CURVAS ASSINTÓTICAS

Este exemplar corresponde a redação final da tese devidamente corrigida e defendida pela Sra. Neuza KazuKo KaKuta e aprovada pela Comissão Julgadora.

Campinas, 05 de dezembro de 1990.

Prof. Dr. Abramo Hefez
Abramo Hefez

Dissertação apresentada ao Instituto de Matematíca, Estatística e Ciência da Computação, UNICAMP, como requisito parcial para obtenção do Título de Doutor em Ciências.

CURVAS ASSINTÓTICAS

Impl.

NEUZA KAZUKO KAKUTA

ORIENTADOR: PROF.DR. ABRAMO HEFEZ

CAMPINAS, NOVEMBRO / 90

- UNICAMP -

AGRADECIMENTOS

Quero agradecer ao Professor Abramo Hefez pela imprescindível orientação, não só na execução deste trabalho, mas também pela dedicação, pelo empenho em me dar uma formação algébrica e por me apresentar a problemática aqui abordada.

Sou grata aos Professores Francesco Mercuri e Antonio Paques que me incentivaram para a escolha da área. Aos demais professores e amigos da UNICAMP que contribuiram para a minha formação matemática.

Quero registrar meus agradecimentos aos amigos do Departamento de Matemática do IBILCE por me proporcionarem a oportunidade de realizar o curso, e especialmente ao professor Hygino H. Domingues pelo estímulo, despertando meu interêsse pelo doutorado.

Agrade o aos colegas da UFES pela acolhida, e em especial à Maria Lúcia T. de Campos pela compreensão, amizade e apoio.

Agradeço à CAPES pela ajuda financeira, e finalmente ao Luiz Cláudio pelo esforço datilográfico.

Aos meus pais,

ÍNDICE

INTRODUÇÃO

Seja X uma curva projetiva plana definida por um polinômio F. Para cada desomogeneização F_* de F, para cada inteiro λ, com $1 \leq \lambda < \deg F$, e para cada $P \in X$, consideramos o desenvolvimento $\tau_P^\lambda F_*$ de F_* em P, truncado em ordem λ. A curva definida pela equação $\tau_P^\lambda F_* = 0$, se existir, é chamada de *curva assintótica* a X em P de ordem λ relativa desomogeneização F_*.

O estudo das curvas assintóticas é iniciado no capítulo I, onde fazemos a análise das possíveis multiplicidades de interseção de um curva afim com as suas curvas assintóticas. Denotando por η_λ a multiplicidade de interseção num ponto geral P da curva com a sua curva assintótica de ordem λ em P, temos que para toda curva, $\eta_\lambda \geq \lambda+1$ e para a curva geral (para o seu grau), $\eta_\lambda = \lambda+1$.

Quando $\eta_\lambda = \lambda+1$, dizemos que a curva é *λ-genérica*, caso contrário, ela é dita *λ-não genérica*. Em (1.11) damos condições sobre a equação da curva e sobre r para se reconhecer quando $\eta_\lambda > \lambda+r$.

No capítulo II estabelecemos condições para a existência projetiva das curvas assintóticas. Mais precisamente, estabelecemos condições para que o fêcho projetivo da curva $\tau_P^\lambda F_* = 0$ independa da desomogeneização F_* de F.

Se p é a característica do corpo de base, temos os seguintes critérios:

Se $p = 0$, a curva assintótica existe projetivamente apenas para $\lambda = 1$. Se $p > 0$, a curva existe projetivamente se, e somente se, λ é um truncamento do desenvolvimento p- ádico do grau d da curva, ou λ é uma potência de p que divide d (note que $\lambda = 1$ se insere no segundo caso).

Na seção 2, estudamos as curvas λ-não genéricas, caracterizando as equações das que tem singularidades amenas. Neste particular, generalizamos resultados obtidos para $\lambda = 1$ por R. Pardini, A. Hefez e E. Ballico.

Na seção 3 determinamos o número de pontos λ estacionários de uma curva λ-genérica, isto é o número de pontos P para os quais

$$I(P, F_{*}.\tau_{P}^{\lambda}\, F_{*}) > \lambda+1,$$

onde $I(P, F_{*}.\tau_{P}^{\lambda}\, F_{*})$ denota a multiplicidade de interseção em P de F_{*} com $\tau_{P}^{\lambda}\, F_{*}$. O resultado que obtemos é que o número de pontos estacionários de uma curva lisa de grau d, contados com apropriadas multiplicidades é dado por

$$d.[d(\lambda+2) - 3(\lambda+1)]$$

Para $\lambda = 1$, obtém-se a fórmula de Plücker clássica em característica arbitrária.

Na seção 4 estudamos as aplicações assintóticas, i.é , as aplicações racionais que a cada ponto P da curva associam as coordenadas projetivas da curva assintótica em P. Obtemos para $\lambda < p$, a caracterização das curvas para as quais o morfismo assintótico é separável. Estes resultados generalizam o Teorema de Ordem Genérica de Contato de Hefez e Kleiman ([H-Kℓ], Teorema 3.5), que relaciona a inseparabilidade da aplicação de Gauss com a multiplicidade de interseção da curva com a sua reta tangente num ponto geral da curva.

O capítulo III contém as aplicações do nosso trabalho à teoria dos números. A fonte de inspiração é o trabalho de Stöhr e Voloch [S-V], onde para contar o número $N(X,q)$ de pontos racionais de uma curva plana X sobre um corpo finito $\mathbb{F}_q$, estes autores contam o número de pontos da curva para os quais a imagem do ponto pelo morfismo de Frobenius F_q pertence a reta tangente à curva no ponto. Deste procedimento, isolamos a seguinte idéia: Seja dada uma família $(\mathcal{F}_P)_{P\in X}$ de curvas planas parametrizadas por X tal que $P \in \mathcal{F}_P$ para todo $P \in X$. Os pontos racionais de X estão entre os pontos para os quais

$$F_q(P) \in (\mathcal{F}_P = 0) \quad (*)$$

Se nem todos os pontos de $X(\bar{\mathbb{F}}_q)$, onde $\bar{\mathbb{F}}_q$ é o fêcho algébrico de $\mathbb{F}_q$, possuem a propriedade (*), dizemos que a curva X é $\mathcal{F}$-Frobenius *não degenerada*; caso contrário dizemos que é *degenerada*. Se X é $\mathcal{F}$-Frobenius não degenerada, então o número de pontos que satisfazem a (*) nos dá uma cota superior para o número de pontos racionais de X.

Aplicamos o método acima descrito no caso em que $\mathcal{F} = \mathcal{F}_\lambda$, com

$$(\mathcal{F}_\lambda) = \{\tau_P^\lambda F_* = 0\}$$

e generalizamos para λ arbitrário vários resultados obtidos por Hefez e Voloch em [H-V] no caso $\lambda = 1$.

O capítulo se encerra com o estudo das curvas do tipo $y^n = \varphi(x)$ para as quais estabelecemos cotas para $N(X,q)$ e as comparamos com as cotas existentes, mostrando com exemplos que as nossas cotas podem em certos casos serem bem melhores do que as cotas conhecidas. O estudo das curvas de Fermat foi abordado pelos autores no trabalho [H-K].

No capítulo IV relacionamos a sequência de ordens de uma curva irredutível mergulhada em $\mathbb{P}^N$ com os graus de inseparabilidade de certos mapas duais. Mais precisamente, a uma curva $X \subseteq \mathbb{P}^N$, não degenerada associa-se uma sequência crescente de inteiros positivos

$$0 = \varepsilon_0 < 1 = \varepsilon_1 < \ldots < \varepsilon_N ,$$

que representam as possíveis multiplicidades de interseção da curva com os hiperplanos nos pontos de um aberto U da curva.

Por outro lado, consideram-se, C_nX o fêcho em $\mathbb{P}^N \times (\mathbb{P}^N)^*$ do conjunto

$$\{(P,H) \in U \times (\mathbb{P}^N)^* : I(P,X.H) \geq \varepsilon_n\},$$

e a projeção sobre o segundo fator

$$\pi'_n : C_nX \longrightarrow X_n \subset (\mathbb{P}^N)^*$$

O Teorema central do capítulo é o teorema 2.5 cujo enunciado é:

O grau de inseparabilidade de π'_n é a maior potência de p que divide ε_n.

Este resultado é demonstrado inicialmente quando n = N e em seguida generalizado por um argumento de seção e projeção. Este teorema é também uma generalização do Teorema de Ordem Genérica de Contato. O caso N = 3 foi tratado anteriormente por Hefez em [H.2].

O capítulo V é devotado a estabelecer as diferenças entre o nosso método e o método de Stöhr-Voloch. No método de Stöhr-Voloch, usa-se a família de curvas osculantes de um determinado grau à curva dada (são os hiperplanos hiperosculantes da curva imersa pelos morfismos de Veronese). Esse método daria boas cotas desde que se tivesse critérios eficientes para a Frobenius não degeneração, o que na prática não ocorre.

Propomos então o método alternativo que utiliza das curvas assintóticas de uma determinada ordem à curva dada. Neste caso, temos critérios bastante simples para a Frobenius não degeneração. Mostramos finalmente que mesmo quando as curvas assintóticas coincidem com as curvas osculantes, a nossa abordagem dá cotas melhores do que as conseguidas em [S-V] .

No apêndice colocamos os resultados sobre polinômios em característica positiva que necessitamos no curso do trabalho. Estes resultados não se encontram na literatura, foram alí incluídos.

Para finalizar, quero registrar que este trabalho foi realizado em co-autoria com o meu orientador de tese Prof. Abramo Hefez.

CAPÍTULO I

CURVAS ASSINTÓTICAS A CURVAS AFINS

Seja

$$C: f(x,y) = 0$$

uma curva plana afim irredutível de grau d, definida sobre um corpo algebricamente fechado K de característica p, com $p \geq 0$.

Para λ um inteiro tal que $1 \leq \lambda < d$ e para $P = (x_0,y_0)$ um ponto de C defina,

$$\tau_P^{\lambda} f = \sum_{i+j=1}^{\lambda} D_{ij} f(P)\ (x-x_0)^i (y-y_0)^j,$$

onde D_{ij} é o operador diferencial de Hasse de ordem i com relação a x, e de ordem j com relação a y.

Chamamos de *Curva assintótica de ordem* λ *à C em* P, a curva definida pela equação:

$$\tau_P^{\lambda} f = 0$$

As curvas assintóticas de ordem $\lambda = 1$ são as retas tangentes, e as de ordem 2, 3,..., serão chamadas respectivamente de cônicas assintóticas, cúbicas assintóticas,...

Observe que pela unicidade do desenvolvimento em série de potências de f em P, temos que $\tau_P^{\lambda} f$ independe de mudança de coordenadas afins.

Seja

$$\pi : \tilde{C} \longrightarrow C,$$

uma desingularização de C. Dado um ramo de C em P, sejam $\tilde{P}$ o ponto de $\tilde{C}$ que lhe corresponde, e $t \in Q_{\tilde{C},\tilde{P}}$ um parâmetro local de $\tilde{C}$ em $\tilde{P}$. Então no completamento $\hat{Q}_{\tilde{C},\tilde{P}}$ do anel local $Q_{\tilde{C},\tilde{P}}$, tem-se:

$$x(t) = x(\tilde{P}) + D_t^1\, x(\tilde{P})\, t + \dots$$

$$y(t) = y(\tilde{P}) + D_t^1\, y(\tilde{P})\, t + \dots,$$

onde D_t^r é o operador diferencial de Hasse de ordem r. Aqui, $x\circ\pi$ e $y\circ\pi$ estão sendo identificados com x e y respectivamente.

(1.1) Proposição *A função:*

$$\begin{aligned} v : \tilde{C} &\longrightarrow \mathbb{N} \\ \tilde{P} &\longrightarrow \mathrm{ORD}_{\tilde{P}}\left(\tau^{\lambda}_{\pi(\tilde{P})} f\right) \end{aligned}$$

é semi contínua superiormente.

Demonstração: Seja $\tilde{P}_0$ um ponto de $\tilde{C}$ e s um parâmetro local de $\tilde{C}$ em $\tilde{P}_0$.

Seja **U** a vizinhança de $\tilde{P}_0$ em $\tilde{C}$ constituída pelos pontos $\tilde{P}$ tais que $t = s - s(\tilde{P})$ é um parâmetro local de $\tilde{P}$.

Para $P(t) = (x(t),y(t))$ uma parametrização como acima, tem-se que:

$$\tau_P^{\lambda} f(P(t)) = \sum_{i_0+i_1=1}^{\lambda} D_{i_0 i_1} f(\tilde{P})\, (x(t)-x(\tilde{P}))^{i_0}\, (y(t)-y(\tilde{P}))^{i_1}$$

Logo,

$$\tau_P^{\lambda} f\,(P(t)) = \sum_{r\geq 1} I_r(\tilde{P}) t^r,$$

com os I_r polinômios em $D_{ij}\, f$, $D_t^i\, x$ e $D_t^j\, y$, e portanto funções regulares em $\mathbf{U}$.

Como $D_s^i = D_t^i$, para $i \geq 1$ (veja por ex. [H_o - 1]), então as funções regulares I_r não dependem do ponto $\tilde{P}$ de $\mathbf{U}$.

Agora, é claro que, para todo η,

$$\{ \tilde{P} \in \mathbf{U} : \mathrm{ORD}_{\tilde{P}} (\tau_p^{\lambda} f) \geq \eta \},$$

é fechado em $\mathbf{U}$.

Logo, $\mathbf{v}$ é semi-contínua superiormente em $\mathbf{U}$ e portanto em $\tilde{C}$ ∎

A semi-continuidade superior de $\mathbf{v}$ implica que o seu mínimo é atingido num aberto de $\tilde{C}$.

Seja

$$\eta_\lambda = \min \{ \mathbf{v}(\tilde{P}) : \tilde{P} \in \tilde{C} \}$$

O mínino η_λ será chamado de *multiplicidade de interseção genérica de* C *com a curva assintótica de ordem* λ.

Indicando por $I(P,f.g)$ a multiplicidade de interseção em P das curvas $f = 0$ e $g = 0$, podemos também dizer:

(1.2) Corolário *A função:*

$$P \in C \longrightarrow I(P,f.\tau_P^{\lambda} f)$$

é *semi-contínua superiormente e o seu valor mínimo é* η_λ.

No que segue suporemos que x é uma variável separante de k(C) e denotaremos $D_x^1 y$ por y'.

(1.3) Observação Se P é um ponto geral de C (i.e no complementar de um fechado próprio de C) então uma parametrização $P(t) = (x(t),y(t))$ de C em P pode ser dada por:

$$x(t) = x(P) + t$$

$$y(t) = b_0 + b_1 t + b_2 t^2 + \dots,$$

onde, $b_i = D_x^i\, y(P)$.

O desenvolvimento da série $\tau_P^\lambda f(P(t))$, mencionado na demosntração de (1.1) é dado pelo seguinte lema:

(1.4) Lema *Se* P *é um ponto geral de* C, *então:*

$$\tau_P^\lambda f(P(t)) = \sum_{r \geq 1} I_r(P) t^r$$

$$\textit{onde, } I_r = \sum_{i+j=1}^{\lambda} D_{ij} f \sum_{s=0}^{j} (-1)^s \binom{j}{s} y^s D_x^{r-i} (y^{j-s}).$$

Demonstração: Como

$$\tau_P^\lambda f = \sum_{i+j=1}^{\lambda} D_{ij} f(P)\, (x-x(P))^i\, (y-y(P))^j,$$

então para uma parametrização P(t) como em (1.3) temos que,

$$\tau_P^\lambda f(P(t)) = \sum_{r \geq 1} (\sum_{i+j=1}^{\lambda} D_{ij} f(P) [\, D_t^{r-i} (y(t) - y(P))^j]_{t=0})\, t^r$$

Sendo,

$$[D_t^{r-i} y(t) - y(P)]_{t=0} = \sum_{s=0}^{j} (-1)^s \binom{j}{s} y^s(P)\, [D_t^{r-i} (y^{j-s}(t))]_{t=0} =$$

$$= (\sum_{s=0}^{j} (-1)^s \binom{j}{s} (y^s D_x^{r-i} (y^{j-s}))(P),$$

obtemos a série requerida. ∎

Note que para $\lambda = 1$, a série contém a seguinte informação: $\eta_1 > 2$ se e somente se $D_x^2 y = 0$ sobre C. Para $\lambda > 1$, a análise de η_λ mediante o anulamento das funções racionais I_r sobre C, é extremamente complicada, e para torná-la acessível propomos uma forma alternativa devido à igualdade:

$$I(P, f.\tau_P^\lambda f) = I(P, f.(f - \tau_P^\lambda f))$$

(1.5) **Teorema** *Se* $C: f(x,y)=0$ *é uma curva irredutível de grau* d, *e* λ *um inteiro tal que* $1 \leq \lambda < d$, *então*

(i) $\eta_\lambda \geq \lambda + 1$

(ii) $\eta_\lambda > \lambda + 1$ *se, e somente se*

$$\sum_{i=0}^{\lambda+1} D_{\lambda+1-i,i}\, f\ (D_{10} f)^i\ (-D_{01} f)^{\lambda+1-i} \equiv 0 \pmod f.$$

Demonstração: A expansão de f em série de potências em $P=(x_0, y_0)$ é da forma: $f = f_1 + \ldots\ldots + f_d$, onde, para $r = 1, \ldots, d$,

$$f_r = \sum_{i+j=r} D_{ij}\, f(P)\ (x-x_0)^i\ (y-y_0)^j$$

Se P é um ponto geral de C, então para uma parametrização P(t) de C em P como em (1.3) temos

$$(f_{\lambda+1} + \ldots + f_d)(P(t)) = [D_{\lambda+1,0}\, f(P) + D_{\lambda,1}\, f(P) b_1 + \\ + \ldots + D_{0,\lambda+1} f(P)\ b_1^{\lambda+1}] t^{\lambda+1} + \ldots \qquad (1.5.1)$$

Como

$$I(P, f.\tau_P^\lambda f) = I(P, f.(f_{\lambda+1} + \ldots + f_d))$$

segue de (1.5.1) que $\eta_\lambda \geq \lambda+1$.

(ii) Como (1.5.1) ocorre para todo P geral em C e b_1 = $-(D_{10}f/D_{0,1}f)(P)$, tem se que $\eta_\lambda > \lambda+1$ se, e somente se

$$\sum_{i=0}^{\lambda+1} D_{\lambda+1-i,i}f\,(D_{10}f)^i\,(-D_{01}f)^{\lambda+1-i} \equiv 0(\mathrm{mod}\ f).$$ ∎

Uma curva C é dita *λ-genérica* se $\eta_\lambda = \lambda+1$, e *λ-não genérica* se $\eta_\lambda > \lambda+1$. Note que para $p \neq 2$, as curvas 1-genéricas são as curvas reflexivas.

A multiplicidade genérica η_1 é em geral denotada por ε_2 e é sabido que:

Se C não é reflexiva, então ε_2 é uma potência de característica.

(1.6) **Exemplo** Para todo d e λ com $1 \leq \lambda < d$, existe uma curva irredutível *λ-genérica* de grau d.

A curva

$$C:\ y + x^d + x^{\lambda+1} = 0$$

é *λ-genérica* por (1.5,ii). ∎

(1.7) **Corolário** *Uma curva genérica de grau* d, *é λ-genérica para todo* λ, $1 \leq \lambda < d$.

A fim de darmos um critério prático para o cálculo de η_λ, introduzimos as seguintes funções racionais:

$$g_{rs} := \sum_{i=r}^{s} \binom{i}{r} D_{s-i,i}f\,(y')^{i-r}.$$

(1.8) Lema *Se* r *e* s *são inteiros tais que* $0 \leq r < s$, *então*

$$D_x(g_{rs}) = (s+1-r)g_{r,s+1} + (r+1)y''g_{r+1,s}\ .$$

Demonstração:

$$D_x(g_{rs}) = \sum_{i=r}^{\lambda} \begin{bmatrix} i \\ r \end{bmatrix} D_x\ (D_{s-i,i}f)\ (y')^{i-r} +$$

$$+ \sum_{i=r}^{s} \begin{bmatrix} i \\ r \end{bmatrix} D_{s-i,i}f\ D_x((y')^{i-r}). \qquad (1.8.1)$$

A primeira parcela de (1.8.1) é igual a:

$$\sum_{i=r}^{s} \begin{bmatrix} i \\ r \end{bmatrix} (s+1-i)\ D_{s+1-i,i}f\ (y')^{i-r} +$$

$$+ \sum_{i=r+1}^{s+1} \begin{bmatrix} i-1 \\ r \end{bmatrix} i\ D_{s+1-i,i}f\ (y')^{i-r}. \qquad (1.8.2)$$

Como $i\begin{bmatrix} i-1 \\ r \end{bmatrix} = (i-r)\begin{bmatrix} i \\ r \end{bmatrix}$, temos que (1.8.2) é igual a:

$$\sum_{i=r}^{s+1}\left[(s+1-i)\begin{bmatrix} i \\ r \end{bmatrix} + (i-r)\begin{bmatrix} i \\ r \end{bmatrix}\right]D_{s+1-i,i}f\ (y')^{i-r} = (s+1-i)g_{r,s+1}.$$

Verifica-se facilmente que a segunda parcela de (1.8.1) é igual a $(r+1)y''g_{r+1,s}$. ∎

(1.9) Lema *Seja* $y(t) = y_0 + b_1 t + \ldots \in K[[t]]$, *então para todo* $i \geq 1$, *tem-se que:*

$$(y(t) - y_0)^i = \sum_{j\geq 0}\left(\sum_{s=0}^{j} \begin{bmatrix} i \\ s \end{bmatrix} b_1^{i-s}\ c_{js}(P)\right) t^{i+j},$$

onde, $c_{js}(P) = D_t^j(b_2 t + \ldots)^s|_{t=0}$.

Demonstração: Pondo $u = b_2 t + \ldots$, temos que

$$(y(t) - y_0)^i = t^i(b_1 + u)^i = t^i \sum_{s=0}^{i} \binom{i}{s} b_1^{i-s} u^s.$$

Assim, para todo $j \geq 0$,

$$\left[D_t^{i+j} (y(t) - y_0)^i\right]_{t=0} = \sum_{s=0}^{i} \binom{i}{s} b_1^{i-s} \left[D_t^j u^s\right]_{t=0}.$$

Pelo fato que $c_{js}(P) = 0$ para $j < s$, segue que

$$(y(t) - y_0)^i = \sum_{j\geq 0} \left[\sum_{s=0}^{j} \binom{i}{s} b_1^{i-s} c_{js}(P)\right] t^{i+j}. \qquad \blacksquare$$

(1.10) Lema *Seja* P(t) *uma parametrizaçãode* C *centrada em um ponto geral* P *como em* (1.3), *então*

$$f(P(t)) = \tau_P^\lambda f\ (P(t)) + \sum_{i\geq 1} \sum_{j=0}^{i-1} [g_{j,\lambda+i-j}(P)\, b_2^j +$$
$$+ \sum_{s=0}^{j-1} c_{js}(P)\, g_{s,\lambda+i-j}(P)]\ t^{\lambda+i},$$

onde c_{js} *é como em* (1.9).

Demonstração: Escrevendo $f = f_1 + \ldots + f_d$, onde para $r = 1,\ldots,d$

$$f_r = \sum_{i=0}^{r} D_{r-i,i} f(P)\ (x-x_0)^{r-i}\ (y-y_0)^i$$

temos por (1.9) que,

$$f_r(P(t)) = \sum_{j\geq 0} \sum_{i=0}^{r} D_{r-i,i} f(P) \left[D_t^{i+j}\ (y(t) - y_0)^i\right]_{t=0} t^{r+j} =$$

$$= \sum_{j\geq 0} \left[\sum_{s=0}^{j} c_{js}(P) \sum_{i=s}^{r} \binom{i}{s} D_{r-i,i}\ f(P)\ b_1^{i-s}\right] t^{r+j} =$$

$$= \sum_{j\geq 0} \left[\sum_{s=0}^{j} c_{js}(P)\ g_{sr}(P)\right] t^{r+j}.$$

Pondo $a_{jr} = \sum_{s=0}^{j} c_{js}(P)\ g_{sr}(P)$, temos:

$$(f_{\lambda+1} + \ldots + f_d)(P(t)) = \sum_{j\geq 0} \sum_{r=\lambda+1}^{d} a_{jr}\ t^{r+j} =$$

$$= \sum_{j\geq 0} \sum_{k=1}^{d-\lambda} a_{j,\lambda+k}\ t^{\lambda+j+k} = \sum_{i\geq 1} \sum_{j=0}^{i-1} a_{j,\lambda+i-j}\ t^{\lambda+i}.$$

Logo

$$(f - \tau_P^{\lambda} f)(P(t)) = \sum_{i\geq 1} \sum_{j=0}^{i-1} \Big[g_{j,\lambda+i-j}(P)\ b_2^j + \sum_{s=0}^{j-1} c_{js}(P)\ g_{s,\lambda+i-j}(P) \Big]\ t^{\lambda+i},$$

onde a última igualdade decorre do fato que $c_{jj} = b_2^j$. ■

(1.11) Teorema *Se* C *é reflexiva então para cada* r *e* λ *tais que* $1 \leq r \leq \lambda+1$ e $p > \lambda+r$, *as seguintes afirmações são equivalentes:*

(i) $\eta_\lambda > \lambda+r$.

(ii) $g_{0,\lambda+1} = \ldots = g_{r-1,\lambda+1} = 0$ *sobre* C.

(iii) $g_{ij} = 0$ *sobre* C, *para* $i+j \leq \lambda+r$ e $j \geq \lambda+1$.

Demonstração:

(ii) ⇒ (iii) A prova desta implicação será feita por indução sobre r.

Para r = 1, é trivial.

Supondo que a implicação (ii) ⇒ (iii) seja verdadeira para r com $1 \leq r \leq \lambda+1$, e que (ii) ocorra para r+1; basta mostrarmos que se $p > \lambda+r+1$, então $g_{ij} = 0$ para $i+j = \lambda+r+1$ e $j \geq \lambda+1$.

Pela hipótese de indução e por (ii) temos respectivamente:

$$g_{r-1,\lambda+1} = \ldots = g_{0,\lambda+r} = 0 \quad \text{e} \quad g_{r,\lambda+1} = 0.$$

Derivando essas funções racionais com respeito a x e usando o fato que C é reflexiva e $p > \lambda+r+1$, conclui-se sobre C que,

$$g_{r,\lambda+1} = g_{r-1,\lambda+2} = \ldots = g_{0,\lambda+r+1} = 0,$$

(iii) $\Rightarrow$ (i) Segue imediatamente de (1.10).

(i) $\Rightarrow$ (ii) Esta implicação será demonstrada por indução sobre r.

O caso $r = 1$, segue de (1.5,ii).

Suponha que (i) $\Rightarrow$ (ii) ocorra para r.

Se $\eta_\lambda > \lambda + (r+1)$ com $p > \lambda + (r+1)$ então (ii) é verificada para r.

Logo, pela implicação (ii) $\Rightarrow$ (iii) já provada, segue que:

$$g_{ij} = 0, \quad i+j \leq \lambda+r \text{ e } j \geq \lambda+1.$$

Portanto,

$$\sum_{j=1}^{i-1} \sum_{s=0}^{j-1} c_{js}\, g_{s,\lambda+i-j} = 0, \quad i = 1,\ldots,r+1. \tag{1.11.1}$$

Assim, por (1.11.1) e (1.10) temos que:

$$(f - \tau_P^\lambda f)(P(t)) = \sum_{i \geq r} \left[\sum_{j=0}^{i-1} g_{j,\lambda+i-j}(P)\, b_2^j \right] t^{\lambda+i}. \tag{1.11.2}$$

A hipótese $\eta_\lambda > \lambda + (r+1)$ juntamente com (1.11.2) implicam o anulamento de

$$\sum_{j=0}^{r} g_{j,\lambda+r+1-j}\, (y^{(2)})^j$$

sobre C, onde $y^{(2)}$ denota $D_x^2 y$.

Logo,

$$\sum_{j=0}^{r-1} g_{j,\lambda+r+1-j}\ (y^{(2)})^j = -g_{r,\lambda+1}\ (y^{(2)})^r. \tag{1.11.3}$$

Por outro lado, sendo $g_{j,\lambda+r-j} = 0$ para $j = 0,\ldots,r-1$, temos que

$$0 = D_x(g_{j,\lambda+r-j}) = (\lambda+r+1-2j)g_{j,\lambda+r+1-j} + 2(j+1)g_{j+1,\lambda+r-j}\ y^{(2)}.$$

Assim,

$$0 = \sum_{j=0}^{r-1} D_x(g_{j,\lambda+r-j})\ (y^{(2)})^j =$$

$$= (\lambda+r+1) \sum_{j=0}^{r-1} g_{j,\lambda+r+1-j}\ (y^{(2)})^j + 2r\ g_{r,\lambda+1}\ (y^{(2)})^r\ ,$$

e daí

$$(\lambda+r+1) \sum_{j=0}^{r-1} g_{j,\lambda+r+1-j}\ (y^{(2)})^j = -2r\ g_{r,\lambda+1}\ (y^{(2)})^r. \tag{1.11.4}$$

Multiplicando-se (1.11.3) por $\lambda+r+1$ e subtraindo-se de (1.11.4), obtém-se

$$(\lambda+1-r)\ y^{(2)}\ g_{r,\lambda+1} = 0.$$

Sendo C reflexiva e $p > \lambda+r+1$, concluimos que $g_{r,\lambda+1} = 0$, e com isso terminamos a demonstração. ∎

(1.12) Lema *Se* j *é um inteiro tal que* $1 \le j \le \lambda$, *então*

$$(\lambda+1-j)\ g_{j,\lambda+1} = \sum_{i=j}^{\lambda} \binom{i}{j}\ D_x(D_{\lambda-i,i}f)\ (y')^{i-j}.$$

Demonstração: Como para todo i, com $j \le i \le \lambda$ tem-se que

$$\lambda+1-j = (\lambda+1-i) + (i-j), \text{ e } \binom{i}{j}\ (i-j) = \binom{i-1}{j}\ i,$$

segue que,

$$(\lambda+1-j)\ g_{j,\lambda+1} = \sum_{i=j}^{\lambda} \binom{i}{j} (\lambda+1-i)\ D_{\lambda+1-i,i}f\ (y')^{i+j} +$$

$$+ \sum_{i=j+1}^{\lambda+1} \binom{i-1}{j}\ i\ D_{\lambda+1-i,i}f\ (y')^{i-j} =$$

$$= \sum_{i=j}^{\lambda} \binom{i}{j} \left[(\lambda+1-i)\ D_{\lambda+1-i,i}f + (i+1)\ D_{\lambda-i,i+1}f\ y'\right] (y')^{i-j} =$$

$$= \sum_{i=j}^{\lambda} \binom{i}{j} D_x(D_{\lambda-i,i}f)\ (y')^{i-j}.$$ ∎

(1.13) Proposição *Se C é reflexiva e* $p > 2\lambda+1$, *então* $\eta_\lambda > 2\lambda+1$ *se, e somente se* $D_x(D_{ij}f) = 0$ *sobre C, para todo* (i,j) *tal que* $i+j = \lambda$.

Demonstração: Pelo teorema (1.11), $\eta_\lambda > 2\lambda+1$ se e somente se $g_{j,\lambda+1} = 0$ sobre C, para $j = 1,\dots,\lambda$.

Assim, de (1.12) segue que,

$$\sum_{i=j}^{\lambda} \binom{i}{j} D_x(D_{\lambda-i,i}f)\ (y')^{i-j} = 0. \qquad (1.13.1)$$

Tomando-se $j = \lambda,\dots,0$ em (1.13.1) obtemos respectivamente:

$$D_x(D_{0,\lambda}f) = \dots = D_x(D_{\lambda,0}f) = 0$$

A recíproca é imediata em vista do lema (1.12). ∎

(1.14) Lema *Se* $D_x(D_{ij}f) = 0$ *sobre C para todo* (i,j) *tal que* $i+j = \lambda$, *então* $\eta_\lambda \equiv 0(p)$.

Demonstração: Para provar o lema basta que se verifique a seguinte afirmação:

(1.14.1) Se $D_x(D_{ij}f) = 0$ para todo (i,j) tal que $i+j = \lambda$, então $D_x(I_r) = (r+1)\ I_{r+1}$ para todo $r \geq \lambda+1$; onde I_r é como no lema (1.4).

De fato:

Admitindo (1.14.1) verdadeira tem-se que: $D_x(I_{\eta_\lambda -1}) = \eta_\lambda\ I_{\eta_\lambda}$ com $I_{\eta_\lambda -1} = 0$ e $I_{\eta_\lambda} \neq 0$ sobre C. Logo, $\eta_\lambda \equiv 0(p)$.

Demonstração da afirmação (1.14.1).

Denotando por:

$$b_{r-i,j} = \sum_{s=0}^{j-1} (-1)^s \begin{bmatrix} j \\ s \end{bmatrix} y^s\ D_r^{r-i}\ (y^{j-s}),$$

podemos escrever:

$$I_r = \sum_{i+j=1,\, j\geq 1}^{\lambda} b_{r-i,j}\ D_{ij}f.$$

Como $\eta_\lambda > 2\lambda+1$, então por (1.13) temos que:

$$D_x(D_{ij}f) = 0, \quad i+j = \lambda.$$

Daí

$$D_x(I_r) = \sum_{i+j=1}^{\lambda} D_x(b_{r-i,j})\ D_{ij}f + \sum_{i+j=1}^{\lambda-1} b_{r-i,j}\ D_x(D_{ij}f). \qquad (1.14.2)$$

Agora, verifica-se facilmente que:

$$D_x(b_{r-i,j}) = -j\ b_{r-i,j-1}\ y' + (r+1-i)\ b_{r+1-i,j} \qquad (1.14.3)$$

e que

$$\sum_{i+j=1}^{\lambda} b_{r-i,j}\ D_x(D_{ij}f) = \sum_{i+j=2,\, j\geq 1}^{\lambda} i\ b_{r+1-i,j}\ D_{ij}f +$$

$$+ \sum_{i+j=2}^{\lambda} j\ b_{r-i,j-1}\ D_{ij}f\ y'. \qquad (1.14.4)$$

De (1.14.2), (1.14.3) e (1.14.4) segue que

$$D_x(I_r) = \sum_{i+j=i,\, j\geq 1}^{\lambda} [(r+1-i) + i]\, b_{r+1-i,j}\, D_{ij}f = (r+1)\, I_{r+1}.$$ ∎

(1.15) Teorema *Seja C uma curva reflexiva e λ um inteiro tal que $p > 2\lambda+1$. Se $\eta_\lambda > 2\lambda+1$, então $\eta_\lambda \equiv 0$ (p).*

Demonstração: Segue imediatamente de (1.13) e (1.14). ∎

(1.16) Proposição *Se C é não reflexiva então para todo λ tal que $\lambda+1 < \varepsilon_2$, C é λ-não genérica e $\eta_\lambda \geq \varepsilon_2$.*

Demonstração: Sendo C não reflexiva, ε_2 é uma potência q' de p e

$$D_x^2\, y = \ldots = D_x^{q'-1}\, y = 0$$

Assim, para uma parametrização P(t) centrada em P geral de C como em (1.3), tem-se para algum $\mu \in K[[t]]$ que

$$[D_t^{r-i}(y(t)-y(P))^j]_{t=0} = [D_t^{r-i}\,(b_1 t + b_{q'} t^{q'} + \ldots)^j]_{t=0} =$$

$$= [D_t^{r-i}(b_1^j t^j + t^{q'}\mu)]_{t=0}.$$

Logo

$$[D_t^{r-i}(y(t) - y(P))^j]_{t=0} = 0, \quad j < r-i < q'. \qquad (1.16.1)$$

Sendo por (1.5) $\eta_\lambda \geq \lambda+1$, temos que

$$\tau_P^\lambda f(P(t)) = \sum_{r\geq\lambda+1} \left(\sum_{i+j=1,\, j\geq 1}^{\lambda} D_{ij} f(P)[D_t^{r-i}(y(t)-y(P))^j]_{t=0} \right) t^r. \qquad (1.16.2)$$

Portanto, de (1.16.1) e (1.16.2) concluimos que C é λ-não genérica e $\eta_\lambda \geq q'$. ∎

(1.17) Exemplos

(1.17.1) Seja $C : ax^{3+p} + by^{3+p} = 1$ com $p > 3$ e $ab \neq 0$.

C é reflexiva, 2 genérica, mas 3-não genérica com $\eta_3 = p$.

(1.17.2) Seja $C : x^{p-1}y^{p-1} + 1 = 0$ com $p > 5$.

C é reflexiva, mas 2-não genérica com $\eta_2 = 4$.

(1.17.3) Seja $C : x^2y^2 + 1 = 0$ com $p \geq 0$ e $p \neq 2, 3$.

C é reflexiva, mas 2-não genérica com $\eta_2 = 4$.

(1.17.4) Seja $C : xy^{p-1} + 1 = 0$, com $p \neq 2$.

C é uma curva estranha (portanto não reflexiva) e $\eta_\lambda \geq p$ para todo $\lambda < p$.

CAPÍTULO II

CURVAS ASSINTÓTICAS A CURVAS PROJETIVAS

1. CONDIÇÕES PARA A EXISTÊNCIA PROJETIVA

Seja X uma curva projetiva plana irredutível definida por uma equação F = 0 de grau d, sobre um corpo algebricamente fechado K, de característica p, $p \geq 0$.

Iniciaremos com o seguinte exemplo:

Exemplo

Considere a curva X definida por

$$F = X_0^5 X_1^2 + X_2^7 = 0$$

Suponha p = 7 e P = (-1:1:1).

Desomogeneizando F com relação a X_2 e a X_1, obtemos respectivamente as curvas afins:

$$f(x,y) = x^5y^2 + 1 = 0$$

$$g(x,y) = x^5 + y^2 = 0$$

Logo

$$\tau^2_{(-1,1)}f = -3x^2 + 3xy + y^2 - 4x - y + 5,$$

e

$$\tau^2_{(-1,1)}g = -3x^2 - x + 2.$$

Portanto, as homogeneizações de $\tau^2_{(-1,1)}f$ e $\tau^2_{(-1,1)}g$ são distintas, mostrando assim que as cônicas assintóticas dependem do aberto afim de X considerado.

A nossa meta neste parágrafo é determinar condições para a existência projetiva das curvas assintóticas.

(1.1) Definição Sejam $F \in K[X_0,X_1,X_2]$ um polinômio homogêneo, $P \in k^3$ e s um inteiro positivo.

Define-se:

$$\mathcal{H}_P^s F(X_0,X_1,X_2) = \sum_{i_0+i_1+i_2=s} D_{i_0 i_1 i_2} F(P)\, X_0^{i_0} X_1^{i_1} X_2^{i_2}.$$

Se para algum (i_0,i_1,i_2) com $i_0+i_1+i_2 = s$, $D_{i_0 i_1 i_2} F(P) \neq 0$, então a curva $\mathcal{H}_P^s F = 0$ é exatamente a (d-s)-ésima curva polar:

$$\mathcal{P}_P^{d-s} F(X_0,X_1,X_2) = \sum_{i_0+i_1+i_2=d-s} a^{i_0} b^{i_1} c^{i_2} D_{i_0 i_1 i_2} F = 0,$$

onde, $P = (a,b,c)$ e $d = \deg F$.

Para ver isto, basta tomar:

$$F = X_0^{n_0} X_1^{n_1} X_2^{n_2}, \quad n_0 + n_1 + n_2 = d.$$

Neste caso,

$$\mathcal{H}_P^s F = \sum_{i_0+i_1+i_2=s} \binom{n_0}{i_0}\binom{n_1}{i_1}\binom{n_2}{i_2} a^{n_0-i_0} b^{n_1-i_1} c^{n_2-i_2} X_0^{i_0} X_1^{i_1} X_2^{i_2} =$$

$$= \sum_{j_0+j_1+j_2=d-s} \binom{n_0}{j_0}\binom{n_1}{j_1}\binom{n_2}{j_2} a^{j_0} b^{j_1} c^{j_2} X_0^{n_0-j_0} X_1^{n_1-j_1} X_2^{n_2-j_2} = \mathcal{P}_P^{d-s} F.$$

(1.2) Lema *Sejam* $P = (a:b:1) \in X$ *e* $f(X_0,X_1) = F(X_0,X_1,1)$. *Para todo* λ, *com* $1 \leq \lambda < d$, *tem-se que:*

$$\sum_{i_0+i_1=\lambda+1} D_{i_0 i_1} f(a,b)\ (x-a)^{i_0}\ (y-b)^{i_1} =$$

$$= \sum_{r=0}^{\lambda} (-1)^r \begin{bmatrix} d-(\lambda+1)+r \\ r \end{bmatrix} \mathcal{H}_p^{\lambda+1-r}\ F(x,y,1).$$

Demonstração: O coeficiente de $x^i y^j$ do polinômio do lado esquerdo da identidade acima é igual a:

$$\sum_{i_0+i_1=\lambda+1} (-1)^{\lambda+1-(i+j)} \begin{bmatrix} i_0 \\ i \end{bmatrix} \begin{bmatrix} i_1 \\ j \end{bmatrix} D_{i_0\ i_1} f(a,b)\ a^{i_0-i}\ b^{i_1-j},$$

que pode ser escrito sob a forma:

$$\sum_{\alpha+\beta=\lambda+1-(i+j)} (-1)^{\lambda+1-(i+j)} (D_{\alpha\beta}\ D_{ij}\ f)\ (a,b)\ a^{\alpha}\ b^{\beta} \tag{1.2.1}$$

Agora por (A.1), para todo k com $0 \le k \le (\lambda+1)-(i+j)$ tem-se que,

$$\begin{bmatrix} d-(i+j+k) \\ \lambda+1-(i+j+k) \end{bmatrix} D_{ijk}\ F(a,b,1) =$$

$$= \sum_{\alpha+\beta+\gamma=(\lambda+1)-(i+j+k)} (D_{\alpha\beta\gamma}\ D_{ijk}\ F)(a,b,1)\ a^{\alpha}\ b^{\beta} =$$

$$= \sum_{\gamma=0}^{\lambda+1-(i+j+k)} \begin{bmatrix} \gamma+k \\ k \end{bmatrix} D_{0,0,\gamma+k} \left[\sum_{\alpha+\beta=\lambda+1-(i+j)-(\gamma+k)} D_{\alpha,\beta,0} \circ D_{i,j,0} F \right]$$

$$(a,b) a^{\alpha}\ b^{\beta} \tag{1.2.2}$$

Multiplicando ambos os lados de (1.2.2) por $(-1)^k$, e somando essas igualdades para todo k, obtemos,

$$\sum_{k=0}^{\lambda+1-(i+j)} (-1)^k \begin{bmatrix} d-(i+j+k) \\ \lambda+1-(i+j+k) \end{bmatrix} D_{ijk}\ F(a,b,1) =$$

$$= \sum_{k=0}^{\lambda+1-(i+j)} \sum_{t=k}^{\lambda+1-(i+j)} (-1)^k \begin{bmatrix} t \\ k \end{bmatrix} D_{0,0,t} \left[\sum_{\alpha+\beta=\lambda+1-(i+j)-t} D_{\alpha,\beta,0} \circ D_{i,j,0} F \right]$$

$$(a,b)\ a^{\alpha}\ b^{\beta}.$$

Como, para $0 < t \leq \lambda+1-(i+j)$,

$$\sum_{k=0}^{\lambda+1-(i+j)} (-1)^k \binom{t}{k} = \sum_{k=0}^{t} (-1)^k \binom{t}{k} = 0,$$

tem-se que:

$$\sum_{k=0}^{\lambda+1-(i+j)} (-1)^k \binom{d-(i+j+k)}{\lambda+1-(i+j+k)} D_{ijk}F(a,b,1) =$$

$$= \sum_{\alpha+\beta=\lambda+1-(i+j)} (D_{\alpha,\beta,0}\, D_{i,j,0}F)\,(a,b)\, a^{\alpha}\, b^{\beta} \tag{1.2.3}$$

Assim, de (1.2.1) e (1.2.3) obtemos,

$$\sum_{i_0+i_1=\lambda+1} D_{i_0 i_1} f(a,b)\,(x-a)^{i_0}\,(y-b)^{i_1} =$$

$$= \sum_{i+j=0}^{\lambda+1} \left[\sum_{k=0}^{\lambda+1-(i+j)} (-1)^{\lambda+1-(i+j)} \binom{d-(i+j+k)}{\lambda+1-(i+j+k)} D_{ijk}\, F(P) \right] x^i\, y^j =$$

$$= \sum_{r=0}^{\lambda} (-1)^r \binom{d-(\lambda+1)+r}{r} \left[\sum_{i+j+k=\lambda+1-r} D_{ijk}F(P)\, x^i\, y^j \right] =$$

$$= \sum_{r=0}^{\lambda} (-1)^r \binom{d-(\lambda+1)+r}{r} \mathcal{H}_P^{\lambda+1-r}\, F(x,y,1).$$ ∎

(1.3) Proposição *Com as mesmas notações de* (1.2), *tem-se que*:

$$\tau_P^{\lambda}\, f(x,y) = \sum_{r=0}^{\lambda-1} (-1)^r \binom{d-(\lambda+1)+r}{r} \mathcal{H}_P^{\lambda-r}\, F(x,y,1).$$

Demonstração: Provaremos o resultado por indução sobre λ.

Para $\lambda = 1$, é trivial.

Suponha a igualdade acima verdadeira para λ. Para provar que a fórmula é verdadeira para $\lambda+1$, basta calcular a diferença:

$$\tau_P^{\lambda+1} f - \tau_P^{\lambda} f = \sum_{i_0+i_1=\lambda+1} D_{i_0 i_1} f(a,b)\,(x-a)^{i_0}\,(y-b)^{i_1},$$

que é dada precisamente pelo lema (1.2). ∎

Denotaremos por f^* a homogeneização do polinômio não homogêneo f e por F_* a desonogeneização do polinômio homogêneo F com relação à uma indeterminada especificada X_i.

(1.4) Proposição *Seja* $X : F = 0$ *uma curva irredutível de grau* d, *e seja* λ *com* $1 \leq \lambda < d$, *um inteiro tal que alguma derivada de ordem* λ *de* F *é não nula, então as seguintes afirmações são equivalentes:*

(i) $(\tau_P^{\lambda} F_*)^*$ *independe da desomogeneização* F_* de F, *para todo ponto* P *geral de* X.

(ii) $\lambda = 1$ *ou* λ *é tal que para todo* r, $1 \leq r \leq \lambda-1$, $\binom{d-\lambda+r-1}{r} \equiv 0(p)$ *ou todas as derivadas de ordem* $\lambda-r$ de F *são nulas.*

(iii) $(\tau_P^{\lambda} F_*)^* = \mathcal{H}_P^{\lambda} F$, *para toda desomogeneização* F_* *de* F *e para todo* P *em* X.

Demonstração:

(i) $\Rightarrow$ (ii) Suponha sem perda de generalidade que f e g são respectivamente as desomogeneizações de F com relação a X_0 e X_1.

Supondo $\lambda > 1$ e $(\tau_P^{\lambda} f)^* = (\tau_P^{\lambda} g)^*$ tem-se que:

$$X_0 \begin{bmatrix} d-\lambda \\ 1 \end{bmatrix} \mathcal{H}_P^{\lambda-1} F + \ldots + X_0^{\lambda-1} \begin{bmatrix} d-2 \\ \lambda-1 \end{bmatrix} \mathcal{H}_P^{1} F =$$

$$= X_1 \begin{bmatrix} d-\lambda \\ 1 \end{bmatrix} \mathcal{H}_P^{\lambda-1} F + \ldots + X_1^{\lambda-1} \begin{bmatrix} d-2 \\ \lambda-1 \end{bmatrix} \mathcal{H}_P^{1} F. \qquad (1.4.1)$$

O coeficiente de $X_0^i\ X_1^j\ X_2^k$, com $i+j+k = \lambda$, do polinômio à esquerda de (1.4.1) é:

$$\begin{cases} \sum\limits_{r=1}^{i} \begin{bmatrix} d-\lambda+r-1 \\ r \end{bmatrix} D_{i-r,j,k}F(P) & \text{se } i \geq 1 \\ 0 & \text{se } i = 0 \end{cases}$$

e do polinômio à direita é:

$$\begin{cases} \sum\limits_{r=1}^{j} \begin{bmatrix} d-\lambda+r-1 \\ r \end{bmatrix} D_{i,j-r,k}F(P) & \text{se } j \geq 1 \\ 0 & \text{se } j = 0 \end{cases}$$

Se $i = \lambda$, i.é $j+k = 0$, então para P geral em X temos:

$$\sum_{r=1}^{\lambda-1} \begin{bmatrix} d-\lambda+r-1 \\ r \end{bmatrix} D_{\lambda-r,0,0}F(P) = 0$$

Portanto, para $r = 1,\ldots,\lambda-1$, $\begin{bmatrix} d-\lambda+r-1 \\ r \end{bmatrix} \equiv 0(p)$ ou $D_{\lambda-r,0,0}\ F = 0$.

A demonstração segue por indução sobre $j+k$, provando para todo $i \geq 1$ e $r = 1,\ldots,i$, que:

$$\begin{bmatrix} d-\lambda+r-1 \\ r \end{bmatrix} \equiv 0(p),$$

ou

$$D_{i-r,j,k}F = 0, \quad \forall\ (j,k)\ ;\ i+j+k = \lambda \qquad (1.4.2)$$

Escapa na nossa análise, o caso em que $i = j = 0$. Supondo que

$\begin{bmatrix} d-\lambda+r-1 \\ r \end{bmatrix} \not\equiv 0(p)$, então por (1.4.2) e (A.1) tem-se que

$$\begin{bmatrix} d \\ \lambda-r \end{bmatrix} F = X_2^{d-r}\ D_{0,0,\lambda-r}\ F$$

Sendo F irredutível, conclui-se que $D_{0,0,\lambda-r}F = 0$.

(ii) $\Rightarrow$ (iii) Pela hipótese (ii) juntamente com (1.3) segue que

$$\tau_p^{\lambda}\ (F_*) = (\mathcal{H}_p^{\lambda}\ F)_*$$

Como $\deg\ \tau_p^{\lambda}\ (F_*) = \lambda = \deg\ \mathcal{H}_p^{\lambda}\ F$ ou ambos os polinômios são nulos, temos que:

$$(\tau_p^{\lambda}\ F_*)^* = \mathcal{H}_p^{\lambda}\ F.$$

(iii) $\Rightarrow$ (i) É imediato. ∎

Definição Dados $a = a_0+\ldots+a_r p^r$ e $b = b_0+\ldots+b_s p^s$ com $a_r b_s \neq 0$ e $s < r$. Diremos que b é *um truncamento de* a se $a_i = b_i$ para $i = 0,\ldots,s$.

(1.5) Lema *As notações sendo as da proposição* (1.4), *suponha que as condições de* (1.4) *sejam verificadas. Se* ρ *é um inteiro positivo menor que* λ, *tal que* ρ *é p-adicamente menor que* λ *ou* ρ *é um truncamento de d, então:*

$$\begin{bmatrix} d-\rho-1 \\ \lambda-\rho \end{bmatrix} \equiv 0(p).$$

Demonstração: Suponha que ρ é p-adicamente menor que λ. Como uma das derivadas de ordem λ de F é não nula, segue de (A.2) que nem todas as derivadas de ordem ρ são nulas.

Agora, se ρ é um truncamento de d, então alguma derivada de ordem ρ de F é não nula, pois caso contrário, por (A.1) teremos $\begin{bmatrix} d \\ \rho \end{bmatrix} \equiv 0(p)$, o que é um absurdo.

Em ambos os casos, por (1.4 (ii)) segue que $\begin{bmatrix} d-\rho-1 \\ \lambda-\rho \end{bmatrix} \equiv 0(p)$. ∎

(1.6) Teorema *Seja* X : F = 0 *uma curva irredutível de grau d, e seja* λ *um inteiro tal que* $1 \leq \lambda < d$. *Suponha que alguma derivada de ordem* λ *de* F *é não nula. Tem-se então que* $(\tau_P^{\lambda} F_*)^*$ *independe da desomogeneização* F_* *de* F, *para todo* P *em* X *se, e somente se* λ *é um truncamento do desenvolvimento p-ádico de* d*; ou* $\lambda = p^s$ *com* $s \geq 0$ *e* λ *divide* d.

Demonstração: Sejam $d = d_0+\ldots+d_r p^r$ e $\lambda = \lambda_0+\ldots+\lambda_s p^s$ com $d_r\lambda_s \neq 0$. Suponhamos inicialmente que $(\tau_P^{\lambda} F_*)^*$ independe da desomogeneização F_* de F, para todo P em X.

Caso $\lambda = p^s$.

Se s = 0, a conclusão segue de (1.4).

Suponhamos então que s > 0, e que exista $d_i \neq 0$ para algum i, $0 \leq i < s$.

Para $\rho = d_0 +\ldots+ d_{s-1}p^{s-1}$, temos que $1 \leq \rho < \lambda$ e $\begin{bmatrix} d-\rho-1 \\ \lambda-\rho \end{bmatrix} \not\equiv 0(p)$, o que contradiz (1.5).

Assim, d é da forma $d_s p^s +\ldots+ d_r p^r$, e portanto λ divide d.

Caso $\lambda \neq p^s$.

A demonstração será feita em 3 etapas:

(a) Se para algum i, $\lambda_i \neq 0$, então $d_i \leq \lambda_i$.

De fato:

Para $\lambda \neq \lambda_s p^s$, tomando-se $\rho_i = \lambda_0 + \ldots + \widehat{\lambda_i p^i} + \ldots + \lambda_s p^s$,

temos pelo lema (1.5) que

$$\begin{bmatrix} d-\rho_i-1 \\ \lambda-\rho_i \end{bmatrix} \equiv 0(p).$$

Se $d_i = 0$, a firmação é trivial.

Agora, se $d_i \neq 0$, então

$$\begin{bmatrix} d-\rho_i-1 \\ \lambda-\rho_i \end{bmatrix} \equiv \begin{bmatrix} d_i \\ \lambda_i \end{bmatrix} \text{ ou } \begin{bmatrix} d-\rho_i-1 \\ \lambda-\rho_i \end{bmatrix} \equiv \begin{bmatrix} d_i-1 \\ \lambda_i \end{bmatrix}$$

Logo, $d_i \leq \lambda_i$

Para $\lambda = \lambda_s p^s$, com $\lambda_s \geq 2$, tomando-se $\rho = (\lambda_s-1)p^s$, temos por (1.5) que $\begin{bmatrix} d-\rho-1 \\ \lambda-\rho \end{bmatrix} \equiv 0(p)$.

Supondo por absurdo que $d_s > \lambda_s$, temos

$$\begin{bmatrix} d-\rho-1 \\ \lambda-\rho \end{bmatrix} \equiv d_s - \lambda_s + 1.$$

Daí, $d_s = \lambda_s - 1$, o que é contra a hipótese.

(b) Se $\lambda \neq p^s$, então existe i, $0 \leq i \leq s$ tal que $d_i \neq 0$.

De fato:

Se $d_0 = \ldots = d_s = 0$ então para $\rho = p^s$ temos por (1.5) que $\begin{bmatrix} d-\rho-1 \\ \lambda-\rho \end{bmatrix} \equiv 0(p)$.

Sendo, $\begin{bmatrix} d-\rho-1 \\ \lambda-\rho \end{bmatrix} \equiv \begin{bmatrix} p-1 \\ \lambda_0 \end{bmatrix} \cdots \begin{bmatrix} p-1 \\ \lambda_{s-1} \end{bmatrix} \begin{bmatrix} p-2 \\ \lambda_s-1 \end{bmatrix} \neq 0,$

concluimos que algum d_i é não nulo.

(c) Por indução sobre i, provemos que

$$d_{s-i} = \lambda_{s-i}\ ,\ i = 0,\dots, s$$

Como $\lambda_s \neq 0$, por (a) $d_s \leq \lambda_s$.

Supondo que $d_s < \lambda_s$, então $\rho = d_0+\dots+d_s p^s$, tal que $\rho < \lambda$ e por (b) temos que $\rho \geq 1$, e ainda $\begin{bmatrix} d-\rho-1 \\ \lambda-\rho \end{bmatrix} \equiv 0(p)$, o que contradiz (1.5).

Suponha verdadeiro que $d_{s-i} = \lambda_{s-i}$, para $i = 0,\dots,j$ com $j<s$.

Se $\lambda_{s-(j+1)} = 0$ mostremos que $d_{s-(j+1)} = 0$.

Se $d_{s-(j+1)} \neq 0$ então para $\rho = d_0 +\dots+ d_{s-(j+1)}p^{s-(j+1)}$, temos que $1 \leq \rho < \lambda$, e sendo $d_{s-i} = \lambda_{s-i}$ para $i \leq j$, segue que $\begin{bmatrix} d-\rho-1 \\ \lambda-\rho \end{bmatrix} \not\equiv 0(p)$, contradizendo (1.5).

Se $\lambda_{s-(j+1)} \neq 0$, então por (a) $d_{s-(j+1)} \leq \lambda_{s-(j+1)}$. Supondo que $d_{s-(j+1)} < \lambda_{s-(j+1)}$, então para $\rho = d_0 +\dots+ d_s p^s$, teremos $1 \leq \rho < \lambda$.

Pelo mesmo argumento anterior, segue que $\begin{bmatrix} d-\rho-1 \\ \lambda-\rho \end{bmatrix} \not\equiv 0(p)$, o que contradiz (1.5).

Reciprocamente, se λ é um truncamento de d, então $d-\lambda = \alpha q'$, para algum α e $q' \geq p^{s+1} > \lambda$.

Logo, para todo r com $1 \leq r < \lambda$, temos que:

$$\begin{bmatrix} d-\lambda+r-1 \\ r \end{bmatrix} = \begin{bmatrix} \alpha q'+r-1 \\ r \end{bmatrix} \equiv \begin{bmatrix} r-1 \\ r \end{bmatrix} = 0.$$

Se $\lambda = p^s$ e $d = d_s p^s +\dots+ d_r p^r$, com $d_s \geq 0$ então $d-\lambda = p^s\beta$, para algum β.

Logo, para todo r, com $1 \le r < \lambda$ temos que:

$$\binom{d-\lambda+r-1}{r} = \binom{p^s\ \beta+r-1}{r} \equiv \binom{r-1}{r} = 0.$$

Em ambos os casos, a proposição (1.4) garante que $(\tau_p^\lambda\ F_*)^*$ independe da desomogeneização F_* de F, para todo P em X. ■

Note que para $1 < \lambda < p$, as curvas assintóticas de ordem λ existem projetivamente se, e somente se $d \equiv \lambda(p)$; e que para $p = 0$ as curvas assintóticas existem projetivamente apenas para $\lambda = 1$.

Definição Diremos que o par (d,λ) é *admissível* se λ é um truncamento de d ou se λ é uma potência de p, que divide d.

(1.7) Corolário *Se* (d,λ) *é um par admissível então as curvas assintóticas de ordem* λ *a uma curva irredutível de grau* d*, independem de mudança de coordenadas projetivas.*

Demonstração: Se T é uma transformação projetiva tal que $T(Q)=P$, então por (A.3) e (1.6) tem-se que:

$$(\tau_Q^\lambda\ (F^T)_*)^* = \mathcal{H}_Q(F^T) = (\mathcal{H}_P^\lambda\ F)^T = ((\tau_P^\lambda\ F_*)^*)^T. \qquad ■$$

2. AS EQUAÇÕES DAS CURVAS λ-NÃO GENÉRICAS

Neste parágrafo, e nos próximos $X : F = 0$ será uma curva projetiva plana irredutível de grau d, e λ é um inteiro positivo tal que (d,λ) é admissível.

Neste caso, o teorema (1.6) garante que a multiplicidade genérica η_λ da curva $F_* = 0$ com as curvas assintóticas de ordem λ, independe da desomogeneização F_* de F, o que torna consistente a seguinte definição:

Definição Uma curva $X : F = 0$ é dita λ-*genérica* se $\eta_\lambda = \lambda+1$ e λ-*não genérica* se $\eta_\lambda > \lambda+1$.

Seja,

$$\Delta_{ij} = \sum_{s=0}^{\lambda+1} (-1)^s \, (D_i^{\lambda+1-s} \, D_j^s \, F) \, (-F_i)^s \, (F_j)^{\lambda+1-s},$$

onde D_i^r denota a r-ésima derivada parcial de Hasse com respeito à variável X_i e $D_i^1 \, F = F_i$.

Tem-se pelos teoremas (I-1.5) e (II-1.6) que, X é λ-não genérica se, e somente se $\Delta_{ij} \equiv 0 (\mathrm{mod}\ F)$, para todo i, j = 0,1,2, $i \neq j$.

A definição que segue é uma adaptação para o nosso caso, de uma definição dada por E. Ballico e A. Hefez em [B-H] .

Definição Diremos que uma curva irredutível $X : F = 0$ tem *singularidades controladas* com relação ao par admissível (d,λ) se:

$$\sum_P e_P < \lambda d + \sum_{m_P > \lambda+1} m_P\,(m_P - (\lambda+1)),$$

onde m_P denota a multiplicidade de F em P, e

$$e_P = \min\,\{I(P,F.F_i),\ i = 0,1,2\}.$$

Exemplos dessas curvas são as curvas lisas.

(2.1) Proposição *Seja* $X : F = 0$ *uma curva com singularidades controladas.* X *é* λ*-não genérica se, e somente se* $D_i^m D_j^n F = 0$ *para todo* $i,j = 0,1,2$ *e todo par* (m,n) *tal que* $m+n = \lambda+1$.

Demonstração: Se X é λ-não genérica então $\Delta_{ij} = 0$ sobre X, para todo $i,j = 0,1,2$, e portanto

$$D_j^{\lambda+1}F\,(F_i)^{\lambda+1} = -F_j \sum_{s=0}^{\lambda} (D_i^{\lambda+1-s}\,D_j^sF)\,(-F_i)^s\,(F_j)^{\lambda-s}. \tag{2.1.1}$$

Supondo por absurdo que $D_j^{\lambda+1}F \neq 0$, para algum j, então para todo $i = 0,1,2$ e todo $P \in X$, temos por (2.1.1) que:

$$I(P,F.D_j^{\lambda+1}F) + (\lambda+1)\,I(P,F.F_i) \geq I(P,F.F_j). \tag{2.1.2}$$

Após uma mudança de coordenadas, se necessário, podemos supor que num ponto singular P qualquer de X,

$$e_P = I(P,F.F_j), \quad j = 0,1,2. \tag{2.1.3}$$

Se P é um ponto regular de X, então $e_P = 0$ e de (2.1.2) temos que

$$I(P,F.D_j^{\lambda+1}F) \geq I(P,F.F_j). \tag{2.1.4}$$

Se P é um ponto múltiplo, então por (2.1.3) temos que

$$I(P,F.D_j^{\lambda+1}F) + e_p \geq e_p = I(P,F.F_j). \qquad (2.1.5)$$

Se P é um ponto múltiplo com $m_p > \lambda+1$, temos que

$$I(P,F.D_j^{\lambda+1}F) \geq m_p\,(m_p - (\lambda+1)).$$

Logo

$$I(P,F.D_j^{\lambda+1}F) + (e_p - m_p(m_p - (\lambda+1)) \geq e_p = I(P,F.F_j). \qquad (2.1.6)$$

Somando (2.1.4) sobre todos os pontos regulares de X, (2.1.5) sobre todos os pontos P singulares de X tais que $m_p \leq \lambda+1$, e (2.1.6) sobre todos os pontos P tais que $m_p > \lambda+1$, tem-se que

$$\sum_P I(P,F.D_j^{\lambda+1}F) + \sum_P e_p - \sum_{m_p>\lambda+1} m_p(m_p - (\lambda+1)) \geq \sum_P I(P,F.F_j).$$

Pelo teorema de Bézout, segue que

$$d(d - (\lambda+1)) + \sum_P e_p - \sum_{m_p>\lambda+1} m_p(m_p - (\lambda+1)) \geq d(d-1).$$

Logo,

$$\sum_P e_p - \sum_{m_p>\lambda+1} m_p(m_p - (\lambda+1)) \geq \lambda d,$$

o que é uma contradição, pois X tem singularidades controladas.

Temos, então que $D_j^{\lambda+1}\, F = 0$, para $j = 0,1,2$.

Agora a expressão (2.1.1) nos fornece:

$$(D_i\; D_j^{\lambda}\; F)\;(F_i)^{\lambda} = -\,F_j \sum_{s=0}^{\lambda-1} (D_i^{\lambda+1-s}\; D_j^{s}\; F)\;(-F_i)^{s}\;(F_j)^{\lambda-s}.$$

Pelo mesmo raciocínio, prova-se que:

$$D_i\; D_j^{\lambda}\; F = 0, \quad \forall\; i,j = 0,1,2.$$

Seguindo passo a passo o argumento acima, obtemos

$$D_i^{m}\; D_j^{n}\; F = 0, \quad \forall\; i,j = 0,1,2, \quad \forall\; m,n,\; m+n = \lambda+1.$$

A recíproca segue trivialmente de (I - 1.5). ∎

Observação Seja $X : F = 0$ uma curva com singularidades controladas de grau d, $d = d_0 + \ldots + d_r p^r$. Se $1 \leq d_0 < p-1$ ou $d_1 < p-1$ e X é d_0-não genérica, então X é $(d_0 + \ldots + d_i p^i)$-não genérica, para todo i, $0 \leq i < r$.

A afirmação acima segue de (2.1), (A.2) e do fato que $\lambda_i + 1 = d_0 + \ldots + d_i p^i + 1$ é p-adicamente maior ou igual a $d_0 + 1$, com d_0 nas condições acima.

(2.2) Teorema *Seja $X : F = 0$ uma curva de grau d, com singularidades controladas e seja λ um inteiro tal que $d \equiv \lambda(p)$ com $1 \leq \lambda < p-1$. As seguintes afirmações são equivalentes:*

(i) X é *λ-não-genérica.*

(ii) $\eta_\lambda = p^\alpha$, *para algum* $\alpha \geq 1$.

(iii) F *é da forma* $\displaystyle\sum_{i_0+i_1+i_2=\lambda} Q_{i_0 i_1 i_2}^{p^\alpha} X_0^{i_0} X_1^{i_1} X_2^{i_2}$, *para algum* $Q_{i_0 i_1 i_2} \in K[X_0, X_1, X_2]$.

Demonstração: (i) ⇒ (ii) Sendo X λ-não genérica e com singularidades controladas, então pela proposição (2.1), temos que

$$D_{m,n,0} F = 0, \quad \forall\ m,n,\ m+n = \lambda+1$$

Segue de (A.2) que $D_{i,j,0}\, F = 0$, para todo (i,j) tal que $i+j$ é p-adicamente maior ou igual a $\lambda+1$.

Sendo $\lambda+1 < p$, temos que $D_{i,j,0}\, F = 0$, para todo (i,j) tal que $\lambda+1 \leq i+j < p^{\alpha}$, para algum $\alpha \geq 1$ e portanto $\eta_{\lambda} = p^{\alpha}$.

(ii) $\Rightarrow$ (iii) Se $\eta_{\lambda} = p^{\alpha}$ para algum $\alpha \geq 1$, então por (2.1) e por (A.4) e (A.2) tem-se que todas as derivadas de ordem $\lambda+1$ até $p^{\alpha}-1$ são nulas.

Temos então, para todo (i_0,i_1,i_2) com $i_0+i_1+i_2 = \lambda$, que:

$$D_{i}^{p^r}\,(D_{i_0 i_1 i_2}\, F) = D_{i_0 i_1 i_2}\,(D_{i}^{p^r} F) = 0,$$

para $i = 0,1,2$ e $r = 0,\dots,\alpha-1$.

Portanto, existem $Q_{i_0 i_1 i_2} \in K[X_0,X_1,X_2]$ tais que

$$D_{i_0 i_1 i_2}\, F = Q_{i_0 i_1 i_2}^{p^{\alpha}}.$$

Sendo $d \equiv \lambda(p)$ então pelo lema (A.1) tem-se que

$$F = \sum_{i_0+i_1+i_2=\lambda} Q_{i_0 i_1 i_2}^{p^{\alpha}}\, X_0^{i_0}\, X_1^{i_1}\, X_2^{i_2}.$$

(iii) $\Rightarrow$ (i) É imediata pelo teorema (I-1.5). ∎

Observação O teorema acima é uma generalização dos resultados de E. Ballico, A. Hefez e R. Pardini em [B-H], [H.1] e [P] que tratam do caso $\lambda = 1$.

(2.3) Exemplo: Curvas de Fermat

Sejam $a, b \in K^{*}$, d e λ inteiros tais que (d,λ) é admissível com $p \nmid d$ e $d > p$.

Seja,

$$X : a X_0^d + b X_1^d = X_2^d.$$

Escrevendo $d = d_0 + \ldots + d_r p^r$, das hipóteses sobre d e λ segue que $\lambda = d_0 + \ldots + d_s p^s$ com $s < r$ e $d_0 \neq 0$.

Portanto, por (2.2) tem-se que:

(2.3.1) X é λ-não genérica se, e somente se $\lambda+1 < p^{s+1}$ ou $d_{s+1}=0$.

Mais ainda, se $d = \lambda+\alpha q'$ com $p \nmid \alpha$, então $\eta_\lambda = q'$.

(2.4) Exemplo

Seja $\varphi(x) \in K[x]$ de grau n, tal que $p \nmid n$, e definamos

$$f(x,y) = \frac{\varphi(x) - \varphi(y)}{x-y}$$

Seja X a curva projetiva definida pela equação afim $f(x,,y) = 0$.

Considere as seguintes condições:

(a) $\varphi'(x) = \dfrac{d\varphi}{dx}$ tem $n-1$ raízes distintas.

(b) φ é injetiva sobre as raízes de φ'.

Em [V], Voloch obtém os seguintes resultados:

(1) X é lisa se, e somente se φ satisfaz às condições (a) e (b).

(2) Se φ satisfaz às condições (a) e (b), então X é reflexiva.

A fim de estudar a λ-genericidade da curva X, necessitamos das seguintes identidades, cujas demonstrações são imediatas

$$D_{m,0}\, f = \frac{D_x^m\, \varphi(x) - D_{m-1,0} f}{x - y}$$

$$D_{0,n}\, f = \frac{- D_y^n\, \varphi(y) + D_{0,n-1} f}{x-y}$$

$$D_{m,n}\, f = \frac{D_{m-1,n} f - D_{m,n-1} f}{x-y}$$

para $m,n \geq 1$.

(2.4.1) Proposição: *Se as condições* (a) *e* (b) *são satisfeitas por* φ *, então X é* λ*-genérica para todo truncamento* λ *de* n-1.

Demonstração: Como (a) e (b) são satisfeitas por φ, X é lisa.

Supondo X λ-não genérica, então pela proposição (2.1), temos que:

$$D_{m,n}\, f = 0, \quad \forall\ m,n,\ m+n = \lambda+1.$$

Portanto, das identidades acima segue que:

$$D_x^{\lambda+1}\, \varphi(x) = D_{\lambda,0}\, f = D_{\lambda-1,1}\, f = \ldots = D_{0,\lambda}\, f = D_y^{\lambda+1}\, \varphi(y).$$

Assim, $D_x^{\lambda+1}\, \varphi(x)$ é uma constante.

Escrevendo $\varphi(x) = \sum_{i=0}^{n} a_i\, x^i$, com $a_n \neq 0$, a condição acima implica em particular que $\binom{n}{\lambda+1} \equiv 0(p)$, o que é um absurdo, pois λ sendo truncamento de n-1, existe q' uma potência de p, tal que

$$n \equiv \lambda+1\ (q'),\ q' > \lambda+1. \qquad \blacksquare$$

3. PONTOS λ-ESTACIONÁRIOS

Assumiremos neste parágrafo que a curva irredutível $X : F = 0$ tenha grau d e que λ é um inteiro tal que (d,λ) é admissível.

Seguiremos de perto o tratamento dado por A. Hefez em [H-2], onde são estudados os pontos de inflexão.

Definição Um ponto $P \in X$ é chamado de *ponto λ-estacionário* se P é um ponto regular de X, e que para alguma desomogeneização F_* de F se tenha:

$$I(P, F_*.\tau_P^{\lambda} F_*) > \eta_{\lambda}.$$

Note que a definição acima é consistente, pois pelo teorema (1.6) tem-se que:

$$I(P, F_*.\tau_P^{\lambda} F_*) = I(P, F.\mathcal{H}_P^{\lambda} F).$$

Note também que $\mathcal{H}_P^{\lambda} F \neq 0$, para todo P regular de X, pois caso contrário $\tau_P^{\lambda} F_* = 0$, e em particular P é singular.

Para relacionar os pontos λ-estacinários com os polinômios Δ_{ij} definidos no parágrafo anterior, necessitamos do seguinte lema:

(3.1) Lema *Se* $F \in K[X_0, X_1, X_2]$ *é um polinômio homogêneo de grau* d, *e* λ *é um inteiro tal que* (d,λ) *é admissível então para todo* $i,j,\ell = 0,1,2,\ i \neq j$ *e* $\ell \neq j$ *tem-se:*

$$X_i^{\lambda+1}\ \Delta_{ij} \equiv (-X_\ell)^{\lambda+1}\ \Delta_{\ell j} \pmod F.$$

Demonstração: Como $(-X_0F_0) \equiv X_1F_1 + X_2F_2 \pmod F$, então

$$(-X_0F_0)^s \equiv \sum_{i=0}^{s} \binom{s}{i} (X_1F_1)^{s-i}\ (X_2F_2)^i. \qquad (3.1.1)$$

Substituindo (3.1.1) na expressão:

$$X_0^{\lambda+1}\ \Delta_{01} = \sum_{s=0}^{\lambda+1} X_0^{\lambda+1-s}\ D_{\lambda+1-s,s,0}F\ (F_1)^{\lambda+1-s}\ (-X_0F_0)^s,$$

e pondo $j = s-i$, obtém-se:

$$X_0^{\lambda+1}\ \Delta_{01} \equiv$$

$$\equiv \sum_{i=0}^{\lambda+1} (F_1)^{\lambda+1-i}(X_2F_2)^i [\sum_{j=0}^{\lambda+1-i} \binom{i+j}{i} D_{\lambda+1-(i+j),i+j,0}F\ X_0^{\lambda+1-(i+j)} X_1^j]$$

$$(3.1.2)$$

Pondo $r = \lambda-i$, temos que (3.1.2) é igual a:

$$X_0^{\lambda+1}\ \Delta_{01} \equiv (X_2F_2)^{\lambda+1}\ D_{0,\lambda+1,0}F\ +$$

$$+ \sum_{r=0}^{\lambda} (F_1)^{r+1}(X_2F_2)^{\lambda-r}[\sum_{j=0}^{r+1} \binom{\lambda+j-r}{j} D_{r+1-j,\lambda+j-r,0}F\ X_0^{r+1-j}\ X_1^j] \qquad (3.1.3)$$

Pelo lema (A.5), a expressão (3.1.3) pode ser escrita como

$$X_0^{\lambda+1}\ \Delta_{01} \equiv$$

$$\equiv (X_2F_2)^{\lambda+1}\ D_{0,\lambda+1,0}F + \sum_{r=0}^{\lambda} (F_1)^{r+1}(X_2F_2)^{\lambda-r}\ [(-X_2)^{r+1}\ D_{0,\lambda-r,r+1}F]$$

Pondo $k = \lambda-r$, obtemos

$$X_0^{\lambda+1}\ \Delta_{01} \equiv X_2^{\lambda+1} \sum_{k=0}^{\lambda+1} D_{0,k,\lambda+1-k}F\ (-F_1)^{\lambda+1-k}\ (F_2)^k = (-X_2)^{\lambda+1}\ \Delta_{21}.$$

As demais identidades se obtém de modo análogo. ∎

(3.2) Proposição *Seja* X : F = 0 *uma curva irredutível* λ*-genérica de grau* d, *tal que* (d,λ) *é admissível. Se* P *é um ponto regular de* X, *então* P *é um ponto* λ*-estacionário se, e somente se* $\Delta_{ij}(P) = 0$ *para* $i,j = 0,1,2$ e $i \neq j$.

Demonstração: Seja $P = (x_0 : x_1 : x_2) \in X$ um ponto λ-estacionário e suponha sem perda de generalidade que $x_2 \neq 0$.

Pelo teorema (I-1.5) temos que

$$I(P, F_*.\tau_P^\lambda F) > \eta_\lambda \text{ se, e somente se } \Delta_{01}(P) = 0.$$

Das identidades:

$$X_0^{\lambda+1}\,\Delta_{01} \equiv (-X_2)^{\lambda+1}\,\Delta_{21} \quad \text{e} \quad X_1^{\lambda+1}\,\Delta_{01} \equiv (-X_2)^{\lambda+1}\,\Delta_{20},$$

juntamente com a hipótese $x_2 \neq 0$, segue que

$$\Delta_{21}(P) = \Delta_{20}(P) = 0.$$

A recíproca é imediata por (I-1.5). ∎

Definição Seja P um ponto de X, e definamos:

$$i_P = \min\{I(P, F.\Delta_{ij}),\ i,j = 0,1,2 \text{ e } i \neq j\}.$$

Se P é um ponto regular de X, i_P é chamado de *multiplicidade do ponto estacionário P.*

(3.3) Teorema *Se* X *é uma curva* λ*-genérica de grau* d, *com* (d,λ) *admissível então*

$$\sum_P i_P = d.[d(\lambda+2) - 3(\lambda+1)].$$

Demonstração: Seja $P = (x_0:x_1:x_2)$ um ponto qualquer de X.

Caso $\mathbf{x_2 \neq 0}$.

Nesse caso temos que $i_P = I(P,F.\Delta_{01})$. (3.3.1)

De fato, das identidades:

$$X_0^{\lambda+1}\ \Delta_{01} \equiv (-X_2)^{\lambda+1}\ \Delta_{21},\quad X_1^{\lambda+1}\ \Delta_{01} \equiv (-X_2)^{\lambda+1}\ \Delta_{20}. \tag{3.3.2}$$

temos que $I(P,F.\Delta_{01}) \leq I(P,F.\Delta_{21})$ e $I(P,F.\Delta_{01}) \leq I(P,F.\Delta_{20})$, e portanto $i_P = I(P,F.\Delta_{01})$.

Caso $\mathbf{x_2 = 0}$.

Mostremos que nesse caso,

$$I(P,F.\Delta_{01}) = (\lambda+1)\ I(P,F.X_2) + i_P.$$

Se $x_0 \neq 0$ (resp. $x_1 \neq 0$), como no caso anterior temos que: $i_P = I(P,F.\Delta_{21})$ (resp $i_P = I(P,F.\Delta_{20})$).

Logo, das identidades em (3.3.2), segue que:

$$I(P,F.\Delta_{01}) = (\lambda+1)\ I(P,F.X_2) + i_P. \tag{3.3.3}$$

Por (3.3.1), (3.3.3) e pelo teorema de Bézout, tem se que:

$$\sum_P i_P + (\lambda+1)\sum_P I(P,F.X_2) = d\ [d - (\lambda+1) + (\lambda+1)(d-1)].$$

Logo,

$$\sum_P i_P = d.[d(\lambda+2) - 3(\lambda+1)].$$ ∎

(3.4) Corolário *Se* X *é uma curva de grau* d, *λ-genérica para o par* (d,λ) *admissível então o número de pontos λ-estacionários é no máximo* $d.[d(\lambda+2) - 3(\lambda+1)]$.

(3.5) Corolário *Suponha o par* (d,λ) *admissível. Contados com as suas respectivas multiplicidades, uma curva lisa de grau* d *tem* $d.[d(\lambda+2) - 3(\lambda+1)]$ *pontos* λ*-estacionários.*

Observe que o teorema acima para $\lambda = 1$, nos fornece a clássica fórmula de Plücker.

4. MORFISMO ASSINTÓTICO

Seja $X : F = 0$ uma curva irredutível de grau d, e seja λ um inteiro tal que $1 \leq \lambda < d$.

Suponhamos que alguma derivada de ordem λ de F é não nula, e definamos a aplicação racional:

$$\begin{aligned} \psi_\lambda : X &\longrightarrow \mathbb{P}^{N(\lambda)} \\ P &\longrightarrow (D_{i_0 i_1 i_2} F(P))_{i_0+i_1+i_2=\lambda} \end{aligned}$$

onde $N(\lambda) = \lambda(\lambda+3)/2$.

Se (d,λ) é um par admissível, o morfismo ψ_λ será chamado de *morfismo assintótico*.

Tem-se pelo teorema (1.6), a seguinte interpretação geométrica: ψ_λ associa a cada ponto P de um aberto afim, as coordenadas em $\mathbb{P}^{N(\lambda)}$ da curva assintótica $\tau_p^\lambda F_*$, onde F_* é uma desomogeneização de F.

Sejam $x = X_0/X_2$, $y = X_1/X_2$ e suponha sem perda de generalidade que x é uma variável separante de $K(X)$.

Ponhamos:

$$\psi_{i_0 i_1 i_2}(x,y) = D_{i_0 i_1 i_2} F(x,y,1)$$

A fim de analisar a inseparabilidade de ψ_λ, usaremos uma parametrização P(t) centrada num ponto geral P de X, como em (I-1.3).

(4.1) Proposição *Suponhamos* $1 < \lambda < p$ *tal que* $d \equiv \lambda(p)$. *Se* ψ_λ é *inseparável então* $D_x(\psi_{i_0 i_1 i_2}) = 0$ *sobre* X, *para todo* (i_0, i_1, i_2) tal que $i_0+i_1+i_2 = \lambda$.

Demonstração: Suponhamos inicialmente que $i_2 \geq 1$. Pela relação de Euler, juntamente com o fato que $d \equiv \lambda(p)$, temos que

$$X_0(i_0+1)D_{i_0+1,i_1,i_2-1}F + X_1(i_1+1)D_{i_0,i_1+1,i_2-1}F + X_2 i_2 D_{i_0 i_1 i_2}F =$$
$$= D_{i_0 i_1, i_2-1} F.$$

Logo

$$i_2\psi_{i_0 i_1 i_2}(P(t)) = \psi_{i_0 i_1, i_2-1}(P(t)) - x(t)(i_0+1)\psi_{i_0+1,i_1,i_2-1}(P(t))$$
$$- y(t)(i_1+1)\psi_{i_0,i_1+1,i_2-1}(P(t)). \qquad (4.1.1)$$

Agora, pela regra da cadeia segue que:

$$D_t\psi_{i_0,i_1,i_2-1}(P(t)) = (i_0+1)\psi_{i_0+1,i_1,i_2-1}(P(t)) +$$
$$+ (i_1+1)\, y'(t)\, \psi_{i_0,i_1+1,i_2-1}(P(t)). \qquad (4.1.2)$$

De (4.1.1) e (4.1.2) temos que

$$i_2[D_t(\psi_{i_0 i_1 i_2})\psi_{i_0+1,i_1,i_2-1} - D_t(\psi_{i_0+1,i_1,i_2-1})\, \psi_{i_0 i_1 i_2}] =$$

$$= y(t)(i_1+1) \quad [D_t(\psi_{i_0,i_1+1,i_2-1}) \quad \psi_{i_0+1,i_1,i_2-1} \quad -$$

$$- D_t(\psi_{i_0+1,i_1,i_2-1})\, \psi_{i_0,i_1+1,i_2-1}] + D_t(\psi_{i_0+1,i_1,i_2-1})\, \psi_{i_0,i_1,i_2-1}$$

(4.1.3)

Sendo ψ_λ inseparável, então por (B.1) e (4.1.3) segue que

$D_t\, (\psi_{i_0+1,i_1,i_2-1})\, (P(t)).\psi_{i_0,i_1,i_2-1}\, (P(t)) = 0$, em $K((t))$.

Se $\psi_{i_0,i_1,i_2-1}(P(t)) \neq 0$ então $D_t(\psi_{i_0+1,i_1,i_2-1})(P(t)) = 0$.

Suponha agora que $\psi_{i_0,i_1,i_2-1}(P(t)) = 0$.

Sendo $P(t)$ centrada num ponto P geral de X, tem-se que:

$$D_{i_0,i_1,i_2-1}F = 0. \qquad (4.1.4)$$

Pela regra da cadeia e por (4.1.4), levando em conta que $i_0+1 \leq \lambda < p$, segue que

$$D_t(\psi_{i_0+1,i_1,i_2-1}) = (i_0+2)\psi_{i_0+2,i_1,i_2-1}+(i_1+1)\psi_{i_0+1,i_1+1,i_2-1}y' = 0.$$

Conclui-se então que

$$D_t(\psi_{j_0 j_1 j_2}) = 0, \quad j_0 \geq 1, \quad 0 \leq j_2 < \lambda. \qquad (4.1.5)$$

Por simetria, segue também que

$$D_t(\psi_{j_0 j_1 j_2}) = 0, \quad j_1 \geq 1, \quad 0 \leq j_2 < \lambda. \qquad (4.1.6)$$

Resta então provar que $D_t(\psi_{0,0,\lambda}) = 0$.

A relação de Euler, juntamente com a condição $d \equiv \lambda(p)$ implicam que:

$$D_t(\psi_{0,0,\lambda-1}) = x(t) \; D_t(\psi_{1,0,\lambda-1}) + \psi_{1,0,\lambda-1} + y(t) \; D_t(\psi_{0,1,\lambda-1}) +$$

$$+ y'(t)\, \psi_{0,1,\lambda-1} + \lambda\, D_t(\psi_{0,0,\lambda}).$$

Assim pela regra da cadeia, temos que

$$\lambda\, D_t(\psi_{0,0,\lambda}) = -[x(t)\, D_t(\psi_{1,0,\lambda-1}) + y(t)\, D_t(\psi_{0,1,\lambda-1})]. \qquad (4.1.7)$$

De (4.1.5), (4.1.6) e (4.1.7) tem-se que $D_t(\psi_{0,0,\lambda}) = 0$ e portanto:

$$D_t\, (\psi_{i_0 i_1 i_2})\, (P(t)) = 0, \quad \forall\, (i_0, i_1, i_2),\ i_0+i_1+i_2 = \lambda \qquad (4.1.8)$$

Como pela regra da cadeia,

$$D_t(\psi_{i_0 i_1 i_2}(P(t))\ _{t=0} = D_x(\psi_{i_0 i_1 i_2})(P)$$

então de (4.1.8) temos que:

$$D_x(\psi_{i_0 i_1 i_2})(P) = 0,$$

para todo ponto P regular em X tal que $t = x - x(P)$ é um parâmetro local.

Portanto, para todo (i_0, i_1, i_2) tal que $i_0+i_1+i_2 = \lambda$, tem-se sobre X que:

$$D_x(\psi_{i_0 i_1 i_2}) = 0. \qquad \blacksquare$$

Observação O resultado acima não é válido para $\lambda = 1$, e nesse caso a inseparabilidade de ψ_1 é caracterizada pela proposição (B.1).

(4.2) Corolário *Com as mesmas hipóteses do teorema* (4.1), *tem-se que: se ψ_λ é inseparável, então $\eta_\lambda \equiv 0(p)$.*

Demonstração: Segue do teorema anterior e do lema (I-1.14). ∎

(4.3) Teorema *Se* X : F = 0 *tem singualridades controladas e* $1 < \lambda < p-1$, *então as seguintes afirmações são equivalentes:*

(i) X *é* λ-*não genérica.*

(ii) ψ_λ *é inseparável.*

Demonstração:

(i) $\Rightarrow$ (ii) O teorema (2.2) prova que se X é λ-não genérica então $\eta_\lambda = p^\alpha$, para algum $\alpha \geq 1$; e que para todo (i_0, i_1, i_2) tal que $i_0+i_1+i_2 = \lambda$ existem $Q_{i_0i_1i_2} \in K[X_0, X_1, X_2]$ tais que:

$$D_{i_0i_1i_2} F = Q_{i_0i_1i_2}(X_0^{p^\alpha}, X_1^{p^\alpha}, X_2^{p^\alpha}).$$

Assim, $\psi_{i_0i_1i_2}(P(t)) = Q_{i_0i_1i_2}((x(t))^{p^\alpha}, y(t)^{p^\alpha}, 1)$ e portanto,

$$D_t^r\,(\psi_{i_0i_1i_2}(P(t)) = 0, \quad r = 1, \ldots, p^\alpha-1.$$

Logo, por (B.1), ψ_λ é inseparável e $\deg_i \psi_\lambda \geq p^\alpha = \eta_\lambda$.

(ii) $\Rightarrow$ (i) Se ψ_λ é inseparável temos por (4.2) que $\eta_\lambda \equiv 0(p)$.

Sendo $1 < \lambda < p-1$, temos que X é λ-não genérica e por (A.2), $\eta_\lambda = p^\alpha$ para algum $\alpha \geq 1$. ∎

OBSERVAÇÕES

(4.3.1) A demonstração acima contém a seguinte informação: Nas mesmas condições de (4.3), se ψ_λ é inseparável, então $\deg_i \psi_\lambda \geq \eta_\lambda$.

(4.3.2) Para $\lambda \geq p-1$, as afirmações do teorema não são necessariamente equivalentes, como se vê no seguinte exemplo:

$$X : X_0^{p^2-1} + X_1^{p^2-1} + X_2^{p^2-1} = 0$$

X é λ-genérica para $\lambda = p-1$, mas ψ_λ é inseparável.

CAPÍTULO III

APLICAÇÕES A TEORIA DOS NÚMEROS

1. TEORIA GERAL

Seja X uma curva projetiva plana e irredutível de grau d, definida sobre um corpo finito $\mathbb{F}_q$. Denotaremos por N(X,q) o número de pontos racionais de X sobre $\mathbb{F}_q$.

Seja C : $F_* = 0$ um modêlo afim de X, e considere a família $\mathcal{F}_\lambda = (\mathcal{C}_P^\lambda F_*)_{P\in C}$.

Note que os pontos racionais afins de C estão entre os pontos para os quais é satisfeita a seguinte condição:

$$F_q(P) \in (\tau_P^\lambda F_* = 0) \tag{1.1}$$

onde F_q é o automorfismo de Frobenius.

Diremos que X é uma curva *λ-Frobenius não degenerada* se nem todos os seus pontos num aberto afim satisfazem à condição (1.1); e *λ-Frobenius degenerada*, caso contrário.

Os pontos P de C para os quais (1.1) é satisfeita são precisamente os pontos para os quais se anula a função racional:

$$h_\lambda(x,y) = \sum_{i+j=1}^{\lambda} D_{ij}(F_*)(x^q-x)^i(y^q-y)^j.$$

Assim, X é uma curva λ-Frobenius não degenerada se, e somente se h_λ é não nula sobre C.

Para as curvas λ-Frobenius não degeneradas uma cota superior para $N(X,q)$ é dada por:

$$N(X,q) \leq \frac{d.\deg h_\lambda}{I} + R \tag{1.2}$$

onde I é uma cota inferior para a multiplicidade de interseção de C com a curva $h_\lambda = 0$ num ponto racional qualquer P em C, e R é o número de pontos racionais no infinito de X que não estão sobre o fêcho projetivo da curva $h_\lambda = 0$.

Trataremos agora do caso em que as curvas assintóticas de ordem λ têm existência projetiva. Para isso definamos:

$$H_\lambda = \sum_{i_0+i_1+i_2=\lambda} D_{i_0 i_1 i_2} F\, X_0^{i_0 q} X_1^{i_1 q} X_2^{i_2 q}.$$

(1.3) Proposição *Se* (d,λ) *é um par admissível então* $h_\lambda(x,y) \equiv$
$\equiv H_\lambda(x,y,1) \pmod{F_*}$.

Demonstração: Ponha:

$$(\tau_P^\lambda F_*)(x,y) - \mathcal{H}_P^\lambda F(x,y,1) = \sum_{i,j} a_{ij}(P) x^i y^j$$

Como (d,λ) é admissível, pelo teorema (II-1.6) temos para todo $P \in C$, que

$$(\tau_p^\lambda F_*)(x,y) = \mathcal{H}_p^\lambda F(x,y,1)$$

e portanto $a_{ij} \in (F_*)$.

Assim,

$h_\lambda(x,y) - H_\lambda(x,y,1) = (\tau_{(x,y)}^\lambda F_*)(x^q,y^q) - \mathcal{H}_{(x,y)}^\lambda F(x^q,y^q,1) =$

$= \sum a_{ij}(x,y)x^{iq}y^{jq} \in (F_*)$.

Logo, $h_\lambda(x,y) \equiv H_\lambda(x,y,1) \pmod{F_*}$. ∎

(1.4) Corolário *Se* (d,λ) *é admissível então:*

(i) X *é uma curva* λ*-Frobenius degenerada se, e somente se* H_λ *é um múltiplo de* F.

(ii) *Se* X *é uma curva* λ*-Frobenius não degenerada e* $I(P, F.H_\lambda) \geq I$, *para todo* P *racional de* X, *então*

$$N(X.q) \leq d(d-\lambda+\lambda q)/I.$$

Demonstração: Imediata. ∎

Considere a seguinte condição:

(1.5) Todas as derivadas de F de ordem $\lambda+1$ até $q'-1$ são nulas, onde q' é uma potência de p.

As curvas $F = 0$ de grau d com singularidades controladas e λ-não genéricas com $1 \leq \lambda < p-1$ e $d \equiv \lambda(p)$ satisfazem à condição (1.5).

(1.6) Proposição *Seja* P *um ponto racional qualquer de* $X : F = 0$. *Tem-se então que:*

(i) $I(P, F.h_\lambda) \geq \lambda+1$.

(ii) *Se a condição* (1.5) *é verificada então,*

$$I(P, F.h_\lambda) \geq \min(q', q).$$

Demonstração: Escrevamos por simplicidade que $F_* = f$.

Para todo P racional e todo $r < q$ tem-se que:

$$D_{r,0}(x^q-x)^i(P) = D_{0,r}(y^q-y)^i(P) = \begin{cases} (-1)^i & \text{se} \quad r = i \\ 0 & \text{se} \quad r \neq i \end{cases}$$

Assim, para todo $m, n < q$ e P racional,

$$D_{mn}h_\lambda(P) = \sum_{i+j=1}^{\lambda} (-1)^{i+j} D_{m-i,n-j} (D_{ij}f)(P) =$$

$$= [\sum_{i+j=1}^{\lambda} (-1)^{i+j} \begin{bmatrix} m \\ i \end{bmatrix} \begin{bmatrix} n \\ j \end{bmatrix}] D_{mn}f(P).$$

Logo, para todo $m, n < q$ e P racional

$$D_{mn}h_\lambda(P) = a_{mn} D_{mn}f(P) \tag{1.6.1}$$

onde,

$$a_{mn} = \sum_{i+j=1}^{\lambda} (-1)^{i+j} \begin{bmatrix} m \\ i \end{bmatrix} \begin{bmatrix} n \\ j \end{bmatrix}.$$

Como, para todo $m+n < q$ tem-se que

$$a_{mn} = \begin{cases} -1 & \text{se } m+n \leq \lambda \\ -1+(-1)^\lambda \begin{bmatrix} \lambda+i-1 \\ \lambda \end{bmatrix} & \text{se } m+n = \lambda+i \end{cases}$$

então de (1.6.1) segue que

$$h_\lambda = -\tau_P^\lambda f + \sum_{i=1}^{q-(\lambda+1)} [-1 + (-1)^\lambda \begin{bmatrix} \lambda+i-1 \\ \lambda \end{bmatrix}] f_{\lambda+i} +$$

$$+ \text{(polinômio de grau maior ou igual a q)},$$

onde $f = f_1 + \ldots + f_d$ é o desenvolvimento em série de potências de f num ponto racional P.

Assim,

$$h_\lambda + f = (-1)^\lambda \sum_{i=1}^{q-(\lambda+1)} \begin{bmatrix} \lambda+i-1 \\ \lambda \end{bmatrix} f_{\lambda+i} +$$

$$+ \text{(polinômio de grau maior ou igual a q)}. \qquad (1.6.2)$$

Por (1.6.2), a asserção (i) é verificada.

Agora, se F satisfaz à condição (1.5), então:

$$f_{\lambda+1} = \dots = f_{q'-1} = 0. \qquad (1.6.3)$$

De (1.6.2) e (1.6.3) segue então para todo P racional de f=0, que:

$$I(P, f.h_\lambda) \geq \min(q, q'). \qquad \blacksquare$$

(1.7) Corolário *Se* X : F = 0 *é uma curva* λ*-Frobenius não degenerada de grau* d, *então:*

$$N(X.q) \leq \frac{d \deg h_\lambda}{\lambda+1} + R.$$

Se além disso, F *satisfaz* (1.5) *então:*

$$N(X.q) \leq \frac{d \deg h_\lambda}{\min(q', q)} + R$$

onde R *é como em* (1.2).

Demonstração: Imediata por (1.2) e (1.6). ■

(1.8) Observação Se X : F = 0 é λ-Frobenius degenerada de grau d, com (d,λ) admissível, então R pode ser omitido das desigualdades acima, pois na interseção de F = 0 e H_λ = 0 já são contados os pontos que dão origem a R.

A proposição seguinte é uma generalização da proposição 5 em [H-V], onde o caso $\lambda = 1$ é considerado.

(1.9) Proposição *Seja* $X : F = 0$ *uma curva de grau* d *e* λ *é um inteiro tal que* (d,λ) *é admissível e suponha que a condição* (1.5) *é satisfeita por* F *com* $q' \geq 2\lambda+1$. *Se* X *λ-Frobenius degenerada, então* $q' < q$ e $d \leq \lambda(q-1)/(q'-1)$.

Demonstração: A condição (1.5) juntamente com (A.6) implicam que

$$F = \sum_{i_0+i_1+i_2=\lambda} Q^{q'}_{i_0 i_1 i_2} X_0^{i_0} X_1^{i_1} X_2^{i_2},$$

para algum $Q_{i_0 i_1 i_2} \in K[X_0, X_1, X_2]$.

Logo

$$H_\lambda = \sum_{i_0+i_1+i_2=\lambda} Q^{q'}_{i_0 i_1 i_2} X_0^{i_0 q} X_1^{i_1 q} X_2^{i_2 q}.$$

Supondo por absurdo que $q' \geq q$, temos que

$$H_\lambda = \Big(\sum_{i_0+i_1+i_2=\lambda} Q^{q'/q}_{i_0 i_1 i_2} X_0^{i_0} X_1^{i_1} X_2^{i_2}\Big)^q.$$

Sendo X uma curva λ-Frobenius degenerada e F irredutível, segue de (1.4) que F divide $H_\lambda^{1/q}$, o que é um absurdo pois $\deg H_\lambda^{1/q} < \deg F$.

Portanto,

$$q' < q \quad e \quad F \text{ divide } H_\lambda^{1/q}. \tag{1.9.1}$$

Como $d = \lambda+\alpha q'$ onde $\alpha = \deg Q_{i_0 i_1 i_2}$ e $\deg H_\lambda^{1/q'} = \alpha+\lambda q/q'$, de (1.9.1) temos que $\lambda+\alpha q' \leq \alpha+\lambda q/q'$.

Logo,

$$d \leq \lambda(q-1)/(q'-1). \qquad \blacksquare$$

Daremos agora uma caracterização de uma classe de curvas λ-Frobenius degeneradas de grau $d = \lambda(q-1)/(q'-1)$, generalizando o Teorema 2 em [H-V]. Usaremos a seguir a seguinte notação: $X = X_0 X_1 X_2$ e $X^I = X_0^{i_0} X_1^{i_1} X_2^{i_2}$, onde $I = (i_0, i_1, i_2)$. Os múlti-índices que aparecerão na proposição abaixo terão todos comprimento λ.

(1.10) Proposição *Suponha que as hipóteses de* (1.9) *sejam satisfeitas e que* $d = \lambda(q-1)/(q'-1)$. X *é* λ*-Frobenius degenerada se e somente se as seguintes condições são satisfeitas:*

(i) F *é da forma* $\sum_{I_1,\dots,I_n} a^{q'^{(n-1)}}_{(I_1,\dots,I_n)} X^{I_n q'^{(n-1)}} \dots X^{I_1}$ *com* $a_{(I_1,\dots I_n)} \in \mathbb{F}_q$ *e* $n = \log_{q'} q$.

(ii) $a_{(I_1,\dots I_n)} = \rho a^{q'}_{(I_2,\dots,I_n,I_1)}$ *para algum* $\rho \in \mathbb{F}_q$ *tal que* $\rho^{d/\lambda} = 1$.

Demonstração: Como X satisfaz (1.9), de (1.9.1) tem-se que, X é

λ-Frobenius degenerada se, e só se

$$F = \sum_I Q_I^{q'} X^I \quad \text{divide} \quad H_\lambda^{1/q'} = \sum_I Q_I X^{Iq/q'}$$

ou seja, para algum μ,

$$\sum_I Q_I X^{Iq/q'} = \mu \sum_I Q_I^{q'} X^I. \qquad (1.10.1)$$

Como $d = \lambda(q-1)/(q'-1)$, os dois polinômios em (1.10.1) têm o mesmo grau, e assim $\mu \in \mathbb{F}_q$.

Supondo que X é λ-Frobenius degenerada, mostremos (i) e (ii).

Para $n = 2$, $\deg Q_I = (d-\lambda)/q' = \lambda$ e portanto,

$$Q_I^q = \sum_{I_2} a_{(I,I_2)}^{q'} X^{I_2 q'}$$

Segue então que, F é da forma (i).

Aplicando o operador diferencial $\Delta = D_{i_0 i_1 i_2}$ com $\lambda+1 < i_0+i_1+i_2 < q'$, à igualdade de (1.10.1) obtemos,

$$\sum_I (\Delta Q_I)\, X^{Iq/q'} = 0. \qquad (1.10.2)$$

Como $d = \lambda(q'^n-1)/(q'-1) = \lambda(q'^{(n-1)}+\ldots+1) < \lambda(q+1)$ e $\deg Q_I = (d-\lambda)/q'$ temos que $\deg Q_I < \lambda q/q'$.

Logo, de (1.10.2), conclui-se que $\Delta Q_I = 0$.

Assim,

$$Q_I = \sum_{I_2} Q_{(I,I_2)}^{q'} X^{I_2}. \qquad (1.10.3)$$

Substituindo (1.10.3) na expressão de F, temos que:

$$F = \sum_{I,I_2} Q_{(I,I_2)}^{q'^2} X^{I_2 q'} X^I. \qquad (1.10.4)$$

Agora, se $n = 3$, então $\deg Q_{(I,I_2)} = \lambda$ e portanto,

$$Q_{(I,I_2)} = \sum_{I_3} a_{(I,I_2,I_3)} X^{I_3},$$

que substituído em (1.10.4) nos dá que F é da forma como em (i).

Prosseguindo com esse raciocínio, por indução sobre n, temos que F é da forma (i).

Logo

$$Q_{I_1} = \sum_{I_2,\ldots,I_n} a^{q'^{(n-2)}}_{(I_1,\ldots,I_n)} X^{I_n q'^{(n-2)}} \ldots X^{I_2}.$$

Pondo $J_1 = I_n$, $J_2 = I_1, \ldots, J_n = I_{n-1}$, então F se escreve como:

$$F = \sum_{J_1,\ldots,J_n} a^{q'^{(n-2)}}_{(J_2,\ldots,J_n,J_1)} X^{J_1 q'^{(n-1)}} X^{J_n q'^{(n-2)}} \ldots X^{J_2}.$$

De (1.10.1) segue que

$$\sum_{I_1,\ldots,I_n} a^{q'^{(n-2)}}_{(I_1,\ldots,I_n)} X^{I_1 q'^{(n-1)}} X^{I_n q'^{(n-2)}} \ldots X^{I_2} =$$

$$= \mu \sum_{J_1,\ldots,J_n} a^{q'^{(n-1)}}_{(J_2,\ldots,J_n,J_1)} X^{J_1 q'^{(n-1)}} \ldots X^{J_2}.$$

Assim,

$$a^{q'^{(n-2)}}_{(I_1,\ldots,I_n)} = \mu a^{q'^{(n-1)}}_{(I_2,\ldots,I_n,I_1)} = \mu (a^{q'}_{(I_2,\ldots,I_n,I_1)})^{q'^{(n-2)}}. \quad (1.10.5)$$

Pondo $\rho = \mu^{1/q'^{(n-2)}}$, (1.10.5) se escreve como:

$$a_{(I_1,\ldots,I_n)} = \rho a^{q'}_{(I_2,\ldots,I_n,I_1)}. \quad (1.10.6)$$

Resta então, provar que $\rho^{d/\lambda} = 1$.

De fato, pela relação obtida em (1.10.6) temos que

$$a_{(I_1,\ldots,I_n)}=\rho a^{q'}_{(I_2,\ldots,I_n,I_1)}=\rho(\rho^{q'}a^{q'^2}_{(I_3,\ldots,I_n,I_1,I_2)})=\ldots=$$

$$=\rho^{1+q'+\ldots+q'^{(n-1)}}a^{q'^n}_{(I_1,\ldots,I_n)}=\rho^{d/\lambda}a_{(I_1,\ldots,I_n)}.$$

Logo, $\rho^{d/\lambda}=1$.

Reciprocamente, se F satisfaz às condições (i) e (ii) então a igualdade (1.10) é satisfeita para $\mu=\rho^{q'^{(n-2)}}$, e portanto X é λ-Frobenius degenerada. ∎

2. COTAS PARA O NÚMERO DE PONTOS RACIONAIS

Contar o número de pontos racionais de uma curva algébrica definida sobre um corpo finito $\mathbb{F}_q$, é um dos problemas clássicos da teoria dos números.

Relacionaremos neste parágrafo ascotas anteriormente conhecidas, para na próxima seção compararmos estas com a cota obtida em (1.7) para as curvas do tipo $y^n=\varphi(x)$.

(2.1) A hipótese de Riemann provada por Weil [W] nos fornece

$$N(X.q)\leq q+1+2gq^{1/2},$$

onde g denota o gênero da curva.

(2.2) K. O. Stöhr e J. F. Voloch em [S-V] demonstram os seguintes fatos:

Se X é curva plana reflexiva de grau d então:

$$N(X.q) < d(d-1+q)/2. \qquad (2.2.1)$$

Se X é uma curva não degenerada em $\mathbb{P}^N$, com sequência de Frobenius $\nu_0 = 0 < \nu_1 <\ldots< \nu_{N-1}$ então,

$$N(X.q) \leq \frac{(\nu_1+\ldots+\nu_{N-1})(2g-2)+(q+N)\deg X}{N}. \qquad (2.2.2)$$

(2.3) Seja X uma curva plana irredutível de grau d, mergulhada em $\mathbb{P}^{N(\lambda)}$, onde $N(\lambda) = \lambda(\lambda+3)/2$, pelo morfismo de Verosese ϕ_λ. Pelas proposições (2.1) e (2.3) em [S-V], tem-se que $\{\nu_1,\ldots,\nu_{N-1}\} \subset \{\varepsilon_1,\ldots,\varepsilon_N\}$ e todo inteiro p-adicamente menor que ν_i é também uma ordem, para cada i. Conclui-se então que:

(2.3.1) Se $p > N(\lambda)$ e X é ϕ_λ-clássica então X é Frobenius clássica para ϕ_λ, e (2.2.2) nos fornece a seguinte cota:

$$N_{SV}^{(\lambda)} = \frac{N(N-1)(g-1)+(q+N)\lambda d}{N}.$$

Se s(P) denota o peso de Frobenius para um ponto racional P de X, resulta de (2.4,a) em [S-V] que,

$$s(P) \geq \sum_{i=1}^{N} (\varepsilon_i-\nu_{i-1}).$$

E portanto:

(2.3.2) Se X é Frobenius clássica para ϕ_λ, então $s(P) \geq \varepsilon_N$, e uma cota para N(X.q) é dada por:

$$N'_{SV} = \frac{N(N-1)(g-1)+(q+N)\lambda d}{\varepsilon_N}.$$

A. Garcia e J. F. Voloch, em [G-V,2], obtém para as curvas de Fermat,

$$X : ax^n + by^n = 1,\ ab\neq 0 \quad e \quad p\nmid n,$$

o seguinte critério de Frobenius classicalidade.

(2.3.3) Se $p > 5$, então X é Frobenius não clássica para ϕ_2 sobre $\mathbb{F}_{p^m}$, exatamente nos seguintes casos:

(i) $p/n-1$.

(ii) $p/n-2$ e $n = 2(p^m-1)/(p^r-1)$ com $r<m$, r/m e $a,b \in \mathbb{F}_{p^r}$.

(iii) $p/2n-1$ e $n = (p^m-1)/2(P^r-1)$ com $m = tr$, t par e a^2, $b^2 \in \mathbb{F}_{p^r}$.

Se X é Frobenius clássica para ϕ_2, então:

$$N(X,q) \leq 2n\,\frac{(q+2n-1)-\ell(2n-5)}{5},$$

onde ℓ é o número de pontos racionais sobre os eixos coordenados.

Nesse caso, usaremos a seguinte notação:

$$N_{GV} = \frac{2n(q+2n-1)}{\varepsilon_5}$$

(2.4) A. Hefez e J. F. Voloch em [H-V] determinam o valor exato de $N(X,q)$ para as curvas X planas, lisas e Frobenius não clássicas

$$N(X,q) = d(q-1)-2(g-1).$$

As cotas citadas em (2.1) e (2.2.1) serão denotadas respectivamente por N_W e N_1.

3. CURVAS DO TIPO $Y^n = \varphi(x)$

Seja X o fêcho projetivo da curva irredutível,

$$C : f(x,y) = 0$$

onde $f(x,y) = y^n - \varphi(x)$, com $\varphi(x) \in \mathbb{F}_q[x]$.

Essas curvas vem sendo estudadas ao longo de muitos anos, e recentemente por M. Homma em $[H_0,2]$ quanto a reflexividade, e por A. Garcia em [G] quanto a contagem de pontos racionais. O caso especial das curvas de Fermat foi tratado em [G-V,2] e em [H-K].

Denotaremos por K o fêcho algébrico de $\mathbb{F}_q$.

A curva X é absolutamente irredutível se e somente se $p \nmid n$ e $mdc(p,r_1,\ldots,r_s) = 1$, onde r_i são as multiplicidades das raízes de $\varphi(x)$ (veja p.ex. $[H_0,2]$).

M. Homma em $[H_0,2]$ mostrou o seguinte:

TEOREMA (Homma) X é não reflexiva se e somente se $\varphi(x) \in K[x^p]$ ou $\varphi(x)$ é da forma:

$$(h_0^p(x) + h_1^p(x))^r\, g^p(x)$$

para algum $g, h_0, h_1 \in K[x]$ com $mdc(h_0, h_1) = 1$ ealgum r com $1 \leq r < p$ tal que $r \equiv n(p)$.

(3.1) OBSERVAÇÃO Se $\varphi(x)$ tem pelo menos uma raiz simples, então, X não é reflexiva se e somente se $\varphi(x)$ é da forma:

$$g_0^p(x) + g_1^p(x)x \quad \text{e} \quad n \equiv 1(p).$$

(3.2) Com algumas exceções (p.ex. $\deg f < p$) podemos tornar a curva C, λ-não genérica para algum λ, com o argumento que descreveremos a seguir.

Suponha $n = n_0 + \ldots + n_t p^t$, $n_t \neq 0$ e $\varphi(x) = a_0 + a_1 x^{m_1} + \ldots + a_\ell x^{m_\ell}$, tal que $\deg\varphi = m_\ell$.

Para $j = 1, \ldots, \ell$, escrevamos:

$$m_j = b_{0j} + b_{1j}p + \ldots + b_{Mj}p^M \text{ , com } b_{M\ell} \neq 0.$$

Para cada i, $0 \leq i < \max\{t, M\}$, definamos:

$$\lambda(i) = \max\{n_0 + \ldots + n_i p^i;\ b_{0j} + \ldots + b_{ij}p^i,\ j = 1, \ldots, \ell\}.$$

Assim,

$$n = u_i + \alpha_i p^{i+1},\ m_j = v_{ij} + \beta_{ij}p^{i+1},$$

para algum u_i, $v_{ij} \leq \lambda(i)$, $j = 1, \ldots, \ell$.

Portanto, $f = y^n - \varphi(x)$ assumirá a forma:

$$y^{u_i + \alpha_i q_i'} - (g_0^{q_i'} + g_1^{q_i'}x + \ldots + g_{\lambda(i)}^{q_i'}x^{\lambda(i)})$$

onde $q'_i = p^{i+1}$ e $g_k \in K[x]$, $k = 0,\dots,\lambda(i)$.

Para cada i tal que $\lambda(i)+1 < q'$ ou $n_{i+1} = b_{i+1,j} = 0$ para $j = 1,\dots,\ell$, temos que C é $\lambda(i)$-não genérica com $\eta_{\lambda(i)} \geq q'_i$, pois nesses casos, temos que:

$$D_{rs}(y^n-\varphi(x)) = 0, \quad r+s = \lambda(i)+1;$$

para r, s tais que $\lambda(i)+1 \leq r+s < q'_i$.

Observe que com o procedimento acima, não temos necessariamente que $\lambda(i)$ seja um truncamento do grau f.

O nosso método para determinar cotas, consiste em escolher $\lambda(i)$, para o qual a curva seja $\lambda(i)$-não genérica e $\lambda(i)$-Frobenius não degenerada, de modo que em (1.2) se tenha um valor grande para I.

A fim de estudar a Frobenius degeneração das curvas λ-não genéricas suporemos $\varphi(x)$ da forma:

$$g_0^{q'} + g_1^{q'}x + \dots + g_\lambda^{q'}x^\lambda,$$

onde $\lambda = \lambda(i)$ e $q' = p^{i+1}$ para algum i. Nesta situação temos que $\lambda < q' < \deg f$.

Observação Se $\mathrm{mdc}(n,q-1) = 1$ podemos reduzir a curva $y^n = \varphi(x)$ à curva $y = \varphi(x)$ com o mesmo número de pontos racionais mediante um automorfismo de $\mathbb{F}_q^*$; além disso se $\deg \varphi > q$, substituindo os termos de φ da forma x^{sq+r} por x^{s+r}, obtemos um polinômio $\psi(x)$, com $\deg\psi < q$, de modo que as curvas $y^n = \varphi(x)$ e $y^n = \psi(x)$ têm o mesmo número de pontos racionais. Assim, sem perda de generalidade suporemos daqui por diante que $n/(q-1)$ e $\deg \varphi < q$.

(3.3) Lema *Seja* $\varphi(x) = \sum_{i=0}^{\lambda} g_i^{q'} x^i$, *com* $\lambda < q' < q$. *Se* $n \equiv u(q')$ *com* $u \leq \lambda$, *então* $h_\lambda + f = y^{n+u(q-1)} - \sum_{i=0}^{\lambda} g_i^{q'} x^{iq}$.

Demonstração: Sendo

$$h_\lambda = \sum_{i=1}^{\lambda}\left[\binom{n}{i} y^{n-i}(y^q - y)^i - (D_x^i\,\varphi)(x^q - x)^i\right]$$

mostremos inicialmente que:

$$\sum_{i=1}^{\lambda}\binom{n}{i} y^{n-i}(y^q - y)^i = y^{n+u(q-1)} - y^n. \tag{3.3.1}$$

Podemos escrever o lado esquerdo de (3.3.1) sob a forma:

$$\sum_{i=1}^{\lambda}\binom{n}{i}\sum_{j=0}^{i}(-1)^j\binom{i}{j} y^{n+(i-j)(q-1)} = \sum_{i=1}^{\lambda}\ \sum_{t=0}^{i}(-1)^{i-t}\binom{i}{t}\binom{n}{i} y^{n+t(q-1)} =$$

$$= -y^n + \sum_{t=1}^{\lambda}\left[\sum_{i=t}^{\lambda}(-1)^{i-t}\binom{i}{t}\binom{n}{i}\right] y^{n+t(q-1)}. \tag{3.3.2}$$

Como $n \equiv u(q')$ e $u \leq \lambda < q'$, então:

$$\binom{n}{i} \equiv \binom{u}{i},\ 0 \leq i \leq u \text{ e } \binom{n}{i} \equiv 0,\ u < i \leq \lambda\,.$$

Portanto,

$$\binom{i}{t}\binom{n}{i} \equiv \binom{i}{t}\binom{u}{i} = \binom{u}{t}\binom{u-t}{i-t}.$$

Assim, pondo $j = i-t$, (3.3.2) é igual a:

$$-y^n + \sum_{t=1}^{\lambda}\binom{u}{t}\left[\sum_{j=0}^{u-t}(-1)^j\binom{u-t}{j}\right] y^{n+t(q-1)} = -y^n + y^{n+u(q-1)}. \tag{3.3.3}$$

Resta provar que

$$\varphi(x) + \sum_{j=0}^{\lambda} (D_x^j\varphi)(x^q-x)^j = \sum_{i=0}^{\lambda} g_i^q\ x^{iq}. \tag{3.3.4}$$

Desenvolvendo $(x^q-x)^j$, para $j = 1,\ldots,\lambda$, podemos escrever o lado esquerdo de (3.3.4) sob a forma:

$$\sum_{i=0}^{\lambda} x^{iq} \sum_{s=1}^{\lambda} (-1)^{s-i} \begin{bmatrix} s \\ i \end{bmatrix} x^{s-i}\ D_x^s\varphi. \tag{3.3.5}$$

Como $D_x^s\varphi = \sum_{t=s}^{\lambda} \begin{bmatrix} t \\ s \end{bmatrix} x^{t-s}\ g_t^{q'}$, segue que (3.3.5) é igual a:

$$\sum_{i=0}^{\lambda} x^{iq} \sum_{s=i}^{\lambda} \sum_{t=s}^{\lambda} (-1)^{s-i} \begin{bmatrix} s \\ i \end{bmatrix} \begin{bmatrix} t \\ s \end{bmatrix} x^{t-i}\ g_t^{q'}. \tag{3.3.6}$$

Sendo $\begin{bmatrix} s \\ i \end{bmatrix} \begin{bmatrix} t \\ s \end{bmatrix} = \begin{bmatrix} t \\ i \end{bmatrix} \begin{bmatrix} t-i \\ s-i \end{bmatrix}$, pondo $r=s-i$, (3.3.6) se escreve como

$$\sum_{i=0}^{\lambda} x^{iq} \sum_{t=i}^{\lambda} \begin{bmatrix} t \\ i \end{bmatrix} \left[\sum_{r=0}^{t-i} (-1)^r \begin{bmatrix} t-i \\ r \end{bmatrix} \right] x^{t-i}\ g_t^{q'} = \sum_{i=0}^{\lambda} x^{iq}\ g_i^{q'}. \tag{3.3.7}$$

De (3.3.3) e (3.3.7), conclui-se que:

$$h_\lambda + f = y^{n+u(q-1)} - \sum_{i=0}^{\lambda} g_i^{q'} x^{iq}. \qquad \blacksquare$$

A proposição a seguir é uma generalização do Teorema 2 em [G], onde é tratado o caso $\lambda = 1$.

(3.4) Proposição *Seja* $\varphi(x) = \sum_{i=0}^{\lambda} g_i^{q'} x^i$ *com* $\lambda < q' < q$ *e suponha* $n \equiv u(q')$ *com* $u \leq \lambda$. *Se a curva* $C : y^n = \varphi(x)$ *é* λ*-Frobenius degenerada, então existe um inteiro* μ *tal que:*

$\mu \equiv -1\ (q')$, $n = u(q-1)/\mu$ e $h_\lambda + f = y^{n(\mu+1)} - \varphi(x)^{\mu+1}$.

Demonstração: Pelo lema anterior,

$$h_\lambda + f = y^{n+u(q-1)} - \sum_{i=0}^{\lambda} g_i^{q'} x^{iq}.$$

Se C é λ-Frobenius degenerada, então sobre C, tem-se que:

$$y^{n+u(q-1)} = \sum_{i=0}^{\lambda} g_i^{q'} x^{iq}.$$

Assim, a função racional y satisfaz a condição:

$$y^{n+u(q-1)} \in \mathbb{F}_q(x). \tag{3.4.1}$$

Pela irredutibilidade de $f = y^n - \varphi(x)$, segue que n é o menor inteiro positivo para o qual $y^n \in \mathbb{F}_q(x)$.

Portanto de (3.4.1), temos que $u(q-1) \equiv 0(n)$. Logo, existe um inteiro μ tal que:

$$n = u(q-1)/\mu$$

e

$$\varphi(x)^{\mu+1} = y^{n(\mu+1)} = y^{n+u(q-1)} = \sum g_i^{q'} x^{iq}. \tag{3.4.2}$$

De (3.4.1) e (3.4.2), tem-se que,

$$h_\lambda + f = y^{n(\mu+1)} - \varphi(x)^{\mu+1}.$$ ∎

(3.5) Corolário *Seja* $\varphi(x) = \sum_{i=0}^{\lambda} g_i^{q'} x^i$ *com* $\lambda < q' < q$ *e suponha* $n = u+\alpha q'$ *com* $u \leq \lambda$. *Se a curva* $C : y^n = \varphi(x)$ *é λ-Frobenius degenerada então:*

$$\deg h_\lambda = \frac{uq+\alpha q'}{n} \deg C.$$

(3.6) Proposição *Seja* $X : x^d + y^d + 1 = 0$, *com* $p \nmid d$ *e seja* λ *um inteiro positivo tal que* $d = \lambda+\alpha q'$ *com* $p \nmid \alpha$. *Tem-se que* X *é*

λ-Frobenius degenerada se, e somente se $d = \lambda(q-1)/(q'-1)$.

Demonstração: Sendo $d = \lambda+\alpha q'$, pelo lema (3.3) tem-se que:

$$h_\lambda+f = (x^{\lambda q/q'+\alpha} + y^{\lambda q/q'+\alpha} + 1)^{q'}.$$

Agora, X é λ-Frobenius degenerada se e somente se f divide

$$g = x^{\lambda q/q'+ \alpha} + y^{\lambda q/q'+ \alpha} + 1.$$

Como $p\nmid\alpha$, a curva de Fermat $g = 0$ é irredutível, e portanto $f = g$.

Assim,

$$d = \lambda q/q' + \alpha = \lambda(q-1)/(q'-1). \qquad \blacksquare$$

Agora, como teremos que considerar curvas assintóticas que possam não existir projetivamente, devemos fazer uma análise mais aprimorada dos pontos racionais comuns à X e a curva $h^*_\lambda = 0$, no infinito.

(3.7) Lema *Sejam* $\varphi(x) = \sum_{i=0}^{v} g_i^{q'} x^i$ *tais que* $\deg\varphi = m$, $g_v \neq 0$, *com* $\deg_v = \beta$ e $n = u + \alpha q'$. *Suponha* $m < q$, $n/(q-1)$ *e ponha* $\lambda = \max\{u,v\}$. *Seja X o fêcho projetivo da curva* $y^n = \varphi(x)$. *Tem-se que:*

(i) *Se* $n \neq m$, *então X possui um único ponto no infinito* P_∞.

Para $n < m$, *tem-se que* $P_\infty \in (h^*_\lambda = 0)$ *se, e somente se* $u = v$ e $\alpha < \beta$.

Para $n > m$, *tem-se que* $P_\infty \in (h^*_\lambda = 0)$ *se, e somente se* $v < u$

ou $v = u$ e $\beta < \alpha$.

Em ambos os casos, tem-se que:

$I(P_\infty, F.h_\lambda^*) > [|v-u|q/q' + |\beta-\alpha|]|m-n|q'$.

(ii) *Se* $n = m$, *então* X *possui* n *pontos no infinito.*

Para $u = \lambda$, *tem-se que* X *e* $h_\lambda^* = 0$ *têm os mesmos pontos racionais no infinito.*

Para $u < \lambda$, *tem-se que* X *e* $h_\lambda^* = 0$ *não têm pontos racionais comuns no infinito.*

Demonstração: Verifica-se facilmente que se $n < m$ (resp. $n > m$) então $P_\infty = (0:1:0)$ (*resp.* $P_\infty = (1:0:0)$) é o único ponto no infinito de X.

Pelo lema (3.3), temos que

$$h_\lambda + f = y^{uq+\alpha q'} - \sum_{i=0}^{v} g_i^{q'} x^{iq}. \tag{3.7.1}$$

Caso $n < m$.

De (3.7.1), segue que $P_\infty \in (h_\lambda^* = 0)$ se, e somente se:

$$uq + \alpha q' < vq + \beta q'$$

e isto, em presença das nossas hipóteses, é equivalente a $u < v$ ou, $u = v$ e $\alpha < \beta$.

Nesse caso, temos também de (3.7.1) que:

$$h_\lambda^* + z^{vq+\beta q'-m} f^* = y^{uq+\alpha q'} z^{(v-u)q+(\beta-\alpha)q'} - \left[\sum_{i=0}^{v} g_i^{q'} x^{iq}\right]^*. \tag{3.7.2}$$

De (3.7.2) tem-se que:

$$m_{P_\infty}(h_\lambda^* + z^{vq+\beta q'-m} f^*) \geq [(v-u)q/q' + (\beta-\alpha)]q'. \tag{3.7.3}$$

A hipótese $n < m$ implica trivialmente que:

$$m_{P_\infty}(F) \geq m-n. \qquad (3.7.4)$$

Como f^* e $h_\lambda^* + z^{vq+\beta q'-m} f^*$ têm no ponto P_∞ tangentes comuns, então de (3.7.3) e (3.7.4) conclui-se que:

$$I(P_\infty, F.h_\lambda^*) > [(v-u)q/q' + (\beta-\alpha)](m-n)q'.$$

Caso $n > m$.

De (3.7.1) segue que $P_\infty \in (h_\lambda^* = 0)$ se e somente se

$$vq + \beta q' < uq + \alpha q'$$

e isto é equivalente, em vista das nossas hipóteses a $v < u$ ou $v = u$ e $\beta < \alpha$.

Nesse caso, (3.7.1) nos fornece:

$$1_\lambda^* + z^{uq+\alpha q'-n}f^* = y^{uq+\alpha q'} - z^{(u-v)q+(\alpha-\beta)q'}\left[\sum_{i=0}^{v} g_i^{q'} x^{iq}\right]^*. \qquad (3.7.5)$$

De (3.7.5) tem-se que

$$m_{P_\infty}(h_\lambda^* + z^{uq+\alpha q'-n}F) \geq [(u-v)q/q' + (\alpha-\beta)]q'. \qquad (3.7.6)$$

Sendo $n > m$, temos que

$$m_{P_\infty}(F) \geq n-m.$$

Como f^* e $h_\lambda^* + z^{uq+\alpha q'-n} f^*$ têm no ponto P_∞ tangentes comuns, então de (3.7.5) e (3.7.6) conclui-se que:

$$I(P_\infty, F.h_\lambda^*) > [(v-u)q/q' + (\alpha-\beta)](n-m)q'.$$

(ii) Se $n = m$, então o conjunto dos pontos no infinito de X é:

$$A = \{(1:y:0):\ y^n = a_n\},$$

onde $\varphi(x) = \sum_{i=0}^{n} a_i x^i$ com $a_n \neq 0$.

Sendo $n/(q-1)$, temos que $\#A = n$.

Se $u = \lambda$, então $m = \lambda+\alpha q' = v+\beta q'$.

Nesse caso, o conjunto dos pontos no infinito de $h_\lambda^* = 0$ é:

$$\{(1:y:0):\ y^{\lambda q+\alpha q'} = a_n\}.$$

Como, $y^n = y^{\lambda q+\alpha q'}$ para $y \in \mathbb{F}_q$, temos que a asserção (ii) é verificada no caso $u = \lambda$.

Se $u < \lambda$, então $v = \lambda$ e $uq'+\alpha q' < \lambda q+\beta q'$.

Portanto, $(0:1:0)$ é o único ponto no infinito de $h_\lambda^* = 0$, e não pertence a A. ∎

(3.8) Proposição *Com as mesmas notações de* (3.7), *se* X *é uma curva* λ*-Frobenius não degenerada, tem-se que:*

(i) *Se* $n \neq m$ *e* $P_\infty \in (h_\lambda^* = 0)$, *então*

$$N(X.q) \leq \frac{\deg X\ \deg h_\lambda}{q'} - [|u-v|q/q' + |\alpha-\beta|]|n-m|.$$

Se $n \neq m$ *e* $P_\infty \in (h_\lambda^* = 0)$, *então* $N(X.q) \leq \dfrac{\deg X\ \deg h_\lambda}{q'} + 1.$

(ii) *Se* $m = n$ *e* $u = \lambda$, *então* $N(X,q) \leq \dfrac{n\ \deg h_\lambda}{q'}$.

Se $m = n$ *e* $u < \lambda$, *então* $N(X,q) \leq \dfrac{n\ \deg h_\lambda}{q'} + n.$

Demonstração:

(i) Se $n \neq m$ e $P_\infty \in (h_\lambda^* = 0)$ então pelo teorema de Bézout e por (3.7) tem-se que:

$$N(X,q') \leq [\deg F \deg h_\lambda^* - (I(P_\infty, F.h_\lambda^*)-q')]/q' \leq$$

$$\leq \frac{\deg F \deg h_\lambda^*}{q'} - [|u-v|q/q' + |\alpha-\beta|]|m-n|.$$

Se $P_\infty \in (h_\lambda^* = 0)$ e $n < m$ (resp. $n > m$) então $\deg h_\lambda^* = \lambda q+\beta q'$ e $v = \lambda$ (resp. $\deg h_\lambda = \lambda q+\alpha q'$ e $u = \lambda$).

Se $P_\infty \notin (h_\lambda^* = 0)$ e $n < m$ (resp. $n > m$) então $\deg h_\lambda^* = \lambda q+\alpha q'$ (resp. $\deg h_\lambda^* = \lambda q+\beta q'$). O resultado decorre trivialmente de (1.7).

(ii) Se $n = m$ e $u = \lambda$ (resp. $u < \lambda$) então $R = 0$ (resp. $R = n$), onde R é como em (1.7). ∎

(3.9) Denotaremos por N_λ a cota obtida em (3.7). Como a escolha de λ pode ser efetuada de diversas maneiras como descrito em (3.2), a melhor cota pode ser obtida calculando para cada λ, as expressões em (3.7).

Observe ainda, que a cota:

$$N'_\lambda = \frac{d[\lambda q + \max(\alpha,\beta)q']}{q'} + 1$$

majora N_λ para cada caso considerado em (3.7).

Basta notar, para $m = n$ e $u < \lambda$, que $\deg h_\lambda^* = \lambda q+\beta q'$.

Assim, $\alpha > \beta$ e $N_\lambda = n(\lambda q+\beta q')/q' + n = n(\lambda q+\beta q'+q') \leq$ $\leq n(\lambda q+\alpha q')/q' < N'_\lambda$.

Suporemos a partir daqui que a curva $y^n = \varphi(x)$ seja irredutível de grau d, com φ separável.

Daremos a seguir, condições suficientes para que a cota N'_λ melhore cada uma das cotas mencionadas no parágrafo 2.

Utilizando-se da cota N_λ, podemos em cada caso considerado em (3.7), obter condições mais precisas.

(3.10) Comparação com a Cota de Weil

Sendo φ separável, tem-se que $g = (m-1)(n-1)/2$ e a cota de Weil é dada por:

$$N_w = q + 1 + (m-1)(n-1)q^{1/2}.$$

(3.10.1) Se $q^{1/2}+1 \leq m,\ n \leq q/q'$, ou $q^{1/2}\lambda/q'+1 \leq m,\ n < (\sqrt{5}-1)q^{1/2}/2$, então $N'_\lambda < N_W$.

De fato:

Supondo $q^{1/2}+1 \leq m \leq n < q/q'$ temos que

$$N_w - N'_\lambda = nq + [(m-1)q^{1/2} - q] - \lambda q/q' - n.\max(\alpha,\beta) >$$
$$> n(qq' - \lambda q)/q' - n^2 \geq n(q/q' - n).$$

Supondo $q^{1/2}\lambda/q' + 1 \leq m \leq n < (\sqrt{5}-1)q^{1/2}/2$ temos,

$$N_w - N'_\lambda = q + [n(m-1)q^{1/2} - (m-1)q^{1/2}] - n\lambda q/q' - n\max(\alpha,\beta) >$$
$$> [n(m-1)q^{1/2} - n\lambda q/q'] + (q - nq^{1/2} - n^2) \geq 0.$$

Se $n \geq m$, a desigualdade é verificada por simetria, pois nesse caso $\max(\alpha,\beta) < m$. ∎

(3.11) Comparações com as cotas de StÖhr-Voloch

Se X é reflexiva e $p > 2$, então

$$N^{(1)}_{sv} = \frac{1}{2}[(m-1)(n-1) - 2 + (q+2)d].$$

(3.11.1) Se $\lambda \leq q'/3$ e $m, n \leq q/6$ então: $N'_\lambda < N^{(1)}_{sv}$.

Supondo $n \geq m$, então $N^{(1)}_{sv} = \frac{1}{2}[mn - 1 + (n-m) + nq]$, e portanto

$$N^{(1)}_{sv} - N'_\lambda \geq \frac{1}{2}(mn-3) + nq/2 - n\lambda q/q' - n\max(\alpha,\beta) >$$

$$> (nq/3 - n\lambda q/q') + (nq/6 - n^2).$$

O caso $n < m$, segue de modo análogo. ∎

Se X é ϕ_2-clássica e $p > 5$, então:

$$N^{(2)}_{sv} = 2((m-1)(n-1)-2) + (q+5)2n/5.$$

(3.11.2) Se $\lambda \leq q'/5$ e $m, n \leq q/5 - 2$, então $N'_\lambda < N^{(2)}_{sv}$

Supondo $n \geq m$, nas condições acima

$$N^{(2)}_{sv} - N'_\lambda = (2mn-3) - 2m + 2nq/5 - n\lambda q/q' - n\max(\alpha,\beta) >$$

$$> nq(1/5 - \lambda/q') + n(q/5 - n) - 2m > 2(n-m).$$

O caso $n < m$ segue de modo análogo. ∎

(3.12) Comparação com a cota N_1

Se X é reflexiva então por (2.2.1) temos que:

$$N_1 = d(d - 1 + q)/2.$$

(3.12.1) Se $\lambda < q'/2$ então $N'_\lambda < N_1$.

Se $n \geq m$ e $\lambda < q^{1/2}$ então,

$$N_1 - N'_\lambda = n(n-1+q)/2 - n(\lambda q/q' - \max(\alpha,\beta)) - 1 > n(q/2 - \lambda q/q') +$$

$$+ n[(n-1)/2 - \max(\alpha,\beta)] - 1 \geq n-1.$$

A última desigualdade segue do fato que:

$\alpha < \alpha q'/2 \leq (n-1)/2$ e $\beta < \beta q'/2 \leq (m-v)/2 \leq (n-1)/2$.

Se $n < m$, a desigualdade é igualmente satisfeita. ∎

(3.13) Comparação com cota Trivial

Se $n \neq m$, então X possui um único ponto no infinito. Se $n<m$, então $\varphi(x)$ assume no máximo q valores em $\mathbb{F}_q$, e para cada valor de $\varphi(x)$, a equação $y^n = \varphi(x)$ tem no máximo n valores, segue então que X tem no máximo $nq + 1$ pontos racionais.

Se $n > m$, temos de modo análogo que X tem no máximo $mq + 1$ pontos racionais. Obtendo assim, uma cota trivial:

$$N_{TR} = \min(n,m)q + 1$$

(3.13.1) Se $q' \geq 2\lambda$ e $m < n \leq mq'/2\lambda$, ou $n < m \leq nq'/2\lambda$, então $N'_\lambda < N_{TR}$.

Supondo $m < n \leq mq'/2\lambda$, temos que

$$N_{TR} - N'_\lambda = mq - n\lambda q/q' - n\max(\alpha,\beta) =$$

$$= m(q/2 - n\lambda q/q') + (mq/2 - n\max(\alpha,\beta) \geq mq/2 - n\max(\alpha,\beta) > 0.$$

A última desigualdade ocorre devido às desigualdades:

$mq/2 > n\lambda q/q'$, $\alpha < nq' < \lambda q/q'$ e $\beta < m/q' < \lambda q/q'$.

Para $n < m \leq nq'/2\lambda$, obtém-se a desigualdade por simetria. ∎

(3.14) Exemplos

A fim de construir exemplos de curvas $y^n = \varphi(x)$ de modo que

$n/q-1$ com $q = p^{\alpha}$, utilizamos do seguinte fato:

Como $x^{\alpha}-1 = \prod_{r/\alpha} \phi_r(x)$, onde ϕ_r são os polinômios ciclotômicos em $\mathbb{Z}[x]$, então os divisores próprios de $\prod_{r/\alpha} \phi_r(p)$ nos fornecem alguns valores para n, que satisfazem a condição: $n/p^{\alpha}-1$.

Nos três primeiros exemplos abaixo, embora não sabendo decidir se a curva é ou não Frobenius clássica para ϕ_2, comparamos a nossa cota com $N_{SV}^{(2)}$, visto que esse número é menor ou igual a cota dada em (III - 2.2.2).

(3.14.1) Seja $X : y^{(p-1)+(p-1)p^2} = x^{2+p^3} + 1$, definida sobre $\mathbb{F}_{p^8}$ com $p > 5$.

Tomando-se $\lambda = p-1$, temos que $n = \lambda + (p-1)p^2$, $m = 2 + p^3$ e $q' = p^2$.

Sendo $\deg h_{\lambda} = (p-1)p^8 + (p-1)p^2 = uq + \alpha q'$, então:

$$\deg h_{\lambda} \neq (uq + \alpha q')m.$$

Logo, por (3.5), X é λ-Frobenius não degenerada.

Como $n < m$ e $u = p-1 > 2 = v$, temos de (3.7) que $P_{\infty} \notin (h_{\lambda}^{*}=0)$, e portanto,

$$N_{\lambda} = \frac{m(uq + \alpha q')}{q'} +1 = (p-1)+p+(p-1)p^3+(p-2)p^6+p^7+(p-1)p^9.$$

Sendo X reflexiva por (3.1), e $p \neq 2$ temos que

$$N_1 = (2 + 3p^3 + p^6 + 2p^8 + p^{11})/2$$

e

$$N_{SV}^{(1)} = (p + (p-1)p^2 + p^4 + (p-1)p^5 + 2p^8 + p^{11})/2.$$

Temos ainda,

$$N_W = 1 + (p-2)p^4 + (p-1)p^6 + (p-2)p^7 + p^8 + (p-1)p^9 ,$$

$$N_{TR} = 1 + (p-1)p^8 + (p-1)p^{10}$$

e

$$N_{SV}^{(2)} = 2[(p-2) + (p-1)p^2 + (p-1)p^3 + (p-1)p^5] + (4 p^8 + 2 p^{11})/5.$$

Obtendo assim, as seguintes desigualdades:

$$N_\lambda < N_W < N_{SV}^{(2)} < N_{SV}^{(1)} < N_1. \qquad \blacksquare$$

(3.14.2) Seja $X : y^{(p-1)+(p-1)p^2} = x^{(p-1)+p^3} + 1$ definida sobre $\mathbb{F}_{p^8}$, com $p > 5$.

Tomando-se $\lambda = p-1$, temos que $n = \lambda + (p-1)p^2$, $m = \lambda + p^3$ e $q' = p^2$.

Como $\deg h_\lambda = (p-1)p^8 + p^3$ e $uq + \alpha q' = (p-1)p^8 + (p-1)p^2$, tem-se que:

$$m \deg h_\lambda \neq n(uq + \alpha q')$$

Assim, por (3.5) X é λ-Frobenius não degenerada.

Sendo $n < m$, $u = v = \lambda$ e $\alpha = p-1 < p = \beta$, temos que $P_\infty \in (h_\lambda^* = 0)$.

Logo, de (3.8) segue que,

$$N_\lambda = \frac{m(\lambda q + \beta q')}{q'} + [(\lambda-u)q/q' + (\beta-\alpha)]\ (m-n) =$$

$$= (p-1)p + (p-1)p^2 + (p-1)^5 + p^6 + (p-2)p^7 + (p-1)p^9.$$

Como X é reflexiva por (3.1), e $p \neq 2$, temos,

$$N_1 = [2 + (p-3)p + (p-3)p^3 + p^4 + p^6 + (p-1)p^8 + p^{11}]/2$$

$$N_{SV}^{(1)} = [(p-2)p + 2p^2 + (p-3)p^3 + p^4 + (p-1)p^5 + (p-1)p^8 + p^{11}]/2.$$

Além disso,

$$N_W = 1 + 2p^4 + (p-3)p^5 + (p-5)p^7 + 2p^8 + (p-1)p^9,$$

$$N_{TR} = 1 + (p-1)p^8 + (p-1)p^{10}$$

e

$$N_{SV}^{(2)}=2[1 + (p-3)p + 2p^2 + (p-4)p^3 + p^4 + p^5] + 2[(p-1)p^8 + p^{11}]/5.$$

Logo,

$$N_\lambda < N_W < N_{TR} < N_{SV}^{(2)} < N_{SV}^{(1)} < N_1. \qquad \blacksquare$$

(3.14.3) Seja $X : y^{(p-1)+p+(p-2)p^2} = x^{(p-1)+2p+p^2} + x^{3p} + 1$, definida sobre $\mathbb{F}_{p^6}$, com $p > 5$.

Tomando-se $\lambda = 3p$, temos que $\deg h_\lambda = 3p^7$ e $uq+\alpha q' = (p-1)p^6 + p^7 + (p-2)p^2$.

Como $\deg X = n$ e $\deg h_\lambda \neq uq + \alpha q'$, temos por (3.5) que X é λ-Frobenius não degenerada.

Sendo $n > m$ e $u = (p-1) + p < 3p = v = \lambda$, então por (3.7) tem-se que $P_\infty \notin (h_\lambda^* = 0)$.

Assim, de (3.8) segue que,

$$N_\lambda = 3n\, p^5 + 1$$

De (3.1) tem-se que:

$$N_1 = n[(p-2) + p + (p-2)p^2 + p^6]/2,$$

$$N_{SV}^{(1)} = [n((p-2) + 2p + p^2 + p^6) + p + (p-3)p^2 + p^3]/2.$$

Além disso,

$$N_W = 1 + p^6 + (n-1)((p-2) + 2p + p^2),$$

$$N_{TR} = 1 + (p-1)p^6 + 2p^7 + p^8$$

e

$$N_{SV}^{(2)} = 2(n-1)[(p-1) + 2p + p^2] + 2n(p^6 + 5)/5.$$

Obtendo assim,

$$N_\lambda < N_W < N_{TR} < N_{SV}^{(2)} < N_{SV}^{(1)} < N_1. \qquad \blacksquare$$

Apresentaremos a seguir dois exemplos de curvas de Fermat, cujo grau não é obtido através de polinômios ciclotômicos.

(3.14.4) Seja $X : x^{240} + y^{240} + 1 = 0$, definida sobre $\mathbb{F}_{7^4}$.

Sendo $n = 240 = 2 + 6.7 + 4.7^2$, então para $\lambda = 2$, temos que X é 2-não genérica e $q' = 7$.

Como $n \neq 2(7^4-1)/(7-1)$, temos por (3.6) que X é 2-Frobenius não degenerada, e

$$N_2 = n(n-2 + 2q)/q' = 720n.$$

Agora, sendo $n \not\equiv 1(7)$ e $n \equiv 2(7)$ temos que X é reflexiva e ϕ_2-não clássica com $\varepsilon_5 \geq 7$(veja Teorema 2, [G-V,1]).

Além disso, sendo $n \neq 2(7^4 - 1)/(7^r - 1)$ para $r = 1, 2$, temos por (2.2.1) e (2.3.3) que:

$$N_1 = n(n-1 + q)/2 = 1260n, \qquad N_{GV} = 2n(q+2n - 1)/7 > 822n.$$

Agora, como X é lisa tem-se que

$$N_W = 7^4 + 1 + (n-1)(n-2)\, 7^2.$$

Assim,

$$N_2 < N_{GV} < N_1 < N_W. \qquad \blacksquare$$

(3.14.5) Seja $X : x^{480} + y^{480} + 1 = 0$, definida sobre $\mathbb{F}_{7^4}$.

Sendo $n = 480 = 4 + 5.7 + 2.7^2 + 7^3$, temos para $\lambda = 4 + 5.7 + 2.7^2$ que X é λ-Frobenius não degenerada com $q' = 7^3$.

Como $n \neq \lambda(7^4-1)/(7^3-1)$, tem-se por (3.6) que X é λ-Frobenius não degenerada, e portanto

$$N_\lambda = 960n.$$

Agora, sendo $n \not\equiv 1(7)$, $2n \equiv 1(7)$ e $n \neq (7^4 - 1)/2(7^2-1)$ temos que:

$$N_1 = 1390n, \qquad N_{GV} = 960n.$$

Logo

$$N_\lambda = N_{GV} < N_1 < N_W. \qquad \blacksquare$$

CAPÍTULO IV

SOBRE A GEOMETRIA DAS CURVAS NÃO CLÁSSICAS

PRELIMINARES.

Seja $X \subseteq \mathbb{P}^N$ uma curva algébrica irredutível definida sobre um corpo K, algébricamente fechado de característica p. Suporemos X não degenerada i.é X não está contida em nenhum hiperplano de $\mathbb{P}^N$.

A sequência de ordens de X em x, é a sequência crescente de números naturais que descreve as possíveis multiplicidades de interseção de X com os hiperplanos de $\mathbb{P}^N$, em x.

Para todo ponto de um aberto U de X temos a mesma sequência de ordens, que é chamada de *sequência de ordens de X*, e denotada por $(\varepsilon_0,\ldots,\varepsilon_N)$. Note que $\varepsilon_0 = 0$ e $\varepsilon_1 = 1$.

A sequência $(\varepsilon_0,\ldots,\varepsilon_N)$ é também caracterizada como sendo a menor sequência de números naturais (em ordem lexicográfica) para a qual é inversível a matriz:

$$(1.0) \qquad W = (D_t^{\varepsilon_i} x_j)_{i,j=0,\ldots,N}$$

onde D_t^r é a r-ésima derivada de Hasse com respeito à uma variável separante t e $x_j = X_j/X_0$ com $X_0,\ldots,X_N$ as coordenadas de $\mathbb{P}^N$(veja p.ex.[S-V]).

Se H é um hiperplano de $\mathbb{P}^N$, denotaremos por H' o ponto em

$(\mathbb{P}^N)^*$ que lhe corresponde.

Definimos para cada $n \in \mathbb{N}$ e $x \in X$, o conjunto:

$$L_{x,n} = \{H' \in (\mathbb{P}^N)^* : I(x, X.H) \geq n\}.$$

É fácil ver que $L_{x,n}$ é um sub-espaço linear de $(\mathbb{P}^N)^*$; e assim para todo $x \in U$, temos a sequência encaixante de espaços lineares:

$$(\mathbb{P}^N)^* = L_{x,\varepsilon_0} \supsetneq \cdots \supsetneq L_{x,\varepsilon_N}.$$

Portanto, L_{x,ε_N} consiste de um único hiperplano denominado de *hiperplano osculante de X em x.*

O dual $\bigcap_{H \in L_{x,\varepsilon_{n+1}}} H$, do espaço $L_{x,\varepsilon_{n+1}}$ é chamado *n-ésimo plano osculante* de X em x, e denotado por $T_x^{(n)} X$. Esse espaço tem dimensão projetiva n, e é gerado pelos pontos:

$$(D_t^{\varepsilon_i} x_0(x), \ldots, D_t^{\varepsilon_i} x_N(x)), \qquad i = 0, \ldots, n.$$

A aplicação racional:

$$\varphi : X \longrightarrow (\mathbb{P}^N)^*$$

que a cada $x \in U$, associa o hiperplano osculante $T_x^{(N-1)}X$, é denominada de *aplicação de Gauss,* e o fêcho de $\varphi(U)$ em $(\mathbb{P}^N)^*$ será denotado por X' e chamado de *dual estrita de X.*

Por outro lado, para cada n, $2 \leq n \leq N$, define-se C_nX, como sendo o fêcho em $\mathbb{P}^N \times (\mathbb{P}^N)^*$ do conjunto:

$$C_nU = \{(x, H') \in U \times (\mathbb{P}^N)^* : H \supseteq T_x^{(n-1)}X\}.$$

Sejam π_n e π'_n respectivamente as projeções de C_nX sobre as imagens em $\mathbb{P}^N$ e $(\mathbb{P}^N)^*$, e seja $X_n = \pi'_n(C_nX)$.

A variedade C_nX será denominada de *n-ésima variedade conormal de X*. Em particular C_2X é a variedade conormal de X e X_2 é a variedade dual de X.

Como C_nU é um fibrado projetivo sobre U com fibra $\mathbb{P}^{N-n}$, temos que C_nX é irredutível e $\dim C_nX = N-n+1$.

Por outro lado, sendo X não degenerada, tem-se que $\dim X_n =$ $= \dim C_nX$, pois caso $\dim C_nX > \dim X_n$, para cada ponto geral H' de X_n, teríamos $X = \pi_n(\pi_n'^{-1}H') \subseteq H$.

Temos assim, o seguinte diagrama:

$$\begin{array}{ccccccc}
C_NX & \subsetneqq & C_{N-1}X & \subsetneqq \cdots \subsetneqq \cdots & C_2X \\
\downarrow{\scriptstyle \pi'_N} & & \downarrow{\scriptstyle \pi'_{N-1}} & & \downarrow{\scriptstyle \pi'_2} \\
X' = X_N & \subsetneqq & X_{N-1} & \subsetneqq \cdots \subsetneqq \cdots & X_2
\end{array}$$

Nos parágrafos que seguem, usaremos as seguintes notações:

$\mathbb{M}(L, n \times m)$, o conjunto das matrizes $n \times m$ com coeficientes em L. Quando $n = m$, tal conjunto ser denotado por $\mathbb{M}(L,n)$.

cofa_{rs}, o cofator do elemento a_{rs} da matriz quadrada (a_{ij}).

1. APLICAÇÃO DE GAUSS

O propósito desta seção é determinar o grau de inseparabilidade da aplicação de Gauss e para tal necessitamos dos seguintes lemas.

(1.1) Lema *Se* $(a_{rs}) \in \mathbb{M}(K((t)),N)$ *e* $n \in \mathbb{N}$, *então:*

$$D_t^n(\det(a_{rs})) = \sum_{j_1+\dots+j_N=n} \det(D_t^{j_r} a_{rs}).$$

Demonstração: Provaremos a identidade acima por indução sobre N.

Para N = 2, a igualdade ocorre trivialmente.

Agora, por hipótese de indução, segue que:

$$\sum_{j_1+\dots j_N=n} \det(D^{j_r} a_{rs}) =$$

$$= \sum_{j=0}^{n} \sum_{s=1}^{N} (-1)^{s+1} D^j(a_{1s}) \sum_{j_2+\dots+j_N=n-j} \begin{vmatrix} D^{j_2}a_{21} \dots \widehat{D^{j_2}a_{2s}} \dots D^{j_2}a_{2N} \\ \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\ D^{j_N}a_{N1} \dots \widehat{D^{j_N}a_{Ns}} \dots D^{j_N}a_{NN} \end{vmatrix}$$

$$= \sum_{j=0}^{n} \sum_{s=1}^{N} (-1)^{s+1} D^j (a_{1s}) D^{n-j} \begin{vmatrix} a_{21} \dots\dots \hat{a}_{2s} \dots\dots a_{2N} \\ \vdots \qquad\qquad \qquad \vdots \\ a_{N1} \dots\dots \hat{a}_{Ns} \dots\dots a_{NN} \end{vmatrix}$$

$$= \sum_{s=1}^{N} \sum_{j=0}^{n} D^j(a_{1s})\ D^{n-j}(\mathrm{cof}a_{1s}) = D^n\Big(\sum_{s=1}^{N} a_{1s}\ \mathrm{cof}a_{1s}\Big) = D^n(\det(a_{rs}))$$

onde $D = D_t$. ∎

(1.2) Lema *Seja* p^{α} *a maior potência de p que divide* ε_N. *Se j e r são inteiros positivos tais que* $r \leq N-1$, $j < p^{\alpha}$ e $\varepsilon_r + j \geq \varepsilon_N$, *então* $\binom{\varepsilon_r + j}{\varepsilon_r} \equiv 0(p)$.

Demonstração: Suponha $\varepsilon_N = cp^\alpha$ com $p \nmid c$.

Como $\varepsilon_r < \varepsilon_N = (c-1)p^\alpha + p^\alpha$, $\varepsilon_r + j \geq \varepsilon_N$ *e* $j < p^\alpha$, temos que $\varepsilon_r > (c-1)p^\alpha$.

Logo $(c-1)p^\alpha < \varepsilon_r < (c-1)p^\alpha + p^\alpha$.

Assim,

$$\varepsilon_r = (c-1)p^\alpha + t, \quad t < p^\alpha.$$

Sendo $\varepsilon_r + j = (c-1)p^\alpha + (t+j) = cp^\alpha + (t+j-p^\alpha)$ e $\varepsilon_r + j \geq cp^\alpha$, tem-se que

$$s = t + j - p^\alpha \geq 0 \quad \text{e} \quad 0 \leq s < t.$$

Portanto,

$$\binom{\varepsilon_r + j}{\varepsilon_r} = \binom{c\,p^\alpha \quad + s}{(c-1)p^\alpha + t} \equiv \binom{s}{t} = 0. \qquad \blacksquare$$

(1.3) Teorema *Seja φ a aplicação de Gauss. O grau de inseparabilidade de φ é a maior potência de p que divide ε_N.*

Demonstração: Para $x \in U$, o hiperplano osculante $T_x^{(N-1)}X$ é gerado pelos pontos:

$$(D_t^{\varepsilon_i} x_0(x), \ldots, D_t^{\varepsilon_i} x_N(x)), \quad i = 0, \ldots, N-1,$$

onde t é um parâmetro local de X em x.

Então $\varphi = (\varphi_0 : \ldots : \varphi_N)$ é tal que:

$$\varphi_i = (-1)^i \begin{vmatrix} x_0 & \dots & \hat{x}_i & \dots & x_N \\ \vdots & & \vdots & & \vdots \\ D_t^{\varepsilon_{N-1}} x_0 & \dots & \widehat{D_t^{\varepsilon_{N-1}} x_i} & \dots & D^{\varepsilon_{N-1}} x_N \end{vmatrix} = (-1)^{N+1} \operatorname{cof} D_t^{\varepsilon_N} x_i,$$

com respeito à matriz W em (1.0).

Se P(t) é uma parametrização primitiva de X num ponto geral $x \in X$, então por (1.1) temos que

$D_t^n \varphi_i(P(t)) =$

$$\sum_{j_1+\dots+j_N=n} (j_2+1)\dots \begin{bmatrix} j_N + \varepsilon_{N-1} \\ \varepsilon_{N-1} \end{bmatrix} \begin{vmatrix} D^{j_1} x_0 & \dots \widehat{D^{j_1} x_i} & \dots D^{j_1} x_n \\ \vdots & \vdots & \vdots \\ D^{j_N+\varepsilon_{N-1}} x_0 & \dots \widehat{D^{j_N+\varepsilon_{N-1}} x_i} & \dots D^{j_N+\varepsilon_{N-1}} x_N \end{vmatrix}$$

Para $n < p^\alpha$, na expressão de $D_t^n \varphi_i(P(t))$ comparecem derivadas da forma $D_t^{\varepsilon_r+j} x_s$ com $j \leq n < p^\alpha$, $r \leq N-1$ e $s \neq i$.

Logo, por (1.2) temos que

$$\varepsilon_r + j < \varepsilon_N \quad \text{ou} \quad \begin{bmatrix} \varepsilon_r + j \\ \varepsilon_r \end{bmatrix} \equiv 0(p).$$

Sendo $(\varepsilon_0, \dots, \varepsilon_N)$ minimal para a ordem lexicográfica tal que os vetores,

$$(D_t^{\varepsilon_i} x_0, \dots, D_t^{\varepsilon_i} x_N)(P(t)), \quad i = 0, \dots, N \tag{1.3.1}$$

são linearmente independentes sobre K((t)), segue que os vetores:

$$(D_t^{\varepsilon_r+j} x_0, \dots, D_t^{\varepsilon_r+j} x_N)(P(t)), \quad \varepsilon_r + j < \varepsilon_N$$

são combinações dos vetores em (1.3.1), para $i = 0, \dots, N-1$.

Assim, para todo $n < p^\alpha$, existe $\lambda_n \in K((t))$ tal que:

$$D_t^n \varphi_i = \lambda_n \varphi_i \,, \quad i = 0,\ldots,N.$$

Portanto, os vetores $D_t^n\varphi(P(t))$ e $\varphi(P(t))$ são linearmente dependentes sobre $K((t))$, para $n = 0,\ldots,p^\alpha-1$; e consequentemente por (B.1) segue que $\deg_i\varphi \geq p^\alpha$.

Agora, pelos lemas (1.1) e (1.2), para $i = 0, \ldots, N$, $D_t^{p^\alpha}\varphi_i(P(t))$ dependem somente dos determinantes que envolvem derivadas da forma:

$$D_t^{\varepsilon_r+j} x_s, \quad j = p^\alpha \text{ ou } \varepsilon_r+j < \varepsilon_N.$$

Logo, $D_t^{p^\alpha}\varphi_i(P(t))$ envolve determinantes que são mútiplos de φ_i, e determinantes com uma linha da forma:

$$(D_t^{\varepsilon_r+p^\alpha} x_0,\ldots,D_t^{\varepsilon_r+p^\alpha} x_i,\ldots,D_t^{\varepsilon_r+p^\alpha} x_N), \quad \varepsilon_r+p^\alpha \geq \varepsilon_N. \tag{1.3.2}$$

Sendo o vetor em (1.3.2) uma combinação dos vetores em (1.3.1) obtemos determinates da forma:

$$\lambda_r \operatorname{cof} D_t^{\varepsilon_r} x_i + \mu_r \operatorname{cof} D_t^{\varepsilon_N} x_i,$$

com λ_r e $\mu_r \in K((t))$, independentes de i. Note que $\varepsilon_s = (c-1)p^\alpha$ é uma ordem (veja p.ex. [G-V,1]).

Assim, para $i = 0,\ldots,N$,

$$D_t^{p^\alpha}\varphi_i(P(t)) = \lambda_s \operatorname{cof} D_t^{\varepsilon_s} x_i + \ldots + \lambda_N \operatorname{cof} D_t^{\varepsilon_N} x_i, \tag{1.3.3}$$

com $\lambda_s,\ldots,\lambda_N \in K((t))$ e

$$\lambda_s = \binom{c\,p^\alpha}{p^\alpha} \not\equiv 0(p).$$

Como $\lambda_s \neq 0$, os vetores $\varphi(P(t))$ e $D_t^{p^\alpha}\varphi(P(t))$ são linearmente independentes sobre K((t)), pois caso contrário,

$$D_t^{p^\alpha}\varphi_i(P(t)) = \lambda\varphi_i(P(t)), \quad i = 0,\dots, N$$

para algum $\lambda \in K((t))$.

Com $\varphi_i = (-1)^{N+1}\mathrm{cof}D_t^{\varepsilon_N}x_i$, então por (1.3.3) segue que

$$\mathrm{cof}D_t^{\varepsilon_s}x_i = -\frac{1}{\lambda_s}\left[\lambda_{s+1}\mathrm{cof}D_t^{\varepsilon_{s+1}}x_i + \dots + (\lambda_N \pm \lambda)\mathrm{cof}D_t^{\varepsilon_N}x_i\right]$$

Assim a s+1-ésima coluna da matriz adjunta de W é uma combinação das demais colunas o que é um absurdo, pois W é inversível. ∎

(1.4) Corolário φ *é separável se e somente se* $\varepsilon_N \not\equiv 0(p)$.

O teorema acima é uma generalização do teorema de ordem genérica de contato [H-Kℓ]. O caso N = 3 foi anteriormente tratado em [H,2].

2. PROJEÇÕES GENÉRICAS E AS n-ÉSIMAS VARIEDADES CONORMAIS DE UMA CURVA

A projeção centrada em $P \in \mathbb{P}^N$, é uma aplicação racional:

$$\begin{aligned} \mathrm{PROJ}_P: \mathbb{P}^N &\longrightarrow \mathbb{P}^{N-1} \\ x &\longrightarrow (L_0(x):\dots:L_{N-1}(x)) \end{aligned}$$

onde $L_i = \sum_{j=0}^{N} a_{ij}x_j$, para $i = 0,\dots,N-1$, e $A = (a_{ij}) \in$ $\mathbb{M}(K, N \times (N+1))$ de posto N, com $\bigcap_{i=0}^{N-1} V(L_i) = \{P\}$.

Se P é um ponto geral de $\mathbb{P}^N$ (i.é P no complementar de um fechado próprio de $\mathbb{P}^N$), $PROJ_p$ é dita *projeção genérica com centro em P.*

(2.1) Proposição *Seja $(\varepsilon_0,\dots,\varepsilon_N)$ a sequência de ordens de uma curva não degenerada $X \subseteq \mathbb{P}^N$ com $N \geq 3$. Se $PROJ_p$ é uma projeção genérica, então $(\varepsilon_0,\dots,\varepsilon_{N-1})$ é a sequência de ordens de $PROJ_pX$ em $\mathbb{P}^{N-1}$.*

Demonstração: Sejam $(x_0:\dots:x_N)$ e $(y_0:\dots:y_{N-1})$ respectivamente as coordenadas de X *em* $\mathbb{P}^N$ *e de* $PROJ_pX$ *em* $\mathbb{P}^{N-1}$.

Então,

$$y_i = \sum_{j=0}^{N} a_{ij}x_j, \quad i = 0,\dots,N-1$$

para algum $A = (a_{ij})$ de posto N.

Como P é um ponto geral de $\mathbb{P}^N$ e $N \geq 3$, X é bi-racionalmente equivalente a $PROJ_pX$.

Assim se t é uma variável separante de $K(X) = K(PROJ_pX)$, temos que

$$\begin{bmatrix} y_0 & \cdots & y_{N-1} \\ \vdots & & \vdots \\ D_t^{\varepsilon_{N-1}}y_0 & \cdots & D_t^{\varepsilon_{N-1}}y_{N-1} \end{bmatrix} = \begin{bmatrix} x_0 & \cdots & x_N \\ \vdots & & \vdots \\ D_t^{\varepsilon_{N-1}}x_0 & \cdots & D_t^{\varepsilon_{N-1}}x_N \end{bmatrix} {}^tA$$

Agora, o posto das matrizes acima é N se e somente se a aplicação linear:

$$^{t}A : K^{N+1} \longrightarrow K^{N}$$

$$v \longrightarrow v.{}^{t}A$$

é tal que os vetores:

$$v_i = (D_t^{\varepsilon_i} x_0, \dots, D_t^{\varepsilon_i} x_N), \quad i = 0, \dots, N-1$$

não estejam contidos no núcleo de ${}^{t}A$. Isto equivale a dizer que $P \notin T_x^{(N-1)}X$ para quase todo $x \in X$, o que é verificado se P é um ponto geral de $\mathbb{P}^N$.

Como $(\varepsilon_0, \dots, \varepsilon_{N-1})$ é a menor sequência em ordem lexicográfica para a qual tem posto N, a matriz:

$$\begin{bmatrix} x_0 & \dots & x_N \\ \vdots & & \vdots \\ D_t^{\varepsilon_{N-1}} x_0 & \dots & D_t^{\varepsilon_{N-1}} x_N \end{bmatrix}$$

segue que $(\varepsilon_0, \dots, \varepsilon_{N-1})$ é a sequência de ordens de $PROJ_P X$ em $\mathbb{P}^{N-1}$. ∎

(2.2) Proposição *Se* P *é um ponto geral de* $\mathbb{P}^N$, *com* $N \geq 3$ *e* $X \subsetneq \mathbb{P}^N$ *uma curva não degenerada então:*

(i) $PROJ_P : T_x^{(n)}X \longrightarrow T^{(n)}_{PROJ_P(x)}(PROJ_P X)$

é um isomorfismo linear, para quase todo $x \in X$, *e* $1 \leq n \leq N-2$.

(ii) $X_n \cap P^* \simeq (PROJ_P X)_n$, $2 \leq n \leq N-1$.

(iii) $C_n(PROJ_P X) \simeq [(PROJ_P \times id_{(\mathbb{P}^N)^*}) C_n X] \cap [\mathbb{P}^{N-1} \times P^*]$, $2 \leq n \leq n-1$.

Demonstração: Primeiramente note que para um ponto geral $P \in \mathbb{P}^N$, tem-se que uma variável separadamente de $PROJ_P X$ é também uma variável separante de X; e que se x é um ponto geral de X, $PROJ_P(x)$ é um ponto geral de $PROJ_P X$.

(i) Como $T_x^{(n)}X$ é gerado por:

$$(D_t^{\varepsilon_i} x_0(x), \ldots, D_t^{\varepsilon_i} x_N(x)), \quad i = 0, \ldots, n,$$

segue que $PROJ_P(T_x^{(n)}X)$ é gerado por

$$\left(\sum_{j=0}^{N} a_{0j}\, D_t^{\varepsilon_i} x_j(x), \ldots, \sum_{j=0}^{N} a_{Nj}\, D_t^{\varepsilon_i} x_j(x)\right), \quad i = 0, \ldots, n. \qquad (2.2.1)$$

Por outro lado, se x é um ponto geral de X, então pela proposição (2.1) tem-se que $T^{(n)}_{PROJ_P(X)}(PROJ_P X)$ é gerado pelos pontos:

$$(D_t^{\varepsilon_i} y_0, \ldots, D_t^{\varepsilon_i} y_0, \ldots, D_t^{\varepsilon_i} y_{N-1})(PROJ_P(x)), \quad i = 0, \ldots, n.$$

Sendo, $y_r = \sum_{j=0}^{N} a_{rj} x_j$, para $r = 0, \ldots, N-1$, $T^{(n)}_{PROJ_P(x)}(PROJ_P X)$ é gerado pelos pontos em (2.2.1), e portanto,

$$PROJ_P(T_x^{(n)}X) = T^{(n)}_{PROJ_P(X)}(PROJ_P X), \ n = 1, \ldots, N-2. \qquad (2.2.2)$$

Como os espaços lineares em (2.2.2) têm a mesma dimensão, concluímos que $PROJ_P$ é um isomorfismo linear entre esses espaços.

(ii) O isomorfismo natural $P^* \simeq (\mathbb{P}^{N-1})^*$ induz um isomorfismo

$$\psi_P : X_n \cap P^* \longrightarrow (PROJ_P X)_n$$

$$H' \longrightarrow (PROJ_P H)'$$

De fato:

Para cada H' de um aberto denso de $X_n \cap P^*$ existe x um ponto geral de X tal que $H \supseteq T_x^{(n-1)}X$.

Assim, por (i) temos que,

$$PROJ_p H \supseteq PROJ_p(T_x^{(n-1)}X) = T^{(n-1)}_{PROJ_p(x)}(PROJ_p X),$$

ou seja $(PROJ_p H)' \in (PROJ_p X)_n$.

Logo

$$\psi_p(X_n \cap P^*) \subseteq (PROJ_p X)_n.$$

Por outro lado, sendo P um ponto geral de $\mathbb{P}^N$, temos que

$$\dim(X_n \cap P^*) = \dim X_n - 1 = N - n = \dim(PROJ_p X)_n.$$

Portanto,

$$X_n \cap P^* \simeq (PROJ_p X)_n.$$

(iii) $[(PROJ_p \times id_{(\mathbb{P}^N)^*})C_n X] \cap [\mathbb{P}^{N-1} \times P^*]$ é o fêcho do conjunto:

$$V = \{(PROJ_p(x), H'): x \in U,\ H \supseteq T_x^{(n-1)}X \text{ e } P \in H\}$$

onde U é como no § 0, eventualmente encolhido de modo que $U \simeq PROJ_p U$, e

$C_n(PROJ_p X)$ é o fêcho do conjunto:

$$V' = \{(PROJ_p(x), (PROJ_p H)'): x \in U,\ P \in H \text{ e } PROJ_p H \supseteq T^{(n-1)}_{PROJ_p(x)}(PROJ_p X)\}$$

O isomorfismo em (i) e (ii) permite identificar V e V', e isto estabelece o isomorfismo em (iii). ∎

(2.3) Proposição *Sejam os morfismos:*

$$\pi'_n : C_n X \longrightarrow X_n \quad e \quad \pi'_{n,P} : C_n(PROJ_P X) \longrightarrow (PROJ_P X)_n$$

e H' *um ponto geral de* $X_n \cap P^*$ *, tem-se então:*

$$(\pi'_n)^{-1}H \simeq (\pi'_{n,P})^{-1}(PROJ_P H)'.$$

Demonstração: Seja U um aberto como no § 0, eventualmente encolhido de modo que $U \simeq PROJ_P U$.

Como,

$$C_n U \times_{X_n} (X_n \cap P^*) \simeq (PROJ_P \times id_{(\mathbb{P}^N)^*}) C_n U \times_{X_n} (X_n \times_{(\mathbb{P}^N)^*} P^*) \simeq$$

$$\simeq (PROJ_P \times id_{(\mathbb{P}^N)^*}) C_n U \times_{(\mathbb{P}^N)^*} P^* \simeq$$

$$\simeq [(PROJ_P \times id_{(\mathbb{P}^N)^*}] C_n U \cap [\mathbb{P}^{N-1} \times P^*] \simeq C_n(PROJ_P U),$$

segue que é cartesiano o diagrama:

$$\begin{tikzcd}
C_n(PROJ_P U) \arrow[rr] \arrow[d, "\pi'_{n,P}"] \arrow[drr, phantom, "\square"] & & C_n U \arrow[d, "\pi'_n"] \\
(PROJ_P X)_n \simeq X_n \cap P^* \arrow[rr] & & X_n
\end{tikzcd}$$

Como um ponto geral de $X_n \cap P^*$ é também um ponto geral de X_n, $\pi'_{n,P}(C_n(PROJ_P U))$ contém um aberto denso de $(PROJ_P X)_n$, e ainda a fibra geral de $C_n U \longrightarrow X_n$ (resp. $C_n(PROJ_P U \longrightarrow (PROJ_P X)_n)$ é igual a fibra geral de π'_n (resp. $\pi'_{n,P}$), o resultado segue.■

(2.4) Corolário *Os graus de separabilidade e inseparabilidade de π'_n são invariantes por projeções genéricas.*

(2.5) Teorema *O grau de inseparabilidade de π'_n é a maior potência de p que divide ε_n.*

Demonstração: (A) Mostremos inicialmente para n = N.

Seja:

$$\begin{tikzcd} & C_N X \arrow[dl, "\pi_N"'] \arrow[dr, "\pi'_N"] & \\ X \arrow[rr, "\varphi"] & & X_N = X' \end{tikzcd}$$

onde φ é a aplicação de Gauss.

Como π_N admite a seção:

$$S : x \in U \longrightarrow (x, T_x^{(N-1)}X),$$

π_N é separável.

Sendo $\varphi \circ \pi_N = \pi'_N$, então pelo teorema (1.3), segue que

$$\deg_i \pi'_N = \deg_i \varphi = [\varepsilon_N]_p,$$

onde $[a]_p$ denota a maior potência de p que divide a.

(B) Suponhamos $n \leq N-1$.

Por meio de projeções genéricas, a proposição (2.1) e o corolário (2.4) permitem reduzir o estudo em questão para X em $\mathbb{P}^n$.

Portanto, pela parte (A), tem-se:

$$\deg_i \pi'_n = [\varepsilon_n]_p . \qquad \blacksquare$$

CAPÍTULO V

RELAÇÃO ENTRE AS CURVAS ASSINTÓTICAS E AS CURVAS OSCULANTES

Seja X uma curva plana irredutível de grau d, mergulhada em $\mathbb{P}^{N(\lambda)}$, onde $N(\lambda) = \lambda(\lambda+3)/2$ com $\lambda<d$, pelo morfismo de Veronese ϕ_λ.

A imagem de X por ϕ_λ é uma curva $\tilde{X}$ em $\mathbb{P}^{N(\lambda)}$ não degenerada. Denotaremos por $\varepsilon_0 <\ldots< \varepsilon_{N(\lambda)}$ a sequência de ordens de $\tilde{X}$.

Diremos, seguindo a terminologia de [GV,1] que X é uma curva ϕ_λ-*clássica* se $\varepsilon_i = i$ para $i = 0,\ldots,N(\lambda)$, caso contrário X é dita ϕ_λ *-não clássica.*

Dizer que X é ϕ_λ-não clássica significa que num ponto geral P de X, existe uma curva $G_p^\lambda = 0$ de grau λ, tal que $I(P,X.G_P^\lambda) > N(\lambda)$.

Num ponto geral de P de X, a curva $G_P^\lambda = 0$ é determinada pela condição: $I(P,X.G_P^\lambda) = \varepsilon_{N(\lambda)}$, é chamada de *curva osculante de X em P.*

A motivação para o estudo das curvas assintóticas vem do fato que estas podem ser expressas em função da equação da curva, enquanto que para as curvas oculantes, isto é praticamente impossível. Isto se reflete na análise da classicalidade em cada caso.

Para distinguir os vários conceitos de classicalidade, consideramos para cada n, $2 \leq n \leq N(\lambda)$ a projeção:

$$\pi'_n : C_n\tilde{X} \longrightarrow \tilde{X}_n$$

Diremos que X é *geometricamente não clássica,* se para algum n, π'_n é inseparável, e que X é *numericamente não clássica,* se para algum n, $\varepsilon_n \neq n$.

Observe que pelo teorema (IV - 2.5), X é geometricamente não clássica se, e somente se $\varepsilon_n \equiv 0(p)$ para algum n. Assim, se $N(\lambda) \geq p$, então X é geometricamente não clássica.

Por outro lado, X é numericamente não clássica se, e somente se $\varepsilon_{N(\lambda)} > N(\lambda)$. Assim, se X é numericamente não clássica então X é geometricamente não clássica, pois é sabido que se $\varepsilon_{N(\lambda)} > N(\lambda)$, então existe n tal que $\varepsilon_n = p^\alpha$ para algum $\alpha \geq 1$ (veja p. ex. [S-V] Cor 1.9).

O resultado que segue, consequência dos teoremas 1 e 2 em [G-V,1] , caracteriza as curvas geometricamente não clássicas.

(1.1) Seja X : f = 0. As seguintes afirmações são equivalentes:

(i) X é geometricamente não clássica.

(ii) $\varepsilon_{N(\lambda)} \geq p^\alpha$, com $\alpha \geq 1$.

(iii) Um múltiplo de f é da forma: $\sum_{0 \leq i+j \leq \lambda} z_{ij}^{p^\alpha} x^i y^j$, com $z_{ij} \not\equiv 0(\mathrm{mod}\ f)$ para algum (i,j).

Observação: Se $N(\lambda) < p$, as afirmações acima são equivalentes a X ser numericamente não clássica.

Considere agora, X : F = 0 uma curva irredutível de grau d, e λ um inteiro positivo tal que (d,λ) é admissível.

Sejá ψ_λ o morfismo assintótico

$$\begin{aligned} \psi_\lambda : X &\longrightarrow \mathbb{P}^{N(\lambda)} \\ P &\longrightarrow \tau_P^\lambda F \end{aligned}$$

Diremos que X é *geometricamente não genérica* se ψ_λ é inseparável; e que X é *numéricamente não genérica* se $\eta_\lambda > \lambda+1$.

(1.2) Se X tem singularidades controladas e $1 < \lambda < p-1$, pelos teoremas (II - 2.2) e (II - 4.3) temos que as seguintes afirmações são equivalentes:

(i) X é numericamente não genérica.

(ii) F é da forma $\sum_{i_0+i_1+i_2=\lambda} Q_{i_0 i_1 i_2}^{p^\alpha} X_0^{i_0} X_1^{i_1} X_2^{i_2}$.

(iii) X é geometricamente não genérica.

Nesse caso, podemos caracterizar a λ-genericidade de X, em termos da equação da curva. De (1.1) e (1.2) podemos estabelecer a seguinte relação:

(1.3) Com as mesmas hipóteses de (1.2) sobre X, tem-se que: se X é geometricamente não genérica então X é geometricamente não clássica.

Do teorema (II - 4.3) resulta que, se X satisfaz a uma das afirmações de (1.2), então $\deg_i \psi_\lambda \geq p^\alpha = \eta_\lambda$.

Pela proposição abaixo, devida a A. Hefez e D. Sevcovitz,

[H-L] Proposição *Se $f:Z \longrightarrow X$ é uma aplicação dominante e Z' é* *uma sub-variedade de Z tal que* $Z' \not\subset singZ$, *então*

$$\deg_1 f|_{Z'} \geq \deg_1 f,$$

o teorema acima é generalizado pela proposição:

(1.4) Proposição *Se* $X : F = 0$ *é uma curva irredutível de grau* d, *então para todo* λ *tal que* (d,λ) *é admissível, tem-se que* $\deg_1 \psi_\lambda \geq [\eta_\lambda]_p$.

Demonstração: Sendo $\tau_P^\lambda F = 0$ uma curva de grau λ para um ponto geral P de X, a esta corresponde um hiperplano H_P em $P^{N(\lambda)}$ tal que $I(\phi_\lambda(P), \tilde{X}.H_P) = \eta_\lambda$.

Logo, existe n tal que $\eta_\lambda = \varepsilon_n$.

Denotando por Z' o fêcho da imagem da aplicação racional,

$$\begin{aligned} \nu : X &\longrightarrow \mathbb{P}^{N(\lambda)} \times (\mathbb{P}^{N(\lambda)})^* \\ P \in U &\longrightarrow (\phi_\lambda(P), \tau_P^\lambda F) \end{aligned}$$

obtemos o seguinte diagrama

$$\begin{tikzcd} & Z' \arrow[rr] & & C_n(\tilde{X}) \arrow[dl, "\pi_n"'] \arrow[dr, "\pi'_n"] & \\ X \arrow[ur, "\nu"] \arrow[rr, "\phi_\lambda"] \arrow[drrrr, "\psi_\lambda"'] & & \tilde{X} & & \\ & & & & \tilde{X}_n \end{tikzcd}$$

Como $\operatorname{sing} C_n(\tilde{X}) \not\subset \pi_n^{-1}(\operatorname{sing} \tilde{X})$, segue que $Z' \not\subset \operatorname{sing} C_n(\tilde{X})$.

Sendo ν claramente separável, então pela preposição [H-L] e por (IV - 2.5) tem-se que

$$\deg_1 \psi_\lambda = \deg_1 \pi'_n|_{Z'} \geq \deg_1 \pi'_n = [\varepsilon_n]_p = [\eta_\lambda]_p. \quad \blacksquare$$

(1.5) Corolário *Se* X *é reflexiva,* $\eta_\lambda > 2\lambda+1$ *e* $p > 2\lambda+1$*, então* ψ_λ *é inseparável.*

Demonstração: Pela proposição (I - 1.15) temos que $\eta_\lambda \equiv 0(p)$, e o resultado segue de (1.4). ∎

(1.6) Relação entre Frobenius classicalidade para ϕ_λ e λ-Frobenius genericidade.

Sejam $f_0,\dots,f_n$ as coordenadas de $\tilde{X}$ em $\mathbb{P}^N$, $N = N(\lambda)$.

Em [S-V] , à curva $\tilde{X}$ é associada uma sequência de números naturais $\nu_0 = 0 < \nu_1 <\dots< \nu_{N-1}$ (menor em ordem lexicográfica) para a qual

$$\det\begin{bmatrix} f_0^q & \dots & f_N^q \\ f_0 & & f_N \\ \vdots & & \vdots \\ D_t^{\nu_{N-1}} f_0 & \dots & D_t^{\nu_{N-1}} f_N \end{bmatrix} \neq 0$$

Diremos, seguindo a terminologia de [S-V] que X é *Frobenius clássica para* ϕ_λ se $\nu_i = i$, $i = 0,\dots,N-1$, e caso contrário X é dita *Frobenius não clássica para* ϕ_λ.

Note que para $\lambda = 1$, o conceito de Frobenius classicalidade para ϕ_1 (ou simplesmente Frobenius classicalidade) coincide com o de λ-Frobenius não degeneração.

Determinar critérios para a Frobenius classicalidade para ϕ_λ, é em geral um problema difícil, pois consiste em determinar as equações das curvas osculantes. As equações das curvas assintóticas são mais fáceis de se determinar. Entretanto não se generaliza a afirmação:

(1.6.1) *Se* $p \neq 2$ *e* X *é reflexiva então* X *é Frobenius clássica* (*veja* III - 2.3.1).

Isto se vê no seguinte exemplo:

$$X : F = X_0^{q-1} + X_1^{q-1} + X_2^{q-1} = 0, \ q > p.$$

Para $\lambda = p-1$, temos que X é λ-genérica, mas λ-Frobenius degenerada, pois $H_\lambda = X_0^{p(q-1)} + X_1^{p(q-1)} + X_2^{p(q-1)} = F^p$.

A discussão que segue trata do caso especial $\lambda = 2$.

(1.6.2) *Seja* X *uma curva reflexiva de grau* d, *com* $d \equiv 2(p)$ *e suponha que* X *seja* 2-*não genérica e* 2-*Frobenius não degenerada.*

Se além disso, X tem singularidades controladas, então por (1.3), X é ϕ_2-não clássica. Nesse caso as cônicas assintóticas coincidem com as cônicas osculantes, e portanto $\eta_2 = \varepsilon_5 = q'$. Em vista disso, seria de se esperar que $N'_{SV} = N_2$. Isto no entanto não ocorre pois se X é lisa temos que:

$$N_2 = \frac{d(d - 2 + 2q)}{q'}$$

e

$$N'_{SV} = \frac{d(10(d-2) + 2q)}{q'}$$

A explicação disso é dada abaixo

Seja:

$$g_2 = \begin{vmatrix} x-x^q & x^2-x^{2q} & y-y^q & 0 & -(y^q-y)^2 \\ 1 & 2x & y^{(1)} & y-y^q & 0 \\ 0 & 1 & y^{(2)} & y^{(1)} & (y^{(1)})^2 \\ 0 & 0 & y^{(3)} & y^{(2)} & 2y^{(1)}\, y^{(2)} \\ 0 & 0 & y^{(4)} & y^{(3)} & 2y^{(2)}y^{(3)}+(y^{(2)})^2 \end{vmatrix}$$

Após alguns cálculos e valendo-se da proposição (II - 2.1), temos que

$$(y^{(2)})^3.h_2 = - D_{01}f.g_2.$$

Observação A relação acima permanece válida sem a hipótese de X ter singularidades controladas, mas com a hipótese de $\eta_2 > 5$.

(1.6.3) Exemplo

Seja X uma hiperelítica definida sobre $\mathbb{F}_{p^{r+1}}$, por

$$y^2 = x^{2+p^r} + 1 , \quad p > 5 \quad e \quad r \geq 1.$$

A curva X é 2-não genérica com $\eta_2 \geq p^r > 5$.

Sendo $\deg h_2 = 2p^{r+1} + p^r$ e $uq + \alpha q' = 2p^{r+1}$, temos por (III - 3.5) que X é 2-Frobenius não degenerada.

Agora, como $n < m$, $u = v = 2$ e $\alpha = 0 < 1 = \beta$ tem-se por (III - 3.7) que $P_\infty \in (h_\lambda^* = 0)$.

Logo

$$N_2 = \frac{m \deg h_\lambda}{q'} - (\beta-\alpha)(m-n) = 2p^{r+1} + 4p + 2.$$

Como, X é reflexiva, 2-Frobenius não degenerada e $\eta_2 > 5$ então pela observação acima temos que X é Frobenius clássica para ϕ_2 e

$$N'_{SV} = \frac{10(2g - 2) + (q + 5)2d}{\varepsilon_5} = 2p^{r+1} + 4p + 20 + (10/p^r).$$

Portanto, $N_2 < N'_{SV}$. ∎

As proposições (III - 3.5, 3.6) nos fornecem critérios de λ-Frobenius genericidade das curvas $y^n = \varphi(x)$ para todo λ, enquanto que critérios de Frobenius classicalidade para ϕ_λ são conhecidas apenas para $\lambda = 1$ e para $\lambda = 2$ no caso especial das curvas de Fermat.

Ter critérios de Frobenius classicalidade, bem como ser alta a multiplicidade de interseção genérica de uma curva X com a família de curvas $(\mathcal{F}_P^\lambda = 0,\ p \in X)$ considerada, são dois fatores que contribuem para a obtenção de boas cotas para o número de pontos racionais de X.

A família de curvas assintóticas preenche tais requisitos para as curvas do tipo $y^n = \varphi(x)$.

APÊNDICE

A. ALGUMAS PROPRIEDADES DOS POLINÔMIOS HOMOGÊNEOS

Desenvolvemos aqui algumas das propriedades de polinômios homogêneos, decorrentes das necessidades surgidas no estudo das curvas assintóticas.

O resultado a seguir é uma generalização da bem conhecida relação de Euler.

(A.1) Lema *Se* $F \in K[X_0,\dots,X_n]$ *é um polinômio homogêneo de grau* d *e* λ *é um inteiro positivo, então*

$$\binom{d}{\lambda}F = \sum_{i_0+\dots+i_n=\lambda} X_0^{i_0}\dots X_n^{i_n}\, D_{i_0,\dots,i_n}F.$$

Demonstração: É claro que basta provar a fórmula para F da forma:

$$F = X_0^{j_0}\dots X_n^{j_n}\,, \quad j_0+\dots+j_n = d$$

Nesse caso,

$$\sum_{i_0+\dots+i_n=\lambda} X_0^{i_0}\dots X_n^{i_n}\, D_{i_0\dots i_n}F = X_0^{j_0}\dots X_n^{j_n} \sum_{i_0+\dots+i_n=\lambda} \binom{j_0}{i_0}\dots\binom{j_n}{i_n} =$$

$$= X_0^{j_0}\dots X_n^{j_n}\binom{d}{\lambda} = \binom{d}{\lambda} F. \quad \blacksquare$$

(A.1.1) Observação Na demonstração acima usamos a seguinte igualdade:

$$\sum_{i_0+\ldots+i_n=\lambda} \binom{j_0}{i_0}\cdots\binom{j_n}{i_n} = \binom{d}{\lambda}$$

que pode ser provada, desenvolvendo ambos os lados da igualdade

$$(t+1)^{j_0}\ldots(t+1)^{j_n} = (t+1)^d.$$

Definição *Sejam* $\rho = \rho_0 + \rho_1 p + \ldots$ e $\mu = \mu_0 + \mu_1 p + \ldots$. *Diremos que* ρ *é p-adicamente maior ou igual à* μ *se* $\rho_i \geq \mu_i$ *para todo* $i = 0, 1, \ldots$.

(A.2) Proposição *Suponha* car $K = p \geq n$. *Sejam* $F \in K[X_0, \ldots, X_n]$ *um polinômio homogêneo e* ρ *um inteiro positivo. Se todas as derivadas parciais de ordem* ρ *de* F *são nulas, então todas de ordem* μ *são nulas, para todo* μ *p-ádicamente maior ou igual à* ρ.

Demonstração: Seja $\rho = \rho_0+\ldots+\rho_s p^s$. Para demonstrar a proposição, é suficiente provar o seguinte:

Se $D_{i_0\ldots i_n}F = 0$ para todo $(i_0,\ldots,i_n)$ tal que $i_0+\ldots+i_n=\rho$, então $D_{j_0\ldots j_n}F = 0$ para todo $j_0+\ldots+j_n = \rho+p^\ell$, com $\rho_\ell < p-1$.

Assim, dado $(j_0,\ldots,j_n)$ com $j_0+\ldots+j_n = \rho+p^\ell$, basta encontrarmos um operador diferencial Δ, índices $i_0,\ldots,i_n$ com $i_0+\ldots+i_n = \rho$ e $c \neq 0$ tais que,

$$\Delta(D_{i_0\ldots i_n}F) = c.D_{j_0\ldots j_n}F, \qquad (A.2.1)$$

Escrevendo,

$$j_r = a_{0r} +\ldots+ a_{sr}p^s, \quad r = 0,\ldots,n,$$

e denotando a soma $a_{i_0}+\ldots+a_{i_n}$ por α_i temos que

$$\alpha_0 +\ldots+ \alpha_s p^s = \rho_0 +\ldots+ (\rho_\ell+1)p^\ell +\ldots+ \rho_s p^s.$$

Assim, existem $r_0,\ldots,r_s \in \{0,\ldots,n\}$ tais que

$$\alpha_i = \rho_i + r_i p - r_{i-1}, \quad i \neq \ell, \quad r_{-1} := 0, \text{ e}$$

$$\alpha_\ell = (\rho_\ell+1) + r_\ell p - r_{\ell-1}.$$

Caso $\alpha_\ell \geq 1$.

Nesse caso $a_{\ell i} \geq 1$, para algum $i = 0,\ldots,n$. Supondo sem perda de generalidade que $a_{\ell 0} \geq 1$ e tomando-se:

$$i_0 = j_0 - p^\ell,\ i_1 = j_1,\ldots,\ i_n = j_n \text{ e } \Delta = D_{p^\ell,0,\ldots,0},$$

obtém-se

$$\Delta(D_{i_0\ldots i_n}F) = a_{\ell 0}\, D_{j_0\ldots j_n}F.$$

Caso $\alpha_\ell = 0$.

Nesse caso $r_\ell = 0$ e $r_{\ell-1} - \rho_\ell = 1$.

Pondo $s_i = r_{i-1} - \rho_i$, para $i = 1,\ldots,\ell$, temos que $s_\ell = 1$, e o resultado segue como consequência dos dois lemas seguintes:

(A.2.1) Lema Se $\alpha_{\ell-1} < s_\ell p,\ldots,\ \alpha_{\ell-i} < s_{\ell-i+1}p$ e $\alpha_{\ell-(i+1)} \geq s_{\ell-i}p$ então existem um operador diferencial Δ e índices $i_0,\ldots,i_n$ com $i_0+\ldots+i_n = \rho$ e $c \neq 0$ tais que

$$\Delta(D_{i_0\ldots i_n}F) = c\ D_{j_0\ldots j_n}F.$$

Demonstração: Mostremos inicialmente a seguinte afirmação:

(A.2.2.) Se $\alpha_j < s_{j+1}P$, para algum $j \leq \ell-1$, então $\alpha_j = s_{j+1}p-s_j$ com $s_j > 0$ e $\rho_{j+1} = 0$.

De fato:

Se $\alpha_j < s_{j+1}p$ então $(r_j-s_{j+1})p < s_j \leq n \leq p$.

Daí, $r_j = s_{j+1}$, pois $s_{j+1} = r_j-\rho_{j+1} \leq r_j$.

Portanto,

$\rho_{j+1} = 0$ e $\alpha_j = r_jp - (r_{j-1}-\rho_j) = s_{j+1}p - s_j$, com $s_j > 0$.

Logo, se $\alpha_{\ell-1} < s_\ell p, \ldots, \alpha_{\ell-i} < s_{\ell-i+1}p$ tem-se por (A.2.2) que

$$\alpha_j = s_{j+1}p - s_j, \quad j = \ell-1, \ldots, \ell-i$$

e

$$\alpha_{\ell-i}p^{\ell-i} + \ldots + \alpha_{\ell-1}p^{\ell-1} = p^\ell - s_{\ell-i}p^{\ell-i}. \qquad (*)$$

Agora, como $\alpha_{\ell-(i+1)} \geq s_{\ell-i}p$, com $s_{\ell-i} > 0$ existem $b_0, \ldots, b_n$ tais que:

$$a_{\ell-(i+1),k} \geq b_k, \quad k = 0, \ldots, n, \quad e$$

$$(a_{\ell-(i+1),0} - b_0) + \ldots + (a_{\ell-(i+1),n} - b_n) = s_{\ell-i}p.$$

Tomando-se, para $k = 0, \ldots, n$,

$$i_k = j_k - (a_{\ell-(i+1),k} - b_k)p^{\ell-(i+1)} - \ldots - a_{\ell-1,k}p^{\ell-1},$$

e

$$\Delta = D_{j_0-i_0, \ldots, j_n-i_n}$$

temos por (*) que,

$$i_0+\ldots+i_n = (j_0+\ldots+j_n) - s_{\ell-i}p^{\ell-i} - (\alpha_{\ell-i}p^{\ell-i}+\ldots+\alpha_\ell{}^{\ell-1}) =$$

$$= (j_0+\ldots+j_n) - p^\ell = \rho, \text{ e}$$

$$\Lambda(D_{i_0\dots i_n}F) = c.D_{j_0\dots j_n}F,$$

onde $c = \begin{bmatrix} a_{\ell-(i+1),0} \\ b_0 \end{bmatrix} \dots \begin{bmatrix} a_{\ell-(i+1),n} \\ b_n \end{bmatrix} \neq 0.$ ∎

(A.2.3) Lema: *Se* $\alpha_{\ell-1} < s_\ell p, \dots, \alpha_1 < s_2 p$, *então* $\alpha_0 \geq s_1 p$.

Demonstração: Como por (A.2.2), $\alpha_1 = s_2 p - s_1$, com $s_1 > 0$ e $s_1 = r_0 - \rho_1$, segue que,

$$\alpha_0 = \rho_0 + r_0 p \geq r_0 p = (s_1+\rho_1)p \geq s_1 p.$$ ∎

(A.3) Proposição *Seja* T *uma transformação projetiva plana tal que*

$$T(Y_0,Y_1,Y_2) = (X_0,X_1,X_2), \text{ com } X_i = \sum_{j=0}^{2} a_{ij}Y_j \text{ para } i = 0,1,2.$$

Se $T(Q) = P$ *então* $(\mathcal{H}_P^\lambda F)^T = \mathcal{H}_Q^\lambda(F^T)$.

Demonstração: É suficiente provar a proposição para F da forma: $X_0^{n_0} X_1^{n_1} X_2^{n_2}$. Escrevendo $P = (P_0,P_1,P_2)$ temos que

$$\mathcal{H}_P^\lambda F = \sum_{|u|=\lambda} (D_{X_0}^{u_0} D_{X_1}^{u_1} D_{X_2}^{u_2} F)(P)\, X_0^{u_0} X_1^{u_1} X_2^{u_2} =$$

$$= \sum_{|u|=\lambda} \prod_{r=0}^{2} \begin{pmatrix} n_r \\ u_r \end{pmatrix} P_r^{n_r-u_r}(a_{r0}Y_0 + a_{r1}Y_1 + a_{r2}Y_2)^{u_r}.$$

Sendo o coeficiente de $Y_0^{\rho_0} Y_1^{\rho_1} Y_2^{\rho_2}$, $\rho_0+\rho_1+\rho_2 = \lambda$, do produto $\prod_{r=0}^{2}(a_{r0}Y_0 + a_{r1}Y_1 + a_{r2}Y_2)^{u_r}$, dado por:

$$\left(D_{Y_0}^{\rho_0} D_{Y_1}^{\rho_1} D_{Y_2}^{\rho_2}\right) \prod_{r=0}^{2}(a_{r0}Y_0 + a_{r1}Y_1 + a_{r2}Y_2)^{u_r}(0),$$

que é igual a

$$\sum_{(*)} \prod_{r=0}^{2} \begin{bmatrix} u_r \\ i_r \end{bmatrix} \begin{bmatrix} u_r - i_r \\ j_r \end{bmatrix} \begin{bmatrix} u_r - i_r - j_r \\ k_r \end{bmatrix} a_{r2}^{k_r} \, a_{r1}^{j_r} \, a_{r0}^{i_r}$$

onde o somatório $(*)$ percorre os índices $i = (i_0, i_1, i_2)$, $j = (j_0, j_1, j_2)$ e $k = (k_0, k_1, k_2)$ tais que $|i| = \rho_2$, $|j| = \rho_1$, $|k| = \rho_0$ e $i_r + j_r + k_r = u_r$, $r = 0, 1, 2$.

Obtemos então:

$\mathcal{H}_P^\lambda \, F =$

$$= \sum_{|\rho|=\lambda} \left[\sum_{|u|=\lambda} \sum_{(*)} u_r! \begin{bmatrix} n_r \\ u_r \end{bmatrix} a_{r2}^{i_r} \, a_{r1}^{j_r} \, a_{r0}^{k_r} \, P_r^{n_r - u_r} / i_r! j_r! k_r! \right] Y_0^{\rho_0} \, Y_1^{\rho_1} \, Y_2^{\rho_2} \qquad \text{(A.3.1)}$$

Por outro lado,

$$\mathcal{H}_Q^\lambda \, (F^T) = \sum_{|\rho|=\lambda} (D_{Y_0}^{\rho_0} \, D_{Y_1}^{\rho_1} \, D_{Y_2}^{\rho_2} \, F^T)(Q) \; Y_0^{\rho_0} \, Y_1^{\rho_1} \, Y_2^{\rho_2}. \qquad \text{(A.3.2)}$$

Como $F^T = \prod_{r=0}^{2} (a_{r0} Y_0 + a_{r1} Y_1 + a_{r2} Y_2)^{n_r}$, temos que,

$(D_{Y_0}^{\rho_0} \, D_{Y_1}^{\rho_1} \, D_{Y_2}^{\rho_2} \, F^T)(Q) =$

$$= \sum_{(**)} \prod_{r=0}^{2} \begin{bmatrix} n_r \\ i'_r \end{bmatrix} \begin{bmatrix} n_r - i'_r \\ j'_r \end{bmatrix} \begin{bmatrix} n_r - i'_r - j'_r \\ k'_r \end{bmatrix} a_{r2}^{i'_r} \, a_{r1}^{j'_r} \, a_{r0}^{k'_r} \, P_r^{n_r - (i'_r + j'_r + k'_r)} / i'_r! j'_r! k'_r! \qquad \text{(A.3.3)}$$

onde o somatório $(**)$ percorre os índices i', j', k' tais que $|i'| = \rho_2$, $|j'| = \rho_1$ e $|k'| = \rho_0$.

Pondo $u_r = i'_r + j'_r + k'_r$ e $u = (u_0, u_1, u_2)$, temos que $|u| = \lambda$ e

$$\begin{bmatrix} n_r \\ i'_r \end{bmatrix} \begin{bmatrix} n_r - i'_r \\ j'_r \end{bmatrix} \begin{bmatrix} n_r - i'_r - j'_r \\ k'_r \end{bmatrix} = u_r! \begin{bmatrix} n_r \\ u_r \end{bmatrix}.$$

Assim, substituindo (A.3.3) em (A.3.2) obtém-se (A.3.1), e portanto:

$$(\mathcal{H}_P^\lambda F)^T(Y_0, Y_1, Y_2) = \mathcal{H}_P^\lambda F(X_0, X_1, X_2) = \mathcal{H}_Q^\lambda (F^T)(Y_0, Y_1, Y_2). \qquad \blacksquare$$

(A.4) Lema *Sejam* $d = \deg F$ *e* λ *um inteiro tal que* $1 \leq \lambda < p-1$ *e* $d \equiv \lambda(p)$. Se $D_i^m D_j^n F = 0$ *para todo* $i,\ j = 0,1,2$ *e todo par* (m,n) *tal que* $m+n = \lambda+1$, *então* $D_{i_0 i_1 i_2} F = 0$ *para todo* (i_0, i_1, i_2) *tal que* $i_0+i_1+i_2 = \lambda+1$.

Demonstração: Basta provar o lema para F do tipo

$$X_0^{n_0} X_1^{n_1} X_2^{n_2}, \quad n_0+n_1+n_2 = d.$$

Pela hipótese segue que:

$$\binom{n_i}{m} \binom{n_j}{n} = 0, \tag{A.4.1}$$

para todo m, n tal que $m+n = \lambda+1$ e $i,j = 0,1,2$.

Escrevendo $n_i = n_{i0} + n_{i1}p + \ldots$, $i = 0,1,2$, segue de $m+n = \lambda+1 < p$, que

$$\binom{n_i}{m} \binom{n_j}{n} \equiv \binom{n_{i0}}{m} \binom{n_{j0}}{n}.$$

Logo, por (A.4.1) segue que $n_{i0} + n_{j0} \leq \lambda$ para $i,j = 0,1,2$.

Assim,

$$2(n_{00} + n_{10} + n_{20}) \leq 3\lambda. \tag{A.4.2}$$

Por outro lado, sendo $d \equiv \lambda(P)$ temos que

$$n_{00} + n_{10} + n_{20} = \lambda + rp, \quad r \in \{0,1,2\}. \tag{A.4.3}$$

De (A.4.2) e (A.4.3) obtemos $2rp \leq \lambda < p$; e portanto $r = 0$ e $n_{00} + n_{10} + n_{20} = \lambda$.

Assim, para todo (i_0, i_1, i_2) tal que $i_0+i_1+i_2 = \lambda$, tem-se que

$$\binom{n_0}{i_0}\binom{n_1}{i_1}\binom{n_2}{i_2} = 0. \qquad \blacksquare$$

Observação: Pode-se provar que (A.4) ainda é verificada para todo $\lambda < p^5$ com (d,λ) admissível. O exemplo abaixo mostra que para valores de $\lambda \geq p^5$, o lema pode falhar.

Sejam $F = X_0^{n_0} X_1^{n_1} X_2^{n_2}$ e $p = 5$,

onde,

$$n_0 = 4 + 1.5 + 4.5^2 + 4.5^4 + 4.5^5$$

$$n_1 = 4 + 1.5 + 3.5^2 + 4.5^3 + 3.5^4$$

$$n_2 = 4 + 4.5 + 4.5^2 + 1.5^3 + 4.5^4 + 1.5^5$$

Daí, $d = 2 + 3.5 + 2.5^2 + 2.5^3 + 2.5^4 + 2.5^5 + 5^6$.

Se $\lambda = d - 5^6$, verifica-se facilmente que $\binom{n_i}{m}\binom{n_j}{n} = 0$ para todo (m,n) tal que $m+n = \lambda+1$ e $i,j = 0,1,2$.

Mas, se

$$i_0 = 1 + 5 + 5^2 + 5^4 + 5^5$$

$$i_1 = 1 + 5 + 5^2 + 5^3 + 5^4 + 5^5$$

$$i_2 = 1 + 5 + 5^3 + 5^5$$

tem-se que,

$$i_0 + i_1 + i_2 = \lambda + 1 \text{ e } \binom{n_0}{i_0}\binom{n_1}{i_1}\binom{n_2}{i_2} \neq 0. \qquad \blacksquare$$

(A.5) Lema *Se* (d,λ) *é um par admissível então para todo inteiro* r, $1 \leq r \leq \lambda$ *tem-se que*

$$\sum_{i=0}^{r+1}\binom{\lambda+i-r}{i} D_{r+1-i,\lambda+i-r,0}\, F\, X_0^{r+1-i}\, X_1^i = (-X_2)^{r+1} D_{0,\lambda-r,r+1}\, F.$$

Demonstração: Para provar o lema, basta tomar:

$$F = X_0^{n_0} X_1^{n_1} X_2^{n_2}, \quad n_0 + n_1 + n_2 = d.$$

Temos então que,

$$\sum_{i=0}^{r+1}\binom{\lambda+i-r}{i} D_{r+1-i,\lambda+i-r,0}\, F\, X_0^{r+1-i} X_1^i + (-X_2)^r D_{0,\lambda-r,r+1}\, F =$$

$$= X_0^{n_0} X_1^{n_1-(\lambda-r)} X_2^{n_2}\left[\sum_{i=0}^{r+1}\binom{\lambda+i-r}{i}\binom{n_0}{r+1-i}\binom{n_1}{\lambda+i+r} + (-1)^r\binom{n_1}{\lambda-r}\binom{n_2}{r+1}\right] =$$

$$= X_0^{n_0} X_1^{n_1-(\lambda-r)} X_2^{n_2}\binom{n_1}{\lambda-r}\left[\sum_{i=0}^{r+1}\binom{n_0}{r+1-i}\binom{n_1-(\lambda-r)}{i} + (-1)^r\binom{n_2}{r+1}\right] \quad \text{(A.5.1)}$$

Pela observação (A.1.1), a expressão (A.5.1) é igual a

$$X_0^{n_0} X_1^{n_1-(\lambda-r)} X_2^{n_2}\binom{n_1}{\lambda-r}\left[\binom{n_0+n_1-(\lambda-r)}{r+1} + (-1)^r\binom{n_2}{r+1}\right] =$$

$$= X_0^{n_0} X_1^{n_1-(\lambda-r)} X_2^{n_2}\binom{n_1}{\lambda-r}\left[\binom{d-\lambda-(n_2-r)}{r+1} + (-1)^r\binom{n_2}{r+1}\right] \quad \text{(A.5.2)}$$

Como (d,λ) é admissível, $d \equiv \lambda(p)$ e portanto

$$\binom{d-\lambda-(n_2-r)}{r+1} \equiv (-1)^{r+1}\binom{n_2}{r+1}. \quad \text{(A.5.3)}$$

Logo, por (A.5.3) conclui-se que o polinômio em (A.5.2) é nulo. ■

Facilmente, segue de (A.5) que,

(A.5.4) *Seja* $F \in K[X_0,X_1,X_2]$ *um polinômio irredutível de grau* d *e seja* λ *um inteiro tal que* (d,λ) *é admissível. Se* $D_{i,j,0}F=0$ *para todo* (i,j) *tal que* $i+j = \lambda+1$, *então* $D_{i,0,j}\, F = D_{0,i,j}\, F = 0$ *para todo* i,j *com* $i+j=\lambda+1$.

(A.6) Proposição *Seja* $F \in K[X_0,X_1,X_2]$ *um polinômio homogêneo de grau* d *e* λ *é um inteiro tal que nem todas as derivadas de ordem* λ *de* F *são nulas.*

(i) *Se* $\lambda = p^s$, p^{s+1} divide d *e todas as derivadas de ordem* $\lambda+1$ *de* F *são nulas então* F *é redutível.*

(ii) *Se* (d,λ) *é admissível, não da forma* (i) *e são nulas todas as derivadas de* F *de ordem* $\lambda+1$ *até* $q'-1$, *onde* q' *é uma potência de* p *e* $q' \geq 2\lambda+1$ *então* F *é da forma*

$$F = \sum_{i_0+i_1+i_2=\lambda} Q^{q'}_{i_0i_1i_2} X_0^{i_0} X_1^{i_1} X_2^{i_2}.$$

Demonstração:

(i) Suponha $F = \sum_I a_I X^I$, onde $X^I = X_0^{n_0} X_1^{n_1} X_2^{n_2}$ com $n_0+n_1+n_2 = d$; e escreva:

$$n_i = a_{i0} + a_{i1}p + \ldots + a_{ir}p^r, \; i = 0,1,2$$

e

$$\alpha_j(I) = \alpha_j = a_{0j} + a_{1j} + a_{2j}\;, \; j = 0,\ldots,s.$$

Como, $\alpha_0 + \ldots + \alpha_s p^s + \ldots = d_{s+1}p^{s+1} + \ldots$, temos que

$$\alpha_j = r_j p - r_{j-1}, \; r_j \in \{0,1,2\}, \; j = 0,\ldots,s. \qquad \text{(A.6.1)}$$

Se $r_s \neq 0$, então $\alpha_s \neq 0$, e daí $a_{is} \neq 0$ para algum $i \in \{0,1,2\}$.

Supondo $a_{0s} \neq 0$, temos pela hipótese que

$$0 = D_{1+p^s,0,0} X^I = \binom{a_{00}}{1}\binom{a_{0s}}{1},$$

e portanto $a_{00} = 0$. Como $D_{p^s,1,0} X^I = 0 = D_{p^s,0,1} X^I$, conclui-se que $a_{10} = a_{20} = 0$, e daí $\alpha_0(I) = 0$.

A conclusão é a mesma se $a_{1s} \neq 0$ ou $a_{2s} \neq 0$.

Se $r_s = 0$ então por (A.6.1), $\alpha_s(I) = \ldots = \alpha_0(I) = 0$.

Em ambos os casos, tem-se que

$$\alpha_0(I) = 0, \quad \forall\ I.$$

Logo, existe $Q \in K[X_0, X_1, X_2]$ tal que $F = Q^p$.

(ii) Para todo (i_0, i_1, i_2) tal que $i_0+i_1+i_2 = \lambda$ e $j = 0,1,2$ temos

$$D_j^{q'-r}(D_{i_0 i_1 i_2} F) = 0, \quad \lambda+1 \leq r \leq q'-1, \text{ e}$$

$$D_j^{q'-r}(D_{i_0 i_1 i_2} F) = D_{i_0 i_1 i_2}(D_j^{q'-r} F) = 0, \quad 1 \leq r \leq q'-(\lambda+1).$$

Como $q' \geq 2\lambda+1$, tem-se que:

$$D_j^{q'-r}(D_{i_0 i_1 i_2} F) = 0, \quad r = 1, \ldots, q'-1. \qquad \text{(A.6.2)}$$

Logo, de (A.6.2) existem $Q_{i_0 i_1 i_2} \in K[X_0, X_1, X_2]$ tais que

$$D_{i_0 i_1 i_2} F = Q^{q'}_{i_0 i_1 i_2}.$$

Agora sendo (d, λ) admissível e não da forma (i) temos por (A.1) que:

$$F = \sum_{i_0+i_1+i_2=\lambda} Q^{q'}_{i_0 i_1 i_2} X_0^{i_0} X_1^{i_1} X_2^{i_2}. \qquad \blacksquare$$

B. A INSEPARABILIDADE DE UMA APLICAÇÃO RACIONAL

Sejam X e Y curvas e $f : X \longrightarrow Y$ uma aplicação racional dominante. O grau de inseparabilidade de f é por definição,

$$\deg_i f = [K(X):K(Y)]_i$$

O estudo de $\deg_i f$ tem um caráter local, e para empreendê-lo estabeleceremos alguns resultados sobre parametrizações.

Uma *parametrização* de uma curva $X \subseteq \mathbb{P}^N$ centrada num ponto $x \in X$, é um ponto:

$$P(t) = (x_0(t):\ldots:x_N(t)) \in \mathbb{P}^N_{K((t))},$$

não racional sobre K, tal que $P(0) = x$ e $P(t) \in X(K(t))$.

Uma parametrização P(t) é dita *primitiva*, se não é racional sobre $K((t^r))$, para algum $r \geq 2$.

Se P(t) é uma parametrização primitiva de X em x, então a parametrização $Q(t) = f(P(t))$ de Y não é necessariamente primitiva.

Tem-se que, $\deg_i f \geq p^r$ se, e somente se Q(t) é racional sobre $K((t^{p^r}))$. Além disso, Q(t) não é racional sobre $K((t^{p^{r+1}}))$ se, e somente se $\deg_i f = p^r$.

Daremos a seguir um critério prático para se determinar o grau de inseparabilidade de uma aplicação racional, e isto nos fornece o valor para ε_1 (veja a definição de ε_1 no capítulo IV).

(B.1) Proposição *Sejam* $Q(t) = (y_0(t):\ldots:y_m(t)) \in \mathbb{P}^M_{K((t))}$ *e* $r \in \mathbb{N}^*$.

Então $Q(t)$ *é racional sobre* $K((t^{p^r}))$ *se, e somente se* $Q(t)$ e $D_t^{p^i}(Q(t))$ *são linearmente dependentes sobre* $K((t))$, *para* $i = 0,\dots,r-1$.

Demonstração: Se $Q(t)$ é racional sobre $K((t^{p^r}))$, então para algum $h(t) \in K((t))^*$, temos que

$$Q(t) = h(t)\,(H_0(t^{p^r}):\dots:H_M(t^{p^r})).$$

Assim, para $i = 0,\dots,r-1$

$$D_t^{p^i}(Q(t)) = D_t^{p^i}h(t).(H_0(t^{p^r}):\dots:H_M(t^{p^r})).$$

Isto implica que, $Q(t)$ e $D_t^{p^i}(Q(t))$ são linearmente dependentes sobre $K((t))$, para $i = 0,\dots,r-1$.

Provaremos a recíproca por indução sobre r.

Para $r = 1$, $Q(t)$ e $Q'(t)$ são linearmente dependentes sobre $K((t))$ se, e somente se

$$y_i(t).y'_j(t) = y_j(t).y'_i(t)\ ,\ i,j = 0,\dots,M.$$

Como $y_i(t) \neq 0$ para algum i, sem perda de generalidade podemos supor $y_M(t) \neq 0$.

Portanto,

$$[(y_i(t)/y_M(t)]' = [y_M(t)y'_i(t) - y'_M(t)y_i(t)]/(y_M(t))^2 = 0.$$

Assim,

$$y_i(t)/y_M(t) \in K((t^p)),\quad i = 0,\dots M,$$

ou seja $Q(t)$ é racional sobre $K((t^p))$.

Suponhamos agora, que $Q(t)$ e $D_t^{p^i}(Q(t))$ sejam linearmente dependentes sobre $K((t))$ para $i = 0,\dots,r$.

Pela hipótese de indução, $Q(t)$ é racional sobre $K((t^{p^r}))$, ou seja $y_i(t)/y_M(t) = z_i(t) \in K((t^{p^r}))$.

Logo,

$$D_t^{p^r} y_i(t) = D_t^{p^r} y_M(t)\ z_i(t) + y_M(t) D_t^{p^r} z_i(t). \qquad (B.1.1)$$

Sendo $Q(t)$ e $D_t^{p^r}(Q(t))$ linearmente dependentes, então por (B.1.1) temos,

$$D_t^{p^r}(y_i(t)/y_M(t)) = [D_t^{p^r} y_i(t)\ y_M(t) - y_i(t)\ D_t^{p^r} y_M(t)]/(y_M(t))^2 = 0.$$

Portanto,

$$y_i(t)/y_M(t) \in K((t^{p^{r+1}})),\ i = 0,\ldots,M. \qquad \blacksquare$$

R E F E R Ê N C I A S

[B-H] E. Ballico e A. Hefez - Non reflexive projetive curves of low degree (a aparecer).

[G] A. Garcia - The curves $y^n = f(x)$ over finite fields - Arch. Math. 54 (1990).

[G-V,1] A. Garcia e J. F. Voloch - Wronskians and linear independence in fields of prime characteristic - Manuscripta Math. 59 (1987), 457-469.

[G-V,2] A. Garcia e J. F. Voloch - Fermat curves over finite fields - J. of Number Theory 30 (1988), 345-356.

[H.1] A. Hefez - Non reflexive curves - Compositio Math-69 (1989), 3-35.

[H.2] A. Hefez - Non classical curves - Atas do 16º colóquio Brasileiro de Matemática (1988), 33-37.

[H.3] A. Hefez - Introdução à geometria projetiva - Ata da X Escola de Álgebra.

[H-K] A. Hefez e N. Kakuta - New Bounds for Fermat curves over finite fields - Proceedings of Zeuthen symposium - S.C.M (a aparecer).

[H-Kℓ] A. Hefez e S. Kleiman - Notes on the duality of projetive varieties - Geometry Today Birkhäuser (1985), 143-183.

[H-L] A. Hefez e D. Levcovitz (em preparação)

[H-V] A. Hefez e J. F. Voloch - Frobenius classical curves - Archiv. der Math. 54 (1990), 263-273.

[H_0-1] M. Homma - Reflexivity of tangent varieties associated with a curve-prepint.

[H_0-2] M. Homma - Non reflexive plane curve of a certain type - preprint

[P] R. Pardini - Some remarks on plane curves over fields of finite characteristic - Compositio Math. 60 (1986), 3-17.

[S-V] K. O. Stöhr e J. F. Voloch - Weirstrass points and curves over finite fields - Proc. London - Math. Soc. (3) 52 (1986), 1-19.

[V] J. F. Voloch - On the number of values taken by polinomial over finite fields - Acta Arithmética L.II (1989)

[W] A. Weil - Courbes algébriques et variétés abéliennes -
Herman, Paris. (1971)