UNIVERSIDADE FEDERAL FLUMINENSE

Instituto de Matemática

O Teorema do Mergulho da Reta

Rodrigo Salomão

Orientador: Abramo Hefez

Coordenação de Pós-Graduação em Matemática

Abril de 2004

.

AOS MEUS PAIS, que tenho como exemplo, e que incentivaram e contribuíram para minha formação como profissional e como pessoa.

Agradecimentos

A Fernanda, minha namorada, por estar sempre do meu lado e compreender todos os momentos difíceis que passei.

A todos os colegas do Mestrado, com os quais tive um excelente relacionamento. Em particular, ao velho amigo Alexandre e aos novos amigos: Charlie, Etereldes, Leonardo, Marcelo e Ricardo, que juntos formamos um grupo de discussão, que muito acrescentou para minha formação.

A todos os professores da UFF, com os quais tive o grande prazer de conviver e que sempre estiveram à disposição para incansáveis debates.

Ao professor e orientador Abramo Hefez, por me oferecer este belo tema e disponibilizar grande parte do seu tempo, para me ajudar na conclusão desta etapa.

Aos funcionários da secretaria, pela atenção e ajuda nos assuntos burocráticos.

Introdução

O objetivo desta monografia é o de apresentar uma demonstração do Teorema do Mergulho da Reta no Plano devido a Abhyankar-Moh.

Na literatura existem várias provas, ultilizando várias técnicas, desde álgebra até topologia. A demonstração original de S.S.Abhyankar e T.T.Moh é bastante extensa e foi substancialmente simplificada por Hai-chao Chang e Lih-chung Wang em [CW], que ultilizam basicamente teoria de interseção para curvas planas e propriedades elementares das raízes aproximadas de Abhyankar-Moh.

Para tornar o trabalho autosuficiente, apresentamos, no Capítulo 1, um resumo dos fatos sobre curvas planas que serão ultilizados. Estes fatos podem ser encontrados com as suas respectivas demonstrações em [Hf]. No Capítulo 2, apresentaremos a teoria das raízes aproximadas de Abhyankar-Moh, fundamental para a prova do Teorema do Mergulho da Reta que apresentaremos aqui. No Capítulo 3, damos a prova propriamente dita do Teorema. No final do Capítulo apresentaremos uma prova do Teorema do Epimorfismo de Abhyankar-Moh, usando o Teorema do Mergulho.

Niterói, Abril de 2004.

Índice

Capítulo 1

Preliminares

Neste capítulo, iremos estabelecer as notações, bem como, apresentar os principais resultados que são pré-requisitos para o desenvolvimento da teoria subseqüente. Os fatos citados sem demonstração encontram-se em [Hf].

1.1 Expoentes Característicos

Denotaremos por $\mathbb{C}[[x,y]]$ e $\mathbb{C}[[t]]$ os anéis das séries de potências com coeficientes em $\mathbb{C}$ e com indeterminadas x, y e t, respectivamente. Para $h \in \mathbb{C}[[x,y]]$ iremos chamar de *curva algebróide plana*, o seguinte conjunto:

$$(h) = \{\ u.h\ ;\ u \in \mathbb{C}[[x,y]]\ \text{ invertível}\}.$$

Quando a série de potências $h \in \mathbb{C}[[x,y]]$ for irredutível, denominaremos por *ramo* a curva algebróide plana (h).

Seja $f \in \mathbb{C}[[x,y]]$ uma série de potências irredutível com $mult(f) = m > 0$, tal que

$$mult(f(0,y)) := n > m.$$

Pelo Teorema da Preparação de Weierstrass([Hf] pág 24), podemos supor que

$$f(x,y) = y^n + a_1(x)y^{n-1} + \cdots + a_n(x),$$

onde $a_i(0) = 0$ para todo $i = 1, \ldots, n$; isto é, $mult(a_i) > 0$. Quando f possui estas características dizemos que f é um *pseudo-polinômio*. Como f é irredutível, temos, necessariamente, pelo Lema da Unitangente([Hf] pág 52), que $mult(a_n) = m$.

Como conseqüência do Teorema de Newton-Puiseux([Hf] pág 52), existe $\varphi(t) \in \mathbb{C}[[t]]$ com $mult_t(\varphi(t)) = mult_x(a_n(x)) = m$ tal que

$$f(t^n, \varphi(t)) = 0.$$

Além disso, $f(t^n, \alpha(t)) = 0$ com $\alpha(t) \in \mathbb{C}[[t]]$ se, e somente se, $\alpha(t) = \varphi(\zeta t)$ onde ζ é uma raiz n-ésima da unidade em $\mathbb{C}$ e

$$n = min\{q \in \mathbb{N}; \varphi \in \mathbb{C}[[x^{\frac{1}{q}}]]\}.$$

Definição 1.1. A parametrização,

$$\begin{cases} x & = & t^n \\ y & = & \varphi(t) & = & \displaystyle\sum_{i=m}^{\infty} b_i t^i, \quad b_i \in \mathbb{C} \end{cases}$$

é denominada *parametrização de Puiseux* do ramo (f).

Tem-se que esta parametrização é primitiva, isto é, o máximo divisor comum entre n e todos os i tal que $b_i \neq 0$ é igual a 1.

Agora, definiremos os expoentes característicos do ramo (f).

Defina,

$$\begin{array}{rcl} \varepsilon_0 & = & \beta_0 \ = \ n \\ \beta_j & = & min\{i \ ; \ i \not\equiv 0 \ mod \ \varepsilon_{j-1} \ \ e \ \ b_i \neq 0\}, \text{ se } \varepsilon_{j-1} \neq 1 \\ \varepsilon_j & = & mdc(\varepsilon_{j-1}, \beta_j) \ = \ mdc(\beta_0, \ldots, \beta_j). \end{array}$$

Note que se $\varepsilon_{j-1} \neq 1$, então

$$\{i; \ i \not\equiv 0 \ mod \ \varepsilon_{j-1} \ \ e \ \ b_i \neq 0\} \neq \emptyset;$$

já que, a parametrização acima é primitiva. Portanto, β_j está bem definido.

Note que, sendo $m < n$, segue que $\beta_1 = m$.

E mais, ε_j divide ε_{j-1} e $\varepsilon_j < \varepsilon_{j-1}$ para todo $j \geq 1$. Assim, existe $g \in \mathbb{N}$ tal que $\varepsilon_g = 1$.

Conseqüentemente, a seqüência dos β_j é crescente para $j \geq 1$ e estaciona em β_g.

Definição 1.2. Os números $(\beta_0, \ldots, \beta_g)$ são denominados de *expoentes característicos* do ramo (f). Definimos também, o número n_j por:

$$n_j = \begin{cases} 1, & \text{se} \quad j = 0; \\ \dfrac{\varepsilon_{j-1}}{\varepsilon_j}, & \text{se} \quad j \in \{1, \ldots, g\}. \end{cases}$$

1.2 O Semigrupo de uma Curva

Dadas duas séries de potências $g, h \in \mathbb{C}[[x, y]]$ tais que $g(0,0) = h(0,0) = 0$ denotaremos por $I(g, h)$, o índice de interseção de (g) e (h); isto é,

$$I(g, h) = dim\, \frac{\mathbb{C}[[x, y]]}{\langle g, h \rangle},$$

como espaço vetorial sobre $\mathbb{C}$.

De agora em diante, (f) será um ramo e $(t^n, \varphi(t))$ será uma parametrização de Puiseux para este ramo.

Define-se a valorização v_f associada a f como:

$$\begin{array}{rcl} v_f : \mathbb{C}[[x, y]] \setminus \langle f \rangle & \longrightarrow & \mathbb{N} \\ h & \longmapsto & v_f(h) = mult(h(t^n, \varphi(t))). \end{array}$$

Sendo f irredutível, segue que, para todo $g \in \mathbb{C}[[x, y]] \setminus \langle f \rangle$, tem-se que $I(f, g) = v_f(g)$ (vide [Hf] pág 83 Teorema 6).

Dados $m_1, \ldots, m_r$ números naturais, vamos denotar por $\langle m_1, \ldots, m_r \rangle$, o semigrupo de $\mathbb{N}$ gerado por $m_1, \ldots, m_r$.

Definição 1.3. O *semigrupo de valores* associado ao ramo (f) é o conjunto

$$S(f) = \{v_f(h); h \in \mathbb{C}[[x, y]] \setminus \langle f \rangle\} \subset \mathbb{N}.$$

E mais, temos ainda que $\beta_1 = m = min(S(f) \setminus \{0\})$.

De fato, como $v_f(y) = mult(\varphi(t)) = m$, temos que $m \in S(f)$. Para provar que $m = min(S(f) \setminus \{0\})$, basta observar que se $h = \sum_{\alpha,\beta} a_{\alpha,\beta} x^\alpha y^\beta$ pertence a $\mathbb{C}[[x,y]] \setminus \langle f \rangle$, então

$$v_f(h) = mult\left(\sum_{\alpha,\beta} a_{\alpha,\beta} t^{n\alpha} \varphi(t)^\beta\right) \geq rn + sm \geq m.$$

Para cada $j = 2, \ldots, g$ defina

$$P_j(t) = \sum_{i=m}^{\beta_j - 1} b_i t^i \ \text{ e } \ G_j = \{\xi \in \mathbb{C}; \xi^{\varepsilon_j} = 1\}.$$

Note que G_j é o grupo das ε_j-ésimas raízes da unidade e que

$$G_0 \supset G_1 \supset \cdots \supset G_g.$$

Denote por $\bar{\xi}$ os elementos dos grupos $\dfrac{G_0}{G_{j-1}}$ e:

$$P_j(\bar{\xi} t) := P_j(\xi t).$$

Lema 1.1. *Para cada $j = 2, \ldots, g$, existe $f_j(x,y) \in \mathbb{C}[[x]][y]$ satisfazendo:*

(1) $\displaystyle f_j(x,y) = \prod_{\bar{\xi} \in \frac{G_0}{G_{j-1}}} (y - P_j(\bar{\xi} x^{\frac{1}{n}}))$;

(2) $\displaystyle gr_y(f_j) = \frac{n}{\varepsilon_{j-1}}$,

onde $gr_y(f_j)$ é o grau de f_j com respeito a indeterminada y.

DEMONSTRAÇÃO: Ver [Hf] cap 6.

□

Desta forma, podemos definir os inteiros:

$$v_j = \begin{cases} \beta_0 = n, & se \quad j = 0 \\ \beta_1 = m, & se \quad j = 1 \\ v_f(f_j), & se \quad j = 2, \ldots, g. \end{cases}$$

Agora, enunciaremos um resultado que relaciona os inteiros v_j com os expoentes característicos e o semigrupo $S(f)$.

Teorema 1.1. (Zariski)

(1) *Para cada* $j = 2, \ldots, g$ *temos que*

$$v_j = \sum_{k=1}^{j-1} \frac{\varepsilon_{k-1} - \varepsilon_k}{\varepsilon_{j-1}} \beta_k \ + \ \beta_j \tag{1.2.1}$$

(2) *Se* $gr_y(h) < n_1 \ldots n_j = \dfrac{n}{\varepsilon_j}$ *então* $v_f(h) \in \langle v_0, \ldots, v_j \rangle$. *Em particular,*

$$S(f) = \langle v_0, \ldots, v_g \rangle .$$

(3) *Para cada* $j = 1, \ldots, g$,

$$\varepsilon_j = mdc(\varepsilon_{j-1}, v_j).$$

Além disso, v_j *é o menor elemento não nulo de* $S(f)$ *que não é divisível por* ε_{j-1}.

Demonstração: Vide [Hf] pág 110.

□

Segue, imediatamente, de (1.2.1) e do fato que $\varepsilon_i = n_{i+1} \ldots n_j \varepsilon_j$, para todo $j = 1, \ldots, g$ *e* $i = 0, \ldots, j-1$, que

$$v_j = (n_1 - 1)n_2 \ldots n_{j-1}\beta_1 + (n_2 - 1)n_3 \ldots n_{j-1}\beta_2 + \cdots + (n_{j-1} - 1)\beta_{j-1} + \beta_j.$$

Conseqüentemente,

$$v_i = n_{i-1}v_{i-1} - \beta_{i-1} + \beta_i. \tag{1.2.2}$$

Como a seqüência (β_i), $i \geq 1$, é crescente, temos que

$$v_{i+1} > n_i v_i. \tag{1.2.3}$$

Devido a esta característica $S(f)$ é chamado de semigrupo *fortemente crescente.*

1.3 Contato entre Curvas

Sejam (f) e (h) dois ramos passando pela origem, com parametrizações de Puiseux:

$$(f):\begin{cases} x &= t^n \\ y &= \varphi(t) = \displaystyle\sum_{i=m}^{\infty} b_i t^i \end{cases}$$

$$(h):\begin{cases} x &= t^{n'} \\ y &= \psi(t) = \displaystyle\sum_{j=m'}^{\infty} b'_j t^j. \end{cases}$$

Denote por

$$\beta_0,\dots,\beta_g \ \ e \ \ \beta'_0,\dots,\beta'_{g'},$$

os expoentes característicos de (f) e (h), respectivamente. Denote também,

$$S(f)=\langle v_0,\dots,v_g\rangle \ \ e \ \ S(h)=\left\langle v'_0,\dots,v'_{g'}\right\rangle.$$

Definição 1.4. Definimos a *ordem de contato* $O(f,h)\in\mathbb{Q}\cup\{\infty\}$ entre os ramos (f) e (h) como

$$O(f,h)=\frac{max_{\zeta,\varepsilon}mult(\varphi(\zeta t^{n'})-\psi(\varepsilon t^n))}{nn'},$$

onde ζ e ε representam as raízes n-ésimas e n'-ésimas da unidade, respectivamente.

Proposição 1.1. *Se* $\dfrac{\beta_q}{n}\le O(f,h)<\dfrac{\beta_{q+1}}{n}$*, onde* $q\ge 1$ *e* $\beta_{g+1}=+\infty$*, então*

$$\frac{n}{n'}=\frac{\varepsilon_i}{\varepsilon'_i}=\frac{\beta_i}{\beta'_i}=\frac{v_i}{v'_i} \ \ para \ \begin{cases} 0\le i\le q-1, \ \ se \ \ O(f,h)=\dfrac{\beta_q}{n} \\ \\ 0\le i\le q, \ \ se \ \ O(f,h)>\dfrac{\beta_q}{n}. \end{cases}$$

Demonstração: Ver [Hf] pág 144-145.

□

Teorema 1.2. *Se* $O(f,h) < \dfrac{\beta_1}{n}$*, então* $I(f,h) = O(f,h)nn'$*. Além disso, se colocarmos* $n_0 = 1$*, então as condições abaixo são equivalentes:*

$$(1) \qquad \frac{\beta_q}{n} \leq O(f,h) < \frac{\beta_{q+1}}{n}, \ \ \textit{para algum} \ \ q = 1, \ldots, g.$$

$$(2) \qquad \frac{I(f,h)}{gr_y(h)} = \frac{v_q}{n_0 \ldots n_{q-1}} + \frac{nO(f,h) - \beta_q}{n_1 \ldots n_q}.$$

DEMONSTRAÇÃO: Vide [Hf] pág 146.

□

Corolário 1.1. *Seja* $q > 0$ *um número inteiro. Então,*

$$O(f,h) \leq \frac{\beta_q}{n} \ \ \textit{se, e somente se,} \ \ \frac{I(f,h)}{gr_y(h)} \leq \varepsilon_{q-1}\frac{v_q}{n}.$$

Além disso,

$$O(f,h) = \frac{\beta_q}{n} \ \ \textit{se, e somente se,} \ \ \frac{I(f,h)}{gr_y(h)} = \varepsilon_{q-1}\frac{v_q}{n}.$$

DEMONSTRAÇÃO: Primeiramente, observe que se $k, q \in \{1, \ldots, g\}$ com $k < q$, então

$$v_k \cdot \frac{\varepsilon_{k-1}}{n} < v_q \cdot \frac{\varepsilon_{q-1}}{n}.$$

Para provar este fato, basta aplicar indutivamente, a desigualdade (1.2.3) e o fato que $\dfrac{\varepsilon_i}{n} = \dfrac{1}{n_0 \ldots n_i}$, para todo $i \in \{1, \ldots, g\}$.

Note que, a equivalência envolvendo a igualdade é conseqüência imediata do Teorema 1.2. Desta forma, iremos nos restringir a equivalência envolvendo a desigualdade estrita.

Suponha que $O(f,h) < \dfrac{\beta_q}{n}$.

Se $q = 1$, então a desigualdade que queremos é conseqüência imediata do Teorema 1.2.

Considere agora, o caso que $q > 1$.

Seja $k \in \{1, \ldots, g\}$ tal que $\dfrac{\beta_k}{n} \leq O(f,h) < \dfrac{\beta_{k+1}}{n}$.

Note que $k < q$, pois, caso contrário, $\dfrac{\beta_q}{n} \leq \dfrac{\beta_k}{n} \leq O(f,h)$, o que contraria a hipótese.

Pelo Teorema 1.2,

$$\frac{I(f,h)}{gr_y(h)} = \frac{v_k}{n_0 \ldots n_{k-1}} + \frac{O(f,h)n - \beta_k}{n_1 \ldots n_k} < \frac{v_k}{n_0 \ldots n_{k-1}} + \frac{\beta_{k+1} - \beta_k}{n_1 \ldots n_k} = v_{k+1} \cdot \frac{\varepsilon_k}{n}.$$

Agora, pela observação inicial e pelo fato que $k < q$, segue que

$$\frac{I(f,h)}{gr_y(h)} < v_q \cdot \frac{\varepsilon_{q-1}}{n}.$$

Para finalizar, suponha que $\dfrac{I(f,h)}{gr_y(h)} < v_q \cdot \dfrac{\varepsilon_{q-1}}{n}$.

Se $O(f,h) < \dfrac{\beta_1}{n}$, então $O(f,h) < \dfrac{\beta_q}{n}$, já que $q \geq 1$.

Considere agora, o caso que $\dfrac{\beta_k}{n} \leq O(f,h) < \dfrac{\beta_{k+1}}{n}$, para algum $k \in \{1, \ldots, g\}$.

Pela desigualdade acima, basta provar que $k + 1 \leq q$.

Para isto, suponha que $k + 1 > q$, isto é, $q \leq k$. Pela observação inicial,

$$v_q \cdot \frac{\varepsilon_{q-1}}{n} \leq v_k \cdot \frac{\varepsilon_{k-1}}{n} = \frac{v_k}{n_0 \ldots n_{k-1}} \leq \frac{v_k}{n_0 \ldots n_{k-1}} + \frac{O(f,h)n - \beta_k}{n_1 \ldots n_k} = \frac{I(f,h)}{gr_y(h)},$$

o que contraria a hipótese.

$\square$

Capítulo 2

Raízes Aproximadas de Abhyankar-Moh

Neste capítulo iremos definir, de forma geral, o conceito de *raiz aproximada* de um polinômio e demonstrar algumas de suas propriedades que nos serão úteis no que segue.

2.1 Raízes Aproximadas

Seja A um anel comutativo com unidade, sem divisores de zero. Denotaremos por $A[Y]$ o anel dos polinômios com coeficientes em A na indeterminada Y. Se $P \in A[Y]\backslash\{0\}$, denotaremos por $gr(P)$ o seu grau. Dado um polinômio mônico $P \in A[Y]$ e um número natural r que divide $gr(P)$, nem sempre existirá uma raiz r-ésima de P em $A[Y]$; isto é, um $Q \in A[Y]$ tal que $Q^r = P$. O nosso objetivo nesta seção será o de estudar as propriedades dos polinômios $Q \in A[Y]$ para os quais $P - Q^r$ tem o menor grau possível, sob algumas condições.

Proposição 2.1. *Sejam $P \in A[Y]$ mônico e r um divisor natural de $gr(P)$ cuja imagem em A é invertível. Então existe um único polinômio mônico $Q \in A[Y]$ tal que:*

$$gr(P - Q^r) < gr(P) - \frac{gr(P)}{r} \tag{2.1.1}$$

Demonstração: Considere $P = Y^n + \alpha_1 Y^{n-1} + \cdots + \alpha_n$, com $\alpha_i \in A$. Se Q satisfaz a desigualdade acima, então $gr(Q) = \dfrac{n}{r}$. Sendo assim, considere

$Q = Y^{\frac{n}{r}} + a_1 Y^{\frac{n}{r}-1} + \cdots + a_{\frac{n}{r}}$. Note que Q satisfaz a desigualdade acima se, e somente se, os coeficientes de $Y^n, Y^{n-1}, \ldots, Y^{n-\frac{n}{r}}$ no polinômio $P - Q^r$ são todos nulos. Este último fato acontece se, e somente se,

$$\begin{cases} \alpha_1 = ra_1 \\ \alpha_2 = ra_2 + \begin{pmatrix} r \\ 2 \end{pmatrix} a_1^2 \\ \alpha_k = ra_k + \sum_{i_1+2i_2+\cdots+(k-1)i_{k-1}=k} c_{i_1\ldots i_{k-1}} a_1^{i_1} \ldots a_{k-1}^{i_{k-1}}, 1 \leq k \leq \frac{n}{r}, \end{cases} \tag{2.1.2}$$

onde, $c_{i_1\ldots i_{k-1}} = \begin{pmatrix} r \\ i_1 + \cdots + i_{k-1} \end{pmatrix} \dfrac{(i_1 + \cdots + i_{k-1})!}{i_1! \ldots i_{k-1}!}$.

□

Corolário 2.1. *Nas condições da Proposição 2.1, existe um único polinômio $Q \in A[Y]$ tal que $gr(P - Q^r)$ é o menor possível.*

Definição 2.1. O único polinômio da proposição anterior é denotado por $\sqrt[r]{P}$ e chamado de *r-raiz aproximada de P.*

Como conseqüência imediata da definição temos que $gr(\sqrt[r]{P}) = \dfrac{gr(P)}{r}$.

Observe que, dado $P = Y^n + \alpha_1 Y^{n-1} + \cdots + \alpha_n \in A[Y]$ e n invertível em A, então

$$\sqrt[n]{P} = Y + \frac{\alpha_1}{n}.$$

Proposição 2.2. *Se $r, s \in \mathbb{N} \setminus \{0\}$ têm imagens invertíveis em A e se o produto rs divide $gr(P)$, então $\sqrt[s]{\sqrt[r]{P}} = \sqrt[rs]{P}$.*

Demonstração: Ponhamos $Q = \sqrt[r]{P}$ e $R = \sqrt[s]{Q}$. Observe que

$$gr(R) = \frac{gr(Q)}{s} = \frac{gr(P)}{rs}$$

Considere $S = Q - R^s$. Note que:

(1) $gr(S) = gr(Q - R^s) < gr(Q) - \dfrac{gr(Q)}{s} = \dfrac{gr(P)}{r} - \dfrac{gr(P)}{rs}$,

onde a primeira desigualdade segue de $R = \sqrt[s]{Q}$ e a última igualdade de

$Q = \sqrt[r]{P}$.

Note agora que,

$$P - Q^r = P - (R^s + S)^r = P - R^{rs} - \textstyle\sum_{k=1}^{r} \begin{pmatrix} r \\ k \end{pmatrix} S^k R^{s(r-k)},$$

donde segue que

$$P - R^{rs} = P - Q^r + \sum_{k=1}^{r} \begin{pmatrix} r \\ k \end{pmatrix} S^k R^{s(r-k)}. \tag{2}$$

$$\begin{aligned} gr(S^k R^{s(r-k)}) &= k \cdot gr(S) + s(r-k)gr(R) \\ &< k \cdot \frac{gr(P)}{r} - k \cdot \frac{gr(P)}{rs} + s(r-k)\frac{gr(P)}{rs} \\ &= gr(P) - k \cdot \frac{gr(P)}{rs} \\ &\leq gr(P) - \frac{gr(P)}{rs}, \end{aligned} \tag{3}$$

onde a primeira desigualdade segue de (1), e a última desigualdade segue do fato de $k \geq 1$.

Desta forma,

$$\begin{aligned} gr(P - R^{rs}) &\leq \max\{gr(P - Q^r), gr(S^k R^{s(r-k)}), \ \text{com } 1 \leq k \leq r\} \\ &< \max\{gr(P) - \frac{gr(P)}{r}, gr(P) - \frac{gr(P)}{rs}\}, \end{aligned}$$

onde a primeira desigualdade segue de (2) e a última segue de (3) e do fato de $Q = \sqrt[r]{P}$.

Como

$$gr(P) - \frac{gr(P)}{r} \leq gr(P) - \frac{gr(P)}{rs},$$

temos que $gr(P - R^{rs}) < gr(P) - \dfrac{gr(P)}{rs}$.

□

Para prosseguirmos com a teoria geral de raízes aproximadas, precisaremos do seguinte fato algébrico básico.

Proposição 2.3. *Dados P e Q em $A[Y]$, mônicos com $gr(Q) < gr(P)$, existe uma única expansão do tipo:*

$$P = a_0 Q^s + a_1 Q^{s-1} + \cdots + a_s,$$

onde $a_0, a_1, \ldots, a_s \in A[Y]$, $a_i = 0$ ou $gr(a_i) < gr(Q)$ para todo $i \in \{0, \ldots, s\}$.

Demonstração: Segue por divisão sucessiva por Q, exatamente como na representação de um número natural numa determinada base.

$\square$

Definição 2.2. Dados P e Q em $A[Y]$ mônicos, denominamos por Q-*expansão* de P a única expansão da proposição anterior.

Proposição 2.4. *Com a mesma notação da proposição anterior temos que:*

(1) $gr(a_i Q^{s-i}) > gr(a_j Q^{s-j})$ *se* $i < j$;

(2) $s = \left[\dfrac{gr(P)}{gr(Q)}\right]$;

(3) $a_0 = 1 \Leftrightarrow gr(Q) | gr(P)$.
E neste último caso, se s for invertível em A, $a_1 = 0 \Leftrightarrow Q = \sqrt[s]{P}$

Demonstração: Iremos nos restringir à demonstração da segunda parte do ítem (3), já que, o restante é conseqüência imediata da definição.

Primeiramente, observe que

$$gr(a_2 Q^{s-2}) = gr(a_2) + (s-2)gr(Q) < gr(Q) + (s-2)gr(Q) = gr(P) - \frac{gr(P)}{s}.$$

Se $a_1 = 0$ e $a_0 = 1$, então

$$gr(P - Q^s) = gr(a_2 Q^{s-2}) < gr(P) - \frac{gr(P)}{s},$$

o que implica que $Q = \sqrt[s]{P}$.

Por outro lado, $gr(P - Q^s) < gr(P) - \dfrac{gr(P)}{s}$ implica que $a_1 = 0$; pois, caso contrário,

$$gr(P - Q^s) = gr(a_1 Q^{s-1}) = gr(a_1) + gr(P) - \frac{gr(P)}{s} \geq gr(P) - \frac{gr(P)}{s},$$

o que é uma contradição.

□

Definição 2.3. Dados $P, Q \in A[Y]$ mônicos com $gr(Q)$ dividindo $gr(P)$ e com $s = \dfrac{gr(P)}{gr(Q)}$ invertível em A, definimos o *operador de Tschirnhausen* τ_P do seguinte modo:

$$\tau_P(Q) = Q + \frac{a_1}{s},$$

onde a_1 é determinado pela Q-expansão de P.

Denotaremos por $\tau_P^j(Q)$ a iterada de τ_P j-vezes aplicada a Q.

Segue direto da definição que $gr(\tau_P^j(Q)) = gr(Q)$, para qualquer $j \in \mathbb{N}$.

Note que se $P = Y^n + a_1 Y^{n-1} + \cdots + a_n \in A[Y]$ com n invertível em A, pela observação após a Definição 2.1, temos que

$$\tau_P(Y) = Y + \frac{a_1}{n} = \sqrt[n]{P}.$$

A igualdade acima se generaliza, conforme podemos ver no seguinte resultado.

Proposição 2.5. *Sejam $P \in A[Y]$ mônico e r um número natural, invertível em A tal que $r | gr(P)$. Então para todo $Q \in A[Y]$ mônico com $gr(Q) = \dfrac{gr(P)}{r}$ temos que*

$$\tau_P^j(Q) = \sqrt[r]{P} \text{ se } j = \frac{gr(P)}{r}.$$

Demonstração: Sejam $Q \in A[Y]$ mônico com $gr(Q) = \dfrac{gr(P)}{r}$ e

$$P = Q^r + a_1 Q^{r-1} + \cdots + a_r$$

a Q-expansão de P.

Se $a_1 = 0$ então, $\tau_P(Q) = Q$ e pela proposição anterior Q é uma r-raiz aproximada de P. Logo, para $j = \frac{gr(P)}{r}$, temos que

$$\tau_P^j(Q) = Q = \sqrt[r]{P}.$$

Suponha agora que $a_1 \neq 0$. Considere,

$$P = (\tau_P^j(Q))^r + a_1^{(j)}(\tau_P^j(Q))^{r-1} + \cdots + a_r^{(j)} \text{ com } gr(a_i^{(j)}) < gr(Q),$$

a $\tau_P^j(Q)$-expansão de P.

Note que basta provarmos que $a_1^{(1)} = 0$ ou $gr(a_1^{(1)}) < gr(a_1)$.

De fato, por iteração, teremos, necessariamente, $a_1^{(j)} = 0$ para $j = \dfrac{gr(P)}{r}(\geq gr(a_1) + 1)$.

Provaremos agora que se $a_1^{(1)} \neq 0$ então, $gr(a_1^{(1)}) < gr(a_1)$.

Primeiramente, observe que

$$(1) \quad P - \tau_P(Q)^r = \sum_{k=2}^{r} a_k Q^{r-k} - \sum_{k=2}^{r} \binom{r}{k} \frac{a_1^k}{r^k} Q^{r-k}.$$

Com efeito, isto segue imediatamente das igualdades:

$$\begin{aligned}
P &= Q^r + a_1 Q^{r-1} + \sum_{k=2}^{r} a_k Q^{r-k} \\
&= Q^r + \binom{r}{1} \frac{a_1}{r} Q^{r-1} + \sum_{k=2}^{r} \binom{r}{k} \frac{a_1^k}{r^k} Q^{r-k} + \\
&\quad \sum_{k=2}^{r} a_k Q^{r-k} - \sum_{k=2}^{r} \binom{r}{k} \frac{a_1^k}{r^k} Q^{r-k} \\
&= (Q + \frac{a_1}{r})^r + \sum_{k=1}^{r} a_k Q^{r-k} - \sum_{k=2}^{r} \binom{r}{k} \frac{a_1^k}{r^k} Q^{r-k}.
\end{aligned}$$

(2) $gr(a_k Q^{r-k}) < (r-1)gr(Q)$, para $k \geq 2$.

Com efeito,

$$\begin{aligned} gr(a_k Q^{r-k}) &= gr(a_k) + gr(Q^{r-k}) \\ &< gr(Q) + (r-k)gr(Q) \\ &\leq gr(Q) + (r-2)gr(Q) \\ &= (r-1)gr(Q). \end{aligned}$$

(3) $gr(a_1^k Q^{(r-k)}) < k \cdot gr(Q) + (r-k)gr(Q) = r \cdot gr(Q)$.

Para cada $k \in \{2, \ldots, r\}$ vamos escrever a $\tau_P(Q)$-expansão de $a_k Q^{r-k}$ e de $a_1^k Q^{r-k}$.

$$a_k Q^{r-k} \quad = \quad d_0^{(k)}(\tau_P(Q))^{s_k} + d_1^{(k)}(\tau_P(Q))^{s_k-1} + \cdots + d_{s_k}^{(k)}$$

e

$$a_1^k Q^{r-k} \quad = \quad c_0^{(k)}(\tau_P(Q))^{t_k} + c_1^{(k)}(\tau_P(Q))^{t_k-1} + \cdots + c_{t_k}^{(k)},$$

onde

$$s_k = \left[\frac{gr(a_k Q^{r-k})}{gr(\tau_P(Q))}\right], \quad t_k = \left[\frac{gr(a_1^k Q^{r-k})}{gr(\tau_P(Q))}\right], \quad gr(d_i^{(k)}) < \frac{gr(P)}{r} \quad \text{e} \quad gr(c_j^{(k)}) < \frac{gr(P)}{r}.$$

Note que, por (2) e (3) segue que

$$s_k \leq r-2 \quad \text{e} \quad t_k \leq r-1.$$

Portanto, por (1) e pela unicidade da $\tau_P(Q)$-expansão de P, temos que

$$a_1^{(1)} = -\sum_{t_k = r-1} \binom{r}{k} \frac{c_0^{(k)}}{r^k}.$$

Desta forma, basta provar que $gr(c_0^{(k)}) < gr(a_1)$, para todo $k \in \{2, \ldots, r\}$ tal que $t_k = r-1$.

Para isto, observe que, como $gr(a_1^k Q^{r-k}) = gr(c_0^{(k)} \tau_P(Q)^{t_k})$, temos que

$$gr(c_0^{(k)}) = gr(a_1^k Q^{r-k}) \ - \ (r-1)gr(\tau_P(Q)),$$

para todo $k \in \{2, \ldots, r\}$ tal que $t_k = r-1$.

Logo,

$$gr(c_0^{(k)}) = k \cdot gr(a_1) \ + \ gr(Q) \ - \ k \cdot gr(Q).$$

Agora, como $gr(a_1) < gr(Q)$ e $k \geq 2$, temos que

$$(k-2) \cdot gr(a_1) \leq (k-2) \cdot gr(Q);$$

isto é,

$$k \cdot gr(a_1) + gr(Q) - k \cdot gr(Q) \leq 2gr(a_1) - gr(Q) < 2gr(a_1) - gr(a_1) = gr(a_1),$$

donde concluímos que $gr(c_0^{(k)}) < gr(a_1)$.

□

Lema 2.1. *Seja $P = Y^n + \alpha_1 Y^{n-1} + \cdots + \alpha_n \in A[X_1, \ldots, X_m][Y]$ com grau total n e seja r um divisor de n invertível em A. Então, o grau total da r-raiz aproximada de P é $\frac{n}{r}$.*

DEMONSTRAÇÃO: Já vimos que a r-raiz aproximada de P é dada por

$$Y^{\frac{n}{r}} + a_1 Y^{\frac{n}{r}-1} + \cdots + a_{\frac{n}{r}},$$

com

$$\alpha_k = r a_k + \sum_{i_1 + 2i_2 + \cdots + (k-1)i_{k-1} = k} c_{i_1 \ldots i_{k-1}} a_1^{i_1} \ldots a_{k-1}^{i_{k-1}},$$

para todo $1 \leq k \leq \frac{n}{r}$, onde

$$c_{i_1 \ldots i_{k-1}} = \binom{r}{i_1 + \cdots + i_{k-1}} \frac{(i_1 + \cdots + i_{k-1})!}{i_1! \ldots i_{k-1}!}.$$

Para provar o lema, basta provar que $gr(a_k) \leq k$, para todo k. Faremos isto por indução em k.

Para $k = 1$, temos que $\alpha_1 = r a_1$; logo $gr(a_1) = gr(\alpha_1) \leq 1$.

Suponha que o resultado seja verdadeiro até $k - 1 \in \{1, \ldots, \frac{n}{r} - 1\}$. Pela fórmula acima, segue que,

$$gr(a_k) \leq \max\{gr(\alpha_k), gr(a_1^{i_1} \ldots a_{k-1}^{i_{k-1}}), \ \ i_1 + 2i_2 + \cdots + (k-1)i_{k-1} = k\}.$$

Note que $gr(\alpha_k) \leq k$ e que

$$\begin{aligned} gr(a_1^{i_1} \dots a_{k-1}^{i_{k-1}}) &= i_1 gr(a_1) + \cdots + i_{k-1} gr(a_{k-1}) \\ &\leq i_1 + 2i_2 + \cdots + (k-1)i_{k-1} \\ &= k, \end{aligned}$$

pela hipótese de indução. Portanto, $gr(a_k) \leq k$.

□

Um argumento idêntico ao usado acima permite provar o seguinte resultado:

Lema 2.2. *Sejam $P = Y^n + \alpha_1 Y^{n-1} + \cdots + \alpha_n \in A[[X_1, \dots, X_m]][Y]$ com $mult(\alpha_i) \geq i$ (respectivamente, $mult(\alpha_i) \geq 1$) para todo $i \in \{1, \dots, n\}$ e r divisor de n invertível em A. Então, se $Q = Y^{\frac{n}{r}} + a_1 Y^{\frac{n}{r}-1} + \cdots + a_{\frac{n}{r}}$ é uma r-raiz aproximada de P , tem-se que $mult(a_i) \geq i$ (respectivamente, $mult(a_i) \geq 1$) para todo $i \in \{1, \dots, \dfrac{n}{r}\}$.*

Daí segue imediatamente o seguinte corolário:

Corolário 2.2. *Sejam $P = Y^n + \alpha_1 Y^{n-1} + \cdots + \alpha_n \in A[X_1, \dots, X_m][Y]$ com α_i homogêneo de grau i, $\forall\ i \in \{1, \dots, n\}$ e r divisor de n invertível em A. Se $Q = Y^{\frac{n}{r}} + a_1 Y^{\frac{n}{r}-1} + \cdots + a_{\frac{n}{r}}$ é uma r-raiz aproximada de P , então a_i é homogêneo de grau i, $\forall\ i \in \{1, \dots, \dfrac{n}{r}\}$.*

2.2 Aplicação às Curvas Algebróides

A partir de agora, iremos considerar

$$f = Y^n + \alpha_1(X) Y^{n-1} + \cdots + \alpha_n(X) \in \mathbb{C}[[X]][Y]$$

mônico, irredutível com $\alpha_1(0) = \cdots = \alpha_n(0) = 0$.

O semigrupo do ramo (f) será denotado por $S(f) = \langle v_0, \dots, v_g \rangle$, onde g é o gênero de $S(f)$.

Os expoentes característicos de (f) serão denotados por $\beta_0, \ldots, \beta_g$ e os inteiros $\varepsilon_1, \ldots, \varepsilon_g$ serão como definidos no capítulo 1.

Observe que, dada a expressão de f, tem-se, pelo fato de $\alpha_i(0) = 0$ para todo i, que

$$I(f, X) = I(Y^n, X) = n,$$

onde $I(f, h)$ representa a multiplicidade de interseção das curvas f e h no ponto $(0, 0)$.

Se $h \in \mathbb{C}[[X]][Y]$, denotaremos por $gr(h)$ o grau de h em Y e só iremos distinguí-lo quando houver possibilidade de confusão.

Definição 2.4. Um polinômio $q_k \in \mathbb{C}[[X]][Y]$ será dito *k-semiraiz* de f quando q_k for mônico, $gr(q_k) = \dfrac{n}{\varepsilon_k}$ e $I(f, q_k) = v_{k+1}$.

Observe que, pelo Lema 1.1, k-semiraízes existem.

Vamos, a seguir, provar um lema técnico que será útil na demonstração de alguns resultados posteriores.

Lema 2.3. *Seja q uma k-semiraiz de f, e sejam ℓ e h polinômios em $\mathbb{C}[[X]][Y]$ com $gr(\ell), gr(h) < \dfrac{n}{\varepsilon_k}$. Então,*

$$I(f, \ell q^i) \neq I(f, hq^j)$$

para todo $i, j \in \{0, \ldots, n_{k+1}\}$, com $i \neq j$, onde $n_{k+1} = \dfrac{\varepsilon_k}{\varepsilon_{k+1}}$.

Demonstração: Primeiramente, observe que, pelo Teorema 1.1, se $gr(\ell), gr(h) < \dfrac{n}{\varepsilon_k}$, então $I(f, \ell), I(f, h) \in \langle v_0, \ldots, v_k \rangle$. Logo $I(f, \ell)$ e $I(f, h)$ são divisíveis por ε_k.

Agora, se existissem $0 \leq i < j \leq n_{k+1}$ tais que $I(f, \ell q^i) = I(f, hq^j)$, então

$$(j - i)v_{k+1} = (j - i)I(f, q) = I(f, \ell) - I(f, h)$$

seria divisível por ε_k.

Portanto, $(j-i)v_{k+1} = \lambda\varepsilon_k$ e, conseqüentemente,

$$(j-i)\frac{v_{k+1}}{\varepsilon_{k+1}} = \lambda\frac{\varepsilon_k}{\varepsilon_{k+1}} = \lambda n_{k+1}.$$

Como $\varepsilon_{k+1} = mdc(v_{k+1}, \varepsilon_k)$, segue que $\dfrac{v_{k+1}}{\varepsilon_{k+1}}$ e n_{k+1} são relativamente primos. Desta forma, $n_{k+1}|(j-i)$, o que é um absurdo, pois $0 < j-i < n_{k+1}$.

□

Proposição 2.6. *Seja* $\ell \in \mathbb{C}[[X]][Y]$ *mônico com* $gr(\ell) = \dfrac{n}{\varepsilon_k}$ *e* $I(f,\ell) > n_k v_k$. *Se* h *é uma* $(k-1)$*-semiraiz de* f *então* $\tau_\ell(h)$ *é uma* $(k-1)$*-semiraiz de* f.

Demonstração: Por hipótese, $gr(\ell) = \dfrac{n}{\varepsilon_k}$ e $gr(h) = \dfrac{n}{\varepsilon_{k-1}}$. Assim, podemos escrever a h-expansão de ℓ como

$$\ell = h^{n_k} + a_1 h^{n_k - 1} + \cdots + a_{n_k},$$

onde $gr(a_i) < gr(h)$. Conseqüentemente, $\tau_\ell(h) = h + \dfrac{a_1}{n_k}$.

Observe que basta provar que $I(f,h) < I(f,a_1)$.

De fato, caso isto ocorresse, teríamos que $gr(\tau_\ell(h)) = \dfrac{n}{\varepsilon_{k-1}}$ e

$$I(f,\tau_\ell(h)) = min\{I(f,h), I(f,a_1)\} = I(f,h) = v_k.$$

Vamos agora, provar que $I(f,h) < I(f,a_1)$.

Pelo lema anterior, temos que $I(f, a_j h^{n_k-j}) \neq I(f, a_i h^{n_k-i})$ para todo $i,j \in \{1,\ldots,n_k\}$, com $i \neq j$.

Assim,

$$I(f,\ell - h^{n_k}) = \min_{1\le i\le n_k}\{I(f, a_i h^{n_k-i})\} \le I(f, a_1 h^{n_k-1}).$$

Por hipótese, $I(f,\ell) > n_k v_k = I(f,h^{n_k})$, logo $I(f,\ell - h^{n_k}) = I(f,h^{n_k})$.

Portanto, concluímos destes dois fatos que

$$n_k I(f,h) \leq I(f, a_1 h^{n_k-1}) = I(f,a_1) + (n_k - 1)I(f,h),$$

donde $I(f,h) \leq I(f,a_1)$.

Por outro lado, como $gr(a_1) < gr(h) = \dfrac{n}{\varepsilon_{k-1}}$, segue do Teorema 1.1 que $I(f,a_1) \in \langle v_0, \ldots, v_{k-1}\rangle$.

Então, para concluir que $I(f,a_1) \neq I(f,h)$, basta observar que $I(f,h) = v_k \notin \langle v_0, \ldots, v_{k-1}\rangle$. Logo, $I(f,h) < I(f,a_1)$.

□

Como conseqüência direta desta proposição e do fato de $S(f)$ ser fortemente crescente temos o seguinte corolário.

Corolário 2.3. *Se ℓ é uma k-semiraiz de f e h é uma $(k-1)$-semiraiz de f então $\tau_\ell(h)$ é uma $(k-1)$-semiraiz de f.*

Proposição 2.7. *Seja $\ell \in \mathbb{C}[[X]][Y]$ mônico com $gr(\ell) = \dfrac{n}{\varepsilon_k}$. Suponha que $I(f,\ell) > n_k v_k$. Então, $I(f, \sqrt[n_k]{\ell}) = v_k$.*

Demonstração: Considere $h \in \mathbb{C}[[X]][Y]$ uma $(k-1)$-semiraiz de f. Lembre que h existe, vide Lema 1.1 e definição do v_k.

Note que $gr(\tau_\ell(h)) = gr(h) = \dfrac{n}{\varepsilon_{k-1}}$. Logo, pela proposição anterior, $I(f, \tau_\ell(h)) = v_k$.

Indutivamente, concluímos que $I(f, \tau_\ell^i(h)) = v_k$ para todo $i \in \mathbb{N}$.

Em particular, temos pela Proposição 2.5 que

$$I(f, \sqrt[n_k]{\ell}) = I(f, \tau_\ell^{(\frac{gr(\ell)}{n_k})}(h)) = v_k.$$

□

2.2.1 Uma Importante Caracterização

Nesta seção apresentaremos o teorema mais importante deste capítulo que é uma generalização de um resultado que caracteriza algumas das raízes aproximadas de uma curva algebróide e é devido a J.Gwoździewicz e A.Ploski [GP].

Lema 2.4. *Seja $h \in \mathbb{C}[[X]][Y]$ mônico e irredutível. Se $\dfrac{I(f,h)}{gr(h)} > \dfrac{\varepsilon_{k-2}v_{k-1}}{n}$, com $1 < k \leq g+1$, então $gr(h) \equiv 0 \ mod \dfrac{n}{\varepsilon_{k-1}}$.*

Além disso, se $gr(h) = \dfrac{n}{\varepsilon_{k-1}}$, então

$$S(h) = \left\langle \frac{v_0}{\varepsilon_{k-1}}, \ldots, \frac{v_{k-1}}{\varepsilon_{k-1}} \right\rangle$$

e os expoentes característicos de (h) são $\dfrac{\beta_0}{\varepsilon_{k-1}}, \ldots, \dfrac{\beta_{k-1}}{\varepsilon_{k-1}}$.

Demonstração: Sejam $\beta'_0, \ldots, \beta'_{g'}$ os expoentes característicos de (h) $(\beta'_0 = gr(h) := n')$.

Note que, pelo Corolário 1.1, $\dfrac{I(f,h)}{gr(h)} > \dfrac{\varepsilon_{k-2}v_{k-1}}{n}$ implica que $O(f,h) > \dfrac{\beta_{k-1}}{n}$.

Desta forma, pela Proposição 1.1, segue que

$$\frac{\beta_i}{n} = \frac{\beta'_i}{n'} \text{ para todo } i = 0, \ldots, k-1 \text{ e } k-1 \leq g'.$$

Como $\varepsilon_{k-1} = mdc(\beta_0, \ldots, \beta_{k-1})$, temos que existem $a_0, \ldots, a_{k-1} \in \mathbb{Z}$ tais que $\varepsilon_{k-1} = \displaystyle\sum_{i=0}^{k-1} a_i\beta_i$. Portanto,

$$n'\varepsilon_{k-1} = \sum_{i=0}^{k-1}(a_i\beta'_i n),$$

o que implica que, $gr(h) = n' \equiv 0 \text{ mod} \dfrac{n}{\varepsilon_{k-1}}$.

Por outro lado, se $n' = \dfrac{n}{\varepsilon_{k-1}}$, então, novamente pela Proposição 1.1, segue que $v'_i = \dfrac{v_i n'}{n} = \dfrac{v_i}{\varepsilon_{k-1}}$ para todo $i = 0, \dots, k-1$. Conseqüentemente, $mdc(v'_0, \dots, v'_{k-1}) = 1$.

Assim, $g' = k-1$ e, portanto, $S(h) = \left\langle \dfrac{v_0}{\varepsilon_{k-1}}, \dots, \dfrac{v_{k-1}}{\varepsilon_{k-1}} \right\rangle$.

$\square$

Teorema 2.1. *Seja $h \in \mathbb{C}[[X]][Y]$ mônico tal que $gr(h) = \dfrac{n}{\varepsilon_{k-1}}$. Então, $I(f,h) \leq v_k$ (onde $v_{g+1} = \infty$). Se $I(f,h) > n_{k-1}v_{k-1}$, então h é irredutível,*

$$S(h) = \left\langle \frac{v_0}{\varepsilon_{k-1}}, \dots, \frac{v_{k-1}}{\varepsilon_{k-1}} \right\rangle$$

e os expoentes característicos de (h) são $\dfrac{\beta_0}{\varepsilon_{k-1}}, \dots, \dfrac{\beta_{k-1}}{\varepsilon_{k-1}}$.

Demonstração: (1^o) Escreva $h = h_1 \dots h_s$ com $h_i \in \mathbb{C}[[X]][Y]$ irredutíveis.

Se $k = g+1$ então $v_k = \infty$, logo, $I(f,h) \leq v_k$.

Se $k \leq g$ então

$$\frac{I(f,h_i)}{gr(h_i)} \leq \frac{\varepsilon_{k-1}v_k}{n}, \tag{1}$$

para todo $i = 1, \dots, s$.

De fato, se para algum $i \in \{1, \dots, s\}$ tivéssemos $\dfrac{I(f,h_i)}{gr(h_i)} > \dfrac{\varepsilon_{k-1}v_k}{n}$ então, pelo lema anterior,

$$I(f,h_i) \equiv 0 \ \ mod \frac{n}{\varepsilon_k}. \tag{2}$$

Como h é mônico e h_i é irredutível temos que $gr(h_i) \neq 0$. Então, por (2), segue que

$$gr(h_i) \geq \frac{n}{\varepsilon_k} > \frac{n}{\varepsilon_{k-1}},$$

já que, $\varepsilon_{k-1} > \varepsilon_k$.

Mas esta desigualdade é um absurdo, pois, $gr(h_i) \leq gr(h) = \dfrac{n}{\varepsilon_{k-1}}$.

Portanto,

$$I(f,h) = \sum_{i=1}^{s} I(f,h_i) \leq \sum_{i=1}^{s} \frac{\varepsilon_{k-1}v_k}{n} \cdot gr(h_i) \leq \frac{\varepsilon_{k-1}v_k}{n} \cdot gr(h) = v_k,$$

onde a primeira desigualdade segue de (1).

(2^o) Suponha que $I(f,h) > n_{k-1}v_{k-1}$.

Afirmamos, que existe algum $j \in \{1,\ldots,s\}$ tal que $\dfrac{I(f,h_j)}{gr(h_j)} > \dfrac{\varepsilon_{k-2}v_{k-1}}{n}$.

Caso contrário, se $\dfrac{I(f,h_i)}{gr(h_i)} \leq \dfrac{\varepsilon_{k-2}v_{k-1}}{n}$, para todo $i = 1,\ldots,s$, teríamos que

$$I(f,h) = \sum_{i=1}^{s} I(f,h_i) \leq \sum_{i=1}^{s} \frac{\varepsilon_{k-2}v_{k-1}}{n} \cdot gr(h_i) = \frac{\varepsilon_{k-2}v_{k-1}}{n}.\frac{n}{\varepsilon_{k-1}} = n_{k-1}v_{k-1},$$

o que é uma contradição.

Pelo lema anterior, $gr(h_j) \equiv 0 \bmod \dfrac{n}{\varepsilon_{k-1}}$, para o valor de j cuja existência provamos acima.

Como $gr(h_j) \leq gr(h) = \dfrac{n}{\varepsilon_{k-1}}$ e $gr(h_j) \neq 0$ segue que

$$gr(h_j) = gr(h) = \frac{n}{\varepsilon_{k-1}},$$

logo $gr(h_i) = 0$ para todo $i \neq j$; isto é, h_i é invertível em $\mathbb{C}[[X]][Y]$ para todo $i \neq j$.

Concluímos então que

(a) $\quad h = h_j p, \quad$ onde p é invertível em $\mathbb{C}[[X]][Y]$. Logo h é irredutível, já que, h_j o é.

(b) Como, para todo $q \in \mathbb{C}[[X]][Y] \setminus \langle h \rangle$, $I(q,h) = I(q, h_j p) = I(q, h_j)$ (pois p é invertível), segue que

$$S(h) = S(h_j) = \left\langle \frac{v_0}{\varepsilon_{k-1}}, \ldots, \frac{v_{k-1}}{\varepsilon_{k-1}} \right\rangle,$$

onde a segunda igualdade segue do lema anterior.

(c) Usando a equação (1.2.2) recursivamente, segue, da última igualdade acima, que os expoentes característicos de h (que são os mesmos que os de h_j) são $\dfrac{\beta_0}{\varepsilon_{k-1}}, \ldots, \dfrac{\beta_{k-1}}{\varepsilon_{k-1}}$.

□

2.2.2 Conseqüências desta Caracterização

Primeiramente, iremos exibir uma importante caracterização de algumas raízes aproximadas de uma curva algebróide.

Definição 2.5. $f_k := \sqrt[\varepsilon_k]{f}$, serão chamadas de *raízes aproximadas características*, ou simplesmente de, *raízes características* de f.

Teorema 2.2. *Seja $f \in \mathbb{C}[[X]][Y]$ um pseudo-polinômio, mônico, irredutível com $gr(f) = n$. As seguintes condições são satisfeitas:*

(1) $gr(f_k) = \dfrac{n}{\varepsilon_k}$ *e* $I(f, f_k) = v_{k+1}$ *(isto é, f_k é uma k-semiraiz de f).*

(2) *f_k é irredutível, $S(f_k) = \left\langle \dfrac{v_0}{\varepsilon_k}, \ldots, \dfrac{v_k}{\varepsilon_k} \right\rangle$ e os expoentes característicos de (f_k) são $\dfrac{\beta_0}{\varepsilon_k}, \ldots, \dfrac{\beta_k}{\varepsilon_k}$.*

Demonstração: (1) Pela definição de f_k segue que $gr(f_k) = \dfrac{n}{\varepsilon_k}$.

Provaremos agora, que $I(f, f_k) = v_{k+1}$, por descida em k.

Se $k = g$ então $\varepsilon_k = 1$; logo, $f_k = f$ e, conseqüentemente, $I(f, f_k) = \infty = v_{k+1}$.

Suponha que $I(f, f_k) = v_{k+1}$, para algum, $1 < k \leq g$. Pelo fato da seqüência $S(f)$ ser fortemente crescente temos que

$$I(f, f_k) = v_{k+1} > n_k v_k.$$

Logo, pela Proposição 2.7, $I(f, \sqrt[n_k]{f_k}) = v_k$. Como

$$\sqrt[n_k]{f_k} = \sqrt[n_k]{\sqrt[\varepsilon_k]{f}} = \sqrt[n_k \varepsilon_k]{f} = \sqrt[\varepsilon_{k-1}]{f} = f_{k-1},$$

segue que $I(f, f_{k-1}) = v_k$.

(2) Este ítem é conseqüência direta do Teorema 2.1, levando em conta o fato de que $gr(f_k) = \dfrac{n}{\varepsilon_k}$ e $I(f, f_k) = v_{k+1} > n_k v_k$.

$\square$

Corolário 2.4. *Para todo* $k \in \{0, \ldots, g\}$, $O(f, f_k) = \dfrac{\beta_{k+1}}{n}$.

Demonstração: Pelo teorema anterior,

$$\frac{I(f, f_k)}{gr(f_k)} = \frac{v_{k+1}}{\frac{n}{\varepsilon_k}} = \frac{v_{k+1}}{n_0 \cdots n_k} = \frac{v_{k+1}}{n_0 \cdots n_k} + \frac{n\frac{\beta_{k+1}}{n} - \beta_{k+1}}{n_1 \cdots n_{k+1}}.$$

Então, pelo Teorema 1.2, $O(f, f_k) = \dfrac{\beta_{k+1}}{n}$.

$\square$

Note que podemos calcular recursivamente os expoentes característicos dos (f_k) como se segue:

(1) Ponha $f_0 = Y + \dfrac{a_1(X)}{n}$ e defina $\varepsilon_0 = n$;

(2) Suponha que f_k foi calculado.

Ponha $v_{k+1} = I(f, f_k)$. Se f_k foi calculado conhecemos ε_k.

Ponha $\varepsilon_{k+1} = mdc(\varepsilon_k, v_{k+1})$. Se $\varepsilon_{k+1} = 1$ pare.

Caso contrário;

(3) Calcule $f_{k+1} = \sqrt[\varepsilon_{k+1}]{f}$ e repita o item (2).

Calculado $S(f)$, podemos calcular os expoentes característicos de (f) pela equação (1.2.2). A partir daí, basta usar o item (2) do Teorema 2.2, para calcular os expoentes característicos de (f_k).

Corolário 2.5. *Todo $h \in \mathbb{C}[[X]][Y]$ pode ser escrito de forma única como uma soma finita*

$$h = \sum_{i_0,\ldots,i_g} \alpha_{i_0,\ldots,i_g} f_0^{i_0} \cdots f_g^{i_g},$$

onde $0 \leq i_g \leq \left[\dfrac{gr(h)}{gr(f)}\right]$, $0 \leq i_k < n_{k+1}$ para todo $0 \leq k \leq g-1$ e os coeficientes $\alpha_{i_0\ldots i_g}$ são elementos de $\mathbb{C}[[X]]$. Além disso,

(1) *O grau em Y de quaisquer dois elementos distintos desta soma são distintos.*

(2) *As multiplicidades em T dos termos*

$$\alpha_{i_0\ldots i_g}(T^n) f_0(T^n, \varphi(T))^{i_0} \cdots f_{g-1}(T^n, \varphi(T))^{i_{g-1}}$$

são todas distintos, onde $(T^n, \varphi(T))$ é uma parametrização de Puiseux para (f).

DEMONSTRAÇÃO: Provaremos uma formulação mais geral deste corolário, ou seja, com q_k k-semiraiz qualquer de f ao invés de f_k.

Considere a q_g-expansão de h:

$$h = \sum_{0 \leq i_g \leq \left[\frac{gr(h)}{gr(q_g)}\right]} \alpha_{i_g} q_g^{i_g},$$

onde $\alpha_{i_g} \in \mathbb{C}[[X]][Y]$ e $gr(\alpha_{i_g}) < gr(q_g) = n$.

Considere agora, a (q_{g-1})-expansão de α_{i_g}, para cada i_g:

$$\alpha_{i_g} = \sum_{0 \leq i_{g,g-1} \leq \left[\frac{gr(\alpha_{i_g})}{gr(q_{g-1})}\right]} \alpha_{i_{g,g-1} i_g} q_{g-1}^{i_{g,g-1}},$$

onde $\alpha_{i_{g,g-1} i_g} \in \mathbb{C}[[X]][Y]$ e $gr(\alpha_{i_{g,g-1} i_g}) < gr(q_{g-1}) = \dfrac{n}{\varepsilon_{g-1}}$.

Note que $gr(\alpha_{i_g}) < \dfrac{n}{\varepsilon_g}$ e $gr(q_{g-1}) = \dfrac{n}{\varepsilon_{g-1}}$ implicam que,

$$\left[\frac{gr(\alpha_{i_g})}{gr(q_{g-1})}\right] < \frac{\varepsilon_{g-1}}{\varepsilon_g} = n_g.$$

Assim,

$$h = \sum_{i_{g,g-1}, i_g} \alpha_{i_{g,g-1} i_g} q_{g-1}^{i_{g,g-1}} q_g^{i_g}$$

com $0 \leq i_g \leq \left[\dfrac{gr(h)}{gr(q_g)}\right]$ e $0 \leq i_{g,g-1} < n_g$.

Com o objetivo de aliviar as notações, iremos cometer um certo abuso ao identificarmos $i_{g,g-1}$ com i_{g-1}. Da mesma forma, indentificaremos os índices que aparecem no decorrer desta construção.

Procedendo de forma análoga obtemos,

$$h = \sum_{i_0, \ldots, i_g} \alpha_{i_0 \ldots i_g} q_0^{i_0} \ldots q_g^{i_g}$$

com $gr(\alpha_{i_0\ldots i_g}) < gr(q_0) = \dfrac{n}{\varepsilon_0} = 1$ (isto é, $\alpha_{i_0\ldots i_g} \in \mathbb{C}[[X]]$), $0 \leq i_j < n_{j+1}$ para todo $j \in \{0, \ldots, g-1\}$ e $0 \leq i_g \leq \left[\dfrac{gr(h)}{gr(q_g)}\right] = \left[\dfrac{gr(h)}{gr(f)}\right]$.

Vamos provar agora que para esta decomposição vale (1).

Caso contrário, se existissem $(i_0, \ldots, i_g) \neq (j_0, \ldots, j_g)$ tais que $gr(\alpha_{i_0\ldots i_g} q_0^{i_0} \ldots q_g^{i_g}) = gr(\alpha_{j_0\ldots j_g} q_0^{j_0} \ldots q_g^{j_g})$, teríamos que,

$$\sum_{l=0}^{g} i_l \frac{n}{\varepsilon_l} = \sum_{l=0}^{g} i_l gr(q_l) = \sum_{l=0}^{g} j_l gr(q_l) = \sum_{l=0}^{g} j_l \frac{n}{\varepsilon_l}$$

Defina $D = \{\ k \in \{0, \ldots, g\}\ ;\ i_k \neq j_k\}$ e tome $p = max\{k \in D\}$. Sem perda de generalidade, podemos supor que $i_p < j_p$.

Pela igualdade acima, segue que

$$\sum_{k \in D \setminus \{p\}} (i_k - j_k) \frac{n}{\varepsilon_k} = (j_p - i_p) \frac{n}{\varepsilon_p} \geq \frac{n}{\varepsilon_p},$$

pois $(j_p - i_p) \geq 1$.

Como $i_k, j_k < n_{k+1}$, para todo $k = 0, \ldots, g$ temos que

$$0 < |i_k - j_k| \leq n_{k+1} - 1.$$

Assim,

$$\frac{n}{\varepsilon_p} \leq \sum_{k \in D \setminus \{p\}} (i_k - j_k) \frac{n}{\varepsilon_k} \leq \sum_{k \in D \setminus \{p\}} |i_k - j_k| \frac{n}{\varepsilon_k} = \sum_{k=0}^{p-1} |i_k - j_k| \frac{n}{\varepsilon_k}$$

$$\leq \sum_{k=0}^{p-1} (n_{k+1} - 1) \frac{n}{\varepsilon_k} = \sum_{k=0}^{p-1} \left(\frac{\varepsilon_k}{\varepsilon_{k+1}} - 1\right) \frac{n}{\varepsilon_k} = \sum_{k=0}^{p-1} \left(\frac{n}{\varepsilon_{k+1}} - \frac{n}{\varepsilon_k}\right) = \frac{n}{\varepsilon_p} - 1,$$

o que é um absurdo.

Vamos agora provar a unicidade da escrita.

Basta observar que dado $\sum_{i_0,\ldots,i_g} \gamma_{i_0\ldots i_g} q_0^{i_0} \ldots q_g^{i_g} = 0$, temos por (1) que os graus em Y dos termos deste somatório são distintos. Logo, cada um destes termos é zero, isto é, $\gamma_{i_0\ldots i_g} = 0$ (já que $q_0, \ldots, q_g$ são não nulos).

Finalmente, provaremos (2).

Para cada $k = 0, \ldots, g$,

$$v_T(q_k(T^n, \varphi(T))) = I(f, q_k) = v_{k+1}.$$

Logo,

$$v_T\left(\alpha_{i_0\ldots i_g}(T^n) q_0(T^n, \varphi(T))^{i_0} \ldots q_{g-1}(T^n, \varphi(T))^{i_{g-1}}\right)$$

é igual a

$$\begin{aligned} v_T(\alpha_{i_0\ldots i_g}(T^n)) + \sum_{k=0}^{g-1} i_k v_T(q_k(T^n, \varphi(T))) &= v_X(\alpha_{i_0\ldots i_g})n + \sum_{k=0}^{g-1} i_k v_{k+1} \\ &= \sum_{k=-1}^{g-1} i_k v_{k+1}, \end{aligned}$$

onde estamos definindo $i_{-1} = v_X(\alpha_{i_0\ldots i_g})$.

Suponha que $\sum_{k=-1}^{g-1} i_k v_{k+1} = \sum_{k=-1}^{g-1} j_k v_{k+1}$ com $(i_{-1}, \ldots, i_{g-1})$ diferente de $(j_{-1}, \ldots, j_{g-1})$.

Defina agora $D = \{\ k \in \{-1, \ldots, g-1\}\ ;\ i_k \neq j_k\}$ e tome p o maior elemento de D. Sem perda de generalidade, podemos supor que $i_p < j_p$.

Observe que, se apenas $i_{-1} \neq j_{-1}$, então

$$\sum_{k=-1}^{g-1} i_k v_{k+1} \neq \sum_{k=-1}^{g-1} j_k v_{k+1}.$$

Conseqüentemente, $p > -1$, e, pela igualdade acima, segue que

$$(j_p - i_p)v_{p+1} = \sum_{k \in D\setminus\{p\}} (i_k v_{k+1} - j_k v_{k+1}) = \sum_{k=-1}^{p-1} (i_k v_{k+1} - j_k v_{k+1}).$$

Agora, como $\varepsilon_p = mdc(v_0, \ldots, v_p)$ temos, pela igualdade acima, que $\varepsilon_p | (j_p - i_p)v_{p+1}$. Conseqüentemente,

$$n_{p+1}\lambda = \frac{\varepsilon_p}{\varepsilon_{p+1}}\lambda = (j_p - i_p)\frac{v_{p+1}}{\varepsilon_{p+1}},$$

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

Como $\varepsilon_{p+1} = mdc(\varepsilon_p, v_{p+1})$ segue que n_{p+1} e $\dfrac{v_{p+1}}{\varepsilon_{p+1}}$ são relativamente primos. Portanto, pela última igualdade, $n_{p+1} | (j_p - i_p)$ o que contradiz o fato de $0 < j_p - i_p < n_{p+1}$.

$\square$

Capítulo 3

O Teorema Principal

Neste capítulo, iremos apresentar uma importante aplicação da teoria desenvolvida no capítulo dois. Demonstraremos o famoso Teorema do Mergulho da reta devido a S.S. Abhyankar e T.T. Moh. A demonstração original bem como as subseqüentes são bastante complicadas. A demonstração que apresentaremos, devida a Hai-chao Chang e Lih-chung Wang [CW], é uma simplificação substancial da prova e só ultiliza propriedades de índice de interseção juntamente com as noções sobre raízes aproximadas desenvolvidas anteriormente.

Na verdade, existem dois enunciados equivalentes para o teorema, a saber,

Teorema 3.1. (Mergulho da Reta) *Se* $f(x,y) = 0$ *define um mergulho da reta afim* $\mathbb{C}$ *em* $\mathbb{C}^2$*, então existe um polinômio* $g(x,y) \in \mathbb{C}[x,y]$ *tal que a aplicação,*

$$\begin{array}{rcl} \phi : \mathbb{C}[x,y] & \longrightarrow & \mathbb{C}[x,y] \\ (x,y) & \longmapsto & (f(x,y), g(x,y)) \end{array}$$

é um isomorfismo.

Teorema 3.2. (Epimorfismo) *Se* $\psi : \mathbb{C}[x,y] \longrightarrow \mathbb{C}[t]$ *é um epimorfismo, então* $gr(\psi(x))$ *divide* $gr(\psi(y))$*; ou vice-versa.*

Entretanto, iremos nos restringir à verificação de que ambos os teoremas são verdadeiros.

3.1 O Teorema do Mergulho da Reta

Definição 3.1. Seja $h : A \longrightarrow B$ uma aplicação regular entre duas variedades afins. Diremos que h é um *mergulho* quando h induz um isomorfismo de A sobre uma subvariedade de B.

Isto se traduz do seguinte modo: Existe um ideal primo J de $\Gamma(B)$, onde $\Gamma(B)$ é o anel das funções regulares sobre B, tal que $h : A \xrightarrow{\sim} V(J)$; ou seja, h induz uma sobrejeção h^* de $\Gamma(B)$ sobre $\Gamma(A)$.

$$\begin{tikzcd}
\Gamma(A) & \Gamma(B)/J = \Gamma(V(J)) \arrow[l, "\sim"'] \\
& \Gamma(B) \arrow[u] \arrow[ul, "h^*"]
\end{tikzcd}$$

Em particular,

$$\begin{array}{rcl} \psi : \mathbb{A}^1 & \longrightarrow & \mathbb{A}^2 \\ t & \longmapsto & (\psi_1(t), \psi_2(t)) \end{array}$$

é um mergulho se, e somente se,

$$\begin{array}{rcl} \psi^* : \mathbb{C}[y,z] & \longrightarrow & \mathbb{C}[t] \\ y & \longmapsto & \psi_1(t) \\ z & \longmapsto & \psi_2(t) \end{array}$$

for sobrejetiva, já que $\Gamma(\mathbb{A}^1) \simeq \mathbb{C}[t]$ e $\Gamma(\mathbb{A}^2) \simeq \mathbb{C}[y,z]$.

Tem-se que todo mergulho da reta no plano é um mergulho do ponto de vista diferencial.

De fato, ψ é injetora: suponha que

$$(\psi_1(t), \psi_2(t)) = (\psi_1(t'), \psi_2(t')).$$

Como ψ^* é sobrejetora, existe $g(x,y)$ tal que

$$g(\psi_1(t), \psi_2(t)) := \psi^* g(x,y) = t.$$

Portanto,

$$t = g(\psi_1(t), \psi_2(t)) = g(\psi_1(t'), \psi_2(t')) = t'.$$

Por outro lado,

$$1 = dt = g_x.\psi_1'(t) + g_y.\psi_2'(t)$$

e portanto

$$\frac{d\psi}{dt} = (\psi_1'(t), \psi_2'(t))$$

não se anula em nenhum ponto $t \in \mathbb{A}^1$.

Ainda, neste caso, como $V(J) = \psi(\mathbb{A}^1)$ é uma variedade afim em $\mathbb{A}^2$, que não é um conjunto finito e é diferente de vazio, temos que $J = \langle f \rangle$ para algum $f \in \mathbb{C}[y, z]$ irredutível.

Podemos ainda supor, a menos de mudança de coordenadas em $\mathbb{A}^2$, que $\psi(0) = (0, 0)$.

Denotemos por:

$$\psi_1(t) = a_r t^r + \cdots + a_1 t, \quad \psi_2(t) = b_m t^m + \cdots + b_1 t \quad \text{e} \quad n = gr(f),$$

onde $gr(f)$ é o grau total do polinômio f.

Note que, se $gr(f) = 1$ então o teorema é trivial. Portanto, iremos considerar apenas o caso em que $gr(f) > 1$.

Iremos supor, também, que $r < m$; pois, caso $r = m$, se tomarmos o isomorfismo

$$\begin{array}{rcl} T : \mathbb{C}[y, z] & \longrightarrow & \mathbb{C}[y, z] \\ y & \longmapsto & y - \frac{a_r}{b_r} z \\ z & \longmapsto & z \end{array}$$

teremos que a aplicação $\psi^* \circ T$ continuará sendo sobrejetiva e passará a possuir a propriedade que desejamos.

Observe que, ψ induz uma aplicação injetiva,

$$\begin{array}{rcl} \tilde{\psi} : \mathbb{P}^1 & \longrightarrow & \mathbb{P}^2 \\ t & \longmapsto & (1 : \psi_1(t) : \psi_2(t)) \\ \infty & \longmapsto & (0 : 0 : 1) \end{array}$$

De fato, basta observar que $\tilde{\psi}$ leva $\mathbb{A}^1$ injetivamente em pontos à distância finita; ou seja, o plano Y-Z. Observe que, com a nossa escolha de coordenadas, em $\mathbb{P}^2$, a reta no infinito é $X = 0$.

Note que $Im(\tilde{\psi}) = \{(X : Y : Z) \in \mathbb{P}^2 \ ; \ F(X : Y : Z) = 0\}$ onde F é a homogenização de f.

De fato, tomando coordenadas homogêneas $(t : s)$ em $\mathbb{P}^1$ temos que,

$$(1 : \psi_1(\frac{t}{s}) : \psi_2(\frac{t}{s})) = (s^m : a_r t^r s^{m-r} + \cdots + a_1 t s^{m-1} : b_m t^m + \cdots + b_1 t s^{m-1}).$$

Fazendo $s = 0$ e $t = 1$ temos que a curva F só toca a reta no infinito no ponto $(0 : 0 : b_m) = (0 : 0 : 1)$.

Note que F é analiticamente irredutível no ponto $(0 : 0 : 1)$, pois se ocorresse o contrário, F iria possuir dois ramos passando por este ponto, o que não ocorre dado que a aplicação $\tilde{\psi}$ é injetiva.

Pelo fato de ψ^* ser sobrejetiva, podemos garantir que existe $h \in \mathbb{C}[y, z]$ tal que $h(\psi_1(t), \psi_2(t)) = t$, o que implica que

$$I(H, F)_{(1:\,0:\,0)} = 1,$$

onde H é a homogenização de h.

Como,

$$1 < gr(H).gr(F) = \sum_{p \in H \cap F} I(H, F)_p = 1 + \sum_{p \in H \cap F \setminus \{(1:0:0)\}} I(H, F)_p \, ,$$

temos que existe um outro ponto de interseção de H com F.

Por outro lado, à distância finita, H e F só se cortam em $(1 : 0 : 0)$. Como F possui um único ponto no infinito, temos que F e H só se cortam em mais um ponto, a saber $(0 : 0 : 1)$. Portanto,

$$I(F, H)_{(0:0:1)} = gr(H).gr(F) - 1.$$

Vamos estabelecer a seguinte notação:

$$I(F, H) = I(F(x, y, 1), H(x, y, 1))_{(0:0:1)};$$

isto é, o índice de interseção entre F e H no infinito.

Observe que $V(F) \cap V(X) = \{(0:0:1)\}$. Logo, pelo teorema de Bézout,

$$I(F,X) = n.$$

Sem perda de generalidade, segue da última igualdade que,

$$F = Y^n + XF_1.$$

Dividindo H por F como polinômios em Y podemos supor que $gr_Y(H) < n$.

Lema 3.1. *Nas condições acima, temos que,*

$$n_1 \dots n_{g-1} \leq gr_Y(H) < n.$$

Demonstração: Suponha que $gr_Y(H) < n_1 \dots n_{g-1}$. Do fato de $gr_y(H(x,y,1)) = gr_Y(H)$, teríamos pelo Teorema 1.1 que

$$I(H,F) \in \langle v_0, \dots, v_{g-1} \rangle .$$

Sendo $\varepsilon_{g-1} = mdc(v_0, \dots, v_{g-1})$, temos que, $\varepsilon_{g-1} | I(H,F)$. Por outro lado, como $\varepsilon_{g-1} | n$ segue da igualdade $I(F,H) = gr(F).gr(H) - 1$ que $\varepsilon_{g-1} | 1$. Absurdo, pois $\varepsilon_{g-1} > 1$.

□

Seja $F_{g-1}(X,Y,Z)$ a ε_{g-1}-raiz aproximada de $F(X,Y,Z)$ em $\mathbb{C}[X,Z][Y]$. Como $F(X,Y,Z) = Y^n + \alpha_1(X,Z)Y^{n-1} + \cdots + \alpha_n(X,Z)$, com $gr(\alpha_i) = i$, segue do Lema 2.1 e do Corolário 2.2 que F_{g-1} é homogêneo de grau $\dfrac{n}{\varepsilon_{g-1}}$; isto é, $F_{g-1}(X,Y,Z) = Y^{\frac{n}{\varepsilon_{g-1}}} + a_1(X,Z)Y^{\frac{n}{\varepsilon_{g-1}}-1} + \cdots + a_{\frac{n}{\varepsilon_{g-1}}}(X,Z)$, com $gr(a_i) = i$.

Note que,

$$\begin{aligned} F_{g-1}(x,y,1) &= y^{\frac{n}{\varepsilon_{g-1}}} + a_1(x,1)Y^{\frac{n}{\varepsilon_{g-1}}-1} + \cdots + a_{\frac{n}{\varepsilon_{g-1}}}(x,1) \\ F_{g-1}(1,y,z) &= y^{\frac{n}{\varepsilon_{g-1}}} + a_1(1,z)Y^{\frac{n}{\varepsilon_{g-1}}-1} + \cdots + a_{\frac{n}{\varepsilon_{g-1}}}(1,z), \end{aligned}$$

onde $a_i(x,1)$ e $a_i(1,z)$ satisfazem as Equações (2.1.2) .

Assim, $F_{g-1}(x,y,1)$ é a $\varepsilon_{g-1}-$raiz aproximada de $F(x,y,1)$ e $F_{g-1}(1,y,z)$ é a $\varepsilon_{g-1}-$raiz aproximada de $F(1,y,z)=f(y,z)$.

Lema 3.2. *Temos que,* $v_g < \dfrac{n}{\varepsilon_{g-1}} \cdot n = gr(F_{g-1}) \cdot gr(F)$.

Demonstração: De fato,

$$v_g = I(F_{g-1},F) \leq \sum_{p\in(F_{g-1}\cap F)} I(F_{g-1},F)_p = gr(F_{g-1}) \cdot gr(F) = \frac{n}{\varepsilon_{g-1}} \cdot n.$$

Por outro lado, se $v_g = \dfrac{n}{\varepsilon_{g-1}} \cdot n$, então teríamos que $\varepsilon_{g-1}|v_g$, pelo fato de $\varepsilon_{g-1}|n$. Mas isto implicaria que $\varepsilon_{g-1} = mdc(v_g,\varepsilon_{g-1}) = \varepsilon_g$, o que é um absurdo.

□

Lema 3.3. *Seja* $H = h_s F_{g-1}^s + h_{s-1}F_{g-1}^{s-1} + \cdots + h_0$ *a* F_{g-1}*-expansão de* H *em* $\mathbb{C}[X,Z][Y]$. *As seguintes condições são satisfeitas:*

(1) $I(H,F) = I(h_1F_{g-1},F)$, $I(h_1,F) = gr(h_1) \cdot gr(F)$ *e*

$$v_g = I(F_{g-1},F) = \frac{n}{\varepsilon_{g-1}} \cdot n - 1;$$

(2) $h_i = 0$, $\forall\, i \geq 2$;

(3) $I(h_0,F) = gr(h_0) \cdot gr(F) = gr(H) \cdot gr(F)$ *ou* $h_0 = 0$.

Demonstração: Note que, como H e F_{g-1} são homogêneos, temos que todas as parcelas desta expansão são polinômios homogêneos de grau igual a $gr(H)$. Recorde que, por definição,

$$s = \left[\frac{gr_Y(H)}{gr_Y(F_{g-1})}\right].$$

Como $gr_Y(H) < n$ e $gr_Y(F_{g-1}) = \dfrac{n}{\varepsilon_{g-1}}$, segue que $s < \varepsilon_{g-1} = n_g$.

Da desigualdade, $gr_Y(h_i) < gr_Y(F_{g-1}) = \dfrac{n}{\varepsilon_{g-1}}$, segue que

$$I(h_i, F) \in \langle v_0, \ldots, v_{g-1} \rangle \text{ , para todo } i \in \{0, \ldots, s\}.$$

Pelo Lema 2.3, segue também que $I(h_i F_{g-1}^i, F) \neq I(h_j F_{g-1}^j, F)$ para todo $i \neq j$, onde $i, j \in \{0, \ldots, s\}$. Desta forma,

$$I(H, F) = min_{\,0 \leq i \leq s} \left\{ I(h_i F_{g-1}^i, F) \right\} = I(h_k F_{g-1}^k, F),$$

para algum $k \in \{0, \ldots, s\}$.

Se $k = 0$ então $I(H, F) = I(h_0, F) \in \langle v_0, \ldots, v_{g-1} \rangle$. Assim, do mesmo modo que procedemos no Lema 3.1, teríamos que $\varepsilon_{g-1} | I(H, F)$, o que é um absurdo. Portanto , $k \geq 1$.

Note que,

$$gr(H).n - 1 = I(H, F) = I(h_k, F) + kv_g < I(h_i, F) + iv_g \leq gr(H).n \quad (3.1.1)$$

para todo $i \neq k$ com $i, k \in \{0, \ldots, s\}$, onde a última desigualdade decorre do teorema de Bézout e do fato de que $gr(h_i F_{g-1}^i) = gr(H)$.

Feitas estas observações preliminares, vamos provar o Lema.

Para provar a primeira igualdade do item (1), basta provar que $k = 1$.

Caso k fosse maior do que 1, teríamos por (3.1.1) que

$$gr(H) \cdot n - 1 < I(h_1, F) + v_g \leq gr(H) \cdot n$$

o que implica que,

$$I(h_1, F) + v_g = gr(H) \cdot n.$$

Como ε_{g-1} divide $I(h_1, F)$ e n, temos que $\varepsilon_{g-1} | v_g$ e conseqüentemente

$$\varepsilon_{g-1} = mdc(\varepsilon_{g-1}, v_g) = \varepsilon_g,$$

o que é um absurdo.

Para provar a segunda igualdade do item (1), basta provar que $gr(h_1) \cdot gr(F) - 1 < I(h_1, F)$, já que, $I(h_1, F) \leq gr(h_1) \cdot gr(F)$. Primeiro observe que do Lema 3.2 decorre que

$$gr(H) \cdot n - 1 = I(H, F) = I(h_1, F) + v_g < I(h_1, F) + \frac{n}{\varepsilon_{g-1}} \cdot n,$$

o que implica que,

$$I(h_1, F) > gr(H) \cdot n - \frac{n}{\varepsilon_{g-1}} \cdot n - 1.$$

Por outro lado, como $gr(h_1 F_{g-1}) = gr(H)$, segue que $gr(h_1) + gr(F_{g-1}) = gr(H)$, o que implica que,

$$gr(h_1) \cdot n = gr(H) \cdot n - \frac{n}{\varepsilon_{g-1}} \cdot n;$$

isto é, $I(h_1, F) > gr(h_1) \cdot gr(F) - 1$.

Já a terceira igualdade do item (1) decorre diretamente da seguinte igualdade:

$$\begin{aligned} gr(H) \cdot n - 1 = I(H, F) = I(h_1, F) + v_g &= gr(h_1) \cdot gr(F) + v_g \\ &= gr(H) \cdot n - n \cdot \frac{n}{\varepsilon_{g-1}} + v_g. \end{aligned}$$

Vamos agora para a demonstração do item (2).

Se para algum $i > 1$, $h_i \neq 0$ então por (3.1.1) segue que,

$$gr(H) \cdot n = I(h_i, F) + i \cdot v_g = I(h_i, F) + i \cdot n \cdot \frac{n}{\varepsilon_{g-1}} - i.$$

Como ε_{g-1} divide n e $I(h_i, F)$, segue que ε_{g-1} divide i, o que é um absurdo pois, $0 < i \leq s < \varepsilon_{g-1}$.

Para finalizar o lema, se $h_0 \neq 0$, então $I(h_0, F) = gr(H) \cdot n = gr(h_0) \cdot n$, onde a primeira igualdade segue de (3.1.1).

□

Note que $I(F_{g-1}, X) = \dfrac{n}{\varepsilon_{g-1}}$.

Observações :

(1) Como $I(F_{g-1}, F) = v_g < \dfrac{n}{\varepsilon_{g-1}} \cdot n = I(bX^{\frac{n}{\varepsilon_{g-1}}}, F)$, temos que,

$$I(F_{g-1} - bX^{\frac{n}{\varepsilon_{g-1}}}, F) = v_g.$$

(2)
$$\begin{aligned} I(F_{g-1} - bX^{\frac{n}{\varepsilon_{g-1}}}, X^n) &= n \cdot I(F_{g-1} - bX^{\frac{n}{\varepsilon_{g-1}}}, X) \\ &= n \cdot I(F_{g-1}, X) \\ &= n \cdot \frac{n}{\varepsilon_{g-1}}, \end{aligned}$$

para qualquer $b \in \mathbb{C}$.

Lema 3.4. *$F_{g-1}(x, y, 1) - bx^{\frac{n}{\varepsilon_{g-1}}}$ é analiticamente irredutível em $(0 : 0 : 1)$, para qualquer $b \in \mathbb{C}$.*

DEMONSTRAÇÃO: Segue direto da observação (1) e do fato que v_g é um dos geradores mínimos do semigrupo $S(f)$.

$\square$

Agora vamos ultilizar estas propriedades para terminar a prova do Teorema do Mergulho.

Segue do Lema 3.4, das observações (1) e (2), acima, que $I(F_{g-1} - bX^{\frac{n}{\varepsilon_{g-1}}}, F - aX^n)$ é igual o mínimo entre $I(F_{g-1} - bX^{\frac{n}{\varepsilon_{g-1}}}, F)$ e $I(F_{g-1} - bX^{\frac{n}{\varepsilon_{g-1}}}, aX^n)$; isto é,

$$I(F_{g-1} - bX^{\frac{n}{\varepsilon_{g-1}}}, F - aX^n) = v_g = n \cdot \frac{n}{\varepsilon_{g-1}} - 1,$$

para quaisquer $a, b \in \mathbb{C}$.

Como $gr(F_{g-1} - bX^{\frac{n}{\varepsilon_{g-1}}}) = \dfrac{n}{\varepsilon_{g-1}}$ e $gr(F - aX^n) = n$, segue do teorema de Bézout que existem $c, d \in \mathbb{C}$ tais que

$$I(F_{g-1} - bX^{\frac{n}{\varepsilon_{g-1}}}, F - aX^n)_{(1:c:d)} = 1; \tag{3.1.2}$$

e que $(1 : c : d)$ é o único ponto de interseção, à distância finita, das curvas $F_{g-1} - bX^{\frac{n}{\varepsilon_{g-1}}}$ e $F - aX^n$.

Desta forma, defina

$$\begin{array}{rcl} \phi : \mathbb{C}[y,z] & \longrightarrow & \mathbb{C}[y,z] \\ y & \longmapsto & F(1,y,z) \\ z & \longmapsto & F_{g-1}(1,y,z). \end{array}$$

Naturalmente, ϕ induz uma aplicação $\Phi : \mathbb{C}^2 \longrightarrow \mathbb{C}^2$ definida por

$$\Phi(y,z) = (F(1,y,z), F_{g-1}(1,y,z)).$$

Por (3.1.2), segue que, as curvas $F(1,y,z) - a$ e $F_{g-1}(1,y,z) - b$ se cortam em um único ponto $(c,d) \in \mathbb{C}^2$. Conseqüentemente, este ponto é a única solução do sistema:

$$\begin{cases} F(1,y,z) & = a \\ F_{g-1}(1,y,z) & = b. \end{cases}$$

Sendo assim, a aplicação Φ é uma bijeção.

Note que, se provarmos que Φ admite uma inversa regular, isto é, suas funções coordenadas são polinomiais, então teremos automaticamente que ϕ é um isomorfismo.

Porém, isto segue diretamente da seguinte proposição:

Proposição 3.1. *Sejam $f, g \in \mathbb{C}[y,z]$ tais que a aplicação $\Gamma : \mathbb{C}^2 \longrightarrow \mathbb{C}^2$, definida por*

$$\Gamma(y,z) = (f(y,z), g(y,z))$$

é uma bijeção. Então, Γ é uma aplicação birregular.

DEMONSTRAÇÃO: Escreva $u = f(y,z)$, $v = g(y,z)$, $h_1(y,z,u,v) = u - f(y,z)$ e $h_2(y,z,u,v) = v - g(y,z)$.

Denotemos por $R_y = R_y(z,u,v)$ e $R_z = R_z(y,u,v)$ os resultantes de h_1 e h_2 com respeito a y e z, respectivamente.

Escreva $R_y = a_0(u,v)z^r + \cdots + a_r(u,v)$ e considere $b_1(z)$ e $b_2(z)$ os coeficientes dos termos de maior grau em y de h_1 e h_2, respectivamente.

Fixado $(u,v) \in \mathbb{C}^2$, sabemos que $z(u,v) \in \mathbb{C}$ é solução da equação

$$a_0(u,v)z^r + \cdots + a_r(u,v) = 0$$

se, e somente se, $b_1(z(u,v)) = b_2(z(u,v)) = 0$ ou existe $y(u,v) \in \mathbb{C}$ solução do sistema

$$\begin{cases} h_1(y, z(u,v), u, v) = 0 \\ h_2(y, z(u,v), u, v) = 0. \end{cases}$$

Como $b_1, b_2 \in \mathbb{C}[z]$, podemos garantir que existe, no máximo, uma quantidade finita de raízes comuns para estes polinômios. A saber, $z_1, \ldots, z_k$.

Considere as variedades algébricas, $V_i = \{(y, z_i) \in \mathbb{C}^2\} = V(z - z_i)$ para $i = 1, \ldots, k$.

Como Γ é um aplicação regular e $V_i \neq \mathbb{C}^2$ para todo i, segue que $\Gamma(V_i)$ é uma subvariedade algébrica própria de $\mathbb{C}^2$. Considere $V = \displaystyle\bigcup_{i=1}^{k} \Gamma(V_i) \cup V(a_0(u,v))$.

Tome $(u,v) \in \mathbb{C}^2 \setminus V$. Note agora que, $z(u,v) \in \mathbb{C}$ é solução da equação

$$a_0(u,v)z^r + \cdots + a_r(u,v) = 0$$

se, e somente se, existe $y(u,v) \in \mathbb{C}$ solução do sistema

$$\begin{cases} h_1(y, z(u,v), u, v) = 0 \\ h_2(y, z(u,v), u, v) = 0. \end{cases}$$

Assim, se existisse mais de uma solução da equação

$$a_0(u,v)z^r + \cdots + a_r(u,v) = 0,$$

iria existir mais de uma solução do sistema

$$\begin{cases} h_1(y, z(u,v), u, v) = 0 \\ h_2(y, z(u,v), u, v) = 0, \end{cases}$$

o que é um absurdo.

Portanto, existe uma única raiz do polinômio $a_0(u,v)z^r + \cdots + a_r(u,v)$, isto é,

$$R_y(z,u,v) = a_0(u,v)\left(z + \frac{a_1(u,v)}{ra_0(u,v)}\right)^r.$$

Prova-se um resultado análogo para $R_z(y,u,v)$.

Assim, tem-se que $\Gamma : \mathbb{C}^2 \longrightarrow \mathbb{C}^2$ é uma aplicação regular birracional.

Suponha agora que $\Gamma(y,z) = (u,v)$. Se Γ^{-1} não fosse regular em (u,v), pelo Teorema Principal de Zariski (veja [Mu], Teorema 3.20, pg. 48), existiria uma curva E em $\mathbb{C}^2$, passando por (y,z), tal que $\Gamma(E) = \{(u,v)\}$, o que é um absurdo, pois Γ deixaria de ser injetora. Portanto, Γ é birregular.

□

3.2 O Teorema do Epimorfismo

Primeiramente, faremos duas observações, sobre a demonstração e o próprio enunciado do Teorema do Mergulho, que serão utilizadas com freqüência:

(1) Claramente, foi demonstrado que $\mathbb{C}[y,z] = \mathbb{C}[f, f_{g-1}]$.

(2) Podemos supor, sem perda de generalidade, que $\psi^*(f_{g-1}) = t$.

Com efeito, como $\psi^*(f) = 0$ e ψ^* é sobrejetiva, temos que $\psi^*(f_{g-1}) = at+b$, para algum $(a,b) \in \mathbb{C}^2$ com $a \neq 0$. Entretanto, usaremos mais adiante, apenas o grau em t de $\psi^*(f_{g-1})$. Sendo assim, com o objetivo de aliviar a notação, não há perda de generalidade em considerar $a = 1$ e $b = 0$.

Seja dado um epimorfismo,

$$\begin{array}{rcl} \psi^* : \mathbb{C}[y,z] & \longrightarrow & \mathbb{C}[t] \\ y & \longmapsto & \psi_1(t) \\ z & \longmapsto & \psi_2(t) \end{array}$$

associado ao mergulho,

$$\begin{array}{rcl} \psi : \mathbb{A}^1 & \longrightarrow & \mathbb{A}^2 \\ t & \longmapsto & (\psi_1(t), \psi_2(t)). \end{array}$$

Como vimos, anteriormente, podemos supor que $gr(\psi_1(t)) < gr(\psi_2(t))$.

Considere então, $f \in \mathbb{C}[y,z]$ tal que $\psi(\mathbb{A}^1) = V(f)$ e $f_{g-1} \in \mathbb{C}[y,z]$ a ε_{g-1}-raiz aproximada de f.

Como vimos, na observação (1) acima, $z \in \mathbb{C}[f, f_{g-1}] = \mathbb{C}[f_{g-1}, f]$. Temos, então que $z = z(f_{g-1}, f)$.

Note que z é irredutível em $\mathbb{C}[y,z] = \mathbb{C}[f_{g-1}, f]$. Portanto, o polinômio $z(f_{g-1}, f)$ é irredutível em $\mathbb{C}[f_{g-1}, f]$.

Como $z(f_{g-1}, f) = 0$ se, e somente se, $z = 0$ e $V(z(f_{g-1}, f))$ que é uma subvariedade afim de $\mathbb{A}^2$; temos que, a parametrização

$$\begin{array}{rcl} \widetilde{\psi} : \mathbb{A}^1 & \longrightarrow & \mathbb{A}^2 \\ y & \longmapsto & (f_{g-1}(y,0), f(y,0)) \end{array}$$

define um mergulho da reta afim no plano $f_{g-1} - f$, onde $\widetilde{\psi}(A^1) = V(z(f_{g-1}, f))$.

Claramente, temos que $gr_y(f_{g-1}(y,0)) < gr_y(f(y,0))$.

Novamente, pelo Teorema do Mergulho, existe $z_{g'-1}(f_{g-1}, f) \in \mathbb{C}[f_{g-1}, f]$, $\varepsilon'_{g'-1}$-raiz aproximada de $z(f_{g-1}, f)$ tal que $\mathbb{C}[f_{g-1}, f] = \mathbb{C}[z_{g'-1}, z]$ e $gr_{f_{g-1}}(z_{g'-1}) = \dfrac{n'}{\varepsilon'_{g'-1}}$ divide $n' = gr_{f_{g-1}}(z)$.

Como vimos na demonstração do Teorema do Mergulho, podemos escrever z e $z_{g'-1}$ da seguinte forma:

$$\begin{array}{rcl} z & = & (f_{g-1})^{n'} + \cdots \\ z_{g'-1} & = & (f_{g-1})^{\frac{n'}{\varepsilon'_{g'-1}}} + \cdots \ . \end{array}$$

Agora, observe que $\mathbb{C}[y,z] = \mathbb{C}[f_{g-1}, f] = \mathbb{C}[z_{g'-1}, z]$. Assim,

$$y = c \cdot z_{g'-1} + P(z),$$

com $c \neq 0$ e $P(z) \in \mathbb{C}[z]$.

Portanto, pela observação (2) do início, temos que

$$\psi_1(t) = \psi^*(y) = \psi^*(c \cdot z_{g'-1} + P(z)) = c \cdot (t^{\frac{n'}{\varepsilon'_{g'-1}}} + \cdots) + P(t^{n'} + \cdots)$$

e

$$\psi_2(t) = \psi^*(z) = t^{n'} + \cdots .$$

Como $gr(\psi_1(t)) < gr(\psi_2(t))$, temos que $P(z)$ é constante. Conseqüentemente,

$$gr(\psi_1(t)) = \frac{n'}{\varepsilon'_{g'-1}} \quad \text{divide} \quad n' = gr(\psi_2(t)).$$

$\square$

Faremos um exemplo para ilustrar a teoria desenvolvida.

Considere o mergulho,

$$\begin{array}{ccc} \mathbb{A}^1 & \longrightarrow & \mathbb{A}^2 \\ t & \longmapsto & (t^2, t+t^8). \end{array}$$

Note que $H = X^3Z - Y^4$ e $F = Y^8 - 2ZX^3Y^4 - X^7Y + Z^2X^6$.

Observe que H possui grau em Y menor do que F. Logo, não é necessário efetuar a divisão de H por F.

Como o ponto de singularidade de F é $(0 : 0 : 1)$, temos que olhar para o polinômio $F(x,y,1) = y^8 - 2x^3y^4 - x^7y + x^6$, a fim de calcularmos o seu semigrupo e os seus expoentes característicos.

Claramente, $\varepsilon_1 = (8,6) = 2$. Como $\varepsilon_2 < \varepsilon_1$, temos que $g = 2$, o que implica que, $S(F(x,y,1)) =< 8, 6, v >$.

Assim, $gr(F_1) = \frac{8}{4} = 2$ e, tomando $Q = Y^4$, temos que

$$F = Q^2 - 2ZX^3Q - X^7Y + Z^2X^6.$$

Desta forma, $F_1 = \tau_F(Q) = Y^4 - \frac{2ZX^3}{2} = Y^4 - ZX^3$.

Portanto, considerando $f = F(1,y,z) = y^8 - 2zy^4 - y + z^2$ e $f_1 = F_1(1,y,z) = y^4 - z$, temos que

$$\begin{array}{rcl} \mathbb{C}[y,z] & \longrightarrow & \mathbb{C}[y,z] \\ (y,z) & \longmapsto & (f,f_1) \end{array}$$

é um isomorfismo, com

$$y = y(f_1,f) = f_1^2 - f \quad \text{e} \quad z = z(f_1,f) = (f - f_1^2)^4 - f_1.$$

Bibliografia

[AM] S.S. Abhyankar, T.T. Moh, Embeddings of the line in the plane, **J. Reine Angew. Math. 276**, (1975), 148-166.

[CW] H.C.Chang, L.C.Wang, An Intersection Theoretical Proof of the Embedding Line Theorem, **Journal of Algebra 161**, 467-479 (1993).

[GP] J.Gwoździewicz, A.Ploski, On the Approximate Roots of Polynomials, **Annales Polonici Mathematici LX3** (1995), 199-210.

[Hf] A.Hefez, Irreducible Plane Curve Singularities, in Real and Complex Singularities, **Lecture Notes in Pure and Applied Mathematics**,vol 232, 2003.

[Mu] D.Mumford, Algebraic Geometry I - Complex Projective Varieties, Springer Verlag.

[Pa] P.P.Pampu, Approximate Roots, **American Mathematical Society**, (1991).