Universidade Federal de Minas Gerais

Departamento de Matemática - Seminário de Álgebra

Tópicos em Equações Diofantinas

Wodson Mendson

1 Introdução

Sejam k um corpo e $F(X_1, ..., X_n) \in k[X_1, ..., X_n]$ homogêneo de grau d. Denote por $X_F(k)$ o conjunto dos k - pontos de F, exceto o trivial, i.e. conjunto dos pontos $(0, ..., 0) \neq (\alpha_1, ...\alpha_n) \in k^n$ tal que $F(\alpha) = 0$. Surgem naturalmente as seguintes perguntas:

- $\#X_F(k) \neq 0$?
- $X_F(k)$ é finito?

Responder as questões acima é uma tarefa um tanto pouco "complicada". De fato, isso depende da natureza do corpo k e do polinômio F em questão. Por exemplo, se fixarmos $k = \mathbb{Q}$ e considerarmos a equação $F = X^2 + Y^2 - 3Z^2$ é fácil verificar, via redução módulo primo, que $\#X_F(k) = 0$. Agora, se $G = X^2 + Y^2 - Z^2$ notemos que $(1, 0, 1) \in X_G(k)$ de modo que $\#X_G(k) \geq 1$. Ainda, se tomarmos $F = X^4 + Y^4 + Z^4$ notamos que $\#X_F(\mathbb{R}) = 0$ enquanto $X_F(\mathbb{C})$ é um conjunto infinito.

O objetivo do texto consiste em estudar uma classe de corpos que possuem a seguinte propriedade: Se $F(X_1, ..., X_n) \in k[X_1, ..., X_n]$ é homogêneo com n "grande" se comparado ao grau então $\#X_F(k) \geq 1$.

2 Caso em que k é algebricamente fechado

Em todo o texto, a palavra anel significa anel comutativo com unidade.

Sejam k um corpo algebricamente fechado e $\mathbb{A}_k^n := \{(\alpha_1, ..., \alpha_n) \mid \alpha_i \in k\}$ o n-espaço afim sobre k. Podemos equipar $\mathbb{A}_k^n$ com uma topologia (ver proposição abaixo) dizendo que um subconjunto X é fechado se existe um ideal $I \subset k[X_1, ..., X_n]$ tal que $X = Z(I) := \{(\alpha_1, ..., \alpha_n) \in \mathbb{A}_k^n \mid F(\alpha_1, ..., \alpha_n) = 0 \quad \forall F \in I\}$. Tal topologia é chamada de **topologia de Zariski**. Dado um conjunto arbitrário $S \subset \mathbb{A}_k^n$ temos associado o ideal $\mathcal{I}(S) := \{f \in k[X_1, ..., X_n] \mid f(P) = 0 \quad \forall P \in S\}$.

Exemplo 1. *Suponha que $S \subset \mathbb{A}_k^n$ é um conjunto arbitrário. Denote por $\overline{S}$ o fecho de S em $\mathbb{A}_k^n$. Então, $\overline{S} = Z(\mathcal{I}(S))$.*

Exemplo 2. *Seja X um fechado de $\mathbb{A}_k^1$ não trivial i.e. $X \neq \varnothing, \mathbb{A}_k^1$. Então, X é finito.*

Proposição 1. *Sejam $X = Z(I)$ e $Y = Z(J)$ fechados em $\mathbb{A}_k^n$. Então,*

(i) $X \subset Y \iff \mathcal{I}(Y) \subset \mathcal{I}(X)$.

(ii) $\bigcap_{\alpha \in T} Z(I_\alpha) = Z(\sum_\alpha I_\alpha)$.

(iii) $X \cup Y = Z(I) \cup Z(J) = Z(IJ)$.

(iv) $Z(1) = \varnothing$ *e* $Z(0) = \mathbb{A}_k^n$.

Seja R um anel e $S \subset R$ um sistema multiplicativo i.e. $1 \in S$ e $x, y \in S \Longrightarrow xy \in S$. Defina

$$S^{-1}R := \{(a, s) \mid a \in R \text{ e } s \in S\}/\sim .$$

onde declaramos $(a, s) \sim (b, t)$ se e só se existir $u \in S$ tal que $u(at - bs) = 0$. Denotaremos por $\frac{a}{s}$ a classe de equivalência de (a, s). É rotineiro verificar, que $S^{-1}R$ é um anel comutativo com 1 munido das operações:

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st} \quad \text{e} \quad \frac{a}{s}\frac{b}{t} := \frac{ab}{st}.$$

Chamamos $S^{-1}R$ de a localização de R pelo sistema multiplicativo S. Existe um homomorfismo natural

$$i_S : R \longrightarrow S^{-1}R \qquad a \mapsto \frac{a}{1}.$$

Se R é um dominio temos que i_S é injetivo, mas em geral i_S não é injetivo.

Seja $P \subset R$ um ideal primo e considere $S := R - P$. Como P é primo temos que S é multiplicativo. Nesse caso, denotamos $S^{-1}R$ por R_P. Observe que R_P é um anel local com ideal maximal PR_P, o ideal gerado por $i_S(P)$. Para ver isso seja $u \in R - PR_P$. Então, temos $u = a/s$ com $a \notin P$. Em particular, $a/1$ é unidade em R_P. Assim, $R_P^* = R_P - PR_P$. [1]

Definição 1. *Seja R um anel.*

- $Spec(R) := \{P \subset R \mid P \text{ é um ideal primo }\}$.
- $Spec_m(R) := \{P \in Spec(R) \mid P \text{ é um ideal maximal }\}$.
- $\dim R := \textbf{\textit{Sup}}\{n \in \mathbb{N} \mid \text{ existe uma cadeia de primos } p_0 \subset p_1 \subset \cdots \subset p_n\}$
- *altura de um ideal primo $P \in Spec(R)$: $ht(P) := \dim R_P$.*

Proposição 2. *Existe uma bijeção*

$$\{\ P \in Spec(R) \mid \text{com } S \cap P = \varnothing\ \} \cong Spec(S^{-1}R).$$

Demonstração. A bijeção é dada pelo mapa i_S. Mais precisamente, se $Q \in S^{-1}R$ é ideal primo então temos $P = i_S^{-1}(Q)$ um ideal primo com $P \cap S = \varnothing$. Dado $P \in Spec(R)$ com $P \cap S = \varnothing$ temos $Q = i_S(P)S^{-1}R$ um ideal primo. Mais detalhes podem ser encontrados no cap 3 de [2].

□

Relembramos alguns resultados importantes de algebra comutativa:

Nullstelensatz Fraco. *Seja k corpo algebricamente fechado. Então, todo ideal $\mathcal{M}$ maximal de $k[X_1, ..., X_n]$ é da forma*

$$\mathcal{M} = (X_1 - u_1, ..., X_n - u_n)$$

por alguns $u_1, ..., u_n \in k$.

Sejam R um anel e $I \subset R$ um ideal. O radical de I consiste no seguinte conjunto

$$\sqrt{I} := \{f \in I \mid f^n \in I\}.$$

Pode-se mostrar que $\sqrt{I}$ é um ideal.

[1] lembre-se: A é local com ideal único ideal maximal $\mathcal{M}$ se e somente se $A^* = A - \mathcal{M}$.

Nullstelensatz. *Seja $X \subset \mathbb{A}_k^n$ um fechado descrito por um ideal I. Então,*

$$\sqrt{I} = \mathcal{I}(X)$$

Demonstração. Observe que a inclusão $\subset$ é trivial. Para a outra inclusão consulte [1].

□

Seja R um anel local noetheriano com ideal maximal $\mathcal{M}$ e corpo residual k. Defina $e(R) := \mathbf{Min}\{n \in \mathbb{N} \mid \exists a_1, ..., a_n \in R \text{ tal que } \sqrt{(a_1, ..., a_n)} = \mathcal{M}\}$. Se $a_1, ..., a_n \in R$ são tais que $\sqrt{(a_1, ..., a_n)} = \mathcal{M}$ dizemos que $a_1, ..., a_n$ formam um sistema de parâmetros para R.

Teorema da Dimensão. *Seja $(R, \mathcal{M}, k)$ um anel local noetheriano. Então,*

$$\dim R = e(R).$$

Demonstração. Para uma prova, veja [2].

□

Observação 1. *Sejam k um corpo e $F_1, ..., F_r \in k[X_1, ..., X_n]$ polinômios lineares i.e. $F_j = \sum_i A_{ij}X_i$ por alguns coeficientes $A_{ij} \in k$ com $1 \leq i \leq n$ e $1 \leq j \leq r < n$. Suponha que a matriz $(A_{ij}) \in \mathcal{M}_{rn}(k)$ tenha posto maximo, com as r-primeiras colunas l.i. Considere $X = Z(F_1, ..., F_r)$ [2], o conjunto dos zeros em $\mathbb{A}_k^n$. Por meio de transformações elementares temos que $X = Z(X_1 - \sum_{p=r+1}^{n-r} B_{1p}X_p, ..., X_r - \sum_{p=r+1}^{n-r} B_{rp}X_p) \subset \mathbb{A}_k^n$ para alguns $B_{ip} \in k$. Em particular, X é um conjunto infinito. Agora, note que se $A \in \mathcal{M}_n(k)$ não é singular e $F_1, ..., F_n$ são polinômios lineares obtidos pelas linhas de A então $Z(F_1, ..., F_n) = \{(0, ..., 0)\}$.*

Nessa direção, temos o seguinte

Teorema 1. *Sejam k corpo algebricamente fechado e $X = Z(I)$ um fechado em $\mathbb{A}_k^n$ onde $I = (F_1, ..., F_r)$. Suponha que $F_1(\alpha) = \cdots = F_r(\alpha) = 0$ para algum $\alpha \in \mathbb{A}_k^n$. Se $n > r$ então X é um conjunto infinito.*

Para demonstrar o teorema acima, usaremos o seguinte

Teorema 2. ***(Ideal Principal de Krull)*** *Seja A um anel noetheriano e $I = (a_1, ..., a_r) \subsetneq A$ um ideal. Seja $P \in Spec(A)$ um primo minimal sobre I. Então, $ht(P) \leq r$.*

Demonstração. Considere o anel $R = A_P$ (localização sobre o sistema multiplicativo $S = A - P$). Por extensão, obtemos um ideal $IA_P \subset A_P$ que está contido no ideal maximal PA_P. Além disso, se Q é um ideal primo de R contendo IA_P por propriedades de localização, obtemos um primo em A que contem I e que está contido em P. Por minimalidade de P sobre I temos que $Q = P$. Assim, PA_P é o único primo contendo IA_P. Como $\sqrt{IA_P} = \bigcap_{P \in V(I)} P$ onde $V(I) = \{Q \in Spec(R) \mid Q \supset IA_P\}$ temos que $\sqrt{IA_P} = PA_P$. Aplicando o teorema da dimensão, vem $ht(P) = \dim A_P \leq r$.

□

Observação 2. *Seja $\mathcal{M}$ um ideal maximal de $k[X_1, ..., X_n]$, com $k = \overline{k}$ (i.e k algebricamente fechado). Por Nullstelensatz, temos $\mathcal{M} = (X_1 - \alpha, ..., X_n - \alpha_n)$ para algum $(\alpha_1, ...\alpha_n) \in k^n$. Em particular,*

$$(0) \subset (X_1 - \alpha) \subset (X_1 - \alpha_1, X_2 - \alpha_2) \subset \cdots \subset (X_1 - \alpha_1, ..., X_n - \alpha_n).$$

Assim, $ht(\mathcal{M}) \geq n$. Pelo teorema acima concluímos que $ht(\mathcal{M}) = n$ para qualquer ideal maximal de $k[X_1, ..., X_n]$.

[2] $Z(F_1, ..., F_r) := \{\alpha \in k^n \mid F_1(\alpha) = \cdots = F_r(\alpha) = 0\}$

Demonstração. (**do teorema 2**) Suponha que tal não ocorra i.e. suponha $X = Z(I) = \{P_1, ..., P_s\}$ com $P_i = (\alpha_1^{(i)}, ..., \alpha_n^{(i)})$ e $I = (F_1, ..., F_r)$. Considere $\mathcal{M}_i := (X_1 - \alpha_1^{(i)}, ..., X_n - \alpha_n^{(i)})$ o ideal maximal associado a P_i. Defina $\mathcal{M} = \prod_{i=1}^{s} \mathcal{M}_i$. Então, $Z(\mathcal{M}) = Z(\prod_i \mathcal{M}_i) = \{P_1, ..., P_s\}$. Pela proposição acima e por **Nullstelensatz** temos que $\sqrt{I} = \sqrt{\mathcal{M}}$. Seja $P \in k[X_1, ..., X_n]$ um primo minimal sobre I. Então, $P \supset \sqrt{I} = \sqrt{\mathcal{M}} = \prod \mathcal{M}_i \Longrightarrow P \supset \mathcal{M}_i$ por algum i. Por maximalidade $P = \mathcal{M}_i$ por algum i. Agora, pelo teorema do ideal principal de Krull, temos que para qualquer primo Q minimal sobre $I = (F_1, ..., F_r)$ temos $ht(Q) \leq r$. Em particular, $ht(P) \leq r < n$, o que é um absurdo.

□

Corolário 1. *Sejam k um corpo algebricamente fechado e $F_1, ..., F_r \in k[X_1, ..., X_n]$ polinômios homogêneos com $n > r$. Então, o sistema*

$$F_1 = F_2 = \cdots = F_r = 0$$

tem uma solução não trivial em k.

3 Corpos de tipo C_i

Seja k um corpo e $F \in k[X_1, ..., X_n]$ um polinômio sem termo constante. Definimos o conjunto dos k-pontos de F pondo

$$X_F(k) := \{(\alpha_1, ..., \alpha_n) \in k^n \mid F(\alpha_1, ..., \alpha_n) = 0\} - \{(0, ..., 0)\}.$$

Definição 2. *Seja k um corpo e $i \in \mathbb{N}$. Dizemos que k é do tipo C_i (ou é C_i) se satisfaz a seguinte propriedade*

- *Para todo polinômio homogêneo $F \in k[X_1, ..., X_n]$ de grau d com $n > d^i$ então $\#X_F(k) \geq 1$.*

Observação 3. *k é do tipo C_0 se e somente se $\overline{k} = k$.*

Lema 1. *Seja $m \in \mathbb{N}$. Então,*

(i) $q - 1 \mid m \Longrightarrow \sum_{\alpha \in \mathbb{F}_q} \alpha^m = -1$.

(ii) $q - 1 \nmid m \Longrightarrow \sum_{\alpha \in \mathbb{F}_q} \alpha^m = 0$.

Demonstração. Considere o mapa $\phi : \mathbb{F}_q^* \longrightarrow \mathbb{F}_q^*$ que associa $u \mapsto u^m$. Observe que ϕ é um mapa de grupos. Note que se $q - 1 \nmid m$ e $g \in \mathbb{F}_q^*$ denota o gerador do grupo $\mathbb{F}_q^*$ então $g^m \neq 1$. Nesse caso,

$$g^m \sum_{\alpha \in \mathbb{F}_q} \alpha^m = \sum_{\alpha \in \mathbb{F}_q} (g\alpha)^m = \sum_{\alpha \in \mathbb{F}_q} \alpha^m$$

e dai $\sum_{\alpha \in \mathbb{F}_q} \alpha = 0$. Agora, se $q - 1 \mid m$ sabemos que

$$\sum_{\alpha \in \mathbb{F}_q} \alpha^m = \sum_{\alpha \in \mathbb{F}_q^*} \alpha^m = \sum_{\alpha \in \mathbb{F}_q^*} 1 = (q-1).1 = -1.$$

□

Nosso próximo objetivo consiste em mostrar que um corpo finito $\mathbb{F}_q$ é do tipo C_1. Para isso, demonstraremos um resultado mais forte.

Teorema 3. ***(Chevalley - Warning)*** *Sejam $\mathbb{F}_q$ corpo finito de característica p e $F_1, ..., F_t \in \mathbb{F}_q[X_1, ..., X_n]$. Defina $d_i := deg(F_i)$ (grau total) e suponha que*

$$d := d_1 + \cdots + d_t < n.$$

Denote $N := \#Z(F_1, ..., F_t)$. Então,

$$N \equiv 0 \mod p.$$

Demonstração. Para cada $i \in \{1, ..., t\}$ defina $G_i \in \mathbb{F}_q[X_1, ..., X_n]$ pondo

$$G_i := 1 - F_i^{q-1}.$$

Sejam $G := \prod_i G_i$ e $Z := Z(F_1, ..., F_t)$. Note que dado $P \in \mathbb{F}_q^n$:

$$G(P) = \begin{cases} 0 & \text{se } P \notin Z. \\ 1 & \text{se } P \in Z. \end{cases}$$

Assim, $N = \sum_{P \in \mathbb{F}_q^n} G(P)$. Observe que G é um polinômio de grau $d(q-1) < n(q-1)$. Seja $M = \beta X_1^{a_1} \cdots X_n^{a_n}$ um monômio ocorrendo em G. É suficiente mostrar que

$$\sum_{P \in \mathbb{F}_q^n} M(P) = 0 \text{ em } \mathbb{F}_q \ .$$

Agora, $\sum_{P \in \mathbb{F}_q^n} M(P) = \sum_{P \in \mathbb{F}_q^n} \prod_j x_j^{a_j} = \prod_{j=1}^n \sum_{x_j \in \mathbb{F}_q} x_j^{a_j}$. A condição $d(q-1) < n(q-1)$ implica que $q-1$ não divide a_j, por algum j. Aplicando o lema acima, vemos que $\sum_{x_j \in \mathbb{F}_q} x_j^{a_j} = 0$ em $\mathbb{F}_q$. Assim, $\sum_{P \in \mathbb{F}_q^n} M(P) = 0$ em $\mathbb{F}_q$.

□

Observação 4. *A cota $n > d$ não pode ser "refinada". Mais precisamente, para cada $n \in \mathbb{N}$ existe uma forma $F \in \mathbb{F}_q[X_1, ..., X_n]$ de grau n tal que $\#Z(F) = 1$. Com efeito, dado n tome $\mathbb{F}_{q^n}$ e fixe $S := \{w_1, ..., w_n\}$ uma $\mathbb{F}_q$-base de $\mathbb{F}_{q^n}$. Sejam $X_1, ..., X_n$ indeterminadas e considere*

$$F(X_1, ..., X_n) := \prod_{\sigma \in Gal(\mathbb{F}_{q^n}/\mathbb{F}_q)} (w_1^\sigma X_1 + \cdots + w_n^\sigma X_n).$$

Por construção, $F \in \mathbb{F}_q[X_1, ..., X_n]$. Se $0 \neq \alpha = \alpha_1 w_1 + \cdots + \alpha_n w_n \in \mathbb{F}_{q^n}$ temos que $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\alpha) = F(\alpha)$. Assim, [3] $F(\alpha) = 0 \iff \alpha = 0$.

Corolário 2. *Seja $F \in \mathbb{F}_q[X_1, ..., X_n]$ homogêneo de grau d com $n > d$. Denote N o inteiro como definido acima. Então, $N \geq 2$.*

Demonstração. Pelo teorema acima, $N \equiv 0 \mod p$. Como $F(0, ..., 0) = 0$ e $p > 1$ temos $N \geq 2$.

□

Corolário 3. *Seja k um corpo finito. Então, k é um corpo do tipo C_1.*

[3] Seja K/k extensão finita galoisiana com $Gal(K/k) = \{\sigma_1, ...\sigma_n\}$. A norma de α é o determinante do mapa $T : K \longrightarrow K \quad \beta \mapsto \alpha\beta$. Pode ser mostrado que tal determinante coincide com $\prod_j \sigma_j(\alpha)$.

Definição 3. *Sejam k um corpo e $P(X_1, ..., X_n) \in k[X_1, ..., X_n]$ homogêneo de grau d. Dizemos que F é uma* ***forma nórmica de ordem*** *i se $n = d^i$ e $\#X_F(k) = 0$ i.e. único zero de F é o trivial $(0, ..., 0)$. Se $i = 1$ diremos, simplesmente que P é uma forma nórmica.*

A terminologia é explicada pela seguinte proposição

Proposição 3. *Seja L/K uma extensão de corpos de grau $n = [L : K] > 1$. Então, existe $F \in K[X_1, ..., X_n]$ uma forma nórmica.*

Demonstração. Sejam $S = \{e_1, ..., e_n\}$ uma K-base de L e $\alpha = X_1e_1 + \cdots + X_ne_n$ um elemento genérico de L. Considere o mapa K-linear $T : E \longrightarrow E$ dado pela multiplicação por α. Defina $P(X_1, ..., X_n) := det([T])$, onde $[T]$ é a matriz associada ao mapa T (com respeito a base V). Temos que $P(Z_1, ..., Z_n) \in K[Z_1, ..., Z_n]$ é um polinômio homogêneo de grau n com $(0, ..., 0)$, único zero em L i.e. é uma forma nórmica.

□

Proposição 4. *Sejam k um corpo não algebricamente fechado. Então, existem formas normicas de grau arbitrariarmente grande.*

Demonstração. Seja L/k uma extensão algébrica de grau $n > 1$ e considere $P \in k[X_1, ..., X_n]$ uma forma nórmica de ordem 1. Considere $P_1 := P(P, ..., P)$ e $P_2 = P_1(P, ..., P)$, onde em cada ocorrência de P introduzimos n-variáveis "novas". Note que P_1 é um polinômio homogêneo de grau $deg(P)^2$ e $deg(P_2) = deg(P_1)deg(P) = deg(P)^3$. Além disso, P_1 e P_2 são formas nórmicas. Repetindo o argumento, vemos que para cada $m \in \mathbb{N}$ construímos uma forma nórmica de grau $deg(P)^m$.

□

Teorema 4. *(Nagata-Lang) Seja k um corpo C_i. Sejam $F_1, ..., F_r \in k[X_1, ..., X_n]$ homogêneos de grau d. Se $n > rd^i$ então $F_1, ..., F_r$ tem um zero não trivial.*

Demonstração. Se k é algebricamente fechado (i.e. C_0) então o resultado é o teorema 1. Assim, podemos supor que k é não algebricamente fechado. Seja $N \in k[X_1, ..., X_e]$ uma forma nórmica de grau e (vide propo. 3).

Se k é do tipo C_1 defina

$$N_1 = N(F_1, ..., F_r \mid F_1, ..., F_r \mid \cdots \mid F_1, ..., F_r \mid 0, 0..., 0) \in k[X_1, ..., X_{n[\frac{e}{r}]}].$$

onde em cada bloco de tamanho r introduzimos n-variáveis "novas". Assim, temos que N_1 é um polinômio homogêneo de grau de com $n[\frac{e}{r}]$ variáveis [4]. Agora, note que $de \leq dr([e/r] + 1)$. Suponha que e é escolhido de tal forma que $n[\frac{e}{r}] > dr([e/r] + 1)$. Nesse caso, $n[e/r] > de$ e dai segue que existe $(u_1, ..., u_{n[e/r]}) \in k^{n[e/r]}$ zero não trivial de N_1. Como N é nórmico, temos $(u_{i_1}, ..., u_{i_n})$ um zero não trivial de $F_1, ..., F_r$, para alguns $i_1, ..., i_n \in \mathbb{N}$.

Suponha agora, que k é um corpo do tipo C_i $(i > 1)$ e $F_1, ..., F_r \in k[X_1, ..., X_n]$ com $n > rd^i$. Seja N uma forma nórmica de grau e e defina $N_1 = N_1 = N(F_1, ..., F_r \mid F_1, ..., F_r \mid \cdots \mid F_1, ..., F_r \mid 0, 0..., 0)$ como acima, onde cada bloco possui um novo conjunto de n variáveis. Analogamente, defina $N_2 = N_1(F_1, ..., F_r \mid F_1, ..., F_r \mid \cdots \mid F_1, ..., F_r \mid 0, 0..., 0)$. Por recorrência podemos construir N_m pondo $N_m = N_{m-1}(F_1, ..., F_r \mid F_1, ..., F_r \mid \cdots \mid F_1, ..., F_r \mid 0, 0..., 0)$. Defina $D_m := deg(N_m)$ e $V_m :=$ #de variáveis de N_m. Então, $D_m = dD_{m-1}$ e $V_m = n[V_{m-1}/r]$. Devemos mostrar que existe $m \in \mathbb{N}$ tal que $V_m > D_m^i$. Daí e do fato de que N_m é nórmico, seguirá que existe um zero não trivial para as equações $F_1 = ... = F_r = 0$.

Seja $b \in \mathbb{R}$ tal que $d^i < b < n/r$. Escolha $e := deg(N_0) = deg(N)$ tal que $n[\frac{x}{r}] \geq bx$ para todo $x \in \mathbb{R}$ com $x \geq e$. Usando o fato de que $V_m = n[\frac{V_{m-1}}{r}]$ e $D_m = dD_{m-1} = d^m D_0$ obtemos

[4] dado $x \in \mathbb{R}$, $[x]$ denota o maior inteiro $\leq x$

$$\frac{V_m}{D_m^i} = \frac{n[\frac{V_{m-1}}{r}]}{D_m^i} \geq \frac{b^m V_0}{d^{mi} D_0^i}.$$

Como $D_0 = V_0 = e$ temos $\frac{V_m}{D_m^i} \geq (\frac{b}{d^i})^m e_0^{1-i}$. Escolhendo m grande vemos que $\frac{V_m}{D_m^i} > 0$ e daí o resultado se segue.

□

Corolário 4. *Seja k um corpo de tipo C_i e E/k uma extensão algébrica. Então, E é do tipo C_i.*

Demonstração. Seja $F \in E[X_1, ..., X_n]$ homogêneo de grau d com $n > d^i$. Devemos mostrar que existe $u = (u_1, ..., u_n) \in E^n - \{0\}$ tal que $F(u) = 0$. Sem perda de generalidade podemos supor que $n = [E : k] < \infty$ (adjuntando coeficientes de F em k). Seja $\{e_1, ..., e_n\}$ uma k-base de E e $\alpha_k = X_{k1}e_1 + \cdots + X_{kn}e_n \in E$ elementos genéricos com $1 \leq k \leq n$. Substituindo $\alpha = (\alpha_1, ..., \alpha_n)$ em F e efetuando as devidas simplificações, obtemos uma expressão do tipo

$$F(\alpha) = f_1(X_{11}, ..., X_{nn})e_1 + \cdots + f_n(X_{11}, ..., X_{nn})e_n$$

onde $f_1(Z_{11}, ..., Z_{nn}), ..., f_n(Z_{11}, ..., Z_{nn}) \in k[Z_{11}, ..., Z_{nn}]$ são homogêneos de grau d com n^2-variáveis. Assim, temos n polinômios à n^2 variáveis de grau d. Pela condição $n > d^i$ concluímos que $n^2 > nd^i$. Usando o fato de que k é C^i e aplicando o teorema de Nagata-Lang temos que existe $(\alpha_{11}, ..., \alpha_{nn}) \in k^{n^2} - \{0\}$ tais que

$$f_1(\alpha_{11}, ..., \alpha_{nn}) = \cdots = f_n(\alpha_{11}, ..., \alpha_{nn}) = 0.$$

Assim, $\alpha = (\alpha_{11}e_1 + \cdots + \alpha_{1n}e_n, ..., \alpha_{n1}e_1 + \cdots + \alpha_{nn}e_n) \in E^n$ é um zero não trivial de F.

□

Seja E/k uma extensão de corpos. Se E/k é algébrica diremos que o grau de transcendência da extensão E/k é 0 e adotamos a notação: $tr.deg_k(E) = 0 \iff E/k$ é algébrica. Se E/k não é algébrica, considere

$$\mathcal{M} := \{S \mid S \subset E \text{ tal que S consiste de elementos algebricamente independentes sobre } k\}.$$

Tal conjunto é parcialmente ordenado por inclusão e indutivo. Assim, pelo lema de Zorn, existem elementos maximais. Um elemento maximal $S \in \mathcal{M}$ é chamado uma base de transcendência de E sobre k. Pode-se mostrar que se S e $S^{'}$ são duas bases de transcendência então existe uma bijeção $S \cong S^{'}$. Se S é finito chamamos E de um corpo de funções à $\#S$ variáveis sobre k e definimos o grau de transcendência pondo $tr.deg_k(E) := \#S$. Pela maximalidade, temos que $E/k(S)$ é algébrica.

Teorema 5. *Seja E um corpo de funções à j-variáveis sobre um corpo k. Se k é do tipo C_i então E é do tipo C_{i+j}.*

Demonstração. Pelo corolário acima e por indução podemos supor $E = k(T)$. Seja $F \in E[X_1, ..., X_n]$ homogêneo de grau d com $n > d^{i+j}$. "Limpando" denominadores podemos supor que $F \in k[T][X_1, ..., X_n]$. Introduza novas variáveis, X_{uv} para $u = 1, ..., n$ e $v = 0, ..., s$ (com s à ser determinado) e tome

$$X_u = X_{u0} + X_{u1}T + \cdots + X_{us}T^s$$

Seja $M_i = \alpha_{i_1 \ldots i_n}(T)X_1^{i_1} \cdots X_n^{i_n}$ monômio ocorrendo em F de maior grau em T, digamos $e = deg(\alpha_{i_1 \ldots i_n}(T))$. Usando as novas variáveis obtemos

$$F = \sum_{i_1, ..., i_n} \alpha_{i_1 \ldots i_n}(T)X_1^{i_1} \cdots X_n^{i_n} = \sum_{i_1, ..., i_n} \alpha_{i_1 \ldots i_n}(T)(\sum_{j_1} X_{1j_1}T^{j_1})^{i_1} \cdots (\sum_{j_n} X_{nj_n}T^{j_n})^{i_n}$$

$$= F_0 + F_1T^1 \cdots + F_{e+ds}T^{e+ds}.$$

onde $F_0, ..., F_{e+ds}$ são polinômios à coeficientes em k nas variáveis $\{X_{uv}\}$. Assim, $F_0, ..., F_{ds+e}$ possuem $n(s+1)$ variáveis e são polinômios homogêneos de grau d. Procuramos s tal que $n(s+1) > (1+ds+e)d^i$. Isso equivale a encontrar s tal que $s(n-d^{i+1}) > ed^i + d^i - n$. Observe que como $n > d^{i+1}$ uma tal escolha é claramente possível.

Finalmente, pela condição C_i em k, obtemos um zero não trivial das equações $F_0 = ... = F_{e+ds} = 0$, o qual determina um zero não trivial para F.

□

Referências

[1] Bump, Daniel. Algebraic geometry. World Scientific Publishing Co Inc, 1998.

[2] Atiyah, M., Macdonald, I. G. (1969). Introduction to commutative algebra.

[3] Greenberg, M. J. (1969). Lectures on forms in many variables (Vol. 31).

[4] W. Aitken and F. Lemmermeyer, Simple Counterexamples to the Local–Global Principle.

[5] Nagata, Masayoshi. "Note on a paper of Lang concerning quasi algebraic closure."Memoirs of the College of Science, University of Kyoto. Series A: Mathematics 30.3 (1957): 237-241.

[6] Serre, Jean-Pierre. A course in arithmetic. Vol. 7. Springer.