UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Caracterização de curvas maximais a partir de mergulhos em variedades hermitianas

Gabriel Eurípedes de Jesus Farias

Dissertação de Mestrado do Programa de Pós-Graduação em Matemática (PPG-Mat)

ICMC USP
SÃO CARLOS

Gabriel Eurípedes de Jesus Farias

Caracterização de curvas maximais a partir de mergulhos em variedades hermitianas

Dissertação apresentada ao Instituto de Ciências Matemáticas e de Computação – ICMC-USP, como parte dos requisitos para obtenção do título de Mestre em Ciências – Matemática. *VERSÃO REVISADA*

Área de Concentração: Matemática

Orientador: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
Maio de 2022

Ficha catalográfica elaborada pela Biblioteca Prof. Achille Bassi
e Seção Técnica de Informática, ICMC/USP,
com os dados inseridos pelo(a) autor(a)

F224c

Farias, Gabriel Eurípedes de Jesus
Caracterização de curvas maximais a partir de mergulhos em variedades hermitianas / Gabriel Eurípedes de Jesus Farias; orientador Herivelto Martins Borges Filho. -- São Carlos, 2022.
76 p.

Dissertação (Mestrado - Programa de Pós-Graduação em Matemática) -- Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2022.

1. Corpos finitos. 2. Curvas maximais. 3. Variedades hermitianas. I. Borges Filho, Herivelto Martins, orient. II. Título.

Bibliotecários responsáveis pela estrutura de catalogação da publicação de acordo com a AACR2:
Gláucia Maria Saia Cristianini - CRB - 8/4938
Juliana de Souza Moraes - CRB - 8/6176

Gabriel Eurípedes de Jesus Farias

Characterization of maximal curves from embeddings in Hermitian varieties

Dissertation submitted to the Instituto de Ciências Matemáticas e de Computação – ICMC-USP – in accordance with the requirements of the Mathematics Graduate Program, for the degree of Master in Science. *FINAL VERSION*

Concentration Area: Mathematics

Advisor: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
May 2022

A meus pais Eurípedes e Fátima
e ao matemático Fernando Torres (in memoriam), dedico.

AGRADECIMENTOS

Em primeiro lugar, agradeço a Deus pela minha saúde e pelas grandes oportunidades que colocou em meu caminho. Agradeço aos meus pais por me fornecerem cuidado e apoio nos estudos. Agradeço ao meus amigos por dividirem suas vivências comigo.

Agradeço a todos os meus professores pelas lições e reflexões. Agradeço aos professores Daniel Levcovitz, Saeed Tafazolian e Victor Gonzalo Lopez Neumann por participarem da banca e pelas sugestões que forneceram em prol do aprimoramento deste trabalho. Em especial, agradeço ao meu orientador, Herivelto Martins Borges Filho, por me direcionar nesta jornada com sua empatia, paciência e sabedoria.

Por fim, agradeço ao PICME-CAPES pela bolsa de mestrado.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

"[...] o estudo das curvas $\mathbb{F}_{q^2}$-maximais é equivalente ao das curvas projetivas, geometricamente irredutíveis e não singulares de grau $q+1$ contidas em uma variedade hermitiana não degenerada definida sobre $\mathbb{F}_{q^2}$ em um espaço projetivo sobre $\overline{\mathbb{F}}_{q^2}$."
(KORCHMÁROS; TORRES, 2001, Seção 1)

RESUMO

FARIAS, G. E. J. **Caracterização de curvas maximais a partir de mergulhos em variedades hermitianas**. 2022. 76 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2022.

Uma curva algébrica projetiva, geometricamente irredutível e não singular definida sobre $\mathbb{F}_{q^2}$ de gênero g será $\mathbb{F}_{q^2}$-maximal se seu número de pontos $\mathbb{F}_{q^2}$-racionais for $1+q^2+2gq$, isto é, a cota superior de Hasse-Weil. Este trabalho detalha a prova do Teorema do Mergulho Natural e a de sua recíproca, desenvolvidas por Gábor Korchmáros e Fernando Torres. Juntos, os dois resultados dão uma caracterização geométrica à propriedade definida aritmeticamente.

Palavras-chave: Corpos finitos, Curvas maximais, Variedades hermitianas.

ABSTRACT

FARIAS, G. E. J. **Characterization of maximal curves from embeddings in Hermitian varieties**. 2022. 76 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2022.

A projective, geometrically irreducible and non-singular algebraic curve defined over $\mathbb{F}_{q^2}$ of genus g is $\mathbb{F}_{q^2}$-maximal if its number of $\mathbb{F}_{q^2}$-rational points is $1+q^2+2gq$, i.e., the Hasse-Weil upper bound. This work details the proof of both Natural Embedding Theorem and its converse, developed by Gábor Korchmáros and Fernando Torres. Together, the two results provide a geometric characterization to the arithmetically defined property.

Keywords: Finite fields, Maximal curves, Hermitian varieties.

SUMÁRIO

CAPÍTULO

1

INTRODUÇÃO

Nesta introdução, o termo curva designará uma curva algébrica projetiva, geometricamente irredutível, não singular e definida sobre $\mathbb{F}_{q^2}$, o corpo finito com q^2 elementos. Um bom exemplo para termos em mente é a curva plana $\mathscr{C}$ definida sobre $\mathbb{F}_{3^2}$ dada em coordenadas afins por

$$\mathscr{C}\colon\ Y^3+Y-X^2=0,$$

ou seja,

$$\mathscr{C}=\{(\alpha:\beta:\gamma)\in\mathbb{P}^2(\overline{\mathbb{F}}_{q^2});\ \beta^3+\beta\gamma^2-\alpha^2\gamma=0\}.$$

A cada curva, podemos associar um número não negativo chamado gênero. O gênero de uma curva plana (não singular) de grau d é dado por

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

Em particular, o gênero de $\mathscr{C}$ é 1.

Na primeira metade do século XX, Hasse e Weil mostraram que uma curva de gênero g pode ter no máximo

$$1+q^2+2gq$$

pontos $\mathbb{F}_{q^2}$-racionais (veja (HASSE, 1936, Seção 4) e (WEIL, 1948, Corolário 3 do Teorema 13)). Uma curva que atinge essa cota é nomeada curva $\mathbb{F}_{q^2}$-maximal. Um exemplo importante desse tipo de curva é a curva hermitiana $\mathscr{H}_q$, que pode ser descrita em coordenadas afins por

$$\mathscr{H}_q\colon\ Y^q+Y-X^{q+1}=0.$$

Serre observou que qualquer curva que é $\mathbb{F}_{q^2}$-recoberta por uma curva $\mathbb{F}_{q^2}$-maximal também é uma curva $\mathbb{F}_{q^2}$-maximal (veja (LACHAUD, 1987, Proposição 6)). Por exemplo, a curva $\mathscr{C}$ é $\mathbb{F}_{3^2}$-recoberta por $\mathscr{H}_3$ no morfismo sobrejetor

$$\begin{array}{ccc}\mathscr{H}_3 & \to & \mathscr{C}\\ (\alpha,\beta) & \mapsto & (\alpha^2,\beta).\end{array}$$

Consequentemente, $\mathscr{C}$ é uma curva $\mathbb{F}_{3^2}$-maximal.

Durante um certo período, todas as curvas maximais conhecidas eram, assim como $\mathscr{C}$, recobertas pelas curva hermitiana (veja (FUHRMANN; GARCIA; TORRES, 1997), (ABDÓN; TORRES, 1999) e (ABDÓN; GARCIA, 2004)). Nesse contexto, a seguinte questão ganhou destaque.

Pergunta. Toda curva $\mathbb{F}_{q^2}$-maximal é $\mathbb{F}_{q^2}$-recoberta pela curva hermitiana $\mathscr{H}_q$?

Em 2006, Garcia e Stichtenoth deram uma resposta parcialmente negativa a essa questão. Eles exibiram uma curva que é $\mathbb{F}_{27^2}$-maximal mas que não é Galois recoberta por $\mathscr{H}_{27}$ (veja (GARCIA; STICHTENOTH, 2006, Teoremas 1 e 3)).

Finalmente, Giulietti e Korchmáros responderam essa pergunta em 2009. Para cada q da forma n^3, onde $n > 2$ é uma potência de algum primo, eles construíram uma curva $\mathbb{F}_{q^2}$-maximal que não é $\mathbb{F}_{q^2}$-recoberta por $\mathscr{H}_q$ (veja (GIULIETTI; KORCHMÁROS, 2009, Teoremas 1 e 5)).

Portanto, se $\mathscr{X}$ for uma curva $\mathbb{F}_{q^2}$-maximal, é possível que não exista um morfismo sobrejetor definido sobre $\mathbb{F}_{q^2}$

$$\phi\colon \mathscr{H}_q \twoheadrightarrow \mathscr{X}.$$

Entretanto, em 2001, Korchmáros e Torres provaram que haverá um morfismo injetor definido sobre $\mathbb{F}_{q^2}$

$$\psi\colon \mathscr{X} \hookrightarrow \mathscr{H},$$

onde $\mathscr{H}$ é alguma variedade hermitiana definida sobre $\mathbb{F}_{q^2}$, uma generalização da curva hermitiana. Mais precisamente, eles mostraram o resultado seguinte.

Teorema. (KORCHMÁROS; TORRES, 2001, Teoremas 3.6 e 4.1). Uma curva é $\mathbb{F}_{q^2}$-maximal se, e somente se, ela admitir como modelo uma curva de grau $q+1$ contida numa variedade hermitiana não degenerada definida sobre $\mathbb{F}_{q^2}$.

No presente trabalho, esta caracterização das curvas maximais será demonstrada em detalhes no terceiro capítulo. Para isso, utilizaremos os fundamentos da teoria de curvas algébricas que serão apresentados no próximo capítulo.

CAPÍTULO

2

FUNDAMENTAÇÃO TEÓRICA

Neste primeiro capítulo, poderão ser consultadas definições, notações e proposições que serão aplicadas, com frequência, no desenvolvimento do segundo capítulo. Em particular, escrito com base nos textos (COUTINHO, 2019, Parte I), (FULTON, 2008, Capítulos 3, 5 e 7), (GOLDSCHMIDT, 2003, Capítulos 1 e 2), (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Capítulos 1, 3, 4, 5, 6, 7, 8, 10 e 11), (STICHTENOTH, 2009, Capítulos 1 e 4), (STÖHR; VOLOCH, 1986, Seção 1) e (TORRES, 2000, Seções 1 e 2), este capítulo coleciona alguns objetos e fatos básicos a respeito da geometria e da aritmética das curvas algébricas.

Ao longo deste capítulo, $\mathbb{K}$ denotará um corpo algebricamente fechado.

2.1 Curvas planas afins

No conjunto $\mathbb{K}[X,Y]\setminus\mathbb{K}$, definamos a relação de equivalência seguinte:

$$F_1 \equiv_a F_2 \Leftrightarrow F_1 = \lambda F_2 \text{ para algum } \lambda \in \mathbb{K}^\times.$$

Consideremos o conjunto quociente

$$\mathfrak{C}_\mathfrak{a} := \frac{\mathbb{K}[X,Y]\setminus\mathbb{K}}{\equiv_a}$$

e a aplicação quociente

$$\mathbf{v}_a \colon \mathbb{K}[X,Y]\setminus\mathbb{K} \to \mathfrak{C}_\mathfrak{a}.$$

Definição 2.1.1. Dado $F \in \mathbb{K}[X,Y]\setminus\mathbb{K}$, denotaremos $\mathbf{v}_a(F)$ por $\mathscr{F}$ usualmente.

1. A **curva plana afim** definida pela equação $F(X,Y)=0$ é a classe $\mathscr{F}$.
2. O **conjunto dos pontos de** $\mathscr{F}$ é o conjunto dos zeros de F em $\mathbb{A}^2(\mathbb{K})$ e também é denotado por $\mathscr{F}$. Isto é,
$$\mathscr{F} = \{(x,y) \in \mathbb{A}^2(\mathbb{K});\ F(x,y)=0\}.$$

3. O **grau** de $\mathscr{F}$ é $\deg(\mathscr{F}) := \deg(F)$.

4. Se $\deg(\mathscr{F}) = 1$, diremos que $\mathscr{F}$ é uma **reta**.

5. Se F for irredutível, diremos que $\mathscr{F}$ é **irredutível**. Caso contrário, diremos que $\mathscr{F}$ é **redutível**.

6. Sejam $G \in \mathbb{K}[X,Y] \setminus \mathbb{K}$ e $\mathscr{G} = \mathbf{v}_a(G)$. Se G dividir F, diremos que $\mathscr{G}$ é uma **componente de** $\mathscr{F}$.

2.2 Curvas planas projetivas

No conjunto

$$\{F \in \mathbb{K}[X,Y,Z] \setminus \mathbb{K};\ F \text{ é homogêneo}\},$$

definamos a relação de equivalência seguinte:

$$F_1 \equiv_p F_2 \Leftrightarrow F_1 = \lambda F_2 \text{ para algum } \lambda \in \mathbb{K}^\times.$$

Consideremos o conjunto quociente

$$\mathfrak{C}_\mathfrak{p} := \frac{\{F \in \mathbb{K}[X,Y,Z] \setminus \mathbb{K};\ F \text{ é homogêneo}\}}{\equiv_p}$$

e a aplicação quociente

$$\mathbf{v}_p \colon \{F \in \mathbb{K}[X,Y,Z] \setminus \mathbb{K};\ F \text{ é homogêneo}\} \to \mathfrak{C}_\mathfrak{p}.$$

Abaixo, temos a versão projetiva da Definição 2.1.1.

Definição 2.2.1. Consideremos um polinômio homogêneo $F \in \mathbb{K}[X,Y,Z] \setminus \mathbb{K}$ e denotemos $\mathbf{v}_p(F)$ por $\mathscr{F}$.

1. A **curva plana projetiva** definida pela equação $F(X,Y,Z) = 0$ é a classe $\mathscr{F}$.

2. O **conjunto dos pontos de** $\mathscr{F}$ é

$$\mathscr{F} = \{(x:y:z) \in \mathbb{P}^2(\mathbb{K});\ F(x,y,z) = 0\}.$$

3. O **grau** de $\mathscr{F}$ é $\deg(\mathscr{F}) := \deg(F)$.

4. Se $\deg(\mathscr{F}) = 1$, diremos que F é uma **reta**.

5. Se F for irredutível, diremos que $\mathscr{F}$ é **irredutível**. Caso contrário, diremos que $\mathscr{F}$ é **redutível**.

6. Sejam $G \in \mathbb{K}[X,Y,Z] \setminus \mathbb{K}$ homogêneo e $\mathscr{G} = \mathbf{v}_p(G)$. Se G dividir F, diremos que $\mathscr{G}$ é uma **componente de** $\mathscr{F}$.

Notemos que o conjunto

$$\mathscr{U}_Z := \{(x:y:z) \in \mathbb{P}^2(\mathbb{K});\ z \neq 0\}$$

é uma cópia do plano afim dentro de $\mathbb{P}^2(\mathbb{K})$. Mais precisamente, as aplicações

$$\begin{array}{rccc} \mathbf{P}_Z\colon & \mathbb{A}^2(\mathbb{K}) & \to & \mathscr{U}_Z \\ & (x,y) & \to & (x:y:1) \end{array} \quad \text{e} \quad \begin{array}{rccc} \mathbf{A}_Z\colon & \mathscr{U}_Z & \to & \mathbb{A}^2(\mathbb{K}) \\ & (x:y:z) & \to & \left(\frac{x}{z}, \frac{y}{z}\right) \end{array}$$

são inversas uma da outra. Além disso, a reta $\mathbf{v}_p(Z)$ é o complementar de $\mathscr{U}_Z$ em $\mathbb{P}^2(\mathbb{K})$.

Definição 2.2.2. 1. O conjunto $\mathscr{U}_Z$ é uma **carta afim** de $\mathbb{P}^2(\mathbb{K})$.

2. A reta $\mathbf{v}_p(Z)$ é a **reta no infinito** e é denotada por $\mathscr{L}_\infty$.

Observação 2.2.3. 1. Analogamente, podemos definir as cartas afins $\mathscr{U}_X$ e $\mathscr{U}_Y$ e as aplicações $\mathbf{P}_X$, $\mathbf{A}_X$, $\mathbf{P}_Y$ e $\mathbf{A}_Y$. As três cartas afins cobrem o plano projetivo, isto é,

$$\mathbb{P}^2(\mathbb{K}) = \mathscr{U}_X \cup \mathscr{U}_Y \cup \mathscr{U}_Z.$$

2. Sejam $\mathscr{F} = \mathbf{v}_a(F)$ uma curva afim e F^Z a **homogeneização** de F com respeito à variável Z. O **fecho projetivo de** $\mathscr{F}$ é a curva plana projetiva $\mathscr{F}^Z = \mathbf{v}_p(F^Z)$. Temos a seguinte relação entre o conjunto dos pontos de $\mathscr{F}$ e o de $\mathscr{F}^Z$:

$$\mathscr{F}^Z = \mathbf{P}_Z(\mathscr{F}) \cup \{(x:y:0) \in \mathbb{P}^2(\mathbb{K});\ F^Z(x,y,0) = 0\}.$$

3. Consideremos $\mathscr{F} = \mathbf{v}_p(F)$ uma curva plana projetiva e $P \in \mathscr{F}$. Sejam $W \in \{X,Y,Z\}$ tal que $P \in \mathscr{U}_W$ e F_W a **desomogeneização** de F com respeito à variável W. Para obtermos informações locais de $\mathscr{F}$ em P utilizando uma notação mais limpa, será conveniente trabalharmos com a curva $\mathscr{F}_W = \mathbf{v}_a(F_W)$ e com ponto $\mathbf{A}_W(P)$.

Exemplo 2.2.4. Consideremos o polinômio $C(X,Y) := Y^3 + YZ^2 - X^2Z \in \mathbb{F}_{3^2}[X,Y]$ e a curva plana projetiva

$$\mathscr{C} := \mathbf{v}_p(C) = \mathbf{v}_p(Y^3 + YZ^2 - X^2Z).$$

Notemos que $P_\infty := (1:0:0)$ é o único ponto de $\mathscr{F}$ que está sobre a reta no infinito $\mathscr{L}_\infty$. De fato, dado $(a:b:c) \in \mathscr{F} \cap \mathscr{L}_\infty$, temos

$$c = 0 \quad \text{e} \quad b^3 + c\left(bc - a^2\right) = 0,$$

ou seja, $(a:b:c) = (a:0:0) = P_\infty$.

Definição 2.2.5. Consideremos uma curva algébrica plana projetiva $\mathscr{F} = \mathbf{v}_p(F)$ e $P \in \mathscr{F}$.

1. Diremos que P é um **ponto singular de** $\mathscr{F}$ se

$$\left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right) = (0,0,0).$$

Caso contrário, diremos que P é um **ponto não singular de** $\mathscr{F}$ e que

$$T_P\mathscr{F} := \mathbf{v}_p\left(\frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z\right)$$

é a **reta tangente** a $\mathscr{F}$ em P.

2. Diremos que $\mathscr{F}$ é uma **curva não singular** se todos os seus pontos forem não singulares. Caso contrário, diremos que $\mathscr{F}$ é uma **curva singular**.

Exemplo 2.2.6. A curva $\mathscr{C} = \mathbf{v}_p(C) = \mathbf{v}_p(Y^3 + YZ^2 - X^2Z)$ é não singular. De fato,

$$\frac{\partial C}{\partial X} = XZ, \quad \frac{\partial C}{\partial Y} = Z^2 \quad \text{e} \quad \frac{\partial F}{\partial Z} = 2(YZ + X^2).$$

O ponto $P_\infty = (1:0:0)$ é não singular, pois

$$\frac{\partial F}{\partial Z}(P_\infty) \neq 0.$$

No Exemplo 2.2.4, vimos que todos os outros pontos de $\mathscr{C}$ estão na carta afim $\mathscr{U}_Z$. Em outras palavras, se $P \in \mathscr{C} \setminus \{P_\infty\}$, então

$$\frac{\partial C}{\partial Y}(P) \neq 0.$$

2.3 Multiplicidade de interseção

Teorema 2.3.1. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teoremas 3.8 e 3.9 da Seção 3.1). Existe uma única aplicação

$$I\colon \mathbb{A}^2(\mathbb{K}) \times \mathfrak{C}_\mathfrak{a} \times \mathfrak{C}_\mathfrak{a} \to \mathbb{N} \cup \{\infty\}$$

que, para todo $P \in \mathbb{A}^2(\mathbb{K})$ e para quaisquer curvas planas afins $\mathscr{F} = \mathbf{v}_a(F)$, $\mathscr{G} = \mathbf{v}_a(G)$ e $\mathscr{H} = \mathbf{v}_a(H)$, tem as sete propriedades seguintes:

(P1) se $\mathscr{F}$ e $\mathscr{G}$ não tiverem uma componente em comum contendo P, então $I(P,\mathscr{F},\mathscr{G}) \in \mathbb{N}$;

(P2) se $\mathscr{F}$ e $\mathscr{G}$ tiverem uma componente em comum passando por P, então $I(P,\mathscr{F},\mathscr{G}) = \infty$;

(P3) $I(P,\mathscr{F},\mathscr{G}) = 0$ se, e somente se, $P \notin \mathscr{F} \cap \mathscr{G}$;

(P4) se $\mathscr{F}$ e $\mathscr{G}$ forem duas retas distintas que contêm P, então $I(P,\mathscr{F},\mathscr{G}) = 1$;

(P5) $I(P,\mathscr{F},\mathscr{G}) = I(P,\mathscr{G},\mathscr{F})$;

(P6) $I(P,\mathscr{F},\mathscr{G}+\mathscr{H}\mathscr{F}) = I(P,\mathscr{F},\mathscr{G})$ onde $\mathscr{G}+\mathscr{H}\mathscr{F} := \mathbf{v}_a(G+HF)$;

(P7) $I(P,\mathscr{F},\mathscr{G}\mathscr{H}) = I(P,\mathscr{F},\mathscr{G}) + I(P,\mathscr{F},\mathscr{H})$ onde $\mathscr{G}\mathscr{H} := \mathbf{v}_a(GH)$.

Observação 2.3.2. Seja I a única aplicação com as sete propriedades listadas no Teorema 2.3.1. Se $\mathscr{F} = \mathbf{v}_a(F)$ e $\mathscr{G} = \mathbf{v}_a(G)$, denotaremos $I(P,\mathscr{F},\mathscr{G})$ por $(F,G)_P$.

Definição 2.3.3. Dado um ponto $P \in \mathbb{P}^2(\mathbb{K})$ e dadas duas curvas planas projetivas $\mathscr{F} = \mathbf{v}_p(F)$ e $\mathscr{G} = \mathbf{v}_p(G)$, a **multiplicidade de interseção de $\mathscr{F}$ e $\mathscr{G}$ em P** é

$$(F,G)_P := \begin{cases} (F_W, G_W)_{\mathbf{A}_W(P)} & \text{se } P \in \mathscr{F}\cap\mathscr{G} \\ 0 & \text{caso contrário,} \end{cases}$$

onde W é uma variável satisfazendo $P \in \mathscr{U}_W$.

Teorema 2.3.4 (Teorema de Bézout)**.** Sejam $\mathscr{F}$ e $\mathscr{G}$ curvas planas sem componentes em comum. Então,

$$\sum_{P\in\mathscr{F}\cap\mathscr{G}} (\mathscr{F},\mathscr{G})_P = \deg(\mathscr{F})\deg(\mathscr{G}).$$

Demonstração. Pode ser encontrada em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 3.14 da Seção 3.2). □

O Teorema de Bézout nos dá o seguinte critério de irredutibilidade.

Corolário 2.3.5. Toda curva plana projetiva e não singular é irredutível.

Exemplo 2.3.6. No Exemplo 2.2.6, vimos que $\mathscr{C} = \mathbf{v}_p(C) = \mathbf{v}_p(Y^3+YZ^2-X^2Z)$ é não singular. Pelo Corolário 2.3.5, $\mathscr{C}$ é também irredutível.

Tomemos $\mathrm{i} \in \mathbb{F}_{3^2}$ tal que $\mathrm{i}^2 = -1$ e consideremos os pontos $P_\infty = (1:0:0)$, $P_1 = (0:0:1)$, $P_2 = (0:i:1)$ e $P_3 = (0:-i:1)$. A multiplicidade de interseção de $\mathscr{C}$ com a reta $\mathbf{v}_p(X)$ e a com a reta $\mathbf{v}_p(Y)$ são dadas por:

$$(X,C)_P = \begin{cases} 1 & \text{se } P \in \{P_1,P_2,P_3\} \\ 0 & \text{caso contrário} \end{cases} \qquad \text{e} \qquad (Y,C)_P = \begin{cases} 1 & \text{se } P = P_\infty \\ 2 & \text{se } P = P_1 \\ 0 & \text{se } P \notin \{P_\infty, P_1\}. \end{cases}$$

De fato, para $P \in \mathscr{U}_Z$,

$$\begin{aligned} (X,C_Z)_{\mathbf{A}_Z(P)} &\overset{\text{(P6)}}{=} (X, C_Z + X\cdot X)_{\mathbf{A}_Z(P)} \\ &= (X, Y^3+Y)_{\mathbf{A}_Z(P)} \\ &\overset{\text{(P7)}}{=} (X,Y)_{\mathbf{A}_Z(P)} + (X,Y-\mathrm{i})_{\mathbf{A}_Z(P)} + (X,Y+\mathrm{i})_{\mathbf{A}_Z(P)} \\ &\overset{\text{(P3) e (P4)}}{=} \begin{cases} 1 & \text{se } \mathbf{A}_Z(P) = (0,0) \\ 1 & \text{se } \mathbf{A}_Z(P) = (0,i) \\ 1 & \text{se } \mathbf{A}_Z(P) = (0,-i) \\ 0 & \text{caso contrário} \end{cases} \end{aligned}$$

e

$$\begin{aligned}(Y,C_Z)_{\mathbf{A}_Z(P)} &\overset{\text{(P6)}}{=} (Y,C_Z-(Y^2+1)Y)_{\mathbf{A}_Z(P)}\\ &= (Y,X^2)_{\mathbf{A}_Z(P)}\\ &\overset{\text{(P7)}}{=} 2(Y,X)_{\mathbf{A}_Z(P)}\\ &\overset{\text{(P3) e (P4)}}{=} \begin{cases} 2 & \text{se } \mathbf{A}_Z(P)=(0,0)\\ 0 & \text{caso contrário.}\end{cases}\end{aligned}$$

Da última computação e do Teorema de Bézout, decorre $(Y,C)_{P_\infty}=1$.

2.4 Ramos de curvas planas

Lembremos que, a ordem de uma série de Laurent $\sum_{i=k}^{\infty} a_iT^i \in \mathbb{K}((T))$ (com $k\in\mathbb{Z}$, $a_i\in\mathbb{K}$ para todo $i\geq k$ e $a_k\neq 0$) é

$$\operatorname{ord}_T\left(\sum_{i=k}^{\infty} a_iT^i\right) := k.$$

Além disso, definimos $\operatorname{ord}_T(0):=\infty$.

Definição 2.4.1. 1. Uma **representação de ramo** $\mathtt{b}$ é um ponto em $\mathbb{P}^2(\mathbb{K}((T)))\setminus\mathbb{P}^2(\mathbb{K})$.

2. Seja $(x(T):y(T):z(T))$ uma representação de ramo. Diremos que $x(T),y(T),z(T)$ são **coordenadas especiais** se tivermos

$$0\in\{\operatorname{ord}_T x(T),\operatorname{ord}_T y(T),\operatorname{ord}_T z(T)\}\subset\mathbb{N}\cup\{\infty\}.$$

Observação 2.4.2. Seja $\mathtt{b}=(x(T):y(T):z(T))$ uma representação de ramo. Definamos

$$e=-\min\{\operatorname{ord}_T x(T),\operatorname{ord}_T y(T),\operatorname{ord}_T z(T)\}.$$

Notemos que $T^e\operatorname{ord}_T x(T),T^e\operatorname{ord}_T y(T),T^e\operatorname{ord}_T z(T)$ são coordenadas especiais de $\mathtt{b}$. Portanto, toda representação de ramo admite uma escrita em coordenadas especiais.

Definição 2.4.3. Seja $\mathtt{b}=(x(T):y(T):z(T))$ uma representação de ramo escrita em coordenadas especiais.

1. O **centro de** $\mathtt{b}$ é o ponto $(x(0):y(0):z(0))$.

2. Se $z(T)=1$, então $(x(T),y(T))$ é o **par de coordenadas afins especiais de** $\mathtt{b}$ **com respeito a** Z. Analogamente, definimos os pares de coordenadas afins especiais de $\mathtt{b}$ com respeito às outras duas variáveis.

Definição 2.4.4. 1. No conjunto $\mathbb{K}[[T]]^2$, definamos a relação de equivalência seguinte:

$$(x_1(T),y_1(T))\equiv_r(x_2(T),y_2(T))\Leftrightarrow x_1(T)=\sigma(x_2(T))\quad\text{e}\quad y_1(T)=\sigma(y_2(T))$$

para algum $\mathbb{K}$-automorfismo σ de $\mathbb{K}[[T]]$.

2. Diremos que $(x(T), y(T)) \in \mathbb{K}[[T]]^2$ é **não primitivo** se existirem $(x_0(T), y_0(T)) \in \mathbb{K}[[T]]^2$ e um $\mathbb{K}$-monomorfismo não sobrejetor σ de $\mathbb{K}[[T]]$ tais que

$$x(T) = \sigma(x_0(T)) \quad \text{e} \quad y(T) = \sigma(y_0(T)).$$

Caso contrário, diremos que $(x(T), y(T))$ é **primitivo**.

Definição 2.4.5. 1. Duas representações de ramo serão **equivalentes** se elas possuírem pares de coordenadas afins especiais com respeito à mesma variável que são equivalentes.

2. Uma representação de ramo será **não primitiva** se ela tiver um par de coordenadas afins especiais com respeito a alguma variável que é não primitivo. Caso contrário, ela será dita **primitiva**.

Definição 2.4.6. 1. Um **ramo** é uma classe de equivalência de representações de ramos primitivas.

2. O **centro** de um ramo é o centro de qualquer um de seus representantes.

3. Seja $\mathscr{F} = \mathbf{v}(F)$ uma curva plana. Um ramo γ é um **ramo de** $\mathscr{F}$ se

$$F(x(T), y(T), z(T)) = 0$$

para todo representante $(x(T) : y(T) : z(T))$ de γ.

Teorema 2.4.7. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teoremas 4.31 e 4.32 da Seção 4.3 e Teorema 4.46 da Seção 4.4). Seja $\mathscr{F} = \mathbf{v}(F)$ uma curva plana.

1. Os centros dos ramos de $\mathscr{F}$ pertencem a $\mathscr{F}$.

2. Cada ponto não singular de $\mathscr{F}$ é o centro de um único ramo de $\mathscr{F}$.

3. Cada ponto de $\mathscr{F}$ é o centro de uma quantidade finita e positiva de ramos de $\mathscr{F}$.

2.5 Corpos de funções algébricas

Definição 2.5.1. Uma extensão de corpos $\Sigma/\mathbb{K}$ é dita um **corpo de funções** se existir $x \in \Sigma$ transcendente sobre $\mathbb{K}$ tal que a extensão $\Sigma/\mathbb{K}(x)$ seja finita.

Observação 2.5.2. (STICHTENOTH, 2009, Observação 1.1.2). Sejam $\Sigma/\mathbb{K}$ um corpo de funções e $f \in \Sigma$. Visto que $\mathbb{K}$ é algebricamente fechado, as afirmações seguintes são equivalentes:

(i) $f \notin \mathbb{K}$;

(ii) f é transcendente sobre $\mathbb{K}$;

(iii) a extensão $\Sigma/\mathbb{K}(f)$ é finita.

Teorema 2.5.3 (Teorema do Elemento Primitivo para Corpos de Funções)**.** Sejam $\Sigma/\mathbb{K}$ um corpo de funções e $x \in \Sigma$. Se x for transcendente sobre $\mathbb{K}$, então existirá $y \in \Sigma$ tal que $\Sigma = \mathbb{K}(x,y)$.

Demonstração. Pode ser encontrada em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema A.5 do Apêndice A.1). □

2.5.1 O corpo das funções de uma curva plana irredutível

Definição 2.5.4. Sejam $\mathscr{F} = \mathbf{v}_a(F)$ uma curva plana afim e $\mathbb{L}$ uma extensão de $\mathbb{K}$. Diremos que $(x,y) \in \mathbb{A}^2(\mathbb{L})$ é um **ponto genérico de** $\mathscr{F}$ se

$$\{G \in \mathbb{K}[X,Y];\ G(x,y) = 0\} \subset (F),$$

onde (F) denota o ideal gerado por F em $\mathbb{K}[X,Y]$.

Teorema 2.5.5. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teoremas 5.3, 5.4 e 5.7 da Seção 5.1). Seja $\mathscr{F}$ uma curva plana afim.

1. A curva $\mathscr{F}$ possuirá um ponto genérico se, e somente se, for irredutível.
2. Se (x_1,y_1) e (x_2,y_2) forem pontos genéricos de $\mathscr{F}$, então os corpos $\mathbb{K}(x_1,y_1)$ e $\mathbb{K}(x_2,y_2)$ serão $\mathbb{K}$-isomorfos.

Definição 2.5.6. Seja $\mathscr{F} = \mathbf{v}_a(F)$ uma curva plana afim irredutível e (x,y) um ponto genérico de $\mathscr{F}$. O **corpo das funções de** $\mathscr{F}$ é $\mathbb{K}(\mathscr{F}) := \mathbb{K}(x,y)$.

Observação 2.5.7. Seja $\mathscr{F} = \mathbf{v}_a(F)$ uma curva plana afim irredutível. Denotemos as classes de X e Y no domínio $\mathbb{K}[X,Y]/(F)$ por x e y, respectivamente. Seja $\mathbb{L}$ o corpo de frações de $\mathbb{K}[X,Y]/(F)$. Notemos que (x,y) é um ponto genérico de $\mathscr{F}$ e que $\mathbb{K}(\mathscr{F}) = \mathbb{L}$.

Definição 2.5.8. Sejam $\mathscr{F} = \mathbf{v}_p(F)$ uma curva plana projetiva e $\mathbb{L}$ uma extensão de $\mathbb{K}$. Diremos que $(x:y:z) \in \mathbb{P}^2(\mathbb{L})$ é um **ponto genérico de** $\mathscr{F}$ se

$$\{G \in \mathbb{K}[X,Y,Z];\ G \text{ é homogêneo e } G(x,y,z) = 0\} \subset (F),$$

onde (F) denota o ideal gerado por F em $\mathbb{K}[X,Y,Z]$.

Observação 2.5.9. O item 1 do Teorema 2.5.5 vale no caso projetivo.

Definição 2.5.10. Sejam $\mathscr{F} = \mathbf{v}_p(F)$ uma curva plana projetiva irredutível e $(x:y:z)$ um ponto genérico de $\mathscr{F}$. O **corpo das funções de** $\mathscr{F}$ é o subcorpo de $\mathbb{K}(x,y,z)$ seguinte:

$$\mathbb{K}(\mathscr{F}) := \left\{ \frac{A(x,y,z)}{B(x,y,z)};\ A,B \in \mathbb{K}[X,Y,Z] \text{ são homogêneos de mesmo grau e } B(x,y,z) \neq 0 \right\}.$$

Observação 2.5.11. Consideremos a notação da Definição 2.5.10. Se $z \neq 0$, então os corpos $\mathbb{K}(\mathscr{F})$ e $\mathbb{K}(x/z, y/z)$ serão $\mathbb{K}$-isomorfos.

Teorema 2.5.12. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 5.10 da Seção 5.1). Seja $\mathscr{F}$ uma curva plana (afim ou projetiva) irredutível. O corpo das funções de $\mathscr{F}$ é um corpo de funções (como na Definição 2.5.1).

2.5.2 Modelos planos

Seja $\Sigma/\mathbb{K}$ um corpo de funções.

Definição 2.5.13. Diremos que um par $(\mathscr{F},(x,y))$ é um **modelo de** Σ se $\Sigma=\mathbb{K}(x,y)$ e $\mathscr{F}$ for uma curva plana projetiva que tem $(x:y:1)$ como um ponto genérico.

Exemplo 2.5.14. Seja $\mathbb{L}=\overline{\mathbb{F}}_{3^2}(x,y)$ com $y^3+yz^2-x^2z=0$ (como construído na Observação 2.5.7). O par $(\mathscr{C},(x,y))$ é um modelo de Σ.

Definição 2.5.15. Seja $(\mathscr{F},(x,y))$ um modelo de Σ.

1. Uma **representação de lugar** é um $\mathbb{K}$-monomorfismo $\tau\colon \Sigma\to\mathbb{K}((T))$.
2. Uma representação de lugar σ será **primitiva** se $(\tau(x):\tau(y):1)$ for uma representação de ramo primitiva de $\mathscr{F}$.
3. Duas representações de lugar τ_1 e τ_2 serão **equivalentes** se existir um $\mathbb{K}$-automorfismo σ de $\mathbb{K}((T))$ tal que $\tau_2=\sigma\circ\tau_1$.
4. Um **lugar** é uma classe de equivalência de representações de lugar primitivas.
5. O **conjunto dos lugares de** Σ é denotado por $\mathfrak{P}(\Sigma)$.

Definição 2.5.16. Sejam $\mathscr{P}\in\mathfrak{P}(\Sigma)$, τ uma representação primitiva de $\mathscr{P}$ e $f\in\Sigma$.

1. A **ordem de** f **em** $\mathscr{P}$ é $v_{\mathscr{P}}(f):=\operatorname{ord}_T(\tau(f))$.
2. Se $v_{\mathscr{P}}(f)=1$, diremos que f é um **parâmetro local em** $\mathscr{P}$.
3. Se $v_{\mathscr{P}}(f)\geq 0$, diremos que f é **regular em** $\mathscr{P}$. Em particular, se $v_{\mathscr{P}}(f)>0$, diremos que $\mathscr{P}$ é um **zero de multiplicidade** $v_{\mathscr{P}}(f)$ **de** f.
4. Se $v_{\mathscr{P}}(f)<0$, diremos que $\mathscr{P}$ é um **polo de multiplicidade** $-v_{\mathscr{P}}(f)$ **de** f.
5. Suponhamos que f seja regular em $\mathscr{P}$. O **valor de** f **em** $\mathscr{P}$, denotado por $f(\mathscr{P})$, é o único elemento $a\in\mathbb{K}$ satisfazendo $v_{\mathscr{P}}(f-a)>0$.

Diretamente da Definição 2.5.16, seguem os dois próximos resultados.

Proposição 2.5.17. Sejam $\mathscr{P}\in\mathfrak{P}(\Sigma)$, $f,g\in\Sigma$ e $a\in\mathbb{K}$. A aplicação $v_{\mathscr{P}}\colon\Sigma\to\mathbb{Z}\cup\{\infty\}$ tem as propriedades seguintes:

1. $v_{\mathscr{P}}(f) = \infty$ se, e somente se, $f = 0$;
2. $v_{\mathscr{P}}(fg) = v_{\mathscr{P}}(f) + v_{\mathscr{P}}(g)$;
3. $v_{\mathscr{P}}(f+g) \geq \min\{v_{\mathscr{P}}(f), v_{\mathscr{P}}(g)\}$;
4. $v_{\mathscr{P}}(a) = 0$.

Diretamente dos itens 1 e 5 da Definição 2.5.16, decorre o resultado seguinte.

Proposição 2.5.18. Seja $\mathscr{P} \in \mathfrak{P}(\Sigma)$ e sejam $f, g \in \Sigma$ regulares em $\mathscr{P}$. Então, $f+g$ e fg também são regulares em $\mathscr{P}$ e valem:

1. $f(\mathscr{P}) + g(\mathscr{P}) = (f+g)(\mathscr{P})$;
2. $(fg)(\mathscr{P}) = f(\mathscr{P})g(\mathscr{P})$.

Proposição 2.5.19. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lema 5.31 da Seção 5.4). Se $\mathscr{P} \in \mathfrak{P}(\Sigma)$, então existirá um parâmetro local em $\mathscr{P}$.

Teorema 2.5.20. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teoremas 5.33 e 5.34 da Seção 5.4). Seja $f \in \Sigma \setminus \mathbb{K}$. O número de zeros de f e o número de polos de f, contados com suas multiplicidades, coincidem e são iguais a $[\Sigma : \mathbb{K}(f)] < \infty$.

Corolário 2.5.21. Sejam $f, g \in \Sigma$. Se existir um subconjunto infinito $S \subset \mathfrak{P}(\Sigma)$ tal que

$$f(\mathscr{P}) = g(\mathscr{P}) \quad \forall\, \mathscr{P} \in S,$$

então $f = g$.

Observação 2.5.22. (FULTON, 2008, Proposição 2 da Seção 7.5). Seja $\mathscr{F} = \mathbf{v}_p(F)$ uma curva plana projetiva, irredutível e não singular que admite um ponto genérico do tipo $(x : y : 1)$. Nesse caso, existe uma correspondência biunívoca

$$\{\text{pontos de } \mathscr{F}\} \leftrightarrow \{\text{lugares de } \mathbb{K}(x,y)\}.$$

Façamos essa identificação. Desse modo, quando $P \in \mathscr{F}$ for correspondente a $\mathscr{P} \in \mathbb{K}(x,y)$, passaremos a escrever $v_P(f)$ e $f(P)$ no lugar de $v_{\mathscr{P}}(f)$ e $f(\mathscr{P})$ respectivamente. Além disso, dados $P_0 \in \mathscr{F} \cap \mathscr{U}_Z$ e $G \in \mathbb{K}[X,Y]$, vale a relação

$$v_P(G(x,y)) = (F, G^Z)_P.$$

Exemplo 2.5.23. Consideremos as notações do Exemplo 2.3.6 e do Exemplo 2.5.14. Pela Observação 2.5.22, dado $P \in \mathscr{C} \setminus \{P_\infty\}$, temos

$$v_P(x) = \begin{cases} 1 & \text{se } P \in \{P_1, P_2, P_3\} \\ 0 & \text{caso contrário} \end{cases} \quad \text{e} \quad v_P(y) = \begin{cases} 2 & \text{se } P = P_1 \\ 0 & \text{caso contrário.} \end{cases}$$

Pelo Teorema 2.5.20,

$$v_{P_\infty}(x) = -3 \quad \text{e} \quad v_{P_\infty}(y) = -2.$$

Pela Proposição 2.5.17, dado $P \in \mathscr{C}$, temos

$$v_P(1) = 0 \quad \text{e} \quad v_P(y^2) = \begin{cases} 4 & \text{se } P = P_1 \\ -4 & \text{se } P = P_\infty \\ 0 & \text{se } P \notin \{P_1, P_\infty\}. \end{cases}$$

Definição 2.5.24. Um elemento $t \in \Sigma$ será dito **variável separante de** $\Sigma/\mathbb{K}$ se a extensão $\Sigma/\mathbb{K}(t)$ for separável.

Proposição 2.5.25. Seja $\mathscr{P} \in \mathfrak{P}(\Sigma)$. Se $t \in \Sigma$ for um parâmetro local em $\mathscr{P}$, então t será uma variável separante de $\Sigma/\mathbb{K}$.

Demonstração. Esse resultado é uma consequência de (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lema 5.38 da Seção 5.5). □

2.5.3 Expansão em série de potências

Definição 2.5.26. Sejam $\mathbb{L}$ um corpo e $v\colon \mathbb{L} \to \mathbb{Z} \cup \{\infty\}$ uma aplicação sobrejetora. Diremos que $(\mathbb{L}, v)$ é um **corpo valorizado** e que v é uma **valorização discreta de** $\mathbb{L}$ se, para todos $f, g \in \mathbb{L}$, tivermos:

(i) $v(f) = \infty$ se, e somente se, $f = 0$;

(ii) $v(fg) = v(f) + v(g)$;

(iii) $v(f+g) \geq \min\{v(f), v(g)\}$.

Observação 2.5.27. Sejam $\Sigma/\mathbb{K}$ um corpo de funções e $\mathscr{P} \in \mathfrak{P}(\Sigma)$. As Proposições 2.5.17 e 2.5.19 nos contam que a aplicação $v_{\mathscr{P}}\colon \Sigma \to \mathbb{Z} \cup \{\infty\}$ é uma valorização discreta de Σ.

Definição 2.5.28. Sejam $(\mathbb{L}, v)$ um corpo valorizado e $(f_i)_{i\geq 0}$ uma sequência em $\mathbb{L}$.

1. Diremos que $(f_i)_{i\geq 0}$ é uma **sequência convergente** se existir $f \in \mathbb{L}$ satisfazendo a propriedade seguinte:

$$\text{para todo } c \in \mathbb{R}, \text{ existe } i_0 \in \mathbb{N} \text{ tal que } v(f - f_i) \geq c \text{ para cada } i \geq i_0. \tag{2.1}$$

2. Seja $s_j = \sum_{i=0}^{j} f_i$. Diremos que $\sum_{i=0}^{\infty} f_i$ é uma **série convergente** se a sequência $(s_j)_{j\geq 0}$ for convergente.

3. Diremos que $(f_i)_{i\geq 0}$ é uma **sequência de Cauchy** se, para todo $c \in \mathbb{R}$, existir $i_0 \in \mathbb{N}$ tal que
$$v(f_i - f_j) \geq c$$
para quaisquer $i, j \geq i_0$.

Observação 2.5.29. Consideremos a notação da Definição 2.5.28.

1. Pode-se verificar que a convergência de $(f_i)_{i\geq 0}$ implica a existência de um único $f \in \mathbb{L}$ satisfazendo a Propriedade (2.1). Nesse caso, diremos que f é o limite de $(f_i)_{i\geq 0}$ e escreveremos $f = \lim_{i\to\infty} f_i$.

2. Se a série $\sum_{i=0}^{\infty} f_i$ for convergente, escreveremos $\sum_{i=0}^{\infty} f_i = \lim_{j\to\infty} s_j$.

3. Será conveniente considerarmos sequências do tipo $(g_i)_{i\geq k}$ e séries do tipo $\sum_{i=k}^{\infty} g_i$ com $g_i \in \mathbb{L}$ e $k \in \mathbb{Z}$. As definições e notações anteriores estendem-se naturalmente a esses objetos.

Definição 2.5.30. Consideremos dois corpos valorizados $(\mathbb{L}, v)$ e $(\hat{\mathbb{L}}, \hat{v})$.

1. Diremos que $(\hat{\mathbb{L}}, \hat{v})$ é **completo** se toda sequência de Cauchy em $\hat{\mathbb{L}}$ for convergente.

2. Diremos que $(\hat{\mathbb{L}}, \hat{v})$ é um **completamento** de $(\mathbb{L}, v)$ se:

   (i) $(\hat{\mathbb{L}}, \hat{v})$ for completo;

   (ii) $\mathbb{L}$ for um subcorpo de $\hat{\mathbb{L}}$ e $v = \hat{v}|_{\mathbb{L}}$;

   (iii) para todo $f \in \hat{\mathbb{L}}$, existir uma sequência $(f_i)_{i\geq 0}$ em $\mathbb{L}$ tal que $\lim_{i\to\infty} f_i = f$.

O resultado seguinte nos conta que o completamento de um corpo valorizado existe e é único a menos de isomorfismo.

Proposição 2.5.31. (STICHTENOTH, 2009, Proposição 4.2.3). Seja $(\mathbb{L}, v)$ um corpo valorizado. Então, existe um completamento $(\hat{\mathbb{L}}, \hat{v})$ de $(\mathbb{L}, v)$. Se $(\tilde{\mathbb{L}}, \tilde{v})$ for outro completamento de $(\mathbb{L}, v)$, então existirá um único isomorfismo $\sigma\colon \hat{\mathbb{L}} \to \tilde{\mathbb{L}}$ tal que $\hat{v} = \tilde{v} \circ \sigma$.

Seja $\Sigma/\mathbb{K}$ um corpo de funções e $\mathscr{P}$ um lugar de Σ.

Definição 2.5.32. O completamento de $(\Sigma, v_{\mathscr{P}})$ é dito **completamento $\mathscr{P}$-ádico de** Σ e é denotado por $(\hat{\Sigma}_{\mathscr{P}}, \hat{v}_{\mathscr{P}})$.

Teorema 2.5.33. (STICHTENOTH, 2009, Teorema 4.2.6). Sejam t um parâmetro local em $\mathscr{P}$ e $f \in \hat{\Sigma}_{\mathscr{P}}$. Então, f admite uma única escrita do tipo
$$f = \sum_{i=r}^{\infty} a_i t^i$$

com $r \in \mathbb{Z}$ e $a_i \in \mathbb{K}$. Reciprocamente, se $(b_i)_{i\geq s}$ for uma sequência em $\mathbb{K}$ com $s \in \mathbb{Z}$, então a série $\sum_{i=s}^{\infty} b_i t^i$ será convergente em $\hat{\Sigma}_{\mathscr{P}}$ e

$$\hat{v}_{\mathscr{P}}\left(\sum_{i=s}^{\infty} b_i t^i\right) = \min\{i;\ b_i \neq 0\}.$$

Definição 2.5.34. A representação $f = \sum_{i=v_{\mathscr{P}}(f)}^{\infty} a_i t^i$ é a **expansão local de f em t.**

2.5.4 Diferenciais

Seja $\Sigma/\mathbb{K}$ um corpo de funções.

Definição 2.5.35. 1. A **derivação em** $\mathbb{K}((T))$ é a aplicação

$$\begin{array}{rccc} \dfrac{\mathrm{d}}{\mathrm{d}T}\colon & \mathbb{K}((T)) & \to & \mathbb{K}((T)) \\ & \sum\limits_{i=k}^{\infty} a_i T^i & \mapsto & \sum\limits_{i=k}^{\infty} i a_i T^{i-1}. \end{array}$$

2. Seja $\mathbb{K}((T))(\mathrm{d}T)$ a extensão transcendente de $\mathbb{K}((T))$ pelo símbolo $\mathrm{d}T$. Dada $f \in K((T))$, definimos a **diferencial de** f por
$$\mathrm{d}f := \frac{\mathrm{d}f}{\mathrm{d}T}\mathrm{d}T.$$

Teorema 2.5.36. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 5.46 da Seção 5.7). Um elemento $f \in \Sigma$ será uma variável separante de $\Sigma/\mathbb{K}$ se, e somente se, tivermos, para cada $\mathscr{P} \in \mathfrak{P}(\Sigma)$,

$$\mathrm{d}\tau_{\mathscr{P}}(f) \neq 0,$$

onde $\tau_{\mathscr{P}}\colon \Sigma \to \mathbb{K}((T))$ é uma representação primitiva de $\mathscr{P}$.

Definição 2.5.37. Sejam t uma variável separante de $\Sigma/\mathbb{K}$ e $f \in \Sigma$. Seja $F \in \mathbb{K}[X,Y]$ irredutível tal que $F(t,f) = 0$. A **derivada de f com respeito a t** é o seguinte elemento de Σ:

$$\frac{\mathrm{d}f}{\mathrm{d}t} := -\frac{\frac{\mathrm{d}F}{\mathrm{d}X}|_{(t,f)}}{\frac{\mathrm{d}F}{\mathrm{d}Y}|_{(t,f)}}.$$

Definição 2.5.38. Seja t uma variável separante de $\Sigma/\mathbb{K}$.

1. Seja $\Sigma(\mathrm{d}t)$ a extensão transcendente de Σ pelo símbolo $\mathrm{d}t$. Uma **diferencial** é um elemento do tipo $f\mathrm{d}t \in \Sigma(\mathrm{d}t)$ com $f \in \Sigma$.

2. A **diferencial de f** é
$$\mathrm{d}f := \frac{\mathrm{d}f}{\mathrm{d}t}\mathrm{d}t.$$

Teorema 2.5.39. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 5.49 da Seção 5.7). Sejam t e t_1 variáveis separantes de $\Sigma/\mathbb{K}$ e $f \in \Sigma$. Em $\Sigma(\mathrm{d}t)$, temos

$$\frac{\mathrm{d}f}{\mathrm{d}t_1} \cdot \frac{\mathrm{d}t_1}{\mathrm{d}t} = \frac{\mathrm{d}f}{\mathrm{d}t}.$$

Observação 2.5.40. Sejam t e t_1 variáveis separantes de $\Sigma/\mathbb{K}$ e $f \in \Sigma$. Podemos considerar a diferencial de f definida a partir de t e a diferencial de f definida a partir de t_1 como o mesmo objeto. Mais precisamente, identificando o novo símbolo $\mathrm{d}t_1$ com $\frac{\mathrm{d}t_1}{\mathrm{d}t}\mathrm{d}t$ e aplicando o Teorema 2.5.39, obtemos

$$\frac{\mathrm{d}f}{\mathrm{d}t}\mathrm{d}t = \frac{\mathrm{d}f}{\mathrm{d}t_1} \cdot \frac{\mathrm{d}t_1}{\mathrm{d}t}\mathrm{d}t = \frac{\mathrm{d}f}{\mathrm{d}t_1}\mathrm{d}t_1.$$

Portanto, a definição de $\mathrm{d}f$ independe da escolha da variável separante nesse sentido.

Definição 2.5.41. Consideremos uma variável separante t e $\mathscr{P} \in \mathfrak{P}(\Sigma)$. Seja $\tau\colon \Sigma \to \mathbb{K}((T))$ uma representação primitiva de $\mathscr{P}$.

1. A **odem de** $\mathrm{d}t$ **em** $\mathscr{P}$ é o inteiro

$$v_{\mathscr{P}}(\mathrm{d}t) := \mathrm{ord}_T \frac{\mathrm{d}\tau(t)}{\mathrm{d}T}.$$

2. Se $v_{\mathscr{P}}(\mathrm{d}t) > 0$, diremos que $\mathscr{P}$ é um **zero de** $\mathrm{d}t$.

3. Se $v_{\mathscr{P}}(\mathrm{d}t) < 0$, diremos que $\mathscr{P}$ é um **polo de** $\mathrm{d}t$.

Observação 2.5.42. Pelo Teorema 2.5.36 e por não depender da escolha da representação primitiva de $\mathscr{P}$, a ordem está bem definida no item 1 da Definição 2.5.41.

Proposição 2.5.43. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lema 5.53 da Seção 5.8). Seja t uma variável separante de $\Sigma/\mathbb{K}$. O conjunto dos zeros e dos polos de $\mathrm{d}t$ é finito.

Teorema 2.5.44. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 5.54 da Seção 5.8). Sejam t e t_1 variáveis separantes de $\Sigma/\mathbb{K}$. Então,

$$\sum_{\mathscr{P}\in\mathfrak{P}(\Sigma)} v_{\mathscr{P}}(t) = \sum_{\mathscr{P}\in\mathfrak{P}(\Sigma)} v_{\mathscr{P}}(t_1).$$

Definição 2.5.45. 1. Seja t uma variável separante de $\Sigma/\mathbb{K}$. O **gênero de** Σ é o único inteiro não negativo g que satisfaz

$$\sum_{\mathscr{P}\in\mathfrak{P}(\Sigma)} v_{\mathscr{P}}(\mathrm{d}t) = 2g - 2.$$

2. Seja $\mathscr{F}$ uma curva plana irredutível. O **gênero de** $\mathscr{F}$ é o gênero de $\mathbb{K}(\mathscr{F})$.

Teorema 2.5.46. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 5.57 e considerações que sucedem a Definição 5.58 da Seção 5.8). Seja $\mathscr{F}$ uma curva plana irredutível. Se $\mathscr{F}$ tiver grau d e gênero g, então

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

A igualdade ocorrerá se, e somente se, $\mathscr{F}$ for não singular.

Exemplo 2.5.47. No Exemplo 2.2.6, vimos que $\mathscr{C} = \mathbf{v}_p(C) = \mathbf{v}_p(Y^3 + YZ^2 - X^2Z)$ é não singular. Como $\deg(\mathscr{C}) = 3$, pelo Teorema 2.5.46, o gênero de $\mathscr{C}$ é igual a 1.

2.5.5 Derivadas de Hasse

Sejam $\Sigma/\mathbb{K}$ um corpo de funções e t uma variável separante de $\Sigma/\mathbb{K}$.

Definição 2.5.48. 1. Estendemos o coeficiente binomial a $\mathbb{N} \times \mathbb{N}$ da seguinte maneira:

$$\binom{k}{i} := \begin{cases} \dfrac{k!}{(k-i)!i!} & \text{se } 0 \leq i \leq k \\ 0 & \text{se } 0 \leq k < i. \end{cases}$$

2. Dado um inteiro não negativo i, a ***i*-ésima derivada de Hasse em** $\mathbb{K}[t]$ é a aplicação $\mathbb{K}$-linear $\mathrm{D}_t^{(i)} : \mathbb{K}[t] \to \mathbb{K}[t]$ tal que

$$\mathrm{D}_t^{(i)}(t^k) = \binom{k}{i} t^{k-i} \quad \forall k \in \mathbb{N}.$$

Proposição 2.5.49. Para cada $i \in \mathbb{N}$, existe uma única extensão de $\mathrm{D}_t^{(i)}$ a uma aplicação $\mathbb{K}$-linear de Σ em Σ. Além disso, vale a relação

$$\mathrm{D}_t^{(i)}(f_1 f_2) = \sum_{k=0}^{i} \mathrm{D}_t^{(k)}(f_1)\mathrm{D}_t^{(i-k)}(f_2) \quad \forall f_1, f_2 \in \Sigma. \tag{2.2}$$

Demonstração. Essa proposição é uma consequência dos resultados (GOLDSCHMIDT, 2003, Lema 1.3.9 e Teorema 1.3.11). □

Definição 2.5.50. 1. A aplicação $\mathrm{D}_t^{(i)} : \Sigma \to \Sigma$ é dita ***i*-ésima derivada de Hasse em** Σ.

2. A relação (2.2) é chamada **Regra do Produto**.

Observação 2.5.51. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Definição 5.78 da Seção 5.10). Consideremos $f \in \Sigma$ e um polinômio irredutível

$$F(X,Y) = \sum_{m,n} a_{m,n} X^m Y^n \in \mathbb{K}[X,Y]$$

tal que $F(t,f)=0$. Alternativamente, podemos definir $\mathrm{D}_t^{(i)}(f)$ de maneira recursiva: declaramos $\mathrm{D}_t^{(0)}(f) := f$ e, para cada $i \geq 1$,

$$\mathrm{D}_t^{(i)}(f) := -\frac{1}{\left.\frac{\partial F}{\partial Y}\right|_{(t,f)}} \left[\left.\frac{\partial^{(i)} F}{\partial X^{(i)}}\right|_{(t,f)} + \sum_{j=1}^{i-1} \left.\frac{\partial^{(i-j+1)} F}{\partial X^{(i-j)} \partial Y}\right|_{(t,f)} \mathrm{D}_t^{(j)}(f) + \sum_{j=2}^{i} \sum_{k=j}^{i} \sum_{i_1+\cdots+i_j=k} \left.\frac{\partial^{(i-k+j)} F}{\partial X^{(i-k)} \partial Y^{(j)}}\right|_{(t,f)} \mathrm{D}_t^{(i_1)}(f) \cdots \mathrm{D}_t^{(i_j)}(f) \right],$$

onde $i_1, \ldots, i_k$ são inteiros positivos e

$$\frac{\partial^{(d_1+d_2)} F}{\partial X^{(d_1)} \partial Y^{(d_2)}} := \sum_{m,n} a_{m,n} \binom{m}{d_1} \binom{n}{d_2} X^{m-d_1} Y^{n-d_2} \quad \forall d_1, d_2 \in \mathbb{N}.$$

Pode-se verificar que essa definição alternativa e o item 1 da Definição 2.5.50 atribuem o mesmo valor a $\mathrm{D}_t^{(i)}(f)$.

Exemplo 2.5.52. Consideremos a notação do Exemplo 2.5.14. Notemos que x é uma variável separante de $\overline{\mathbb{F}}_{3^2}(\mathscr{C}) = \overline{\mathbb{F}}_{3^2}(x,y)$.

1. Para calcularmos as derivadas de Hasse de x com relação a x, tomamos $t = x$, $f = x$ e $F = X - Y$ na Observação 2.5.51. Com isso:
   (i) $\mathrm{D}_x^{(1)}(x) = 1$;
   (ii) $\mathrm{D}_x^{(i)} = 0$ para todo $i \geq 2$.
2. Tomando $t = x$, $f = y$ e $F = C_Z$ na Observação 2.5.51, obtemos:
   (i) $\mathrm{D}_x^{(1)}(y) = 2x$;
   (ii) $\mathrm{D}_x^{(2)}(y) = 1$;
   (iii) $\mathrm{D}_x^{(3)} = x^3$.
3. Pela Regra do Produto:
   (i) $\mathrm{D}_x^{(1)}(y^2) = 2\mathrm{D}_x^{(0)}(y)\mathrm{D}_x^{(1)}(y) = xy$;
   (ii) $\mathrm{D}_x^{(2)}(y^2) = \mathrm{D}_x^{(1)}(y)^2 + 2\mathrm{D}_x^{(0)}(y)\mathrm{D}_x^{(2)}(y) = x^2 + 2y$;
   (iii) $\mathrm{D}_x^{(3)}(y^2) = 2(\mathrm{D}_x^{(0)}(y)\mathrm{D}_x^{(3)}(y) + \mathrm{D}_x^{(1)}(y)\mathrm{D}_x^{(2)}(y)) = x - x^3 y$.

Teorema 2.5.53. (GOLDSCHMIDT, 2003, Teorema 2.5.13). Consideremos $\mathscr{P} \in \mathfrak{P}(\Sigma)$, um parâmetro local t em $\mathscr{P}$ e $f \in \Sigma$ regular em $\mathscr{P}$. Seja

$$f = \sum_{j=0}^{\infty} a_j t^j$$

a expansão local de f em t. Para cada $i \in \mathbb{N}$,

$$\mathrm{D}_t^{(i)}(f) = \sum_{j=i}^{\infty} \binom{j}{i} a_j t^{j-i}$$

é a expansão local de $D_t^{(i)}(f)$ em t.

2.5.6 Divisores

Seja $\Sigma/\mathbb{K}$ um corpo de funções.

Definição 2.5.54. Um **divisor de** Σ é uma soma formal

$$D = \sum_{\mathscr{P}\in\mathfrak{P}(\Sigma)} n_{\mathscr{P}}\mathscr{P},$$

onde $n_{\mathscr{P}} \in \mathbb{Z}$ para todo $\mathscr{P} \in \mathfrak{P}(\Sigma)$ e o conjunto

$$\{\mathscr{P} \in \mathfrak{P}(\Sigma);\ n_{\mathscr{P}} \neq 0\}$$

é finito.

1. Esse conjunto é chamado **suporte de** D e é denotado por $\mathrm{Supp}(D)$.
2. Para cada $\mathscr{P} \in \mathfrak{P}(\Sigma)$, o número $n_{\mathscr{P}}$ é chamado **multiplicidade de** D **em** $\mathscr{P}$ e é denotado por $v_{\mathscr{P}}(D)$.
3. A soma $\sum_{\mathscr{P}\in\mathfrak{P}(\Sigma)} n_{\mathscr{P}}$ é chamada **grau de** D e é simbolizada por $\deg(D)$.

Seja $\mathrm{Div}(\Sigma)$ o conjunto de todos os divisores de Σ. Esse conjunto com a soma

$$\begin{array}{rccc} +: & \mathrm{Div}(\Sigma)\times\mathrm{Div}(\Sigma) & \to & \mathrm{Div}(\Sigma) \\ & \left(\sum_{\mathscr{P}\in\mathfrak{P}(\Sigma)} n_{\mathscr{P}}\mathscr{P}, \sum_{\mathscr{P}\in\mathfrak{P}(\Sigma)} m_{\mathscr{P}}\mathscr{P}\right) & \mapsto & \sum_{\mathscr{P}\in\mathfrak{P}(\Sigma)} (n_{\mathscr{P}}+m_{\mathscr{P}})\mathscr{P} \end{array}$$

é um grupo abeliano livre sobre $\mathfrak{P}(\Sigma)$ e recebe o nome **grupo dos divisores de** Σ.

Observação 2.5.55. A aplicação $\deg\colon \mathrm{Div}(\Sigma) \to \mathbb{Z}$ é um homomorfismo de grupos.

Podemos introduzir uma ordem parcial em $\mathrm{Div}(\Sigma)$ comparando as multiplicidades de dois divisores em cada ponto:

$$D \geq E \Leftrightarrow v_{\mathscr{P}}(D) \geq v_{\mathscr{P}}(E) \quad \forall \mathscr{P} \in \mathfrak{P}(\Sigma).$$

Definição 2.5.56. Seja D um divisor de Σ. Diremos que D é **efetivo** se $D \geq 0$.

O Teorema 2.5.20 nos permite associar um divisor a cada função racional não nula em Σ de maneira natural.

Definição 2.5.57. Seja $f \in \Sigma^{\times}$.

1. O **divisor de** f é $\mathrm{div}(f) := \sum_{\mathscr{P}\in\mathfrak{P}(\Sigma)} v_{\mathscr{P}}(f)\mathscr{P}$.

2. O **divisor de zeros de** f é $\mathrm{div}_0(f) := \sum_{\substack{\mathscr{P}\in\mathfrak{P}(\Sigma)\\ v_{\mathscr{P}}(f)>0}} v_{\mathscr{P}}(f)\mathscr{P}$.

3. O **divisor de polos de** f é $\mathrm{div}_\infty(f) := \sum_{\substack{\mathscr{P}\in\mathfrak{P}(\Sigma)\\ v_{\mathscr{P}}(f)<0}} (-v_{\mathscr{P}}(f))\mathscr{P}$.

Um divisor do tipo apresentado no item 1 acima é chamado **divisor principal**.

Observação 2.5.58. Claramente, para $f \in \Sigma^\times$, temos

$$\mathrm{div}(f) = \mathrm{div}_0(f) - \mathrm{div}_\infty(f).$$

O próximo resultado segue do Teorema 2.5.20 de maneira imediata.

Lema 2.5.59. 1. Todo divisor principal tem grau zero.

2. Sejam $f, g \in \Sigma^\times$. Teremos $\mathrm{div}(f) = \mathrm{div}(g)$ se, e somente se, existir $\lambda \in \mathbb{K}^\times$ tal que $f = \lambda g$.

Pela Proposição 2.5.17, temos as propriedades seguintes:

1. $0 = \mathrm{div}(1)$;

2. $\mathrm{div}(f_1) + \mathrm{div}(f_2) = \mathrm{div}(f_1 f_2)$ para todas $f_1, f_2 \in \Sigma$;

3. $-\mathrm{div}(f) = \mathrm{div}(1/f)$ para cada $f \in \Sigma^\times$.

Isso nos conta que o conjunto dos divisores principais é um subgrupo de $\mathrm{Div}(\Sigma)$. Naturalmente, podemos considerar a relação de equivalência que introduzimos em $\mathrm{Div}(\Sigma)$ para obtermos o grupo quociente por esse subgrupo.

Definição 2.5.60. Sejam $D, E \in \mathrm{Div}(\Sigma)$. Se $D - E = \mathrm{div}(f)$ para alguma função $f \in \Sigma^\times$, diremos que D e E são **linearmente equivalentes** e denotaremos $D \sim E$.

O resultado seguinte é uma consequência da Observação 2.5.55 e do item 1 do Lema 2.5.59.

Proposição 2.5.61. Divisores linearmente equivalentes têm o mesmo grau.

A Proposição 2.5.43 nos permite associar um divisor a cada diferencial.

Definição 2.5.62. Sejam $f \in \Sigma^\times$ e t uma variável separante de $\Sigma/\mathbb{K}$.

1. O **divisor da diferencial** $\mathrm{d}t$ é

$$\mathrm{div}(\mathrm{d}t) := \sum_{\mathscr{P}\in\mathfrak{P}(\Sigma)} v_{\mathscr{P}}(\mathrm{d}t)\mathscr{P}.$$

2. O **divisor da diferencial** $f\mathrm{d}t$ é

$$\mathrm{div}(f\mathrm{d}t) := \mathrm{div}(f) + \mathrm{div}(\mathrm{d}t).$$

Observação 2.5.63. Pela Definição 2.5.62, o conjunto

$$\{\mathrm{div}(f\mathrm{d}t);\ f \in \Sigma^\times\}$$

é uma classe de equivalência linear. Essa classe é chamada **classe canônica** e seus elementos são ditos **divisores canônicos**. Pela Definição 2.5.45, o grau de qualquer divisor canônico é $2g-2$, onde g é o gênero de Σ.

2.5.7 Espaços de Riemann-Roch

Seja $\Sigma/\mathbb{K}$ um corpo de funções. Dado $E \in \mathrm{Div}(\Sigma)$, podemos considerar o conjunto dos divisores efetivos que são linearmente equivalentes a E:

$$|E| := \{D \in \mathrm{Div}(\Sigma);\ D \sim E \text{ e } D \geq 0\}.$$

Sabemos que os divisores linearmente equivalentes a E são da forma $E + \mathrm{div}(f)$ para alguma função $f \in \Sigma^\times$. Num primeiro momento, coletemos as funções racionais para as quais esses divisores são efetivos.

Definição 2.5.64. O **espaço de Riemann-Roch** associado ao divisor E é o $\mathbb{K}$-espaço vetorial

$$\mathscr{L}(E) := \{f \in \Sigma^\times;\ E + \mathrm{div}(f) \geq 0\} \cup \{0\}.$$

Denotamos a dimensão desse espaço por $\ell(E)$.

A proposição seguinte nos garante que os espaços de Riemann-Roch têm dimensão finita.

Proposição 2.5.65. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Lema 6.69 da Seção 6.4). Sejam $D, E \in \mathrm{Div}(\Sigma)$.

1. Se $E \geq D$, então $\mathscr{L}(D)$ será um subespaço $\mathbb{K}$-linear de $\mathscr{L}(E)$.
2. Se $\deg(E) < 0$, então $\mathscr{L}(E) = \{0\}$.
3. Se $\deg(E) \geq 0$, então $\ell(E) \leq \deg(E) + 1$. Em particular, $\mathscr{L}(0) = \mathbb{K}$.
4. Se $E \sim D$, então $\mathscr{L}(E)$ e $\mathscr{L}(D)$ serão $\mathbb{K}$-isomorfos.

Teorema 2.5.66 (Teorema de Riemann-Roch)**.** Seja K um divisor canônico de Σ. Para qualquer $E \in \mathrm{Div}(\Sigma)$, vale

$$\ell(E) = \deg(E) - g + 1 + \ell(K - E),$$

onde g é o gênero de Σ.

Demonstração. Pode ser consultada em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 6.70 da Seção 6.4). □

O resultado seguinte decorre do item 2 da Proposição 2.5.65 e do Teorema 2.5.66.

Corolário 2.5.67. Seja $E \in \mathrm{Div}(\Sigma)$ com $\deg(E) > 2g-2$, então

$$\ell(E) = \deg(E) - g + 1.$$

Exemplo 2.5.68. No Exemplo 2.5.47, vimos que $\mathscr{C} = \mathbf{v}_p(C) = \mathbf{v}_p(Y^3 + YZ^2 - X^2Z)$ é uma curva de gênero 1. Consideremos o divisor $4P_\infty$ de $\mathscr{C}$, onde $P_\infty = (1:0:0)$. Pelo Corolário 2.5.67,

$$\ell(4P_\infty) = \deg(4P_\infty) - 1 + 1 = 4.$$

Pelo Exemplo 2.3.6, as funções 1, x, y e y^2 são elementos de $\mathscr{L}(4P_\infty)$. Mostraremos que $\{1, x, y, y^2\}$ é uma base de $\mathscr{L}(4P_\infty)$. Para isso, basta mostrarmos que $\{1, x, y, y^2\}$ é linearmente independente sobre $\overline{\mathbb{F}}_{3^2}$.

Sejam $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \overline{\mathbb{F}}_{3^2}$ tais que

$$\alpha_0 + \alpha_1 x + \alpha_2 y + \alpha_3 y^2 = 0 \quad \text{em} \quad \overline{\mathbb{F}}_{3^2}(x,y) = \mathrm{Frac}\left(\frac{\overline{\mathbb{F}}_{3^2}[X,Y]}{(C_Z)}\right).$$

Então,

$$C_Z \mid \alpha_0 + \alpha_1 X + \alpha_2 Y + \alpha_3 Y^2 \quad \text{em} \quad \overline{\mathbb{F}}_{3^2}[X,Y]$$

Visto que $\deg(C_Z) = 3$, o polinômio $\alpha_0 + \alpha_1 X + \alpha_2 Y + \alpha_3 Y^2$ é nulo. Portanto, $\{1, x, y, y^2\}$ é linearmente independente sobre $\overline{\mathbb{F}}_{3^2}$.

2.5.8 Séries lineares

Feita a definição dos espaços de Riemann-Roch, podemos reescrever o conjunto dos divisores efetivos que são linearmente equivalentes a $E \in \mathrm{Div}(\Sigma)$:

$$|E| = \{E + \mathrm{div}(f);\ f \in \mathscr{L}(E) \setminus \{0\}\}.$$

Definição 2.5.69. Uma **série linear** $\mathscr{D}$ em Σ é um conjunto da forma

$$\{E + \mathrm{div}(f);\ f \in \mathscr{S} \setminus \{0\}\}$$

onde $\mathscr{S}$ é um subespaço vetorial de $\mathscr{L}(E)$. Quando $\mathscr{D} = |E|$, diremos que $\mathscr{D}$ é uma **série linear completa**.

Pelo item 2 do Lema 2.5.59, a aplicação

$$\begin{array}{ccc} \mathscr{D} & \to & \mathbb{P}(\mathscr{S}) \\ E + \mathrm{div}(f) & \mapsto & [f] \end{array}$$

é uma bijeção. Ela induz uma estrutura de espaço projetivo em $\mathscr{D}$.

Observação 2.5.70. Para indicarmos o divisor e o subespaço vetorial que originaram a série linear, utilizaremos a notação $\mathscr{D} \cong \mathbb{P}(\mathscr{S}) \subset |E|$ em vez de, simplesmente, $\mathscr{D}$.

Definição 2.5.71. 1. A **dimensão de** $\mathscr{D}$ é o número $\dim(\mathscr{D}) := \dim_{\mathbb{K}}(\mathscr{S}) - 1$.

2. O **grau de** $\mathscr{D}$ é o número $\deg(\mathscr{D}) := \deg(E)$.

3. Dizemos que $\mathscr{D}$ é uma g^N_d em $\mathscr{X}$ onde $N := \dim(\mathscr{D})$ e $d := \deg(\mathscr{D})$.

Observação 2.5.72. Pela Proposição 2.5.61, todos os divisores de $\mathscr{D}$ têm o mesmo grau, a saber, $\deg(\mathscr{D})$.

Exemplo 2.5.73. No Exemplo 2.5.68, vimos que $\mathscr{L}(4P_\infty) = \langle 1, x, y, y^2 \rangle$. A série linear completa

$$|4P_\infty| = \{4P_\infty + \operatorname{div}(\alpha_0 + \alpha_1 x + \alpha_2 y + \alpha_3 y^2);\ (\alpha_0 : \alpha_1 : \alpha_2 : \alpha_3) \in \mathbb{P}^3(\overline{\mathbb{F}}_{3^2})\}$$

é uma g^3_4 em $\mathscr{C} = \mathbf{v}_p(C) = \mathbf{v}_p(Y^3 + YZ^2 - X^2Z)$.

Definição 2.5.74. Uma série linear $\mathscr{D}_1 \cong \mathbb{P}(\mathscr{S}_1) \subset |E_1|$ será dita **subsérie** de $\mathscr{D}_2 \cong \mathbb{P}(\mathscr{S}_2) \subset |E_2|$ se tivermos as inclusões $\mathscr{L}(E_1) \subset \mathscr{L}(E_2)$ e $\mathscr{S}_1 \subset \mathscr{S}_2$.

2.6 Curvas espaciais

Definição 2.6.1. Uma **representação de ramo** é um ponto de $\mathbb{P}^N(\mathbb{K}((T))) \setminus \mathbb{P}^N(\mathbb{K})$.

Observação 2.6.2. De maneira análoga ao que fizemos na Seção 2.4 para $N = 2$, podemos definir as noções de coordenadas especiais, centro de uma representação de ramo, coordenadas afins especiais, representações de ramo equivalentes e representações de ramo primitivas para $N \geq 3$.

Definição 2.6.3. Um **ramo** é uma classe de equivalência de representações de ramos primitivas. O **centro de um ramo** é o centro de qualquer uma de suas representações primitivas.

Consideremos um corpo de funções $\Sigma/\mathbb{K}$. Seja $Q = (x_0 : \cdots : x_M) \in \mathbb{P}^M(\Sigma)$. Dados $i, j \in \{0, \ldots, M\}$ com $x_i \neq 0$ e $x_j \neq 0$, temos

$$\mathbb{K}\left(\frac{x_0}{x_i}, \ldots, \frac{x_M}{x_i}\right) = \mathbb{K}\left(\frac{x_0}{x_j}, \ldots, \frac{x_M}{x_j}\right),$$

uma vez que

$$\frac{x_k}{x_i} = \frac{x_k}{x_j} \cdot \frac{x_j}{x_i} \quad \text{e} \quad \frac{x_k}{x_j} = \frac{x_k}{x_i} \cdot \frac{x_i}{x_j}$$

para cada $k \in \{0, \ldots, M\}$.

Definição 2.6.4. Seja $Q = (x_0 : \cdots : x_M) \in \mathbb{P}^M(\Sigma)$. O **corpo de** Q é

$$\mathbb{K}(Q) := \mathbb{K}\left(\frac{x_0}{x_i}, \ldots, \frac{x_M}{x_i}\right)$$

para qualquer $i \in \{0, \ldots, M\}$ com $x_i \neq 0$.

Definição 2.6.5. Sejam $Q = (x_0 : \cdots : x_M) \in \mathbb{P}^M(\Sigma)$ e $\mathscr{P} \in \mathfrak{P}(\Sigma)$. O **ramo associado a $\mathscr{P}$ com respeito a Q** é o ramo com representação primitiva $(\tau(x_0) : \cdots : \tau(x_M))$.

Definição 2.6.6. Seja $Q = (x_0 : \cdots : x_M) \in \mathbb{P}^M(\Sigma)$. A **curva irredutível em $\mathbb{P}^M(\mathbb{K})$ dada por Q** é o conjunto

$$\mathscr{X} := \{P \in \mathbb{P}^M(\mathbb{K});\ P \text{ é o centro do ramo associado a algum lugar de } \Sigma \text{ com respeito a } Q\}.$$

Nesse caso:

1. o **corpo de funções de $\mathscr{X}$** é $\mathbb{K}(\mathscr{X}) := \Sigma$;
2. um **ramo de $\mathscr{X}$** é um ramo associado a algum lugar de Σ com respeito a Q;
3. o **gênero de $\mathscr{X}$** é o gênero de Σ;
4. o par $(\mathscr{X}, Q)$ é um **modelo de Σ em $\mathbb{P}^M(\mathbb{K})$**;
5. as funções $x_0, \ldots, x_M$ são as **funções coordenadas de $\mathscr{X}$**.

Teorema 2.6.7. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teoremas 7.2 e 7.3 da Seção 7.1). Seja $\mathscr{X}$ uma curva projetiva irredutível.

1. Cada ponto de $\mathscr{X}$ é o centro de uma quantidade finita de ramos de $\mathscr{X}$.
2. O conjunto $\mathscr{X}$ é infinito.

Generalizemos a definição de curvas planas projetivas. No conjunto

$$\{F \in \mathbb{K}[X_0, \ldots, X_M] \setminus \mathbb{K};\ F \text{ é homogêneo}\},$$

definamos a relação de equivalência seguinte:

$$F_1 \equiv_h F_2 \Leftrightarrow F_1 = \lambda F_2 \text{ para algum } \lambda \in \mathbb{K}^\times.$$

Consideremos o conjunto quociente

$$\mathfrak{H} := \frac{\{F \in \mathbb{K}[X_0, \ldots, X_M] \setminus \mathbb{K};\ F \text{ é homogêneo}\}}{\equiv_h}$$

e a aplicação quociente

$$\mathbf{v}\colon \{F \in \mathbb{K}[X_0, \ldots, X_M] \setminus \mathbb{K};\ F \text{ é homogêneo}\} \to \mathfrak{H}.$$

Definição 2.6.8. Sejam $G \in \mathbb{K}[X_0, \ldots, X_M] \setminus \mathbb{K}$ um polinômio homogêneo e $\Delta = \mathbf{v}(G)$.

1. A **hipersuperfície definida pela equação $G(X_0, \ldots, X_M) = 0$ em $\mathbb{P}^M(\mathbb{K})$** é a classe Δ.

2. O **conjunto dos pontos de** Δ é

$$\Delta = \{(\alpha_0 : \cdots : \alpha_M) \in \mathbb{P}^M(\mathbb{K});\ G(\alpha_0, \ldots, \alpha_M) = 0\}.$$

3. O grau de Δ é $\deg(\Delta) := \deg(G)$.

4. Se $\deg(\Delta) = 1$, diremos que Δ é um hiperplano.

5. Seja $P \in \Delta$. Diremos que P é um **ponto singular de** Δ se

$$\left(\frac{\partial G}{\partial X_0}, \ldots, \frac{\partial G}{\partial X_M}\right) = (0, \ldots, 0).$$

   Caso contrário, diremos que P é um **ponto não singular de** Δ e que

$$T_P\Delta = \mathbf{v}\left(\frac{\partial G}{\partial X_0}X_0 + \cdots + \frac{\partial G}{\partial X_M}X_M\right)$$

   é o **hiperplano tangente a** Δ **em** P.

6. Diremos que Δ é uma **hipersuperfície não singular** se todos os seus pontos forem não singulares. Caso contrário, diremos que Δ é uma **hipersuperfície singular**.

7. Consideremos $A \in \mathrm{GL}(M+1, \mathbb{K})$ e escrevamos $A^{-1} = (b_{ij})_{0 \leq i,j \leq M}$. A imagem de Δ por $\mathfrak{T}_A \in \mathrm{PGL}(M+1, \mathbb{K})$, a transformação $\mathbb{K}$-linear dada por A em $\mathbb{P}^M(\mathbb{K})$, é

$$\mathfrak{T}_A \cdot \Delta := \mathbf{v}\left(G\left(\sum_{j=0}^{M} b_{0j}X_j, \ldots, \sum_{j=0}^{M} b_{Mj}X_j\right)\right).$$

Definição 2.6.9. Consideremos uma hipersuperfície $\Delta = \mathbf{v}(G)$ em $\mathbb{P}^M(\mathbb{K})$ e um ramo γ. Sejam P o centro de γ e $(x_0(T) : \cdots : x_M(T))$ uma representação primitiva de γ escrita em coordenadas especiais.

1. A **multiplicidade de interseção de** Δ **e** γ é

$$(\Delta, \gamma)_P := \mathrm{ord}_T G(x_0(T), \ldots, x_M(T)).$$

2. Se existir um hiperplano H em $\mathbb{P}^M(\mathbb{K})$ satisfazendo $(H, \gamma)_P = 1$, diremos que γ é **linear**.

Teorema 2.6.10. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teoremas 7.5 e 7.6 da Seção 7.1). Sejam $\mathscr{X}$ uma curva irredutível dada pelo ponto $Q = (x_0 : \cdots : x_M)$ e $\Delta = \mathbf{v}(G)$ uma hipersuperfície em $\mathbb{P}^M(\mathbb{K})$. Consideremos um ramo γ de $\mathscr{X}$ com centro P.

1. Teremos $\mathscr{X} \subset \Delta$ se, e somente se, $G(x_0, \ldots, x_M) = 0$;

2. Se $\mathscr{X}$ não estiver contida em Δ, então $\mathscr{X} \cap \Delta$ será finito e valerá $(\Delta, \gamma)_P \in \mathbb{N}$.

Definição 2.6.11. Sejam $\mathscr{X}$ uma curva irredutível e Δ uma hipersuperfície em $\mathbb{P}^M(\mathbb{K})$. Suponhamos que Δ não contenha $\mathscr{X}$. O **divisor cortado por Δ em $\mathscr{X}$** é

$$\Delta \cdot \mathscr{X} := \sum_{\substack{\gamma \text{ é o ramo de } \mathscr{X} \\ \text{associado a } \mathscr{P} \in \mathfrak{P}(\mathbb{K}(\mathscr{X}))}} (\Delta, \gamma)_P \mathscr{P}.$$

Proposição 2.6.12. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Corolário 7.8 da Seção 7.1). Seja $\mathscr{X}$ uma curva irredutível em $\mathbb{P}^M(\mathbb{K})$. Se H_1 e H_2 forem dois hiperplanos em $\mathbb{P}^M(\mathbb{K})$ que não contêm $\mathscr{X}$, então

$$\deg(H_1 \cdot \mathscr{X}) = \deg(H_2 \cdot \mathscr{X}).$$

Definição 2.6.13. Seja $\mathscr{X}$ uma curva irredutível em $\mathbb{P}^M(\mathbb{K})$. O **grau de $\mathscr{X}$** é

$$\deg(\mathscr{X}) := \deg(H \cdot \mathscr{X})$$

para qualquer hiperplano H em $\mathbb{P}^M(\mathbb{K})$ que não contém $\mathscr{X}$.

Definição 2.6.14. Sejam $\mathscr{X}$ uma curva irredutível em $\mathbb{P}^M(\mathbb{K})$ e $P \in \mathscr{X}$.

1. Se P for o centro de pelo menos dois ramos de $\mathscr{X}$ ou se P for o centro de um ramo não linear de $\mathscr{X}$, diremos que P é um **ponto singular de $\mathscr{X}$**. Caso contrário, diremos que P é um **ponto não singular de $\mathscr{X}$**.

2. Se todos os pontos de $\mathscr{X}$ forem não singulares, diremos que $\mathscr{X}$ é uma **curva não singular**. Caso contrário, diremos que $\mathscr{X}$ é uma **curva singular**.

Teorema 2.6.15. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 7.15 da Seção 7.1). Seja $\mathscr{X}$ uma curva irredutível em $\mathbb{P}^M(\mathbb{K})$. O conjunto de todos os pontos singulares de $\mathscr{X}$ é finito.

2.7 Aplicações racionais

Sejam $\Sigma/\mathbb{K}$ um corpo de funções e $Q = (x_0 : \cdots : x_M) \in \mathbb{P}^M(\Sigma)$ satisfazendo $\Sigma = \mathbb{K}(Q)$. Seja $\mathscr{X}$ a curva irredutível dada por Q.

Definição 2.7.1. (COUTINHO, 2019, Definições 1.3.20, 1.3.21 e 1.3.23). Consideremos o ponto $\phi = (f_0 : \cdots : f_N) \in \mathbb{P}^N(\Sigma)$.

1. Dizemos que ϕ é a **aplicação racional com funções coordenadas** $f_0, \ldots, f_N$ e a denotamos por $\phi : \mathscr{X} \dashrightarrow \mathbb{P}^N(\mathbb{K})$.

2. Seja $P = (\alpha_0 : \cdots : \alpha_M) \in \mathscr{X}$. Diremos que ϕ **está definida em** P se existirem polinômios $A_0, \ldots, A_N \in \mathbb{K}[X_0, \ldots, X_M]$ homogêneos do mesmo grau satisfazendo

$$(f_0 : \cdots : f_N) = (A_0(x_0, \ldots, x_M) : \cdots : A_N(x_0, \ldots, x_M))$$

e

$$A_i(\alpha_0,\ldots,\alpha_M) \neq 0$$

para algum $i \in \{0,\ldots,N\}$. Nesse caso, definimos

$$\phi(P) \coloneqq (A_0(\alpha_0,\ldots,\alpha_M) : \cdots : A_N(\alpha_0,\ldots,\alpha_M)).$$

3. Se ϕ estiver definida em todos os pontos de $\mathscr{X}$, diremos que ϕ é um **morfismo**. Se esse for o caso, denotaremos ϕ por $\phi\colon \mathscr{X} \to \mathbb{P}^N(\mathbb{K})$.

Observação 2.7.2. (COUTINHO, 2019, Observação 1.3.24). Consideremos uma aplicação racional $\phi = (f_0 : \cdots : f_N)\colon \mathscr{X} \dashrightarrow \mathbb{P}^N(\mathbb{K})$. Dois casos são possíveis.
CASO 1. Se $\mathbb{K} = \mathbb{K}(\phi)$, então ϕ é um morfismo constante.
CASO 2. Se $\mathbb{K} \subsetneq \mathbb{K}(\phi)$, então $\mathbb{K}(\phi)/\mathbb{K}$ será um corpo de funções e será possível definir a curva irredutível em $\mathbb{P}^N(\mathbb{K})$ dada por ϕ:

$$\mathscr{Y} \coloneqq \{P \in \mathbb{P}^N(\mathbb{K});\ P \text{ é o centro do ramo assciado a algum lugar de } \mathbb{K}(\phi) \text{ com respeito a } \phi\}.$$

Sempre que dissermos que $\phi\colon \mathscr{X} \dashrightarrow \mathbb{P}^N(\mathbb{K})$ é uma aplicação racional, estaremos assumindo que se trata do segundo caso.

Proposição 2.7.3. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Considerações que sucedem a Definição 7.16 da Seção 7.2). Consideremos o segundo caso da Observação 2.7.2. Seja $P \in \mathscr{X}$. Se ϕ estiver definida em P, então $\phi(P) \in \mathscr{Y}$.

Definição 2.7.4. (COUTINHO, 2019, Definição 1.3.26). Consideremos o segundo caso da Observação 2.7.2.

1. Dizemos que $\mathscr{Y}$ é a **imagem de** ϕ e denotamos ϕ por $\phi\colon \mathscr{X} \dashrightarrow \mathscr{Y}$.

2. Se $\Sigma = \mathbb{K}(\phi)$, diremos que ϕ é uma **equivalência birracional** e que $\mathscr{X}$ e $\mathscr{Y}$ são **birracionalmente equivalentes**. Nesse caso, existirá uma aplicação birracional $\phi^{-1}\colon \mathscr{Y} \dashrightarrow \mathscr{X}$ satisfazendo $\phi^{-1} \circ \phi = \mathrm{id}_{\mathscr{X}}$ e $\phi \circ \phi^{-1} = \mathrm{id}_{\mathscr{Y}}$. Aqui, $\phi^{-1} \circ \phi = \mathrm{id}_{\mathscr{X}}$ significa que, para todo $P \in \mathscr{X}$ tal que ϕ está definida em P e ϕ^{-1} está definida em $\phi(P)$, vale $\phi^{-1}(\phi(P)) = P$. A expressão $\phi \circ \phi^{-1} = \mathrm{id}_{\mathscr{Y}}$ deve ser entendida de forma análoga.

3. Se $\Sigma = \mathbb{K}(\phi)$ e ϕ for um morfismo, diremos que ϕ é um **morfismo birracional**. Se ϕ^{-1} for um morfismo, diremos que ϕ é um **isomorfismo** e que $\mathscr{X}$ e $\mathscr{Y}$ são **isomorfas**.

Teorema 2.7.5. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 7.17 da Seção 7.2). Toda curva irredutível é birracionalmente equivalente a uma curva plana.

Proposição 2.7.6. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Considerações que sucedem a Definição 7.16 da Seção 7.2). Sejam $\phi = (f_0 : \cdots : f_N)\colon \mathscr{X} \to \mathbb{P}^N(\mathbb{K})$ uma aplicação

racional e $P \in \mathscr{X}$ um ponto não singular. Sejam $\mathscr{P}$ o único lugar de Σ correspondente a P, t um parâmetro local em $\mathscr{P}$ e

$$e_{\mathscr{P}} = -\min\{v_{\mathscr{P}}(f_0), \ldots, v_{\mathscr{P}}(f_N)\}.$$

Então, ϕ está definida em P. Mais precisamente,

$$0 \in \{v_{\mathscr{P}}(t^{e_{\mathscr{P}}} f_0), \ldots, v_{\mathscr{P}}(t^{e_{\mathscr{P}}} f_N)\} \subset \mathbb{N}$$

e

$$\phi(P) = ((t^{e_{\mathscr{P}}} f_0)(\mathscr{P}) : \cdots : (t^{e_{\mathscr{P}}} f_N)(\mathscr{P})).$$

Em particular, se $\mathscr{X}$ for não singular, então ϕ será um morfismo.

Definição 2.7.7. Seja $\phi\colon \mathscr{X} \to \mathbb{P}^N(\mathbb{K})$ um morfismo. Diremos que ϕ é **não degenerado** se sua imagem não estiver contida em nenhum hiperplano de $\mathbb{P}^N(\mathbb{K})$.

Observação 2.7.8. Pelo item 1 do Teorema 2.6.10, o morfismo $\phi = (f_0 : \cdots : f_N)\colon \mathscr{X} \to \mathbb{P}^N(\mathbb{K})$ será não degenerado se, e somente se, o conjunto $\{f_0, \ldots, f_N\}$ for linearmente independente sobre $\mathbb{K}$.

2.7.1 Modelos não singulares

Seja $\Sigma/\mathbb{K}$ um corpo de funções e seja $(\mathscr{X}, Q)$ um modelo de Σ em $\mathbb{P}^M(\mathbb{K})$. O resultado seguinte nos conta que existe um modelo não singular de Σ e que esse modelo é único a menos de isomorfismo.

Teorema 2.7.9. (FULTON, 2008, Teorema 3 da Seção 7.5). Existem uma curva irredutível e não singular $\tilde{\mathscr{X}}$ e um morfismo birracional sobrejetor $\phi\colon \tilde{\mathscr{X}} \to \mathscr{X}$. Além disso, se $\mathscr{X}'$ for outra curva irredutível e não singular equipada com um morfismo birracional sobrejetor $\phi'\colon \mathscr{X}' \to \mathscr{X}$, então existirá um único isomorfismo $\psi\colon \tilde{X} \to \mathscr{X}'$ tal que $\phi' \circ \psi = \phi$.

Definição 2.7.10. Consideremos a notação do Teorema 2.7.9. A curva $\tilde{X}$ é o **modelo não singular de** $\mathscr{X}$.

O próximo resultado decorre das Definições 2.6.5, 2.6.6 e 2.6.14.

Proposição 2.7.11. Suponhamos que $\mathscr{X}$ seja um modelo não singular de Σ. Então, existem as correspondências biunívocas seguintes:

$$\{\text{pontos de } \mathscr{X}\} \leftrightarrow \{\text{lugares de } \Sigma\} \leftrightarrow \{\text{ramos de } \mathscr{X}\}.$$

Observação 2.7.12. Na Seção 2.5, definimos muitos objetos indexados por lugares de Σ. A partir de agora, quando considerarmos um modelo não singular $\mathscr{X}$ de Σ, passaremos a indexar esses objetos pelos pontos correspondentes. Por exemplo, escreveremos v_P e $\sum_{P \in \mathscr{X}} n_P P \in \mathrm{Div}(\mathscr{X})$ no lugar de $v_{\mathscr{P}}$ e $\sum_{\mathscr{P} \in \mathfrak{P}(\Sigma)} n_{\mathscr{P}} \mathscr{P} \in \mathrm{Div}(\Sigma)$ respectivamente.

2.8 Relação entre séries lineares e morfismos

Seja $\mathscr{X}$ uma curva irredutível e não singular. O objetivo desta seção é mostrar a equivalência entre séries lineares livres de ponto base de dimensão N e as classes de equivalência projetiva de morfismos não degenerados de $\mathscr{X}$ em $\mathbb{P}^N(\mathbb{K})$.

2.8.1 Morfismos provenientes de séries lineares

Seja $\mathscr{D} \cong \mathbb{P}(\mathscr{S}) \subset |E|$ uma série linear em $\mathscr{X}$ de dimensão N e grau d.

Definição 2.8.1. Para cada $i \in \mathbb{N}$ e cada $P \in \mathscr{X}$, definimos o conjunto

$$\mathscr{D}_i(P) := \{D \in \mathscr{D};\ D \geq iP\}.$$

Observação 2.8.2. 1. Visto que $(i+1)P \geq iP$, temos $\mathscr{D}_i(P) \supset \mathscr{D}_{i+1}(P)$.

2. Como todos os divisores em $\mathscr{D}$ são efetivos de grau d, vale $\mathscr{D}_j(P) = \emptyset$ quando $j > d$.

Lema 2.8.3. (TORRES, 2000, Lema 1.3 da Seção 1.2). Sejam $i \in \mathbb{N}$ e $P \in \mathscr{X}$. Temos:
1. $\mathscr{D}_i(P)$ é uma subsérie de $\mathscr{D}$;
2. $\dim(\mathscr{D}_i(P)) - \dim(\mathscr{D}_{i+1}(P)) \leq 1$.

Definição 2.8.4. A **multiplicidade de $\mathscr{D}$ em P** é o inteiro não negativo

$$b(P) := \min\{v_P(D);\ D \in \mathscr{D}\}.$$

Notemos que $b(P) > 0$ se, e somente se, $P \in \mathrm{Supp}(D)$ para todo $D \in \mathscr{D}$. Consequentemente, $b(P) \neq 0$ somente para um número finito de $P \in \mathscr{X}$. Isso nos permite definir o seguinte divisor efetivo de $\mathscr{X}$:

$$\mathsf{B} := \sum_{P \in \mathscr{X}} b(P)P.$$

Observação 2.8.5. Notemos que B é o maior divisor que aparece em todos os divisores de $\mathscr{D}$. Mais precisamente:

1. $D \geq \mathsf{B}$ para todo $D \in \mathscr{D}$;

2. dado $A \in \mathrm{Div}(\mathscr{X})$ tal que $D \geq A$ para todo $D \in \mathscr{D}$, temos $\mathsf{B} \geq A$.

Definição 2.8.6. 1. O divisor B é chamado **divisor fixo de $\mathscr{D}$**.

2. Um ponto $P \in \mathrm{Supp}(\mathsf{B})$ é chamado **ponto base de $\mathscr{D}$**.

3. Se $\mathsf{B} = 0$, diremos que $\mathscr{D}$ é **livre de ponto base**.

Observação 2.8.7. A série linear $\mathscr{D}$ será livre de ponto base se, e somente se, para cada $P \in \mathscr{X}$, existir $f \in \mathscr{S} \setminus \{0\}$ tal que $v_P(E + \mathrm{div}(f)) = 0$.

Construiremos uma série linear livre de ponto base a partir de $\mathscr{D}$. A maneira mais natural de fazer isso é remover o divisor fixo de cada divisor de $\mathscr{D}$:

$$\mathscr{D}^{\mathsf{B}} := \{D - \mathsf{B};\ D \in \mathscr{D}\}.$$

Com certeza, não há pontos comuns aos suportes de todos os divisores desse conjunto. Falta verificar que $\mathscr{D}^{\mathsf{B}}$ é uma série linear.

Notemos que $\mathscr{S} \subset \mathscr{L}(E - \mathsf{B})$. De fato, dada $f \in \mathscr{S}$, temos $E + \operatorname{div}(f) \geq \mathsf{B}$ e, por conseguinte, $f \in \mathscr{L}(E - \mathsf{B})$. Reescrevendo

$$\mathscr{D}^{\mathsf{B}} = \{E + \operatorname{div}(f) - \mathsf{B};\ f \in \mathscr{S} \setminus \{0\}\} \subset |E - \mathsf{B}|,$$

percebemos que $\mathscr{D}^{\mathsf{B}} \cong \mathbb{P}(\mathscr{S}) \subset |E - \mathsf{B}|$ é uma $g^N_{d-\deg(\mathsf{B})}$ livre de ponto base em $\mathscr{X}$. Como $\mathscr{L}(E - \mathsf{B}) \subset \mathscr{L}(E)$, $\mathscr{D}^{\mathsf{B}}$ é uma subsérie de $\mathscr{D}$.

O próximo resultado nos conta que podemos recuperar o divisor E a partir de $\mathscr{D}$.

Lema 2.8.8. (TORRES, 2000, Lema 1.4 da Seção 1.2). Sejam $\mathscr{D} \cong \mathbb{P}(\mathscr{S}) \subset |E|$ uma série linear e $\{f_0, \ldots, f_N\}$ uma base de $\mathscr{S}$. Então,

$$v_P(E) = b(P) - \min\{v_P(f_0), \ldots, v_P(f_N)\}$$

para cada $P \in \mathscr{X}$.

Definiremos um morfismo de $\mathscr{X}$ num espaço projetivo a partir da série linear $\mathscr{D}$. Dado $P \in \mathscr{X}$, podemos tomar $D \in \mathscr{D}$ satisfazendo $v_P(D) = b(P)$. Notemos que D está em $\mathscr{D}_{b(P)}$, mas não em $\mathscr{D}_{b(P)+1}$. Em outras palavras, $\mathscr{D} = \mathscr{D}_{b(P)} \supsetneq \mathscr{D}_{b(P)+1}$. Pelo item 2 do Lema 2.8.3, $\dim(\mathscr{D}_{b(P)+1}) = \dim(\mathscr{D}) - 1$, ou seja, $\mathscr{D}_{b(P)+1}$ é um hiperplano em $\mathscr{D}$. Como $\mathscr{D}_{b(P)+1}$ é um ponto do espaço dual $\mathscr{D}^*$, podemos considerar a aplicação

$$\begin{array}{rccc} \phi_{\mathscr{D}}\colon & \mathscr{X} & \to & \mathscr{D}^* \cong \mathbb{P}(\mathscr{S})^* \\ & P & \mapsto & \mathscr{D}_{b(P)+1}. \end{array}$$

Descreveremos $\phi_{\mathscr{D}}$ em coordenadas homogêneas. Para isso, fixemos $\{f_0, \ldots, f_N\}$ como uma base de $\mathscr{S}$. Tomando $P \in \mathscr{X}$, determinaremos a equação do hiperplano $\mathscr{D}_{b(P)+1}$. Dada $f \in \mathscr{S} \setminus \{0\}$ qualquer, podemos escrever

$$f = \sum_{i=0}^{N} a_i f_i$$

para certos $a_0, \ldots, a_N \in \mathbb{K}$ não todos nulos; em particular, a classe de f em $\mathbb{P}(\mathscr{S})$ é representada pelo ponto $(a_0 : \cdots : a_N)$ em $\mathbb{P}^N(\mathbb{K})$.

Pela definição de $b(P)$, temos

$$v_P(E) - b(P) + v_P(f) \geq 0.$$

Escolhendo um parâmetro local t de $\mathscr{X}$ em P, podemos reescrever a desigualdade anterior:

$$v_P(t^{v_P(E)-b(P)}f) \geq 0.$$

Em outras palavras, podemos avaliar a função $t^{v_P(E)-b(P)}f$ em P. Além disso, temos as equivalências

$$\begin{aligned} E+\operatorname{div}(f) \in \mathscr{D}_{b(P)+1} &\Leftrightarrow v_P(t^{v_P(E)-b(P)}f) \geq 1 \\ &\Leftrightarrow (t^{v_P(E)-b(P)}f)(P) = 0 \\ &\Leftrightarrow \sum_{i=0}^{N} (t^{v_P(E)-b(P)}f_i)(P)a_i = 0. \end{aligned}$$

Em outras palavras, o hiperplano $\mathscr{D}_{b(P)+1}$ tem a equação

$$\sum_{i=0}^{N} (t^{v_P(E)-b(P)}f_i)(P)X_i = 0$$

na base fixada. No espaço dual, esse hiperplano é representado pelo ponto

$$((t^{v_P(E)-b(P)}f_0)(P) : \cdots : (t^{v_P(E)-b(P)}f_N)(P)).$$

Pelo Lema 2.8.8, o morfismo $\phi_{f_0,\ldots,f_N} := (f_0 : \cdots : f_N)$ fornece a descrição de $\phi_{\mathscr{D}}$ desejada. Ele será chamado **morfismo associado a** $\mathscr{D}$.

Observação 2.8.9. Notemos que $\phi_{\mathscr{D}}$ e $\phi_{\mathscr{D}^{\mathrm{B}}}$ possuem a mesma descrição em coordenadas.

Exemplo 2.8.10. No Exemplo 2.5.68, vimos que $\{1,x,y,y^2\}$ é uma base de $\mathscr{L}(4P_\infty)$. Portanto, o morfismo associado à série linear $|4P_\infty|$ é

$$\pi = (1 : x : y : y^2) \colon \mathscr{C} \to \mathbb{P}^3(\overline{\mathbb{F}}_{3^2}).$$

Proposição 2.8.11. (TORRES, 2000, Lema 1.5 da Seção 1.2). Se $\{f_0,\ldots,f_N\}$ e $\{g_0,\ldots,g_N\}$ forem duas bases de $\mathscr{S}$ sobre $\mathbb{K}$, então existirá uma transformação $\mathbb{K}$-linear $\mathfrak{T}$ de $\mathbb{P}^N(\mathbb{K})$ tal que

$$\phi_{g_0,\ldots,g_N} = \mathfrak{T} \circ \phi_{f_0,\ldots,f_N}.$$

2.8.2 Séries lineares provenientes de morfismos

Seja $\phi = (f_0 : \cdots : f_N) \colon \mathscr{X} \to \mathbb{P}^N(\mathbb{K})$ um morfismo. Definamos

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

para cada $P \in \mathscr{X}$. Visto que $e_P \neq 0$ apenas para uma quantidade finita de $P \in \mathscr{X}$, podemos definir o divisor

$$E = E_{f_0,\ldots,f_N} = \sum_{P\in\mathscr{X}} e_P P.$$

Notemos que $f_i \in \mathscr{L}(E)$ para cada $i \in \{0,\ldots,N\}$. Seja

$$\mathscr{S} = \langle f_0,\ldots,f_N\rangle \subset \mathscr{L}(E).$$

Temos a seguinte série linear em $\mathscr{X}$:

$$\mathscr{D}_{f_0,\ldots,f_N} := \{E + \operatorname{div}(f);\ f \in \mathscr{S}\setminus\{0\}\} \subset |E|.$$

Essa série linear é livre de ponto base. De fato, se tomarmos $i_0 \in \{0,\ldots,N\}$ de modo que $e_P = -v_P(f_{i_0})$, teremos $v_P(E+\operatorname{div}(f_{i_0})) = 0$.

Observação 2.8.12. Dada $h \in \mathbb{K}(\mathscr{X})^\times$, temos

$$E_{f_0h,\ldots,f_Nh} = E_{f_0,\ldots,f_N} - \operatorname{div}(h)$$

e, por consequência,

$$\mathscr{D}_{f_0h,\ldots,f_Nh} = \mathscr{D}_{f_0,\ldots,f_N}.$$

Em outras palavras, a série linear definida acima não depende da escolha das funções coordenadas para o morfismo ϕ. Com isso, denotaremos $\mathscr{D}_{f_0,\ldots,f_N}$ por $\mathscr{D}_\phi$.

Lema 2.8.13. (TORRES, 2000, Lema 1.9 da Seção 1.3).

1. Se ϕ for não degenerado, então $\dim(\mathscr{D}_\phi) = N$.
2. Se $\mathfrak{T}$ for uma projetividade em $\mathbb{P}^N(\mathbb{K})$, então $\mathscr{D}_{\mathfrak{T}\circ\phi} = \mathscr{D}_\phi$.

Agora, suponhamos que ϕ seja não degenerado. Então,

$$\mathscr{D}_\phi = \left\{ E + \operatorname{div}\left(\sum_{i=0}^{N} a_i f_i\right);\ (a_0:\cdots:a_N) \in \mathbb{P}^N(\mathbb{K}) \right\},$$

pois

$$\sum_{i=0}^{N} a_i f_i = 0 \Leftrightarrow a_i = 0\ \forall i \in \{0,\ldots,N\}.$$

Identificando o ponto $(a_0:\cdots:a_N)$ com o hiperplano de equação

$$\sum_{i=0}^{N} a_i X_i = 0,$$

podemos reescrever

$$\mathscr{D}_\phi = \{\phi^{-1}(H);\ H \text{ é um hiperplano em } \mathbb{P}^N(\mathbb{K})\},$$

onde $\phi^{-1}(H)$ denota $E + \operatorname{div}\left(\sum_{i=0}^{N} a_i f_i\right)$.

Finalmente, estabeleceremos a equivalência anunciada no início desta seção. Seja $\mathscr{L}$ o conjunto das séries lineares livres de ponto base de dimensão N em $\mathscr{X}$ e seja $\mathscr{M}$ o conjunto

das classes de equivalência projetiva de morfismos não degenerados de $\mathscr{X}$ em $\mathbb{P}^N(\mathbb{K})$. Isto é, os elementos de $\mathscr{M}$ são da forma

$$[\phi] := \{\mathfrak{T}\circ\phi;\ \mathfrak{T} \text{ é uma projetividade em } \mathbb{P}^N(\mathbb{K})\},$$

onde ϕ é um morfismo de $\mathscr{X}$ em $\mathbb{P}^N(\mathbb{K})$.

Os Lemas 2.8.11 e 2.8.13 nos permitem definir as duas aplicações seguintes:

$$M\colon \begin{array}{ccc}\mathscr{L} & \to & \mathscr{M}\\ \mathscr{D} & \mapsto & [\phi_{\mathscr{D}}]\end{array} \quad \text{e} \quad L\colon \begin{array}{ccc}\mathscr{M} & \to & \mathscr{L}\\ [\phi] & \mapsto & \mathscr{D}_\phi.\end{array}$$

Proposição 2.8.14. (TORRES, 2000, Lema 1.13 da Seção 1.4). Temos

$$M\circ L = \mathrm{id}_{\mathscr{M}} \quad \text{e} \quad L\circ M = \mathrm{id}_{\mathscr{L}}.$$

2.9 Teoria de Stöhr-Voloch

Consideremos uma curva irredutível e não singular $\mathscr{X}$ e um morfismo não degenerado $\phi = (f_0 : \cdots : f_N)\colon \mathscr{X} \to \mathbb{P}^N(\mathbb{K})$. Seja $\mathscr{D}$ a g^N_d livre de ponto base proveniente de ϕ. Como vimos na Subseção 2.8.1, podemos escrever

$$\mathscr{D} = \left\{ \mathrm{div}\left(\sum_{i=0}^{N} a_i f_i\right) + E;\ (a_0 : \cdots : a_N) \in \mathbb{P}^N(\mathbb{K}) \right\},$$

onde

$$E = \sum_{P\in\mathscr{X}} e_P P \quad \text{com} \quad e_P = -\min\{v_P(f_0), \ldots, v_P(f_N)\}.$$

Retomaremos o estudo das séries lineares $\mathscr{D}_i(P)$. Lembremos que $\mathscr{S}_i(P) = \mathscr{S}\cap\mathscr{L}(E-iP)$ e que $\mathscr{D}_i(P) \supset \mathscr{D}_{i+1}(P)$.

Definição 2.9.1. Chamaremos um inteiro não negativo j de $(\mathscr{D},P)$**-ordem** (ou de P**-invariante hermitiano**) quando $\mathscr{D}_i(P) \supsetneq \mathscr{D}_{i+1}(P)$.

Pelo item 2 do Lema 2.8.3, a dimensão cai em uma unidade ou se mantém a cada passo que damos ao longo da cadeia

$$\mathscr{D} = \mathscr{D}_0(P) \supset \mathscr{D}_1(P) \supset \cdots \supset \mathscr{D}_d(P) \supset \mathscr{D}_{d+1}(P) = \emptyset.$$

Como começamos com dimensão N e chegamos ao conjunto vazio, houveram $N+1$ quedas de dimensão. Isso significa que existem $N+1$ $(\mathscr{D},P)$-ordens, digamos

$$j_0(P) < j_1(P) < \cdots < j_N(P).$$

Em particular, a dimensão cai de um em um ao longo da cadeia

$$\mathscr{D} = \mathscr{D}_{j_0}(P) \supsetneq \mathscr{D}_{j_1}(P) \supsetneq \cdots \supsetneq \mathscr{D}_{j_N}(P)$$

e $\mathscr{D}_{j_i}(P)$ é uma g^{N-i}_d em $\mathscr{X}$.

Definição 2.9.2. 1. A **sequência de** $(\mathscr{D},P)$**-ordens** é a $(N+1)$-upla $(j_0,\ldots,j_N)$.

2. Para cada $i\in\{0,\ldots,N-1\}$, seja $\Pi_i(P)$ a interseção de todos os hiperplanos H em $\mathbb{P}^N(\mathbb{K})$ que satisfazem
$$v_P(\phi^{-1}(H))\geq j_{i+1}.$$
Dizemos que $\Pi_i(P)$ é o ***i*-ésimo espaço osculador em** P. Em particular, $\Pi_1(P)$ é a **reta tangente em** P e $\Pi_{N-1}(P)$ é o **hiperplano osculador em** P.

Observação 2.9.3. Notemos que $\Pi_0(P)=\{\phi(P)\}$. Além disso, o hiperplano osculador em P é o único hiperplano em $\mathbb{P}^N(\mathbb{K})$ tal que $v_P(\phi^{-1}(H))=j_N$.

Teorema 2.9.4. (STÖHR; VOLOCH, 1986, Teorema 1.1 da Seção 1). Sejam $P\in\mathscr{X}$ e $t\in\mathbb{K}(\mathscr{X})$ um parâmetro local de $\mathscr{X}$ em P. Suponhamos que $e_P=0$. Para cada $i\in\{0,\ldots,N\}$, j_i é o menor inteiro tal que o seguinte conjunto de vetores em $\mathbb{K}^{N+1}$ é linearmente indenpendente sobre $\mathbb{K}$:
$$\left\{\left((\mathrm{D}_t^{(j_0)}f_0)(P),\ldots,(\mathrm{D}_t^{(j_0)}f_N)(P)\right),\ldots,\left((\mathrm{D}_t^{(j_i)}f_0)(P),\ldots,(\mathrm{D}_t^{(j_i)}f_N)(P)\right)\right\}.$$

Além disso, o hiperplano osculador a $\phi(\mathscr{X})$ em P é gerado pelo conjunto
$$\left\{\left((\mathrm{D}_t^{(j_0)}f_0)(P),\ldots,(\mathrm{D}_t^{(j_0)}f_N)(P)\right),\ldots,\left((\mathrm{D}_t^{(j_{N-1})}f_0)(P),\ldots,(\mathrm{D}_t^{(j_{N-1})}f_N)(P)\right)\right\}.$$

Corolário 2.9.5. (STÖHR; VOLOCH, 1986, Corolário 1.3 da Seção 1). Sejam $P\in\mathscr{X}$ e $t\in\mathbb{K}(\mathscr{X})$ um parâmetro local de $\mathscr{X}$ em P. Suponhamos que $e_P=0$. O conjunto dos zeros do polinômio
$$\det\begin{pmatrix} X_0 & \cdots & X_N\\ (\mathrm{D}^{(j_0)}f_0)(P) & \cdots & (\mathrm{D}^{(j_0)}f_N)(P)\\ \vdots & \ddots & \vdots\\ (\mathrm{D}^{(j_{N-1})}f_0)(P) & \cdots & (\mathrm{D}^{(j_{N-1})}f_N)(P)\end{pmatrix}=0$$
em $\mathbb{P}^N(\mathbb{K})$ é o hiperplano osculador em P.

Definição 2.9.6. Seja t uma variável separante de $\mathbb{K}(\mathscr{X})/\mathbb{K}$ e sejam $g_0,\ldots,g_M\in\mathbb{K}(\mathscr{X})$.

1. Um **wronskiano** é uma função racional do tipo
$$\mathscr{W}_t^{k_0,\ldots,k_M}(g_0,\ldots,g_M):=\det\begin{pmatrix}\mathrm{D}_t^{(k_0)}(g_0) & \cdots & \mathrm{D}_t^{(k_0)}(g_M)\\ \vdots & \ddots & \vdots\\ \mathrm{D}_t^{(k_M)}(g_0) & \cdots & \mathrm{D}_t^{(k_M)}(g_M)\end{pmatrix},$$
onde $k_0,\ldots,k_M$ são inteiros não negativos com $k_0<\cdots<k_M$.

2. Definimos o conjunto
$$\mathscr{A}(g_0,\ldots,g_N;t):=\{(k_0,\ldots,k_M)\in\mathbb{N}^{M+1};\ k_0<\cdots<k_M \text{ e } \mathscr{W}_t^{k_0,\ldots,k_M}(g_0,\ldots,g_M)\neq 0\}.$$

A **ordem lexicográfica em** $\mathbb{N}^{M+1}$ é a relação de ordem parcial definida da seguinte maneira:

$$(k_0,\dots,k_M) < (l_0,\dots,l_M) \Leftrightarrow l_m - k_m > 0 \text{ para } m = \min\{i;\ l_i - k_i \neq 0\}.$$

Pode-se verificar que a ordem lexicográfica é uma boa ordem em $\mathbb{N}^{M+1}$, isto é, todo subconjunto não vazio de $\mathbb{N}^{M+1}$ possui um elemento mínimo.

Seja t uma variável separante de $\mathbb{K}(\mathscr{X})/\mathbb{K}$. O resultado seguinte decorre do Teorema 2.9.4.

Proposição 2.9.7. O conjunto $\mathscr{A}(f_0,\dots,f_N;t_0)$ é não vazio e, em particular, possui um elemento mínimo, digamos, $(\varepsilon_0,\dots,\varepsilon_N)$.

Observação 2.9.8. (STÖHR; VOLOCH, 1986, Considerações que sucedem o Corolário 1.3 na Seção 1). A $(N+1)$-upla $(\varepsilon_0,\dots,\varepsilon_N)$ é minimal no conjunto $\mathscr{A}(f_0,\dots,f_N;t)$ em um sentido mais forte: se $0 \leq m_0 < \cdots < m_N$ forem tais que o conjunto

$$\{(\mathrm{D}_t^{(m_0)}(f_0),\dots,\mathrm{D}_t^{(m_0)}(f_N)),\dots,(\mathrm{D}_t^{(m_N)}(f_0),\dots,\mathrm{D}_t^{(m_N)}(f_N))\}$$

é linearmente independente sobre $\mathbb{K}$, então $\varepsilon_i \leq m_i$ para cada $i \in \{0,\dots,N\}$.

Proposição 2.9.9. (STÖHR; VOLOCH, 1986, Proposicao 1.4 da Seção 1).

1. Seja $(a_{ij})_{0\leq i,j\leq N} \in \mathrm{GL}(N+1,\mathbb{K})$. Para cada $i \in \{0,\dots,N\}$, definamos $g_i = \sum_{k=0}^{N} a_{ij} f_j$. Então,
$$\mathscr{W}_t^{\varepsilon_0,\dots,\varepsilon_N}(g_0,\dots,g_N) = \det(a_{ij})\mathscr{W}_t^{\varepsilon_0,\dots,\varepsilon_N}(f_0,\dots,f_N).$$
2. Dada $h \in \mathbb{K}(\mathscr{X})$, temos
$$\mathscr{W}_t^{\varepsilon_0,\dots,\varepsilon_N}(hf_0,\dots,hf_N) = h^{N+1}\mathscr{W}_t^{\varepsilon_0,\dots,\varepsilon_N}(f_0,\dots,f_N).$$
3. Se t_1 for outra variável separante de $\mathbb{K}(\mathscr{X})/\mathbb{K}$, então
$$\mathscr{W}_{t_1}^{\varepsilon_0,\dots,\varepsilon_N}(f_0,\dots,f_N) = \left(\frac{t}{t_1}\right)^{\varepsilon_0+\cdots+\varepsilon_N} \mathscr{W}_t^{\varepsilon_0,\dots,\varepsilon_N}(f_0,\dots,f_N).$$

Observação 2.9.10. A Proposição 2.9.9 mostra que a sequência $(\varepsilon_0,\dots,\varepsilon_N)$ depende apenas da série linear $\mathscr{D}$.

Definição 2.9.11. A **sequência de $\mathscr{D}$-ordens** é a $(N+1)$-upla $(\varepsilon_0,\dots,\varepsilon_N)$. Para cada $i \in \{0,\dots,N\}$, ε_i é dito **$\mathscr{D}$-ordem**.

Da Proposição 2.9.9, segue que o divisor

$$R := \mathrm{div}(\mathscr{W}_x^{\varepsilon_0,\dots,\varepsilon_N}(f_0,\dots,f_N)) + (\varepsilon_0+\cdots+\varepsilon_N)\mathrm{div}(dx) + (N+1)E.$$

depende apenas da série linear $\mathscr{D}$.

Definição 2.9.12. O **divisor de ramificação de** $\mathscr{D}$ é R.

Observação 2.9.13. Notemos que

$$\deg(R) = (\varepsilon_1 + \cdots + \varepsilon_N)(2g-2) + (n+1)d.$$

Teorema 2.9.14. (STÖHR; VOLOCH, 1986, Teorema 1.5 da Seção 1). Consideremos $P \in \mathscr{X}$ e as $(\mathscr{D}, P)$-ordens $j_0, \ldots, j_N$. Temos

$$v_P(R) \geq \sum_{i=0}^{N} (j_i - \varepsilon_i).$$

E valerá a igualdade se, e somente se,

$$\det\left(\binom{j_i}{\varepsilon_r}\right) \not\equiv 0 \pmod{p}.$$

Corolário 2.9.15. (STÖHR; VOLOCH, 1986, Considerações que sucedem o Teorema 1.5 da Seção 1).

1. O divisor de ramificação R é efetivo.
2. Dado $P \in \mathscr{X}$, valerá $v_P(R) = 0$ se, e somente se, $j_i = \varepsilon_i$ para cada $i \in \{0, \ldots, N\}$.

Definição 2.9.16. Sejam $P \in \mathscr{X}$ e $(j_0, \ldots, j_N)$ a sequência de $(\mathscr{D}, P)$-ordens. Diremos que P é um $\mathscr{D}$**-ponto ordinário** se $(j_0, \ldots, j_N)$ for a sequência de $\mathscr{D}$-ordens. Caso contrário, diremos que P é um $\mathscr{D}$**-ponto de Weierstrass**.

Observação 2.9.17. Pelo item 2 do Corolário 2.9.15, o conjunto de todos os $\mathscr{D}$-pontos de Weierstrass de $\mathscr{X}$ é $\mathrm{Supp}(R)$.

2.10 Curvas definidas sobre corpos finitos

Seja p um número primo e sejam ℓ e q potências de p.

Definição 2.10.1. Seja $\mathscr{F} = \mathbf{v}_a(F)$ uma curva plana afim. Diremos que $\mathscr{F}$ **está definida sobre** $\mathbb{F}_\ell$ se existir $\lambda \in \overline{\mathbb{F}}_\ell$ tal que $\lambda F \in \mathbb{F}_\ell[X,Y]$. Se esse for o caso e se F for irredutível em $\overline{\mathbb{F}}_\ell[X,Y]$, diremos que $\mathscr{F}$ é **geometricamente irredutível**.

Definição 2.10.2. Sejam $\mathscr{F}$ uma curva plana afim e geometricamente irredutível definida sobre $\mathbb{F}_\ell$ e (x,y) um ponto genérico de $\mathscr{F}$. O **corpo das funções** $\mathbb{F}_\ell$**-racionais de** $\mathscr{F}$ é o subcorpo de $\overline{\mathbb{F}}_\ell(\mathscr{F})$ seguinte:

$$\mathbb{F}_\ell(\mathscr{F}) := \left\{ \frac{A(x,y)}{B(x,y)};\ A, B \in \mathbb{F}_\ell[X,Y] \text{ e } B(x,y) \neq 0 \right\}.$$

Os elementos de $\mathbb{F}_\ell(\mathscr{F})$ são as **funções** $\mathbb{F}_\ell$**-racionais de** $\overline{\mathbb{F}}_\ell(\mathscr{F})$.

Observação 2.10.3. A Definição 2.10.2 independe da escolha do ponto genérico.

Definição 2.10.4. 1. A conjugação de $\overline{\mathbb{F}}_\ell((T))$ é o automorfismo

$$\begin{array}{rccc} \kappa\colon & \overline{\mathbb{F}}_\ell((T)) & \to & \overline{\mathbb{F}}_\ell((T)) \\ & \sum a_i T^i & \mapsto & \sum a_i^\ell T^i. \end{array}$$

2. Seja γ um ramo com representação primitiva $(x(T) : y(T) : z(T))$. A **imagem de Frobenius de** γ é o ramo $\Phi(\gamma)$ com representação primitiva

$$(\kappa(x(T)) : \kappa(y(T)) : \kappa(z(T))).$$

Seja $\mathscr{F}$ uma curva plana afim, geometricamente irredutível e definida sobre $\mathbb{F}_\ell$.

Definição 2.10.5. Sejam $\mathscr{P}_0$ um lugar de $\overline{\mathbb{F}}_\ell(\mathscr{F})$, γ o ramo de $\mathscr{F}$ correspondente a $\mathscr{P}$ e

$$D = \sum_{\mathscr{P}\in\mathfrak{P}(\overline{\mathbb{F}}_\ell(\mathscr{F}))} n_{\mathscr{P}}\mathscr{P} \in \mathrm{Div}(\overline{\mathbb{F}}_\ell(\mathscr{F})).$$

1. A **imagem de Frobenius de** $\mathscr{P}_0$ é o lugar $\Phi(\mathscr{P}_0)$ de $\overline{\mathbb{F}}_\ell(\mathscr{F})$ correspondente ao ramo $\Phi(\gamma)$.

2. Definimos

$$\Phi(D) := \sum_{\mathscr{P}\in\mathfrak{P}(\overline{\mathbb{F}}_\ell(\mathscr{F}))} n_{\mathscr{P}}\Phi(\mathscr{P}).$$

3. Diremos que D é um **divisor $\mathbb{F}_\ell$-racional** se $\Phi(D) = D$.

4. Seja $\mathscr{D} \cong \mathbb{P}(\mathscr{S}) \subset |E|$ uma série linear em $\overline{\mathbb{F}}_\ell(\mathscr{F})$. Se $\mathscr{S}$ tiver uma base contida em $\mathbb{F}_\ell(\mathscr{F})$ e E for um divisor $\mathbb{F}_\ell$-racional, diremos que $\mathscr{D}$ é uma **série linear $\mathbb{F}_\ell$-racional** .

Teorema 2.10.6. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 8.26 da Seção 8.3). Se E for um divisor $\mathbb{F}_\ell$-racional de $\overline{\mathbb{F}}_\ell(\mathscr{F})$, então $|E|$ será uma série linear $\mathbb{F}_\ell$-racional em $\overline{\mathbb{F}}_\ell(\mathscr{F})$.

Definição 2.10.7. (COUTINHO, 2019, Definição 2.5.1). Um curva irredutível $\mathscr{X}$ **está definida sobre** $\mathbb{F}_\ell$ se ela for dada por um ponto $(x_0 : \cdots : x_M) \in \mathbb{P}^M(\overline{\mathbb{F}}_\ell(\mathscr{F}))$ com $x_0, \ldots, x_M \in \mathbb{F}_\ell(\mathscr{F})$.

Observação 2.10.8. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Observação 8.30 da Seção 8.4). Toda curva definida sobre $\mathbb{F}_\ell$ admite um modelo não singular definido sobre $\mathbb{F}_\ell$.

Definição 2.10.9. Sejam $\mathscr{X}$ uma curva irredutível e definida sobre $\mathbb{F}_\ell$ e

$$\phi = (f_0 : \cdots : f_N)\colon \mathscr{X} \dashrightarrow \mathbb{P}^N(\overline{\mathbb{F}}_\ell)$$

uma aplicação racional. Diremos que ϕ **é uma aplicação racional definida sobre** $\mathbb{F}_\ell$ se

$$(f_0 : \cdots : f_N) \in \mathbb{P}^N(\mathbb{F}_\ell(\mathscr{X})).$$

Teorema 2.10.10 (Cota de Hasse-Weil)**.** Seja $\mathscr{X}$ uma curva projetiva, não singular e definida sobre $\mathbb{F}_\ell$ de gênero g. O número de pontos $\mathbb{F}_\ell$-racionais de $\mathscr{X}$ está no intervalo real

$$[1+\ell-2\sqrt{\ell}g, 1+\ell+2\sqrt{\ell}g].$$

Demonstração. Pode ser consultada em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Seção 9.2). □

Definição 2.10.11. O q-ésimo **morfismo de Frobenius** é a aplicação

$$\begin{array}{rccc} \mathbf{Fr}_q\colon & \mathbb{P}^M(\overline{\mathbb{F}}_\ell) & \to & \mathbb{P}^M(\overline{\mathbb{F}}_\ell) \\ & (\alpha_0 : \cdots : \alpha_M) & \mapsto & (\alpha_0^q : \cdots : \alpha_M^q). \end{array}$$

Definição 2.10.12. Seja $\mathscr{X}$ uma curva projetiva, não singular e definida sobre $\mathbb{F}_{q^2}$ de gênero g. Diremos que $\mathscr{X}$ **é uma curva maximal sobre** $\mathbb{F}_{q^2}$ se $\mathscr{X}$ atingir a cota superior de Hasse-Weil, isto é, se

$$\#\mathscr{X}(\mathbb{F}_{q^2}) = 1+q^2+2qg.$$

Teorema 2.10.13. (FUHRMANN; GARCIA; TORRES, 1997, Corolário 1.2 da Seção 1). Sejam $\mathscr{X}$ uma curva maximal sobre $\mathbb{F}_{q^2}$ e $P_0 \in \mathscr{X}(\mathbb{F}_{q^2})$. Então,

$$qP + \mathbf{Fr}_{q^2}(P) \sim (q+1)P_0 \quad \forall P \in \mathscr{X}. \tag{2.3}$$

Observação 2.10.14. A relação (2.3) é chamada **Equivalência Fundamental**.

Definição 2.10.15. Sejam $\mathscr{X}$ e P_0 como no Teorema 2.10.13.

1. O **divisor de Frobenius de** $\mathscr{X}$ é o divisor efetivo e $\mathbb{F}_{q^2}$-racional $(q+1)P_0$.
2. A **série linear de Frobenius de** $\mathscr{X}$ é a série linear completa e $\mathbb{F}_{q^2}$-racional $|(q+1)P_0|$.

Teorema 2.10.16. (FUHRMANN; GARCIA; TORRES, 1997, Teorema 1.4 da Seção 1). Sejam $\mathscr{X}$ uma curva $\mathbb{F}_{q^2}$-maximal de gênero positivo, $\mathscr{D}$ a série linear de Frobenius e $\varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_N$ as $\mathscr{D}$-ordens de $\mathscr{X}$. Dado $P \in \mathscr{X}$, temos

$$j_N(P) = \begin{cases} q+1 & \text{se } P \in \mathscr{X}(\mathbb{F}_{q^2}) \\ q & \text{caso contrário.} \end{cases}$$

Em particular, $\varepsilon_N = q$ e todos os pontos $\mathbb{F}_{q^2}$-racionais de $\mathscr{X}$ são $\mathscr{D}$-pontos de Weierstrass.

Proposição 2.10.17. (FUHRMANN; GARCIA; TORRES, 1997, Proposição 1.9 da Seção 1). Sejam $\mathscr{X}$ uma curva $\mathbb{F}_{q^2}$-maximal, $\mathscr{D}$ a série linear de Frobenius e $\pi\colon \mathscr{X} \to \mathbb{P}^N(\mathbb{F}_{q^2})$ o morfismo associado a $\mathscr{D}$. As curvas $\mathscr{X}$ e $\pi(\mathscr{X})$ serão $\mathbb{F}_{q^2}$-isomorfas se, e somente se,

$$\{P \in \mathscr{X}(\mathbb{F}_{q^4});\ \pi(P) \in \mathbb{P}^N(\mathbb{F}_{q^2})\} \subset \mathscr{X}(\mathbb{F}_{q^2}).$$

Teorema 2.10.18. (GARCIA; VOLOCH, 1987, Teorema 1 da Seção 1). Sejam $\mathscr{X}$ uma curva irredutível definida sobre $\mathbb{F}_{q^2}$ e $t \in \mathbb{F}_{q^2}(\mathscr{X})$ uma variável separante de $\overline{\mathbb{F}}_{q^2}(\mathscr{X})/\overline{\mathbb{F}}_{q^2}$. Um conjunto $\{f_0,\ldots,f_N\} \subset \mathbb{F}_{q^2}(\mathscr{X})$ será linearmente independente sobre $\mathbb{F}_{q^2}(\mathscr{X})^q$ se, e somente se, existirem inteiros positivos $k_1 < \cdots < k_N < q$ satisfazendo $\mathscr{W}_t^{0,k_1,\ldots,k_N}(f_0,\ldots,f_N) \neq 0$.

2.11 Dualidade e estranheza

Definição 2.11.1. Seja $\mathscr{X}$ uma curva irredutível e não degenerada em $\mathbb{P}^N(\mathbb{K})$. A **curva dual de** $\mathscr{X}$ é a curva irredutível de $\mathbb{P}^N(\mathbb{K})$ que contém todos, exceto possivelmente um número finito, os pontos $P = (b_0 : \cdots : b_N)$ tal que o hiperplano

$$H\colon b_0X_0 + \cdots + b_NX_N = 0$$

é um hiperplano osculador a $\mathscr{X}$.

Proposição 2.11.2. (KAJI, 1992, Proposição 1 da Seção 2). Suponhamos que $\mathbb{K}$, além de ser algebricamente fechado, tenha caracterítica positiva. Sejam $\mathscr{F}$ uma curva irredutível e não singular definida sobre $\mathbb{K}$, $\mathscr{D}$ uma série linear em $\mathscr{F}$ e $\phi\colon \mathscr{F} \to \mathbb{P}^N(\mathbb{K})$ o morfismo associado a $\mathscr{D}$. Sejam $\mathscr{X}$ a imagem não degenerada de ϕ em $\mathbb{P}^N(\mathbb{K})$ e $\mathscr{X}^*$ a dual de $\mathscr{X}$ em $\mathbb{P}^N(\mathbb{K})$. Sejam R o conjunto dos $\mathscr{D}$-pontos ordinários de $\mathscr{F}$ e

$$S = \bigcap_{P\in R} H_P,$$

onde H_P é o hiperplano osculador de $\mathscr{D}$ em P. Temos

$$\dim_{\mathbb{K}}(S) = N - \dim_{\mathbb{K}}(\langle \mathscr{X}^* \rangle) - 1.$$

Definição 2.11.3. Seja $\mathscr{X}$ uma curva irredutível e não degenerada em $\mathbb{P}^N(\mathbb{K})$. Diremos que $\mathscr{X}$ é **estranha** se existir um ponto $P \in \mathbb{P}^N(\mathbb{K})$ que pertence a infinitas retas tangentes a $\mathscr{X}$.

Teorema 2.11.4 (Cota de Castelnuovo)**.** Seja $\mathscr{X}$ uma curva irredutível e não degenerada em $\mathbb{P}^M(\mathbb{K})$ de grau d e gênero g. Sejam r e s os únicos inteiros que satisfazem

$$0 \le r < M-1 \quad \text{e} \quad d-1 = (M-1)s + r.$$

Se $\mathscr{X}$ não for estranha, então

$$g \le \frac{s(s-1)(M-1)}{2} + sr.$$

Demonstração. Pode ser encontrada em (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 7.111 da Seção 7.13). □

2.12 Geometria projetiva sobre corpos finitos

Seja q uma potência de algum número primo.

Teorema 2.12.1. (HIRSCHFELD, 1979, Teorema 3.1.1). Seja ℓ uma potência de algum primo. O número de pontos em $\mathbb{P}^M(\mathbb{F}_q)$ é

$$q^M + q^{M-1} + \cdots + q + 1.$$

Definição 2.12.2. Seja $A = (a_{ij})_{0\leq i,j\leq N}$ uma matriz não nula com entradas em $\mathbb{F}_{q^2}$ satisfazendo $a_{ji} = a_{ij}^q$. A variedade hermitiana definida sobre $\mathbb{F}_{q^2}$ em $\mathbb{P}^N(\overline{\mathbb{F}}_{q^2})$ associada à matriz A é a hipersuperfície

$$\mathbf{v}\left(\sum_{i,j=0}^{N} a_{ij}X_i^q X_j\right).$$

Proposição 2.12.3. (HIRSCHFELD, 1979, Lema 5.1.2). Seja $\mathscr{H}$ uma variedade hermitiana. Existe um único $k \in \{0,\ldots,N\}$ tal que $\mathscr{H}$ é $\mathbb{F}_{q^2}$-projetivamente equivalente à

$$\mathbf{v}(X_0^{q+1} + \cdots + X_k^{q+1}).$$

Definição 2.12.4. Sejam $\mathscr{H}$ uma variedade hermitiana e k o único número do conjunto $\{0,\ldots,N\}$ tal que

$$\mathfrak{T}\cdot\mathscr{H} = \mathbf{v}(X_0^{q+1} + \cdots + X_k^{q+1})$$

para alguma $\mathfrak{T} \in \mathrm{PGL}(N+1,\mathbb{F}_{q^2})$. Se $k = N$, diremos que $\mathscr{H}$ é uma **variedade hermitiana não degenerada**. Caso contrário, diremos que $\mathscr{H}$ é uma **variedade hermitiana degenerada**.

Proposição 2.12.5. (HIRSCHFELD, 1979, Corolário 2 do Lema 5.1.2). Seja $\mathscr{H}$ a variedade hermitiana associada à matriz A. A variedade $\mathscr{H}$ será não degenerada se, e somente se, a matriz A for invertível.

Definição 2.12.6. Seja $\mathscr{H} = \mathbf{v}(X_0^{q+1} + \cdots + X_N^{q+1})$. O **grupo projetivo unitário** é o conjunto

$$\mathrm{PGU}(N+1,\mathbb{F}_{q^2}) := \{\mathfrak{T} \in \mathrm{PGL}(N+1,\mathbb{F}_{q^2});\ \mathfrak{T}\cdot\mathscr{H} = \mathscr{H}\}.$$

Teorema 2.12.7. (HIRSCHFELD; THAS, 2016, Item (ii) do Teorema 2.22 da Seção 2.4). Sejam $P, Q \in \mathbb{P}^N(\mathbb{F}_{q^2}) \setminus \mathscr{H}$. Então, existe $\mathfrak{T} \in \mathrm{PGU}(N+1,\mathbb{F}_{q^2})$ tal que $\mathfrak{T}(P) = Q$.

Proposição 2.12.8. (BOSE; CHAKRAVARTI, 1966, Corolário do Teorema 4.1). Consideremos uma matriz hermitiana $H = (c_{ij})_{0\leq i,j\leq N}$ de posto M. Então, existe uma transformação $\mathbb{F}_{q^2}$-linear $\mathfrak{T}$ de $\mathbb{P}^N(\mathbb{F}_{q^2})$ tal que

$$\mathfrak{T}\cdot\mathbf{v}\left(\sum_{i,j=0}^{N} c_{ij}X_j X_i^q\right) = \mathbf{v}(X_0^{q+1} + \cdots + X_M^{q+1}).$$

Teorema 2.12.9. (BOSE; CHAKRAVARTI, 1966, Teorema 8.1). A quantidade de pontos $\mathbb{F}_{q^2}$-racionais em uma variedade hermitiana $\mathscr{H}$ não degenerada em $\mathbb{P}^M(\overline{\mathbb{F}}_{q^2})$ é

$$\mathscr{H}(\mathbb{F}_{q^2}) := \frac{(q^{M+1} - (-1)^{M+1})(q^M - (-1)^M)}{q^2 - 1}.$$

CAPÍTULO

3

A CARACTERIZAÇÃO DAS CURVAS MAXIMAIS

Escrito com base no artigo (KORCHMÁROS; TORRES, 2001, Seções 1, 2, 3 e 4), o objetivo deste capítulo é justificar a epígrafe. Para relembrar as definições de objetos e justificar argumentos que aparecerão aqui, faremos menção a trechos do capítulo anterior, onde boa parte da bagagem conceitual foi desenvolvida.

3.1 O morfismo associado à série linear de Frobenius

Para esta seção e para a próxima, assumamos que $\mathscr{X}$ seja uma curva $\mathbb{F}_{q^2}$-maximal de gênero positivo. Consideremos a série linear de Frobenius $\mathscr{D} := |(q+1)P_0|$ com $P_0 \in \mathbb{F}_{q^2}(\mathscr{X})$ e denotemos sua dimensão por N. Seja $\pi\colon \mathscr{X} \to \mathbb{P}^N(\overline{\mathbb{F}}_{q^2})$ o morfismo associado a $\mathscr{D}$. No fim desta seção, mostraremos que as curvas $\mathscr{X}$ e $\pi(\mathscr{X})$ são $\mathbb{F}_{q^2}$-isomorfas. Pela Proposição 2.10.17, basta mostrarmos que todo ponto de $\mathscr{X}$ que tem imagem $\mathbb{F}_{q^2}$-racional é $\mathbb{F}_{q^2}$-racional.

Sejam $\varepsilon_0 = 0 < \varepsilon_1 = 1 < \cdots < \varepsilon_N$ as $\mathscr{D}$-ordens da curva $\mathscr{X}$. Tomemos uma base $\{f_0, \ldots, f_N\}$ de $\mathscr{L}((q+1)P_0)$. Pelo Teorema 2.10.16 e pela Observação 2.9.8, para quaisquer inteiros positivos $k_1 < \cdots < k_N < q$, temos $\mathscr{W}_t^{0,k_1,\ldots,k_N}(f_0, \ldots, f_N) = 0$. Pelo Teorema 2.10.18, existem $z_0, \ldots, z_N \in \mathbb{F}_{q^2}(\mathscr{X})$, não todas nulas, tais que

$$z_0^q f_0 + \cdots + z_N^q f_N = 0. \tag{3.1}$$

Os próximos três lemas apresentam algumas propriedades da $(N+1)$-upla $(z_0 : \cdots : z_N)$.

Para cada $P \in \mathscr{X}$ e $i \in \{0, \ldots, N\}$, definamos

$$e_P = -\min\{v_P(z_0), \ldots, v_P(z_N)\} \quad \text{e} \quad w_i = t^{e_P} z_i,$$

onde t é um parâmetro local de $\mathscr{X}$ em P.

Lema 3.1.1. Dado $P \in \mathscr{X}$, o hiperplano osculador a $\mathscr{X}$ em P tem equação

$$w_0^q(P)X_0 + w_1^q(P)X_1 + \cdots + w_N^q(P)X_N = 0.$$

Demonstração. Para cada $i \in \{0,\ldots,N\}$, seja

$$w_i(t) = \sum_{j=0}^{\infty} a_j^{(i)} t^j$$

a expansão local de w_i em P. Tomando $k \in \{0,\ldots,N\}$ tal que $e_P = -v_P(z_k)$, temos

$$v_P(w_k) = e_P v_P(t) + v_P(z_k) = e_P - e_P = 0,$$

ou seja, $a_0^{(k)} \neq 0$. Isso nos permite considerar o seguinte hiperplano em $\mathbb{P}^N(\overline{\mathbb{F}}_{q^2})$:

$$H : \sum_{i=0}^{N} (a_0^{(i)})^q X_i = 0.$$

Multiplicando ambos os lados da relação (3.1) por t^{qe_P}, obtemos

$$\sum_{i=0}^{N} w_i^q f_i = 0.$$

Desse modo,

$$\begin{aligned} v_P\left(\sum_{i=0}^{N}(a_0^{(i)})^q f_i\right) &= v_P\left(\sum_{i=0}^{N}(a_0^{(i)})^q f_i - \sum_{i=0}^{N} w_i^q f_i\right) \\ &= v_P\left(\sum_{i=0}^{N}(a_0^{(i)})^q f_i - \sum_{i=0}^{N}\left((a_0^{(i)})^q + \sum_{j=1}^{\infty}(a_j^{(i)})^q t^{qj}\right) f_i\right) \\ &= v_P\left(t^q \sum_{i=0}^{N}\sum_{j=1}^{\infty}(a_j^{(i)})^q t^{q(j-1)} f_i\right) \\ &= q v_P\left(\sum_{i=0}^{N}\sum_{j=1}^{\infty}(a_j^{(i)})^q t^{q(j-1)} f_i\right). \end{aligned}$$

Temos

$$\begin{aligned} v_P(\pi^{-1}(H)) &= v_P\left(\sum_{i=0}^{N}(a_0^{(i)})^q f_i\right) + v_P((q+1)P_0) \\ &= q v_P\left(\sum_{i=0}^{N}\sum_{j=1}^{\infty}(a_j^{(i)})^q t^{q(j-1)} f_i\right) + v_P((q+1)P_0). \end{aligned}$$

Pela desigualdade triangular, $v_P(\pi^{-1}(H)) \geq q$. Pelo Teorema 2.10.16, H é o hiperplano osculador a $\mathscr{X}$ em P. □

Lema 3.1.2. Também é válida a relação

$$z_0 f_0^q + \cdots + z_N f_N^q = 0. \tag{3.2}$$

Demonstração. Pelo Corolário 2.5.21, basta mostrarmos que a função $\sum_{i=0}^{N} z_i f_i^q$ se anula em uma quantidade infinita de pontos $P \in \mathscr{X}$. Pela Equivalência Fundamental (2.3), os divisores do tipo $qP + \mathbf{Fr}_{q^2}(P)$, com $P \in \mathscr{X}$, são elementos da série linear $\mathscr{D}$. Para cada $P \in \mathscr{X}$, valem

$$v_P(qP + \mathbf{Fr}_{q^2}(P)) \geq q \quad \text{e} \quad v_{\mathbf{Fr}_{q^2}(P)}(qP + \mathbf{Fr}_{q^2}(P)) \geq 1;$$

em outras palavras, o hiperplano correspondente ao divisor $P + \mathbf{Fr}_{q^2}(P)$ é o hiperplano osculador a $\mathscr{X}$ em P e contém o ponto $\mathbf{Fr}_{q^2}(P)$. Do Lema 3.1.1, decorre

$$\left(\sum_{i=0}^{N} z_i(P) f_i(P)^q\right)^q = \sum_{i=0}^{N} z_i(P)^q f_i(P)^{q^2} = 0$$

para todo $P \in \mathscr{X}$ satisfazendo $e_P = 0$. Isso conclui a prova. □

Lema 3.1.3. As funções racionais $z_0, z_1, \ldots, z_N \in \mathbb{F}_{q^2}(\mathscr{X})$ satisfazendo a relação (3.1) são únicas a menos de um fator não nulo em $\mathbb{F}_{q^2}(\mathscr{X})$.

Demonstração. Definamos o conjunto

$$I = \{i \in \{0, \ldots, N\};\ z_i \neq 0\}.$$

Sejam $\tilde{z}_0, \ldots, \tilde{z}_N \in \mathbb{F}_{q^2}(\mathscr{X})$, não todas nulas, tais que

$$\tilde{z}_0^q f_0 + \cdots + \tilde{z}_N^q f_N = 0.$$

Mostraremos que se $\tilde{z}_k \neq 0$ para algum $k \in \{0, \ldots, N\}$, então $z_k \neq 0$ e

$$\tilde{z}_i = \frac{\tilde{z}_k}{z_k} z_i$$

para todo $i \in \{0, \ldots, N\}$. Para isso, basta provarmos as afirmações seguintes:
(A1) se $z_i = 0$, então $\tilde{z}_i = 0$;
(A2) as funções $\mathbb{F}_{q^2}$-racionais do tipo $\dfrac{\tilde{z}_i}{z_i}$, com $i \in I$, são iguais.

Definamos $\tilde{e}_P = -\min\{v_P(\tilde{z}_0), \ldots, v_P(\tilde{z}_N)\}$ para cada $P \in \mathscr{X}$. Consideremos os conjuntos seguintes:

$$U = \{P \in \mathscr{X};\ e_P = 0 \text{ e } \tilde{e}_P = 0\} \quad \text{e} \quad V = \{P \in U;\ z_i(P) \neq 0 \text{ para todo } i \in I\}.$$

Para cada $P \in U$, segue do Lema 3.1.1 que

$$\tilde{z}_0^q(P) X_0 + \cdots + \tilde{z}_N^q(P) X_N = 0 \quad \text{e} \quad z_0^q(P) X_0 + \cdots + z_N^q(P) X_N = 0$$

são equações do hiperplano osculador a $\mathscr{X}$ em P e, consequentemente, existe $\lambda_P \in \overline{\mathbb{F}}_{q^2}$ tal que

$$\tilde{z}_i^q(P) = \lambda_P^q z_i^q(P) \tag{3.3}$$

para todos $i \in \{0,\dots,N\}$. Em particular,

$$\frac{\tilde{z}_i}{z_i}(P) = \lambda_P \tag{3.4}$$

para todos $i \in I$ e $P \in V$. Pelo Corolário 2.5.21, as afirmações (A1) e (A2) decorrem das relações (3.3) e (3.4) respectivamente. □

Lema 3.1.4. Seja $P \in \mathscr{X}$. Se $\pi(P) \in \mathbb{P}^N(\mathbb{F}_{q^2})$, então $P \in \mathscr{X}(\mathbb{F}_{q^2})$.

Demonstração. Suponhamos que $\pi(P)$ seja um ponto racional. Compondo π com uma transformação $\mathbb{F}_{q^2}$-linear se for necessário, podemos supor que $\pi(P) = (1:0:\cdots:0)$. Suponhamos também que $\pi = (1 : f_1 : \cdots : f_N)$ de modo que $v_P(f_i) \geq 1$ para todo $i \in \{1,\dots,N\}$. Multiplicando ambos os lados da relação (3.2) por t^{e_P}, obtemos

$$\sum_{j=0}^{\infty} a_j^{(0)} t^j + \sum_{i=1}^{N} f_i^q \sum_{j=0}^{\infty} a_j^{(i)} t^j = 0.$$

Utilizando a desigualdade triangular,

$$v_P\left(\sum_{j=0}^{\infty} a_j^{(0)} t^j\right) = v_P\left(\sum_{i=1}^{N} f_i^q \sum_{j=0}^{\infty} a_j^{(i)} t^j\right) \geq q \geq 2.$$

Em particular, $a_1^{(0)} = 0$.

Pelas computações feitas na demonstração do Lema 3.1.1, temos

$$v_P(\pi^{-1}(H)) = q + v_P\left(t^q \sum_{j=2}^{\infty} (a_j^{(0)})^q t^{q(j-2)} + \sum_{i=1}^{N} f_i \sum_{j=1}^{\infty} (a_j^{(i)})^q t^{q(j-1)}\right).$$

Pela desigualdade triangular, como $v_P(t^q) = q$ e $v_P(f_i) \geq 1$ para todo $i \in \{1,\dots,N\}$,

$$v_P\left(t^q \sum_{j=2}^{\infty} (a_j^{(0)})^q t^{q(j-2)} + \sum_{i=1}^{N} f_i \sum_{j=1}^{\infty} (a_j^{(i)})^q t^{q(j-1)}\right) \geq 1.$$

Portanto, $v_P(\pi^{-1}(H)) = q+1$. Pelo Teorema 2.10.16, P é um ponto racional. □

O resultado seguinte é uma consequência dos Lemas 2.10.17 e 3.1.4.

Teorema 3.1.5. As curvas $\mathscr{X}$ e $\pi(\mathscr{X})$ são $\mathbb{F}_{q^2}$-isomorfas.

Observação 3.1.6. Para aplicar o Teorema 3.1.5 nas próximas seções, ressaltamos que a condição de $\mathscr{D}$ ser uma série linear completa não foi usada. Portanto, esse teorema ainda será válido se substituirmos $\mathscr{D}$ por uma subsérie linear (não completa) $\mathscr{R}$ de $\mathscr{D}$ contendo todos os divisores do tipo $qP + \mathbf{Fr}_{q^2}(P)$, com $P \in \mathscr{X}$, e ressignificarmos π como o morfismo associado a $\mathscr{R}$.

3.2 O Teorema do Mergulho Natural

Comecemos esta seção identificando $\mathscr{X}$ com $\pi(\mathscr{X})$ de acordo com o Teorema 3.1.5. Sejam $z_0,\dots,z_N \in \mathbb{F}_{q^2}(\mathscr{X})$ satisfazendo a relação (3.1). Definamos o morfismo

$$\pi^* = (z_0 : \cdots : z_N) \colon \mathscr{X} \to \mathbb{P}^N(\overline{\mathbb{F}}_{q^2}).$$

Pelo Lema 3.1.1, $\mathbf{Fr}_q \circ \pi^*$ é a aplicação de Gauss $P \mapsto \Pi_{N-1}(P)$.

Consideremos a curva $\pi^*(\mathscr{X})$ em $\mathbb{P}^N(\overline{\mathbb{F}}_{q^2})$. Seja $\mathbb{P}^M$ o subespaço de dimensão M em $\mathbb{P}^N(\overline{\mathbb{F}}_{q^2})$ onde $\pi^*(\mathscr{X})$ é uma curva não degenerada, ou seja, $\mathbb{P}^M = \langle \pi^*(\mathscr{X}) \rangle$. Visto que $\mathscr{X}^* = \mathbf{Fr}_q \circ \pi^*(\mathscr{X})$, $\dim(\langle \mathscr{X}^* \rangle) = M$. Pela Proposição 2.11.2, existe um subespaço $\mathbb{P}^{N-M-1}$ de dimensão $N-M-1$ em $\mathbb{P}^N(\overline{\mathbb{F}}_{q^2})$ que é a interseção dos hiperplanos osculadores a $\mathscr{X}$ em quase todos os pontos $P \in \mathscr{X}$.

Lema 3.2.1. Nenhum ponto de $\mathscr{X}$ pertence a $\mathbb{P}^{N-M-1}$.

Demonstração. Suponhamos, por absurdo, que exista $R \in \mathbb{P}^{N-M-1} \cap \mathscr{X}$. Escolhamos um ponto $Q \in \mathscr{X} \setminus \{R, \mathbf{Fr}_{q^2}^{-1}(R)\}$ de modo que o hiperplano osculador $\Pi_{N-1}(Q)$ a $\mathscr{X}$ em Q contenha $\mathbb{P}^{N-M-1}$. Desse modo,

$$R \in \Pi_{N-1}(Q) \cap \mathscr{X} = \{Q, \mathbf{Fr}_{q^2}(Q)\},$$

contradizendo o fato de que $Q \notin \{R, \mathbf{Fr}_{q^2}^{-1}(R)\}$. □

Notemos que $\mathbb{P}^M$ está definido sobre $\mathbb{F}_{q^2}$. Apliquemos uma transformação $\mathbb{F}_{q^2}$-linear em $\mathbb{P}^N(\overline{\mathbb{F}}_{q^2})$ de modo que $\mathbb{P}^M$ tenha equação $X_{M+1} = 0, \dots, X_N = 0$. Então, $z_{M+1} = 0, \dots, z_N = 0$ e $\pi^* \colon \mathscr{X} \to \mathbb{P}^M$ é dado por $(z_0 : \cdots : z_M)$.

Observação 3.2.2. Segundo o Lema 3.1.1, a equação do hiperplano osculador a $\mathscr{X}$ em Q é $\gamma_0^q X_0 + \cdots + \gamma_M^q X_M = 0$, onde $\pi^*(Q) = (\gamma_0 : \cdots : \gamma_M)$.

Lema 3.2.3. Temos $\deg(\pi^*(\mathscr{X})) = q+1$. Além disso, a série linear cortada em $\pi^*(\mathscr{X})$ por hiperplanos de $\mathbb{P}^M$ contém todos os divisores do tipo $qP + \mathbf{Fr}_{q^2}(P)$, com $P \in \mathscr{X}$.

Demonstração. Escolhamos um ponto $P_0 = (\alpha_0 : \cdots : \alpha_N) \in \mathscr{X}(\mathbb{F}_{q^2})$. Suponhamos, por absurdo, que $\alpha_0 = \cdots = \alpha_M = 0$. Pela Observação 3.2.2, P_0 pertenceria a todos os hiperplanos osculadores a $\mathscr{X}$ e, consequentemente, a $\mathbb{P}^{N-M-1}$, o que não é possível devido ao Lema 3.2.1. Então, existe $k \in \{0,\dots,M\}$ tal que $\alpha_k \neq 0$. Agora, consideremos o hiperplano

$$H = \mathbf{v}(\alpha_0^q X_0 + \cdots + \alpha_M^q X_M),$$

o qual pode ser reconhecido como um hiperplano em $\mathbb{P}^M$.

Seja $P \in \mathscr{X}$ tal que $\pi^*(P) = (\gamma_0 : \cdots : \gamma_M) \in H \cap \pi^*(\mathscr{X})$, com $\gamma_i \in \overline{\mathbb{F}}_{q^2}$. Temos

$$\alpha_0^q \gamma_0 + \cdots + \alpha_M^q \gamma_M = 0$$

e, elevando ambos os lados a q,

$$\gamma_0^q \alpha_0 + \cdots + \gamma_M^q \alpha_M = 0.$$

Pelo Lema 3.1.1, o hiperplano osculador a $\mathscr{X}$ em P passa por P_0. Isso mostra que $P = P_0$, uma vez que $P_0 \in \mathscr{X}(\mathbb{F}_{q^2})$. Com isso, concluímos que a interseção $H \cap \pi^*(\mathscr{X})$ não contém nenhum ponto diferente de $\pi^*(P_0)$. Queremos mostrar que o divisor $(\pi^*)^{-1}(H)$ de $\mathscr{X}$ é $(q+1)P_0$. Para tal, provaremos que

$$v_{P_0}((\pi^*)^{-1}(H)) = v_{P_0}(\alpha_0^q w_0 + \cdots + \alpha_N^q w_N) = q+1,$$

onde $w_i := t^{e_P} z_i$ com t um parâmetro local em P_0 e $e_{P_0} := -\min\{v_{P_0}(z_0), \ldots, v_{P_0}(z_N)\}$ (lembremos que $z_{M+1} = \cdots = z_N = 0$).

Depois de uma transformação $\mathbb{F}_{q^2}$-linear de $\mathbb{P}^N(\overline{\mathbb{F}}_{q^2})$, podemos assumir que

$$P_0 = (1:0:\cdots:0), \quad f_0 = 1, \quad f_1 = a_1 t^{j_1} + \cdots, \quad f_N = a_N t^{j_N} + \cdots,$$

onde $(0, j_1, \ldots, j_N)$ é a sequência de $(\mathscr{D}, P_0)$-ordens de $\mathscr{X}$. Desse modo, precisamos mostrar que $v_{P_0}(w_0) = q+1$.

Seja $m = \min\{i;\ v_{P_0}(w_i) = 0\}$. Multiplicando os dois lados da relação (3.1) por $t^{qe_{P_0}}$, obtemos

$$w_0(t)^q + w_1(t)^q(a_1 t^{j_1} + \cdots) + \cdots + w_N(t)^q(a_N t^{j_N} + \cdots) = 0$$

e, por conseguinte,

$$\begin{aligned} w_0(t)^q + w_1(t)^q(a_1 t^{j_1} + \cdots) + \cdots + w_N(t)^q(a_N t^{j_N} + \cdots) - w_m(t)^q(a_m t^{j_m} + \cdots) = \\ - w_m(t)^q(a_m t^{j_m} + \cdots). \end{aligned} \tag{3.5}$$

Se existisse $k \neq m$ tal que $v_{P_0}(w_k) = 0$, a ordem do segundo membro de (3.5) em P_0 seria j_m, enquanto, pela desigualdade triangular, a ordem do primeiro membro de (3.5) em P_0 seria maior do que j_m, o que é impossível. Isso mostra que m é o único elemento do conjunto $\{i;\ v_{P_0}(w_i) = 0\}$. Desse modo, a ordem do primeiro membro de (3.5) em P_0 é no mínimo q. Visto que $1 = j_1 < \cdots < j_{N-1} < q$ e $j_N = q+1$ devido ao Lema 2.10.16, $m = N$ e $v_{P_0}(w_1) = 1$.

Multiplicando ambos os lados da relação (3.2) por $t^{e_{P_0}}$, obtemos

$$w_0(t) + w_1(t)(a_1 t^{j_1} + \cdots)^q + \cdots + w_N(t)(a_N t^{j_N} + \cdots)^q = 0$$

e, consequentemente,

$$w_0(t) = -w_1(t)(a_1 t^{j_1} + \cdots)^q - \cdots - w_N(t)(a_N t^{j_N} + \cdots)^q.$$

Logo, $v_{P_0}(w_0) = q+1$. Isso mostra que o divisor $(\pi^*)^{-1}(H)$ de $\mathscr{X}$ é $(q+1)P_0$ e, assim, $\deg(\pi^*(\mathscr{X})) = q+1$. Aplicando esse argumento a um ponto de $\mathscr{X} \setminus \mathscr{X}(\mathbb{F}_{q^2})$ no lugar de P_0, mostra-se que $(\pi^*)^{-1}(H) = qP + \mathbf{Fr}_{q^2}(P)$. □

Visto que $\mathscr{D}$ é uma série linear completa, o Lema 3.2.3 nos conta que $|\pi^*|$ é uma subsérie linear de $\mathscr{D}$.

Lema 3.2.4. Para cada $i \in \{0,\ldots,N\}$, z_i é uma combinação $\mathbb{F}_{q^2}$-linear das funções $f_0,\ldots,f_N$.

O Lema 3.2.3 junto com a Observação 3.1.6 nos fornece o resultado seguinte.

Lema 3.2.5. As curvas $\mathscr{X}$ e $\pi^*(\mathscr{X})$ são $\mathbb{F}_{q^2}$-isomorfas.

Teorema 3.2.6. A curva $\mathscr{X}$ está contida em uma variedade hermitiana definida sobre $\mathbb{F}_{q^2}$ de $\mathbb{P}^N(\overline{\mathbb{F}}_{q^2})$.

Demonstração. Sem perda de generalidade, suponhamos que $f_0 = z_0 = 1$. Para cada $i \in \{0,\ldots,N\}$, escrevamos

$$z_i = \sum_{j=0}^{N} c_{ij} f_j \tag{3.6}$$

com $c_{ij} \in \mathbb{F}_{q^2}$. Em particular, $c_{01} = \cdots = c_{0N} = 0$ e $c_{ij} = 0$ para cada $i \in \{M+1,\ldots,N\}$. Como $\pi^*(\mathscr{X})$ é uma curva não degenerada em $\mathbb{P}^M$, o conjunto $\{z_0,\ldots,z_M\}$ é linearmente independente sobre $\mathbb{F}_{q^2}$ e, por conseguinte, a matriz $C := (c_{ij})$ tem posto $M+1$.

Mostraremos que C é uma matriz hermitiana sobre $\mathbb{F}_{q^2}$. Reescrevendo a relação (3.2), obtemos

$$\sum_{i=0}^{N}\sum_{j=0}^{N} c_{ij} f_j f_i^q = 0. \tag{3.7}$$

ou seja,

$$1^q f_0 + \sum_{i=0}^{N} (c_{i1}^q f_i)^q f_1 + \cdots + \sum_{i=0}^{N} (c_{iN}^q f_i)^q f_N = 0.$$

Pelo Lema 3.1.3, existe $\lambda \in \mathbb{F}_{q^2}(\mathscr{X})$ tal que

$$1 = \lambda z_0 \tag{3.8}$$

e

$$\sum_{i=0}^{N} c_{ij}^q f_i = \lambda z_j \quad \forall j \in \{1,\ldots,N\}. \tag{3.9}$$

Da relação (3.8), $\lambda = 1$. Isso nos permite reescrever a relação (3.9) da maneira seguinte:

$$\sum_{i=0}^{N} c_{ij}^q f_i = \sum_{i=0}^{N} c_{ji} f_i \quad \forall j \in \{1,\ldots,N\}.$$

Como $\{f_0, f_1, \ldots, f_N\}$ é linearmente independente sobre $\mathbb{F}_{q^2}$, $c_{ij}^q = c_{ji}$ para todos $i, j \in \{0,\ldots,N\}$. Em outras palavras, C é hermitiana. Temos

$$\sum_{i=0}^{N}\sum_{j=0}^{N} c_{ij} f_j f_i^q = 0.$$

Pela relação (3.6), $\mathscr{X}$ está contida na variedade de posto $M+1$ seguinte:

$$\mathbf{v}\left(\sum_{i=0}^{N}\sum_{j=0}^{N} c_{ij}X_jX_i^q\right).$$

□

Teorema 3.2.7 (Teorema do Mergulho Natural)**.** A curva $\mathscr{X}$ admite um modelo não singular dado por uma curva definida sobre $\mathbb{F}_{q^2}$ que tem grau $q+1$ e está contida em uma variedade hermitiana não degenerada definida sobre $\mathbb{F}_{q^2}$ de $\mathbb{P}^M(\overline{\mathbb{F}}_{q^2})$ com $M \leq N$.

Demonstração. Pelo Lema 3.2.5, já sabemos que $\pi^*(\mathscr{X})$ é um modelo não singular de $\mathscr{X}$. Mostraremos que $\pi^*(\mathscr{X})$ está contida em uma variedade hermitiana não degenerada de $\mathbb{P}^M(\mathbb{F}_{q^2})$.

Consideremos a notação da prova do Teorema 3.2.6. Pela Proposição 2.12.8, existe uma transformação $\mathbb{F}_{q^2}$-linear $\mathfrak{T}$ tal que

$$\mathfrak{T}\cdot\mathbf{v}\left(\sum_{i,j=0}^{N} c_{ij}X_jX_i^q\right) = \mathbf{v}\left(X_0^{q+1}+\cdots+X_M^{q+1}\right)$$

Compondo π com $\mathfrak{T}$ se for necessário, podemos supor que

$$f_0^{q+1}+\cdots+f_M^{q+1}=0, \tag{3.10}$$

ou seja,

$$f_0^q f_0+\cdots+f_M^q f_M+0^q f_{M+1}+\cdots+0^q f_N=0.$$

Então, podemos tomar

$$z_i=\begin{cases} f_i & \text{se } i\in\{0,\ldots,M\}\\ 0 & \text{se } i\in\{M+1,\ldots,N\}.\end{cases}$$

Com essa escolha, π^* é a projeção

$$\begin{array}{rccc}(f_0:\cdots:f_M):& \mathscr{X} & \to & \mathbb{P}^M\\ & (\alpha_0:\cdots:\alpha_N) & \mapsto & (\alpha_0:\cdots:\alpha_M)\end{array}$$

e, pela relação (3.10),

$$\pi^*(\mathscr{X})\subset\mathbf{v}(X_0^{q+1}+\cdots+X_M^{q+1}).$$

□

Observação 3.2.8. Veremos que nossas principais conclusões ainda valerão se $\mathscr{X}$ tiver gênero zero. Suponhamos que $\mathscr{X}$ seja a reta $\mathbf{v}_p(Y)\subset\mathbb{P}^2(\overline{\mathbb{F}}_{q^2})$ e que $P_0=(1:0:0)$. Pelo Teorema de Riemann-Roch, $\ell((q+1)P_0)=q+2$. Notemos que $\{x^{q+1},x^q,\ldots,x^2,-x,-1\}$ é uma base de $\mathscr{L}((q+1)P_0)$. O morfismo

$$\pi=(x^{q+1}:-x:x^q:-1:x^2:x^3:\cdots:x^{q-1}),$$

associado a $\mathscr{D} := |(q+1)P_0|$, é dado por

$$\begin{array}{rcl} \mathscr{X} & \to & \mathbb{P}^{q+1}(\overline{\mathbb{F}}_{q^2}) \\ (\alpha:0:\gamma) & \mapsto & (\alpha^{q+1}:-\alpha\gamma^q:\alpha^q\gamma:-\gamma^{q+1}:\alpha^2\gamma^{q-1}:\cdots:\alpha^{q-1}\gamma^2). \end{array}$$

AFIRMAÇÃO 1. As curvas $\mathscr{X}$ e $\pi(\mathscr{X})$ são isomorfas.
De fato, π admite o morfismo inverso

$$\begin{array}{rcl} \pi(\mathscr{X}) & \to & \mathscr{X} \\ (\alpha_0:\cdots:\alpha_{q+1}) & \mapsto & \begin{cases} (\alpha_1:0:\alpha_3) & \text{se } (\alpha_1,\alpha_3)\neq(0,0) \\ (\alpha_0:0:\alpha_2) & \text{se } (\alpha_0,\alpha_2)\neq(0,0). \end{cases} \end{array}$$

Identifiquemos $\mathscr{X}$ com $\pi(\mathscr{X})$. Observando que

$$1^q\cdot x^{q+1}+x^q\cdot(-x)+(x^q)^q\cdot x^q+(x^{q+1})^q\cdot(-1)=0, \tag{3.11}$$

tomemos

$$z_0=1,\quad z_1=x,\quad z_2=x^q,\quad z_3=x^{q+1}\quad\text{e}\quad z_i=0\quad\forall i\in\{4,\ldots,q+1\}.$$

O morfismo $\pi^* := (1:x:x^q:x^{q+1})$ é dado por

$$\begin{array}{rcl} \mathscr{X} & \to & \mathbb{P}^3(\overline{\mathbb{F}}_{q^2}) \\ (\alpha_0:\cdots:\alpha_{q+1}) & \mapsto & (-\alpha_3:-\alpha_1:\alpha_2:\alpha_0). \end{array}$$

AFIRMAÇÃO 2. As curvas $\mathscr{X}$ e $\pi^*(\mathscr{X})$ são isomorfas.
De fato, π^* admite o morfismo inverso

$$\begin{array}{rcl} \pi^*(\mathscr{X}) & \to & \mathscr{X} \\ (\alpha_0:\cdots:\alpha_3) & \mapsto & \begin{cases} (\alpha_1^{q+1}:-\alpha_1\alpha_0^q:\alpha_1^q\alpha_0:-\alpha_0^{q+1}:\alpha_1^2\alpha_0^{q-1}:\cdots:\alpha_1^{q-1}\alpha_0^2) \\ (\alpha_3^{q+1}:-\alpha_3\alpha_2^q:\alpha_3^q\alpha_2:-\alpha_2^{q+1}:\alpha_3^2\alpha_2^{q-1}:\cdots:\alpha_3^{q-1}\alpha_2^2). \end{cases} \end{array}$$

AFIRMAÇÃO 3. A série linear $|\pi^*|$ contém todos os divisores da forma $qP+\mathbf{Fr}_{q^2}(P)$.
Com efeito, consideremos $a\in\overline{\mathbb{F}}_{q^2}$, o ponto

$$P=\pi(a:0:1)=(a^{q+1}:-a^q:a^{q-1}:a^{q-2}:\cdots:a^2:a:-1)$$

e o hiperplano

$$H=\mathbf{v}(a^{q^2+q}X_0-a^qX_1-a^{q^2}X_2+X_3).$$

A função $t := x-a$ é um parâmetro local de $\mathscr{X}$ em P. Assim,

$$x^i=(a+t)^i$$

é a expansão local de x^i em P para cada $i\in\{0,1,q,q+1\}$. Temos

$$a^{q^2+q}-a^q(a+t)-a^{q^2}(a+t)^q+(a+t)^{q+1}=t^q(a-a^{q^2}+t).$$

Além disso,

$$\pi^*(\mathbf{Fr}_{q^2}(P)) = (1 : a^{q^2} : a^{q^3} : a^{q^3+q^2})$$

e

$$a^{q^2+q} - a^q a^{q^2} - a^{q^2} a^{q^3} + a^{q^3+q^2} = 0.$$

Logo, $\pi^{-1}(H) = qP + \mathbf{Fr}_{q^2}(P)$. Além disso,

$$\pi^{-1}(\mathbf{v}(X_0)) = (q+1)(\pi(P_0)).$$

AFIRMAÇÃO 4. A curva $\pi^*(\mathscr{X})$ está contida em uma variedade hermitiana não degenerada definida sobre $\mathbb{F}_{q^2}$ em $\mathbb{P}^3(\overline{\mathbb{F}}_{q^2})$.
De fato, pela relação (3.11),

$$\pi^*(\mathscr{X}) \subset \mathbf{v}(X_0^q X_3 - X_1^{q+1} + X_2^{q+1} - X_0 X_3^q).$$

3.3 A recíproca do Teorema do Mergulho Natural

O objetivo desta seção é mostrar a direção oposta do Teorema 3.2.7. Mais precisamente, desejamos provar o resultado seguinte.

Teorema 3.3.1. Seja $\mathscr{X}$ uma curva algébrica projetiva, geometricamente irredutível e não singular definida sobre $\mathbb{F}_{q^2}$ e que está equipada com um morfismo $\mathbb{F}_{q^2}$-birracional não degenerado $\pi = (f_0 : \cdots : f_M) \colon \mathscr{X} \to \mathbb{P}^M(\overline{\mathbb{F}}_{q^2})$ tal que a curva $\mathscr{Y} := \pi(\mathscr{X})$:
(i) tem grau $q+1$;
(ii) está contida em uma variedade hermitiana não degenerada $\mathscr{H} \subset \mathbb{P}^M(\overline{\mathbb{F}}_{q^2})$ definida sobre $\mathbb{F}_{q^2}$.
Então, a curva $\mathscr{X}$ é $\mathbb{F}_{q^2}$-maximal.

De agora em diante, assumiremos que $\mathscr{X}$ é uma curva satisfazendo as hipóteses do Teorema 3.3.1. Assumiremos também que

$$\mathscr{H} = \mathbf{v}(X_0^{q+1} + \cdots + X_M^{q+1}).$$

Por hipótese,

$$f_0^{q+1} + \cdots + f_M^{q+1} = 0. \tag{3.12}$$

Dado $P \in \mathscr{X}$, escrevamos $\pi(P) = (\alpha_0 : \cdots : \alpha_M)$. Seja t um parâmetro local de $\mathscr{X}$ em P. Arrumemos as funções coordenadas de modo que tenhamos $v_P(f_i) \geq 0$ para cada $i \in \{0, \ldots, M\}$ e $v_P(f_k) = 0$ para pelo menos um índice $k \in \{0, \ldots, M\}$. Então,

$$f_i(t) = \sum_{i=0}^{\infty} a_{i,j} t^j$$

é a expansão local de f_i em P para cada $i \in \{0, \ldots, M\}$. Aqui, $\alpha_i = a_{i,0}$ e $a_{k,0} \neq 0$. O hiperplano tangente H_P à variedade hermitiana em $\pi(P)$ tem equação

$$\alpha_0^q X_0 + \cdots + \alpha_M^q X_M = 0.$$

O primeiro passo em direção ao Teorema 3.3.1 é o lema seguinte.

Lema 3.3.2. A série linear $\mathscr{R}$ cortada em $\mathscr{Y}$ por hiperplanos contém o divisor $qP+\mathbf{Fr}_{q^2}(P)$ para todo $P \in \mathscr{X}$.

Demonstração. Seja $P \in \mathscr{X}$. Queremos mostrar que H_P corta em $\mathscr{Y}$ o divisor $qP+\mathbf{Fr}_{q^2}(P)$. Pela relação (3.13),

$$\left(\sum_{j=0}^{\infty} a_{0,j}t^j\right)^q f_0+\cdots+\left(\sum_{j=0}^{\infty} a_{M,j}t^j\right)^q f_M=0. \tag{3.13}$$

Escrevendo os termos de menor ordem em t, obtemos

$$\sum_{i=0}^{M} a_{i,0}^q f_i + t^q \sum_{i=0}^{M} a_{i,1}^q a_{i,0} + t^{q+1} \sum_{i=0}^{M} a_{i,1}^{q+1} + t^{q+2}[\cdots] = 0,$$

ou seja,

$$\sum_{i=0}^{M} \alpha_i^q f_i = -t^q \sum_{i=0}^{M} a_{i,1}^q a_{i,0} - t^{q+1} \sum_{i=0}^{M} a_{i,1}^{q+1} - t^{q+2}[\cdots].$$

Então, $v_P(\pi^{-1}(H_P)) \geq q$ e a igualdade ocore se, e somente se, $\sum_{i=0}^{M} a_{i,1}^q a_{i,0} \neq 0$. Temos dois casos.

CASO 1: Suponhamos que $P \in \mathscr{X}(\mathbb{F}_{q^2})$. Queremos mostrar que $\sum_{i=0}^{M} a_{i,1}^q a_{i,0} = 0$. Pela relação (3.13),

$$\sum_{i=0}^{M} a_{i,0}^{q+1} + t \sum_{i=0}^{M} a_{i,0}^q a_{i,1} + t^2[\cdots] = 0.$$

Assim, $\sum_{i=0}^{M} a_{i,0}^q a_{i,1} = 0$. Visto que $\left(\sum_{i=0}^{M} a_{i,0}^q a_{i,1}\right)^q = \sum_{i=0}^{M} a_{i,1}^q a_{i,0}$, temos $\sum_{i=0}^{M} a_{i,1}^q a_{i,0} = 0$.

CASO 2: Suponhamos que $P \notin \mathscr{X}(\mathbb{F}_{q^2})$. Visto que $\pi(P) \in \mathscr{H}$, temos $\sum_{i=0}^{M} \alpha_i^{q+1} = 0$ e, logo,

$$\sum_{i=0}^{M} \alpha_i^{q^2+q} = \left(\sum_{i=0}^{M} \alpha_i^{q+1}\right)^q = 0.$$

Isso mostra que $\mathbf{Fr}_{q^2}(P) \in H_P$.

Em ambos os casos, temos $\pi^{-1}(H_P) = qP+\mathbf{Fr}_{q^2}(P)$ uma vez que π é birracional e $\deg(\mathscr{Y}) = q+1$. □

Da Observação 3.1.6 e do Lema 3.3.2, decorre que $\mathscr{X}$ e $\mathscr{Y} = \pi(\mathscr{X})$ são $\mathbb{F}_{q^2}$-isomorfas. Então, se $M = 2$, $\mathscr{Y}$ é a curva hermitiana e, consequentemente, $\mathscr{X}$ é $\mathbb{F}_{q^2}$-maximal. De agora em diante, assumiremos que $M \geq 3$.

Observação 3.3.3. A curva $\mathscr{Y}$ não é estranha. De fato, dado um ponto $P = (\alpha_0 : \cdots : \alpha_M) \in \mathscr{H}$, a equação do hiperplano tangente a $\mathscr{H}$ em P é

$$\alpha_0^q X_0 + \cdots + \alpha_M^q X_M = 0.$$

Consideremos $Q \in \mathbb{P}^M(\overline{\mathbb{F}}_{q^2})$ e escrevamos $Q = (\beta_0^q : \cdots : \beta_M^q)$. Notemos que Q pertencerá ao hiperplano tangente a $\mathscr{H}$ em P se, e somente se,

$$\alpha_0^q\beta_0^q + \cdots + \alpha_M^q\beta_M^q = 0,$$

o que ocorrerá se e, somente se,

$$\alpha_0\beta_0 + \cdots + \alpha_M\beta_M = 0.$$

Ou seja, Q pertence ao hiperplano tangente aos pontos da secção de $\mathscr{H}$ pelo hiperplano de equação

$$\beta_0 X_0 + \cdots + \beta_M X_M = 0.$$

Visto que $\mathscr{Y}$ é não degenerada, existem apenas uma quantidade finita de pontos de $\mathscr{Y}$ nesse hiperplano.

Encontraremos uma certa relação entre o determinante wronskiano de $\mathscr{Y}$ e o de sua projeção $\overline{\mathscr{Y}}$ a um subespaço $(M-1)$-dimensional de $\mathbb{P}^M(\overline{\mathbb{F}}_{q^2})$. Mais precisamente, seja

$$\overline{\pi} = (f_0 : \cdots : f_{M-1}) \colon \mathscr{X} \to \mathbb{P}^{M-1}(\overline{\mathbb{F}}_{q^2}),$$

isto é, $\overline{\mathscr{Y}}$ é a projeção de $\mathscr{Y}$ pelo ponto $(0 : \cdots : 0 : 1)$ ao hiperplano $X_M = 0$. Pode acontecer que $\mathscr{Y}$ e $\overline{\mathscr{Y}}$ não sejam $\mathbb{F}_{q^2}$-birracionalmente equivalentes. Entretanto, é sempre possível evitar essa situação mudando o sistema de coordenadas em $\mathbb{P}^M(\overline{\mathbb{F}}_{q^2})$. Dois lemas técnicos são necessários.

Lema 3.3.4. A curva $\mathscr{Y}$ não é estranha.

Demonstração. Fixemos $P \in \mathbb{P}^M(\overline{\mathbb{F}}_{q^2})$ e escrevamos $P = (\beta_0^q : \cdots : \beta_M^q)$ com $\beta_0, \ldots, \beta_M \in \overline{\mathbb{F}}_{q^2}$. Dado $Q = (\alpha_0 : \cdots : \alpha_M) \in \mathscr{H}$, o hiperplano tangente a $\mathscr{H}$ em Q é

$$H_Q = \mathbf{v}(\alpha_0^q X_0 + \cdots + \alpha_M^q X_M)$$

e $P \in H_Q$ se, e somente se,

$$\alpha_0\beta_0 + \cdots + \alpha_M\beta_M = 0.$$

Isso mostra que os únicos hiperplanos tangentes a $\mathscr{H}$ que contém P são aqueles que tangenciam $\mathscr{H}$ nos pontos da secção

$$\mathscr{H} \cap \mathbf{v}(\beta_0 X_0 + \cdots + \beta_M X_M).$$

Como $\mathscr{Y}$ é não degenerada, existe apenas uma quantidade finita de pontos de $\mathscr{Y}$ nessa secção. Portanto, P pertence apenas a uma quantidade finita de hiperplanos osculadores a $\mathscr{Y}$ e, a fortiori, pertence apenas a uma quantidade finita de retas tangentes a $\mathscr{Y}$. □

Lema 3.3.5. A curva $\mathscr{Y}$ tem no máximo $q^3 + 1$ pontos $\mathbb{F}_{q^2}$-racionais.

Demonstração. Seja g o gênero de $\mathscr{Y}$. Pela Cota de Hasse-Weil,

$$\#\mathscr{Y}(\mathbb{F}_{q^2}) \leq 1+q^2+2qg.$$

Pelo Lema 3.3.4 e pela Cota de Castelnuovo,

$$g \leq \frac{qs+rs+r-q}{2},$$

onde r e s são os únicos inteiros que satisfazem

$$0 \leq r < M-1 \quad \text{e} \quad q = (M-1)s+r.$$

Para concluir essa demonstração, verificaremos que $qs+rs+r \leq q^2$ analisando dois casos.

CASO 1. Suponhamos que $M \leq q+3$. Substituindo s por $\frac{q-r}{M-1}$, obtemos

$$qs+sr+r = \frac{q^2-r^2}{M-1}+r \leq \frac{q^2}{M-1}+M-2.$$

Observemos que $q^2 \geq M-1$. Multiplicando os dois membros dessa desigualdade por $2-M$, obtemos $(2-M)q^2 \leq (2-M)(M-1)$. Logo,

$$\frac{q^2}{M-1}+M-2 \leq q^2.$$

CASO 2. Suponhamos que $M \geq q+3$. Colocando $q-(M-1)s$ no lugar de r, obtemos

$$qs+sr+r = 2qs+(1-M)s^2+(1-M)s+q \leq 2sq+q.$$

Visto que $s \leq \frac{q}{M-1}$ e $\frac{1}{M-1} \leq \frac{1}{q+2}$,

$$2sq+q \leq \frac{2q^2}{M-1}+q \leq \frac{2q^2}{q+2}+q = \frac{3q^2+2q}{q+2}.$$

Notemos que $2q \leq q^2$. Somando q^2 em ambos os lados dessa desigualdade, obtemos $q^2+2q \leq 2q^2$. Como $q \geq 2$, temos $q^2+2q \leq q^3$. Logo,

$$3q^2+2q \leq q^3+2q^2,$$

ou seja,

$$\frac{3q^2+2q}{q+2} \leq q^2.$$

□

Lema 3.3.6. 1. Seja $\mathscr{L}$ uma reta $\mathbb{F}_{q^2}$-racional passando por um ponto $\mathbb{F}_{q^2}$-racional R de $\mathscr{Y}$. Então, $\mathscr{L} \cap \mathscr{Y}$ contém apenas pontos $\mathbb{F}_{q^2}$-racionais de $\mathscr{Y}$.

2. Seja $Q \in \mathscr{Y}(\mathbb{F}_{q^2})$. O espaço $\mathbb{P}^M(\mathbb{F}_{q^2})$ contém um ponto P satisfazendo as duas condições seguintes:

   (i) $P \notin \mathscr{H}$;

   (ii) a reta que liga P e Q não é tangente a $\mathscr{Y}$ em Q

   (iii) a reta que liga P e Q não passa por outro ponto de $\mathscr{Y}$ além de Q.

Demonstração. 1. Suponhamos, por absurdo, que a interseção $\mathscr{L} \cap \mathscr{Y}$ contenha um ponto S que não seja $\mathbb{F}_{q^2}$-racional. Então, $\mathscr{L}$ é a reta que passa pelos pontos S e $\mathbf{Fr}_{q^2}(S)$. Isso implica que a reta $\mathscr{L}$ está contida no hiperplano osculador a $\mathscr{Y}$ em S. Como $H_S \cap \mathscr{Y} = \{S, \mathbf{Fr}_{q^2}(S)\}$, temos $\mathscr{L} \cap \mathscr{Y} = \{S, \mathbf{Fr}_{q^2}(S)\}$. Isso contradiz a hipótese de que o ponto $\mathbb{F}_{q^2}$-racional R pertence à interseção $\mathscr{L} \cap \mathscr{Y}$.

2. Pelo item anterior, basta mostrarmos que existe $P \in \mathbb{P}^M(\mathbb{F}_{q^2})$ satisfazendo (i), (ii) e:

   (iii') a reta que liga P e Q não passa por outro ponto $\mathbb{F}_{q^2}$-racional de $\mathscr{Y}$ além de Q.

   Para isso, basta provarmos a desigualdade

$$\#\mathbb{P}^M(\mathbb{F}_{q^2}) > \#\mathscr{H}(\mathbb{F}_{q^2}) + \#\left\{\begin{array}{c}\text{pontos } \mathbb{F}_{q^2}\text{-racionais}\\ \text{diferentes de } Q\\ \text{nas cordas ligando}\\ Q \text{ a outros pontos}\\ \mathbb{F}_{q^2}\text{-racionais de } \mathscr{Y}\end{array}\right\} + \#\left\{\begin{array}{c}\text{pontos } \mathbb{F}_{q^2}\text{-racionais}\\ \text{diferentes de } Q\\ \text{na tangente a } \mathscr{Y} \text{ em } Q\end{array}\right\}.$$

   Pelo Lema 3.3.5, existem no máximo q^3 cordas ligando Q a outro ponto $\mathbb{F}_{q^2}$-racional de $\mathscr{Y}$. Por isso e pelo Teorema [], o membro direito da desiguladade anterior é no máximo

$$\frac{(q^{M+1}-(-1)^{M+1})(q^M-(-1)^M)}{q^2-1} + q^2q^3 + q^2.$$

   Assim, para mostrarmos que a desigualdade acima é verdadeira, basta verificarmos a desigualdade

$$q^{2M} + q^{2M-2} + \cdots + q^2 + 1 > \frac{(q^{M+1}-(-1)^{M+1})(q^M-(-1)^M)}{q^2-1} + q^5 + q^2,$$

   que equivale a

$$q^{2M+2} - 1 > (q^{M+1}-(-1)^{M+1})(q^M-(-1)^M) + q^7 - q^5 + q^4 - q^2$$

   e, que por sua vez, equivale a

$$\begin{cases} q^{2M+2} + q^{M+1} + q^5 + q^2 > q^{2M+1} + q^M + q^7 + q^4 & \text{se } M \text{ for par} \\ q^{2M+2} + q^M + q^5 + q^2 > q^{2M+1} + q^{M+1} + q^7 + q^4 & \text{se } M \text{ for ímpar.} \end{cases} \tag{3.14}$$

   Para concluirmos a demonstração, verificaremos as desigualdades de (3.14).

CASO 1. Suponhamos que M seja par e que $M \geq 6$. Notemos que $q^{2M+1} > q^M$. Somando q^{2M+1} em ambos os lados dessa desigualdade, obtemos $2q^{2M+1} > q^{2M+1}$. Como $q \geq 2$, temos $q^{2M+2} > q^{2M+1} + q^M$. Além disso, valem as desigualdades $q^{M+1} \geq q^7$ e $q^5 > q^4$.

CASO 2. Suponhamos que M seja impar e que $M \geq 7$. Nesse caso, temos $q^{2M+2} > q^{2M+1} + q^{M+1}$, $q^M \geq q^7$ e $q^5 > q^4$.

CASO 3. Se $M = 3$, então $q^{2M+2} \geq q^{2M+1} + q^7$ e $q^5 > q^{M+1} + q^4$.

CASO 4. Se $M = 4$, então $q^{2M+2} > q^{2M+1} + q^7$ e $q^{M+1} \geq q^M + q^4$.

CASO 5. Se $M = 5$, então $q^{2M+2} > q^{2M+1} + q^{M+1} + q^7$ e $q^M > q^4$.

□

Tomemos um ponto P como no item 2 do Lema 3.3.6. Pelo Teorema 2.12.7, podemos aplicar uma transformação $\mathbb{F}_{q^2}$-linear de $\mathbb{P}^M(\overline{\mathbb{F}}_{q^2})$ que preserva $\mathscr{H}$ e leva P em $(0 : \cdots : 0 : 1)$. O Lema 3.3.6 garante que $\mathscr{Y}$ e $\overline{\mathscr{Y}}$ são $\mathbb{F}_{q^2}$-birracionalmente equivalentes. Então, assumamos que $\mathscr{Y}$ é $\mathbb{F}_{q^2}$-birracionalmente equivalente a $\overline{\mathscr{Y}}$.

Escolhamos uma variável separante t de $\mathscr{X}$. Consideremos as notações seguintes:

$$\mathscr{W}(f_0, \ldots, f_{M-1}) := \det \begin{pmatrix} \mathrm{D}_t^{(\varepsilon_0)} f_0 & \mathrm{D}_t^{(\varepsilon_0)} f_1 & \cdots & \mathrm{D}_t^{(\varepsilon_0)} f_{M-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{D}_t^{(\varepsilon_{M-1})} f_0 & \mathrm{D}_t^{(\varepsilon_{M-1})} f_1 & \cdots & \mathrm{D}_t^{(\varepsilon_{M-1})} f_{M-1} \end{pmatrix}$$

e

$$\mathscr{W}(f_0, \ldots, f_M) := \det \begin{pmatrix} \mathrm{D}_t^{(\varepsilon_0)} f_0 & \mathrm{D}_t^{(\varepsilon_0)} f_1 & \cdots & \mathrm{D}_t^{(\varepsilon_0)} f_M \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{D}_t^{(\varepsilon_M)} f_0 & \mathrm{D}_t^{(\varepsilon_M)} f_1 & \cdots & \mathrm{D}_t^{(\varepsilon_M)} f_M \end{pmatrix}. \tag{3.15}$$

Notemos que $\varepsilon_0 = 0$, $\varepsilon_1 = 1$ e $\varepsilon_M = q$.

Lema 3.3.7. Temos

$$\mathrm{div}(\mathscr{W}(f_0, \ldots, f_M)) = \mathrm{div}(\mathscr{W}(f_0, \ldots, f_{M-1})) - q\,\mathrm{div}(f_M) + \mathrm{div}(f_0 \mathrm{D}_t^{(q)} f_0^q + \cdots + f_M \mathrm{D}_t^{(q)} f_M^q).$$

Demonstração. Sejam $c_0, \ldots, c_M$ as colunas da matriz em (3.15). Substituindo a coluna c_M pela combinação

$$f_0^q c_0 + f_1^q c_1 + \cdots + f_{M-1}^q c_{M-1} + f_M^q c_M,$$

obtemos

$$f_M^q \mathscr{W}(f_0, \ldots, f_M) = \det \begin{pmatrix} f_0 & \cdots & f_{M-1} & f_0^{q+1} + \cdots + f_M^{q+1} \\ \mathrm{D}_t f_0 & \cdots & \mathrm{D}_t f_{M-1} & f_0^q \mathrm{D}_t f_0 + \cdots + f_M^q \mathrm{D}_t f_M \\ \vdots & \ddots & \vdots & \vdots \\ \mathrm{D}_t^{(\varepsilon_{M-1})} f_0 & \cdots & \mathrm{D}_t^{(\varepsilon_{M-1})} f_{M-1} & f_0^q \mathrm{D}_t^{(\varepsilon_{M-1})} f_0 + \cdots + f_M^q \mathrm{D}_t^{(\varepsilon_{M-1})} f_M \\ \mathrm{D}_t^{(q)} f_0 & \cdots & \mathrm{D}_t^{(q)} f_{M-1} & f_0^q \mathrm{D}_t^{(q)} f_0 + \cdots + f_M^q \mathrm{D}_t^{(q)} f_M \end{pmatrix}.$$

Derivando ambos os membros da relação (3.12), concluímos que cada elemento da última coluna é 0, exceto o último. Além disso, calculando a q-ésima derivada de Hasse de ambos os lados, obtemos

$$f_0^q \mathrm{D}_t^{(q)} f_0 + \cdots + f_M^q \mathrm{D}_t^{(q)} f_M + f_0 \mathrm{D}_t^{(q)} f_0^q + \cdots + f_M \mathrm{D}_t^{(q)} f_M^q = 0.$$

Utilizando o método de Laplace, obtemos

$$f_M^q \mathscr{W}(f_0,\ldots,f_M) = -(f_0 \mathrm{D}_t^{(q)} f_0^q + \cdots + f_M \mathrm{D}_t^{(q)} f_M^q)\mathscr{W}(f_0,\ldots,f_{M-1})$$

e, logo,

$$q\mathrm{div}(f_M) + \mathrm{div}(\mathscr{W}(f_0,\ldots,f_M)) = \mathrm{div}(f_0 \mathrm{D}_t^{(q)} f_0^q + \cdots + f_M \mathrm{D}_t^{(q)} f_M^q) + \mathrm{div}(\mathscr{W}(f_0,\ldots,f_{M-1})).$$

□

Seja R_M o divisor de ramificação da série linear cortada em $\mathscr{Y}$ por hiperplanos de $\mathbb{P}^M(\overline{\mathbb{F}}_{q^2})$. O resultado seguinte segue do fato de que $e_P = 0$.

Lema 3.3.8. Seja $P \in \mathscr{X}$. Se t for um parâmetro local de $\mathscr{X}$ em P, então

$$v_P(R_M) = v_P(\mathscr{W}(f_0,\ldots,f_M)).$$

Similarmente, seja R_{M-1} o divisor de ramificação da série linear cortada em $\overline{\mathscr{Y}}$ por hiperplanos de $\mathbb{P}^{M-1}(\overline{\mathbb{F}}_{q^2})$.

Lema 3.3.9. Seja $P \in \mathscr{X}$. Se t for um parâmetro local de $\mathscr{X}$ em P, então

$$v_P(R_{M-1}) = v_P(\mathscr{W}(f_0,\ldots,f_{M-1})).$$

Demonstração. Temos

$$v_P(R_{M-1}) = v_P(\mathscr{W}(f_0,\ldots,f_{M-1})) + (\varepsilon_0 + \cdots + \varepsilon_{M-1})v_P(dt) + M\overline{e}_P$$

onde $\overline{e}_P = -\min\{v_P(f_0),\ldots,v_P(f_{M-1})\}$. Suponhamos, por absurdo, que $\overline{e}_P < 0$. Como $e_P = 0$, temos $f_M(P) \neq 0$ e $f_i(P) = 0$ para todo $i \in \{0,\ldots,M-1\}$, contradizendo a relação (3.12). Assim, $\overline{e}_P = 0$. Visto que t é um parâmetro local de $\mathscr{X}$ em P, temos $v_P(dt) = 0$. Isso conclui a prova. □

O resultado seguinte será fundamental para calcularmos $\#\mathscr{X}(\mathbb{F}_{q^2})$.

Lema 3.3.10. Temos

$$v_P(f_0 \mathrm{D}_t^{(q)} f_0^q + \cdots + f_M \mathrm{D}_t^{(q)} f_M^q) = \begin{cases} 1 & \text{se } P \in \mathscr{X}(\mathbb{F}_{q^2}) \\ 0 & \text{se } P \notin \mathscr{X}(\mathbb{F}_{q^2}). \end{cases}$$

Demonstração. Notemos que

$$f_0 \mathrm{D}_t^{(q)} f_0^q + \cdots + f_M \mathrm{D}_t^{(q)} f_M^q = \left(\sum_{j=0}^{\infty} a_{0,j} t^j \right) (a_{0,1}^q + t^q[\cdots]) + \cdots + \left(\sum_{j=0}^{\infty} a_{M,j} t^j \right) (a_{M,1}^q + t^q[\cdots])$$
$$= \sum_{i=0}^{M} a_{i,0} a_{i,1}^q + t \sum_{i=0}^{M} a_{i,1}^{q+1} + t^2[\cdots].$$

Temos dois casos.

CASO 1: Suponhamos que $P \in \mathscr{X}(\mathbb{F}_{q^2})$. Pela demonstração do Lema 3.3.2, temos $\sum_{i=0}^{M} a_{i,1}^q a_{i,0} = 0$ e $\sum_{i=0}^{M} a_{i,1}^{q+1} \neq 0$. Assim, $v_P(f_0 \mathrm{D}_t^{(q)} f_0^q + \cdots + f_M \mathrm{D}_t^{(q)} f_M^q) = 1$.

CASO 2: Suponhamos que $P \notin \mathscr{X}(\mathbb{F}_{q^2})$. Utilizando a demonstração do Lema 3.3.2 novamente, concluímos que $\sum_{i=0}^{M} a_{i,1}^q a_{i,0} \neq 0$. Logo, $v_P(f_0 \mathrm{D}_t^{(q)} f_0^q + \cdots + f_M \mathrm{D}_t^{(q)} f_M^q) = 0$. □

Observação 3.3.11. Esse lema nos conta que

$$\sum v_P(f_0 \mathrm{D}_t^{(q)} f_0^q + \cdots + f_M \mathrm{D}_t^{(q)} f_M^q) = \#\mathscr{X}(\mathbb{F}_{q^2}).$$

Agora, estamos preparados para finalizar a demonstração do Teorema 3.3.1.

Demonstração. [Demonstração do Teorema 3.3.1] Temos

$$\sum_{P \in \mathscr{X}} v_P(R_M) = (\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_M)(2g-2) + (M+1)(q+1)$$

e

$$\sum_{P \in \mathscr{X}} v_P(R_{M-1}) = (\varepsilon_0 + \varepsilon_1 + \cdots + \varepsilon_{M-1})(2g-2) + M(q+1).$$

Então,

$$\sum_{P \in \mathscr{X}} (v_P(R_M) - v_P(R_{M-1})) = q(2g-2) + q + 1.$$

Pelo Lema 3.3.7, temos

$$\mathrm{div}(f_0 \mathrm{D}_t^{(q)} f_0^q + \cdots + f_M \mathrm{D}_t^{(q)} f_M^q) = \mathrm{div}(\mathscr{W}(f_0, \ldots, f_M)) - \mathrm{div}(\mathscr{W}(f_0, \ldots, f_{M-1})) + q\,\mathrm{div}(f_M).$$

Pelos Lemas 3.3.8 e 3.3.9, temos

$$v_P(\mathrm{div}(f_0 \mathrm{D}_t^{(q)} f_0^q + \cdots + f_M \mathrm{D}_t^{(q)} f_M^q)) = v_P(R_M) - v_P(R_{M-1}) + q v_P(\mathrm{div}(f_M))$$

para todos $P \in \mathscr{X}$. Pelo Lema 3.3.10, temos

$$\#\mathscr{X}(\mathbb{F}_{q^2}) = \sum_{P \in \mathscr{X}} (v_P(R_M) - v_P(R_{M-1})) + q \sum_{P \in \mathscr{X}} v_P(f_M)$$
$$= q(2g-2) + q + 1 + q(q+1)$$
$$= 1 + q^2 + 2qg.$$

Portanto, a curva $\mathscr{X}$ é $\mathbb{F}_{q^2}$-maximal. □

Observação 3.3.12. Interpretamos os somatórios acima sendo efetuados de maneira dinâmica no seguinte sentido: para cada ponto $P \in \mathscr{X}$, consideramos um parâmetro local e "normalizamos" as funções $f_0, \ldots, f_M$. Com essa interpretação, temos

$$\sum_{P \in \mathscr{X}} v_P(f_M) = q + 1.$$

REFERÊNCIAS

ABDÓN, M.; GARCIA, A. On a characterization of certain maximal curves. **Finite Fields and Their Applications**, v. 10, n. 2, p. 133–158, 2004. Citado na página 18.

ABDÓN, M.; TORRES, F. On maximal curves in characteristic two. **Manuscripta mathematica**, v. 99, p. 39–53, 1999. Citado na página 18.

BOSE, R. C.; CHAKRAVARTI, I. M. Hermitian varieties in a finite projective space PG(n,q^2). **Canadian Journal of Mathematics**, v. 18, p. 1161–1182, 1966. Citado na página 56.

COUTINHO, M. A. N. **Three topics in algebraic curves over finite fields**. 150 p. Tese (Doutorado) — Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2019. Citado nas páginas 19, 42, 43 e 53.

FUHRMANN, R.; GARCIA, A.; TORRES, F. On maximal curves. **Journal of Number Theory**, v. 67, p. 29–51, 1997. Citado nas páginas 18 e 54.

FULTON, W. **Algebraic curves**: an introduction to algebraic geometry. [S.l.: s.n.], 2008. Disponível em: <http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf>. Acesso em: 7 out. 2021. Citado nas páginas 19, 28 e 44.

GARCIA, A.; STICHTENOTH, H. A maximal curve which is not a Galois subcover of the Hermitian curve. **Bulletin of the Brazilian Mathematical Society**, v. 37, n. 1, p. 139–152, 2006. Citado na página 18.

GARCIA, A.; VOLOCH, J. F. Wronskians and linear independence in fields of prime characteristic. **Manuscripta mathematica**, v. 59, p. 457–469, 1987. Citado na página 54.

GIULIETTI, M.; KORCHMÁROS, G. A new family of maximal curves over a finite field. **Mathematische Annalen**, v. 343, p. 229–245, 2009. Citado na página 18.

GOLDSCHMIDT, D. M. **Algebraic functions and projective curves**. New York: Springer, 2003. Citado nas páginas 19, 33 e 34.

HASSE, H. Zur Theorie der abstrakten elliptischen Funktionenkörper III. Die Struktur des Meromorphismenrings. Die Riemannsche Vermutung. **Journal für die reine und angewandte Mathematik**, v. 175, p. 193–208, 1936. Citado na página 17.

HIRSCHFELD, J. W. P. **Projective geometries over finite fields**. New York: Oxford University Press, 1979. Citado nas páginas 55 e 56.

HIRSCHFELD, J. W. P.; KORCHMÁROS, G.; TORRES, F. **Algebraic curves over a finite field**. Princeton: Princeton University Press, 2008. Citado nas páginas 19, 22, 23, 25, 26, 27, 28, 29, 31, 32, 33, 37, 38, 40, 41, 42, 43, 53, 54 e 55.

HIRSCHFELD, J. W. P.; THAS, J. A. **General Galois geometries**. London: Springer, 2016. Citado na página 56.

KAJI, H. Strangeness of higher order for space curves. **Communications in algebra**, v. 20, n. 6, p. 1535–1548, 1992. Citado na página 55.

KORCHMÁROS, G.; TORRES, F. Embedding of a maximal curve in a Hermitian variety. **Compositio Mathematica**, v. 128, p. 95–113, 2001. Citado nas páginas 9, 18 e 57.

LACHAUD, G. Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis. **Comptes rendus de l'Académie des Sciences**, v. 305, p. 729–732, 1987. Citado na página 17.

STICHTENOTH, H. **Algebraic function fields and codes**. 2. ed. Berlin: Springer, 2009. Citado nas páginas 19, 25 e 30.

STÖHR, K.-O.; VOLOCH, J. F. Weierstrass points and curves over finite fields. **Proceedings of the London Mathematical Society**, s3-52, n. 1, p. 1–19, 1986. Citado nas páginas 19, 50, 51 e 52.

TORRES, F. **The approach of Stöhr-Voloch to the Hasse-Weil bound with applications to optimal curves and plane arcs**. 2000. Disponível em: <https://arxiv.org/pdf/math/0011091.pdf>. Acesso em: 7 out. 2021. Citado nas páginas 19, 45, 46, 47, 48 e 49.

WEIL, A. **Sur les courbes algébriques et les variétés qui s'en déduisent**. Paris: Hermann, 1948. Citado na página 17.


ICMC
USP
SÃO CARLOS