O TEOREMA DE SEIDENBERG-TARSKI
E ALGUMAS DE SUAS APLICAÇÕES AS
EQUAÇÕES DIFERENCIAIS PARCIAIS LINEARES

FRANCISCO VILLARREAL ALVARADO

DISSERTAÇÃO APRESENTADA

AO

INSTITUTO DE MATEMÁTICA E ESTATÍSTICA

DA

UNIVERSIDADE DE SÃO PAULO

PARA OBTENÇÃO DO GRAU DE MESTRE

EM

MATEMÁTICA

ORIENTADOR:

Prof. Dr. Antonio Gilioli

- SÃO PAULO, ABRIL DE 1978 -

Durante a realização deste trabalho, o autor teve apoio financeiro da
Organização dos Estados Americanos (OEA), FINEP e CAPES.

ÍNDICE

INTRODUÇÃO	v
NOTAÇÕES	ix
CAP. 0 - PRELIMINARES.	1
0.1 - Definições e Resultados de Álgebra Elementar.	1
0.2 - O Teorema de Sturm.	22
0.3 - Definições e Algumas Propriedades das Distribuições	31
CAP. I - O TEOREMA DE SEIDENBERG-TARSKI.	35
1.1 - O Algoritmo de Euclides e Propriedades.	35
1.2 - Lemas Auxiliares.	59
1.3 - Prova do Teorema S-T.	83
CAP. II - PROLONGAMENTO ANALÍTICO E COMPORTAMENTO ASSINTÓTICO DOS CONJUNTOS SEMI-ALGÉBRICOS EM $\mathbb{R}^2$	89
2.1 - Prolongamento Analítico ao longo de Curvas.	90
2.2 - Prova do Teorema A.	97
2.3 - Série Formal de Potências e Propriedades.	104
2.4 - Comportamento Assintótico dos Conjuntos Semi-algêbricos em $\mathbb{R}^2$	107
CAP. III - APLICAÇÕES DO TEOREMA DE SEIDENBERG-TARSKI.	115
3.1 - Propriedades Assintóticas	116
3.2 - Lemas Algébricos.	125
CAP. IV - HIPOELIPTICIDADE.	131
4.1 - Preliminares.	131
4.2 - As Propriedades $(HE)_d$	137
4.3 - Condições Necessária e Suficiente de Hipoelipticidade.	143
CAP. V - DIVISÃO DE DISTRIBUIÇÕES POR POLINÔMIOS	151
5.1 - Preliminares.	151
5.2 - Lemas Auxiliares.	162
5.3 - Teorema E	173
5.4 - Teoremas de Existência no Espaço das Distribuições	179
APÊNDICE - O TEOREMA DE EXTENSÃO DE WHITNEY	185
A.1 - Preliminares.	185
A.2 - Prova do Teorema de Extensão de Whitney	197
BIBLIOGRAFIA	206

INTRODUÇÃO

O objetivo fundamental deste trabalho foi dar uma exposição detalhada e sistemática do Teorema de Seidenberg-Tarski (S-T) e de alguma de suas aplicações à teoria das equações diferenciais parciais lineares com coeficientes constantes (EDPL) de modo a tornar tais resultados acessíveis a qualquer leitor em nível de estudante de pós-graduação. Damos também os pré-requisitos necessários para tanto, que não se encontram nos cursos básicos de Mestrado. Além do Teorema S-T ser importante devido a essas e outras aplicações as EDPL, fomos informados de que ele tem sido também utilizado em geometria.

A primeira parte é de caráter algébrico, consistindo de uma demonstração minuciosa do Teorema S-T e de aplicações ao estudo do comportamento assintótico de certas funções de natureza algébrica. A segunda parte consiste na aplicação das propriedades dessas funções, ao estudo da hipoeipticidade e da existência de soluções fundamentais temperadas de EDPL.

Este trabalho consiste de seis capítulos e um apêndice os quais passamos a descrever de forma sucinta:

No Capítulo 0 apresentamos os resultados que serão usados nos capítulos posteriores e provamos somente aqueles; entre os quais uma versão não usual do Teorema de Sturm, pa

ra os quais não encontramos fácil referência. Essa versão de Sturm é fortemente usado para a prova do Teorema S-T.

O Capítulo I contém a formulação e a prova do Teorema S-T, a qual é dada na seção 1.3. Nas seções 1.1 e 1.2 formulamos e resolvemos questões de caráter algébrico os quais descrevem as propriedades dos elementos de $A_m \times \mathbb{R}[X_1, \dots, X_n, Z_1, \dots, Z_m]$ (onde A_m denota uma certa classe de conjuntos semi-algêbricos em $\mathbb{R}^m$). A mais importante dessas propriedades é a dada no Lema 1.2.7. Utilizamos as idéias básicas encontradas em [4] (Cap.7), cuja demonstração entretanto, ficou muito modificada.

O Capítulo II é dedicado ao estudo do comportamento assintótico dos conjuntos semi-algêbricos em $\mathbb{R}^2$ por meio do Teorema A e dos resultados da seção 2.3: na seção 2.4 chegamos a provar a Proposição 2.4.1 (e seguintes), que é essencialmente encontrada em Chaillou [2] (Cap.B), o qual era o objetivo do capítulo.

Os resultados do Capítulo III são baseados no Teorema S-T e nas propriedades da seção 2.4. Aqui consideramos um resultado, o Lema 3.1.2, que permite caracterizar os operadores diferenciais hipoelípticos no Capítulo IV. Um outro resultado, o Lema 3.2.1 (devido a Hörmander) é usado no Capítulo V para resolver o problema da divisão de uma distribuição por um polinômio não identicamente nulo. As demonstrações dos lemas citados é bem mais simples que as dadas em [8] e [15] (Cap.5), devido a utilizarmos os resultados da seção 2.4.

No Capítulo IV obtemos condições necessárias e suficientes para hipoelipticidade de um ODPL. Damos aqui uma exposição mais detalhada de alguns resultados de [15], assim como uma prova do Teorema 4.3.1 o que, ao contrário de [15] (Cap.7), não utiliza parametrises de operadores diferenciais.

No Capítulo V, usando o Teorema de Extensão de Whi

tney e os resultados obtidos a partir do Teorema S-T demonstramos o Teorema E, o qual prova ser possível a divisão de uma distribuição por um polinômio não identicamente nulo. Neste capítulo fazemos essencialmente uma exposição bem mais minuciosa que as dadas em [8] e [15].

No Apêndice damos uma demonstração detalhada do Teorema de Extensão de Whitney. Nós resolvemos incluí-la dada a dificuldade de leitura das provas que aparecem em [8], [15] e [18].

A originalidade do trabalho encontra-se principalmente na primeira parte, pois não se encontra em literatura matemática uma demonstração suficientemente compreensível e detalhada do Teorema S-T. A mais minuciosa que conhecemos encontra-se em [4], porém mesmo essa demonstração é de leitura difícil. Também a prova da Proposição 2.4.1 (Teorema P.1 [2]) pressupõe o conhecimento de certos fatos relacionados com séries de Puiseux, que em geral não são expostos com detalhe, e que constituíram as seções 2.1 a 2.3.

Os agradecimentos que se seguem não são de praxe, são o profundo e sincero reconhecimento pela colaboração obtida: ao Professor Doutor Chaïm Samuel Hönl pelo seu apoio, assim como pela confiança em mim depositada; ao Professor Doutor Antonio Gilioli por haver-nos sugerido o tema e pelo constante e paciente trabalho de orientação e todos aquelas pessoas e entidades que, de uma ou outra forma, colaboraram para a execução do presente trabalho.

São Paulo, abril de 1978

Francisco Villarreal Alvarado

NOTAÇÕES

$\overset{\circ}{A}$: interior de um conjunto A

$|A|$: cardinal de um conjunto A

$\delta(A)$: diâmetro de um conjunto A

$A[X]$: anel de um polinômio na indeterminada X com coeficientes num anel A

$B_r(x)$: bola aberta de centro x e raio $r > 0$

Ω : um conjunto aberto do espaço que estiver contido

$C^m(\Omega)$: $m = 0, 1, \dots, \infty$, espaço das funções definidas em $\Omega \subset \mathbb{R}^n$, com valores complexos e m vezes continuamente diferenciáveis

$\Omega_* \subset \subset \Omega$: $\bar{\Omega}_*$ é compacto e está contido em Ω

f_X : derivada parcial de f em relação a X

$\mathbb{N}^n$: Subconjunto de $\mathbb{R}^n$ consistindo dos elementos $\alpha = (\alpha_1, \dots, \alpha_n)$ com α_i número natural, $i = 1, \dots, n$

Para $(\alpha, \beta) \in \mathbb{N}^n \times \mathbb{N}^n$: $|\alpha| = \alpha_1 + \dots + \alpha_n$; $\alpha! = \alpha_1! \dots \alpha_n!$

$$D^\alpha = \frac{\partial^{|\alpha|}}{\partial x_1^{\alpha_1} \dots \partial x_n^{\alpha_n}}; \quad \binom{\alpha}{\beta} = \frac{\alpha!}{(\alpha - \beta)! \beta!}, \text{ se } \beta_i \leq \alpha_i, \quad 1 \leq i \leq n$$

Para $(x, \alpha) \in \mathbb{R}^n \times \mathbb{N}^n$: $x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$

$\mathbb{K}[X]$: anel de polinômios em X com coeficientes num corpo $\mathbb{K}$

$\mathbb{K}(X)$: corpo de frações racionais de $\mathbb{K}[X]$

∂P : grau total de um polinômio P

TEOREMA 2.3.1: se refere ao Teorema 1 da seção 3 do capítulo II. Análogo com os lemas, proposições, definições, etc.

$$\|x\| = (x_1^2 + \dots + x_n^2)^{1/2}; \quad x \in \mathbb{C}^n$$

$$\langle x, y \rangle = x_1 y_1 + \dots + x_n y_n; \quad (x, y) \in \mathbb{C}^n \times \mathbb{C}^n$$

CAPÍTULO 0

PRELIMINARES

Neste capítulo daremos algumas definições e resultados que serão usados nos capítulos subsequentes.

0.1 - DEFINIÇÕES E RESULTADOS DE ÁLGEBRA ELEMENTAR

DEFINIÇÃO 0.1.1 - Diz-se que um elemento a , de um anel A comutativo com elemento unidade 1 , é *invertível* em A se existe um elemento $b \in A$ tal que $ab = 1$.

Indicaremos por A^* o conjunto dos elementos não nulos de A e por $U(A)$ o grupo dos elementos invertíveis do anel A .

DEFINIÇÃO 0.1.2 - Sejam x e y dois elementos quaisquer de um anel de integridade A ; diz-se que x é *associado* a y em A se existe um elemento $u \in U(A)$ tal que $x = uy$.

DEFINIÇÃO 0.1.3 - Para todo elemento não nulo a , de um anel de integridade A , colocaremos

$$D_A(a) = \{x \in A; x \text{ divide } a \text{ em } A\}.$$

Então, para todo $a \in A^*$, $U(A) \cup aU(A)$ é um subconjunto de $D_A(a)$. Os elementos do conjunto $U(A) \cup aU(A)$ passam a ser denominados *divisores triviais* de a em A e qualquer outro divisor de a em A (caso exista) é chamado *divisor não trivial* de a em A .

DEFINIÇÃO 0.1.4 - Diz-se que um elemento a de um anel de integridade A é *irredutível* em A se, e somente se,

$$I_1. a \notin [U(A) \cup \{0\}]$$

$I_2.$ os únicos divisores de a em A são os divisores triviais.

DEFINIÇÃO 0.1.5 - Diz-se que um elemento a de um anel de integridade A é *reduzível* em A se, e somente se,

$$R_1. a \notin [U(A) \cup \{0\}]$$

$R_2.$ a admite pelo menos um divisor não trivial em A .

DEFINIÇÃO 0.1.6 - Diz-se que um anel de integridade A é um anel *fatorial* se, e somente se,

$AF_1.$ para todo elemento não nulo e não inversível $a \in A$ e existem elementos irredutíveis $a_1, \dots, a_r$ em A tais que

$$(0.1.1) \quad a = a_1 a_2 \dots a_r.$$

$AF_2.$ quaisquer que sejam as famílias $\{a_i: 1 \leq i \leq r\}$ e $\{b_j: 1 \leq j \leq s\}$ de elementos irredutíveis de A , se $a_1 a_2 \dots a_r = b_1 b_2 \dots b_s$ então $r = s$ e existe uma permutação σ de $\{1, \dots, r\}$

tal que a_i é associado a $b_{\sigma(i)}$ em A para $i=1, \dots, r$.

OBSERVAÇÃO 0.1.1 - Na Condição AF_1 os elementos $a_1, \dots, a_r$ não são necessariamente, não associados em A dois a dois. Consideremos, então, o conjunto $\{a_i U(A) : 1 \leq i \leq r\}$; indicando por v o número de elementos deste conjunto ponhamos

$$\{a_1 U(A), \dots, a_r U(A)\} = \{c_1 U(A), \dots, c_v U(A)\}$$

onde cada c_i , $1 \leq i \leq v$, é irredutível em A e se $i \neq j$ ($1 \leq i, j \leq v$) então c_i não é associado a c_j em A ; além disso, cada elemento a_i , $1 \leq i \leq r$, é associado em A a um e somente um fator irredutível c_k , $1 \leq k \leq v$. Portanto, é claro que, a decomposição (0.1.1) pode ser representado sob a forma

$$(0.1.2) \quad a = u a_1^{\alpha_1} a_2^{\alpha_2} \dots a_v^{\alpha_v}, \quad u \in U(A)$$

onde $\alpha_i \in \mathbb{N}$, $\alpha_i \geq 1$, $1 \leq i \leq v$ (notemos que $\alpha_1 + \dots + \alpha_v = r$). Para abreviar a linguagem diremos que (0.1.1) e (0.1.2), onde ficam subentendidos as condições acima, são as decomposições canônicas de a em A . A condição AF_2 exprime o fato que a decomposição de a , cuja existência é assegurada pela condição AF_1 , é única a menos da ordem dos fatores irredutíveis e a menos de elementos inversíveis.

TEOREMA 0.1.1 ([9], pg.385) - Todo anel de polinômios $\mathbb{K}[X_1, \dots, X_n]$ nas indeterminadas $X_1, \dots, X_n$ e com coeficientes num corpo $\mathbb{K}$,

é um anel fatorial.

OBSERVAÇÃO 0.1.2 - Seja K o corpo de fração de um anel fatorial A . Então, $K[X]$ é um anel com mdc ([9],pg.361) e um mdc de dois polinômios P e Q , não nulos simultaneamente, está determinado a menos de uma constante não nula (pois $U(K[X]) = K^*$), portanto, existe um único polinômio unitário em $K[X]$ que será chamado o mdc de P e Q ; indicaremos tal polinômio por $\text{mdc}(P,Q)$ que, por extensão, também será usado quando $P=Q=0$ caso este em que se tem $\text{mdc}(P,Q) = 0$.

DEFINIÇÃO 0.1.7 - Seja A um anel fatorial. Então, diz-se que um polinômio não nulo P em $A[X]$, dado sob a forma

$$P(X) = \sum_{i=0}^n a_i X^i, \quad n \in \mathbb{N},$$

é *primitivo* em $A[X]$ se um mdc de $\{a_0, \dots, a_n\}$ é associado a 1 em A .

LEMA 0.1.1 ([9],pg.381) - Seja A um anel fatorial. Então, um elemento $d \in A$ é um mdc dos coeficientes de um polinômio não nulo P em $A[X]$ se, e somente se, existe um polinômio primitivo P^* em $A[X]$ tal que $P = dP^*$.

COROLÁRIO 0.1.1 - Se P é um polinômio não nulo de $A[X]$ e se $P = dP^* = d_1 P_1^*$, onde $d, d_1 \in A$ e P^*, P_1^* são primitivos em $A[X]$, então d e d_1 são associadas em A .

LEMA 0.1.2 ([9],pg.381) - O produto de dois polinômios primiti-

vos é primitivo.

LEMA 0.1.3 ([9],pg.382) - Seja $\mathbb{K}$ o corpo de frações de um anel fatorial A . Então, para todo polinômio não nulo P , de $\mathbb{K}[X]$, existem $a, b \in A^*$ e $P^* \in A[X]$ primitivo tais que $P = \frac{a}{b} P^*$.

LEMA 0.1.4 - Seja A um anel fatorial e seja P um polinômio em $A[X]$. Então, valem as seguintes propriedades:

- 1) $a \in A$ é um divisor de P em $A[X]$ se, e somente se, a é um divisor de todos os coeficientes de P em A .
- 2) Se $a \in A$ é um divisor de P em $A[X]$ então a é um divisor de P' em $A[X]$ (P' = derivada de P).

PROVA -

- 1) Se a divide P em $A[X]$, existe $Q \in A[X]$ tal que $P = aQ$; donde $\partial P = \partial Q$. Suponhamos que $P = \sum_{i=0}^n a_i X^i$, $a_n \neq 0$, $n \in \mathbb{N}$, e $Q = \sum_{i=0}^n b_i X^i$, $b_n \neq 0$. Então, $a_i = ab_i$, $0 \leq i \leq n$; donde a divide a_i em A . Reciprocamente, se $a_i = ab_i$, $0 \leq i \leq n$, com $b_i \in A$, seja Q como acima. Então, $P = aQ$ e portanto a divide P em $A[X]$.
- 2) Se $P = aQ$, com $Q \in A[X]$ então $P' = aQ'$ e como $Q' \in A[X]$ segue que a divide P' em $A[X]$.

LEMA 0.1.5 ([10],pg.155) - Se P e $Q \neq 0$ são dois polinômios em $\mathbb{K}[X]$, $\mathbb{K}$ um corpo qualquer, e se R é o resto da divisão de P por Q então $\text{mdc}(P, Q) = \text{mdc}(Q, R)$.

LEMA 0.1.6 ([10],pg.177) - Seja $\mathbb{K}$ um corpo e seja P um polinômio

não constante em $\mathbb{K}[X]$. Então, P possui um fator múltiplo (não constante) em $\mathbb{K}[X]$ se, e somente se, $\text{mdc}(P, P') \neq 1$.

LEMA 0.1.7 ([10].pg.178) - Se $\mathbb{K}$ é um corpo e P um polinômio não constante em $\mathbb{K}[X]$, sendo

$$P = k P_1^{\alpha_1} P_2^{\alpha_2} \dots P_v^{\alpha_v}, \quad k \in \mathbb{K}^*$$

a decomposição canônica de P , então,

$$\text{mdc}(P, P') = P_1^{\alpha_1-1} P_2^{\alpha_2-1} \dots P_v^{\alpha_v-1}.$$

COROLÁRIO 0.1.2 - Se $D = \text{mdc}(P, P')$ então $Q = PD^{-1}$ é um polinômio que tem as mesmas raízes que P , exceto que todas as raízes de Q são simples.

LEMA 0.1.8 - Seja $\mathbb{K}$ o corpo de frações de um anel fatorial A e seja P um polinômio não constante em $A[X]$. Então,

- 1) Se P possui um fator não trivial em $\mathbb{K}[X]$ então P possui um fator não trivial em $A[X]$.
- 2) Se P possui um fator múltiplo, de grau maior que zero, em $\mathbb{K}[X]$ então P possui um fator múltiplo em $A[X]$, de grau maior que zero.
- 3) Seja $Q \in A[X]$. P e Q possuem um fator comum não constante em $\mathbb{K}[X]$ se, e somente se, P e Q possuem um fator comum não constante em $A[X]$.

PROVA -

- 1) Seja $D \in \mathbb{K}[X]$ irredutível em $\mathbb{K}[X]$ tal que D seja divi-

sor não trivial de P em $\mathbb{K}[X]$ e $\partial D \geq 1$. Então, existe $Q \in \mathbb{K}[X]$ tal que $P = DQ$ e $\partial Q \geq 1$. Pelo Lema 0.1.3 existem $a_1, a_2 \in A^*$ e $D^* \in A[X]$ primitivo tais que

$$(0.1.3) \quad D = \frac{a_1}{a_2} D^*$$

e chamando $\Phi = \frac{a_1}{a_2} Q$, pelo mesmo lema, existem $b_1, b_2 \in A^*$ e $\Phi^* \in A[X]$ primitivo tais que

$$(0.1.4) \quad \Phi = \frac{b_1}{b_2} \Phi^* \text{ (e portanto } \partial \Phi^* \geq 1 \text{)}.$$

Por outro lado, pelo Lema 0.1.1, existem $d \in A$ e $P^* \in A[X]$ primitivo tais que

$$(0.1.5) \quad P = dP^*$$

Logo, como $P = DQ$, por (0.1.3), (0.1.4) e (0.1.5) tem-se $dP^* = P = DQ = \frac{b_1}{b_2} D^* \Phi^*$; mas, pelo Lema 0.1.2, $D^* \Phi^*$ é primitivo em $A[X]$ e sendo P^* primitivo em $A[X]$, pelo Corolário 0.1.1, existe $u \in U(A)$ tal que $P^* = uD^* \Phi^*$, donde, como $P = dP^* = D^*(u\Phi^*)$ e $(u\Phi^*) \in A[X]$ segue que D^* divide P em $A[X]$. Como $\partial \Phi^* \geq 1$, e portanto $\partial(u\Phi^*) \geq 1$, segue que D^* é um divisor não trivial de P em $A[X]$.

- 2) Segue por um argumento similar ao feito em 1): Se D é um fator múltiplo de P em $\mathbb{K}[X]$ então D^* é um fator múltiplo de P em $A[X]$.
- 3) Também a prova é análoga as anteriores.

LEMA 0.1.9 - Seja $\mathbb{K}$ o corpo de frações de um anel fatorial A e seja P um polinômio não constante em $A[X]$. Então,

- 1) P e P' possuem um fator comum não constante em $\mathbb{K}[X]$ se, e somente se, P possui um fator múltiplo em $A[X]$ de grau maior que zero
- 2) Se $D \in A[X]$ é um mdc de P e P' em $A[X]$ então P e PD^{-1} tem os mesmos fatores irredutíveis em $A[X]$, exceto que PD^{-1} não tem fatores repetidos.

PROVA - 1) Segue dos lemas (0.1.6), (0.1.7) e (0.1.8).

- 2) Seja $P = ua_1^{\alpha_1} \dots a_{\mu}^{\alpha_{\mu}} P_1^{\beta_1} \dots P_v^{\beta_v}$ (onde $u \in U(A[X]) = U(A)$, $a_i \in A$, $1 \leq i \leq \mu$, é irredutível e $P_i \in A[X] \setminus A$, $1 \leq i \leq v$, é irredutível) a decomposição canônica de P em $A[X]$ (vide a Observação 0.1.1) e seja $M \in \mathbb{K}[X]$ o mdc de P e P' em $\mathbb{K}[X]$. Então, pelo Lema 0.1.7, segue que $M = P_1^{\beta_1-1} \dots P_v^{\beta_v-1}$; mas, existe $k \in \mathbb{K}^*$ tal que $M = kD$ (vide a Observação 0.1.2). Logo, $D = k^{-1} P_1^{\beta_1-1} \dots P_v^{\beta_v-1}$ e portanto $PD^{-1} = uka_1^{\alpha_1} \dots a_{\mu}^{\alpha_{\mu}} P_1 \dots P_v$; donde PD^{-1} tem os mesmos fatores irredutíveis de grau maior que zero em $A[X]$ que P , mas com fatores não repetidos.

TEOREMA 0.1.2 ([9], pg.289) - Sejam P e $F \neq 0$ polinômios em $A[X]$, onde A é um anel comutativo com elemento unidade; suponhamos que $\partial F = n$ e que $\partial P \leq m$. Se a_n é o coeficiente dominante de F e se $k = \max\{m-n+1, 0\}$ então existem polinômios Q e R em $A[X]$ tais que $a_n^k P = FQ + R$, onde $\partial R < n = \partial F$, se $R \neq 0$.

COROLÁRIO 0.1.3 - Se P e $F \neq 0$ são dois polinômios na indeterminada

nada X e com coeficientes num corpo $\mathbb{K}$ então existe um único par (Q, R) , de elementos de $\mathbb{K}[X]$, tal que $P = FQ + R$ onde $\partial R < \partial F$, se $R \neq 0$.

LEMA 0.1.10 - Sejam P e $P_1 \neq 0$ polinômios em $A[X]$, onde A é um anel de integridade, tais que $\partial P_1 \leq \partial P$. Então, existem polinômios $Q_1, \dots, Q_v, P_2, \dots, P_v$ em $A[X]$ e elementos correspondentes $a_1, \dots, a_v$ em A^* tais que

$$a_1 P = P_1 Q_1 - P_2, \partial P_2 < \partial P_1, \text{ se } P_2 \neq 0$$

$$(0.1.6) \quad a_2 P_1 = P_2 Q_2 - P_3, \partial P_3 < \partial P_1, \text{ se } P_3 \neq 0$$

[illegible]

$$a_{\nu} p_{\nu-1} = p_{\nu} q_{\nu} \quad (\text{i.e., } p_{\nu+1} = 0).$$

PROVA - A prova será por indução finita sobre $m = \partial P + \partial P_1$. De fato, se $m = 0$ ou $m = 1$ o lema é imediato. Suponhamos, então, que o lema seja verdadeiro para todo par de polinômios F e G em $A[X]$, com $(\partial F + \partial G) \leq m-1$. Pelo Teorema 0.1.2, existem $a_1 \in A^*$ e polinômios Q_1 e R em $A[X]$ tais que

$$a_1 P = P_1 Q_1 + R, \quad \partial P < \partial P_1, \quad \text{se } R \neq 0.$$

Seja $P_2 = -R$. Se $P_2 = 0$ então o lema está provado. Suponhamos que $P_2 \neq 0$. Como A é um anel de integridade tem-se $\partial P_2 = \partial R < \partial P_1$ e como $\partial P_1 \leq \partial P$ segue que $\partial P_1 + \partial P_2 < \partial P + \partial P_1 = m$. Portanto, pela hipótese de indução (aplicado aos polinômios P_1 e P_2), existem polinômios $Q_2, \dots, Q_v, P_3, \dots, P_v$ em $A[X]$ e elementos

correspondentes $a_2, \dots, a_v$ em A^* tais que

$$\begin{aligned} a_2 P_1 &= P_2 Q_2 - P_3, \quad \partial P_3 < \partial P_2, \quad \text{se } P_3 \neq 0 \\ &\vdots \\ a_i P_{i-1} &= P_i Q_i - P_{i+1}, \quad \partial P_{i+1} < \partial P_i, \quad \text{se } P_{i+1} \neq 0 \\ &\vdots \\ a_v P_{v-1} &= P_v Q_v \text{ (i.e., } P_{v+1} = 0). \quad \blacksquare \end{aligned}$$

COROLÁRIO 0.1.4 - Nas hipóteses e notações do Lema. Se A é um anel fatorial e se $\mathbb{K}$ é o corpo de frações de A então

- 1) $M = P_v$ é um mdc de P e P_1 em $\mathbb{K}[X]$.
- 2) existem ϕ e ϕ_1 em $A[X]$ tais que $M = \phi P + \phi_1 P_1$.

PROVA -

- 1) Sejam $b_i \in \mathbb{K}^*$, $1 \leq i \leq v$, tais que $a_i b_i = 1$. Então, por (0.1.6)

$$P = P_1(b_1 Q_1) - b_1 P_2$$

$$P_1 = b_1 P_2(a_1 b_2 Q_2) - b_2 P_3$$

$$b_1 P_2 = b_2 P_3(b_1 a_2 b_3 Q_3) - b_3 P_4$$

$$\vdots$$

$$b_{v-3} P_{v-2} = b_{v-2} P_{v-1}(b_{v-3} a_{v-2} b_{v-1} Q_{v-1}) - b_{v-1} P_v$$

$$b_{v-2} P_{v-1} = b_{v-1} P_v(b_{v-2} a_{v-1} b_v Q_v),$$

Como $(b_{v-1} P_v)$ divide $(b_{v-2} P_{v-1})$ em $\mathbb{K}[X]$ resulta que

$$\text{mdc}(b_{v-2}P_{v-1}, b_{v-1}P_v) = k^{-1}b_{v-1}P_v,$$

onde $k \in \mathbb{K}^*$ é o coeficiente dominante de $(b_{v-1}P_v)$. Por outro lado, o Lema 0.1.5 nos mostra que

$$\text{mdc}(P, P_1) = \text{mdc}(P_1, b_1 P_2)$$

$$\text{mdc}(P_1, b_1 P_2) = \text{mdc}(b_1 P_2, b_2 P_3)$$

.....

$$\text{mdc}(b_{v-3}P_{v-2}, b_{v-2}P_{v-1}) = \text{mdc}(b_{v-2}P_{v-1}, b_{v-1}P_v).$$

Portanto, $\text{mdc}(P, P_1) = (k^{-1}b_{v-1})P_v$ e como $(k^{-1}b_{v-1}) \in \mathbb{K}^*$ segue que $M = P_v$ é um mdc de P e P_1 em $\mathbb{K}[X]$.

- 2) Em (0.1.6) observamos que $P_2 = (-a_1)P + Q_1P_1$ e portanto $P_3 = Q_2P_2 - a_2P_1 = (-a_1Q_2)P + (Q_1Q_2 - a_2)P_1$. Logo, por indução, podemos achar $\Phi_{v-2}, \Psi_{v-2}, \Phi_{v-1}$ e Ψ_{v-1} em $A[X]$ tais que $P_{v-2} = \Phi_{v-2}P + \Psi_{v-2}P_1$ e $P_{v-1} = \Phi_{v-1}P + \Psi_{v-1}P_1$. Portanto, como $P_v = (-a_{v-1})P_{v-2} + Q_{v-1}P_{v-1}$, segue que $P_v = (\Phi_{v-1}Q_{v-1} - a_{v-1}\Phi_{v-2})P + (\Psi_{v-1}Q_{v-1} - a_{v-1}\Psi_{v-2})P_1$ o que implica 2). ■

LEMA 0.1.11 - Seja $\mathbb{K}$ o corpo de frações de um anel fatorial A . Sejam P_1 e P_2 dois polinômios não constantes em $A[X]$, X uma variável, e seja $D \in A[X]$ um mdc de P_1 e P_2 em $\mathbb{K}[X]$. Sejam p_1, p_2, d em A^* e P_1^*, P_2^*, D^* primitivos em $A[X]$ tais que $P_i = p_i P_i^*$, $i=1,2$, e $D = d D^*$. Se m é um mdc de p_1 e p_2 em A então $\tilde{D} = m D^*$

$\tilde{e}$ um mdc de P_1 e P_2 em $A[X]$.

PROVA -

1) $\tilde{D}$ divide P_1 e P_2 em $A[X]$. De fato, como D divide P_i ($i=1,2$) em $K[X]$, existe $Q_i \in K[X]$ tal que $P_i = DQ_i$. Pelo Lema 0.1.3, existem $a_i, b_i \in A^*$ e Q_i^* primitivo em $A[X]$ tais que $Q_i = \frac{a_i}{b_i} Q_i^*$; donde, $p_i P_i^* = P_i = DQ_i = d \frac{a_i}{b_i} D^* Q_i^*$. Pelo Lema 0.1.2, o polinômio $D^* Q_i^*$ é primitivo em $A[X]$ e sendo P_i^* primitivo em $A[X]$ (e $b_i p_i P_i^* = d a_i D^* Q_i^*$), pelo Corolário 0.1.1, existe $u_i \in U(A)$ tal que $P_i^* = D^* (u_i Q_i^*)$. Mas, como m divide p_i em A , existe $q_i \in A$ tal que $p_i = m q_i$; logo, $P_i = p_i P_i^* = (m D^*) (q_i u_i Q_i^*)$ e como $(q_i u_i Q_i^*) \in A[X]$ segue que $\tilde{D} = m D^*$ divide P_i $i = 1, 2$, em $A[X]$.

2) Agora provaremos que se $HEA[X]$ divide P_1 e P_2 em $A[X]$ então H divide $\tilde{D}$ em $A[X]$. De fato, sejam $F_i \in A[X]$, $i = 1, 2$, tais que $P_i = H F_i$. Pelo Lema 0.1.1, existem $h, a_i \in A^*$ e H^*, F_i^* primitivos em $A[X]$ tais que $H = h H^*$ e $F_i = a_i F_i^*$; donde $p_i P_i^* = P_i = H F_i = h a_i H^* F_i^*$. Pelo Lema 0.1.2, $H^* F_i^*$ é primitivo em $A[X]$ e sendo P_i^* primitivo em $A[X]$, pelo Corolário 0.1.1, existe $u_i \in U(A)$ tal que $p_i = h(u_i a_i)$; isto é, h divide p_1 e p_2 em A ; logo, h divide m em A e portanto existe $q \in A$ tal que $m = h q$. Por outro lado, pela hipótese, segue que H divide P_1 e P_2 em $K[X]$ e portanto H divide D em $K[X]$; logo, e-

xiste $F \in \mathbb{K}[X]$ tal que $D = HF$. Pelo Lema 0.1.3, existem $a, b \in A^*$ e F^* primitivo em $A[X]$ tal que $F = \frac{a}{b} F^*$; donde $dD^* = D = HF = h \frac{a}{b} H^* F^*$. Sendo $H^* F^*$ e D^* primitivos em $A[X]$, pelo Corolário 0.1.1, existe $v \in U(A)$ tal que $D^* = vH^* F^*$; portanto, como $D = HF$ e $m = hq$, segue que $\bar{D} = mD^* = hqvH^* F^* = (hH^*)(qvF^*)$ e como $(qvF^*) \in A[X]$ resulta que $H = hH^*$ divide $\bar{D}$ em $A[X]$. ■

De modo análogo ao Lema 0.1.10, usando o Corolário 0.1.3, prova-se o seguinte

LEMA 0.1.12 - Sejam P e P_1 polinômios não nulos na indeterminada X e com coeficientes num corpo $\mathbb{K}$ tais que $\partial P_1 \leq \partial P$. Então, existem polinômios $q_1, \dots, q_v, P_2, \dots, P_v$ em $\mathbb{K}[X]$ tais que

$$\begin{aligned} P &= P_1 q_1 - P_2, \quad \partial P_2 < \partial P_1, \text{ se } P_2 \neq 0 \\ (0.1.6') \quad P_1 &= P_2 q_2 - P_3, \quad \partial P_3 < \partial P_2, \text{ se } P_3 \neq 0 \\ &\vdots \\ P_{v-1} &= P_v q_v \text{ (i.e., } P_{v+1} = 0). \end{aligned}$$

COROLÁRIO 0.1.5 - Com as hipóteses e notações do Lema. O polinômio P_v é um mdc de P e P_1 em $\mathbb{K}[X]$.

PROVA - Segue (usando o Lema 0.1.5) por um raciocínio análogo ao que foi feito na prova do Corolário 0.1.4, 1). ■

DEFINIÇÃO 0.1.8 - Seja A um anel fatorial e sejam P e Q polinô

mios em $A[X]$, X uma variável, dados sob a forma

$$P(X) = \sum_{i=0}^n a_i X^i, \quad Q(X) = \sum_{i=0}^m b_i X^i, \quad n > 0, \quad m > 0.$$

Então, a *resultante* $R(P, Q)$, de P e Q é o elemento de A dado por

$$R(P, Q) = \left| \begin{array}{ccccccc} a_0 & \dots & a_n & & & & \\ & \ddots & & \ddots & & & \\ & & & a_0 & \dots & a_n & \\ b_0 & \dots & b_m & & & & \\ & \ddots & & \ddots & & & \\ & & & b_0 & \dots & b_m & \end{array} \right| \left. \begin{array}{l} \\ \\ \\ \\ \\ \end{array} \right\} \begin{array}{l} m \text{ filas} \\ \\ \\ n \text{ filas} \end{array}$$

TEOREMA 0.1.3 ([17], pg.24) - Seja $\mathbb{K}$ o corpo de frações de um anel fatorial A e sejam P e Q polinômios em $A[X]$ dados como na definição anterior. Então, $R(P, Q) = 0$ se, e somente se, ou $a_n = 0 = b_m$ ou P e Q possuem um fator comum de grau maior que zero em $\mathbb{K}[X]$.

LEMA 0.1.13 ([12], pg.186) - Dado um polinômio P em $\mathbb{C}[Z_1, \dots, Z_n]$, com $\partial P = m \geq 0$, existe uma rotação T de $\mathbb{R}^n$ tal que $Q = PT$ é um polinômio na forma

$$Q(Z_1, \dots, Z_n) = a_0 Z_1^m + \sum_{k=0}^{m-1} Q_k(Z_2, \dots, Z_n) Z_1^k, \quad a_0 \neq 0,$$

onde $Q_k \in \mathbb{C}[Z_2, \dots, Z_n]$ e $\partial Q_k \leq m-k$.

DEFINIÇÃO 0.1.9 - Seja A um anel comutativo com elemento unida

de e seja $(S(I_n), o)$ o grupo simétrico de $I_n = \{1, \dots, n\}$. Um polinômio P em $A[X_1, \dots, X_n]$ diz-se *simétrico nas indeterminadas* $X_1, \dots, X_n$ se $P(X_1, \dots, X_n) = P(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ para todo $\sigma \in S(I_n)$.

Indicaremos por $S_n(A)$ o conjunto de todos os polinômios simétricos do anel $A[X_1, \dots, X_n]$. É claro que A é um subconjunto de $S_n(A)$ e $S_n(A)$ é um anel de polinômios sobre A . Consideremos

$$S_1 = \sum_{i=1}^n X_i, S_2 = \sum_{i < j} X_i X_j, \dots, S_n = X_1 X_2 \dots X_n$$

Então, prova-se ([9], p.334) que os polinômios $S_1, \dots, S_n$ são simétricos e são denominados *polinômios simétricos elementares (p.s.e) nas indeterminadas* $X_1, \dots, X_n$. Prova-se também que $A[S_1, \dots, S_n]$ é um subconjunto de $S_n(A)$ e o seguinte teorema prova a igualdade.

TEOREMA 0.1.4 (Teor.fundam.dos polinômios simétricos; [9], pg.336) -

1) A aplicação $\Phi: A[X_1, \dots, X_n] \longrightarrow S_n(A)$ definido por

$$\Phi(P) = P(S_1, \dots, S_n), P \in A[X_1, \dots, X_n]$$

é um A -isomorfismo.

2) Para todo polinômio simétrico $Q \in A[X_1, \dots, X_n]$ existe um único polinômio $P \in A[X_1, \dots, X_n]$ tal que $Q = P(S_1, \dots, S_n)$.

LEMA 0.1.14 - Seja $P \in \mathbb{Z}[X, Y, Z]$ o polinômio nas indeterminadas $X = (X_1, \dots, X_r)$, $Y = (Y_1, \dots, Y_s)$ e Z dado por

$$P(X,Y,Z) = \prod_{\substack{i \neq j \\ k \neq \ell}} [X_i - X_j]Z - (Y_k - Y_\ell)].$$

Então, existe um polinômio $Q \in \mathbb{Z}[X,Y,Z]$ tal que $P = Q(S_1, \dots, S_r, T_1, \dots, T_s, Z)$, onde $S_1, \dots, S_r$ são os p.s.e. nas variáveis $X_1, \dots, X_r$ e $T_1, \dots, T_s$ são os p.s.e. nas variáveis $Y_1, \dots, Y_s$.

PROVA - Consideremos o polinômio $f \in \mathbb{Z}[Y,W]$, W uma variável, da do por $f(Y,W) = \prod_{k \neq \ell} [W - (Y_k - Y_\ell)]$; logo,

$$(0.1.7) \quad f(Y,W) = \sum_{i=0}^{m-1} f_i(Y)W^i + W^m, \quad m = s(s-1), \quad f_i \in \mathbb{Z}[Y].$$

É claro que f (e portanto também os f_i) é invariante sob qualquer permutação das indeterminadas $Y_1, \dots, Y_s$; logo, os polinômios f_i são simétricos nas variáveis $Y_1, \dots, Y_s$ com coeficientes em $\mathbb{Z}$. Se $T_1 = \sum_{k=1}^s Y_k$, $T_2 = \sum_{k < \ell} Y_k Y_\ell, \dots, T_s = Y_1 Y_2 \dots Y_s$ então, pelo Teorema 0.1.4, para cada $f_i, 0 \leq i \leq m-1$, existe um único polinômio $g_i \in \mathbb{Z}[Y_1, \dots, Y_s]$ tal que

$$(0.1.8) \quad f_i(Y_1, \dots, Y_s) = g_i(T_1, \dots, T_s),$$

logo, por (0.1.7) e (0.1.8), se $T = (T_1, \dots, T_s)$ então

$$(0.1.9) \quad f(Y,W) = \sum_{i=0}^{m-1} g_i(T)W^i + W^m.$$

Por outro lado, é claro que, P pode ser escrito como

$$P = \prod_{i \neq j} f(Y, (X_i - X_j)Z);$$

donde, usando (0.1.9), tem-se

$$P = \prod_{i \neq j} \left[\sum_{k=0}^{m-1} g_k(T) (X_i - X_j)^k Z^k + (X_i - X_j)^m Z^m \right].$$

Logo,

$$(0.1.10) \quad P = \sum_{j=0}^{n-1} h_j(X, T) Z^j + h_n(X) Z^n, \quad n = mr(r-1), \quad h_j \in \mathbb{Z}[T][X], \quad h_n \in \mathbb{Z}[X].$$

Como o polinômio $P(X, Y, Z)$ é inalterado sob permutações das indeterminadas $X_1, \dots, X_r$ segue que os polinômios h_j , $1 \leq j \leq n$, são simétricos nas indeterminadas $X_1, \dots, X_r$. Novamente, se $S_1 = \sum_{i=1}^r X_i$, $S_2 = \sum_{i < j} X_i X_j$, $\dots$, $S_r = X_1 X_2 \dots X_r$ então, pelo Teorema 0.1.4 (aplicado para $A = \mathbb{Z}[T]$), para cada h_j existe um único polinômio $Q_j \in \mathbb{Z}[T][X_1, \dots, X_r]$ tal que $h_j = Q_j(S_1, \dots, S_r, T)$; donde, se $S = (S_1, \dots, S_r)$ então levando isto a (0.1.10) obtem-se

$$P(X, Y, Z) = \sum_{j=0}^n Q_j(S, T) Z^j. \quad \blacksquare$$

LEMA 0.1.15 - Seja P um polinômio em $\mathbb{C}[Z_1, \dots, Z_n]$, com $\partial P = m \geq 0$. Então, existe uma constante $C = C(P) > 0$ tal que

$$|P(x)| \leq C(1 + \|x\|^2)^{m/2}, \quad \text{para todo } x \in \mathbb{R}^n.$$

PROVA - Suponhamos que P tem a forma

$$P(Z) = \sum_{|\alpha| \leq m} a_\alpha Z^\alpha, \quad Z = (Z_1, \dots, Z_n),$$

onde $a_\alpha \in \mathbb{C}$, $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ e $|\alpha| = \alpha_1 + \dots + \alpha_n$. Então, para todo $x \in \mathbb{R}^n$, tem-se $|P(x)| \leq \sum |a_\alpha| |x^\alpha|$ e como $|x^\alpha| \leq \|x\|^\alpha$ (pois, $|x_i| \leq \|x\|$, $1 \leq i \leq n$) segue que $|P(x)| \leq \sum |a_\alpha| \|x\|^\alpha$. Se $C_1 = \max\{|a_\alpha| : |\alpha| \leq m\}$ então $|P(x)| \leq C_1 \sum \|x\|^\alpha$ para todo $x \in \mathbb{R}^n$. Mas, se $a \geq 0$ então $a^{(2|\alpha|)/m} \leq 1$, se $0 \leq a \leq 1$, e $a^{(2|\alpha|)/m} \leq a^2$, se $a \geq 1$ (pois $2|\alpha|/m \leq 2$); isto é, $a^{(2|\alpha|)/m} \leq a^2 + 1$, para todo $a \geq 0$. Logo, $\|x\|^{|\alpha|} \leq (1 + \|x\|^2)^{m/2}$ para todo $x \in \mathbb{R}^n$ e portanto existe $C_2 > 0$ tal que

$$|P(x)| \leq C_1 \sum_{|\alpha| \leq m} \|x\|^\alpha \leq C_2 (1 + \|x\|^2)^{m/2}, \text{ para todo } x \in \mathbb{R}^n. \quad \blacksquare$$

DEFINIÇÃO 0.1.10 - Seja A um subconjunto de $\mathbb{R}^m$. Então,

- 1) A é algébrico em $\mathbb{R}^m$ se existe um polinômio $P \in \mathbb{R}[X_1, \dots, X_m]$ tal que $A = \{x \in \mathbb{R}^m : P(x) = 0\}$.
- 2) A é um elemento de A_m se tem uma das seguintes formas

$$A = \{x \in \mathbb{R}^m : P(x) = 0\} \text{ ou } A = \{x \in \mathbb{R}^m : Q(x) \neq 0\} \text{ ou}$$

$$A = \{x \in \mathbb{R}^m : R(x) = 0 \text{ e } S(x) \neq 0\}$$

onde $P, Q, R, S \in \mathbb{R}[X_1, \dots, X_m]$.

- 3) A é semi-algébrico elementar (SAE) em $\mathbb{R}^m$ se existem $(r+s)$ -polinômios $P_i, Q_j \in \mathbb{R}[X_1, \dots, X_m]$, $1 \leq i \leq r$, $r \geq 0$, $1 \leq j \leq s$, $s \geq 0$, tais que

$$A = \{x \in \mathbb{R}^m : P_i(x) = 0, 1 \leq i \leq r, \text{ e } Q_j(x) > 0, 1 \leq j \leq s\}.$$

se $r = 0$, significa que $A = \{x \in \mathbb{R}^m : Q_j(x) > 0, 1 \leq j \leq s\}$. Análogo, se $s = 0$.

- 4) A é *semi-algêbrico* (SA) em $\mathbb{R}^m$ se A for uma reunião finita de SAE em $\mathbb{R}^m$.

LEMA 0.1.16 - Valem as seguintes propriedades:

- 1) todo conjunto algêbrico é um elemento de A_m .
- 2) uma intersecção finita de SAE é SAE.
- 3) todo elemento de A_m é SAE.
- 4) união e intersecção finita de SA é SA.
- 5) Intersecção finita de elementos de A_m é um elemento de A_m .
- 6) o complementar de um SA é SA.

PROVA -

- 1) Segue diretamente da definição: 1) e 2).
- 2) Sejam A e B SAE em $\mathbb{R}^m$. Então, por definição, existem polinômios $P_i, Q_j \in \mathbb{R}[X_1, \dots, X_m]$, $1 \leq i \leq r+s$, $1 \leq j \leq v+t$, tais que

$$A = \{x: P_i(x) = 0, 1 \leq i \leq r, \text{ e } P_i(x) > 0, r+1 \leq i \leq r+s\}, r \geq 0, s \geq 0$$

$$B = \{x: Q_j(x) = 0, 1 \leq j \leq t, \text{ e } Q_j(x) > 0, t+1 \leq j \leq t+v\}, t \geq 0, v \geq 0.$$

Logo, é claro que

$$A \cap B = \{x: \sum_{i=1}^r P_i^2(x) + \sum_{j=1}^t Q_j^2(x) = 0 \text{ e}$$

$$P_i(x) > 0, Q_j(x) > 0, r+1 \leq i \leq r+s, t+1 \leq j \leq t+v\}.$$

Assim, pela Definição 0.1.10, 3), $A \cap B$ é SAE em $\mathbb{R}^m$. No caso geral segue por indução.

- 3) segue da equivalência: $Q \neq 0 \iff Q^2 > 0$.
- 4) A reunião segue da Definição 0.1.10, 4) e a intersecção segue imediatamente de 2) e da Definição 0.1.10 4).
- 5) Sejam $A_i \in \mathcal{A}_m$, $1 \leq i \leq n$. Então pela Definição 0.1.10, 2), existem $P_i, Q_i \in \mathbb{R}[X_1, \dots, X_m]$ tais que $A_i = \{P_i(x) = 0 \text{ e } Q_i(x) \neq 0\}$. Logo, é claro que, $\bigcap_{i=1}^n A_i = \{x: \sum_{i=1}^n P_i^2(x) = 0 \text{ e } \prod_{i=1}^n Q_i(x) \neq 0\}$; donde, pela Definição 0.1.10, 2),
- $$\bigcap_{i=1}^n A_i \in \mathcal{A}_m.$$
- 6) Em virtude de 4) basta provar que o complementar de um SAE é SA. Seja A um SAE em $\mathbb{R}^m$. Então, pela Definição 0.1.10, 3), existem $P_i, Q_j \in \mathbb{R}[X_1, \dots, X_m]$, $1 \leq i \leq r$, $1 \leq j \leq s$, tais que $A = \{x: P_i(x) = 0, 1 \leq i \leq r, \text{ e } Q_j(x) > 0, 1 \leq j \leq s\}$, $r \geq 0, s \geq 0$; donde,

$$\mathbb{R}^m \setminus A = \bigcup_{i=1}^r \{x: P_i(x) \neq 0\} \cup \bigcup_{j=1}^s \{x: Q_j(x) \leq 0\}.$$

Por outro lado, cada

$$\{x: P_i(x) \neq 0\} = \{x: P_i^2(x) > 0\} \text{ e } \{x: Q_j(x) \leq 0\} = \{x: Q_j(x) = 0\} \cup \{x: Q_j(x) < 0\}$$

são SA em $\mathbb{R}^m$ (por 4)). Logo, também por 4), $\mathbb{R}^m \setminus A$ é SA

em $\mathbb{R}^m$. ■

DEFINIÇÃO 0.1.11 - Uma função $\phi = (\phi_1, \dots, \phi_m): \mathbb{R}^n \longrightarrow \mathbb{R}^m$ diz-se *polinomial* se cada $\phi_i \in \mathbb{R}[X_1, \dots, X_n]$, $1 \leq i \leq m$. Chamaremos *projeção* a uma aplicação de $\mathbb{R}^n$ sobre $\mathbb{R}^m$, $m \leq n$, da forma $(x_1, \dots, x_n) \longmapsto (x_{i_1}, \dots, x_{i_m})$, onde $\{i_1, \dots, i_m\}$ é um subconjunto ordenado de $\{1, \dots, n\}$.

LEMA 0.1.17 - Todo conjunto SA é imagem de algum conjunto algébrico por uma projeção.

PROVA - Provaremos primeiro que para cada SAE A em $\mathbb{R}^m$ existem $v = v_A \in \mathbb{N}$, $v \geq m$, e um conjunto algébrico $B = B_A$ em $\mathbb{R}^v$ tais que se $\pi: \mathbb{R}^v \longrightarrow \mathbb{R}^m$ é a projeção dada por $\pi(x_1, \dots, x_m, \dots, x_v) = (x_1, \dots, x_m)$ então $A = \pi(B)$. De fato, se A é SAE em $\mathbb{R}^m$ então, pela Definição 0.1.10, 3), existem $P_i, Q_j \in \mathbb{R}[X_1, \dots, X_m]$, $1 \leq i \leq r$, $1 \leq j \leq s$, tais que $A = \{x: P_i(x) = 0, 1 \leq i \leq r, \text{ e } Q_j(x) > 0, 1 \leq j \leq s\}$, $r \geq 0$, $s \geq 0$. Seja $v \in \mathbb{N}$, com $v \geq r+m$, e seja B o subconjunto de $\mathbb{R}^v$ dado por

$$B = \{x \in \mathbb{R}^v: P_i(x_1, \dots, x_m) = 0, 1 \leq i \leq r, \text{ e}$$

$$x_{m+j}^2 Q_j(x_1, \dots, x_m) - 1 = 0, 1 \leq j \leq s\}.$$

Então, B é algébrico em $\mathbb{R}^v$ e como

$$\exists x_{m+j} \in \mathbb{R}: x_{m+j}^2 Q_j(x_1, \dots, x_m) - 1 = 0 \iff Q_j(x_1, \dots, x_m) > 0$$

é claro que $A = \pi(B)$. Agora, seja A um SA em $\mathbb{R}^m$. Então, pela

Definição 0.1.10, 4), existem $A_1, \dots, A_n$ SAE em $\mathbb{R}^m$ tais que $A = \bigcup_{i=1}^n A_i$. Logo, pelo que vimos acima, existem $v_i \geq m$ e B_i (algébrico em $\mathbb{R}^{v_i}$), $1 \leq i \leq n$, tais que se π_i é a projeção correspondente então $A_i = \pi_i(B_i)$. Seja $v = \max\{v_i : 1 \leq i \leq n\}$ e seja $\pi: \mathbb{R}^v \rightarrow \mathbb{R}^m$ a projeção dada por $\pi(x_1, \dots, x_m, \dots, x_v) = (x_1, \dots, x_m)$. Então, é claro que, $A_i = \pi(B_i)$, $1 \leq i \leq n$, e $A = \pi(B)$, onde $B = \bigcup_{i=1}^n B_i$. Mas, B é algébrico em $\mathbb{R}^v$ devido ao fato $\prod_{i=1}^k P_i = 0$ se, e somente se, $P_i = 0$ para algum $i \in \{1, \dots, k\}$. ■

0.2 - O TEOREMA DE STURM

Nesta seção obteremos um resultado clássico, o Teorema de Sturm, o qual dá um método para determinar o número exato de raízes reais distintas de um polinômio $P \in \mathbb{R}[X]$ e tal resultado será fortemente usado na prova do Teorema de Seidenberg-Tarski.

DEFINIÇÃO 0.2.1 - Se $x = \{x_1, \dots, x_n\}$ é uma sequência finita de elementos não nulos de $\mathbb{R}$ definimos o número de variações de sinal em x , denotado por $V(x)$, como sendo o número dos i 's, $1 \leq i \leq v-1$, tal que $x_i x_{i+1} < 0$, isto é,

$$V(x) = |\{i=1, \dots, v-1 : x_i x_{i+1} < 0\}|$$

onde $|A|$ indica o cardinal de A . Se $x = \{x_1, \dots, x_v\}$ é uma sequência arbitrária de elementos de $\mathbb{R}$, definimos o número de

variações de sinal em x , como sendo o número de variações de sinal da sequência reduzida x_0 obtida eliminando os zeros de x .

DEFINIÇÃO 0.2.2 - Seja P um polinômio em $\mathbb{R}[X]$, X uma variável e sejam $a, b \in \mathbb{R}$. Então diremos que a sequência $S_P = \{P_0=P, P_1, \dots, P_v\}$, $v \geq 1$, é uma sequência de Sturm para P no intervalo $[a, b]$ se $P_i \in \mathbb{R}[X]$, $1 \leq i \leq v$, e

$S_1)$ P_v não tem raízes em $[a, b]$

$S_2)$ $P(a)P(b) \neq 0$

$S_3)$ se $x \in [a, b]$ é uma raiz de P_i , $0 < i < v$, então

$$P_{i-1}(x)P_{i+1}(x) < 0.$$

$S_4)$ se $P(x_0) = 0$ para $x_0 \in [a, b]$ então existem intervalos abertos $]a_1, x_0[$ e $]x_0, b_1[$ tais que $P_0(x)P_1(x) < 0$ para todo $x \in]a_1, x_0[$ e $P_0(x)P_1(x) > 0$ para todo $x \in]x_0, b_1[$.

DEFINIÇÃO 0.2.3 - Seja P um polinômio em $\mathbb{K}[X]$, X uma variável e $\mathbb{K}$ um corpo qualquer. Então, definimos a sequência padrão associada a P como sendo $S(P, P') = \{P_0, P_1, \dots, P_v\}$, onde os polinômios P_i , $2 \leq i \leq v$, são determinados pelo Lema 0.1.12, aplicado aos polinômios P e $P_1 = P'$ (vide (0.1.6')).

Notemos que se $\mathbb{K} = \mathbb{R}$ e se P tem raízes múltiplas então a sequência padrão $S(P, P')$ não é uma sequência de Sturm para um intervalo contendo uma raiz múltipla de P (pois a condição (S_1) não será verificada); mesmo assim, podemos u-

sar a sequência padrão para determinar o número exato de raízes distintas de P num intervalo $]a, b[$, tal como veremos no Teorema 0.2.2. No que segue denotaremos por $V_x = V_P(x)$ o número de variações de sinal de sequência $\{P_0(x) = P(x), \dots, P_v(x)\}$ para todo $x \in \mathbb{R}$.

TEOREMA 0.2.1 - Seja P um polinômio em $\mathbb{R}[X]$ e seja $S_P = \{P_0 = P, \dots, P_v\}$ uma sequência de Sturm para P num intervalo $[a, b]$. Então, o número de raízes distintas de P em $]a, b[$ é $V_a - V_b$.

PROVA - As raízes dos polinômios P_i , $i \leq v$, determinam uma partição do intervalo $[a, b]$. Assim teremos uma sequência

$$a = t_0 < t_1 < \dots < t_m = b,$$

tal que nenhum dos P_i , $i \leq v$, tem uma raiz em cada $]t_j, t_{j+1}[$, $0 \leq j \leq m-1$, e tal que pelo menos um dos polinômios P_i se anula em cada t_j , se $j \neq 0, m$. A seguir provaremos as seguintes propriedades

$$T_1) \text{ se } x \in]a, t_1[\text{ então } V_x = V_a$$

$$T_2) \text{ se } x \in]t_{m-1}, b[\text{ então } V_x = V_b$$

$$T_3) \text{ se } 1 < j < m-1, x \in]t_{j-1}, t_j[\text{ e } y \in]t_j, t_{j+1}[\text{ então } V_x - V_y = 0, \text{ se } P(t_j) \neq 0 \text{ e } V_x - V_y = 1, \text{ se } P(t_j) = 0.$$

De fato. $T_1)$ se $x_0 \in]a, t_1[$ então nenhum dos P_i , $0 \leq i \leq v$, possui uma raiz em $]a, x_0[$; logo, pelo Teorema do valor médio, $P_i(a)P_i(x_0) \geq 0$ para $i=0, \dots, v$. Se para todo $i=0, \dots, v$ se tivesse $P_i(a) \neq 0$ então $P_i(a)P_i(x_0) > 0$, isto é, $P_i(a)$ e $P_i(x_0)$

tem o mesmo sinal, para todo $i=0, \dots, v$, logo $V_{x_0} = V_a$. Suponhamos que existe $k \in \{0, \dots, v\}$ tal que $P_k(a) = 0$. Como $P_v(a)P(a) \neq 0$, pelas propriedades $S_1)$ e $S_2)$, segue que $1 \leq k < v$. Logo, por $S_3)$, obtem-se

$$(0.2.1) \quad P_{k-1}(a)P_{k+1}(a) < 0.$$

Como P_{k-1} e P_{k+1} não possuem raízes em $]a, x_0[$ segue que

$$(0.2.2) \quad P_{k-1}(a)P_{k-1}(x_0) > 0 \text{ e } P_{k+1}(a)P_{k+1}(x_0) > 0;$$

logo, por (0.2.1) e (0.2.2), resulta que $P_{k-1}(x_0)P_{k+1}(x_0) < 0$. Assim, cada um dos trechos da sequência

$$P_{k-1}(a), 0, P_{k+1}(a) \text{ e } P_{k-1}(x_0), P_k(x_0), P_{k+1}(x_0)$$

contribuirão com uma variação de sinal para V_a e V_{x_0} respectivamente. Considerando todos os k 's tais que $P_k(a) = 0$ tem-se $V_{x_0} = V_a$.

$T_2)$ segue por um argumento similar a $T_1)$.

$T_3)$ sejam $j \in \{1, \dots, m-1\}$, $x \in]t_{j-1}, t_j[$ e $y \in]t_j, t_{j+1}[$. Se $P(t_j) \neq 0$, o mesmo raciocínio usado em $T_1)$ prova que $V_x = V_{t_j}$ e $V_y = V_{t_j}$; logo, $V_x - V_y = 0$. Suponhamos agora que $P(t_j) = 0$. Então, por $S_4)$, tem-se

$$(0.2.3) \quad P_0(x)P_1(x) < 0 \text{ e } P_0(y)P_1(y) > 0.$$

Logo, a sequência $P_0(x), P_1(x)$ tem uma variação de sinal ao passo que $P_0(y), P_1(y)$ não tem nenhum. Por outro lado, como

$P(t_j) = 0$, segue de S_3) que $P_1(t_j) \neq 0$. Logo,

$$(0.2.4) \quad P_1(x)P_1(y) > 0.$$

O argumento usado em T_1) prova que

$$(0.2.5) \quad V(\{P_1(x), \dots, P_v(x)\}) = V(\{P_1(t_j), \dots, P_v(t_j)\}) = \\ = V(\{P_1(y), \dots, P_v(y)\});$$

donde, de (0.2.3), (0.2.4) e (0.2.5), obtêm-se $V_x - V_y = 1$.

Finalmente, sejam $x_j \in]t_{j-1}, t_j[$, $1 \leq j \leq m$. Então,

$$V_a - V_b = (V_a - V_{x_1}) + \sum_{j=1}^{m-1} (V_{x_j} - V_{x_{j+1}}) + (V_{x_m} - V_b).$$

Logo, de T_1), T_2) e T_3), segue imediatamente que

$$V_a - V_b = \text{número de raízes distintas de } P \text{ em }]a, b[. \quad \blacksquare$$

TEOREMA 0.2.2 (de Sturm) - Seja P um polinômio em $\mathbb{R}[X]$ e seja $S(P, P')$ a sequência padrão associada a P . Seja $[a, b]$ um intervalo tal que $P(a)P(b) \neq 0$. Então, o número de raízes distintas de P em $]a, b[$ é $V_P(a) - V_P(b)$.

PROVA - Para cada $i \in \{0, \dots, v\}$ consideremos o polinômio Q_i dado por $Q_i = P_i P_v^{-1}$ (vide (0.1.6') e a Definição 0.2.3). Então, é claro que, P e Q_0 possuem as mesmas raízes (exceto pela multiplicidade) em $[a, b]$ e que Q_0 possui unicamente raízes simples (Corolário 0.1.2), pois P_v é um mdc de P e P' em

$\mathbb{R}[X]$ (Corolário 0.1.5). A seguir provaremos que $S_Q = \{Q_0, \dots, Q_v\}$ é uma sequência de Sturm para Q_0 em $[a, b]$. Com efeito, como $Q_v \equiv 1$ e $P(a)P(b) \neq 0$, S_1 e S_2 se verificam.

S_3) Seja $x_0 \in [a, b]$ tal que $Q_j(x_0) = 0$ para $0 < j < v$. Dividindo os polinômios em $S(P, P')$ por P_v obtemos $Q_{j-1} = q_j Q_j - Q_{j+1}$ (vide (0.1.6')); donde, $Q_{j-1}(x_0) = -Q_{j+1}(x_0)$ e portanto $Q_{j-1}(x_0)Q_{j+1}(x_0) \leq 0$, sendo $Q_{j-1}(x_0) = 0$ se, e só se, $Q_{j+1}(x_0) = 0$. Se $Q_{j-1}(x_0)Q_{j+1}(x_0) = 0$ então $0 = Q_{j-1}(x_0) = Q_j(x_0) = Q_{j+1}(x_0) = \dots = Q_v(x_0)$ o que contradiz $Q_v \equiv 1$. Logo, $Q_{j-1}(x_0)Q_{j+1}(x_0) < 0$.

S_4) Seja $x_0 \in [a, b]$ tal que $Q_0(x_0) = 0$. Então, $P(x_0) = 0$; logo, existe $(r, \phi) \in \mathbb{N}^* \times \mathbb{R}[X]$ tal que

$$(0.2.6) \quad P = (X - x_0)^r \phi \quad \text{e} \quad \phi(x_0) \neq 0$$

e portanto

$$(0.2.7) \quad P' = (X - x_0)^r \phi' + r(X - x_0)^{r-1} \phi.$$

Seja $\phi = c \phi_1^{\alpha_1} \dots \phi_s^{\alpha_s}$, $c \neq 0$, a decomposição canônica de ϕ em $\mathbb{R}[X]$. Então, como P_v é um mdc de P e P' em $\mathbb{R}[X]$ (Corolário 0.1.5), pelo Lema 0.1.7 existe $d \in \mathbb{R}$, $d \neq 0$ tal que

$$P_v = d(X - x_0)^{r-1} \phi_1^{\alpha_1-1} \dots \phi_s^{\alpha_s-1}.$$

Seja $\psi_1 = d \phi_1^{\alpha_1-1} \dots \phi_s^{\alpha_s-1}$. Então, $\psi_1(x_0) \neq 0$ e ψ_1 divide ϕ e ϕ' em $\mathbb{R}[X]$ (Lema 0.1.7); donde, existem $\psi_2, \psi_3 \in \mathbb{R}[X]$ tais que

$$(0.2.8) \quad \phi = \psi_1 \psi_2, \psi_2(x_0) \neq 0 \quad (\text{pois } \phi(x_0) \neq 0) \quad \text{e} \quad \phi' = \psi_1 \psi_3.$$

Sendo $P_v = (X-x_0)^{r-1} \Psi_1$, $\Psi_1(x_0) \neq 0$, de (0.2.6), (0.2.7) e (0.2.8) obtêm-se $Q_0 = (X-x_0) \Psi_2$, $\Psi_2(x_0) \neq 0$, e $Q_1 = (X-x_0) \Psi_3 + r \Psi_2$; assim $Q_1(x_0) = r \Psi_2(x_0)$. Logo, como $r > 0$, podemos escolher um intervalo $[a_1, b_1]$ tal que $x_0 \in]a_1, b_1[$ e $Q_1(x) \Psi_2(x) \neq 0$ para todo $x \in [a_1, b_1]$. Como além disso $r > 0$ e $Q_1(x_0) \Psi_2(x_0) = r \Psi_2^2(x_0) > 0$ segue pelo Teorema do valor médio que $Q_1(x) \Psi_2(x) > 0$ para todo $x \in [a_1, b_1]$. Logo, $Q_0 Q_1 = (X-x_0) Q_1 \Psi_2$ tem o mesmo sinal que $(X-x_0)$ em $[a_1, b_1]$; assim obtemos que $Q_0(x) Q_1(x) < 0$ para todo $x \in]a_1, x_0[$ e $Q_0(x) Q_1(x) > 0$ para todo $x \in]x_0, b_1[$. Acabamos, assim, de provar que S_Q é uma sequência de Sturm para Q_0 em $[a, b]$.

Finalmente, se P não tem raízes múltiplas então $\text{mdc}(P, P') = 1$ e portanto a sequência $S(P, P')$ difere de S_Q por um múltiplo não nulo em $\mathbb{R}$; logo, $S(P, P')$ é uma sequência de Sturm para P em $[a, b]$ e o teorema segue pelo Teorema 0.2.1. Em caso contrário, sendo S_Q uma sequência de Sturm para Q_0 em $[a, b]$, pelo Teorema 0.2.1 segue que $V_{Q_0}(a) - V_{Q_0}(b) = \text{número de raízes distintas de } Q_0 \text{ em }]a, b[$. Como $P_i = Q_i P_v$, $0 \leq i \leq v$, e $P_v(a) P_v(b) \neq 0$ (caso contrário teríamos $P(a) P(b) = 0$), é claro que, $V_{Q_0}(a) = V_P(a)$ e $V_{Q_0}(b) = V_P(b)$; logo, o teorema está demonstrado. ■

LEMA 0.2.1 - Seja P um polinômio em $\mathbb{R}[X]$, X uma variável, dado sob a forma

$$P = \sum_{i=0}^n a_i X^i, \quad a_n \neq 0, \quad n \in \mathbb{N}.$$

Seja $\lambda = (1+a_n^{-2}) (n + \sum_{i=0}^{n-1} a_i^2)$ se $n \neq 0$, e $\lambda = 1$ se $n = 0$. Então,

$$(0.2.9) \quad \{x \in \mathbb{R} : P(x)=0\} \subset]-\lambda, \lambda[$$

$$(0.2.10) \quad \exists x_0 \in \mathbb{R} : P(x_0)=0 \iff V_P(-\lambda) > V_P(\lambda)$$

PROVA - O caso $n = 0$ é evidente. Seja então $n \geq 1$. Afirmando

$$(0.2.11) \quad x \in \mathbb{R} \text{ e } |x| \geq 1 \implies \left| \sum_{i=1}^n a_i x^i \right| \geq |a_n x| - \sum_{i=1}^{n-1} |a_i|.$$

De fato, a prova será por indução finita sobre n . Seja $x \in \mathbb{R}$ tal que $|x| \geq 1$. Se $n = 2$ então, como $|a_1 x + a_2 x^2| = |x| |a_1 + a_2 x|$ e $|a_1 + a_2 x| \geq |a_2 x| - |a_1|$, tem-se $|a_1 x + a_2 x^2| \geq |a_2 x| - |a_1|$. Suponhamos, então, que (0.2.11) é verdadeira para toda soma $\sum_{i=1}^k a_i x^i$, com $k \leq n-1$. Consideremos uma soma $\sum_{i=1}^n a_i x^i$ com n termos. Como valem

$$\left| \sum_{i=1}^n a_i x^i \right| = |x| \left| a_1 + \sum_{i=1}^{n-1} a_{i+1} x^i \right|$$

$$\left| a_1 + \sum_{i=1}^{n-1} a_{i+1} x^i \right| \geq \left| \sum_{i=1}^{n-1} a_{i+1} x^i \right| - |a_1|$$

segue que

$$\left| \sum_{i=1}^n a_i x^i \right| \geq \left| \sum_{i=1}^{n-1} a_{i+1} x^i \right| - |a_1|;$$

donde, aplicando a hipótese de indução a $\sum_{i=1}^{n-1} a_{i+1} x^i$, tem-se

$$\left| \sum_{i=1}^n a_i x^i \right| \geq |a_n x| - \sum_{i=1}^{n-2} |a_{i+1}| - |a_1|$$

o que implica (0.2.11). Para provar (0.2.9) seja $x \in \mathbb{R}$ tal que $P(x) = 0$. Se $|x| < 1$, o resultado é imediato, pois $\lambda \geq 0$ e $n \geq 1$. Suponhamos, então, que $|x| \geq 1$. A igualdade $P(x) = 0$ pode ser escrita $-a_0 = \sum_{i=1}^n a_i x^i$; logo, por (0.2.11),

$$|a_0| \geq |a_n x| - \sum_{i=1}^{n-1} |a_i|; \text{ isto é, } |a_n x| \leq \sum_{i=0}^{n-1} |a_i|.$$

Mas, $|a_i| < 1 + a_i^2$, para todo $i \in \{0, \dots, n-1\}$; donde

$$|a_n x| < \left(n + \sum_{i=0}^{n-1} a_i^2 \right) \text{ e portanto } |x| < |a_n|^{-1} \left(n + \sum_{i=0}^{n-1} a_i^2 \right).$$

Como $|a_n|^{-1} < 1 + a_n^{-2}$ segue que

$$|x| < (1 + a_n^{-2}) \left(n + \sum_{i=0}^{n-1} a_i^2 \right)$$

o que implica (0.2.9). Por outro lado, como $P(-\lambda)P(\lambda) \neq 0$, pelo Teorema 0.2.2 tem-se que $V_P(-\lambda) - V_P(\lambda) = \text{número de raízes distintas de } P \text{ em }]-\lambda, \lambda[= |\{x \in]-\lambda, \lambda[: P(x) = 0\}|$. Mas, por (0.2.9)

$$\exists x_0 \in \mathbb{R}: P(x_0) = 0 \iff |\{x \in]-\lambda, \lambda[: P(x) = 0\}| > 0,$$

donde segue (0.2.10). ■

03 - DEFINIÇÕES E ALGUMAS PROPRIEDADES DAS DISTRIBUIÇÕES

No que segue Ω será um aberto qualquer de $\mathbb{R}^n$ e denotaremos por $\mathcal{D}(\Omega)$ o conjunto das funções pertencentes a $C^\infty(\Omega)$ cujos suportes são compactos contidos em Ω .

DEFINIÇÃO 0.3.1 - (1) Seja ϕ_j uma sequência de elementos de $\mathcal{D}(\Omega)$ e seja $\phi \in \mathcal{D}(\Omega)$. Dizemos que ϕ_j converge para ϕ em $\mathcal{D}(\Omega)$ se: (i) existe um compacto K contido em Ω tal que para todo j , o suporte de ϕ_j está contido em K ; (ii) para cada $\alpha \in \mathbb{N}^n$ (separadamente), a sequência $D^\alpha \phi_j$ converge para $D^\alpha \phi$ em Ω .

(2) Chamamos *distribuição sobre Ω* a qualquer forma linear T sobre $\mathcal{D}(\Omega)$ que é contínua no seguinte sentido: se $\phi_j \rightarrow \phi$ em $\mathcal{D}(\Omega)$ então $\langle T, \phi_j \rangle \rightarrow \langle T, \phi \rangle$ em $\mathbb{C}$. O conjunto de todas as distribuições sobre Ω será denotado por $\mathcal{D}'(\Omega)$.

(3) Sejam $T, T_j \in \mathcal{D}'(\Omega)$, $j \in \mathbb{N}$. Dizemos que a sequência T_j converge para T em $\mathcal{D}'(\Omega)$ se $\langle T_j, \phi \rangle \rightarrow \langle T, \phi \rangle$ em $\mathbb{C}$, para todo $\phi \in \mathcal{D}(\Omega)$.

TEOREMA 0.3.1 ([5], Apêndice) - Se $T: \mathcal{D}(\Omega) \rightarrow \mathbb{C}$ é linear, então T é contínua se, e somente se, para cada conjunto compacto K contido em Ω , existe $(C, k) \in]0, \infty[\times \mathbb{N}$ (dependendo de K) tal que

$$|\langle T, \phi \rangle| \leq C \sup_{|\alpha| \leq k, x \in K \text{ ou } \Omega} |(D^\alpha \phi)(x)|, \text{ para todo } \phi \in \mathcal{D}(\Omega) \text{ com } \text{supp} \phi \subset K.$$

DEFINIÇÃO 0.3.2 - Se $f \in L^1(\mathbb{R}^n)$, definimos sua *transformada de Fourier* Ff (ou $\hat{f}$) por

$$Ff(x) = \int_{\mathbb{R}^n} f(y) e^{-2\pi i \langle x, y \rangle} dy, \text{ para } x \in \mathbb{R}^n$$

onde $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$. A transformada conjugada (ou inversa) de Fourier $\bar{F}f$ é definido por

$$\bar{F}f(x) = \int_{\mathbb{R}^n} f(y) e^{2\pi i \langle x, y \rangle} dy, \text{ para } x \in \mathbb{R}^n.$$

DEFINIÇÃO 0.3.3 - (1) Denotamos por $S(\mathbb{R}^n)$ o conjunto das funções ϕ pertencentes a $C^\infty(\mathbb{R}^n)$ tais que

$$\sup_{x \in \mathbb{R}^n} |x^\beta D^\alpha \phi(x)| < \infty, \text{ para todo } \alpha, \beta \in \mathbb{N}^n.$$

(2) Se $\phi, \phi_j \in S(\mathbb{R}^n)$, $j \in \mathbb{N}$, dizemos que a sequência ϕ_j converge para ϕ em $S(\mathbb{R}^n)$ se para cada $(\alpha, k) \in \mathbb{N}^n \times \mathbb{N}$, a sequência $(1 + \|X\|^2)^k D^\alpha \phi_j$ converge uniformemente para $(1 + \|X\|^2)^k D^\alpha \phi$ em $\mathbb{R}^n$.

(3) Denotaremos por $S'(\mathbb{R}^n)$ o conjunto de todas as formas lineares T sobre $S(\mathbb{R}^n)$ que são contínuas (isto é, tais que se $\phi_j \rightarrow \phi$ em $S(\mathbb{R}^n)$ então $\langle T, \phi_j \rangle \rightarrow \langle T, \phi \rangle$ em $\mathbb{C}$). Os elementos de $S'(\mathbb{R}^n)$ são denominados *distribuições temperadas*.

(4) Se $T \in S'(\mathbb{R}^n)$, definimos sua transformada de Fourier $\hat{T}$ ou FT por

$$\langle \hat{T}, \phi \rangle = \langle T, \hat{\phi} \rangle, \text{ para } \phi \in S(\mathbb{R}^n).$$

Definimos a transformada conjugada $\bar{F}T$ de Fourier de T de modo a-

nálogo.

TEOREMA 0.3.2 (Fórmula de inversão de Fourier; [5], pg. 317) - A transformada de Fourier $F: S(\mathbb{R}^n) \longrightarrow S(\mathbb{R}^n)$ é bijetora e bicontínua, sendo sua inversa a transformada conjugada $\bar{F}$ de Fourier. Também vale o afirmado acima sobre $S'(\mathbb{R}^n)$.

DEFINIÇÃO 0.3.4 - Dizemos que uma função f mensurável em Ω é *localmente integrável* em Ω se

$$\int_K |f| < \infty, \text{ para todo compacto } K \subset \Omega.$$

Designamos por $L^1_{loc}(\Omega)$ o conjunto de todas as funções localmente integráveis em Ω , sendo que identificamos duas funções que só diferem num conjunto de medida nula.

DEFINIÇÃO 0.3.5 - Se $s \in \mathbb{R}$, denotaremos por $H^s(\mathbb{R}^n)$ o espaço vetorial $H^s(\mathbb{R}^n) = \{T \in S'(\mathbb{R}^n) : \hat{T} \text{ é uma função, em } L^1_{loc}(\mathbb{R}^n), \text{ e } (1 + \|X\|^2)^{s/2} \hat{T} \in L^2(\mathbb{R}^n)\}$, e denotamos por $H^s_{loc}(\Omega)$ o espaço vetorial

$$H^s_{loc}(\Omega) = \{T \in \mathcal{D}'(\Omega) : \phi T \in H^s(\mathbb{R}^n), \text{ para todo } \phi \in \mathcal{D}(\Omega)\}.$$

TEOREMA 0.3.3 (Fórmula de Leibnitz) - Sejam $\phi, \psi \in C^\infty(\Omega)$. Então

$$D^\alpha(\phi\psi) = \sum_{\beta \leq \alpha} \binom{\alpha}{\beta} \phi \cdot D^{\alpha-\beta} \psi, \quad \alpha \in \mathbb{N}^n.$$

PROVA - Segue sem muita dificuldade, por indução.

TEOREMA 0.3.4 (Fórmula generalizada de Leibnitz; [19], pg.51) - Seja $P(D)$ um ODPL e seja $(T, \phi) \in \mathcal{D}'(\Omega) \times C^\infty(\Omega)$. Então,

$$P(D)(\phi T) = \sum_{\alpha \in \mathbb{N}^n} D^\alpha \phi \cdot \frac{P^{(\alpha)}(D)T}{\alpha!}$$

TEOREMA 0.3.5 (de estrutura de distribuições; [19]; pg.100) - Seja $T \in \mathcal{D}'(\Omega)$. Então, para cada compacto K contido em Ω existem um número natural $m = m(T, K)$ e uma função $f = f(T, K, m) \in L^2(K)$ tais que

$$T = D^m f, \text{ onde } D^m = D_1^m \dots D_n^m \text{ e } D_j = \frac{1}{i} \frac{\partial}{\partial x_j}, \quad 1 \leq j \leq n.$$

TEOREMA 0.3.6 ([19], pg.191) - Se $(T, \phi) \in H^s(\mathbb{R}^n) \times \mathcal{D}(\mathbb{R}^n)$, $s \in \mathbb{R}$, então $(\phi T) \in H^s(\mathbb{R}^n)$.

CAPÍTULO I

O TEOREMA DE SEIDENBERG-TARSKI

Neste capítulo provaremos o teorema mencionado acima o qual afirma que *a imagem de um conjunto algébrico por uma projeção é um conjunto semi-algébrico*, que essencialmente é uma generalização do Teorema de Sturm em relação ao número de soluções reais de equações algébricas reais para o caso de várias variáveis.

1.1 - O ALGORITMO DE EUCLIDES E PROPRIEDADES

Aqui daremos alguns resultados algébricos de futura utilidade. Denotaremos por $A = A_m$ (vide a Definição 0.1.10 2)) e por $Z = (Z_1, \dots, Z_m)$, $m \in \mathbb{N}$. Além disso, se P é um polinômio em $\mathbb{R}[X, Y, Z]$, X e Y de uma variável, indicaremos por $\partial_X P$ ($\partial_Y P$) o grau de P considerado como um elemento de $\mathbb{R}[Y, Z][X]$ ($\mathbb{R}[X, Z][Y]$); isto é, considerado como um polinômio em X e com coeficientes pertencentes a $\mathbb{R}[Y, Z]$; por $\partial_{XY} P$ o grau de P considerado como um elemento de $\mathbb{R}[Z][X, Y]$ e por ∂P o grau

total de P . De modo análogo definimos $\partial_X P$ e ∂P para polinômios P em $\mathbb{R}[X, Z]$, X de uma variável.

LEMA 1.1.1 - (A) Se P é um polinômio em $\mathbb{R}[X, Z]$, com X uma variável, então existem (Γ_i, P_i) em $A \times \mathbb{R}[X, Z]$, $1 \leq i \leq r$, $r \geq 1$, tais que

$$(1.1.1) \quad \mathbb{R}^m \text{ é reunião disjunta dos } \Gamma_i, \quad 1 \leq i \leq r.$$

$$(1.1.2) \quad P(X, a) = P_i(X, a) \quad \text{e} \quad \partial P_i(X, a) = \partial_X P_i \quad \text{para todo} \\ a \in \Gamma_i, \quad 1 \leq i \leq r.$$

(B) Se Q é um polinômio em $\mathbb{R}[X, Y, Z]$ com X e Y uma variável, então existem (Δ_i, Q_i) em $A \times \mathbb{R}[X, Y, Z]$, $1 \leq i \leq s$, $s \geq 1$, tais que

$$(1.1.3) \quad \mathbb{R}^m \text{ é reunião disjunta dos } \Delta_i, \quad 1 \leq i \leq s$$

$$(1.1.4) \quad Q(X, Y, a) = Q_i(X, Y, a), \quad \partial Q_i(X, Y, a) = \partial_{XY} Q_i \quad \text{e} \\ \partial_Y Q_i(X, Y, a) = \partial_Y Q_i \quad \text{para todo } a \in \Delta_i, \quad 1 \leq i \leq s.$$

PROVA -

(A) Expressando o polinômio P sob a forma

$$P(X, Z) = \sum_{\alpha=0}^n p_{\alpha}(Z) X^{\alpha}, \quad p_{\alpha} \in \mathbb{R}[Z], \quad p_n \neq 0, \quad n \in \mathbb{N},$$

consideremos os seguintes elementos de A

$$\Gamma_i = \{a \in \mathbb{R}^m: p_i(a) \neq 0 \text{ e } \sum_{\alpha=i+1}^n p_\alpha^2(a) = 0\}, \quad 0 \leq i \leq n-1$$

$$\Gamma_n = \{a \in \mathbb{R}^m: p_n(a) \neq 0\}$$

$$\Gamma_{n+1} = \{a \in \mathbb{R}^m: \sum_{\alpha=0}^n p_\alpha^2(a) = 0\}.$$

Então, é claro que, $\mathbb{R}^m$ é reunião disjunta destes conjuntos; além disso, se $i \in \{0, \dots, n+1\}$ então $P(X, a) = P_i(X, a)$ para todo $a \in \Gamma_i$, se denominarmos $P_i(X, Z) = \sum_{\alpha=0}^i p_\alpha(Z) X^\alpha$, sendo $\partial P_i(X, a) = i = \partial_X P_i$ para todo $a \in \Gamma_i$, se $0 \leq i \leq n$; e $P_i(X, Z) = 0$, se $i = n+1$.

(B) Consideremos o polinômio Q sob a forma

$$Q(X, Y, Z) = \sum_{\alpha=0}^n \sum_{\beta=0}^{N_\alpha} q_{\alpha\beta}(Z) X^\beta Y^\alpha, \quad q_{\alpha\beta} \in \mathbb{R}[Z], \quad q_{\alpha N_\alpha} \neq 0, \quad n \in \mathbb{N},$$

e seja $N = \max\{\alpha + N_\alpha : \alpha = 0, \dots, n\}$. Então, $n \leq N$ e, é claro que, $\partial_{XY} Q = N$. Se $i \in \{0, \dots, N\}$ então para cada $j \leq i$, $j \leq k \leq i$ e $\ell \leq i - k$, com $j \leq n$ e $k \leq n$ consideremos o elemento de A

$$\Delta_{ijkl} = \{a \in \mathbb{R}^m: q_{j, i-j}(a) q_{k\ell}(a) \neq 0 \text{ e } \sum_{\alpha+\beta > i} q_{\alpha\beta}^2(a) + \sum_{\alpha > k, \beta \leq N} q_{\alpha\beta}^2(a) = 0\},$$

e seja $\Delta_0 \in A$ dado por

$$\Delta_0 = \{a \in \mathbb{R}^m: \sum_{\alpha=0}^n \sum_{\beta=0}^{N_\alpha} q_{\alpha\beta}^2(a) = 0\}.$$

Então, ve-se facilmente que, $\mathbb{R}^m$ é reunião disjunta dos conjuntos definidos acima, o que implica (1.1.3). Por outro lado, se $Q_{ijkl}(X,Y,Z) = \sum_{\alpha+\beta \leq i, \alpha \leq k} q_{\alpha\beta}(Z) X^\beta Y^\alpha$ então

$$Q(X,Y,a) = Q_{ijkl}(X,Y,a), \quad \partial Q_{ijkl}(X,Y,a) = i = \partial_{xy} Q_{ijkl}$$

$$\text{e } \partial_y Q_{ijkl}(X,Y,a) = k = \partial_y Q_{ijkl} \text{ para todo } a \in \Delta_{ijkl}.$$

Além disso, $Q(X,Y,a) \equiv 0$ para todo $a \in \Delta_0$. ■

LEMA 1.1.2 - Sejam P e $F \neq 0$ um par de polinômios em $\mathbb{R}[X,Z]$, com X uma variável. Então existem (Γ_i, Q_i, R_i) em $A \times \mathbb{R}(Z)[X] \times \mathbb{R}(Z)[X]$, $1 \leq i \leq r$, $r \geq 1$, onde $Q_i = G_i H_i^{-1}$, $R_i = \phi_i \psi_i^{-1}$, com $G_i, \phi_i \in \mathbb{R}[X,Z]$, $H_i, \psi_i \in \mathbb{R}[Z]$, tais que

$$(1.1.5) \quad \mathbb{R}^m \text{ é reunião disjunta dos } \Gamma_i, \quad 1 \leq i \leq r.$$

$$(1.1.6) \quad H_i(a) \psi_i(a) \neq 0 \text{ (portanto } Q_i(X,a) \text{ e } R_i(X,a) \text{ estão bem definidos), } \partial Q_i(X,a) = \partial G_i(X,a) = \partial_X G_i \text{ e } \partial R_i(X,a) = \partial \phi_i(X,a) = \partial_X \phi_i \text{ para todo } a \in \Gamma_i; \text{ além disso, } \partial P(X,a) \text{ e } \partial F(X,a) \text{ não dependem de } a \in \Gamma_i, \quad 1 \leq i \leq r.$$

$$(1.1.7) \quad P(X,a) = F(X,a) Q_i(X,a) - R_i(X,a), \text{ para todo } a \in \Gamma_i, \quad 1 \leq i \leq r, \\ \text{onde } \partial R_i(X,a) < \partial F(X,a), \text{ se } R_i(X,a) \neq 0 \text{ (a menos que } F(X,a) \equiv 0) \text{ e } \partial_X R_i < \partial_X F, \text{ se } R_i \neq 0.$$

PROVA - Pelo Lema 1.1.1 (A), existem (Γ_i, P_i) e (Γ'_j, IF_j) em $A \times \mathbb{R}[X,Y]$, $1 \leq i \leq r$, $r \geq 1$, $1 \leq j \leq s$, $s \geq 1$, satisfazendo, res-

pectivamente (1.1.1), (1.1.2) e

(1.1.1') $\mathbb{R}^m$ é reunião disjunta dos Γ'_j , $1 \leq j \leq l$

(1.1.2') $F(X,a) = \mathbb{F}_j(X,a)$ e $\partial \mathbb{F}_j(X,a) = \partial_X \mathbb{F}_j$ para todo $a \in \Gamma_i$, $1 \leq j \leq s$

Para cada $i = 1, \dots, r$ e $j = 1, \dots, s$ seja $\Gamma_{ij} = \Gamma_i \cap \Gamma'_j$. Então, pelo Lema 0.1.16 (5), $\Gamma_{ij} \in A$ e, por (1.1.1) e (1.1.1'), $\mathbb{R}^m$ é reunião disjunta destes conjuntos, o que prova (1.1.5). Por outro lado, sejam $\Gamma = \Gamma_{ij}$, $\mathbb{P} = \mathbb{P}_i$ e $\mathbb{F} = \mathbb{F}_j$, $1 \leq i \leq r$, $1 \leq j \leq s$, fixados. Se $\mathbb{P}(X,a) \equiv 0$ para todo $a \in \Gamma$ ou $\mathbb{F}(X,a) \equiv 0$ para todo $a \in \Gamma$ então (1.1.6) e (1.1.7) segue imediatamente. Suponhamos, então, que $\mathbb{P}(X,a)\mathbb{F}(X,a) \not\equiv 0$ para todo $a \in \Gamma$, o que ocorre por (1.1.2) e (1.1.2'). Logo, existe $(n,v) \in \mathbb{N}^2$ tal que

$$\mathbb{P}(X,Z) = \sum_{\alpha=0}^n p_{\alpha}(Z)X^{\alpha} \quad \text{e} \quad \mathbb{F}(X,Z) = \sum_{\alpha=0}^v f_{\alpha}(Z)X^{\alpha},$$

onde $p_{\alpha}, f_{\alpha} \in \mathbb{R}[Z]$ e $p_n(a)f_v(a) \neq 0$ para todo $a \in \Gamma$. Se $k = \max\{n-v+1, 0\}$ então, pelo Teorema 0.1.2 (aplicado ao par $\mathbb{P}$ e $\mathbb{F}$), existem polinômios Q^* e R^* em $\mathbb{R}[Z][X]$ tais que

$$f_v^k \mathbb{P} = \mathbb{F}Q^* + R^*, \quad \text{onde} \quad \partial_X R^* < \partial_X \mathbb{F}, \quad \text{se} \quad R^* \neq 0; \quad \text{logo,} \quad \mathbb{P} = \mathbb{F}Q^* f_v^{-k} + R^* f_v^{-k}.$$

Se escolhermos $Q = Q^* f_v^{-k}$ e $R = -R^* f_v^{-k}$ (portanto, $G = Q^*$, $\phi = -R^*$ e $H = f_v^{-k} = \psi$ no lema) então, por (1.1.2) e (1.1.2'), para todo $a \in \Gamma$ tem-se

$$P(X,a) = \mathbb{P}(X,a) = \mathbb{F}(X,a)Q(X,a) - R(X,a) = F(X,a)Q(X,a) - R(X,a)$$

sendo $\partial R(X,a) < v = \mathbb{F}(X,a) = \partial F(X,a)$, se $R(X,a) \neq 0$. Observe-mos que $\partial_X R = \partial_X R^* < \partial_X \mathbb{F} = v \leq \partial_X F$ e se $n < v$ então $Q \equiv 0$; se $n \geq v$ então $\partial_X Q^* = \partial_X Q = n-v$ e o coeficiente dominante de Q é $p_n f_v^{-1}$; como $p_n(a) f_v(a) \neq 0$ para todo $a \in \Gamma$, tem-se $\partial Q^*(X,a) = \partial Q(X,a) = n-v$ para todo $a \in \Gamma$. Se $\partial R(X,a)$ não for constante em Γ então, pelo Lema 1.1.1 (A), podemos subdividir este conjunto em um número finito de elementos de A satisfazendo (1.1.2). ■

COROLÁRIO 1.1.1 - Além das hipóteses do lema, seja Δ em A tal que $F(X,a) \neq 0$ e $F(X,a)$ divide $P(X,a)$ em $\mathbb{R}[X]$ para todo $a \in \Delta$. Então, existem (Δ_i, G_i, H_i) em $A \times \mathbb{R}[X, Z] \times \mathbb{R}[Z]$, $1 \leq i \leq s$, $s \geq 1$, tais que

$$(1.1.8) \quad \Delta \text{ é reunião disjunta dos } \Delta_i, \quad 1 \leq i \leq s.$$

$$(1.1.9) \quad H_i(a) \neq 0 \text{ e } \partial G_i(X,a) = \partial_X G_i \text{ para todo } a \in \Delta_i; \text{ além disso, } \partial P(X,a) \text{ e } \partial F(X,a) \text{ não dependem de } a \in \Delta_i, \quad 1 \leq i \leq r.$$

$$(1.1.10) \quad P(X,a) = H_i^{-1}(a) G_i(X,a) F(X,a), \text{ para todo } a \in \Delta_i, \quad 1 \leq i \leq r.$$

PROVA - Para cada $i \in \{1, \dots, r\}$ fixo, com as notações do lema, seja $\Delta_i = \Delta \cap \Gamma_i$. Então, pelo Lema 0.1.16 (5), $\Delta_i \in A$; além disso, por (1.1.5), Δ é reunião disjunta dos Δ_i o que prova (1.1.8). Por outro lado, como cada $F(X,a)$ divide $P(X,a)$, $a \in \Delta$, em (1.1.7) tem-se $R_i(X,a) \equiv 0$ para todo $a \in \Delta_i \subset \Delta$ e portanto, vale (1.1.10). Finalmente (1.1.9) segue de (1.1.6). ■

Uma consequência imediata deste Corolário é o

LEMA 1.1.3 - Seja (Γ, P, M) em $A \times \mathbb{R}[X, Y, Z] \times \mathbb{R}[X, Z]$, com X e Y uma variável, tal que $M(X, a) \neq 0$ e $M(X, a)$ é um mdc (em $\mathbb{R}[X]$) dos coeficientes de $P(X, Y, a)$, considerado como um elemento de $\mathbb{R}[X][Y]$, para todo $a \in \Gamma$. Então, existem (Γ_i, F_i, ψ_i) em $A \times \mathbb{R}[X, Y, Z] \times \mathbb{R}[Z]$, $1 \leq i \leq r$, $r \geq 1$, tais que

$$(1.1.11) \quad \Gamma \text{ é reunião disjunta dos } \Gamma_i, \quad 1 \leq i \leq r.$$

$$(1.1.12) \quad \begin{aligned} \psi_i(a) \neq 0, \quad F_i(X, Y, a) \text{ é primitivo em } \mathbb{R}[X][Y], \quad \partial M(X, a) = \text{cte}, \\ \partial F_i(X, Y, a) = \partial_{XY} F_i \text{ e } \partial_Y F_i(X, Y, a) = \partial_Y F_i \text{ para todo } a \in \Gamma_i, \\ 1 \leq i \leq r. \end{aligned}$$

$$(1.1.13) \quad P(X, Y, a) = \psi_i^{-1}(a) M(X, a) F_i(X, Y, a), \text{ para todo } a \in \Gamma_i, \quad 1 \leq i \leq r.$$

PROVA - Por comodidade de notação suporemos que $\partial_Y P = 1$ (a demonstração é análoga para $\partial_Y P > 1$); isto é, P tem a forma $P(X, Y, Z) = P_0(X, Z) + P_1(X, Z)Y$. Como $M(X, a)$ divide $P_0(X, a)$ em $\mathbb{R}[X](a \in \Gamma)$, pelo Corolário 1.1.1 (aplicado a (Γ, P_0, M)), existem (Γ_i, G_i, H_i) em $A \times \mathbb{R}[X, Z] \times \mathbb{R}[Z]$, $1 \leq i \leq s$, $s \geq 1$, satisfazendo (1.1.8), (1.1.9) e

$$(1.1.14) \quad P_0(X, a) = H_i^{-1}(a) G_i(X, a) M(X, a), \text{ para todo } a \in \Gamma_i, \quad 1 \leq i \leq s.$$

Por um argumento similar, aplicado a cada (Γ_i, P_1, M) ($1 \leq i \leq s$), existem $(\Gamma_{ij}, G_{ij}, H_{ij})$ em $A \times \mathbb{R}[X, Z] \times \mathbb{R}[Z]$, $1 \leq j \leq t_i$, $t_i \geq 1$, tais que

(1.1.8') Γ_i é reunião disjunta dos Γ_{ij}

(1.1.9') $H_{ij}(a) \neq 0$ e $\partial M(X,a) = \text{cte}$ para todo $a \in \Gamma_{ij}$

(1.1.15) $P_1(X,a) = H_{ij}^{-1}(a)G_{ij}(X,a)M(X,a)$, para todo $a \in \Gamma_{ij}$

Para cada $i \in \{1, \dots, s\}$ e $j \in \{1, \dots, t_i\}$ seja ψ_{ij} um mmc de H_i e H_{ij} em $\mathbb{R}[Z]$. Então, por (1.1.9) e (1.1.9'), $\psi_{ij}(a) \neq 0$ para todo $a \in \Gamma_{ij}$; além disso, por (1.1.14) e (1.1.15), é claro que existe um polinômio F_{ij} em $\mathbb{R}[X,Y,Z]$ tal que

$$P(X,Y,a) = \psi_{ij}^{-1}(a)M(X,a)F_{ij}(X,Y,a), \text{ para todo } a \in \Gamma_{ij},$$

o que implica (1.1.13). A condição (1.1.11) segue de (1.1.8) e (1.1.8'). Sendo $\psi_{ij}^{-1}(a)M(X,a)$ um mdc em $\mathbb{R}[X]$ dos coeficientes de $P(X,Y,a)$, $a \in \Gamma_{ij}$, pelo Lema 0.1.1 e pela última igualdade, $F_{ij}(X,Y,a)$ é primitivo em $\mathbb{R}[X][Y]$. Finalmente, se $\partial F_{ij}(X,Y,a)$ ou se $\partial_y F_{ij}(X,Y,a)$ não for constante em Γ_{ij} então, pelo Lema 1.1.1 (B), podemos subdividir este conjunto em um número finito de elementos de A satisfazendo (1.1.3) e (1.1.4); assim, os novos conjuntos satisfarão a última parte de (1.1.12). ■

LEMA 1.1.4 - Sejam P e $F \neq 0$ um par de polinômios em $\mathbb{R}[X,Z]$, com X uma variável. Então existem $(\Delta_i, Q_{ij}, R_{ij})$ em

$$A \times \mathbb{R}(Z)[X] \times \mathbb{R}(Z)[X], \quad 0 \leq j \leq v_i + 1, \quad v_i \geq 1, \quad 1 \leq i \leq r, \quad r \geq 1,$$

onde

$$Q_{ij} = G_{ij}H_{ij}^{-1}, R_{ij} = \phi_{ij}\psi_{ij}^{-1}, \text{ com } G_{ij}, \phi_{ij} \in \mathbb{R}[X, Z], H_{ij}, \psi_{ij} \in \mathbb{R}[Z],$$

tais que

$$(1.1.16) \quad \mathbb{R}^m \text{ é reunião disjunta dos } \Delta_i, 1 \leq i \leq r.$$

$$(1.1.17) \quad H_{ij}(a)\psi_{ij}(a) \neq 0 \text{ (portanto } Q_{ij}(X,a) \text{ e } R_{ij}(X,a) \text{ estão bem definidos), } \partial Q_{ij}(X,a) = \partial G_{ij}(X,a) = \partial_X G_{ij} \text{ e } \partial R_{ij}(X,a) = \partial \phi_{ij}(X,a) = \partial_X \phi_{ij} \text{ para todo } a \in \Delta_i; \text{ além disso, } \partial P(X,a) \text{ e } \partial F(X,a) \text{ não dependem de } a \in \Delta_i, 1 \leq i \leq r.$$

$$(1.1.18) \quad \text{se } i \in \{1, \dots, r\} \text{ então para todo } a \in \Delta_i \text{ tem-se}$$

$$P(X,a) = F(X,a)Q_{i0}(X,a) - R_{i0}(X,a), \partial R_{i0}(X,a) < \partial F(X,a), R_{i0}(X,a) \neq 0$$

$$F(X,a) = R_{i0}(X,a)Q_{i1}(X,a) - R_{i1}(X,a); \partial R_{i1}(X,a) < \partial R_{i0}(X,a), R_{i1}(X,a) \neq 0$$

$$\dots \dots \dots$$

$$R_{i\nu_i-1}(X,a) = R_{i\nu_i}(X,a)Q_{i\nu_i+1}(X,a) \text{ (i.e., } R_{i\nu_i+1}(X,a) \equiv 0).$$

PROVA - A prova será feita por indução finita sobre $n = \partial_X P + \partial_X F$. De fato, se $n=0$ ou $n=1$, o resultado é imediato. Suponhamos, então, que o lema seja verdadeiro para todo par de polinômios $G, H \in \mathbb{R}[X, Z]$ tal que $(\partial_X G + \partial_X H) \leq n-1$. Pelo Lema 1.1.2, existem (Γ_i, Q_i, R_i) em $A \times \mathbb{R}(Z)[X] \times \mathbb{R}(Z)[X]$, $1 \leq i \leq s$, $s \geq 1$, onde $R_i = \phi_i \psi_i^{-1}$, com $\phi_i \in \mathbb{R}[X, Z]$, $\psi_i \in \mathbb{R}[Z]$, satisfazendo (1.1.5), (1.1.6) e (1.1.7). Sejam $\Gamma = \Gamma_i$, $Q = Q_i$, $\phi = \phi_i$ e $\psi = \psi_i$, $1 \leq i \leq s$, fixados. Se $\phi = 0$ então o lema está provado. Suponhamos que $\phi \neq 0$. Então, por (1.1.7) $\partial_X R < \partial_X F \leq \partial_X F + \partial_X Q = \partial(FQ)$ e portanto $\partial_X P = \partial_X(FQ - R) = \partial_X(FQ) > \partial_X R$. Logo, $\partial_X(\psi F) + \partial_X \phi = \partial_X F + \partial_X R <$

$< \partial_X F + \partial_X P = n$. Assim, pela hipótese de indução (aplicado ao par $(\psi F, \phi)$), existem (A_j, Q_{jk}, R_{jk}) em $A \times \mathbb{R}(Z)[X] \times \mathbb{R}(Z)[X]$, $1 \leq k \leq v_j + 1$, $1 \leq j \leq t = t_i$, $v_j = v_{ij} \geq 1$, $t \geq 1$, satisfazendo (1.1.17) e

(1.1.19) Γ é reunião disjunta dos $\Delta_j = \Gamma \cap A_j$, $1 \leq j \leq t$

(1.1.20) se $j \in \{1, \dots, t\}$ então para todo $a \in \Delta_j$ tem-se

$$\psi(a)F(X,a) = \phi(X,a)Q_{j1}(X,a) - R_{j1}(X,a); \partial_{R_{j1}}(X,a) < \partial\phi(X,a), R_{j1}(X,a) \neq 0$$

$$\phi(X,a) = R_{j1}(X,a)Q_{j2}(X,a) - R_{j2}(X,a); \partial_{R_{j2}}(X,a) < \partial_{R_{j1}}(X,a), R_{j2}(X,a) \neq 0$$

$$R_{j1}(X,a) = R_{j2}(X,a)Q_{j3}(X,a) - R_{j3}(X,a); \partial_{R_{j3}}(X,a) < \partial_{R_{j2}}(X,a), R_{j3}(X,a) \neq 0$$

$$\dots \dots \dots$$

$$R_{jv_j-1}(X,a) = R_{jv_j}(X,a)Q_{jv_j+1}(X,a) \text{ (i.é, } R_{jv_j+1}(X,a) \equiv 0);$$

logo, de (1.1.7) e (1.1.20), segue imediatamente (1.1.18).
Notemos que cada $\Delta_j \in A$, devido ao Lema 0.1.16 (5). A condição (1.1.16) segue de (1.1.5) e (1.1.19). ■

COROLÁRIO 1.1.2 - Com as hipóteses e notações do lema. Se $M_i = \phi_{iv_i}$, $1 \leq i \leq r$, então $\partial_{M_i}(X,a) = \partial_X M_i$ e $M_i(X,a)$ é um mdc em $\mathbb{R}[X]$ dos polinômios $P(X,a)$ e $F(X,a)$ para todo $a \in \Delta_i$.

PROVA - Seja $i \in \{1, \dots, r\}$. Então, por (1.1.18) e pelo Corolário 0.1.5, tem-se que $R_{iv_i}(X,a)$ é um mdc de $P(X,a)$ e $F(X,a)$ em $\mathbb{R}[X]$, para todo $a \in \Delta_i$. Como $\psi_{iv_i}(a) \neq 0$ para todo $a \in \Delta_i$, segue que $M_i(X,a) = \psi_{iv_i}(a)R_{iv_i}(X,a)$ também é um mdc de $P(X,a)$

e $F(X,a)$ em $\mathbb{R}[X]$, para todo $a \in \Delta_i$. ■

LEMA 1.1.5 - Seja (Γ, P) em $A \times \mathbb{R}[X, Z]$, com X uma variável. Então, existem (Γ_i, P_i) em $A \times \mathbb{R}[X, Z]$, $1 \leq i \leq s$, $s \geq 1$, tais que

(1.1.23) Γ é reunião disjunta dos Γ_i , $1 \leq i \leq s$.

(1.1.24) $\partial P_i(X, a) = \partial_X P_i$ para todo $a \in \Gamma_i$, $1 \leq i \leq s$.

(1.1.25) $P_i(X, a)$ tem os mesmos fatores irredutíveis em $\mathbb{R}[X]$ que $P(X, a)$, mas com fatores não repetidos, para todo $a \in \Gamma_i$, $1 \leq i \leq s$.

PROVA - Pelo Corolário 1.1.2 (aplicado ao par (P, P_X) , onde P_X indica a derivada de P em relação a X), existem (Δ_i, M_i) em $A \times \mathbb{R}[X, Z]$, $1 \leq i \leq r$, $r \geq 1$, tais que

(1.1.26) Γ é reunião disjunta dos $\Lambda_i = \Gamma \cap \Delta_i$, $1 \leq i \leq r$

(1.1.27) $\partial M_i(X, a) = \partial_X M_i$, para todo $a \in \Lambda_i$, $1 \leq i \leq r$

(1.1.28) $M_i(X, a)$ é um mdc de $P(X, a)$ e $P_X(X, a)$ em $\mathbb{R}[X]$ para todo $a \in \Lambda_i$, $1 \leq i \leq r$.

Sejam $A = \Lambda_i$ e $M = M_i$, $1 \leq i \leq r$, fixados. Então, pelo Lema 0.1.16 (5), $A \in A$ e se $M(X, a) \equiv 0$ para todo $a \in A$, o resultado é imediato; pois, neste caso $P(X, a) \equiv 0$ para todo $a \in A$. Suponha_{mos} que $M(X, a) \not\equiv 0$ para todo $a \in A$, o que ocorre por (1.1.27). Então, por (1.1.28) e pelo Corolário 1.1.1 (aplicado a (A, P, M)),

existem (B_j, P_j, H_j) em $A \times \mathbb{R}[X, Z] \times \mathbb{R}[Z]$, $1 \leq j \leq t$, $t = t_i \geq 1$, tais que

$$(1.1.8) \quad A \text{ é reunião disjunta dos } B_j$$

$$(1.1.9) \quad H_j(a) \neq 0 \text{ e } \partial P_j(X, a) = \partial_X P_j \text{ para todo } a \in B_j, 1 \leq j \leq t.$$

$$(1.1.10) \quad P(X, a) = H_j^{-1}(a) M(X, a) P_j(X, a), \text{ para todo } a \in B_j, 1 \leq j \leq t.$$

Sejam $j \in \{1, \dots, t\}$ e $a \in B_j$. Então, como $H_j(a) \neq 0$, por (1.1.28) segue que $H_j^{-1}(a) M(X, a)$ é um mdc de $P(X, a)$ e $P_X(X, a)$ em $\mathbb{R}[X]$; logo, por (1.1.10) e pelo Lema 0.1.9 (2), tem-se que $P_j(X, a)$ tem os mesmos fatores irredutíveis em $\mathbb{R}[X]$ que $P(X, a)$, mas com fatores não repetidos, o que prova (1.1.25). A condição (1.1.23) obtém-se de (1.1.26) e (1.1.8)). Finalmente, (1.1.24) segue de (1.1.9). ■

LEMA 1.1.6 - Sejam $P_1, \dots, P_n$, $n \geq 2$, polinômios não nulos em $\mathbb{R}[X, Z]$, com X uma variável. Então, existem (Γ_i, M_i) em $A \times \mathbb{R}[X, Z]$, $1 \leq i \leq s$, $s \geq 1$, tais que

$$(1.1.29) \quad \mathbb{R}^m \text{ é reunião disjunta dos } \Gamma_i, 1 \leq i \leq s.$$

$$(1.1.30) \quad \partial M_i(X, a) = \partial_X M_i \text{ para todo } a \in \Gamma_i, \text{ além disso, o grau dos polinômios } P_j(X, a), 1 \leq j \leq n, \text{ não dependem de } a \in \Gamma_i, 1 \leq i \leq s.$$

$$(1.1.31) \quad M_i(X, a) \text{ é um mdc em } \mathbb{R}[X] \text{ dos polinômios } P_j(X, a), 1 \leq j \leq n, \text{ para todo } a \in \Gamma_i, 1 \leq i \leq s.$$

PROVA - O Lema 1.1.4, com seu Corolário 1.1.2, contém o Lema 1.1.6 no caso $n=2$. Para $n > 2$, o resultado segue por indução. ■

LEMA 1.1.7 - Seja (Γ, P, D) em $A \times \mathbb{R}[X, Y, Z] \times \mathbb{R}[X, Z]$, X uma variável, tal que $D(X, a) \neq 0$ e $D(X, a)$ divide $P(X, Y, a)$ em $\mathbb{R}[X, Z]$, para todo $a \in \Gamma$. Então, existem $(\Gamma_i, P_i, \phi_i, \psi_i)$ em $A \times \mathbb{R}[X, Y, Z] \times \mathbb{R}[X, Z] \times \mathbb{R}[Z]$, $1 \leq i \leq r$, $r \geq 1$, tais que

(1.1.32) Γ é reunião disjunta dos Γ_i , $1 \leq i \leq r$

(1.1.33) $\psi_i(a) \neq 0$, $\partial \phi_i(X, a) = \partial_X \phi_i$, $\partial D(X, a) = \text{cte}$, $P_i(X, Y, a)$ é primitivo em $\mathbb{R}[X][Y]$, $\partial P_i(X, Y, a) = \partial_{XY} P_i$ e $\partial_Y P_i(X, Y, a) = \partial_Y P_i$ para todo $a \in \Gamma_i$; além disso, o grau total (e o grau em Y) de $P(X, Y, a)$ não depende de $a \in \Gamma_i$, $1 \leq i \leq r$.

(1.1.34) $P(X, Y, a) = \psi_i^{-1}(a) \phi(X, a) D(X, a) P_i(X, Y, a)$, para todo $a \in \Gamma_i$, $1 \leq i \leq r$.

PROVA - Expressando o polinômio P sob a forma

$$P(X, Y, Z) = \sum_{\alpha=0}^n p_{\alpha}(X, Z) Y^{\alpha}, \quad p_{\alpha} \in \mathbb{R}[X, Z], \quad p_n \neq 0, \quad n \in \mathbb{N},$$

consideremos (Γ_i, M_i) em $A \times \mathbb{R}[X, Z]$, $1 \leq i \leq s$, $s \geq 1$, satisfazendo (1.1.29), (1.1.30) e (1.1.31) do Lema 1.1.6, aplicado aos polinômios p_{α} , $0 \leq \alpha \leq n$. Então, é imediato que Γ é reunião disjuntas dos $A_i = \Gamma \cap \Gamma_i$, $1 \leq i \leq s$, que são elementos de A , pelo Lema 0.1.16 (5). Sejam $A = A_i$ e $M = M_i$, $1 \leq i \leq s$, fixados. Se

$M(X,a) \equiv 0$ para todo $a \in A$ então $P(X,Y,a) \equiv 0$, $a \in A$, e o resultado é imediato. Suponhamos, então, que $M(X,a) \not\equiv 0$ para todo $a \in A$, o que ocorre por (1.1.30). Então, existem (B_j, F_j, ψ_j) em $A \times \mathbb{R}[X,Y,Z] \times \mathbb{R}[Z]$, $1 \leq j \leq t$, $t = t_i \geq 1$, satisfazendo (1.1.11), (1.1.12) e (1.1.13) do Lema 1.1.3, aplicado a (A,P,M) . Sejam $B = B_j$, $F = F_j$ e $\psi = \psi_j$, $1 \leq j \leq t$, fixados. Então pelo Lema 0.1.4 (1), $D(X,a)$ divide $p_\alpha(X,a)$, $0 \leq \alpha \leq n$, e portanto divide $M(X,a)$ em $\mathbb{R}[X]$ para todo $a \in B$. Logo, pelo Corolário 1.1.1 (aplicado a (B,M,D)), existem (C_k, D_k, ϕ_k) em $A \times \mathbb{R}[X,Z] \times \mathbb{R}[Z]$, $1 \leq k \leq u$, $u = u_j \geq 1$, tais que

$$(1.1.8) \quad B \text{ é reunião disjunta dos } C_k$$

$$(1.1.9) \quad \phi_k(a) \neq 0 \text{ e } \partial D_k(X,a) = \partial_X D_k \text{ para todo } a \in C_k; \text{ além disso, } \\ \partial M(X,a) \text{ e } \partial D(X,a) \text{ não dependem de } a \in C_k.$$

$$(1.1.10) \quad M(X,a) = \phi_k^{-1}(a) D_k(X,a) D(X,a), \text{ para todo } a \in C_k.$$

Se $k \in \{1, \dots, u\}$ então, por (1.1.10) e (1.1.13), tem-se

$$P(X,Y,a) = \psi^{-1}(a) \phi_k^{-1}(a) D_k(X,a) D(X,a) F(X,Y,a), \text{ para todo } a \in C_k,$$

o que, evidentemente, implica (1.1.34). A condição (1.1.32) segue de (1.1.29), (1.1.11) e (1.1.8). Finalmente, (1.1.33) obtém-se de (1.1.12) e (1.1.9). ■

LEMA 1.1.8 - Sejam P e $F \neq 0$ um par de polinômios em $\mathbb{R}[X,Y,Z]$, com X e Y uma variável. Então, existem (Δ_i, Q_i, R_i) em

$A \times (\mathbb{R}(X, Z)[Y])^2$, $1 \leq i \leq r$, $r \geq 1$, onde $Q_i = G_i H_i^{-1}$, $R_i = \phi_i \psi_i^{-1}$, com $G_i, \phi_i \in \mathbb{R}[X, Y, Z]$, $H_i, \psi_i \in \mathbb{R}[X, Z]$, tais que

(1.1.35) $\mathbb{R}^m$ é reunião disjunta dos Γ_i , $1 \leq i \leq r$.

(1.1.36) $H_i(X, a) \psi_i(X, a) \neq 0$ (portanto, $Q_i(X, Y, a)$ e $R_i(X, Y, a)$ estão bem definidos), $\partial H_i(X, a) = \partial_X H_i$, $\partial \psi_i(X, a) = \partial_X \psi_i$; $\partial G_i(X, Y, a) = \partial_{XY} G_i$, $\partial_Y G_i(X, Y, a) = \partial_Y G_i$, $\partial \phi_i(X, Y, a) = \partial_{XY} \phi_i$ e $\partial_Y \phi_i(X, Y, a) = \partial_Y \phi_i$, para todo $a \in \Delta_i$; além disso, o grau total (e o grau em Y) de $P(X, Y, a)$ e $F(X, Y, a)$ não dependem de $a \in \Gamma_i$, $1 \leq i \leq r$.

(1.1.37) $P(X, Y, a) = F(X, Y, a) Q_i(X, Y, a) - R_i(X, Y, a)$, para todo $a \in \Delta_i$, onde $\partial_Y R_i(X, Y, a) < \partial_Y F(X, Y, a)$, se $R(X, Y, a) \neq 0$ (a menos que $F(X, Y, a) \equiv 0$); além disso, $\partial_Y R_i < \partial_Y F$, se $R_i \neq 0$, $1 \leq i \leq r$.

PROVA - A demonstração é análoga à do Lema 1.1.2. De fato, usando o Lema 1.1.1 (B), podemos achar elementos $(\Gamma_i, \mathbb{P}_i, \mathbb{F}_i)$ em $A \times (\mathbb{R}[X, Y, Z])^2$, $1 \leq i \leq r$, tais que

(1.1.3) $\mathbb{R}^m$ é reunião disjunta dos Γ_i , $1 \leq i \leq r$.

(1.1.4) $P(X, Y, a) = \mathbb{P}_i(X, Y, a)$, $\partial_Y \mathbb{P}_i(X, Y, a) = \partial_Y \mathbb{P}_i$, $\partial \mathbb{P}_i(X, Y, a) = \partial_{XY} \mathbb{P}_i$, $F(X, Y, a) = \mathbb{F}_i(X, Y, a)$, $\partial_Y \mathbb{F}_i(X, Y, a) = \partial_Y \mathbb{F}_i$ e $\partial \mathbb{F}_i(X, Y, a) = \partial_{XY} \mathbb{F}_i$, para todo $a \in \Delta_i$, $1 \leq i \leq r$.

Sejam $\Gamma = \Gamma_i$, $\mathbb{P} = \mathbb{P}_i$ e $\mathbb{F} = \mathbb{F}_i$, $1 \leq i \leq r$, fixados. Se $\mathbb{P}(X,Y,a) \equiv 0$ para todo $a \in \Gamma$ ou $\mathbb{F}(X,Y,a) \equiv 0$ para todo $a \in \Gamma$, o resultado é imediato. Suponhamos, então, que $\mathbb{P}(X,Y,a)\mathbb{F}(X,Y,a) \neq 0$ para todo $a \in \Gamma$, o que ocorre por (1.1.4). Logo existe $(n,v) \in \mathbb{N}^2$ tal que $\mathbb{P} = \sum_{\alpha=0}^n p_{\alpha} Y^{\alpha}$ e $\mathbb{F} = \sum_{\alpha=0}^v f_{\alpha} Y^{\alpha}$, onde

$$p_{\alpha}, f_{\alpha} \in \mathbb{R}[X,Z] \text{ e } p_n(X,a)f_v(X,a) \neq 0 \text{ para todo } a \in \Gamma.$$

Se $k = \max\{n-v+1, 0\}$ então, pelo Teorema 0.1.2 (aplicado ao par $\mathbb{P}$ e $\mathbb{F}$), existe polinômios G e ϕ em $\mathbb{R}[X,Z][Y]$ tais que $f_v^k \mathbb{P} = \mathbb{F}G + \phi$, onde $\partial_Y \phi < \partial_Y \mathbb{F}$, se $\phi \neq 0$. Sejam $Q = Gf_v^{-k}$ e $R = -\phi f_v^{-k}$. Então, para todo $a \in \Gamma$ tem-se

$$\begin{aligned} P(X,Y,a) &= \mathbb{P}(X,Y,a) = \mathbb{F}(X,Y,a)Q(X,Y,a) - R(X,Y,a) = \\ &= F(X,Y,a)Q(X,Y,a) - R(X,Y,a), \end{aligned}$$

sendo $\partial_Y R(X,Y,a) < v = \partial_Y F(X,Y,a)$, se $R(X,Y,a) \neq 0$. Notemos que $\partial_Y R = \partial_Y \phi < \partial_Y \mathbb{F} \leq \partial_Y F$ e se $n < v$ então $Q \equiv 0$; se $n \geq v$ então $\partial_Y G = n-v$ e o coeficiente dominante de Q (considerado como um elemento de $\mathbb{R}[X,Z][Y]$) é $p_n f_v^{-1}$; como $p_n(X,a)f_v(X,a) \neq 0$ para todo $a \in \Gamma$, tem-se $\partial_Y G(X,Y,a) = \partial_Y Q(X,Y,a) = n-v$ para todo $a \in \Gamma$. Se $\partial Q(X,Y,a)$ ou $\partial R(X,Y,a)$ ou $\partial_Y R(X,Y,a)$ ou $\partial p_n(X,a)$ ou $\partial f_v(X,a)$ não for constante em Γ então, usando o Lema 1.1.1 (A ou B), podemos subdividir este conjunto em um número finito de elementos de A satisfazendo (1.1.4) ou (1.1.2). Os novos conjuntos estão satisfarão (1.1.36). ■

A partir do Lema 1.1.8 é imediato o

COROLÁRIO 1.1.3 - Além das hipóteses do lema, seja Γ em A tal que $F(X,Y,a) \neq 0$ e $F(X,Y,a)$ divide $P(X,Y,a)$ em $\mathbb{R}(X)[Y]$ para todo $a \in \Gamma$. Então, existem (Γ_i, G_i, H_i) em $A \times \mathbb{R}[X,Y,Z] \times \mathbb{R}[X,Z]$, $1 \leq i \leq s$, $s \geq 1$, tais que

$$(1.1.38) \quad \Gamma \text{ é reunião disjunta dos } \Gamma_i, \quad 1 \leq i \leq s.$$

$$(1.1.39) \quad H_i(X,a) \neq 0, \quad \partial_{G_i}(X,Y,a) = \partial_{XY} G_i, \quad \partial_Y G_i(X,Y,a) = \partial_Y G_i$$

e $\partial_{H_i}(X,a) = \partial_X H_i$ para todo $a \in \Gamma_i$; além disso, o grau total (e o grau em Y) de $P(X,Y,a)$ e $F(X,Y,a)$ não dependem de $a \in \Gamma_i$, $1 \leq i \leq s$.

$$(1.1.40) \quad P(X,Y,a) = H_i^{-1}(X,a) G_i(X,Y,a) F(X,Y,a), \text{ para todo } a \in \Gamma_i,$$

$$1 \leq i \leq s.$$

PROVA - Análoga à do Corolário 1.1.1. ■

LEMA 1.1.9 - Seja (Δ, P, D) em $A \times (\mathbb{R}[X,Y,Z])^2$, com X e Y uma variável, tal que $D(X,Y,a) \neq 0$, $D(X,Y,a)$ divide $P(X,Y,a)$ em $\mathbb{R}[X,Y]$ e $P(X,Y,a)$ é primitivo em $\mathbb{R}[X][Y]$ para todo $a \in \Gamma$. Então, existem $(\Delta_i, F_i, \lambda_i)$ em $A \times \mathbb{R}[X,Y,Z] \times \mathbb{R}(Z)$, $1 \leq i \leq r$, $r \geq 1$, onde $\lambda_i = \phi_i \psi_i^{-1}$ com $\phi_i, \psi_i \in \mathbb{R}[Z]$, tais que

$$(1.1.41) \quad \Delta \text{ é reunião disjunta dos } \Delta_i, \quad 1 \leq i \leq r.$$

(1.1.42) $\phi_i(a)\psi_i(a) \neq 0$, $\partial F_i(X,Y,a) = \partial_{xy} F_i$, $\partial_y F_i(X,Y,a) = \partial_y F_i$ e $F_i(X,Y,a)$ é primitivo em $\mathbb{R}[X][Y]$ para todo $a \in \Delta_i$; além disso, o grau total (e o grau em Y) de $P(X,Y,a)$ e $D(X,Y,a)$ não dependem de $a \in \Delta_i$, $1 \leq i \leq r$.

(1.1.43) $P(X,Y,a) = \lambda_i(a)D(X,Y,a)F_i(X,Y,a)$, para todo $a \in \Delta_i$, $1 \leq i \leq r$.

PROVA - Pelo Corolário 1.1.3 (aplicado a (Δ, P, D)), existem (Γ_i, G_i, H_i) em $A \times \mathbb{R}[X, Y, Z] \times \mathbb{R}[X, Z]$, $1 \leq i \leq s$, $s \geq 1$, satisfazendo (1.1.39) e

(1.1.38) Δ é reunião disjunta dos Γ_i

(1.1.40) $P(X,Y,a) = H_i^{-1}(X,a)G_i(X,Y,a)D(X,Y,a)$, para todo $a \in \Gamma_i$.

Sejam $\Gamma = \Gamma_i$, $G = G_i$ e $H = H_i$, $1 \leq i \leq r$, fixados. Então, como $D(X,Y,a)$ divide $P(X,Y,a)$ em $\mathbb{R}[X,Y]$, por (1.1.40) segue que $H(X,a)$ divide $G(X,Y,a)$ em $\mathbb{R}[X,Y]$ para todo $a \in \Gamma$ e como, por (1.1.39), $H(X,a) \neq 0$ para todo $a \in \Gamma$, pelo Lema 1.1.7 (aplicado a (Γ, G, H)) existem $(A_j, F_j, \phi_j, \psi_j)$ em $A \times \mathbb{R}[X, Y, Z] \times \mathbb{R}[X, Z] \times \mathbb{R}[Z]$, $1 \leq j \leq t$, $t = t_i \geq 1$, tais que

(1.1.32) Γ é reunião disjunta dos A_j .

(1.1.33) $\psi_j(a) \neq 0$, $\partial \phi_j(X,a) = \partial_x \phi_j$, $\partial F_j(X,Y,a) = \partial_{xy} F_j$, $\partial_y F_j(X,Y,a) = \partial_y F_j$ e $F_j(X,Y,a)$ é primitivo em $\mathbb{R}[X][Y]$ para todo $a \in A_j$.

$$(1.1.34) \quad G(X,Y,a) = \psi_j^{-1}(a)\phi_j(X,a)H(X,a)F_j(X,Y,a), \text{ para todo } a \in A_j.$$

Sejam $A = A_j$, $F = F_j$, $\phi = \phi_j$ e $\psi = \psi_j$, $1 \leq j \leq t$, fixados. Então, por (1.1.33), existe $n = n_j \in \mathbb{N}$ tal que $\phi = \sum_{k=0}^n \alpha_k X^k$, onde $\alpha_k \in \mathbb{R}[Z]$ e $\alpha_n(a) \neq 0$ para todo $a \in A$. Por outro lado, para cada $a \in A$ fixo, de (1.1.34) e (1.1.40) (pois $H(X,a) \neq 0$), segue que

$$(1.1.44) \quad P(X,Y,a) = \psi^{-1}(a)\phi(X,a)D(X,Y,a)F(X,Y,a),$$

e pelo Lema 0.1.1, existem $d_a(X) \in \mathbb{R}[X]^*$ e $D_a(X,Y)$ primitivo em $\mathbb{R}[X][Y]$ tais que $D(X,Y,a) = d_a(X)D_a(X,Y)$; logo, por (1.1.44), tem-se

$$P(X,Y,a) = \psi^{-1}(a)d_a(X)\phi(X,a)D_a(X,Y)F(X,Y,a).$$

Mas, por (1.1.33) e pelo Lema 0.1.2, $D_a(X,Y)F(X,Y,a)$ é primitivo em $\mathbb{R}[X][Y]$ e sendo $P(X,Y,a)$ primitivo, pelo Corolário 0.1.1, exista $u_a \in \mathbb{R}^*$ tal que

$$[\phi(X,a)\alpha_n^{-1}(a)]d_a(X) = u_a\psi(a)\alpha_n^{-1}(a); \text{ logo, } \partial[\phi(X,a)\alpha_n^{-1}(a)] = 0$$

e como $\phi(X,a)\alpha_n^{-1}(a)$ é um polinômio unitário obtém-se $\phi(X,a) = \alpha_n(a)$. Levando isto a (1.1.44) resulta

$$P(X,Y,a) = \alpha_n(a)\psi^{-1}(a)D(X,Y,a)F(X,Y,a), \quad a \in A,$$

o que prova (1.1.43), se escolhermos $\lambda = \alpha_n\psi^{-1}$, $\lambda = \lambda_{ij}$. A condição (1.1.41) segue de (1.1.32) e (1.1.38). Finalmente, (1.1.33) prova a primeira parte de (1.1.42) (notemos que

$\alpha_n(a) \neq 0$ para todo $a \in A$) e a última parte segue de (1.1.39). ■

LEMA 1.1.10 - Sejam P e $F \neq 0$ um par de polinômios em $\mathbb{R}[X, Y, Z]$, com X e Y uma variável. Então, existem (A_i, D_i) em $A \times \mathbb{R}[X, Y, Z]$, $1 \leq i \leq r$, $r \geq 1$, tais que

(1.1.45) $\mathbb{R}^m$ é reunião disjunta dos A_i , $1 \leq i \leq r$.

(1.1.46) $\partial_{D_i}(X, Y, a) = \partial_{xy} D_i$ e $\partial_Y D_i(X, Y, a) = \partial_Y D_i$ para todo $a \in A_i$;
além disso o grau total (e o grau em Y) de $P(X, Y, a)$ e $F(X, Y, a)$ não dependem de $a \in A_i$, $1 \leq i \leq r$.

(1.1.47) $D_i(X, Y, a)$ é um mdc de $P(X, Y, a)$ e $F(X, Y, a)$ em $\mathbb{R}(X)[Y]$
para todo $a \in A_i$, $1 \leq i \leq r$.

PROVA - Segue por um processo completamente análogo ao que foi feito na prova do Lema 1.1.14 e o seu Corolário 1.1.2, neste caso usando o Lema 1.1.8. ■

LEMA 1.1.11 - Sejam P e $F \neq 0$ um par de polinômios em $\mathbb{R}[X, Y, Z]$, com X e Y uma variável. Então, existem (Γ_i, M_i) em $A \times \mathbb{R}[X, Y, Z]$, $1 \leq i \leq r$, $r \geq 1$, tais que

(1.1.48) $\mathbb{R}^m$ é reunião disjunta dos Γ_i , $1 \leq i \leq r$

(1.1.49) $\partial_{M_i}(X, Y, a) = \partial_{xy} M_i$ e $\partial_Y M_i(X, Y, a) = \partial_Y M_i$ para todo $a \in \Gamma_i$;
além disso, o grau total (e o grau em Y) de $P(X, Y, a)$ e $F(X, Y, a)$ não dependem de $a \in \Gamma_i$, $1 \leq i \leq r$.

(1.1.50) $M_i(X,Y,a)$ é um mdc de $P(X,Y,a)$ e $F(X,Y,a)$ em $\mathbb{R}[X,Y]$

para todo $a \in \Gamma_i$, $1 \leq i \leq r$.

PROVA - Com as notações do Lema 1.1.10, sejam $A = A_i$ e $D = D_i$, $1 \leq i \leq r$, fixados. Se $D(X,Y,a) \equiv 0$ para todo $a \in A$, o resultado é imediato. Suponhamos, então, que $D(X,Y,a) \not\equiv 0$ para todo $a \in A$, o que ocorre por (1.1.46). Consideremos D como um elemento de $\mathbb{R}[X,Z][Y]$. Então, usando o Lema 1.1.6, podemos achar (B_j, d_j) em $A \times \mathbb{R}[X,Z]$, $1 \leq j \leq s$, $s = s_i \geq 1$, tais que

(1.1.51) A é reunião disjunta dos B_j

(1.1.52) $\partial_{d_j}(X,a) = \partial_X d_j$ para todo $a \in B_j$

(1.1.53) $d_j(X,a)$ é um mdc em $\mathbb{R}[X]$ dos coeficientes de $D(X,Y,a)$

(considerado como um elemento de $\mathbb{R}[X][Y]$) para todo $a \in B_j$.

Sejam $B = B_j$ e $d = d_j$, $1 \leq j \leq s$, fixados. Como $D(X,Y,a) \not\equiv 0$, é claro que, $d(X,a) \not\equiv 0$ para todo $a \in B$, devido a (1.1.52). Logo, por (1.1.53) e pelo Lema 1.1.3 (aplicado a (B,D,d)), existem (C_k, D_k^*, α_k) em $A \times \mathbb{R}[X,Y,Z] \times \mathbb{R}[Z]$, $1 \leq k \leq t$, $t = t_j \geq 1$, tais que

(1.1.54) B é reunião disjunta dos C_k

(1.1.55) $\alpha_k(a) \neq 0$, $\partial_{D_k^*}(X,Y,a) = \partial_{XY} D_k^*$, $\partial_Y D_k^*(X,Y,a) = \partial_Y D_k^*$ e $D_k^*(X,Y,a)$ é primitivo em $\mathbb{R}[X][Y]$ para todo $a \in C_k$.

$$(1.1.56) \quad D(X,Y,a) = \alpha_k^{-1}(a) d(X,a) D_k^*(X,Y,a), \text{ para todo } a \in C_k$$

Sejam $C = C_k$, $D^* = D_k^*$ e $\alpha = \alpha_k$, $1 \leq k \leq t$, fixados. Então, por um raciocínio análogo ao que foi feito acima (neste caso com os polinômios P e F por separado) podemos achar elementos $(E_\ell, P_\ell^*, p_\ell, \beta_\ell)$ e $(E_\ell, F_\ell^*, f_\ell, \gamma_\ell)$ em $A \times \mathbb{R}[X,Y,Z] \times \mathbb{R}[X,Z] \times \mathbb{R}[Z]$, $1 \leq \ell \leq u$, $u = u_k \geq 1$, tais que

$$(1.1.57) \quad C \text{ é reunião disjunta dos } E_\ell$$

$$(1.1.58) \quad \beta_\ell(a) \gamma_\ell(a) \neq 0, \quad \partial p_\ell(X,a) = \partial_X p_\ell, \quad \partial f_\ell(X,a) = \partial_X f_\ell \text{ e } P_\ell^*(X,Y,a) \text{ e } F_\ell^*(X,Y,a) \text{ são primitivos em } \mathbb{R}[X][Y] \text{ para todo } a \in E_\ell.$$

$$(1.1.59) \quad P(X,Y,a) = \beta_\ell^{-1}(a) p_\ell(X,a) P_\ell^*(X,Y,a) \text{ e } F(X,Y,a) = \gamma_\ell^{-1}(a) f_\ell(X,a) F_\ell^*(X,Y,a). \text{ para todo } a \in E_\ell.$$

Sejam $E = E_\ell$, $P^* = P_\ell^*$, $F^* = F_\ell^*$, $p = p_\ell$, $f = f_\ell$, $\beta = \beta_\ell$ e $\gamma = \gamma_\ell$, $1 \leq \ell \leq u$, fixados. Se $p(X,a) \equiv 0$ para todo $a \in E$ ou $f(X,a) \equiv 0$ para todo $a \in E$, o resultado é imediato; pois, neste caso $P(X,Y,a) \equiv 0$, $a \in E$, ou $F(X,Y,a) \equiv 0$, $a \in E$. Suponhamos que $p(X,a) f(X,a) \neq 0$ para todo $a \in E$, o que ocorre por (1.1.58). Então, usando o Lema 1.1.6 (aplicado ao par (p,f)), podemos achar (Γ_v, m_v) em $A \times \mathbb{R}[X,Z]$, $1 \leq v \leq v$, $v = v_\ell \geq 1$, tais que

$$(1.1.60) \quad E \text{ é reunião disjunta dos } \Gamma_v$$

$$(1.1.61) \quad \partial m_v(X,a) = \partial_X m_v \text{ para todo } a \in \Gamma_v$$

(1.1.62) $m_v(X,a)$ é um mdc em $\mathbb{R}[X]$ de $p(X,a)$ e $f(X,a)$ (e portanto de $\beta^{-1}(a)p(X,a)$ e $\gamma^{-1}(a)f(X,a)$) para todo $a \in \Gamma_v$.

Seja M_v , $1 \leq v \leq v$, o polinômio em $\mathbb{R}[X,Y,Z]$ dado por $M_v = m_v D^*$. Então, por (1.1.55), (1.1.56), (1.1.58), (1.1.59), (1.1.62) e pelo Lema 0.1.11, $M_v(X,Y,a)$ é um mdc de $P(X,Y,a)$ e $F(X,Y,a)$ em $\mathbb{R}[X][Y] = \mathbb{R}[X,Y]$ para todo $a \in \Gamma_v$, o que prova (1.1.50). A condição (1.1.48) segue de (1.1.45), (1.1.51), (1.1.54), (1.1.57) e (1.1.60). Finalmente, (1.1.49) obtém-se de (1.1.46), (1.1.55) e (1.1.61). ■

LEMA 1.1.12 - Seja (Γ, P) em $A \times \mathbb{R}[X,Y,Z]$, com X e Y uma variável, tal que $P(X,Y,a)$ é primitivo em $\mathbb{R}[X][Y]$ para todo $a \in \Gamma$. Então, existem (Γ_i, F_i) em $A \times \mathbb{R}[X,Y,Z]$, $1 \leq i \leq s$, $s \geq 1$, tais que

(1.1.63) Γ é reunião disjunta dos Γ_i , $1 \leq i \leq s$

(1.1.64) $\partial F_i(X,Y,a) = \partial_{xy} F_i$, $\partial_Y F_i(X,Y,a) = \partial_Y F_i$, $\partial_X F_i(X,Y,a) = \text{cte}$ e $F_i(X,Y,a)$ é primitivo em $\mathbb{R}[X][Y]$ para todo $a \in \Gamma_i$, $1 \leq i \leq s$.

(1.1.65) $F_i(X,Y,a)$ possui os mesmos fatores irredutíveis em $\mathbb{R}[X,Y]$, de grau maior que zero em Y , que $P(X,Y,a)$, mas com fatores não repetidos, para todo $a \in \Gamma_i$ ($1 \leq i \leq s$).

PROVA - Pelo Lema 1.1.11, aplicado aos polinômios P e P_Y , existem (Δ_i, M_i) em $A \times \mathbb{R}[X,Y,Z]$, $1 \leq i \leq r$, $r \geq 1$, tais que

(1.1.66) Γ é reunião disjunta dos $A_i = \Gamma \cap \Delta_i$, $1 \leq i \leq r$

(1.1.67) $\partial M_i(X, Y, a) = \partial_{xy} M_i$ e $\partial_y M_i(X, Y, a) = \partial_y M_i$ para todo $a \in A_i$

(1.1.68) $M_i(X, Y, a)$ é um mdc de $P(X, Y, a)$ e $P_y(X, Y, a)$ em $\mathbb{R}[X, Y]$
para todo $a \in A_i$.

Sejam $A = A_i$ e $M = M_i$, $1 \leq i \leq r$, fixados. Então pelo Lema 0.1.16 (5), $A \in A$ e se $M(X, Y, a) \equiv 0$ para todo $a \in A$, o resultado é imediato; pois, neste caso $P(X, Y, a) \equiv 0$ para todo $a \in A$. Suponhamos, então, que $M(X, Y, a) \neq 0$ para todo $a \in A$, o que ocorre por (1.1.67). Como $M(X, Y, a)$ divide $P(X, Y, a)$ em $\mathbb{R}[X, Y]$ e como $P(X, Y, a)$ é primitivo em $\mathbb{R}[X][Y]$ para todo $a \in A$, pelo Lema 1.1.9 (aplicado a (A, P, M)), existem (B_j, F_j, λ_j) em $A \times \mathbb{R}[X, Y, Z] \times \mathbb{R}(Z)$, $1 \leq j \leq s$, $s = s_i \geq 1$, tais que

(1.1.69) A é reunião disjunta dos B_j

(1.1.70) $\lambda_j(a) \neq 0$, $\partial F_j(X, Y, a) = \partial_{xy} F_j$, $\partial_y F_j(X, Y, a) = \partial_y F_j$ e
 $F_j(X, Y, a)$ é primitivo em $\mathbb{R}[X][Y]$ para todo $a \in B_j$.

(1.1.71) $P(X, Y, a) = \lambda_j(a) M(X, Y, a) F_j(X, Y, a)$, para todo $a \in B_j$.

Sejam $j \in \{1, \dots, s\}$ e $a \in B_j$. Então, como $\lambda_j(a) \neq 0$, segue que $\lambda_j(a) M(X, Y, a)$ é um mdc de $P(X, Y, a)$ e $P_y(X, Y, a)$ em $\mathbb{R}[X, Y]$; donde, por (1.1.71) e pelo Lema 0.1.9 (2), segue facilmente que $F_j(X, Y, a)$ e $P(X, Y, a)$ tem os mesmos fatores irredutíveis

em $\mathbb{R}[X,Y]$ que dependem de Y , mas $F_j(X,Y,a)$ não tem tais fatores repetidos. Por outro lado, $F_j(X,Y,a)$ e $P(X,Y,a)$ são ambos primitivos em $\mathbb{R}[X][Y]$, donde não possuem fatores irreduzíveis pertencentes a $\mathbb{R}[X]$. Daí segue (1.1.65). A condição (1.1.63) segue de (1.1.66) e (1.1.69); e (1.1.70) prova uma parte de (1.1.64). Se $\partial_x F_j(X,Y,a)$ não for constante em B_j então, por um processo análogo ao que foi feito na prova do Lema 1.1.1, podemos subdividir este conjunto em um número finito de elementos de A de tal modo que os novos conjuntos satisfaçam (1.1.64). ■

1.2 - LEMAS AUXILIARES

Nesta seção provaremos os lemas auxiliares aos quais consideramos cruciais, para a prova do Teorema de Seidenberg - Tarski. Para este fim, quaisquer que sejam os polinômios $P \in \mathbb{R}[X,Z]$ e $F \in \mathbb{R}[X]$, nas variáveis $X = (X_1, \dots, X_n)$ e $Z = (Z_1, \dots, Z_m)$, denotaremos por $N(P,a)$, $a \in \mathbb{R}^m$, e $N(F)$ respectivamente os conjuntos

$$N(P,a) = \{z \in \mathbb{C}^n : P(z,a) = 0\}, \quad N(F) = \{z \in \mathbb{C}^n : F(z) = 0\}.$$

LEMA 1.2.1 - Seja P um polinômio em $\mathbb{R}[X,Y,Z]$, X e Y uma variável. Então, existem (Γ_i, F_i) em $A \times \mathbb{R}[X,Y,Z]$, $1 \leq i \leq r$, $r \geq 1$, tais que

0) $\mathbb{R}^m$ é reunião disjunta dos Γ_i , $1 \leq i \leq r$.

- 1) $F_i(X, Y, a)$ tem os mesmos fatores irredutíveis em $\mathbb{R}[X, Y]$ que $P(X, Y, a)$, mas com fatores não repetidos, para todo $a \in \Gamma_i$, $1 \leq i \leq r$.
- 2) $\partial F_i(X, Y, a) = \partial_{XY} F_i$, $\partial_Y F_i(X, Y, a) = \partial_Y F_i$ e $\partial_X F_i(X, Y, a) = \text{cte}$ para todo $a \in \Gamma_i$, $1 \leq i \leq r$.

Além disso,

$$(1.2.1) \quad a \in \mathbb{R}^m \text{ e } \mathbb{R}^2 \cap N(P, a) \neq \emptyset \iff \exists i \in \{1, \dots, r\} : a \in \Gamma_i \text{ e } \mathbb{R}^2 \cap N(F_i, a) \neq \emptyset.$$

PROVA - Expressando o polinômio P sob a forma

$$P = \sum_{\alpha=0}^n P_{\alpha} Y^{\alpha}, \quad P_{\alpha} \in \mathbb{R}[X, Z], \quad P_n \neq 0, \quad n \in \mathbb{N},$$

consideremos $(\Gamma_i, M_i) \in A \times \mathbb{R}[X, Z]$, $1 \leq i \leq s$, $s \geq 1$, satisfazendo (1.1.29), (1.1.30) e (1.1.31) do Lema 1.1.6, aplicado aos polinômios P_j , $0 \leq j \leq n$. Sejam $\Gamma = \Gamma_i$ e $M = M_i$, $1 \leq i \leq s$, fixados. Se $M(X, a) \equiv 0$ para todo $a \in \Gamma$, o resultado é imediato; pois, neste caso $P(X, Y, a) \equiv 0$ para todo $a \in \Gamma$. Suponhamos, então, que $M(X, a) \not\equiv 0$ para todo $a \in \Gamma$, o que ocorre por (1.1.30). Por (1.1.31) e pelo Lema 1.1.3 (aplicado a (Γ, P, M)), existem $(A_j, F_j, \psi_j) \in A \times \mathbb{R}[X, Y, Z] \times \mathbb{R}[Z]$, $1 \leq j \leq t$, $t = t_i \geq 1$, satisfazendo (1.1.11), (1.1.12) e (1.1.13). Sejam $A = A_j$, $F = F_j$ e $\psi = \psi_j$, $1 \leq j \leq t$, fixados. Então, por (1.1.13), tem-se que

- 3) $F(X, Y, a)$ e $P(X, Y, a)$ possuem os mesmos fatores irredutíveis (de grau maior que zero em Y) em $\mathbb{R}[X, Y]$; além dis

so, $M(X,a)$ e $P(X,Y,a)$ possuem os mesmos fatores irreduzíveis em $\mathbb{R}[X,Y]$ dependendo de X somente, para todo $a \in A$.

Usando os lemas 1.1.5 e 1.1.11, aplicado a (A,M) e (A,F) respectivamente, podemos construir (B_k, g_k) em $A \times \mathbb{R}[X,Z]$ e (B_k, G_k) em $A \times \mathbb{R}[X,Y,Z]$, $1 \leq k \leq u$, $u = u_j \geq 1$, tais que A (e portanto $\mathbb{R}^m$, por (1.1.11) e (1.1.30)) é reunião disjunta dos B_k e

- 4) $\partial g_k(X,a) = \partial_x g_k$ para todo $a \in B_k$
- 5) $g_k(X,a)$ e $M(X,a)$ possuem os mesmos fatores irreduzíveis em $\mathbb{R}[X]$, mas $g_k(X,a)$ não tem tais fatores repetidos, para todo $a \in B_k$
- 6) $\partial G_k(X,Y,a) = \partial_{xy} G_k$, $\partial_y G_k(X,Y,a) = \partial_y G_k$, $\partial_x G_k(X,Y,a) = \text{cte}$ e $G_k(X,Y,a)$ é primitivo em $\mathbb{R}[X][Y]$ para todo $a \in B_k$
- 7) $G_k(X,Y,a)$ e $F(X,Y,a)$ possuem os mesmos fatores irreduzíveis (de grau maior que zero em Y) em $\mathbb{R}[X,Y]$, mas $G_k(X,Y,a)$ não tem tais fatores repetidos, para todo $a \in B_k$

Seja F_k o polinômio em $\mathbb{R}[X,Y,Z]$ dado por $F_k = g_k G_k$, $1 \leq k \leq u$. Então, de 3), 5) e 7) segue imediatamente 1). A condição 2) obtém-se facilmente de 4) e 6). Finalmente, como $\mathbb{R}^m$ é reunião dos B_k , $1 \leq k \leq u$, (1.2.1) é consequência de 1) e 2). ■

LEMA 1.2.2 - Seja (Γ, R) em $A \times \mathbb{R}[X,Z]$, X uma variável, tal que

$R(X,a) \neq 0$ para todo $a \in \Gamma$. Então, existem $(\Gamma_i, R_i, \lambda_i)$ em $A \times \mathbb{R}[X,Z] \times \mathbb{R}(Z)$, $1 \leq i \leq s$, $s \geq 1$, onde $\lambda_i = \phi_i \psi_i^{-1}$ com ϕ_i e ψ_i em $\mathbb{R}[Z]$, tais que $R(X,a) = R_i(X,a)$, $a \in \Gamma_i$, e

- 1) Γ é reunião disjunta dos Γ_i , $1 \leq i \leq s$
- 2) $\phi_i(a)\psi_i(a) \neq 0$, para todo $a \in \Gamma_i$, $1 \leq i \leq s$
- 3) $R(\lambda_i(a), a) \neq 0$, para todo $a \in \Gamma_i$, $1 \leq i \leq s$.

PROVA - Expressando o polinômio R sob a forma

$$R = \sum_{\alpha=0}^r \rho_{\alpha} X^{\alpha}, \quad \rho_{\alpha} \in \mathbb{R}[Z], \quad \rho_r \neq 0, \quad r \in \mathbb{N},$$

consideremos os seguintes conjuntos

$$\Gamma_i = \Gamma \cap \{a \in \mathbb{R}^m : \rho_i(a) \neq 0 \text{ e } \sum_{\alpha=i+1}^r \rho_{\alpha}^2(a) = 0\}, \quad 0 \leq i \leq r.$$

Então, pela Definição 0.1.10 (2) e pelo Lema 0.1.16 (5), $\Gamma_i \in A$ e Γ é reunião disjunta dos Γ_i ; pois, por hipótese

$$\left\{ a \in \mathbb{R}^m : \sum_{\alpha=0}^r \rho_{\alpha}^2(a) = 0 \right\} = \emptyset$$

Além disso, $R(X,a) = R_i(X,a)$ para todo $a \in \Gamma_i$, onde

$$R_i = \sum_{\alpha=0}^i \rho_{\alpha} X^{\alpha}, \text{ sendo } \partial R_i(X,a) = i = \partial_X R_i, \text{ para todo } a \in \Gamma_i, \quad 0 \leq i \leq r.$$

Seja λ_i a função em $\mathbb{R}(Z)$ dado por

$$\lambda_i = (1 + \rho_i^{-2}) \left(i + \sum_{j=0}^{i-1} \rho_j^2 \right) \text{ se } 1 \leq i \leq r, \text{ e } \lambda_i(Z) \equiv 1 \text{ se } i = 0.$$

Então, como $\rho_i(a) \neq 0$ para todo $a \in \Gamma_i$, pelo Lema 0.2.1 (aplicado ao polinômio $R_i(X,a)$ $a \in \Gamma_i$) tem-se

$$R(\lambda_i(a), a) = R_i(\lambda_i(a), a) \neq 0 \text{ para todo } a \in \Gamma_i, \quad 0 \leq i \leq r. \quad \blacksquare$$

LEMA 1.2.3 - Seja (Γ, F) em $A \times \mathbb{R}[X, Y, Z]$, X e Y uma variável tal que $\partial F(X, Y, a) = n$ para todo $a \in \Gamma$. Então, existem (Γ_i, F_i, μ_i) em $A \times \mathbb{R}[X, Y, Z] \times \mathbb{R}$, $0 \leq i \leq n$, tais que

- 1) Γ é reunião dos Γ_i , $1 \leq i \leq n$.
- 2) $F_i(X, Y, a) = F(X + \mu_i Y, Y, a)$ e $\partial_Y F_i(X, Y, a) = \partial F_i(X, Y, a)$ para todo $a \in \Gamma_i$, $1 \leq i \leq n$.

PROVA - Consideremos o polinômio F sob a forma

$$F(X, Y, a) = \sum_{\alpha + \beta \leq n} f_{\alpha\beta}(a) X^\alpha Y^\beta, \quad f_{\alpha\beta} \in \mathbb{R}[Z], \quad \forall a \in \Gamma,$$

e seja f o polinômio em $\mathbb{R}[V, Z]$, V uma variável, dado por $f(V, Z) = \sum_{\alpha + \beta = n} f_{\alpha\beta}(Z) V^\alpha$. Então, por hipótese, para cada $a \in \Gamma$, existe $(\alpha, \beta) \in \mathbb{N}^2$ com $\alpha + \beta = n$, tal que $f_{\alpha\beta}(a) \neq 0$; logo, o polinômio $f(V, a)$ é não nulo para todo $a \in \Gamma$. Donde, por uma propriedade conhecida

$$(1.2.2) \quad \forall a \in \Gamma, \exists \mu_a \in \{0, \dots, n\}: f(\mu_a, a) \neq 0.$$

Seja Γ_μ o elemento de A dado por $\Gamma_\mu = \{a \in \Gamma: f(\mu, a) \neq 0\}$, $0 \leq \mu \leq n$. Então, por (1.2.2), Γ é reunião dos Γ_μ . Por outro lado, se $F_\mu(X, Y, a) = F(X + \mu Y, Y, a)$ então para todo $a \in \Gamma$ tem-se

$$F_\mu(X, Y, a) = \sum_{\alpha + \beta \leq n} f_{\alpha\beta}(a) (X + \mu Y)^{\alpha} Y^{\beta} = \sum_{\alpha + \beta \leq n, \gamma \leq \alpha} f_{\alpha\beta}(a) \mu^{\alpha - \gamma} \binom{\alpha}{\gamma} X^{\gamma} Y^{\alpha + \beta - \gamma},$$

e portanto, é claro que, o termo dominante de $F_\mu(X,Y,a)$, considerado como um elemento de $\mathbb{R}[X][Y]$ é

$$\left(\sum_{\alpha+\beta=n} f_{\alpha\beta}(a) \mu^\alpha \right) Y^n = f(\mu,a) Y^n,$$

onde, por construção de Γ_μ , $f(\mu,a) \neq 0$. Assim, $\partial_Y F_\mu(X,Y,a) = n = \partial F_\mu(X,Y,a)$ para todo $a \in \Gamma_\mu$, $0 \leq \mu \leq n$, o que prova 2). $\square$

DEFINIÇÃO 1.2.1 - Dado um polinômio F em $\mathbb{R}[X,Y]$, X e Y de uma variável, indicaremos por G_μ , $\mu \in \mathbb{R}$, o polinômio em $\mathbb{R}[X,Y]$ dado por

$$(1.2.4) \quad G_\mu = (X-\mu)F_Y - YF_X;$$

além disso, denotaremos por $N(F,G_\mu)$ o conjunto

$$N(F,G_\mu) = \{z \in \mathbb{C}^2 : F(z) = 0 \text{ e } G_\mu(z) = 0\}.$$

LEMA 1.2.4 - Seja F um polinômio em $\mathbb{R}[X,Y]$, com X e Y uma variável, tal que F não possui fatores múltiplos em $\mathbb{R}[X,Y]$.

Então,

- 1) todo fator comum não trivial em $\mathbb{R}[X,Y]$ de F e G_μ , $\mu \in \mathbb{R}$, tem grau maior que zero em Y .
- 2) se $H \in \mathbb{R}[X,Y]$, com $\partial_Y H > 0$, é irreduzível em $\mathbb{R}[X,Y]$ e é divisor de F em $\mathbb{R}[X,Y]$ então existe no máximo um valor real de μ para o qual H divide G_μ em $\mathbb{R}[X,Y]$.
- 3) se $\partial_Y F = n$ então existe $\mu \in \{0, \dots, n\}$ tal que F e G_μ não possuem fator comum não trivial em $\mathbb{R}[X,Y]$ ou $\mathbb{R}(X)[Y]$.

Além disso, vale ainda

$$(1.2.5) \quad \mathbb{R}^2 nN(F) \neq \emptyset \iff \mathbb{R}^2 nN(F, G_\mu) \neq \emptyset, \mu \in \mathbb{R}.$$

PROVA - 1) Provaremos que F e G_μ não possuem fator comum não trivial em $\mathbb{R}[X]$. De fato, suponhamos que existe $d \in \mathbb{R}[X] \setminus \mathbb{R}$ tal que d divide F e G_μ em $\mathbb{R}[X, Y]$. Como d divide F e d não depende de Y , pelo Lema 0.1.4 (2), segue que d divide F_y em $\mathbb{R}[X, Y]$ e portanto divide $(X-\mu)F_y$ em $\mathbb{R}[X, Y]$. Mas, sendo d divisor de G_μ e de $(X-\mu)F_y$ em $\mathbb{R}[X, Y]$, segue de (1.2.4) que d é divisor de YF_x e portanto de F_x em $\mathbb{R}[X, Y]$. Assim, d divide F e F_x em $\mathbb{R}[X, Y]$; logo, pelo Lema 0.1.9 (1), F possui fatores múltiplos em $\mathbb{R}[X, Y]$, contra a hipótese.

2) Suponhamos que houvessem $\mu_1 \neq \mu_2$ reais tais que H divide F , G_{μ_1} e G_{μ_2} em $\mathbb{R}[X, Y]$. Como H divide G_{μ_1} e G_{μ_2} , H divide $G_{\mu_1} - G_{\mu_2} = (\mu_1 - \mu_2)F_y$; logo H divide F_y em $\mathbb{R}[X, Y]$. Mas, se H divide F e F_y em $\mathbb{R}[X, Y]$ então, pelo Lema 0.1.9 (1), F teria um fator múltiplo em $\mathbb{R}[X, Y]$ de grau maior que zero em Y , contra a hipótese.

3) Como, pelo Teorema 0.1.1 (onde $\mathbb{K} = \mathbb{R}$), $\mathbb{R}[X, Y]$ é um anel fatorial e como F não possui fatores múltiplos em $\mathbb{R}[X, Y]$, pela Observação 0.1.1, existem exatamente $v, v \leq n$, polinômios $F_i, 1 \leq i \leq v$, em $\mathbb{R}[X, Y]$ irredutíveis em $\mathbb{R}[X, Y]$, com $\partial_y F_i > 0$, e F_i não é associado a F_j em $\mathbb{R}[X, Y]$ para $i \neq j$ ($1 \leq i, j \leq v$) tais que $F = DF_1 \dots F_v$, onde D é um produto de fatores irredutíveis, de F , em $\mathbb{R}[X, Y]$ que dependem só de X . Su

ponhamos que para cada $\mu \in \{0, \dots, n\}$ os polinômios F e G_μ possuem um fator comum não trivial em $\mathbb{R}[X, Y]$, digamos $H_\mu \in \mathbb{R}[X, Y]$; logo, para cada $\mu \in \{0, \dots, n\}$ existe um subconjunto $\{i_1, \dots, i_\mu\}$ de $\{1, \dots, v\}$ tal que $H_\mu = c_\mu F_{i_1} \dots F_{i_\mu}$, $c_\mu \neq 0$; pois, por 1), H_μ não pode conter D (nem fatores de D) como fator. Então, como o cardinal de $\{0, \dots, n\}$ é maior que o cardinal de $\{1, \dots, v\}$, é claro que, existem $\mu_1, \mu_2 \in \{0, \dots, v\}$, $\mu_1 \neq \mu_2$, tais que os polinômios F , G_{μ_1} e G_{μ_2} possuem como fator comum, um fator polinômio F_i , $i \leq i \leq v$; mas, este fato contradiz 2). Portanto, existe $\mu \in \{0, \dots, n\}$ verificando 3).

Agora provaremos (1.2.5). A condição suficiente é evidente. Demonstraremos a condição necessária. Por hipótese o conjunto $\mathbb{R}^2 \cap N(F)$ é não vazio e, é claro que, é fechado. Portanto, existe $(a, b) \in \mathbb{R}^2 \cap N(F)$ tal que $d((\mu, 0), (a, b)) = d((\mu, 0), \mathbb{R}^2 \cap N(F))$. Se $(\mu, 0) = (a, b)$ ou $(F_x(a, b), F_y(a, b)) = (0, 0)$, o resultado é imediato. Suponhamos, então, que $(\mu, 0) \neq (a, b)$ e que $(F_x(a, b), F_y(a, b)) \neq (0, 0)$. No caso em que $F_y(a, b) \neq 0$, pelo Teorema da função implícita, existem vizinhanças U e B de (a, b) e a , respectivamente, e existe uma função $y: B \rightarrow \mathbb{R}$ de classe C^∞ tais que $G_r(y) = U \cap N(F)$ (onde $G_r(y)$ denota o gráfico da função y), $F(x, y(x)) = 0$ para todo $x \in B$ e $y(a) = b$. Seja S a circunferência de centro $(\mu, 0)$ e raio $\delta = d((\mu, 0), (a, b)) > 0$. Pelo modo como (a, b) foi escolhido, é claro que, $N(F)$ não possui pontos dentro do disco a-

berto, de centro $(\mu, 0)$ e raio δ ; mas $(a, b) \in N(F) \cap S$. Noutros termos se $g: B \rightarrow \mathbb{R}$ é dado por $g(x) = (x-\mu)^2 + y^2(x)$, $x \in B$, então $g(x) \geq \delta^2$ para todo $x \in B$ e $g(a) = \delta^2$; donde, a é ponto de mínimo de g ; logo, $g'(a) = 0$. Como $g'(x) = 2(x-\mu) + 2y(x)y'(x)$, $x \in B$, daí segue que

$$(1.2.6) \quad (a-\mu) + by'(a) = 0$$

Mas, $F(x, y(x)) = 0$ para todo $x \in B$; logo, $F_x(x, y(x)) + F_y(x, y(x))y'(x) = 0$ para todo $x \in B$ e portanto $F_x(a, b) + F_y(a, b)y'(a) = 0$. Multiplicando esta igualdade por b e levando (1.2.6) em conta obtém-se $(a-\mu)F_y(a, b) - bF_x(a, b) = 0$; isto é, por (1.2.4), $\mathbb{R}^2 \cap N(F, G_\mu) \neq \emptyset$. No caso em que $(\mu, 0) \neq (a, b)$ e $F_x(a, b) \neq 0$, usando o Teorema da função implícita, obtém-se $x = x(y)$ e segue o resultado por um raciocínio análogo ao que foi feito acima. ■

LEMA 1.2.5 - Seja F um polinômio em $\mathbb{R}[X, Y]$, X e Y uma variável, tal que $\partial_x F > 0$, $n = \partial_y F > 0$ e F não possui fatores múltiplos em $\mathbb{R}[X, Y]$. Sejam $G_\mu, \mu \in \mathbb{R}$, os polinômios dados por (1.2.4). Então, existe $\mu \in \{0, \dots, n\}$ tal que

- 1) Se $R_\mu \in \mathbb{R}[X]$ é a resultante de F e G_μ , considerados como elementos de $\mathbb{R}(X)[Y]$, então $R_\mu \neq 0$.
- 2) Se $Q_\mu \in \mathbb{R}[Y]$ é a resultante de F e G_μ , considerados como elementos de $\mathbb{R}(Y)[X]$, então $Q_\mu \neq 0$.

PROVA - 1) Como F não possui fatores múltiplos em $\mathbb{R}[X, Y]$, pe

lo Lema 1.2.4 (3), existe $\mu \in \{0, \dots, n\}$ tal que F e G_μ não possuem fator comum não trivial em $\mathbb{R}(X)[Y]$ e como $\partial_Y F > 0$, pelo Teorema 0.1.3, segue que $R_\mu \neq 0$.

2) Com o $\mu \in \{0, \dots, n\}$ considerado em 1). Se $Q_\mu = 0$ então, como $\partial_X F > 0$, pelo Teorema 0.1.3 os polinômios F e G_μ possuem um fator comum não trivial em $\mathbb{R}(Y)[X]$; logo, pelo Lema 0.1.8 (3), F e G_μ possuem um fator comum não trivial em $\mathbb{R}[Y][X]$, o que contradiz o Lema 1.2.4 (3). Logo $Q_\mu \neq 0$. ■

COROLÁRIO 1.2.1 - Nas hipóteses do lema, com o $\mu \in \{0, \dots, n\}$ construído. Se para cada $\lambda \in \mathbb{R}$, $\lambda \neq 0$, fixo, consideramos os polinômios $\tilde{F}$ e $\tilde{G}_\mu$ em $\mathbb{R}[X', Y']$ dados por $\tilde{F}(X', Y') = F(X' + Y', \lambda Y')$ e $\tilde{G}_\mu(X', Y') = G_\mu(X' + Y', \lambda Y')$, respectivamente, então $\tilde{F}$ e $\tilde{G}_\mu$ não possuem fator comum de grau maior que zero em $\mathbb{R}(X')[Y']$.

PROVA - Suponhamos que $\tilde{F}$ e $\tilde{G}_\mu$ possuem um fator comum de grau maior que zero em $\mathbb{R}(X')[Y']$. Então, pelo Lema 0.1.8 (3), existe $\tilde{D} \in \mathbb{R}[X', Y']$, com $\partial_{Y'} \tilde{D} > 0$, tal que $\tilde{D}$ divide $\tilde{F}$ e $\tilde{G}_\mu$ em $\mathbb{R}[X', Y']$. Se $D(X, Y) = \tilde{D}(X - \lambda^{-1}Y, \lambda^{-1}Y)$ então $D \in \mathbb{R}[X, Y]$ e D divide F e G_μ em $\mathbb{R}[X, Y]$; logo, pelo Lema 1.2.4 (1), D é constante em $\mathbb{R}[X, Y]$ ou $\partial_Y D > 0$. Mas, como $\partial_{Y'} \tilde{D} > 0$, D não é constante e portanto $\partial_Y D > 0$ o que contradiz o Lema 1.2.4 (3). Logo, $\tilde{F}$ e $\tilde{G}_\mu$ não possuem fator comum de grau maior que zero em $\mathbb{R}(X')[Y']$. ■

OBSERVAÇÃO 1.2.1 - Seja (R, Q) em $\mathbb{R}[X, Z] \times \mathbb{R}[Y, Z]$, X e Y de uma variável. Então, $A = \{a \in \mathbb{R}^m : R(X, a)Q(Y, a) \neq 0\}$ é um elemento de

A. De fato, expressando os polinômios R e Q sob a forma

$$R = \sum_{\alpha=0}^r R_{\alpha} X^{\alpha}, Q = \sum_{\beta=0}^s Q_{\beta} Y^{\beta}, R_{\alpha}, Q_{\beta} \in \mathbb{R}[Z], R_r Q_s \neq 0, r, s \in \mathbb{N},$$

é claro que $A = \left\{ a \in \mathbb{R}^m : \left(\sum_{\alpha=0}^r R_{\alpha}^2(a) \right) \left(\sum_{\beta=0}^s Q_{\beta}^2(a) \right) \neq 0 \right\}$; logo, pela Definição 0.1.10 (2), $A \in A$.

LEMA 1.2.6 - Seja (A^*, R^*, Q^*) em $A \times \mathbb{R}[X, Z] \times \mathbb{R}[Y, Z]$, X e Y uma variável, tal que

1*) $R^*(X, a)$ e $Q^*(Y, a)$ tem sô raízes simples, para todo $a \in A^*$

2*) Os polinômios R^* e Q^* tem a forma

$$R^* = \sum_{\alpha=0}^r R_{\alpha} X^{\alpha}, Q^* = \sum_{\beta=0}^s Q_{\beta} Y^{\beta}, (r, s) \in \mathbb{N}^2$$

onde $R_{\alpha}, Q_{\beta} \in \mathbb{R}[Z]$ e $R_r(a)Q_s(a) \neq 0$ para todo $a \in A^*$. Então, valem as seguintes Propriedades:

3*) para cada $a \in A^*$ existem $x_1(a), \dots, x_r(a), y_1(a), \dots, y_s(a)$ em $\mathbb{C}$ tais que $x_i(a) \neq x_j(a)$ se $i \neq j$ ($1 \leq i, j \leq r$), $y_k(a) \neq y_{\ell}(a)$ se $k \neq \ell$ ($1 \leq k, \ell \leq s$), $R^*(x_i(a), a) = 0$ e $Q^*(y_k(a), a) = 0$, $1 \leq i \leq r$, $1 \leq k \leq s$.

4*) existe um polinômio H^* em $\mathbb{R}[W, Z]$, W uma variável, tal que para todo $a \in A^*$ tem-se que $H^*(W, a) \neq 0$ e

$$H^* \left(\frac{y_k(a) - y_{\ell}(a)}{x_i(a) - x_j(a)}, a \right) = 0, (1 \leq i, j \leq r, i \neq j), (1 \leq k, \ell \leq s, k \neq \ell).$$

PROVA - Por 1*), 2*) e por um teorema bem conhecido, para cada $a \in A^*$ existem elementos em $\mathbb{C}$ satisfazendo 3*). Considere-mos o polinômio P em $\mathbb{Z}[W, X_1, \dots, X_r, Y_1, \dots, Y_s]$ dado por

$$P = \prod_{\substack{i \neq j \\ k \neq \ell}} [(X_i - X_j)W - (Y_k - Y_\ell)].$$

Então, pelo Lema 0.1.14, existe $P^* \in \mathbb{Z}[W, \dots, Y_s]$ tal que

$$P(W, X_1, \dots, Y_s) = P^*(W, S_1(X_1, \dots, X_r), \dots, T_s(Y_1, \dots, Y_s)),$$

onde S_i e T_k são os p.s.e. nas indeterminadas X_i e Y_k , respectivamente, $1 \leq i \leq r$, $1 \leq k \leq s$. Logo, para todo $a \in A^*$ tem-se

$$\begin{aligned} P(W, x_1(a), \dots, y_s(a)) &= P^*(W, S_1(x_1(a), \dots, x_r(a)), \dots, T_s(y_1(a), \dots, y_s(a))) \\ &= P^*(W, S^*(a), T^*(a)), \end{aligned}$$

onde $S^*, T^* \in \mathbb{R}[Z]$ são (a menos de sinal) os coeficientes $R_i R_r^{-1}$ e $Q_k Q_s^{-1}$, respectivamente ($0 \leq i \leq r$, $0 \leq k \leq s$). Seja H^* o polinômio em $\mathbb{R}[W, Z]$ dado por

$$H^*(W, Z) = R_r^{r^*}(Z) Q_s^{s^*}(Z) P^*(W, S^*(Z), T^*(Z)),$$

onde $r^*, s^* \in \mathbb{N}$ são suficientemente grandes para que H^* seja polinômio. Então, para todo $a \in A^*$

$$\begin{aligned} H^*(W, a) &= K(a) P(W, x_1(a), \dots, y_s(a)) = \\ &= K(a) \prod_{i \neq j, k \neq \ell} [(x_i(a) - x_j(a))W - (y_k(a) - y_\ell(a))] \neq 0, \end{aligned}$$

e além disso, para $1 \leq i, j \leq r$, $i \neq j$, e $1 \leq k, \ell \leq s$, $k \neq \ell$

$$H^* \left(\frac{y_k(a) - y_\ell(a)}{x_i(a) - x_j(a)}, a \right) = K(a) P \left(\frac{y_k(a) - y_\ell(a)}{x_i(a) - x_j(a)}, x_1(a), \dots, y_s(a) \right) = 0,$$

onde $K = R_r^{r^*} Q_s^{s^*}$ (notemos que, por 2^*), $K(a) \neq 0$, $a \in A^*$). ■

LEMA 1.2.7 - Seja P um polinômio em $\mathbb{R}[X, Y, Z]$, X e Y uma variável. Então, existem (Δ_i, R_i) em $A \times \mathbb{R}[X, Z]$, $1 \leq i \leq v$, $v \geq 1$, tais que para todo $a \in \mathbb{R}^m$ tem-se

$$(1.2.7) \quad \mathbb{R}^2 \cap N(P, a) \neq \emptyset \iff i \in \{1, \dots, v\}: a \in \Delta_i \text{ e } \mathbb{R} \cap N(R_i, a) \neq \emptyset.$$

PROVA - Consideremos os elementos (Γ_i, F_i) em $A \times \mathbb{R}[X, Y, Z]$, $1 \leq i \leq u$, $u \geq 1$, satisfazendo as condições do Lema 1.2.1. Sejam $\Gamma = \Gamma_i$ e $F = F_i$, $1 \leq i \leq u$, fixados. Se $F(X, Y, a) \equiv 0$ para todo $a \in \Gamma_i$, é imediato o lema. Se $\partial_Y F(X, Y, a) = 0$ para todo $a \in \Gamma_i$, pelo Lema 1.2.1 (2), existe um polinômio F_0 em $\mathbb{R}[X, Z]$ tal que $F(X, Y, a) = F_0(X, a)$ para todo $a \in \Gamma$; logo tomando $R_i = F_0$, pelo Lema 1.2.1 (1.2.1) segue o resultado. Se $\partial_X F(X, Y, a) = 0$ para todo $a \in \Gamma$, por um argumento similar segue o lema. Suponhamos, então, que $F(X, Y, a) \neq 0$, $\partial_X F(X, Y, a) > 0$ e $\partial_Y F(X, Y, a) > 0$ para todo $a \in \Gamma$, o que ocorre pelo Lema 1.2.1 (2). Em virtude do Lema 1.2.3 podemos supor que $\partial F(X, Y, a) = \partial_Y F(X, Y, a)$ para todo $a \in \Gamma$ (vide o Lema 1.2.1 (2)); isto é, o polinômio F pode-se expressar sob a forma

$$(1.2.8) \quad F = \sum_{\alpha=0}^n f_\alpha Y^\alpha, \quad f_\alpha \in \mathbb{R}[X, Z], \quad 0 \leq \alpha \leq n-1, \quad f_n \in \mathbb{R}[Z], \quad n \in \mathbb{N}^*,$$

onde $f_n(a) \neq 0$ para todo $a \in \Gamma$. Consideremos o polinômio $G_\mu = G_{i,\mu}$ em $\mathbb{R}[X,Y,Z]$ dado por

$$G_\mu = (X-\mu)F_Y - YF_X, \mu \in \mathbb{R}.$$

Então, pelo Lema 1.2.1 (1), $F(X,Y,a)$ e $G_\mu(X,Y,a)$ verificam todas as condições do Lema 1.2.4, para todo $(\mu,a) \in \mathbb{R} \times \Gamma$; em particular

$$(1.2.9) \quad \mathbb{R}^2 \cap N(F,a) \neq \emptyset \iff \mathbb{R}^2 \cap N(F,G_\mu,a) \neq \emptyset, (\mu,a) \in \mathbb{R} \times \Gamma,$$

onde $N(F,G_\mu,a) = \{z \in \mathbb{C}^2 : F(z,a)=0 \text{ e } G_\mu(z,a)=0\}$. Sejam $R_\mu \in \mathbb{R}[X,Z]$ e $Q_\mu \in \mathbb{R}[Y,Z]$, $\mu \in \mathbb{R}$, as resultantes de F e G_μ , considerados como elementos de $\mathbb{R}(X,Z)[Y]$ e $\mathbb{R}(Y,Z)[X]$ respectivamente. Como $\partial_X F(X,Y,a) > 0$ e $\partial_Y F(X,Y,a) > 0$ para todo $a \in \Gamma$, segue pelos lemas: 1.2.1 (1) e 1.2.5 que

$$(1.2.10) \quad \forall a \in \Gamma, \exists \mu_a \in \{0, \dots, n\} : R_{\mu_a}(X,a)Q_{\mu_a}(Y,a) \neq 0.$$

Seja $A_\mu = A_{i,\mu}$ o subconjunto de Γ dado por $A_\mu = \{a \in \Gamma : R_\mu(X,a)Q_\mu(Y,a) \neq 0\}$, $0 \leq \mu \leq n$. Então, pela Observação 1.2.1, $A_\mu \in \mathcal{A}$ e por (1.2.10) segue que

1) Γ é reunião dos A_μ , $0 \leq \mu \leq n$.

Sejam $A = A_\mu$, $G = G_\mu$, $R = R_\mu$ e $Q = Q_\mu$, $0 \leq \mu \leq n$, fixados. Usando o Lema 1.1.5, aplicado aos pares (A,R) e (A,Q) respectivamente, podemos achar (A_j^*, R_j^*) em $A \times \mathbb{R}[X,Z]$ e (A_j^*, Q_j^*) em $A \times \mathbb{R}[Y,Z]$, $1 \leq j \leq s$, $s = s_\mu \geq 1$, tais que

- 2) A é reunião disjunta dos A_j^*
- 3) $\partial R_j^*(X,a) = \partial_x R_j^*$ e $\partial Q_j^*(Y,a) = \partial_y Q_j^*$ para todo $a \in A_j^*$
- 4) $R_j^*(X,a)$ e $R(X,a)$ ($Q_j^*(Y,a)$ e $Q(Y,a)$) possuem as mesmas raízes exceto que todas as raízes de $R_j^*(X,a)$ ($Q_j^*(Y,a)$) são simples, para todo $a \in A_j^*$.

Sejam $A^* = A_j^*$, $R^* = R_j^*$ e $Q^* = Q_j^*$, $1 \leq j \leq s$, fixados. Então, por (1.2.10), 1), 2), 3) e 4), é fácil ver que (A^*, R^*, Q^*) satisfaz as condições 1*) e 2*) (e portanto 3*) e 4*)) do Lema 1.2.6. Fixemos, por um momento, um ponto $a \in A^*$. Seja (b,c) em $N(F,G,a)$. Então os polinômios $F(b,Y,a)$ e $G(b,Y,a)$ possuem como fator comum $(Y-c)$; logo, pelo Teorema 0.1.3, o resultante $R(b,a) = 0$ e portanto, por 4), $R^*(b,a) = 0$. De modo análogo, prova-se $Q^*(c,a) = 0$. Assim, com as notações do Lema 1.2.6, temos provado

$$(1.2.11) \quad N(F,G,a) \subset \{(x_i(a), y_j(a)) : 1 \leq i \leq r, 1 \leq j \leq s\};$$

além disso, por (1.2.9),

$$(1.2.12) \quad \mathbb{R}^2 \cap N(F,a) \neq \emptyset \implies \mathbb{R} \cap N(R^*,a) \neq \emptyset.$$

Seja, agora, $x(a) \in \mathbb{R}$ tal que $R^*(x(a),a) = 0$. Então, $R(x(a),a) = 0$ e como $f_n(a) \neq 0$ (vide (1.2.8)), pelo Teorema 0.1.3, os polinômios $F(x(a),Y,a)$ e $G(x(a),Y,a)$ possuem um fator comum não trivial em $\mathbb{R}[Y]$ e portanto existe $y(a) \in \mathbb{C}$ tal que $(x(a), y(a)) \in N(F,G,a)$. Se $y(a) \in \mathbb{R}$ então $(x(a), y(a)) \in \mathbb{R}^2 \cap N(F,G,a)$.

logo por (1.2.9), $\mathbb{R}^2 \cap N(F,a) \neq \emptyset$. Mas, se $y(a) \in \mathbb{C} \setminus \mathbb{R}$ então $(x(a), y(a)), (x(a), \overline{y(a)}) \in N(F,G,a)$, pois o fator comum não trivial de $F(x(a), Y, a)$ e $G(x(a), Y, a)$ pertence a $\mathbb{R}[Y]$. Então, observemos que, se para todo $(x_0, y_0), (x_1, y_1)$ em $N(F,G,a)$, com $(x_0, y_0) \neq (x_1, y_1)$ se tivesse $x_0 \neq x_1$, então teríamos sempre $y(a) \in \mathbb{R}$ e portanto, por (1.2.12)

$$\mathbb{R}^2 \cap N(F,a) \neq \emptyset \iff \exists j \in \{0, \dots, n\} : a \in A_j^* \text{ e } \mathbb{R} \cap N(R^*, a) \neq \emptyset;$$

logo, por (1.2.1), o lema estaria provado. Por uma conveniente mudança linear nas (X, Y, Z) - coordenadas (no caso, uma translação do eixo X e uma homotetia do eixo Y) estaremos na situação da observação acima. De fato, seja H o polinômio em $\mathbb{R}[W, Z]$, W uma variável, dado por

$$(1.2.13) \quad H(W, Z) = H^*(W, Z) F_n(1, W, Z), \quad n = \partial F(X, Y, a), \quad a \in A^*$$

onde H^* é dado no Lema 1.2.6 (4*) e F_n é a parte principal de F . Como $\partial_Y F(X, Y, a) = \partial F(X, Y, a) = n$ para todo $a \in A^*$, é claro que, $F_n(1, W, a) \neq 0$, $a \in A^*$; logo, pelo Lema 1.2.6 (4*), segue que $H(W, a) \neq 0$ para todo $a \in A^*$. Então, pelo Lema 1.2.2 (aplicado a (A^*, H)), existem (Δ_v, λ_v) em $A \times \mathbb{R}(Z)$, $0 \leq v \leq t$, $t = t_j \geq 1$, onde $\lambda_v = \phi_v \psi_v^{-1}$ com $\phi_v, \psi_v \in \mathbb{R}[Z]$ tais que

5) A^* é reunião disjunta dos Δ_v

6) $\lambda_v(a) \neq 0$ para todo $a \in \Delta_v$.

Além disso,

$$(1.2.14) \quad H(\lambda_v(a), a) \neq 0, \text{ para todo } a \in \Delta_v.$$

Logo, pelo Lema 1.2.6 (4*), (1.2.13) e (1.2.14), tem-se

$$(1.2.15) \quad \lambda_v(a) \neq \frac{y_k(a) - y_\ell(a)}{x_i(a) - x_j(a)}, (1 \leq i, j \leq r, i \neq j), (1 \leq k, \ell \leq s, k \neq \ell), (a \in \Delta_v),$$

$$(1.2.16) \quad F_n(1, \lambda_v(a), a) \neq 0, \text{ para todo } a \in \Delta_v, 1 \leq v \leq t.$$

Sejam $\Delta = \Delta_v$ e $\lambda = \lambda_v$, $1 \leq v \leq t$, fixados, e consideremos os polinômios $\tilde{F}$ e $\tilde{G}$ em $\mathbb{R}[X', Y', Z]$ dados por

$$\tilde{F}(X', Y', Z) = \tilde{\psi}(Z) F(X' + Y', \lambda(Z) Y', Z), \quad \tilde{\psi} = \psi^{2n},$$

$$\tilde{G}(X', Y', Z) = \tilde{\phi}(Z) G(X' + Y', \lambda(Z) Y', Z), \quad \tilde{\phi} = \psi^{2d}, \quad d = \partial G;$$

além disso, para cada $a \in \Delta$ fixo, seja

$$\tilde{N}(F, G, a) = \{z \in \mathbb{C}^2 : \tilde{F}(x, a) = 0 \text{ e } \tilde{G}(z, a) = 0\}.$$

Então, como

$$x' = x - \lambda^{-1} y \text{ e } y' = \lambda^{-1} y \iff x = x' + y' \text{ e } y = \lambda y'$$

obtém-se facilmente que

$$(1.2.17) \quad \mathbb{R}^2 \cap N(F, G, a) \neq \emptyset \iff \mathbb{R}^2 \cap \tilde{N}(F, G, a) \neq \emptyset;$$

além disso, por (1.2.11), segue que

$$(1.2.18) \quad \tilde{N}(F,G,a) \subset \{(x_i(a) - \lambda^{-1}(a)y_k(a), \lambda^{-1}(a)y_k(a)) : 1 \leq i \leq r, 1 \leq k \leq s\}.$$

Afirmamos que

7) O termo dominante de $\tilde{F}(X', Y', a)$, considerado como um elemento de $\mathbb{R}(X')[Y']$, é da forma $h(a)(Y')^n$, onde $h \in \mathbb{R}[Z]$ e $h(a) \neq 0$. De fato, se $\tilde{F}_n(X', Y', a)$ é a parte principal de $\tilde{F}(X, Y, a)$ então, é claro que, $\tilde{F}_n(X', Y', a) = F_n(X' + Y', \lambda(a)Y', a)$, logo, por (1.2.16), $\tilde{F}_n(0, 1, a) = F_n(1, \lambda(a), a) \neq 0$, donde segue a afirmação.

Seja $\tilde{R} \in \mathbb{R}[X', Z]$ a resultante de $\tilde{F}$ e $\tilde{G}$, considerados como elementos de $\mathbb{R}(X', Z)[Y]$. Então, como (pelo Corolário 1.2.1) $\tilde{F}(X, Y, a)$ e $\tilde{G}(X, Y, a)$ não possuem fator comum de grau maior que zero em $\mathbb{R}(X')[Y]$, segue (pelo Teorema 0.1.3 e por 7)) que $\tilde{R}(X', a) \neq 0$. Agora provaremos que

$$(1.2.19) \quad \mathbb{R}^2 \cap \tilde{N}(F, G, a) \neq \emptyset \iff \mathbb{R} \cap \tilde{N}(\tilde{R}, a) \neq \emptyset.$$

Com efeito, se $(x(a), y(a)) \in \mathbb{R}^2 \cap \tilde{N}(F, G)$ então $\tilde{F}(x(a), Y', a)$ e $\tilde{G}(x(a), Y', a)$ possuem como fator comum $(Y' - y(a))$; logo, pelo Teorema 0.1.3, a resultante $\tilde{R}(x(a), a) = 0$. Reciprocamente, se $x(a) \in \mathbb{R}$ e $\tilde{R}(x(a), a) = 0$, como $h(a) \neq 0$, pelo Teorema 0.1.3 os polinômios $\tilde{F}(x(a), Y', a)$ e $\tilde{G}(x(a), Y', a)$ possuem um fator comum em $\mathbb{R}[Y']$ de grau maior que zero e portanto existe $y(a) \in \mathbb{C}$ tal que $(x(a), y(a)) \in \tilde{N}(F, G, a)$. Se $y(a) \in \mathbb{C} \setminus \mathbb{R}$ então $(x(a), y(a))$, $(x(a), \overline{y(a)}) \in \tilde{N}(F, G, a)$; logo, por (1.2.18), existem $i, j \in \{1, \dots, r\}$ e $k, \ell \in \{1, \dots, s\}$ tais que $x_i(a) - \lambda^{-1}(a)y_k(a) = x_j(a) -$

- $\lambda^{-1}(a)y_{\ell}(a)$, como $y(a) \neq \overline{y(a)}$ e $\lambda(a) \neq 0$ segue que $k \neq \ell$ e portanto $i \neq j$, mas este fato contradiz (1.2.15). Assim, $y(a) \in \mathbb{R}$ o que prova que $\mathbb{R}^2 \cap \tilde{N}(F, G, a) \neq \emptyset$. Finalmente, pelo Lema 2.1.1 (0), por 1), 2) e 5) segue que $\mathbb{R}^m$ é reunião dos Δ_v , $1 \leq v \leq t$, e portanto de (1.2.1), (1.2.9), (1.2.17) e (1.2.19) obtém-se diretamente (1.2.7). ■

LEMA 1.2.8 - Seja (P, H) em $\mathbb{R}[X, Y, Z]$, X e Y uma variável. Então, existem (Δ_i, P_i) em $A \times \mathbb{R}[X, Z]$, $1 \leq i \leq s$, $s \geq 1$, tais que para todo $a \in \mathbb{R}^m$ tem-se

$$[\exists x_0 \in \mathbb{R}: \mathbb{R} \cap N(P, x_0, a) \neq \emptyset \text{ e } H(x_0, a) \neq 0] \iff [\exists i \in \{1, \dots, s\}; a \in \Delta_i \text{ e } \mathbb{R} \cap N(P_i, a) \neq \emptyset].$$

PROVA - Pelo Lema 1.1.11, aplicado a (P, H) , existem (Γ_i, M_i) em $A \times \mathbb{R}[X, Z]$, $1 \leq i \leq r$, $r \geq 1$, tais que

- 1) $\mathbb{R}^m$ é reunião disjunta dos Γ_i
- 2) $\partial M_i(X, a) = \partial_X M_i$ e $\partial H(X, a) = \text{cte}$ para todo $a \in \Gamma_i$.
- 3) $M_i(X, a)$ é um mdc de $P(X, Y, a)$ e $H(X, a)$ em $\mathbb{R}[X, Y]$ para todo $a \in \Gamma_i$.

Sejam $\Gamma = \Gamma_i$ e $M = M_i$, $1 \leq i \leq r$, fixados. Se $M(X, a) \equiv 0$ para todo $a \in \Gamma$, não existe nenhuma solução de $P(X, Y, a)$ e $H(X, a) \neq 0$ para nenhum $a \in \Gamma$; nesse caso basta escolher $R(X, Z) = X^2 + 1$. Suponhamos, então, que $M(X, a) \not\equiv 0$ para todo $a \in \Gamma$, o que ocorre por 2); logo, por 3) e pelo Lema 1.1.7 (aplicado a (Γ, P, M)), existem (A_j^*, F_j^*, ψ_j^*) em $A \times \mathbb{R}[X, Y, Z] \times \mathbb{R}[Z]$, $1 \leq j \leq s$, $s = s_i \geq 1$, tais

que

- 4) Γ é reunião disjunta dos A_j^*
- 5) $\psi_j^*(a) \neq 0$ e $\partial F_j^*(X, Y, a) = \partial_{xy} F^*$, para todo $a \in A_j^*$
- 6) $P(X, Y, a) = \psi_j^{*-1}(a) M(X, a) F_j^*(X, Y, a)$ para todo $a \in A_j^*$

(aqui, tomamos $F_j^* = \phi_j P_j$, sendo ϕ_j e P_j dados no Lema 1.1.7). Notemos que se $x_0 \in \mathbb{R}$ e $H(x_0, a) \neq 0$ então $M(x_0, a) \neq 0$ (pois $M(X, a)$ é um divisor de $H(X, a)$) e portanto, para todo $a \in A_j^*$, $1 \leq j \leq s$, por 5) e 6) segue facilmente

$$(1.2.20) \quad [\exists x_0 \in \mathbb{R}: \mathbb{R} \cap N(P, x_0, a) \neq \emptyset \text{ e } H(x_0, a) \neq 0] \iff [\exists x_0 \in \mathbb{R}: \mathbb{R} \cap N(F_j^*, x_0, a) \neq \emptyset \text{ e } H(x_0, a) \neq 0].$$

Sejam $A^* = A_j^*$ e $F^* = F_j^*$, $1 \leq j \leq s$, fixados. Se $F^*(X, Y, a) \equiv 0$ para todo $a \in A^*$, o resultado é imediato; pois neste caso, por 6), $P(X, Y, a) \equiv 0$ para todo $a \in A^*$ e basta escolher $R(X, Z) \equiv 0$. Suponhamos, então, que $F^*(X, Y, a) \not\equiv 0$ para todo $a \in A^*$, o que ocorre por 5). Repetindo o que foi feito com (P, H) fazemos com (F, H) e continuando o processo um número finito de vezes, podemos achar (A_k, F_k) em $A \times \mathbb{R}[X, Y, Z]$, $1 \leq k \leq t$, $t = t_j \geq 1$, tais que

- 7) A^* é reunião disjunta dos A_k
- 8) $F_k(X, Y, a)$ e $H(X, a)$ não possuem fator comum não constante em $\mathbb{R}[X, Y]$, para todo $a \in A_k$.

Além disso, para todo $a \in A_k$, $1 \leq k \leq t$, tem-se

$$(1.2.21) \quad [\exists x_0 \in \mathbb{R}: \mathbb{R} \cap N(F^*, x_0, a) \neq \emptyset \text{ e } H(x_0, a) \neq 0] \Leftrightarrow [\exists x_0 \in \mathbb{R}: N(F_k^*, x_0, a) \neq \emptyset \\ \text{ e } H(x_0, a) \neq 0].$$

Sejam $A = A_k$ e $F = F_k$, $1 \leq k \leq t$, fixados. Então, por 8) e pelo Lema 0.1.8 (3), $F(X, Y, a)$ e $H(X, a)$ não possuem fator comum (de grau maior que zero em relação a X) em $\mathbb{R}(Y)[X]$. Logo, se $R \in \mathbb{R}[Y, Z]$ é a resultante de F e H (considerados como elementos de $\mathbb{R}(Y, Z)[X]$) então, por 2) e pelo Teorema 0.1.3, tem-se que $R(Y, a) \neq 0$ para todo $a \in A$. Donde, pelo Lema 1.2.2 (aplicado a (A, R)), existem (B_ℓ, λ_ℓ) em $A \times \mathbb{R}(Z)$, $1 \leq \ell \leq u, u = u_k \geq 1$, onde $\lambda_\ell = \phi_\ell \psi_\ell^{-1}$ com $\phi_\ell, \psi_\ell \in \mathbb{R}[Z]$ tais que

9) A é reunião disjunta dos B_ℓ

10) $\phi_\ell(a) \psi_\ell(a) \neq 0$ para todo $a \in B_\ell$

11) $R(\lambda_\ell(a), a) \neq 0$ para todo $a \in B_\ell$.

Sejam $B = B_\ell$, $\phi = \phi_\ell$ e $\psi = \psi_\ell$, $1 \leq \ell \leq u$, fixados. Então, por (11) e pelo Teorema 0.1.3, segue que

12) $F(X, \lambda(a), a)$ e $H(X, a)$ não possuem fator comum (de grau maior que zero) em $\mathbb{R}[X]$, para nenhum $a \in B$.

Consideremos o polinômio G em $\mathbb{R}[X, Y^*, Z]$ dado por

$$G(X, Y^*, Z) = \psi^{2n}(Z) F(X, Y^* H(X, Z) + \lambda(Z), Z), \quad n = \partial F.$$

Notemos que se o polinômio $G(X, Y^*, a)$, $a \in B$, possui uma raiz $(x_0, y_0, a) \in \mathbb{R}^2 \times \mathbb{R}^m$ então $H(x_0, a) \neq 0$. De fato, se $H(x_0, a) = 0$ en

tão, como $\psi(a) \neq 0$, segue que $F(x_0, \lambda(a), a) = 0$ e portanto $F(X, \lambda(a), a)$ e $H(X, a)$ possuem como fator comum $(X - x_0)$ o que contradiz 12). Desta observação, para todo $a \in B$, segue imediatamente

$$(1.2.22) \quad \exists x_0 \in R: N(F, x_0, a) \neq \emptyset \text{ e } H(x_0, a) \neq 0 \iff \mathbb{R}^2_n N(G, a) \neq \emptyset;$$

pois, se $H(x_0, a) \neq 0$ então

$$x_0^* = x_0 \text{ e } y_0^* = H^{-1}(x_0, a)(y_0 - \lambda(a)) \iff x_0 = x_0^* \text{ e } y_0 = y_0^* H(x_0, a) + \lambda(a).$$

Pelo Lema 1.2.7, aplicado a G , existem (Δ_v, P_v) em $A \times \mathbb{R}[X, Z]$, $1 \leq v \leq v$, $v = v_\emptyset \geq 1$, tais que para todo $a \in B$ tem-se

$$(1.2.23) \quad \mathbb{R}^2_n N(G, a) \neq \emptyset \iff \exists v \in \{1, \dots, v\}: a \in \Delta_v^* \text{ e } \mathbb{R}_n N(P_v, a) \neq \emptyset,$$

onde $\Delta_v^* = B \cap \Delta_v \in A$, devido ao Lema 0.1.16 (5). Finalmente de 1), 4), (1.2.20), 7), (1.2.21), 9), (1.2.22) e (1.2.23), segue o lema. ■

LEMA 1.2.9 - Seja P um polinômio em $\mathbb{R}[X, Z]$ com $X = (X_1, \dots, X_n)$. Então, existem (Δ_i, P_i) em $\mathbb{R}[W, Z]$, W uma variável, $1 \leq i \leq r$, $r \geq 1$, tais que para todo $a \in \mathbb{R}^m$ tem-se

$$\mathbb{R}^n_n N(P, a) = \emptyset \iff \exists i \in \{1, \dots, r\}: a \in \Delta_i \text{ e } \mathbb{R}_n N(P_i, a) \neq \emptyset.$$

PROVA - A demonstração será por indução finita sobre n . Com efeito, se $n = 1$ então, escolhendo $\Delta_1 = \mathbb{R}^m$ e $P_1 = P$ segue o lema. Se $n = 2$ é o Lema 1.2.7. Suponhamos, então, que o lema se

ja verdadeiro para todo $k \leq n-1$ e consideremos um polinômio P em $\mathbb{R}[X_1, \dots, X_{n-1}][X_n, Z]$. Logo, pela hipótese de indução, existem (Δ_i, F_i) em $A_{m+1} \times \mathbb{R}[W, X_n, Z]$, $1 \leq i \leq r$, $r \geq 1$, tais que para todo $(x_n, a) \in \mathbb{R} \times \mathbb{R}^m$ tem-se

$$\mathbb{R}^{n-1} \cap N(P, x_n, a) \neq \emptyset \iff \exists i \in \{1, \dots, r\} : (x_n, a) \in \Delta_i \text{ e } \mathbb{R} \cap N(F_i, x_n, a) \neq \emptyset;$$

logo, para todo $a \in \mathbb{R}^m$ tem-se

$$(1.2.24) \quad [\exists x_n \in \mathbb{R} : \mathbb{R}^{n-1} \cap N(P, x_n, a) \neq \emptyset] \iff [\exists (i, x_n) \in \{1, \dots, r\} \times \mathbb{R} : (x_n, a) \in \Delta_i \\ \text{ e } \mathbb{R} \cap N(F_i, x_n, a) \neq \emptyset].$$

Para cada $i \in \{1, \dots, r\}$ fixo, pela Definição 0.1.10 (2), existem polinômios G_i e H_i em $\mathbb{R}[X_n, Z]$ tais que

$$\Delta_i = \{(x_n, a) \in \mathbb{R} \times \mathbb{R}^m : G_i(x_n, a) = 0 \text{ e } H_i(x_n, a) \neq 0\}.$$

Consideremos o polinômio P_i em $\mathbb{R}[W, X_n, Z]$ dado por

$$P_i = F_i^2 + G_i^2, \quad 1 \leq i \leq r.$$

Então, para todo $a \in \mathbb{R}^m$ é claro que

$$(1.2.25) \quad [\exists x_n \in \mathbb{R} : (x_n, a) \in \Delta_i \text{ e } \mathbb{R} \cap N(F_i, x_n, a) \neq \emptyset] \iff [\exists x_n \in \mathbb{R} : \mathbb{R} \cap N(P_i, x_n, a) \neq \emptyset \\ \text{ e } H_i(x_n, a) \neq 0].$$

Tomando $X = W$ e $Y = X_n$, pelo Lema 1.2.8 aplicado ao par (P_i, H_i) , existem (Δ_{ij}, P_{ij}) em $A \times \mathbb{R}[W, Z]$, $1 \leq j \leq s_i$, $s_i \geq 1$, tais que para todo $a \in \mathbb{R}^m$ tem-se

$$(1.2.26) \quad [\exists x_n \in \mathbb{R}: \mathbb{R} \cap N(P_i, x_n, a) \neq \emptyset \text{ e } H_i(x_n, a) \neq \emptyset] \iff [\exists j \in \{1, \dots, s_i\}: a \in \Delta_{ij} \\ \text{ e } \mathbb{R} \cap N(P_{ij}, a) \neq \emptyset].$$

Finalmente, como

$$\mathbb{R}^n \cap N(P, a) \neq \emptyset \iff \exists x_n \in \mathbb{R}: \mathbb{R}^{n-1} \cap N(P, x_n, a) \neq \emptyset,$$

de (1.2.24), (1.2.25) e (1.2.26), para todo $a \in \mathbb{R}^m$, tem-se

$$\mathbb{R}^n \cap N(P, a) \neq \emptyset \iff [\exists i \in \{1, \dots, r\} \text{ e } \exists j \in \{1, \dots, s_i\}: a \in \Delta_{ij} \\ \text{ e } \mathbb{R} \cap N(P_{ij}, a) \neq \emptyset],$$

o que prova o lema. ■

DEFINIÇÃO 1.2.1 - Seja B um subconjunto de $\mathbb{R} \times \mathbb{R}^m$. Então, diremos que B é *semi-algêbrico especial* em $\mathbb{R}^{m+1}$ se tem uma das formas

$$B = \{(x, a) \in \mathbb{R} \times \mathbb{R}^m: P(x, a) = 0\} \text{ ou } B = \{(x, a): Q(a) \neq 0 \text{ e } R(x, a) = 0\}$$

onde $P, R \in \mathbb{R}[X, Z]$ e $Q \in \mathbb{R}[Z]$, X uma variável.

Denotemos por π a projeção $(x, a) \in \mathbb{R}^n \times \mathbb{R}^m \mapsto a$ e por p a projeção $(\xi, a) \in \mathbb{R} \times \mathbb{R}^m \mapsto a$.

COROLÁRIO 1.2.1 (do Lema 1.2.9) - Seja A um conjunto algêbrico em $\mathbb{R}^n \times \mathbb{R}^m$. Então, existem conjuntos semi-algêbricos especiais B_i em $\mathbb{R} \times \mathbb{R}^m$, $1 \leq i \leq r$, $r \geq 1$, tais que

$$\pi(A) = \bigcup_{i=1}^r p(B_i).$$

1.3 - PROVA DO TEOREMA S-T

Dado um conjunto algébrico A em $\mathbb{R}^n \times \mathbb{R}^m$ provaremos a seguir que $\pi(A)$ é semi-algébrico em $\mathbb{R}^m$. Para isso, começaremos demonstrando o caso $n=1$ que é o seguinte.

LEMA 1.3.1 - Seja A um conjunto algébrico em $\mathbb{R} \times \mathbb{R}^m$. Então a imagem de A pela projeção $\pi: (x,a) \in \mathbb{R} \times \mathbb{R}^m \mapsto a$ é SA em $\mathbb{R}^m$.

PROVA - Pela Definição 0.1.10 (1), existe um polinômio P em $\mathbb{R}[X,Z]$, nas variáveis X e $Z = (Z_1, \dots, Z_m)$ tal que $A = \{(x,a): P(x,a) = 0\}$. Notando que

$$a \in \pi(A) \iff (\exists x \in \mathbb{R}: P(x,a) = 0) \iff a \in \mathbb{R}^m \text{ e } \mathbb{R} \cap N(P,a) \neq \emptyset,$$

para nosso objetivo basta achar um SA Γ em $\mathbb{R}^m$ tal que

$$(1.3.1) \quad a \in \mathbb{R}^m \text{ e } \mathbb{R} \cap N(P,a) \neq \emptyset \iff a \in \Gamma.$$

De fato, pelo Lema 1.1.4 (aplicado ao par $(P, \dot{P}_X)$) existem $(\Gamma_i, Q_{ij}, R_{ij})$ em $A_m \times (\mathbb{R}(Z)[X])^2$, $0 \leq j \leq v_i + 1$, $1 \leq i \leq r$, $r \geq 1$, onde $R_{ij} = \phi_{ij} \psi_{ij}^{-1}$, com $\phi_{ij} \in \mathbb{R}[X,Z]$, $\psi_{ij} \in \mathbb{R}[Z]$, satisfazendo (1.1.16), (1.1.17) e (1.1.18). Sejam $\Gamma = \Gamma_i$, $R_j = R_{ij}$ e $\psi_j = \psi_{ij}$, $1 \leq i \leq r$, $0 \leq j \leq v+1$, $v = v_i$, fixados. Se $P(X,a) \equiv 0$ para todo $a \in \Gamma$, é claro que, $\mathbb{R} \cap N(P,a) \neq \emptyset$ para todo $a \in \Gamma$. Suponhamos, então, que $P(X,a) \not\equiv 0$ para todo $a \in \Gamma$, o que ocorre por (1.1.17). Das igualdades em (1.1.18) segue que a sequência padrão associada ao polinômio $P(X,a)$ é dada por

$$S(P,a) = \{P(X,a), P_X(X,a), R_0(X,a), \dots, R_v(X,a)\}, a \in \Gamma.$$

Em virtude de (1.1.17) podemos supor que

$$P = \sum_{\alpha=0}^n p_{\alpha} X^{\alpha}, p_{\alpha} \in \mathbb{R}[Z], n \in \mathbb{N},$$

onde $p_n(a) \neq 0$ para todo $a \in \Gamma$. Consideremos a função racional $\lambda \in \mathbb{R}(Z)$ dada por

$$\lambda = (1+p_n^{-2}) \left(n + \sum_{\alpha=0}^{n-1} p_{\alpha}^2 \right) \text{ se } n \neq 0 \text{ e } \lambda(Z) \equiv 1 \text{ se } n = 0.$$

Então, pela Definição 0.2.1 e pelo Lema 0.2.1, para todo $a \in \Gamma$ tem-se

$$(1.3.2) \quad \mathbb{R}nN(P,a) \neq \emptyset \iff V(-\lambda(a)) > V(\lambda(a)).$$

Consideremos os seguintes polinômios em $\mathbb{R}[Z]$

$$(1.3.3) \quad \begin{aligned} F^- &= p_n^{4n} P(-\lambda, Z), F^+ = p_n^{4n} P(\lambda, Z) \\ G^- &= p_n^{4m} P_X(-\lambda, Z), G^+ = p_n^{4m} P_X(\lambda, Z) \\ R_j^- &= p_n^{4m_j} R_j^*(-\lambda, Z), R_j^+ = p_n^{4m_j} R_j^*(\lambda, Z) \end{aligned}$$

onde $m = \partial P_X$, $m_j = \partial_X R_j^*$, $R_j^* = (\psi^2 R_j) \in \mathbb{R}[X, Z]$, e ψ é um mmc dos ψ_j , $0 \leq j \leq v$. Então para todo $(x,a) \in \mathbb{R} \times \Gamma$, como $\psi^2(a) > 0$ e $p_n^2(a) > 0$, é claro que

$$V\{P(x,a), \dots, R_v(x,a)\} = V\{P(x,a), \dots, R_v^*(x,a)\}$$

e portanto, para todo $a \in \Gamma$ tem-se

$$V[\{P(\lambda(a), a), \dots, R_V^*(\lambda(a), a)\}] = V[\{F^+(a), \dots, R_V^+(a)\}]$$

$$V[\{P(-\lambda(a), a), \dots, R_V^*(-\lambda(a), a)\}] = V[\{F^-(a), \dots, R_V^-(a)\}];$$

logo, relacionando estas igualdades com (1.3.2), para todo $a \in \Gamma$, segue que

$$(1.3.4) \quad \mathbb{R}nN(P, a) \neq \emptyset \iff V[\{F^+(a), \dots, R_V^+(a)\}] < V[\{F^-(a), \dots, R_V^-(a)\}].$$

Observando que $0 \leq V[\{F^-(a), \dots, R_V^-(a)\}] \leq v+2$, $a \in \Gamma$, afirmamos que existem conjuntos SA A_j (os quais são determinados pelos polinômios dados em (1.3.3) considerando todas as possíveis combinações de sinal da sequência $\{F^+(a), \dots, R_V^+(a), F^-(a), \dots, R_V^-(a) : a \in \Gamma\}$), $1 \leq j \leq t$, $t = t_i \geq 1$, tais que para todo $a \in \Gamma$ tem-se

$$V[\{F^+(a), \dots, R_V^+(a)\}] < V[\{F^-(a), \dots, R_V^-(a)\}] \iff \bigcup_{j=1}^t A_j$$

e portanto, por (1.3.4), para todo $a \in \Gamma$ tem-se

$$(1.3.5) \quad \mathbb{R}nN(P, a) \neq \emptyset \iff a \in \bigcup_{j=1}^t A_j.$$

De fato, por comodidade de notação, suporemos que a sequência padrão $S(P, a)$ consiste de dois elementos (a demonstração é análoga quando $S(P, a)$ tem mais de dois elementos). Consideremos, então, os seguintes conjuntos SA em $\mathbb{R}^m$.

$$A_1 = \{a: F^-(a) > 0, G^-(a) < 0, F^+(a) > 0 \text{ e } G^+(a) > 0\}$$

$$A_2 = \{a: F^-(a) > 0, G^-(a) < 0, F^+(a) < 0 \text{ e } G^+(a) < 0\}$$

$$A_3 = \{a: F^-(a) < 0, G^-(a) > 0, F^+(a) > 0 \text{ e } G^+(a) > 0\}$$

$$A_4 = \{a: F^-(a) < 0, G^-(a) > 0, F^+(a) < 0 \text{ e } G^+(a) < 0\}.$$

Então, como $V[\{F^-(a), G^-(a)\}] \leq 1$, para todo $a \in \Gamma$ é claro que

$$V[\{F^+(a), G^+(a)\}] < V[\{F^-(a), G^-(a)\}] \iff a \in \bigcup_{i=1}^4 A_i.$$

Finalmente, se $\Gamma = \bigcup_{i=1}^r \bigcup_{j=1}^{t_i} (\Gamma_i \cap A_{ij})$ então, por (1.1.16) e (1.3.5), segue (1.3.1). Notemos que cada $\Gamma_i \cap A_{ij}$ é SA em $\mathbb{R}^m$, devido ao Lema 0.1.16 (3 e 4), e portanto pelo mesmo lema Γ é SA em $\mathbb{R}^m$. $\square$

TEOREMA 1.3.1 (de Seidenberg - Tarski) - Seja A um conjunto algébrico em $\mathbb{R}^n \times \mathbb{R}^m$. Então, a imagem de A pela projeção

$$\pi: (x, a) \in \mathbb{R}^n \times \mathbb{R}^m \longmapsto a \text{ é SA em } \mathbb{R}^m.$$

PROVA - Pela Definição 0.1.10 (1), existe um polinômio P em $\mathbb{R}[X, Z]$ nas variáveis $X = (X_1, \dots, X_n)$ e $Z = (Z_1, \dots, Z_m)$ tal que $A = \{(x, a) \in \mathbb{R}^{m+n}: P(x, a) = 0\}$. Observando que

$$a \in \pi(A) \iff (\exists x \in \mathbb{R}^n: P(x, a) = 0) \iff a \in \mathbb{R}^m \text{ e } \mathbb{R}^n \cap N(P, a) \neq \emptyset,$$

para nosso objetivo basta achar um SA Γ tal que

$$(1.3.6) \quad a \in \mathbb{R}^m \text{ e } \mathbb{R}^n \cap N(P, a) \neq \emptyset \iff a \in \Gamma.$$

De fato, pelo Lema 1.2.9, existem (Δ_i, P_i) em $A_m \times \mathbb{R}[W, Z]$, $1 \leq i \leq s$, $s \geq 1$, W uma variável, tais que

$$(1.3.7) \quad a \in \mathbb{R}^m \text{ e } \mathbb{R}^n \cap N(P, a) \neq \emptyset \iff \exists i \in \{1, \dots, s\} : a \in \Delta_i \text{ e } \mathbb{R}^n \cap N(P_i, a) \neq \emptyset.$$

Para cada P_i , pelo Lema 1.3.1, existe um SA Γ_i em $\mathbb{R}^m$ tal que

$$(1.3.8) \quad a \in \Delta_i \text{ e } \mathbb{R}^n \cap N(P_i, a) \neq \emptyset \iff a \in \Delta_i \cap \Gamma_i, \quad 1 \leq i \leq s.$$

Logo, de (1.3.7) e (1.3.8), tomando $\Gamma = \bigcup_{i=1}^s (\Delta_i \cap \Gamma_i)$, segue

(1.3.6). Observemos que cada $\Delta_i \cap \Gamma_i$, pelo Lema 0.1.16 (3 e 4), é SA em $\mathbb{R}^m$ e portanto, pelo mesmo lema, Γ é SA em $\mathbb{R}^m$. ■

Uma consequência importante deste teorema é o

TEOREMA 1.3.2 - A imagem de um conjunto SA por uma função polinomial é SA.

PROVA - Devido ao Lema 0.1.17, basta provar que a imagem de um conjunto algébrico A em $\mathbb{R}^n$ sob uma função polinomial Φ de $\mathbb{R}^n$ em $\mathbb{R}^m$ é SA em $\mathbb{R}^m$. Ora, seja G o gráfico de Φ

$$G = \{(x, y) \in \mathbb{R}^n \times \mathbb{R}^m : y = \Phi(x)\},$$

que evidentemente é algébrico em $\mathbb{R}^n \times \mathbb{R}^m$ e seja $B = \{(x, y) \in \mathbb{R}^{m+n} : x \in A\}$. Então, é claro que, B é algébrico em $\mathbb{R}^n \times \mathbb{R}^m$; logo $B \cap G$ é algébrico em $\mathbb{R}^n \times \mathbb{R}^m$ e também é claro que

$$B \cap G = \{(x, y) \in \mathbb{R}^n \times \mathbb{R}^m : x \in A \text{ e } y = \Phi(x)\}.$$

Mas a imagem de B_0G , sob a projeção $(x,y) \mapsto y$ é $\Phi(A)$ e portanto, pelo Teorema 1.3.1, $\Phi(A)$ é SA em $\mathbb{R}^m$. ■

CAPÍTULO II

PROLONGAMENTO ANALÍTICO E COMPORTAMENTO ASSINTÓTICO

DOS CONJUNTOS SEMI-ALGÉBRICOS EM $\mathbb{R}^2$

Em todo o presente capítulo chamaremos de plano com plexo — ou simplesmente de plano — ao conjunto $\mathbb{C}$, dos números complexos, junto com o ponto do infinito. Se a é um pon to do plano e r um elemento de $]0, \infty[$ então denotaremos por $\Delta(a, r)$ o conjunto de todos os pontos $z \neq \infty$ tais que $0 < |z - a| < r$ e será chamado uma *vizinhança anular* do ponto a . Denotaremos por $\hat{\Delta}(a, r)$ o conjunto $\Delta(a, r)$ menos o segmento $[a - r, a]$ ao qual de nominaremos *vizinhança logarítmica* de a .

Nosso objetivo nas duas primeiras seções é demonstrar o seguinte

TEOREMA A - Seja P um polinômio em $\mathbb{C}[Z, W]$ dado sob a forma

$$P(Z, W) = \sum_{j=0}^m p_j(Z) W^j, \quad m \geq 1,$$

onde $p_j \in \mathbb{C}[Z]$ e $p_m \neq 0$. Então, para cada ponto a do plano

existem m elementos de função $(f_j, \hat{\Delta}(a, r))$, $r = r(a) > 0; 1 \leq j \leq m$, e números naturais correspondentes $h_j \in \{1, \dots, m\}$ tais que

$$(2.0.1) \quad P(z, W) = p_m(z) \prod_{j=1}^m [W - f_j(z)], \text{ para todo } z \in \hat{\Delta}(a, r)$$

se $j = 1, \dots, m$ então para todo $z \in \hat{\Delta}(a, r)$ tem-se

$$f_j(z) = \sum_{n=m_j}^{\infty} a_{n,j} [(z-a)^{1/h_j}]^n, \text{ se } a \neq \infty,$$

(2.0.2)

$$f_j(z) = \sum_{n=m_j}^{\infty} a_{n,j} [z^{-1/h_j}]^n, \text{ se } a = \infty,$$

onde $m_j \in \mathbb{Z}$, $a_{n,j} \in \mathbb{C}$ e $a_{m_j,j} \neq 0$.

Para este fim usaremos o método do prolongamento analítico e tudo o que será feito, nas seções acima mencionados, é unicamente para provar este teorema, deixando de lado alguns resultados importantes, de funções analíticas gerais, que não são de nossa utilidade. Para maiores detalhes ou generalidade recomendamos [1], [11], [13], etc.

2.1 - PROLONGAMENTO ANALÍTICO AO LONGO DE CURVAS

Uma curva num aberto Ω de $\mathbb{C}$ será uma função contínua de finida num intervalo fechado da reta real com valores em Ω .

DEFINIÇÃO 2.1.1 - Seja Ω um aberto conexo do plano e seja f uma função holomorfa em Ω . Então, ao par (f, Ω) chama-se um

elemento de função (e.f.). Dois e.f. (f, Ω) e (g, D) são ditos iguais, e escrevemos $(f, \Omega) = (g, D)$, se $\Omega = D$ e $f \equiv g$ em Ω .

DEFINIÇÃO 2.1.2 - Se (f, Ω) é um e.f. então o *ramo analítico* de f num ponto $z_0 \in \Omega$, denotado por $[f, z_0]$ é definido como sendo o conjunto de todos os e.f. (g, D) tais que $z_0 \in D$ e $f \equiv g$ numa vizinhança de z_0 .

DEFINIÇÃO 2.1.3 - Seja $C = \{(f_1, B_1), \dots, (f_n, B_n)\}$ uma família de e.f. tal que

- 1) Cada B_j , $1 \leq j \leq n$, é uma bola aberta
- 2) $B_j \cap B_{j+1} \neq \emptyset$ e $f_j \equiv f_{j+1}$ em $B_j \cap B_{j+1}$, $1 \leq j \leq n-1$.

Então, diz-se que C é uma cadeia de e.f. que une (f_n, B_n) a (f_1, B_1) .

DEFINIÇÃO 2.1.4 - Seja $\gamma: [a, b] \longrightarrow \mathbb{C}$ uma curva. Suponhamos que para cada $t \in [a, b]$ existe um e.f. (f_t, Ω_t) tal que

- 1) $\gamma(t) \in \Omega$
- 2) Se $t \in [a, b]$ então existe $\delta_t > 0$ tal que

$$|s-t| < \delta_t, s \in [a, b] \implies \gamma(s) \in \Omega_t \text{ e } [f_s, \gamma(s)] = [f_t, \gamma(s)].$$

Então, diz-se que (f_b, Ω_b) é um *prolongamento analítico* (p.a.) de (f_a, Ω_a) ao longo de γ - ou que $\{(f_t, \Omega_t) : t \in [a, b]\}$ é um p.a. ao longo de γ .

Desta definição é imediato a seguinte

OBSERVAÇÃO 2.1.1 - Se $\gamma_1: [b, c] \longrightarrow \Omega_b$ é uma curva qualquer e se

$(f_t, \Omega_t) = (f_b, \Omega_b)$ para todo $t \in [b, c]$ então $\{(f_t, \Omega_t) : t \in [a, c]\}$ é um p.a. ao longo da curva $\gamma\gamma_1$.

Além disso, se $\{(f_t, \Omega_t) : t \in [a, b]\}$ e $\{(g_t, D_t) : t \in [a, b]\}$ são dois p.a. ao longo da curva γ tal que $[f_a, \gamma(a)] = [g_a, \gamma(a)]$ então $[f_b, \gamma(b)] = [g_b, \gamma(b)]$ ([1], pg.279). Logo, tem sentido a seguinte

DEFINIÇÃO 2.1.5 - Se $\{(f_t, \Omega_t) : t \in [a, b]\}$ é um p.a. ao longo de uma curva $\gamma : [a, b] \rightarrow \mathbb{C}$ então o ramo $[f_b, \gamma(b)]$ é o p.a. de $[f_a, \gamma(a)]$ ao longo de γ . Os ramos $[f_a, \gamma(a)]$ e $[f_b, \gamma(b)]$ são chamados ramo inicial e ramo final, respectivamente.

DEFINIÇÃO 2.1.6 - Um e.f. (f, Ω) diz-se *prolongável ao longo de uma curva* $\gamma : [a, b] \rightarrow \mathbb{C}$, com $\gamma(a) \in \Omega$, se existe um p.a. $\{(f_t, \Omega_t) : t \in [a, b]\}$ ao longo de γ tal que $(f_a, \Omega_a) = (f, \Omega)$. E (f, Ω) diz-se *prolongável num conjunto aberto* Δ , do plano, se for prolongável ao longo de toda curva $\gamma : [a, b] \rightarrow \Delta$ tal que $\gamma(a) \in \Omega$.

LEMA 2.1.1 ([1], pg.280) - Seja $\{(f_t, \Omega_t) : t \in [a, b]\}$ um p.a. ao longo de uma curva $\gamma : [a, b] \rightarrow \mathbb{C}$. Então existe uma cadeia de e.f. $C = \{(g_j, B_j) : 1 \leq j \leq n\}$ tal que γ está contido na reunião dos B_j , $1 \leq j \leq n$, $[f_a, \gamma(a)] = [g_1, \gamma(a)]$ e $[f_b, \gamma(b)] = [g_n, \gamma(b)]$.

Uma consequência direta deste lema é o

LEMA 2.1.2 - Seja $\{(f_t, \Omega_t) : t \in [a, b]\}$ um p.a. ao longo de uma curva $\gamma : [a, b] \rightarrow \mathbb{C}$. Então,

- 1) Se P é um polinômio em $\mathbb{C}[Z, W]$ tal que $P(Z, f_a(Z)) \equiv 0$ numa bola aberta contido em Ω_a então $P(Z, f_b(Z)) \equiv 0$ numa bola aberta contido em Ω_b .
- 2) Se (f, Ω) é um e.f. tal que a reunião dos $\Omega_t, t \in [a, b]$, está contido em Ω e $f \equiv f_a$ numa bola aberta contido em Ω_a então $f \equiv f_b$ numa bola aberta contido em Ω_b .

DEFINIÇÃO 2.1.7 - Seja Δ um aberto conexo do plano e sejam $\gamma_1, \gamma_2: [a, b] \longrightarrow \Delta$ curvas tais que $\gamma_1(a) = \gamma_2(a) = z_0$ e $\gamma_1(b) = \gamma_2(b) = z_1$. Então diz-se que γ_1 e γ_2 são Δ -homotópicos se existe uma função contínua $H: [a, b] \times [0, 1] \longrightarrow \Delta$ tal que

$$(1) \quad H(t, 0) = \gamma_1(t) \quad \text{e} \quad H(t, 1) = \gamma_2(t), \quad \text{para todo } t \in [a, b]$$

$$(2) \quad H(a, s) = z_0 \quad \text{e} \quad H(b, s) = z_1, \quad \text{para todo } s \in [0, 1].$$

TEOREMA DE MONODROMIA ([1], pg.285) - Seja Δ um aberto conexo do plano e sejam γ_1, γ_2 curvas Δ -homotópicos. Se um e. f. (f, Ω) é prolongável em Δ então qualquer p.a. deste e.f. ao longo das curvas γ_1 e γ_2 leva ao mesmo ramo final.

COROLÁRIO 2.1.1 - Se Δ é um aberto simplesmente conexo do plano e se um e.f. (f, Ω) , com $\Omega \subset \Delta$, é prolongável em Δ então existe uma função holomorfa F em Δ tal que $F \equiv f$ em Ω .

PROVA (do Corolário) - Seja $z_0 \in \Omega$ fixo e seja $z \in \Delta$ arbitrário. Seja $\{(f_t, \Omega_t): t \in [a, b]\}$ um p.a. ao longo de uma curva qualquer $\gamma: [a, b] \longrightarrow \mathbb{C}$ tal que $(f, \Omega) = (f_a, \Omega_a)$. Então, seja $F_\gamma(z) = f_b(z)$.

Como Δ é simplesmente conexo, pelo Teorema de Monodromia, tem-se $F_\gamma(z) = F_\alpha(z)$ para qualquer par de curvas γ e α em Δ de z_0 a z ; assim $F(z) = F_\gamma(z)$ está bem definido para todo $z \in \Delta$. Para provar que F é holomorfa num ponto z de Δ , consideremos $\{(f_t, \Omega_t) : t \in [a, b]\}$ e γ como acima. Seja B uma bola aberta de centro z , contido em Ω_b , e seja τ um ponto arbitrário em B . Se $\gamma_1 : [b, c] \rightarrow B$ é uma curva de z a τ , então pela Observação 2.1.1, $\{(f_t, \Omega_t) : t \in [a, c]\}$ é um p.a. ao longo da curva $\gamma\gamma_1$; onde $(f_t, \Omega_t) = (f_b, \Omega_b)$ para todo $t \in [b, c]$; logo, pela definição de F , segue que $F(\tau) = f_b(\tau)$; isto é, $F \equiv f_b$ em B o que prova que F é holomorfa em z . ■

LEMA 2.1.3 ([1].pg.287) - Seja $z_0 = r_0 \in]0, r[$, $r > 0$, e seja C a curva fechada de equação $z = r_0 e^{it}$, $0 \leq t \leq 2\pi$. Então, para toda curva fechada γ em $\Delta(0, r)$, com extremidade z_0 , existe $m \in \mathbb{Z}$, $m \neq 0$, tal que γ e C^m são $\Delta(0, r)$ -homotópicos.

A partir deste lema é imediato a

OBSERVAÇÃO 2.1.2 - Seja (f, Ω) um e.f. tal que $z_0 \in \Omega$. Se denotarmos por $[f, z_0]_m$ o ramo final do p.a. de (f, Ω) ao longo de C^m , $m \in \mathbb{Z}$, então ocorre um, e um só, dos seguintes casos

- 1) $[f, z_0]_m \neq [f, z_0]$, para todo $m \in \mathbb{Z}$, $m \neq 0$
- 2) existe um menor inteiro $h > 0$ tal que $[f, z_0]_h = [f, z_0]$

No segundo caso, é claro que $[f, z_0]_m = [f, z_0]$ se, e somente se, h é um divisor de m . Neste caso consideraremos a função holomorfa $H : \tau \in \Delta(0, r) \mapsto \tau^h \in \Delta(0, r^h)$.

LEMA 2.1.4 - Seja $\Delta(a,r)$ uma vizinhança anular de um ponto a do plano, seja (f,Ω) um e.f. prolongável em $\Delta(a,r)$ tal que $\Omega \subset \hat{\Delta}(a,r)$ e seja $z_0 = a + r_0 \in \Omega$, onde $0 < r_0 < r$. Suponhamos que existe um menor inteiro $h > 0$ tal que $[f, z_0]_h = [f, z_0]$. Então,

(2.1.1) existe um e.f. $(\phi, \Delta(0, r^{1/h}))$ tal que em Ω vale $f(Z) \equiv \phi((Z-a)^{1/h})$, se $a \neq \infty$, e $f(Z) \equiv \phi(Z^{-1/h})$, se $a = \infty$.

(2.1.2) (f,Ω) pode ser estendido a um e.f. $(F, \hat{\Delta}(a,r))$ da forma
 ma $F(Z) \equiv \sum_{n \in \mathbb{Z}} a_n [(Z-a)^{1/h}]^n$, se $a \neq \infty$, e $F(Z) \equiv \sum_{n \in \mathbb{Z}} a_n [Z^{-1/h}]^n$,
 se $a = \infty$, onde $a_n \in \mathbb{C}$.

PROVA - Podemos supor que $a = 0$, aplicando uma translação ou, se $a = \infty$, uma inversão. Consideremos um ponto $\tau_0 \in \Delta' = \Delta(0, r^{1/h})$ tal que $\tau_0^h = z_0$ (como $z_0 > 0$ podemos supor $\tau_0 > 0$) e seja H a função holomorfa $\tau \in \Delta' \mapsto \tau^h \in \Delta = \Delta(0, r)$.

1) Para $\tau \in \Delta'$ fixado consideremos uma curva γ' em Δ' de τ_0 a τ e seja $\gamma: [a,b] \rightarrow \Delta$ a imagem de γ' por H . Então, como (f,Ω) é prolongável em Δ , existe um p.a. $\{(f_t, \Omega_t): t \in [a,b]\}$ ao longo de γ tal que $(f,\Omega) = (f_a, \Omega_a)$. Definimos $\phi(\tau) = f_b(\tau^h)$. ϕ está bem definido. Com efeito, sejam γ'_1 e γ'_2 duas curvas de τ_0 e τ e sejam γ_1 e γ_2 as respectivas imagens por H . Pelo Lema 2.1.3, existe $m \in \mathbb{Z}$, $m \neq 0$, tal que $\gamma'_1 \gamma'^{-1}_2$ é Δ' -homotópico a C'^m , onde C' é a curva fechada de equação $\tau = |\tau_0| e^{it}$, $0 \leq t \leq 2\pi$. Logo, é claro que, a curva imagem $\gamma_1 \gamma^{-1}_2$ é Δ -homotópico a C^{mh} . Como $[f, z_0]_h = [f, z_0]$, pela Observação 2.1.2,

tem-se $[f, z_0]_{mh} = [f, z_0]$; logo, pelo Teorema de Menodromia, o p.a. ao longo de $\gamma_1 \gamma_2^{-1}$ também leva novamente ao ramo inicial. Portanto, γ_1 e γ_2 determinam o mesmo ramo final. Para provar que ϕ é holomorfa num ponto $\tau \in \Delta'$, consideramos γ' , γ e $\{(f_t, \Omega_t) : t \in [a, b]\}$ como acima. Usando a continuidade de H podemos achar uma bola aberta B de centro τ e contido em Δ' tal que $H(B) \subset \Delta \cap \Omega_b$. Sejam $\tau_1 \in B$ e $z_1 = H(\tau_1)$ e seja γ'_1 uma curva em B de τ a τ_1 . Se $\gamma_1 : [b, c] \rightarrow H(B)$ é a imagem de γ'_1 por H então, pela Observação 2.1.1, $\{(f_t, \Omega_t) : t \in [a, b]\}$ é um p.a. ao longo da curva $\gamma \gamma_1$, onde $(f_t, \Omega_t) = (f_b, \Omega_b)$ para $t \in [b, c]$; donde, pela definição de ϕ , tem-se $\phi(\tau_1) = f_b(\tau_1^h)$, assim $\phi \equiv f_b \circ H$ em B o que prova que ϕ é holomorfa em τ . No caso particular $\tau = \tau_0$, por um argumento similar, prova-se que $\phi \equiv f \circ H$ numa bola aberta B_0 de centro τ_0 tal que $H(B_0) \subset \Omega$. Por outro lado, notando que $H(B_0)$ é um conjunto aberto contendo z_0 e definindo

$$H^{-1}(z) = z^{1/h} = \exp(1/h \operatorname{Ln} z) \text{ para todo } z \in \hat{\Delta}$$

onde $\operatorname{Ln} z$ é o logaritmo principal de z , é claro que $\phi \circ H^{-1} \equiv f \circ H \circ H^{-1} \equiv f$ em $H(B_0)$ e como Ω é conexo tem-se $\phi \circ H^{-1} \equiv f$ em Ω , isto é,

$$f(Z) \equiv \phi(H^{-1}(Z)) \equiv \phi(Z^{1/h}) \text{ em } \Omega,$$

o que implica (2.1.1). Além disso, como $\phi \equiv f \circ H$, se tomarmos

$T_j(z) = \exp[1/h(Lnz + 2\pi ij)]$ para $z \in \hat{\Delta}$, $1 \leq j \leq h-1$, teremos $H \circ T_j = I$; donde $\phi \circ T_j \equiv f \circ H \circ T_j \equiv f$ em $H(B_0)$.

2) Sendo ϕ uma função holomorfa em Δ' , ϕ possui um desenvolvimento de Laurent

$$(2.1.3) \quad \phi(\tau) = \sum_{n \in \mathbb{Z}} a_n \tau^n, \quad a_n \in \mathbb{C}, \text{ para todo } \tau \in \Delta'.$$

Além disso, como $\hat{\Delta}$ é um aberto simplesmente conexo, pelo Corolário 2.1.1 existe uma função holomorfa F em $\hat{\Delta}$ tal que $F \equiv f$ em Ω ; logo, por (2.1.1), segue que $F \equiv \phi \circ H^{-1}$ em $\hat{\Delta}$ e portanto, por (2.1.3), segue imediatamente (2.1.2). ■

2.2 - PROVA DO TEOREMA A

Seja $P \in \mathbb{C}[Z, W]$ um polinômio irreduzível em $\mathbb{C}(Z)[W]$ dado sob a forma

$$(2.2.1) \quad P(Z, W) = \sum_{j=0}^m p_j(Z) W^j, \quad m \geq 1,$$

onde $p_j \in \mathbb{C}[Z]$ e $p_m \neq 0$. Então, pelo Corolário 0.1.4 (do Lema 0.1.10) aplicado ao anel fatorial $A = \mathbb{C}[Z]$ e aos polinômios P e P_W (derivada parcial de P em relação a W), existe um polinômio M_P em $\mathbb{C}[Z, W]$ tal que M_P é um mdc de P e P_W em $\mathbb{C}(Z)[W]$ e $M = \phi P + \psi P_W$, onde $\phi, \psi \in \mathbb{C}[Z, W]$ (no caso $M_P = P_V$ em (0.1.6) e que é M no Corolário 0.1.4). Como P é irreduzível

em $\mathbb{C}(Z)[W]$, pelo Lema 0.1.6, é claro que P e P_w são relativamente primos (donde um mdc de P e P_w em $\mathbb{C}(Z)[W]$ é 1); logo $M_p(Z, W) = M_p(Z)$, isto é, o polinômio M_p não depende da variável W . Considerando os seguintes subconjuntos de $\mathbb{C}$: $\mathcal{D}_p = \{z: M_p(z) = 0\}$ e $N_p = \{z: p_m(z) = 0\}$, denotemos por $\{z_1, \dots, z_v\} = \mathcal{D}_p \cup N_p$ e $\Omega_p = \mathbb{C} \setminus (\mathcal{D}_p \cup N_p)$. Seja $z_0 \in \Omega_p$. Se (z_0, w_0) é um zero de P e P_w então, como $M_p = \phi P + \psi P_w$, z_0 é um zero de M_p e portanto $z_0 \notin \Omega_p$ o que contradiz $z_0 \in \Omega_p$. Logo, $P_w(z_0, w_0) \neq 0$. Assim, se (z, w) é um zero de P e $z \in \Omega_p$ então w é raiz simples de P (consequência do Lema 0.1.6). Portanto, o polinômio $P(z_0, W)$ (na variável W) tem exatamente m raízes distintas $w_1, \dots, w_m$. A seguir serão usados todos os elementos e as notações consideradas acima.

LEMA 2.2.1 ([1], pg.293) - Se $z_0 \in \Omega_p$ então existem m e.f. (f_k, B) , $1 \leq k \leq m$, onde B é uma bola aberta de centro z_0 , tais que

$$(2.2.2) \quad P(Z, f_k(Z)) \equiv 0 \text{ em } B \text{ e } f_k(z_0) = w_k$$

$$(2.2.3) \quad \text{Se } z \in B \text{ e } P(z, w) = 0 \text{ então existe } k \in \{1, \dots, m\} \text{ tal que } w = f_k(z).$$

LEMA 2.2.2 - Se (f, Ω) é um e.f. tal que $\Omega \subset \Omega_p$ e $P(Z, f(Z)) \equiv 0$ em Ω então (f, Ω) é prolongável em Ω_p .

PROVA - Seja $\gamma: [a, b] \rightarrow \Omega_p$ uma curva tal que $\gamma(a) \in \Omega$. Então, denotemos por T o conjunto de todos os pontos $t \in [a, b]$ tal que (f, Ω) possui um p.a. ao longo da curva $\gamma[a, t]$; isto é, ao longo da curva γ restrita a $[a, t]$. Seja $d = \sup T$. Como

$\gamma(a) \in \Omega$ e f é holomorfa em Ω , é claro que $a < d$; além disso, como $\gamma(d) \in \Omega$, existem m e.f. (f_k, B) , $1 \leq k \leq m$, satisfazendo as condições do Lema 2.2.1, onde B é uma bola aberta de centro $\gamma(d)$. Seja $c \in]a, d[$ tal que a curva $\gamma[c, d]$ esteja inteiramente contido em B e seja $\{(g_t, \Omega_t) : t \in [a, c]\}$ um p.a. ao longo da curva $\gamma[a, c]$ tal que $(f, \Omega) = (g_a, \Omega_a)$. Então, como $P(Z, f(Z)) \equiv 0$ em Ω , pelo Lema 2.1.2 (1) segue que $P(Z, g_c(Z)) \equiv 0$ numa bola aberta $B_0 \subset B \cap \Omega_c$ de centro $\gamma(c)$. Consideremos uma seqüência de pontos distintos z_j em B_0 , $j \in \mathbb{N}$, tal que $z_j \rightarrow \gamma(c)$. Então, por (2.2.3), para cada $j \in \mathbb{N}$ existe $k_j \in \{1, \dots, m\}$ tal que $g_c(z_j) = f_{k_j}(z_j)$; logo, é claro que, existem $k \in \{1, \dots, m\}$ e um subconjunto infinito I de $\mathbb{N}$ tais que $g_c(z_j) = f_k(z_j)$ para todo $j \in I$. Assim, sendo I infinito e $\gamma(c)$ um ponto de acumulação de $\{z_j : j \in I\}$ em B_0 , segue que $g_c \equiv f_k$ em B_0 . Portanto, se $(g_t, \Omega_t) = (f_k, B)$ para todo $t \in [c, d]$, então, pela Definição 2.1.4, é imediato que $\{(g_t, \Omega_t) : t \in [a, d]\}$ é um p.a. ao longo da curva $\gamma[a, d]$; isto é, (f_k, B) é um p.a. de (f, Ω) ao longo de $\gamma[a, d]$ e portanto $d \in T$. Afirmamos que $d = b$. De fato, caso contrário, usando a Observação 2.1.1 e por um argumento similar ao feito acima, podemos obter um p.a. de (f, Ω) ao longo de uma curva $\gamma[a, c_0]$ para um ponto $c_0 \in [a, b]$ escolhido de tal modo que $d < c_0 < b$ e tal que a curva $\gamma[d, c_0]$ esteja inteiramente contido em B ; assim, $d < c_0 \in T$ o que contradiz a definição de d . Logo, $b = d \in T$ e portanto (f, Ω) é prolongável ao

longo de γ ; donde, pela Definição 2.1.6, segue o lema. ■

LEMA 2.2.3 - Seja a um ponto do plano. Então, existem m e. f. $(f_k, \hat{\Delta}(a, r))$, $r = r(a) > 0$, e números naturais correspondentes $h_k \in \{1, \dots, m\}$, $1 \leq k \leq m$, satisfazendo as condições do Teorema A.

PROVA - Podemos supor que $a \neq \infty$, aplicando uma inversão se $a = \infty$. Se $a \in \Omega_p$ então o resultado é imediato, em virtude do Lema 2.2.1, neste caso $h_k = 1$ para todo $k = 1, \dots, m$. Suponhamos, então que $a \in \mathbb{C} \setminus \Omega_p = \{z_1, \dots, z_v\}$ e seja $r = r(a) > 0$ tal que a bola $B_r(a)$ não contém mais pontos $z_j \neq a$, $1 \leq j \leq v$. Seja $z_0 = a + r_0$ em $\hat{\Delta} = \hat{\Delta}(a, r)$, fixo, onde $0 < r_0 < r$. Então, como $z_0 \in \Omega_p$ podemos achar uma bola aberta Ω de centro z_0 , contido em $\hat{\Delta}$, e m.f. (f_k, Ω) , $1 \leq k \leq m$, satisfazendo as propriedades do Lema 2.2.1; além disso, podemos supor Ω tão pequeno que $f_i(z) \neq f_j(z)$ para todo $z \in \Omega$, se $i \neq j$. Seja $f = f_k$, $1 \leq k \leq m$, fixado. Então, como $\Omega \subset \Omega_p$, por (2.2.2) e pelo Lema 2.2.2, (f, Ω) é prolongável em Ω_p e portanto em $\Delta = \Delta(a, r)$. Seja $\{(g_t, \Omega_t) : t \in [0, 2\pi]\}$ um p.a. ao longo da curva fechada C de equação $z = a + r_0 e^{it}$, $0 \leq t \leq 2\pi$, tal que $(g_0, \Omega_0) = (f, \Omega)$. Como $P(Z, f(Z)) \equiv 0$ em Ω , pelo Lema 2.1.2 (1), segue que $P(Z, g_{2\pi}(Z)) \equiv 0$ numa bola aberta B_0 de centro z_0 e contido em $\Omega \cap \Omega_{2\pi}$. Logo, por um argumento similar ao feito na prova do Lema 2.2.2 (usando (2.2.3)), existe $j \in \{1, \dots, m\}$ tal que $g_{2\pi} \equiv f_j$ em B_0 ; isto é, $[f, z_0]_1 = [f_j, z_0]$. Se prolongamos, novamente, o ramo $[f_j, z_0]$ ao longo de C e-

xiste $\ell \in \{1, \dots, m\}$ tal que $[f_j, z_0]_1 = [f_\ell, z_0]$; isto é, $[f, z_0]_2 = [f_\ell, z_0]$; e assim por diante. Mas, como tais elementos são em número finito m , segue da Observação 2.1.2 que deve existir um menor inteiro $h = h_k \in \{1, \dots, m\}$ tal que $[f, z_0]_h = [f, z_0]$. Portanto, pelo Lema 2.1.4, tem-se

(2.2.5) existe um e.f. $(\phi, \Delta(0, r^{1/h}))$, $\phi = \phi_k$, tal que $f(Z) \equiv \phi((Z-a)^{1/h})$ em Ω .

(2.2.6) (f, Ω) pode ser estendido a um e.f. $(F, \hat{\Delta})$, $F = F_k$, da forma

$$F(Z) \equiv \sum_{n \in \mathbb{Z}} a_n [(Z-a)^{1/h}]^n \text{ em } \hat{\Delta}.$$

Logo, como a função $z \in \hat{\Delta} \mapsto P(z, F(z))$ é holomorfa e $P(Z, F(Z)) \equiv 0$ em Ω , segue que $P(Z, F(Z)) \equiv 0$ em $\hat{\Delta}$.

1) Como k é arbitrário, tem-se $P(Z, f_k(Z)) \equiv 0$ em Ω e $P(Z, F_k(Z)) \equiv 0$ em $\hat{\Delta}$ para todo $k \in \{1, \dots, m\}$. Logo para todo $z \in \Omega$, como $f_i(z) \neq f_j(z)$, se $i \neq j$, e como o polinômio $P(z, W)$ tem exatamente m raízes distintas, tem-se $P(z, W) = p_m(z) \prod_{j=1}^m [W - f_j(z)]$ e portanto $P(z, W) = p_m(z) \prod_{j=1}^m [W - F_j(z)]$, $z \in \hat{\Delta}$. Ora, essa igualdade consiste de fato em $(m+1)$ identidades, obtidas considerando os coeficientes de cada W^j , $0 \leq j \leq m$. Como as identidades valem em Ω e ambos os termos são holomorfas em $\hat{\Delta}$, elas também valem em $\hat{\Delta}$, o que implica (2.0.1) do Teorema A.

2) Para provar (2.0.2) suponhamos primeiro que $p_m(a) \neq 0$

Afirmamos que F é limitada numa vizinhança (em $\hat{\Delta}$) de a . De fato, supondo o contrário podemos achar uma seqüência de pontos z_j em $\hat{\Delta}$, $j \in \mathbb{N}$, tais que $z_j \rightarrow a$ e $F(z_j) \rightarrow \infty$ (donde, podemos supor $F(z_j) \neq 0$ para todo $j \in \mathbb{N}$). Como $P(z_j, F(z_j)) = 0$, a partir de (2.2.1), obtém-se

$$\frac{p_0(z_j)}{F^m(z_j)} + \frac{p_1(z_j)}{F^{m-1}(z_j)} + \dots + p_m(z_j) = 0, \quad j \in \mathbb{N},$$

logo, $\lim_{j \rightarrow \infty} p_m(z_j) = 0$ e portanto $p_m(a) = 0$ o que contradiz $p_m(a) \neq 0$. Aplicando o Lema 2.1.4 ao par $(F, \hat{\Delta})$ (vide (2.1.2) e (2.2.5)), concluimos que a função ϕ (dado em (2.1.1)) é limitada numa certa vizinhança da origem e como é holomorfa em $\Delta(0, r^{1/h})$ ela admite um desenvolvimento de Taylor em torno da origem; logo $a_n = 0$ para $n < 0$. Donde, por (2.2.6), é claro que $F(Z) \equiv \sum_{n=0}^{\infty} a_n [(Z-a)^{1/h}]^n$ em $\hat{\Delta}$. Suponhamos agora que $p_m(a) = 0$. Sejam $\sigma \in \{1, \dots, m\}$ e $q_m \in \mathbb{C}[Z]$ tais que

$$(2.2.7) \quad p_m(Z) = (Z-a)^\sigma q_m(Z) \quad \text{e} \quad q_m(a) \neq 0.$$

Então, multiplicando por $(Z-a)^{\sigma(m-1)}$ a equação (2.2.1) tem-se

$$(Z-a)^{\sigma(m-1)} P(Z, W) = p_0(Z-a)^{\sigma(m-1)} + \dots + p_m(Z-a)^{\sigma(m-1)}$$

logo, substituindo $(Z-a)^\sigma W$ por V , segue

$$(Z-a)^{\sigma(m-1)}P(Z,V(Z-a)^{-\sigma}) = p_0(Z-a)^{\sigma(m-1)} + p_1(Z-a)^{\sigma(m-2)} + \\ + \dots + p_{m-1}V^{m-1} + p_mV^m(Z-a)^{-\sigma}.$$

Se $q_0 = p_0(Z-a)^{\sigma(m-1)}$, $q_1 = p_1(Z-a)^{\sigma(m-2)}$, ..., $q_{m-1} = p_{m-1}$ então, por (2.2.7) e pela última igualdade, conclui-se

$$(2.2.8) \quad (Z-a)^{\sigma(m-1)}P(Z,V(Z-a)^{-\sigma}) = q_0 + q_1V + \dots + q_mV^m,$$

com $q_m(a) \neq 0$. Seja Q o polinômio em $\mathbb{C}[Z,V]$ dado por (2.2.8). Então, não é difícil ver que, Q é irredutível em $\mathbb{C}(Z)[V]$, pois o polinômio $P(Z,W)$ o é. Além disso, observando que $Q_V(Z,V) = (Z-a)^{\sigma(m-2)}P_W(Z,V(Z-a)^{-\sigma})$ e multiplicando (0.1.6) por $(Z-a)^{\sigma(m-1)}$, é fácil ver que $M_q(Z) = M_p(Z)(Z-a)^{\sigma(m-1)}$. Então, por (2.2.7) (usando as notações dadas no início desta seção), é claro que $N_p = N_q \cup \{a\}$, $\mathcal{D}_q = \mathcal{D}_p \cup \{a\}$ e $\mathcal{D}_q \subset N_p \cup \mathcal{D}_p$ (pois $a \in N_p$). Logo, $N_q \cup \mathcal{D}_q \subset N_p \cup \mathcal{D}_p$ e portanto $\Omega_p \subset \Omega_q$. Por outro lado, se $g(Z) \equiv (Z-a)^{\sigma}f(Z)$, $g = g_k$, em B então

$$(2.2.2') \quad Q(Z,g(Z)) \equiv (Z-a)^{\sigma(m-1)}P(Z,f(Z)) \equiv 0 \text{ em } B$$

$$(2.2.3') \quad \text{se } z \in B \text{ e } Q(z,v) = 0 \text{ então } (z-a)^{\sigma(m-1)}P(z,v(z-a)^{-\sigma}) = 0 \text{ e como } z \neq a, \text{ por (2.2.3), existe } k \in \{1, \dots, m\} \text{ tal que } v(z-a)^{-\sigma} = f_k(z); \text{ isto é, } v = (z-a)^{\sigma}f_k(z) = g_k(z).$$

Além disso, como $\hat{\Delta} \subset \Omega_p \subset \Omega_q$, por (2.2.2') e pelo Lema 2.2.2 (aplicado a Q) segue que (g, B) é prolongável em Ω_q e portanto

em $\Delta(a, r)$. Logo, como $q_m(a) \neq 0$ e como ao polinômio Q e a o e. f. (g, B) pode aplicar-se tudo o estabelecido no primeiro caso, achamos para este e. f. o seguinte desenvolvimento

$$(Z-a)^{\sigma}F(Z) \equiv \sum_{n=0}^{\infty} b_n [(Z-a)^{1/h}]^n, \quad b_n \in \mathbb{C}, \text{ em } \hat{\Delta};$$

logo,

$$F(Z) \equiv \sum_{n=-\sigma h}^{\infty} b_{n+\sigma} [(Z-a)^{1/h}]^n \text{ em } \hat{\Delta}.$$

Assim, o lema está provado. ■

Finalmente, o Teorema A segue imediatamente aplicando este último lema a cada fator irredutível de P , em $\mathbb{C}(Z)[W]$.

2.3 - SÉRIE FORMAL DE POTÊNCIAS E PROPRIEDADES

Dado um anel de integridade A indicaremos por

$$A[[Z]] = \left\{ \sum_{n \in \mathbb{N}} a_n Z^n : a_n \in A \right\}.$$

A cada elemento deste conjunto chamaremos uma *série formal de potências* em A . Com as operações usuais $A[[Z]]$ é também um anel de integridade e $A[Z] \subset A[[Z]]$.

LEMA 2.3.1 - Seja $\sum a_n Z^n$ uma série formal de potências em $\mathbb{C}$, com raio de convergência $\rho > 0$ tal que não tem todos os seus coeficientes reais. Então, existe $R \in]0, \rho[$ tal que $\sum a_n x^n \in \mathbb{C} \setminus \mathbb{R}$

para todo $x \in \mathbb{R}$, com $0 < |x| < R$.

PROVA - Consideremos a função f dado por

$$f(z) = \sum_{n \geq 0} a_n z^n, \quad |z| < \rho.$$

Se $I = \{n \in \mathbb{N} : a_n \in \mathbb{C} \setminus \mathbb{R}\}$ e $\tilde{I} = \mathbb{N} \setminus I$ então, suponhamos que $a_n = b_n + i c_n$, com $c_n \neq 0$, para todo $n \in I$. Assim,

$$(2.3.1) \quad f(z) = \sum_{n \in \tilde{I}} a_n z^n + \sum_{n \in I} b_n z^n + i \sum_{n \in I} c_n z^n, \quad |z| < \rho.$$

Por hipótese $I \neq \emptyset$; logo, existe $k = \min I$. Seja g a função dada por

$$(2.3.2) \quad g(z) = \sum_{n \in I} c_n z^n, \quad |z| < \rho.$$

Então, como g é holomorfa em $\{z : |z| < \rho\}$, existe uma função holomorfa h numa vizinhança do ponto $z = 0$ tal que $g(z) = z^k h(z)$ e $h(0) \neq 0$. Logo, pela continuidade de h , existe $R \in]0, \rho[$ tal que $h(z) \neq 0$ para todo z , com $|z| < R$; donde

$$(2.3.3) \quad g(z) \neq 0, \quad \text{para } 0 < |z| < R.$$

Portanto, de (2.3.1), (2.3.2) e (2.3.3), segue que $f(x) \in \mathbb{C} \setminus \mathbb{R}$ para todo $x \in \mathbb{R}$, com $0 < |x| < R$. ■

LEMA 2.3.2 - Sejam $f_1, \dots, f_n$ séries formais de potências em $\mathbb{C}$

com todos os seus coeficientes reais e com raio de convergência maior que zero tais que $f_i \neq f_j$, para $i \neq j$ ($1 \leq i, j \leq n$). Então, existem um número real $R > 0$ e uma permutação $\sigma \in S_n$ (grupo de permutações de n elementos) tais que

$$f_{\sigma(1)}(x) < f_{\sigma(2)}(x) < \dots < f_{\sigma(n)}(x), \text{ para todo } x \in]0, R[.$$

PROVA - Por indução, basta provar para $n = 2$. Com efeito, seja $f = f_1 - f_2$ e seja $\rho > 0$ o seu raio de convergência. Suponhamos que

$$f(z) = \sum_{n \in \mathbb{N}} a_n z^n, \text{ para } |z| < \rho.$$

Então, é claro que, $a_n \in \mathbb{R}$, $n \in \mathbb{N}$. Se $k = \min\{n \in \mathbb{N} : a_n \neq 0\}$ então, como f é holomorfa em $\{z : |z| < \rho\}$, existe uma função holomorfa h numa vizinhança do ponto $z = 0$ tal que $f(z) = z^k h(z)$ e $h(0) \neq 0$. Logo, pela continuidade de h , existe $R \in]0, \rho[$ tal que $h(z) \neq 0$ para todo z , com $|z| < R$; donde, $f(x) \neq 0$ para todo $x \in \mathbb{R}$, com $0 < |x| < R$. Portanto, pelo Teorema do valor médio, verifica-se uma das seguintes condições

- 1) $f_1(x) < f_2(x)$, para todo $x \in]0, R[$
- 2) $f_2(x) < f_1(x)$, para todo $x \in]0, R[$,

o que, evidentemente, prova o lema. ■

2.4 - COMPORTAMENTO ASSINTÓTICO DOS CONJUNTOS SEMI-ALGÉBRICOS EM $\mathbb{R}^2$

Aqui será tratado em detalhe, usando o Teorema A, propriedades assintóticas importantes que nos servirão para estudar as aplicações do Teorema de Seidenberg-Tarski, no capítulo seguinte. Para este fim, se E é um subconjunto de $\mathbb{R}^2$ então, para cada $x \in \mathbb{R}$, denotaremos por E_x o conjunto

$$E_x = \{y \in \mathbb{R} : (x, y) \in E\}.$$

PROPOSIÇÃO 2.4.1 - Se E é semi-algêbrico elementar em $\mathbb{R}^2$ então, existe $M > 0$ tal que se verifica uma, e só uma, das seguintes condições:

- 1) $E_x = \emptyset$ para $x > M$
- 2) $E_x \neq \emptyset$ para $x > M$ e existe $(\alpha, \beta) \in \mathbb{Q} \times \mathbb{R}$ tal que

$$\sup E_x = \beta x^\alpha (1 + o(1)), \quad x \longrightarrow \infty$$

- 3) $E_x \neq \emptyset$ e $\sup E_x = \infty$, para $x > M$.

PROVA - Pela Definição 0.1.10 (3), existem $(r+s)$ polinômios P_i em $\mathbb{R}[X, Y]$, $1 \leq i \leq r+s$, $r \geq 0$, $s \geq 0$, tais que

$$E = \{(x, y) : P_i(x, y) = 0, 1 \leq i \leq r, \text{ e } P_j(x, y) > 0, r+1 \leq j \leq r+s\}.$$

Então, para todo $x \in \mathbb{R}$, é claro que

$$(2.4.1) \quad E_x = \{(x, y) : P_i(x, y) = 0, 1 \leq i \leq r\}_x \cap \{(x, y) : P_j(x, y) > 0, r+1 \leq j \leq r+s\}_x.$$

Expressando cada P_i , $1 \leq i \leq r+s$, sob a forma

$$P_i(X,Y) = \sum_{j=0}^{m_i} p_{ij}(X)Y^j, \quad m_i \in \mathbb{N},$$

onde $p_{ij} \in \mathbb{R}[X]$ e $p_i = p_{im_i} \neq 0$, seja N o conjunto dado por

$$N = \bigcup_{i=1}^{r+s} \bigcup_{j=0}^{m_i} \{x \in \mathbb{R} : p_{ij}(x) = 0\}$$

Então, $0 \leq |N| < \infty$ e escolhendo $M_0 > \sup N$ tem-se

$$(2.4.2) \quad p_{ij}(x) \neq 0, \text{ para } x > M_0, \quad 0 \leq j \leq m_i, \quad 1 \leq i \leq r+s.$$

Para cada polinômio P_i , $1 \leq i \leq r+s$, pelo Teorema A, existem $\rho_i > 0$, m_i e.f. $(f_{ij}, \hat{\Delta}(\infty, \rho_i))$ e números naturais correspondentes $h_{ij} \in \{1, \dots, m_i\}$, $1 \leq j \leq m_i$, tais que

$$(2.4.3) \quad f_{ij}(Z) \equiv \sum_{k=n_{ij}}^{\infty} a_{ijk} [Z^{-1/h_{ij}}]^k \text{ em } \hat{\Delta}(\infty, \rho_i),$$

onde $n_{ij} \in \mathbb{Z}$, $a_{ijk} \in \mathbb{C}$ e $a_{ijn_{ij}} \neq 0$; além disso,

$$(2.4.4) \quad P_i(z,W) = p_i(z) \prod_{j=1}^{m_i} [W - f_{ij}(z)], \text{ para todo } z \in \hat{\Delta}(\infty, \rho_i).$$

Se $\mathbb{F} = \{f_{ij} : 1 \leq j \leq m_i, 1 \leq i \leq r+s\}$ então denotemos por $\mathbb{F}_1$ e $\mathbb{F}_2$ respectivamente os conjuntos

$$\mathbb{F}_1 = \{f \in \mathbb{F} : f \text{ possui pelo menos um coeficiente não real}\}$$

$$\mathbb{F}_2 = \{f \in \mathbb{F} : \text{todos os coeficientes de } f \text{ são reais}\}$$

Então, é claro que, $\mathbb{F}_1 \cap \mathbb{F}_2 = \emptyset$ e $\mathbb{F} = \mathbb{F}_1 \cup \mathbb{F}_2$. Além disso, por (2.4.3) (usando o Lema 2.3.1), podemos achar $M_1 \geq M_0$ tal que

$$(2.4.5) \quad f(x) \in \mathbb{C} \setminus \mathbb{R}, \text{ para todo } (x, f) \in]M_1, \infty[\times \mathbb{F}_1.$$

Suponhamos primeiro que $\mathbb{F}_2 = \emptyset$. Então $\mathbb{F}_1 = \mathbb{F}$ e afirmamos que

$$(2.4.6) \quad P_i(x, y) \neq 0, \text{ para todo } (x, y) \in]M_1, \infty[\times \mathbb{R}, 1 \leq i \leq r+s.$$

De fato, se existissem $i \in \{1, \dots, r+s\}$ e $(x_0, y_0) \in]M_1, \infty[\times \mathbb{R}$ tais que $P_i(x_0, y_0) = 0$ então, por (2.4.2) e (2.4.4), existe $j \in \{1, \dots, m_i\}$ tal que $y_0 = f_{ij}(x_0)$; isto é, $f_{ij}(x_0) \in \mathbb{R}$ o que contra diz (2.4.5), pois $\mathbb{F}_1 = \mathbb{F}$. Portanto, vale (2.4.6). Agora pro varemos que $E_x = \emptyset$, para todo $x > M_1$ ou $E_x = \mathbb{R}$, para todo $x > M_1$. Com efeito, por (2.4.6), ocorre um, e só um, dos seguintes casos:

I) $r > 0$ ou existem $i \in \{1, \dots, r+s\}$ e $(x_0, y_0) \in]M_1, \infty[\times \mathbb{R}$ tais que $P_i(x_0, y_0) < 0$. Se $r > 0$ então, por (2.4.6), $\{(x, y) : P_i(x, y) = 0, 1 \leq i \leq r\}_x = \emptyset$ para todo $x > M_1$; logo por (2.4.1), $E_x = \emptyset$ para to do $x > M_1$. No segundo caso, por (2.4.6) (sendo $]M_1, \infty[\times \mathbb{R}$ cone xo), segue que $P_i(x, y) < 0$ para todo $(x, y) \in]M_1, \infty[\times \mathbb{R}$; isto é, $\{(x, y) : P_j(x, y) > 0, r+1 \leq k \leq r+s\}_x = \emptyset$ para todo $x > M_1$; logo, por (2.4.1), $E_x = \emptyset$ para todo $x > M_1$.

II) $r=0$ e para cada $j=1, \dots, s$ tem-se $P_j(x, y) > 0$ para to do (x, y) em $]M_1, \infty[\times \mathbb{R}$. Então, $E = \{(x, y) : P_j(x, y) > 0, 1 \leq j \leq s\}$; lo go, pela segunda condição, $E_x = \mathbb{R}$ para todo $x > M_1$. Assim, (I)

Implica (1) e (II) implica (3). Suponhamos agora que $\mathbb{F}_2 \neq \emptyset$ e que $\mathbb{F}_2$ possui n elementos distintos. Então, por (2.4.3) (usando o Lema 2.3.3), podemos achar $M > M_1$ e uma permutação destes elementos tais que

$$(2.4.7) \quad f_1(x) < f_2(x) < \dots < f_n(x), \text{ para todo } x \geq M.$$

Consideremos os seguintes subconjuntos de $\mathbb{R}^2$:

$$A_1 = \{(x, y) : x \geq M \text{ e } y < f_1(x)\}$$

$$A_k = \{(x, y) : x \geq M \text{ e } f_{k-1}(x) < y < f_k(x)\}, \quad 2 \leq k \leq n$$

$$A_{n+1} = \{(x, y) : x \geq M \text{ e } f_n(x) < y\}$$

$$B_k = \{(x, y) : x \geq M \text{ e } y = f_k(x)\}, \quad 1 \leq k \leq n.$$

Então, para cada $k=1, \dots, n+1$, afirmamos que

$$(2.4.8) \quad P_i(x, y) \neq 0, \text{ para todo } (x, y) \in A_k, \quad 1 \leq i \leq r+s.$$

Com efeito, seja $(x, y) \in A_k$. Então, como $A_k \cap B_j = \emptyset$, tem-se $y \neq f_j(x)$, $1 \leq j \leq n$. Além disso, por (2.4.5), $y \neq f(x)$ para todo $f \in \mathbb{F}_1$; logo, por (2.4.2) e (2.4.4), segue (2.4.8).

A seguir provaremos as seguintes propriedades:

$$4) \text{ Se } E \cap A_k \neq \emptyset, \quad 1 \leq k \leq n+1, \text{ então } A_k \subset E$$

$$5) \text{ Se } E \cap B_k \neq \emptyset, \quad 1 \leq k \leq n, \text{ então } B_k \subset E.$$

De fato, se $E \cap A_k \neq \emptyset$ então, por (2.4.8), $r = 0$; logo, $E = \{(x, y) : P_j(x, y) > 0, \quad 1 \leq j \leq s\}$. Seja $(x_0, y_0) \in E \cap A_k$. Então, ca

da $P_j(x_0, y_0) > 0$ e como A_k é conexo, por (2.4.8), segue que $P_j(x, y) > 0$ para todo $(x, y) \in A_k$, $1 \leq j \leq s$; isto é, $A_k \subset E$ o que prova (4). Agora seja $(a, b) \in E \cap B_k$. Então,

$$a \geq M, P_i(a, f_k(a)) = 0, 1 \leq i \leq r, \text{ e } P_j(a, f_k(a)) > 0, r+1 \leq j \leq r+s$$

De (2.4.2), (2.4.4) e do fato anterior tem-se $P_i(X, f_k(X)) \equiv 0$ em $[M, \infty[$; isto é

$$(2.4.9) \quad P_i \equiv 0 \text{ em } B_k, 1 \leq i \leq r.$$

De modo análogo, como $P_j(a, f_k(a)) = p_j(a) \prod_{v=1}^{m_j} [f_k(a) - f_{jv}(a)] > 0$, tem-se $f_k(a) \neq f_{jv}(a)$, $1 \leq v \leq m_j$; logo, por (2.4.5) e (2.4.7), segue que $P_j(x, f_k(x)) \neq 0$ para todo $x \geq M$ e como B_k é conexo

$$(2.4.10) \quad P_j(x, y) > 0, \text{ para todo } (x, y) \in B_k, r+1 \leq j \leq r+s.$$

Portanto, de (2.4.9) e (2.4.10), segue (5). Se $E \cap [M, \infty[\times \mathbb{R} = \emptyset$ então $E_x = \emptyset$ para todo $x > M$, o que implica (1). Suponhamos que $E \cap [M, \infty[\times \mathbb{R} \neq \emptyset$. Então, como $[M, \infty[\times \mathbb{R} = A_{n+1} \cup \bigcup_{k=1}^n (A_k \cup B_k)$, ocorre um, e só um, dos seguintes casos:

III) $E \cap A_{n+1} \neq \emptyset$. Então, por (4), $A_{n+1} \subset E$ e como valem $(A_{n+1})_x \subset E_x$ e $\text{Sup}(A_{n+1})_x = +\infty$ para todo $x > M$ tem-se $E_x \neq \emptyset$ e $\text{Sup } E_x = +\infty$ para todo $x > M$ o que implica (3).

IV) $E \cap A_{n+1} = \emptyset$. Então, é claro que, $E \cap \bigcup_{k=1}^n (A_k \cup B_k) \neq \emptyset$, $E_x \neq \emptyset$ e $\text{Sup } E_x < +\infty$ para todo $x > M$. Seja $k \in \{1, \dots, n\}$ o maior inteiro tal que $E \cap (A_k \cup B_k) \neq \emptyset$. Se $E \cap A_k \neq \emptyset$ então, por (4), $A_k \subset E$ e

portanto $(A_k)_x \subset E_x$ para todo $x > M$. Logo, do modo como foi escolhido o k segue imediatamente que $\text{Sup } E_x = f_k(x)$ para todo $x > M$. Mas f_k é da forma

$$f_k(X) \equiv \sum_{i=n_k}^{\infty} a_{i,k} [X^{-1/h_k}]^i \text{ em } [M, \infty[,$$

onde $n_k \in \mathbb{Z}$, $a_{i,k} \in \mathbb{R}$ e $a_{n_k,k} \neq 0$; portanto, f_k pode ser escrito sob a forma

$$f_k(X) \equiv b_0 \left(X^{-1/h_k} \right)^{n_k} \left[1 + b_1 \left(X^{-1/h_k} \right) + b_2 \left(X^{-1/h_k} \right)^2 + \dots \right] \text{ em } [M, \infty[, \quad b_0 \neq 0.$$

Se g é a função $x \in [M, \infty[\mapsto \sum_{i=1}^{\infty} b_i (x^{-1/h_k})^i$ então, é claro que, $\lim_{x \rightarrow \infty} g(x) = 0$ e portanto, escolhendo $\beta = b_0$ e $\alpha = -n_k h_k^{-1} \in \mathbb{Q}$ tem-se

$$\text{Sup } E_x = \beta x^{\alpha} (1 + g(x)), \text{ para todo } x > M;$$

o que implica (2). No caso em que $E \cap B_k \neq \emptyset$, por um processo análogo (usando (5)), obtem-se (2). ■

Observemos que se a condição (2) é satisfeita então, é imediato que, existe um polinômio P em $\mathbb{R}[X, Y]$ tal que $P(x, \text{Sup } E_x) = 0$ para todo $x > M$.

Da proposição anterior seguem imediatamente as seguintes proposições:

PROPOSIÇÃO 2.4.2 - Se E é semi-algêbrico em $\mathbb{R}^2$ então, existe $M > 0$ tal que se verifica uma, e só uma, das condições da Pro

proposição 2.4.1.

PROPOSIÇÃO 2.4.3 - Se E é semi-algêbrico em $\mathbb{R}^2$ então, existe $\delta > 0$ tal que se verifica uma, e só uma, das seguintes condições:

- 1) $E_x = \emptyset$ para $0 < x < \delta$.
- 2) $E_x \neq \emptyset$ para $0 < x < \delta$ e existe $(\alpha, \beta) \in \mathbb{Q} \times \mathbb{R}$ tal que

$$\sup E_x = \beta x^\alpha (1+o(1)), x \rightarrow 0, (x > 0)$$

- 3) $E_x \neq \emptyset$ e $\sup E_x = +\infty$, para todo $0 < x < \delta$.

De modo análogo, tem-se ainda as seguintes proposições:

PROPOSIÇÃO 2.4.4 - Se E é semi-algêbrico em $\mathbb{R}^2$ então, existe $M > 0$ tal que se verifica uma, e só uma, das seguintes condições:

- 1) $E_x = \emptyset$ para $x > M$.
- 2) $E_x \neq \emptyset$ para $x > M$ e existe $(\alpha, \beta) \in \mathbb{Q} \times \mathbb{R}$ tal que

$$\inf E_x = \beta x^\alpha (1+o(1)), x \rightarrow \infty.$$

- 3) $E_x \neq \emptyset$ e $\inf E_x = -\infty$ para $x > M$.

PROPOSIÇÃO 2.4.5 - Se E é semi-algêbrico em $\mathbb{R}^2$ então, existe $\delta > 0$ tal que se verifica uma, e só uma, das seguintes condições:

- 1) $E_x = \emptyset$ para $0 < x < \delta$.

2) $E_x \neq \emptyset$ para $0 < x < \delta$ e existe $(\alpha, \beta) \in \mathbb{Q} \times \mathbb{R}$ tal que

$$\inf E_x = \beta x^\alpha (1+o(1)), \quad x \rightarrow 0, \quad (x>0).$$

3) $E_x \neq \emptyset$ e $\inf E = -\infty$ para $0 < x < \delta$.

OBSERVAÇÃO 2.4.1 - Seja E um conjunto semi-algébrico em $\mathbb{R}^2$. Suponhamos que existe $M_0 \in \mathbb{R}$ tal que $E_x \neq \emptyset$ e $\inf E_x < \infty$ para todo $x > M_0$. Então, existe um polinômio P em $\mathbb{R}[X, Y]$ tal que

$$P(x, \inf E_x) = 0, \quad \text{para } x > M_0.$$

Este fato é um resultado imediato da Proposição 2.4.4 se $M_0 \geq M$ e em caso contrário a prova não é tão fácil. Como não a usaremos em nenhum resultado posterior, não nos preocupamos com a sua demonstração.

CAPÍTULO III

APLICAÇÕES DO TEOREMA DE SEIDENBERG-TARSKI

Seja P um polinômio em $\mathbb{C}[Z]$, na variável $Z = (Z_1, \dots, Z_n)$, de grau total $d > 0$. Denotaremos por N^k , $N_{\mathbb{R}}$, $N_{\mathbb{C}}$, respectivamente, os conjuntos

$$N^k = \{x \in \mathbb{R}^n : D^{\alpha} P(x) = 0, \forall \alpha \in \mathbb{N}^n, \text{ com } |\alpha| < k\}, \quad 1 \leq k \leq d+1$$

$$N^1 = N_{\mathbb{R}} = \{x \in \mathbb{R}^n : P(x) = 0\} \quad \text{e} \quad N_{\mathbb{C}} = \{z \in \mathbb{C}^n : P(z) = 0\}.$$

Como existe $\alpha_0 \in \mathbb{N}^n$, com $|\alpha_0| = d$, tal que $D^{\alpha_0} P(x) = a_{\alpha_0} \neq 0$ para todo $x \in \mathbb{R}^n$, é claro que $N^{d+1} = \emptyset$; logo chamando $N^0 = \mathbb{R}^n$, tem-se

$$\mathbb{R}^n = N^0 \supset N^1 \supset \dots \supset N^{d+1} = \emptyset.$$

Indicaremos por $d(x, N)$ a distância de um ponto $x \in \mathbb{R}^n$ a N ($N = N_{\mathbb{R}}$ ou $N_{\mathbb{C}}$); isto é, $d(x, N) = \inf_{y \in N} d(x, y)$. Observe-se que sendo N um subconjunto fechado não vazio (de $\mathbb{C}^n$), existe um ponto $y \in N$ tal que $d(x, N) = d(x, y)$. No presente capítulo, assim como no Capítulo V, serão mantidos os elementos

e as anotações considerados acima. Além disso, suporemos sempre $d(x, \emptyset) = 1$ para todo $x \in \mathbb{R}^n$.

3.1 - PROPRIEDADES ASSINTÓTICAS

Seja E um subconjunto de $\mathbb{R}^2$. Então, as seguintes observações são imediatas:

OBSERVAÇÃO 3.1.1 - Seja $\delta > 0$ tal que

- i) $E_x \neq \emptyset$ para $0 < x < \delta$.
- ii) existe $(\alpha, \beta) \in \mathbb{R} \times \mathbb{R}$ tal que

$$\sup E_x = \beta x^\alpha (1 + g(x)) > 0, \text{ para } 0 < x < \delta,$$

$$\text{onde } \lim_{x \rightarrow 0} g(x) = 0.$$

Então, $\beta > 0$. Se além disso, vale

$$\text{iii) } \limsup_{x \rightarrow 0} E_x = 0$$

Então, $\alpha > 0$.

OBSERVAÇÃO 3.1.2 - Valem as mesmas propriedades substituindo-se o Sup pelo Inf.

LEMA 3.1.1 - Existem constantes $b > 0$ e $c > 0$ tais que

$$(3.1.1) \quad |P(x)| \geq c d(x, N_{\mathbb{R}})^b, \text{ para } \|x\| \leq 1, x \in \mathbb{R}^n.$$

PROVA - Escrevendo $N = N_{\mathbb{R}}$ podemos supor que $N \neq \emptyset$, $N \neq \mathbb{R}^n$ e $N \cap B_1[0] \neq \emptyset$; onde $B_1[0]$ é a bola unitária fechada em $\mathbb{R}^n$. De

fato, se $N = \emptyset$ então $d(x, N) = 1$, $x \in \mathbb{R}^n$, e portanto existe $c_0 > 0$ tal que $|P(x)| \geq c_0$ para todo $x \in B_1[0]$; donde segue (3.1.1). Se $N = \mathbb{R}^n$ então o resultado é imediato. Se $N \cap B_1[0] = \emptyset$ então é claro que existe $c_1 > 0$ tal que $|P(x)| \geq c_1$ para todo $x \in B_1[0]$. Mas é fácil achar $c_2 > 0$ tal que $d(x, N) \leq c_2$ para todo $x \in B_1[0]$. Logo, segue imediatamente (3.1.1). Agora sejam A e D os subconjuntos de $\mathbb{R}^{n+1}$ dados por

$$A = \{(\rho, x) \in \mathbb{R} \times \mathbb{R}^n : \|x\| \leq 1 \text{ e } \rho > 0\}.$$

$$D = \{(\rho, x) : \|x\| \leq 1, \rho > 0 \text{ e } d(x, N) \geq \rho\}.$$

Então, A é semi-algêbrico em $\mathbb{R}^{n+1}$ e para provar que D é semi-algêbrico consideremos o conjunto

$$C = \{(\rho, x, y) \in \mathbb{R} \times \mathbb{R}^n \times \mathbb{R}^n : \|x\| \leq 1, \rho > 0, |P(y)|^2 = 0 \text{ e } \|x - y\|^2 < \rho^2\}$$

e a projeção $\pi: (\rho, x, y) \mapsto (\rho, x)$ de $\mathbb{R}^{2n+1}$ sobre $\mathbb{R}^{n+1}$. Então é claro que C é semi-algêbrico em $\mathbb{R}^{2n+1}$; logo pelo Teorema 1.3.2 $\pi(C)$ é semi-algêbrico em $\mathbb{R}^{n+1}$ e como

$$d(x, N) < \rho \iff \exists y \in \mathbb{R}^n : |P(y)| = 0 \text{ e } \|x - y\| < \rho$$

segue facilmente que $A \setminus D = \pi(C)$; donde, pelo Lema 0.1.16 (6), D é semi-algêbrico em $\mathbb{R}^{n+1}$. Para cada $\rho > 0$ seja $D_\rho = \{x \in \mathbb{R}^n : (x, y) \in D\}$. Então, como $N \neq \mathbb{R}^n$, existe $x_0 \in B_1(0)$ tal que $P(x_0) \neq 0$. Logo, se $\delta_0 = d(x_0, N) > 0$ e $\rho \in]0, \delta_0]$ então $x_0 \in D_\rho$; isto é, $D_\rho \neq \emptyset$ e além disso, $|P(x)| > 0$ para todo $x \in D_\rho$. Seja

f a função $x \in \mathbb{R}^n \mapsto d(x, N)$. Então, f é contínua e portanto cada $D_\rho = f^{-1}([\rho, \infty[) \cap B_1[0]$, $\rho \in]0, \delta_0]$, é um conjunto compacto; logo, considerando a função $\tau_\rho: \rho \in]0, \delta_0] \longrightarrow \min_{x \in D_\rho} |P(x)|^2$, conclui-se

$$(3.1.2) \quad \tau_\rho(\rho) > 0, \text{ para todo } \rho \in]0, \delta_0].$$

Além disso, afirmamos que

$$(3.1.3) \quad \lim_{\rho \rightarrow 0} \tau_\rho(\rho) = 0.$$

De fato, seja $x_1 \in N \cap B_1[0]$ (é não vazio por hipótese). Então, pela continuidade de $|P|$, para cada $\varepsilon > 0$ existe um $\delta_\varepsilon > 0$ tal que

$$\|x - x_1\| < \delta_\varepsilon \implies |P(x)|^2 < \varepsilon,$$

e como $N \neq \mathbb{R}^n$, é claro que, existe $x_2 \in B_1(0)$ tal que $x_2 \notin N$ e $\|x_1 - x_2\| < \delta_\varepsilon$ (donde, $|P(x_2)|^2 < \varepsilon$). Logo, se $\bar{\delta} = d(x_2, N) > 0$ e $\rho \in]0, \bar{\delta}[$ então $d(x_2, N) > \rho$; isto é, $x_2 \in D_\rho$. Mas $|P(x_2)|^2 < \varepsilon$ e portanto $\tau_\rho(\rho) \leq |P(x_2)|^2 < \varepsilon$, se $\rho \in]0, \bar{\delta}[$; donde, segue (3.1.3). Por outro lado, se E é a imagem de D sob a função polinomial $(\rho, x) \mapsto (\rho, |P(x)|^2)$ então, pelo Teorema 1.3.2, E é semi-algébrico em $\mathbb{R}^2$; além disso, é claro que

$$(3.1.4) \quad (\rho, \tau) \in E \iff \exists x \in \mathbb{R}^n: |P(x)|^2 = \tau \text{ e } x \in D_\rho.$$

Seja $\rho \in]0, \delta_0]$. Então, como D_ρ é compacto e a função $x \mapsto |P(x)|^2$ é contínua, existe um ponto $x_3 \in \mathbb{R}^n$ tal que

$x_3 \in D_\rho$ e $\tau_P(\rho) = |P(x_3)|^2$; logo, por (3.1.4), $\tau_P(\rho) \in E_\rho$ e portanto $E_\rho \neq \emptyset$ e $\inf E_\rho \leq \tau_P(\rho)$. Por outro lado, por (3.1.4), para cada $\tau \in E_\rho$ existe $x_4 \in \mathbb{R}^n$ tal que $x_4 \in D_\rho$ e $|P(x_4)|^2 = \tau$; logo, $\tau_P(\rho) \leq |P(x_4)|^2 = \tau$, $\tau \in E_\rho$, e portanto $\tau_P(\rho) \leq \inf E_\rho$. Em resumo

$$(3.1.5) \quad E_\rho \neq \emptyset \text{ e } \inf E_\rho = \tau_P(\rho), \text{ para todo } \rho \in]0, \delta_0];$$

donde, pela Proposição 2.4.5 e por (3.1.5), existe $0 < \delta_1 < \delta_0$ tal que

$$(3.1.6) \quad \inf E_\rho = \beta \rho^\alpha (1+g(\rho)), \text{ para } 0 < \rho < \delta_1,$$

onde $(\alpha, \beta) \in \mathbb{Q} \times \mathbb{R}$ e $\lim_{t \rightarrow 0} g(t) = 0$. Logo, por (3.1.2), (3.1.3), (3.1.5), (3.1.6) e pela Observação 3.1.2, segue que $\alpha > 0$ e $\beta > 0$. Seja $0 < \delta_2 < \delta_1$ tal que

$$(3.1.7) \quad 0 < \rho < \delta_2 \implies \frac{1}{2} < 1+g(\rho) < \frac{3}{2}.$$

Seja $x_0 \in B_1[0]$ fixado. De $0 < d(x_0, N) < \delta_2$ então, tomando $\rho = d(x_0, N)$, tem-se $x_0 \in D_\rho$; logo, por (3.1.5) e (3.1.6),

$$\beta \rho^\alpha (1+g(\rho)) = \inf E_\rho = \tau_P(\rho) = \min_{x \in D_\rho} |P(x)|^2 \leq |P(x_0)|^2$$

e portanto, por (3.1.7), segue facilmente que

$$|P(x_0)| \geq \left(\frac{\beta}{2}\right)^{1/2} d(x_0, N)^{\alpha/2}.$$

Se $\delta_2 \leq d(x_0, N)$ então $x_0 \in D_{\delta_2}$. Mas, é claro que, existe $C_3 > 0$ tal que $|P(x)| \geq C_3$ para todo $x \in D_{\delta_2}$. Logo é imediato que

$$|P(x_0)| \geq C_3 C_2^{-\alpha/2} d(x_0, N)^{\alpha/2}.$$

Finalmente, se $C = \min \left\{ \left(\frac{\beta}{2} \right)^{1/2}, C_3 C_2^{-\alpha/2} \right\}$ e $b = \frac{\alpha}{2}$ então, das desigualdades acima, segue (3.1.1). ■

COROLÁRIO 3.1.1 - Se $P(0) = 0$ e se $|P(x)| > 0$ para $0 < \|x\| \leq 1$ então, existem constantes $b > 0$ e $c > 0$ tais que

$$|P(x)| \geq c \|x\|^b, \text{ para } \|x\| \leq 1, x \in \mathbb{R}^n.$$

PROVA - Como $P(0) = 0$ e $N \cap \{x \in \mathbb{R}^n : 0 < \|x\| \leq 1\} = \emptyset$ ($N = N_{\mathbb{R}}$) não é difícil provar que $d(x, N) = \|x\|$ para $\|x\| \leq \frac{1}{2}$ e pelo lema existem $c_1 > 0$ e $b > 0$ tais que

$$|P(x)| \geq c_1 d(x, N)^b = c_1 \|x\|^b, \text{ para } \|x\| \leq 1/2.$$

Por outro lado, como $|P(x)| > 0$ para $\frac{1}{2} \leq \|x\| \leq 1$, existe $c_2 > 0$ tal que $|P(x)| \geq c_2$ para todo $\frac{1}{2} \leq \|x\| \leq 1$. Logo, é claro que

$$|P(x)| \geq c_2 \|x\|^b, \text{ para } \frac{1}{2} \leq \|x\| \leq 1.$$

Portanto, se $c = \max \{c_1, c_2\}$ então, das desigualdades acima, segue o Corolário. ■

LEMA 3.1.2 - $\lim_{\substack{\|x\| \rightarrow \infty \\ x \in \mathbb{R}^n}} d(x, N) = \infty$ se, e somente se, existe $(d^*, c) \in \mathbb{Q} \times]0, \infty[$,

$d^* > 0$, tal que

$$(3.1.8) \quad \|x\|^{1/d^*} \leq c[1+d(x,N)], \text{ para todo } x \in \mathbb{R}^n, N = N_{\mathbb{C}}.$$

PROVA - A condição suficiente é imediata. Para provar a condição necessária, seja A o conjunto dos pontos (ρ, τ, x, y, z) em $\mathbb{R} \times \mathbb{R} \times \mathbb{R}^n \times \mathbb{R}^n \times \mathbb{R}^n$ tais que

$$|P(x+iy)|^2 = 0, \tau > 0, \|x-z\|^2 + \|y\|^2 \leq \tau^{-2}, \rho > 0 \text{ e } \|z\|\rho = 1.$$

Então A é semi-algêbrico em $\mathbb{R}^{3n+2}$. Logo, se π_1 é a projeção $(\rho, \tau, x, y, z) \mapsto (\rho, \tau, z)$ de $\mathbb{R}^{3n+2}$ sobre $\mathbb{R}^{n+2}$ então, pelo Teorema 1.3.2, $B = \pi_1(A)$ é semi-algêbrico em $\mathbb{R}^{n+2}$ e como

$$d(z, N) \leq \tau^{-1} \iff \exists (x, y) \in \mathbb{R}^{2n}: P(x+iy) = 0 \text{ e } \|x-z\|^2 + \|y\|^2 \leq \tau^{-2}$$

é imediato que

$$(3.1.9) \quad (\rho, \tau, z) \in B \iff d(z, N) \leq \tau^{-1} \text{ e } \|z\|\rho = 1.$$

De modo análogo, considerando a projeção $\pi_2: (\rho, \tau, z) \mapsto (\rho, \tau)$, pelo Teorema 1.3.2, $E = \pi_2(B)$ é semi-algêbrico em $\mathbb{R}^2$ e além disso, por (3.1.9), é claro que

$$(3.1.10) \quad (\rho, \tau) \in E \iff \exists z \in \mathbb{R}^n: d(z, N) \leq \tau^{-1} \text{ e } \|z\|\rho = 1.$$

Como $\lim_{\|z\| \rightarrow \infty, z \in \mathbb{R}^n} d(z, N) = \infty$, podemos escolher um $\delta_1 > 0$ tal que

$$0 < \rho < \delta_1 \text{ e } \|z\|\rho = 1, z \in \mathbb{R}^n \implies d(z, N) \geq 1;$$

portanto, para cada $\rho \in]0, \delta_1[$, é fácil provar que a fun-

ção $\psi_\rho: z \in \{z \in \mathbb{R}^n: \|z\|_\rho=1\} \mapsto d(z,N)^{-1}$ é contínua. Logo, a função $\tau_\rho: \rho \in]0, \delta_1[\longrightarrow \sup_{\|z\|_\rho=1, z \in \mathbb{R}^n} \{d(z,N)^{-1}\}$ está bem definida e, pela hipótese, não é difícil ver que

$$(3.1.11) \quad \lim_{\rho \rightarrow 0} \tau_\rho(\rho) = 0 \quad \text{e} \quad \tau_\rho(\rho) > 0 \quad \text{para todo } \rho \in]0, \delta_1[.$$

Seja $\rho \in]0, \delta_1[$. Então, como o conjunto $\{z \in \mathbb{R}^n: \|z\|_\rho=1\}$ é compacto e a função ψ_ρ é contínua, existe um ponto $z_0 \in \mathbb{R}^n$ tal que $\|z_0\|_\rho=1$ e $\tau_\rho(\rho) = d(z_0, N)^{-1}$; logo, por (3.1.10), $\tau_\rho(\rho) \in E_\rho$ e portanto $E_\rho \neq \emptyset$ e $\tau_\rho(\rho) \leq \sup E_\rho$. Por outro lado, por (3.1.10), para cada $\tau \in E_\rho$ existe um ponto $z_1 \in \mathbb{R}^n$ tal que $d(z_1, N) \leq \tau^{-1}$ e $\|z_1\|_\rho=1$; logo, $\tau \leq d(z_1, N)^{-1} \leq \tau_\rho(\rho)$, $\tau \in E_\rho$, e portanto $\sup E_\rho \leq \tau_\rho(\rho)$. Assim temos provado

$$(3.1.12) \quad E_\rho \neq \emptyset \quad \text{e} \quad \sup E_\rho = \tau_\rho(\rho), \quad \text{para todo } \rho \in]0, \delta_1[.$$

Pela definição de τ_ρ , é imediato que

$$(3.1.13) \quad \frac{1}{\tau_\rho(\rho)} = \inf_{\|z\|_\rho=1, z \in \mathbb{R}^n} d(z, N), \quad \text{para todo } \rho \in]0, \delta_1[.$$

Sendo E semi-algêbrico em $\mathbb{R}^2$, Proposição 2.4.3 e por (3.1.12), existe $0 < \delta_2 < \delta_1$ tal que

$$(3.1.14) \quad \sup E_\rho = \beta \rho^\alpha (1+g(\rho)), \quad \text{para } 0 < \rho < \delta_2,$$

onde $(\beta, \alpha) \in \mathbb{Q} \times \mathbb{R}$ e $\lim_{t \rightarrow 0} g(t) = 0$. Logo, por (3.1.11), (3.1.12), (3.1.14) e pela Observação 3.1.1, segue que $\alpha > 0$ e $\beta > 0$. Se

ja $0 < \delta_0 < \delta_2$ tal que

$$(3.1.15) \quad 0 < \rho < \delta_0 \implies \frac{1}{2} < 1+g(\rho) < \frac{3}{2}.$$

Se $\rho \in]0, \delta_0[$ então, por (3.1.12) e (3.1.14), $\tau_P(\rho) = \beta \rho^\alpha (1+g(\rho))$ e portanto, por (3.1.15), $\frac{\beta}{2} \rho^\alpha < \tau_P(\rho) < \frac{3}{2} \beta \rho^\alpha$; logo, por (3.1.13), é imediato que $0 < d(z, N)^{-1} \leq \frac{3}{2} \beta \rho^\alpha$ para todo $z \in \mathbb{R}^n$, com $\|z\|_\rho = 1$. Isto é,

$$(3.1.16) \quad \left(\frac{1}{\rho}\right)^\alpha \leq \frac{3}{2} \beta d(z, N), \text{ para todo } z \in \mathbb{R}^n, \text{ com } \|z\|_\rho = 1, \rho \in]0, \delta_0[.$$

Seja $C = \max\{\delta_0^\alpha, \frac{3}{2}\beta\}$ e seja $z \in \mathbb{R}^n$. Se $\|z\| < \delta_0$, então $\|z\|^\alpha < \delta_0^\alpha \leq c[1+d(z, N)]$. Se $\|z\| \geq \delta_0$ então existe $\rho \in]0, \delta_0[$ tal que $\|z\|_\rho = 1$; logo por (3.1.16),

$$\|z\|^\alpha = \left(\frac{1}{\rho}\right)^\alpha \leq \frac{3}{2} \beta d(z, N) \leq \frac{3}{2} \beta [1+d(z, N)].$$

Portanto, escolhendo $d^* = \frac{1}{\alpha}$, segue (3.1.8). ■

LEMA 3.1.3 - Seja $\tau_P:]0, \infty[\longrightarrow \mathbb{R}$ a função dada por

$$\tau_P(\rho) = \min_{\|x\|=\rho} |P(x)|, \text{ para } \rho > 0$$

Então, existe $(\alpha, \beta) \in \mathbb{Q} \times [0, \infty[$ tal que

$$\tau_P(\rho) = \beta \rho^\alpha (1+o(1)), \rho \longrightarrow \infty.$$

PROVA - Seja A o conjunto dos pontos $(\rho, \tau, x) \in \mathbb{R} \times \mathbb{R} \times \mathbb{R}^n$ tais que

$$|P(x)|^2 = \tau^2, \|x\|^2 = \rho^2, \tau \geq 0, \rho \geq 0.$$

Então, A é semi-algêbrico em $\mathbb{R}^{n+2}$ e considerando a projeção $\pi: (\rho, \tau, x) \mapsto (\rho, x)$, pelo Teorema 1.3.2, $E = \pi(A)$ é semi-algêbrico em $\mathbb{R}^2$; além disso, é imediato que

$$(3.1.17) \quad (\rho, \tau) \in E \iff x \in \mathbb{R}^n: |P(x)| = \tau \text{ e } \|x\| = \rho.$$

Seja $\rho > 0$. Então, como o conjunto $\{x \in \mathbb{R}^n, \|x\| = \rho\}$ é compacto e a função $x \mapsto |P(x)|$ é contínua, existe um ponto $x_0 \in \mathbb{R}^n$ tal que $\|x_0\| = \rho$ e $\tau_P(\rho) = |P(x_0)|$; logo, por (3.1.17), $\tau_P(\rho) \in E_\rho$ e assim $E_\rho \neq \emptyset$ e $\inf E_\rho \leq \tau_P(\rho)$. Além disso, por (3.1.17) para cada $\tau \in E_\rho$ existe $x_1 \in \mathbb{R}^n$ tal que $|P(x_1)| = \tau$ e $\|x_1\| = \rho$; logo, $\tau_P(\rho) \leq |P(x_1)| = \tau$, $\tau \in E_\rho$, e portanto $\tau_P(\rho) \leq \inf E_\rho$. Resumindo o que foi feito acima, tem-se

$$(3.1.18) \quad E_\rho \neq \emptyset \text{ e } \inf E_\rho = \tau_P(\rho), \text{ para todo } \rho > 0.$$

Logo, pela Proposição 2.4.4 e por (3.1.18), existe $M > 0$ tal que

$$(3.1.19) \quad \inf E_\rho = \beta \rho^\alpha (1+g(\rho)), \text{ para todo } \rho > M$$

onde $(\alpha, \beta) \in \mathbb{Q} \times \mathbb{R}$ e $\lim_{t \rightarrow 0} g(t) = 0$. Donde, por (3.1.18) e (3.1.19), $\tau_P(\rho) = \beta \rho^\alpha (1+g(\rho))$ para todo $\rho > M$ e portanto $\beta \geq 0$ pois $\tau_P(\rho) \geq 0$ para todo $\rho > 0$. Isto prova o lema. ■

Uma consequência imediata deste lema e da Observa-

ção 2.4.1 é a seguinte

OBSERVAÇÃO 3.1.1 - Existe um polinômio Q em $\mathbb{R}[X,Y]$ tal que $Q(x, \tau_P(x)) = 0$ para todo $x > 0$.

COROLÁRIO 3.1.2 - Se existe $\delta_0 > 0$ tal que $P(x) \neq 0$ para $\|x\| > \delta_0$ então existem $a \in \mathbb{Q}$, $c > 0$ e $\delta_1 > 0$ tais que

$$\|x\| > \delta_1 \implies |P(x)| > c\|x\|^a.$$

PROVA - Seja $\delta_1 > \max\{M, \delta_0\} > 0$ tal que

$$(3.1.20) \quad \rho > \delta_1 \implies \frac{1}{2} < 1+g(\rho) < \frac{3}{2}.$$

Seja $x \in \mathbb{R}^n$ tal que $\|x\| > \delta_1$. Então, tomando-se $\rho = \|x\|$, pela definição de τ_P tem-se $\tau_P(\|x\|) = \beta\|x\|^\alpha(1+g(\|x\|))$ e portanto por (3.120), $\beta > 0$ (pois, por hipótese, $\tau_P(\|x\|) = \min_{\|y\|=\|x\|>\delta_0} |P(y)| > 0$); além disso,

$$|P(x)| \geq \tau_P(\|x\|) = \beta\|x\|^\alpha(1+g(\|x\|)) > \frac{\beta}{2} \|x\|^\alpha,$$

o que prova o Corolário. ■

3.2 - LEMAS ALGÉBRICOS

LEMA 3.2.1 - Existem constantes $a > 0$, $b > 0$ e $c > 0$, tais que

$$(3.2.1) \quad |P(x)| \geq c(1+\|x\|^2)^{-a} d(x, N)^b, \text{ para todo } x \in \mathbb{R}^n, N = N_{\mathbb{R}}.$$

PROVA - Em virtude do Lema 3.1.1, resta estudar unicamente o caso $\|x\| > 1$. Para isso consideremos a função $x \in \mathbb{R}^n \mapsto x^* = x\|x\|^{-2}$, $x \neq 0$. Então, $x = x^*\|x^*\|^{-2}$ e ($\|x\| \geq 1$ se, e só se, $\|x^*\| \leq 1$, $x^* \neq 0$). Seja P^* o polinômio em $\mathbb{C}[Z^*]$ dado por

$$P^*(Z^*) = \|Z^*\|^{2d} P(Z^*\|Z^*\|^{-2}), \quad d = \partial P,$$

e seja $N^* = \{x \in \mathbb{R}^n : P^*(x) = 0\}$. Então, pelo Lema 3.1.1 (aplicado a P^*), existem $b^* > 0$ e $c^* > 0$ satisfazendo (3.1.1); donde, pela definição de P^*

$$(3.2.2) \quad |P(x)| \geq \|x\|^{2d} c^* d(x^*, N^*)^{b^*}, \quad \text{para } \|x\| \geq 1.$$

Para cada $x, y \in \mathbb{R}^n$, com $xy \neq 0$, é fácil ver que

$$(3.2.3) \quad \frac{\|x - y\|}{\|x\| \|y\|} \geq \frac{d(x, N)}{2\|x\|^2}, \quad \text{se } y \in N \quad \text{e} \quad \|y\| \leq 2\|x\|$$

$$(3.2.4) \quad \frac{\|x - y\|}{\|x\| \|y\|} \geq \frac{1}{2\|x\|}, \quad \text{se } \|y\| > \|x\|.$$

Seja $x_0 \in \mathbb{R}^n$, com $\|x_0\| \geq 1$, fixado. Suponhamos primeiro que $N \neq \emptyset$. Então, é claro que, existe $C_0 > 0$ tal que

$$(3.2.5) \quad d(x, N) \leq C_0 \|x\|, \quad \text{para } \|x\| \geq 1.$$

Seja $y \in N$ tal que $y \neq 0$. Se $\|y\| \leq 2\|x_0\|$ então por (3.2.3)

$$(3.2.6) \quad d(x_0, N) \leq 2 \frac{\|x_0 - y\|}{\|x_0\| \|y\|} \|x_0\|^2.$$

Se $\|y\| > 2\|x_0\|$ então, por (3.2.4) e (3.2.5)

$$(2.3.7) \quad d(x_0, N) \leq C_0 \|x_0\| \leq 2C_0 \frac{\|x_0 - y\|}{\|x_0\| \|y\|} \|x_0\|^2.$$

Assim, por (3.2.6) e (3.2.7), conclui-se que

$$(2.3.8) \quad d(x_0, N) \leq 2(1+C_0) \frac{\|x_0 - y\|}{\|x_0\| \|y\|} \|x_0\|^2, \text{ para todo } y \in N, \text{ com } y \neq 0.$$

Se $C_1 = 2(1+C_0)$ então afirmamos que

$$(3.2.9) \quad d(x_0, N) \leq C_1 \|x_0\|^2 d(x_0^*, N^*).$$

Com efeito, seja $y \in \mathbb{R}^n$ tal que $y^* \in N^*$ e $\|x_0 - y^*\| = d(x_0^*, N^*)$.

Se $y^* = 0$ então $d(x_0^*, N^*) = \|x_0^*\| = \|x_0\|^{-1}$, donde

$$d(x_0, N) \leq C_0 \|x_0\| = C_0 \|x_0\|^2 d(x_0^*, N^*) \leq C_1 \|x_0\|^2 d(x_0^*, N^*)$$

Se $y^* \neq 0$, então, com $y^* \in N^*$, é fácil ver que $y \in N$, $y \neq 0$ e

$$\|x_0^* - y^*\|^2 = \|x_0^*\|^2 + \|y^*\|^2 - 2\langle x_0^*, y^* \rangle = \frac{\|x_0\|^2 + \|y\|^2 - 2\langle x_0, y \rangle}{\|x_0\|^2 \|y\|^2}$$

donde segue imediatamente que

$$d(x_0^*, N^*) = \|x_0^* - y^*\| = \frac{\|x_0 - y\|}{\|x_0\| \|y\|}$$

e portanto, relacionando esta igualdade com (3.2.8), segue (3.2.9). Por outro lado, de (3.2.2) e (3.2.9), segue facil-

mente que

$$|P(x_0)| \geq C_2 \|x_0\|^{2(d-b^*)} d(x_0, N)^{b^*}, \quad C_2 = C^* C_1^{-b^*};$$

mas $\|x_0\|^{2b^*} \leq (1+\|x_0\|^2)^{b^*}$ e $\|x_0\|^{2d} \geq 1$ (pois $\|x_0\| \geq 1$) e portanto $|P(x_0)| \geq C_2 (1+\|x_0\|^2)^{-b^*} d(x_0, N)^{b^*}$.

Agora se $N = \emptyset$ então, pela convenção, $d(x_0, N) = 1$ e

$$N^* = \{x \in \mathbb{R}^n : P^*(x) = 0\} = \{x \in \mathbb{R}^n \setminus \{0\} : \|x\|^{2d} P^*(x^*) = 0\} \cup \{0\} = \emptyset \cup \{0\} = \{0\};$$

logo, $d(x_0^*, N^*) = d(x_0^*, 0) = \|x_0^*\| = \|x_0\|^{-1}$ e portanto, por (3.2.2), obtém-se $|P(x_0)| \geq C^* \|x_0\|^{2d} (\|x_0\|^{-1})^{b^*}$. Mas, $1 + \|x_0\|^2 \geq 2\|x_0\|$, donde segue

$$|P(x_0)| \geq C_3 (1+\|x_0\|^2)^{-b^*}, \quad C_3 = C^* 2^{b^*},$$

e assim o lema está provado (note que $a = b = b^*$). $\blacksquare$

LEMA 3.2.2 - Seja $(k, m) \in \{0, 1, \dots, d\} \times \mathbb{N}$, $m \geq 1$. Então existem constantes $a = a(k, m) > 0$, b_j , $1 \leq j \leq m+1$ e $C = C(k, m) > 0$ tais que para todo $j \in \{1, \dots, m+1\}$ tem-se

$$(3.2.10) \quad \left[\sum_{|\beta| \leq jk} |D^\beta P^j(x)|^2 \right]^{1/2} \geq C (1+\|x\|^2)^{-a} d(x, N^{k+1})^{b_j}, \text{ para todo } x \in N^k.$$

PROVA - Para cada $j \in \{1, \dots, m+1\}$, fixo, seja P_j o polinômio em $\mathbb{C}[Z]$ dado por

$$P_j = \sum_{|\beta| \leq jk} |D^\beta P^j|^2.$$

Então, afirmamos que

$$(3.2.11) \quad (D^{\beta} P^j)(x) = 0 \text{ para todo } (x, \beta) \in \mathbb{N}^k \times \mathbb{N}^n, \text{ com } |\beta| < jk \text{ e } k \neq 0.$$

A prova será por indução finita sobre j . De fato, se $j=1$ então, pela definição de N^k , vale (3.2.11). Suponhamos que vale (3.2.11) para todo $\ell \leq j-1$. Seja $\beta \in \mathbb{N}^n$ tal que $|\beta| < jk$. Então, pela fórmula de Leibnitz

$$(3.2.12) \quad D^{\beta} P^j = \sum_{\gamma+\lambda=\beta, |\lambda|<k} \binom{\beta}{\gamma} (D^{\gamma} P^{j-1}) D^{\lambda} P + \sum_{\gamma+\lambda=\beta, |\lambda|\geq k} \binom{\beta}{\gamma} (D^{\gamma} P^{j-1}) D^{\lambda} P.$$

Notemos que se $|\lambda| < k$ então, pela hipótese de indução, $D^{\lambda} P(x) = 0$ para todo $x \in N^k$; logo, $\sum_{\gamma+\lambda=\beta, |\lambda|<k} \binom{\beta}{\gamma} (D^{\gamma} P^{j-1}(x)) D^{\lambda} P(x) = 0$ para todo $x \in N^k$. Se $|\lambda| \geq k$ então (em 3.2.12)) $|\gamma| < (j-1)k$, pois se $|\gamma| \geq (j-1)k$ teria-se $|\beta| = |\gamma+\lambda| \geq (j-1)k+k = jk$ o que contradiz $|\beta| < jk$; logo pela hipótese de indução, $D^{\gamma} P^{j-1}(x) = 0$, $x \in N^k$, e portanto $\sum_{\gamma+\lambda=\beta, |\lambda|\geq k} \binom{\beta}{\gamma} (D^{\gamma} P^{j-1}(x)) D^{\lambda} P(x) = 0$ para todo $x \in N^k$. Assim, por (3.2.12), $D^{\beta} P^j(x) = 0$ para todo $x \in N^k$, o que prova (3.2.11); donde segue que

$$(3.2.13) \quad P_j(x) = \sum_{|\beta|=jk} |D^{\beta} P^j(x)|^2, \text{ para todo } x \in N^k.$$

No caso em que $k=0$, (3.2.13) é imediato. Além disso, por um argumento similar ao feito acima, prova-se que

$$(3.2.14) \quad N^{k+1} = \{x \in \mathbb{R}^n : P_j(x) = 0\}.$$

Por outro lado, pelo Lema 3.2.1 (aplicado a P_j), existem $a_j > 0$, $b_j > 0$ e $c_j > 0$ satisfazendo (3.2.1) (onde $N_{\mathbb{R}} = N^{k+1}$, por (3.2.14)). Finalmente, escolhendo

$$(3.2.15) \quad a = \max_{1 \leq j \leq m+1} \{a_j\}, \quad b = \max_{1 \leq j \leq m+1} \{b_j\}, \quad C = \max_{1 \leq j \leq m+1} \{c_j\},$$

de (3.2.1), (3.2.13) e (3.2.15), segue facilmente (3.2.10).

Antes de terminar o capítulo ressaltamos que a escolha de a , b e C em (3.2.15) será usada posteriormente nas seções 2 e 3 do Capítulo V.

CAPÍTULO IV

HIPOELIPTICIDADE

Neste capítulo daremos uma descrição completa (condição necessária e suficiente) do conjunto dos operadores diferenciais parciais lineares (ODPL, com coeficientes constantes) $P(D)$ tais que as soluções T da equação

$$P(D)T = f$$

são sempre de classe C^∞ quando f é de classe C^∞ .

4.1 - PRELIMINARES

Seja $P(D)$ um ODPL dado na forma

$$P(D) = \sum_{|\alpha| \leq m} a_\alpha D^\alpha, \quad a_\alpha \in \mathbb{C}, \quad m \in \mathbb{N}^*,$$

Indicaremos por $P(Z)$ o seu polinômio associado:

$$P(Z) = \sum_{|\alpha| \leq m} a_\alpha Z^\alpha.$$

Além disso, usaremos as seguintes notações

$$N = \{z \in \mathbb{C}^n: P(z) = 0\}$$

$$d(x, N) = \inf_{y \in N} d(x, y), \quad x \in \mathbb{R}^n.$$

Como a ordem de $P(D)$ é m

$$(4.1.0) \quad \exists \lambda \in \mathbb{N}^n: |\lambda| = m \text{ e } D^\lambda P(x) = a_\lambda \neq 0, \quad \forall x \in \mathbb{R}^n.$$

DEFINIÇÃO 4.1.1 - Seja Ω um aberto não vazio de $\mathbb{R}^n$. Denotando por $K = K(\Omega)$ o conjunto de todos os compactos K contido em Ω , consideremos o espaço vetorial

$$L_{loc}^\infty(\Omega) = \{f: \Omega \longrightarrow \mathbb{C}: \text{Ess Sup}_{x \in K} |f(x)|, \quad \forall K \in K\},$$

sendo que identificamos duas funções mensuráveis que só diferem num conjunto de medida nula. Consideremos a topologia sobre este espaço como sendo a definida pelas seminormas

$$p_K: \phi \in L_{loc}^\infty(\Omega) \longmapsto \|\phi \chi_K\|_\infty, \quad K \in K,$$

onde χ_K é a função característica de K . Com esta topologia $L_{loc}^\infty(\Omega)$ é um espaço de Frechet, dado que Ω pode-se expressar como uma reunião enumerável de conjuntos compactos crescentes e $L_{loc}^\infty(\Omega)$ é completo (pois L^∞ é incompleto).

DEFINIÇÃO 4.1.2 - Diz-se que $P(D)$ é *hipoelíptico sobre $\mathbb{R}^n$* se para todo aberto não vazio Ω de $\mathbb{R}^n$ e para toda distribuição T so

bre Ω o fato de ser $P(D)T$ uma função de classe C^∞ em Ω implica que T é uma função de classe C^∞ em Ω .

LEMA 4.1.1 - Para cada m em $\mathbb{N}^*$ existe uma constante $C_m > 0$ tal que para todo polinômio não nulo P em $\mathbb{C}[Z]$, com $\partial P \leq m$, tem-se

$$(4.1.1) \quad C_m^{-1} \leq d(x, N) \sum_{|\alpha| \neq 0} \left| \frac{D^\alpha P(x)}{P(x)} \right|^{1/|\alpha|} \leq C_m, \text{ para todo } x \in \mathbb{R}^n \text{ com } P(x) \neq 0.$$

PROVA - Seja $m \in \mathbb{N}^*$ e seja P um polinômio não nulo em $\mathbb{C}[Z]$, com $\partial P \leq m$, fixados. Para cada $x_0 \in \mathbb{R}^n$, com $P(x_0) \neq 0$, fixo, denotemos por $F = F(x_0)$ o elemento

$$F = \sum_{|\alpha| \neq 0} \left| \frac{D^\alpha P(x_0)}{P(x_0)} \right|^{1/|\alpha|}.$$

Então, tem-se

$$(4.1.2) \quad |D^\alpha P(x_0)| \leq F^{|\alpha|} |P(x_0)|, \text{ para todo } \alpha \in \mathbb{N}^n \text{ com } |\alpha| \neq 0.$$

Por outro lado, pela fórmula de Taylor, vale

$$(4.1.3) \quad |P(x_0+z) - P(x_0)| \leq \sum_{1 \leq |\alpha| \leq m} |D^\alpha P(x_0)| \frac{\|z\|^{|\alpha|}}{\alpha!}, \text{ para todo } z \in \mathbb{C}^n.$$

Logo, por (4.1.2) e (4.1.3)

$$(4.1.4) \quad |P(x_0+z) - P(x_0)| \leq |P(x_0)| \sum_{1 \leq |\alpha| \leq m} \frac{\|Fz\|^{|\alpha|}}{\alpha!}, \text{ para todo } z \in \mathbb{C}^n.$$

Como $\lim_{t \rightarrow 0} e^t = 1$, existe $C > 0$ tal que $e^{C-1} < 1$; donde, se $F\|z\| \leq C$ então

$$\sum_{1 \leq |\alpha| \leq m} \frac{\|Fz\|^{|\alpha|}}{\alpha!} \leq \sum_{1 \leq |\alpha| \leq m} \frac{C^{|\alpha|}}{\alpha!} \leq e^{C-1} < 1;$$

logo, por (4.1.4), $|P(x_0+z) - P(x_0)| < |P(x_0)|$. Assim

$$(4.1.5) \quad P(x_0+z) \neq 0, \text{ para todo } z \in \mathbb{C}^n \text{ com } F\|z\| \leq C.$$

Afirmamos que $Fd(x_0, N) > C$. De fato, caso contrário, como N é fechado e não vazio, tem-se $F\|x_0 - y_0\| \leq C$ para algum $y_0 \in N$; logo, tomando $z_0 = y_0 - x_0$, de (4.1.5) segue que $P(y_0) = P(x_0 + z_0) \neq 0$; isto é, $y_0 \notin N$ o que contradiz a escolha de y_0 . Portanto, escolhendo $C_1 > 0$ tal que $C_1 > C^{-1}$ tem-se

$$(4.1.6) \quad C_1^{-1} \leq Fd(x_0, N),$$

onde C_1 não depende de x_0 nem de P . Por outro lado, para cada $z_0 \in \mathbb{C}^n$ com $2\|z_0\| \leq d(x_0, N)$, seja Q o polinômio em $\mathbb{C}[Y]$ dado por $Q(Y) = P(x_0 + z_0 Y)$. Então, $\partial Q \leq m$ e denotado por y_i , $1 \leq i \leq r$, $r \leq m$, todas as raízes de Q , como $(x_0 + z_0 y_i) \in N$, tem-se $d(x_0, N) \leq \|z_0 y_i\|$; logo

$$|y_i| \frac{d(x_0, N)}{2} \geq \|z_0 y_i\| \geq d(x_0, N)$$

e portanto (como $d(x_0, N) > 0$) $|y_i| \geq 2$ o que implica

$$\left| \frac{P(x_0 + z_0)}{P(x_0)} \right| = \left| \frac{Q(1)}{Q(0)} \right| = \prod_{i=1}^r \left(\frac{y_i - 1}{y_i} \right) = \prod_{i=1}^r \left(1 - \frac{1}{y_i} \right) \leq \left(\frac{3}{2} \right)^m$$

Logo,

$$(4.1.7) \quad \left| \frac{P(x_0 + z)}{P(x_0)} \right| \leq \left(\frac{3}{2} \right)^m, \text{ para todo } z \in \mathbb{C}^n \text{ com } 2\|z\| \leq d(x_0, N).$$

Seja $\Gamma = \{z \in \mathbb{C}^n : a\sqrt{n} \|z_j\| = d(x_0, N), 1 \leq j \leq n\}$. Então Γ é um subconjunto de $\{z \in \mathbb{C}^n : 2\|z\| \leq d(x_0, N)\}$ e como a função $f: z \mapsto P(x_0 + z)$ é holomorfa em $\mathbb{C}^n$, pela fórmula de Cauchy, tem-se

$$D^\alpha f(0) = \frac{\alpha!}{(2\pi i)^n} \int_{\Gamma} \frac{f(z)}{z^{\alpha+1}} dz, \quad \alpha = (1, 1, \dots, 1), \text{ para todo } \alpha \in \mathbb{N}^n;$$

logo, pela definição de f , segue que

$$(4.1.8) \quad D^\alpha P(x_0) = \frac{\alpha!}{(2\pi i)^n} \int_{\Gamma} \frac{P(x_0 + z)}{z_1^{\alpha_1+1} \dots z_n^{\alpha_n+1}} dz.$$

Portanto, de (4.1.7) e (4.1.8), obtêm-se

$$|D^\alpha P(x_0)| \leq \alpha! \left(\frac{3}{2} \right)^m |P(x_0)| d(x_0, N)^{-|\alpha|} (2\sqrt{n})^{|\alpha|}, \text{ para todo } \alpha \in \mathbb{N}^n;$$

donde,

$$(4.1.9) \quad d(x_0, N) \sum_{|\alpha| \neq 0} \left| \frac{D^\alpha P(x_0)}{P(x_0)} \right|^{1/|\alpha|} \leq \left(\frac{3}{2} \right)^m (2\sqrt{n}) \sum_{0 \neq |\alpha| \leq m} (\alpha!)^{1/|\alpha|} = C_2.$$

Finalmente, se $C_m = \max\{C_1, C_2\}$ então, de (4.1.6) e (4.1.9), segue (4.1.1). ■

LEMA 4.1.2 - São equivalentes as seguintes propriedades:

$$(HE_1) \quad \lim_{\substack{\|z\| \rightarrow \infty \\ z \in N}} \|Imz\| = \infty$$

$$(HE_2) \quad \lim_{\substack{\|x\| \rightarrow \infty \\ x \in \mathbb{R}^n}} d(x, N) = \infty$$

$$(HE_3) \quad \lim_{\substack{\|x\| \rightarrow \infty \\ x \in \mathbb{R}^n}} \frac{|D^\alpha P(x)|}{1 + |P(x)|} = 0, \text{ para todo } \alpha \in \mathbb{N}^n \text{ com } \alpha \neq 0.$$

PROVA - $(HE_1) \Rightarrow (HE_2)$: Se (HE_2) é falso então, existem $M > 0$ e $x_j \in \mathbb{R}^n$, $j \in \mathbb{N}$, tais que

$$(4.1.10) \quad \lim_{j \rightarrow \infty} \|x_j\| = 0 \text{ e } d(x_j, N) \leq M, \text{ para todo } j \in \mathbb{N}.$$

Seja $z_j \in N$ tal que $d(x_j, N) = d(x_j, z_j)$, isto é

$$(4.1.11) \quad d(x_j, N) = (\|x_j - \operatorname{Re} z_j\|^2 + \|\operatorname{Im} z_j\|^2)^{1/2}, \quad j \in \mathbb{N};$$

logo, por (4.1.10) e (4.1.11), $\lim_{j \rightarrow \infty} \|z_j\| = \infty$ e $\|\operatorname{Im} z_j\| \not\rightarrow \infty$ e portanto (HE_1) é falso.

$(HE_2) \Rightarrow (HE_1)$: Se (HE_1) é falso, existem $M > 0$ e $z_j \in N$, $j \in \mathbb{N}$, tais que $\lim_{j \rightarrow \infty} \|z_j\| = \infty$ e $\|\operatorname{Im} z_j\| \leq M$ para todo $j \in \mathbb{N}$. Se $x_j = \operatorname{Re} z_j$, $j \in \mathbb{N}$, então $\lim_{j \rightarrow \infty} \|x_j\| = \infty$ e como $d(x_j, N) \leq \|\operatorname{Im} z_j\| \leq M$ para todo $j \in \mathbb{N}$ segue que (HE_2) é falso.

$(HE_2) \Rightarrow (HE_3)$: Para cada $x \in \mathbb{R}^n$ com $P(x) \neq 0$, seja $F(x)$ como no Lema 4.1.1 e seja $\alpha \in \mathbb{N}^n$, $\alpha \neq 0$. Então, de (4.1.1) segue que

$$d(x, N) \left| \frac{D^\alpha P(x)}{P(x)} \right|^{1/|\alpha|} \leq F(x) d(x, N) \leq C_m, \text{ para todo } x \in \mathbb{R}^n \text{ com } P(x) \neq 0;$$

donde, segue facilmente que

$$\frac{|D^\alpha P(x)|}{1+|P(x)|} \leq \left(\frac{C_m}{d(x,N)} \right)^{|\alpha|}, \text{ para todo } x \in \mathbb{R}^n \text{ com } P(x) \neq 0,$$

e portanto, é claro que, (HE_2) implica (HE_3) .

$(HE_3) \Rightarrow (HE_2)$: De (4.1.0) e (HE_3) (tomando $\alpha = \lambda$) segue que

$\lim_{\|x\| \rightarrow \infty, x \in \mathbb{R}^n} |P(x)| = \infty$. Logo, existe $R > 0$ tal que $|P(x)| > 1$ para todo $x \in \mathbb{R}^n$ com $\|x\| > R$ e portanto

$$\|x\| > R, x \in \mathbb{R}^n \Rightarrow \left| \frac{D^\alpha P(x)}{P(x)} \right|^{1/|\alpha|} \leq \left(\frac{2|D^\alpha P(x)|}{1+|P(x)|} \right)^{1/|\alpha|}, \text{ para todo } \alpha \in \mathbb{N}^n, \alpha \neq 0;$$

isto é, $F(x) \leq G(x)$ para $\|x\| > R$, onde

$$G(x) = \sum_{|\alpha| \neq 0} \left(2 \frac{|D^\alpha P(x)|}{1+|P(x)|} \right)^{1/|\alpha|}.$$

É claro que (HE_3) implica que $\lim_{\|x\| \rightarrow \infty, x \in \mathbb{R}^n} G(x) = 0$. Logo,

$$(4.1.12) \quad \lim_{\substack{\|x\| \rightarrow \infty \\ x \in \mathbb{R}^n}} F(x) = 0.$$

De (4.1.1) e (4.1.12) segue (HE_2) ; pois $(C_m F(x))^{-1} \leq d(x,N)$ para todo $x \in \mathbb{R}^n$ com $P(x) \neq 0$. ■

DEFINIÇÃO 4.1.3 - Diz-se que $P(D)$ tem a propriedade (HE) se tem as propriedades equivalentes (HE_i) , $1 \leq i \leq 3$.

4.2 - AS PROPRIEDADES $(HE)_d$

Para cada d em $]0, \infty[$ consideremos as seguintes pro

priedades:

$(HE_1)_d$ existe uma constante $C_1 > 0$ tal que

$$\|z\|^a \leq C_1(1+\|Imz\|), \text{ para todo } z \in \mathbb{N}$$

$(HE_2)_d$ existe uma constante $C_2 > 0$ tal que

$$\|x\|^a \leq C_2[1+d(x,N)], \text{ para todo } x \in \mathbb{R}^n$$

$(HE_3)_d$ existe uma constante $C_3 > 0$ tal que

$$\|x\|^{|\alpha|a} |D^\alpha P(x)| \leq C_3(1+|P(x)|), \text{ para todo } (x,\alpha) \in \mathbb{R}^n \times \mathbb{N}^n,$$

onde $a = d^{-1}$.

LEMA 4.2.1 - Se $P(D)$ satisfaz $(HE_3)_d$ então $d \geq 1$.

PROVA - Em virtude do Lema 0.1.13 podemos supor que o polinômio P tem a forma

$$P(Z) = a_0 Z_1^m + \sum_{j=0}^{m-1} p_j Z_1^j, \quad a_0 \in \mathbb{C} \setminus \{0\},$$

onde $p_j \in \mathbb{C}[Z_2, \dots, Z_n]$ e $\partial p_j \leq m-j$. De $(HE_3)_d$ tem-se

$$(4.2.1) \quad |t|^a |P_{Z_1}(t, 0, \dots, 0)| \leq C_3(1+|P(t, 0, \dots, 0)|), \text{ para todo } t \in \mathbb{R}$$

onde P_{Z_1} denota a derivada parcial de P em relação a Z_1 . Logo, como o grau de P é m e o grau de P_{Z_1} é $(m-1)$, é claro que (4.2.1) só pode ocorrer se $d \geq 1$. ■

LEMA 4.2.2 - Se $P(D)$ satisfaz $(HE_3)_d$ então, para cada $\alpha \in \mathbb{N}^n$, existe $C_\alpha > 0$ tal que

$$(4.2.2) \quad (1+\|x\|^2)^{a|\alpha|} |D^\alpha P(x)|^2 \leq C_\alpha (1+|P(x)|^2), \text{ para todo } x \in \mathbb{R}^n,$$

e portanto

$$(4.2.3) \quad (1+\|x\|^2)^{r+a|\alpha|} |D^\alpha P(x)|^2 \leq C_\alpha (1+\|x\|^2)^r (1+|P(x)|^2),$$

para todo $(x,r) \in \mathbb{R}^n \times \mathbb{R}$.

PROVA - Seja $\alpha \in \mathbb{N}^n$, fixo. Então, de $(HE_3)_d$, segue que

$$\|x\|^{2|\alpha|a} |D^\alpha P(x)|^2 \leq C_3^2 (1+|P(x)|^2), \text{ para todo } x \in \mathbb{R}^n.$$

Mas, $(1+|P(x)|^2) \leq 2(1+\|x\|^2)$ para todo $x \in \mathbb{R}^n$; logo,

$$(4.2.4) \quad \|x\|^{2|\alpha|a} |D^\alpha P(x)|^2 \leq 2C_3^2 (1+\|x\|^2), \text{ para todo } x \in \mathbb{R}^n.$$

Seja $x_0 \in \mathbb{R}^n$ fixado. Se $\|x_0\| > 1$ então é claro que

$$(4.2.5) \quad (1+\|x_0\|^2)^{a|\alpha|} \leq (2\|x_0\|^2)^{2a|\alpha|}.$$

Assim, de (4.2.4) e (4.2.5), segue (4.2.2). Se $\|x_0\| \leq 1$ a desigualdade (4.2.2) é imediato, notando que a função $x \mapsto (1+\|x\|^2)^{a|\alpha|} |D^\alpha P(x)|^2 (1+|P(x)|^2)^{-1}$ é contínua e portanto limitada no compacto $\{x \in \mathbb{R}^n : \|x\| \leq 1\}$. ■

LEMA 4.2.3 - Seja $d > 0$ tal que $P(D)$ satisfaz $(HE_3)_d$. Se $TEH^r(\mathbb{R}^n)$ e $P(D)TEH^r(\mathbb{R}^n)$, $r \in \mathbb{R}$, então

$$1) \quad P^{(\alpha)}(D)TEH^{r+a|\alpha|}(\mathbb{R}^n), \text{ para todo } \alpha \in \mathbb{N}^n.$$

$$2) \quad TEH^{r+am}(\mathbb{R}^n).$$

PROVA - Seja $\alpha \in \mathbb{N}^n$. Então, pelo Lema 4.2.2, existe $C_\alpha > 0$ satisfazendo (4.2.3). Por outro lado, por hipótese, tem-se

$$\int_{\mathbb{R}^n} (1+\|X\|^2)^r |\hat{T}|^2 < \infty \quad \text{e} \quad \int_{\mathbb{R}^n} (1+\|X\|^2)^r |P|^2 |\hat{T}|^2 < \infty$$

e portanto

$$\int_{\mathbb{R}^n} (1+\|X\|^2)^r (1+|P|^2) |\hat{T}|^2 < \infty.$$

Logo, de (4.2.3), resulta que

$$\int_{\mathbb{R}^n} (1+\|X\|^2)^{r+a|\alpha|} |D^\alpha P|^2 |\hat{T}|^2 \leq C_\alpha \int_{\mathbb{R}^n} (1+\|X\|^2)^r (1+|P|^2) |\hat{T}|^2 < \infty;$$

isto é, $P^{(\alpha)}(D)T \in H^{r+a|\alpha|}(\mathbb{R}^n)$ o que prova (1). Finalmente, de (4.1.0) e 1) (para $\alpha=\lambda$) segue que $T \in H^{r+am}(\mathbb{R}^n)$. $\square$

LEMA 4.2.4 - As propriedades $(HE_2)_d$ e $(HE_3)_d$, $d > 0$, são equivalentes.

PROVA - $(HE_2)_d \implies (HE_3)_d$: De $(HE_2)_d$ tem-se

$$(4.2.6) \quad \|x\|^a \left| \frac{D^\alpha P(x)}{P(x)} \right|^{1/|\alpha|} \leq C_2 [1+d(x,N)] \left| \frac{D^\alpha P(x)}{P(x)} \right|^{1/|\alpha|},$$

para todo $(x,\alpha) \in \mathbb{R}^n \times \mathbb{N}^n$ com $|\alpha|P(x) \neq 0$.

Seja $x_0 \in \mathbb{R}^n$ fixado. Se $d(x_0, N) > 1$ então $P(x_0) \neq 0$; logo, por (4.1.1) e (4.2.6), tem-se

$$\|x_0\|^a \left| \frac{D^\alpha P(x_0)}{P(x_0)} \right|^{1/|\alpha|} \leq 2C_2 d(x_0, N) \left| \frac{D^\alpha P(x_0)}{P(x_0)} \right|^{1/|\alpha|} \leq 2C_2 C_m,$$

para todo $\alpha \in \mathbb{N}^n$ com $\alpha \neq 0$,

e portanto

$$\|x_0\|^{|\alpha|a} |D^\alpha P(x_0)| \leq (2C_2 C_m)^{|\alpha|} (1+|P(x_0)|), \text{ para todo } \alpha \in \mathbb{N}^n.$$

Se $d(x_0, N) \leq 1$ então, por $(HE_2)_d$, $\|x_0\| \leq (2C_2)^d$; logo, segue imediatamente $(HE_3)_d$, lembrando que, para cada $\alpha \in \mathbb{N}^n$, a função $x \mapsto \|x\|^{|\alpha|a} |D^\alpha P(x)| (1+|P(x)|)^{-1}$ é contínua e portanto limitada no compacto $\{x \in \mathbb{R}^n : \|x\| \leq (2C_2)^d\}$.

$(HE_3)_d \implies (HE_2)_d$: Seja $R = (2C_3 |a_\lambda|^{-1})^{d/m} > 0$, onde $a_\lambda \in \mathbb{C}$ e $\lambda \in \mathbb{N}^n$ são dados em (4.1.0). Seja $x_0 \in \mathbb{R}^n$ fixado. Se $\|x_0\| > R$, de $(HE_3)_d$ para $\alpha = \lambda$, tem-se

$$2C_3 < \|x_0\|^{|\lambda|a} |D^\lambda P(x_0)| \leq C_3 (1+|P(x_0)|);$$

logo $|P(x_0)| > 1$ e portanto $d(x_0, N) > 0$. Além disso, de $(HE_3)_d$, segue que

$$\|x_0\|^{|\alpha|a} |D^\alpha P(x_0)| \leq 2C_3 |P(x_0)|, \text{ para todo } \alpha \in \mathbb{N}^n,$$

o que implica

$$(4.2.7) \quad \|x_0\|^a \sum_{|\alpha| \neq 0} \left| \frac{D^\alpha P(x_0)}{P(x_0)} \right|^{1/|\alpha|} \leq \sum_{|\alpha| \neq 0} (2C_3)^{1/|\alpha|} = C_4.$$

Assim, de (4.1.1) e (4.2.7), segue que

$$\|x_0\|^a \leq C_4 C_m d(x_0, N) \leq C_4 C_m [1+d(x_0, N)].$$

Se $\|x_0\| \leq R$, o resultado é imediato notando que a função $x \mapsto \|x\|^a [1+d(x, N)]^{-1}$ é contínua e portanto limitada no com

pacto $\{x \in \mathbb{R}^n : \|x\| \leq R\}$. ■

Dos lemas 4.2.1 e 4.2.4 segue o seguinte

COROLÁRIO 4.2.1 - Se $P(D)$ satisfaz $(HE_2)_d$ então $d \geq 1$.

COROLÁRIO 4.2.2 - $P(D)$ satisfaz (HE_2) se, e somente se, existe $d \in \mathbb{Q}$, $d \geq 0$, tal que $P(D)$ satisfaz $(HE_2)_d$.

PROVA - Pelo Lema 3.1.2, $P(D)$ satisfaz (HE_2) se, e só se, existe $d \in \mathbb{Q}$, $d > 0$, tal que $P(D)$ satisfaz $(HE_2)_d$ e portanto, pelo Corolário 4.2.1, segue o resultado. ■

LEMA 4.2.5 - Sejam d e d_0 em $]0, \infty[$ tais que $d_0 \leq d$. Se $P(D)$ satisfaz $(HE_2)_{d_0}$ então $P(D)$ satisfaz $(HE_2)_d$.

PROVA - Seja $a_0 = d_0^{-1}$. Então, $a \leq a_0$; logo, $\|x\|^a \leq \|x\|^{a_0}$ para todo $\|x\| > 1$. Onde, pela definição de $(HE_2)_{d_0}$, $\|x\|^a \leq \|x\|^{a_0} \leq C_0(1+d(x,N))$, para todo $\|x\| \geq 1$. Por outro lado, como a função $x \in \mathbb{R}^n \mapsto \|x\|^a(1+d(x,N))^{-1}$ é contínua e portanto limitada no compacto $\{x \in \mathbb{R}^n : \|x\| \leq 1\}$, existe $C_1 > 0$ tal que $\|x\|^a \leq C_1(1+d(x,N))$, para todo $\|x\| \leq 1$. Se $C = \max\{C_0, C_1\}$, das desigualdades acima, segue $(HE_2)_d$. ■

LEMA 4.2.6 - Seja $d \geq 1$. Então, as propriedades $(HE_1)_d$ e $(HE_2)_d$ são equivalentes.

PROVA - $(HE_1)_d \implies (HE_2)_d$: Sejam $x \in \mathbb{R}^n$ e $z \in \mathbb{N}$ tais que $d(x,z) = d(x,N)$. Então, como $\|Imz\| \leq d(x,N)$ e $d(x,N) \leq [1+d(x,N)]^d$ (pois $d \leq 1$), a partir de $(HE_1)_d$ tem-se

$$\|x\| \leq \|z\| + \|x-z\| \leq C_1^d(1+\|Imz\|)^d + d(x,N) \leq C_1^d[1+d(x,N)]^d + [1+d(x,N)]^d;$$

donde segue $(HE_2)_d$.

$(HE_2)_d \implies (HE_1)_d$: Se $z \in N$, $Re z$ satisfaz $(HE_2)_d$ e como $d(Re z, N) \leq \|Imz\|$, tem-se

$$(4.2.8) \quad \|Re z\|^a \leq C_2(1+\|Imz\|).$$

Por outro lado, como $d \geq 1$, vale

$$(4.2.9) \quad \|Imz\|^a \leq 1+\|Imz\| \quad \text{e} \quad \|z\|^a \leq 2^a[\|Re z\|^a + \|Imz\|^a].$$

Portanto, de (4.2.8) e (4.2.9), segue $(HE_1)_d$. ■

Dos lemas (4.2.4) e (4.2.6) segue o

LEMA 4.2.7 - As propriedades $(HE_i)_d$, $d \geq 1$, $1 \leq i \leq 3$, são equivalentes.

DEFINIÇÃO 4.2.1 - Diz-se que $P(D)$ tem a propriedade $(HE)_d$, $d \geq 1$, se tem as propriedades equivalentes $(HE_i)_d$, $1 \leq i \leq 3$.

Do Corolário 4.2.2 e dos Lemas 4.1.2 e 4.2.7 segue o

TEOREMA 4.2.1 - $P(D)$ tem a propriedade (HE) se, e somente se, existe $d \in \mathbb{Q}$, $d \geq 1$, tal que $P(D)$ tem a propriedade $(HE)_d$.

4.3 - CONDIÇÃO NECESSÁRIA E SUFICIENTE DE HIPCELIPTICIDADE

LEMA 4.3.1 - Se para algum aberto não vazio Ω de $\mathbb{R}^n$, todas as

distribuições T sobre Ω soluções da equação $P(D)T=0$ são funções de classe C^∞ em Ω então $P(D)$ satisfaz (HE_1) .

PROVA - Seja

$$H_P(\Omega) = \{\phi \in L_{loc}^\infty(\Omega) : P(D)\phi=0\},$$

com a topologia induzida por $L_{loc}^\infty(\Omega)$ (vide a Definição 4.1.1). Então, por hipótese, $H_P(\Omega)$ é um subconjunto de $C^\infty(\Omega)$. Sejam $\phi_j \in H_P(\Omega)$, $j \in \mathbb{N}$, e $\phi \in L_{loc}^\infty(\Omega)$ tais que $\phi_j \longrightarrow \phi$ em $L_{loc}^\infty(\Omega)$. Então $\phi_j \longrightarrow \phi$ em $\mathcal{D}'(\Omega)$; logo, $P(D)\phi_j \longrightarrow P(D)\phi$ em $\mathcal{D}'(\Omega)$ e como $P(D)\phi_j = 0$ segue que $P(D)\phi = 0$; isto é, $\phi \in H_P(\Omega)$. Assim, $H_P(\Omega)$ é um subespaço fechado de $L_{loc}^\infty(\Omega)$. Portanto, $H_P(\Omega)$ é um espaço de Frechet.

Seja Ω_1 um aberto não vazio, qualquer, de $\mathbb{R}^n$ tal que $\Omega_1 \subset \subset \Omega$ (isto é, $\overline{\Omega_1}$ compacto e está contido em Ω). Denotando por $T|_{\Omega_1}$ a restrição sobre Ω_1 de $T \in \mathcal{D}'(\Omega)$, consideremos a aplicação linear

$$L_k : \phi \in H_P(\Omega) \longmapsto \frac{\partial \phi}{\partial x_k} \Big|_{\Omega_1} \in L^\infty(\Omega_1), \quad 1 \leq k \leq n.$$

Afirmamos que L_k é fechado. De fato, sejam ϕ, ϕ_j em $H_P(\Omega)$, $j \in \mathbb{N}$, tais que $\phi_j \longrightarrow \phi$ em $L_{loc}^\infty(\Omega)$ e $L_k \phi_j \longrightarrow \psi$ em $L^\infty(\Omega_1)$. Desejamos provar que $L_k \phi = \psi$. Da hipótese tem-se $\phi_j \longrightarrow \phi$ em $\mathcal{D}'(\Omega)$; logo, $\frac{\partial \phi_j}{\partial x_k} \longrightarrow \frac{\partial \phi}{\partial x_k}$ em $\mathcal{D}'(\Omega)$; donde,

$$L_k \phi_j = \left. \left(\frac{\partial \phi_j}{\partial x_k} \right) \right|_{\Omega_1} \longrightarrow \left. \left(\frac{\partial \phi}{\partial x_k} \right) \right|_{\Omega_1} = L_k \phi \text{ em } \mathcal{D}'(\Omega_1); \text{ isto é,}$$

$$(4.3.1) \quad L_k \phi_j \longrightarrow L_k \phi \text{ em } \mathcal{D}'(\Omega_1).$$

Mas, como $L_k \phi_j \longrightarrow \psi$ em $L^\infty(\Omega_1)$ e $L^\infty(\Omega_1)$ está continuamente imerso em $\mathcal{D}'(\Omega_1)$, tem-se

$$(4.3.2) \quad L_k \phi_j \longrightarrow \psi \text{ em } \mathcal{D}'(\Omega_1).$$

Assim, de (4.3.1) e (4.3.2), segue que $\psi = L_k \phi$.

Por outro lado, sendo $H_p(\Omega)$ um espaço de Frechet e $L^\infty(\Omega)$ um espaço de Banach, pelo Teorema do gráfico fechado L_k é contínua. Então, existem compactos $K_k \subset \Omega$ e constantes $C_k > 0$ tais que

$$(4.3.3) \quad \|L_k \phi\|_\infty^1 \leq C_k \|\phi\|_{K_k}, \text{ para todo } \phi \in H_p(\Omega), 1 \leq k \leq n,$$

onde $\|\cdot\|_\infty^1$ indica a norma de $L^\infty(\Omega_1)$. Considerando a função $\phi_z: x \in \mathbb{R}^n \longmapsto \exp[i\langle x, z \rangle]$, $z \in \mathbb{N}$, é claro que

$$(4.3.4) \quad \phi_z \in H_p(\Omega) \text{ e } \frac{\partial \phi_z}{\partial x_k} = i z_k \phi_z, z \in \mathbb{N}, 1 \leq k \leq n.$$

Escolhendo

$$J = \sup_{x \in K_1 \cup \dots \cup K_n} \|x\| \text{ e } J_1 = \sup_{x \in \Omega_1} \|x\|,$$

para cada $(k, z) \in \{1, \dots, n\} \times \mathbb{N}$, segue facilmente que

$$(4.3.5) \quad \|\phi_z X_{K_k}\|_\infty \leq \exp[\delta \|Imz\|] \quad \text{e} \quad \exp[-\delta_1 \|Imz\|] \leq \|\phi_z\|_\infty^1.$$

Como $\|L_k \phi_z\|_\infty^1 = |z_k| \|\phi_z\|_\infty^1$, de (4.3.3), (4.3.4) e (4.3.5), tem-se $|z_k| \leq C_k \exp[(\delta + \delta_1) \|Imz\|]$, para todo $(k, z) \in \{1, \dots, n\} \times \mathbb{N}$ e portanto $\lim_{\|z\| \rightarrow \infty, z \in \mathbb{N}} \|Imz\| = \infty$. $\blacksquare$

COROLÁRIO 4.3.1 - Nas hipóteses do lema, $P(D)$ tem a propriedade (HE).

PROVA - É consequência dos Lemas 4.1.2 e 4.3.1. $\blacksquare$

TEOREMA 4.3.1 - Sejam Ω um aberto não vazio de $\mathbb{R}^n$ e $s \in \mathbb{R}$. Suponhamos que $P(D)$ satisfaz $(HE_3)_d$, $d > 0$. Se $T \in \mathcal{D}'(\Omega)$ e $P(D)T \in H_{loc}^s(\Omega)$ então

$$P^{(\alpha)}(D)T \in H_{loc}^{s+|\alpha|}(\Omega), \text{ para todo } \alpha \in \mathbb{N}^n.$$

Em particular, de (4.1.0), $T \in H_{loc}^{s+am}(\Omega)$.

PROVA - Provaremos primeiro que para cada Ω_* aberto de $\mathbb{R}^n$ tal que $\Omega_* \subset \subset \Omega$ tem-se

- 1) $P^{(\alpha)}(D)(\phi T) \in H^s(\mathbb{R}^n)$, para todo $(\phi, \alpha) \in \mathcal{D}(\Omega_*) \times \mathbb{N}^n$, $\alpha \neq 0$.
- 2) $\phi T \in H^s(\mathbb{R}^n)$ para todo $\phi \in \mathcal{D}(\Omega_*)$.

De fato, sejam Ω_0 e Ω_1 abertos de $\mathbb{R}^n$ tais que

$$\Omega_* \subset \subset \Omega_1 \subset \subset \Omega_0 \subset \subset \Omega.$$

Então, pelo Teorema 0.3.5, existe $(\lambda, f) \in \mathbb{N} \times L^2(\Omega)$ tal que

$T|_{\Omega_0} = D^\lambda f$. Seja $\phi \in \mathcal{D}(\Omega_0)$ tal que $\phi \equiv 1$ em Ω_1 e seja $T_0 = D^\lambda(\phi f) \in \mathcal{D}'(\mathbb{R}^n)$. Então $T|_{\Omega_1} = T_0|_{\Omega_1} = (D^\lambda f)|_{\Omega_1} \in \mathcal{D}'(\Omega_1)$ e é claro que $\phi f \in L^2(\mathbb{R}^n) = H^0(\mathbb{R}^n)$, donde $T_0 \in H^{-n\lambda}$. Logo $D^\beta T_0 \in H^k(\mathbb{R}^n)$ para $0 < |\beta| \leq m$ e portanto $P(D)T_0 \in H^k(\mathbb{R}^n)$, $k = -m - n\lambda$; pois, como $-n\lambda \leq k$ resulta que

$$(4.3.6) \quad T_0 \in H^k(\mathbb{R}^n).$$

Logo, é claro que $P^{(\alpha)}(D)T_0 \in H^k(\mathbb{R}^n)$ para $|\alpha| \leq m$ e como $P^{(\alpha)}(D)T_0 = 0$ para $|\alpha| > m$ vem que

$$(4.3.7) \quad P^{(\alpha)}(D)T_0 \in H^k(\mathbb{R}^n), \text{ para todo } \alpha \in \mathbb{N}^n.$$

Seja $\phi_1 \in \mathcal{D}(\Omega_1)$ arbitrário. Então, por (4.3.6) e pelo Teorema 0.3.6, tem-se

$$(4.3.8) \quad T_1 = \phi_1 T_0 \in H^k(\mathbb{R}^n).$$

Por outro lado, pelo Teorema 0.3.4, vale

$$(4.3.9) \quad P(D)T_1 = \phi_1 P(D)T_0 + \sum_{|\alpha| > 0} \frac{1}{\alpha!} D^\alpha \phi_1 \cdot P^{(\alpha)}(D)T_0.$$

Como cada $D^\alpha \phi_1 \in \mathcal{D}(\Omega_1)$, $\alpha \in \mathbb{N}^n$, de (4.3.7) e do Teorema 0.3.6, segue que

$$(4.3.10) \quad P(D)T_1 \in H^k(\mathbb{R}^n).$$

De (4.3.8), (4.3.10) e do Lema 4.2.3 (para $r = k$) conclui-se

$$3) \quad P^{(\alpha)}(D)(\phi_1 T) = P^{(\alpha)}(D)T_1 \in H^{k+a}(\mathbb{R}^n), \text{ para } \alpha \in \mathbb{N}^n, \alpha \neq 0$$

$$4) \quad T_1 \in H^{k+a}(\mathbb{R}^n).$$

Se $k+a \geq s$, como $\phi_1 \in \mathcal{D}(\Omega_1)$ é arbitrário, de 3) e 4) segue imediatamente 1) e 2). Se $k+a < s$, seja Ω_2 um aberto de $\mathbb{R}^n$ tal que $\Omega_* \subset \subset \Omega_2 \subset \subset \Omega_1$. Seja $\phi_1 \in \mathcal{D}(\Omega_1)$ tal que $\phi_1 \equiv 1$ em Ω_2 e seja $T_1 = \phi_1 T_0$. Por hipótese $P(D)T_1 = P(D)T \in H_{loc}^s(\Omega)$ e portanto

$$\phi_2 P(D)T_1 \in H^s(\mathbb{R}^n) \subset H^{k+a}(\mathbb{R}^n), \quad \phi_2 \in \mathcal{D}(\Omega_2);$$

logo, de 3), usando como antes o Teorema 0.3.4 segue que

$$(4.3.11) \quad P(D)(\phi_2 T_1) \in H^{k+a}(\mathbb{R}^n), \quad (\phi_2 \in \mathcal{D}(\Omega_2)),$$

e, de 4), pelo Teorema 0.3.6 segue que

$$(4.3.12) \quad \phi_2 T_1 \in H^{k+a}(\mathbb{R}^n), \quad (\phi_2 \in \mathcal{D}(\Omega_2)).$$

Donde, de (4.3.11), (4.3.12) e do Lema 4.2.3, para todo

$(\phi_2, \alpha) \in \mathcal{D}(\Omega_2) \times \mathbb{N}^n$, $\alpha \neq 0$, tem-se

$$5) \quad P^{(\alpha)}(D)(\phi_2 T) = P^{(\alpha)}(D)(\phi_2 T_1) \in H^{k+2a}(\mathbb{R}^n).$$

$$6) \quad \phi_2 T_1 \in H^{k+2a}(\mathbb{R}^n).$$

Se $k+2a < s$, como existe $v \in \mathbb{N}$ tal que $k+va \geq s$, repetindo o mesmo argumento um número finito de vezes obtêm-se 1) e 2); pois, podemos construir v conjuntos abertos Ω_j ; $0 \leq j \leq v-1$, tais que

$$\Omega_* = \Omega_{V-1} \subset \dots \subset \Omega_0 \subset \Omega.$$

Agora, de 1) e 2), segue imediatamente

$$7) \ P^{(\alpha)}(D)(\phi T) \in H^S(\mathbb{R}^n), \text{ para } (\phi, \alpha) \in \mathcal{D}(\Omega) \times \mathbb{N}^n, \ \alpha \neq 0.$$

$$8) \ \phi T \in H^S(\mathbb{R}^n), \text{ para } \phi \in \mathcal{D}(\Omega).$$

De fato, dado $\phi \in \mathcal{D}(\Omega)$ basta considerar $\Omega_* = \Omega_\phi$, onde Ω_ϕ é uma vizinhança de $\text{Supp } \phi$ tal que $\Omega_\phi \subset \Omega$.

Por hipótese $\phi P(D)T \in H^S(\mathbb{R}^n)$, $\phi \in \mathcal{D}(\Omega)$; logo, por 7) e pelos Teoremas 0.3.4 e 0.3.6 vem que

$$9) \ P(D)(\phi T) \in H^S(\mathbb{R}^n), \text{ para todo } \phi \in \mathcal{D}(\Omega).$$

Portanto, de 8) e 9) e do Lema 4.2.3, obtém-se

$$10) \ P^{(\alpha)}(D)(\phi T) \in H^{S+|\alpha|}(\mathbb{R}^n), \text{ para } (\phi, \alpha) \in \mathcal{D}(\Omega) \times \mathbb{N}^n.$$

Finalmente, seja $\phi \in \mathcal{D}(\Omega)$ e seja Ω_ϕ como acima. Seja $\psi \in \mathcal{D}(\Omega)$ tal que $\psi \equiv 1$ em Ω_ϕ . Então é claro que

$$\phi P^{(\alpha)}(D)T = \phi P^{(\alpha)}(D)(\psi T), \quad (\alpha \in \mathbb{N}^n).$$

Mas, por 10) e pelo Teorema 0.3.6, tem-se

$$\phi P^{(\alpha)}(D)(\psi T) \in H^{S+|\alpha|}(\mathbb{R}^n)$$

e portanto $\phi P^{(\alpha)}(D)T \in H^{S+|\alpha|}(\mathbb{R}^n)$, como $\phi \in \mathcal{D}(\Omega)$ é arbitrário, pela Definição 0.3.5, segue o lema. ■

COROLÁRIO 4.3.2 - Se $P(D)$ satisfaz $(HE_3)_d$, $d > 0$, então $P(D)$ é hipoeelíptico sobre $\mathbb{R}^n$.

PROVA - Segue imediatamente do teorema lembrando que

$$C^\infty(\Omega) = \bigcap_{s \in \mathbb{R}} H_{loc}^s(\Omega). \quad \blacksquare$$

LEMA 4.3.2 - Se $P(D)$ tem a propriedade $(HE)_d$, $d \geq 1$, então $P(D)$ é hipoelíptico sobre $\mathbb{R}^n$.

PROVA - Segue do Lema 4.2.7 e do Corolário 4.3.2. $\blacksquare$

Dos resultados anteriores temos o seguinte

TEOREMA 4.3.2 - São equivalentes as seguintes propriedades:

- 1) $P(D)$ é hipoelíptico sobre $\mathbb{R}^n$.
- 2) existe um aberto não vazio Ω de $\mathbb{R}^n$ tal que se
 $P(D)T = 0$, $T \in \mathcal{D}'(\Omega)$, então $T \in C^\infty(\Omega)$.
- 3) $P(D)$ tem a propriedade (HE) .
- 4) existe $d \in \mathbb{Q}$, $d \geq 1$, tal que $P(D)$ tem a propriedade $(HE)_d$.

PROVA - 2) $\Rightarrow$ 3) (Corolário 4.3.1). 3) $\Leftrightarrow$ 4) (Teorema 4.2.1).

4) $\Rightarrow$ 1) (Lema 4.3.2). É claro que 1) $\Rightarrow$ 2). $\blacksquare$

OBSERVAÇÃO 4.3.1 - Existe $d_0 \in \mathbb{Q}$, $d_0 \geq 1$, tal que

$$\{d \geq 1: P(D) \text{ satisfaz } (HE_2)_d\} = [d_0, \infty[,$$

se $P(D)$ satisfaz as condições equivalentes do teorema. De fato, não é difícil provar usando o Lema 4.2.5.

CAPÍTULO V

DIVISÃO DE DISTRIBUIÇÕES POR POLINÔMIOS

Nosso propósito no presente capítulo é provar, usando o Teorema de Seidenberg-Tarski e o Teorema de extensão de Whitney, que a divisão de uma distribuição por um polinômio não identicamente nulo é sempre possível. Isso será feito de modo a se obter diretamente o resultado de mais utilidade: dado um polinômio não nulo P , a aplicação $T \mapsto PT$ do espaço das distribuições temperadas nele mesmo é sobrejetora. Usando a transformação de Fourier podemos afirmar que toda EDPL, com coeficientes constantes, $P(D)S = T$ tem uma solução temperada S para cada distribuição temperada T . Em particular, todo ODPL, $P(D)$, tem uma solução fundamental temperada.

5.1 - PRELIMINARES

DEFINIÇÃO 5.1.1 - Para cada $f \in C^m(\mathbb{R}^n)$, $m \geq 0$, definimos

$$f_m(x, y) = \sum_{|\beta| \leq m} (D^\beta f)(y) \frac{(x-y)^\beta}{\beta!}, \text{ para } x, y \in \mathbb{R}^n;$$

$$R(m, f, x, y) = f(x) - f_m(x, y), \text{ para } x, y \in \mathbb{R}^n,$$

onde $D^\beta = \left(\frac{\partial}{\partial x_1} \right)^\beta \dots \left(\frac{\partial}{\partial x_n} \right)^\beta$. Notemos que, para cada $y \in \mathbb{R}^n$, $f_m(x, y)$ é um polinômio de grau menor ou igual a m em relação a x .

OBSERVAÇÃO 5.1.0 - Da definição anterior é imediato que

$$(5.1.0) \quad (D^\alpha f)(x) = \sum_{|\beta| \leq m - |\alpha|} (D^{\alpha+\beta} f)(y) \cdot \frac{(x-y)^\beta}{\beta!} + D_x^\alpha R(m, f, x, y)$$

$$x, y \in \mathbb{R}^m, |\alpha| \leq m,$$

e portanto

$$(5.1.0^*) \quad D_x^\alpha R(m, f, x, y) = R(m - |\alpha|, D^\alpha f, x, y), \quad x, y \in \mathbb{R}^n, |\alpha| \leq m.$$

Em tudo o que se segue escrevemos $R_m(x, y)$ em lugar de $R(m, f, x, y)$, para simplificar a notação.

OBSERVAÇÃO 5.1.1 - Se K for um compacto, fixo, de $\mathbb{R}^n$ e se x e y forem elementos de K , então

$$|D_x^\alpha R_m(x, y)| \leq \|x-y\|^{m-|\alpha|} O(\|x-y\|), \text{ para } |\alpha| \leq m$$

onde $O(t) \rightarrow 0$ quando $t \rightarrow 0$. Com efeito, se $\alpha = 0$, este é um resultado conhecido e se $\alpha > 0$, isto resulta de (5.1.0*).

TEOREMA 5.1.1 (Fórmula de Taylor) - Seja Ω um aberto de $\mathbb{R}^n$ e seja $f \in C^m(\Omega)$. Então, para cada $(x, y) \in \Omega \times \Omega$ tal que

$$[x, y] = \{ty + (1-t)x : t \in [0, 1]\} \subset \Omega,$$

existe um ponto $z \in [x, y]$ tal que

$$(5.1.1) \quad f(x) = \sum_{|\beta| < m} (D^\beta f)(y) \frac{(x-y)^\beta}{\beta!} + \sum_{|\beta|=m} (D^\beta f)(z) \frac{(x-y)^\beta}{\beta!}$$

é portanto

$$(5.1.1^*) \quad (D^\alpha f)(x) = \sum_{|\beta| < m-|\alpha|} (D^{\alpha+\beta} f)(y) \frac{(x-y)^\beta}{\beta!} + \sum_{|\beta|=m-|\alpha|} (D^{\alpha+\beta} f)(z) \frac{(x-y)^\beta}{\beta!},$$

$$|\alpha| \leq m.$$

DEFINIÇÃO 5.1.2 - Se $(x, f) \in \mathbb{R}^n \times C^m(\mathbb{R}^n)$ definimos

$$|D^m f, x| = \sup_{|\alpha| \leq m} |(D^\alpha f)(x)|;$$

se B for subconjunto de $\mathbb{R}^n$, com $|B| \geq 2$, definimos

$$|D^m f, B| = \sup_{\substack{x, y \in B \\ x \neq y}} \left\{ |D^m f, x|, \sup_{|\alpha| \leq m} \frac{|D_x^\alpha R_m(x, y)|}{\|x-y\|^{m-|\alpha|}} \right\};$$

se $B = \emptyset$, definimos $|D^m f, B| = 0$ e se $B = \{y\}$ escrevemos

$$|D^m f, B| = |D^m f, y|.$$

DEFINIÇÃO 5.1.3 - Se $x \in \mathbb{R}^n$ e B for um subconjunto de $\mathbb{R}^n$, definimos

$$B_x = \{y \in B : \|x-y\| \leq 10\sqrt{n}\}$$

Do Teorema 5.1.1, resulta a seguinte

OBSERVAÇÃO 5.1.2 - Seja $f \in C^m(\mathbb{R}^n)$. Então, valem as seguintes propriedades:

1) se B é um subconjunto limitado de $\mathbb{R}^n$, existe $C_B > 0$ tal que para cada $(x,y) \in B \times B$, existe $z \in [x,y]$ tal que

$$|(D^\alpha f)(x)| \leq C_B (|D^m f, y| + |D^m f, z|), \text{ para todo } \alpha \in \mathbb{N}^n \text{ com } |\alpha| \leq m.$$

2) existe $C_0 > 0$ tal que para cada $(x,y) \in \mathbb{R}^{2n}$, existe $z_0 \in [x,y]$ tal que

$$|D_{x,m}^\alpha R(x,y)| \leq C_0 \|x-y\|^{m-|\alpha|} (|D^m f, y| + |D^m f, z_0|), \text{ para todo } \alpha \in \mathbb{N}^n \text{ com } |\alpha| \leq m.$$

De fato, é claro que 1) segue de (5.1.1) e da Definição 5.1.2. Por outro lado, de (5.1.0) e (5.1.1*), vem que

$$D_{x,m}^\alpha R(x,y) = \sum_{|\beta|=m-|\alpha|} (D^{\alpha+\beta} f)(z) \frac{(x-y)^\beta}{\beta!} - \sum_{|\beta|=m-|\alpha|} (D^{\alpha+\beta} f)(y) \frac{(x-y)^\beta}{\beta!}$$

e portanto, pela Definição 5.1.2, segue imediatamente 2).

A seguir só daremos o enunciado (que será demonstrado no Apêndice) do seguinte

TEOREMA 5.1.2 (de extensão de Whitney) - Seja A um subconjunto fechado de $\mathbb{R}^n$. Então, existe uma aplicação linear

$$L: f \in C^m(\mathbb{R}^n) \longmapsto \tilde{f} \in C^m(\mathbb{R}^n)$$

tal que

$$E_1) D^\alpha f \equiv D^\alpha \tilde{f} \text{ em } A \text{ para todo } (f, \alpha) \in C^m(\mathbb{R}^n) \times \mathbb{N}^n, |\alpha| \leq m.$$

$$E_2) \text{ existe } C > 0 \text{ tal que}$$

$$|D^m \tilde{f}, x| \leq C |D^m f, A_x|, \text{ para todo } (x, f) \in \mathbb{R}^n \times C^m(\mathbb{R}^n).$$

LEMA 5.1.1 - Seja $f \in C^m(\mathbb{R}^n)$. Então, verificam-se as seguintes propriedades:

1) Se A é um subconjunto de $\mathbb{R}^n$ e se

$$(5.1.2) \quad (D^\lambda f)(x) = 0, \text{ para todo } (x, \lambda) \in A \times \mathbb{N}^n, |\lambda| \leq m,$$

então $F = Pf$ também satisfaz (5.1.2) para todo polinômio P em $\mathbb{C}[Z]$, $Z = (Z_1, \dots, Z_n)$.

2) Se $m' \leq m$ então $|D^{m'} f, x| \leq |D^m f, x|$ para todo $x \in \mathbb{R}^n$.

3) Se $g \in C^m(\mathbb{R}^n)$, para cada subconjunto B de $\mathbb{R}^n$, tem-se

$$|D^m(f+g), B| \leq |D^m f, B| + |D^m g, B|$$

4) Seja P um polinômio em $\mathbb{C}[Z]$, com $\partial P > 0$. Então, existe $C = C(m, P) > 0$ (independente de f) tal que

$$(5.1.3) \quad |D^m(Pf), x| \leq C(1 + \|x\|^2)^{d/2} |D^m f, x|, \text{ para todo } x \in \mathbb{R}^n.$$

5) Seja B um subconjunto limitado de $\mathbb{R}^n$ e seja $s \in \mathbb{N}$. Então, existe $C = C(B, s) > 0$ tal que

$$(5.1.4) \quad \sup_{x \in \mathbb{R}^n} (1 + \|x\|^2)^s |D^m f, B_x| \leq C \sup_{y \in \mathbb{R}^n} (1 + \|y\|^2)^s |D^m f, y|,$$

PROVA - As propriedades 1), 2) e 3) são imediatas.

4) Seja $\alpha \in \mathbb{N}^n$ tal que $|\alpha| \leq m$. Então, usando o Teorema 0.3.3, segue facilmente que

$$|D^\alpha(Pf)(x)| \leq |D^m f, x| \sum_{\beta \leq \alpha} \binom{\alpha}{\beta} |(D^\beta P)(x)|, \text{ para todo } x \in \mathbb{R}^n,$$

e, pelo Lema 0.1.15, para cada $\beta \in \mathbb{N}^n$, com $\beta \leq \alpha$, existe $C_\beta > 0$ tal

que

$$|(D^\beta P)(x)| \leq C_\beta (1+\|x\|^2)^{d_\beta/2}, \text{ para todo } x \in \mathbb{R}^n,$$

onde $d_\beta = \partial(D^\beta P)$. Logo, como cada $d_\beta \leq d$ e α é arbitrário, das desigualdades acima segue (5.1.3) para uma constante conveniente $C = C(m, P) > 0$.

5) Seja $(z, s) \in \mathbb{R}^n \times \mathbb{N}$, fixado.

Seja $x \in B_z$. Pela Observação 5.1.2(1), existem $C_1 > 0$ (independente de x e z) e $x_0 \in [x, z]$ tais que

$$(5.1.5) \quad (1+\|z\|^2)^S |D^\alpha f(x)| \leq C_1 (1+\|z\|^2)^S (|D^m f, z| + |D^m f, x_0|),$$

para $|\alpha| \leq m$.

Mas, como $\|x_0 - z\| \leq \|x - z\| \leq 10\sqrt{n}$, é fácil ver que

$$(5.1.6) \quad (1+\|z\|^2) \leq C_2 (1+\|x_0\|^2), \quad C_2 = (1+10\sqrt{n})^2;$$

donde, de (5.1.5) e (5.1.6), vem

$$(1+\|z\|^2)^S |(D^\alpha f)(x)| \leq C_1 (1+\|x\|^2)^S |D^m f, z| + C_1 C_2^S (1+\|x_0\|^2)^S |D^m f, x_0|, \quad |\alpha| \leq m.$$

Se $C' = \max\{C_1, C_1 C_2^S\}$, é claro que

$$(5.1.6^*) \quad (1+\|z\|^2)^S |D^m f, x| \leq C' \sup_{y \in \mathbb{R}^n} (1+\|y\|^2)^S |D^m f, y|.$$

Seja $y \in B_z$ tal que $y \neq x$. Pela Observação 5.1.2 (2), existem $C_3 > 0$ (independente de x, y e z) e $x_1 \in [x, y]$ tais que

$$(5.1.7) \quad (1+\|z\|^2)^S \frac{|D_x^{\alpha} R_m(x,y)|}{\|x-y\|^{m-|\alpha|}} \leq C_3 (1+\|z\|^2)^S (|D^{m_f, x_1}| + |D^{m_f, y}|),$$

para $|\alpha| \leq m$.

Como $\|x_1 - z\| \leq 10\sqrt{n}$ e $\|y - z\| \leq 10\sqrt{n}$, é fácil ver que

$$(1+\|z\|^2) \leq C_2(1+\|x_1\|^2) \quad \text{e} \quad (1+\|z\|^2) \leq C_2(1+\|y\|^2);$$

e, relacionando isto com (5.1.7), tem-se

$$(1+\|z\|^2)^S \frac{|D_x^{\alpha} R_m(x,y)|}{\|x-y\|^{m-|\alpha|}} \leq C_4 [(1+\|x_1\|^2)^S |D^{m_f, x_1}| + (1+\|y\|^2)^S |D^{m_f, y}|], \quad |\alpha| \leq m,$$

onde $C_4 = C_3 C_2^S$, donde vem

$$(5.1.7^*) \quad (1+\|z\|^2)^S \sup_{|\alpha| \leq m} \frac{|D_x^{\alpha} R_m(x,y)|}{\|x-y\|^{m-|\alpha|}} \leq 2C_4 \sup_{y \in \mathbb{R}^n} (1+\|y\|^2)^S |D^{m_f, y}|.$$

Finalmente, como $x, y \in B_z$, $x \neq y$, são arbitrários, de (5.1.6*) e (5.1.7*) segue (5.1.4), onde $C = \max\{C', 2C_4\}$. ■

Dado um polinômio P em $\mathbb{C}[Z]$, $Z = (Z_1, \dots, Z_n)$, com $\partial P = d > 0$, consideremos os conjuntos N^k , $0 \leq k \leq d+1$, definidos no início do Capítulo III. Com essas notações temos o seguinte

LEMA 5.1.2 - Seja $(k, f) \in \{0, \dots, d\} \times C^m(\mathbb{R}^n)$. Se $F = Pf$, valem as seguintes propriedades:

1) $(D^\beta F)(x) = (D^\beta P)(x)f(x)$, para todo $(x, \beta) \in N^k \times \mathbb{N}^n$, com

$$|\beta| = k.$$

2) para cada $\alpha \in \mathbb{N}^n$, $|\alpha| \leq m$, existem polinômios P_λ em $\mathbb{C}[Z]$, $\lambda \leq \alpha$, tais que

$$(5.1.8) \quad P^{|\alpha|+1}(x) (D^\alpha f)(x) = \sum_{\lambda \leq \alpha} P_\lambda(x) (D^\lambda F)(x), \text{ para todo } x \in \mathbb{R}^n.$$

3) para cada $(\alpha, \beta) \in \mathbb{N}^n \times \mathbb{N}^n$ tal que $|\alpha| \leq m$ e $|\beta| = (|\alpha|+1)k$, existem polinômios P_λ em $\mathbb{C}[Z]$, $\lambda \leq \alpha + \beta$, tais que

$$(5.1.9) \quad (D^\beta P^{|\alpha|+1})(x) (D^\alpha f)(x) = \sum_{\lambda \leq \alpha + \beta} P_\lambda(x) (D^\lambda F)(x), \text{ para todo } x \in \mathbb{N}^k.$$

4) para cada $\alpha \in \mathbb{N}^n$ tal que $|\alpha| \leq m$, existem polinômios P_λ e Q_μ em $\mathbb{C}[Z, W]$, $W = (W_1, \dots, W_n)$, $\lambda \leq \alpha$, $|\mu| \leq m$, tais que para todo x e y em $\mathbb{R}^n$ tem-se

$$(5.1.10) \quad P^{|\alpha|+1}(x) P^{m+1}(y) D_x^\alpha R_m(x, y) = \sum_{\lambda \leq \alpha} P_\lambda(x, y) (D^\lambda F)(x) + \\ + \sum_{|\mu| \leq m} Q_\mu(x, y) (D^\mu F)(y)$$

5) para cada $(\alpha, \beta, \gamma) \in \mathbb{N}^{3n}$ tal que $|\alpha| \leq m$, $|\beta| = (|\alpha|+1)k$ e $|\gamma| = (m+1)k$, existem polinômios P_λ e Q_μ em $\mathbb{C}[Z, W]$, $\lambda \leq \alpha + \beta$, $|\mu| \leq (m+1)k$, tais que para todo $x, y \in \mathbb{N}^k$ tem-se

$$(5.1.11) \quad (D_x^\beta P^{|\alpha|+1})(x) (D_y^\gamma P^{m+1})(y) D_x^\alpha R_m(x, y) = \sum_{\lambda \leq \alpha + \beta} P_\lambda(x, y) (D^\lambda F)(x) + \\ + \sum_{|\mu| \leq (m+1)k+m} Q_\mu(x, y) (D^\mu F)(y)$$

6) seja $(\alpha, \beta, \gamma) \in \mathbb{N}^{3n}$ tal que $|\alpha| \leq m$, $|\beta| = (|\alpha|+1)k$ e $|\gamma| = (m+1)k$. Para cada $y \in \mathbb{N}^k$, fixo, consideremos a função

$$x \in \mathbb{R}^n \mapsto g(x) = G(x, y),$$

onde $G(x, y)$ é a soma do segundo membro em (5.1.11). Se $|r| \leq m - |\alpha|$ então, $(D^r g)(y) = 0$.

PROVA - 1) Seja $(x, \beta) \in \mathbb{N}^k \times \mathbb{N}^n$, com $|\beta| = k$. Pelo Teorema 0.3.3, tem-se

$$(D^{\beta} F)(x) = \sum_{\lambda \leq \beta} \binom{\beta}{\lambda} (D^{\lambda} P)(x) (D^{\beta-\lambda} f)(x);$$

e, pela definição de N^k ,

$$(D^{\lambda} P)(x) = 0 \text{ para todo } \lambda \in \mathbb{N}^n \text{ com } |\lambda| < k = |\beta|,$$

donde, é claro que vem $(D^{\beta} F)(x) = (D^{\beta} P)(x) f(x)$.

2) Seja $(x, \alpha) \in \mathbb{R}^n \times \mathbb{N}^n$. Se $f(x) = F(x) (P^{-1})(x)$, $P(x) \neq 0$, pelo Teorema 0.3.3, tem-se

$$(5.1.12) \quad (D^{\alpha} f)(x) = \sum_{\beta \leq \alpha} \binom{\alpha}{\beta} (D^{\beta} F)(x) \cdot D^{\alpha-\beta} (P^{-1})(x).$$

Por outro lado, não é difícil provar por indução que

$$D^{\gamma} (P^{-1})(x) = \frac{1}{P^{|\gamma|+1}(x)} \sum_i a_i \prod_j (D^{\gamma_{ij}} P)(x),$$

onde $a_i \in \mathbb{C}$ e $\sum_{i,j} \gamma_{ij} = |\gamma|$. Esta igualdade pode ser escrita sob a forma

$$(5.1.13) \quad D^{\gamma} (P^{-1})(x) = \frac{H_{\gamma}(x)}{P^{|\gamma|+1}(x)}, \quad H_{\gamma} \in \mathbb{C}[Z].$$

Logo, para $\gamma = \alpha - \beta$, $\beta \leq \alpha$, de (5.1.12) e (5.1.13), resulta que

$$(D^\alpha f)(x) = \sum_{\beta \leq \alpha} \frac{\binom{\alpha}{\beta} H_{\alpha-\beta}(x) (D^\beta F)(x)}{p^{|\alpha|+1-|\beta|}(x)}.$$

Finalmente, escolhendo $P_\beta = \binom{\alpha}{\beta} H_{\alpha-\beta} p^{|\beta|}$, $\beta \leq \alpha$, segue (5.1.8).

3) É consequência direta de 2), por um raciocínio análogo ao que foi feito na prova de 1).

4) Sejam $x, y \in \mathbb{R}^n$ e seja $\alpha \in \mathbb{N}^n$ tal que $|\alpha| \leq m$. Então, de (5.1.0), segue que

$$\begin{aligned} p^{|\alpha|+1}(x) p^{m+1}(y) D_{x,m}^\alpha R_m(x,y) &= p^{|\alpha|+1}(x) p^{m+1}(y) (D^\alpha f)(x) - \\ &- p^{|\alpha|+1}(x) \sum_{|\beta| \leq m-|\alpha|} p^{m+1}(y) (D^{\alpha+\beta} f)(y) \frac{(x-y)^\beta}{\beta!} = p^{m+1}(y) [p^{|\alpha|+1}(x) (D^\alpha f)(x)] - \\ &- p^{|\alpha|+1}(x) \sum_{|\beta| \leq m-|\alpha|} p^{m-|\alpha+\beta|}(y) [(D^{\alpha+\beta} f)(y) p^{|\alpha+\beta|+1}(y)] \frac{(x-y)^\beta}{\beta!}. \end{aligned}$$

Como $|\alpha| \leq m$ e β é tal que $|\alpha+\beta| \leq m$, usando 2), obtêm-se

$$\begin{aligned} p^{|\alpha|+1}(x) p^{m+1}(y) D_{x,m}^\alpha R_m(x,y) &= p^{m+1}(y) \sum_{\lambda \leq \alpha} P_\lambda(x) (D^\lambda F)(x) - \\ &- p^{|\alpha|+1}(x) \sum_{|\beta| \leq m-|\alpha|} p^{m-|\alpha+\beta|}(x) \left(\sum_{\mu \leq \alpha+\beta} Q_\mu(y) (D^\mu F)(y) \right) \frac{(x-y)^\beta}{\beta!} \end{aligned}$$

donde, é claro que segue (5.1.10).

5) É consequência de 4). De fato, basta aplicar D_x^β e D_y^γ sucessivamente a ambos os membros de (5.1.10) e usar, em ca

da passo, um raciocínio análogo ao utilizado na prova 1).

6) De (5.1.11), pelo Teorema 0.3.3, tem-se

$$D^r g(x) = (D_y^{\alpha} P^{m+1})(y) \sum_{\lambda \leq \alpha} \binom{r}{\lambda} (D_x^{\beta+r-\lambda} P^{|\alpha|+1})(x) D_x^{\alpha+\lambda} R_m(x, y), \quad \forall x \in \mathbb{N}^k.$$

Mas, por (5.1.0), é claro que $D_x^s R_m(y, y) = 0$ para todo $(y, s) \in \mathbb{R}^n \times \mathbb{N}^n$, com $|s| \leq m$. Agora, se $|r| \leq m - |\alpha|$ e se $\lambda \leq r$ então $|\alpha + \lambda| \leq |\alpha| + |r| \leq |\alpha| + m - |\alpha| = m$; logo, $D_x^{\alpha+\lambda} R_m(y, y) = 0$ para todo $\lambda \in \mathbb{N}^n$ tal que $\lambda \leq r$ e portanto, da igualdade acima (para $x=y$), segue que $D^r g(y) = 0$. ■

LEMA 5.1.3 - Seja A um subconjunto de $\mathbb{R}^n$. Então, existe uma constante $C_A \geq 1$ tal que

$$(5.1.14) \quad d(x, A) \leq C_A (1 + \|x\|^2), \text{ para todo } x \in \mathbb{R}^n.$$

PROVA - Se $A = \emptyset$ basta tomar $C_A = 1$. Caso contrário, seja $x_0 \in A$. Então,

$$d(x, A) \leq \|x - x_0\| \leq \|x\| + \|x_0\|, \text{ para todo } x \in \mathbb{R}^n.$$

Se $\|x_0\| \leq 1$ então para todo $x \in \mathbb{R}^n$ tem-se

$$d(x, A) \leq 1 + \|x\| \leq 1 + \frac{1}{2}(1 + \|x\|^2) \leq \frac{3}{2}(1 + \|x\|^2).$$

Se $\|x_0\| > 1$ então para todo $x \in \mathbb{R}^n$ tem-se

$$d(x, A) \leq \|x_0\| \left(1 + \frac{\|x\|}{\|x_0\|} \right) \leq \|x_0\| (1 + \|x\|) \leq \frac{3}{2} \|x_0\| (1 + \|x\|^2). \quad \blacksquare$$

5.2 - LEMAS AUXILIARES

Seja P um polinômio arbitrário, mas fixo, em $\mathbb{C}[Z]$, $Z = (Z_1, \dots, Z_n)$, com $\partial P = d > 0$. Com as notações dadas no início do Capítulo III, para cada $k \in \{0, \dots, d+1\}$, consideremos as seguintes propriedades:

Propriedade (P_k) - Para cada $(m, s) \in \mathbb{N}^2$ existe $(m', s', C) \in \mathbb{N}^2 \times]0, \infty[$, com $m' \geq m$, tal que

$$(5.2.1) \quad \sup_{x \in \mathbb{R}^n} (1 + \|x\|^2)^s |D_x^m f, N_x^k| \leq C \sup_{y \in \mathbb{R}^n} (1 + \|y\|^2)^{s'} |D^{m'}(Pf), y|,$$

para todo $f \in C^{m'}(\mathbb{R}^n)$ tal que

$$(5.2.2) \quad (D^\lambda f)(x) = 0, \text{ para todo } (x, \lambda) \in \mathbb{N}^{k+1} \times \mathbb{N}^n, |\lambda| \leq m'.$$

Propriedade (P_k^*) - É a mesma propriedade (P_k) sem a condição (5.2.2).

Nosso propósito na presente seção é dar os lemas auxiliares que ajudarão a provar que P satisfaz às propriedades (P_k) e (P_k^*) . Com este fim, seja $(k, m, m') \in \{0, \dots, d\} \times \mathbb{N}^2$ tal que

$$m' \geq 2m + (m+1)k + 2b,$$

onde $b > 0$ é o dado em (3.2.15) (vide o Lema 3.2.2). Para cada $f \in C^{m'}(\mathbb{R}^n)$ denotaremos por F o produto Pf e por

$$\sigma_m = |k, m, m'| - b > 0,$$

onde $|k, m, m'| = m' - (m+1)k - m > 0$. Os elementos e as notações considerados acima serão mantidas tanto nesta como na próxima seção.

LEMA 5.2.1 - Existe $(s, C) \in \mathbb{N} \times]0, \infty[$ tal que

$$(5.2.3) \quad |(D_x^\alpha P^{|\alpha|+1})(x)| |(D_x^\alpha f)(x)| \leq C(1+\|x\|^2)^S d(x, N^{k+1})^{|k, m, m'|} |D^{m'} B_1(x)|$$

para todo $\alpha, \beta \in \mathbb{N}^n$, com $|\alpha| \leq m$, $|\beta| = (|\alpha|+1)k$ e para todo $(x, f) \in \mathbb{N}^k \times C^{m'}(\mathbb{R}^n)$ tal que f satisfaz (5.2.2).

PROVA - Seja $(\alpha, \beta) \in \mathbb{N}^{2n}$ tal que $|\alpha| \leq m$ e $|\beta| = (|\alpha|+1)k$ e seja $(x, f) \in \mathbb{N}^k \times C^{m'}(\mathbb{R}^n)$ tal que f satisfaz (5.2.2). Então, pelo Lema 5.1.2 (3), existem polinômios P_λ em $\mathbb{C}[Z]$, $\lambda \leq \alpha + \beta$, satisfazendo (5.1.9). Logo, usando o Lema 0.1.15, podemos achar $(s, C) \in \mathbb{N} \times]0, \infty[$ tal que

$$(5.2.4) \quad \sum_{\lambda \leq \alpha + \beta} |P_\lambda(x)| \leq C(1+\|x\|^2)^S.$$

Se $d(x, N^{k+1}) \geq 1$, de (5.1.9), (5.2.4) e do Lema 5.1.1 (2), segue imediatamente (5.2.3); pois $m' \geq (m+1)k + m$. Suponhamos, então, que $d(x, N^{k+1}) < 1$. Seja $x_1 \in N^{k+1}$ tal que $\|x - x_1\| = d(x, N^{k+1})$. Então, por (5.1.0), tem-se

$$(D^\lambda F)(x) = \sum_{|\theta| \leq m' - |\lambda|} (D^{\lambda + \theta} F)(x_1) \frac{(x - x_1)^\theta}{\theta!} + D_x^\lambda R_{m'}(x, x_1), \quad \lambda \leq \alpha + \beta,$$

onde $R_{m'}(x, x_1) = R(m', F, x, x_1)$ (vide a Definição 5.1.1). Logo, como $x_1 \in N^{k+1}$, de (5.2.2) e do Lema 5.1.1 (1) (para $A = N^{k+1}$),

segue facilmente que

$$(5.2.5) \quad (D^\lambda F)(x) = D_{x_m}^\lambda R_{m'}(x, x_1), \quad \lambda \leq \alpha + \beta$$

Assim, de (5.1.9) e (5.2.5), resulta que

$$(5.2.6) \quad |(D^{\beta_P |\alpha|+1})(x)| |(D^\alpha F)(x)| \leq \sum_{\lambda \leq \alpha + \beta} |P_\lambda(x)| |D_{x_m}^\lambda R_{m'}(x, x_1)|.$$

Por outro lado, se $x \neq x_1$ e se $\lambda \leq \alpha + \beta$, é claro que

$$|D_{x_m}^\lambda R_{m'}(x, x_1)| = \frac{\|x - x_1\|^{[k, m, m']}}{\|x - x_1\|^{[k, m, m']}} |D_{x_m}^\lambda R_{m'}(x, x_1)| \leq \|x - x_1\|^{[k, m, m']} \frac{|D_{x_m}^\lambda R_{m'}(x, x_1)|}{\|x - x_1\|^{m' - |\lambda|}}$$

pois, $0 < \|x - x_1\| < 1$ e $|\lambda| \leq (m+1)k + m$. Logo, como $x, x_1 \in B_1(x)$, segue que

$$(5.2.7) \quad |D_{x_m}^\lambda R_{m'}(x, x_1)| \leq \|x - x_1\|^{[k, m, m']} |D^{m'} F, B_1(x)|, \quad \lambda \leq \alpha + \beta.$$

Assim, de (5.2.4), (5.2.6) e (5.2.7), segue (5.2.3). ■

LEMA 5.2.2 - Existe $(s, C) \in \mathbb{N} \times]0, \infty[$ tal que para todo $(x, y) \in \mathbb{N}^k \times \mathbb{N}^k$, existe $z \in [x, y]$ tal que

$$(5.2.8) \quad |(D_x^{\beta_P |\alpha|+1})(x)| |(D_y^{\gamma_P m+1})(y)| |D_{x_m}^\alpha R_{m'}(x, y)| \leq \\ \leq C \|x - y\|^{m - |\alpha|} (1 + \|y\|^2 + \|z\|^2)^s [d(y, \mathbb{N}^{k+1}) + d(z, \mathbb{N}^{k+1})]^{2b} |D^{m'} F, B(x, y)|,$$

para todo $(\alpha, \beta, \gamma, f) \in \mathbb{N}^{3n} \times C^{m'}(\mathbb{R}^n)$ tal que $|\alpha| \leq m$, $|\beta| = (|\alpha| + 1)k$, $|\gamma| = (m+1)k$ e f satisfaz (5.2.2), onde

$$B(x, y) = \{z \in \mathbb{R}^n : d(z, [x, y]) < 1\}.$$

PROVA - Seja $(x_0, y_0) \in \mathbb{N}^k \times \mathbb{N}^k$ e seja $(\alpha, \beta, \gamma, f) \in \mathbb{N}^{3n} \times C^{m'}(\mathbb{R}^n)$ satisfazendo às condições acima. Então, pelo Lema 5.1.2 (5), existem polinômios P_λ, Q_μ em $\mathbb{C}[Z, W]$, $\lambda \leq \alpha + \beta$ $|\mu| \leq (m+1)k+m$, satisfazendo (5.1.11). Seja $g(X) = G(X, y_0)$ a função definida no Lema 5.1.2 (6). Então, é claro que $g \in C^{m-|\alpha|}(\mathbb{R}^n)$; donde, pelo Teorema 5.1.1, existe $z_0 \in [z_0, y_0]$ tal que

$$g(x_0) = \sum_{|\theta| < m-|\alpha|} (D^\theta g)(y_0) \frac{(x_0 - y_0)^\theta}{\theta!} + \sum_{|\theta| = m-|\alpha|} (D^\theta g)(z_0) \frac{(x_0 - y_0)^\theta}{\theta!}.$$

Mas, pelo Lema 5.1.2 (6), $(D^\theta g)(y_0) = 0$ para $|\theta| < m-|\alpha|$ e portanto, da igualdade anterior segue que

$$(5.2.9) \quad g(x_0) = \sum_{|\theta| = m-|\alpha|} (D^\theta g)(z_0) \frac{(x_0 - y_0)^\theta}{\theta!}$$

Da definição de g , obtem-se

$$(5.2.10) \quad (D^\theta g)(z_0) = \sum_{\lambda \leq \alpha + \beta, \sigma \leq \theta} \binom{\theta}{\sigma} (D^{\theta+\lambda} F)(z_0) (D_X^{\theta-\sigma} P_\lambda)(z_0, y_0) + \\ + \sum_{|\mu| \leq (m+1)k+m} (D^\mu F)(y_0) (D_X^{\theta} Q_\mu)(z_0, y_0), \quad |\theta| = m-|\alpha|,$$

Usando o Lema 0.1.15, podemos achar $(s, C_1) \in \mathbb{N} \times]0, \infty[$ tal que

$$(5.2.11) \quad \sum_{\lambda \leq \alpha + \beta, \sigma \leq \theta} \binom{\theta}{\sigma} |(D_X^{\theta-\sigma} P_\lambda)(z_0, y_0)| \leq C_1 (1 + \|y_0\|^2 + \|z_0\|^2)^s \\ |\theta| = m-|\alpha| \\ \sum_{|\mu| \leq (m+1)k+m} |(D_X^{\theta} Q_\mu)(z_0, y_0)| \leq C_1 (1 + \|y_0\|^2 + \|z_0\|^2)^s.$$

Se $d(y_0, N^{k+1}) \geq 1$ ou $d(z_0, N^{k+1}) \geq 1$, de (5.2.9), (5.2.10), (5.1.11)

e (5.2.11), segue imediatamente (5.2.8). Suponhamos, então, que $d(y_0, N^{k+1}) < 1$ e $d(z_0, N^{k+1}) < 1$. Sejam $y_1, z_1 \in N^{k+1}$ tais que $\|y_0 - y_1\| = d(y_0, N^{k+1})$ e $\|z_0 - z_1\| = d(z_0, N^{k+1})$. É claro que

$$(5.2.12) \quad \|y_0 - y_1\|^{2b} + \|z_0 - z_1\|^{2b} \leq 2(\|y_0 - y_1\| + \|z_0 - z_1\|)^{2b}, \quad \forall b > 0.$$

Por outro lado, por (5.1.0), (5.2.2) e pelo Lema 5.1.1 (1) (por um raciocínio análogo ao que foi feito na prova do Lema 5.2.1, para obter (5.2.5)), tem-se

$$(5.2.13) \quad (D^{\lambda+\theta} F)(z_0) = D_x^{\lambda+\theta} R_m(z_0, z_1), \quad \lambda \leq \alpha + \beta, \quad |\theta| = m - |\alpha|;$$

$$(D^\mu F)(y_0) = D_x^\mu R_m(y_0, y_1), \quad |\mu| \leq (m+1)k + m,$$

onde $R_m(X, Y) = R(m', F, X, Y)$. Como $y_1, z_1 \in B(x_0, y_0)$ (também por um argumento similar ao que foi feito para obter (5.2.7)) seguem

$$(5.2.14) \quad |D_x^{\lambda+\theta} R_m(z_0, z_1)| \leq \|z_0 - z_1\|^{k, m, m'} |D^{m'} F, B(x_0, y_0)|, \quad \lambda \leq \alpha + \beta, \quad |\theta| = m - |\alpha|;$$

$$|D^\mu R_m(y_0, y_1)| \leq \|y_0 - y_1\|^{k, m, m'} |D^{m'} F, B(x_0, y_0)|, \quad |\mu| \leq (m+1)k + m.$$

Donde, de (5.2.10), (5.2.11), (5.2.13) e (5.2.14), vem que

$$|(D^\theta g)(z_0)| \leq 2C_1(1 + \|y_0\|^2 + \|z_0\|^2)^S (\|y_0 - y_1\|^{2b} + \|z_0 - z_1\|^{2b}) |D^{m'} F, B(x_0, y_0)|, \\ |\theta| = m - |\alpha|;$$

pois, como $\|y_0 - y_1\| < 1$ e $\|z_0 - z_1\| < 1$, tem-se

$$\|y_0 - y_1\|^{[k, m, m']} \leq \|y_0 - y_1\|^{2b} \text{ e } \|z_0 - z_1\|^{[k, m, m']} \leq \|z_0 - z_1\|^{2b}.$$

Logo, relacionando a última desigualdade com (5.2.12), segue que

$$(5.2.15) \quad |(D^\theta g)(z_0)| \leq 4C_1(1 + \|y_0\|^2 + \|z_0\|^2)^S (\|y_0 - y_1\| + \|z_0 - z_1\|)^{2b} |D^{m'} F, B(x_0, y_0)|, \\ |\theta| = m - |\alpha|.$$

Assim, de (5.2.9) e (5.2.15), resulta que

$$|g(x_0)| \leq C(1 + \|y_0\|^2 + \|z_0\|^2)^S (\|y_0 - y_1\| + \|z_0 - z_1\|)^{2b} |D^{m'} F, B(x_0, y_0)|$$

e, portanto, pela definição de g (vide o Lema 5.1.1 (5 e 6)) segue (5.2.8). ■

LEMA 5.2.3 - Existe $(s, C) \in \mathbb{N} \times]0, \infty[$ tal que

$$(5.2.16) \quad |(D^\alpha f)(x)| \leq C(1 + \|x\|^2)^S d(x, N^{k+1})^{\sigma_m} |D^{m'} F, B_1(x)|$$

$$(5.2.17) \quad |(D^\alpha f)(x)| \leq C(1 + \|x\|^2)^S |D^{m'} F, B_1(x)|$$

para todo $(x, \alpha, f) \in \mathbb{N}^k \times \mathbb{N}^n \times C^{m'}(\mathbb{R}^n)$ tal que $|\alpha| \leq m$ e f satisfaz (5.2.2).

PROVA - Aqui será usado o Lema 3.2.2, assim como as relações dadas em (3.2.10) e (3.2.15). De fato, seja $(x, \alpha, f) \in \mathbb{N}^k \times \mathbb{N}^n \times C^{m'}(\mathbb{R}^n)$ tal que $|\alpha| \leq m$ e f satisfaz (5.2.2). Pelo Lema 5.2.1, existe $(s_1, C_1) \in \mathbb{N} \times]0, \infty[$ satisfazendo (5.2.3) e portanto, elevando ao quadrado, depois somando em relação a β , com $|\beta| = (|\alpha| + 1)k$, e finalmente extraindo a raiz quadrada, tem-

se

$$(5.2.18) \quad |(D^\alpha f)(x)| \left[\sum_{|\beta|=(|\alpha|+1)k} |(D^\beta p^{|\alpha|+1})(x)| \right]^{1/2} \leq \\ \leq C_2(1+\|x\|^2)^{s_1} 1_{d(x, N^{k+1})}^{|k,m,m'|} |D^{m'} F, B_1(x)|,$$

onde $C_2 > 0$ é uma constante conveniente. Logo, de (3.2.10) (para $j = |\alpha|+1$) e de (5.2.18), segue facilmente que

$$(5.2.19) \quad |(D^\alpha f)(x)| \leq C_3(1+\|x\|^2)^{s_1+a} 1_{d(x, N^{k+1})}^{|k,m,m'|} b^{-|\alpha|+1} |D^{m'} F, B_1(x)|, C_3 = \\ = C_2 C^{-1} \text{ (onde } C \text{ é dado em (3.2.15))}.$$

Por outro lado, pelo Lema 5.1.3 (para $\Lambda = N^{k+1}$), existe $C_4 \geq 1$ satisfazendo (5.1.14). Como

$$b_{|\alpha|+1} \leq b \text{ (por (3.2.15)) e } (1+\|x\|^2)^{b-|\alpha|+1} \leq (1+\|x\|^2)^b$$

de (5.1.14) e (5.2.19) obtêm-se facilmente que

$$(5.2.20) \quad |(D^\alpha f)(x)| \leq C^*(1+\|x\|^2)^{s_1+a+b} 1_{d(x, N^{k+1})}^{\sigma_m} |D^{m'} F, B_1(x)|,$$

onde $\sigma_m = |k,m,m'| - b$ e $C^* = C_3 C_4^b$, o que prova (5.2.16). Finalmente, de (5.1.14) e (5.2.20), segue imediatamente (5.2.17). ■

LEMA 5.2.4 - Existe $(s, C) \in \mathbb{N} \times]0, \infty[$ tal que

$$(5.2.21) \quad |D_{x,m}^\alpha R(x,y)| \leq C(1+\|x\|^2+\|y\|^2)^s [1_{d(x, N^{k+1})}^{\sigma_m} + \\ + 1_{d(y, N^{k+1})}^{\sigma_m}] |D^{m'} F, B_1(x) \cup B_1(y)|,$$

para todo $(x,y) \in \mathbb{N}^k \times \mathbb{N}^k$ e para todo $(\alpha, f) \in \mathbb{N}^n \times C^{m'}(\mathbb{R}^n)$ tal que $|\alpha| \leq m$ e f satisfaz (5.2.2).

PROVA - Seja $(s_1, C_1) \in \mathbb{N} \times]0, \infty[$ verificando (5.2.16). De (5.1.0), para $|\alpha| \leq m$, tem-se

$$(5.2.22) \quad |D_{x,m}^{\alpha} R(x,y)| \leq |(D^{\alpha} f)(x)| + \sum_{|\beta| \leq m-|\alpha|} |(D^{\alpha+\beta} f)(y)| \|x-y\|^{|\beta|}, \quad x,y \in \mathbb{R}^n,$$

para todo $f \in C^{m'}(\mathbb{R}^n)$. Seja $C_2 > 0$ tal que

$$(5.2.23) \quad \sum_{|\beta| \leq m-|\alpha|} \|x-y\|^{|\beta|} \leq C_2 (1+\|x\|^2+\|y\|^2)^m, \quad x,y \in \mathbb{R}^n.$$

Se $C = \max\{C_1, C_1 C_2\}$ e se $s = s_1 + m$, de (5.2.22), (5.2.23) e (5.2.16), segue diretamente (5.2.21); pois $|\alpha| \leq m$ e β é tal que $|\alpha+\beta| \leq m$. ■

LEMA 5.2.5 - Existe $(s, C) \in \mathbb{N} \times]0, \infty[$ tal que

$$(5.2.24) \quad \frac{|D_{x,m}^{\alpha} R(x,y)|}{\|x-y\|^{m-|\alpha|}} \leq C(1+\|x\|^2+\|y\|^2)^s |D^{m'} F, B(x,y)|,$$

para todo $(x,y) \in \mathbb{N}^k \times \mathbb{N}^k$, $x \neq y$, e para todo $(\alpha, f) \in \mathbb{N}^n \times C^{m'}(\mathbb{R}^n)$ tal que $|\alpha| \leq m$ e f satisfaz (5.2.2).

PROVA - Seja $(x,y) \in \mathbb{N}^k \times \mathbb{N}^k$, $x \neq y$, e seja $(\alpha, f) \in \mathbb{N}^n \times C^{m'}(\mathbb{R}^n)$ satisfazendo as condições acima.

I) Suponhamos primeiro que

$$2\|x-y\| \geq d(x, N^{k+1}) + d(y, N^{k+1}).$$

Seja $(s_1, C_1) \in \mathbb{N} \times]0, \infty[$ satisfazendo (5.2.21). Logo, como

$$d(x, N^{k+1}) \leq 2\|x-y\| \quad \text{e} \quad d(y, N^{k+1}) \leq 2\|x-y\|,$$

a partir de (5.2.21) é claro que

$$\frac{|D_{x,m}^{\alpha} R(x,y)|}{\|x-y\|^{m-|\alpha|}} \leq C_1 2^{1+\sigma_m} (1+\|x\|^2+\|y\|^2)^{\sigma_m-m-|\alpha|} |D^{m'} F, B(x,y)|$$

e portanto, como $m+|\alpha| \leq \sigma_m$, existe $C_2 > 0$ tal que

$$(5.2.25) \quad \frac{|D_{x,m}^{\alpha} R(x,y)|}{\|x-y\|^{m-|\alpha|}} \leq C_2 (1+\|x\|^2+\|y\|^2)^{s_1+\sigma_m} |D^{m'} F, B(x,y)|.$$

II) Suponhamos agora que

$$(5.2.26) \quad 2\|x-y\| < d(x, N^{k+1}) + d(y, N^{k+1}).$$

Como $|d(x, N^{k+1}) - d(y, N^{k+1})| \leq \|x-y\|$, de (5.2.26), segue facilmente que

$$(*) \quad \frac{1}{3} d(y, N^{k+1}) < d(x, N^{k+1}) < 3d(y, N^{k+1});$$

além disso, de (5.2.26), tem-se

$$d(z, N^{k+1}) \leq \|x-y\| + d(x, N^{k+1}) < \frac{1}{2} d(y, N^{k+1}) + \frac{3}{2} d(x, N^{k+1})$$

para todo $z \in [x, y]$ e portanto, das duas últimas desigualdades, segue que

$$(**) \quad d(z, N^{k+1}) < 3d(x, N^{k+1}), \quad \forall z \in [x, y];$$

de modo análogo prova-se que

$$(***) \quad d(z, N^{k+1}) < 3d(y, N^{k+1}), \quad \forall z \in [x, y].$$

Logo, de (*), (**) e (***), vem que

$$\begin{aligned} [d(y, N^{k+1}) + d(z, N^{k+1})]^2 &= d(y, N^{k+1})^2 + 2d(y, N^{k+1})d(z, N^{k+1}) + d(z, N^{k+1})^2 \leq \\ &\leq 3d(x, N^{k+1})d(y, N^{k+1}) + 6d(x, N^{k+1})d(y, N^{k+1}) + 9d(x, N^{k+1})d(y, N^{k+1}); \end{aligned}$$

portanto

$$(5.2.27) \quad [d(y, N^{k+1}) + d(z, N^{k+1})]^2 \leq 18d(x, N^{k+1})d(y, N^{k+1}), \quad \forall z \in [x, y].$$

Por outro lado, pelo Lema 5.2.2, existem $(s_2, M_1) \in \mathbb{N} \times]0, \infty[$ (independente de x, y, α e f) e um ponto $z \in [x, y]$ (correspondente a x e y) satisfazendo (5.2.8). Como $z = tx + (1-t)y$, para algum $t \in [0, 1]$, é claro que existe $M_2 > 0$ tal que

$$(5.2.28) \quad (1 + \|y\|^2 + \|z\|^2) \leq M_2(1 + \|x\|^2 + \|y\|^2).$$

Se $M_3 = M_1 M_2^{s_2} (18)^b$, de (5.2.8), (5.2.27) e (5.2.28), resulta que

$$\begin{aligned} &|D_x^{\beta} P^{|\alpha|+1}(x)| |D_y^{\gamma} P^{m+1}(y)| \frac{|D_x^{\alpha} R_m(x, y)|}{\|x-y\|^{m-|\alpha|}} \leq \\ &\leq M_3(1 + \|x\|^2 + \|y\|^2)^{s_2} d(x, N^{k+1})^b d(y, N^{k+1})^b |D^{m'} F, B(x, y)|, \end{aligned}$$

para todo $(\beta, \gamma) \in \mathbb{N}^{2n}$ tal que $|\beta| = (|\alpha|+1)k$ e $|\gamma| = (m+1)k$. Logo, para cada $\gamma \in \mathbb{N}^n$, com $|\gamma| = (m+1)k$, fixo, elevando ao qua-

drado, depois somando em relação a β , com $|\beta| = (|\alpha|+1)k$, e finalmente extraindo a raiz quadrada (na última desigualdade) existe $M_4 > 0$ tal que

$$(5.2.29) \quad \left[\sum_{|\beta|=(|\alpha|+1)k} |D^{\beta} P^{|\alpha|+1}(x)|^2 \right]^{1/2} |D^{\gamma} P^{m+1}(y)| \frac{|D_x^{\alpha} R_m(x,y)|}{\|x-y\|^{m-|\alpha|}} \leq \\ \leq M_4 (1+\|x\|^2+\|y\|^2)^{s_2} d(x, N^{k+1})^b d(y, N^{k+1})^b |D^{m'} F, B(x,y)|,$$

para todo $\gamma \in \mathbb{N}^n$ tal que $|\gamma| = (m+1)k$; e portanto, de (3.2.10) (para $j = |\alpha|+1$, no Lema 3.2.2) e de (5.2.29), obtêm-se facilmente que

$$|D^{\gamma} P^{m+1}(y)| \frac{|D_x^{\alpha} R_m(x,y)|}{\|x-y\|^{m-|\alpha|}} \leq M_5 (1+\|x\|^2+\|y\|^2)^{s_2+a} d(x, N^{k+1})^{b-b_{|\alpha|+1}} \times \\ \times d(y, N^{k+1})^b |D^{m'} F, B(x,y)|$$

para todo $\gamma \in \mathbb{N}^n$ tal que $|\gamma| = (m+1)k$. A partir desta desigualdade, por um argumento similar ao que foi feito acima (agora com os γ , $|\gamma| = (m+1)k$, usando o Lema 3.2.2, para $j = m+1$) tem-se

$$\frac{|D_x^{\alpha} R_m(x,y)|}{\|x-y\|^{m-|\alpha|}} \leq M_6 (1+\|x\|^2+\|y\|^2)^{s_2+2a} d(x, N^{k+1})^{b-b_{|\alpha|+1}} d(y, N^{k+1})^{b-b_{m+1}} \times \\ \times |D^{m'} F, B(x,y)|.$$

Pelo Lema 5.1.3 (para $\Lambda = N^{k+1}$), existe $M_7 \geq 1$ (independente de x e y) tal que

$$d(x, N^{k+1}) \leq M_7(1 + \|x\|^2 + \|y\|^2) \quad \text{e} \quad d(y, N^{k+1}) \leq M_7(1 + \|x\|^2 + \|y\|^2).$$

Como $b_{|\alpha|+1} \leq b$, $b_{m+1} \leq b$ e

$$\begin{aligned} (1 + \|x\|^2 + \|y\|^2)^{b-b_{|\alpha|+1}} &\leq (1 + \|x\|^2 + \|y\|^2)^b, \quad (1 + \|x\|^2 + \|y\|^2)^{b-b_{m+1}} \leq \\ &\leq (1 + \|x\|^2 + \|y\|^2)^b \end{aligned}$$

das desigualdades acima segue facilmente que

$$(5.2.30) \quad \frac{|D_m^\alpha R(x, y)|}{\|x - y\|^{m-|\alpha|}} \leq M_8(1 + \|x\|^2 + \|y\|^2)^{s_2+2(a+b)} |D^{m'} F, B(x, y)|,$$

onde $M_8 = M_6 M_7^{2b}$. Finalmente, se $C = \max\{C_2, M_8\}$ e se $s = \max\{s_1 + \sigma_m, s_2 + 2(a+b)\}$, de (5.2.25) e (5.2.30), segue (5.2.24). ■

5.3 - TEOREMA E

Nesta seção provaremos um teorema chave (o Teorema E) que resolve o problema da divisão de distribuições por polinômios não nulos, para o qual usaremos o Teorema de extensão de Whitney com ajuda dos resultados da seção anterior, obtidos como consequência do Teorema de Seidenberg-Tarski. A idéia da demonstração do Teorema E, consiste em estimar $f \in C^{m'}(\mathbb{R}^n)$ (com m' adequado) em termos de $F = Pf$ primeiro em N^k , depois em N^{k-1} e assim por diante; para isso pro-

varemos sucessivamente para k decrescente a Propriedade (P_k^*) .

PROPOSIÇÃO 5.3.1 - P satisfaz a Propriedade (P_k) para todo $k \in \{0, \dots, d\}$.

PROVA - Seja $k \in \{0, \dots, d\}$, fixado, e seja $(m, s) \in \mathbb{N}^2$. Então, de vemos achar $(m', s', C) \in \mathbb{N}^2 \times]0, \infty[$, com $m' \geq m$, tal que P satisfaz a Propriedade (P_k) com (m, s, m', s', C) . Consideremos $m' \in \mathbb{N}$ tal que

$$m' \geq 2m + (m+1)k + 2b,$$

onde $b > 0$ é dado em (3.2.15) (vide o Lema 3.2.2). Seja $(s_1, C_1) \in \mathbb{N} \times]0, \infty[$ satisfazendo (5.2.17) e (5.2.24). Denotaremos por $\rho = 10\sqrt{n}$ e por $R = 1 + \rho$. Seja $z \in \mathbb{R}^n$, fixado.

1) Estimaremos primeiro $(1 + \|z\|^2)^S |D^{m'} f, N_z^k|$ para $f \in C^{m'}(\mathbb{R}^n)$ satisfazendo (5.2.2).

Seja $x \in N_z^k$. Então, $\|x - z\| \leq \rho$ (e $x \in N_z^k$) e portanto $(1 + \|x\|^2) \leq (1 + \rho)^2 (1 + \|z\|^2)$. Se $C_2 = C_1 (1 + \rho)^{2S_1}$, como $B_1(x) \subset B_R(z)$, por (5.2.17) tem-se

$$(5.3.1) \quad |D^\alpha f(x)| \leq C_2 (1 + \|z\|^2)^{S_1} |D^{m'} f, B_R(z)|$$

para todo $(\alpha, f) \in \mathbb{N}^n \times C^{m'}(\mathbb{R}^n)$ tal que $|\alpha| \leq m$ e f satisfaz (5.2.2).

Seja $y \in N_z^k$ tal que $y \neq x$. Então, $\|y - z\| \leq \rho$ e portanto

é fácil ver que

$$1 + \|x\|^2 + \|y\|^2 \leq 2(1+\rho)^2(1+\|z\|^2).$$

Se $C_3 = 2^{s_1} C_1 (1+\rho)^{2s_1}$, como $B(x,y) \subset B_R(z)$, por (5.2.24) tem-se

$$(5.3.2) \quad \frac{|D_{x,m}^{\alpha} R(x,y)|}{\|x-y\|^{m-|\alpha|}} \leq C_3 (1+\|z\|^2)^{s_1} |D^{m'} F, B_R(z)|.$$

para todo $(\alpha, f) \in \mathbb{N}^n \times C^{m'}(\mathbb{R}^n)$ tal que $|\alpha| \leq m$ e f satisfaz (5.2.2). Logo, como $x, y \in \mathbb{N}^k$, $x \neq y$, são arbitrários, de (5.3.1), (5.3.2) e da Definição 5.1.2 segue que

$$(5.3.3) \quad (1+\|z\|^2)^s |D^{m'} f, N_z^k| \leq C' (1+\|z\|^2)^{s'} |D^{m'} F, B_R(z)|$$

para todo $f \in C^{m'}(\mathbb{R}^n)$ satisfazendo (5.2.2), onde $s' = s + s_1$ e $C' = \max\{C_2, C_3\}$.

2) Agora estimaremos $|D^{m'} F, B_R(z)|$, para $f \in C^{m'}(\mathbb{R}^n)$ satisfazendo (5.2.2).

Seja $x \in B_R(z)$. Então, pela Observação 5.1.2 (1), existem $M_1 > 0$ (independente de x e z) e $\tilde{x} \in [x, z]$ tais que

$$|(D^{\alpha} F)(x)| \leq M_1 (|D^{m'} F, z| + |D^{m'} F, \tilde{x}|), \quad |\alpha| \leq m',$$

donde, como $\|x-z\| \leq R$, resulta que

$$(1+\|z\|^2)^{s'} |(D^{\alpha} F)(x)| \leq M_1 (1+\|z\|^2)^{s'} |D^{m'} F, z| + M_2 (1+\|\tilde{x}\|^2)^{s'} |D^{m'} F, \tilde{x}|, \quad |\alpha| \leq m',$$

onde, $M_2 = M_1(1+R)^{2s'}$. Logo,

$$(5.3.4) \quad (1+\|z\|^2)^{s'} |(D^\alpha F)(x)| \leq 2M_2 \sup_{x' \in \mathbb{R}^n} (1+\|x'\|^2)^{s'} |D^{m'} F, x'|, \quad |\alpha| \leq m'$$

Seja $y \in B_R(z)$ tal que $y \neq x$. Então, por um argumento similar ao que foi feito acima (neste caso usando a Observação 5.2.1 (2)), podemos achar $M' \geq 2M_2$ tal que

$$(5.3.5) \quad (1+\|z\|^2)^{s'} \frac{|D^{\alpha} R_{m'}(x, y)|}{\|x - y\|^{m' - |\alpha|}} \leq M' \sup_{x' \in \mathbb{R}^n} (1+\|x'\|^2)^{s'} |D^{m'} F, x'|, \quad |\alpha| \leq m',$$

onde $R_{m'}(X, Y) = R(m', F, X, Y)$. Portanto, como $x, y \in B_R(z)$, $x \neq y$, são arbitrários, de (5.3.4) e (5.3.5) segue que

$$(5.3.6) \quad (1+\|z\|^2)^{s'} |D^{m'} F, B_R(z)| \leq M' \sup_{y \in \mathbb{R}^n} (1+\|y\|^2)^{s'} |D^{m'} F, y|.$$

Finalmente, de (5.3.3) e (5.3.6), segue que

$$\sup_{z \in \mathbb{R}^n} (1+\|z\|^2)^s |D^{m'} F, N_z^k| \leq C' M' \sup_{y \in \mathbb{R}^n} (1+\|y\|^2)^{s'} |D^{m'} F, y|$$

para todo $f \in C^{m'}(\mathbb{R}^n)$ satisfazendo (5.2.2). Isto é, P satisfaz a Propriedade (P_k) . ■

PROPOSIÇÃO 5.3.2 - Seja $k \in \{0, \dots, d\}$. Se P satisfaz as propriedades (P_k) e (P_{k+1}^*) então P satisfaz a Propriedade (P_k^*) .

PROVA - Notemos que (P_d) e (P_d^*) são equivalentes, pois $N^{d+1} = \emptyset$. Também (P_{d+1}) e (P_{d+1}^*) são vazias. Seja $(m, s) \in \mathbb{N}^2$. Então, como P satisfaz a Propriedade (P_k) podemos achar $(m', s', C') \in \mathbb{N}^2 \times]0, \infty[$, com $m' \geq m$ e $s' \geq s$, verificando (5.2.1) para todo

$f \in C^{m'}(\mathbb{R}^n)$ que satisfaz (5.2.2). Além disso, como P satisfaz a Propriedade (P_{k+1}^*) , existe $(m'', s'', C'') \in \mathbb{N}^2 \times]0, \infty[$, com $s'' \geq s' + d$ e $m'' \geq m'$, tal que

$$(5.3.7) \quad \sup_{x \in \mathbb{R}^n} (1 + \|x\|^2)^{s' + d} |D^{m'} f, N_x^{k+1}| \leq C'' \sup_{y \in \mathbb{R}^n} (1 + \|y\|^2)^{s''} |D^{m''} F, y|,$$

$$\forall f \in C^{m''}(\mathbb{R}^n).$$

Seja $f \in C^{m''}(\mathbb{R}^n)$. Então, pelo Teorema 5.1.2, existe uma função $g \in C^{m'}(\mathbb{R}^n)$ tal que

$E_1)$ se $h = f - g$ então h satisfaz (5.2.2)

$E_2)$ existe $C_1 > 0$ (independente de g) tal que

$$|D^{m'} g, x| \leq C_1 |D^{m'} f, N_x^{k+1}|, \text{ para todo } x \in \mathbb{R}^n.$$

Usando o Lema 5.1.1 (4) podemos achar $C_2 > 0$ tal que

$$(5.3.8) \quad \sup_{x \in \mathbb{R}^n} (1 + \|x\|^2)^{s'} |D^{m'} (Pg), x| \leq C_2 \sup_{y \in \mathbb{R}^n} (1 + \|y\|^2)^{s' + d} |D^{m'} g, y|$$

Donde, de $E_2)$ e (5.3.8), vem

$$\sup_{x \in \mathbb{R}^n} (1 + \|x\|^2)^{s'} |D^{m'} (Pg), x| \leq C_1 C_2 \sup_{y \in \mathbb{R}^n} (1 + \|y\|^2)^{s' + d} |D^{m'} f, N_y^{k+1}|;$$

logo, relacionando isto com (5.3.7), resulta que

$$(5.3.9) \quad \sup_{x \in \mathbb{R}^n} (1 + \|x\|^2)^{s'} |D^{m'} (Pg), x| \leq C^* \sup_{y \in \mathbb{R}^n} (1 + \|y\|^2)^{s''} |D^{m''} F, y|,$$

sendo $C^* = C_1 C_2 C''$. Pelo Lema 5.1.1 ((2) e (3)), tem-se

$$|D^{m'} (Ph), x| \leq |D^{m''} F, x| + |D^{m'} (Pg), x|, \text{ para todo } x \in \mathbb{R}^n,$$

e portanto

$$(5.3.10) \quad \sup_{x \in \mathbb{R}^n} (1+\|x\|^2)^{s'} |D^{m'}(Ph), x| \leq \sup_{y \in \mathbb{R}^n} (1+\|y\|^2)^{s''} |D^{m''}F, y| + \\ + \sup_{y \in \mathbb{R}^n} (1+\|y\|^2)^{s'} |D^{m'}(Pg), y|;$$

logo, de (5.3.9) e (5.3.10), obtêm-se

$$(5.3.11) \quad \sup_{x \in \mathbb{R}^n} (1+\|x\|^2)^{s'} |D^{m'}(Ph), x| \leq (1+C^*) \sup_{y \in \mathbb{R}^n} (1+\|y\|^2)^{s''} |D^{m''}F, y|.$$

Mas h satisfaz (5.2.1) e (5.2.2); donde, a partir de (5.3.11), segue que

$$(5.3.12) \quad \sup_{x \in \mathbb{R}^n} (1+\|x\|^2)^s |D^{m_h, N_x^k}| \leq C' (1+C^*) \sup_{y \in \mathbb{R}^n} (1+\|y\|^2)^{s''} |D^{m''}F, y|.$$

Por outro lado, de (5.3.7) e (E_2) , tem-se

$$(5.3.13) \quad \sup_{x \in \mathbb{R}^n} (1+\|x\|^2)^{s'} |D^{m'}g, x| \leq C_1 C'' \sup_{y \in \mathbb{R}^n} (1+\|y\|^2)^{s''} |D^{m''}F, y|,$$

e, pelo Lema 5.1.1 (5) (para $B = N^k$), existe $C_3 > 0$ tal que

$$(5.3.14) \quad \sup_{x \in \mathbb{R}^n} (1+\|x\|^2)^s |D^{m_g, N_x^k}| \leq C_3 \sup_{y \in \mathbb{R}^n} (1+\|y\|^2)^s |D^{m_g}, y|.$$

Como $m \leq m'$ e $s \leq s'$, de (5.3.13), (5.3.14) e do Lema 5.1.1 (2), obtêm-se

$$(5.3.15) \quad \sup_{x \in \mathbb{R}^n} (1+\|x\|^2)^s |D^{m_g, N_x^k}| \leq C_1 C'' C_3 \sup_{y \in \mathbb{R}^n} (1+\|y\|^2)^{s''} |D^{m''}F, y|.$$

Portanto, como $f = g + h$, de (5.3.12), (5.3.14) e do Lema 5.1.1 (3), resulta que

$$\sup_{x \in \mathbb{R}^n} (1 + \|x\|^2)^S |D^m f, N_x^k| \leq C \sup_{y \in \mathbb{R}^n} (1 + \|y\|^2)^{S''} |D^{m''} F, y|,$$

onde $C = C'(1 + C^*) + C_1 C_3 C''$. Logo, como $f \in C^{m''}(\mathbb{R}^n)$ é arbitrário, P satisfaz a Propriedade (P_k^*) . ■

TEOREMA E - Para cada $(m, k) \in \mathbb{N}^2$, existe $(m', k', C) \in \mathbb{N}^2 \times]0, \infty[$, com $m' \geq m$, tal que

$$(5.3.16) \quad \sup_{x \in \mathbb{R}^n} (1 + \|x\|^2)^k |D^m \phi, x| \leq C \sup_{y \in \mathbb{R}^n} (1 + \|y\|^2)^{k'} |D^{m'} (P\phi), y|,$$

$$\forall \phi \in \mathcal{S}(\mathbb{R}^n).$$

PROVA - Das proposições (5.3.1) e (5.3.2) prova-se, por indução que P satisfaz a Propriedade (P_k^*) para todo $k \in \{0, 1, \dots, d+1\}$. Em particular, P satisfaz (P_0^*) . Logo, para cada $(m, s) \in \mathbb{N}^2$ existe $(m', k', C') \in \mathbb{N}^2 \times]0, \infty[$, com $m' \geq m$, tal que

$$(5.3.17) \quad \sup_{x \in \mathbb{R}^n} (1 + \|x\|^2)^S |D^m f, B_\rho(x)| \leq C \sup_{y \in \mathbb{R}^n} (1 + \|y\|^2)^{k'} |D^{m'} (Pf), y|,$$

$$\forall f \in C^{m'}(\mathbb{R}^n);$$

onde, $\rho = 10\sqrt{n}$. Portanto, como

$$|D^m f, x| \leq |D^m f, B_\rho(x)|, \text{ para todo } (x, f) \in \mathbb{R}^n \times C^{m'}(\mathbb{R}^n),$$

de (5.3.17) segue (5.3.16). ■

5.4 - TEOREMAS DE EXISTÊNCIA NO ESPAÇO DAS DISTRIBUIÇÕES

Agora veremos que o problema da divisão de distri-

ções por polinômios nulos pode facilmente ser resolvido usando o Teorema E. De fato, no caso das distribuições temperadas é imediato a partir do seguinte

TEOREMA 5.4.1 - Seja P um polinômio não nulo em $\mathbb{C}[Z]$, $Z = (Z_1, \dots, Z_n)$. Então, a aplicação linear

$$L: \phi \in S(\mathbb{R}^n) \mapsto (P\phi) \in PS(\mathbb{R}^n)$$

é bijetora e bicontínua.

PROVA - Indiquemos por N o conjunto dos zeros de P em $\mathbb{R}^n$. No temos que $\phi = 0$, se $P\phi = 0$; pois o conjunto $\mathbb{R}^n \setminus N$ é denso em $\mathbb{R}^n$; isto é, L é injetora. L é sobrejetora por definição e a continuidade de L é um fato conhecido. Resta ver que a inversa

$$L^{-1}: (P\phi) \in PS(\mathbb{R}^n) \mapsto \phi \in S(\mathbb{R}^n)$$

é contínua, com $PS(\mathbb{R}^n)$ munido da topologia induzida por $S(\mathbb{R}^n)$. Para isso, basta provar que se $P\phi_j \rightarrow 0$ em $S(\mathbb{R}^n)$ então $\phi_j \rightarrow 0$ em $S(\mathbb{R}^n)$; isto é, pela Definição 0.3.3 (2), para cada $(\alpha, k, \epsilon) \in \mathbb{N}^n \times \mathbb{N} \times]0, \infty[$, existe $j_0 \in \mathbb{N}$ tal que

$$(5.4.1) \quad \sup_{x \in \mathbb{R}^n} (1 + \|x\|^2)^k |(D^\alpha \phi_j)(x)| < \epsilon, \text{ para } j \geq j_0.$$

De fato, pelo Teorema E (para $(m = |\alpha|, k)$), existe $(m', k', C) \in \mathbb{N}^2 \times]0, \infty[$, com $m' \geq m$, satisfazendo (5.3.16). Por outro lado, pela hipótese, para cada $\beta \in \mathbb{N}^n$, com $|\beta| \leq m'$, e-

xiste $j_\beta \in \mathbb{N}$ tal que

$$\sup_{y \in \mathbb{R}^n} (1 + \|y\|^2)^{k'} |(D^\beta (P\phi_j))(y)| < \varepsilon C^{-1}, \text{ para } j \geq j_\beta.$$

Se $j_0 \geq \max\{j_\beta : |\beta| \leq m'\}$ então

$$(5.4.2) \quad \sup_{y \in \mathbb{R}^n} (1 + \|y\|^2)^{k'} |D^{m'}(P\phi_j), y| < \varepsilon C^{-1}, \text{ para } j \geq j_0.$$

Logo, de (5.3.16) e (5.4.2), segue imediatamente (5.4.1). ■

COROLÁRIO 5.4.1 - Na hipótese do teorema, seja $T \in S'(\mathbb{R}^n)$. Então, existe $S \in S'(\mathbb{R}^n)$ tal que

$$(5.4.3) \quad PS = T.$$

PROVA - Pelo teorema segue que a aplicação

$$T \circ L^{-1}: (P\phi) \in \mathcal{PS}(\mathbb{R}^n) \longmapsto \langle T, \phi \rangle \in \mathbb{C}$$

é linear e contínua; logo, pelo Teorema de Hann-Banach, existe $S \in S'(\mathbb{R}^n)$ tal que

$$\langle S, P\phi \rangle = \langle T, \phi \rangle, \text{ para todo } \phi \in S(\mathbb{R}^n).$$

Dai segue (5.4.3). De fato,

$$\langle PS, \phi \rangle = \langle S, P\phi \rangle = \langle T, \phi \rangle, \forall \phi \in S(\mathbb{R}^n). \quad \blacksquare$$

OBSERVAÇÃO 5.4.1 - Em geral a solução S de (5.4.3) não é única. Mas temos que a equação (5.4.3) tem solução única se, e somente se,

$N = \phi$. Com efeito, se $P(a) = 0$ para algum $a \in \mathbb{R}^n$, para todo $\phi \in S(\mathbb{R}^n)$, tem-se

$$\begin{aligned} \langle P(S + \delta_a), \phi \rangle &= \langle PS, \phi \rangle + \langle P\delta_a, \phi \rangle = \langle PS, \phi \rangle + \langle \delta_a, P\phi \rangle = \\ &= \langle T, \phi \rangle + (P\phi)(a) = \langle T, \phi \rangle; \end{aligned}$$

isto é, a solução não é única. Reciprocamente, se $P(x) \neq 0$ para todo $x \in \mathbb{R}^n$ então a função $x \in \mathbb{R}^n \mapsto P(x)^{-1}$ é de classe C^∞ ; assim, se $PS_1 = PS_2$ então $S_1 = S_2$.

A equação (5.4.3) é a equação da divisão de T pelo polinômio P , pois S pode ser considerado como uma espécie de *quociente* T/P .

Uma consequência direta do Teorema 5.4.1 é o

TEOREMA 5.4.2 - Seja $P(D)$ um ODPL, sobre $\mathbb{R}^n$, com coeficientes constantes não todos nulos. Então, para cada $T \in S'(\mathbb{R}^n)$ existe $S \in S'(\mathbb{R}^n)$ tal que

$$(5.4.4) \quad P(D)S = T$$

PROVA - Para cada $T \in S'(\mathbb{R}^n)$, aplicando a transformação de Fourier, a equação (5.4.4) fica transformado na equação

$$P(-iX)\hat{S} = \hat{T}.$$

Esta equação, pelo Teorema 5.4.1, tem uma solução temperada $\hat{S}$; logo, invertendo a transformação de Fourier obtemos a so

lução de (5.4.4). ■

COROLÁRIO 5.4.2 - Todo ODPL não nulo tem uma solução fundamental temperada.

PROVA - Seja $P(D)$ um ODPL. Então, como $\delta \in S'(\mathbb{R}^n)$ (onde $\delta(\phi) = \phi(0)$, para $\phi \in S'(\mathbb{R}^n)$), pelo teorema existe $SES'(\mathbb{R}^n)$ tal que $P(D)S = \delta$. ■

TEOREMA 5.4.3 - Seja Ω um aberto de $\mathbb{R}^n$ e seja P um polinômio não nulo em $\mathbb{C}[Z]$, $Z = (Z_1, \dots, Z_n)$. Então, para cada $T \in \mathcal{D}'(\Omega)$ existe $SE\mathcal{D}'(\Omega)$ tal que

$$(5.4.5) \quad PS = T$$

PROVA - Seja $T \in \mathcal{D}'(\Omega)$ fixado. Provaremos que a aplicação linear

$$F: (P\phi) \in \mathcal{PD}(\Omega) \longmapsto \langle T, \phi \rangle \in \mathbb{C}$$

é contínua. De fato, pelo Teorema 0.3.1, basta demonstrar que se K é um compacto contido em Ω , existe $(m, C) \in \mathbb{N} \times]0, \infty[$ (dependendo de K) tal que

$$(5.4.6) \quad |\langle T, \phi \rangle| \leq \sup_{x \in \Omega} |D^m(P\phi), x|, \quad \forall \phi \in \mathcal{D}(\Omega) \text{ com } \text{Supp}(P\phi) \subset K.$$

Como $T \in \mathcal{D}'(\Omega)$, existe $(m^*, C^*) \in \mathbb{N} \times]0, \infty[$ tal que

$$(5.4.7) \quad |\langle T, \phi \rangle| \leq C^* \sup_{x \in \Omega} |D^{m^*} \phi, x|, \quad \forall \phi \in \mathcal{D}(\Omega) \text{ com } \text{Supp } \phi \subset K.$$

Por outro lado, pelo Teorema E (para $(m^*, 0)$), existe $(m', k', C') \in \mathbb{N}^2 \times]0, \infty[$ tal que

$$(5.4.8) \quad \sup_{x \in \mathbb{R}^n} |D^{m'} \phi, x| \leq C' \sup_{y \in \mathbb{R}^n} (1 + \|y\|^2)^{k'} |D^{m'}(P\phi), y|, \quad \forall \phi \in \mathcal{S}(\mathbb{R}^n).$$

Seja $\phi \in \mathcal{D}(\Omega)$ tal que $\text{Supp } (P\phi) \subset K$. Então $\text{Supp } \phi \subset K$. Com efeito, se $\Omega_K = \{x \in \Omega \setminus K : P(x) \neq 0\}$, é claro que Ω_K é denso em $\Omega \setminus K$; logo, como $P\phi \equiv 0$ em $\Omega \setminus K$ e portanto em Ω_K , tem-se $\phi \equiv 0$ em Ω_K . Donde, pela densidade de Ω_K em $\Omega \setminus K$ e pela continuidade de ϕ , vem que $\phi \equiv 0$ em $\Omega \setminus K$, isto é, $\text{Supp } \phi \subset K$.

Considerando a função $\tilde{\phi}$ sobre $\mathbb{R}^n$, como sendo ϕ em Ω e nula fora de Ω , tem-se que $\tilde{\phi} \in \mathcal{S}(\mathbb{R}^n)$; logo, de (5.4.7) e (5.4.8), resulta que

$$\begin{aligned} |\langle T, \phi \rangle| &\leq C^* \sup_{x \in \Omega} |D^{m^*} \phi, x| = C^* \sup_{x \in \mathbb{R}^n} |D^{m^*} \tilde{\phi}, x| \leq \\ &\leq C^* C' \sup_{y \in \mathbb{R}^n} (1 + \|y\|^2)^{k'} |D^{m'}(P\tilde{\phi}), y| = \\ &= C^* C' \sup_{y \in K} (1 + \|y\|^2)^{k'} |D^{m'}(P\phi), y| \end{aligned}$$

e portanto

$$|\langle T, \phi \rangle| \leq C \sup_{y \in \Omega} |D^{m'}(P\phi), y|$$

sendo $C = C^* C' \sup_{y \in K} (1 + \|y\|^2)^{k'}$, o que prova (5.4.6), pois $\phi \in \mathcal{D}(\Omega)$, com $\text{Supp } (P\phi) \subset K$, é arbitrário. Finalmente, uma vez que F é contínua, por um argumento similar ao que foi feito na prova do Corolário 5.4.1 (usando o Teorema de Hann-Banach) segue o Teorema. $\blacksquare$

APÊNDICE

O TEOREMA DE EXTENSÃO DE WHITNEY

A seguir provaremos que dados um conjunto fechado A de $\mathbb{R}^n$ e uma função $f \in C^m(\mathbb{R}^n)$, $m \geq 0$, existe outra função $g \in C^m(\mathbb{R}^n)$ (vide o Teorema 5.1.2) tal que $D^\alpha g \equiv D^\alpha f$ em A para $\alpha \in \mathbb{N}^n$, com $|\alpha| \leq m$; ainda mais, o qual é a parte importante, é possível estimar as derivadas de g , de ordem menor ou igual a m , sobre $\mathbb{R}^n$ em termos das derivadas de f unicamente, de ordem menor ou igual a m , sobre A . O propósito desde Apêndice é simplificar e detalhar a demonstração do Teorema 5.2.1 de modo a torná-lo acessível para a leitura.

A.1 - PRELIMINARES

A prova do seguinte lema é imediata.

LEMA A.1.1 - Valem as seguintes propriedades:

1) para cada $(m, n) \in \mathbb{N}^2$ tem-se

$$(1+x^m)(1+x^n) \leq 3(1+x^{m+n}), \text{ para todo } x \in]0, \infty[.$$

2) para cada $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ existe $C_\alpha > 0$ tal que

$$\prod_{i=1}^n (1+x^{\alpha_i}) \leq C_\alpha (1+x^{|\alpha|}), \text{ para todo } x \in]0, \infty[.$$

LEMA A.1.2 - Sejam I um intervalo aberto de $\mathbb{R}$ e F um subconjunto fechado de I . Seja $f: I \rightarrow \mathbb{R}$ uma função contínua e seja $(x_0, y_0) \in I \times \mathbb{R}$. Suponhamos que para cada $\varepsilon > 0$ existe $\delta_\varepsilon > 0$ tal que

$$(A.1.2) \quad x \in F \text{ e } 0 < |x - x_0| < \delta_\varepsilon \implies \left| \frac{f(x) - f(x_0)}{x - x_0} - y_0 \right| < \varepsilon$$

$$(A.1.2) \quad x \in F \text{ e } 0 < |x - x_0| < \delta_\varepsilon \implies \exists f'(x) \text{ e } |f'(x) - y_0| < \varepsilon.$$

Então, existe $f'(x_0)$ e $f'(x_0) = y_0$.

PROVA - Se $x_0 \in \overset{\circ}{F} \cup (I \setminus F)$ o resultado segue facilmente. Suponhamos, então, que $x_0 \in \text{Fr}(F)$. É suficiente provar que, dado $\varepsilon > 0$, existe $\delta > 0$ tal que

$$(A.1.3) \quad \left| \frac{f(x) - f(x_0)}{x - x_0} - y_0 \right| < \varepsilon, \text{ para todo } x \in I \text{ com } 0 < |x - x_0| < \delta.$$

De fato, sejam $\varepsilon > 0$ e $\delta > 0$ tal que $\varepsilon/2 > 0$ verifica (A.1.1) e (A.1.2). Seja $x_1 \in I$ tal que $0 < |x - x_0| < \delta$. Se $x_1 \in F$ então, por (A.1.1), (A.1.3) está satisfeita. Suponhamos que $x_1 \notin F$ e $x_0 < x_1$. Seja $r > 0$ tal que $]x_1 - r, x_1 + r[\subset I \setminus F$ e seja $a = \max\{x \in F : x \leq x_1 - r\}$. Então, por (A.1.2), resulta que

$$(A.1.4) \quad \exists f'(x) \text{ e } |f'(x) - y_0| < \frac{\varepsilon}{2}, \forall x \in]a, x_1[.$$

Seja $x_2 \in]a, x_1[$ tal que $f(x_1) - f(a) = f'(x_2)(x_1 - a)$. Se $a = x_0$, por (A.1.4), tem-se

$$\left| \frac{f(x_1) - f(x_0)}{x_1 - x_0} - y_0 \right| = |f'(x_2) - y_0| < \frac{\varepsilon}{2} < \varepsilon.$$

Suponhamos que $a \neq x_0$ (logo, $x_0 < a < x_1$). Então como

$$a \in F, \quad 0 < |a - x_0| < \delta, \quad |x_1 - a| \leq |x_1 - x_0| \quad \text{e} \quad |a - x_0| \leq |x_1 - x_0|$$

e também como

$$\frac{f(x_1) - f(x_0)}{x_1 - x_0} - y_0 = \frac{x_1 - a}{x_1 - x_0} \left(\frac{f(x_1) - f(a)}{x_1 - a} - y_0 \right) + \frac{a - x_0}{x_1 - x_0} \left(\frac{f(a) - f(x_0)}{a - x_0} - y_0 \right)$$

de (A.1.1) e (A.1.4) vem que

$$\begin{aligned} \left| \frac{f(x_1) - f(x_0)}{x_1 - x_0} - y_0 \right| &\leq \left| \frac{f(x_1) - f(a)}{x_1 - a} - y_0 \right| + \left| \frac{f(a) - f(x_0)}{a - x_0} - y_0 \right| = \\ &= \left| f'(x_2) - y_0 \right| + \left| \frac{f(a) - f(x_0)}{a - x_0} - y_0 \right| < \varepsilon. \end{aligned}$$

Se $x_1 \notin F$ e $x_1 < x_0$, por um argumento similar segue (A.1.3). ■

DEFINIÇÃO A.1.1 - Um cubo fechado (aberto) em $\mathbb{R}^n$ é o produto de n intervalos fechados (abertos) do mesmo comprimento. Se

Q é um cubo em $\mathbb{R}^n$, denotaremos por $\lambda(Q)$ o comprimento da sua aresta.

Observe-se que as faces de cada cubo (fechado ou aberto) em $\mathbb{R}^n$ são paralelos aos hiperplanos de coordenadas.

LEMA A.1.3 - Seja A um subconjunto fechado de $\mathbb{R}^n$. Então, existe uma família $\{K_i: i \in \mathbb{N}\}$ onde cada K_i é uma coleção de cubos fechados em $\mathbb{R}^n$ satisfazendo as seguintes propriedades:

- 1) Se $K = \bigcup_{i \geq 0} K_i$ então $\mathbb{R}^n \setminus A = \bigcup_{Q \in K} Q$.
- 2) $d(Q, A) \geq \sqrt{n} 2^{-i}$, para todo $Q \in K_i$, $i \geq 0$.
- 3) $d(Q, A) < 3\sqrt{n} 2^{-i}$, para todo $Q \in K_i$, $i > 0$.
- 4) Se $Q \in K_i$, $i > 0$, então $\sqrt{n} 2^{-i} \leq d(x, A) < 4\sqrt{n} 2^{-i}$, para todo $x \in Q$.
- 5) Se $Q \in K_i$ e $Q' \in K_j$, com $Q \cap Q' \neq \emptyset$, então $|i - j| \leq 1$.
- 6) Cada $Q \in K_i$, $i \geq 0$, intersecta no máximo 4^n cubos de K . Além disso, se a cada elemento $Q \in K$ associamos o cubo aberto V_Q como mesmo centro que Q e aresta $\lambda(V_Q) = (1 + 1/4)\lambda(Q)$, se denotarmos $V_i = \{V_Q: Q \in K_i\}$ e $V = \{V_Q: Q \in K\}$, tem-se
- 7) Se $Q \in K_i$, $i > 0$, então $d(x, A) < 5\sqrt{n} 2^{-i}$, para todo $x \in V_Q$.
- 8) Se $Q \in K_i$, $i \geq 0$, então $d(V_Q, A) \geq \frac{7}{8} \frac{\sqrt{n}}{2^i}$; em particular, V_Q é disjunto de A .
- 9) Se $Q \in K_i$ e $Q' \in K_j$, com $V_Q \cap V_{Q'} \neq \emptyset$, então $|i - j| \leq 1$.

10) Cada V_Q , $Q \in K$, intersecta no máximo 4^n cubos de V .

PROVA - Dividindo $\mathbb{R}^n$ num reticulado de cubos Q , com $\lambda(Q) = 1$ e vértices de coordenadas inteiras, e denotando por C_0 o conjunto de todos esses cubos tem-se

$$(A.1.5) \quad \mathbb{R}^n = \bigcup_{Q \in C_0} Q.$$

Sejam $K_0 = \{Q \in C_0 : d(Q, A) \geq \sqrt{n}\}$ e $\tilde{K}_0 = C_0 \setminus K_0$. Então, dividindo cada elemento de $\tilde{K}_0$ em 2^n cubos Q com $\lambda(Q) = 1/2$ e denotando por C_1 o conjunto de todos esses cubos consideremos $K_1 = \{Q \in C_1 : d(Q, A) \geq \sqrt{n}/2\}$ e $\tilde{K}_1 = C_1 \setminus K_1$. Em geral, tendo constituído as famílias C_{i-1} e K_{i-1} consideremos $\tilde{K}_{i-1} = C_{i-1} \setminus K_{i-1}$. Então, dividindo cada elemento Q de $\tilde{K}_{i-1}$ em 2^n cubos com aresta $1/2^i$ denotamos por C_i o conjunto de todos esses cubos; isto é,

$$(A.1.6) \quad Q \in C_i \iff (a) \lambda(Q) = 1/2^i$$

$$(b) \text{ os v\u00e9rtices de } Q \text{ pertencem a } \left(\frac{\mathbb{Z}}{2^i}\right)^n.$$

$$(c) \exists Q' \in \tilde{K}_{i-1} : Q \subset Q'.$$

Definimos $K_i = \{Q \in C_i : d(Q, A) \geq \frac{\sqrt{n}}{2^i}\}$ e $\tilde{K}_i = C_i \setminus K_i$. Provaremos que a família $\{K_i : i \in \mathbb{N}\}$, assim construído, satisfaz as condições do lema.

1) Seja $x \in \mathbb{R}^n \setminus A$. Então, por (A.1.5), existe $Q_0 \in \mathcal{C}_0$ tal que $x \in Q_0$. Se $d(Q_0, A) \geq \sqrt{n}$ então $Q_0 \in K_0$ e portanto segue (1). Se $d(Q_0, A) < \sqrt{n}$, dividimos Q_0 em 2^n cubos com aresta $1/2$. Onde, existe Q_1 em $\mathcal{C}_1$ tal que $x \in Q_1$. Novamente, se $d(Q_1, A) \geq \frac{\sqrt{n}}{2}$ então $Q_1 \in K_1$ e assim (1) está verificado. Se $d(Q_1, A) < \frac{\sqrt{n}}{2}$, dividimos Q_1 em 2^n cubos com aresta $1/4$; e assim sucessivamente. Deste modo foi construído uma família $\{Q_i : i \in \mathbb{N}\}$ de cubos tais que $Q_i \in \mathcal{C}_i$ e $x \in Q_i$. Mas, como $d(x, A) > 0$, existe $i \in \mathbb{N}$ tal que $d(x, A) > \sqrt{n} 2^{-i}$. Seja $Q_i \in \mathcal{C}_i$, com $x \in Q_i$, o correspondente cubo construído acima. Se $d(Q_i, A) \geq \frac{\sqrt{n}}{2^i}$ então $Q_i \in K_i$ e portanto (1) está satisfeita. Se $d(Q_i, A) < \frac{\sqrt{n}}{2^i}$, dividimos Q_i em 2^n cubos com aresta $1/2^{i+1}$; logo, existe $Q_{i+1} \in \mathcal{C}_{i+1}$ tal que $x \in Q_{i+1}$ e assim

$$\frac{\sqrt{n}}{2^i} < d(x, A) \leq d(Q_{i+1}, A) + \delta(Q_{i+1}) \leq d(Q_{i+1}, A) + \frac{\sqrt{n}}{2^{i+1}}.$$

Portanto, $d(Q_{i+1}, A) > \frac{\sqrt{n}}{2^i} - \frac{\sqrt{n}}{2^{i+1}} = \frac{\sqrt{n}}{2^{i+1}}$; isto é $Q_{i+1} \in K_{i+1}$ e desta forma $x \in \bigcup_{Q \in K} Q$.

2) É imediato pela definição de K_i .

3) Seja $Q \in K_i$, $i > 0$. Então, por (A.1.6), existe $Q' \in K_{i+1}$ tal que $Q \subset Q'$; mas, por construção, $\lambda(Q') = 1/2^{i-1}$ e $d(Q', A) < \sqrt{n}/2^{i-1}$. Seja $x' \in Q'$ tal que $d(x', A) = d(Q', A)$. Se x é o centro de Q' então $x \in Q$ e $d(x, x') \leq \sqrt{n}/2^i$. Onde

$$d(Q, A) \leq d(x, A) \leq d(x, x') + d(x', A) < \frac{\sqrt{n}}{2^i} + \frac{\sqrt{n}}{2^{i-1}} = 3 \frac{\sqrt{n}}{2^i}.$$

4) Seja $x_0 \in Q$ tal que $d(x_0, A) = d(Q, A)$. Então, por (3), $d(x_0, A) < 3\sqrt{n}2^{-i}$. Logo, para todo $x \in Q$ tem-se $d(x, x_0) \leq \sqrt{n}2^{-i}$ e

$$\frac{\sqrt{n}}{2^i} \leq d(Q, A) \leq d(x, A) \leq d(x, x_0) + d(x_0, A) < \frac{\sqrt{n}}{2^i} + 3 \frac{\sqrt{n}}{2^i} = 4 \frac{\sqrt{n}}{2^i}.$$

5) Por absurdo, suponhamos que $|i-j| > 1$. Se $j > i+1$ então $\frac{\sqrt{n}}{2^j} \leq \frac{\sqrt{n}}{2^{i+2}}$. Seja $x_1 \in (Q \cap Q')$ então, por (2), $d(x_1, A) \geq \frac{\sqrt{n}}{2^i}$; donde, para todo $x \in Q'$, $d(x_1, x) \leq \frac{\sqrt{n}}{2^j} \leq \frac{\sqrt{n}}{2^{i+2}}$ e

$$d(x, A) \geq d(x_1, A) - d(x_1, x) \geq \frac{\sqrt{n}}{2^i} - \frac{\sqrt{n}}{2^{i+2}} = 3 \frac{\sqrt{n}}{2^{i+2}}.$$

Logo, como $j > 0$ a partir de (3), tem-se

$$3 \frac{\sqrt{n}}{2^{i+2}} \leq d(Q', A) < 3 \frac{\sqrt{n}}{2^j} \leq 3 \frac{\sqrt{n}}{2^{i+2}},$$

o que é uma contradição. Se $i > j+1$ raciocinamos de modo análogo.

6) Sejam $Q \in K_i$, $i \geq 0$, e $Q' \in K$ tal que $Q \cap Q' \neq \emptyset$. Se $Q' \in K_j$, $j \geq 0$, por (5), tem-se $|i-j| \leq 1$; donde

$$\frac{1}{2}\lambda(Q) \leq \lambda(Q') \leq 2\lambda(Q).$$

Portanto, é claro que, Q intersecta no máximo 4^n cubos da família K .

7) Seja $y \in Q$ tal que $d(y, A) = d(Q, A)$. Então, por (3), tem-

se

$$d(x,A) \leq d(x,y) + d(y,A) < \frac{5}{4} \frac{\sqrt{n}}{2^i} + 3 \frac{\sqrt{n}}{2^i} < 5 \frac{\sqrt{n}}{2^i}, \text{ para todo } x \in V_Q.$$

8) Sejam $y \in \bar{V}_Q$ e $x \in Q$ tais que $d(y,A) = d(V_Q,A)$ e $d(x,y) \leq \frac{1}{8} \frac{\sqrt{n}}{2^i}$. Então,

$$\frac{\sqrt{n}}{2^i} \leq d(Q,A) \leq d(x,A) \leq d(x,y) + d(y,A) \leq \frac{1}{8} \frac{\sqrt{n}}{2^i} + d(V_Q,A);$$

$$\text{donde, } d(V_Q,A) \geq \frac{\sqrt{n}}{2^i} - \frac{1}{8} \frac{\sqrt{n}}{2^i} = \frac{7}{8} \frac{\sqrt{n}}{2^i}.$$

9) e 10) seguem de modo análogo a (5) e (6) respectivamente. ■

LEMA A.1.4 - Seja A um subconjunto fechado de $\mathbb{R}^n$ e seja $\Omega = \mathbb{R}^n \setminus A$. Então, existe uma sequência de funções $\phi_j \in \mathcal{D}(\Omega)$, $j \in \mathbb{N}$, tal que

$$1) \phi_j(x) \geq 0, \quad j \in \mathbb{N}, \text{ e } \sum_{j \geq 0} \phi_j(x) = 1, \text{ para todo } x \in \Omega.$$

2) se K é um compacto contido em Ω , existe um subconjunto finito J de $\mathbb{N}$ tal que

$$K \cap \text{Supp } \phi_j = \emptyset, \text{ para todo } j \notin J.$$

3) existe uma constante $C > 0$ (independente de j e de A) tal que

$$\delta(\text{Supp } \phi_j) \leq C d(\text{Supp } \phi_j, A), \text{ para todo } j \in \mathbb{N},$$

onde, $\delta(\text{Supp } \phi_j)$ indica o diâmetro de $\text{Supp } \phi_j$.

4) para cada $\alpha \in \mathbb{N}^n$ existe $C_\alpha > 0$ tal que

$$\sum_{j \geq 0} |(D^\alpha \phi_j)(x)| \leq C_\alpha [1 + d(x, A)^{-|\alpha|}], \text{ para todo } x \in \Omega.$$

PROVA - Consideremos a família $K = \{K_i : i \in \mathbb{N}\}$ de cubos fechados em $\mathbb{R}^n$ satisfazendo as condições do Lema A.1.3. Então, ordenando todos esses cubos numa sequência $Q_0, Q_1, \dots$, ve-se que cada Q_j e $V_j = V_{Q_j}$, $j \in \mathbb{N}$, tem a forma

$$Q_j = \{x = (x_1, \dots, x_n) : |x_i - a_{ij}| \leq \frac{1}{2} \lambda_j, 1 \leq i \leq n\}$$

$$V_j = \{x : |x_i - a_{ij}| < (\frac{1}{2} + \frac{1}{8}) \lambda_j, 1 \leq i \leq n\},$$

onde $a_j = (a_{1j}, \dots, a_{nj})$ é o centro de Q_j e λ_j o comprimento da aresta de Q_j . Se

$$Q = \{x : |x_i| \leq \frac{1}{2}, 1 \leq i \leq n\} \text{ e } V = \{x : |x_i| < \frac{1}{2} + \frac{1}{8}, 1 \leq i \leq n\}$$

então, sabemos que, existe uma função $\phi \in \mathcal{D}(\mathbb{R}^n)$ tal que

a) $0 \leq \phi(x) \leq 1$, para todo $x \in \mathbb{R}^n$.

b) $\phi \equiv 1$ em Q .

c) $\text{Supp } \phi \subset V$ (donde, $Q \subset \text{Supp } \phi$).

Para cada $j \in \mathbb{N}$ consideremos as seguintes funções sobre $\mathbb{R}^n$:

$$\psi_j(X) \equiv \phi\left(\frac{X-a_j}{\lambda_j}\right), \quad \psi \equiv \sum_{j \geq 0} \psi_j \quad \text{e} \quad \phi_j \equiv \begin{cases} \frac{\psi_j}{\psi} & \text{em } \Omega \\ 0 & \text{em } A. \end{cases}$$

Então, é claro que, $Q_j \subset \text{Supp } \psi_j \subset V_j$; donde, pelo Lema A.1.3 (8), $\text{Supp } \phi_j \subset \Omega$. Além disso, pelo Lema A.1.3 (10), $\psi_j \equiv 0$ exceto em V_j . Se $x \in \Omega$ então, pelo Lema A.1.3 (1), existe $k = k(x) \geq 0$ tal que $x \in Q_k \subset V_k$ e, pelo Lema A.1.3 (10), V_k intersecta no máximo 4^n cubos V_j . Logo, a cada $x \in \Omega$ podemos associar uma vizinhança V_k de x que intersecta o suporte de no máximo 4^n funções ϕ_j . Portanto: $\psi(x)$ está bem definida para todo $x \in \Omega$, ψ é de classe C^∞ em Ω e

$$(A.1.7) \quad 1 \leq \sum_{j \geq 0} \psi_j(x) \leq 4^n, \quad \text{para todo } x \in \Omega,$$

isto é; (1) está satisfacita. A prova de (2) segue diretamente do Lema A.1.3 (10) e o típico argumento de compacidade.

3) Pelo Lema A.1.3 (8), tem-se $\frac{7}{8} \sqrt{n} \lambda_j \leq d(V_j, A)$ e, é claro que, $\delta(V_j) = \frac{5}{4} \lambda_j$. Então, destes fatos, segue $\delta(V_j) \leq \frac{10}{7} d(V_j, A)$. Portanto,

$$\delta(\text{Supp } \phi_j) \leq \delta(V_j) \leq \frac{10}{7} d(V_j, A) \leq \frac{10}{7} d(\text{Supp } \phi_j, A), \quad \text{para } j \in \mathbb{N}.$$

4) Seja $\alpha \in \mathbb{N}^n$, fixado. Então, para todo $j \in \mathbb{N}$, é claro que

$$(4.1.8) \quad 1 \leq (5\sqrt{n})^{|\alpha|} [1+d(x,A)^{-|\alpha|}], \text{ para todo } x \in \text{Supp } \psi_j.$$

Além disso, pelo Lema A.1.3 (7), tem-se $d(x,A) < 5\sqrt{n}\lambda_j$ para todo $x \in \text{Supp } \psi_j$, desde que $\lambda_j < 1$, pois nesse caso $Q_j \in K_i$, com $i > 0$. Logo,

$$\lambda_j^{-|\alpha|} \leq (5\sqrt{n})^{|\alpha|} [1+d(x,A)^{-|\alpha|}], \text{ para todo } x \in \text{Supp } \psi_j, \text{ se } \lambda_j < 1.$$

Desse fato e (A.1.8), para todo $j \in \mathbb{N}$, obtém-se

$$(A.1.9) \quad \lambda_j^{-|\alpha|} \leq (5\sqrt{n})^{|\alpha|} [1+d(x,A)^{-|\alpha|}], \text{ para todo } x \in \text{Supp } \psi_j.$$

Por outro lado, para cada $(\gamma, j) \in \mathbb{N}^n \times \mathbb{N}$, é fácil ver que

$$(A.1.10) \quad (D^\gamma \psi_j)(x) = \lambda_j^{-|\alpha|} \phi(\gamma) \left(\frac{x-a_j}{\lambda_j} \right), \text{ para todo } x \in \text{Supp } \psi_j.$$

Donde, de (A.1.9) e (A.1.10), para cada $\gamma \in \mathbb{N}^n$ podemos achar uma constante $C_\gamma > 0$ tal que para todo $j \in \mathbb{N}$ vale

$$(A.1.11) \quad |(D^\gamma \psi_j)(x)| \leq C_\gamma [1+d(x,A)^{-|\gamma|}], \text{ para } x \in \text{Supp } \psi_j \text{ (logo, para } x \in \Omega).$$

Portanto, pelo Lema A.1.3 (10), pela definição de ψ e por (A.1.11), tem-se

$$(A.1.12) \quad |(D^\gamma \psi)(x)| \leq C'_\gamma [1+d(x,A)^{-|\gamma|}], \text{ para todo } x \in \Omega \text{ e } \gamma \in \mathbb{N}^n,$$

se tomarmos $C'_\gamma = (1+4^n)C_\gamma$. Agora provaremos que para cada $\gamma \in \mathbb{N}^n$ existe $C''_\gamma > 0$ tal que

$$(A.1.13) \quad |(D^\gamma(\frac{1}{\psi}))(x)| \leq C_Y'' [1+d(x,A)^{-|\gamma|}], \text{ para todo } x \in \Omega.$$

Com efeito, não é difícil verificar por indução que

$$(D^\gamma(\frac{1}{\psi}))(x) = \frac{1}{\psi^{|\gamma|+1}(x)} \sum_{i=1}^{n_Y} d_i \prod_j (D^{\gamma_{ij}} \psi)(x)$$

onde $d_i \in \mathbb{R}$, $\sum_{i,j} |\gamma_{ij}| = |\gamma|$ e $n_Y \in \mathbb{N}$. Se r_i é o número de elementos do conjunto $\{j: \gamma_{ij} \neq 0\}$, por (A.1.7) e (A.1.12), tem-se

$$|(D^\gamma(\frac{1}{\psi}))(x)| \leq \sum_{i=1}^{n_Y} d_i (4^n)^{r_i} \prod_{\gamma_{ij} \neq 0} C_{ij} [1+d(x,A)^{-|\gamma_{ij}|}],$$

e, pelo Lema A.1.1 (2) (aplicado a $d(x,A)^{-1}$), segue (A.1.13) se escolhermos $C_Y'' = n_Y \cdot \max_{1 \leq i \leq n_Y} \{d_i (4^n)^{r_i} \prod_j C_{ij}\}$. Usando o Teorema 0.3.3 e o Lema A.1.1 (1), a partir de (A.1.11) e (A.1.13), é fácil achar uma constante $M_\alpha > 0$ tal que para todo $x \in \text{Supp } \phi_j$, $j \in \mathbb{N}$, vale

$$|(D^\alpha \phi_j)(x)| \leq M_\alpha [1+d(x,A)^{-|\alpha|}], \text{ (logo, para } x \in \Omega).$$

Finalmente, pelo Lema A.1.3 (10) e por este último fato, segue imediatamente (4). ■

OBSERVAÇÃO A.1.1 - Sejam

$$\Omega_1 = \{x \in \mathbb{R}^n: d(x,A) > \frac{5}{2} \sqrt{n}\}$$

$$\Omega_2 = \{x \in \Omega: d(x,A) < \frac{7}{8}\}.$$

Então, valem as seguintes propriedades:

1) $\phi_j \equiv 0$ em Ω_1 para todo $j \in \mathbb{N}$, com $\lambda_j < 1$.

2) $\phi_j \equiv 0$ em Ω_2 para todo $j \in \mathbb{N}$, com $\lambda_j = 1$.

De fato. (1) é consequência direta do Lema A.1.3 (7), pois $d(x, A) < \frac{5}{2} \sqrt{n}$, para todo $x \in \text{Supp } \phi_j$, se $\lambda_j < 1$. Também (2) é imediato a partir do Lema A.1.3 (8), dado que

$$d(\text{Supp } \phi_j, A) \geq \frac{7}{8} \sqrt{n}, \text{ para todo } j \in \mathbb{N}, \text{ com } \lambda_j = 1.$$

OBSERVAÇÃO A.1.2 - Para cada $j \in \mathbb{N}$, seja $x_j \in A$ tal que $d(x_j, \text{Supp } \phi_j) = d(A, \text{Supp } \phi_j)$. Então,

$$(A.1.14) \quad \|x - x_j\| \leq (1+C)d(x, A), \text{ para todo } x \in \text{Supp } \phi_j \text{ e } j \in \mathbb{N},$$

onde $C = \frac{10}{7}$, a constante que aparece no Lema A.1.4 (3). Com efeito, por este lema, para cada $x \in \text{Supp } \phi_j$, $j \in \mathbb{N}$, tem-se

$$\begin{aligned} \|x - x_j\| &\leq \delta(\text{Supp } \phi_j) + d(A, \text{Supp } \phi_j) \leq C d(\text{Supp } \phi_j, A) + d(A, \text{Supp } \phi_j) = \\ &= (1+C)d(A, \text{Supp } \phi_j) \leq (1+C)d(x, A). \end{aligned}$$

A.2 - PROVA DO TEOREMA DE EXTENSÃO DE WHITNEY

Seja A um subconjunto fechado de $\mathbb{R}^n$ e seja $\Omega = \mathbb{R}^n \setminus A$. Consideremos as funções ϕ_j em $\mathcal{D}(\Omega)$, $j \in \mathbb{N}$, satisfazendo as propriedades do Lema A.1.4; além disso, para cada $j \in \mathbb{N}$ seja $x_j \in A$ tal que $d(x_j, \text{Supp } \phi_j) = d(A, \text{Supp } \phi_j)$. Seja $f \in C^m(\mathbb{R}^n)$, $m \geq$

≥ 0 . Então, definimos a função $g: \mathbb{R}^n \longrightarrow \mathbb{R}$ como sendo

$$g(x) = \begin{cases} f(x), & \text{se } x \in A \\ \sum_{\lambda_j < 1} \phi_j(x) f_m(x, x_j), & \text{se } x \in \Omega. \end{cases}$$

É claro que $g \in C^m(\overset{\circ}{A}) \cap C^\infty(\Omega)$. Os elementos considerados acima serão mantidos em todo o que se segue

LEMA A.2.1 - Seja $\alpha \in \mathbb{N}^n$ tal que $|\alpha| \leq m$. Então,

$$\lim_{d(x,a) \rightarrow 0, x \in \Omega} [(D^\alpha g)(x) - (D^\alpha f)(x)] = 0.$$

PROVA - Sejam $x \in \Omega$ e $y \in A$ tais que $d(x, A) < \frac{7}{8}$ e $\|x - y\| = d(x, A)$. Então, pela Observação A.1.1 (2), segue que $\sum_{\lambda_j < 1} \phi_j(x) = \sum_{j \geq 0} \phi_j(x) = 1$; donde

$$g(x) = f_m(x, y) + \sum_{\lambda_j < 1} \phi_j (f_m(x, x_j) - f_m(x, y)),$$

e usando a fórmula de Leibnitz obtém-se

$$\begin{aligned} (A.2.1) \quad (D^\alpha g)(x) &= D_x^\alpha f_m(x, y) + \sum_{\lambda_j < 1} \sum_{\beta + \gamma = \alpha} \binom{\alpha}{\beta} (D^\gamma \phi_j)(x) [D_x^\gamma f_m(x, x_j) - \\ &\quad - D_x^\gamma f_m(x, y)] \end{aligned}$$

o que implica, pela Definição 5.1.1, que

$$(A.2.2) \quad (D^\alpha g)(x) = (D^\alpha f)(x) - D_X^\alpha R_m(x, y) + \sum_{\lambda_j < 1} \sum_{\beta + \gamma = \alpha} \binom{\alpha}{\beta} (D^\beta \phi_j)(x) \times \\ \times [D_X^\gamma R_m(x, y) - D_X^\gamma R_m(x, x_j)].$$

Seja $j \in \mathbb{N}$ tal que $x \in \text{Supp } \phi_j$. É claro que, se x varia num com pacto fixo então ocorre o mesmo com os correspondentes y (idem para as pontas x_j). Logo, pela Observação 5.1.1 e (A.2.2), resulta que

$$(A.2.3) \quad |(D^\alpha g)(x) - (D^\alpha f)(x)| \leq \|x-y\|^{m-|\alpha|} O(\|x-y\|) + \sum_{\lambda_j < 1} \sum_{\beta + \gamma = \alpha} \binom{\alpha}{\beta} \times \\ \times |(D^\beta \phi_j)(x)| [\|x-y\|^{m-|\gamma|} O(\|x-y\|) + \|x-x_j\|^{m-|\gamma|} O(\|x-x_j\|)]$$

Denotemos por Σ_1 e Σ_2 , respectivamente, a primeira e segunda somatória do segundo membro em (A.2.3). Então, pelo Lema A.1.4 (4) e por (A.1.14), tem-se

$$\Sigma_1 \leq \sum_{\beta + \gamma = \alpha} \binom{\alpha}{\beta} C_\beta [1+d(x, A)^{-|\beta|}] d(x, A)^{m-|\gamma|} O(d(x, A)) \\ \Sigma_2 \leq \sum_{\beta + \gamma = \alpha} \binom{\alpha}{\beta} C_\beta [1+d(x, A)^{-|\beta|}] [3d(x, A)]^{m-|\gamma|} O(d(x, A));$$

logo, de (A.2.3) e destas desigualdades, vem que

$$|(D^\alpha g)(x) - (D^\alpha f)(x)| \leq d(x, A)^{m-|\alpha|} O(d(x, A)) + \\ + \sum_{\beta + \gamma = \alpha} M_\beta [1+d(x, A)^{-|\beta|}] d(x, A)^{m-|\gamma|} O(d(x, A)).$$

Finalmente, como cada $m - |\beta + \gamma| = m - |\alpha| \geq 0$ e $|\gamma| \leq m$, segue imediatamente o lema. ■

LEMA A.2.2 - Seja $\alpha \in \mathbb{N}^n$ tal que $|\alpha| \leq m$ e seja $x_0 \in \text{Fr}(A)$. Então, para cada $\varepsilon > 0$ existe $\delta > 0$ tal que

$$(A.2.4) \quad x \in \Omega \text{ e } \|x - x_0\| < \delta \implies |(D^\alpha g)(x) - (D^\alpha f)(x_0)| < \varepsilon.$$

PROVA - Pelo Lema A.2.1, existe $\delta_0 > 0$ tal que

$$x \in \Omega \text{ e } d(x, A) < \delta_0 \implies |(D^\alpha g)(x) - (D^\alpha f)(x)| < \frac{\varepsilon}{2};$$

logo,

$$(A.2.5) \quad x \in \Omega \text{ e } \|x - x_0\| < \delta_0 \implies |(D^\alpha g)(x) - (D^\alpha f)(x)| < \frac{\varepsilon}{2}.$$

Como $D^\alpha f$ é contínua em x_0 , existe $0 < \delta < \delta_0$ tal que

$$(A.2.6) \quad x \in \mathbb{R}^n \text{ e } \|x - x_0\| < \delta \implies |(D^\alpha f)(x) - (D^\alpha f)(x_0)| < \frac{\varepsilon}{2}.$$

Portanto, de (A.2.5) e (A.2.6), segue (A.2.4). ■

A partir deste lema é imediato a seguinte

OBSERVAÇÃO A.2.1 - A função g é contínua em $\mathbb{R}^n$.

Agora já estamos em condições de provar o Teorema de extensão de Whitney. Com efeito, que $g \in C^m(\mathbb{R}^n)$ e a validade de (E_1) será provado por indução finita sobre o número natural m . Para isso, pela Observação A.2.1, basta provar o seguinte

LEMA A.2.3 - Valem as seguintes propriedades:

- 1) existe $g_{x_1}(x)$ para todo $x \in \mathbb{R}^n$.
- 2) $g_{x_1} \equiv f_{x_1}$ em A .
- 3) g_{x_1} é contínua em $\mathbb{R}^n$.

PROVA - Em $\mathring{A} \cup \Omega$ o resultado segue facilmente. Seja $x_0 = (x_1, x_2, \dots, x_n) \in \text{Fr}(A)$, fixado, e seja $F = \{t \in \mathbb{R} : (t, x_2, \dots, x_n) \in A\}$. Então, é claro que, F é um subconjunto fechado de $\mathbb{R}$. Dado $\varepsilon > 0$, acharemos um $\delta > 0$ satisfazendo (A.1.1) e (A.1.2) do Lema A.1.2, onde $f(t) = g(t, x_2, \dots, x_n)$, $t \in \mathbb{R}$. De fato, como existe $f_{x_1}(x_0)$ podemos tomar um $\delta_0 > 0$ tal que

$$(A.2.7) \quad t \in \mathbb{R} \text{ e } 0 < |t - x_1| < \delta_0 \implies \left| \frac{f(t, x_2, \dots, x_n) - f(x_0)}{t - x_1} - f_{x_1}(x_0) \right| < \varepsilon.$$

Além disso, pelo Lema A.2.2, existe $\delta \in]0, \delta_0[$ satisfazendo (A.2.4), para $\alpha = (1, 0, \dots, 0)$. Seja $t \in \mathbb{R}$ tal que $0 < |t - x_1| < \delta$. Se $t \in F$ então $(t, x_2, \dots, x_n) \in A$ e como $g \equiv f$ em A , de (A.2.7), segue que

$$\left| \frac{g(t, x_2, \dots, x_n) - g(x_0)}{t - x_1} - f_{x_1}(x_0) \right| < \varepsilon, \text{ (i.e., vale (A.1.1))}.$$

Se $t \notin F$ então $(t, x_2, \dots, x_n) \in \Omega$; logo, por (A.2.4), existe

$$g_{x_1}(t, x_2, \dots, x_n) \text{ e } |g_{x_1}(t, x_2, \dots, x_n) - f_{x_1}(x_0)| < \varepsilon, \text{ (i.e., vale (A.2.2))}.$$

Portanto, pelo Lema A.1.2, existe $g_{x_1}(x_0)$ e $g_{x_1}(x_0) = f_{x_1}(x_0)$; o que também prova (usando (A.2.4)) que g_{x_1} é contínua em x_0 . ■

Observe-se que valem as propriedades do lema anterior para qualquer derivada D^α , com $|\alpha| \leq m$, e a prova é a mesma que se fez acima.

Provaremos $E_2)$ por meio do

LEMA A.2.4 - Existe uma constante $C > 0$ (que não depende de f) tal que

$$E_2) \quad |D^m g, x| \leq C |D^m f, A_x|, \text{ para todo } x \in \mathbb{R}^n.$$

PROVA - Pela Observação A.1.1, segue que $g \equiv 0$ em Ω_1 ; donde, vale $E_2)$ com qualquer $C > 0$ (em Ω_1). Portanto, resta provar (E_2) em $\mathbb{R}^n \setminus \Omega_1$. De fato, seja $x \in \mathbb{R}^n \setminus \Omega_1$, fixado, e seja $y \in A$ tal que $\|x - y\| = d(x, A)$; logo, $d(x, A) \leq \frac{5}{2} \sqrt{n}$ e, é claro que, $y \in A_x$. Seja $j \in \mathbb{N}$ tal que $x \in \text{Supp } \phi_j$. Então, pela Observação A.1.2; x satisfaz (A.1.14) e portanto $x_j \in A_x$. Seja $\alpha \in \mathbb{N}^n$, com $|\alpha| \leq m$, fixado. Suponhamos primeiro que $d(x, A) \geq 1$. Pela definição de g tem-se

$$(A.2.8) \quad (D^\alpha g)(x) = \sum_{\lambda_j < 1} \sum_{\beta + \gamma = \alpha} \binom{\alpha}{\beta} (D^\beta \phi_j)(x) D_x^\gamma f_m(x, x_j).$$

Além disso, pela Definição 5.1.1, para todo $z \in \mathbb{R}^n$ vale

$$(A.2.9) \quad D_{x_m}^{\gamma} f_m(x, z) = \sum_{|\lambda| \leq m - |\gamma|} (D^{\lambda + \gamma} f)(z) \frac{(x-z)^{\lambda}}{\lambda!}, \text{ para } \gamma \in \mathbb{N}^n \text{ com } |\gamma| \leq m;$$

logo, é claro que, existe uma constante $C_m > 0$ tal que

$$(A.2.10) \quad |D_{x_m}^{\gamma} f_m(x, z)| \leq C_m |D^m f, A_x|, \text{ para } z \in A_x \text{ e } \gamma \in \mathbb{N}^n, \text{ com } |\gamma| \leq m.$$

Mas $x_j \in A_x$ e portanto, pelo Lema A.1.4 (4), (A.2.8) e por (A.2.10), resulta que

$$|(D^{\alpha} g)(x)| \leq |D^m f, A_x| \sum_{\beta \leq \alpha} C_m C_{\beta} \binom{\alpha}{\beta} [1 + d(x, A)^{-|\beta|}]$$

e como $d(x, A) \geq 1$ podemos achar $M_1 > 0$ tal que

$$(A.2.11) \quad |(D^{\alpha} g)(x)| \leq M_1 |D^m f, A_x|.$$

Suponhamos agora que $d(x, A) < 1$. Neste caso, para obter (E_2) , usaremos a fórmula (A.2.1) e para isso estimaremos primeiro cada diferença

$$|D_{x_m}^{\gamma} f_m(x, x_j) - D_{x_m}^{\gamma} f_m(x, y)|.$$

Pela Definição 5.1.1 e por (A.2.9), tem-se

$$(A.2.12) \quad D_{x_m}^{\gamma} f_m(x, x_j) = \sum_{|\lambda| \leq m - |\gamma|} (D^{\gamma + \lambda} f_m(x_j, y) + D_{x_m}^{\gamma + \lambda} R_m(x_j, y)) \frac{(x - x_j)^{\lambda}}{\lambda!}.$$

Denotando por Σ_1 a primeira soma parcial, em (A.2.12), vem que

$$\begin{aligned}
 \sum_1 &= \sum_{|\lambda| \leq m-|\gamma|} \frac{1}{\lambda!} \sum_{|r| \leq m-|\gamma+\lambda|} (D^{\gamma+\lambda+r} f)(y) \frac{(x_j-y)^r}{r!} (x-x_j)^\lambda = \\
 &= \sum_{|\beta| \leq m-|\gamma|} (D^{\beta+\gamma} f)(y) \frac{1}{\beta!} \left[\sum_{\lambda \leq \beta} \binom{\beta}{\lambda} (x_j-y)^{\beta-\lambda} (x-x_j)^\lambda \right] = \\
 &= \sum_{|\beta| \leq m-|\gamma|} (D^{\beta+\gamma} f)(y) \frac{(x-y)^\beta}{\beta!} = D_x^\gamma f_m(x,y),
 \end{aligned}$$

substituindo $\sum_1 = D_x^\gamma f_m(x,y)$ em (A.2.12) segue que

$$(A.2.13) \quad D_x^\gamma f_m(x, x_j) - D_x^\gamma f_m(x, y) = \sum_{|\lambda| \leq m-|\gamma|} D_x^{\lambda+\gamma} R_m(x_j, y) \frac{(x-x_j)^\lambda}{\lambda!}.$$

Por outro lado, como $y, x_j \in A$, pela Definição 5.1.2 tem-se

$$(A.2.14) \quad |D_x^{\lambda+\gamma} R_m(x_j, y)| \leq \|x_j - y\|^{m-|\lambda+\gamma|} |D^m f, A_x|;$$

além disso, usando (A.1.14), segue facilmente que

$$(A.2.15) \quad \|x_j - y\| \leq (2+C)d(x, A), \quad C = \frac{10}{7}.$$

Logo, de (A.1.14), (A.2.13), (A.2.14) e (A.2.15), conclui-se

$$|D_x^\gamma f_m(x, x_j) - D_x^\gamma f_m(x, y)| \leq |D^m f, A_x| \sum_{|\lambda+\gamma| \leq m} \frac{1}{\lambda!} [(2+C)d(x, A)]^{m-|\lambda+\gamma|+|\lambda|};$$

donde, para uma constante conveniente $C_\gamma > 0$, tem-se

$$(A.2.16) \quad |D_x^\gamma f_m(x, x_j) - D_x^\gamma f_m(x, y)| \leq C_\gamma |D^m f, A_x| d(x, A)^{m-|\gamma|}.$$

Denotando por $\sum_2$ a somatória em (A.2.1) e usando o Lema A.1.4 (4), a partir de (A.2.16), obtém-se

$$\begin{aligned} |\sum_2| &\leq |D^m f, A_x| \sum_{\lambda_j < 1} \sum_{\beta + \gamma = \alpha} C_\gamma \binom{\alpha}{\beta} |(D^\beta \phi_j)(x)| \leq \\ &\leq |D^m f, A_x| \sum_{\beta + \gamma = \alpha} C_\gamma C_\beta [d(x, A)^{m-|\gamma|} + d(x, A)^{m-|\beta+\gamma|}], \end{aligned}$$

mas, como $|\alpha| \leq m$, $|\gamma| \leq m$ e $d(x, A) < 1$, podemos achar uma constante $M > 0$ tal que

$$(A.2.17) \quad |\sum_2| \leq M |D^m f, A_x|.$$

Portanto, de (A.2.1), (A.2.10) (pois $y \in A_x$ e $|\alpha| \leq m$) e de (A.2.17), segue facilmente que

$$(A.2.18) \quad |(D^\alpha g)(x)| \leq M_2 |D^m f, A_x|,$$

onde $M_2 > 0$ é uma constante conveniente.

Finalmente, sendo $\alpha \in \mathbb{N}^n$ (com $|\alpha| \leq m$) arbitrário, pela Definição 5.1.2, por (A.2.11) e por (A.2.18), segue imediatamente (E_2) . ■

BIBLIOGRAFIA

- [1] - Ahlfors, L. - *Complex Analysis*, McGraw-Hill, 1966.
- [2] - Chaillow, J. - *Les polynômes différentiels hyperboliques et leurs perturbations singulières*, Gauthier-Villars Editeur, 1973.
- [3] - Figueiredo D. e Treves F. - *Espaços vetoriais topológicos e distribuições*, Notas de Matemática n° 41, IMPA, 1968.
- [4] - Friedman, A. - *Generalized functions and partial differential equations*, Prentice-Hall, Inc., 1963.
- [5] - Gilioli, A. - *Equações diferenciais parciais elípticas*, 10º Colóquio Brasileiro de Matemática, 1975.
- [6] - Gorin, E. - "Asymptotic properties of polynomials and algebraic functions of several variables", *Uspekhi Mat. Nauk*, SSSR, 16: 1 (1961), 91-118.
- [7] - Hörmander, L. - *Linear partial differential operators*, Springer-Verlag, 1973.
- [8] - Hörmander, L. - "On the division problem of distributions by polynomials", *Arkiv för Matematik*, 3 (1958), 555-568.
- [9] - Monteiro, L.H. - *Elementos de álgebra*, Ao Livro Técnico, 1971.
- [10] - Monteiro, L.H. - *Polinômios-Divisibilidade*, Publicações do GEEM-SP, 1971.
- [11] - Markushevich A. I. - *Teoría de las funciones analíticas*, MIR, 1970.

- [12] - Rivera, P.H. - *Introducción a la teoría de las distribuciones*,
Tex. de Met. Mat., 6, Instituto de Matemática, UFRJ, 1974.
- [13] - Saks S. & Sygmund, A. - *Analytic functions*, Elsevier Publishing
Company, 1971.
- [14] - Seidenberg, A. - "A new decision method for elementary algebra",
Am. of Math. Ser. 2, 60 (1954), 365-374.
- [15] - Treves, F. - *Linear partial differential operators with constant
coefficients*, Gordon & Brach, 1966.
- [16] - Van der Waeden, B.L. - *Modern algebra*, Springer-Verlag, 1970.
- [17] - Walker, R. - *Algebraic curves*, Princeton University Press, 1950.
- [18] - Whitney, H. - "Analytic extensions of differentiable functions
defined in closed sets", *Trans. Amer. Math. Soc.*, 36 (1934), 63-
-89.
- [19] - Yosida, K. - *Functional analysis*, Springer-Verlag, 1966.