Universidade Estadual de Campinas

Instituto de Matemática, Estatística e Computação Científica

Departamento de Matemática

Dissertação de Mestrado

Sobre o Número de Pontos Racionais de Curvas Sobre Corpos Finitos

por

Tiago N. Castilho[†]

Mestrado em Matemática - Campinas - SP

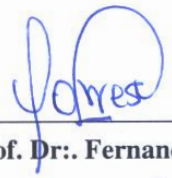
Orientador: Prof. Dr. Fernando Eduardo Torres Orihuela

[†]Este trabalho contou com apoio financeiro do CNPq.

Sobre o Número de Pontos Racionais de Curvas Sobre Corpos Finitos

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por **Tiago Nunes Castilho** e aprovada pela comissão julgadora.

Campinas, 03 de Abril de 2008



Prof. Dr:. Fernando Eduardo Torres Orihuela

Banca Examinadora:

Prof. Dr Fernando Eduardo Torres Orihuela
Prof. Dr. Paulo Roberto Brumatti.
Prof. Dr. Mirian Del Milagro Abdon

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica, UNICAMP, como requisito parcial para obtenção do Título de **Mestre em Matemática**.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP
Bibliotecária: Miriam Cristina Alves – CRB8a / 5094

Castilho, Tiago Nunes

C278s Sobre o número de pontos racionais de curvas sobre corpos finitos/Tiago Nunes Castilho -- Campinas, [S.P. :s.n.], 2008.

Orientador : Fernando Eduardo Torres Orihuela

Dissertação (mestrado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Curvas algébricas. 2. Corpos finitos (Álgebra). 3. Weierstrass, Pontos de. 4. Geometria algébrica aritmética. I. Torres Orihuela, Fernando Eduardo. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Título em inglês: On the number of rational points of curves over finite fields

Palavras-chave em inglês (Keywords): 1. Algebraic curves. 2. Finite fields (Algebra). 3. Weierstrass points. 4. Arithmetical algebraic geometry.

Área de concentração: Álgebra comutativa, Geometria algébrica

Titulação: Mestre em Matemática

Banca examinadora: Prof. Dr. Fernando Eduardo Torres Orihuela (IMECC-Unicamp)
Prof. Dr. Paulo Roberto Brumatti (IMECC-Unicamp)
Profa. Dra. Mirian Del Milagro Abdon (Depto. De Matemática-UFF)

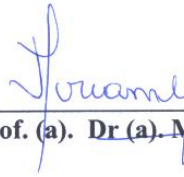
Data da defesa: 19/03/2008

Programa de Pós-Graduação: Mestrado em Matemática

Dissertação de Mestrado defendida em 19 de março de 2008 e aprovada

Pela Banca Examinadora composta pelos Profs. Drs.

Prof. (a). Dr (a). FERNANDO EDUARDO TORRES ORIHUELA



Prof. (a). Dr (a). MIRIAM DEL MILAGRO ABDON

Prof. (a). Dr (a). PAULO ROBERTO BRUMATTI

À minha família: Tercides, Celeste e Tomas.

Agradecimentos

Não só pela orientação, mas também por sua dedicação e amizade, muito tenho a agradecer ao meu orientador Fernando Eduardo Torres Orihuela.

Aos professores do Imecc. De modo especial, aos professores Paulo Brumatti e Antonio Engler, os quais, juntamente com o Fernando, são fundamentais para a minha formação em Álgebra.

À professora Iara Fernandes, pelo incetivo inicial; à Mirian Abdon, pelos conselhos e correções; aos amigos e funcionários do Imecc, pela presença constante e companheirismo; aos amigos de Atibaia que compreendem e apoiam a minha ausência; à toda a minha família, em especial as famílias de meu tio Dedeca e minha tia Eliane que durante todo o curso de mestrado me abrigaram e permitiram que este trabalho fosse realizado; à minha avó Mariana, por suas orações e dedicação no cuidado de toda a minha família; ao meu time de coração, o Corinthians, pelos momentos de distração tão necessários para as tardes de domingo; ao CNPq, pelo suporte financeiro necessário para a realização deste trabalho.

À Camile, pelo companheirismo, amizade, carinho, paciência,.....São muitas as palavras que descrevem o quão valiosa é sua presença em minha vida.

À meu Deus, pelas oportunidades e pessoas que coloca em meu caminho.

Resumo

Nesta dissertação estudamos cotas para o número de pontos racionais de curvas definidas sobre corpos finitos tendo como ponto de partida a teoria de Stöhr-Voloch.

Abstract

In this work we study upper bounds on the number of rational points of curves over finite fields by using the Stöhr-Voloch theory.

Introdução

O problema de contar pontos racionais de curvas definidas sobre corpos finitos tem importância nas mais diversas áreas da tecnologia. Por exemplo, a qualidade dos códigos geométricos depende da quantidade de pontos racionais da curva sobre a qual os códigos são construídos. A relação entre tais códigos e curvas algébricas é consequência de uma construção introduzida pelo matemático V.D. Goppa em 1977 [11]. Esta construção permite definir códigos com bons parâmetros a partir de curvas definidas sobre corpos finitos e com muitos pontos racionais.

Para obter Códigos de Goppa com uma boa relação entre seus parâmetros relativos, é necessário que a razão entre o número N de pontos racionais e o gênero g da curva, sobre a qual o código é construído, seja a maior possível, ou seja, a qualidade do código aumenta conforme a proporção

$$\frac{N}{g}.$$

Esta é a motivação principal desta dissertação.

A construção de Códigos de Goppa a partir de curvas algébricas estabelece uma relação entre duas diferentes áreas da matemática – teoria de códigos (aplicada) e geometria algébrica (pura) – e providencia uma motivação para o estudo dos pontos racionais de tais curvas que, despistando esta motivação, é também um interessante problema matemático. A questão – descrever propriedades aritméticas de curvas em termos de propriedades geométricas – é o que orienta a pesquisa realizada.

Seja $\mathcal{X}$ uma curva não-singular, de gênero g e definida sobre um corpo finito com q elementos. Para estudar valores quantitativos sobre o número N de pontos racionais de $\mathcal{X}$, é conveniente considerar a função complexa

$$\zeta_{\mathcal{X}}(s) := \sum_{D} q^{-s \cdot deg(D)},$$

onde D percorre os divisores efetivos de $\mathcal{X}$. Em 1948, Weil [28] demonstrou que os zeros desta função estão sobre a reta $Re(s) = 1/2$. Este importante resultado tem como consequência a seguinte estimativa:

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

onde g é gênero desta curva. Em particular,

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

Existem curvas que atingem a cota acima, são as chamadas *curvas maximais*. Quando isto não ocorre, surge o problema de saber sobre quais condições esta estimativa pode ser melhorada.

Em [26], Stöhr e Voloch estudam um método para abordar este problema de uma maneira mais geral. A técnica desenvolvida tem como ponto de partida o seguinte: define-se um morfismo ϕ de $\mathcal{X}$ em algum espaço projetivo e estuda-se o conjunto dos pontos $P \in \mathcal{X}$ tais que a imagem de $\phi(P)$, via a aplicação de Frobenius, pertence ao hiperplano osculador de P. A partir disto, é possível obter uma cota para o número de pontos racionais de $\mathcal{X}$ que depende de q, de g, da dimensão do espaço projetivo ambiente e do morfismo que aplica $\mathcal{X}$ neste espaço. Com uma escolha apropriada do morfismo é possível obter a estimativa de Weil, em algumas circunstâncias é possível também melhorá-la.

Nesta dissertação, iremos abordar o problema de contar pontos racionais de curvas algébricas usando a teoria de Stöhr-Voloch. Iremos obter diversas propriedades aritméticas e geométricas, e algumas delas irão auxiliar na caracterização de certas curvas.

Agora apresentaremos uma descrição de cada capítulo desta dissertação ressaltando os principais resultados.

No primeiro capítulo, fixaremos as notações e os principais resultados obtidos da teoria de variedades algébricas para o caso particular de curvas algébricas. É um capítulo de referência podendo ser omitido pelo leitor que seja familiarizado com conceitos introdutórios de geometria algébrica.

No segundo capítulo, iremos descrever uma correspondência entre morfismos de curvas em espaços projetivos e famílias de divisores efetivos (i.e. séries lineares). Estudaremos as principais propriedades destas famílias e como elas se relacionam com *espaços osculadores*. Tais espaços são generalizações de retas tangentes de curvas planas para dimensões superiores.

No terceiro capítulo, iremos utilizar o método de Stöhr-Voloch para obter uma cota para o número de pontos de uma curva $\mathcal{X}$ que satisfazem certas propriedades. O teorema de Stöhr-Voloch (teo.2.13 [26]) será demonstrado como um caso particular.

No quarto capítulo, iremos definir a função Zeta sobre uma curva algébrica, enunciar algumas propriedades e usar a teoria de Stöhr-Voloch para demonstrar o teorema de Hasse-Weil, que é a hipótese de Riemann para curvas algébricas sobre corpos finitos. Como consequência, iremos obter o teorema de Serre. Este teorema fornece a melhor estimativa para o número de pontos racionais de uma curva quando esta é genérica.

No quinto capítulo, aplicaremos os resultados obtidos em curvas maximais. Em particular, poderemos concluir algumas propriedades aritméticas e geométricas de tais curvas. Aqui iremos obter uma importante caracterização da curva Hermitiana.

Encerraremos a dissertação com dois apêndices. No primeiro enunciamos algumas definições e resultados clássicos da teoria de corpos de funções, os quais são utilizados sem maiores comentários ao longo do texto. No segundo, fornecemos algumas propriedades relevantes da aplicação de Frobenius sobre curvas definidas sobre corpos finitos. Tal aplicação caracteriza os pontos racionais da curva como sendo seus pontos fixos, portanto é uma das principais ferramentas para contar pontos.

Conteúdo

Capítulo 1

Geometria das Curvas Algébricas

Neste capítulo pretendemos fixar as notações e enunciar os principais resultados sobre a geometria das curvas algébricas, os quais serão utilizados ao longo de toda esta dissertação. Este é na verdade um capítulo de referência e pode naturalmente ser omitido pelo leitor que seja familiarizado com conceitos introdutórios de Geometria Algébrica. Caso contrário, os livros [2], [6], [12] e os capítulos introdutórios de [23] e [24] são as referências indicadas.

1.1 Variedades Algébricas

Em toda esta dissertação usaremos as notações

$$\begin{array}{cc} k & \text{um corpo perfeito.} \\ \bar{k} & \text{um fecho algébrico de } k \\ Gal(\bar{k}/k) & \text{o grupo de Galois da extensão } \bar{k}/k. \end{array}$$

Seja $\mathbb{A}^n$ o conjunto de todas as n-úplas com coeficientes em $\bar{k}$. Um *conjunto algébrico afim* V é um conjunto formado por pontos de $\mathbb{A}^n$ que são zeros de todos os polinômios de algum ideal $I \subseteq \bar{k}[X_1, \ldots, X_n]$. O *ideal* de um conjunto algébrico afim V é o ideal I_V gerado por todos os polinômios que se anulam em V. Uma *variedade afim* é um conjunto algébrico afim V tal que I_V é um ideal primo. Uma variedade afim V é *definida* sobre k se I_V pode ser gerado por polinômios em $k[X_1, \ldots, X_n]$. O *anel de coordenadas afim* de uma variedade afim V é definido por

$$k[V] := k[X_1, \ldots, X_n]/I_V.$$

Um elemento típico de $k[V]$ é da forma $f = F + I_V$, onde $F \in k[X_1, \ldots, X_n]$, logo define uma função $f : V \to \bar{k}$ dada por

$$f(P) := F(P).$$

O anel $k[V]$ é um domínio de integridade e seu corpo quociente, denotado por $k(V)$, é o conjunto das frações dos elementos de $k[V]$. Os elementos de $k(V)$ são chamados *funções racionais* de V. Por esta razão, o corpo $k(V)$ é chamado *corpo das funções racionais* de V. Um elemento típico de $k(V)$ é uma função racional $f = g/h$, onde $g, h \in k[V]$ e $h \neq 0$. Note que um elemento $f \in k(V)$ é uma função $f : V \to \bar{k}$ dada por

$$f(P) := g(P)/h(P),$$

que é bem definida em todo ponto $P \in V$ tal que $h(P) \neq 0$. Em termos de polinômios, a função racional f pode ser escrita na forma $f = G/H$ onde G, H são polinômios em $k[X_1, \ldots, X_n]$ que satisfazem:

(i) $H \notin I_V$;

(ii) G/H e G'/H' são identificados se, e somente se, $HG' - H'G \in I_V$.

Seja V uma variedade afim definida sobre k. O corpo $\bar{k}(V)$ é definido similarmente substituindo k por $\bar{k}$ na construção acima. O corpo $k(V)$ é caracterizado como sendo o subconjunto fixo pela ação do grupo de Galois $Gal(\bar{k}/k)$ sobre $\bar{k}(V)$. [1] A *dimensão* de V, denotada por $dim(V)$, é o grau de transcendência da extensão $\bar{k}(V)/\bar{k}$.

O teorema da base de Hilbert ([3], teo.7.5) afirma que qualquer ideal de polinômios é finitamente gerado. Em particular, qualquer conjunto algébrico pode ser escrito como o conjunto de zeros em comum de um número finito de polinômios. Suponha que a variedade afim V é definida pelas equações

$$F_1(X_1, \ldots, X_n) = \ldots = F_m(X_1, \ldots, X_n) = 0.$$

Um ponto $P \in V$ é *não-singular* em V, se a matriz $(\frac{\partial F_i}{\partial X_j}(P))$, chamada matriz *Jacobiana* da variedade afim V no ponto P, tem posto $n - dim(V)$. A variedade afim é *não-singular* se todo ponto for não-singular.

Seja P um ponto na variedade afim V. Uma função racional $f \in \bar{k}(V)$ é *regular* em P se existe uma representação $f = g/h$ tal que $h(P) \neq 0$. O *anel local* de V em P é o anel $\mathcal{O}_P(V)$ de todas as funções racionais de V que são regulares em P. Este é de fato um anel local, logo admite um único ideal maximal, a saber, o ideal $M_P(V)$ de todas as funções de $\mathcal{O}_P(V)$ que se anulam em P. Um elemento típico de $M_P(V)$ é da forma $f = g/h$ com $h(P) \neq 0$ e $g(P) = 0$.

Seja $\mathbb{P}^n$ o conjunto de todas as retas que passam pela origem de $\mathbb{A}^{n+1}$. Um *ponto* $P = (a_0 : \ldots : a_n) \in \mathbb{P}^n$ é a reta que passa pela origem e por $(a_0, \ldots, a_n)$. As coordenadas $a_0, \ldots, a_n$ são chamadas *coordenadas homogêneas* de P. Para estudar conjuntos em $\mathbb{P}^n$ que são zeros de equações polinomiais, devemos considerar polinômios homogêneos de $\bar{k}[X_0, \ldots, X_n]$. De fato, um polinômio homogêneo F de

[1] Se F é um polinômio em $\bar{k}[X_0, \ldots, X_n]$ então o grupo de Galois $Gal(\bar{k}/k)$ age em F sobre os seus coeficientes. Deste modo, se V é uma variedade afim definida sobre k, então o ideal I_V é fixo por $Gal(\bar{k}/k)$. Em particular, existe uma ação bem definida de $Gal(\bar{k}/k)$ sobre $\bar{k}(V)$.

grau d satisfaz a equação

$$F(\lambda a_0, \ldots, \lambda a_n) = \lambda^d F(a_0, \ldots, a_n) \quad \forall \quad \lambda \in \bar{k}\backslash\{0\},$$

portanto faz sentido considerar os pontos $P = (a_0 : \ldots : a_n) \in \mathbb{P}^n$ tais que $F(a_0, \ldots, a_n) = 0$. Um *conjunto algébrico projetivo* V é um conjunto formado por pontos de $\mathbb{P}^n$ que são zeros de todos os polinômios de algum ideal homogêneo[2] $I \subseteq \bar{k}[X_0, \ldots, X_n]$. O *ideal* de um conjunto algébrico projetivo é o ideal I_V gerado por todos os polinômios homogêneos que se anulam em V. Uma *variedade projetiva* é um conjunto algébrico projetivo V tal que I_V é um ideal primo. Uma variedade projetiva V é *definida* sobre k se I_V pode ser gerado por polinômios homogêneos em $k[X_0, \ldots, X_n]$. O *anel de coordenadas homogêneas* de uma variedade projetiva V é definido por

$$S[V] := k[X_0, \ldots, X_n]/I_V.$$

Em contraste com o caso afim, os elementos de $S[V]$ não definem funções sobre a variedade projetiva V. Contudo, o quociente g/h, onde $g, h \in S[V]$ são elementos que podem ser representados por polinômios homogêneos de mesmo grau, são funções sobre V bem definidas. De fato, se g e h podem ser representados pelos polinômios homogêneos G e H, respectivamente, ambos de grau d, então

$$\frac{G(\lambda X_0, \ldots, \lambda X_n)}{H(\lambda X_0, \ldots, \lambda X_n)} = \frac{\lambda^d G(X_0, \ldots, X_n)}{\lambda^d H(X_0, \ldots, X_n)} = \frac{G(X_0, \ldots, X_n)}{H(X_0, \ldots, X_n)},$$

logo a função $f : V \to \bar{k}$ dada por

$$f(P) := g(P)/h(P),$$

é bem definida em todo ponto $P \in V$ tal que $h(P) \neq 0$. Uma tal função é chamada *função racional* de V. O *corpo das funções racionais* de uma variedade projetiva V, denotado por $k(V)$, é o conjunto de todas as funções racionais sobre V. Em termos de polinômios, a função racional f pode ser escrita na forma $f = G/H$ onde G, H são polinômios em $k[X_0, \ldots, X_n]$ que satisfazem:

(i) $H \notin I_V$;

(i) G e H são homogêneos de mesmo grau;

(ii) G/H e G'/H' são identificados se, e somente se, $FG' - F'G \in I_V$.

Seja P um ponto na variedade projetiva V. Uma função racional $f \in \bar{k}(V)$ é *regular* em P se existe uma representação $f = g/h$ tal que $h(P) \neq 0$. O *anel local* de V é o anel $\mathcal{O}_P(V)$ de todas as funções racionais de V que são regulares em P. Este é de fato um anel local, logo admite um único ideal maximal, a saber, o ideal $M_P(V)$ de todas as funções em $\mathcal{O}_P(V)$ que se anulam em P. Um elemento típico de $M_P(V)$ é da forma $f = g/h$ com $h(P) \neq 0$ e $g(P) = 0$.

Como no caso afim, a *dimensão* da variedade projetiva V, denotada por $dim(V)$, é o grau de transcendência da extensão $\bar{k}(V)/\bar{k}$.

[2]Um ideal é chamado homogêneo se pode ser gerado por polinômios homogêneos.

Note que para cada $0 \leq i \leq n$ existe uma decomposição $\mathbb{P}^n = \mathbb{A}_i^n \cup \mathbb{P}_i^{n-1}$ onde $\mathbb{A}_i^n$ é o conjunto obtido de $\mathbb{P}^n$ tomando a i-ésima coordenada igual a 1 e $\mathbb{P}_i^{n-1}$ é o conjunto obtido de $\mathbb{P}^n$ tomando a i-ésima coordenada igual a 0. Deste modo, para cada variedade projetiva V, podemos considerar a decomposição

$$V = (V \cap \mathbb{A}_i^n) \cup (V \cap \mathbb{P}_i^{n-1}),$$

para algum i fixo. O conjunto $V \cap \mathbb{A}_i^n$ é uma variedade afim chamada *parte afim* de V e $V \cap \mathbb{P}_i^{n-1}$ é o conjunto dos *pontos no infinito* de V.

Seja P um ponto da variedade projetiva V. O ponto P é *não-singular* em V, se existe i tal que P é um ponto não-singular da variedade afim $V \cap \mathbb{A}_i^n$. A variedade projetiva V é *não-singular* se todo ponto for não-singular.

Dada uma variedade afim V, considere as $n+1$ inclusões em $\mathbb{P}^n$ dadas por

$$V \subseteq \mathbb{A}^n \longrightarrow \mathbb{P}^n, \quad (a_1, \ldots, a_n) \longmapsto (a_1 : \ldots : a_{i-1} : 1 : a_i : \ldots : a_n).$$

O *fecho projetivo* de uma variedade afim V é a variedade projetiva $\bar{V}$ tal que os polinômios homogêneos em $I_{\bar{V}}$ se anulam na imagem de V via a aplicação acima. Note que $I_{\bar{V}}$ é o conjunto dos polinômios $F^*(X_0, \ldots, X_n) \in \bar{k}[X_0, \ldots, X_n]$ tais que

$$F^*(X_0, \ldots, X_n) := X_i^{deg(F)} F(X_0/X_i, \ldots, X_n/X_i)$$

e $F \in I_V$. O polinômio F^* é a *homogeneização* do polinômio F.

Exemplo 1.1.1 *Seja V a variedade afim definida pelo polinômio*

$$F(X, Y) = Y^2 + Y - X^9 \in \mathbb{F}_7[X, Y].$$

O fecho projetivo de V é a variedade projetiva $\bar{V}$ definida pelo polinômio homogêneo

$$G(X, Y, Z) = Y^2 Z^7 + Y Z^8 - X^9 \in \mathbb{F}_7[X, Y, Z].$$

Note que G é a homogeneização de F. Os pontos afins de $\bar{V}$ são os pontos $(a : b : 1)$ tais que $G(a : b : 1) = 0$, logo são tais que $b^2 + b = a^9$. Os pontos no infinito de $\bar{V}$ são os pontos $(a : b : 0)$ tais que $G(a : b : 0) = 0$, logo são tais que $b \cdot 0^2 + b \cdot 0 = a^9$. Portanto $(0 : 1 : 0)$ é o único ponto no infinito de V. Note que este é um ponto singular da variedade $\bar{V}$.

1.2 Curvas Projetivas

Após o prelúdio da seção anterior já estamos em condições de definir o principal objeto desta dissertação.

Definição 1.2.1 *Uma **curva algébrica projetiva** , ou simplesmente uma **curva**, é uma variedade projetiva $\mathcal{X}$ de dimensão 1, ou seja, existe $f \in \bar{k}(\mathcal{X})$ transcendente sobre $\bar{k}$ tal que $\bar{k}(\mathcal{X})$ é uma extensão algébrica e finita de $\bar{k}(f)$. Uma curva **plana** é uma curva $\mathcal{X}$ contida em $\mathbb{P}^2$.*

Proposição 1.2.2 *Um ponto $P \in \mathcal{X}$ é não-singular se, e somente se, $\mathcal{O}_P(\mathcal{X})$ é um domínio de valorização discreta.*

Demonstração: Em [23], veja (I.1.7, pag.9), (II.1.1, pag. 21) e (exer.2.1, pag. 42).

□

Definição 1.2.3 *Seja $\mathcal{X}$ uma curva e seja $P \in \mathcal{X}$ um ponto não-singular. A **valorização** sobre $\mathcal{O}_P(\mathcal{X})$ é dada por*

$$v_P : \mathcal{O}_P(\mathcal{X}) \to \{0, 1, 2, \ldots, \} \cup \{\infty\},$$
$$v_P(f) := max\{d \in \mathbb{N}_0 \ ; \ f \in M_P(\mathcal{X})^d\}.$$

*Definindo $v_P(f/g) := v_P(f) - v_P(g)$, v_P pode ser naturalmente estendida para $\bar{k}(\mathcal{X})$. Um **parâmetro local** de P é uma função racional $t \in \bar{k}(\mathcal{X})$ tal que $v_P(t) = 1$.*

O parâmetro local $t \in \bar{k}(\mathcal{X})$ do ponto P dado na definição é o gerador do ideal $M_P(\mathcal{X})$. Em particular, todo elemento $f \in \bar{k}(\mathcal{X})^*$ pode ser escrito na forma $f = t^n u$ onde t é um parâmetro local de P, $u \in \mathcal{O}_P(\mathcal{X})^*$ e $n = v_P(f)$. As principais propriedades da valorização v_P são

(a) $v_P(a) = 0$ para todo $a \in \bar{k}^*$,

(b) $v_P(fg) = v_P(f) + v_P(g)$,

(c) $v_P(t) = 1$ sempre que t for um parâmetro local para P e

(d) $v_P(f + g) \geq min\{v_P(f), v_P(g)\}$ com igualdade sempre que $v_P(f) \neq v_P(g)$.

Esta última propriedade chama-se *desigualdade triangular estrita*. A valorização v_P determina completamente o anel local $\mathcal{O}_P(\mathcal{X})$ e seu ideal maximal $M_P(\mathcal{X})$. De fato,

$$\begin{aligned} \mathcal{O}_P(\mathcal{X}) &= \{f \in \bar{k}(\mathcal{X}) \ ; \ v_P(f) \geq 0\}, \\ \mathcal{O}_P^*(\mathcal{X}) &= \{f \in \bar{k}(\mathcal{X}) \ ; \ v_P(f) = 0\} \text{ e} \\ M_P(\mathcal{X}) &= \{f \in \bar{k}(\mathcal{X}) \ ; \ v_P(f) > 0\}. \end{aligned}$$

O número $v_P(f)$ é chamado *ordem* de f em P. Se $v_P(f) = m < 0$ então P é chamado *pólo* de ordem m de f. Se $v_P(f) = m > 0$ então P é chamado *zero* de ordem m de f. Para maiores detalhes sobre anéis locais e valorizações consulte o apêndice A e as referências que lá estão indicadas.

Proposição 1.2.4 *Se f é uma função racional em $\bar{k}(\mathcal{X})$ então f admite apenas um número finito de zeros e de pólos. Mais ainda, se f não tem pólos então $f \in \bar{k}$.*

Demonstração: Para ver este resultado em termos de variedades veja ([12], II.6.1, pag.131) ou ([22], pag.153). Em termos de corpos de funções veja ([25], I.3.4, pag.14) ou ([20], pag.47).

□

Agora suponha que $\mathcal{X}$ é definida sobre k. Um elemento $x \in k(\mathcal{X})$ é chamado *elemento de separação* de $k(\mathcal{X})$ sobre k se a extensão $k(\mathcal{X})/k(x)$ é finita e separável. O próximo teorema resume as principais propriedades dos elementos de separação.

Teorema 1.2.5 *Seja $\mathcal{X}$ uma curva não-singular definida sobre o corpo k cuja característica é p.*

(a) Sempre existem elementos de separação de $k(\mathcal{X})$ sobre k.

(b) Um elemento $z \in k(\mathcal{X})$ é separável se, e somente se, $z \notin k(\mathcal{X})^p$.

(c) Um elemento $z \in k(\mathcal{X})$ é separável sempre que a característica p de k não divide $v_P(z)$ para algum ponto $P \in \mathcal{X}$.

(d) Parâmetros locais sempre serão elementos de separação.

Demonstração: Estes são resultados conhecidos da teoria de corpos de funções em uma variável, veja ([25], III.9.5, pag.128). Note que (c) implica (d) uma vez que $v_P(t) = 1$ sempre que t é um parâmetro local de P.

□

Teorema 1.2.6 *Seja $\mathcal{X}$ uma curva definida sobre k e seja $P \in \mathcal{X}$ um ponto não-singular com um parâmetro local $t \in k(\mathcal{X})$, então todo elemento $f \in k(\mathcal{X})$ admite uma única representação da forma*

$$f = \sum_{s=m}^{\infty} a_s t^s \quad com \quad m \in \mathbb{Z} \quad e \quad a_i \in k.$$

Ainda mais, se $(c_i)_{i \geq n}$ é uma sequência em k então

$$v_P(\sum_{s=n}^{\infty} c_s t^s) = min\{s \ ; \ c_s \neq 0\}.$$

Demonstração: Sobre séries de potências em termos de variedades arbitrárias veja ([22], pag.101), somente em termos de curvas veja ([6], pag.49) e em termos de corpos de funções veja ([10], pag.22) ou ([25], pag.143).

□

A representação do elemento f dada no teorema é chamada *expansão local* de f em P.

1.3 Morfismos entre Curvas

Tendo definido curvas algébricas, precisamos definir aplicações entre elas. O que faremos nesta seção é definir morfismos entre curvas e estabelecer quais informações são invariantes por estes morfismos.

Definição 1.3.1 *Seja $\mathcal{X}$ uma curva. Uma* ***aplicação racional*** $\phi : \mathcal{X} \to \mathbb{P}^n$ *é dada por uma n-úpla $(f_0 : \ldots : f_n)$ de elementos de $\bar{k}(\mathcal{X})$ tal que $(f_0 : \ldots : f_n)$ e $(g_0 : \ldots : g_n)$ definem a mesma aplicação racional se, e somente se, existe $h \in \bar{k}(\mathcal{X})^*$ tal que $g_i = hf_i$. Se $\mathcal{X}'$ é uma curva em $\mathbb{P}^m$, uma* ***aplicação racional*** $\phi : \mathcal{X} \to \mathcal{X}'$ *é justamente uma aplicação racional $\phi : \mathcal{X} \to \mathbb{P}^m$ com $\phi(P) \in \mathcal{X}'$ para todo P. A aplicação ϕ é* ***definida*** *sobre k se existe uma representação $\phi = (f_0 : \ldots : f_n)$ tal que $f_0, \ldots, f_n \in k(\mathcal{X})$.*

Definição 1.3.2 *Seja $P \in \mathcal{X}$. Uma aplicação racional $\phi : \mathcal{X} \to \mathbb{P}^n$ é* ***regular*** *em P se existe uma representação $\phi = (f_0 : \ldots : f_n)$ onde cada $f_i \in \mathcal{O}_P(\mathcal{X})$ e existe j tal que $f_j(P) \neq 0$. Um* ***morfismo*** *$\phi : \mathcal{X} \to \mathcal{X}'$ é uma aplicação racional que é regular em todo ponto. Um* ***isomorfismo*** *$\phi : \mathcal{X} \to \mathcal{X}'$ é um morfismo que admite um morfismo inverso $\psi : \mathcal{X}' \to \mathcal{X}$.*

Se as funções $f_0, \ldots, f_n$ que definem o morfismo ϕ formam um conjunto linearmente independente, então ϕ é chamado de morfismo *não-degenerado*. Isto significa que a imagem de $\mathcal{X}$ via ϕ não está contida em nenhum hiperplano de $\mathbb{P}^n$. Daqui para frente ϕ será sempre um morfismo não-degenerado.

Teorema 1.3.3 *Seja $P \in \mathcal{X}$ um ponto não-singular. Se $\phi : \mathcal{X} \to \mathbb{P}^n$ é uma aplicação racional então ϕ é regular em P. Em particular, se $\mathcal{X}$ é não-singular então ϕ é um morfismo.*

Demonstração: Suponha $\phi = (f_0 : \ldots : f_n)$ com $f_i \in \bar{k}(\mathcal{X})$ e seja t um parâmetro local de P. Uma vez que P é não singular, $\mathcal{O}_P(\mathcal{X})$ é um domínio de valorização discreta e portanto podemos considerar o número $e_P := -min\{v_P(f_i)\ ;\ 0 \leq i \leq n\}$. Note que $v_P(t^{e_P} f_i) \geq 0$ para todo i e que existe j tal que $v_P(t^{e_P} f_j) = 0$, logo $t^{e_P} f_i$ é regular para todo i e $t^{e_P} f_j(P) \neq 0$ para algum j. Portanto ϕ é regular em P.

□

Teorema 1.3.4 *Imagens de curvas projetivas por morfismos são também curvas projetivas. Se $\phi : \mathcal{X} \to \mathcal{X}'$ é um morfismo entre curvas não-singulares, então ϕ é sobrejetivo ou é constante.*

Demonstração: A primeira parte deste teorema é na verdade um caso particular de um resultado mais geral que afirma que a imagem de qualquer variedade projetiva por morfismos é ainda uma

variedade projetiva, veja ([22], pag.57). Este resultado não vale em geral para variedades afins, veja ([23], pag.17). Para ver que morfismos não constantes entre curvas é sempre sobrejetivo consulte ([22],5.3.4, pag.61).

□

Exemplo 1.3.5 *Seja $\mathcal{X}$ uma curva definida sobre k e seja $f \in k(\mathcal{X})$. Então f induz a seguinte aplicação racional de $\mathcal{X}$ em $\mathbb{P}^1$:*

$$\begin{array}{rcl} \phi_f : \mathcal{X} & \longrightarrow & \mathbb{P}^1 \\ P & \longmapsto & \phi_f(P) = \begin{cases} (f(P):1) & \text{se } f \text{ é regular em } P \\ (1:0) & \text{se } f \text{ tem um pólo em } P. \end{cases} \end{array}$$

Sejam $\mathcal{X}$ e $\mathcal{X}'$ curvas definidas sobre k. Então cada aplicação racional não constante $\phi : \mathcal{X} \to \mathcal{X}'$, definida sobre k, induz um k-homomorfismo injetor

$$\begin{array}{rcl} \phi^* & : & k(\mathcal{X}') \to k(\mathcal{X}) \\ & & \phi^* f \mapsto f \circ \phi. \end{array}$$

A aplicação ϕ^* é chamada de *pull-back* de ϕ induzido em $k(\mathcal{X}')$. O próximo teorema resume as principais propriedades desta aplicação.

Teorema 1.3.6 *Sejam $\mathcal{X}$ e $\mathcal{X}'$ curvas definidas sobre k.*

(a) Se $\phi : \mathcal{X} \to \mathcal{X}'$ é um morfismo definido sobre k, então $k(\mathcal{X})$ é uma extensão finita de $\phi^* k(\mathcal{X}')$.

(b) Seja $\iota : k(\mathcal{X}') \to k(\mathcal{X})$ um k-homomorfismo injetor, então existe um único morfismo não constante $\phi : \mathcal{X}' \to \mathcal{X}$, definido sobre k, tal que $\phi^* = \iota$.

(c) Seja K um subcorpo de $k(\mathcal{X})$ tal que o índice $[k(\mathcal{X}) : K]$ é finito. Então existe uma única curva não-singular $\mathcal{X}'$ (única a menos de isomorfismo), definida sobre k, e um morfismo não constante $\phi : \mathcal{X} \to \mathcal{X}'$, definida sobre k, tal que $\phi^* k(\mathcal{X}') = K$.

Demonstração: Veja ([23], II.2.4, pag. 25).

□

Definição 1.3.7 *Seja $\phi : \mathcal{X} \to \mathcal{X}'$ um morfismo de curvas definido sobre k. O **grau** do morfismo ϕ é o número $deg(\phi) := [k(\mathcal{X}) : \phi^* k(\mathcal{X}')]$. O morfismo ϕ é **birracional** se $deg(\phi) = 1$. O morfismo é **separável** se a extensão $k(\mathcal{X})/\phi^* k(\mathcal{X}')$ é separável. O **grau de separabilidade** do morfismo ϕ, denotado por $deg_s(\phi)$, é o grau de separabilidade desta extensão.*

Teorema 1.3.8 *Um morfismo birracional entre curvas não-singulares é um isomorfismo. Qualquer curva é birracional a uma única curva não-singular (única a menos de isomorfismo).*

Demonstração: Veja ([24], A.4.1.3-A.4.1.4, pag. 69-70).

□

Definição 1.3.9 *Seja $\phi : \mathcal{X} \to \mathcal{X}'$ um morfismo entre curvas não-singulares e seja t um parâmetro local de $\phi(P)$ em $\bar{k}(\mathcal{X}')$. O inteiro positivo*

$$e_\phi(P) := v_P(\phi^*(t)),$$

onde ϕ^* é o pull-back de ϕ induzido em $\bar{k}(\mathcal{X}')$, é chamado ***índice de ramificação*** *de ϕ em P. Se $e_\phi(P) = 1$ então ϕ é* ***não-ramificado*** *em P, caso contrário ϕ é* ***ramificado*** *em P.*

Não é difícil verificar que o número $e_\phi(P)$ não depende do parâmetro local t de $\phi(P)$ em $\bar{k}(\mathcal{X}')$. Note também que para cada ponto $P \in \mathcal{X}$ e para cada $f \in \bar{k}(\mathcal{X}')$ vale

$$v_P(\phi^* f) = e_\phi(P) v_{\phi(P)}(f). \quad [3]$$

Teorema 1.3.10 *Seja $\phi : \mathcal{X} \to \mathcal{X}'$ um morfismo não-constante entre curvas não-singulares.*

(a) Para todo $Q \in \mathcal{X}'$,

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = deg(\phi).$$

(b) Vale a igualdade

$$\#\phi^{-1}(Q) = deg_s(\phi)$$

para quase todo $Q \in \mathcal{X}'$, ou seja, a menos de um número finito de pontos de $\mathcal{X}'$.

(c) Seja $\psi : \mathcal{X}' \to \mathcal{X}''$ um outro morfismo não-constante. Então para cada $P \in \mathcal{X}$,

$$e_{\psi \circ \phi}(P) = e_\phi(P) e_\psi(\phi(P)).$$

Demonstração: Veja ([23], 2.6, pag. 28).

□

[3] De fato, escolha um parâmetro local t de $\phi(P)$ e escreva $f = t^n u$ com $u \in \mathcal{O}_{\phi(P)}(\mathcal{X}')^*$, agora aplique ϕ^* em $t^n u$ e note que $n = v_{\phi(P)}(f)$ e $v_P(\phi^*(u)) = 0$.

Corolário 1.3.11 *Seja $\phi : \mathcal{X} \to \mathcal{X}'$ um morfismo não-constante entre curvas não-singulares e seja $Q \in \mathcal{X}'$. Então ϕ é não-ramificado nos pontos da fibra $\phi^{-1}(Q)$ se, e somente se, $\#\phi^{-1}(Q) = deg(\phi)$. Em particular, se ϕ é separável então existe apenas um número finito de pontos de $\mathcal{X}$ que são ramificados por ϕ.*

Demonstração: Pelo item (a) do teorema (1.3.10), $\#\phi^{-1}(Q) = deg(\phi)$ é equivalente a

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \#\phi^{-1}(Q).$$

Isto ocorre se, e somente se, $e_\phi(P) = 1$ para todo $P \in \phi^{-1}(Q)$. Se ϕ é separável então $deg(\phi) = deg_s(\phi)$ e portanto existe apenas um número finito de pontos $Q \in \mathcal{X}'$ tais que $\#\phi^{-1}(Q) \neq deg(\phi)$ (item (b), teo. (1.3.10)). Pela primeira parte deste corolário, cada ponto ramificado por ϕ está em uma destas fibras, as quais são sempre finitas, logo existe apenas um número finito de pontos em $\mathcal{X}$ que são ramificados por ϕ.

□

1.4 Divisores sobre Curvas

Para esta seção, a palavra *curva* significa curva algébrica, projetiva, não-singular e irredutível.

Definição 1.4.1 *Seja $\mathcal{X}$ uma curva. O **grupo de divisores** de $\mathcal{X}$ é o grupo abeliano livre $Div(\mathcal{X})$ gerado por todos os pontos de $\mathcal{X}$. Um **divisor** é um elemento deste grupo da forma $D = \sum_P n_P P$ onde n_P é nulo quase sempre. O **suporte** de D é o conjunto $supp(D)$ de todos os pontos $P \in \mathcal{X}$ tais que $n_P \neq 0$. O divisor D é **efetivo** se $n_P \geq 0$ para todo P. O **grau** de D é o número $deg(D) := \sum_P n_P$. O divisor D é **definido** sobre k se for invariante pela ação do grupo de Galois $Gal(\bar{k}/k)$* [4].

A notação $D \geq 0$ será usada para indicar que o divisor D é efetivo e a notação $D \geq D'$ será usada para indicar que o divisor $D - D'$ é efetivo. É conveniente estender valorizações para o conjunto dos divisores de $\mathcal{X}$. Para cada ponto $Q \in \mathcal{X}$ e cada divisor $D = \sum_P n_P P$ defina $v_Q(D) := n_Q$. Deste modo,

$$D = \sum_{P \in \ supp(D)} v_P(D) P.$$

Seja $f \in \bar{k}(\mathcal{X})$ não nulo e denote por Z o conjunto de todos os zeros de f e por N o conjunto de todos os pólos de f. Note que estes conjuntos são finitos, pela proposição (1.2.4). Deste modo, os

[4] O grupo de Galois $Gal(\bar{k}/k)$ age nos pontos de $\mathcal{X}$ sobre as suas coordenadas homogêneas. Esta ação é naturalmente estendida $\mathbb{Z}$-linearmente ao conjunto $Div(\mathcal{X})$.

divisores

$$div(f)_0 := \sum_{P \in Z} v_P(f)P \quad \text{e} \quad div(f)_\infty := \sum_{P \in N} v_P(f)P,$$

são bem definidos. Ambos são divisores efetivos e recebem, respectivamente, o nome de *divisor de zeros* de f e *divisor de pólos* de f. A diferença entre estes dois divisores fornece o divisor

$$div(f) := div(f)_0 - div(f)_\infty,$$

que é chamado *divisor principal* de f.

Segue das definições que $div(f) = 0$ sempre que $f \in \bar{k}^*$ e que $div(fg) = div(f) + div(g)$. Note também que $v_P(div(f)) = v_P(f)$. Dois divisores D e D' sobre $\mathcal{X}$ são chamados *equivalentes* sempre que o divisor $D - D'$ for principal. A notação $D \sim D'$ será usada para indicar que D e D' são equivalentes.

Teorema 1.4.2 *Seja $\mathcal{X}$ uma curva e seja $f \in \bar{k}(\mathcal{X})$. Então*

(a) $div(f) = 0$ se, e somente se, $f \in \bar{k}^*$.

(b) $deg(div(f)_0) = deg(div(f)_\infty) = [\bar{k}(\mathcal{X}) : \bar{k}(f)]$. Em particular, o grau de qualquer divisor principal é sempre zero.

(c) Suponha que $\mathcal{X}$ é definida sobre k. Se D é um divisor definido sobre k e existe uma função racional $f \in \bar{k}(\mathcal{X})$ tal que $D = div(f)$, então existe uma função racional $f' \in k(\mathcal{X})$ tal que $D = div(f')$.

Demonstração: O item (a) segue de ([23],II.3.1, pag. 32), o item (b) de ([25], I.4.11, pag. 18) e o item (c) de ([24], A.2.2.10(ii), pag. 43).

□

Um morfismo não-constante $\phi : \mathcal{X} \to \mathcal{X}'$ induz a seguinte aplicação entre os grupos dos divisores de $\mathcal{X}$ e $\mathcal{X}'$:

$$\begin{aligned} \phi^* \quad : \quad & Div(\mathcal{X}') \to Div(\mathcal{X}) \\ & Q \mapsto \sum_{P \in \phi^{-1}(Q)} e_\phi(P)P, \end{aligned}$$

estenda $\mathbb{Z}$-linearmente sobre divisores arbitrários. As principais propriedades a respeito desta aplicação será resumida no próximo teorema.

Teorema 1.4.3 *Seja $\phi : \mathcal{X} \to \mathcal{X}'$ uma aplicação não-constante entre curvas. Então*

(a) $deg(\phi^* D) = deg(\phi) deg(D)$ para todo $D \in Div(\mathcal{X}')$.

(b) $\phi^*(div(f)) = div(\phi^* f)$ para todo $f \in \bar{k}(\mathcal{X}')^*$.

Demonstração: O item (a) segue rapidamente do teorema (1.3.10) e o item (b) segue das definições e da igualdade $v_P(\phi^* f) = e_\phi(P) v_{\phi(P)}(f)$, onde $P \in \mathcal{X}$ e $f \in \bar{k}(\mathcal{X}')$.

□

1.5 Diferenciais sobre Curvas

Definição 1.5.1 *Seja $\mathcal{X}$ uma curva. O conjunto dos **diferenciais** sobre $\mathcal{X}$ é o conjunto $\Omega^1[\mathcal{X}]$ de todas as somas finitas $\sum_1 f_i dg_i$ onde $f_i, g_i \in \bar{k}(\mathcal{X})$ e*

(i) $da = 0$ para todo $a \in \bar{k}$.

(ii) $d(f+g) = df + dg$ para todo $f, g \in \bar{k}(\mathcal{X})$.

(iii) $d(fg) = fdg + gdf$ para todo $f, g \in \bar{k}(\mathcal{X})$.

Proposição 1.5.2 *O conjunto $\Omega^1[\mathcal{X}]$ é um espaço vetorial unidimensional sobre $\bar{k}(\mathcal{X})$ e com gerador dx, onde x é qualquer elemento de separação de $\bar{k}(\mathcal{X})$ sobre $\bar{k}$. Ainda mais, $dx \neq 0$ se, e somente se, x é um elemento de separação de $\bar{k}(\mathcal{X})$ sobre $\bar{k}$.*

Demonstração: Veja ([23], II.4.2, pag. 35).

□

Teorema 1.5.3 *Seja $P \in \mathcal{X}$ com parâmetro local t.*

(a) Para cada $\omega \in \Omega^1[\mathcal{X}]$ existe uma única $f \in \bar{k}(\mathcal{X})$ (que depende de ω e t) tal que $\omega = fdt$.

(b) Se $f \in \bar{k}(\mathcal{X})$ é regular em P, então df/dt é regular em P.

(c) O número $v_P(\omega/dt)$ depende somente de ω, ou seja, não depende de t.

(d) Se x é um elemento de separação de $\in \bar{k}(\mathcal{X})$ tal que $v_P(x) > 0$, então para cada $f \in \bar{k}(\mathcal{X})$ vale

$$v_P(fdx) = v_P(f) + v_P(x) - 1.$$

Em particular, $v_P(dt) = 0$.

(e) $v_P(\omega/dt) = 0$ quase sempre.

Demonstração:Veja ([23], II.4.3(a e d), pag. 35).

□

Pelo item (c) do teorema anterior é bem definido o número $v_P(\omega) := v_P(\omega/dt)$, onde t é um parâmetro local de P. Este valor é chamado *ordem* de ω. Um diferencial ω é chamado *regular* em P se $v_P(\omega) \geq 0$.

Definição 1.5.4 *Seja $\omega \in \Omega^1[\mathcal{X}]$. O divisor $div(\omega)$ definido por*

$$div(\omega) := \sum_P v_P(\omega)P$$

*é chamado de **divisor canônico** sobre $\mathcal{X}$.*

Note que se ω_1, ω_2 são dois diferenciais não nulos, então o item (a) do teorema (1.5.3) implica que existe uma função não nula $f \in \bar{k}(\mathcal{X})$ tal que $\omega_1 = f\omega_2$. Deste modo,

$$div(\omega_1) = div(f) + div(\omega_2).$$

Em particular, divisores canônicos são sempre equivalentes.

1.6 O Teorema de Riemann-Roch e a Fórmula de Riemann-Hurwitz

Um dos resultados centrais da teoria de curvas algébricas é o teorema de Riemann-Roch. Este teorema calcula a dimensão de uma importante classe de espaços vetoriais que definiremos agora.

Definição 1.6.1 *Seja D um divisor sobre $\mathcal{X}$. O **espaço de Riemann-Roch** em relação a D é o $\bar{k}$-espaço vetorial definido por*

$$\mathcal{L}(D) := \{f \in \bar{k}(\mathcal{X}) \ ; \ D + div(f) \geq 0\} \cup \{0\}.$$

A dimensão de $\mathcal{L}(D)$ (que é finita) é denotada por $l(D)$.

Para ver que $l(D)$ é de fato um número finito consulte ([22],III.2.3.5, pag.173). Seja $\mathcal{X}$ uma curva definida sobre k e suponha que D é um divisor também definido sobre k. Nestas condições, considere o k-espaço vetorial $\mathcal{L}_k(D)$ definido por

$$\mathcal{L}_k(D) := \{f \in \mathcal{L}(D) \ ; \ \sigma(f) = f \ \forall \ \sigma \in Gal(\bar{k}/k)\}.$$

É claro que $\mathcal{L}_{\bar{k}}(D) = \mathcal{L}(D)$. O próximo teorema irá estabelecer uma conexão entre os espaços $\mathcal{L}_k(D)$ e $\mathcal{L}(D)$ e justificará o porque podemos sempre trabalhar no fecho algébrico $\bar{k}$ do corpo perfeito k.

Teorema 1.6.2 *Seja $\mathcal{X}$ uma curva definida sobre k e suponha que D é um divisor também definido sobre k. Nestas condições, o espaço vetorial $\mathcal{L}(D)$ admite uma base com elementos em $k(\mathcal{X})$. Em particular, $dim\mathcal{L}(D) = dim\mathcal{L}_k(D)$.*

Demonstração: Veja ([23], A.2.2.10(i), pag. 43).

□

O próximo lema resume as principais propriedades referentes aos espaços de Riemann-Roch.

Lema 1.6.3 *Seja $\mathcal{X}$ uma curva não-singular e sejam D e D' dois divisores sobre esta curva.*

(a) $\bar{k} \subseteq \mathcal{L}(D)$ se, e somente se, $D \geq 0$.

(b) Se $D \geq D'$ então $\mathcal{L}(D) \supseteq \mathcal{L}(D')$

(c) Se $D' = D + div(g)$, então a aplicação $f \mapsto gf$ define um $\bar{k}$-isomorfismo do espaço $\mathcal{L}(D')$ sobre o espaço $\mathcal{L}(D)$. Em particular, a dimensão $l(D)$ é um invariante por equivalência de divisores.

(d) Se $deg(D) < 0$ então $l(D) = 0$

(e) $l(D - P) \geq l(D) - 1$ para cada ponto $P \in \mathcal{X}$.

Demonstração: As demonstrações de (a), (b),(c) e (d) são simples e decorrem rapidamente das definições, logo apenas o item (e) será demonstrado. Seja $n = v_P(D)$ e t um parâmetro local de P. Considere a aplicação

$$\begin{aligned} \varphi \quad : \quad & \mathcal{L}(D) \longrightarrow \bar{k} \\ & f \longmapsto (t^n f)(P) \end{aligned}$$

Note que $v_P(t^n f) = v_P(D) + v_P(f) \geq 0$, logo φ é um homomorfismo bem definido cujo núcleo $Ker(\varphi)$ são todos os elementos $g \in \mathcal{L}(D)$ tais que $t^n g \in M_P(\mathcal{X})$, ou seja, $v_P(D) + v_P(g) \geq 1$. Deste modo $Ker(\varphi) = \mathcal{L}(D-P)$, logo a dimensão do quociente $\mathcal{L}(D)/\mathcal{L}(D-P)$ é no máximo igual a um e portanto $l(D - P) \geq l(D) - 1$.

□

Na seção anterior foi definido divisores canônicos sobre a curva $\mathcal{X}$ e foi visto que dois deles são sempre equivalentes. No que segue, a notação $K_{\mathcal{X}}$ será usada para designar algum divisor canônico sobre $\mathcal{X}$.

Teorema 1.6.4 (Teorema de Riemann-Roch) *Seja $\mathcal{X}$ uma curva não-singular. Então existe um inteiro $g \geq 0$ tal que, para todo divisor D sobre $\mathcal{X}$,*

$$l(D) = deg(D) - g + 1 + l(K_{\mathcal{X}} - D)$$

Demonstração: Para uma demonstração em termos de curvas veja ([6], pag. 210) ou ([22], pag. 215), em característica zero veja ([18], pag. 312). Para uma demonstração em termos de corpos de funções veja ([25], pag. 22), ([20], pag. 73) ou ([10], pag. 50).

□

Definição 1.6.5 *O inteiro g dado no teorema anterior é chamado **gênero** da curva $\mathcal{X}$.*

O gênero de uma curva com pontos singulares é por definição o gênero de seu modelo não-singular (teo. 1.3.8).

Corolário 1.6.6 *Com as notações do teorema.*

(a) Para todo divisor canônico $K_{\mathcal{X}}$ temos $l(K_{\mathcal{X}}) = g$.

(b) Um divisor D é canônico se, e somente se, $deg(D) = 2g - 2$ e $l(D) \geq g$.

(c) Se $deg(D) \geq 2g - 1$ então $l(D) = deg(D) - g + 1$.

(d) O gênero de $\mathcal{X}$ é zero se, e somente se, $\mathcal{X}$ e $\mathbb{P}^1$ são isomorfos.

Demonstração: (a) Basta considerar $D = 0$ no teorema.

(b) Se D é canônico, substitua $K_{\mathcal{X}}$ por D no teorema de Riemann-Roch e use o item anterior para concluir que $deg(D) = 2g - 2$ e $l(D) \geq g$. Reciprocamente, se D é um divisor satisfazendo $deg(D) = 2g - 2$ e $l(D) \geq g$, então

$$g \leq l(D) = deg(D) + 1 - g + l(K_{\mathcal{X}} - D) = g - 1 + l(K_{\mathcal{X}} - D),$$

logo $l(K_{\mathcal{X}} - D) \geq 1$, ou seja, existe $x \in \bar{k}(\mathcal{X})^*$ tal que o divisor $K_{\mathcal{X}} - D + div(x)$ é efetivo e com grau nulo. Isto significa que $K_{\mathcal{X}} - D + div(x) = 0$, logo $K_{\mathcal{X}} - D$ é principal e portanto D é canônico.

(c) Se $deg(D) \geq 2g - 1$ então $deg(K_{\mathcal{X}} - D) < 0$ e o resultado segue como consequência dos itens anteriores e do item (d) do lema (1.6.3).

(d) Veja ([22], III.6.6.3, pag. 216).

□

Dado um morfismo não-constante $\phi : \mathcal{X} \to \mathcal{X}'$ entre curvas não-singulares, a fórmula de Riemann-Hurwitz estabelece uma relação precisa entre os gêneros g e g' de $\mathcal{X}$ e $\mathcal{X}'$, respectivamente.

Teorema 1.6.7 (Fórmula de Riemann-Hurwitz) *Seja $\phi : \mathcal{X} \to \mathcal{X}'$ um morfismo não-constante de grau d entre curvas não-singulares. Então*

$$2g' - 2 \geq d(2g-2) + \sum_{P \in \mathcal{X}} (e_\phi(P) - 1),$$

com igualdade se, e somente se, a característica p de $\bar{k}$ é nula ou se p não divide qualquer um dos $e_\phi(P)'s$.

Demonstração: Veja ([23], II.5.9, pag. 41) ou ([24], A.4.2.5, pag. 72).

□

Corolário 1.6.8 *Se $\phi : \mathcal{X} \to \mathcal{X}'$ é um morfismo birracional, então os gêneros de $\mathcal{X}$ e $\mathcal{X}'$ coincidem.*

Demonstração: Todo morfismo birracional é não-ramificado e tem grau 1. Agora basta aplicar a fórmula de Riemann-Hurwitz.

□

Se $\mathcal{X}$ é uma curva projetiva plana, então existe um polinômio homogêneo $F \in \bar{k}[X, Y, Z]$ tal que $I_{\mathcal{X}} = (F)$ (veja [10], 4.1.10, pag. 107). O *grau* $deg(\mathcal{X})$ de uma curva projetiva plana $\mathcal{X}$ é por definição o grau do polinômio F tal que $I_{\mathcal{X}} = (F)$.

Teorema 1.6.9 *Seja $\mathcal{X}$ uma curva plana não-singular de gênero g e grau d. Então*

$$g = \frac{(d-1)(d-2)}{2}.$$

Demonstração: Este resultado segue da existência de uma diferencial $\omega \in \Omega^1[\mathcal{X}]$ cujo grau do seu divisor é $deg(\omega) = d(d-3)$. Então o item (b) do corolário (1.6.6) implica $d(d-3) = 2g-2$, de onde o resultado segue. Para verificar a existência de uma tal diferencial veja a demonstração de ([24], A.4.2.6, pag. 72).

□

Capítulo 2

Séries Lineares e Invariantes Hermitianos

Neste capítulo iremos estabelecer uma correspondência entre famílias de divisores efetivos sobre uma curva projetiva e morfismos não degenerados.

2.1 Séries Lineares e Morfismos

Seja $\mathcal{X}$ uma curva projetiva e não-singular. Para cada divisor E sobre $\mathcal{X}$ está associado o espaço de Riemann-Roch

$$\mathcal{L}(E) = \{f \in \bar{k}(\mathcal{X}) \ ; \ E + div(f) \geq 0\} \cup \{0\},$$

cuja dimensão é finita e é denotada por $l(E)$. O conjunto de todos os divisores efetivos e equivalentes a E admite uma estrutura de espaço projetivo e pode ser parametrizado por

$$\mathbb{P}(\mathcal{L}(E)) \simeq \mathbb{P}^{l(E)-1}.$$

Esta parametrização é dada via a aplicação

$$\mathbb{P}(\mathcal{L}(E)) \longrightarrow \{D \geq 0 \ ; \ D \sim E\}, \quad f \ mod \ \bar{k}^* \longmapsto E + div(f).$$

A próxima definição irá generalizar esta construção.

Definição 2.1.1 *Uma **série linear** $\mathcal{D}$ sobre $\mathcal{X}$ é o conjunto de todos os divisores efetivos, linearmente equivalentes a um divisor fixo E e parametrizado por um sub-espaço projetivo de $\mathbb{P}(\mathcal{L}(E))$. A série linear $\mathcal{D}$ é **definida** sobre k se todos os divisores em $\mathcal{D}$ são definidos sobre k.*

Note que uma série linear é um conjunto da forma

$$\mathcal{D} = \{E + div(f) \ ; \ f \in \mathcal{L}'(E)\backslash\{0\}\},$$

onde $\mathcal{L}'(E)$ é um $\bar{k}$-subespaço de $\mathcal{L}(E)$.

O conjunto de todos os divisores efetivos e equivalentes a E, denotado por $|E|$, é uma série linear chamada de *série linear completa*.

Uma série linear $\mathcal{D}$ depende apenas da classe de equivalência de E. De fato, se $D = E + div(h)$ para algum $h \in \bar{k}(\mathcal{X})$ então $\mathcal{L}'(E) = h\mathcal{L}'(D)$, logo

$$\begin{aligned} \{D + div(g) \ ; \ g \in \mathcal{L}'(D)\backslash\{0\}\} &= \{E + div(hg) \ ; \ g \in \mathcal{L}'(D)\backslash\{0\}\} \\ &= \{E + div(f) \ ; \ f \in \mathcal{L}'(E)\backslash\{0\}\}. \end{aligned}$$

Em particular, se $\mathcal{D}$ é completa, ou seja, se $\mathcal{D} = |E|$ então $|E| = |D|$. Divisores canônicos são sempre equivalentes, logo a série *canônica* sobre a curva $\mathcal{X}$ é definida como sendo a série linear completa $|K_{\mathcal{X}}|$, onde $K_{\mathcal{X}}$ é um divisor canônico sobre $\mathcal{X}$.

Definição 2.1.2 *Seja $\mathcal{D}$ uma série linear parametrizada por $\mathbb{P}(\mathcal{L}'(E))$. O **grau** de $\mathcal{D}$ é o grau do divisor E e a **dimensão** de $\mathcal{D}$ é sua dimensão como $\bar{k}$-espaço projetivo linear, ou seja, é a dimensão do subespaço $\mathbb{P}(\mathcal{L}'(E))$ de $\mathbb{P}(\mathcal{L}(E))$.*

A partir de agora estaremos sempre supondo que a dimensão de uma série linear $\mathcal{D}$ é n, ou seja, se $\mathcal{D}$ está parametrizada por $\mathbb{P}(\mathcal{L}'(E))$, então estaremos supondo que $\mathcal{L}'(E)$ é um $\bar{k}$-subespaço de $\mathcal{L}(E)$ cuja dimensão é $n + 1$.

Lema 2.1.3 *Seja $\mathcal{D}$ uma série linear parametrizada por $\mathbb{P}(\mathcal{L}'(E))$ e seja $P \in \mathcal{X}$, então*

$$v_P(E) = m_P - min\{v_P(f_0), \ldots, v_P(f_n)\},$$

onde $m_P := \min\{v_P(D) \ ; \ D \in \mathcal{D}\}$ e $\{f_0, \ldots, f_n\}$ é uma $\bar{k}$-base arbitrária de $\mathcal{L}'(E)$.

Demonstração: O número $min\{v_P(f_0), \ldots, v_P(f_n)\}$ não depende da $\bar{k}$-base de $\mathcal{L}'(E)$, portanto o mesmo ocorre com $m_P - min\{v_P(f_0), \ldots, v_P(f_n)\}$. Para cada i é claro que $v_P(E + div(f_i)) \geq m_P$, logo $v_P(E) \geq m_P - min\{v_P(f_0), \ldots, v_P(f_n)\}$. Por outro lado, existe $f \in \mathcal{L}'(E)$ tal que $m_P = v_P(E + div(f))$, ou seja, $v_P(E) = m_P - v_P(f)$. Se $f = \sum_i a_i f_i$ então $v_P(E) \leq m_P - min\{v_P(f_0), \ldots, v_P(f_n)\}$ e isto conclui a demonstração.

□

Definição 2.1.4 *Seja $\mathcal{D}$ uma série linear e seja $P \in \mathcal{X}$.*

(a) A ***multiplicidade*** *de $\mathcal{D}$ em P é definida por*

$$m_P := min\{v_P(D) \ ; \ D \in \mathcal{D}\}.$$

(b) Um ponto $P \in \mathcal{X}$ é um ***ponto base*** *de $\mathcal{D}$ se a multiplicidade m_P de $\mathcal{D}$ em P é não nula.*

Segue rapidamente da definição que

$$\{\text{pontos base de } \mathcal{D}\} = \bigcap_{D \in \mathcal{D}} supp(D).$$

Proposição 2.1.5 *Seja $\mathcal{D}$ uma série linear parametrizada por $\mathbb{P}(\mathcal{L}'(E))$. São equivalentes:*

(a) $v_P(E) = -min\{v_P(f_0), \ldots, v_P(f_n)\}$ para todo $P \in \mathcal{X}$.

(b) $m_P = 0$ para todo $P \in \mathcal{X}$.

(c) $\bigcap_{D \in \mathcal{D}} supp(D) = \emptyset$.

(d) Existe $f \in \mathcal{L}'(E) \backslash \{0\}$ tal que $v_P(E) + v_P(f) = 0$ para todo $P \in \mathcal{X}$.

Demonstração: Trivial a partir das definições e do lema (2.1.3).

□

Definição 2.1.6 *Uma série linear $\mathcal{D}$ é chamada* ***livre de pontos bases****, ou simplesmente* ***livre****, se as condições da proposição anterior são satisfeitas.*

Cada série linear está associada a uma série linear livre de pontos base. De fato, se $\mathcal{D}$ é uma série linear então o conjunto

$$\mathcal{D}^L := \{D - L \ ; \ D \in \mathcal{D}\},$$

onde $v_P(L) := m_P$ para todo $P \in \mathcal{X}$, define uma série linear livre sobre $\mathcal{X}$. Ainda mais, se a dimensão de $\mathcal{D}$ é n e o grau é d então a dimensão de $\mathcal{D}^L$ também é n e o grau é $d - deg(L)$. Note que se $\mathbb{P}(\mathcal{L}'(E))$ é uma parametrização de $\mathcal{D}$ então $\mathcal{D}^L \subseteq |E - L|$.

O que faremos agora é mostrar que séries lineares têm uma estreita ligação com uma certa classe de morfismos.

Definição 2.1.7 *Seja $\mathcal{D}$ uma série linear parametrizada por $\mathbb{P}(\mathcal{L}'(E))$ e sejam $f_0, \ldots, f_n$ funções racionais que formam uma $\bar{k}$-base para $\mathcal{L}'(E)$. A* ***aplicação racional associada*** *a $\mathcal{D}$, denotada por $\phi_{\mathcal{D}}$, é a aplicação*

$$\begin{aligned} \phi_{\mathcal{D}} \ : \ & \mathcal{X} \longrightarrow \mathbb{P}^n \\ & P \longmapsto (t^{e_P} f_0(P) : \ldots : t^{e_P} f_n(P)), \end{aligned}$$

onde t é um parâmetro local de P e

$$e_P := -min\{v_P(f_0), \ldots, v_P(f_n)\}.$$

A aplicação $\phi_{\mathcal{D}}$ é um morfismo, isto segue do teorema (1.3.3) uma vez que $\mathcal{X}$ é uma curva não-singular. Obviamente a aplicação $\phi_{\mathcal{D}}$ depende da escolha da base de $\mathcal{L}'(E)$, logo é bem definida a menos de uma transformação em $\mathbb{P}^n$. Note também que se $\mathcal{D}^L$ é a série linear, livre de pontos base, associada a $\mathcal{D}$, então $\phi_{\mathcal{D}} = \phi_{\mathcal{D}^L}$. Como antes, a notação

$$\phi_{\mathcal{D}} = (f_0 : \ldots : f_n)$$

será usada para identificar as funções racionais $f_0, \ldots, f_n$ que definem $\phi_{\mathcal{D}}$. Quando a série linear $\mathcal{D}$ é completa, digamos $\mathcal{D} = |E|$, o morfismo $\phi_{\mathcal{D}}$ é chamado *morfismo associado* ao divisor E. Note que estão construídos vários morfismos de $\mathcal{X}$ em diferentes espaços projetivos. De fato, basta considerar divisores variados sobre $\mathcal{X}$ e seus morfismos associados.

Definição 2.1.8 *Uma série linear $\mathcal{D}$ é **simples** se o morfismo $\phi_{\mathcal{D}} : \mathcal{X} \to \mathbb{P}^n$ for birracional.*

Agora suponha que um morfismo não-degenerado $\phi = (f_0 : \ldots : f_n) : \mathcal{X} \to \mathbb{P}^n$ é dado. A este morfismo associaremos uma série linear. Ainda mais, esta série será livre de pontos base.

Definição 2.1.9 *Seja $\phi = (f_0 : \ldots : f_n) : \mathcal{X} \to \mathbb{P}^n$ um morfismo não-degenerado. A **série linear associada** a ϕ, denotada por $\mathcal{D}_{(\phi)}$, é a série linear, livre de pontos base, definida por*

$$\mathcal{D}_{(\phi)} := \{E_{(\phi)} + div(f) \ ; \ f \in \mathcal{L}'(E_{(\phi)})\backslash\{0\}\},$$

onde $\mathcal{L}'(E_{(\phi)})$ é o espaço gerado pelas funções racionais $f_0, \ldots, f_n$ e $E_{(\phi)}$ é o divisor definido por

$$v_P(E_{(\phi)}) := -min\{v_P(f_0), \ldots, v_P(f_n)\}.$$

Note que o conjunto $\mathcal{L}'(E_{(\phi)})$ é um $\bar{k}$-subespaço de $\mathcal{L}(E_{(\phi)})$. Para ver que a série $\mathcal{D}_{(\phi)}$ é de fato livre, note que se $v_P(f_i) = min\{v_P(f_0), \ldots, v_P(f_n)\}$ então $v_P(E_{(\phi)}) + v_P(f_i) = 0$ (por definição de $E_{(\phi)}$), portanto a multiplicidade m_P de $\mathcal{D}_{(\phi)}$ é nula.

Agora podemos formular a correspondência entre morfismos e aplicações racionais.

Teorema 2.1.10 *Existe uma bijeção natural entre séries lineares livres de pontos base e de dimensão n e classes de equivalência projetiva de morfismos não-degenerados de $\mathcal{X}$ em $\mathbb{P}^n$.*

Demonstração: Suponha $\mathcal{D}$ parametrizada por $\mathbb{P}(\mathcal{L}'(E))$ e considere os seguintes conjuntos

$$\mathbf{L} := \{\mathcal{D} \ ; \ \mathcal{D} \text{ é série linear livre de dimensão } n \ \}$$

e

$$\mathbf{M} := \{< \phi > \ ; \ \phi : \mathcal{X} \to \mathbb{P}^n \text{ é não degenerado}\},$$

onde $< \phi >:= \{T \circ \phi \ ; \ T \in Aut(\mathbb{P}^n)\}$ denota a classe de equivalência projetiva de ϕ. Considere as aplicações

$$\Phi : \mathbf{L} \to \mathbf{M} \quad e \quad \Psi : \mathbf{M} \to \mathbf{L}$$

dadas por $\Phi(\mathcal{D}) :=< (f_0 : \ldots : f_n) >$ onde $f_0, \ldots, f_n$ é uma $\bar{k}$-base qualquer de $\mathcal{L}'(E)$ e $\Psi(< \phi >) := \mathcal{D}_{(\phi)}$. Segue rapidamente das definições que Φ e Ψ são aplicações bem definidas e inversas uma da outra.

□

2.2 Lacunas de Weierstrass e Invariantes Hermitianos

Nesta seção iremos estudar certas cadeias indexadas de sub-espaços de Riemann-Roch cujos índices irão fornecer algumas informações sobre a geometria da curva. O que ocorre na verdade é a tentativa de transformar um problema geométrico em uma problema de aritmética.

2.2.1 Lacunas de Weierstrass

A próxima proposição é uma das principais motivações para a nossa definição e é um aplicação direta do teorema de Riemann-Roch.

Proposição 2.2.1 *Sejam $P \in \mathcal{X}$, D um divisor e ℓ um inteiro não negativo. São equivalentes:*

(a) $\mathcal{L}(D + \ell P) = \mathcal{L}(D + (\ell - 1)P)$,

(b) $\mathcal{L}(K_{\mathcal{X}} - D - lP) \subsetneq \mathcal{L}(K_{\mathcal{X}} - D - (\ell - 1)P)$ para todo divisor canônico $K_{\mathcal{X}}$.

Se D é o divisor nulo então (a) e (b) também são equivalentes a

(c) Não existe $f \in \bar{k}(\mathcal{X})$ tal que $div(f)_\infty = \ell P$.

(d) Não existe $f \in \mathcal{L}(\ell P)$ tal que $v_P(f) = -\ell$.

Demonstração: $(a) \Leftrightarrow (b)$ É claro que $\mathcal{L}(K_{\mathcal{X}} - D - \ell P) \subseteq \mathcal{L}(K_{\mathcal{X}} - D - (\ell - 1)P)$. Agora basta observar que o teorema de Riemann-Roch implica que $l(K_{\mathcal{X}} - D - \ell P) = l(K_{\mathcal{X}} - D - (\ell - 1)P)$ se, e somente se, $l(D + \ell P) = l(D + (\ell - 1)P) + 1$. A partir disto, o resultado segue.

Agora suponha que D é nulo.

$(a) \Rightarrow (c)$ Se existe $f \in \bar{k}(\mathcal{X})$ tal que $div(f)_\infty = \ell P$ então $v_P(f) = -\ell$ e $v_Q(f) \geq 0$ sempre que $Q \neq P$, em particular $f \in \mathcal{L}(\ell P)$. Por outro lado, $v_P(f) = -\ell < -\ell + 1 = -v_P((\ell-1)P)$, logo $v_P((\ell-1)P) + v_P(f) < 0$ e portanto $f \notin \mathcal{L}((\ell-1)P)$, ou seja, $\mathcal{L}(\ell P) \subsetneq \mathcal{L}((\ell-1)P)$, o que é uma contradição.

$(c) \Rightarrow (d)$ Se $f \in \mathcal{L}(\ell P)$ então $v_Q(f) \geq 0$ para todo $Q \neq P$. Deste modo, se f satisfaz a condição $v_P(f) = -\ell$ então o ponto P é o único pólo de f, ou seja, $div(f)_\infty = \ell P$, o que contradiz a hipótese.

$(d) \Rightarrow (a)$ Se existe $f \in \mathcal{L}(\ell P)$ tal que $f \notin \mathcal{L}((\ell-1)P)$ então $-\ell \leq v_P(f) < -(\ell-1)$, ou seja, $v_P(f) = -\ell$, o que é uma contradição.

□

Definição 2.2.2 *Seja $P \in \mathcal{X}$ e seja D um divisor. Um inteiro não negativo ℓ é chamado* ***lacuna*** *de D em P se as condições (a) e (b) da proposição acima são satisfeitas. Se D é o divisor nulo então toda lacuna de D em P é chamada* ***lacuna de Weierstrass*** *em P.*

Proposição 2.2.3 *Seja $P \in \mathcal{X}$ e seja D um divisor. Se ℓ é uma lacuna de D em P então $\ell < 2g - deg(D)$, onde g é o gênero de $\mathcal{X}$. Em particular, não existem lacunas de Weierstrass iguais ou superiores a $2g$.*

Demonstração: Se $\ell \geq 2g - deg(D)$ então o item (c) do corolário (1.6.6) aplicado aos divisores $(\ell-1)P + D$ e $\ell P + D$ fornece $l((\ell-1)P + D) = \ell - g + deg(D)$ e $l(\ell P + D) = \ell - g + deg(D) + 1$, logo $l((\ell-1)P + D) < l(\ell P + D)$ e portanto $\mathcal{L}((\ell-1)P + D) \subsetneq \mathcal{L}(\ell P + D)$, ou seja, ℓ é uma não-lacuna de D em P, o que é um absurdo.

□

Teorema 2.2.4 (Lacunas de Weierstrass) *Seja $\mathcal{X}$ uma curva de gênero $g > 0$ e seja $P \in \mathcal{X}$. Então existem exatamente g lacunas de Weierstrass $\ell_1 < \ldots < \ell_g$ em P com*

$$\ell_1 = 1 \qquad e \qquad \ell_g \leq 2g - 1.$$

Demonstração: Considere a sequência

$$\mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \ldots \subseteq \mathcal{L}((2g-1)P),$$

onde 0 é o divisor nulo. Pela proposição (2.2.3) não existem lacunas de Weierstrass iguais ou superiores a $2g$. Agora note que $l(0) = 1$ e que o item (c) do corolário (1.6.6) e o item (e) do lema (1.6.3) implicam

$l((2g-1)P) = g$ e $l(iP)-l((i-1)P)) \leq 1$, respectivamente. A dimensão de cada espaço está variando de 1 até g, logo existem $g-1$ inclusões próprias na sequência acima e portanto existem $(2g-1)-(g-1) = g$ igualdades, ou seja, existem g números $\ell \in \{1, \ldots, 2g-1\}$ tais que $\mathcal{L}((\ell-1)P) = \mathcal{L}(\ell P)$. Portanto existem exatamente g lacunas. Finalmente, se 1 é uma não-lacuna de Weierstrass em P então existe $f \in \bar{k}(\mathcal{X})$ tal que $div(f)_\infty = P$ e assim $1 = deg(f)_\infty = [\bar{k}(\mathcal{X}) : \bar{k}(f)]$, ou seja, $\mathcal{X}$ e $\mathbb{P}^1$ são birracionais. Absurdo pois o gênero de $\mathbb{P}^1$ é nulo.

□

Dado um ponto $P \in \mathcal{X}$ considere o conjunto

$$H(P) := \{\eta \in \mathbb{N} \ ; \ \eta \text{ é uma não-lacuna de Weierstrass em } P\}.$$

Pela proposição (2.2.3), todo $\eta \in \mathbb{N}$ maior que $2g-1$ está em $H(P)$, logo $H(P)$ é não vazio. Se $\eta_1, \eta_2 \in H(P)$ então existem $f_1, f_2 \in \bar{k}(\mathcal{X})$ não nulos tais que $div(f_1)_\infty = \eta_1 P$ e $div(f_2)_\infty = \eta_2 P$. Disto segue que $div(f_1 f_2)_\infty = div(f_1)_\infty + div(f_2)_\infty = \eta_1 P + \eta_2 P = (\eta_1 + \eta_2)P$, assim $\eta_1 + \eta_2 \in H(P)$. Isto quer dizer que $H(P)$ é um subconjunto de $\mathbb{N}$ equipado com uma estrutura de semigrupo. A próxima definição irá formalizar esta observação.

Definição 2.2.5 *O conjunto $H(P)$ complementar ao conjunto formado pelas lacunas de Weierstrass em P é chamado de* ***semigrupo de Weierstrass*** *em P.*

Uma vez que $H(P)$ é um conjunto infinito de números naturais podemos enumerar e ordenar seus elementos. A notação

$$(\eta_i(P))_{i \in \mathbb{N}_0},$$

onde $\mathbb{N}_0 = \{0, 1, 2 \ldots\}$, será usada para designar a sequência crescente das não-lacunas de Weierstrass em P. Note que o item (e) do lema (1.6.3) e a proposição (2.2.3) implicam, respectivamente, que

$$l(\eta_i(P)P) = i+1 \ \text{ para todo } i \quad \text{e} \quad \eta_i(P) = g+i \ \text{ sempre que } \quad i \geq g.$$

2.2.2 Invariantes Hermitianos

Seja $\mathcal{D}$ uma série linear parametrizada por $\mathbb{P}(\mathcal{L}'(E))$ e fixe $P \in \mathcal{X}$. Considere o conjunto

$$\mathcal{D}_i(P) := \{D \in \mathcal{D} \ ; \ D \geq iP\},$$

onde i é um inteiro positivo. Equivalentemente,

$$\mathcal{D}_i(P) = \{E + div(f) \in \mathcal{D} \ ; \ f \in \mathcal{L}'(E) \cap \mathcal{L}(E - iP)\},$$

Em particular, $\mathcal{D}_i(P)$ é uma série linear sobre $\mathcal{X}$ e, neste caso, sua parametrização é $\mathbb{P}(\mathcal{L}'(E) \cap \mathcal{L}(E - iP))$.

Se d é o grau da série linear $\mathcal{D}$, então $\mathcal{D}_i(P) = \emptyset$ para cada $i > d$ ((d), lema (1.6.3)). Outra observação que pode ser verificada rapidamente é que $\mathcal{D}_j(P) \supseteq \mathcal{D}_{j+1}(P)$ para todo j.

Proposição 2.2.6 *Seja $\mathcal{D}$ uma série linear sobre $\mathcal{X}$ parametrizada por $\mathbb{P}(\mathcal{L}'(E))$ e seja $P \in \mathcal{X}$. São equivalentes:*

(a) $\mathcal{D}_j(P) \supsetneq \mathcal{D}_{j+1}(P)$.

(b) $\mathcal{L}'(E) \cap \mathcal{L}(E - jP) \supsetneq \mathcal{L}'(E) \cap \mathcal{L}(E - (j+1)P)$.

(c) Existe $f \in \mathcal{L}'(E)$ tal que $v_P(E) + v_P(f) = j$.

Demonstração: Basta observar que a inclusão própria $\mathcal{D}_j(P) \supsetneq \mathcal{D}_{j+1}(P)$ equivale a existência de um elemento não nulo $f \in \mathcal{L}'(E)$ tal que $v_P(E) + v_P(f) \geq j$ e $v_P(E) + v_P(f) < (j+1)$, ou seja, $f \in \mathcal{L}'(E) \cap \mathcal{L}(E - jP)$ e $f \notin \mathcal{L}'(E) \cap \mathcal{L}(E - (j+1)P)$. Por outro lado esta mesma desigualdade equivale a $j \leq v_P(E) + v_P(f) < j + 1$, ou seja, $v_P(E) + v_P(f) = j$.

□

Note que um inteiro j satisfazendo as condições desta proposição não depende da parametrização de $\mathcal{D}$.

Definição 2.2.7 *Seja $\mathcal{D}$ uma série linear e seja $P \in \mathcal{X}$. Um inteiro não negativo j é chamado **invariante P-hermitiano** de $\mathcal{D}$ se as condições da proposição acima são satisfeitas. Também costuma-se dizer que j é uma **ordem** de $\mathcal{D}$ em P.*

O próximo exemplo estabelece uma primeira conexão entre ordens de uma série linear em um ponto dado e não-lacunas de Weierstrass.

Exemplo 2.2.8 *Seja $P \in \mathcal{X}$ e seja $(\eta_i)_{i \in \mathbb{N}_0}$ a sequência das não lacunas de Weierstrass em P. Para cada $n \in \mathbb{N}_0$ considere a série linear completa $\mathcal{D} := |\eta_n P|$. Então*

(i) $\mathcal{D}$ é uma série linear de dimensão n, grau η_n e livre de pontos base.

(ii) Os números

$$\eta_n - \eta_i \quad \text{onde} \quad i = 0, \ldots, n$$

são ordens de $\mathcal{D}$ em P. [1]

[1] Mais tarde veremos que estas são de fato todas as possíveis ordens de $\mathcal{D}$ em P (prop. 2.2.10).

De fato, é claro que η_n é o grau de $\mathcal{D}$. Para ver que n é a dimensão de $\mathcal{D}$ basta observar que $\mathcal{L}(\eta_i(P)\backslash\mathcal{L}(\eta_{i-1}P)$ tem co-dimensão 1 e que $l(0) = 1$ onde 0 denota o divisor nulo, agora indução conclui o argumento. Uma vez que η_n é uma não-lacuna em P, existe $f \in \mathcal{L}(\eta_n P)$ tal que $v_P(f) = -\eta_n$, ou seja, $v_P(\eta_n P) + v_P(f) = 0$ e portanto P não é um ponto base. Por outro lado o divisor $D := \eta_n P + div(1)$ pertence a $\mathcal{D}$ e $v_Q(D) = 0$ sempre que $Q \neq P$, ou seja, Q também não é um ponto base, logo $\mathcal{D}$ não admite pontos bases e portanto é livre. Isto demonstra (i). Para ver (ii) escolha $f_i \in \bar{k}(\mathcal{X})$ tal que $div(f_i)_\infty = \eta_i P$, ou seja, $div(f_i) = div(f_i)_0 - \eta_i P$. Disto segue rapidamente que

$$\eta_n P + div(f_i) = (\eta_n - \eta_i)P + div(f_i)_0,$$

logo

$$v_P(\eta_n P) + v_P(f_i) = \eta_n - \eta_i.$$

Agora o resultado segue da proposição (2.2.6).

Lema 2.2.9 *Seja $\mathcal{D}$ uma série linear sobre $\mathcal{X}$. Então para cada ponto $P \in \mathcal{X}$,*

$$dim(\mathcal{D}_i(P)) \leq dim(\mathcal{D}_{i+1}(P)) + 1.$$

Demonstração: Basta observar que o quociente $\mathcal{L}'(E) \cap \mathcal{L}(E - iP)/\mathcal{L}'(E) \cap \mathcal{L}(E - (i+1)P)$ é isomorfo a um subespaço de $\mathcal{L}(E - iP)/\mathcal{L}(E - (i+1)P)$ cuja dimensão é menor ou igual a 1 (lema 1.6.3).

□

Proposição 2.2.10 *Seja $\mathcal{D}$ uma série linear parametrizada por $\mathbb{P}(\mathcal{L}'(E))$ e seja $P \in \mathcal{X}$. Se a dimensão de $\mathcal{D}$ é n então existem exatamente $n+1$ ordens $j_0, \ldots, j_n$ de $\mathcal{D}$ em P, cada uma das quais cumprem a condição*

$$j_i = min\{v_P(E) + v_P(f) \ ; \ f \in \mathcal{L}'(E) \cap \mathcal{L}(E - j_i P)\}.$$

Demonstração: Por comodidade denote $\mathcal{D}_j = \mathcal{D}_j(P)$ e $\mathcal{L}'_i = \mathcal{L}'(E) \cap \mathcal{L}(E - iP)$. Se d é o grau de $\mathcal{D}$ então é claro que $\mathcal{D}_j = \emptyset$ sempre que $j > d$. Logo considere a cadeia de espaços lineares associados

$$\mathcal{L}' = \mathcal{L}'_0 \supseteq \mathcal{L}'_1 \supseteq \ldots \supseteq \mathcal{L}'_d.$$

Pelo lema, $dim(\mathcal{L}'_j(P)) - dim(\mathcal{L}'_{j+1}) \leq 1$. Como $dim(\mathcal{L}'_0) = n+1$, existem exatamente $n+1$ inclusões próprias na cadeia acima, ou seja, $n+1$ inteiros $j \in \{0, \ldots, d\}$ tais que $\mathcal{D}_j \supsetneq \mathcal{D}_{j+1}$, portanto existem $n+1$ ordens de $\mathcal{D}$ em P. Se j_i é uma destas ordens então existe $f \in \mathcal{L}'_i \backslash \mathcal{L}'_{i+1}$, logo $j+1 > v_P(E) + v_P(f) \geq j_i$ e portanto $v_P(E) + v_P(f) = j_i$. A minimalidade é trivial.

□

Note que, por construção, as ordens $j_0, \ldots, j_n$ de uma série linear em algum ponto de $\mathcal{X}$ são inteiros não negativos que foram indexados de tal maneira que satisfazem $j_0 < \ldots < j_n$. Em alguns momentos a notação $j_i(P)$ será usada para indicar a i-ésima ordem de $\mathcal{D}$ em P.

Corolário 2.2.11 *Um ponto $P \in \mathcal{X}$ não é um ponto base de $\mathcal{D}$ se, e somente se, $j_0(P) = 0$. Em particular, $\mathcal{D}$ é livre de pontos base se, e somente se, $j_0(P) = 0$ para todo $P \in \mathcal{X}$.*

Demonstração: Basta observar que P não é um ponto base se, e somente se, existe $D \in \mathcal{D}$ tal que $v_P(D) = 0$. Se $\mathcal{D}$ está parametrizada por $\mathbb{P}(\mathcal{L}'(E))$ isto equivale a dizer que existe $f \in \mathcal{L}'(E)$ tal que $v_P(E) + v_P(f) = 0$. Isto conclui a demonstração.

□

Corolário 2.2.12 *Seja $\mathcal{D}$ uma série linear completa com grau $d \geq 2g$. Se $j_0, \ldots, j_n$ são as ordens de $\mathcal{D}$ em um ponto $P \in \mathcal{X}$, então $j_i = i$ sempre que $0 \leq i \leq d - 2g$. Em particular, $\mathcal{D}$ é livre de pontos base.*

Demonstração: Suponha $\mathcal{D} = |E|$ e seja $P \in \mathcal{X}$. Se $0 \leq i \leq d - 2g$ então $deg(E - iP) = d - i \geq 2g$ e $deg(E - (i+1)P) = d - (i+1) \geq 2g - 1$, logo o item (c) do corolário (1.6.6) implica $l(E - iP) > l(E - (i+1)P)$, ou seja, $\mathcal{L}(E - (i+1)P) \subsetneq \mathcal{L}(E - iP)$. Agora o resultado segue da proposição (2.2.6). O corolário anterior implica que $\mathcal{D}$ é livre.

□

Pela proposição (2.2.10) é sempre possível escolher $h_i \in \mathcal{L}'(E)$ tal que $j_i = v_P(E) + v_p(h_i)$. Note que as funções $h_0, \ldots, h_n$ formam uma $\bar{k}$-base de $\mathcal{L}'(E)$. De fato, se existe uma relação não trivial $\sum_i a_i h_i = 0$, então existem $i \neq l$ com $v_P(h_i) = v_p(h_l)$, logo $j_i = j_l$, o que é uma contradição.

Definição 2.2.13 *Sejam $j_0, \ldots, j_n$ as ordens de $\mathcal{D}$ em $P \in \mathcal{X}$. A $\bar{k}$-base $\{h_0, \ldots, h_n\}$, onde os $h_i's$ satisfazem $v_P(E) + v_P(h_i) = j_i$, é chamada de $\bar{k}$-base P-**hermitiana** de $\mathcal{L}'(E)$.*

Proposição 2.2.14 *Seja $P \in \mathcal{X}$ e seja $K_{\mathcal{X}}$ um divisor canônico.*

(a) Se D é um divisor de $\mathcal{X}$ então um inteiro positivo ℓ é uma lacuna de D em P se, e somente se, $\ell - 1$ é uma ordem de $|K_{\mathcal{X}} - D|$ em P.

(b) ℓ é uma lacuna de Weierstrass em P se, e somente se, $\ell - 1$ é uma ordem de $|K_{\mathcal{X}}|$ em P.

(c) Se $g > 0$ é o gênero de $\mathcal{X}$ então existem exatamente g ordens $j_0, \ldots, j_{g-1}$ de $|K_{\mathcal{X}}|$ em P com

$$j_0 = 0 \qquad e \qquad j_{g-1} < 2g - 1.$$

Em particular, a série linear canônica $|K_{\mathcal{X}}|$ é livre de pontos base.

Demonstração: O item (a) é uma consequência imediata das proposições (2.2.1) e (2.2.6). Para obter (b) basta tomar D em (a) como sendo o divisor nulo. Finalmente obtemos (c) como uma consequência de (b), de (a) e do teorema das lacunas de Weierstrass.

□

Exemplo 2.2.15 *Seja $\mathcal{X}$ uma curva de gênero $g = 1$. O divisor canônico $K_{\mathcal{X}}$ tem grau $deg(K_{\mathcal{X}}) = 0$ e dimensão $l(K_{\mathcal{X}}) = 1$, logo o divisor nulo é equivalente a $K_{\mathcal{X}}$. Em outras palavras, o divisor nulo é canônico. Em particular, o semigrupo de Weierstrass em cada ponto $P \in \mathcal{X}$ é*

$$H(P) = \{0, 2, 3, \ldots\}.$$

2.3 Diferenciais de Hasse e o Hiperplano Osculador

Muitas informações sobre uma curva plana podem ser obtidas analisando a intersecção entre a curva e a sua reta tangente em algum ponto não-singular dado. Em geral, para curvas não-degeneradas imersas em espaços de dimensões superiores, também são considerados os *espaços osculadores* sobre algum ponto não-singular. Estes espaços podem ser vistos como uma generalização de retas tangentes para curvas planas. Para estabelecê-los precisamos introduzir os *diferenciais de Hasse*, que são nada mais que operadores diferenciais, mas que são extremamente interessantes em característica positiva.

2.3.1 Diferenciais de Hasse

Nesta seção serão definidos os diferenciais de Hasse. Para cobrir os detalhes das afirmações que serão enunciadas consulte ([10], pag.28). Consulte também ([27], pag,17) e ([14], pag.12).

Seja x um elemento de separação de $\bar{k}(\mathcal{X})/\bar{k}$. Dados inteiros não negativos $i, j \in \mathbb{N}_0$ defina

$$D_x^i x^j := \binom{j}{i} x^{j-i}.$$

Esta aplicação pode ser estendida linearmente sobre $\bar{k}[x]$, sobre $\bar{k}(x)$ e sobre cada extensão finita e separável de $\bar{k}(x)$. As aplicações D_x^i também podem ser estendidas ao conjunto $\bar{k}((x))$ de todas as séries de potências com coeficientes em $\bar{k}$ da seguinte maneira:

$$D_x^i\Big(\sum_{s=m}^{\infty} a_s x^s\Big) := \sum_{s=m}^{\infty} \binom{s}{i} a_s x^{s-i}.$$

Definição 2.3.1 *Seja x um elemento de separação de $\bar{k}(\mathcal{X})/\bar{k}$. O operador $\bar{k}$-linear D_x^i é chamado i-**ésimo diferencial de Hasse** com relação a x.*

Note que

$$D_x^1 = \frac{d}{dx} \quad \text{e} \quad D_x^i x^i = 1.$$

O i-ésimo diferencial de Hasse D_x^i satisfaz as seguintes condições:

(h1) $D_x^0 = Id$;

(h2) $D^i_{x|\bar{k}} = 0$ para $i \geq 1$;

(h3) $D_x^i(fg) = \sum_{j=0}^{i} D_x^j f D_x^{i-j} g$;

(h4) $D_x^i \circ D_x^j = \binom{i+j}{i} D_x^{i+j}$;

O item (h3) é conhecido como a *regra do produto*.

Lema 2.3.2 *Seja x um elemento de separação de $\bar{k}(\mathcal{X})/\bar{k}$.*

(a) Se a característica p de k é zero ou se $i < p$, então

$$D_x^i = \frac{1}{i!}\frac{d^i}{dx^i}.$$

(b) Se y é outro elemento de separação, então para cada i existem $i-1$ funções racionais $d_1, \ldots, d_{i-1} \in \bar{k}(\mathcal{X})$, que são expressões polinomiais em $D_x^j(y)$ onde $1 \leq j \leq i$, tais que

$$D_x^i(f) = \left(\frac{dy}{dx}\right)^i D_y^i(f) + \sum_{j=1}^{i-1} d_j D_y^j(f)$$

para cada $f \in \bar{k}(\mathcal{X})$. Em particular, se $f \in \bar{k}(\mathcal{X})^p$ então

$$D_x^p(f) = \left(\frac{dy}{dx}\right)^p D_y^p(f).$$

Demonstração: Veja ([10], pag. 29-30).

□

Aplicando D_x^i na igualdade $f \cdot f^{-1} = 1$ não é difícil verificar que

$$\sum_{j=0}^{i} D_x^j(f^{-1}) D_x^{i-j} f = 0.$$

Se $i = 1$ então

$$D_x^1(f^{-1}) = -f^{-2} D_x^1 f.$$

Suponha que a característica p de $\bar{k}$ é positiva. É bem conhecido e fácil de provar que se $a = \sum_{i=0}^{s} a_i p^i$ e $b = \sum_{i=0}^{s} b_i p^i$ são as expansões p-ádicas dos inteiros positivos a e b, respectivamente, então

$$\binom{a}{b} \equiv \binom{a_0}{b_0} \ldots \binom{a_s}{b_s} \ (mod\ p).$$

Em particular, $\binom{a}{b} \not\equiv 0 \ (mod\ p)$ se, e somente se, a é p-adicamente maior ou igual a b, ou seja, cada coeficiente da expansão p-ádica de a é maior ou igual ao coeficiente correspondente a expansão p-ádica de b.

Proposição 2.3.3 *Sejam a, b, l, s inteiros onde $0 < a, b < p$ e q uma potência de p. Se x é um elemento de separação de $\bar{k}(\mathcal{X})/\bar{k}$ então*

(a) $D_x^{ap^l+bp^s} = D_x^{ap^l} \circ D_x^{bp^s}$;

(b) $D_x^{ap^l} = (D_x^{p^l})^a/a!$

(c) $D_x^i f^q = (D_x^{j/q})^q$ se $i = jq$ e $D_x^i f^q = 0$ se $i \not\equiv 0 \ (mod\ q)$.

(d) Existe $g \in \bar{k}(\mathcal{X})$ tal que $f = g^q$ se, e somente se, $D_x^i(f) = 0$ para todo $i = 1, \ldots, q-1$.

Demonstração: Os itens (a) e (b) são triviais a partir de (h4) e da propriedade binomial acima. Para os itens (c) e (d) veja ([27], pag. 18-19). O item (c) ainda pode ser encontrado em ([10], pag.39).

□

Em característica positiva os itens (a) e (b) da proposição acima implicam que os diferenciais de Hasse $D_x^{i\prime}s$ são determinados pelos operadores

$$D_x^1, D_x^p, D_x^{p^2}, \ldots$$

Proposição 2.3.4 *Seja $\mathcal{X}$ uma curva definida sobre k e seja $P \in \mathcal{X}$ com parâmetro local $t \in k(\mathcal{X})$. Se g é um elemento de $k(\mathcal{X})$ satisfazendo $v_P(g) = n$, então g pode ser escrito na forma*

$$g = a_n t^n + v_n t^{n+1},$$

onde $a_n \in k^*$ e $v_n \in \mathcal{O}_P(\mathcal{X}) \cap k(\mathcal{X})$. Mais ainda,

$$D_t^i g = a_n \binom{n}{i} t^{n-i} + v_{ni} t^{n-i+1},$$

onde $v_{ni} \in \mathcal{O}_P(\mathcal{X}) \cap k(\mathcal{X})$.

Demonstração: Se $g = \sum_{s=m}^{\infty} a_s t^s$ é a expansão local de g em P, onde $a_m \in k^*$, então $m = n$, pois $v_P(g) = n$ (teo. (1.2.6)), logo

$$g = a_n t^n + \sum_{s=n+1}^{\infty} a_s t^s = a_n t^n + \Big(\sum_{s=1}^{\infty} a_{n+s} t^{s-1}\Big) t^{n+1}.$$

Agora basta definir

$$v_n := \sum_{s=1}^{\infty} a_{n+s} t^{s-1} \quad \text{e} \quad v_{ni} := \sum_{j=0} D_t^j v_n \binom{n+1}{i-j} t^j.$$

□

2.3.2 Espaços Osculadores

Seja $\mathcal{D}$ uma série linear, sobre $\mathcal{X}$, livre de pontos base e parametrizada por $\mathbb{P}(\mathcal{L}'(E))$. Sejam $f_0, \ldots, f_n$ funções racionais que definem uma base $\mathcal{L}'(E)$. Pelo lema (2.1.3) isto significa que

$$v_P(E) = -min\{v_P(f_0), \ldots, v_P(f_n)\} \ \ \forall \ \ P \in \mathcal{X}.$$

Seja

$$\phi_{\mathcal{D}} = (f_0 : \ldots : f_n) : \mathcal{X} \to \mathbb{P}^n$$

o morfismo associado a $\mathcal{D}$. Este morfismo é único a menos de uma transformação em $\mathbb{P}^n$ e induz uma aplicação no conjunto de todos os hiperplanos de $\mathbb{P}^n$ sobre o conjunto dos divisores efetivos de $\mathcal{X}$. Isto é feito da seguinte maneira: se H é o hiperplano de $\mathbb{P}^n$ dado pela equação $\sum a_i X_i$, então defina

$$\phi^*_{\mathcal{D}}(H) := E + div(\sum_{i=0}^{n} a_i f_i).$$

A aplicação $\phi^*_{\mathcal{D}}$ é chamada de *pull-back* de $\phi_{\mathcal{D}}$ induzido sobre o conjunto dos hiperplanos de $\mathbb{P}^n$. Note que

$$\begin{aligned} \mathcal{D} &= \{E + div(f) \ ; \ f \in \mathcal{L}'(E)\backslash\{0\}\} \\ &= \{E + div(\sum_{i=0}^{n} a_i f_i) \ ; \ (a_0 : \ldots : a_n) \in \mathbb{P}^n\} \\ &= \{\phi^*_{\mathcal{D}}(H) \ ; \ H \text{ é hiperplano em } \mathbb{P}^n\}. \end{aligned}$$

Agora suponha que $g_0, \ldots, g_n$ são funções racionais que definem uma outra base de $\mathcal{L}'(E)$ e seja (c_{ij}) uma matriz em $GL_{n+1}(\bar{k})$ tal que $f_i = \sum_j c_{ij} g_j$. Então

$$\phi^*_{\mathcal{D}}(H) = E + div(\sum_i a_i f_i) = E + div(\sum_{ij} a_i c_{ij} g_i) = (T \circ \phi_{\mathcal{D}})^*(T(H)),$$

onde $T(H)$ é o hiperplano dado pela equação $\sum_i b_i Y_i = 0$, $(b_0, \ldots, b_n) = (a_0, \ldots, a_n)C^{-1}$ e $C = (c_{ij})$ é a matriz do operador T.

Se $\mathcal{F} = \{f_0, \ldots, f_n\}$ é uma base de $\mathcal{L}'(E)$ fixada, então o número $v_P(\phi^*_{\mathcal{D}}(H))$ é chamado de *multiplicidade* de H em P (em relação a base $\mathcal{F}$).

Proposição 2.3.5 *Seja $\mathcal{D}$ uma série linear livre de pontos base e seja $\phi_{\mathcal{D}} : \mathcal{X} \to \mathbb{P}^n$ o seu morfismo associado. Se H é um hiperplano em $\mathbb{P}^n$ e $P \in \mathcal{X}$, então $P \in supp(\phi^*_{\mathcal{D}}(H))$ se, e somente se, $\phi_{\mathcal{D}}(P) \in H$.*

Demonstração: Se H é definido pela equação $\sum a_i X_i = 0$, então

$$\begin{aligned} P \in supp(\phi^*_{\mathcal{D}}(H)) &\Leftrightarrow v_P(\phi^*_{\mathcal{D}}(H)) \geq 1 \quad \Leftrightarrow \quad v_P(\sum a_i t^{e_P} f_i) \geq 1 \\ &\Leftrightarrow \sum a_i t^{e_P} f_i(P) = 0 \ \Leftrightarrow \ (t^{e_P} f_0(P) : \ldots : t^{e_P} f_n(P)) \in H \\ &\Leftrightarrow \phi_{\mathcal{D}}(P) \in H. \end{aligned}$$

□

Ainda supondo que $\mathcal{D}$ é uma série linear, sobre $\mathcal{X}$, livre de pontos base, fixe um ponto P e sejam $j_0, \ldots, j_n$ as ordens de $\mathcal{D}$ em P. Para cada $i = 0, \ldots, n-1$ denote por $L_i^{\mathcal{F}}(P)$ a intersecção de todos os hiperplanos em $\mathbb{P}^n$ com multiplicidade em P (em relação a $\mathcal{F}$) maior ou igual a j_{i+1}, ou seja,

$$L_i^{\mathcal{F}}(P) := \bigcap \{H \ ; \ v_P(\phi_{\mathcal{D}}^*(H)) \geq j_{i+1}\}.$$

Definição 2.3.6 *O conjunto $L_i^{\mathcal{F}}(P)$ é chamado i-**ésimo espaço osculador** em P de $\mathcal{D}$ (em relação a base $\mathcal{F}$).*

Não é difícil verificar que

$$L_0^{\mathcal{F}}(P) \subseteq \ldots \subseteq L_{n-1}^{\mathcal{F}}(P).$$

Observe também que se $\mathcal{G}$ é obtida de $\mathcal{F}$ por uma transformação T com coeficientes em $\bar{k}$ então

$$L_i^{\mathcal{G}}(P) = T(L_i^{\mathcal{F}}(P)).$$

Isto significa que os espaços osculadores são unicamente determinados pela série linear $\mathcal{D}$, a menos de uma transformação projetiva com coeficientes em $\bar{k}$.

Se $\mathcal{D}$ é uma uma série linear com pontos base, o *i-ésimo espaço osculador* em P de $\mathcal{D}$ é por definição o i-ésimo espaço osculador em P da série linear livre associada $\mathcal{D}^L$.

Proposição 2.3.7 *Seja $\mathcal{D}$ uma série linear livre de pontos base parametrizada por $\mathbb{P}(\mathcal{L}'(E))$ e seja $P \in \mathcal{X}$ com parâmetro local t. Suponha que $\mathcal{F} = \{f_0, \ldots, f_n\}$ é uma $\bar{k}$-base para $\mathcal{L}'(E)$ e defina $g_l = t^{v_P(E)} f_l$. Suponha também que as i primeiras ordens $j_0, \ldots, j_{i-1}$ de $\mathcal{D}$ em P são conhecidas. Então j_i é o menor inteiro maior que j_{i-1} tal que os vetores*

$$(D_t^{j_s} g_0(P), \ldots, D_t^{j_s} g_n(P)) \quad com \quad s = 0, \ldots, i,$$

são linearmente independentes sobre $\bar{k}$. Em particular, a matriz $(D_t^{j_i} g_l(P))$ é não-singular.

Demonstração: Por uma transformação projetiva com coeficientes em $\bar{k}$, suponha que $\mathcal{F}$ é uma base P-hermitiana de $\mathcal{D}$, ou seja, se $g_l = t^{v_P(E)} f_l$ então $v_P(g_l) = j_l$ para todo l. Para cada $m \in \mathbb{N}^*$, a proposição (2.3.4) implica

$$D_t^m g_l = a_{lm} \binom{j_l}{m} t^{j_l - m} + v_{lm} t^{j_l - m + 1}, \tag{2.1}$$

onde $a_{lm} \in k^*$ e $v_{lm} \in \mathcal{O}_P(\mathcal{X})$. Pondo $m = j_i$ vemos rapidamente que

$$D_t^{j_i} g_l(P) = \begin{cases} 0 & \text{se } l > i \\ a_{lj_l} & \text{se } l = i \\ a_{lj_l} & \text{se } l < i, \end{cases}$$

logo $(D_t^{j_i} g_l(P))$ é uma matriz triangular com elementos não nulos na diagonal principal, portanto é não-singular. Seja r um inteiro tal que $j_{i-1} < r < j_i$. Pondo $m = r$ na equação (2.1) vemos que $D_t^r g_l(P) = 0$ sempre que $l \geq i$, ou seja, as $n-(i+1)$ últimas entradas do vetor $(D_t^r g_0(P), \ldots, D_t^r g_n(P))$ são nulas. Agora um argumento simples de álgebra linear mostra que este vetor é combinação linear dos vetores $(D_t^{j_s} g_0(P), \ldots, D_t^{j_s} g_n(P))$ com $s = 0, \ldots, i-1$. [2] Portanto j_i tem a minimalidade desejada.

□

Corolário 2.3.8 *Com as hipóteses da proposição, seja $m_0 < \ldots < m_r$ uma sequência de inteiros com $r \leq n$ tais que os vetores $(D_t^{m_s} g_0(P), \ldots, D_t^{m_s} g_n(P))$ são linearmente independentes para $s = 0, \ldots, r$. Então $j_i \leq m_i$ para todo $i \leq r$.*

Demonstração: Usando a minimalidade dos $j_i's$ não é difícil verificar que o espaço gerado pelos vetores $(D_x^s g_0(P), \ldots, D_x^s g_n)$ com $s = 0, \ldots, j_i - 1$ é i-dimensional para cada $i \leq r$. Se tivermos $m_i \geq j_i - 1$ existirão $i+1$ vetores linearmente independentes neste espaço, o que é um absurdo. Logo $j_i - 1 < m_i$ e portanto $j_i \leq m_i$.

□

Definição 2.3.9 *Seja $\mathcal{D}$ uma série linear livre de pontos base e seja $P \in \mathcal{X}$. Suponha que $\mathbb{P}(\mathcal{L}'(E))$ é uma parametrização de $\mathcal{D}$ e seja $\mathcal{F}$ uma base de $\mathcal{L}'(E)$.*

*(a) $L_1^{\mathcal{F}}(P)$ é chamado de **linha tangente** de P (em relação a base $\mathcal{F}$),*

*(b) $L_{n-1}^{\mathcal{F}}(P)$ é chamado **hiperplano osculador** de P (em relação a base $\mathcal{F}$).*

Lema 2.3.10 *Seja $\mathcal{D}$ uma série linear livre de pontos base e seja $P \in \mathcal{X}$. Suponha que $\mathbb{P}(\mathcal{L}'(E))$ é uma parametrização de $\mathcal{D}$ e seja $\mathcal{F}$ uma base P-hermitiana de $\mathcal{L}'(E)$. Então*

$$L_i^{\mathcal{F}}(P) = H_{i+1} \cap \ldots \cap H_n,$$

onde H_j é o hiperplano dado pela equação $X_j = 0$. Em particular, $L_i^{\mathcal{G}}(P)$ é i-dimensional para qualquer base $\mathcal{G}$ de $\mathcal{L}'(E)$.

Demonstração: Suponha $\mathcal{F} = \{f_0, \ldots, f_n\}$ e sejam $j_0, \ldots, j_n$ as ordens de $\mathcal{D}$ em P. Se H é o hiperplano em $\mathbb{P}^n$ dado pela equação $\sum a_i X_i = 0$ então $v_P(\phi_{\mathcal{D}}^*(H)) = v_P(E) + v_P(\sum a_i f_i) \geq v_P(E)$ $+min\{v_P(f_i)\ ;\ a_i \neq 0 \text{ e } 0 \leq i \leq n\}$, logo $v_P(\phi_{\mathcal{D}}^*(H)) \geq j_{i+1}$ se, e somente se, $a_1 = \ldots = a_i = 0$. Segue da definição de espaço osculador que $L_i^{\mathcal{F}}(P) = H_{i+1} \cap \ldots \cap H_n$ e assim $L_i^{\mathcal{F}}(P)$ é i-dimensional. Como $\mathcal{G}$ pode ser obtida de $\mathcal{F}$ por uma transformação com coeficientes em $\bar{k}$, existe $T \in Aut(\mathbb{P}^n)$ tal que $L_i^{\mathcal{G}}(P) = T(L_i^{\mathcal{F}}(P))$ e portanto $L_i^{\mathcal{G}}(P)$ é também i-dimensional, isto conclui a demonstração.

[2] Isto segue do fato que a matriz formada pelos vetores $(D_t^{j_s} g_0(P), \ldots, D_t^{j_s} g_n(P))$ com $s = 0, \ldots, n$ é triangular inferior.

□

Corolário 2.3.11 *Seja $\mathcal{D}$ uma série linear livre de pontos base e seja $P \in \mathcal{X}$. Suponha que $\mathbb{P}(\mathcal{L}'(E))$ é uma parametrização de $\mathcal{D}$ e seja $\mathcal{F}$ uma base de $\mathcal{L}'(E)$. Se $g_l = t^{v_P(E)} f_l$ então os vetores $(D_t^{j_s} g_0(P) : \ldots : D_t^{j_s} g_n(P))$, com $s = 0, \ldots, i$, geram o i-ésimo espaço osculador $L_i^{\mathcal{F}}(P)$.*

Demonstração: Por uma transformação projetiva com coeficientes em $\bar{k}$ suponha que $\mathcal{F}$ é uma base P-hermitiana de $\mathcal{L}'(E)$. Como na demonstração da proposição (2.3.7), vemos que a matriz $(D_t^{j_i} g_l(P))$ é triangular inferior com elementos não nulos na diagonal principal, ou seja, as $n - i$ últimas entradas do vetor $(D_t^{j_i} g_0(P) : \ldots : D_t^{j_i} g_n(P))$ são nulas. Isto significa que este vetor pertence ao hiperplano $H_j : X_j = 0$ sempre que $j \geq i + 1$, ou seja, pertence a intersecção $H_{i+1} \cap \ldots \cap H_n$, que é justamente o hiperplano osculador $L_i^{\mathcal{F}}(P)$, pelo lema. Uma vez que cada um destes vetores são linearmente independentes sobre $\bar{k}$, o resultado segue.

□

Corolário 2.3.12 *Seja $\mathcal{D}$ uma série linear livre de pontos base parametrizada por $\mathbb{P}(\mathcal{L}'(E))$ e seja $P \in \mathcal{X}$. Se $j_0, \ldots, j_n$ são as ordens de $\mathcal{D}$ em P então o hiperplano osculador $L_{n-1}^{\mathcal{F}}(P)$ de P em relação a uma base $\mathcal{F} = \{f_0, \ldots, f_n\}$ de $\mathcal{L}'(E)$ é dado pela equação*

$$det \begin{pmatrix} X_0 & \ldots & X_n \\ D_t^{j_0} g_0(P) & \ldots & D_t^{j_0} g_n(P) \\ \vdots & \ddots & \vdots \\ D_t^{j_n - 1} g_0(P) & \ldots & D_t^{j_n - 1} g_n(P) \end{pmatrix} = 0$$

onde $g_l := t^{v_P(E)} f_l$.

Demonstração: Este resultado é trivial a partir do corolário anterior.

□

Capítulo 3

Teorema de Stöhr-Voloch

Uma parte clássica da teoria das curvas algébricas, chamada geometria enumerativa, é dedicada a contar o número de pontos de uma curva que satisfazem certas propriedades. Neste capítulo iremos introduzir o método desenvolvido por Stöhr e Voloch [26] para estudar este problema.

3.1 τ-ordens de $\mathcal{D}$

Seja $\mathcal{X}$ uma curva não-singular definida sobre o corpo k cuja característica é p (positiva ou não). Fixe, sobre $\mathcal{X}$, uma série linear $\mathcal{D}$ definida sobre k, uma parametrização $\mathbb{P}(\mathcal{L}'(E))$ de $\mathcal{D}$ e uma k-base $\mathcal{F} = \{f_0, \ldots, f_n\}$ para $\mathcal{L}'(E)$ (teo. 1.6.2). Seja $\tau : k(\mathcal{X}) \to k(\mathcal{X})$ uma k-inclusão. Pelo item (b) do teorema (1.3.6), τ induz um único morfismo sobre $\mathcal{X}$, definido sobre k, que continuaremos a denotar por τ, tal que se $f \in k(\mathcal{X})$ então $\tau(f)$ é a função racional $f \circ \tau : \mathcal{X} \to k$. Este morfismo induz uma aplicação sobre o conjunto dos divisores de $\mathcal{X}$ por

$$\begin{aligned} D \in Div(\mathcal{X}) &\longmapsto D^\tau := \tau(D) \\ Q \in supp(D) &\longmapsto \sum_{P \in \tau^{-1}(Q)} e_\tau(P)P. \end{aligned}$$

Considere os morfismos

$$\phi = (f_0 : \ldots : f_n) : \mathcal{X} \to \mathbb{P}^n \quad \text{e} \quad \phi^\tau = (\tau(f_0) : \ldots : \tau(f_n)) : \mathcal{X} \to \mathbb{P}^n.$$

Seja x um elemento de separação de $k(\mathcal{X})/k$ e seja D_x^i o i-ésimo diferencial de Hasse com respeito a x. Para cada inteiro positivo m, considere também o vetor

$$D_x^m \phi := (D_x^m f_0, \ldots, D_x^m f_n).$$

A notação

$$D_x^0 \phi^\tau := (\tau(f_0), \ldots, \tau(f_n)),$$

também será utilizada para distinguir o vetor $(\tau(f_0),\ldots,\tau(f_n))$ do morfismo $(\tau(f_0):\ldots:\tau(f_n))$.

Dado um ponto $P\in\mathcal{X}$, o corolário (2.3.12) fornece uma condição necessária e suficiente para que um ponto pertença ao hiperplano osculador de P. Isto sugere estudarmos os determinantes das matrizes

$$H^{\mathcal{F}}_{m,\tau,x}:=\begin{pmatrix}\tau(f_0) & \ldots & \tau(f_n)\\ D_x^{m_1}f_0 & \ldots & D_x^{m_1}f_n\\ \vdots & \ddots & \vdots\\ D_x^{m_n}f_0 & \ldots & D_x^{m_n}f_n\end{pmatrix}=\begin{pmatrix}D_x^0\phi^\tau\\ D_x^{m_1}\phi\\ \vdots\\ D_x^{m_n}\phi\end{pmatrix},$$

onde

$$\begin{aligned} m &\quad \text{representa a lista } (m_1,\ldots,m_n),\\ \mathcal{F} &\quad \text{representa a } k\text{-base } \{f_0,\ldots,f_n\} \text{ e}\\ x &\quad \text{é elemento de separação de } k(\mathcal{X})/k\ .\end{aligned}$$

A notação

$$W^{\mathcal{F}}_{m,\tau,x}:=det(H^{\mathcal{F}}_{m,\tau,x})$$

será usada para o determinante da matriz $H^{\mathcal{F}}_{m,\tau,x}$. Note que $W^{\mathcal{F}}_{m,\tau,x}$ define uma aplicação racional $\mathcal{X}\to k$ via $P\mapsto W^{\mathcal{F}}_{m,\tau,x}(P)$.

Estamos interessados em estudar sobre quais condições $W^{\mathcal{F}}_{m,\tau,x}\neq 0$ para finalmente poder saber sobre quais condições $W^{\mathcal{F}}_{m,\tau,x}(P)=0$. Para isto, considere a lista

$$\varepsilon:=(\varepsilon_1,\ldots,\varepsilon_n), \tag{3.1}$$

onde $\varepsilon_1,\ldots,\varepsilon_n$ são inteiros tais que $0\leq\varepsilon_1<\ldots<\varepsilon_n$ e cada ε_i é obtido, indutivamente, como sendo o menor inteiro onde os vetores

$$D_x^0\phi^\tau, D_x^{\varepsilon_1}\phi,\ldots,D_x^{\varepsilon_i}\phi$$

são linearmente independentes sobre $k(\mathcal{X})$.

Lema 3.1.1 *Para cada $i=2,\ldots,n$ os conjuntos*

$$\{D_x^0\phi^\tau, D_x^s\phi;\ 0\leq s\leq\varepsilon_i-1\}\quad e\quad \{D_x^0\phi^\tau, D_x^{\varepsilon_s}\phi\ ;\ 1\leq s\leq i-1\}$$

geram o mesmo espaço.

Demonstração: Denote por V e por U os espaços gerados pelos conjuntos na ordem respectiva em que aparecem no enunciado. A inclusão $U\subseteq V$ é trivial. Para mostrar a inclusão inversa é suficiente mostrar que cada gerador de V está em U. Seja r um inteiro positivo tal que $0\leq r<\varepsilon_i$. Se $r=\varepsilon_j$ para algum $j<i$ então $D_x^r\phi\in U$ e acabou. Se $r\neq\varepsilon_j$ para qualquer $j<i$, então a minimalidade dos $\varepsilon_i's$ garante que $D_x^r\phi$ é combinação linear dos vetores $D_x^0\phi^\tau, D_x^{\varepsilon_1}\phi,\ldots,D_x^{\varepsilon_{i-1}}\phi$, ou seja, $D_x^r\phi\in U$. Portanto $V\subseteq U$.

□

Os elementos $\varepsilon_1, \ldots, \varepsilon_n$ são os inteiros tais que $(\varepsilon_1, \ldots, \varepsilon_n)$ é o elemento mínimo, na ordem lexicográfica, do conjunto de todas as n-úplas de inteiros $m = (m_1, \ldots, m_n)$ tais que $0 \leq m_1 < \ldots < m_n$ e $H^{\mathcal{F}}_{m,\tau,x}$ é uma matriz não-singular. Mais precisamente:

Corolário 3.1.2 *Se $m_1, \ldots, m_n$ é uma sequência de inteiros não negativos tais que $m_1 < \ldots < m_n$ e $W^{\mathcal{F}}_{m,\tau,x} \neq 0$ então $\varepsilon_i \leq m_i$.*

Demonstração: Se existe $\varepsilon_i > m_i$ com $W^{\mathcal{F}}_{m,\tau,x} \neq 0$, então existem $i+1$ vetores linearmente independentes no espaço definido no lema anterior, o qual é obviamente i-dimensional, logo $\varepsilon_i \leq m_i$.

□

Proposição 3.1.3 *(a) Seja $\mathcal{G} = \{g_0, \ldots, g_n\}$ onde $g_i = \sum a_{ij} f_j$ com $(a_{ij}) \in GL_{n+1}(k)$ então*

$$W^{\mathcal{G}}_{\varepsilon,\tau,x} = det(a_{ij}) W^{\mathcal{F}}_{\varepsilon,\tau,x}.$$

(b) Se $h \in k(\mathcal{X})$ e $\mathcal{G} = \{hf_0, \ldots, hf_n\}$ então

$$W^{\mathcal{G}}_{\varepsilon,\tau,x} = \tau(h) h^n W^{\mathcal{F}}_{\varepsilon,\tau,x}.$$

(c) Se y é outro elemento de separação de $k(\mathcal{X})/k$ então

$$W^{\mathcal{F}}_{\varepsilon,\tau,x} = \Big(\frac{dy}{dx}\Big)^{\varepsilon_1 + \ldots + \varepsilon_n} W^{\mathcal{F}}_{\varepsilon,\tau,y}.$$

Demonstração: (a) Este resultado segue rapidamente da k-linearidade de τ e da $\bar{k}$-linearidade dos operadores de Hasse e não depende do fato que a lista $(\varepsilon_1, \ldots, \varepsilon_n)$ é mínima.

(b) Pela regra do produto para os diferenciais de Hasse

$$D^{(\varepsilon_i)}_x(hf_j) = \sum_{s=0}^{\varepsilon_i} D^s_x h D^{(\varepsilon_i - s)}_x f_j = h D^{(\varepsilon_i)}_x f_j + \sum_{s=1}^{\varepsilon_i} a_s D^{(\varepsilon_i - s)}_x f_j.$$

onde $a_s := D^s_x h$. Deste modo, a i-ésima linha da matriz $(D^{\varepsilon_i}_x(hf_j))_{n \times n-1}$, onde $1 \leq i \leq n$ e $0 \leq j \leq n$, é tal que

$$\begin{aligned} (D^{(\varepsilon_i)}_x(hf_0), \ldots, D^{(\varepsilon_i)}_x(hf_n)) &= (hD^{(\varepsilon_i)}_x f_0, \ldots, hD^{(\varepsilon_i)}_x f_n) \ + \\ &+ \ \sum_{s=1}^{\varepsilon_i} a_s (D^{(\varepsilon_i - s)}_x f_0, \ldots, D^{(\varepsilon_i - s)}_x f_n). \end{aligned}$$

Pelo lema (3.1.1) a segunda parcela da soma acima é combinação linear dos vetores $D_x^0\phi^\tau, D_x^{\varepsilon_1}\phi, \ldots, D_x^{\varepsilon_{i-1}}\phi$. Agora um simples argumento de álgebra linear mostra que os determinantes das matrizes

$$\begin{pmatrix} \tau(hf_0) & \ldots & \tau(hf_n) \\ D_x^{\varepsilon_1}hf_0 & \ldots & D_x^{\varepsilon_1}hf_n \\ \vdots & \ddots & \vdots \\ D_x^{\varepsilon_n}(hf_0) & \ldots & D_x^{\varepsilon_n}(hf_n) \end{pmatrix} \quad e \quad \begin{pmatrix} \tau(h)\tau(f_0) & \ldots & \tau(h)\tau(f_n) \\ hD_x^{\varepsilon_1}f_0 & \ldots & hD_x^{\varepsilon_1}f_n \\ \vdots & \ddots & \vdots \\ hD_x^{\varepsilon_n}f_0 & \ldots & hD_x^{\varepsilon_n}f_n \end{pmatrix}$$

coincidem, [1] ou seja, $W^{\mathcal{G}}_{\varepsilon,\tau,x} = \tau(h)h^n W^{\mathcal{F}}_{\varepsilon,\tau,x}$.

(c) A prova é essencialmente a mesma que a do item (b) usando a regra da cadeia para as derivadas de Hasse em vez da regra do produto. De fato, para cada i,

$$D_x^{(\varepsilon_i)}(f_j) = (\frac{dy}{dx})^{\varepsilon_i} D_y^{(\varepsilon_i)}(f_j) + \sum_{s=1}^{\varepsilon_i - 1} d_s D_y^s(f_j).$$

onde $d_s \in k(\mathcal{X})$ (lema 2.3.2). A partir disto o resultado segue como no item (b).

□

Note que esta proposição diz que os inteiros $\varepsilon_1, \ldots, \varepsilon_n$ não dependem de qualquer parametrização de $\mathcal{D}$ e de qualquer elemento de separação de $k(\mathcal{X})$. Isto justifica a próxima definição.

Definição 3.1.4 *Os inteiros $\varepsilon_1, \ldots, \varepsilon_n$ definidos em (3.1) unicamente determinados por $\mathcal{D}$ e por τ são chamados de τ-**ordens** de $\mathcal{D}$, ou simplesmente **ordens** de $\mathcal{D}$ quando $\tau = 1$.*

Corolário 3.1.5 *Se $\tau = 1$ e $\mathcal{D}$ é livre de pontos base então $\varepsilon_i \leq j_i(P)$ para todo $P \in \mathcal{X}$.*

Demonstração: Seja t um parâmetro local de P. Pela proposição anterior podemos supor que $\mathbb{P}(\mathcal{L}'(E))$ é uma parametrização de $\mathcal{D}$ tal que $v_P(E) = 0$. Seja $\mathcal{F} = \{f_0, \ldots, f_n\}$ uma base para $\mathcal{L}'(E)$ e seja $j = (j_1, \ldots, j_n)$ a lista das ordens de $\mathcal{D}$ em P. Note que $j_0 = 0$ e que $W^{\mathcal{F}}_{j,1,t} = (D_t^{j_i} f_l)_{0\leq i,l\leq n}$. Se existe $j_i > \varepsilon_i$ então $W^{\mathcal{F}}_{j,1,x} = 0$, pela minimalidade das ordens $\varepsilon_1, \ldots, \varepsilon_n$, logo $det(D_t^{j_i} f_l(P)) = 0$, o que é uma contradição com a proposição (2.3.7).

□

Sejam $\varepsilon_1, \ldots, \varepsilon_n$ as τ-ordens de $\mathcal{D}$. Dado um elemento de separação x da extensão $k(\mathcal{X})/k$ considere o divisor

$$R_x^{\mathcal{F}}(\mathcal{D}, \tau) := div(W^{\mathcal{F}}_{\varepsilon,\tau,x}) + (\varepsilon_1 + \ldots + \varepsilon_n)div(dx) + nE + E^\tau,$$

onde $div(W^{\mathcal{F}}_{\varepsilon,\tau,x})$ é o divisor principal de $W^{\mathcal{F}}_{\varepsilon,\tau,x}$.

[1] Para ver que os determinantes coincidem note que i-ésima linha da primeira matriz é obtida da i-ésima linha da segunda matriz mais uma combinação $k(\mathcal{X})$-linear das demais linhas.

Corolário 3.1.6 *O divisor $R_x^{\mathcal{F}}(\mathcal{D},\tau)$ depende somente de $\mathcal{D}$ e de τ.*

Demonstração: Seja y um outro elemento de separação de $k(\mathcal{X})/k$ e suponha que $\mathcal{G}=\{g_0,\ldots,g_n\}$ é uma base para $\mathcal{L}'(D)$, onde $\mathbb{P}(\mathcal{L}'(D))$ é outra parametrização de $\mathcal{D}$. Logo existem $h\in k(\mathcal{X})^*$ e $(a_{ij})\in GL_{n+1}(k)$ tais que $g_i=\sum_j a_{ij}hf_j$. Se $\varepsilon_1,\ldots,\varepsilon_n$ são as τ-ordens de $\mathcal{D}$ então a proposição (3.1.3) implica

$$W^{\mathcal{G}}_{\varepsilon,\tau,y}=\tau(h)h^n\Big(\frac{dx}{dy}\Big)^{\varepsilon_1+\ldots+\varepsilon_n}det(a_{ij})W^{\mathcal{F}}_{\varepsilon,\tau,x}.$$

Note que $D=E-div(h)$ e $D^\tau=E^\tau-div(\tau(h))$, logo

$$\begin{aligned}
R^{\mathcal{G}}_y(\mathcal{D},\tau) &= div(W^{\mathcal{G}}_{\varepsilon,\tau,y})+(\varepsilon_1+\ldots+\varepsilon_n)div(dy)+nD+D^\tau\\
&= div(\tau(h))+n\cdot div(h)+(\varepsilon_1+\ldots+\varepsilon_n)(div(dx)-div(dy))+div(W^{\mathcal{F}}_{\varepsilon,\tau,x})\\
&+ (\varepsilon_1+\ldots+\varepsilon_n)div(dy)+nE-n\cdot div(h)+E^\tau-div(\tau(h))\\
&= div(W^{\mathcal{F}}_{\varepsilon,\tau,x})+(\varepsilon_1+\ldots+\varepsilon_n)div(dx)+nE+E^\tau\\
&= R^{\mathcal{F}}_x(\mathcal{D},\tau).
\end{aligned}$$

Isto conclui a demonstração.

□

Definição 3.1.7 *O divisor $R(\mathcal{D},\tau):=R_x^{\mathcal{F}}(\mathcal{D},\tau)$, unicamente determinado por $\mathcal{D}$ e por τ, é chamado* ***divisor de Weierstrass*** *de $\mathcal{D}$* ***com respeito a*** *τ, ou simplesmente* ***divisor de Weierstrass*** *de $\mathcal{D}$, quando τ é a identidade.*

Decorre do corolário (3.1.6) que o divisor $R(\mathcal{D},\tau)$ é efetivo. De fato, dado um ponto $P\in\mathcal{X}$ é sempre possível encontrar uma parametrização $\mathbb{P}(\mathcal{L}'(E))$ de $\mathcal{D}$ tal que $v_P(E)=0=v_P(E^\tau)$, logo $v_P(R(\mathcal{D},\tau))=v_P(W^{\mathcal{G}}_{\varepsilon,\tau,t})$, onde t é um parâmetro local de P. Por uma troca de variáveis podemos supor que os elementos de $\mathcal{G}$ são regulares em P, disto a afirmação segue.

No caso particular em que $\tau=1$ o divisor $R(\mathcal{D}):=R(\mathcal{D},1)$ também é conhecido como o divisor de *ramificação* de $\mathcal{D}$ e claramente depende somente de $\mathcal{D}$. Se o grau da série $\mathcal{D}$ é d, então

$$deg(R(\mathcal{D},\tau))=(\varepsilon_1+\ldots+\varepsilon_n)(2g-2)+(deg(\tau)+n)d,$$

onde $deg(\tau):=[k(\mathcal{X}):\tau k(\mathcal{X})]$.

Definição 3.1.8 *Os pontos do suporte de $R(\mathcal{D},\tau)$ são chamados $\mathcal{D}$-****pontos de Weierstrass com respeito*** *a τ, ou simplesmente $\mathcal{D}$-****pontos de Weierstrass*** *quando $\tau=1$. Quando $\mathcal{D}$ é uma série canônica os pontos do suporte de $R(\mathcal{D})$ são chamados* ***pontos de Weierstrass****.*

Exemplo 3.1.9 *Suponha $\tau = 1$, seja x um elemento de separação de $k(\mathcal{X})$ sobre k e considere o morfismo $\phi_x = (1 : x) : \mathcal{X} \to \mathbb{P}^1$ definido no exemplo (1.3.5). Seja $\mathcal{D}_{(\phi_x)}$ a série linear associada a ϕ_x. Se $\mathcal{D}_{(\phi_x)}$ está parametrizada por $\mathbb{P}(\mathcal{L}'(E))$ então*

$$v_P(E) = -min\{v_P(1), v_P(x)\},$$

portanto E é o divisor de pólos de x, ou seja, $E = div(x)_\infty$. Agora observe que

$$det \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} = 1,$$

logo 1 é a ordem de $\mathcal{D}_{(\phi_x)}$, portanto $\varepsilon = (1)$. Em particular, $div(W^{\mathcal{F}}_{\varepsilon,1,x}) = 0$, portanto

$$R(\mathcal{D}_{(\phi_x)}) = div(dx) + 2div(x)_\infty.$$

O divisor $R(\mathcal{D}_{(\phi_x)})$ definido acima, também denotado por R_x, é chamado *divisor de ramificação de x*.

Exemplo 3.1.10 *Seja x como no exemplo anterior e seja $\tau : k(\mathcal{X}) \to k(\mathcal{X})$ uma k-inclusão. Se ε_1 é a τ-ordem de $\mathcal{D}_{(\phi_x)}$, então ε_1 é o menor inteiro não negativo tal que*

$$det \begin{pmatrix} 1 & \tau(x) \\ D_t^{\varepsilon_1} 1 & D_t^{\varepsilon_1} x \end{pmatrix} \neq 0.$$

Deste modo, $\varepsilon_1 > 0$ se, e somente se,

$$det \begin{pmatrix} 1 & \tau(x) \\ 1 & x \end{pmatrix} = x - \tau(x) = 0;$$

ou seja, x é uma função racional fixa por τ.

Exemplo 3.1.11 *Suponha $\tau = 1$ e sejam x e y dois elementos linearmente independentes sobre $k(\mathcal{X})$, onde x é um elemento de separação de $k(\mathcal{X})$ sobre k. Considere o morfismo $\phi = (1 : x : y) : \mathcal{X} \to \mathbb{P}^2$ e seja $\mathcal{D}_{(\phi)}$ sua série linear associada. Iremos calcular a lista $\varepsilon = (\varepsilon_1, \varepsilon_2)$ das ordens de $\mathcal{D}_{(\phi)}$. Note que para cada inteiro positivo s,*

$$det \begin{pmatrix} 1 & x & y \\ 0 & 1 & D_x y \\ 0 & 0 & D_x^s y \end{pmatrix} = D_x^s y,$$

logo $\varepsilon_1 = 1$. Se $m = \{1, s\}$, então $W^{\mathcal{F}}_{m,1,x} = 0$ se, e somente se, $D_x^s y = 0$ o que ocorre sempre que $\varepsilon_1 < s < \varepsilon_2$ (pela minimalidade das ordens). Note que em característica positiva pode ser que $D_x^2 y = 0$, mas se $D_x^2 y \neq 0$ então é claro que $\varepsilon_2 = 2$. Se este for o caso então

$$R(\mathcal{D}) = div(W^{\mathcal{F}}_{\varepsilon,1,x}) + 3div(dx) + 3E,$$

onde E é o divisor definido por $v_P(E) = -min\{v_P(1), v_P(x), v_P(y)\}$.

3.2 O Teorema de Stöhr-Voloch

Nesta seção enunciaremos e demonstraremos uma versão do teorema de Stöhr-Voloch [26]. Para isto passaremos a analisar valores quantitativos do divisor $R(\mathcal{D}, \tau)$ definido na seção precedente. A partir de agora estaremos assumindo que a série linear $\mathcal{D}$ é livre de pontos base.

A próxima definição é um abuso de linguagem, mas irá facilitar na identificação de certos pontos.

Definição 3.2.1 *Um ponto $P \in \mathcal{X}$ é **fixo** (resp. **ramificado**) por τ se é um ponto fixo (resp. ramificado) do morfismo induzido em $\mathcal{X}$ por τ.*

Estamos usando a mesma notação τ para o morfismo induzido, logo, se P é um ponto fixo por τ e se t é um parâmetro local de P em $k(\mathcal{X})$, então

$$v_P(\tau(t)) = e_\tau(P).$$

Se P é também ramificado por τ então $e_\tau(P) > 1$.

Exemplo 3.2.2 *Se k é um corpo finito com q elementos, então todo ponto k-racional de $\mathcal{X}$ é fixo e ramificado pela q-ésima aplicação de Frobenius $x \mapsto x^q$. De fato, o morfismo induzido por esta aplicação é*

$$(x_0 : \ldots : x_n) \longmapsto (x_0^q : \ldots : x_n^q).$$

Este morfismo é ramificado em todos os pontos e seu grau é q (apêndice B).

Teorema 3.2.3 *Seja $P \in \mathcal{X}$ um ponto k-racional fixo por τ com um parâmetro local $t \in k(\mathcal{X})$. Suponha que $\mathcal{D}$ é uma série linear livre de pontos base com uma parametrização $\mathbb{P}(\mathcal{L}'(E))$ tal que o ponto P não pertence ao suporte de E. Sejam $m_1, \ldots, m_n$ inteiros tais que $0 \leq m_1 < \ldots < m_n$. Se $\mathcal{F}$ é uma k-base para $\mathcal{L}'(E)$, então*

$$v_P(W^{\mathcal{F}}_{m,\tau,x}) \geq \sum_{s=1}^{n} (j_s - m_s),$$

onde $j_0, \ldots, j_n$ são as ordens de $\mathcal{D}$ em P. Mais ainda, se $m_1 > 0$ ou se P é ramificado por τ, então vale a igualdade se, e somente se,

$$det(\binom{j_l}{m_i}) \not\equiv 0 \ (mod\ p) \qquad 1 \leq l, i \leq n.$$

Demonstração: A demonstração é dividida em três casos, a saber, o caso em que $m_1 > 0$, o caso em que $m_1 = 0$ e P é ramificado por τ e finalmente o caso em que $m_1 = 0$ e P é um ponto k-racional arbitrário (i.e., não necessariamente ramificado por τ). Neste último devemos apenas mostrar que a desigualdade é válida. Suponha $\mathcal{F} = \{f_0 \ldots, f_n\}$ e seja $\mathcal{G} = \{g_0, \ldots, g_n\}$ uma base P-hermitiana de

$\mathcal{L}'(E)$ tal que $g_0 = 1$, logo $v_P(g_l) = j_l$ e $v_P(g_0) = 0$, pois $v_P(E) = 0$. Uma vez que P é k-racional, existe $(c_{li}) \in GL_{n+1}(k)$ tal que $g_l = \sum_j c_{lj} f_j$, logo

$$\tau(g_l) = \sum_j c_{lj}\tau(f_j),$$

portanto

$$W^{\mathcal{G}}_{m,\tau,x} = det(c_{lj}) W^{\mathcal{F}}_{m,\tau,x}.$$

Se t é um parâmetro local de P em $k(\mathcal{X})$, então para todos $0 \leq l, i \leq n$,

$$g_l = a_{lj_l} t^{j_l} + v_l t^{j_l+1} \quad \text{e} \quad D_t^{m_i} g_l = \Big(a_{lj_l}\binom{j_l}{m_i} + t v_{li}\Big) t^{j_l - m_i},$$

onde $a_{lj_l} \in k^*$ e $v_l, v_{li} \in \mathcal{O}_P(\mathcal{X}) \cap k(\mathcal{X})$ (prop. (2.3.4)).

Se $m_1 > 0$ então a primeira coluna da matriz $H^{\mathcal{G}}_{m,\tau,t}$ é $(1, 0, \ldots, 0)$. A expansão do determinante ao longo desta coluna fornece

$$W^{\mathcal{G}}_{m,\tau,t} = det(D_t^{m_i} g_l) \qquad 1 \leq i, l \leq n,$$

logo

$$W^{\mathcal{F}}_{m,\tau,t} \;=\; a \cdot c \cdot det\Big(\binom{j_l}{m_i}_{n\times n} + tV\Big) t^u, \tag{3.2}$$

onde $a = \prod_l a_{lj_l}$, $c = det(c_{li})^{-1}$, $V = (a^{-1}_{lj_l} v_{li})_{n\times n}$ e $u = \sum_{i=1}^n j_i - m_i$. Agora o teorema pode ser concluído analisando esta expressão.

Se $m_1 = 0$ então a primeira coluna da matriz $H^{\mathcal{G}}_{m,\tau,x}$ é $(1, 1, 0, \ldots, 0)$. Repassando a segunda linha por ela mesma menos a primeira, obtemos

$$W^{\mathcal{G}}_{m,\tau,t} \;=\; det\begin{pmatrix} g_1 - \tau(g_1) & \ldots & g_n - \tau(g_n) \\ D_t^{m_2} g_1 & \ldots & D_t^{m_2} g_n \\ \vdots & \ddots & \vdots \\ D_t^{m_n} g_1 & \ldots & D_t^{m_n} g_n \end{pmatrix}. \tag{3.3}$$

Como P é fixo por τ então $\tau(t) = t^r u$, onde $r := e_\tau(P)$ e $u \in \mathcal{O}_P(\mathcal{X})^* \cap k(\mathcal{X})$. Se P é também ramificado por τ então $r > 1$ e é possível encontrar $\beta_l \in \mathcal{O}_P(\mathcal{X}) \cap k(\mathcal{X})$ tal que

$$g_l - \tau(g_l) = a_{lj_l} t^{j_l} + \beta_l t^{j_l+1}.$$

A partir disto, da hipótese $m_1 = 0$ e de (3.3), uma equação como (3.2) pode ser obtida apenas redefinindo V, de onde o resultado segue. Se P não é ramicado por τ então $r = 1$ e é possível encontrar $\alpha_l, \beta_l \in \mathcal{O}_P(\mathcal{X}) \cap k(\mathcal{X})$ tais que

$$g_l - \tau(g_l) \;=\; \alpha_l t^{j_l} + \beta_l t^{j_l+1}.$$

Como no caso anterior, uma equação como (3.2) pode ser obtida redefinindo as matrizes $\binom{j_l}{m_i}_{n\times n}$ e V. Neste caso, é possível mostrar a desigualdade.

□

Corolário 3.2.4 *Seja $P \in \mathcal{X}$ um ponto k-racional fixo por τ e sejam $\varepsilon_1, \ldots, \varepsilon_n$ as τ-ordens de $\mathcal{D}$. Então*

$$v_P(R(\mathcal{D}, \tau)) \geq \sum_{s=1}^{n} (j_s - \varepsilon_s),$$

onde $j_0, \ldots, j_n$ são as ordens de $\mathcal{D}$ em P. Mais ainda, se $\varepsilon_1 > 0$ ou se P é ramificado por τ, então vale igualdade se, e somente se,

$$det(\binom{j_l}{\varepsilon_i}) \not\equiv 0 \ (mod\ p) \qquad 1 \leq l, i \leq n.$$

Demonstração: Suponha que $\mathcal{F} = \{f_0, \ldots, f_n\}$ é uma base P-hermitiana de $\mathcal{L}'(E)$. Seja t um parâmetro local de P em $k(\mathcal{X})$ e defina $\mathcal{G} = \{g_0, \ldots, g_n\}$, onde $g_l = t^{v_P(E)} f_l$. Note que $v_P(g_0) = 0$ e $v_P(g_l) = j_l$. A proposição (3.1.3) implica

$$W^{\mathcal{G}}_{\varepsilon,\tau,t} = \tau(t)^{v_P(E)} t^{n v_P(E)} W^{\mathcal{F}}_{\varepsilon,\tau,t},$$

ou seja,

$$W^{\mathcal{F}}_{\varepsilon,\tau,t} = \tau(t)^{-v_P(E)} t^{-n v_P(E)} W^{\mathcal{G}}_{\varepsilon,\tau,t}.$$

Como P é fixo por τ então $v_P(E^\tau) = v_P(\tau(t)) v_P(E)$. Desta igualdade e da equação acima não é difícil verificar que $v_P(R(\mathcal{D}, \tau)) = v_P(W^{\mathcal{G}}_{\varepsilon,\tau,t})$. Se D é o divisor equivalente a E tal que $\mathcal{G}$ é base para o espaço $\mathcal{L}'(D)$, onde $\mathbb{P}(\mathcal{L}'(D))$ é uma parametrização de $\mathcal{D}$, então $v_P(D) = 0$, pois $\mathcal{D}$ é livre de pontos base e os $g_i's$ são regulares em P, logo P não pertence ao suporte de D. Agora basta aplicar o teorema (3.2.3) para esta parametrização e para $m_i = \varepsilon_i$.

□

Corolário 3.2.5 *Suponha que $\tau = 1$ e sejam $\varepsilon_1, \ldots, \varepsilon_n$ as ordens da série linear livre $\mathcal{D}$. Então*

(a) $\varepsilon_1 > 0$

(b) Sejam $m_1, \ldots, m_n$ inteiros tais que $0 < m_1 < \ldots < m_n$. Se existe $P \in \mathcal{X}$ tal que as ordens $j_0, \ldots, j_n$ de $\mathcal{D}$ em P satisfazem

$$det(\binom{j_i}{m_s}) \not\equiv 0 \ (mod\ p) \qquad 1 \leq i, s \leq n,$$

então $\varepsilon_i \leq m_i$ para todo $i = 1, \ldots, n$.

(c) Seja $P \in \mathcal{X}$. Então $v_P(R(\mathcal{D})) = 0$ se, e somente se, $\varepsilon_i = j_i(P)$ para todo $i = 1, \ldots, n$.

(d) Se ε_n é menor que a característica p de k, então as ordens de $\mathcal{D}$ são $1, 2, \ldots, n$.

Demonstração: (a) Trivial.

(b) Suponha que $\mathbb{P}(\mathcal{L}'(E))$ é uma parametrização de $\mathcal{D}$ tal que $v_P(E) = 0$. O teorema (3.2.3) aplicado a uma base $\mathcal{F}$ de $\mathcal{L}'(E)$ junto com a hipótese feita sobre os inteiros $m_i's$, implica que $v_P(W^{\mathcal{F}}_{m,1,x}) = \sum_{s=1}^{n}(j_s - m_s) \neq \infty$, logo $W^{\mathcal{F}}_{m,1,x} \neq 0$ e portanto $\varepsilon_i \leq m_i$, pelo corolário (3.1.2).

(c) Este resultado é uma aplicação do corolário (3.2.4). Se $v_P(R(\mathcal{D})) = 0$ então $\sum_i(j_i - \varepsilon_i) = 0$, portanto $j_i = \varepsilon_i$, pois $\varepsilon_i \leq j_i$. Reciprocamente, se $j_i = \varepsilon_i$ então $det(\binom{j_l}{\varepsilon_i}) \not\equiv 0 \ (mod\ p)$, portanto $v_P(R(\mathcal{D})) = \sum_{s=1}^{n}(j_s - \varepsilon_s) = 0$.

(d) Seja $\ell \in \{1, \ldots, n\}$ e seja r tal que $\varepsilon_r < \ell \leq \varepsilon_{r+1}$ (se $r = 0$ então defina $\varepsilon_0 = 0$). Defina

$$m_1 := \varepsilon_1,\ \ldots,\ m_r := \varepsilon_r,\ m_{r+1} := \ell,\ m_{r+2} := \varepsilon_{r+2},\ \ldots,\ m_n := \varepsilon_n.$$

Se P é um ponto fora do suporte de $R(\mathcal{D})$, então $v_P(R(\mathcal{D})) = 0$ e pelo item (c) vale $\varepsilon_i = j_i(P)$. A matriz $(\binom{\varepsilon_i}{m_s})$ é triangular com elementos diagonais $1, \ldots, 1, \binom{\varepsilon_{r+1}}{\ell}$. Considerando a hipótese feita sobre a característica p vemos que $\binom{\varepsilon_{r+1}}{\ell} \not\equiv 0 \ (mod\ p)$. Deste modo, o item (b) aplicado aos inteiros $m_1, \ldots, m_n$ e as ordens $j_0(P), \ldots, j_n(P)$, fornece $\varepsilon_{r+1} \leq m_{r+1} = \ell$, ou seja, $\varepsilon_{r+1} = \ell$, por definição de r. Portanto ℓ é uma ordem para $\mathcal{D}$.

□

Note que o item (c) do corolário anterior implica que os $\mathcal{D}$-pontos de Weierstrass são todos os pontos P tais que as ordens $j_1, \ldots, j_n$ de $\mathcal{D}$ em P diferem das ordens $\varepsilon_1, \ldots, \varepsilon_n$ de $\mathcal{D}$, ou seja, $(\varepsilon_1, \ldots, \varepsilon_n) < (j_1, \ldots, j_n)$ na ordem lexicográfica.

Agora iremos obter uma cota superior para o número de pontos de $\mathcal{X}$ que são fixos e também ramificados por τ. O próximo lema é a chave para a demonstração.

Lema 3.2.6 *Sejam $\varepsilon_1, \ldots, \varepsilon_n$ as τ-ordens da série linear livre $\mathcal{D}$ e suponha que $\varepsilon_1 = 0$. Se $P \in \mathcal{X}$ é um ponto k-racional fixo e ramificado por τ, então*

$$\varepsilon_i \leq j_i - j_1,$$

onde $j_1, \ldots, j_n$ são as ordens de $\mathcal{D}$ em P. Em particular,

$$v_P(R(\mathcal{D}, \tau)) \geq nj_1,$$

onde n é a dimensão da série $\mathcal{D}$.

Demonstração: Seja $\mathbb{P}(\mathcal{L}'(E))$ uma parametrização de $\mathcal{D}$ tal que $v_P(E) = 0$ e seja $\mathcal{F} = \{f_0, \ldots, f_n\}$ uma base para $\mathcal{L}'(E)$. Note que a sequência $0, j_2 - j_1, \ldots j_n - j_1$ são as ordens do morfismo $\mathbb{P}^1 \to \mathbb{P}^{n-1}$, dado por

$$(1 : x) \longmapsto (1 : x^{j_2 - j_1} : \ldots : x^{j_n - j_1}) = (x^{j_1} : \ldots : x^{j_n}),$$

no ponto $(1:0)$, onde $div(x) = (1:0) - (0:1)^2$. Se $\varepsilon' = (\varepsilon'_1, \ldots, \varepsilon'_{n-1})$ é a lista das ordens deste morfismo então $\varepsilon'_i \leq j_{i+1} - j_1$ (cor. 3.1.5). Defina $\varepsilon'_0 := 0$ e $\varepsilon'' := (\varepsilon'_0, \varepsilon'_1, \ldots, \varepsilon'_{n-1})$. Se $\mathcal{H} = \{x^{j_1}, \ldots, x^{j_n}\}$ então

$$0 \neq W^{\mathcal{H}}_{\varepsilon',1,x} = det(D_x^{\varepsilon'_i} x^{j_l}) = det(\binom{j_l}{\varepsilon'_i}) x^{j_1+\ldots+j_n-\varepsilon'_1-\ldots-\varepsilon'_n},$$

onde $1 \leq l \leq n$ e $0 \leq i \leq n-1$. Em particular, $det(\binom{j_l}{\varepsilon'_i}) \neq 0$. Uma vez que P é ramificado e fixo por τ, o teorema (3.2.3), aplicado para $m_i = \varepsilon'_{i-1}$, fornece $v_P(W^{\mathcal{F}}_{\varepsilon'',\tau,x}) = \sum_s j_s - \varepsilon_{s-1}$, logo $W^{\mathcal{F}}_{\varepsilon'',\tau,x} \neq 0$ e portanto $\varepsilon_i \leq \varepsilon'_{i-1} \leq j_i - j_1$. A segunda parte segue do corolário (3.2.4).

□

Teorema 3.2.7 (Stöhr-Voloch) *Seja $\mathcal{X}$ uma curva de gênero g definida sobre k e seja $\tau : k(\mathcal{X}) \to k(\mathcal{X})$ uma k-inclusão. Suponha que existe uma série linear $\mathcal{D}$, definida sobre k, livre de pontos base, dimensão n, grau d e com τ-ordens $\varepsilon_1, \ldots, \varepsilon_n$, onde $\varepsilon_1 = 0$. Então o número de pontos k-racionais de $\mathcal{X}$ que são fixos e ramificados por τ é no máximo*

$$\frac{1}{n}\Big[(\varepsilon_1 + \ldots + \varepsilon_n)(2g-2) + (n + deg(\tau))d\Big].$$

Demonstração: Pelo lema anterior, cada ponto k-racional $P \in \mathcal{X}$ que é fixo e ramificado por τ satisfaz $v_P(R(\mathcal{D}, \tau)) \geq n$. Deste modo, se Γ é o conjunto de tais pontos, então $\sum_{P\in\Gamma} v_P(R(\mathcal{D}, \tau)) \geq n\#\Gamma$, ou seja, $\#\Gamma \leq deg(R(\mathcal{D}, \tau))/n$, isto conclui a demonstração.

□

Veremos na próxima seção que este teorema é mais interessante quando $\mathcal{X}$ é definida sobre um corpo finito. Neste caso a k-inclusão será a de Frobenius. Para o próximo exemplo, suponha que $\tau = 1$.

Exemplo 3.2.8 *Seja $\mathcal{X}$ uma curva de gênero g e suponha que existe um elemento de separação $x \in \bar{k}(\mathcal{X})$ de grau 2 com um único pólo no ponto P_∞, ou seja, $div_\infty(x) = 2P_\infty$. Em particular,*

$$H(P_\infty) = \{0, 2, 4, \ldots, 2g, 2g+1, \ldots\} \quad e \quad G(P_\infty) = \{1, 3, \ldots, 2g-1\}.$$

Iremos contar o número de pontos de Weierstrass de $\mathcal{X}$. Para isto, considere a série linear

$$\mathcal{D} := |(g-1)div_\infty(x)|.$$

[2]De fato, primeiramente note que o divisor $(1:0)-(0:1)$ tem grau zero, uma vez que o gênero de $\mathbb{P}^1$ é zero, este divisor é principal, logo o elemento x existe. Defina $P_0 := (1:0)$ e $P_\infty := (0:1)$. Se $\mathcal{D}_\phi$ é a série linear livre associada a ϕ e parametrizada por $\mathbb{P}(\mathcal{L}'(E_\phi))$, então $\{x^{j_1}, \ldots, x^{j_n}\}$ é base para $\mathcal{L}'(E_\phi)$ e E_ϕ é definido por $v_P(E_\phi) = -min\{v_P(x^{j_i})\ ;\ 0 \leq 1 \leq n\}$, logo $E_\phi = j_n P_\infty - j_i P_0$ e portanto $v_{P_0}(E_\phi) + v_{P_0}(x^{j_i}) = j_i - j_1$. Agora a afirmação segue da proposição (2.2.6).

Esta é uma série linear livre de pontos base, grau $2g-2$ *e dimensão* $g-1$ *(ex. (2.2.8)), logo* $l((g-1)div_\infty(x)) = g$ *e portanto* $(g-1)div_\infty(x) = K_\mathcal{X}$*, ou seja,* $\mathcal{D} = |K_\mathcal{X}|$ *é canônica. Em particular, os elementos* $1, x, x^2, \ldots, x^{g-1}$ *formam uma base para o espaço* $\mathcal{L}((g-1)div_\infty(x))$*. Agora observe que*

$$D_x^i x^j = \begin{cases} 0 & se\ i > j \\ 1 & se\ i = j \\ \binom{j}{i} x^{j-i} & se\ i < j. \end{cases}$$

Se $\mathcal{F} = \{1, x, x^2, \ldots, x^{g-1}\}$ *e* $m = (1, \ldots, g-1)$*, então*

$$W^\mathcal{F}_{m,1,x} = det(D_x^i x^j)_{0\leq i,j,\leq g-1} = 1$$

e portanto $1, 2, \ldots, g-1$ *são as ordens de* $|K_\mathcal{X}|$*. Assim*

$$\begin{aligned} R(|K_\mathcal{X}|) &= \frac{g(g-1)}{2} div(x) + g(g-1)div_\infty(x) \\ &= \frac{g(g-1)}{2} R_x, \end{aligned}$$

onde $R_x = div(x) + 2div_\infty(x)$ *é o divisor de ramificação de* x *definido no exemplo (3.1.9). Note que* $deg(R_x) = 2g+2$ *e que os suportes de* R_x *e* $R(|K_\mathcal{X}|)$ *coincidem, ou seja, os pontos do suporte de* R_x *são os pontos de Weierstrass de* $\mathcal{X}$*. Pelo exemplo (3.1.9),* R_x *é o divisor de Weierstrass da série completa* $|div(x)_\infty|$ *cuja única ordem é* 1 *e cujo grau é* 2*, por hipótese. Sejam* $j_0(P)$ *e* $j_1(P)$ *as ordens desta série em um ponto de Weierstrass* P*. Então* $1 < j_1(P) \leq 2$ *e portanto* $j_0(P) = 0$ *e* $j_1(P) = 2$*. Note que* $det(\binom{2}{1}) = 2$*. Em particular, se a característica do corpo de definição de* $\mathcal{X}$ *é diferente de* 2*, então o corolário (3.2.4) aplicado a série* $|div_\infty(x)|$ *implica* $v_P(R_x) = 1$*, logo* $v_P(R(|K_\mathcal{X}|) = g(g-1)/2$*, portanto existem exatamente* $2g+2$ *pontos de Weierstrass em* $\mathcal{X}$*, cada um dos quais tem multiplicidade* $g(g-1)/2$ *em* $R(|K_\mathcal{X}|)$*.*

3.3 Ordens de Frobenius

Seja $\mathbb{F}_q$ um corpo finito com q elementos e característica positiva p. Suponha que $\mathcal{X}$ é uma curva definida sobre $\mathbb{F}_q$. Nesta seção iremos aplicar os resultados obtidos sobre a curva $\mathcal{X}$ considerando a aplicação de Frobenius $\mathrm{Fr} : \mathbb{F}_q(\mathcal{X}) \to \mathbb{F}_q(\mathcal{X})$ dada por $x \mapsto x^q$. Muitos dos resultados que iremos descrever são simples reformulações dos resultados da seção anterior.

Seja $\mathcal{D}$ uma série linear livre de pontos base, definida sobre $\mathbb{F}_q$, parametrizada por $\mathbb{P}(\mathcal{L}'(E))$ e com uma $\mathbb{F}_q$-base $\mathcal{F} = \{f_0, \ldots, f_n\}$ de $\mathcal{L}'(E)$ fixada. A aplicação de Frobenius define uma inclusão em

$\mathbb{F}_q(\mathcal{X})$ que é a identidade sobre $\mathbb{F}_q$, logo podemos considerar a matriz

$$H^{\mathcal{F}}_{\nu,\mathrm{Fr},x} = \begin{pmatrix} f_0^q & \dots & f_n^q \\ D_x^{\nu_0} f_0 & \dots & D_x^{\nu_0} f_n \\ \vdots & \ddots & \vdots \\ D_x^{\nu_{n-1}} f_0 & \dots & D_x^{\nu_{n-1}} f_n \end{pmatrix},$$

onde

$$\begin{aligned} \nu &\quad \text{representa a lista } \{\nu_0 < \ldots < \nu_{n-1}\}, \\ \phi &\quad \text{representa o morfismo } (f_0 : \ldots : f_n) \text{ e} \\ x &\quad \text{é um elemento de separação de } \mathbb{F}_q(\mathcal{X})/\mathbb{F}_q \ . \end{aligned}$$

Na seção anterior a notação $W^{\mathcal{F}}_{\nu,\mathrm{Fr},x}$ estava sendo usada para o determinante da matriz $H^{\mathcal{F}}_{\nu,\mathrm{Fr},x}$. Aqui usaremos a notação

$$V^{\mathcal{F}}_{\nu,x} := det(H^{\mathcal{F}}_{\nu,\mathrm{Fr},x}).$$

Definição 3.3.1 *As* Fr*-ordens $\nu_0, \ldots, \nu_{n-1}$ de $\mathcal{D}$ são chamadas de* ***ordens de Frobenius*** *de $\mathcal{D}$.*

Note que, em contraste com a seção anterior, indexamos as Fr-ordens $\nu_0, \ldots, \nu_{n-1}$ começando por 0. A igualdade $\nu_0 = 0$ justifica esta convenção. Na verdade, esta é a notação clássica original de [26].

Lema 3.3.2 *Sejam $\varepsilon_1 \ldots, \varepsilon_n$ as ordens de $\mathcal{D}$. Então existe um inteiro $I \geq 1$ tal que*

$$\nu_i = \begin{cases} \varepsilon_i & \text{se } 0 < i < I \\ \varepsilon_{i+1} & \text{se } I \leq i \leq n \end{cases}$$

Em particular, $\nu_i \leq j_{i+1}(P)$ para todo $P \in \mathcal{X}$.

Demonstração: Considere as matrizes

$$H^{\mathcal{F}}_{\varepsilon,1,x} = \begin{pmatrix} f_0 & \dots & f_n \\ D_x^{\varepsilon_1} f_0 & \dots & D_x^{\varepsilon_1} f_n \\ \vdots & \ddots & \vdots \\ D_x^{\varepsilon_n} f_0 & \dots & D_x^{\varepsilon_n} f_n \end{pmatrix} \quad \text{e} \quad H^{\mathcal{F}}_{\nu,\mathrm{Fr},x} = \begin{pmatrix} f_0^q & \dots & f_n^q \\ f_0 & \dots & f_n \\ D_x^{\nu_1} f_0 & \dots & D_x^{\nu_1} f_n \\ \vdots & \ddots & \vdots \\ D_x^{\nu_{n-1}} f_0 & \dots & D_x^{\nu_{n-1}} f_n \end{pmatrix}$$

Comparando as n últimas linhas de $H^{\mathcal{F}}_{\nu,\mathrm{Fr},x}$ com as n primeiras linhas de $H^{\mathcal{F}}_{\varepsilon,1,x}$ obtemos, pela minimalidade das ordens, que $\varepsilon_s \leq \nu_s$ para todo $s = 1, \ldots, n-1$. Seja I o menor inteiro tal que o vetor $(f_0^q, \ldots, f_n^q)$ é combinação linear dos vetores

$$D_x^{\nu_0}\phi, D_x^{\varepsilon_1}\phi, \ldots, D_x^{\varepsilon_I}\phi.$$

Note que $I \geq 1$ pois $\nu_0 = 0$ e por sua minimalidade vemos que os vetores

$$D_x^{\nu_0}\phi, D_x^{\varepsilon_1}\phi, \ldots, D_x^{\varepsilon_{I-1}}\phi \text{ e } (f_0^q, \ldots, f_n^q)$$

são linearmente independentes. Novamente pela minimalidade das ordens temos $\nu_s \leq \varepsilon_s$ para todo $s = 1, \ldots, I-1$ e portanto $\nu_s = \varepsilon_s$ para todo $s = 1, \ldots, I-1$. A igualdade $\nu_s = \varepsilon_{s+1}$ para $s = I, \ldots, n$ é obtida analogamente e portanto a demonstração será omitida. A desigualdade $\nu_i \leq j_{i+1}(P)$ é uma consequência do corolário (3.1.5).

□

Estamos sempre assumindo que a série linear $\mathcal{D}$ é livre de pontos base e está parametrizada por $\mathbb{P}(\mathcal{L}'(E))$, logo os divisores E e E^{Fr} satisfazem

$$v_P(E) = -min\{v_P(f_0), \ldots, v_P(f_n)\} \text{ e } v_P(E^{\mathrm{Fr}}) = -min\{v_P(f_0^q), \ldots, v_P(f_n^q)\}.$$

Em particular, $E^{\mathrm{Fr}} = qE$ e portanto o divisor de Weierstrass de $\mathcal{D}$ com respeito a Fr é dado por

$$R(\mathcal{D}, \mathrm{Fr}) = (V_{\nu,x}^{\mathcal{F}}) + (\nu_0 + \ldots + \nu_{n-1})(dx) + (q+n)E.$$

Note que este divisor depende somente de $\mathcal{D}$ e de q.

Definição 3.3.3 *O divisor*

$$S(\mathcal{D}, q) := R(\mathcal{D}, \mathrm{Fr}),$$

*unicamente determinado por $\mathcal{D}$ e por q, é chamado **divisor de Frobenius** de $\mathcal{D}$.*

Note que se d é o grau da série $\mathcal{D}$ então o grau de E^{Fr} é qd. Em particular,

$$deg(S(\mathcal{D}, q)) = (\nu_0 + \ldots + \nu_{n-1})(2g-2) + (q+n)d.$$

Seja t um parâmetro local de P e considere o conjunto $\mathcal{G} = \{g_0, \ldots, g_n\}$, onde $g_i := t^{v_P(E)} f_i$. A proposição (3.1.3) implica que

$$V_{\nu,t}^{\mathcal{G}} = t^{v_P(E)(q+n)} V_{\nu,t}^{\mathcal{F}},$$

ou seja,

$$V_{\nu,t}^{\mathcal{F}} = t^{-v_P(E)(q+n)} V_{\nu,t}^{\mathcal{G}}$$

e portanto $v_P(S(\mathcal{D}, q)) = v_P(V_{\nu,t}^{\mathcal{G}})$. Em particular, esta é uma nova prova de que o divisor $S(\mathcal{D}, q)$ é efetivo.

Proposição 3.3.4 *Se ν_{n-1} é menor que a característica p de $\mathbb{F}_q$, então as ordens de Frobenius de $\mathcal{D}$ são $0, 1, \ldots, n-1$.*

Demonstração: Por uma reparametrização podemos supor que $\mathcal{F} = \{1, f_1, \ldots, f_n\}$ é uma base para $\mathcal{L}'(E)$, logo a expansão do determinante da matriz $H^{\mathcal{F}}_{\nu,\mathrm{Fr},t}$ ao longo da primeira coluna fornece

$$V^{\mathcal{F}}_{\nu,t} = det \begin{pmatrix} f_1 - f_1^q & \ldots & f_n - f_n^q \\ D_t^{\nu_1} f_1 & \ldots & D_t^{\nu_1} f_n \\ \vdots & \ddots & \vdots \\ D_t^{\nu_{n-1}} f_1 & \ldots & D_t^{\nu_{n-1}} f_n \end{pmatrix}.$$

A hipótese feita sobre p e a proposição (2.3.3) implicam que $D_t^{\nu_i} f_j^q = 0$, logo os inteiros $\nu_1, \ldots, \nu_{n-1}$ são as ordens do morfismo

$$\phi = (f_1 - f_1^q : \ldots : f_n - f_n^q) : \mathcal{X} \longrightarrow \mathbb{P}^{n-1},$$

ou seja, são as ordens de sua série linear associada $\mathcal{D}_{(\phi)}$. Agora basta aplicar o item (d) do corolário (3.2.5) para esta série.

□

Proposição 3.3.5 *Seja $P \in \mathcal{X}$ um ponto $\mathbb{F}_q$-racional e sejam $j_0, \ldots, j_n$ as ordens de $\mathcal{D}$ em P. Então*

$$v_P(S(\mathcal{D}, q)) \geq \sum_{i=1}^{n} (j_i - \nu_{i-1}),$$

e vale a igualdade se, e somente se,

$$det(\binom{j_i}{\nu_s}) \not\equiv 0 \ (mod\ p),$$

onde $0 \leq s \leq n-1$ e $1 \leq i \leq n$.

Demonstração: Este é o corolário (3.2.4), observando que todo ponto $\mathbb{F}_q$-racional é fixo e ramificado por Fr.

□

Proposição 3.3.6 *Seja P um ponto arbitrário de $\mathcal{X}$ e sejam $j_0, \ldots, j_n$ as ordens de $\mathcal{D}$ em P. Então*

$$v_P(S(\mathcal{D}, q)) \geq \sum_{i=1}^{n-1} (j_i - \nu_i),$$

e vale a desigualdade estrita se

$$det(\binom{j_i}{\nu_s}) \equiv 0 \ (mod\ p) \qquad 0 \leq i, s \leq n-1.$$

Demonstração: Note que não estamos na situação do teorema (3.2.3). Seja $\mathcal{H} = \{h_0, \ldots, h_n\}$ uma base P-hermitiana de $\mathcal{L}'(E)$. Uma vez que P não é necessariamente um ponto $\mathbb{F}_q$-racional não podemos assumir que $\mathcal{H}$ é uma $\mathbb{F}_q$-base, mas podemos encontrar uma matriz $(a_{ij}) \in GL_{n+1}(\bar{\mathbb{F}}_q)$ tal que $h_i = \sum_j a_{ij} f_j$, logo $g'_i = \sum_j a_{ij} g_j$, onde $g'_i = t^{v_P(E)} h_i$ e $g_j = t^{v_P(E)} f_j$. Defina $h'_i = \sum_j a_{ij} g_j^q$. Observe que em geral não vale a igualdade $h'_i = g_i'^q$, contudo é claro que $v_P(h'_i) \geq 0$. Se $\mathcal{G} = \{g_0, \ldots, g_n\}$ então

$$\begin{aligned} V^{\mathcal{G}}_{\nu,t} \cdot det(a_{ij}) &= det \begin{pmatrix} h'_0 & \ldots & h'_n \\ D_t^{\nu_0} g'_0 & \ldots & D_t^{\nu_0} g'_n \\ \vdots & \ddots & \vdots \\ D_t^{\nu_{n-1}} g'_0 & \ldots & D_t^{\nu_{n-1}} g'_n \end{pmatrix} \\ &= \sum_{i=0}^{n} (-1)^i h'_i d_i, \end{aligned}$$

onde cada d_i é o i-ésimo determinante obtido pela regra de Crammer. Deste modo,

$$v_P(S(\mathcal{D}, q)) \geq min\{v_P(d_0), \ldots, v_P(d_n)\}.$$

Note que $d_s = det(D_t^{\nu_i} g'_j)$ onde $i = 0, \ldots, n-1$ e $j = 1, \ldots, \hat{s}, \ldots, n$. Uma vez que $v_P(g'_l) = j_l$, a proposição (2.3.4) implica que $D_t^{\nu_i} g'_l = \left(a_{lj_l} \binom{j_l}{\nu_i} + t v_{li}\right) t^{j_l - \nu_i}$, logo

$$v_P(d_s) \geq j_1 + \ldots + j_n - j_s - \nu_1 - \ldots - \nu_{n-1},$$

portanto $v_P(S(\mathcal{D}, q)) \geq \sum_{i=1}^{n-1} (j_i - \nu_i)$. Se $det(\binom{j_i}{\nu_s}) \equiv 0 \ (mod\ p)$, onde $0 \leq i, s \leq n-1$, então $v_P(d_n) > j_0 + \ldots + j_{n-1} - \nu_0 - \ldots - \nu_{n-1}$, portanto a desigualdade é estrita.

□

Lema 3.3.7 *Se P é um ponto $\mathbb{F}_q$-racional de $\mathcal{X}$ e $j_0, \ldots, j_n$ são as ordens de $\mathcal{D}$ em P, então, para todo i,*

$$\nu_i \leq j_{i+1} - j_1.$$

Em particular,

$$v_P(S(\mathcal{D}, q)) \geq n j_1.$$

Demonstração: Este é o lema (3.2.6), observando que todo ponto $\mathbb{F}_q$-racional é fixo e ramificado por Fr.

□

Corolário 3.3.8 *(a) Sejam $\varepsilon_1, \ldots, \varepsilon_n$ as ordens de $\mathcal{D}$. Se existe i tal que $\nu_i \neq \varepsilon_i$ então todo ponto $\mathbb{F}_q$-racional é um $\mathcal{D}$-ponto de Weierstrass.*

(b) Se existe i tal que $\nu_i \neq i$, então $j_n(P) > n$ para todo ponto $\mathbb{F}_q$-racional P.

Demonstração: (a) Basta mostrar que com as hipóteses acima, todo ponto $\mathbb{F}_q$-racional está no suporte do divisor de Weierstrass $R(\mathcal{D})$. De fato, suponha que existe um ponto $\mathbb{F}_q$-racional P fora do suporte de $R(\mathcal{D})$, então para todo i, a ordem ε_i de $\mathcal{D}$ coincide com a i-ésima ordem $j_i(P)$ de $\mathcal{D}$ em P (veja o comentário abaixo do corolário (3.2.5)). Pelo lema anterior isto significa que $\nu_i \leq \varepsilon_{i+1} - \varepsilon_1$, ou seja, $\nu_i < \varepsilon_{i+1}$ e portanto $\nu_i = \varepsilon_i$ (lema 3.3.2), o que contradiz a hipótese.

(b) Se existe um ponto $\mathbb{F}_q$-racional P tal que a $j_n(P) = n$, então $\nu_{n-1} \leq n - j_1(P)$, logo $\nu_{n-1} \leq n-1$ e portanto $\nu_i = i$, o que é um absurdo.

□

Agora enunciaremos o teorema de Stöhr-Voloch como originalmente foi feito em [26].

Teorema 3.3.9 (Stöhr-Voloch) *Seja $\mathcal{X}$ uma curva de gênero g definida sobre $\mathbb{F}_q$. Suponha que existe uma série linear $\mathcal{D}$, livre de pontos base, dimensão n, grau d e com ordens de Frobenius $\nu_0, \ldots, \nu_{n-1}$. Então*

$$\#\mathcal{X}(\mathbb{F}_q) \leq \frac{1}{n}\Big[(\nu_0 + \ldots + \nu_{n-1})(2g-2) + (q+n)d\Big].$$

Demonstração: A demonstração é essencialmente a mesma do teorema (3.2.7). Se $S(\mathcal{D}, q)$ é o divisor de Frobenius associado a série linear $\mathcal{D}$ então, pelo lema (3.3.7), $v_P(S(\mathcal{D}, q)) \geq n$ para todo $P \in \mathcal{X}(\mathbb{F}_q)$ e portanto $\sum_{P \in \mathcal{X}(\mathbb{F}_q)} v_P(S(\mathcal{D}, q)) \geq n\#\mathcal{X}(\mathbb{F}_q)$, ou seja, $\#\mathcal{X}(\mathbb{F}_q) \leq deg(S(\mathcal{D}, q))/n$, isto conclui a demonstração.

□

Exemplo 3.3.10 *Seja $\mathcal{X}$ uma curva definida sobre $\mathbb{F}_q$ de gênero 3 tal que $\#\mathcal{X}(\mathbb{F}_q) > 2q+8$. Considere a série linear canônica $|K_\mathcal{X}|$ e note que $l(K_\mathcal{X}) = 3$, $deg(K_\mathcal{X}) = 4$ e $dim(|K_\mathcal{X}|) = 2$. Sejam $\varepsilon_1, \varepsilon_2$ as ordens de $|K_\mathcal{X}|$, ν_0, ν_1 as ordens de Frobenius de $|K_\mathcal{X}|$ e $j_0(P), j_1(P), j_2(P)$ as ordens de $|K_\mathcal{X}|$ no ponto $P \in \mathcal{X}(\mathbb{F}_q)$. Note que se*

$$\varepsilon_2 = 2 \overset{\text{lema (3.3.2)}}{\Rightarrow} \nu_1 \leq 2,$$

logo o teorema (3.3.9) implica $\#\mathcal{X}(\mathbb{F}_q) \leq 2q+8$, o que é absurdo. Portanto $\varepsilon_2, \nu_1 > 2$, ou seja, $\nu_1, \varepsilon_2 \in \{3, 4\}$. Note também que

$$j_1(P) > 1 \overset{\text{lema (3.3.7)}}{\Rightarrow} j_2(P) > 4,$$

o que é absurdo, pois a ordem $j_2(P)$ de $|K_\mathcal{X}|$ em P não é superior ao grau de $|K_\mathcal{X}|$. Portanto $j_1(P) = 1$ e assim $\varepsilon_1 = 1$. Por outro lado, se P é um ponto de Weierstrass, então $\varepsilon_2 \neq j_2(P) \leq 4$, ou seja, $\varepsilon_2 = 3$ e $j_2(P) = 4$. Agora o lema (3.3.7) implica $\nu_1 = 3$ e o teorema (3.3.9) implica

$$\#\mathcal{X}(\mathbb{F}_q) \leq 28.$$

Suponha que a característica p de $\mathbb{F}_q$ é diferente de 2. Neste caso,

$$det \begin{pmatrix} \binom{1}{1} & \binom{1}{3} \\ \binom{4}{1} & \binom{4}{3} \end{pmatrix} = 4 \not\equiv 0 \ (mod\ p),$$

logo o corolário (3.2.4) implica que $v_P(R(|K_{\mathcal{X}}|) = (1-1)+(4-3) = 1$, ou seja, cada ponto de Weierstrass tem multiplicidade igual a 1 em $|K_{\mathcal{X}}|$, uma vez que $deg(R(|K_{\mathcal{X}}|) = 28$, existem exatamente 28 pontos de Weierstrass em $\mathcal{X}$.

Exemplo 3.3.11 *Seja $\mathcal{X}$ a curva definida pelo polinômio homogêneo*

$$f(X,Y,Z) = Y^3Z + YZ^3 - X^4 \in \mathbb{F}_{3^2}[X,Y,Z].$$

Esta é uma curva plana, não-singular, irredutível, de grau 4 e gênero 3. Note que $(0:1:0)$ é o único ponto no infinito de $\mathcal{X}$. Os pontos afins de $\mathcal{X}$ são os pontos $(a:b:1)$, com $(a,b) \in \bar{\mathbb{F}}_{3^2} \times \bar{\mathbb{F}}_{3^2}$, tais que

$$b^3 + b = a^4.$$

Note que se $a \in \mathbb{F}_{3^2}$ então $b \in \mathbb{F}_{3^2}$. Uma vez que a equação $Y^3 + Y = a^4$ define um polinômio irredutível e separável sobre $\mathbb{F}_{3^2}$, existem exatamente 3 soluções distintas para Y, cada uma das quais pertence a $\mathbb{F}_{3^2}$, logo $\#\mathcal{X}(\mathbb{F}_{3^2}) = 28$. Pelo exemplo anterior, os pontos de Weierstrass de $\mathcal{X}$ são os pontos $\mathbb{F}_{3^2}$-racionais.

Capítulo 4

O Teorema de Hasse-Weil

Neste capítulo continuaremos a estudar curvas algébricas definidas sobre corpos finitos. O teorema de Stöhr-Voloch (teo. (3.2.7)) será usado para obter uma nova cota superior para o número de pontos racionais destas curvas. Com argumentos da teoria de Galois, dual a demonstração feita por E. Bombieri em [4], esta cota superior será convertida em uma cota inferior. A partir disto, poderemos demonstrar o teorema de Hasse-Weil, que é equivalente a hipótese de Riemann para a teoria de curvas algébricas.

4.1 A Função Zeta sobre uma Curva

A clássica função *Zeta de Riemann* é a aplicação dada por

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s} = \prod_{p} \frac{1}{1-p^{-s}},$$

onde $s \in \mathbb{C}$ é tal que $Re(s) > 1$ e o produto a direita (identidade de Euler) percorre todos os números primos. A *Hipótese de Riemann*, até hoje não demonstrada, afirma que os zeros não triviais[1] de $\zeta(s)$ estão sobre a reta $Re(s) = 1/2$. É bem conhecido que a função $\zeta(s)$ tem um único pólo em $s = 1$ e admite uma extensão meromórfica para todo $\mathbb{C}$.

Nesta seção definiremos a função Zeta sobre uma curva e enunciaremos as suas principais propriedades. Para cobrir os detalhes omitidos nas afirmações sugerimos as referências ([25], cap. V), ([10], cap. 5), ([20], cap. 5) e [5].

Seja $\mathcal{X}$ uma curva definida sobre $\mathbb{F}_q$. A aplicação de Frobenius Fr é definida sobre os pontos de $\mathcal{X}$ por

$$(a_0 : \ldots : a_n) \mapsto (a_0^q : \ldots : a_n^q).$$

[1] Os chamados zeros triviais de $\zeta(s)$ são s=-2,-4,-6,...

Para cada $P \in \mathcal{X}$ seja $deg_{\mathbb{F}_q}(P)$ o menor inteiro positivo d tal que $\mathrm{Fr}^d(P) = P$. Se $D = \sum_{P\in\mathcal{X}} n_P P$ é um divisor sobre $\mathcal{X}$, então defina

$$deg_{\mathbb{F}_q}(D) := \sum_{P\in\mathcal{X}} n_P deg_{\mathbb{F}_q}(P).$$

Definição 4.1.1 *A **função Zeta** de $\mathcal{X}$ sobre $\mathbb{F}_q$ é a aplicação complexa*

$$\zeta_{\mathcal{X}/\mathbb{F}_q}(s) := \sum_{D\geq 0} \mathcal{N}(D)^{-s},$$

*onde $\mathcal{N}(D) := q^{deg_{\mathbb{F}_q}(D)}$ é a **norma absoluta** do divisor efetivo D em relação ao corpo base $\mathbb{F}_q$.*

Note que

$$\zeta_{\mathcal{X}/\mathbb{F}_q}(s) \;\; = \;\; \sum_{n=0}^{\infty} \#\{D \in Div(\mathcal{X}) \; ; \; D \geq 0 \text{ e } deg_{\mathbb{F}_q}(D) = n\} q^{-ns}.$$

Mediante a troca de variáveis $t = q^{-s}$ podemos escrever $\zeta_{\mathcal{X}/\mathbb{F}_q}(s) = Z_{\mathcal{X}/\mathbb{F}_q}(t)$, onde

$$Z_{\mathcal{X}/\mathbb{F}_q}(t) := \sum_{n=1}^{\infty} \#\{D \in Div(\mathcal{X}) \; ; \; D \geq 0 \text{ e } deg_{\mathbb{F}_q}(D) = n\} t^n.$$

Em particular, o coeficiente de t nesta série é justamente o número de pontos $\mathbb{F}_q$-racionais de $\mathcal{X}$. Um estudo detalhado desta função pode ser encontrado em ([25], cap.V).

Proposição 4.1.2 *Seja $\mathcal{X}$ uma curva de gênero g definida sobre $\mathbb{F}_q$. A série de potências $Z_{\mathcal{X}/\mathbb{F}_q}(t)$ converge sempre que $|t| < q^{-1}$. Nesta região,*

(a) a função $Z_{\mathcal{X}/\mathbb{F}_q}(t)$ satisfaz a equação funcional

$$Z_{\mathcal{X}/\mathbb{F}_q}(t) = q^{2g-1}t^{2g-2}Z_{\mathcal{X}/\mathbb{F}_q}(\frac{1}{qt}).$$

(b) existe um polinômio $L_{\mathcal{X}/\mathbb{F}_q}(t)$ de grau $2g$ tal que

$$Z_{\mathcal{X}/\mathbb{F}_q}(t) = \frac{L_{\mathcal{X}/\mathbb{F}_q}(t)}{(1-t)(1-qt)}.$$

Ainda mais, se $L_{\mathcal{X}/\mathbb{F}_q}(t) = \sum_{i=0}^{2g} a_i t^i$ então

$$a_0 = 1, \quad a_{2g} = q^g \quad e \quad a_{2g-i} = q^{g-i}.$$

Demonstração: Consulte as referências ([25], cap. V), ([10], cap. 5), ([20], cap. 5) ou [5].

□

Note que o polinômio $L_{\mathcal{X}/\mathbb{F}_q}(t)$ satisfaz

$$L_{\mathcal{X}/\mathbb{F}_q}(t) = q^g t^{2g} L_{\mathcal{X}/\mathbb{F}_q}(\frac{1}{qt}).$$

Esta igualdade é simplesmente uma reformulação da equação funcional dada na proposição. Para uma curva $\mathcal{X}$ de gênero g definida sobre $\mathbb{F}_q$ é possível associar $2g$ números complexos $\alpha_1, \ldots, \alpha_{2g}$, os quais satisfazem

$$L_{\mathcal{X}/\mathbb{F}_q}(t) = \prod_{i=1}^{2g}(1 - \alpha_i t).$$

Note que estes números são as inversas das raízes de $L_{\mathcal{X}/\mathbb{F}_q}(t)$, ou seja, são as raízes do polinômio mônico

$$h_{\mathcal{X}/\mathbb{F}_q}(t) := t^{2g} L_{\mathcal{X}/\mathbb{F}_q}(1/t).$$

A equação funcional de $L_{\mathcal{X}/\mathbb{F}_q}(t)$ implica que $L_{\mathcal{X}/\mathbb{F}_q}(\alpha^{-1}) = 0$ se, e somente se, $L_{\mathcal{X}/\mathbb{F}_q}(\alpha/q) = 0$, logo o conjunto $\{\alpha_1, \ldots, \alpha_{2g}\}$ é permutado pela aplicação $\alpha \mapsto q/\alpha$. Deste modo, por uma troca de índices se necessário, podemos sempre supor que $\alpha_i \alpha_{g+i} = q$.

Definição 4.1.3 *O polinômio $L_{\mathcal{X}/\mathbb{F}_q}(t)$ é chamado L-**polinômio** de $\mathcal{X}$ sobre $\mathbb{F}_q$. O polinômio $h_{\mathcal{X}/\mathbb{F}_q}(t)$ é chamado **polinômio recíproco** de $L_{\mathcal{X}/\mathbb{F}_q}(t)$. As raízes de $h_{\mathcal{X}/\mathbb{F}_q}(t)$ são chamadas **raízes recíprocas** de $L_{\mathcal{X}/\mathbb{F}_q}(t)$.*

Mais geralmente, se $L_{\mathcal{X}/\mathbb{F}_{q^n}}(t)$ denota o L-polinômio de $\mathcal{X}$ sobre $\mathbb{F}_{q^n}$, então, via a identidade

$$Z_{\mathcal{X}/\mathbb{F}_{q^n}}(t^n) = \prod_{\zeta^n=1} Z_{\mathcal{X}/\mathbb{F}_q}(\zeta t),$$

onde ζ percorre o conjunto das n-ésimas raízes da unidade, é possível concluir que

$$L_{\mathcal{X}/\mathbb{F}_{q^n}}(t) = \prod_{i=1}^{2g}(1 - \alpha_i^n t).$$

Em particular, $\alpha_1, \ldots, \alpha_{2g}$ são as raízes recíprocas de $L_{\mathcal{X}/\mathbb{F}_q}(t)$ se, e somente se, $\alpha_1^n, \ldots, \alpha_{2g}^n$ são as raízes recíprocas de $L_{\mathcal{X}/\mathbb{F}_{q^n}}(t)$.

Corolário 4.1.4 *Seja $\mathcal{X}$ uma curva de gênero g definida sobre $\mathbb{F}_q$ e seja a_1 o coeficiente de t no L-polinômio $L_{\mathcal{X}/\mathbb{F}_q}(t)$. Se $\alpha_1, \ldots, \alpha_{2g}$ são as raízes recíprocas de $L_{\mathcal{X}/\mathbb{F}_q}(t)$ então*

$$a_1 = -\sum_{i=1}^{2g} \alpha_i$$

e

$$\#\mathcal{X}(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g} \alpha_i^n.$$

Demonstração: Por uma lado, $L_{\mathcal{X}/\mathbb{F}_{q^n}}(t) = (1-t)(1-q^n t)Z_{\mathcal{X}/\mathbb{F}_{q^n}}(t)$ e o coeficiente de t nesta expansão é $\#\mathcal{X}(\mathbb{F}_{q^n}) - (q^n+1)$. Por outro lado, $L_{\mathcal{X}/\mathbb{F}_{q^n}}(t) = \prod_{i=1}^{2g}(1-\alpha_i^n t)$ e o coeficiente de t nesta expansão é $-\sum_{i=1}^{2g}\alpha_i^n$.

□

Exemplo 4.1.5 *Seja $\mathcal{X}$ a curva definida pelo polinômio homogêneo*

$$F(X,Y,Z) = Y^2Z + YZ^2 + XZ^2 + X^3 \in \mathbb{F}_2[X,Y,Z].$$

Esta é uma curva plana não-singular de gênero 1. Os pontos no infinito de $\mathcal{X}$ são os pontos $(a:b:0)$ tais que $F(a,b,0)=0$, logo são tais que

$$b^2\cdot 0 + b\cdot 0 = a\cdot 0 + a^3.$$

Portanto $(0:1:0)$ é o único ponto no infinito de $\mathcal{X}$. Os pontos afins de $\mathcal{X}$ são os pontos $(a:b:1)$ tais que $F(a,b,1)=0$, logo são tais que

$$b^2 + b = a + a^3,$$

portanto os pontos $\mathbb{F}_2$-racionais de $\mathcal{X}$ são $(1:0:1),(0:1:1),(1:1:1)$ e $(0:0:1)$, logo $\#\mathcal{X}(\mathbb{F}_2)=5$. Se $L_{\mathcal{X}/\mathbb{F}_2}(t) = a_0 + a_1t + a_2t^2$ é o L-polinômio de $\mathcal{X}$, então $a_0=1, a_2=2$ e $a_1 = \#\mathcal{X}(\mathbb{F}_2) - (2+1) = 2$ (cor. (4.1.4) e prop. (4.1.2)). Deste modo,

$$L_{\mathcal{X}/\mathbb{F}_2}(t) = 1 + 2t + 2t^2 \quad e \quad h_{\mathcal{X}/\mathbb{F}_2}(t) = t^2 + 2t + 2,$$

logo $\alpha := \sqrt{2}\cdot e^{\frac{3i\pi}{4}}$ e $\bar{\alpha}$ são as raízes recíprocas de $L_{\mathcal{X}/\mathbb{F}_2}(t)$, portanto

$$\#\mathcal{X}(\mathbb{F}_{2^n}) = 2^n + 1 - 2\cdot 2^{n/2}\cdot Re(z^n),$$

onde $z = e^{\frac{3i\pi}{4}}$. Agora, por um cálculo exaustivo, é possível concluir que

$$\#\mathcal{X}(\mathbb{F}_{2^n}) = \begin{cases} 2^n+1 & se \;\; n \equiv 2,6 \;\; (mod\ 8) \\ 2^n+1+2\cdot 2^{n/2} & se \;\; n \equiv 4 \;\; (mod\ 8) \\ 2^n+1-2\cdot 2^{n/2} & se \;\; n \equiv 0 \;\; (mod\ 8) \\ 2^n+1+2\cdot 2^{(n+1)/2} & se \;\; n \equiv 1,7 \;\; (mod\ 8) \\ 2^n+1-2\cdot 2^{(n+1)/2} & se \;\; n \equiv 3,5 \;\; (mod\ 8). \end{cases}$$

4.2 O Teorema de Hasse-Weil

Nesta seção provaremos que o valor absoluto dos zeros de $Z_{\mathcal{X}/\mathbb{F}_q}(t)$ é $q^{-1/2}$. Este é o conteúdo do teorema de Hasse-Weil (teo. 4.2.8). Este teorema garante que os zeros de $\zeta_{\mathcal{X}/\mathbb{F}_q}(s)$ estão sobre a reta

$Re(s) = 1/2$. De fato,

$$\begin{aligned} \zeta_{\mathcal{X}/\mathbb{F}_q}(s) = 0 \quad &\Rightarrow \quad Z_{\mathcal{X}/\mathbb{F}_q}(q^{-s}) = 0 \quad \overset{\text{Teo. H.W.}}{\Rightarrow} \quad |q^{-s}| = q^{-1/2} \\ &\Rightarrow \quad q^{-Re(s)} = q^{-1/2} \quad \Rightarrow \quad Re(s) = 1/2. \end{aligned}$$

Esta é a razão pela qual alguns textos se referem ao teorema de Hasse-Weil por *hipótese de Riemann* para curvas algébricas sobre corpos finitos.

Lema 4.2.1 *São equivalentes:*

(a) A hipótese de Riemann vale para $\mathcal{X}/\mathbb{F}_q$.

(b) A hipótese de Riemann vale para $\mathcal{X}/\mathbb{F}_{q^n}$ *para todo* $n \geq 1$.

(c) Existem constantes c_1 *e* c_2 *tais que*

$$|\#\mathcal{X}(\mathbb{F}_{q^n}) - q^n| \leq c_1 + c_2 q^{n/2},$$

para todo $n \geq 1$.

Demonstração: (a) $\Leftrightarrow$ (b) Se as raízes recíprocas de $L_{\mathcal{X}}(t)$ são $\alpha_1, \ldots, \alpha_{2g}$, então as raízes recíprocas de $L_{\mathcal{X}/\mathbb{F}_{q^n}}(t)$ são $\alpha_1^n, \ldots, \alpha_{2g}^n$. Agora basta observar que $|\alpha_i| = q^{1/2}$ se, e somente se, $|\alpha_i^n| = q^{n/2}$.

(c) $\Rightarrow$ (b). Pelo corolário (4.1.4) as raízes recíprocas $\alpha_1, \ldots, \alpha_{2g}$ do L-polinômio $L_{\mathcal{X}/\mathbb{F}_q}(t)$ satisfazem a igualdade $\#\mathcal{X}(\mathbb{F}_{q^n}) - (q^n + 1) = -\sum_{i=1}^{2g} \alpha_i^n$. Logo, pela hipótese, existe uma constante positiva c tal que $|\sum_{i=1}^{2g} \alpha_i^n| \leq c q^{n/2}$. Considere a função

$$H(t) := \sum_{i=1}^{2g} \frac{\alpha_i t}{1 - \alpha_i t}.$$

Note que $\mu := min\{|\alpha_i^{-1}| \ ; \ 1 \leq i \leq 2g\}$ é precisamente o raio de convergência de $H(t)$ em torno de $t = 0$. Deste modo, quando $|t| < \mu$ vale

$$H(t) = \sum_{i=1}^{2g} \sum_{n=1}^{\infty} (\alpha_i t)^n = \sum_{n=1}^{\infty} (\sum_{i=1}^{2g} \alpha_i^n) t^n,$$

logo

$$|H(t)| \leq \sum_{n=1}^{\infty} c q^{n/2} |t|^n = c \sum_{n=1}^{\infty} (q^{1/2}|t|)^n.$$

Note que a série $H(t)$ converge quando $|t| < q^{-1/2}$. Deste modo, $q^{-1/2} \leq \mu$ e portanto $q^{1/2} \geq |\alpha_i|$. Por outro lado, por uma troca de índices se necessário, podemos supor $\alpha_i \alpha_{2g+i} = q$, logo $\prod_{i=1}^{2g} \alpha_i = q^g$ e portanto $|\alpha_i| = q^{1/2}$.

(b) $\Rightarrow$ (c) Pelo corolário (4.1.4) as raízes recíprocas $\alpha_1, \ldots, \alpha_{2g}$ do L-polinômio $L_{\mathcal{X}/\mathbb{F}_{q^n}}(t)$ satisfazem a igualdade $\#\mathcal{X}(\mathbb{F}_{q^n}) - (q^n + 1) = -\sum_{i=1}^{2g} \alpha_i^n$, logo o resultado segue com $c_1 = 1$ e $c_2 = 2g$.

□

Para obter a estimativa sobre o número de pontos racionais dada pelo item (c) do lema acima iremos considerar uma curva $\mathcal{X}'$ tal que a extensão $\bar{\mathbb{F}}_q(\mathcal{X}')/\bar{\mathbb{F}}_q(\mathcal{X})$ é Galois. A idéia é contar o número de pontos de $\mathcal{X}'$ satisfazendo certas propriedades e que estão na contra imagem dos pontos racionais de $\mathcal{X}$, via o morfismo induzido pela inclusão $\bar{\mathbb{F}}_q(\mathcal{X}) \hookrightarrow \bar{\mathbb{F}}_q(\mathcal{X}')$. Isto será feito durante a demonstração do teorema de Hasse-Weil (teo. (4.2.8)), por agora precisamos de alguns resultados preliminares.

Definição 4.2.2 *Um morfismo não-constante $\phi : \mathcal{X}' \to \mathcal{X}$, entre curvas definidas sobre um corpo perfeito k, é **Galois** se a extensão $k(\mathcal{X}')/\phi^* k(\mathcal{X}')$ é Galois.*

Sejam $\mathcal{X}'$ e $\mathcal{X}$ curvas definidas sobre $\mathbb{F}_q$ e suponha que $\phi : \mathcal{X}' \to \mathcal{X}$ é Galois. Identifique $\bar{\mathbb{F}}_q(\mathcal{X})$ com sua imagem $\phi^*\bar{\mathbb{F}}_q(\mathcal{X})$ e denote por $Gal(\bar{\mathbb{F}}_q(\mathcal{X}')/\bar{\mathbb{F}}_q(\mathcal{X}))$ o grupo de Galois correspondente ao morfismo ϕ. Este grupo age nos pontos de $\mathcal{X}'$ da seguinte maneira:

$$P \longmapsto P^\sigma,$$

onde P^σ é a imagem de P, via o morfismo induzido por σ, em $\mathcal{X}'$. Note que P^σ é o único ponto que corresponde ao ideal maximal $\sigma^{-1}(M_P(\mathcal{X}'))$. De fato, use a mesma notação σ para o morfismo induzido. Se $f \in \bar{\mathbb{F}}_q(\mathcal{X}')$, então $\sigma(f)$ é a função racional $f \circ \sigma$, logo

$$v_P(\sigma(f)) = e_\sigma(P) v_{P^\sigma}(f),$$

portanto $\sigma(f) \in M_P(\mathcal{X}')$ se, e somente se, $f \in M_{P^\sigma}(\mathcal{X}')$, ou seja, $\sigma^{-1}(M_P(\mathcal{X}')) = M_{P^\sigma}(\mathcal{X}')$. Isto demonstra a afirmação.

Lema 4.2.3 *Seja $\phi : \mathcal{X}' \to \mathcal{X}$ Galois e seja $Q \in \mathcal{X}$.*

(a) O grupo de Galois $Gal(\bar{\mathbb{F}}_q(\mathcal{X}')/\bar{\mathbb{F}}_q(\mathcal{X}))$ permuta os elementos da fibra $\phi^{-1}(Q)$ e esta ação é transitiva.

(b) Os índices de ramificação de ϕ, nos pontos de $\phi^{-1}(Q)$, coincidem.

(c) Sejam $P \in \phi^{-1}(Q)$, $n \geq 1$ e denote por P^{q^n} a imagem de P via a q^n-ésima aplicação de Frobenius. Então existe $\sigma \in Gal(\bar{\mathbb{F}}_q(\mathcal{X}')/\bar{\mathbb{F}}_q(\mathcal{X}))$ tal que $P^{q^n} = P^\sigma$ se, e somente se, Q é um ponto $\mathbb{F}_{q^n}$-racional.

Demonstração: Observe que $\bar{\mathbb{F}}_q(\mathcal{X}) \subseteq \bar{\mathbb{F}}_q(\mathcal{X}')$ via a inclusão $\bar{\mathbb{F}}_q(\mathcal{X}) \hookrightarrow \bar{\mathbb{F}}_q(\mathcal{X}')$, logo os ideais $M_P(\mathcal{X})$, onde $P \in \phi^{-1}(Q)$, são os lugares de $\bar{\mathbb{F}}_q(\mathcal{X}')$ que estão sobre o lugar $M_Q(\mathcal{X})$ (veja apêndice A). Logo, o teorema (A.2.7) e o corolário (A.2.8) implicam (a) e (b), respectivamente. Note que $P^{q^n} \in \phi^{-1}(Q^{q^n})$, logo $Q^{q^n} = Q$ se, e somente se, os pontos P^{q^n} e P pertencem a $\phi^{-1}(Q)$, e isto ocorre se, e somente se, existe $\sigma \in Gal(\bar{\mathbb{F}}_q(\mathcal{X}')/\bar{\mathbb{F}}_q(\mathcal{X}))$ tal que $P^{q^n} = P^\sigma$, por (a).

□

Considere o conjunto

$$\mathbb{P}_n(\mathcal{X}'/\mathcal{X},\sigma) := \{P \in \mathcal{X}' \ ; \ e_\phi(P) = 1 \text{ e } P^{q^n} = P^\sigma\}.$$

Note que existe apenas um número finito de pontos $P \in \mathcal{X}'$ satisfazendo $P^{q^n} = P^\sigma$ que não pertencem ao conjunto $\mathbb{P}_n(\mathcal{X}'/\mathcal{X},\sigma)$. De fato, tais pontos são ramificados por ϕ (cor. 1.3.11).

Lema 4.2.4 *Com as notações acima.*

(a) O conjunto $\mathbb{P}_n(\mathcal{X}'/\mathcal{X},\sigma)$ é sempre finito.

(b) A intersecção $\mathbb{P}_n(\mathcal{X}'/\mathcal{X},\sigma_1) \cap \mathbb{P}_n(\mathcal{X}'/\mathcal{X},\sigma_2)$ é vazia sempre que $\sigma_1 \neq \sigma_2$.

Demonstração: (a) Um ponto $P \in \mathbb{P}_n(\mathcal{X}'/\mathcal{X},\sigma)$ é tal que $\phi(P) = Q$ para algum ponto $\mathbb{F}_{q^n}$-racional $Q \in \mathcal{X}$, pelo item (c) do lema (4.2.3). Como existe apenas um número finito de pontos $\mathbb{F}_{q^n}$-racionais e a fibra $\phi^{-1}(Q)$ é sempre finita, o resultado segue.

(b) Basta observar que a existência de um ponto P na intersecção $\mathbb{P}_n(\mathcal{X}'/\mathcal{X},\sigma_1) \cap \mathbb{P}_n(\mathcal{X}'/\mathcal{X},\sigma_2)$ contradiz o item (a) do lema (4.2.3).

□

Daqui para frente iremos investigar a expressão

$$p_n(\mathcal{X}'/\mathcal{X},\sigma) := \#\mathbb{P}_n(\mathcal{X}'/\mathcal{X},\sigma).$$

Lema 4.2.5 *Com as notações acima, existe uma constante c independente de n tal que*

$$|\#\mathcal{X}(\mathbb{F}_{q^n}) - \frac{1}{|G|}\sum_{\sigma\in G} p_n(\mathcal{X}'/\mathcal{X},\sigma)| \leq c,$$

onde $G = Gal(\bar{\mathbb{F}}_q(\mathcal{X}')/\bar{\mathbb{F}}_q(\mathcal{X}))$.

Demonstração: O item (c) do lema (4.2.3) implica que

$$\bigcup_{\sigma\in G} \mathbb{P}_n(\mathcal{X}'/\mathcal{X},\sigma) \subseteq \bigcup_{Q\in\mathcal{X}(\mathbb{F}_{q^n})} \phi^{-1}(Q),$$

onde o complementar desta inclusão é um conjunto finito de pontos de $\mathcal{X}'$ que são ramificados por ϕ. Por outro lado, o teorema (1.3.10) implica que $|G| = \sum_{P\in\phi^{-1}(Q)} e_\phi(P)$, logo

$$|\sum_{\sigma\in G} p_n(\mathcal{X}'/X,\sigma) - |G|\#\mathcal{X}(\mathbb{F}_{q^n})| \leq c',$$

onde c' é uma constante que não depende de n, assim

$$|\#\mathcal{X}(\mathbb{F}_{q^n}) - \frac{1}{|G|}\sum_{\sigma\in G} p_n(\mathcal{X}'/\mathcal{X},\sigma)| \leq \frac{c'}{|G|}.$$

Agora basta tomar $c = c'/|G|$.

□

Para um q apropriado, iremos utilizar o teorema de Stöhr-Voloch para obter uma cota superior para o número $p_n(\mathcal{X}'/\mathcal{X},\sigma)$. Para isto precisamos de um lema.

Lema 4.2.6 *Seja $P \in \mathcal{X}'$ e seja g o gênero de $\mathcal{X}'$. Para cada $m \geq g+1$, a série linear completa $|(m+g)P|$ é livre de pontos base, tem dimensão m e as ordens $j_0,\ldots,j_m$ de $|(m+g)P|$ em P satisfazem $j_0 = 0, j_1 = 1$ e*

$$\sum_{i=1}^{m} j_i \quad \leq \quad \frac{(m-g)(m-g-1)}{2} + \frac{(2m-g)(g+1)}{2}.$$

Demonstração: Se $d = m+g$ então o grau da série $|(m+g)P|$ é $d \geq 2g+1$ e portanto a dimensão de $|dP|$ é m (cor. (1.6.6)). O corolário (2.2.12) implica que a série $|dP|$ é livre de pontos base e que as ordens $j_0,\ldots,j_m$ de $|(m+g)P|$ em P satisfazem

$$j_i = i \text{ sempre que } i \leq d-2g.$$

Portanto $j_0 = 0$ e $j_1 = 1$. Os inteiros $j_0,\ldots,j_m$ são não negativos, distintos e menores que d, logo $j_i \leq i+d-m$. Agora basta usar a fórmula clássica da soma finita de uma PA para obter

$$\begin{aligned}\sum_{i=1}^{m} j_i &\leq (1+\ldots+d-2g-1)+((d-g)+\ldots+(m-g)) \\ &= \frac{(m-g)(n-g-1)}{2} + \frac{(2m-g)(g+1)}{2}.\end{aligned}$$

Isto conclui a demonstração.

□

Proposição 4.2.7 *Com as notações acima, suponha que q é um quadrado maior que $4g^4(g-1)^2$, onde g é o gênero de $\mathcal{X}'$, e seja $\sigma \in Gal(\bar{\mathbb{F}}_q(\mathcal{X}')/\bar{\mathbb{F}}_q(\mathcal{X}))$. Nestas condições, o número $p_n(\mathcal{X}'/\mathcal{X},\sigma)$ pode ser estimado por*

$$p_n(\mathcal{X}'/\mathcal{X},\sigma) \leq (q^n+1) + 2gq^{n/2}.$$

Demonstração: Se $\bar{\mathrm{Fr}}$ é a aplicação de Frobenius $x \to x^q$, que é a identidade em $\bar{\mathbb{F}}_q$, então $\tau := \bar{\mathrm{Fr}}^n \circ \sigma^{-1} : \bar{\mathbb{F}}_q(\mathcal{X}') \to \bar{\mathbb{F}}_q(\mathcal{X}')$ define uma $\bar{\mathbb{F}}_q$-inclusão de $\bar{\mathbb{F}}_q(\mathcal{X}')$ de grau q^n (item (b) da prop. B.0.12) e que fixa todos os pontos $P \in \mathcal{X}'$ sujeitos a condição $P^{q^n} = P^\sigma$, ou seja, τ fixa os pontos de $\mathbb{P}_n(\mathcal{X}'/\mathcal{X}, \sigma)$. Conforme a definição dada em (3.2.1), tais pontos são também ramificados por τ. Fixe $P \in \mathcal{X}$ fixo e ramificado por τ, suponha que $m \geq g+1$ e sejam $\varepsilon_1, \ldots, \varepsilon_m$ as τ-ordens da série linear completa $|(m+g)P|$ (lema (4.2.6)). Para cada base $\{f_0, \ldots, f_m\}$ de $\mathcal{L}((m+g)P)$, o vetor $(f_0, \ldots, f_m)$ não é um múltiplo de $(\tau(f_0), \ldots, \tau(f_n))$, logo $\varepsilon_1 = 0$. Sejam $j_0, \ldots, j_m$ as ordens de $|(m+g)P|$ em P. O lema (4.2.6) e o lema (3.2.6) implicam

$$\begin{aligned} \sum_{i=1}^{m} \varepsilon_i &\leq \sum_{i=1}^{m} j_i - 1 = -m + \sum_{i=1}^{m} j_i \\ &\leq g(g-1) + \frac{m(m-1)}{2}. \end{aligned}$$

Esta cota, aplicada no teorema de Stöhr-Voloch (teo. (3.2.7)), fornece

$$\begin{aligned} p_n(\mathcal{X}'/\mathcal{X}, \sigma) &\leq \Big(1 + \frac{q^n}{m}\Big)(m+g) + \frac{2g(g-1)^2}{m} + (g-1)(m-1) \\ &= 1 + q^n + \Big(m + \frac{q^n}{m}\Big)g + \frac{2g^2(g-1)}{m}. \end{aligned}$$

Agora o resultado segue rapidamente supondo $m = q^{n/2}$.

□

Agora estamos em condições de demonstrar o resultado principal deste capítulo.

Teorema 4.2.8 (Hasse-Weil) *Seja $\mathcal{X}$ uma curva de gênero g definida sobre $\mathbb{F}_q$. As raízes recíprocas, $\alpha_1, \ldots, \alpha_{2g}$, do L-polinômio $L_{\mathcal{X}/\mathbb{F}_q}(t)$ de $\mathcal{X}$ satisfazem*

$$|\alpha_i| = q^{1/2}.$$

Demonstração: Seja $x \in \bar{\mathbb{F}}_q(\mathcal{X})$ tal que $\bar{\mathbb{F}}_q(\mathcal{X})/\bar{\mathbb{F}}_q(x)$ é uma extensão finita e separável e seja F' a menor extensão de $\bar{\mathbb{F}}_q(\mathcal{X})$ que é Galois sobre $\bar{\mathbb{F}}_q(x)$.[2] Note que $F' = \bar{\mathbb{F}}_q(x, y)$ para algum elemento $y \in F'$ satisfazendo um polinômio sobre $\bar{\mathbb{F}}_q(x)$, logo F' é isomorfo a $\bar{\mathbb{F}}_q(\mathcal{X}')$, onde $\mathcal{X}'$ é o modelo projetivo não-singular da curva definida por este polinômio (teo. 1.3.8). Tomando q maior se necessário, podemos supor que $\mathcal{X}'$ é definida sobre $\mathbb{F}_q$. Portanto, existem morfismos não-constantes

$$\mathcal{X}' \xrightarrow{\phi} \mathcal{X} \xrightarrow{\phi'} \mathbb{P}^1,$$

[2] O elemento de separação x sempre existe, veja ([25], pag. 127). O corpo F' pode ser construído adicionando a $\bar{\mathbb{F}}_q(\mathcal{X})$ todas as raízes dos polinômios minimais dos elementos de uma $\bar{\mathbb{F}}_q(x)$-base separável de $\bar{\mathbb{F}}_q(\mathcal{X})$.

tais que ϕ e ϕ' são ambos Galois. Usando o lema (4.2.1) suponha que q é um quadrado maior que $4g^4(g-1)^2$, onde g é o gênero de $\mathcal{X}'$. Sejam $G = Gal(\bar{\mathbb{F}}_q(\mathcal{X}')/\bar{\mathbb{F}}_q(x))$ e $H = Gal(\bar{\mathbb{F}}_q(\mathcal{X}')/\bar{\mathbb{F}}_q(\mathcal{X}))$. Então

$$\bigcup_{\sigma\in H} \mathbb{P}_n(\mathcal{X}'/\mathcal{X},\sigma) \subseteq \bigcup_{\sigma\in H} \mathbb{P}_n(\mathcal{X}'/\mathbb{P}^1,\sigma),$$

e o complemento desta inclusão é um conjunto finito de pontos que são ramificados por ϕ', logo

$$\sum_{\sigma\in H} p_n(\mathcal{X}'/\mathcal{X},\sigma) = \sum_{\sigma\in H} p_n(\mathcal{X}'/\mathbb{P}^1,\sigma) + c_1 \tag{4.1}$$

para alguma constate c_1 independente de n. O lema (4.2.5) para as curvas $\mathcal{X}'$ e $\mathcal{X}$ implica

$$|\#\mathcal{X}(\mathbb{F}_{q^n}) - \frac{1}{|H|}\sum_{\sigma\in H} p_n(\mathcal{X}'/\mathcal{X},\sigma)| \leq c_2,$$

onde c_2 é uma constante independente de n, logo, pela equação (4.1), existe uma constante c_3 independente de n tal que

$$|\#\mathcal{X}(\mathbb{F}_{q^n}) - \frac{1}{|H|}\sum_{\sigma\in H} p_n(\mathcal{X}'/\mathbb{P}^1,\sigma)| \leq c_3. \tag{4.2}$$

É bem conhecido e não é difícil de provar que $\#\mathbb{P}^1(\mathbb{F}_{q^n}) = q^n + 1$, logo o lema (4.2.5) para as curvas $\mathcal{X}'$ e $\mathbb{P}^1$ implica

$$|q^n + 1 - \frac{1}{|G|}\sum_{\sigma\in G} p_n(\mathcal{X}'/\mathbb{P}^1,\sigma)| \leq c_4,$$

onde c_4 é uma constante independente de n, ou seja,

$$\sum_{\sigma\in G} p_n(\mathcal{X}'/\mathbb{P}^1,\sigma) \geq (q^n + 1 - c_4)|G|.$$

Deste modo, a proposição (4.2.7) implica que

$$\begin{aligned} q^n + 1 + 2gq^{n/2} \geq p_n(\mathcal{X}'/\mathbb{P}^1,\sigma) &= \sum_{\sigma\in G} p_n(\mathcal{X}'/\mathbb{P}^1,\sigma) - \sum_{\gamma\in G\setminus\{\sigma\}} p_n(\mathcal{X}'/\mathbb{P}^1,\gamma) \\ &\geq (q^n + 1 - c_4)|G| + (1 - |G|)(q^n + 1 + 2gq^{n/2}), \end{aligned}$$

onde g é o gênero de $\mathcal{X}'$. Agora com uma conta simples é possível mostrar que existem constantes a e b independentes de n tais que

$$|p_n(\mathcal{X}'/\mathbb{P}^1,\sigma) - q^n| \leq a + bq^{n/2}.$$

Usando a desigualdade (4.2), temos

$$|\#\mathcal{X}(\mathbb{F}_{q^n}) - q^n| \leq |\#\mathcal{X}(\mathbb{F}_{q^n}) - \frac{1}{|H|}\sum_{\sigma\in H} p_n(\mathcal{X}'/\mathbb{P}^1,\sigma)| + |\frac{1}{|H|}\sum_{\sigma\in H} p_n(\mathcal{X}'/\mathbb{P}^1,\sigma) - q^n|,$$

logo existem constantes a' e b' independentes de n tais que

$$|\#\mathcal{X}(\mathbb{F}_{q^n}) - q^n| \leq a' + b'q^{n/2}.$$

Agora o teorema de Hasse-Weil é uma consequência imediata do lema (4.2.1).

□

Corolário 4.2.9 *Se $\mathcal{X}$ é uma curva de gênero g definida sobre $\mathbb{F}_q$, então a cardinalidade do conjunto dos pontos $\mathbb{F}_{q^n}$-racionais de $\mathcal{X}$ pode ser estimada por*

$$|\#\mathcal{X}(\mathbb{F}_{q^n}) - (q^n + 1)| \leq 2gq^{n/2}.$$

Demonstração: Basta aplicar o teorema de Hasse-Weil na igualdade descrita no corolário (4.1.4).

□

Teorema 4.2.10 (Serre) *Se $\mathcal{X}$ é uma curva de gênero g definida sobre $\mathbb{F}_q$, então a cardinalidade do conjunto dos pontos $\mathbb{F}_{q^n}$-racionais de $\mathcal{X}$ pode ser estimada por*

$$|\#\mathcal{X}(\mathbb{F}_{q^n}) - (q^n + 1)| \leq g[2q^{n/2}],$$

onde $[2q^{n/2}]$ denota a parte inteira de $2q^{n/2}$.

Demonstração: Suponha $n = 1$, o caso geral é análogo. Seja $L_{\mathcal{X}}(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$ o L-polinômio de $\mathcal{X}$. Os α_i's são inteiros algébricos que cumprem $|\alpha_i| = q^{1/2}$ e podem ser ordenados de forma que $\alpha_i\alpha_{g+i} = q$. Portanto

$$\overline{\alpha_i} = \alpha_{g+i} = q/\alpha_i.$$

Defina

$$\gamma_i := \overline{\alpha_i} + \alpha_{g+i} + [2q^{1/2}] + 1.$$

Note que os elementos $\gamma_i's$ são inteiros algébricos positivos e cada homomorfismo $\sigma : \mathbb{Q}(\alpha_1, \ldots, \alpha_{2g}) \to \mathbb{C}$ permuta os elementos $\alpha_1, \ldots, \alpha_{2g}$. Ainda mais, se $\sigma(\alpha_i) = \alpha_j$ então $\sigma(\overline{\alpha_i}) = \sigma(q/\alpha_i) = q/\sigma(\alpha_i) = \overline{\sigma(\alpha_i)} = \overline{\alpha_j}$. Deste modo, σ age permutando os elementos de $\{\gamma_1, \ldots, \gamma_g\}$ e portanto

$$\gamma := \prod_{i=1}^{2g} \gamma_i$$

é um inteiro algébrico fixo por qualquer homomorfismo de $\mathbb{Q}(\alpha_1, \ldots, \alpha_{2g})$ em $\mathbb{C}$, logo $\gamma \in \mathbb{Z}$. Os elementos $\alpha_i's$ são positivos, logo $\gamma > 0$ e portanto $\prod_{i=1}^{2g} \gamma_i \geq 1$. A desigualdade entre a média aritmética e a geométrica fornece

$$\frac{1}{g} \cdot \sum_{i=1}^{2g} \gamma_i \geq (\prod_{i=1}^{2g} \gamma_i)^{1/g} \geq 1.$$

Deste modo,

$$\sum_{i=1}^{g} (\alpha_i + \overline{\alpha_i} + [2q^{1/2}] + 1) \geq g,$$

portanto

$$\sum_{i=1}^{2g} \alpha_i \geq -g[2q^{1/2}].$$

Agora o resultado segue desta desigualdade e do corolário (4.1.4).

□

Note que a curva dada no exemplo (3.3.11) atinge a cota superior de Hasse-Weil, que neste caso é igual a cota superior de Serre. Não é sempre que isto ocorre e existem situações em que o teorema de Stöhr-Voloch fornece uma estimativa melhor que os teoremas de Hasse-Weil e Serre, como mostra o próximo exemplo.

Exemplo 4.2.11 *Seja $\mathcal{X}$ uma curva de gênero 4 definida sobre $\mathbb{F}_7$. Por exemplo, considere a única curva projetiva não-singular birracional a curva definida pelo polinômio*

$$F(X,Y) = Y^2 + Y - X^9 \in \mathbb{F}_7[X,Y].$$

A hipótese de Riemann garante que $\#\mathcal{X}(\mathbb{F}_7) \leq 29$ e o teorema de Serre que $\#\mathcal{X}(\mathbb{F}_7) \leq 28$. A série canônica $|K_{\mathcal{X}}|$ sobre $\mathcal{X}$ é uma série linear livre de pontos base, dimensão 3 e grau 6. Em particular, se ν_0, ν_1, ν_2 são as ordens de Frobenius de $|K_{\mathcal{X}}|$, então $\nu_2 < 7$, portanto $\nu_0 = 0, \nu_1 = 1$ e $\nu_2 = 2$ (prop. (3.3.4)). O teorema (3.3.9) de Stöhr-Voloch aplicado a série $|K_{\mathcal{X}}|$ implica $\#\mathcal{X}(\mathbb{F}_7) \leq 26$, que é uma estimativa melhor que a fornecida pelos teoremas de Hasse-Weil e Serre.

Exemplo 4.2.12 (Quartica de Klein) *Seja $\mathcal{X}$ a curva plana definida pelo polinômio homogêneo*

$$F(X,Y,Z) = X^3Y + Y^3Z - XZ^3 \in \mathbb{F}_{2^3}[X,Y,Z].$$

Esta é uma curva não-singular e seu gênero é 3. Os pontos no infinito de $\mathcal{X}$ são os pontos $(a:b:0)$ tais que $F(a,b,0) = 0$, ou seja, tais que

$$a^3b + b^3 \cdot 0 + a \cdot 0 = 0.$$

Portanto $(1:0:0)$ e $(0:1:0)$ são os pontos no infinito de $\mathcal{X}$. Note que tais pontos, assim como $(0:0:1)$, são $\mathbb{F}_{2^3}$-racionais. Os demais pontos $\mathbb{F}_{2^3}$-racionais de $\mathcal{X}$ são os pontos afins $(a:b:1)$ tais que $(a,b) \in \mathbb{F}_{2^3}^* \times \mathbb{F}_{2^3}^*$ e

$$a^3b + b^3 + a = 0.$$

Multiplicando a igualdade acima por a^6 e usando as igualdades $a^7 = 1$ e $a^9 = a^2$, obtemos

$$z^3 + z = 1,$$

onde $z = a^3b$. *Elevando esta equação ao quadrado e multiplicando ambos os lados por* z^2, *obtemos* $z^8 - (z^4 + z^2) = 0$, *ou seja,* $z^8 - z = 0$, *logo* $z \in \mathbb{F}_{2^3}$, *portanto as três soluções de* $z^3 + z + 1$ *são elementos de* $\mathbb{F}_{2^3}$. *Note que* $a \in \mathbb{F}_{2^3}^*$ *implica* $b = z/a^3 \in \mathbb{F}_{2^3}^*$, *logo existem* 21 *pontos* $(a, b) \in \mathbb{F}_{2^3}^* \times \mathbb{F}_{2^3}^*$ *tais que* $F(a, b, 1) = 0$. *Portanto*

$$\mathcal{X}(\mathbb{F}_{2^3}) = 24 = (2^3 + 1) + 3 \cdot [4\sqrt{2}],$$

ou seja, $\mathcal{X}$ *atinge a cota superior de Serre. Em particular, se* $\alpha_1, \ldots, \alpha_6$ *são as raízes recíprocas de* $L_{\mathcal{X}/\mathbb{F}_{2^3}}(t)$ *então* $\sum_{i=1}^{3}(\alpha_i + \overline{\alpha}_i) = -15$ *(cor. 4.1.4) e* $\alpha_i\overline{\alpha_i} = 8$ *(teo. 4.2.8), logo* $\alpha_i + \overline{\alpha}_i = -5$, *portanto*

$$\begin{aligned} h_{\mathcal{X}/\mathbb{F}_{2^3}}(t) &= \prod_{i=1}^{3}(t - \alpha_i)(t - \overline{\alpha_i}) = \prod_{i=1}^{3}(t^2 - (\alpha_i + \alpha_i)t - \alpha_i\overline{\alpha_i}) \\ &= \prod_{i=1}^{3}(t^2 + 5t + 8) = (t^2 + 5t + 8)^3. \end{aligned}$$

Agora as raízes recíprocas de $L_{\mathcal{X}/\mathbb{F}_{2^3}}(t)$ *podem ser calculadas explicitamente. Se* $\beta_1, \ldots \beta_6$ *são as raízes recíprocas de* $L_{\mathcal{X}/\mathbb{F}_2}(t)$ *então* $\beta_i^3 = \alpha_i$ *e* $\beta_i^3 + \overline{\beta_i}^3 = -5$. *Em particular,* $\beta_1^3, \ldots, \beta_{2g}^3$ *são raízes do polinômio* $T^2 + 5T + 8 = 0$. *Portanto*

$$h_{\mathcal{X}/\mathbb{F}_2}(t) = t^6 + 5t^3 + 8 \quad e \quad L_{\mathcal{X}/\mathbb{F}_2}(t) = 8t^6 + 5t^3 + 1.$$

Observe que o coeficiente de t *em* $L_{\mathcal{X}/\mathbb{F}_2}(t)$ *é nulo, logo* $-\sum_{i=1}^{2g}\beta_i = 0$ *(cor. 4.1.4), portanto* $\#\mathcal{X}(\mathbb{F}_2) = 3$. *Calculando explicitamente as raízes recíprocas de* $L_{\mathcal{X}/\mathbb{F}_2}(t)$ *é possível encontrar as raízes recíprocas de* $L_{\mathcal{X}/\mathbb{F}_{2^2}}(t)$. *A partir disto, usando o corolário (4.1.4), é possível concluir que* $\#\mathcal{X}(\mathbb{F}_{2^2}) = 5$.

Capítulo 5

Curvas Maximais e a Curva Hermitiana

Vimos na introdução que curvas definidas sobre corpos finitos com muitos pontos racionais são interessantes por suas diversas aplicações. O corolário (4.2.9) é uma das principais consequências do teorema de Hasse-Weil e fornece a seguinte estimativa para o número de pontos racionais de uma curva $\mathcal{X}$, definida sobre o corpo $\mathbb{F}_q$:

$$(q+1) - 2gq^{1/2} \leq \#\mathcal{X}(\mathbb{F}_q) \leq (q+1) + 2gq^{1/2},$$

onde g é o gênero de $\mathcal{X}$. Note que estas cotas dependem de g, que em geral não é um número fácil de calcular. Existem diversas maneiras de caracterizar o gênero de uma curva, as quais proporcionam algumas estimativas para este número. Dentre elas destacamos a seguinte: se existe sobre $\mathcal{X}$ uma série linear livre de pontos base de dimensão $n \geq 2$ e grau d, então

$$g \leq \begin{cases} \frac{(d-1-(n-1)/2)^2}{2(n-1)} & \text{se } n \text{ é ímpar} \\ \frac{(d-1-(n-1)/2-1/4)^2}{2(n-1)} & \text{se } n \text{ é par.} \end{cases}$$

Esta cota é conhecida por *cota de Castelnuovo*, para uma demonstração veja ([2], pag. 116).

5.1 Curvas Maximais

Nesta seção estaremos seguindo [7] e apresentaremos algumas propriedades geométricas e aritméticas de curvas que atingem a cota superior de Hasse-Weil.

Definição 5.1.1 *Uma curva $\mathcal{X}$ de gênero g e definida sobre $\mathbb{F}_q$ é chamada $\mathbb{F}_{q^n}$-**maximal** se $\#\mathcal{X}(\mathbb{F}_{q^n}) = q^n + 1 + 2gq^{n/2}$.*

Proposição 5.1.2 *Seja $\mathcal{X}$ uma curva de gênero g definida sobre $\mathbb{F}_q$ e sejam $\alpha_1, \ldots, \alpha_{2g}$ as raízes recíprocas do L-polinômio $L_{\mathcal{X}/\mathbb{F}_{q^2}}(t)$ de $\mathcal{X}$.*

(a) São equivalentes:

(i) $\mathcal{X}$ *é* $\mathbb{F}_{q^2}$*-maximal.*

(ii) $\alpha_i = -q$*.*

(iii) $h_{\mathcal{X}/\mathbb{F}_{q^2}}(t) = (t+q)^{2g}$*.*

(b) Se $\mathcal{X}$ *é* $\mathbb{F}_{q^2}$*-maximal, então*

$$\#\mathcal{X}(\mathbb{F}_{q^n}) = \begin{cases} q^n + 1 & se \;\; n \equiv 1 \;(mod\; 2) \\ q^n + 1 + 2g \cdot 2^{n/2} & se \;\; n \equiv 2 \;(mod\; 4) \\ q^n + 1 - 2g \cdot 2^{n/2} & se \;\; n \equiv 0 \;(mod\; 4). \end{cases}$$

Demonstração: (a) Pelo corolário (4.1.4), $\mathcal{X}$ é $\mathbb{F}_{q^2}$-maximal se, e somente se, $\sum_{i=1}^{2g}(\alpha_i - \overline{\alpha}_i) = -2gq$. Pelo teorema de Hasse-Weil, isto ocorre se, e somente se, $\alpha_i = -q$. Como $\alpha_1, \ldots, \alpha_{2g}$ são as raízes de $h_{\mathcal{X}/\mathbb{F}_{q^2}}(t)$, a equivalência é imediata.

(b) Sejam $\beta_1, \ldots, \beta_{2g}$ as raízes recíprocas do L-polinômio $L_{\mathcal{X}/\mathbb{F}_q}(t)$. Pelo corolário (4.1.4), $\mathcal{X}(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{i=1}^{2g}\beta_i^n$. Pelo item (a) acima, cada raíz recíproca β de $L_{\mathcal{X}/\mathbb{F}_q}(t)$ satisfaz $\beta^2 = -q$. Em particular, a parte real de β é nula.

Se $n \equiv 1 \;(mod\; 2)$ então n é da forma $2a+1$, logo $\beta^n + \overline{\beta}^n = 0$ e isto implica o primeiro item da tabela. Se $n \equiv 2 \;(mod\; 4)$ então n é da forma $2(2a+1)$, logo $\beta^n = -q^{n/2}$ e isto implica o segundo item da tabela. Finalmente, se $n \equiv 0 \;(mod\; 4)$ então n é forma $2(2a)$, logo $\beta = q^{n/2}$ e isto conclui a demonstração.

□

Note que para uma curva $\mathcal{X}$ definida sobre $\mathbb{F}_q$ ser $\mathbb{F}_{q^n}$-maximal, é necessário que q^n seja uma potência par da característica de $\mathbb{F}_q$. Por esta razão, passaremos a supor que $\mathcal{X}$ é uma curva definida sobre $\mathbb{F}_{q^2}$ e diremos simplesmente *maximal*, significando que $\mathcal{X}$ é $\mathbb{F}_{q^2}$-maximal, ou seja,

$$\#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq.$$

Neste capítulo, um ponto *racional* é um ponto $\mathbb{F}_{q^2}$-racional.

A próxima proposição mostra que para uma curva ser maximal existe uma condição necessária sobre o gênero g em relação a q.

Proposição 5.1.3 (Ihara) *Se* $\mathcal{X}$ *é uma curva maximal definida sobre* $\mathbb{F}_{q^2}$ *então*

$$g \leq q(q-1)/2.$$

Demonstração: Sejam $\alpha_1, \ldots, \alpha_{2g}$ as raízes recíprocas do L-polinômio $L_{\mathcal{X}/\mathbb{F}_{q^2}}(t)$. Pelo corolário (4.1.4), $\#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 + 1 - \sum_{i=1}^{2g} \alpha_i$, onde cada α_i satisfaz $|\alpha_i| = q$ (teo. Hasse-Weil). Por hipótese $\mathcal{X}$ é maximal, logo $\#\mathcal{X}(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq$ e portanto $\alpha_i = -q$. Note que $\#\mathcal{X}(\mathbb{F}_{q^4}) \geq \#\mathcal{X}(\mathbb{F}_{q^2})$, logo

$$\#\mathcal{X}(\mathbb{F}_{q^4}) = q^4 + 1 - \sum_{i=1}^{2g} \alpha_i^2 = q^4 + 1 - 2gq^2.$$

Assim, $q^2 + 1 + 2gq \leq q^4 + 1 - 2gq^2$. Agora uma manipulação simples desta desigualdade mostra que $g \leq q(q-1)/2$.

□

O próximo lema é a chave para todos os resultados obtidos neste capítulo. Apesar do enunciado simples a demonstração não é trivial. Para demonstrá-lo é necessário resultados sofisticados sobre variedades abelianas.

Lema 5.1.4 *Seja* Fr *a aplicação de Frobenius com relação ao corpo base* $\mathbb{F}_{q^2}$*, ou seja,* $\mathrm{Fr}(P) = P^{q^2}$ *para cada* $P \in \mathcal{X}$*. Se* P_0 *é um ponto racional da curva maximal* $\mathcal{X}$*, então*

$$\mathrm{Fr}(P) + qP \sim (q+1)P_0 \quad \forall \quad P \in \mathcal{X}.$$

Demonstração: Veja ([7], 1.2, pag. 4) ou veja a demonstração do lema (1) de [21].

□

Corolário 5.1.5 *Se* P_0 *e* Q *são dois pontos racionais de* $\mathcal{X}$ *então* $(q+1)P_0 \sim (q+1)Q$*, ou seja, o divisor* $(q+1)(P_0 - Q)$ *é principal. Em particular,* $q+1$ *é uma não-lacuna de Weierstrass em qualquer ponto racional.*

Demonstração: A primeira parte segue diretamente do lema observando que a relação $\sim$ é transitiva. Para ver que $q+1$ é uma não-lacuna de Weierstrass em Q, escolha x tal que $div(x) = (q+1)(P_0 - Q)$, logo $v_Q(x) = -(q+1)$ e $v_P(x) \geq 0$ para todo $P \neq Q$, ou seja, $div(x)_\infty = (q+1)Q$. Agora o resultado segue da proposição (2.2.1).

□

A equivalência dada no lema acima, chamada de *equivalência fundamental*, é uma motivação para definirmos, sobre $\mathcal{X}$, a série linear completa

$$\mathcal{D}_{\mathcal{X}} := |(q+1)P_0|,$$

onde P_0 é um ponto racional de $\mathcal{X}$, que estaremos supondo fixado. É claro que $\mathcal{D}_{\mathcal{X}}$ não depende do ponto racional P_0 escolhido. Uma vez que $q+1$ é uma não-lacuna de Weierstrass em P_0 o exemplo (2.2.8) implica que $\mathcal{D}_{\mathcal{X}}$ é uma série linear livre de pontos base.

Seja n a dimensão da série $\mathcal{D}_{\mathcal{X}}$ e denote por $\varepsilon_1, \ldots, \varepsilon_n$ as ordens de $\mathcal{D}_{\mathcal{X}}$, $\nu_0, \ldots, \nu_{n-1}$ as ordens de Frobenius de $\mathcal{D}_{\mathcal{X}}$ e $j_0(P), \ldots, j_n(P)$ as ordens de $\mathcal{D}_{\mathcal{X}}$ no ponto P.

Teorema 5.1.6 *Seja $\mathcal{X}$ uma curva maximal definida sobre $\mathbb{F}_{q^2}$. Então,*

(a) $j_n(P) = q+1$ se P é um ponto racional de $\mathcal{X}$ e $j_n(P) = q$ caso contrário.

(b) $\varepsilon_n = \nu_{n-1} = q$. Em particular, todo ponto racional de $\mathcal{X}$ é um ponto de Weierstrass de $\mathcal{D}_{\mathcal{X}}$.

(c) $j_1(P) = 1$ para todo ponto P de $\mathcal{X}$. Em particular $\varepsilon_1 = 1$

Demonstração: (a) Seja $P \in \mathcal{X}$. Pelo lema (5.1.4) existe $f \in \bar{\mathbb{F}}_{q^2}(\mathcal{X})$ tal que $\mathrm{Fr}(P) + qP = (q+1)P_0 + div(f)$, logo $f \in \mathcal{L}((q+1)P_0)$ e

$$v_P((q+1)P_0) + v_P(f) = \begin{cases} q+1 & \text{se } P \in \mathcal{X}(\mathbb{F}_{q^2}) \\ q & \text{se } P \notin \mathcal{X}(\mathbb{F}_{q^2}). \end{cases}$$

Agora o resultado segue do item (c) da proposição (2.2.6) observando que não existem ordens em P superiores ao grau de $\mathcal{D}_{\mathcal{X}}$, que é $q+1$.

(b) Seja P um ponto não racional fora do suporte de $R(\mathcal{D}_{\mathcal{X}})$, então $j_n(P) = \varepsilon_n$ (item (c), cor. (3.2.5)) e portanto $\varepsilon_n = q$, pelo item (a). Agora mostraremos que $\varepsilon_n = \nu_{n-1}$. Se $f \in \mathbb{F}_q(\mathcal{X})$ é tal que

$$\mathrm{Fr}(P) + qP = (q+1)P_0 + div(f),$$

então $f \in \mathcal{L}((q+1)P_0)$ e $v_P((q+1)P_0) + v_P(f) = q$, logo $f = f_n$ onde $\mathcal{F} = \{f_0, \ldots, f_n\}$ é uma base P-hermitiana de alguma parametrização de $\mathcal{D}_{\mathcal{X}}$. Pelo lema (2.3.10) podemos supor que o hiperplano osculador $L^{\mathcal{F}}_{n-1}(P)$ em P é o hiperplano dado pelo equação $X_n = 0$, logo

$$\phi^*_{\mathcal{D}_{\mathcal{X}}}(L^{\mathcal{F}}_{n-1}(P)) = (q+1)P_0 + div(f_n) = \mathrm{Fr}(P) + qP.$$

Note que $\mathrm{Fr}(P)$ está no suporte de $\phi^*_{\mathcal{D}_{\mathcal{X}}}(L^{\mathcal{F}}_{n-1}(P))$, logo a proposição (2.3.5) implica que $(f_0 \circ \mathrm{Fr}(P), \ldots, f_n \circ \mathrm{Fr}(P)) \in L^{\mathcal{F}}_{n-1}(P)$. Pelo corolário (2.3.12) isto significa que o determinante

$$W(P) := det \begin{pmatrix} f_0 \circ \mathrm{Fr}(P) & \ldots & f_0 \circ \mathrm{Fr}(P) \\ f_0(P) & \ldots & f_n(P) \\ D_x^{\varepsilon_1} f_0(P) & \ldots & D_x^{\varepsilon_1} f_n(P) \\ \vdots & \ddots & \vdots \\ D_x^{\varepsilon_n - 1} f_0(P) & \ldots & D_x^{\varepsilon_n - 1} f_n(P) \end{pmatrix}$$

é nulo. [1] Em particular, a aplicação $W : \mathcal{X} \to \bar{\mathbb{F}}_q$ define uma função racional que se anula em todos os pontos fora do suporte de $R(\mathcal{D}_\mathcal{X})$, logo $W = 0$. Mas isto significa que existe i tal que $\varepsilon_i \neq \nu_i$ e pelo lema (3.3.2) isto implica que $\varepsilon_n = \nu_{n-1}$. Isto conclui a demonstração.

(c) Primeiramente suponha $P \in \mathcal{X}(\mathbb{F}_{q^2})$. Os itens (a) e (b) implicam que $j_n(P) = q + 1$ e $\nu_{n-1} = q$, respectivamente. O lema (3.3.7) implica que $q \leq q + 1 - j_1$, logo $j_1 = 1$. Agora suponha $P \notin \mathcal{X}(\mathbb{F}_{q^2})$ e escolha $Q \in \mathcal{X}$ tal que $\mathrm{Fr}(Q) = P$. Pelo lema (5.1.4), existe $f \in \mathcal{L}((q+1)P_0)$ tal que $P + qQ = \mathrm{Fr}(Q) + qQ = (q+1)P_0 + div(f)$, logo $v_P(f) = 1$ e portanto $j_1(P) = 1$. Uma vez que $0 < \varepsilon_1 \leq j_1(P)$, é claro que $\varepsilon_1 = 1$.

□

A próxima proposição fornece informações sobre ordens de $\mathcal{D}_\mathcal{X}$ e não-lacunas de Weierstrass em pontos de $\mathcal{X}$.

Proposição 5.1.7 *Seja $\mathcal{X}$ uma curva maximal definida sobre $\mathbb{F}_{q^2}$ e seja $(\eta_i(P))_{i\in\mathbb{N}_0^*}$ a sequência crescente das não-lacunas de Weierstrass no ponto $P \in \mathcal{X}$.*

(a) Se $P \in \mathcal{X}$ então $l(qP) = n$, ou seja,

$$\eta_{n-1}(P) \leq q < \eta_n(P).$$

(b) Se P não é um ponto racional de $\mathcal{X}$ então

$$0 \leq q - \eta_n(P) < \ldots < q - \eta_1(P) < q$$

são as ordens de $\mathcal{D}_\mathcal{X}$ em P.

(c) Se P é um ponto racional de $\mathcal{X}$ então

$$0 \leq q + 1 - \eta_n(P) < \ldots < q + 1 - \eta_1(P) < q + 1$$

são as ordens de $\mathcal{D}_\mathcal{X}$ em P. Ainda mais, se j é uma ordem em um ponto racional P então $q + 1 - j$ é uma não-lacuna de Weierstrass de P. Em particular, q e $q + 1$ são não-lacunas de Weierstrass em qualquer ponto racional de $\mathcal{X}$.

Demonstração: (a) Note que

$$\mathcal{L}(qP) \simeq \mathcal{L}((q+1)P_0 - \mathrm{Fr}(P)) \subsetneq \mathcal{L}((q+1)P_0).$$

[1] Aqui estamos usando que $v_P((q+1)P_0) = 0$, $\varepsilon_i = j_i(P)$ para todo i e que $j_0(P) = 0$ pois $\mathcal{D}_\mathcal{X}$ é livre.

De fato, o isomorfismo segue do lema (5.1.4) e do item (c) do lema (1.6.3). A inclusão estrita segue do fato que $j_0(\mathrm{Fr}(P)) = 0$, pois $\mathcal{D}_\mathcal{X}$ é livre. Por hipótese $l((q+1)P_0) = n+1$, logo $l(qP) = n$, pois a inclusão própria acima tem co-dimensão 1. A segunda parte é uma consequência do exemplo (2.2.8).

(b e c) Seja $P \in \mathcal{X}$ e seja η uma não-lacuna de Weierstrass de P com $\eta \leq q$. Se $f \in \mathbb{F}_{q^2}(\mathcal{X})$ é tal que $div(f)_\infty = \eta P$, então

$$div(f)_0 + div(f^{-1}) = div(f)_\infty = \eta P,$$

ou seja, $div(f)_0 \sim \eta P$. Somando o divisor $(q-\eta)P + \mathrm{Fr}(P)$ em ambos os lados desta equivalência obtemos

$$div(f)_0 + (q-\eta)P + \mathrm{Fr}(P) \sim qP + \mathrm{Fr}(P),$$

logo

$$div(f)_0 + (q-\eta)P + \mathrm{Fr}(P) \sim (q+1)P_0.$$

Uma vez que $div(f)_0$ e $(q-\eta)P$ são efetivos e $div(f)_0$ é disjunto de P, os itens (b) e (c) seguem rapidamente desta relação, da proposição (2.2.6) e do fato que $\mathrm{Fr}(P) = P$ se, e somente se, P é $\mathbb{F}_{q^2}$-racional. A segunda parte de (c) é trivial lembrando que 0 e 1 são ordens de $\mathcal{D}_\mathcal{X}$ em P.

□

Corolário 5.1.8 *A série linear $\mathcal{D}_\mathcal{X}$ é simples.*

Demonstração: Seja P_0 um ponto $\mathbb{F}_{q^2}$-racional e seja $\phi := \phi_{\mathcal{D}_\mathcal{X}}$ o morfismo associado a $\mathcal{D}_\mathcal{X}$. Pelo item (c) da proposição (5.1.7) podemos escolher $x, y \in \mathbb{F}_{q^2}(\mathcal{X})$ tais que $div(x)_\infty = qP_0$ e $div(y)_\infty = (q+1)P_0$. Note que as funções x, y definem inclusões $\bar{\mathbb{F}}_{q^2}(x) \hookrightarrow \bar{\mathbb{F}}_{q^2}(\mathcal{X})$ e $\bar{\mathbb{F}}_{q^2}(y) \hookrightarrow \bar{\mathbb{F}}_{q^2}(\mathcal{X})$ tais que $[\bar{\mathbb{F}}_{q^2}(\mathcal{X}) : \bar{\mathbb{F}}_{q^2}(x)] = q$ e $[\bar{\mathbb{F}}_{q^2}(\mathcal{X}) : \bar{\mathbb{F}}_{q^2}(y)] = q+1$ (item (b), teo. (1.4.2)), logo $[\bar{\mathbb{F}}_{q^2}(\mathcal{X}) : \bar{\mathbb{F}}_{q^2}(\phi(\mathcal{X}))] = 1$ e portanto $\mathcal{X}$ e $\phi(\mathcal{X})$ são birracionais.

□

5.2 A Curva Hermitiana

Um exemplo importante de curva maximal é a curva Hermitiana $\mathcal{H}$ cuja equação é dada pelo polinômio homogêneo

$$f(X,Y,Z) = Y^q Z + Y Z^q - X^{q+1} \in \mathbb{F}_{q^2}[X,Y,Z].$$

Não é difícil verificar que $\mathcal{H}$ é uma curva plana não-singular cujo gênero é igual a $q(q-1)/2$. Note que $(0:1:0)$ é o único ponto no infinito sobre $\mathcal{H}$. Os pontos afins de $\mathcal{H}$ são os pontos $(a:b:1)$, com $(a,b) \in \bar{\mathbb{F}}_{q^2} \times \bar{\mathbb{F}}_{q^2}$, tais que

$$b^q + b = a^{q+1}.$$

Note que se $a \in \mathbb{F}_{q^2}$ então $b \in \mathbb{F}_{q^2}$. Uma vez que $Y^q + Y - a^{q+1}$ define um polinômio irredutível e separável, a equação $Y^q + Y = a^{q+1}$ admite exatamente q soluções distintas, cada uma das quais pertence a $\mathbb{F}_{q^2}$. Portanto

$$\#\mathcal{H}(\mathbb{F}_{q^2}) = q^3 + 1 = 1 + q^2 + 2q \cdot \frac{q(q-1)}{2},$$

ou seja, $\mathcal{H}$ atinge a cota superior de Hasse-Weil e portanto é de fato uma curva maximal. Note que a dimensão da série $\mathcal{D}_{\mathcal{H}}$ é 2. De fato, caso contrário a cota de Castelnuovo aplicada a série $\mathcal{D}_{\mathcal{H}}$ iria fornecer $g \leq (q-1)^2/4$, o que é um absurdo.

O que faremos nesta seção é mostrar que a curva Hermitiana $\mathcal{H}$ é a *única* curva maximal, definida sobre $\mathbb{F}_{q^2}$, cujo gênero é $q(q-1)/2$. A idéia é mostrar que $\mathcal{H}$ é a única curva tal que a dimensão de $\mathcal{D}_{\mathcal{H}}$ é 2. A partir disto, é possível mostrar que dada uma curva maximal $\mathcal{X}$ de gênero maior que $(q-1)^2/4$, existem geradores $x, y \in \mathbb{F}_{q^2}(\mathcal{X})$ que satisfazem $y^q + y = x^{q+1}$, logo poderemos concluir que $\mathcal{H}$ e $\mathcal{X}$ são $\mathbb{F}_{q^2}$-isomorfas. O próximo lema é a chave para esta demonstração e é uma aplicação direta dos resultados obtidos na seção precedente.

Lema 5.2.1 *Seja $\mathcal{X}$ uma curva maximal sobre $\mathbb{F}_{q^2}$ e suponha que a dimensão de $\mathcal{D}_{\mathcal{X}} = |(q+1)P_0|$ é 2. Sejam $x, y \in \mathbb{F}_{q^2}(\mathcal{X})$ tais que*

$$div(x)_\infty = qP_0 \quad e \quad div(y)_\infty = (q+1)P_0.$$

Então existe $f \in \mathbb{F}_{q^2}(\mathcal{X})$ tal que $f^q = D_x^1 y$, $div(f)_\infty = qP_0$ e

$$(y - y^{q^2}) = f^q(x - x^{q^2}).$$

Demonstração: Primeiramente note que o item (c) da proposição (5.1.7) implica que q e $q+1$ são não-lacunas de P_0, logo sempre existem elementos $x, y \in \mathbb{F}_{q^2}(\mathcal{X})$ satisfazendo $div(x)_\infty = qP_0$ e $div(y)_\infty = (q+1)P_0$. O teorema (5.1.6) garante que

$$\varepsilon = (\varepsilon_1, \varepsilon_2) = (1, q) \quad \text{e} \quad \nu = (\nu_0, \nu_1) = (0, q).$$

Defina $\mathcal{F} = \{1, x, y\}$, $m = (0, 1)$ e observe que x é um elemento de separação de $\mathbb{F}_q(\mathcal{X})$, [2] logo

$$V_{m,x}^{\mathcal{F}} = det \begin{pmatrix} 1 & x^{q^2} & y^{q^2} \\ 1 & x & y \\ 0 & 1 & D_x y \end{pmatrix} = (x - x^{q^2}) D_x^1 y - (y - y^{q^2}),$$

portanto

$$(y - y^{q^2}) = D_x^1 y (x - x^{q^2}), \tag{5.1}$$

[2] De fato, caso contrário existiria $z \in \mathbb{F}_q(\mathcal{X})$ tal que $x = z^p$ (teo. (1.2.5), logo $qP_0 = div(x)_\infty = p div(z)_\infty$ e portanto $div(z)_\infty = q/pP_0$, ou seja, q/p é uma não-lacuna de P_0, isto é uma contradição.

pois $m < \nu$. Pela proposição (2.3.3), para mostrar a existência de um elemento f satisfazendo $f^q = D_x y$, é suficiente mostrar que

$$D_x^i(D_x y) = 0 \text{ para todo } \quad i = 0, \ldots, q-1. \tag{5.2}$$

Isto será feito por indução. Aplicando D_x na equação (5.1), usando a regra do produto para os diferenciais de Hasse e a proposição (2.3.3), se obtém

$$(x - x^{q^2}) D_x D_x y \quad = \quad 0,$$

logo $D_x D_x y = 0$ e (5.2) vale para $i = 1$. Suponha que (5.2) vale para todo $i = 1, \ldots, j$ com $1 \leq j \leq q-2$. Devemos mostrar que (5.2) vale também para $i = j+1$. De fato, aplicando D_x^{j+1} em (5.1) e usando a hipótese de indução se obtém

$$(x - x^{q^2}) D_x^{j+1} D_x y = D_x^{j+1} y.$$

Agora observe que

$$W^{\mathcal{F}}_{\varepsilon,1,x} \quad = \quad det \begin{pmatrix} 1 & x & y \\ 0 & 1 & D_x^1 y \\ 0 & 0 & D_x^q y \end{pmatrix} = D_x^q y,$$

logo $D_x^s y = 0$ sempre que $1 < s < q$. Em particular, $D_x^{j+1} y = 0$ pois $j+1 < q$, logo $D_x^{j+1}(D_x y) = 0$ e (5.2) vale também para $i = j+1$. Agora mostraremos que $div(f)_\infty = qP_0$. Aplicando a valorização v_{P_0} na equação (5.1) e usando as definições de x e y se obtém $v_{P_0}(D_x^1) = -q^2$. A partir disto é possível concluir que $v_{P_0}(dx) = q^2 - q - 2$. [3] Agora, x é regular em todo ponto P diferente de P_0, logo $v_P(dx) \geq 0$, portanto

$$2g - 2 = deg(dx) = \sum_{P \neq P_0} v_P(dx) + v_{P_0}(dx) \geq v_{P_0}(dx) = q^2 - q - 2. \tag{5.3}$$

Uma manipulação simples desta igualdade mostra que $g \geq q(q-2)/2$, portanto $g = q(q-2)/2$ (prop. (5.1.3)). Substituindo este valor na expressão (5.3) se obtém

$$q^2 - q - 2 = \sum_{P \neq P_0} v_P(dx) + v_{P_0}(dx) = \sum_{P \neq P_0} v_P(dx) + q^2 - q - 2,$$

logo $v_P(dx) = 0$ sempre que $P \neq P_0$, portanto

$$v_P(f) = q^{-1} v_P(D_x^1 y) = q^{-1} v_P(dy) \geq 0,$$

ou seja, $v_{P_0}(f) = -q$ e $v_P(f) \geq 0$ para $P \neq P_0$. Portanto $div(f)_\infty = qP_0$ e a demonstração está concluída.

[3] De fato, seja t um parâmetro local de P_0, pela regra da cadeia temos que $D_t^1 y = D_t^1 x D_x^1 y$, logo $v_{P_0}(dx) = q^2 + v_{P_0}(dy)$, observando que y^{-1} satisfaz as hipóteses do item (d) do teorema (1.5.3), vemos rapidamente que $v_{P_0}(d(y^{-1}) = q$. Por outro lado, a identidade $d(y^{-1})/dt = -y^{-2} dy/dt$ implica $v_{P_0}(dy) = v_{P_0}(d(y^{-1})) + 2v_{P_0}(y) = -q - 2$. Isto demonstra a afirmação.

□

Teorema 5.2.2 *Seja $\mathcal{X}$ uma curva maximal de gênero g e definida sobre $\mathbb{F}_{q^2}$. Suponha que a dimensão da série $\mathcal{D}_{\mathcal{X}}$ é N. São equivalentes:*

(a) $\mathcal{X}$ é isomorfa sobre $\mathbb{F}_{q^2}$ a curva Hermitiana $\mathcal{H}$.

(b) $g > (q-1)^2/4$.

(c) $N = 2$.

Demonstração: Já é conhecido que o gênero de $\mathcal{H}$ é $q(q-1)/2$, logo (a) implica (b). Assuma (b) e suponha que $N \geq 3$. A cota de Castelnuovo aplicada a série $\mathcal{D}_{\mathcal{X}}$ fornece $g \leq (q-1)^2/4$, o que contradiz a hipótese. Para demonstrar que (c) implica (a) usaremos o lema anterior, logo estaremos supondo as mesmas notações. O lema anterior garante a existência de um elemento $f \in \mathbb{F}_{q^2}(\mathcal{X})$ tal que $f^q = D_x y$, $div(f)_\infty = qP_0$ e

$$(y - y^{q^2}) = f^q(x - x^{q^2}), \tag{5.4}$$

onde x é um elemento de separação de $\mathbb{F}_q(\mathcal{X})/\mathbb{F}_q$ tal que $div(x)_\infty = qP_0$, ou seja, $div(f)_\infty = div(x)_\infty$, logo $f, x \in \mathcal{L}(qP_0) \subsetneq \mathcal{L}((q+1)P_0)$ e portanto $f = ax + b$ com $a, b \in \mathbb{F}_{q^2}$. Substituindo estes valores na equação (5.4) se obtém

$$(y_1^q + y_1 - x_1^{q+1})^q = y_1^q + y_1 - x_1^{q+1},$$

onde $x_1 = ax + b$ e $y_1 = ay$, logo $y_1^q + y_1 - x_1^{q+1} = c \in \mathbb{F}_q$ e portanto

$$y_2^q + y_2 - x_1^{q+1} = 0,$$

onde $y_2 = y_1 + \alpha$ e $\alpha^q + \alpha = c$, logo $\mathcal{X}$ e $\mathcal{H}$ são birracionais e portanto são $\mathbb{F}_{q^2}$-isomorfas, pois ambas são não-singulares (teo. 1.3.8). Isto conclui a demonstração.

□

O próximo corolário é uma importante e imediata consequência deste teorema.

Corolário 5.2.3 *Se o gênero g de uma curva maximal $\mathcal{X}$ definida sobre $\mathbb{F}_{q^2}$ satisfaz $g > (q-1)^2/4$, então $g = q(q-1)/2$.*

□

Exemplo 5.2.4 *Seja $\mathcal{X}$ a curva dada pelo polinômio homogêneo*

$$F(X,Y,Z) = X^{q+1} + Y^{q+1} - Z^{q+1} \in \mathbb{F}_{q^2}[X,Y,Z].$$

Esta é uma curva projetiva, plana, não-singular e com gênero $g = q(q-1)/2$. Os pontos no infinito de $\mathcal{X}$ são os pontos $P = (a : b : 0)$ tais que

$$a^{q+1} + b^{q+1} = 0,$$

assim $b \neq 0$ e podemos assumir $b = 1$, ou seja, $P = (a : 1 : 0)$, onde a é solução de $X^{q+1} + 1 = 0$. Portanto existem $q+1$ pontos $\mathbb{F}_{q^2}$-racionais no infinito de $\mathcal{X}$. Os pontos $\mathbb{F}_{q^2}$-racionais afins de $\mathcal{X}$ são os pontos $(a : b : 1)$ tais que $(a,b) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ e

$$a^{q+1} + b^{q+1} = 1.$$

Se $a^{q+1} = 1$ então $b = 0$ e portanto existe um único ponto tal que $F(a,b,1) = 0$. Se $a^{q+1} \neq 1$, então b é solução de $Y^{q+1} + a^{q+1} - 1 = 0$. Neste caso, existem $q+1$ pontos $(a,b) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ tais que $F(a,b,1) = 0$. A partir disto é possível concluir que

$$\#\mathcal{X}(\mathbb{F}_{q^2}) = q^3 + 1 = 1 + q^2 + 2q \cdot \frac{q(q-1)}{2},$$

logo $\mathcal{X}$ é maximal com gênero $g > (q-1)^2/4$. Portanto, pelo teorema (5.2.2), $\mathcal{X}$ e $\mathcal{H}$ são $\mathbb{F}_{q^2}$-isomorfas.

Apêndice A

Noções da Teoria de Corpos de Funções

Neste apêndice destacaremos algumas definições e resultados da teoria de corpos de funções e que são usados ao longo desta dissertação. Para cobrir os detalhes recomendamos as referências [25], [20] e [10].

A.1 Corpos de Funções e Anéis Locais

Seja K um corpo perfeito.

Definição A.1.1 *Um **corpo de funções** em uma variável sobre o corpo K é um corpo L contendo K e no mínimo um elemento x, transcendente sobre K, tal que $L/K(x)$ é uma extensão algébrica finita. Se K é algebricamente fechado em L, então K é chamado de o **corpo de constantes** de L.*

Estaremos sempre supondo que K é o corpo de constantes de L.

Definição A.1.2 *Seja L/K um corpo de funções algébricas. Um **anel de valorização** de L é um anel $\mathcal{O}$ tal que :*

(i) $K \subsetneq \mathcal{O} \subsetneq L$

(ii) para todo $a \in L$, $a \in \mathcal{O}$ ou $a^{-1} \in \mathcal{O}$

Teorema A.1.3 *Seja $\mathcal{O}$ um anel de valorização do corpo de funções L/K.*

(a) O anel $\mathcal{O}$ é um anel local cujo único ideal maximal é $\mathcal{P} := \mathcal{O} \backslash \mathcal{O}^*$.

(b) $\mathcal{P}$ é um ideal principal.

(c) Se $\mathcal{P} = t\mathcal{O}$ então todo elemento $a \in L^*$ admite uma única representação $a = t^n u$, onde $n \in \mathbb{Z}$ e $u \in \mathcal{O}^*$.

(d) Se $\mathcal{P} = t\mathcal{O}$ e $I \subseteq \mathcal{O}$ é um ideal não nulo, então existe $n \in \mathbb{N}$ tal que $I = t^n\mathcal{O}$.

Definição A.1.4 *Um **lugar** $\mathcal{P}$ do corpo de funções L/K é o ideal maximal de algum anel de valorização $\mathcal{O}$ de L/K. Um elemento $t \in L$ tal que $\mathcal{P} = t\mathcal{O}$ é chamado de **elemento primo** de $\mathcal{P}$ ou de **parâmetro local** para $\mathcal{P}$. Para cada $a \in L^*$ definimos a **multiplicidade** de a em $\mathcal{P}$ como sendo o único inteiro n tal que $a = t^n u$, onde $u \in \mathcal{O}^*$. Neste caso, usamos a notação $v_{\mathcal{P}}(a) = n$. Por convenção, $v_{\mathcal{P}}(0) = \infty$.*

O símbolo ∞ representa um elemento não pertencente a $\mathbb{Z}$ tal que $\infty+\infty = \infty+n = n+\infty = \infty > m$ para todo $m, n \in \mathbb{Z}$. Note que para todo $a \in \mathcal{O}$, $v_{\mathcal{P}}(a)$ é o maior inteiro n tal que $a \in \mathcal{P}^n$. Por outro lado, se $a^{-1} \in \mathcal{O}$, então $v_{\mathcal{P}}(a) = -n$, onde n é o maior inteiro tal que $a^{-1} \in \mathcal{P}^n$.

Observe que a definição depende somente de $\mathcal{P}$ e não da escolha do elemento primo t. De fato, se t' é outro elemento primo de $\mathcal{P}$ então $\mathcal{P} = t\mathcal{O} = t'\mathcal{O}$ e assim $t = t'v$ para algum $v \in \mathcal{O}^*$. Deste modo, $t^n u = t'^n(v^n u)$ com $v^n u \in \mathcal{O}^*$.

Teorema A.1.5 *Seja $\mathcal{O}$ um anel de valorização de L/K cujo único ideal maximal é $\mathcal{P}$. Então*

(a) $v_{\mathcal{P}}(ab) = v_{\mathcal{P}}(a) + v_{\mathcal{P}}(b)$ para todo $a, b \in L$.

(b) $v_{\mathcal{P}}(a+b) \geq min\{v_{\mathcal{P}}(a), v_{\mathcal{P}}(b)\}$ para todo $a, b \in L$.

(c) Existe um elemento $a \in L$ tal que $v_{\mathcal{P}}(a) = 1$.

(d) $v_{\mathcal{P}}(a) = 0$ sempre que $a \in K^*$.

(e) Se $v_{\mathcal{P}}(a) \neq v_{\mathcal{P}}(b)$, então $v_{\mathcal{P}}(a+b) = min\{v_{\mathcal{P}}(a), v_{\mathcal{P}}(b)\}$ para todo $a, b \in L$.

(f) $\mathcal{O} = \{a \in L \ ; \ v_{\mathcal{P}}(a) \geq 0\}$.

(g) $\mathcal{O}^* = \{a \in L \ ; \ v_{\mathcal{P}}(a) = 0\}$.

(h) $\mathcal{P} = \{a \in L \ ; \ v_{\mathcal{P}}(a) > 0\}$.

(i) $t \in L^*$ é um elemento primo de $\mathcal{P}$ se, e somente se, $v_{\mathcal{P}}(t) = 1$.

Observe que $v_{\mathcal{P}}$ é uma função definida em L e tomando valores em $\mathbb{Z} \cup \{\infty\}$. A aplicação $v_{\mathcal{P}}$ é chamada de *valorização* (*discreta*) de $\mathcal{P}$. No teorema anterior, os itens $(f), (g)$ e (h) mostram que os conjuntos $\mathcal{O}, \mathcal{P}$ e $\mathcal{O}^*$ são inteiramente determinados pela valorização $v_{\mathcal{P}}$. Note também que o anel de valorização $\mathcal{O}$ de L/K é completamente determinado por seu único ideal maximal $\mathcal{P}$, pois

$$\mathcal{O} = \{x \in L \ ; \ x^{-1} \notin \mathcal{P}\}.$$

Por esta razão, usa-se a notação $\mathcal{O}_{\mathcal{P}}$ e diz-se que este anel é o *anel de valorização do lugar* $\mathcal{P}$.

Teorema A.1.6 (Aproximação Fraca) *Seja L/K um corpo de funções e sejam $\mathcal{P}_1, \ldots, \mathcal{P}_n$ lugares em L dois a dois distintos. Escolha n elementos $x_1, \ldots, x_n \in L$ e n inteiros $m_1, \ldots, m_n \in \mathbb{Z}$. Então existe $x \in L$ tal que*

$$v_{\mathcal{P}_i}(x - x_i) = m_i \text{ para } i = 1, \ldots, n.$$

A.2 Extensão de Corpos de Funções

Nesta seção serão consideradas extensões L'/L, onde L' e L são ambos corpos de funções.

Definição A.2.1 *(a) Um corpo de funções L'/K' é chamado uma* ***extensão algébrica*** *de L/K se L' é uma extensão algébrica de L e $K' \supseteq K$.*

(b) A extensão algébrica L'/K' de L/K é chamada ***extensão finita*** *se $[L' : L] < \infty$.*

(c) Dada uma extensão algébrica L'/K' de L/K, dizemos que um lugar $\mathcal{P}'$ de L' é ***sobre*** *um lugar $\mathcal{P}$ de L se $\mathcal{P} \subseteq \mathcal{P}'$. Neste caso, a notação $\mathcal{P}'|\mathcal{P}$ é usada.*

Proposição A.2.2 *Seja L'/K' uma extensão de algébrica de L/K.*

(a) Para cada lugar $\mathcal{P}'$ de L' existe um único lugar $\mathcal{P}$ de L tal que $\mathcal{P}'|\mathcal{P}$, a saber $\mathcal{P} = \mathcal{P}' \cap L$.

(b) Para cada lugar $\mathcal{P}$ de L existe apenas um número finito de lugares $\mathcal{P}'$ em L' tal que $\mathcal{P}'|\mathcal{P}$.

O que faremos agora é associar dois inteiros a esta situação. Note que se $\mathcal{P}'|\mathcal{P}$ então $\mathcal{P}\mathcal{O}_{\mathcal{P}'}$ é um ideal não nulo de $\mathcal{O}_{\mathcal{P}'}$ contido em $\mathcal{P}'$, logo, pelo teorema (A.1.3), existe um inteiro $e \geq 1$ tal que $\mathcal{P}\mathcal{O}_{\mathcal{P}'} = t^e\mathcal{O}_{\mathcal{P}'}$, onde t é um parâmetro local de $\mathcal{P}'$. Este inteiro e é mínimo com esta propriedade, não depende do parâmetro t e satisfaz a igualdade $v_{\mathcal{P}'}(a) = ev_{\mathcal{P}}(a)$, para todo $a \in L$. Note também que $\mathcal{O}_P/\mathcal{P} \hookrightarrow \mathcal{O}_{\mathcal{P}'}/\mathcal{P}'$ via $x + \mathcal{P} \mapsto x + \mathcal{P}'$.

Definição A.2.3 *Seja L'/K' uma extensão algébrica de L/K e suponha que $\mathcal{P}'|\mathcal{P}$.*

(a) O ***grau relativo*** *$e(\mathcal{P}'|\mathcal{P})$ de $\mathcal{P}'$ sobre $\mathcal{P}$ é o único inteiro e tal que $\mathcal{P}\mathcal{O}_{\mathcal{P}'} = t^e\mathcal{O}_{\mathcal{P}'}$.*

(b) O ***índice de ramificação*** *$f(\mathcal{P}'|\mathcal{P})$ de $\mathcal{P}'$ sobre $\mathcal{P}$ é a dimensão de $\mathcal{O}_{\mathcal{P}'}/\mathcal{P}'$ como espaço vetorial sobre o corpo $\mathcal{O}_{\mathcal{P}}/\mathcal{P}$, ou seja, $f(\mathcal{P}'|\mathcal{P}) = [\mathcal{O}_{\mathcal{P}'}/\mathcal{P}' : \mathcal{O}_{\mathcal{P}}/\mathcal{P}]$.*

O índice de ramificação e o grau relativo tem um bom comportamento com relação a torre de extensões. Mais precisamente, suponha que $L \subseteq L' \subseteq L''$ são corpos de funções tais que L''/L' e L'/L são ambas extensões finitas. Se $\mathcal{P}''$ é um lugar de L'' que está sobre os lugares $\mathcal{P}'$ e $\mathcal{P}$ de L' e L, respectivamente, então $e(\mathcal{P}''|\mathcal{P}) = e(\mathcal{P}''|\mathcal{P}')e(\mathcal{P}'|\mathcal{P})$ e $f(\mathcal{P}''|\mathcal{P}) = f(\mathcal{P}''|\mathcal{P}')f(\mathcal{P}'|\mathcal{P})$. Ambas as relações seguem rapidamente das definições.

Definição A.2.4 *Seja L'/K' uma extensão algébrica de L/K e suponha que $\mathcal{P}'|\mathcal{P}$. O lugar $\mathcal{P}$ é* ***não-ramificado*** *em L' se $e(\mathcal{P}'|\mathcal{P}) = 1$. Caso contrário, $\mathcal{P}$ é* ***ramificado*** *em L'.*

Dada uma extensão algébrica L'/K' de L/K, existem inúmeras propriedades relativas ao índice de ramificação dos lugares de L sobre os lugares de L'. Dentre as quais, destacamos que se L'/L é uma

extensão finita e separável, então o número de lugares de L que são ramificados em L' é sempre finito. Este importante resultado é consequência da teoria do *different*. Um tratamento detalhado pode ser encontrado em ([25], III.5.5(b), pag.95).

Teorema A.2.5 *Seja L'/K' uma extensão algébrica de L/K e suponha que L' é uma extensão algébrica finita de L cujo grau é n. Suponha que $\mathcal{P}$ é um lugar de L e que $\mathcal{P}_1, \ldots, \mathcal{P}_m$ são todos os lugares de L' que estão sobre $\mathcal{P}$. Então*

$$\sum_{i=1}^{m} e_i f_i = n,$$

onde e_i e f_i são, respectivamente, o índice de ramificação e o grau relativo de $\mathcal{P}_i$ sobre $\mathcal{P}$.

Proposição A.2.6 *Seja L'/L uma extensão finita e Galois tal que L' e L são corpos de funções sobre K. Considere um automorfismo $\sigma \in Gal(L'/L)$. Se $\mathcal{P}'$ é um lugar em L' tal que $\mathcal{P}'|\mathcal{P}$, então:*

(a) $\sigma(\mathcal{O}_{\mathcal{P}'}) := \{\sigma(x)\ ;\ x \in \mathcal{O}_{\mathcal{P}'}\}$ é anel de valorização em L'.

(b) $\sigma(\mathcal{P}') := \{\sigma(x)\ ;\ x \in \mathcal{P}'\}$ é um lugar em L'.

(c) $\sigma(\mathcal{P}')|\mathcal{P}$

(d) $v_{\sigma(\mathcal{P}')}(y) = v_{\mathcal{P}'}(\sigma^{-1}(y))\ \forall\ y \in L'$.

Demonstração: É claro que $\sigma(\mathcal{O}_{\mathcal{P}'})$ é um anel de valorização e $\sigma(\mathcal{P}')$ é seu ideal maximal, logo $\sigma(\mathcal{P}')$ é um lugar em L' que corresponde ao anel $\mathcal{O}_{\sigma(\mathcal{P}')} = \sigma(\mathcal{O}_{\mathcal{P}'})$. Se t' é um elemento primo de $\mathcal{P}'$, então $\mathcal{P}' = t'\mathcal{O}_{\mathcal{P}'}$ e portanto $\sigma(\mathcal{P}') = \sigma(t')\sigma(\mathcal{O}_{\mathcal{P}'})$, ou seja, $\sigma(t')$ é um elemento primo de $\sigma(\mathcal{P})$. Isto demonstra (a) e (b). Para obter (c) basta observar que $\mathcal{P} = \sigma(\mathcal{P}) \subseteq \sigma(P')$. Para obter (d) escolha um elemento não nulo $y \in L'$ e suponha que $u = \sigma(z)$ com $z = t'^r u$, onde $r = v_{\mathcal{P}'}(z)$ e $u \in \mathcal{O}_{\mathcal{P}'} \backslash \mathcal{P}'$, logo $y = \sigma(t')^r \sigma(u)$, onde $\sigma(u) \in \mathcal{O}_{\sigma(\mathcal{P}')} \backslash \sigma(\mathcal{P}')$ e $\sigma(t')$ é um elemento primo de $\sigma(\mathcal{P}')$. Portanto $v_{\sigma(\mathcal{P}')}(y) = r = v_{\mathcal{P}'}(z) = v_{\mathcal{P}'}(\sigma^{-1}(y))$. Isto conclui a demonstração.

□

Teorema A.2.7 *Sejam L'/K' uma extensão de L/K tal que L'/L é uma extensão finita e Galois. Suponha que $\mathcal{P}_1$ e $\mathcal{P}_2$ são lugares em L' sobre um lugar $\mathcal{P}$ de L. Então $\mathcal{P}_2 = \sigma(\mathcal{P}_1)$ para algum $\sigma \in Gal(L'/L)$. Em outras palavras, o grupo de Galois age transitivamente sobre o conjunto das extensões de $\mathcal{P}$.*

Demonstração: Pelo teorema da aproximação fraca (A.1.6), existe $x \in L'$ tal que $v_{\mathcal{P}_1}(x) = 1$ e $v_{\mathcal{P}'}(x) = 0$ para qualquer $\mathcal{P}' \in L'$ que é sobre $\mathcal{P}$. Em particular,

$$v_{\mathcal{P}'}(\sigma(x)) = \begin{cases} 1 & \text{se } \sigma^{-1}(\mathcal{P}') = \mathcal{P}_1 \\ 0 & \text{caso contrário.} \end{cases}$$

Seja $y := \prod_{\sigma \in Gal(L'/L)} \sigma(x)$. Então

$$v_{\mathcal{P}'}(y) = \sum_{\sigma \in Gal(L'/L)} v_{\mathcal{P}'}(\sigma(x))$$

para todo $\mathcal{P}'|\mathcal{P}$, logo $v_{\mathcal{P}'}(y) > 0$ se, e somente se, $\sigma^{-1}(\mathcal{P}') = \mathcal{P}_1$ para algum $\sigma \in Gal(L'/L)$. Agora, y é fixo pelo Galois, logo $y \in \mathcal{P}_1 \cap L = \mathcal{P}$ e portanto $v_{\mathcal{P}'}(y) > 0$. Isto conclui a demonstração.

□

Corolário A.2.8 *Com as hipóteses do teorema (A.2.7), sejam $\mathcal{P}_1, \ldots, \mathcal{P}_r$ todos os lugares de L' que estão sobre $\mathcal{P}$, então*

(a) $e(\mathcal{P}_i|\mathcal{P}) = e(\mathcal{P}_j|\mathcal{P})$ e $f(\mathcal{P}_i|\mathcal{P}) = f(\mathcal{P}_j|\mathcal{P})$ para todos i, j. Deste modo, podemos definir

$$e(\mathcal{P}) := e(\mathcal{P}_i|\mathcal{P}) \quad e \quad f(\mathcal{P}) := f(\mathcal{P}_i|\mathcal{P}),$$

(b) $e(\mathcal{P}) \cdot f(\mathcal{P}) \cdot r = [L' : L]$. Em particular, os números $e(\mathcal{P})$, $f(\mathcal{P})$ e r dividem o grau $[L' : L]$.

Demonstração: (a) é evidente do teorema anterior e da proposição (A.2.6) . O item (b) é uma consequência de (a) e da igualdade $\sum_{i=1}^{r} e_i f_i = [L' : L]$.

□

Seja L/K um corpo de funções. Para qualquer extensão K' de K considere o compositum [1] LK' de L e K'. Por definição L é uma extensão de K finitamente gerada e com grau de transcendência igual a 1, logo LK' é também uma extensão de K' finitamente gerada e com grau de transcendência igual a 1. Portanto LK' é um corpo de funções sobre K'. Em particular,

$$LK' \simeq K' \otimes_K L.$$

Isto segue do fato que o corpo K é perfeito ([10], 2.5.4, pag.54).

Proposição A.2.9 *Seja L'/K' uma extensão algébrica finita de L/K tal que $L' = LK'$, então todo lugar de L é não-ramificado em L'.*

Corolário A.2.10 *Seja L'/K' uma extensão algébrica finita de L/K tal que $L' = LK'$. Se $\mathcal{P}'$ é um lugar em L' sobre o lugar $\mathcal{P}$ em L, então todo parâmetro local de $\mathcal{P}$ é também um parâmetro local de $\mathcal{P}'$.*

Demonstração: $\mathcal{P}$ é não-ramificado em L', logo $e(\mathcal{P}'|\mathcal{P}) = 1$ e portanto $v_{\mathcal{P}'}(t) = v_{\mathcal{P}}(t)$ para todo $t \in L$. Em particular, se t é um parâmetro local para $\mathcal{P}$ então $v_{\mathcal{P}'}(t) = v_{\mathcal{P}}(t) = 1$ e portanto t é também um parâmetro local para $\mathcal{P}'$.

□

[1] O compositum entre dois corpos é por definição o menor corpo contendo ambos.

Apêndice B

A Aplicação de Frobenius

Neste apêndice iremos descrever algumas propriedades da aplicação de Frobenius sobre uma curva $\mathcal{X}$ (não-singular e projetiva) definida sobre um corpo perfeito k de característica p.

Seja q uma potência de p. Para cada polinômio $F \in I_{\mathcal{X}}$, seja F^q o polinômio obtido de F elevando seus coeficientes a q-ésima potência. Deste modo, fica definida uma nova curva não-singular $\mathcal{X}^q$ cujo ideal é dado por

$$I_{\mathcal{X}^q} := \{F^q \ ; \ F \in I_{\mathcal{X}}\}.$$

Considere o morfismo

$$\begin{array}{rcl} \mathrm{Fr} : \mathcal{X} & \longrightarrow & \mathcal{X}^q \\ (x_0 : \ldots : x_n) & \longmapsto & (x_0^q : \ldots : x_n^q). \end{array}$$

Para ver que Fr realmente aplica sobre $\mathcal{X}^q$ é suficiente verificar que, para cada $P \in \mathcal{X}$, o ponto $\mathrm{Fr}(P)$ é um zero de cada gerador F^q de $I_{\mathcal{X}^q}$. De fato, se $P = (a_0 : \ldots : a_n)$ então

$$\begin{array}{rcl} F^q(\mathrm{Fr}(P)) & = & F^q(a_0^q, \ldots, a_n^q) \\ & = & (F(a_0, \ldots, a_n))^q \\ & = & 0 \end{array}$$

logo $\mathrm{Fr}(P) \in \mathcal{X}^q$ e portanto Fr é bem definido. Note que o morfismo Fr é injetor, portanto é uma bijeção, pois é não-constante (teo. 1.3.4).

Note que se k é o corpo finito $\mathbb{F}_q$, com q elementos, então cada gerador $F \in I_{\mathcal{X}}$ satisfaz $F = F^q$, logo $\mathcal{X} = \mathcal{X}^q$. Ainda neste caso, o conjunto $\mathcal{X}(\mathbb{F}_{q^r})$ dos pontos $\mathbb{F}_{q^r}$-racionais é caracterizado por

$$\mathcal{X}(\mathbb{F}_{q^r}) = \{P \in \mathcal{X} \ ; \ \mathrm{Fr}^r(P) = P\},$$

onde $\mathrm{Fr}^r = \mathrm{Fr} \circ \cdots \circ \mathrm{Fr}$ $(r\times)$. Em particular, todos os pontos $\mathbb{F}_q$-racionais são fixos por Fr.

Definição B.0.11 *A aplicação* $\mathrm{Fr} : \mathcal{X} \to \mathcal{X}^q$ *definida acima é chamada de* q-***ésima aplicação de Frobenius***.

Conforme foi demonstrado acima, a aplicação de Frobenius Fr é uma bijeção, mas não é um isomorfismo, conforme será demonstrado na próxima proposição.

Proposição B.0.12 *Seja* $\mathcal{X}$ *uma curva definida sobre o corpo* k *de característica* p *e seja* $\mathrm{Fr} : \mathcal{X} \to \mathcal{X}^q$ *a* q*-ésima aplicação de Frobenius, onde* q *é uma potência de* p*. Então,*

(a) $\mathrm{Fr}^* k(\mathcal{X}^q) = k(\mathcal{X})^q$.

(b) Fr *é puramente inseparável (i.e.,* $k(\mathcal{X})/\mathrm{Fr}^* k(\mathcal{X}^q)$ *é puramente inseparável.)*[1]

(c) $deg(\mathrm{Fr}) = q$.

(d) Todo ponto de $\mathcal{X}$ *é ramificado por* Fr*. Mais precisamente,* $e_{\mathrm{Fr}}(P) = q$ *para cada* $P \in \mathcal{X}$.

Demonstração: (a) Os elementos de $k(\mathcal{X})$ podem ser descritos como quocientes F/G onde F e G são polinômios homogêneos de mesmo grau, logo $\mathrm{Fr}^* k(\mathcal{X}^q)$ é formado por elementos da forma

$$\mathrm{Fr}^*(F/G) = F(X_0^q, \ldots, X_n^q)/G(X_0^q, \ldots, X_n^q).$$

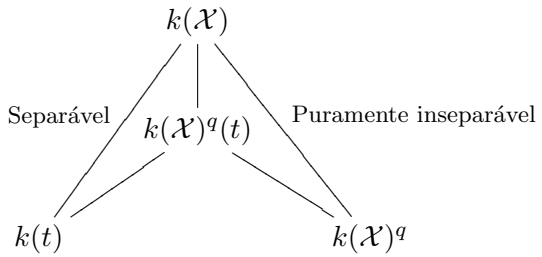
Analogamente, $k(\mathcal{X})^q$ é formado por elementos da forma

$$F(X_0, \ldots, X_n)^q / G(X_0, \ldots, X_n)^q.$$

Agora basta observar que cada elemento de k é uma q-ésima potência (pois k é perfeito) para concluir que $\mathrm{Fr}^* k(\mathcal{X}^q) = k(\mathcal{X})^q$.

(b) Trivial, pelo item (a).

(c) Seja t um parâmetro local de um ponto não-singular $P \in \mathcal{X}$, então $k(\mathcal{X})/k(t)$ é uma extensão finita e separável e portanto $k(\mathcal{X}) = k(\mathcal{X})^q(t)$ pois



Em particular, $deg(\mathrm{Fr}) = [k(\mathcal{X})^q(t) : k(\mathcal{X})^q]$. Note que $t^q \in k(\mathcal{X})^q$, logo, para provar que $deg(\mathrm{Fr}) = q$, basta mostrar que $t^{q/p} \notin k(\mathcal{X})^q$. Mas se $t^{q/p} = f^q$ para algum $f \in k(\mathcal{X})$, então $q/p = v_P(t^{q/p}) = q v_P(f)$, o que é um absurdo. Isto conclui a demonstração.

(d) Basta combinar o item (c), o teorema (1.3.10) e o fato que Fr é injetor.

[1] Uma extensão L/K, onde $charac(K) = p > 0$, é *puramente inseparável* se para todo $x \in L$ existe $r \geq 1$ tal que $x^{p^r} \in K$.

□

Corolário B.0.13 *Qualquer aplicação não-constante $\phi : \mathcal{X} \to \mathcal{X}'$ entre curvas não-singulares e definidas sobre um corpo k de característica $p > 0$ admite uma fatoração*

$$\mathcal{X} \xrightarrow{\mathrm{Fr}} \mathcal{X}^q \xrightarrow{\psi} \mathcal{X}',$$

onde q é o grau de inseparabilidade de ϕ, Fr *é a q-ésima aplicação de Frobenius e ψ é uma aplicação separável.*

Demonstração: Seja K o fecho separável de $\phi^* k(\mathcal{X}')$ em $k(\mathcal{X})$, ou seja, K é a maior extensão de $\phi^* k(\mathcal{X}')$ contida em $k(\mathcal{X})$ que é separável sobre $\phi^* k(\mathcal{X}')$. Em particular, $k(\mathcal{X})/K$ é uma extensão puramente inseparável e por hipótese seu grau é q, logo $k(\mathcal{X})^q \subseteq K$ e portanto $k(\mathcal{X})^q = K$. Pelo item (a) da proposição (B.0.12), $K = \mathrm{Fr}^* k(\mathcal{X}^q)$. Em particular, existem inclusões

$$k(\mathcal{X}') \hookrightarrow k(\mathcal{X}^q) \overset{\mathrm{Fr}^*}{\hookrightarrow} k(\mathcal{X}).$$

Agora o resultado é uma consequência do teorema (1.3.6).

□

Referências Bibliográficas

[1] Aguglia,A., Korchmáros, G., Torres,F. *Plane Maximal Curves*, Acta Arithmetica, **98**(2),(2001), 165-179.

[2] Arbarello, E., Cornalba,M., Griffiths,P.A., Harris, J. *Geometry of Algebraic Curves, Vol 1*, Springer-Verlag, New York-Heidelberg-Berlin, (1985).

[3] Atiyah, M.F., Macdonald, I.G. *Introduction to Commutative Algebra*, Addison-Wesley, (1969).

[4] Bombieri,E. *Counting Points on Curves over Finite Fields*, Sém. Bourbaki, **430**,(1972/1973), 234-241.

[5] Fried,M.D., Jarden, M., *Field Arithmetic*, Springer-Verlag, New York-Heidelberg-Berlin, (1980).

[6] Fulton,W., *Algebraic Curves*, W. A. Benjamin INC, New York, , (1969).

[7] Fuhrmann,R., Garcia,A. e Torres,F., *On maximal curves*, J. Number Theory, **67**(1),(1997), 29-51.

[8] Fuhrmann,R., Torres,F., *The genus of curves over finite fields with many rational points*, Manuscripta Math , **89**,(1996), 103-106.

[9] Garcia,A., *Some arithmetic properties of order-sequences of algebraic curves*, J. Pure Appl. Algebra , **85**,(1993), 259-269.

[10] Goldshimdt,D.M., *Algebraic Function Fileds and Projective Curves*, Springer-Verlag, New York-Heidelberg-Berlin, (2003).

[11] Goppa,V.D., *Codes associated with divisors*, Probl. Peredachi Inform., **13**(1),(1977), 22-26. Translation: Probl. Inform. Transmission 13 (1), (1977), pp. 33-39.

[12] Hartshorne,R., *Algebraic Geometry*, Springer-Verlag, New York-Heidelberg-Berlin, (1977).

[13] Harris,J., *Algebraic Geometry- A First Course*, Springer-Verlag, New York-Heidelberg-Berlin, (1992).

[14] Hefez,A., *Non-reflexive curves*, Compositio Math , **69**,(1989), 3-35.

[15] Lang,S., *Algebra*, Springer-Verlag, New York-Heidelberg-Berlin, (2006).

[16] Levcovitz, *Bounds for the number of fixed points of automorphisms of curves*, Proc. London. Math. Soc., **62**(3),(1991), 133-150.

[17] Moreno,C., *Algebraic Curves over Finite Fields*, Cambridge U. Press, Cambridge-New York-Melbourne, (1991).

[18] Namba,M., *Geometry of Projctive Algebraic Curves*, Marcel Dekker INC, New York-Basel, (1984).

[19] Recio,T., *La Columna de Matemática Computacional*, La Gaceta de La RSME , **9.1**,(2006), 203-222.

[20] Rosen,M., *Number Theory in Function Fields*, Springer-Verlag, New York-Heidelberg-Berlin, (2002).

[21] Ruch,H.G. e Stichtenoth,H., *A characterization of Hermitian function fields over finite fields*, J. Reine Angel. Math , **457**,(1994), 185-188.

[22] Shafarevich,I.R., *Basic Algebraic Geometry - Varieties in Projective Space*, Springer-Verlag, New York-Heidelberg-Berlin, (1988).

[23] Silverman,J.H., *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York-Heidelberg-Berlin, (1986).

[24] Silverman,J.H. e Hindry,M. *Diophantine Geometry - An Introduction*, Springer-Verlag, New York-Heidelberg-Berlin, (2000).

[25] Stichtenoth,H., *Algebraic Function Fields and Codes*, Springer-Verlag, New York-Heidelberg-Berlin, (1993).

[26] Stöhr,K.O., Voloch,J.F., *Weierstrass points and curves over finite fields*, Proc. London. Math. Soc., **52**(3),(1986), 1-19.

[27] Torres,F., *The approach of Stöhr-Voloch to the Hasse-Weil bound with applications to optimal curves and plane arcs*, Lecture Notes, Campinas.

[28] Weil,A., *Courbes algebriques et varietes abeliennes*, Hermann, Paris, (1971).

[29] Xing,R. e Stichtenoth,H., *The genus of maximal curves over finite fields*, Manuscripta Math , **86**,(1995), 217-224.