Psi_{d_0}(h)) \neq 0$ e, por (2.38), q não divide o conteúdo de $\Psi_{d_0+qn}(h)$. Assim, $\operatorname{cont}\big(\Psi_{d_0}(h)\big)$ e $\operatorname{cont}\big(\Psi_{d_0+qn}(h)\big)$ têm inversos em $\mathbb{Z}_{\mathfrak{q}}$ e

$$\pi(f) = \pi\left(\frac{\Psi_{d_0}(h)}{\operatorname{cont}\big(\Psi_{d_0}(h)\big)}\right) = \pi\left(\frac{\Psi_{d_0+qn}(h)}{\operatorname{cont}\big(\Psi_{d_0}(h)\big)}\right) = \pi(g)\cdot\pi\left(\frac{\operatorname{cont}\big(\Psi_{d_0+qn}(h)\big)}{\operatorname{cont}\big(\Psi_{d_0}(h)\big)}\right).$$

Dessa forma, $\pi(f)$ é associado à $\pi(g)$. Além disso, como $f = \Psi_{d_0}(h)/\operatorname{cont}\big(\Psi_{d_0}(h)\big)$, temos que q não divide $\operatorname{lc}(f)$. Logo, $\deg(\pi(f)) = \deg(f)$. Portanto,

$$\deg(g) \geq \deg(\pi(g)) = \deg(\pi(f)) = \deg(f) = m(k).$$

Por outro lado, como $\mathcal{G}_G$ gera $\mathcal{S}(\theta_{u,G})$, podemos aplicar a proposição 2.2.6 e concluir que $\deg(g) \leq m(k)$. Logo, $\deg(g) = \deg(\pi(g)) = m(k)$ e q não divide $\operatorname{lc}(g)$. Agora, como F é q-mínimo e $\pi(f)$ é associado à $\pi(g)$, temos que $\pi(g)$ é irredutível. Assim, $\deg(g) = \deg(\pi(g))$ nos diz que g é irredutível em $\mathbb{Z}_{\mathfrak{q}}[y]$. Portanto, g é irredutível em $\mathbb{Q}[y]$. Com isso, verificamos as condições: g é irredutível de grau $m(k)$ e q não divide $\operatorname{lc}(g)$.

Veremos agora que q não divide $n_G \cdot m_G$. Por hipótese, q não divide $r(d_0) \cdot s(d_0)$. Contudo, $r(d_0) \equiv r(d_0 + qn) \bmod q$ e $s(d_0) \equiv s(d_0 + qn) \bmod q$. Logo, q não divide

$r(d_0+qn)\cdot s(d_0+qn)$. Como n_G e m_G são divisores de $r(d_0+qn)$ e $s(d_0+qn)$, respectivamente, segue-se que q não divide $n_G \cdot m_G$. E isto conclui a verificação de que G é q-compatível.

Quanto à q-equivalência entre F e G, já vimos que $\pi(f)$ e $\pi(g)$ são associados. Agora, como $\tilde{\Psi}_{d_0+qn}(H) = \tilde{\Psi}_{d_0}(H) + qP$ para algum $P \in \mathbb{Z}[u,x,y,z]$, então $G \equiv F \mod q$. Além disso, $\deg\big(\tilde{\Psi}_{d_0}(H)\big) = \deg H$ ou $\tilde{\Psi}_{d_0}(H) = 0$. Se $F = \tilde{\Psi}_{d_0}(H) = 0$, então $h_F = 0$ e $\mathrm{Sing}(\rho_F) = \mathbb{P}^3$ não é finito. Mas isto contradiz o fato de F ser q-mínimo. Assim, $\deg F = \deg H$. Da mesma forma, sendo $\mathrm{Sing}(\rho_G)$ finito, temos que $\deg G = \deg H$. Portanto,

$$\deg F = \deg G, \text{ com } G \equiv F \mod q.$$

Resta mostrar apenas que $\pi(f_1/n_F) = \pi(g_1/n_G)$ e $\pi(f_3/m_F) = \pi(g_3/m_G)$. Pelas construções de f_1 e n_F, se $c_1 = \mathrm{cont}\big(r(d_0)x - \Psi_{d_0}(h_1)\big)$, então $f_1 = \Psi_{d_0}(h_1)/c_1$ e $n_F = r(d_0)/c_1$. Logo,

$$f_1/n_F = \Psi_{d_0}(h_1)/r(d_0).$$

E, de forma semelhante, $g_1/n_G = \Psi_{d_0+qn}(h_1)/r(d_0+qn)$. Assim, usando as congruências $\Psi_{d_0}(h_1) \equiv \Psi_{d_0+qn}(h_1) \mod q$ e $r(d_0) \equiv r(d_0+qn) \not\equiv 0 \mod q$, temos que

$$\pi\left(\frac{f_1}{n_F}\right) = \pi\left(\frac{\Psi_{d_0}(h_1)}{r(d_0)}\right) = \pi\left(\frac{\Psi_{d_0+qn}(h_1)}{r(d_0+qn)}\right) = \pi\left(\frac{g_1}{n_G}\right).$$

De forma análoga, de $\pi\big(\Psi_{d_0}(h_3)\big) = \pi\big(\Psi_{d_0+qn}(h_3)\big)$ e $\pi\big(s(d_0)\big) = \pi\big(s(d_0+qn)\big)$, concluímos que $\pi(f_3/m_F) = \pi(g_3/m_G)$. Com isso, $F \sim_q G$ e, por 2.4.3, $\mathcal{Z}(G)$ é involutiva mínima. ■

No caso de uma família de variedades mínimas de grau igual a 4, o cálculo direto da base $\mathcal{G}$ de M_H, tal que $\mathcal{G} \subset L_H$, mostrou-se inviável na prática. Por isto, precisamos da próxima proposição que, através do cálculo de uma base para L_H em $\mathbb{Q}[t,x,y,z]$, nos dá uma forma indireta de obtermos $\mathcal{G}$ satisfazendo as condições do teorema 2.5.2.

Proposição 2.5.3 *Seja $H \in \mathbb{Z}[\mathbf{t}][u,x,y,z]$ um polinômio homogêneo em u,x,y,z. Se existem $h, h_3 \in \mathbb{Z}[\mathbf{t},y], h_1 \in \mathbb{Z}[\mathbf{t},y,z]$ e $0 \neq r, s \in \mathbb{Z}[\mathbf{t}]$, tais que*

$$\{h, rx - h_1, sz - h_3\} \subset L_H,$$

em que h é irredutível em $\mathbb{Q}(\mathbf{t})[y]$, então M_H admite uma base de Gröbner $\mathcal{G} = \{h, r'x - h'_1, s'z - h'_3\}$ como em (2.33), de forma que $\mathcal{G} \subset L_H$. Além disso, r' e s' podem ser tomados nas formas $r' = lc(h)^j s^m r$ e $s' = lc(h)^i s$, com $i, j, m \in \mathbb{N}$.

Demonstração. Seja m o grau de h_1 como polinômio em z. Substituindo sz por h_3 em $s^m(rx - h_1)$, temos um polinômio da forma $\tilde{r}x - \tilde{h}_1 \in L_H$, em que $\tilde{r} = s^m r$ e $\tilde{h}_1$ depende apenas de $\mathbf{t}$ e y. Nosso primeiro passo será mostrar que

$$M_H = (h, \tilde{r}x - \tilde{h}_1, sz - h_3).$$

Seja $P(x,y,z) \in M_H$. Defina $\tilde{P}$ como o polinômio obtido, a partir de P, substituindo-se x e z por $\tilde{h}_1/\tilde{r}$ e h_3/s, respectivamente. Em $\mathbb{Q}(\mathbf{t})[x,y,z]$, temos que o ideal gerado por $\{h, \tilde{r}x - \tilde{h}_1, sz - h_3, P\}$ é igual ao ideal gerado por $\{h, \tilde{r}x - \tilde{h}_1, sz - h_3, \tilde{P}\}$. Por outro lado, $\tilde{P} \in \mathbb{Q}(\mathbf{t})[y] \cap M_H$ que é gerado por h, pois $\mathbb{Q}(\mathbf{t})[y]$ é domínio de ideais principais e $h \in \mathbb{Q}(\mathbf{t})[y] \cap M_H$ é irredutível. Portanto, $P \in (h, \tilde{r}x - \tilde{h}_1, sz - h_3)$ e $M_H = (h, \tilde{r}x - \tilde{h}_1, sz - h_3)$.

Resta mostrar que é possível obter h'_1 e h'_3 de forma que os graus sejam menores que $\deg h$ como polinômios em y. Se $\deg h_3 \geq \deg h$, então tomando $\tilde{h}_3$ o resto da divisão, em $\mathbb{Q}[\mathbf{t}][y]$, de $\mathrm{lc}(h) \cdot h_3$ por h, temos que $M_H = (h, \tilde{r}x - \tilde{h}_1, \mathrm{lc}(h) \cdot sz - \tilde{h}_3)$, com a vantagem de $\mathrm{lc}(h) \cdot sz - \tilde{h}_3$ ainda pertencer a L_H e $\deg \tilde{h}_3 < \deg h_3$. Repetindo o processo um número suficiente de vezes, obtemos que $M_H = (h, \tilde{r}x - \tilde{h}_1, s'z - h'_3)$, em que $s' = \mathrm{lc}(h)^i \cdot s$, para algum $i \in \mathbb{N}$, $s'z - h'_3 \in L_H$ e $\deg h'_3 < \deg h$. Aplicando a mesma estratégia no caso de $\deg \tilde{h}_1 \geq \deg h$, obtemos $\mathcal{G} = (h, r'x - h'_1, s'z - h'_3) \subset L_H$ satisfazendo as condições em (2.33), em que $r' = \mathrm{lc}(h)^j s^m r$, para algum $j \in \mathbb{N}$. ■

Para podermos usar a proposição acima, precisamos manter o controle sobre os zeros de r' e s'. Além disso, também é necessário saber se q divide $\Psi_d\big(r's' \cdot \mathrm{lc}(h)\big)$.

Esse controle é garantido, de maneira imediata, pela forma como r' e s' foram construídos.

Corolário 2.5.4 *Nas condições da proposição anterior,*

$$\mathcal{Z}\big(r's' \cdot lc(h)\big) = \mathcal{Z}\big(rs \cdot lc(h)\big).$$

Além disso, se q é um número primo e $d \in \mathbb{Z}^l$, então q divide $\Psi_d\big(r's' \cdot lc(h)\big)$ se, e somente se, q divide $\Psi_d\big(rs \cdot lc(h)\big)$.

Demonstração. Como r' e s' são produtos de r,s, e $\mathrm{lc}(h)$, então os conjuntos dos zeros são iguais. Além disso, para provar a equivalência: "q divide $\Psi_d\big(r's' \cdot \mathrm{lc}(h)\big)$ se, e somente se, q divide $\Psi_d\big(rs \cdot \mathrm{lc}(h)\big)$", basta usar a primalidade de q. ■

2.6 Exemplos

A partir do teorema 2.5.2, podemos exibir um teste para determinar famílias de variedades involutivas mínimas.

Entrada: $H \in \mathbb{Z}[\mathbf{t}][u, x, y, z]$ um polinômio homogêneo em u, x, y, z de grau 3 ou 4, q um número primo e $d_0 \in \mathbb{Z}^l$.

Saída: Uma mensagem de erro ou uma família de variedades involutivas mínimas.

Passo 1: Calcular uma base de Gröbner de L_H, com respeito à ordem lexicográfica para a qual $x > z > y > t$, e verificar se existem geradores $h, rx - h_1, sz - h_3$ satisfazendo as condições da proposição 2.5.3. Caso não existam, imprima

"$\mathcal{G}$ não é da forma correta."

e pare.

Passo 2: Tomar $F := \tilde{\Psi}_{d_0}(H)$, calcular $\mathcal{G}_F = \{f, nx - f_1, mz - f_3\}$ a base $\mathbb{Z}$-reduzida de $\mathcal{S}(\theta_{u,F})$ e verificar se:

1. $\mathcal{Z}(F)$ é não singular;

2. $\mathrm{Sing}(\rho_F)$ é finito;

3. f tem grau $m(k)$ e é irredutível;

4. q não divide $r(d_0) \cdot s(d_0) \cdot \Psi_{d_0}(\mathrm{lc}(h))$.

Caso não sejam satisfeitas as 4 condições, imprima

"$\tilde{\Psi}_{d_0}(H)$ pode não ser q-compatível."

e pare.

Passo 3: Seguindo o algoritmo no passo 1 da demonstração de 2.3.3, construir μ_F e η_F.

Passo 4: Sendo f calculado no passo 3, verificar se

1. $\pi(f)$ é irredutível em $\mathbb{F}_q[y]$;

2. $\pi(\eta_F) \not\equiv 0 \mod (\pi(f))$;

3. $T^2 - \overline{\pi(\mu_F)}$ é irredutível em $\dfrac{\mathbb{F}_q[y]}{(\pi(f))}[T]$.

Caso não sejam satisfeitas as 3 condições, imprima

"$\tilde{\Psi}_d(H)$ não é q-mínimo."

e pare.

Passo 5: Determinar elementos $d \in d_0 + q\mathbb{Z}^l$, de forma que $\mathcal{Z}\big(\tilde{\Psi}_d(H)\big)$ é não singular e $\mathrm{Sing}(\rho_{\tilde{\Psi}_d(H)}) \subset D_+(u)$. $\square$

O passo 1, com o auxílio da proposição 2.5.3, permite verificar se existe uma base $\mathcal{G} = \{h, rx - h_1, sz - h_3\}$ satisfazendo as condições iniciais do teorema 2.5.2. O passo 2 permite verificar a condição (1) do mesmo teorema e se $\tilde{\Psi}_{d_0}(H)$ é q-compatível. Note que, se $\mathcal{G}_F = \{f, nx - f_1, mz - f_3\}$ é a base calculada no passo 2, então não é necessário verificar se q divide $\mathrm{lc}(f) \cdot n \cdot m$. De fato, de acordo com a demonstração do teorema 2.5.2, $\{\Psi_{d_0}(h), r(d_0)x - \Psi_{d_0}(h_1), s(d_0)z - \Psi_{d_0}(h_3)\}$ é uma base de $\mathcal{S}(\theta_{u,F})$. Assim, dividindo cada gerador pelo seu conteúdo, obtemos a base $\mathbb{Z}$-reduzida de $\mathcal{S}(\theta_{u,F})$, que é justamente $\mathcal{G}_F$. Em particular, $\mathrm{lc}(f) \cdot n \cdot m$ divide $\Psi_{d_0}(\mathrm{lc}(h)) \cdot r(d_0) \cdot s(d_0)$. Com isso, se o item 4 do passo 2 se verifica, então q não divide $\mathrm{lc}(f) \cdot n \cdot m$.

Quanto aos passos 3 e 4, eles nos dizem se $\tilde{\Psi}_{d_0}(H)$ é q-mínimo. No passo 3, devemos tomar o cuidado de usar $\tilde{f}_1 = f_1/n$ e $\tilde{f}_3 = f_3/m$ no cálculo de η_F e μ_F, pois, na demonstração de 2.3.3, os polinômios na base de $\mathcal{S}(\theta_{u,F})$, usados para a construção de η_F e μ_F, têm os coeficientes de x e z iguais a 1. No passo 5, a princípio deveríamos verificar se $\mathrm{Sing}(\rho_{\tilde{\Psi}_d(H)})$ é finito. Mas, em vista da observação 2.6.1 abaixo, é suficiente verificarmos se $\mathrm{Sing}(\rho_{\tilde{\Psi}_d(H)}) \subset D_+(u)$.

Observação 2.6.1 Seja F q-compatível. Por definição, $\mathrm{Sing}(\rho_F)$ é finito. Como $\mathcal{S}(\theta_u)$ admite uma base da forma (2.28), em que f é irredutível de grau $m(k)$, então $\mathrm{Sing}(\theta_u)$ contém $m(k)$ pontos e, por (2.5), $\mathrm{Sing}(\rho_F) \subset D_+(u)$. Reciprocamente, se F é tal que $\mathrm{Sing}(\rho_F) \subset D_+(u)$, com $\mathcal{S}(\theta_u) = (f, nx - f_1, mz - f_3)$, em que $f, f_1, f_3 \in \mathbb{Z}[y]$, então os pontos de $\mathrm{Sing}(\rho_F)$ estão em bijeção com os zeros de f, em particular, $\mathrm{Sing}(\rho_F)$ é finito.

Exemplo 2.6.2 Sejam $H = y^3 + u^2x + 2x^2u + tz^3$, $q = 7$ e $d_0 = 3$. Usando o Singular, obtemos:

$$\mathcal{G} = \{h, 4x + 3zy^2 + 1, (1024t^3 + 2t^2)z - h_3\} \subset L_H,$$

em que $h = 27y^{15} + (128t^2 + 2t)y^6 - 32t^2y^3 + 2t^2$, e h_3 é dado por:

$$(6912t - 27)y^{13} + 864ty^{10} + 36ty^7 + (32768t^3 - 384t^2 - 2t)y^4 + (-4096t^3 + 64t^2)y.$$

Pelo Singular, h é irredutível em $\mathbb{Q}(\mathbf{t})[y]$. Assim as condições do passo 1 estão verificadas, em que $r(t) = 4$ e $s(t) = 1024t^3 + 2t^2$. Para o passo 2, tomando

$F = \tilde{\Psi}_3(H)$ e calculando a base $\mathbb{Z}$-reduzida do ideal das singularidades de $\theta_{u,F}$, obtemos:

$$\mathcal{S}(\theta_u) = \big(9y^{15} + 386y^6 - 96y^3 + 6, 3074x - f_1, 9222z - f_3\big),$$

em que $f_1 = -216y^{12} - 9y^9 + 576y^6 - 9240y^3 + 382$ e

$$f_3 = 6903y^{13} + 864y^{10} + 36y^7 + 293758y^4 - 36672y.$$

Pelo critério de Eisenstein, para o primo $p = 2$, $f = 9y^{15} + 386y^6 - 96y^3 + 6$ é irredutível e verificamos o item 3 deste passo. Quanto ao item 4, basta observar que $r(3) \cdot s(3) \cdot \Psi_3(\mathrm{lc}(h)) \equiv 4 \cdot (1024 \cdot 27 + 2 \cdot 9) \cdot 27 \equiv 6 \mod 7$. Ainda no passo 2, resta mostrar que $\mathcal{Z}(F)$ é não singular e $\mathrm{Sing}(\rho_F)$ é finito. Preferimos verificar estas duas condições para todos os membros da família $\{\tilde{\Psi}_{3+qn}(H) : n \in \mathbb{Z}\}$, pois isto será útil no passo 5. Mas isto já foi demonstrado nas duas afirmações contidas no exemplo 2.3.6. Ainda neste exemplo, obtivemos que:

$$\eta_F \equiv (81540y^{13} + 10314y^{10} + 3888y^7 + 3538821y^4 - 437772y)/1537 \mod (f) \text{ e}$$
$$\mu_F \equiv (-81540y^{13} - 10314y^{10} - 3888y^7 - 3524988y^4 + 437772y)/1537 \mod (f).$$

Note que já exibimos η_F e μ_F reduzidos por (f), pois estamos interessados em suas imagens em $\mathbb{F}_7[y]/(\pi(f))$. Para o passo 4, construindo o anel $\mathbb{F}_7[y]$ no Singular e fatorando $\pi(f) = 2y^{15} + y^6 + 2y^3 - 1$, temos como resultado que $\pi(f)$ é irredutível. Além disso, calculando a redução de $\pi(\eta_F)$ temos:

$$\pi(\eta_F) \equiv y^{13} - y^{10} - y^7 - 2y^4 + 2y \mod (\pi(f)).$$

Finalmente, construindo o corpo $\mathbb{L} = \mathbb{F}_7[y]/(\pi(f))$ e fatorando $T^2 - \overline{\pi(\mu_F)}$ em $\mathbb{L}[T]$, temos também como resultado que $T^2 - \overline{\pi(\mu_F)}$ é irredutível. Para o último passo, lembre-se que já verificamos que as duas condições exigidas são satisfeitas para todo $d \in 3 + 7\mathbb{Z}$. Dessa forma,

$$\mathcal{F} = \{\mathcal{Z}(F_n) : n \in \mathbb{Z}, F_n = y^3 + u^2x + 2x^2u + (3 + 7n)z^3\}$$

é uma família de variedades involutivas mínimas. $\square$

Note que o cálculo de $\mathcal{G}$ independe de q e de d_0. Assim, o exemplo acima pode ser estendido observando-se o seguinte: sejam q primo e $d_0 \in \mathbb{Z} \setminus \{0\}$, tais que q não divide

$$27 \cdot 4 \cdot (1024 d_0^3 + 2 d_0^2),$$

ou de forma equivalente, que q não divide $3 \cdot 2 \cdot d_0 \cdot (512 d_0 + 1)$. Pelo lema 2.5.1, $F_{q,d_0} := y^3 + u^2 x + 2x^2 u + d_0 z^3$ é tal que $\mathcal{S}(\theta_{u,F_{q,d_0}})$ tem base $\mathbb{Z}$-reduzida da forma $\{f, nx - f_1, mz - f_3\}$ com q não dividindo $\mathrm{lc}(f) \cdot n \cdot m$. Pelas duas afirmações do exemplo 2.3.6, temos que $\mathcal{Z}(F_{q,d_0})$ é não singular e $\rho_{F_{q,d_0}}$ admite apenas um número finito de singularidades. Assim, para provar que F_{q,d_0} é q-mínimo, basta verificar se f é irredutível de grau 15 e executar os passos 3 e 4 do teste acima. Verificando tais condições, temos, na tabela abaixo, pares (q, d_0) satisfazendo as exigências.

q	7	13	19	31	37	43	61	67	73	79	97
d_0	3	4	15	11	24	24	29	5	3	7	4

Portanto, para cada par acima, concluímos, por 2.5.2, que

$$\mathcal{F}_{q,d_0} = \{\mathcal{Z}(F_n) : n \in \mathbb{Z}, F_n = y^3 + u^2 x + 2x^2 u + (d_0 + qn) z^3\}$$

é uma família de variedades involutivas mínimas. Note que o único caso em que não provamos que $\tilde{\Psi}_d(H)$ é não singular e seu campo de retas admite apenas um número finito de singularidades, foi o caso $d = 0$. Mas este caso não é relevante, pois $0 \notin d_0 + q\mathbb{Z}$, qualquer que seja (q, d_0) na tabela acima.

Exemplo 2.6.3 Sejam $H = y^4 + u^3 x + 2x^3 u + tz^4 + x^2 y^2 + u^3 y$, $q = 61$ e $d_0 = 3$. Usando o Singular, obtemos que L_H é gerado por uma base de Gröbner com seis elementos, entre os quais podemos escolher três que são da forma $h, rx - h_1, sz - h_3$ satisfazendo as condições da proposição 2.5.3. Não escreveremos explicitamente tais polinômios, pois seria de pouca valia, já que possuem uma grande quantidade de termos[1]. No entanto, podemos destacar que $r = 1875965850$ e $s = 185315271772840448 \cdot t \cdot w$, em que w é um polinômio irredutível em $\mathbb{Z}[t]$ de grau 74. Além disso,

$$h = 65536(t-16)^2 y^{40} + \text{ (termos de menor grau em } y)$$

é irredutível em $\mathbb{Q}(t)[y]$, de grau $m(4) = 40$.

Para o passo 2, com $F = \tilde{\Psi}_3(H)$, calculamos $\mathcal{G}_F = \{f, nx - f_1, mz - f_3\}$ e verificamos computacionalmente que $r(3) \cdot s(3) \cdot \Psi_3(\mathrm{lc}(h))$ não é divisível por q e que f é irredutível de grau $m(4) = 40$. Quanto a F ser não singular e $\mathrm{Sing}(\rho_F)$ ser finito, faremos, como no exemplo anterior, uma demonstração mais geral, pois será útil no passo 5.

Afirmação 1 Se $d \neq 0$, então $\tilde{\Psi}_d(H)$ é não singular.

Demonstração da afirmação. Seja I o ideal de $\mathbb{Q}[t][u, x, y, z]$ gerado por H e por suas derivadas parciais. Calculando a base de Gröbner para I, temos que

$$y^7 \in I. \tag{2.39}$$

Além disso, denotando $G = \tilde{\Psi}_d(H)$, temos que o ideal das singularidades de G é $\tilde{\Psi}_d(I)$, pois $\tilde{\Psi}_d(\partial_u H) = \partial_u G$ e valem igualdades semelhantes para x, y e z. Assim, se $p = [u_0 : x_0 : y_0 : z_0]$ é uma singularidade de G, então, por (2.39), $y_0 = 0$. Portanto, de $0 = \partial_y G(p) = 4y_0^3 + 2x_0^2 y_0 + u_0^3$, temos que $u_0 = 0$. Consequentemente, $0 = \partial_u G(p) = 3u_0^2 x_0 + 2x_0^3 + 3u_0^2 y_0$ nos diz que $x_0 = 0$. Por fim, de $0 = \partial_z G(p) = 4dz_0^3$, segue-se que $z_0 = 0$, o que é um absurdo. Com isso, $\tilde{\Psi}_d(H)$ é não singular, para todo $d \neq 0$.

Afirmação 2 Se $d \neq 0, 16$, então $\mathrm{Sing}(\rho_{\tilde{\Psi}_d(H)})$ é finito.

Demonstração da afirmação. Pelo lema 2.5.1,

$$\mathcal{S}(\theta_{u,\tilde{\Psi}_d(H)}) = \big(\Psi_d(h), \Psi_d(r'x - h'_1), \Psi_d(s'z - h'_3)\big),$$

[1]O programa para o cálculo de $h, rx - h_1, sz - h_3$ e os próprios polinômios podem ser obtidos no endereço eletrônico `www.dcc.ufrj.br/~collier/Folia.html`.

em que r', s', h'_1 e h'_3 são obtidos através da proposição 2.5.3. Assim, para mostrarmos que $\mathrm{Sing}(\rho_{\tilde{\Psi}_d(H)})$ é finito, é suficiente que tenhamos $\mathrm{Sing}(\rho_{\tilde{\Psi}_d(H)}) \subset D_+(u)$. Denote $\tilde{\Psi}_d(H)$ por G e suponha, por absurdo, que $p = [0 : x_0 : y_0 : z_0]$ é uma singularidade de ρ_G. Tomando J como sendo o ideal gerado pelos menores da matriz

$$\begin{bmatrix} \frac{\partial G}{\partial y} & \frac{\partial G}{\partial z} & -\frac{\partial G}{\partial u} & -\frac{\partial G}{\partial x} \\ 0 & x & y & z \end{bmatrix}_{|u=0},$$

temos, usando o Singular, que $y^8(d-16) \in J$. Contudo, os zeros de J são justamente os pontos singulares de ρ_G contidos no complementar de $D_+(u)$. Logo, $p \in \mathcal{Z}(J)$ e $y_0 = 0$, pois $d \neq 16$. Sendo o hamiltoniano de G em $\check{p} = (0, x_0, y_0, z_0)$ proporcional a $E(\check{p})$, segue-se que $0 = -\partial_u G(\check{p}) = 2x_0^3$ e temos $x_0 = 0$. Consequentemente, $0 = \partial_z G(\check{p}) = 4dz_0^3$ e $z_0 = 0$, que é uma contradição, o que prova a afirmação.

Para os passos 3 e 4, calculamos uma base de Gröbner para o ideal das singularidades do campo associado a $F = \tilde{\Psi}_{d_0}(H)$ e, de acordo com a demonstração da proposição 2.3.3 em seu passo 1, construímos μ_F e η_F. Da mesma forma que no exemplo anterior, efetuando as fatorações sobre $\mathbb{F}_{61}$ e $\mathbb{L} = \mathbb{F}_{61}[y]/\big(\pi(f)\big)$ dos respectivos polinômios, temos que as exigências do passo 4 são cumpridas.

Para o passo 5, usando as afirmações 1 e 2 acima, temos que se $d \neq 0, 16$, então $\tilde{\Psi}_d(H)$ é não singular e $\mathrm{Sing}(\rho_{\tilde{\Psi}_d(H)})$ é finito. Como $0, 16 \notin 3 + 61\mathbb{Z}$, segue-se que

$$\mathcal{F} = \{\mathcal{Z}(F_n) : n \in \mathbb{Z}, F_n = y^4 + u^3x + 2x^3u + (3 + 61n)z^4 + x^2y^2 + u^3y\}$$

é uma família de variedades involutivas mínimas. □

Como no exemplo de grau 3, podemos estender o exemplo acima para os casos em que $0, 16 \neq d_0$ e q satisfazem:

1. q não divide $r(d_0) \cdot s(d_0) \cdot \mathrm{lc}\big(\Psi_{d_0}(h)\big)$;

2. $\tilde{\Psi}_{d_0}(H)$ é q-mínimo.

Assim, efetuando a busca para $0 < q < 100$, obtemos que

$$\mathcal{F}_{q,d_0} = \{\mathcal{Z}(F_n) : n \in \mathbb{Z}, F_n = y^4 + u^3x + 2x^3u + (d_0 + qn)z^4 + x^2y^2 + u^3y\}$$

é uma família de variedades involutivas mínimas, para os pares (q, d_0) na tabela abaixo:

q	43	61	67	79	83	89
d_0	6	3	51	32	4	48

Exemplo 2.6.4 (**Múltiplos parâmetros**) Seja

$$H = t_1y^3 + t_2u^2x + t_3x^2u + t_4uz^2 + t_5xyz.$$

Calculando uma base de Gröbner para L_H, obtemos

$$\mathcal{G} = \{h, t_2x + 2t_1y^3, (729t_1^4t_2^7t_4^3 - 2t_2^5t_4^2t_5^7)z - h_3\} \subset L_H,$$

em que $h_3 \in \mathbb{Q}[y]$ com $\deg h_3 = 14$ e

$$h = 16t_1^5t_3t_5^2y^{15} - 16t_1^4t_2^2t_5^2y^{12} + 4t_1^3t_2^2t_5^3y^{11} - 16t_1^3t_2^2t_3t_4t_5y^9 + 9t_1^3t_2^4t_4y^7 \\ + 4t_1^2t_2^4t_4t_5y^6 - t_1t_2^4t_4t_5^2y^5 + 4t_1t_2^4t_3t_4^2y^3 - t_2^6t_4^2$$

é irredutível em $\mathbb{Q}(t_1, \ldots, t_5)[y]$. Mantendo a notação já estabelecida, temos que $s = 729t_1^4t_2^7t_4^3 - 2t_2^5t_4^2t_5^7$ e $r = t_2$ e $\mathrm{lc}(h) = 16t_1^5t_3t_5^2$. Agora, tomando $q = 101$ e $d_0 = (1, 5, 1, 1, 1)$, segue-se que $\Psi_{d_0}(r \cdot s \cdot \mathrm{lc}(h)) \equiv 16 \cdot 5 \cdot 45 \equiv 65 \mod 101$. Além disso, tomando

$$F := \tilde{\Psi}_{d_0}(H) = y^3 + 5u^2x + x^2u + uz^2 + xyz$$

e aplicando as rotinas dos passos 3 e 4 do algoritmo da página 63, concluímos que, se $\mathcal{Z}(F)$ é não singular e $\mathrm{Sing}(\rho_F)$ é finito, então F é q-mínimo. Como de costume, a verificação, desta duas últimas condições sobre F, será feita de forma mais geral por ser útil no passo 5 do algoritmo da página 63. Assim, para obtermos uma família de variedades mínimas, precisamos determinar para que parâmetros $d \in \mathbb{Z}^5$, o polinômio $G = \tilde{\Psi}_d(H)$ define uma variedade não singular em que $\mathrm{Sing}(\rho_G)$ é finito.

Afirmação 1. Seja $d = (d_1, d_2, d_3, d_4, d_5) \notin \mathcal{Z}(s)$, em que $d_1 d_2 d_3 d_4 d_5 \neq 0$. Se $G = \tilde{\Psi}_d(H)$, então $\mathrm{Sing}(\rho_G)$ é finito.

Demonstração da Afirmação. Note que $d \notin \mathcal{Z}(s \cdot t_2 \cdot t_1 t_3 t_5) = \mathcal{Z}\big(s \cdot r \cdot \mathrm{lc}(h)\big)$. Assim, o lema 2.5.1 e a proposição 2.5.3 nos dizem que as singularidades de ρ_G, contidas em $D_+(u)$, estão em bijeção com os zeros de $\Psi_d(h)$. Portanto, é suficiente mostrarmos que toda singularidade de ρ_G é afim. Seja, então, J o ideal de $\mathbb{Q}[t_1, \ldots, t_5][u, x, y, z]$ gerado por u e pelos menores da matriz

$$\begin{bmatrix} \frac{\partial H}{\partial y} & \frac{\partial H}{\partial z} & -\frac{\partial H}{\partial u} & -\frac{\partial H}{\partial x} \\ u & x & y & z \end{bmatrix}.$$

Calculando uma base de Gröbner para J, com respeito à ordem lexicográfica para a qual $u > x > z > y > t_1 > \ldots > t_5$, obtemos que

$$N = \left\{ t_1 y^3, t_4 t_5^2 z^4 - t_5^3 z^2 y^2 + 9 t_1^2 t_3 y^4, t_3 x^3 + t_4 x z^2 + t_5 x y^2 \right\} \subset J.$$

Agora, suponha por absurdo que $p = [0 : x_0 : y_0 : z_0] \in \mathrm{Sing}(\rho_G)$. Como $\tilde{\Psi}_d(J)$ é o ideal que define as singularidades de G no infinito ($u = 0$), temos que $\tilde{\Psi}_d(g)(p) = 0$, para todo $g \in N$. Sendo $d_1 \neq 0$, segue-se que $y_0 = 0$, pois $t_1 y^3 \in N$. Com isso, o segundo polinômio em N nos diz que $z_0 = 0$, pois $d_4 d_5^2 \neq 0$. Finalmente, $d_3 \neq 0$ implica, com o auxilio do terceiro polinômio em N, que $x_0 = 0$. Logo, $x_0 = y_0 = z_0 = 0$, que é um absurdo. Dessa forma, ρ_G não admite singularidade no infinito e a afirmação segue.

Afirmação 2. Sejam $b = 110592 t_1^3 t_3^5 t_4^3 - 3125 t_1 t_2^4 t_5^6$ e $G = \tilde{\Psi}_d(H)$, com $d \in \mathbb{Z}^5$. Se $d = (d_1, \ldots, d_5) \notin \mathcal{Z}(b)$ e $d_1 d_2 d_3 d_4 d_5 \neq 0$, então $\mathcal{Z}(G)$ é não singular.

Demonstração da Afirmação. Seja I o ideal de $\mathbb{Q}[t_1, \ldots, t_5][u, x, y, z]$ gerado pelas derivadas parciais de H em relação a u, x, y e z. Calculando uma base de Gröbner para I, obtemos que

$$T = \{by^5, t_4^2t_5^2z^5 + \big(9t_1^2t_3t_4z - 9t_1^2t_2t_5y\big)y^4, 3t_3^2x^3 + 3t_3t_4xz^2 - 5t_2t_5xzy,$$
$$t_2u^2 + 2t_3ux + t_5zy\} \subset I.$$

Agora, suponha, por absurdo, que $p = [u_0 : x_0 : y_0 : z_0]$ é um ponto singular de $\mathcal{Z}(G)$. Como $\tilde{\Psi}_d(I)$ é o ideal que define as singularidades de $\mathcal{Z}(G)$, temos, da igualdade $\tilde{\Psi}_d(by^5)(p) = 0$, que $y_0 = 0$. Assim, $\tilde{\Psi}_d$ aplicado no segundo polinômio de T e calculado em p, nos diz que $d_4^2d_5^2z_0^5 = 0$. Como os d_i's são todos não nulos, segue-se que $z_0 = 0$. Aplicando a mesma estratégia para o terceiro polinômio em T, concluímos que $x_0 = 0$ e, de forma análoga, a partir do quarto polinômio em T, temos que $u_0 = 0$. Portanto, $u_0 = x_0 = y_0 = z_0 = 0$, o que não é possível. Dessa forma, $\mathcal{Z}(G)$ é não singular e provamos a afirmação.

Como último passo, mostraremos que $(d_0 + 101\mathbb{Z}^5) \cap \mathcal{Z}(b \cdot s \cdot t_1t_2t_3t_4t_5) = \emptyset$. Denote $g = b \cdot s \cdot t_1t_2t_3t_4t_5$ e suponha, por absurdo, que $d = d_0 + 101\xi \in \mathcal{Z}(g)$, com $\xi \in \mathbb{Z}^5$. Como $g(d) \equiv g(d_0) \bmod 101$, segue-se que 101 divide $g(d_0)$. Já sabemos que 101 não divide $s(d_0)$ e 101 não divide $1 \cdot 5 \cdot 1 \cdot 1 \cdot 1$. Portanto, 101 divide $b(d_0)$. Contudo, $b(d_0) \equiv 110592 - 3125 \cdot 5^4 \equiv 20 \bmod 101$. O que é uma contradição. Assim, de fato, $(d_0 + 101\mathbb{Z}^5) \cap \mathcal{Z}(b \cdot s \cdot t_1t_2t_3t_4t_5) = \emptyset$. Com isso, pelo algoritmo da página 63 e pelas afirmações acima, temos que

$$\mathcal{F} = \{\tilde{\Psi}_d(H) : d \in d_0 + 101\mathbb{Z}^5\}$$

é uma família de variedades involutivas mínimas. $\square$

Vale destacar que as famílias de exemplos anteriores são todas infinitas. No entanto, mesmo que apresentássemos enumeráveis famílias deste tipo, não esgotaríamos todas as variedades involutivas mínimas, de grau 3 ou 4, na medida em que sua quantidade é não enumerável; veja [15, Theorem 1, pg. 532].

Capítulo 3

Variedades Mínimas e Grupo de Picard

No capítulo anterior, vimos um critério que nos diz quando um polinômio de grau 3 ou 4 define uma variedade involutiva mínima. Neste capítulo, determinaremos um novo critério que aplicaremos a polinômios de grau maior ou igual a 5.

3.1 Grupo de Picard

Nesta seção, reuniremos alguns resultados envolvendo o grupo de Picard que serão úteis para a construção do critério de minimalidade exibido na próxima seção.

Proposição 3.1.1 *Sejam $X \subset \mathbb{P}^n$ uma variedade projetiva com anel de coordenadas homogêneas A e H um hiperplano de $\mathbb{P}^n$ que não contém X. Então A é um domínio de fatoração única se, e somente se, são satisfeitas as seguintes condições:*

1. *A é um domínio integralmente fechado;*

2. $\operatorname{Pic} X \simeq \mathbb{Z}$, *em que* $\operatorname{Pic} X$ *é gerado pela classe de $X.H$.*

Demonstração. [12, Exercise II.6.3(c), pg. 147]. ∎

Se $X \subset \mathbb{P}^3$ é uma variedade satisfazendo as condições da proposição anterior, então, como veremos a seguir, toda curva irredutível em X é uma interseção completa. Esta propriedade será fundamental para a demonstração do critério de minimalidade no teorema 3.2.2.

Observação 3.1.2 Seja $X \subset \mathbb{P}^3$ uma superfície cujo anel de coordenadas homogêneas $A = \mathbb{C}[u, x, y, z]/\mathcal{I}(X)$ é um domínio de fatoração única. Se $C \subset X$ é uma subvariedade irredutível de dimensão igual a 1, então seu ideal $\mathcal{I}_X(C)$ em A é primo de altura $2 - 1 = 1$. Sendo A um domínio fatorial, $\mathcal{I}_X(C)$ é um ideal principal, digamos $\mathcal{I}_X(C) = (\overline{G})$, com $G \in \mathbb{C}[u, x, y, z]$ homogêneo. Assim, o ideal de C em $\mathbb{C}[u, x, y, z]$ é gerado por $\mathcal{I}(X)$ e G. Consequentemente, se $\mathcal{I}(X) = (F)$, então $\mathcal{I}(C) = (F, G)$ e C é uma interseção completa.

Seja X uma variedade projetiva e não singular. Definimos o *grupo de Néron-Severi* $NS(X)$ de X, como o quociente de $\operatorname{Pic} X$ pelo subgrupo $\operatorname{Pic}^0 X$ dos divisores algebricamente equivalentes a zero; isto é,

$$0 \to \operatorname{Pic}^0 X \to \operatorname{Pic} X \to NS(X) \to 0$$

é exata. Pelo teorema da base de Néron-Severi [14, Proposition 1.1.16, pg. 18], $NS(X)$ é um grupo livre de posto finito. O posto de $NS(X)$ é chamado de *número de Picard de* X. Para futura referência, destacamos que:

Observação 3.1.3 Se X é uma variedade projetiva não singular com número de Picard igual a 1, então $NS(X) \simeq \mathbb{Z}$.

Veremos agora que, se $F \in \mathbb{C}[u, x, y, z]$ é um polinômio homogêneo e irredutível de grau primo, tal que $\mathcal{Z}(F) \subset \mathbb{P}^3$ tem número de Picard igual a 1, então a condição (2) de 3.1.1 é satisfeita.

Lema 3.1.4 *Seja $F \in \mathbb{C}[u,x,y,z]$ um polinômio homogêneo e irredutível. Seja ainda $X = \mathcal{Z}(F) \subset \mathbb{P}^3$. Se h é uma seção hiperplana própria de X, então*

$$h \cdot h = \deg F.$$

Demonstração. Sejam h_1, h_2 seções hiperplanas próprias de $\mathcal{Z}(F)$, definidas pelos hiperplanos $H_1 = \mathcal{Z}(G_1)$ e $H_2 = \mathcal{Z}(G_2)$ de $\mathbb{P}^3$, respectivamente. Se g_1, g_2 são as imagens de G_1, G_2 no anel de coordenadas de X, então $h_1 - h_2 = \operatorname{Div}(g_1/g_2)$ e $h_1 = h_2$ em $\operatorname{Pic} X$. Em outras palavras, quaisquer duas seções hiperplanas de $\mathcal{Z}(F)$ definem o mesmo elemento em $\operatorname{Pic} X$. Assim, $h \cdot h = h_1 \cdot h_2$ e, sem perda de generalidade, podemos supor que h_1 e h_2 são curvas que se interceptam transversalmente, em que a reta $H_1 \cap H_2$ se encontra em posição geral em relação a $\mathcal{Z}(F)$. Portanto,

$$h \cdot h = h_1 \cdot h_2 = \#(h_1 \cap h_2) = \#\big((H_1 \cap H_2) \cap \mathcal{Z}(F)\big) = \deg F.$$

Como queríamos demonstrar. ∎

Lema 3.1.5 *Seja $X \subset \mathbb{P}^n$ uma hipersuperfície com $\mathcal{I}(X) = (F)$. Se $0 < i < n-1$, então $H^i(X, \mathcal{O}_X)$ é nulo.*

Demonstração. Sejam k o grau de F e $S = \mathbb{C}[x_0, \ldots, x_n]$ o anel de coordenadas homogêneas de $\mathbb{P}^n$. Se $j : S(-k) \to S$ é dado por $j(G) = FG$, então temos a sequência exata de anéis graduados

$$0 \to S(-k) \to S \to S/(F) \to 0,$$

que induz a sequência exata de feixes sobre $\mathbb{P}^n$,

$$0 \to \mathcal{O}_{\mathbb{P}^n}(-k) \to \mathcal{O}_{\mathbb{P}^n} \to \imath_* \mathcal{O}_X \to 0,$$

em que $\imath : X \to \mathbb{P}^n$ é a inclusão. Passando à sequência exata de co-homologia, temos:

$$\ldots \to H^i\left(\mathcal{O}_{\mathbb{P}^n}\right) \to H^i\left(\imath_* \mathcal{O}_X\right) \to H^{i+1}\left(\mathcal{O}_{\mathbb{P}^n}(-k)\right) \to \ldots.$$

No entanto, se $0 < i \leq n-1$, então $H^i(\mathcal{O}_{\mathbb{P}^n}(d)) = 0$, qualquer que seja $d \in \mathbb{Z}$; veja [16, Theorem VII.4.1(b), pg. 122]. Portanto, $H^i(\imath_* \mathcal{O}_X) = 0$, se $0 < i < n-1$. E o resultado segue da existência de um isomorfismo entre $H^i(\mathbb{P}^n, \imath_* \mathcal{O}_X)$ e $H^i(X, \mathcal{O}_X)$; veja [16, Proposition VII.2.11, pg. 121]. ∎

Proposição 3.1.6 *Seja $F \in \mathbb{C}[u,x,y,z]$ um polinômio homogêneo e irredutível de grau k. Se $X = \mathcal{Z}(F) \subset \mathbb{P}^3$ é não singular e tem número de Picard igual a 1, então* $\operatorname{Pic} X \simeq \mathbb{Z}$. *Além disso, se k é primo e h é uma seção hiperplana de X, então* $\operatorname{Pic} X$ *é gerado pela classe de h.*

Demonstração. Sejam $\mathscr{X}$ a variedade analítica associada a X e $\exp : \mathcal{O}_{\mathscr{X}} \to \mathcal{O}^*_{\mathscr{X}}$ definido por $\exp(U)(\varphi)(x) = e^{2\pi i \varphi(x)}$. Sendo $\ker(\exp)$ igual ao feixe constante $\mathbb{Z}$, temos a sequência exata

$$0 \to \mathbb{Z} \to \mathcal{O}_{\mathscr{X}} \to \mathcal{O}^*_{\mathscr{X}} \to 0.$$

Passando à sequência de co-homologia, obtemos:

$$\cdots \to H^1(\mathscr{X}, \mathcal{O}_{\mathscr{X}}) \to H^1(\mathscr{X}, \mathcal{O}^*_{\mathscr{X}}) \to H^2(\mathscr{X}, \mathbb{Z}) \to \ldots.$$

Por GAGA [18], $H^i(\mathscr{X}, \mathcal{O}_{\mathscr{X}}) \simeq H^i(X, \mathcal{O}_X)$ e $H^1(\mathscr{X}, \mathcal{O}^*_{\mathscr{X}}) \simeq H^1(X, \mathcal{O}^*_X) \simeq \operatorname{Pic} X$. Assim, usando o lema 3.1.5,

$$\ldots \to 0 \to \operatorname{Pic} X \xrightarrow{c_1} H^2(\mathscr{X}, \mathbb{Z}) \to \ldots .$$

Por outro lado, [11, Lemma §3.5, pg. 462] nos diz que $\ker(c_1) = \operatorname{Pic}^0 X$. Dessa forma, $\operatorname{Pic}^0 X = 0$ e $\operatorname{Pic} X = NS(X) \simeq \mathbb{Z}$, na medida em que $NS(X)$ tem posto igual a 1; veja observação 3.1.3.

Para o caso em que k é primo, resta mostrar que se h é uma seção hiperplana de X, então sua classe, que também será denotada por h, gera $\operatorname{Pic} X$. Sejam g um gerador de $\operatorname{Pic} X$ e $a \in \mathbb{Z}$, tais que $h = ag$. Pelo lema 3.1.4,

$$k = h \cdot h = ag \cdot ag = a^2(g \cdot g).$$

Com isso, a^2 divide k e, sendo k primo, segue-se que $a \in \{-1, 1\}$. Portanto, $h = -g$ ou $h = g$. Em qualquer dos casos, h gera $\operatorname{Pic} X$. ■

Corolário 3.1.7 *Seja $X = \mathcal{Z}(F) \subset \mathbb{P}^3$, em que F é um polinômio homogêneo e irredutível de grau primo. Se X tem número de Picard igual a 1 e o seu anel de coordenadas homogêneas A é integralmente fechado, então A é um domínio de fatoração única.*

Demonstração. Basta verificarmos as duas condições da proposição 3.1.1. A condição (1) é satisfeita por hipótese. Se h é uma seção hiperplana própria de X, então a proposição anterior implica que vale a condição (2) de 3.1.1. ■

3.2 Critério de Minimalidade

Seja $X \subset \mathbb{P}^3$ uma variedade projetiva complexa não singular. Se seu anel de coordenadas é um domínio de fatoração única, então toda curva irredutível $C \subset X$ é uma interseção completa. A partir disto, poderemos estudar o grau de C e demonstrar o principal teorema deste capítulo, a saber, o teorema 3.2.2.

Comecemos com duas definições. Sejam $A = \mathbb{C}[u, x, y, z]$ e M um A-módulo graduado. Dizemos que $\mathfrak{p}$ é um *ideal primo* de M, se $\mathfrak{p}$ é um ideal primo de A contendo o anulador de M. Se $\mathfrak{p}$ é um primo mínimo de M, então definimos a *multiplicidade* $\mu_{\mathfrak{p}}(M)$ de M em $\mathfrak{p}$ como o comprimento de $M_{\mathfrak{p}}$ sobre $A_{\mathfrak{p}}$.

Lema 3.2.1 *Seja $C \subset \mathbb{P}^3$ uma curva irredutível. Se $\mathcal{I}(C) = (F, G)$ com $F, G \in \mathbb{C}[u, x, y, z]$ polinômios homogêneos, então* $\deg(C) = \deg(F) \cdot \deg(G)$.

Demonstração. Denote $X = \mathcal{Z}(F)$, $Y = \mathcal{Z}(G)$ e $\mathfrak{p} = \mathcal{I}(C)$. Inicialmente, mostraremos que $\mu_{\mathfrak{p}}(A/\mathfrak{p})$ é igual a 1. De fato, se $s \notin \mathfrak{p}$, então $1/s \in A_{\mathfrak{p}}$ e a ação de $1/s$ em

$\overline{s} \in (A/\mathfrak{p})_\mathfrak{p}$ nos diz que $\overline{1} \in (A/\mathfrak{p})_\mathfrak{p}$. Consequentemente, $\overline{s}$ gera $(A/\mathfrak{p})_\mathfrak{p}$, qualquer que seja $0 \neq \overline{s} \in (A/\mathfrak{p})_\mathfrak{p}$. Dessa forma, $(A/\mathfrak{p})_\mathfrak{p}$ é simples, ou seja, sua multiplicidade é igual a 1.

Por outro lado, por [12, Theorem I.7.7, pg. 53],

$$\mu_\mathfrak{p}\big(A/(\mathcal{I}(X)+\mathcal{I}(Y))\big) \cdot \deg C = \deg X \cdot \deg Y = \deg F \cdot \deg G,$$

onde a segunda igualdade segue de [12, Proposition I.7.6(d), pg. 52]. Contudo, temos que $\mathcal{I}(X)+\mathcal{I}(Y) = (F, G) = \mathfrak{p}$. Assim, $\mu_\mathfrak{p}\big(A/(\mathcal{I}(X)+\mathcal{I}(Y))\big) = \mu_\mathfrak{p}(A/\mathfrak{p}) = 1$ e $\deg(C) = \deg(F) \cdot \deg(G)$. ■

Teorema 3.2.2 *Seja $F \in \mathbb{Q}[u, x, y, z]$ um polinômio homogêneo de grau $k \geq 5$, tal que* $\mathrm{Sing}(\rho_F)$ *é finito, $\mathcal{Z}(F)$ é não singular, ρ_F é não degenerado e $\mathbb{C}[u, x, y, z]/(F)$ é um domínio de fatoração única. Se $\mathcal{S}(\theta_u) \cap \mathbb{Q}[y]$ é gerado por um polinômio irredutível de grau $m(k)$ e, para todo $p \in \mathrm{Sing}(\theta_u)$, os autovalores λ_1, λ_2 de $J_p(\theta_u)_{|T_p\mathcal{Z}(F)}$ satisfazem $\lambda_1/\lambda_2 \notin K_p$, então $\mathcal{Z}(F)$ é uma variedade involutiva mínima.*

Demonstração. Suponha, por absurdo, que $X = \mathcal{Z}(F)$ contém uma subvariedade involutiva própria Y. Por 2.2.14, F é irredutível e, pelos mesmos argumentos iniciais da demonstração do teorema 2.2.15, temos que Y é invariante por ρ_F e $\dim Y = 1$. Aplicando 2.2.1, existe uma curva $C \subset X$ irredutível, definida sobre $\mathbb{Q}$ e invariante por ρ_F. Agora, sendo $\mathcal{I}(X) = (F)$, temos que $\mathbb{C}[u, x, y, z]/(F)$ é o anel de coordenadas homogêneas de $X \subset \mathbb{P}^3$ e, por 3.1.2, C é uma interseção completa. Em outras palavras, existe um polinômio homogêneo $G \in \mathbb{C}[u, x, y, z]$, tal que $\mathcal{I}(C) = (F, G)$. Assim, por 3.2.1,

$$\deg(C) = \deg(F) \cdot \deg(G). \tag{3.1}$$

Por outro lado, afirmamos que $\mathrm{Sing}(C) = \mathrm{Sing}(\rho_F)$. De fato, 2.2.11 nos diz que $\mathrm{Sing}(C) \subset \mathrm{Sing}(\rho_F)$. Além disso, se $p \in \mathrm{Sing}(\rho_F)$, então $p \in \mathrm{Sing}(\theta_u)$ e, pela proposição 2.2.2, $p \in \mathrm{Sing}(C)$, pois, por hipótese, o quociente dos autovalores associados a p não pertence a K_p. Portanto, $\text{Sing}(\rho_F) \subset \text{Sing}(C)$ o que prova nossa afirmação. Dessa forma, as hipóteses de 2.2.12 são satisfeitas e, portanto,

$$2g + (4 - k)\deg(C) = -2k^3 + 4k^2 + 2,$$

em que g é o gênero da normalização de C. Além disso, [10, Theorem 1.6, pg. 212] nos diz que $\deg(G)+\deg(F) \leq k-1+3$, ou seja, $\deg(G) \leq 2$. Por (3.1), $\deg(C) \leq 2k$ e, como $k \geq 5$, concluímos que

$$\begin{aligned} 2g &= -2k^3 + 4k^2 + 2 + (k-4)\deg(C) \\ &\leq -2k^3 + 4k^2 + 2 + (k-4)2k \\ &= -2k^3 + 6k^2 - 8k + 2 \\ &< 0. \end{aligned}$$

O que é um absurdo. Dessa forma, $X = \mathcal{Z}(F)$ não contém subvariedade involutiva própria, ou seja, é involutiva mínima. ■

3.3 Exemplos

Nesta seção, mostraremos que se $k = 5$ ou $k = 7$, então

$$F = u^k + x(x+y)^{k-1} + (x+y)z^{k-1} + zx^{k-1} \tag{3.2}$$

satisfaz as condições do teorema 3.2.2. Para tanto, verificaremos cada uma das hipóteses do teorema separadamente.

Lema 3.3.1 *Se $F = u^k + x(x+y)^{k-1} + (x+y)z^{k-1} + zx^{k-1}$, em que $k \geq 3$, então ∇F nunca se anula em $\mathcal{Z}(F) \subset \mathbb{P}^3$.*

Demonstração. Suponha, por absurdo, que $p = [u_0 : x_0 : y_0 : z_0] \in \mathcal{Z}(F)$ é tal que as derivadas parciais de F se anulam em p. De imediato, $(\partial F/\partial u)(p) = 0$ implica em $u_0 = 0$. Como $p \in \mathcal{Z}(F)$, então

$$x_0(x_0 + y_0)^{k-1} = -(x_0 + y_0)z_0^{k-1} - z_0 x_0^{k-1}. \tag{3.3}$$

Além disso, $0 = (\partial F/\partial z)(p) = (k-1)(x_0+y_0)z_0^{k-2} + x_0^{k-1}$ nos diz que

$$0 = (k-1)z_0 \cdot \frac{\partial F}{\partial z}(p) = (k-1)^2(x_0+y_0)z_0^{k-1} + (k-1)z_0x_0^{k-1}. \tag{3.4}$$

Enquanto de $0 = (\partial F/\partial y)(p) = (k-1)x_0(x_0+y_0)^{k-2} + z_0^{k-1}$, obtemos que

$$0 = (x_0+y_0) \cdot \frac{\partial F}{\partial y}(p) = (k-1)\cdot x_0(x_0+y_0)^{k-1} + (x_0+y_0)z_0^{k-1}.$$

Desta última equação e de (3.3), concluímos que

$$\begin{aligned} 0 = & \ (k-1)\left[-(x_0+y_0)z_0^{k-1} - z_0x_0^{k-1}\right] + (x_0+y_0)z_0^{k-1} \\ = & \ (-k+2)(x_0+y_0)z_0^{k-1} - (k-1)z_0x_0^{k-1}. \end{aligned}$$

Ou seja, $(k-1)z_0x_0^{k-1} = (-k+2)(x_0+y_0)z_0^{k-1}$. Aplicando em (3.4):

$$0 = \big((k-1)^2 + (-k+2)\big)(x_0+y_0)z_0^{k-1}.$$

Com isso, $(x_0+y_0)z_0 = 0$, pois $(k-1)^2 + (-k+2)$ não tem raiz real. Dessa forma, $x_0 = 0$, pois $(\partial F/\partial z)(p) = 0$. Portanto, $z_0 = 0$, pois $(\partial F/\partial y)(p) = 0$. Finalmente, de $0 = (\partial F/\partial x)(p) = y_0^{k-1}$, temos que $y_0 = 0$. Sendo assim, $u_0 = x_0 = y_0 = z_0 = 0$, o que não é possível. Logo, ∇F não se anula em ponto algum de $\mathcal{Z}(F)$. ∎

Proposição 3.3.2 *Se $F = u^k + x(x+y)^{k-1} + (x+y)z^{k-1} + zx^{k-1}$, em que $k \geq 3$, então F é irredutível e $\mathcal{Z}(F) \subset \mathbb{P}^3$ é não singular.*

Demonstração. Sejam $G, H \in \mathbb{C}[u,x,y,z]$, tais que $F = GH$. É de fácil verificação que ∇F se anula em $\mathcal{Z}(G) \cap \mathcal{Z}(H) \subset \mathcal{Z}(F)$. Assim, o lema anterior nos diz que $\mathcal{Z}(G) \cap \mathcal{Z}(H) = \emptyset$. Pelo teorema da dimensão projetiva [12, Theorem I.7.2, pg. 48], temos que G ou H é invertível. O que prova a irredutibilidade de F. Agora, sendo F irredutível, temos que $\mathcal{I}\big(\mathcal{Z}(F)\big) = (F)$ e as singularidades de $\mathcal{Z}(F)$ são os pontos que anulam ∇F. Pelo o lema anterior, segue-se que $\mathcal{Z}(F)$ é não singular. ∎

Proposição 3.3.3 *Se $F = u^k + x(x+y)^{k-1} + (x+y)z^{k-1} + zx^{k-1}$, em que $k \geq 3$, então ρ_F não admite singularidade em $u = 0$.*

Demonstração. Suponha, por absurdo, que $p = [0 : x_0 : y_0 : z_0]$ é um ponto singular de ρ_F. Sendo o hamiltoniano de F em $\breve{p} = (0, x_0, y_0, z_0)$ proporcional ao campo de Euler em $\breve{p}$, então existe $\lambda \in \mathbb{C}^*$, tal que

$$\lambda \cdot (0, x_0, y_0, z_0) = \left(\frac{\partial F}{\partial y}, \frac{\partial F}{\partial z}, -\frac{\partial F}{\partial u}, -\frac{\partial F}{\partial x}\right)(\breve{p}).$$

Como $\partial F/\partial u = ku^{k-1}$, então $(\partial F/\partial u)(\breve{p}) = 0$ e temos que $y_0 = 0$. Consequentemente, $0 = (\partial F/\partial y)(\breve{p}) = (k-1)x_0^{k-1} + z_0^{k-1}$. Ou seja,

$$-(k-1)x_0^{k-1} = z_0^{k-1}. \tag{3.5}$$

Usando esta identidade, obtemos:

$$-\lambda z_0 = \frac{\partial F}{\partial x}(\breve{p}) = (k-1)x_0^{k-1} + x_0^{k-1} + z_0^{k-1} + (k-1)z_0 x_0^{k-2} = x_0^{k-1} + (k-1)z_0 x_0^{k-2}.$$

Dessa forma,

$$-\lambda z_0 x_0 = x_0^k + (k-1)z_0 x_0^{k-1}. \tag{3.6}$$

Por outro lado, (3.5) também nos diz que

$$z_0 \lambda x_0 = z_0 \frac{\partial F}{\partial z}(\breve{p}) = (k-1)x_0 z_0^{k-1} + x_0^{k-1} z_0 = -(k-1)^2 x_0^k + x_0^{k-1} z_0.$$

Logo, esta última igualdade e (3.6) implicam em

$$\begin{aligned} 0 = &\ \big(1 - (k-1)^2\big)x_0^k + kz_0 x_0^{k-1} \\ = &\ x_0^{k-1}\big(-(k^2-2k)x_0 + kz_0\big) \\ = &\ kx_0^{k-1}\big(-(k-2)x_0 + z_0\big). \end{aligned} \tag{3.7}$$

Como $p = [0 : x_0 : 0 : z_0]$, então, por (3.5), necessariamente $x_0 \neq 0$. Portanto, $-(k-1) = (z_0/x_0)^{k-1}$. Por outro lado, (3.7) nos diz que $k - 2 = z_0/x_0$. Assim,

$$0 > -(k-1) = (z_0/x_0)^{k-1} = (k-2)^{k-1} > 0,$$

o que é um absurdo. Consequentemente, $\mathrm{Sing}(\rho_F) \subset D_+(u)$. ■

Para o nosso próximo resultado, faremos uso da seguinte versão simplificada de [12, Proposition II.8.23, pg. 186]:

Proposição 3.3.4 *Se $Y \subset \mathbb{C}^n$ é uma interseção completa, então Y é normal se, e somente se, é regular em codimensão 1.*

Proposição 3.3.5 *Seja $F = u^k + x(x+y)^{k-1} + (x+y)z^{k-1} + zx^{k-1}$, em que $k \geq 5$ é um número primo. Então, $A = \mathbb{C}[u,x,y,z]/(F)$ é um domínio de fatoração única.*

Demonstração. Verificaremos que $X = \mathcal{Z}(F) \subset \mathbb{P}^3$ satisfaz as condições de 3.1.7. Por 3.3.2, $\mathcal{Z}(F) \subset \mathbb{P}^3$ é não singular. Assim, seu cone afim $\mathcal{C} \subset \mathbb{C}^4$ é não singular em todo ponto diferente de $(0,0,0,0)$. Portanto, o conjunto de pontos singulares de $\mathcal{C}$ tem codimensão 2, ou seja, $\mathcal{C}$ é regular em codimensão 1. Além disso, $\mathcal{C} = \mathcal{Z}(F) \subset \mathbb{C}^4$ é uma interseção completa. Aplicando 3.3.4, temos que $\mathcal{C}$ é normal. Sendo $\mathcal{C}$ uma variedade afim e A seu anel de coordenadas, segue-se que A é integralmente fechado; veja [12, Exercise I.3.17(d), pg. 23]. Quanto ao número de Picard, T. Shioda mostrou em [20, Theorem 4.1, pg. 312] que $\mathcal{Z}(F)$ tem número de Picard igual a 1. Finalmente, a condição de irredutibilidade de F é dada por 3.3.2. Dessa forma, 3.1.7 nos diz que A é um domínio de fatoração única. ■

Proposição 3.3.6 *Sejam q e $k \geq 5$ números primos e*

$$F = u^k + x(x+y)^{k-1} + (x+y)z^{k-1} + zx^{k-1}.$$

Se F é q-mínimo, então $\mathcal{Z}(F)$ é uma variedade involutiva mínima.

Demonstração. Basta verificarmos cada uma das condições do teorema 3.2.2. Sendo F um polinômio q-mínimo, segue-se que a base $\mathbb{Z}$-reduzida de $\mathcal{S}(\theta_u)$ é da forma $\{f, nx - f_1, mz - f_3\}$ com f irredutível de grau $m(k)$. Como a proposição 3.3.3 nos diz que $\mathrm{Sing}(\rho_F) \subset D_+(u)$, então, pela observação 2.6.1, $\mathrm{Sing}(\rho_F)$ é finito. Quanto às condições: $\mathcal{Z}(F)$ é não singular e $\mathbb{C}[u,x,y,z]/(F)$ é um domínio de fatoração única, temos que elas são verificadas pelas proposições 3.3.2 e 3.3.5, respectivamente. Quanto a ρ_F ser não degenerado e à condição sobre os autovalores, temos, tomando $G = F$ na proposição 2.4.2, que $\sqrt{\mu_F} \notin \mathbb{Q}[y]/(f)$ e $\eta_F \not\equiv 0 \mod f$. Portanto, por 2.3.3, ρ_F é não degenerado e $\lambda_1/\lambda_2 \notin K_p$, para todo $p \in \mathrm{Sing}(\rho_F)$, em que λ_1, λ_2 são os autovalores associados a p. Concluímos, assim, que $\mathcal{Z}(F)$ é uma variedade involutiva mínima. ∎

Com base nesta última proposição, fixados um número primo $k \geq 5$ e

$$F_k = u^k + x(x+y)^{k-1} + (x+y)z^{k-1} + zx^{k-1},$$

precisamos encontrar um número primo q, tal que F_k seja um polinômio q-mínimo. Relembrando a definição, precisamos encontrar q, de forma que, se $\pi : \mathbb{Z}_{\mathfrak{q}}[y] \to \mathbb{F}_q[y]$ é como em (2.29) e μ_{F_k}, η_{F_k} são como em 2.3.3, então

1. $\mathcal{S}(\theta_{u,F_k})$ admite uma base da forma $\{f, nx-f_1, mz-f_3\}$, em que $f, f_1, f_3 \in \mathbb{Z}[y]$ e f é irredutível de grau $m(k)$;

2. q não divide $\mathrm{lc}(f) \cdot n \cdot m$;

3. $\pi(f)$ é irredutível de grau $m(k)$;

4. $\pi(\eta_{F_k}) \not\equiv 0 \bmod \pi(f)$;

5. $T^2 - \overline{\pi(\mu_{F_k})}$ é irredutível em $\dfrac{\mathbb{F}_q[y]}{(\pi(f))}[T]$.

Para efetuar esta busca, usamos o sistema de computação algébrica Singular. Primeiramente calculamos a base $\mathbb{Z}$-reduzida de Gröbner de $\mathcal{S}(\theta_{u,F_k})$ e verificamos se o item (1) é satisfeito. Em caso afirmativo, iniciamos com $q = 2$ e testamos se todas as condições de (2) à (5) são satisfeitas. Caso alguma destas últimas condições não se verifique, tomamos o próximo número primo maior que q e testamos novamente as condições de (2) à (5). Seguimos com este procedimento até encontrarmos um primo q adequado.

Exemplo 3.3.7 $\mathcal{Z}(F_k)$ é involutiva mínima para $k = 5, 7$. De fato, aplicando o algoritmo acima nos casos $k = 5$ e $k = 7$, obtemos que F_5 é 1373-mínimo e que F_7 é 1103-mínimo. Com isso, a afirmação segue de 3.3.6. $\square$

Para $k \geq 11$, não foi possível obter a base $\mathbb{Z}$-reduzida de $\mathcal{S}(\theta_{u,F_k})$ devido a limitações computacionais. Por exemplo, para $k = 11$, espera-se que $\mathcal{S}(\theta_{u,F_{11}})$ contenha em sua base um polinômio de grau $m(11) = 1111$. Além disso, um outro aspecto é o tamanho dos coeficientes. No caso $k = 5$, os coeficientes de cada termo dos polinômios f_1 e f_3 da base $\mathbb{Z}$-reduzida de $\mathcal{S}(\theta_{u,F_5})$ contêm cerca de 1.200 dígitos. Mas, no caso $k = 7$, esta média já salta para mais de 11.970 dígitos! Dessa forma, não é uma surpresa que os computadores de que dispomos não sejam capazes de manipular os polinômios para o cálculo da base de Gröbner $\mathcal{G}$, nos casos em que $k \geq 11$. No entanto, para fins práticos, a base explícita serve apenas para verificar se $\text{Sing}(\theta_{u,F})$ é finito. Todas as outras verificações podem ser feitas sobre $\mathbb{F}_q$, ou seja, usando-se a imagem de $\mathcal{G}$ pela aplicação $\pi : \mathbb{Z}_{\mathfrak{q}}[y] \to \mathbb{F}_q[y]$.

Como objetivo futuro, pretendemos investigar se a teoria pode ser generalizada de forma que seja suficiente calcularmos a base reduzida diretamente sobre o corpo finito $\mathbb{F}_q$, ao invés de $\mathbb{Q}$. Isto reduziria drasticamente o uso da memória do computador, permitindo provarmos que F_k define uma variedade mínima para alguns k's maiores que 7. Se de fato for suficiente calcular $\mathcal{S}(\theta_{u,F_k})$ diretamente sobre $\mathbb{F}_q$, então teremos, por exemplo, que F_{11} é 3391-mínimo e que F_{13} é 10343-mínimo. Vale ressaltar que T. Shioda generalizou seu resultado obtido em [20], provando que F_k possui número de Picard igual a 1, sempre que k é um número ímpar não divisível por 3; veja [21, §4]. Dessa forma, podemos generalizar a proposição 3.3.6 e buscaríamos variedades mínimas quando k é ímpar, satisfaz $k \not\equiv 0 \mod 3$ e é livre de quadrados. Esta última condição se deve a uma generalização da proposição 3.1.6, pois, em sua demonstração, a condição efetivamente usada foi: se a^2 divide k, então $a \in \{-1, 1\}$.

Um outro aspecto a ser explorado, é aplicar deformações em F_k no sentido de polinômios q-equivalentes como visto no capítulo 2. Aqui, o ponto crucial é determinar se a deformação preserva o número de Picard.

Apêndice A

Spec $\mathbb{Z}[y]$

Dado $p \in \mathbb{Z}$ um número primo, denote por $\mathbb{F}_p$ o corpo $\mathbb{Z}/p\mathbb{Z}$.

Proposição A.1 *Os ideais primos de $\mathbb{Z}[y]$ são da forma*

$$\{0\}, \quad (p), \quad (g) \quad ou \quad (h, p)$$

em que $p \in \mathbb{Z}$ é primo, $g \in \mathbb{Z}[y]$ é irredutível e $h \in \mathbb{Z}[y]$ é irredutível em $\mathbb{F}_p[y]$.

Demonstração. É de fácil verificação, que se $g \in \mathbb{Z}[y]$ é um polinômio irredutível, então (g) é um ideal primo. Note que permitimos que g seja constante, igual a um primo de $\mathbb{Z}$. Reciprocamente, se I é um ideal primo, principal e não nulo, então $I = (g)$, para algum g irredutível.

Seja, agora, $I \in \operatorname{Spec} \mathbb{Z}[y]$ um ideal não principal. Tome $g \in I$ irredutível e $f \in I \setminus (g)$. Sendo $\mathbb{Q}[y]/(g)$ um corpo, existem $a, b \in \mathbb{Q}[y]$, tais que $af + bg = 1$. Eliminando-se os denominadores, existem $\tilde{a}, \tilde{b} \in \mathbb{Z}[y]$, tais que $\tilde{a}f + \tilde{b}g = n$, para algum $n \in \mathbb{N}^*$. Como $f, g \in I$, então $1 \neq n \in I$ e algum fator primo p de n pertence a I. Em particular, $(p) \subset I$. Tome $\phi : \mathbb{Z}[y] \to \mathbb{F}_p[y]$ a aplicação canônica. Como ϕ é sobrejetiva e $\ker(\phi) = (p) \subset I$, então $\phi(I)$ é um ideal primo. Sendo $\mathbb{F}_p[y]$ um domínio de ideais principais, $\phi(I) = \big(\phi(h)\big)$, com $\phi(h)$ irredutível. Por um lado,

$\phi(I)^{-1}$ é gerado por $h \cup \ker(\phi)$, ou seja, $\phi(I)^{-1} = (h, p)$. Por outro, $\phi(h) \in \phi(I)$ nos diz que existe $\xi \in I$, tal que $\phi(\xi) = \phi(h)$ e $\xi - h \in \ker(\phi)$. E como $\ker(\phi) \subset I$, temos que $h \in I$. Assim, $(p, h) \subset I \subset \phi(I)^{-1} \subset (p, h)$. Logo, $I = (p, h)$ é da forma desejada. Reciprocamente, sejam $p \in \mathbb{Z}$ primo e $h \in \mathbb{Z}[y]$, tais que $\phi(h)$ é irredutível. Sendo $J := \big(\phi(h)\big)$ um ideal primo de $\mathbb{F}_p[y]$, temos que $(p, h) = \phi(J)^{-1}$ é ideal primo de $\mathbb{Z}[y]$. E isto conclui a demonstração. ■

Dado $q \in \mathbb{Z}$ um número primo, denote por $\mathbb{Z}_{\mathfrak{q}}$ a localização de $\mathbb{Z}$ em $q\mathbb{Z}$.

Lema A.2 *Sejam $g \in \mathbb{Z}[y]$ irredutível e q um número primo. Se g é irredutível em $\mathbb{F}_q[y]$, então $\mathbb{Z}[y]/(g)$ localizado em $(\overline{q})$ é isomorfo a $\mathbb{Z}_{\mathfrak{q}}[y]/(g)$.*

Demonstração. Seja $\varphi : \mathbb{Z}[y]/(g) \to \mathbb{Z}_{\mathfrak{q}}[y]/(g)$ o homomorfismo induzido pela inclusão de $\mathbb{Z}[y]$ em $\mathbb{Z}_{\mathfrak{q}}[y]$. Se $\varphi(\overline{a}) = 0$, então existe $h \in \mathbb{Z}_{\mathfrak{q}}[y]$, tal que $a = gh$. Como g é irredutível, então g tem conteúdo igual a 1. Assim,

$$\operatorname{cont}(a) = \operatorname{cont}(g)\operatorname{cont}(h) = \operatorname{cont}(h)$$

e $h \in \mathbb{Z}[y]$. Logo, $\overline{a} = 0$ e φ é injetiva. Além disso, afirmamos que se $\overline{f} \in \mathbb{Z}[y]/(g)$ é tal que $\overline{f} \notin (\overline{q}) = \overline{(q, g)}$, então $\varphi(\overline{f})$ possui inverso. De fato, tome $a_0, b_0 \in \mathbb{Q}[y]$ tais que $fa_0 + gb_0 = 1$. Eliminando-se os denominadores, existem $a_1, b_1 \in \mathbb{Z}[y]$, tais que $fa_1 + gb_1 = n_1$, para algum $n_1 \in \mathbb{Z}$. Se q divide n_1, então $fa_1 \in (q, g)$ e, sendo (q, g) um ideal primo, $a_1 \in (q, g)$. Se $a_1 = qc_1 + gd_1$, então $fqc_1 + g(fd_1 + b_1) = qn_2$, em que $qn_2 = n_1$. Como (q) é ideal primo de $\mathbb{Z}[y]$ e q não divide g, então q divide $(fd_1 + b_1)$. Simplificando por q, existem $a_2, b_2 \in \mathbb{Z}[y]$ tais que $fa_2 + gb_2 = n_2$. Se q divide n_2, então, repetindo o processo um número finito de vezes, obtemos $a_k, b_k \in \mathbb{Z}[y]$, tais que $fa_k + gb_k = n_k \notin q\mathbb{Z}$. Assim, $\overline{a_k}/n_k$ é o inverso de $\varphi(\overline{f})$ em $\mathbb{Z}_{\mathfrak{q}}[y]/(g)$. E segue a afirmação. Dessa forma, pela propriedade universal, existe um homomorfismo $\psi : \big(\mathbb{Z}[y]/(g)\big)_{(\overline{q})} \to \mathbb{Z}_{\mathfrak{q}}[y]/(g)$, tal que o diagrama

$$\begin{tikzcd} \mathbb{Z}[y]/(g) \arrow[r, hook, "\varphi"] \arrow[d, "\imath"] & \mathbb{Z}_{\mathfrak{q}}[y]/(g) \\ \big(\mathbb{Z}[y]/(g)\big)_{(\overline{q})} \arrow[ur, dotted, "\psi"'] & \end{tikzcd}$$

comuta. Como φ é injetivo, ψ é injetivo. Além disso, sendo $\mathbb{Z}_{\mathfrak{q}}[y]/(g)$ gerado, como anel, por $\operatorname{im}(\varphi)$ e $\{\psi(\imath(s)^{-1}) : s \notin q\mathbb{Z}\}$, segue-se que ψ é sobrejetivo. Portanto, $\big(\mathbb{Z}[y]/(g)\big)_{(\overline{q})} \simeq \mathbb{Z}_{\mathfrak{q}}[y]/(g)$. ∎

Proposição A.3 *Sejam $g \in \mathbb{Z}[y]$ irredutível e q um número primo. Se g é irredutível em $\mathbb{F}_q[y]$, então $\mathbb{Z}_{\mathfrak{q}}[y]/(g)$ é um domínio fatorial, cujo corpo de frações é $\mathbb{Q}[y]/(g)$.*

Demonstração. Seja I um ideal primo de $\mathbb{Z}[y]$. Por A.1, I é da forma

$$\{0\}, \quad (p), \quad (h_1) \quad \text{ou} \quad (p, h_2),$$

em que $p \in \mathbb{Z}$ é primo, $h_1 \in \mathbb{Z}[y]$ é irredutível e h_2 é irredutível em $\mathbb{F}_p[y]$. Sendo g irredutível, temos, pelo teorema da correspondência, que os ideais primos não nulos, em $\mathbb{Z}[y]/(g)$, são imagens de ideais, em $\mathbb{Z}[y]$, da forma (p, g). Ou seja, todo ideal primo não nulo de $\mathbb{Z}[y]/(g)$ é da forma $(\overline{p})$, para algum $p \in \mathbb{Z}$ primo. Em particular, todo ideal primo de $\mathbb{Z}[y]/(g)$ é principal. Logo, $\mathbb{Z}[y]/(g)$ tem dimensão igual a 1. Portanto, $\big(\mathbb{Z}[y]/(g)\big)_{(\overline{q})}$ é um anel local regular (de dimensão 1). Mas, todo anel local regular é um domínio fatorial; veja [9, Teorema 19.19, pg. 487]. E como A.2 nos diz que $\mathbb{Z}_{\mathfrak{q}}[y]/(g)$ é isomorfo a $\big(\mathbb{Z}[y]/(g)\big)_{(\overline{q})}$, temos que $\mathbb{Z}_{\mathfrak{q}}[y]/(g)$ é um domínio fatorial.

Para determinar o corpo de frações de $\mathbb{Z}_{\mathfrak{q}}[y]/(g)$, comece tomando $\varphi : \mathbb{Z}_{\mathfrak{q}}[y]/(g) \to \mathbb{Q}[y]/(g)$ o homomorfismo induzido pela inclusão de $\mathbb{Z}_{\mathfrak{q}}[y]$ em $\mathbb{Q}[y]$. Se $\bar{a} \in \ker \varphi$, então existe $h \in \mathbb{Q}[y]$, tal que $a = hg$. Sendo g irredutível, g tem conteúdo 1 e

$\text{cont}(a) = \text{cont}(h)$. Logo, $h \in \mathbb{Z}_{\mathfrak{q}}[y]$ e $\overline{a} = 0$. Com isso, φ é injetiva. Dessa forma, se $\mathbb{F}$ é o corpo de frações de $\mathbb{Z}_{\mathfrak{q}}[y]/(g)$, então, pela propriedade universal, existe um homomorfismo injetivo Ψ de $\mathbb{F}$ em $\mathbb{Q}[y]/(g)$, tal que o diagrama

$$\begin{tikzcd}
\mathbb{Z}_{\mathfrak{q}}[y]/(g) \arrow[r, hook, "\varphi"] \arrow[d, "\imath"] & \mathbb{Q}[y]/(g) \\
\mathbb{F} \arrow[ur, dotted, "\Psi"'] &
\end{tikzcd}$$

comuta. Sendo $\mathbb{Q}[y]/(g)$ gerado, como anel, por $\text{im}\,(\varphi)$ e $\Psi\big(\imath(q)^{-1}\big)$, temos que Ψ é sobrejetivo e $\mathbb{F} \simeq \mathbb{Q}[y]/(g)$. $\blacksquare$

Observação A.4 Sejam $\phi_1 : \mathbb{Z}_{\mathfrak{q}}[y] \to \mathbb{Z}_{\mathfrak{q}}[y]/(g)$ e $\phi_2 : \mathbb{Z}_{\mathfrak{q}}[y] \to \mathbb{Q}[y]/(g)$ os homomorfismos canônicos. Como φ, na demonstração acima, é induzido pela inclusão de $\mathbb{Z}_{\mathfrak{q}}[y]$ em $\mathbb{Q}[y]$, então o diagrama

$$\begin{tikzcd}
\mathbb{Z}_{\mathfrak{q}}[y] \arrow[r, "\phi_1"] \arrow[dr, "\phi_2"'] & \mathbb{Z}_{\mathfrak{q}}[y]/(g) \arrow[d, "\varphi"] \\
& \mathbb{Q}[y]/(g)
\end{tikzcd}$$

comuta. Em particular, se $\eta \in \mathbb{Z}_{\mathfrak{q}}[y]$ é tal que $\overline{\eta} = 0$ em $\mathbb{Z}_{\mathfrak{q}}[y]/(g)$, então $\overline{\eta} = 0$ em $\mathbb{Q}[y]/(g)$.

Apêndice B

Extensão de Escalares

Seja I um ideal de $\mathbb{Q}[\mathtt{x}]$, onde $\mathtt{x}$ representa o conjunto de variáveis $x_1, \ldots, x_n$. Nesta seção, veremos que $\dim_{\mathbb{Q}}(\mathbb{Q}[\mathtt{x}]/I) = \dim_{\mathbb{C}}(\mathbb{C}[\mathtt{x}]/I\mathbb{C}[\mathtt{x}])$. Para facilitar a notação se $i = (i_1, \ldots, i_n)$, então $\mathtt{x}^i$ representará $x_1^{i_1} \ldots x_n^{i_n}$. Além disso, se V é um espaço vetorial e $B = \{b_i\}$ é uma base de V, então b_i^* denota o funcional linear que satisfaz $b_i^*(b_j) = \delta_{ij}$, em que δ_{ij} é o delta de Kronecker.

Lema B.1 *Sejam V e W dois $\mathbb{Q}$-espaços vetoriais e $e_1, \ldots, e_n \in W$ linearmente independentes. Se $\sum_{i=1}^n (v_i \otimes e_i) = 0$ em $V \otimes_{\mathbb{Q}} W$, então $v_i = 0$, para $i = 1, \ldots, n$.*

Demonstração. Suponha, por absurdo, que $v_j \neq 0$, para algum $j \in \{1, \ldots, n\}$. Tome f um funcional linear de V, tal que $f(v_j) = 1$ e defina $\eta : V \times W \to \mathbb{Q}$ por $\eta(v, w) = f(v)e_j^*(w)$. Sendo η bilinear e $\mathbb{Q}$-balanceada, temos que η induz a aplicação linear

$$\begin{aligned} \zeta : V \otimes_{\mathbb{Q}} W &\to \mathbb{Q} \\ v \otimes w &\mapsto f(v)e_j^*(w). \end{aligned}$$

Aplicando ζ a $\sum_{i=1}^n (v_i \otimes e_i)$, obtemos que

$$0 = \zeta\left(\sum_{i=1}^n (v_i \otimes e_i)\right) = \sum_{i=1}^n f(v_i)e_j^*(e_i) = f(v_j) = 1.$$

O que é um absurdo. Sendo assim, $v_i = 0$, para $i = 1, \ldots, n$. ■

Proposição B.2 *Se V é um $\mathbb{Q}$-espaço vetorial, então*

$$\dim_{\mathbb{Q}}(V) = \dim_{\mathbb{C}}(V \otimes_{\mathbb{Q}} \mathbb{C}).$$

Em particular, $\dim_{\mathbb{Q}}(\mathbb{Q}[\mathtt{x}]/I) = \dim_{\mathbb{C}}(\mathbb{Q}[\mathtt{x}]/I \otimes_{\mathbb{Q}} \mathbb{C})$.

Demonstração. Seja B uma $\mathbb{Q}$-base de V. Mostraremos que $\beta = \{b \otimes 1 : b \in B\}$ é uma $\mathbb{C}$-base de $V \otimes_{\mathbb{Q}} \mathbb{C}$. Seja $v \otimes \lambda \in V \otimes_{\mathbb{Q}} \mathbb{C}$. Como

$$v \otimes \lambda = \sum_{b \in B} b^*(v) b \otimes \lambda = \sum_{b \in B} b^*(v) \lambda \cdot (b \otimes 1),$$

temos que β gera $V \otimes_{\mathbb{Q}} \mathbb{C}$. Note que as somas acima são finitas, pois $b^*(v) \neq 0$ apenas para um número finito de b's.

Resta mostrar a independência linear. Suponha que $\sum_{b \in B} \lambda_b (b \otimes 1) = 0$, com $\lambda_b \in \mathbb{C}$ quase todos nulos e tome E uma base de $\mathbb{C}$ como $\mathbb{Q}$-espaço. Escrevendo os λ_b's em função da base E, temos que

$$0 = \sum_{b \in B} \lambda_b (b \otimes 1) = \sum_{b \in B} \left(\sum_{e \in E} e^*(\lambda_b) e \right) (b \otimes 1) = \sum_{e \in E} \left(\sum_{b \in B} e^*(\lambda_b) b \otimes e \right).$$

Pelo lema anterior, $\sum_{b \in B} e^*(\lambda_b) b = 0$, para todo $e \in E$. Sendo B uma base de V, temos, para cada $b \in B$, que $e^*(\lambda_b) = 0$, para todo $e \in E$. Dessa forma, $\lambda_b = \sum_{e \in E} e^*(\lambda_b) e = 0$, para todo $b \in B$, e temos a independência linear. Portanto, β é uma $\mathbb{C}$-base de $V \otimes_{\mathbb{Q}} \mathbb{C}$ que possui a mesma cardinalidade de B. Assim sendo, $\dim_{\mathbb{Q}}(V) = \dim_{\mathbb{C}}(V \otimes_{\mathbb{Q}} \mathbb{C})$. ■

De maneira geral, se R é um anel, J é um ideal de R e M é um R-módulo, então $\varphi : R/J \otimes_R M \to M/JM$, definido a partir de $\varphi(\overline{r} \otimes m) = \overline{rm}$, é um isomorfismo de R-módulos. Dessa forma,

$$\mathbb{Q}[\mathtt{x}]/I \otimes_{\mathbb{Q}[\mathtt{x}]} \mathbb{C}[\mathtt{x}] \simeq \mathbb{C}[\mathtt{x}]/I\mathbb{C}[\mathtt{x}]. \tag{1}$$

Note que este isomorfismo é na verdade $\mathbb{C}[\mathtt{x}]$-linear. Em particular, é um isomorfismo de $\mathbb{C}$-espaços vetoriais. Assim, para nossos propósitos, é suficiente mostrarmos que $\mathbb{Q}[\mathtt{x}]/I \otimes_{\mathbb{Q}} \mathbb{C}$ é isomorfo a $\mathbb{Q}[\mathtt{x}]/I \otimes_{\mathbb{Q}[\mathtt{x}]} \mathbb{C}[\mathtt{x}]$ como $\mathbb{C}$-espaços. Comecemos com a aplicação bilinear $\Phi : \mathbb{Q}[\mathtt{x}]/I \times \mathbb{C}[\mathtt{x}] \to \mathbb{Q}[\mathtt{x}]/I \otimes_{\mathbb{Q}} \mathbb{C}$ dada por

$$\Phi(\overline{f}, \sum \lambda_i \mathtt{x}^i) = \sum \overline{f\mathtt{x}^i} \otimes \lambda_i.$$

Mostraremos que Φ é $\mathbb{Q}[\mathtt{x}]$-balanceada. Se $g = \sum \alpha_j \mathtt{x}^j \in \mathbb{Q}[\mathtt{x}]$, então

$$\Phi\left(\overline{f}, g \cdot \sum_i \lambda_i \mathtt{x}^i\right) = \Phi\left(\overline{f}, \sum_j \alpha_j \mathtt{x}^j \sum_i \lambda_i \mathtt{x}^i\right) = \sum_{i,j} \overline{f\mathtt{x}^{j+i}} \otimes \alpha_j \lambda_i = \sum_{i,j} \overline{f\alpha_j \mathtt{x}^{j+i}} \otimes \lambda_i,$$

pois os α_j's pertencem a $\mathbb{Q}$. Assim,

$$\Phi\left(\overline{f}, g \cdot \sum_i \lambda_i \mathtt{x}^i\right) = \sum_i \overline{f} \sum_j \overline{\alpha_j \mathtt{x}^j \mathtt{x}^i} \otimes \lambda_i = \sum_i \overline{fg\mathtt{x}^i} \otimes \lambda_i = \Phi\left(\overline{fg}, \sum_i \lambda_i \mathtt{x}^i\right),$$

e temos que Φ, de fato, é $\mathbb{Q}[\mathtt{x}]$-balanceada. Com isso, Φ induz uma aplicação no produto tensorial, que, por abuso de notação, ainda denotaremos por

$$\Phi : \mathbb{Q}[\mathtt{x}]/I \otimes_{\mathbb{Q}[\mathtt{x}]} \mathbb{C}[\mathtt{x}] \to \mathbb{Q}[\mathtt{x}]/I \otimes_{\mathbb{Q}} \mathbb{C}.$$

Seja, agora, $\Psi : \mathbb{Q}[\mathtt{x}]/I \otimes_{\mathbb{Q}} \mathbb{C} \to \mathbb{Q}[\mathtt{x}]/I \otimes_{\mathbb{Q}[\mathtt{x}]} \mathbb{C}[\mathtt{x}]$ a aplicação linear, tal que $\Psi(\overline{f} \otimes \lambda) = \overline{f} \otimes \lambda$. Como

$$\Psi \circ \Phi\left(\overline{f} \otimes \sum \lambda_i \mathtt{x}^i\right) = \Psi\left(\sum \overline{f\mathtt{x}^i} \otimes \lambda_i\right) = \sum \overline{f\mathtt{x}^i} \otimes \lambda_i = \sum \overline{f} \otimes \mathtt{x}^i \lambda_i,$$

segue-se que $\Psi \circ \Phi = \mathrm{id}$. Por outro lado, $\Phi \circ \Psi(\overline{f} \otimes \lambda) = \Phi(\overline{f} \otimes \lambda) = \overline{f} \otimes \lambda$ e $\Phi \circ \Psi = \mathrm{id}$. Com isso, Ψ é uma bijeção. Como Ψ é $\mathbb{C}$-linear, então Ψ é um isomorfismo de $\mathbb{C}$-espaços e obtemos:

$$\dim_{\mathbb{Q}} \frac{\mathbb{Q}[\mathtt{x}]}{I} = \dim_{\mathbb{C}} \left(\frac{\mathbb{Q}[\mathtt{x}]}{I} \otimes_{\mathbb{Q}} \mathbb{C}\right) = \dim_{\mathbb{C}} \left(\frac{\mathbb{Q}[\mathtt{x}]}{I} \otimes_{\mathbb{Q}[\mathtt{x}]} \mathbb{C}[\mathtt{x}]\right) = \dim_{\mathbb{C}} \frac{\mathbb{C}[\mathtt{x}]}{I\mathbb{C}[\mathtt{x}]},$$

em que a primeira igualdade segue da proposição B.2, enquanto que a terceira igualdade segue do isomorfismo em (1).

Apêndice C

Completamento

Sejam A um anel e $\mathfrak{m}$ um ideal de A. Definimos o *completamento* de A com respeito a $\mathfrak{m}$ por:

$$\hat{A} = \varprojlim A/\mathfrak{m}^i = \{g = (\overline{g}_1, \overline{g}_2, \ldots) \in \prod A/\mathfrak{m}^i \,|\, g_j \equiv g_i \mod \mathfrak{m}^i, \text{se}\, j > i\}.$$

Em $\hat{A}$, tome o ideal $\hat{\mathfrak{m}} = \{(\overline{g}_1, \overline{g}_2, \ldots) \,|\, \overline{g}_1 = 0\}$. No caso em que $\mathfrak{m}$ é máximo, temos que $\hat{A}$ é local. De fato, seja $\varphi : A \to \hat{A}/\hat{\mathfrak{m}}$ dada por $\varphi(a) = \overline{(\overline{a}, \overline{a}, \overline{a} \ldots)}$. Note que φ é sobrejetiva, pois $(\overline{a}, \overline{g}_2, \overline{g}_3 \ldots) \equiv (\overline{a}, \overline{a}, \overline{a}, \ldots) \mod \hat{\mathfrak{m}}$. Assim, de $\ker \varphi = \mathfrak{m}$, segue-se que $\hat{A}/\hat{\mathfrak{m}} \simeq A/\mathfrak{m}$ é um corpo. Em outras palavras, $\hat{\mathfrak{m}}$ é um ideal máximo. Resta mostrar, que $\hat{\mathfrak{m}}$ é o único ideal máximo. Seja $g = (\overline{g}_1, \overline{g}_2, \ldots) \in \hat{A} \setminus \hat{\mathfrak{m}}$. De imediato $\overline{g}_1 \neq 0$ e $\overline{g}_i \notin \mathfrak{m}(A/\mathfrak{m}^i)$, para todo i. Começamos mostrando que cada g_i tem inverso em $A/\mathfrak{m}^i$. Fixado i, tome $\psi : A/\mathfrak{m}^i \to A/\mathfrak{m}$ a projeção canônica, ou seja, $\psi(\overline{a})$ é a classe de a em $A/\mathfrak{m}$. Como $\overline{g}_i \notin \mathfrak{m}(A/\mathfrak{m}^i)$, então $g_i \notin \mathfrak{m}$ e existe $b \in A$, tal que $g_i b - 1 \in \mathfrak{m}$. Logo, $(g_i b - 1)^i \in \mathfrak{m}^i$. Contudo,

$$(g_i b - 1)^i = \sum_{k=0}^{i} \binom{i}{k} (g_i b)^k (-1)^{i-k} = (-1)^i + g_i \cdot \sum_{k=1}^{i} \binom{i}{k} g_i^{k-1} b^k (-1)^{i-k}.$$

Dessa forma, $h_i = (-1)^{i+1} \sum_{k=1}^{i} \binom{i}{k} g_i^{k-1} b^k (-1)^{i-k}$ é o inverso de g_i em $A/\mathfrak{m}^i$. De $\overline{g}_j = \overline{g}_i$ em $A/\mathfrak{m}^i$, segue-se que seus inversos são iguais, ou seja, $h_j \equiv h_i \mod \mathfrak{m}^i$. Assim, $h = (\overline{h}_1, \overline{h}_2, \ldots) \in \hat{A}$ e h é o inverso de g. Portanto, $(\hat{A}, \hat{\mathfrak{m}})$ é um anel local.

Proposição C.1 *Seja* $(A, \mathfrak{m})$ *um anel local noetheriano. Então* A *é regular se, e somente se, seu completamento* $\mathfrak{m}$*-ádico é regular.*

Demonstração. Denotando $A/\mathfrak{m}$ por K e identificando $\hat{A}/\hat{\mathfrak{m}}$ com K, temos um isomorfismo natural entre $\mathfrak{m}/\mathfrak{m}^2$ e $\hat{\mathfrak{m}}/\hat{\mathfrak{m}}^2$ como K-espaços. Além disso, A e $\hat{A}$ possuem a mesma dimensão. Dessa forma, $\mathfrak{m}/\mathfrak{m}^2$ é um espaço vetorial de dimensão igual a $\dim A$ se, e somente se, $\hat{\mathfrak{m}}/\hat{\mathfrak{m}}^2$ é um espaço de dimensão igual a $\dim \hat{A}$. E o resultado segue das equivalências em [25, Theorem VIII.25, pg. 301]. ■

Sejam B uma K-álgebra, $\delta : B \to B$ uma derivação e $\mathfrak{m}$ um ideal máximo de B preservado por δ. Passando à localização, temos a derivação induzida

$$\begin{aligned} \delta_{\mathfrak{m}} : B_{\mathfrak{m}} &\to B_{\mathfrak{m}} \\ \frac{b}{s} &\mapsto \frac{s\bar{\delta}(b) - b\bar{\delta}(s)}{s^2}. \end{aligned}$$

Como δ preserva $\mathfrak{m}$, então $\delta_{\mathfrak{m}}$ preserva $\underline{\mathfrak{m}} = \mathfrak{m}B_{\mathfrak{m}}$ e, portanto, $\delta_{\mathfrak{m}}(\underline{\mathfrak{m}}^i) \subset \underline{\mathfrak{m}}^i$, para todo $i \in \mathbb{N}$. Com isso, $\delta_{\mathfrak{m}}$ induz uma derivação no completamento

$$\begin{aligned} \Delta : \hat{B}_{\mathfrak{m}} &\to \hat{B}_{\mathfrak{m}} \\ (\overline{g}_1, \overline{g}_2, \ldots) &\mapsto \left(\overline{\delta_{\mathfrak{m}}(g_1)}, \overline{\delta_{\mathfrak{m}}(g_2)}, \ldots\right). \end{aligned}$$

Exemplo C.2 Sejam $X \subset \mathbb{C}^3$ uma superfície não singular, $C \subset X$ uma curva e p um ponto singular de C. Sejam, ainda, B o anel de coordenadas de X, $\mathfrak{m}$ o ideal máximo de B associado a p e $\delta : B \to B$ uma derivação com uma quantidade finita de singularidades. Se δ preserva $\mathcal{I}(C)$, então, pelo teorema da vizinhança tubular, $p \in \mathrm{Sing}(\delta)$; vide lema 2.2.11. Assim, $\delta(\mathfrak{m}) \subset \mathfrak{m}$. Aplicando a construção anterior, δ induz uma derivação $\Delta : \hat{B}_{\mathfrak{m}} \to \hat{B}_{\mathfrak{m}}$. Sendo X não singular, temos que $B_{\mathfrak{m}} = \mathcal{O}_{X,p}$ é regular e, por [25, Corolário VIII §12, p. 307], $\hat{\mathcal{O}}_{X,p} \simeq \mathbb{C}[[t, v]]$. Dessa forma, podemos considerar,

$$\Delta : \mathbb{C}[[t, v]] \to \mathbb{C}[[t, v]].$$

Além disso, [19, Teorema II.1, pg. 108] nos diz que existe $g \in \mathcal{O}_{X,p}$, tal que a imagem de $\mathcal{I}(C)$ em $\mathcal{O}_{X,p}$ é o ideal (g). Como δ preserva $\mathcal{I}(C)$, então Δ preserva (g). $\square$

Proposição C.3 *Nas condições do exemplo anterior, se*

$$\Delta = \lambda_1 t\frac{\partial}{\partial t} + \lambda_2 v\frac{\partial}{\partial v},$$

em que $\lambda_1/\lambda_2 \notin \mathbb{Q}$, então $(g) = (t)$ ou $(g) = (v)$ ou $(g) = (tv)$.

Demonstração. Como $\delta_\mathfrak{m}$ preserva (g), então existe $h \in \mathcal{O}_{X,p}$, tal que $\delta_\mathfrak{m}(g) = hg$. Se $\hat{h}, \hat{g} \in \mathbb{C}[[t,v]]$ são as imagens de h e g pela composição $\mathcal{O}_{X,p} \hookrightarrow \hat{\mathcal{O}}_{X,p} \simeq \mathbb{C}[[t,v]]$, então

$$\hat{h}\hat{g} = \Delta(\hat{g}) = \lambda_1 t\frac{\partial \hat{g}}{\partial t} + \lambda_2 v\frac{\partial \hat{g}}{\partial v}.$$

Afirmação 1. $\hat{g}$ é da forma $t^i v^j q$ com q invertível.

Demonstração da Afirmação. Se $\hat{h} = \sum d_{\alpha\beta} t^\alpha v^\beta$ e $\hat{g} = \sum c_{ij} t^i v^j$, então

$$\sum_{\alpha\beta} d_{\alpha\beta} t^\alpha v^\beta \cdot \sum_{ij} c_{ij} t^i v^j = \Delta(\hat{g}) = \sum_{ij} (i\lambda_1 + j\lambda_2) c_{ij} t^i v^j. \tag{1}$$

Sejam $N = \{(i,j) : c_{ij} \neq 0\}$ e $m = \min\{i+j : (i,j) \in N\}$. Tome $(i_0, j_0) \in N$, tal que $i_0 + j_0 = m$. Por (1), $d_{00} = i_0\lambda_1 + j_0\lambda_2$. Suponha, por absurdo, que exista outro par $(i_0, j_0) \neq (i_1, j_1) \in N$ que também satisfaça $i_1 + j_1 = m$. Como antes, $d_{00} = i_1\lambda_1 + j_1\lambda_2$ e obtemos que $i_0\lambda_1 + j_0\lambda_2 = i_1\lambda_1 + j_1\lambda_2$. Dessa forma, $\lambda_1/\lambda_2 = (j_1 - j_0)/(i_0 - i_1) \in \mathbb{Q}$. Contradizendo as hipóteses. Logo, o termo de menor grau de $\hat{g}$ é $t^{i_0} v^{j_0}$. Seja, agora, $k > m$ e suponha, por indução, que todo termo de $\hat{g}$ de grau menor que k é divisível por $t^{i_0} v^{j_0}$. Sejam $r, s \in \mathbb{N}$, tais que $r + s = k$ e $c_{rs} \neq 0$. Por (1),

$$\sum_{\substack{(\alpha+i,\beta+j)=(r,s)\\(i,j)\neq(r,s)}} d_{\alpha\beta} t^\alpha v^\beta c_{ij} t^i v^j = \big((r\lambda_1 + s\lambda_2)c_{rs} - d_{00}c_{rs}\big) t^r v^s.$$

Por hipótese de indução, a lado esquerdo da igualdade acima é divisível por $t^{i_0}v^{j_0}$. E como $d_{00} \neq r\lambda_1 + s\lambda_2$, segue-se que $t^{i_0}v^{j_0}$ divide $t^r v^s$. Assim, $t^{i_0}v^{j_0}$ divide todo termo de $\hat{g}$ e concluímos que $\hat{g} = t^{i_0}v^{j_0}(c_{i_0j_0} + \ldots)$. Sendo $c_{i_0j_0} \neq 0$, temos que $(c_{i_0j_0} + \ldots)$ é invertível e a afirmação segue.

Afirmação 2. $\hat{g}$ é reduzido.

Demonstração da Afirmação. Denote $A = \mathcal{O}_{X,p}$ e seu ideal (g) por I. Sendo A um anel local e noetheriano, temos, por [25, Theorem VIII.11, pg. 264], que a sequência exata $0 \to I \to A \to A/I \to 0$ induz a sequência exata

$$0 \to \hat{I} \to \hat{A} \to \widehat{(A/I)} \to 0.$$

Sendo g irredutível, segue-se que A/I é um domínio noetheriano e, portanto, a topologia de A/I, com relação ao seu ideal máximo, é Hausdorff. Aplicando [25, Theorem VIII.5, pg 256], concluímos que $\hat{I} = \hat{A}I$. Dessa forma,

$$\widehat{(A/I)} \simeq \hat{A}/\hat{I} = \hat{A}/\hat{A}I.$$

Contudo, [25, Lemma VIII.1, pg 314] nos diz que $\widehat{(A/I)}$ não possui elementos nilpotentes, a menos do zero. Assim, $\mathbb{C}[[t,v]]/(\hat{g})$ é livre de nilpotentes. E isto garante que $\hat{g}$ é reduzido. De fato, se $\hat{g} = a^2b$, então $(ab)^2 \equiv 0 \bmod (\hat{g})$. Logo, $ab = \hat{g}c$, para algum $c \in \mathbb{C}[[t,v]]$. Portanto, $ab = a^2bc$ e $1 = ac$. Dessa forma, a é invertível e $\hat{g}$ é reduzido. O que prova a afirmação.

Pelas afirmações 1 e 2, o ideal gerado por $\hat{g}$ é também gerado por $t^i v^j$, em que $i, j \in \{0, 1\}$. Como p pertence à curva de germe g, então não é possível que i e j sejam ambos nulos. Portanto, $(g) = (t)$ ou $(g) = (v)$ ou $(g) = (tv)$. ■

Observação C.4 Na demonstração acima, para provar que o completamento de $\mathcal{O}_{X,p}/(g)$ é livre de nilpotentes, é exigido uma condição técnica sobre $\mathcal{O}_{X,p}/(g)$. Condição esta que é satisfeita segundo o comentário de [25] no item (a) da página 318.

Referências Bibliográficas

[1] R. Abraham, J. E. Marsden, *Foundation of Mechanics*, 2ed., Addison-Weley Publishing Company, (1987).

[2] L. C. O. Almeida, S. C. Coutinho, 'On Homogenous Minimal Involutive Varieties', *LMS Journal of Computation and Mathematics* **8** (2005), 301–315.

[3] V. I. Arnold, *Geometrical Methods in the Theory of Ordinary Differential Equations*, Springer-Verlag, New York, (1983).

[4] A. Beauville, *Complex algebraic surfaces*, 2 ed., Cambridge University Press, (1996).

[5] J. Bernstein, V. Lunts, 'On non-holonomic irreducible $\mathcal{D}$-modules', *Invent. Math.* **94** (1988), 223–243.

[6] B. Buchberger, 'Ein algorithmisches Kriterium für die Lösbarkeit eines algebraischen Gleichungssystems', *Aeq. Math.*, (1970) 374–383.

[7] S. C. Coutinho, *A primer of algebraic $\mathcal{D}$-modules*, London Mathematical Society Student Texts 33, Cambridge University Press, (1995).

[8] S. C. Coutinho, *Polinômios e Computação Algébrica*, Coleção Matemática e Aplicações, IMPA, (2012).

[9] D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Graduate Texts in Mathematics 150, Springer, (1994).

[10] J. García, 'Multiplicity of a Foliation on Projective Spaces along an Integral Curve', *Rev. Mat. Univ. Complut. Madrid* **6** (1993), 207–217.

[11] P. Griffiths, J. Harris, *Principles of Algebraic Geometry*, Wiley-Interscience, (1978).

[12] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics 52, Springer, (1977).

[13] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, (1985).

[14] R. Lazarsfeld, *Positivity in Algebraic Geometry I*, Springer, (2004).

[15] V. Lunts, 'Algebraic varieties preserved by generic flows', *Duke Math. J.* **58** (1989), 531–554.

[16] D. Perrin, *Algebraic Geometry, An Introduction*, Springer-Verlag, (2008).

[17] F. S. Salas, 'Number of Singularities of Foliation on $\mathbb{P}^n$', *Proc. Amer. Math. Soc.* **130** (2002), 69–72.

[18] J. P. Serre, 'Géométric algébrique et géométrie analytique', *Annales de L'institut Fourier* **6** (1956), 1–42.

[19] I. R. Shafarevich, *Basic Algebraic Geometry,* vol. 1, 2ed., Springer-Verlag, (1994).

[20] T. Shioda, 'On the Picard number of a complex projective variety', *Annales scientifiques de l'É.N.S.* 4^e série **14** (1981), 303–321.

[21] T. Shioda, 'An Explicit Algorithm for Computing the Picard Number of Certain Algebraic Surfaces', *Amer. J. of Math.* **108** (1986), 415–432.

[22] M. G. Soares, 'On algebraic sets invariant by one-dimensional foliations on $CP(3)$', *Ann. Inst. Fourier* **43** (1993), 143–162.

[23] J. T. Stafford, 'Non-holonomic modules over Weyl algebras and enveloping algebras', *Invent. math.* **79** (1985), 619–638.

[24] T. Suwa, 'Indices of holomorphics vector fields relative to invariant curves on surfaces', *Proc. Amer. Math. Soc.* **123** (1995), 2989–2997.

[25] O. Zariski, P. Samuel, *Commutative Algebra*, vol. 2, Springer-Verlag, (1975).