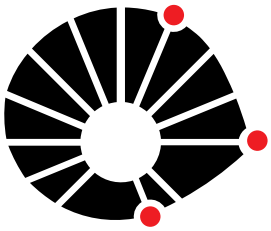

UNICAMP

UNIVERSIDADE ESTADUAL DE CAMPINAS

Instituto de Matemática, Estatística e Computação Científica

LINA ISABEL TRIVIÑO VIERA

Algumas propriedades de curvas algébricas em característica positiva

Campinas

2019

Lina Isabel Triviño Viera

Algumas propriedades de curvas algébricas em característica positiva

Dissertação apresentada ao Instituto de Matemática, Estatística e Computação Científica da Universidade Estadual de Campinas como parte dos requisitos exigidos para a obtenção do título de Mestra em Matemática.

Orientador: Saeed Tafazolian

Este exemplar corresponde à versão final da Dissertação defendida pela aluna Lina Isabel Triviño Viera e orientada pelo Prof. Dr. Saeed Tafazolian.

Campinas

2019

Ficha catalográfica
Universidade Estadual de Campinas
Biblioteca do Instituto de Matemática, Estatística e Computação Científica
Ana Regina Machado - CRB 8/5467

T739a

Triviño Viera, Lina Isabel, 1993-
Algumas propriedades de curvas algébricas em característica positiva / Lina Isabel Triviño Viera. – Campinas, SP : [s.n.], 2019.

Orientador: Saeed Tafazolian.
Dissertação (mestrado) – Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Corpos de funções algébricas. 2. Curvas algébricas. 3. a-número. I. Tafazolian, Saeed, 1978-. II. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. III. Título.

Informações para Biblioteca Digital

Título em outro idioma: Some properties of algebraic curves in positive characteristic
Palavras-chave em inglês:
Algebraic function fields
Algebraic curves
a-number
Área de concentração: Matemática
Titulação: Mestra em Matemática
Banca examinadora:
Saeed Tafazolian [Orientador]
Herivelto Martins Borges Filho
Fernando Eduardo Torres Orihuela
Data de defesa: 14-08-2019
Programa de Pós-Graduação: Matemática

Identificação e informações acadêmicas do(a) aluno(a)
- ORCID do autor: https://orcid.org/0000-0003-4656-1842
- Currículo Lattes do autor: http://lattes.cnpq.br/7565150254033895

Dissertação de Mestrado defendida em 14 de agosto de 2019 e aprovada pela banca examinadora composta pelos Profs. Drs.

Prof(a). Dr(a). SAEED TAFAZOLIAN

Prof(a). Dr(a). HERIVELTO MARTINS BORGES FILHO

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

A Ata da Defesa, assinada pelos membros da Comissão Examinadora, consta no SIGA/Sistema de Fluxo de Dissertação/Tese e na Secretaria de Pós-Graduação do Instituto de Matemática, Estatística e Computação Científica.

Agradecimentos

Agradeço ao meu orientador Saeed Tafazolian por ter aceitado me orientar e depositar sua confiança em mim.
Agradeço ao professor Fernando Torres por sua disposição, sua ajuda, sua alegria e não menos importante, sua amizade.
Agradeço a minha mãe por seu incondicional apoio e sua fortaleza.
Agradeço especialmente ao meu companheiro de vida e colega, Alejandro Otero, por sua força, amor e por me ajudar a ganhar confiança nos momentos de debilidade.
Um outro agradecimento especial é para o professor Lucas Catão de Freitas Ferreira, por seu excelente trabalho e seu incondicional apoio durante seu período de coordenador de pós-graduação.
Finalmente, agradeço à agencia de fomento FAEPEX/FUNCAMP pelo apoio financeiro (através do processo 2034/18) sem o qual eu não poderia ter feito este trabalho.

Resumo

O objetivo principal da presente dissertação é calcular o a-número de algumas curvas algébricas definidas sobre um corpo K de característica positiva, especificamente, para infinitas curvas hiperelípticas, de Fermat e de Hurwitz.
Para realizar o anterior, principalmente estudamos algumas das noções fundamentais sobre corpos de funções, curvas algébricas e o operador de Cartier, no último caso, centrando nossa atenção em sua ação sobre curvas adjuntas canônicas.

Palavras-chave: Corpos de funções algébricas. Curvas algébricas. a-número.

Abstract

The aim of this dissertation is to calculate the a-number for some algebraic curves which are defined on a field K with positive characteristic, specifically, for infinite hyperelliptic, Fermat and Hurwitz curves.
To carry out this, we study some fundamental notions about algebraic function fields, algebraic curves and Cartier's operator, in the last case, we will focus our attention on the way how the operator acts on canonical adjoints curves.

Keywords: algebraic function fields. algebraic curves. a-number.

Sumário

Introdução

As propriedades geométricas relevantes de uma curva algébrica encontram-se codificadas em seus invariantes birracionais. Entre os invariantes birracionais mais importantes de uma curva encontram-se o gênero e o p-posto -comumente conhecido como invariante de Hasse-Witt- estando este último relacionado ao operador de Cartier mediante sua coincidência com a dimensão do espaço gerado pelos vetores no espaço das diferenciais regulares que são fixas sob a ação do operador de Cartier.
Um outro invariante birracional relacionado com o operador de Cartier tem sido objeto de estudo nos últimos anos, este invariante é conhecido como o a-número. Em geral, o a-número é definido para variedades abelianas sobre corpos de característica $p > 0$, e, no caso do corpo de funções de uma curva $\mathcal{X}$, o a-número da curva, $a(\mathcal{X})$, coincide com a dimensão do núcleo do operador de Cartier, que, por sua vez, coincide com a dimensão do espaço das diferenciais regulares exatas sobre a curva.

Calcular o a-número de uma curva pode ser uma tarefa difícil, aliás, o valor exato do a-número é conhecido somente para algumas poucas famílias de curvas.
O objetivo desta dissertação é calcular o a-número para infinitas curvas pertencentes a três famílias de curvas, a saber,

- Curvas hiperelípticas
- Curvas tipo Fermat
- Curvas tipo Hurwitz

Uma curva projetiva plana sobre uma corpo K de característica $p > 0$ é do tipo Kummer se sua equação afim é da forma:

$$y^n = a \cdot \prod_{i=1}^{s} p_i(x)^{n_i}$$

com $s > 0$, $p_i(x) \in K[x]$, onde os $p_i(x)$ são mônicos irredutíveis diferentes dois a dois, $p \nmid n$, $a \in K$, $n \in \mathbb{Z}$ (ambos não nulos), $\gcd(n, n_i) = 1$ e K contem todas as raízes primitivas da unidade.
Entre as curvas que são objeto do estudo aqui, as curvas hiperelípticas e as curvas do tipo Fermat são casos especiais de curvas tipo Kummer.

Uma Curva generalizada de Hurwitz é representada pela equação afim:

$$x^m y^a + y^n + x^b = 0$$

donde a, b, m, n são inteiros não negativos com algumas restrições adicionais. Em nosso caso, vamos estudar a curva de Hurwitz clássica, isto é, para o caso em que $a = b = 1$ e $m = n$, obtendo uma representação afim do tipo

$$x^n y + y^n + x = 0;$$

quando $n = 3$, a curva $x^3y + y^3 + x = 0$ é conhecida como *curva quártica de Klein*, de fato, para este caso especial, a curva é do tipo Kummer, uma apresentação mais detalhada deste fato será dada no capítulo 3.

Para este trabalho, nos centraremos em calcular o a-número para infinitos valores de n das curvas

$$\begin{aligned} y^2 &= x^n + 1, \\ y^2 &= x^n + x, \\ y^n &= 1 - x^n, \\ y^n &= -x^n y - x. \end{aligned}$$

Para calcular o a-número das curvas hiperelípticas acima, faremos uma exposição detalhada dor resultados apresentados em (NOUROZI; RAHMATI; TAFAZOLIAN, 2019).
Para as curvas de Fermat e Hurwitz, nos basearemos em (MONTANUCCI; SPEZIALI, 2017).

Para finalizar esta introdução, apresentaremos uma descrição de cada capítulo do documento.

No primeiro capítulo, fixaremos as notações e os principais resultados obtidos da teoria dos corpos de funções e das curvas algébricas. É um capítulo de referência, podendo ser omitido pelo leitor que esteja familiarizado.

No segundo capítulo, faremos um estudo detalhado das diferenciais sobre corpos de funções e calcularemos a base para o espaço das diferenciais regulares sobre um corpo de funções hiperelíptico.

No terceiro capítulo, faremos uma revisão rápida das extensões cíclicas de corpos e caracterizaremos um tipo especial dessas extensões, a saber, as extensões de Kummer.

No quarto capítulo estudaremos o operador de Cartier e suas propriedades básicas, dando especial atenção a sua ação sobre curvas adjuntas canônicas e exporemos uma fórmula para esta ação devida a (STöHR; VOLOCH, 1987).

No quinto capítulo falaremos sobre o p-posto e o a-número de uma curva e sua relação com respeito ao operador de Cartier.

Finalmente, o último capítulo é dedicado ao cálculo do a-número das curvas mencionadas acima.

1 Corpos de funções e curvas algébricas

Neste capítulo fazemos uma revisão geral dos conceitos básicos da teoria dos corpos de funções algébricas e das curvas algébricas que serão de grande utilidade no desenvolvimento tanto teórico quanto prático do documento.
Todos os resultados exibidos no presente capítulo serão baseados principalmente em duas referências: (STICHTENOTH, 2008) para a parte dedicada aos corpos de funções e (FULTON, 2008) para a parte dedicada às curvas algébricas; para consultar as demonstrações dos resultados aqui apresentados, encaminharemos o leitor a tais referências indicando o capítulo e o número de tal resultado na respectiva referência no começo de cada enunciado.

1.1 Corpos de funções

Ao longo desta seção vamos supor que K é um corpo. Aqui tomamos como referência o livro (STICHTENOTH, 2008).

1.1.1 Definições fundamentais

Um *corpo de funções algébricas* F/K de uma variável sobre K é uma extensão de K, $F \supset K$, tal que F é uma extensão algébrica finita de $K(x)$ para algum elemento $x \in F$ que é transcendente sobre K.

Na maioria das ocasiões escreveremos simplesmente F para fazer referência ao corpo de funções F/K.

O conjunto

$$\tilde{K} := \{z \in F \mid z \text{ é algébrico sobre } K\},$$

é um subcorpo de F denominado *corpo das constantes* de F/K.

Da definição de corpo de funções segue que $\tilde{K} \subsetneq F$ e, claramente, $K \subseteq \tilde{K}$, assim, temos a torre: $K \subseteq \tilde{K} \subsetneq F$.

Mais adiante veremos uma justificativa do particular nome do corpo $\tilde{K}$.

Dizemos que K é *algebricamente fechado* em F ou que K é o *corpo completo das constantes* de F, se $K = \tilde{K}$.

Outra forma de representar um corpo de funções.

Um corpo de funções F/K é chamado *racional* se $F = K(x)$ para algum $x \in F$ transcendente sobre K.

Um *corpo de funções* F/K é uma extensão algébrica simples de um corpo de funções racional $K(x)$, isto é, $F = K(x, y)$, onde $\phi(y) = 0$ para algum polinômio $\phi \in K(x)[T]$ irredutível.

1.1.2 Anéis de valoração, lugares e valorações

Um anel de valoração do corpo de funções F/K é um anel $\mathcal{O} \subseteq F$ com as seguintes propriedades:

(i) $K \subsetneq \mathcal{O} \subsetneq F$.

(ii) Para todo $z \in F$ não nulo, temos que $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.

Proposição 1.1.1. *(§1.1, Proposition 1.1.5) Seja $\mathcal{O}$ um anel de valoração do corpo de funções F/K. Então $\mathcal{O}$ é um anel local, sendo seu único ideal maximal $P := \mathcal{O}\backslash\mathcal{O}^\times$ onde $\mathcal{O}^\times$ é o grupo das unidades de $\mathcal{O}$.*

Segue trivialmente da proposição acima a seguinte caracterização dos elementos do ideal maximal P:

$$\textit{Seja } 0 \neq x \in F\textit{, então, } x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}.$$

A seguir, um teorema que caracteriza fortemente o anel de valoração $\mathcal{O}$ e o ideal P.

Teorema 1.1.1. *(§1.1, Theorem 1.1.6) Seja $\mathcal{O}$ um anel de valoração do corpo de funções F/K e seja P o seu único ideal maximal, então:*

(a) P é principal.

(b) Se $P = t\mathcal{O}$, então cada $0 \neq z \in F$ tem uma única representação da forma $z = ut^n$ onde $n \in \mathbb{Z}$ e $u \in \mathcal{O}^\times$.

(c) $\mathcal{O}$ é um D.I.P. Mais precisamente, se $P = t\mathcal{O}$ e $\{0\} \neq I \subseteq \mathcal{O}$ é um ideal, então $I = t^n\mathcal{O}$.

Um anel $\mathcal{O}$ satisfazendo as propriedades do teorema acima é denominado *anel de valoração discreta.*

Um *lugar* P do corpo de funções F/K é o ideal maximal de algum anel de valoração $\mathcal{O}$ de F/K.
O elemento gerador de P, ou seja t no caso que $P = t\mathcal{O}$ é chamado de *elemento primo* ou *parâmetro local* de P. O conjunto $\{P \mid P \text{ é um lugar de } F/K\}$ é denotado por $\mathbb{P}_F$.

A continuação vamos definir o conceito de valoração discreta para um corpo de funções, a seguir, vamos procurar uma valoração que dependa do anel $\mathcal{O}_P$ para cada lugar P.

Definição 1.1.1. Uma *valoração discreta* de F/K é uma função $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades:

1. $v(x) = \infty$ se $x = 0$.
2. $v(xy) = v(x) + v(y)$ para todo par $x, y \in F$.
3. $v(x + y) \geqslant \min\{v(x), v(y)\}$ para todo par $x, y \in F$.
4. Existe um elemento $z \in F$ tal que $v(z) = 1$.
5. $v(a) = 0$ para todo $a \in K$.

Observação 1.1.1. Segue das propriedades que v é sobrejetora. A propriedade 3 é chamada de *desigualdade triangular.*

Lema 1.1.1. *(Desigualdade triangular estrita). Seja v uma valoração discreta de F/K e sejam $x, y \in F$ com $v(x) \neq v(y)$. Então $v(x + y) = \min\{v(x), v(y)\}$.*

Ao lugar $P \in \mathbb{P}_F$ associamos a seguinte função

$$v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$$

de tal forma que se t é um parâmetro local de P, teremos que:

$$v_P(z) = \begin{cases} n & se \quad z \neq 0 \\ \infty & se \quad z = 0 \end{cases}$$

Onde $z = ut^n$ se $z \neq 0$, com $u \in \mathcal{O}_P^{\times}$.

Observação 1.1.2. Na definição acima, v_P depende unicamente do lugar P e não do parâmetro local t, como podemos ver: sejam t_1 e t_2 parâmetros locais de P, então $P = t_1\mathcal{O}$

e $P = t_2\mathcal{O}$, assim, $t_1 = t_2x$ e $t_2 = t_1y$, o que implica que $t_1 = (t_1y)x = t_1(xy)$, portanto, x e y são unidades em $\mathcal{O}$. Assim, se $z = ut_1^n$, então $z = ut_2^n x^n = t_2^n(ux^n) = t_2^n w$ sendo $w = ux^n \in \mathcal{O}^\times$. Portanto, $v_P(z)$ é o mesmo para os dois parâmetros locais.

O seguinte teorema caracteriza os anéis de valoração, seus lugares associados e os parâmetros locais desses lugares a partir da função v_P.

Teorema 1.1.2. *(§1.1, Theorem 1.1.13) Seja F/K um corpo de funções.*

(a) Para um lugar $P \in \mathbb{P}_F$, a função v_P definida acima é uma valoração discreta de F/K. Mais ainda, temos:

$$\begin{aligned} \mathcal{O}_P &= \{z \in F \mid v_P(z) \geqslant 0\}, \\ \mathcal{O}_P^\times &= \{z \in F \mid v_P(z) = 0\}, \\ P &= \{z \in F \mid v_P(z) > 0\}. \end{aligned}$$

(b) Um elemento $x \in F$ é um parâmetro local para P se e só se $v_P(x) = 1$.

(c) Reciprocamente, suponha que v é uma valoração discreta de F/K. Então o conjunto $P = \{z \in F \mid v(z) > 0\}$ é um lugar de F/K e $\mathcal{O}_P = \{z \in F \mid v(z) \geqslant 0\}$ é o seu correspondente anel de valoração.

Observação 1.1.3. A projeção canônica $\pi : \mathcal{O}_P \longrightarrow \mathcal{O}_P/P$ induz um mergulho (canônico) de K em $\mathcal{O}_P/P$, isto é, podemos identificar a K com sua imagem em $\mathcal{O}_P/P$ e assim considerar a K como um subcorpo de $\mathcal{O}_P/P$.

Seja $P \in \mathbb{P}_F$. Denotaremos com $F_P := \mathcal{O}_P/P$ ao corpo das classes residuais de P. A função:

$$\begin{array}{ccc} F & \longrightarrow & F_P \cup \{\infty\} \\ x & \longmapsto & x(P) = \begin{cases} x + P & se \quad x \in \mathcal{O}_P \\ \infty & se \quad x \in F \backslash \mathcal{O}_P, \end{cases} \end{array}$$

é chamada *aplicação classe residual com respeito a P.*

Definimos grau$P := [F_P : K]$ como o *grau do lugar P*. Um lugar de grau um é chamado comumente de *racional*.

Proposição 1.1.2. *(§1.1, Proposition 1.1.15) Se P é um lugar de F/K e $0 \neq x \in P$, então grau$P \leqslant [F : K(x)] < \infty$.*

Se K é um corpo algebricamente fechado, então todos os lugares de F são racionais; com efeito, observe primeiro que P é racional se e só se $F_P = K$. Agora, da proposição acima sabemos que $[F_P : K] < \infty$, assim, F_P/K é algébrica, isso significa que $F_P \subseteq \tilde{K}$, assim,

$$K \subseteq F_P \subseteq \tilde{K} = K.$$

Segue que P é racional.
Atrás vimos que a função classe residual envia elementos de F para $F_P \cup \{\infty\}$; se $K = \tilde{K}$, então essa função vai enviar os elementos de F para $K \cup \{\infty\}$ e podemos interpretar cada elemento $z \in F$ como uma função da seguinte forma:

$$\begin{array}{rccc} z & : & \mathbb{P}_F & \longrightarrow & K \cup \{\infty\} \\ & & P & \longmapsto & z(P) \end{array}$$

É por essa razão que F/K é chamado de corpo de funções. Da mesma forma, os elementos de K, interpretados como a função descrita acima, são funções constantes e por isso, K é denominado o corpo das constantes de F.

Definição 1.1.2. Sejam $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um *zero* de z se $v_P(z) > 0$. Se $v_P(z) = m > 0$, dizemos que P é um zero de ordem m. Analogamente, P é dito *polo* de z se $v_P(z) < 0$, e polo de ordem m se $v_P(z) = m < 0$.

Até agora construíram-se alguns fundamentos teóricos em torno dos lugares de um corpo de funções, mas, é necessário garantir a existência deles para que faça sentido tal construção. O teorema seguinte garante aquela existência, por essa razão é um dos teoremas mais importantes desta seção.

Teorema 1.1.3. *(§1.1, Theorem 1.1.19) Sejam F/K um corpo de funções e R um subanel de F com $K \subseteq R \subseteq F$. Suponha que $\{0\} \neq I \neq R$ é um ideal próprio de R. Então existe um lugar $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$.*

Corolário. *Sejam F/K um corpo de funções e $z \in F$ transcendente sobre K. Então z tem pelo menos um zero e um polo; em particular, $\mathbb{P}_F \neq \varnothing$.*

Proposição 1.1.3. *(§1.3, corollary 1.3.4)*

Em um corpo de funções F/K todo elemento não nulo tem só uma quantidade finita de zeros e polos.

Sobre o corpo de funções racionais $K(x)$.

É possível mostrar que existe a seguinte correspondência biunívoca:

$$\mathbb{P}_{K(x)/K} \longleftrightarrow \{\text{polinômios irredutíveis de } K[x]\} \cup \{1/x\},$$

onde o lugar $P_{p(x)}$ é associado ao polinômio $p(x)$ e o lugar P_∞ é associado a $1/x$. O grau do lugar $P_{p(x)}$ coincide com o grau do polinômio $p(x)$ e o lugar P_∞ (denominado lugar no infinito) é racional, aliás, um parâmetro local para $P_{p(x)}$ é $p(x)$ e um para P_∞ é $1/x$. A função valoração v_{P_∞} está dada por $v_{P_\infty}(f(x)/g(x)) = \text{grau}(g(x)) - \text{grau}(f(x))$ sendo $z = f(x)/g(x)$ um elemento de $K(x)$.

No caso em que K é algebricamente fechado, os polinômios irredutíveis em $K[x]$ são da forma $x - \alpha$ onde $\alpha \in K$, assim, como foi afirmado atrás, todos os lugares de $K(x)$ são racionais, neste caso, para simplificar a notação, entenderemos que o lugar P_α está associado ao polinômio $p(x) = x - \alpha$.

Demonstrações para as afirmações acima podem ser encontradas em §1.2 da referência principal desta seção.

1.1.3 Divisores

O grupo de *divisores de* F/K é definido como o grupo abeliano livre que é gerado pelos lugares de F/K e é denotado por $(\text{Div}(F/K), +)$, de forma que se $D \in \text{Div}(F/K)$ então

$$D = \sum_{P \in \mathbb{P}_F} n_P P,$$

com $n_P \in \mathbb{Z}$ quase todos nulos.
A operação " + " do grupo de divisores é definida da seguinte forma:

$$\text{se } D = \sum_{P \in \mathbb{P}_F} n_P P \text{ e } D' = \sum_{P \in \mathbb{P}_F} n'_P P \text{ então } D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P.$$

O *suporte* do divisor D é definido por:

$$\text{Supp}(D) = \{P \in \mathbb{P}_F \mid n_P \neq 0\}.$$

Um divisor da forma $D = P$ onde $P \in \mathbb{P}_F$ é chamado de *divisor primo*.

Seja $D \in \mathrm{Div}(F/K)$ com $D = \sum_{P \in \mathbb{P}_F} n_P P$.

Se $Q \in \mathbb{P}_F$, definimos $v_Q(D) := n_Q$, assim, $\mathrm{Supp}(D) = \{P \in \mathbb{P}_F | v_P(D) \neq 0\}$ e podemos expressar D como a soma finita:

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

Se $D_1, D_2 \in \mathrm{Div}(F/K)$, dizemos que $D_1 \leqslant D_2$ se e só se $v_P(D_1) \leqslant v_P(D_2)$ para todo $P \in \mathbb{P}_F$.

Se $D \geqslant 0$, dizemos que D é um *divisor efetivo*.

O *grau* do divisor D é definido por:

$$\mathrm{grau}(D) := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \mathrm{grau}(P).$$

Observação 1.1.4. A função grau : $\mathrm{Div}(F/K) \longrightarrow \mathbb{Z}$ é um homomorfismo de grupos.

Como vimos atrás, qualquer elemento não nulo de F tem uma quantidade finita de zeros e polos, baseados neste resultado vamos definir uns divisores especiais associados a cada elemento x de F.

Definição 1.1.3. Sejam $0 \neq x \in F$, Z o conjunto dos zeros de x e N o conjunto dos polos de x. Definimos os divisores:

$$\begin{aligned} (x)_0 &:= \sum_{P \in Z} v_P(x) P, \\ (x)_\infty &:= \sum_{P \in N} (-v_P(x)) P, \\ (x) &:= (x)_0 - (x)_\infty. \end{aligned}$$

$(x)_0$ é chamado de *divisor dos zeros* de x, $(x)_\infty$ é chamado de *divisor dos polos* de x e (x) é chamado de *divisor principal* de x.

Consequências imediatas:

- $(x)_0$ e $(x)_\infty$ são divisores efetivos.
- $(x) = \sum_{P \in \mathbb{P}_F} v_P(x) P.$

- $x \in K$ se e somente se $(x) = 0$. Com efeito, se $(x) = 0$ temos que $\sum_{P \in \mathbb{P}_F} v_P(x)P = 0$, assim, $v_P(x) = 0$ para todo $P \in \mathbb{P}_F$. Se $x \notin K$, como assumimos que $K = \tilde{K}$ então x é transcendental sobre K e por tanto deve ter pelo menos um polo e um zero, i.e, devem existir $P, Q \in \mathbb{P}_F$ tais que $v_P(x) > 0$ e $v_Q(x) < 0$, contrariando a afirmação anterior, portanto $x \in K$. A outra implicação é trivial.

O conjunto $\text{Princ}(F/K) := \{(x) \ : \ 0 \neq x \in F\}$ é um subgrupo de $\text{Div}(F/K)$ chamado de grupo dos divisores principais de F/K. O grupo quociente

$$\text{Cl}(F) := \text{Div}(F/K)/\text{Princ}(F/K),$$

é o grupo das classes dos divisores de F/K, assim, dado $D \in \text{Div}(F/K)$ o seu correspondente elemento no grupo $\text{Cl}(F)$ é denotado por $[D]$.

Dizemos que dois divisores D e D' são *equivalentes* e escrevemos $D \sim D'$ se $[D] = [D']$, isto é, se $D = D' + (x)$ para algum $x \in F \backslash \{0\}$.

Observação 1.1.5. $\sim$ é uma relação de equivalência.

Definição 1.1.4. Seja $D \in \text{Div}(F/K)$. Definimos o espaço de Riemman-Roch associado a D por:

$$\mathscr{L}(D) := \{x \in F : (x) + D \geqslant 0\} \cup \{0\}.$$

Consequências imediatas:

Seja $D \in \text{Div}(F/K)$ com $D = \sum v_P(D)P$. Então:

(a) $x \in \mathscr{L}(D)$ se e somente se $v_P(x) \geqslant -v_P(D)$ para todo $P \in \mathbb{P}_F$.

De fato, $x \in \mathscr{L}(D) \Leftrightarrow (x) \geqslant -D \Leftrightarrow \sum v_P(x)P \geqslant \sum(-v_P(D))P \Leftrightarrow v_P(x) \geqslant -v_P(D)$ para todo $P \in \mathbb{P}_F$.

(b) $\mathscr{L}(D) \neq 0$ se e só se existe um divisor $D' \geqslant 0$ tal que $D \sim D'$.

Com efeito, $\mathscr{L}(D) \neq \{0\} \Leftrightarrow \exists x \in F$ tal que $(x) \geqslant -D \Leftrightarrow (x) + D \geqslant 0$. Seja $D' = (x) + D$, então $(x) + D \geqslant 0 \Leftrightarrow D' \geqslant 0$ e $D \sim D'$.

(c) $\mathscr{L}(D)$ é um espaço vetorial sobre K.

Sejam $x, y \in \mathscr{L}(D)$ e $a \in K$. $v_P(x+y) \geqslant \min\{v_P(x), v_P(y)\} \geqslant -v_P(D)$ para todo $P \in \mathbb{P}_F$ (por (a)), portanto, $x+y \in \mathscr{L}(D)$. Por outra parte, $v_P(ax) = v_P(x) \geqslant -v_P(D)$ para todo $P \in \mathbb{P}_F$. logo $ax \in \mathscr{L}(D)$.

Proposição 1.1.4. *(§1.4, Lemmas 1.4.6, 1.4.7, 1.4.8) Sejam A, B divisores de F/K.*

(a) $\mathscr{L}(0) = K$; Se $A < 0$ então $\mathscr{L}(A) = \{0\}$.

(b) Se $A \leqslant B$, então, $\mathscr{L}(A) \subseteq \mathscr{L}(B)$ e $\dim_K(\mathscr{L}(A)/\mathscr{L}(B)) \leqslant grau(B) - grau(A)$.

(c) Se $A \sim B$ então $\mathscr{L}(A) \cong \mathscr{L}(B)$.

Proposição 1.1.5. *(§1.4, Proposition 1.4.9) Para cada divisor $A \in Div(F/K)$, o espaço $\mathscr{L}(A)$ é finito dimensional.*

O número $\ell(A) := \dim_K(\mathscr{L}(A))$ é chamado de *dimensão do divisor A*.

Teorema 1.1.4. *(§1.4, Theorem 1.4.11) Todos os divisores principais tem grau zero. Mais precisamente: Seja $x \in F \backslash K$ e $(x)_0$ e $(x)_\infty$ os divisores dos zeros e os polos de x respectivamente. Então*

$$grau(x)_0 = grau(x)_\infty = [F : K(x)].$$

Corolário. *Sejam A, A' divisores tais que $A \sim A'$, Então, $\ell(A) = \ell(A')$ e $grau(A) = grau(A')$.*

Demonstração. Se $A \sim A'$, então existe $x \in F$ não nulo tal que $A = A' + (x)$, logo, $\text{grau}(A) = \text{grau}(A') + \text{grau}((x))$, mas $\text{grau}((x)) = 0$, assim, $\text{grau}(A) = \text{grau}(A')$; da parte (c) da Proposição 1.1.4 segue que $\ell(A) = \ell(A')$. ■

Corolário. *Se grau$A < 0$, então $\ell(A) = 0$.*

Demonstração. Suponha que $\ell(A) \neq 0$, então existe $A' \geqslant 0$ tal que $A \sim A'$ e pelo corolário anterior $0 \leqslant \text{grau}(A') = \text{grau}(A) < 0$. Absurdo. ■

1.1.4 Gênero

Nesta seção vamos definir um dos invariantes mais importantes de um corpo de funções, este invariante é comumente conhecido como gênero; estudaremos alguns resultados básicos

que envolvem o mesmo.

A seguinte proposição garante a existência de uma cota inferior para $\ell(A)$.

Proposição 1.1.6. *(§1.4, Proposition 1.4.14) Existe uma constante $\gamma \in \mathbb{Z}$ tal que para todo divisor A, tem-se:*

$$grau(A) - \ell(A) \leqslant \gamma.$$

O *gênero* g de F/K é definido por:

$$g := \max\{\text{grau}(A) - \ell(A) + 1 \mid A \in \text{Div}(F/K)\}.$$

Observe que a existência de g está determinada pela proposição anterior, assim, g está bem definido.

Corolário. *O gênero de F/K é um inteiro não negativo.*

Demonstração. É claro que $g \in \mathbb{Z}$. Se $A = 0$, então $\text{grau}(A) - \ell(A) + 1 = \text{grau}(0) - \ell(0) + 1 = 0$ assim, $g \geqslant 0$. ■

Teorema 1.1.5. *(§1.4, Theorem 1.4.17) (Teorema de Riemann). Seja F/K um corpo de funções de gênero g. Então:*

(a) Para todo divisor A, $\ell(A) \geqslant grau(A) + 1 - g$.

(b) Existe um inteiro c, dependendo unicamente de F/K tal que

$$\ell(A) = grau(A) + 1 - g$$

sempre que $grau(A) \geqslant c$.

Exemplo. Vamos mostrar por meio do teorema de Riemann que o corpo das funções racionais $K(x)/K$ tem gênero g igual a zero.

Com efeito, Considere $r > 0$ e o espaço vetorial:

$$\mathscr{L}(r(x)_\infty) = \{z \in K(x) \mid (z) + r(x)_\infty \geqslant 0\}.$$

Observe que $x \in \mathscr{L}(r(x)_\infty)$, pois $(x) + r(x)_\infty = (x)_0 + (r-1)(x)_\infty \geqslant 0$, aliás, para cada i com $1 \leqslant i \leqslant r$, tem-se que $x^i \in \mathscr{L}(r(x)_\infty)$, pois $(x^i) + r(x)_\infty = i(x)_0 + (r-i)(x)_\infty \geqslant 0$. Como $1 \in \mathscr{L}(r(x)_\infty)$, temos que $1, x, \ldots, x^r$ são elementos de $\mathscr{L}(r(x)_\infty)$ linearmente independentes, de onde, $r + 1 \leqslant \ell(r(x)_\infty)$. Por outra parte, pelo teorema de Riemann, para r suficientemente grande temos que:

$$\ell(r(x)_\infty) = \text{grau}(r(x)_\infty) + 1 - g = r \cdot \text{grau}((x)_\infty) + 1 - g,$$

como $(x)_\infty = P_\infty$ em $K(x)$ e grau$(P_\infty) = 1$, temos que:

$$\ell(r(x)_\infty) = r + 1 - g,$$

para $r >> 0$. Segue que $g \leqslant 0$, portanto, $g = 0$. □

Seja $A \in \mathrm{Div}(F/K)$. O inteiro

$$i(A) = \ell(A) - \mathrm{grau}(A) + g - 1$$

é chamado de *índice de especialidade* de A.

Segue do teorema de Riemann que o índice de especialidade é não negativo e será nulo se grau(A) é suficientemente grande.

1.1.5 Adeles

Um *adele de* F/K é um mapa $\alpha : \mathbb{P}_F \longrightarrow F$ tal que $P \longmapsto \alpha_P$, onde $\alpha_P \in \mathcal{O}_P$ para quase todo $P \in \mathbb{P}_F$.

O conjunto

$$\mathcal{A}_F = \{\alpha \mid \alpha \text{ é um adele de } F/K\},$$

é chamado o *espaço dos adeles* de F/K.

A definição anterior implica que podemos visualizar um adele como um elemento de $\prod_{P \in \mathbb{P}_F} F$, assim, denotamos o adele α por $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ ou simplesmente por $\alpha = (\alpha_P)$. Com isso, definindo a soma e produto por escalar sobre K em $\mathcal{A}_F$ por:

$$\alpha + \beta := (\alpha_P + \beta_P)_{P \in \mathbb{P}_F} \text{ para todo } \alpha, \beta \in \mathcal{A}_F,$$

$$a\alpha := (a\alpha_P)_{P \in \mathbb{P}_F} \text{ para todo } \alpha \in \mathcal{A}_F \text{ e } a \in K,$$

obtemos que $\mathcal{A}_F$ é um espaço vetorial sobre K.

O *adele principal* de um elemento $x \in F$ é o adele cujas componentes são todas iguais a x, isso permite considerar o mergulho $F \hookrightarrow \mathcal{A}_F$ naturalmente definido, isto é, cada elemento é enviado a seu adele principal, assim, podemos estender a noção de valoração ao conjunto $\mathcal{A}_F$ como segue: $v_P(\alpha) := v_P(\alpha_P)$ sendo α_P a P-ésima componente do adele α.
A noção de zero e polo de um elemento também é estendida aos adeles naturalmente: o lugar P será chamado de *zero de* α se $v_P(\alpha) > 0$ e será chamado de *polo de* α se $v_P(\alpha) < 0$.

Observação 1.1.6.

- Pela definição de adele sabemos que $\alpha_P \in \mathcal{O}_P$ para quase todo $P \in \mathbb{P}_F$, assim, segue da definição de adele principal que $x \in \mathcal{O}_P$ para quase todo $P \in \mathbb{P}_F$, o que significa que $v_P(x) \geqslant 0$ para todo P exceto uma quantidade finita de lugares, fato que é consistente com o fato de que x tem uma quantidade finita de polos.
- Segue da definição que $v_P(\alpha) \geqslant 0$ para quase todo $P \in \mathbb{P}_F$.

Seja $A \in \mathrm{Div}(F/K)$, definimos o conjunto:

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F \mid v_P(\alpha) \geqslant -v_P(A) \text{ para todo } P \in \mathbb{P}_F\}.$$

Observação 1.1.7. $\mathcal{A}_F(A)$ é um K-subespaço vetorial de $\mathcal{A}_F$.

Teorema 1.1.6. *(§1.5, Theorem 1.5.4) Para todo $A \in Div(F/K)$, o índice de especialidade de A está dado por:*

$$i(A) := \dim_K(\mathcal{A}_F/(\mathcal{A}_F(A) + F))$$

Segue deste teorema e a definição de $i(A)$ que para todo divisor A,

$$\ell(A) = \mathrm{grau}(A) - g + 1 + \dim_K(\mathcal{A}_F/(\mathcal{A}_F(A) + F))$$

1.1.6 Diferenciais de Weil

Uma *diferencial de Weil* de F/K é um mapa K-linear $\omega : \mathcal{A}_F \longrightarrow K$ que é zero sobre $\mathcal{A}_F(A) + F$ para algum divisor A. Definimos o *módulo* das diferenciais de F/K, Ω_F, por:

$$\Omega_F := \{\omega \mid \omega \text{ é uma Weil diferencial de } F/K\}$$

Observação 1.1.8. Ω_F é um K- espaço vetorial definindo as operações da seguinte forma: Se ω_1 é zero sobre $\mathcal{A}_F(A_1) + F$ e ω_2 é zero sobre $\mathcal{A}_F(A_2) + F$, então $\omega_1 + \omega_2$ é zero sobre $\mathcal{A}_F(A_3) + F$ onde $A_3 \leqslant A_1$ e $A_3 \leqslant A_2$ e $a\omega_1$ é zero sobre $\mathcal{A}_F(A_1) + F$ para todo $a \in K$.

Seja $A \in \mathrm{Div}(F/K)$, definimos o conjunto $\Omega_F(A)$ por:

$$\Omega_F(A) := \{\omega \in \Omega_F \mid \omega \text{ é zero sobre } \mathcal{A}_F(A) + F\}.$$

Observação 1.1.9. $\Omega_F(A)$ é um K-subespaço vetorial de Ω_F.

Lema 1.1.2. *Para todo divisor A têm-se que* $\dim_K \Omega_F(A) = i(A)$.

Demonstração. Observe que pela sua definição, $\Omega_F(A)$ está naturalmente identificado com o espaço dual de $V := \mathcal{A}_F/(\mathcal{A}_F(A) + F)$ mediante o mapa $\psi : \Omega_F(A) \longrightarrow V^*$ dado por $(\psi(\omega))([\alpha]) = \omega(\alpha)$. Claramente ψ está bem definida e é K-linear.

$$\begin{aligned}
\ker(\psi) &= \{\omega \in \Omega_F(A) \ : \ \psi(\omega) = 0_{V^*}\} \\
&= \{\omega \in \Omega_F(A) \ : \ \psi(\omega)([\alpha]) = 0 \ \forall \alpha \in \mathcal{A}_F\} \\
&= \{\omega \in \Omega_F(A) \ : \ \omega(\alpha) = 0 \ \forall \alpha \in \mathcal{A}_F\} \\
&= 0_{\Omega_F}.
\end{aligned}$$

Por outra parte, se $f \in V^*$, então $f([\alpha]) = f([0]) = 0$ para todo $\alpha \in \mathcal{A}_F(A) + F$. Para mostrar a sobrejetividade de ψ, dada $f \in V^*$, construímos $\omega \in \Omega_F$ tal que $\omega(\alpha) = f([\alpha])$ para todo $\alpha \in \mathcal{A}_F$; segue da linearidade de f que ω é K-linear e da primeira afirmação no parágrafo segue que $\omega(\alpha) = 0$ para todo $\alpha \in \mathcal{A}_F(A) + F$, logo, $\omega \in \Omega_F(A)$.
logo, $V^* \cong \Omega_F(A)$, e sabemos que (em dimensão finita) $\dim_K(V^*) = \dim_K(V)$, assim, como $\dim(V) = i(A)$ (Teorema 1.1.6) concluímos o desejado. ■

A primeira consequência do lema acima é que $\Omega_F \neq \{0\}$. De fato, se A é um divisor de grau menor ou igual que -2 (que sempre é possível achar, por exemplo, $A = -2P$) temos que

$$\dim_K(\Omega_F(A)) = i(A) = \ell(A) - \text{grau}(A) + g - 1.$$

Como $\text{grau}(A) < 0$, então, $\ell(A) = 0$, assim,

$$\dim_K(\Omega_F(A)) \geqslant -(-2) + g - 1 = g + 1,$$

e como g é não negativo, concluímos que $\dim_K(\Omega_F(A)) \geqslant 1$. Portanto, $\Omega_F \neq \{0\}$.

Sejam $x \in F$ e $\omega \in \Omega_F$, definimos $x\omega : \mathcal{A}_F \longrightarrow K$ por $x\omega(\alpha) := \omega(x\alpha)$.

Lembremos que o produto $x\alpha$ deve se considerar como o produto do adele principal x com o adele α.

Observação 1.1.10. $x\omega \in \Omega_F$ e portanto Ω_F é um F-espaço vetorial.

Proposição 1.1.7. *(§1.5, Proposition 1.5.9) Ω_F é unidimensional como espaço vetorial sobre F.*

1.1.7 Divisores canônicos

Agora, o objetivo principal é tentar associar a cada $\omega \in \Omega_F$ um divisor; dessa tentativa vai surgir a definição de um tipo especial de divisores denominados *divisores canônicos*. Eles

serão especiais porque estarão completamente caracterizados por somente duas propriedades.

Seja $\omega \in \Omega_F$ fixo, definimos o conjunto $M(\omega)$ como segue:

$$M(\omega) := \{A \in \mathrm{Div}(F/K) \mid \omega(\mathcal{A}_F(A) + F) = 0\}.$$

Lema 1.1.3. *(§1.5, Lemma 1.5.10) Seja $0 \neq \omega \in \Omega_F$. Existe um divisor $W \in M(\omega)$ unicamente determinado tal que $A \leqslant W$ para todo $A \in M(\omega)$.*

Definição 1.1.5.

(a) O divisor (ω) de uma diferencial não nula $\omega \in \Omega_F$ é o divisor de F/K unicamente determinado que satisfaz:

1. $\omega(\mathcal{A}_F((\omega)) + F) = 0$,
2. Se $\omega(\mathcal{A}_F(A) + F) = 0$, então $A \leqslant (\omega)$.

(b) Para $0 \neq \omega \in \Omega_F$ e $P \in \mathbb{P}_F$, definimos $v_P(\omega) := v_P((\omega))$.

(c) Um lugar P é chamado de *zero de* ω se $v_P(\omega) > 0$ e é chamado de *polo de* ω se $v_P(\omega) < 0$. Por outra parte, se diz que ω é *regular em* P se $v_P(\omega) \geqslant 0$, e se isso acontece para todo $P \in \mathbb{P}_F$ diremos simplesmente que ω é regular.

(d) Um divisor $W \in \mathrm{Div}(F/K)$ é chamado de *divisor canônico* de F/K se $W = (\omega)$ para algum $\omega \in \Omega_F$.

Com a definição anterior queda completamente estabelecida a relação entre os elementos de Ω_F e os divisores, dada pelos divisores canônicos.

Lembremos que $\Omega_F(A) = \{\omega \in \Omega_F \mid \omega \text{ é zero sobre } \mathcal{A}_F(A) + F\}$, vamos redefinir este conjunto usando a linguagem dada na ultima definição: Fixando A, observamos que os elementos não nulos desse conjunto cumprem a condição 2 de um divisor canônico, assim, essa definição é equivalente à seguinte:

$$\Omega_F(A) := \{\omega \in \Omega_F \mid \ \omega = 0 \text{ ou } (\omega) \geqslant A\}.$$

Em particular, se $\omega \neq 0$ e $A = 0$, temos que

$$\Omega_F(0) = \{\omega \in \Omega_F \mid (\omega) \geqslant 0\} = \{\omega \in \Omega_F \mid v_P(\omega) \geqslant 0 \text{ para todo } P \in \mathbb{P}_F\}.$$

Assim, a parte (c) da definição anterior nos permite definir este conjunto assim:

$$\Omega_F(0) := \{\omega \in \Omega_F \mid \omega \text{ é regular }\}.$$

Proposição 1.1.8. *Seja F/K um corpo de funções de gênero g, então,*

$$\dim_K \Omega_F(0) = g.$$

Demonstração. Sabemos que $\dim_K \Omega_F(A) = i(A)$, assim,

$$\dim_K \Omega_F(0) = i(0) = \ell(0) - \text{grau}(0) + g - 1 = 1 + g - 1 = g.$$

■

Este resultado é muito útil, vamos fazer uso dele no futuro para calcular a base das diferenciais regulares de certos corpos de funções.

Proposição 1.1.9. *(§1.5, Proposition 1.5.13)*

(a) Para $0 \neq x \in F$ e $0 \neq \omega \in \Omega_F$ temos que $(x\omega) = (x) + (\omega)$.

(b) Quaisquer dois divisores canônicos de F/K são equivalentes.

Como consequência da proposição temos que os divisores canônicos formam uma classe de equivalência em $\text{Cl}(F)$.

Proposição 1.1.10. *Seja W um divisor canônico. Então:*

$$\begin{cases} grau(W) &= 2g - 2, \\ \ell(W) &\geqslant g. \end{cases}$$

A demonstração dessa proposição é uma consequência imediata do teorema de Riemann-Roch, que diz que se W é um divisor canônico, então para todo divisor A tem-se que:

$$\ell(A) = \text{grau}(A) + 1 - g + \ell(W - A).$$

As propriedades dadas na proposição para os divisores canônicas são as que foram mencionadas no inicio da seção como as propriedades que caracterizam completamente aos divisores canônicos.

1.1.8 Índice de ramificação

Um corpo de funções algébricas F'/K' é denominado *extensão algébrica* de F/K, se $F' \supseteq F$ é uma extensão de corpos algébrica e $K' \supseteq K$. A extensão algébrica F'/K' de F/K é dita *finita* se $[F' : F] < \infty$.

Considere a extensão algébrica F'/K' de F/K. Dizemos que o lugar $P' \in \mathbb{P}_{F'}$ mora sobre (ou é uma extensão de) $P \in \mathbb{P}_F$, se $P \subseteq P'$, neste caso, escrevemos $P'|P$.

Proposição 1.1.11. *(§3.1, Proposition 3.1.4) Seja F'/K' uma extensão algébrica de F/K. Suponha que $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$, sejam $\mathcal{O}_P \subseteq F$ e $\mathcal{O}_{F'} \subseteq F'$ os respectivos aneis de valoração de F/K e F'/K' e sejam v_P e $v_{P'}$ suas respectivas funções de valoração, então, as seguintes afirmações são equivalentes:*

1. *$P'|P$.*
2. *$\mathcal{O}_P \subseteq \mathcal{O}'_P$.*
3. *Existe um inteiro $e \geqslant 1$ tal que $v_{P'}(x) = e \cdot v_P(x)$ para todo $x \in F$.*

Definição 1.1.6. Seja F'/K' uma extensão algébrica de F/K e $P' \in \mathbb{P}_{F'}$ uma extensão de $P \in \mathbb{P}_F$.

(a) O inteiro $e(P'|P) := e$ tal que $v_{P'}(x) = e \cdot v_P(x)$ para todo $x \in F$ é denominado *índice de ramificação* de P' sobre P. Dizemos que $P'|P$ é *ramificado* se $e(P'|P) > 1$ e que $P'|P$ é *não ramificado* se $e(P'|P) = 1$.

(b) $f(P'|P) := [F'_{P'} : F_P]$ é denominado *o grau relativo* de P' sobre P.

Observação 1.1.11. $f(P'|P)$ pode ser finito ou infinito entanto $e(P'|P)$ é sempre um número natural.

Proposição 1.1.12. *(§3.1, Proposition 3.1.6) Seja F'/K' uma extensão algébrica de F/K e $P' \in \mathbb{P}_{F'}$ uma extensão de $P \in \mathbb{P}_F$. Então,*

(a) $f(P'|P) < \infty$ se e só se $[F' : F] < \infty$.

(b) Se F''/K'' uma extensão algébrica de F'/K' e $P'' \in \mathbb{P}_{F''}$ uma extensão de P', então,

$$\begin{cases} e(P''|P) &= e(P''|P')e(P'|P), \\ f(P''|P) &= f(P''|P')f(P'|P). \end{cases}$$

Proposição 1.1.13. *(§3.1, Proposition 3.1.7) Seja F'/K' uma extensão algébrica de F/K.*

(a) Para cada $P' \in \mathbb{P}_{F'}$ existe exatamente um lugar $P \in \mathbb{P}_F$ tal que $P'|P$ dado por

$$P = P' \cap F.$$

(b) Reciprocamente, cada $P \in \mathbb{P}_F$ tem pelo menos uma, mas só uma quantidade finita de extensões $P' \in \mathbb{P}_{F'}$.

Teorema 1.1.7. (Igualdade fundamental) *(§3.1, Theorem 3.1.11)*
Seja F'/K' uma extensão finita de F/K, seja P um lugar de F/K e $P_1, \ldots, P_m$ todos os lugares de F'/K' morando sobre P. Sejam $e_i := e(P_i|P)$ e $f_i := f(P_i|P)$ para cada i. Então

$$\sum_{i=1}^{m} e_i f_i = [F' : F].$$

1.1.9 Extensões inseparáveis

Lembremos que um polinômio mônico $f(x) \in K[x]$ de grau d é dito separável se existir uma extensão $L \supseteq K$ tal que $f(x) = \prod_{i=1}^{d}(x - \alpha_i)$ com $\alpha_i \neq \alpha_j$ para todo $i \neq j$. Agora, se L é uma extensão de K algébrica, então $\alpha \in L$ será chamado de separável sobre K se o seu polinômio mínimo (em $K[x]$, obviamente) é separável. Finalmente, dizemos que a extensão L (algébrica) é uma extensão separável se todos seus elementos são separáveis sobre K.

Um corpo K é dito *perfeito* se todas suas extensões algébricas são separáveis. Se K tem característica $p > 0$, então K é perfeito se e somente se cada $a \in K$ pode-se escrever da seguinte forma:

$$a = b^p$$

para algum $b \in K$.

Se K é um corpo de característica $p > 0$ e L/K é uma extensão algébrica, um elemento $x \in L$ será chamado *puramente inseparável* sobre K se $x^{p^r} \in K$ para algum $r \geqslant 0$; nesse caso, o polinômio mínimo de x sobre K tem a forma:

$$f(X) = X^{p^e} - c,$$

onde $c \in K$ e $e \leqslant r$.
A extensão L é *puramente inseparável* se todos seus elementos são puramente inseparáveis sobre K.

Definição 1.1.7. Um elemento $x \in F$ é chamado *variável separante* (ou elemento separador) de F/K se $F/K(x)$ é uma extensão separável; neste caso F/K é dita *separavelmente gerada.*

O seguinte teorema mostra que sob a condição de ser K perfeito, F/K sempre será separavelmente gerada.

Teorema 1.1.8. *(§3.10, Proposition 3.10.2)*

Seja K um corpo perfeito com característica $p > 0$ e seja F/K o corpo de funções algébricas onde K é o corpo das constantes.

(a) Se $z \in F$ e $p \nmid v_P(z)$ para algum $P \in \mathbb{P}_F$, então z é uma variável separante para F/K.

(b) Existem $x, y \in F$ tais que $F = K(x, y)$.

(c) Para cada $n \geqslant 1$, o conjunto:

$$F^{p^n} := \{z^{p^n} \ : \ z \in F\}$$

é um subcorpo de F com as seguintes propriedades:

1. *$K \subseteq F^{p^n} \subseteq F$ e F/F^{p^n} é puramente inseparável com $[F : F^{p^n}] = p^n$.*
2. *O mapa de Frobenius $\varphi_n : F \longrightarrow F$, definido por $\varphi_n(z) = z^{p^n}$ é um isomorfismo de F sobre F^{p^n}, assim, o corpo de funções F^{p^n}/K tem o mesmo gênero que F/K.*
3. *Suponha que $K \subseteq F_0 \subseteq F$ e F_0 é puramente inseparável de grau p^n. Então, $F_0 = F^{p^n}$.*

(d) Um elemento $z \in F$ é uma variável separante para F/K se e só se $z \notin F^p$.

1.2 Curvas Algébricas

Ao longo desta seção vamos assumir que K é um corpo algebricamente fechado. Aqui tomamos como referência o livro (FULTON, 2008).

1.2.1 Espaço afim e espaço projetivo

Se definimos

$$\mathbb{A}^n(K) := K \times \cdots \times K$$

onde o produto acima é feito n vezes, dizemos que $\mathbb{A}^n(K)$ é o *n-espaço afim* sobre K, em particular, se $n = 2$, $\mathbb{A}^2(K)$ é chamado o plano afim.

Se $F \in K[X_1, \ldots, X_n]$ e $P = (a_1, \ldots, a_n) \in \mathbb{A}^n(K)$, diremos que P é um *zero* de F se $F(P) = 0$. O conjunto dos zeros de F (assumindo F não constante) é denominado a *hiper-superfície* definida por F e é denotado por $V(F)$. Uma hiper-superfície em $\mathbb{A}^2$ é chamada de curva plana afim.

Seja $S \subset K[X_1, \ldots, X_n]$, denotamos por $V(S)$ ao conjunto:

$$\{P \in \mathbb{A}^n \ : \ F(P) = 0 \text{ para todo } F \in S\}.$$

$X \subset \mathbb{A}^n$ é denominado *conjunto algébrico afim* se $X = V(S)$ para algum S.

O conjunto

$$I(X) = \{F \in K[X_1, \ldots, X_n] \ : \ F(a_1, \ldots, a_n) = 0 \text{ para todo } (a_1, \ldots, a_n) \in X\}$$

é um ideal chamado o ideal de X.

Um conjunto algébrico $V \subset \mathbb{A}^n$ é *redutível* se $V = V_1 \cup V_2$ onde V_1 e V_2 são conjuntos algébricos em $\mathbb{A}^n$ diferentes de V. Se V não é redutível, será chamado de *irredutível*.

Proposição 1.2.1. *(§1.5, Proposition 1). Um conjunto algébrico V é irredutível se e somente se $I(V)$ é primo.*

Dizemos que V é uma *variedade afim* se V é um conjunto algébrico irredutível.

Se $V \subset \mathbb{A}^n$ é uma variedade não vazia então $K[X_1, ..., X_n]/I(V)$ é um domínio; chamaremos esse domínio de *anel de coordenadas* de V e denotaremos ele por $\Gamma(V)$.

O corpo quociente de $\Gamma(V)$ é denominado *corpo das funções racionais* sobre V e é denotado por $K(V)$; os elementos de $K(V)$ são denominados *funções racionais* sobre V.

Seja $P \in V$. O conjunto das funções racionais sobre V que estão definidas em P é denominado *anel local* de V em P e é denotado por $\mathcal{O}_P(V)$; como seu nome indica, $\mathcal{O}_P(V)$ é um anel satisfazendo:

$$K \subseteq \Gamma(V) \subseteq \mathcal{O}_P(V) \subseteq K(V).$$

O conjunto

$$\mathfrak{m}_P(V) := \{f \in \mathcal{O}_P(V) \mid f(P) = 0\},$$

é um ideal maximal de $\mathcal{O}_P(V)$. Aqui $f(P)$ é definido como segue: como $\mathcal{O}_P(V) \subseteq K(V)$, existem $a, b \in \Gamma(V)$ tais que $f = a/b$ com $b(P) \neq 0$, então $f(P) = a(P)/b(P)$

Observação 1.2.1. De acordo com o estudado na seção anterior, podemos ver que para cada $P \in V$, $\mathcal{O}_P(V)$ é um anel de valorização discreta de $K(V)$ cujo lugar associado é o ideal $\mathfrak{m}_P(V)$, assim, do Teorema 1.1.1 segue que podemos encontrar um parâmetro local para $\mathfrak{m}_P(V)$ e portanto, associar a valoração discreta $ord_P : K(V) \longrightarrow \mathbb{Z} \cup \{\infty\}$ dada por:

$$ord_P(f) := v_{\mathfrak{m}_P(V)}(f).$$

Agora estudaremos o espaço projetivo. Primeiro, vamos definir os conceitos de homogeneização e deshomogeneização de um polinômio.

Seja $F \in K[X_1, \ldots, X_{n+1}]$ uma forma. Definimos $F_* \in K[X_1, \ldots, X_n]$ como sendo:

$$F_* = F(X_1, X_2, \ldots, X_n, 1).$$

Reciprocamente, dado um polinômio $f \in K[X_1, \ldots, X_n]$ de grau d, se escrevemos

$$f = f_0 + f_1 + \cdots + f_d,$$

onde f_i é uma forma de grau i, então, definimos $f^* \in K[X_1, \ldots, X_{n+1}]$ como:

$$f^* = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + \cdots + X_{n+1} f_{d-1} + f_d.$$

O primeiro processo é conhecido como *deshomogeneização* com respeito a X_{n+1} e o segundo *homogeneização* com respeito a X_{n+1}.

O *n-espaço projetivo* sobre K, denotado por $\mathbb{P}^n(K)$ se define como o conjunto de todas as retas que passam por $(0, 0, ..., 0)$ em $\mathbb{A}^{n+1}(K)$. Formalmente, se $(x) = (x_1, \ldots, x_{n+1})$ e $(y) = (y_1, \ldots, y_{n+1})$ são elementos de $\mathbb{A}^{n+1}$, definindo a relação:

$$(x) \sim (y) \;\Leftrightarrow\; \text{existe } 0 \neq \lambda \in K \text{ tal que } y_i = \lambda x_i \;\; i = 1, \ldots, n+1.$$

podemos identificar o espaço projetivo $\mathbb{P}^n$ com o conjunto de equivalências dos pontos de $\mathbb{A}^{n+1} \backslash (0, \ldots, 0)$.
Os elementos de $\mathbb{P}^n$ serão chamados pontos. Se um ponto $P \in \mathbb{P}^n$ está determinado por algum $(x_1, \ldots, x_{n+1}) \in \mathbb{A}^{n+1}$, diremos que $(x_1, \ldots, x_{n+1})$ são *coordenadas homogêneas* para P e escrevemos $P = [x_1 : \cdots : x_{n+1}]$.
Seja

$$U_i := \{[x_1, \ldots, x_{n+1}] \in \mathbb{P}^n \;:\; x_i \neq 0\};$$

cada $P \in U_i$ pode ser escrito unicamente da forma:

$$P = [x_1 : ... : x_{i-1} : 1 : x_{i+1} : ... : x_{n+1}];$$

as coordenadas $(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_{n+1})$ são denominadas *coordenadas não homogêneas* para P com respeito a U_i.
Considere a função: $\varphi_i : \mathbb{A}^n \longrightarrow U_i$ tal que

$$(a_1, \ldots, a_n) \longmapsto [a_1 : ... : a_{i-1} : 1 : a_{i+1} : ... : a_{n+1}]$$

então φ_i dá uma correspondência 1-1 entre os pontos de $\mathbb{A}^n$ e os pontos de U_i, assim, como $\mathbb{P}^n = \bigcup_{i=1}^{n+1} U_i$, temos que $\mathbb{P}^n$ é coberto por $n+1$ conjuntos que são semelhantes ao n-espaço afim.

O conjunto

$$H_\infty := \mathbb{P}^n \backslash U_{n+1} = \{[x_1 : \cdots : x_{n+1}] \mid x_{n+1} = 0\},$$

é denominado o *hiperplano no infinito*.

Um ponto $P \in \mathbb{P}^n$ é dito *zero* de um polinômio $F \in K[X_1, \ldots, X_{n+1}]$ se $F(x_1, \ldots, x_{n+1}) = 0$ para cada escolha de coordenadas homogêneas $(x_1, \ldots, x_{n+1})$ para P, neste caso escrevemos $F(P) = 0$. Se F é uma forma e F se anula em alguma representação de P, então F se anula em todas as representações de P.

Se $S \subset K[X_1, \ldots, X_n]$, então, análogo ao caso afim, temos que:

$$V(S) = \{P \in \mathbb{P}^n \mid F(P) = 0 \text{ para todo } F \in S\}.$$

O conjunto dos zeros de um número finito de formas (ou seja $V(S)$ onde os elementos de S são formas) é denominado *conjunto algébrico projetivo*.

Para todo conjunto $X \subset \mathbb{P}^n$, temos que:

$$I(X) = \{F \in K[X_1, \ldots, X_n] \ : \ F(P) = 0 \text{ para todo } P \in X\}$$

é um ideal chamado o ideal de X.

Um ideal $I \subset K[X_1, \ldots, X_{n+1}]$ é denominado *homogêneo* se para cada $F = \sum_{i=0}^{m} F_i$, onde F_i é uma forma de grau i, também se tem que $F_i \in I$.

Um conjunto algébrico $V \subset \mathbb{P}^n$ é *irredutível* se não é a união de dois conjuntos algébricos menores, neste caso, V é denominado *variedade projetiva*.

Seja V uma variedade projetiva não vazia em $\mathbb{P}^n$. O anel $K[X_1, ..., X_n]/I(V)$ é um domínio denominado *anel de coordenadas homogêneas* de V e é denotado por $\Gamma_h(V)$.

Dado qualquer ideal homogêneo $I \subset K[X_1, \ldots, X_{n+1}]$, um elemento f de $\Gamma = K[X_1, \ldots, X_{n+1}]/I$ é denominado *forma* de grau d se existir uma forma F de grau d em $K[X_1, \cdots, X_{n+1}]$ cujo resíduo seja F.

O corpo quociente de $\Gamma_h(V)$ é denominado *corpo de funções homogêneas* de V e é denotado por $K_h(V)$. Em contraste com o caso afim, com excepção das constantes, nenhum elemento de $\Gamma_h(V)$ determina funções sobre V, desta forma, a maioria dos elementos de $K_h(V)$ não

podem ser tratados como funções. Porém, se f e g são formas em $\Gamma_h(V)$ do mesmo grau, então, f/g define uma função onde g não é zero.

O conjunto

$$K(V) = \{z \in K_h(V) \mid z = f/g \text{ para algumas formas } f, g \in \Gamma_h(V) \text{ do mesmo grau}\}$$

é denominado *corpo de funções* de V. $K(V)$ é um subcorpo de $K_h(V)$ que contém K, seus elementos são denominados *funções racionais* sobre V.

Sejam $P \in V$ e $z \in K(V)$. Diremos que z está definida em P se z pode ser escrita como $z = f/g$ onde f e g são formas do mesmo grau e $g(P) \neq 0$.

Análogo ao caso afim definimos o anel

$$\mathcal{O}_P(V) = \{z \in K(V) \mid z \text{ está definida em } P\};$$

$\mathcal{O}_P(V)$ é um subanel de $K(V)$ que é local, o seu ideal maximal é:

$$\mathfrak{m}_P(V) = \{z \in \mathcal{O}_P(V) \mid z = f/g \text{ e } f(P) = 0\}.$$

Observação 1.2.2. Todos os conceitos atrás podem ser generalizados a multi-espaços ou espaços mistos $\mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{A}^m$. Neste caso, definindo $\mathbb{A}^0$ como um ponto, então as variedades afim e projetivas são casos especiais de variedades em $\mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{A}^m$.

1.2.2 Curvas planas afins e projetivas

Definimos a seguinte relação sobre $K[X, Y]$:

$$F \sim G \;\Leftrightarrow\; F = \lambda G \text{ para algum } \lambda \in K.$$

A relação $\sim$ é de equivalência.

Uma *curva plana afim* é uma classe de equivalência de polinômios não constantes sob a relação $\sim$. O *grau* de uma curva plana afim, é o grau de um polinômio definindo a curva.

Se F é uma curva e $P = (a, b) \in F$, diremos que P é um ponto *simples* de F se $F_X(P) \neq 0$ ou $F_Y(P) \neq 0$, e, neste caso, a curva $F_X(P)(X - a) + F_Y(P)(Y - b) = 0$ é denominada *linha tangente* a F em P. Um ponto que não é simples é chamado *múltiplo* ou *singular*. Uma curva com só pontos simples é chamada de *curva não singular*.

Se $P = (0, 0)$, escrevendo

$$F = F_m + F_{m+1} + \cdots + F_n,$$

onde cada F_i é uma forma em $K[X, Y]$ de grau i, definimos a *multiplicidade* de F em P, como sendo m, e denotamos ela por $m_P(F)$.
Se escrevemos:

$$F_m = \prod L_i^{r_i}$$

(onde cada L_i é uma curva de grau um), dizemos que L_i é uma *reta tangente* a F em P e que r_i é a multiplicidade da tangente. Se $r_i = 1$ diremos que L_i é uma tangente *simples*.
Se $P = (a, b) \neq (0, 0)$, então definimos a multiplicidade de F em P assim:

$$m_P(F) := m_{(0,0)}(F(X + a, Y + b)).$$

Com isso, as demais definições podem ser estendidas naturalmente para o ponto P.

Se F, G são duas formas em $K[X, Y, Z]$, definimos a seguinte relação de equivalência entre F e G:

$$F \sim G \;\Leftrightarrow\; G = \lambda F \;\text{ para algum }\; \lambda \in K,$$

e definimos uma curva plana projetiva como sendo uma classe de equivalência de formas (sob a relação $\sim$).
O *grau* de uma curva projetiva plana é o grau de uma forma definindo a curva.

Se F é uma curva projetiva plana e $P \in U_i$ ($i = 1, 2$ ou 3), podemos deshomogeneizar F com respeito a X_i e definir a *multiplicidade* de F em P como segue:

$$m_P(F) := m_{P_*}(F_*)$$

esta definição é independente da eleição de U_i, ou seja, da variável sobre a que se faz o processo de deshomogeneização. Igual que no espaço afim, P será chamado simples se $m_P(F) = 1$ e múltiplo (ou singular) se não é simples.

Se F e G são duas curvas planas projetivas e $P \in \mathbb{P}^2$, definimos o *número de interseção* de F e G

$$I(P, F \cap G) := \dim_K(\mathcal{O}_P(\mathbb{P}^2)/(F_*, G_*)),$$

e dizemos que a reta L é *tangente* à curva F em P se $I(P, F \cap L) > m_P(F)$, finalmente, dizemos que P é um *ponto múltiplo ordinário* de F se F tem $m_P(F)$ distintas tangentes em P.

A seguinte proposição dá um critério para encontrar os pontos múltiplos de uma curva.

Proposição 1.2.2. *Seja F uma curva projetiva plana. $P \in \mathbb{P}^2$ é um ponto múltiplo de F se e somente se*

$$F(P) = F_X(P) = F_Y(P) = F_Z(P) = 0.$$

Demonstração. Escrevemos

$$F = \sum_{i=0}^{m} F_i(X,Y)Z^{m-i},$$

onde F_i é uma forma que grau i. Suponha que $P = [a : b : c]$ é um ponto múltiplo de F, então, $m_P(F) = m_P(F_*) > 1$. Como sabemos que $m_{(a,b)}(G) = m_{(0,0)}(G(X+a, Y+b))$ para toda curva plana afim G, então podemos supor $P = [0 : 0 : 1]$.
Por hipótese temos que $F_* = \sum_{i=0}^{m} F_i(X,Y)$ e $m_{(0,0)}(F_*) > 1$, assim

$$(F_*)_X(0,0) = (F_*)_Y(0,0) = F_*(0,0) = 0.$$

Como $F_* = F(X,Y,1)$ concluímos que $F_X(P) = F_Y(P) = F(P) = 0$. Por outra parte, sabemos que:

$$mF = XF_X + YF_Y + ZF_Z$$

logo,

$$mF(P) = 0 \cdot F_X(P) + 0 \cdot F_Y(P) + F_Z(P),$$

isto é, $F_Z(P) = 0$. Reciprocamente, se $F(P) = F_X(P) = F_Y(P) = F_Z(P) = 0$, supondo $P = [0 : 0 : 1]$, temos:

$$(F_X)_*(0,0) = (F_Y)_*(0,0) = F_*(0,0) = 0,$$

o que significa que $(0,0)$ é um ponto múltiplo de F_*, assim, $m_P(F) = m_P(F_*) > 1$. ■

Exemplos: Vamos determinar os pontos múltiplos das seguintes curvas planas usando o critério na proposição anterior:

1. Considere a curva representada pela forma $F(X,Y,Z) = X^n + Y^n - Z^n$. Suponha que $\mathrm{char}K = p$ e que $p \nmid n$, então:

   $F_X = nX^{n-1}$,
   $F_Y = nY^{n-1}$,
   $F_Z = nZ^{n-1}$;

assim, se $P \in \mathbb{P}^2$ tem coordenadas homogêneas (x, y, z), temos que $F_X(P) = 0$ se e só se $x = 0$, $F_Y(P) = 0$ se e só se $y = 0$ e $F_Z(P) = 0$ se e só se $z = 0$. isso significa que o único ponto satisfazendo $F(P) = F_X(P) = F_Y(P) = F_Z(P) = 0$ é $(x, y, z) = (0, 0, 0)$ e sabemos que a origem não é um ponto do espaço $\mathbb{P}^2$. Concluindo que a curva não tem pontos múltiplos.

2. Considere a curva representada pela forma $H(X, Y, Z) = ZX^n + XY^n + YZ^n$. Suponha que char$K = p$ e que $p \nmid n^2 - n + 1$, então:

$$H_X = Y^n + nX^{n-1}Z,$$
$$H_Y = Z^n + nY^{n-1}X,$$
$$H_Z = X^n + nZ^{n-1}Y;$$

assim, se $P \in \mathbb{P}^2$ tem coordenadas homogêneas (x, y, z), temos o seguinte:

$$H_X(P) = 0 \text{ implica } y^n = -nx^{n-1}z,$$
$$H_Y(P) = 0 \text{ implica } z^n = -ny^{n-1}x,$$
$$H_Z(P) = 0 \text{ implica } x^n = -nz^{n-1}y;$$

de onde temos que $(n^3 + 1)z^n y = 0$, isto é, $z = 0$ ou $y = 0$.

No caso $z = 0$, temos, das equações acima que $x = y = 0$; analogamente, se $y = 0$, temos que $x = z = 0$. O anterior significa que o único ponto satisfazendo $F(P) = F_X(P) = F_Y(P) = F_Z(P) = 0$ é $(x, y, z) = (0, 0, 0)$, assim, a curva não possui pontos múltiplos.

Observação 1.2.3. As curvas nos dois exemplos são bastante conhecidas; a primeira é denominada *curva de Fermat* e a segunda, *curva de Hurwitz*. Desde agora escreveremos $\mathcal{F}_n$, para nos referir à curva de Fermat de grau n e $\mathcal{H}_n$ para nos referir à curva de Hurwitz de grau $n + 1$.

1.2.3 Funções racionais

Seja $X = \mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{A}^m$. A *topologia de Zariski* sobre X é definida como segue: Um conjunto $U \subset X$ é aberto se $X \backslash U$ é um subconjunto algébrico de X.

Qualquer subconjunto de X é dotado com a topologia induzida.

Se V é uma variedade em X, um subconjunto de V é fechado se e só se é algébrico. Observemos que todos os subconjuntos abertos de uma variedade tem interseção não vazia dois a dois, assim, todo subconjunto aberto não vazio de uma variedade V é denso em V.

Seja V um conjunto algébrico irredutível em $\mathbb{P}^{n_1} \times \mathbb{P}^{n_2} \times \cdots \times \mathbb{A}^m$. Qualquer subconjunto aberto X de V será denominado *variedade*. X está munido com a topologia induzida de V, que será chamada de *topologia de Zariski* sobre X.

Seja X uma variedade e U um subconjunto aberto não vazio de X, definimos $\Gamma(U, \mathcal{O}_X)$ como o conjunto de funções racionais sobre X que estão definidas em cada $P \in U$, isto é,

$$\Gamma(U, \mathcal{O}_X) := \bigcap_{P \in U} \mathcal{O}_P(X).$$

Note que se $U = X$ é uma variedade afim, então $\Gamma(X)$ é o anel de coordenadas de X, o que significa que a notação é consistente.

Sejam X e Y variedades. Um *morfismo* de X em Y é uma aplicação $\varphi : X \longrightarrow Y$ tal que:

1. φ é continua.
2. Para cada conjunto aberto U de Y, se $f \in \Gamma(U, \mathcal{O}_Y)$, então $\tilde{\varphi}(f) = f \circ \varphi$ está em $\Gamma(\varphi^{-1}(U), \mathcal{O}_X)$.

Um *isomorfismo* de X com Y é um morfismo 1-1 φ de X sobre Y tal que φ^{-1} é um morfismo.

Sejam X e Y variedades. Sejam U_1 e U_2 subvariedades abertas de X, considere os morfismos $f_1 : U_1 \longrightarrow Y$ e $f_2 : U_2 \longrightarrow Y$, definimos a relação:

$$f_1 \sim f_2 \Leftrightarrow f_1|_{U_1 \cap U_2} = f_2|_{U_1 \cap U_2}$$

Uma classe de equivalência para esses morfismos é denominada *função racional* de X em Y.

Uma função racional $F : X \longrightarrow Y$ é denominada *birracional* se existem conjuntos abertos $U \subset X$, $V \subset Y$ e um isomorfismo $f : U \longrightarrow V$ que represente F; dizemos que X e Y são birracionalmente equivalentes se existir uma função birracional de X em Y.

1.2.4 Modelos não singulares de curvas

Teorema 1.2.1. *(§7.5, Theorem 3). Seja C uma curva projetiva. Então existe uma curva projetiva não singular X e um morfismo birracional $f : X \to C$. Se $f' : X' \to C$ é*

um outro morfismo birracional, então existe um único isomorfismo $g : X \to X'$ tal que $f'g = f$.

Corolário. *Existe uma correspondência natural 1-1 entre curvas projetivas não singulares X e corpos de funções algébricas F sobre K.*

Se C é uma curva projetiva e $f : X \longrightarrow C$ é como no teorema anterior, diremos que X é o *modelo não singular* de C.

Dada uma curva projetiva não singular X, o corpo F em correspondência com X (mediante o corolário anterior) é o corpo $K(X)$ (ou $K(C)$ no caso em que X seja o modelo não singular da curva C).

Com o corolário anterior, conceitos como gênero e diferenciais vão poder ser associados a uma curva projetiva da seguinte forma:

Se C é uma curva projetiva e X é o seu modelo não singular, o gênero da curva C será o gênero do corpo de funções $K(X)$ associado a X.

Dizemos que ω é uma diferencial sobre C se $\omega \in \Omega_{K(X)}$.

De agora em diante, falaremos do gênero de uma curva (ou corpo de funções) e da diferencial de uma curva (ou corpo de funções) de acordo aos requerimentos da situação.

Se C é uma curva plana de grau n e G é uma curva plana que não contém C como componente, definimos o divisor:

$$\operatorname{div}(G) := \sum_{P \in X} ord_P(G) \cdot P,$$

onde $ord_P(G) = ord_Q(g)$ sendo $f(P) = Q$ ($f : X \to C$ o morfismo birracional do teorema acima) e g a imagem de G_* em $K(C) = K(X)$. $\operatorname{div}(G)$ é denominado o *o divisor da curva* G.

Observação 1.2.4. $\operatorname{div}(G)$ é um divisor de grau mn onde m é o grau da curva G, (isto segue do Teorema de Bézout).

Existe um método útil para calcular o gênero de uma curva plana com pontos múltiplos ordinários:

Proposição 1.2.3. *(§8.3, Proposition 5) Seja C uma curva plana com só pontos múltiplos ordinários. Seja n o grau de C e $r_P = m_P(C)$. Então, o gênero de C é dado pela fórmula:*

$$g = \frac{(n-1)(n-2)}{2} - \sum_{P \in C} \frac{r_P(r_P - 1)}{2}. \tag{1.1}$$

Exemplo. Como vimos atrás, as curvas de Fermat e de Hurwitz são não singulares, isso significa que para todo ponto P satisfazendo a equação da curva, $m_P(\mathcal{F}_n) = 1$ e $m_P(\mathcal{H}_n) = 1$, assim, $r_P = 1$ para todo P na proposição acima e segue de (1.1) que,

$$g(\mathcal{F}_n) = \frac{(n-1)(n-2)}{2}$$

e

$$g(\mathcal{H}_n) = \frac{n(n-1)}{2}.$$

2 Diferenciais de corpos de funções

2.1 Derivações e diferenciais

Definição 2.1.1. Seja M um módulo sobre F. Uma aplicação $\delta : F \longrightarrow M$ é chamada de *derivação de F/K* se δ é K-linear e cumpre a *regra do produto*:

$$\delta(u \cdot v) = u \cdot \delta(v) + v \cdot \delta(u),$$

para todo par $u, v \in F$.

Lema 2.1.1. ***(Propriedades básicas de uma derivação.)***

(a) $\delta(a) = 0$ *para todo* $a \in K$.

(b) $\delta(z^n) = nz^{n-1}\delta(z)$ *para todo* $z \in F$ *e para todo* $n \geqslant 0$.

(c) Se $char(K) = p > 0$, *então* $\delta(z^p) = 0$ *para todo* $z \in F$.

(d) $\delta\left(\dfrac{x}{y}\right) = \dfrac{y \cdot \delta(x) - x \cdot \delta(y)}{y^2}$, *para todo par* $x, y \in F$ *com* $y \neq 0$.

Demonstração.

(a) Se $a = 0$, o resultado é imediato. Suponha que $a \neq 0$, como δ é K-linear, por um lado temos que $\delta(a) = a\delta(1)$ para todo $a \in K$. Por outra parte, como δ satisfaz a regra do produto, então $\delta(a) = \delta(a \cdot 1) = a\delta(1) + \delta(a)$, de onde temos que $a\delta(1) = 0$, assim, $\delta(a) = 0$.

(b) Por indução sobre n:

$n = 2$: $\quad \delta(z^2) = \delta(z \cdot z) = z \cdot \delta(z) + z \cdot \delta(z) = 2z \cdot \delta(z) = 2z^{2-1}\delta(z)$.

Suponha que $\delta(z^k) = kz^{k-1}\delta(z)$ para $k > 2$.
Vamos mostrar que $\delta(z^{k+1}) = (k+1)z^{(k+1)-1}\delta(z)$.

$$\begin{aligned} \delta(z^{k+1}) = \delta(z^k \cdot z) &= z \cdot \delta(z^k) + z^k\delta(z) \\ &= z(kz^{k-1}\delta(z)) + z^k\delta(z) \\ &= kz^k\delta(z) + z^k\delta(z) \\ &= (k+1)z^k\delta(z). \end{aligned}$$

(c) Pelo item (b) temos que:

$$\delta(z^p) = pz^{p-1}\delta(z) = (p \cdot 1_K)z^{p-1}\delta(z) = 0.$$

(d) Lembre que $1_F = 1_K$, assim, pelo item (a) e a regra do produto temos que:

$$0 = \delta(1_K) = \delta(1_F) = \delta(y \cdot y^{-1}) = y \cdot \delta(y^{-1}) + y^{-1} \cdot \delta(y),$$

de onde,

$$y \cdot \delta(y^{-1}) = -y^{-1} \cdot \delta(y). \tag{2.1}$$

Por outra parte,

$$\delta(x/y) = \delta(x \cdot y^{-1}) = x\delta(y^{-1}) + y^{-1}\delta(x) = \frac{x \cdot y^2 \cdot \delta(y^{-1}) + y \cdot \delta(x)}{y^2}.$$

Usando a equação 2.1, concluímos:

$$\delta(x/y) = \frac{x \cdot y(-y^{-1} \cdot \delta(y)) + y \cdot \delta(x)}{y^2} = \frac{y \cdot \delta(x) - x \cdot \delta(y)}{y^2}.$$

■

A continuação, vamos ver que algumas derivações com uma propriedade específica, no caso de existir, são únicas.

Lema 2.1.2. *Suponha que x é uma variável separante de F/K e que $\delta_1, \delta_2 : F \longrightarrow M$ são derivações de F/K com $\delta_1(x) = \delta_2(x)$, então $\delta_1 = \delta_2$.*

Demonstração. Seja $f(x) = \sum a_i x^i$ um polinômio em $K[x]$ arbitrário. Pelo item (b) do lema anterior temos que, para $j = 1, 2$:

$$\delta_j(f(x)) = \delta_j\left(\sum a_i x^i\right) = \sum a_i \delta_j(x^i) = \sum i a_i x^{i-1}\delta_j(x),$$

mas, por hipótese, $\delta_1(x) = \delta_2(x)$, assim, $\delta_1(f(x)) = \delta_2(f(x))$.
Seja $z \in K(x)$ arbitrário, então $z = f(x)/g(x)$, e usando o anterior temos:

$$\begin{aligned}
\delta_1(z) = \delta_1(f(x)/g(x)) &= \frac{g(x)\delta_1(f(x)) - f(x)\delta_1(g(x))}{(g(x))^2} \\
&= \frac{g(x)\delta_2(f(x)) - f(x)\delta_2(g(x))}{(g(x))^2} \\
&= \delta_2(z).
\end{aligned}$$

Assim, provamos que as restrições de δ_1 e δ_2 a $K(x)$ são iguais.
Agora, seja $y \in F$ e $h(T)$ o seu polinômio mínimo em $K(x)[T]$; sabemos que $h(y) = 0$, suponha que $h(T) = \sum u_i T^i$, então, $\sum u_i y^i = 0$, logo,

$$0 = \delta_j(h(y)) = \sum_i \delta_j(u_i y^i) = \sum_i (u_i \delta_j(y^i) + y^i \delta_j(u_i)) = \delta_j(y) \sum_i i u_i y^{i-1} + \sum_i y^i \delta_j(u_i),$$

e sabemos que para todo $f(x) = \sum a_i x^i$ em $K[x]$, sua derivada $f'(x)$ está dada por $f'(x) = \sum i a_i x^{i-1}$, assim,

$$0 = \delta_j(y) h'(y) + \sum_i y^i \delta_j(u_i).$$

Agora, como x é um elemento separante, então F/K é uma extensão separável, assim, $h(T)$ é separável e sabemos que um polinômio $f \in K[x]$ tem só raízes simples se e somente se $mcd(f, f') = 1$, com isso, se acontece que $h'(y) = 0$, teríamos que $(T - y)|h'(T)$ e $(T - y)|h(T)$ contrariando a asserção anterior, logo, $h'(y) \neq 0$ e temos que

$$\delta_j(y) = \frac{1}{h'(y)} \sum_i y^i \delta_j(u_i),$$

e como $u_i \in K(x)$, temos que $\delta_1(u_i) = \delta_2(u_i)$ para todo i, portanto, $\delta_1(y) = \delta_2(y)$ como queríamos provar. ■

Proposição 2.1.1. *Suponha que E/F é uma extensão finita separável de F e $\delta_0 : F \longrightarrow N$ é uma derivação de F/K em algum corpo $N \supset E$. Então δ_0 pode-se estender a uma derivação $\delta : E \longrightarrow N$; esta extensão está unicamente determinada por δ_0.*

Demonstração. Primeiro vamos definir duas aplicações s^0 e s' da seguinte forma:

$$\begin{array}{rccc} s^0 & : & F[T] & \longrightarrow & N[T] \\ & & \sum s_i T^i & \longmapsto & \sum \delta_0(s_i) T^i \end{array} \qquad \begin{array}{rccc} s' & : & F[T] & \longrightarrow & N[T] \\ & & \sum s_i T^i & \longmapsto & \sum i s_i T^{i-1} \end{array}$$

As duas aplicações são K-lineares: a linearidade de s' é imediata, a de s^0 segue da linearidade de δ_0. Agora, vamos mostrar que s^0 e s' satisfazem a regra do produto: suponha que $f(T) = \sum_{k=0}^{n} a_k T^k$ e $g(T) = \sum_{j=0}^{m} b_j T^j$, sem perda de generalidade, suponha que $m \geqslant n$. Sabemos que

$$f(T) \cdot g(T) = \sum_{j=0}^{m} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) T^j,$$

assim,

$$\begin{aligned} s^0(f(T)\cdot g(T)) &= s^0\left(\sum_{j=0}^{m}\left(\sum_{k=0}^{j}a_kb_{j-k}\right)T^j\right) \\ &= \sum_{j=0}^{m}\delta_0\left(\sum_{k=0}^{j}a_kb_{j-k}\right)T^j \\ &= \sum_{j=0}^{m}\left(\sum_{k=0}^{j}\delta_0(a_kb_{j-k})\right)T^j \\ &= \sum_{j=0}^{m}\sum_{k=0}^{j}[a_k\delta_0(b_{j-k})+b_{j-k}\delta_0(a_k)]T^j \\ &= \sum_{j=0}^{m}\sum_{k=0}^{j}a_k\delta_0(b_{j-k})T^j+\sum_{j=0}^{m}\sum_{k=0}^{j}b_{j-k}\delta_0(a_k)T^j, \end{aligned}$$

e sabemos que $s^0(f(T))=\sum_{k=0}^{n}\delta_0(a_k)T^k$ e $s^0(g(T))=\sum_{j=0}^{m}\delta_0(b_j)T^j$, logo,

$$\sum_{j=0}^{m}\sum_{k=0}^{j}a_k\delta_0(b_{j-k})T^j+\sum_{j=0}^{m}\sum_{k=0}^{j}b_{j-k}\delta_0(a_k)T^j=f(T)s^0(g(T))+g(T)s^0(f(T)).$$

Analogamente,

$$\begin{aligned} s'(f(T)\cdot g(T)) &= \sum_{j=0}^{m}j\left(\sum_{k=0}^{j}a_kb_{j-k}\right)T^{j-1} \\ &= \sum_{j=0}^{m}\sum_{k=0}^{j}ja_kb_{j-k}T^{j-1} \\ &= f(T)s'(g(T))+g(T)s'(f(T)). \end{aligned}$$

Como E é separável, pelo teorema do elemento primitivo, existe $u\in E$, tal que $E=F(u)$. Seja $f(T)$ o polinômio mínimo de u e $n=\text{grau}(f)=[E:F]$; lembremos que $F(u)=\{a_0+a_1u+\cdots+a_ru^r \mid a_i\in F,\ r<n\}$, assim, se $y\in E$, então $y=h(u)$ onde $h(T)\in F[T]$ e $\text{grau}(h)<n$.
Definimos $\delta: E\longrightarrow N$ da seguinte forma:

$$\delta(y):=h^0(u)-\frac{f^0(u)}{f'(u)}\cdot h'(u),$$

Novamente, como f é o polinômio mínimo de u e E é uma extensão separável de F, então f é separável e temos que $m.c.d(f,f')=1$, segue que $f'(u)\neq 0$ e δ está bem definida. Claramente, se $y\in F$, então $\text{grau}(h)=0$ e segue que $h'(T)\equiv 0$ e $h^0=\delta_0(y)$, logo,

$$\delta(y)=\delta_0(y)-\frac{f^0(u)}{f'(u)}\cdot 0=\delta_0(y);$$

isso significa que $\delta|_F = \delta_0$. Falta provar que δ é K-linear e que satisfaz a regra do produto.

(i) δ é K-linear: Sejam $x, y \in E$ e $\lambda \in K$.

$$\begin{aligned}
\delta(\lambda x + y) &= \delta(\lambda h_1(u) + h_2(u)) = \delta((\lambda h_1 + h_2)(u)) \\
&= (\lambda h_1 + h_2)^0(u) - \frac{f^0(u)}{f'(u)}(\lambda h_1 + h_2)'(u) \\
&= \lambda h_1^0(u) + h_2^0(u) - \frac{f^0(u)}{f'(u)}(\lambda h_1'(u) + h_2'(u)) \\
&= \lambda\left(h_1^0(u) - \frac{f^0(u)}{f'(u)}h_1'(u)\right) + \left(h_2^0(u) - \frac{f^0(u)}{f'(u)}h_2'(u)\right) \\
&= \lambda\delta(h_1(u)) + \delta(h_2(u)) = \lambda\delta(x) + \delta(y).
\end{aligned}$$

(ii) Regra do produto: Sejam $y, z \in E$, então $y = h(u)$ e $z = g(u)$ com $\text{grau}(h) < n$ e $\text{grau}(g) < n$. Pelo algoritmo da divisão: $h(T)g(T) = c(T)f(T) + r(T)$, onde $c(T), r(T) \in F[T]$ e $\text{grau}(r(T)) < n$, assim, $h(u)g(u) = c(u)f(u) + r(u) = r(u)$ e

$$\delta(y \cdot z) = \left(r^0 - \frac{f^0}{f'}r'\right)(u) = \frac{1}{f'(u)}(r^0 f' - f^0 r')(u),$$

mas, pelo dado acima, $r = hg - cf$, assim,

$r^0 = (hg - cf)^0 = (hg)^0 - (cf)^0 = g^0h + gh^0 - c^0f - f^0c$
e
$r' = (hg - cf)' = (hg)' - (cf)' = g'h + gh' - c'f - f'c$
e segue que

$$\begin{aligned}
\delta(y \cdot z) &= \frac{1}{f'(u)}\left((g^0h + gh^0 - c^0f - f^0c)f' - (g'h + gh' - c'f - f'c)f^0\right)(u) \\
&= \frac{1}{f'(u)}\left(g^0hf' + gh^0f' - f^0g'h - f^0h'g\right)(u), \qquad (1)
\end{aligned}$$

Por outra parte, temos que:

$$\begin{aligned}
y \cdot \delta(z) + z \cdot \delta(y) &= h(u)\left(g^0(u) - \frac{f^0}{f'(u)}g'(u)\right) + g(u\left(h^0(u) - \frac{f^0(u)}{f'(u)}h'(u)\right)) \\
&= \frac{1}{f'(u)}\left[(hg^0f' - hf^0g')(u) + (gh^0f' - gf^0h')(u)\right] \\
&= \frac{1}{f'(u)}\left(g^0hf' + gh^0f' - f^0g'h - f^0h'g\right)(u) \qquad (2)
\end{aligned}$$

Obtendo que as expressões (1) e (2) coincidem.

Unicidade: Suponha que δ_1 e δ_2 são duas extensões de δ_0, então, $\delta_1|_F = \delta_2|_F = \delta_0$.
Sabemos que F é um corpo de funções algébricas sobre K, isso significa que existe $x \in F$ transcendente sobre K para o qual $F/K(x)$ é uma extensão algébrica e finita.
Observe que $F/K(x)$ é separável: de fato, se $y \in F$ não é separável e o seu polinômio mínimo é $p(t) \in K(x)[T]$, teremos que $p(t)$ não é separável, mas, por hipótese E/F é separável e $K(x) \subseteq F$, assim, $p(t) \in F[T]$ é separável, absurdo. Logo, $F/K(x)$ é separável.
Como E/F e $F/K(x)$ são separáveis, temos que $E/K(x)$ é separável, assim, pela definição, concluímos que x é um elemento separante de E/K, e como $x \in F$, temos que $\delta_1(x) = \delta_2(x)$; segue do lema anterior que $\delta_1 = \delta_2$. ■

Teorema 2.1.1. ***(Existência das derivações).*** *Se $x \in F$ é um elemento separante de F/K e $N \supseteq F$ é algum corpo, então existe uma única derivação $\delta : F \longrightarrow N$ de F/K com a propriedade $\delta(x) = 1$.*

Demonstração. A unicidade é imediata do Lema 2.1.2, pois se δ_1 e δ_2 são derivações como no teorema, então $\delta_1(x) = \delta_2(x)$ e x é um elemento separante, assim, $\delta_1 = \delta_2$.

Vamos mostrar a existência: Seja $\delta_0 : K(x) \longrightarrow N$ dada por:

$$\delta_0\left(\frac{f(x)}{g(x)}\right) = \frac{g(x)f'(x) - f(x)g'(x)}{(g(x))^2},$$

sendo f' e g' as derivadas formais dos polinômios $f, g \in K[x]$ respectivamente. Queremos provar que δ_0 é uma derivação. É claro que δ_0 é K-linear. Vamos mostrar que δ_0 satisfaz a regra do produto.
Sejam $z_1 = f_1(x)/g_1(x)$ e $z_2 = f_2(x)/g_2(x)$ em $K(x)$, então $z_1 \cdot z_2 = (f_1f_2)(x)/(g_1g_2)(x)$, logo,

$$\begin{aligned}
\delta_0(z_1 \cdot z_2) &= \frac{(g_1g_2)(x)(f_1f_2)'(x) - (f_1f_2)(x)(g_1g_2)'(x)}{((g_1g_2)(x))^2} \\
&= \frac{(g_1g_2)(x)(f_1'f_2 + f_1f_2')(x) - (f_1f_2)(x)(g_1'g_2 + g_1g_2')(x)}{((g_1g_2)(x))^2} \\
&= \frac{f_1(x)}{g_1(x)}\frac{g_2(x)f_2'(x) - f_2(x)g_2'(x)}{(g_2(x))^2} + \frac{f_2(x)}{g_2(x)}\frac{g_1(x)f_1'(x) - f_1(x)g_1'(x)}{(g_1(x))^2} \\
&= z_1 \cdot \delta_0(z_2) + z_2 \cdot \delta_0(z_1).
\end{aligned}$$

Assim, pela proposição anterior, δ_0 pode-se estender a uma derivação $\delta : F \longrightarrow N$. Observe que $x \in K(x)$ e $\delta_0(x) = \delta_0\left(\frac{f(x)}{g(x)}\right)$ sendo $f(x) = x$ e $g(x) = 1$, assim, $g'(x) \equiv 0$ e $f'(x) = 1$, logo, $\delta_0(x) = \frac{1 - 0 \cdot x}{1^2} = 1$ e como $\delta|_{K(x)} = \delta_0$ temos que $\delta(x) = 1$ e concluímos que δ é a derivação procurada. ■

Definição 2.1.2. (a) Seja x um elemento separante de F/K. A única derivação $\delta_x : F \longrightarrow F$ tal que $\delta_x(x) = 1$ é chamada de *derivação com respeito a x*.

(b) Seja

$$\mathrm{Der}_F := \{\eta : F \to F \mid \eta \text{ é uma derivação de } F/K\}$$

Para $\eta_1, \eta_2 \in \mathrm{Der}_F$ e $u, z \in F$ definimos:

- $(\eta_1 + \eta_2)(z) := \eta_1(z) + \eta_2(z)$
- $(u\eta_1(z)) := u\eta_1(z)$.

Observação 2.1.1. Claramente $(\eta_1 + \eta_2)$ e $(u\eta_1)$ são K-lineares, pois η_1 e η_2 são. Vamos ver que também satisfazem a regra do produto:

$$\begin{aligned}(\eta_1 + \eta_2)(z_1 \cdot z_2) &= (z_1 \cdot \eta_1(z_2) + z_2 \cdot \eta_1(z_1)) + (z_1 \cdot \eta_2(z_2) + z_2 \cdot \eta_2(z_2)) \\ &= z_1(\eta_1(z_2) + \eta_2(z_2)) + z_2(\eta_1(z_1) + \eta_2(z_1)) \\ &= z_1(\eta_1 + \eta_2)(z_2) + z_2(\eta_1 + \eta_2)(z_1).\end{aligned}$$

e

$$\begin{aligned}(u\eta_1)(z_1 \cdot z_2) &= u(z_1 \cdot \eta_1(z_2) + z_2 \cdot \eta_1(z_1)) \\ &= z_1(u\eta_1)(z_2) + z_2(u\eta_1)(z_1).\end{aligned}$$

Assim, $(\eta_1 + \eta_2)$ e $u\eta$ são derivações. Logo, com as operações definidas em (b) temos que Der_F é um espaço vetorial sobre F, ou seja, um F-módulo, desta forma, Der_F é chamado de *módulo das derivações de* F/K.

Lema 2.1.3. *Seja x um elemento separante de F/K.*

(a) Para cada derivação $\eta \in Der_F$, temos que $\eta = \eta(x)\delta(x)$, em particular, Der_F é um F-módulo unidimensional.

(b) ***(Regra da cadeia).*** *Se y é um outro elemento separante de F/K, então*

$$\delta_y = \delta_y(x) \cdot \delta_x.$$

(c) Para $t \in F$ temos que $\delta_x(t) \neq 0$ se e só se t é um elemento separante.

Demonstração.

(a) Considere as derivações em Der_F: η e $\underbrace{\eta(x)}_{\in F} \cdot \delta_x$.

Observe que $(\eta(x)\cdot\delta_x)(x) = \eta(x)\cdot\delta_x(x) = \eta(x)\cdot 1 = \eta(x)$; assim, como x é um elemento separante , o Lema 2.1.2 permite concluir que $\eta = \eta(x) \cdot \delta_x$, logo, $\mathrm{Der}_F = span\{\delta_x\}$.

(b) Sabemos que $\delta_y \in \mathrm{Der}_F$, assim, tomando $\eta = \delta_y$ em (a) obtemos que $\delta_y = \delta_y(x) \cdot \delta_x$.

(c) Se t é separante, pela regra da cadeia temos que $\delta_t = \delta_t(x)\delta_x$, assim, $\delta_t(t) = \delta_t(x)\delta_x(t)$ isto é, $1 = \delta_t(x)\delta_x(t)$ o que significa que $\delta_x(t) \neq 0$, pois F é um corpo.

Reciprocamente, Suponha que $\delta_x(t) \neq 0$ e que t não é separante. Se $\text{char}K = 0$, temos que $t \in K$ e como δ_x é uma derivação, temos $\delta_x(t) = 0$, absurdo.
Suponha que $\text{char}K = p > 0$, como t não é separante temos que $t \in F^p$, isto é, existe existe $u \in F$ tal que $t = u^p$, assim, $\delta_x(t) = \delta_x(u^p) = 0$, absurdo.

■

Considere agora o conjunto $Z = \{(u, x) \in F \times F \mid u \in F \text{ e } x \text{ é separante}\}$ e considere a seguinte relação sobre esse conjunto:

$$(u, x) \sim (v, y) \Leftrightarrow v = u \cdot \delta_y(x).$$

Afirmação. $\sim$ é uma relação de equivalência sobre Z:

- *Reflexividade:* Sabemos que $\delta_x(x) = 1$, assim, $u = u \cdot \delta_x(x)$, isto é, $(u, x) \sim (u, x)$.
- *Simetria:* Suponha que $(u, x) \sim (v, y)$; pela regra da cadeia sabemos que $\delta_y = \delta_y(x) \cdot \delta_x$, assim, $\delta_y(y) = \delta_y(x) \cdot \delta_x(y)$, e como consequência temos que $(\delta_y(x))^{-1} = \delta_x(y)$.
  Por hipótese temos que $v = u \cdot \delta_y(x)$, assim, $u = v \cdot (\delta_y(x))^{-1} = v \cdot \delta_x(y)$, portanto, $(v, y) \sim (u, x)$.
- *Transitividade:* Suponha que $(u, x) \sim (v, y)$ e $(v, y) \sim (w, z)$.
  Temos que $v = u \cdot \delta_y(x)$ e $w = v \cdot \delta_z(y)$, substituindo o resultado da primeira equação na segunda, temos: $w = (u \cdot \delta_y(x))\delta_z(y)$, assim,

$$w = u(\delta_x(y))^{-1}\delta_z(y). \tag{2.2}$$

  Agora, pela regra da cadeia temos que $\delta_z = \delta_z(x)\delta_x$ e segue que $\delta_z(y) = \delta_z(x)\delta_x(y)$ e substituindo em 2.2 temos que

$$w = u(\delta_x(y))^{-1}\delta_z(x)\delta_x(y) = u \cdot \delta_z(x),$$

  Logo, $(u, x) \sim (w, z)$.

Definição 2.1.3. (a) Denotamos a classe de equivalência de (u, x) em Z com respeito a $\sim$ por udx e chamamos ela de *diferencial de* F/K. Assim, por definição temos que

$$udx = vdy \Leftrightarrow v = u\delta_y(x)$$

A classe de equivalência de $(1, x)$ é denotada simplesmente por dx.

(b) Seja

$$\Delta_F := \{udx \mid u \in F \text{ e } x \text{ é separante}\},$$

o conjunto de todas as diferenciais de F/K. Escolhemos um elemento separante z e observamos o seguinte:

Claramente, $u\delta_z(x) = u \cdot \delta_z(x)$, assim, $(u, x) \sim (u\delta_z(x), z)$, isso significa que $udx = (u\delta_z(x))dz$. Analogamente, $vdy = (v\delta_z(y))dz$; desta forma, definimos a operação *soma* em Δ_F como segue:

$$udx + vdy := (u\delta_z(x) + v\delta_z(y))dz$$

Também, dado $w \in F$ definimos a seguinte operação:

$$w(udx) := (wu)dx$$

Observações.

- A definição da operação soma acima é independente da escolha do elemento z:

  De fato, suponha que t é um outro elemento separante de F/K. Pela regra da cadeia sabemos que $\delta_t = \delta_t(z)\delta_z$, assim, $\delta_t(z) = \delta_t(z) \cdot \delta_z(z) = 1 \cdot \delta_t(z)$, isso significa que $(1, z) \sim (\delta_t(z), t)$, assim, $dz = \delta_t(z)dt$ e

  $$\begin{aligned}(u\delta_z(x) + v\delta_z(y))dz &= (u\delta_z(x) + v\delta_z(y))\delta_t(z)dt \\ &= (u\delta_z(x)\delta_t(z) + v\delta_z(y)\delta_t(z))dt.\end{aligned}$$

  Pela regra da cadeia temos que $\delta_t(x) = \delta_t(z)\delta_z(x)$ e $\delta_t(y) = \delta_t(z)\delta_z(y)$, logo,

  $$udx + vdy = (u\delta_z(x) + v\delta_z(y))dz = (u\delta_t(x) + v\delta_t(y))dt.$$

- Δ_F vira um espaço vetorial sobre F (ou F-módulo) com as operações definidas acima.

Definição 2.1.4. Para um elemento $t \in F$ não separante definimos $dt := 0 \in \Delta_F$, e definimos a seguinte aplicação:

$$\begin{array}{rccc} d & : & F & \longrightarrow & \Delta_F \\ & & t & \longmapsto & dt \end{array}$$

O par (Δ_F, d) é chamada de *módulo das diferenciais de F/K.*

Agora, vamos estudar algumas propriedades básicas de Δ_F.

Proposição 2.1.2. *(a) Seja $z \in F$ um elemento separante, então, $dz \neq 0$ e cada $\omega \in \Delta_F$ pode ser escrito de forma única como $\omega = udz$ onde $u \in F$. Assim, Δ_F é um F-módulo unidimensional.*

(b) A aplicação definida na parte (d) da definição anterior $d : F \longrightarrow \Delta_F$ é uma derivação.

(c) Para $t \in F$ temos $dt \neq 0$ se e só se t é separante.

(d) Suponha que $\delta : F \longrightarrow M$ é uma derivação de F/K em algum F-módulo M. Então existe uma unica aplicação F-linear $\mu : \Delta_F \longrightarrow M$ tal que $\delta = \mu \circ d$.

Demonstração.

(a) $0 = 0 \cdot dz$, a diferencial nula, assim, $0 \cdot dz = u \cdot dz$ implica que $(0, z) \sim (u, z)$ para $u \neq 0$, mas, se isso acontece, $u = 0 \cdot \delta_z(z) = 0$, contradição. Logo, se particularmente $u = 1$, temos que $dz \neq 0 \cdot dz = 0$.
Agora, seja $\omega \in \Delta_F$ arbitrária. Então, $\omega = vdy$ para algum elemento separante y. Escolhemos $u = v\delta_z(y)$, assim,

$$udz = (v\delta_z(y))dz, \qquad (*)$$

e como $\delta_y = \delta_y(z)\delta_z$, temos que $1 = \delta_y(z)\delta_z(y)$, assim, $v = v\delta_y(z)\delta_z(y)$, o que significa que $(v\delta_z(y), z) \sim (v, y)$, isto é, $v\delta_z(y)dz = vdy$, logo, em $(*)$ queda que $udz = vdy = \omega$.
Se $\omega = u_1dz$ e $\omega = u_2dz$, então, $u_1dz - u_2dz \equiv 0$ e $(u_1 - u_2)dz \equiv 0$, como $dz \neq 0$, temos que $u_1 = u_2$.

(b) Fixamos $z \in F$ separante. Observe que do fato que $\delta_z(t) = 1 \cdot \delta_z(t)$, segue que $(1, t) \sim (\delta_z(t), z)$ e portanto,

$$dt = \delta_z(t)dz \qquad (2.3)$$

Observe que se t não fosse separante, do item (c) do lema anterior teríamos que $\delta_z(t) = 0$ e por definição temos que $dt = 0$, portanto, a igualdade vale acima vale para todo t.
Logo, $d(ax) = \delta_z(ax)dz = a\delta_z(x) = adx$ e $d(x + y) = \delta_z(x + y)dz = (\delta_z(x) + \delta_z(y))dz = \delta_z(x)dz + \delta_z(y)dz = dx + dy$. Falta mostrar que d satisfaz a regra do produto:
Da equação (2.3) segue que:

$$\begin{aligned} d(xy) = \delta_z(xy)dz &= (x\delta_z(y) + y\delta_z(x))dz \\ &= x(\delta_z(y)dz) + y(\delta_z(x)dz) \\ &= xdy + ydx. \end{aligned}$$

(c) A implicação "$\Leftarrow$"segue de (a).
Se $dt \neq 0$ e t não fosse separante, contrariaríamos a definição da aplicação d, logo t deve ser separante.

(d) Dado $z \in F$ separante, pelo item (a), cada $\omega \in \Delta_F$ pode ser escrito como $\omega = udz$ sendo u um elemento de F; Definimos μ por $\mu(\omega) := u \cdot \delta(z)$ se $w = udz$. É claro que $u \cdot \delta(z) \in M$ por ser M um F-módulo.

- μ é F-linear: De fato, se $v \in F$ e $\omega_1, \omega_2 \in \Delta_F$, com $\mu(\omega_1) = u \cdot \delta(z)$ e $\mu(\omega_2) = y \cdot \delta(z)$, então,

$$\mu(v\omega_1) = \mu((vu)dz) = (vu) \cdot \delta(z) = v(u \cdot \delta(z)) = v\mu(\omega)$$

$$\mu(\omega_1 + \omega_2) = \mu((u + y)dz) = (u + v) \cdot \delta(z) = \mu(\omega_1) + \mu(\omega_2)$$

- Agora, vamos mostrar que $\mu \circ d$ é uma derivação: é claro que $\mu \circ d$ é K-linear porque μ é F-linear e d é uma derivação. Verificamos então a regra do produto para $\mu \circ d$.

  Sejam $u, v \in F$, então,

  $(\mu \circ d)(u \cdot v) = \mu(d(u \cdot v)) = \mu(udv + vdu) = \mu(udv) + \mu(vdu) = u(\mu \circ d)(v) + v(\mu \circ d)(u)$,

  com isso, concluímos que $\mu \circ d$ é uma derivação.

  De acordo com o Lema 2.1.2, é suficiente mostrar que para z temos que $\delta(z) = (\mu \circ d)(z)$, isso é claro pela definição de μ. Logo, $\delta = \mu \circ d$.

- Unicidade de μ: Se $\nu : \Delta_F \longrightarrow M$ é uma outra aplicação F-linear com $\delta = \nu \circ d$, então, dado $udz \in \Delta_F$ arbitrário, temos que:

$$\nu(udz) = u\nu(dz) = u(\nu \circ d)(z) = u \cdot \delta(z) = u(\mu(dz)) = \mu(udz);$$

  portanto, $\mu = \nu$.

■

Observações Importantes.

(i) Uma diferencial da forma específica $\omega = dx$ com $x \in F$ é chamada *exata.*

As diferenciais exatas formam um K-subespaço vetorial de Δ_F: pela K-linearidade de d temos que $ad(x) = d(ax)$ para todo $x \in F$ e $a \in K$, e claramente $d(ax)$ é exata. Por outra parte, se dx e dy são formas exatas, sabemos pela linearidade de d que $dx + dy = d(x + y)$, sendo $x + y$ um elemento de F.

(ii) Uma diferencial da forma especifica $\omega = dz/z$, com $z \in F$, é denominada *logarítmica.*

(iii) Como Δ_F é um F-módulo 1-dimensional, podemos definir o *quociente* $\omega_1/\omega_2 \in F$ para $\omega_1, \omega_2 \in \Delta_F$ e $\omega_2 \neq 0$ da seguinte forma: seja $u \in F$, diremos que:

$$u = \frac{\omega_1}{\omega_2} \quad \Leftrightarrow \quad \omega_1 = u\omega_2.$$

Em particular, se $y \in F$ e z é um elemento separante, da equação (2.3) segue que:

$$\frac{dy}{dz} = \delta_z(y). \tag{2.4}$$

Portanto, reescrevendo a definição temos:

$$udx = vdy \quad \Leftrightarrow \quad v = u \cdot \frac{dx}{dy} \quad \Leftrightarrow \quad u = v \cdot \frac{dy}{dx},$$

e reescrevendo a regra da cadeia para os elementos separantes x e z temos:

$$\frac{dy}{dx} = \frac{dy}{dz} \cdot \frac{dz}{dx}.$$

2.2 Diferenciais e diferenciais de Weil

Existe uma derivação $\delta : F \longrightarrow \Omega_F$, onde Ω_F é o módulo das diferencias de Weil. Mostrar explicitamente esta derivação requer ferramentas teóricas que se afastam do objetivo deste documento; todo o referido a esta derivação pode ser encontrado em (STICHTENOTH, 2008), aqui somente estamos interessados em sua existência.

Da parte (d) da Proposição 2.1.2, temos que existe uma aplicação F-linear $\mu : \Delta_F \longrightarrow \Omega_F$ com $\delta = \mu \circ d$; neste caso, de fato, μ é um isomorfismo, isso significa que é possível identificar o módulo das diferenciais Δ_F com o módulo das diferenciais de Weil Ω_F, assim, se $x \in F$ é uma variável separante e z é qualquer elemento de F, a diferencial $\omega = z \cdot dx \in \Delta_F$ é o mesmo que a diferencial de Weil $z \cdot \delta(x) \in \Omega_F$.

Com o anterior, se $0 \neq \omega \in \Delta_F$ e t é um parâmetro local de $P \in \mathbb{P}_F$, escrevendo $\omega = z \cdot dt$ podemos definir:

$$v_P(\omega) := v_P(z)$$

como a valoração em P da diferencial ω, e

$$(\omega) := \sum_{P \in \mathbb{P}_F} v_P(\omega) \cdot P$$

como o divisor associado à diferencial ω.

Para cada divisor $A \in \mathrm{Div}(F)$, definimos o K- espaço vetorial:

$$\Delta_F(A) := \{\omega \in \Delta_F \mid \omega = 0 \text{ ou } (\omega) \geqslant A\}.$$

Por meio da identificação de Δ_F com Ω_F (mediante μ), temos que $\Delta_F(A)$ se corresponde com $\Omega_F(A)$, assim, dizemos que $\omega \in \Delta_F$ é *regular (ou holomorfa ou de primeira ordem)* se

$\omega \in \Delta_F(0)$.

Aplicação: Vamos calcular uma base para o espaço das diferencias regulares sobre um corpo de funções específico.

Suponha que char$K \neq 2$ e considere o corpo de funções $F = K(x, y)$ satisfazendo a equação:

$$y^2 = \prod_{i=1}^{2m+1} (x - a_i), \tag{2.5}$$

onde $m \geqslant 0$ e $a_1, \ldots, a_{2m+1} \in K$ são elementos distintos de K. Vamos mostrar que o conjunto

$$\mathcal{B} = \{x^i dx/y \mid 0 \leqslant i \leqslant m-1\}$$

é uma base do espaço das diferenciais regulares de $F/K(x)$.

Primeiro, vamos determinar o divisor da diferencial $\omega = dx/y$.

Sabemos que $v_P(\omega) = v_P(y^{-1}) + v_P(dx)$. Seja $G(x) = \prod_{i=1}^{2m+1} (x - a_i)$.

Os lugares de $K(x)$ são da forma P_a com $a \in K$ e P_∞, onde $x - a$ é um parâmetro local de P_a e $1/x$ é um parâmetro local de P_∞. (ver §1.1.2).

Seja $P \in \mathbb{P}_F$, temos os seguintes casos:

- $P|P_\infty$:

  Pela definição de e sabemos que $v_P(x^{-1}) = e(P|P_\infty)$, assim, $v_P(x) = -e(P|P_\infty)$. De (2.5) temos que
  $$2v_P(y) = \sum_{i=1}^{2m+1} v_P(x - a_i).$$
  Como $v_P(x) < 0$ e $v_P(a_i) = 0$ para todo i, da desigualdade triangular estrita segue que $v_P(x - a_i) = -e(P|P_\infty)$ para todo i, assim,
  $$\sum_{i=1}^{2m+1} v_P(x - a_i) = -(2m+1)e(P|P_\infty),$$
  isto é,
  $$2v_P(y) = -(2m+1)e(P|P_\infty),$$

de onde temos que $e(P|P_\infty) = 2$ (igualdade fundamental); logo,

$$v_P(y^{-1}) = 2m + 1.$$

Seja t um parâmetro local de P, como $v_P(x) = -2$, temos que $x = ut^{-2}$ onde u é uma unidade, assim, $dx = d(ut^{-2}) = -2ut^{-3}dt$ e temos que

$$\frac{dx}{dt} = -2ut^{-3},$$

logo, $v_P(dx) = -3$ e concluímos que $v_P(\omega) = 2m - 2$.

- $P|P_a$ e $(x-a) \mid G(x)$:

Pela definição de e sabemos que $v_P(x-a) = e(P|P_a)$. Observe que $v_P(x-a_i) = 0$ para todo $a_i \neq a$. De (2.5) temos que

$$2v_P(y) = v_P(x-a) + \sum_{a_i \neq a} v_P(x-a_i),$$

portanto, $2v_P(y) = e(P|P_a)$ e novamente, pela igualdade fundamental, $e(P|P_a) = 2$. Concluímos que $v_P(y^{-1}) = -1$.
Agora, como $v_P(x-a) = 2$, se t é um parâmetro local para P, temos que $x - a = ut^2$ onde u é uma unidade, assim, $d(x-a) = dx - da = 2utdt$, isto é, $dx = 2utdt$, logo,

$$\frac{dx}{dt} = 2ut.$$

Segue que $v_P(dx) = 1$ e $v_P(\omega) = 0$.

- $P|P_a$ e $(x-a) \nmid G(x)$:

Aqui, como no caso anterior temos que $v_P(x-a_i) = 0$ para todo $i = 1, \ldots, 2m+1$, de onde segue que $2v_P(y) = 0$, portanto, $v_P(y^{-1}) = 0$. Temos duas opções para $v_P(x-a)$:
Se $v_P(x-a) = 1$, então temos que $v_P(\omega) = 0$ e concluímos que

$$v_P(\omega) = \begin{cases} 0 & \text{se} \quad P|P_a \\ 2m-2 & \text{se} \quad P|P_\infty. \end{cases}$$

Se $v_P(x-a) = 2$, então temos que $v_P(\omega) = 1$ e concluímos que

$$v_P(\omega) = \begin{cases} 0 & \text{se} \quad P|P_a \ \ e \ \ (x-a) \mid G(x) \\ 1 & \text{se} \quad P|P_a \ \ e \ \ (x-a) \nmid G(x) \\ 2m-2 & \text{se} \quad P|P_\infty. \end{cases}$$

No primeiro caso temos que $(\omega) = (2m-2)P_\infty$ e no segundo, $(\omega) = P_a + (2m-2)P_\infty$. Como (ω) é um divisor canônico, temos que $\text{grau}((\omega)) = 2g-2$, assim, se $v_P(x-a) = 2$ acima, temos que $m = g - \dfrac{1}{2}$, mas sabemos que m é um inteiro não negativo. Portanto, $(\omega) = (2m-2)P_\infty$ e temos que $m = g$.

Do anterior segue que se $d = \text{grau}(G(x))$ é ímpar, então,

$$g = \frac{d-1}{2}. \tag{2.6}$$

Agora, vamos mostrar que o conjunto $\mathcal{B}$ $(m = g)$ é uma base das diferenciais regulares. Primeiro, vamos mostrar que $\mathcal{B} \subset \Delta_F(0)$. Continuamos denotando por ω a diferencial dx/y.

Sabemos que $v_P(x^i\omega) = iv_P(x) + v_P(\omega)$ para todo $P \in \mathbb{P}_F$.

Se $P|P_\infty$, então $v_P(x) = -2$. Como $i \leqslant g-1$, temos que $iv_P(x) \geqslant -2(g-1)$, assim, $iv_P(x) + v_P(\omega) \geqslant -2(g-1) + 2g - 2$, isto é, $v_P(x^i\omega) \geqslant 0$ para todo i com $1 \leqslant i \leqslant g-1$.

Se $P|P_a$, temos que $v_P(x) = v_P((x-a)+a)$, como $v_P(x-a) \in \{1,2\}$ e $v_P(a) = 0$ para todo $a \in K$, da desigualdade triangular estrita segue que $v_P(x) = 0$, assim, $iv_P(x) = 0$, portanto, $v_P(x^i\omega) = 0$ para todo i com $0 \leqslant i \leqslant g-1$. Segue que $\mathcal{B} \subset \Delta_F(0) = \Omega_F(0)$.

Como vimos no capítulo anterior, $\dim_K \Omega_F(0) = g$; como o conjunto $\mathcal{B}$ tem g elementos, basta mostrar que eles são linearmente independentes sobre K.

Suponha que

$$\sum_{i=0}^{g-1} \alpha_i x^i \omega = 0, \tag{2.7}$$

onde $\alpha_i \in K$ para $0 \leqslant i \leqslant g-1$ e não são todos nulos.
Seja $P \in \mathbb{P}_F$ com $P|P_\infty$. Sabemos que $v_P(x) = -2$, assim, se $i < j$, então $iv_P(x) > jv_P(x)$ e temos que

$$v_P(\alpha_i x^i \omega) > v_P(\alpha_j x^j \omega)$$

para todo $i < j$. O anterior significa que $v_P(\alpha_i x^i\omega) \neq v_P(\alpha_j x^j\omega)$ para todo $i \neq j$, assim, segue da desigualdade triangular estrita que

$$v_P\left(\sum_{i=0}^{g-1} \alpha_i x^i \omega\right) = \min\{v_P(x^i\omega) \mid \alpha_i \neq 0,\ 0 \leqslant i \leqslant g-1\}.$$

Por outra parte, de (2.7) temos que

$$v_P\left(\sum_{i=0}^{g-1} \alpha_i x^i \omega\right) = v_P(0) = \infty.$$

Logo, $\alpha_i = 0$ para todo i com $0 \leqslant i \leqslant g-1$; concluímos que $\mathcal{B}$ é uma base para as diferenciais regulares sobre F. □

O corpo F acima é um caso especial de um tipo de corpo de funções denominado *corpo de funções hiperelíptico*; Aliás, F/K é um corpo de funções hiperelíptico sobre K se $K(x) \subseteq F$ com $[F : K(x)] = 2$ para algum $x \in F \backslash K$ onde o gênero g de F satisfaz $g \geqslant 2$.

Pode mostrar-se que um corpo de funções hiperelíptico é da forma $F = K(x, y)$ (assumindo char$K \neq 2$) onde se satisfaz:

$$y^2 = f(x),$$

sendo $f(x) \in K[x]$ um polinômio livre de quadrados de grau $2g+1$ ou $2g+2$, onde g é o gênero de F. ((STICHTENOTH, 2008), §6.2)

A condição $y^2 = f(x)$ é equivalente a que existe uma curva projetiva plana com equação afim $y^2 - f(x) = 0$, cujo modelo não singular é identificado com o corpo de funções F.

2.3 Resíduo de uma diferencial

Em geral, uma valoração discreta pode ser definida sobre um corpo arbitrário; desta forma, dado um corpo T e uma valoração discreta $v : T \longrightarrow \mathbb{Z} \cup \{\infty\}$, dizemos que (T, v) é um *corpo valorado*.
Se T é um corpo valorado, uma sequência $(x_n)_{n\geqslant 0}$ em T é *convergente* se existir um elemento $x \in T$ satisfazendo:

$$\forall c \in \mathbb{R} \ \ \exists n_0 \in \mathbb{N} \text{ tal que } v(x - x_n) \geqslant c \quad \forall n \geqslant n_0.$$

A sequência $(x_n)_{n\geqslant 0}$ será *de Cauchy* se:

$$\forall c \in \mathbb{R} \ \ \exists n_0 \in \mathbb{N} \text{ tal que } v(x_n - x_m) \geqslant c \quad \forall n, m \geqslant n_0.$$

Um corpo valorado T será denominado *completo* se cada sequência de Cauchy em T é convergente.

Se T é um corpo valorado que não é completo, é possível encontrar uma extensão dele que seja completa, isto é, diremos que $(\hat{T}, \hat{v})$ é um *completamento* de (T, v), se $(\hat{T}, \hat{v})$ satisfaz as condições:

1. $T \subseteq \hat{T}$ e v é a restrição de $\hat{v}$ a T.
2. $\hat{T}$ é completo com respeito à valoração $\hat{v}$.

3. Para cada $z \in \hat{T}$, existe $(x_n)_{n\geqslant 0}$ em T tal que $\lim_{n\to\infty} x_n = z$.

Proposição 2.3.1. *((STICHTENOTH, 2008), §4.2, Proposition 4.2.3) Seja (T, v) um corpo valorado. Então, existe um único completamento $(\hat{T}, \hat{v})$ de (T, v).*

Se $(z_n)_{n\geqslant 0}$ é uma sequência em um corpo valorado T e $S_m = \sum_{i=0}^{m} z_i$, dizemos que a série infinita $\sum_{i=0}^{\infty} z_i$ é convergente se $(S_m)_{m\geqslant 0}$ é convergente, e, nesse caso:

$$\sum_{i=0}^{\infty} z_i := \lim_{n\to\infty} S_n.$$

Se P é um lugar de F/K, o completamento de F com respeito a v_P é denominado *completamento P-ádica* de F e é denotada por $\hat{F}_P$.

Teorema 2.3.1. *((STICHTENOTH, 2008), §4.2, Theorem 4.2.6). Seja $P \in \mathbb{P}_F$ de grau um e t um parâmetro local para P. Então cada $z \in \hat{F}_P$ tem una única representação da forma:*

$$z = \sum_{i=n}^{\infty} a_i t^i,$$

onde $n \in \mathbb{Z}$ e $a_i \in K$. Esta representação é chamada expansão P-ádica em série de potências de z.

Definição 2.3.1. Sejam $P \in \mathbb{P}_F$ (de grau um) e t um parâmetro local de P. Se $z \in F$ tem expansão P-ádica:

$$z = \sum_{i=n}^{\infty} a_i t^i,$$

com $n \in \mathbb{Z}$ e $a_i \in K$, definimos o *resíduo* de z com respeito a P e t por:

$$\mathrm{res}_{P,t}(z) := a_{-1}.$$

Proposição 2.3.2. *((STICHTENOTH, 2008), §4.2, Proposition 4.2.9). Sejam $s, t \in F$ parâmetros locais para P, sendo $P \in \mathbb{P}_F$ de grau um. Então:*

$$res_{P,s}(z) = res_{P,t}(z \cdot \frac{ds}{dt}).$$

Observação 2.3.1. Se t é um parâmetro local de P, K é perfeito e $\mathrm{char}K = p$, então t é uma variável separante. Com efeito, se t é parâmetro local de P, então $v_P(t) = 1$, assim $p \nmid v_P(t)$ para todo primo p e segue do Teorema 1.1.8 que t é uma variável separante.

Sejam $\omega \in \Delta_F$, $P \in \mathbb{P}_F$ e t um parâmetro local de P, escrevemos $\omega = udt$ sendo $u \in F$. Definimos o *resíduo de ω em P* por:

$$\mathrm{res}_P(\omega) := \mathrm{res}_{P,t}(u).$$

Essa definição é independente da escolha do parâmetro local:

Se s é um outro parâmetro local de P, então, como Δ_F é de dimensão um, existe $z \in F$ tal que $\omega = udt = zds$, isto implica que

$$u = z\frac{ds}{dt}$$

e da proposição acima segue que

$$\mathrm{res}_{P,s}(z) = \mathrm{res}_{P,t}\left(z\frac{ds}{dt}\right) = \mathrm{res}_{P,t}(u) = \mathrm{res}_P(\omega)$$

Concluindo o desejado.

3 Extensões de Kummer

Ao longo deste capítulo vamos assumir que K é um corpo de característica $p > 0$.

3.1 Extensões cíclicas e de Kummer

Dizemos que $\gamma \in K$ é uma *raiz n-ésima da unidade* se $\gamma^n = 1$. Se a ordem de γ é n no grupo multiplicativo K^*, então γ é denominado *raiz n-ésima primitiva da unidade*. No caso em que K contém todas as raízes da unidade o polinômio $X^n - 1$ decompõe em fatores lineares em $K[X]$, sempre que $p \nmid n$.

Uma extensão de Galois L/K é denominada *cíclica* se $\mathrm{Gal}(L/K)$ é um grupo cíclico.

Estamos especialmente interessados em alguns tipos de extensões cíclicas, a saber, aquelas extensões cíclicas de grau n de um corpo que contém uma raiz n-ésima primitiva da unidade.

Teorema 3.1.1. *((MORANDI, 1996), II, §9, Theorem 9.5). Suponha que $L \supset K$, K contém uma raiz n-ésima primitiva da unidade e que L/K é cíclica de grau n. Então existe $a \in L$ com $L = K(a)$ e $a^n = b \in K$.*

A recíproca do teorema acima é verdadeira:

Proposição 3.1.1. *((MORANDI, 1996), II, §9, Proposition 9.6). Suponha que $L \supset K$ e que K contém uma raiz n-ésima primitiva da unidade. Seja $L = K(\sqrt[n]{b})$ para algum $b \in K$, então L/K é uma extensão cíclica.*

Se no teorema 3.1.1 temos que $p \nmid n$ e K contém todas as raízes primitivas da unidade, então $b \neq w^d$ para todo $w \in K$ e todo divisor d de n, com $d > 1$.
Uma extensão cíclica L com essas propriedades é denominada *extensão de Kummer*.

A teoria de Extensões cíclicas pode-se estender a corpos de funções algébricos, aqui estamos interessados especificamente nas extensões de corpos de funções F'/K' do corpo de funções F/K onde a extensão de corpos F'/F é uma extensão de Kummer. Vejamos

alguns resultados úteis e alguns exemplos.

Uma extensão F'/K' de um corpo de funções F/K é denominada *Galois* se F'/F é uma extensão de Galois de grau finito.

Proposição 3.1.2. *((STICHTENOTH, 2008), §3.7, corollary 3.7.4) Seja F/K um corpo de funções e $F' = F(y)$ com $y^n = u$, sendo F'/F uma extensão de Kummer. Assuma que existe um lugar $Q \in \mathbb{P}_F$ tal que $\gcd(v_Q(u), n) = 1$. Então,*

$$g' = 1 + n(g-1) + \frac{1}{2}\sum_{P \in \mathbb{P}_F} (n - r_P) grau P, \tag{3.1}$$

onde g' e g são os gêneros de F'/K e F/K respectivamente e $r_P := \gcd(n, v_P(u)) > 0$.

Se F na proposição acima é o corpo de funções racionais, isto é, $F = K(x)$, então a extensão de Kummer $F' = K(x, y)$ está definida pela equação:

$$y^n = a \cdot \prod_{i=1}^{s} p_i(x)^{n_i} \tag{3.2}$$

com $s > 0$, $p_i(x) \in K[x]$, onde os $p_i(x)$ são mônicos irredutíveis diferentes dois a dois, $a \in K$, $n \in \mathbb{Z}$ (ambos não nulos) e $\gcd(n, n_i) = 1$.

3.2 Exemplos

1. Observe que se $\mathrm{char} K \neq 2$ e K é algebricamente fechado, o corpo de funções hiperelíptico $F(x, y)$ dado pela equação

$$y^2 = \prod_{i=1}^{s} p_i(x) = G(x),$$

onde $\mathrm{grau}(p_i(x)) = 1$ e todos os p_i são mônicos diferentes dois a dois, é um caso especial de uma extensão de Kummer sobre $K(x)$, de fato, nesse caso temos que, se $\mathrm{grau}(G(x)) = m$, então o gênero de F está dado por:

$$g' = \begin{cases} (m-1)/2 & se \quad m \equiv 1 \mod 2, \\ (m-2)/2 & se \quad m \equiv 0 \mod 2. \end{cases}$$

Com efeito, se P_i é o zero do polinômio $p_i(x)$ (lembremos que é único via a correspondência dada no capítulo 1) e P_∞ é o polo de x em $K(x)$, então $v_{P_i}(G(x)) = 1$ e $v_{P_\infty}(G(x)) = \text{grau}(1) - \text{grau}(G(x)) = -m$; assim, para cada lugar em $K(x)$ temos:

$$r_{P_i} = \text{mdc}(2,1) = 1 \quad \text{se} \quad i = 1, \ldots, s,$$
$$r_{P\infty} = \text{mdc}(2,m) = \begin{cases} 1 & se \quad m \equiv 1 \mod 2, \\ 2 & se \quad m \equiv 0 \mod 2. \end{cases}$$

Logo, da Proposição 3.1.2 segue:

$$g' = \begin{cases} 1 + 2(g-1) + \dfrac{1}{2}\displaystyle\sum_{i=1}^{m}(2-1)\text{grau}(P_i) + \dfrac{(2-1)}{2}\text{grau}(P_\infty) & se \quad m \equiv 1 \mod 2, \\ 1 + 2(g-1) + \dfrac{1}{2}\displaystyle\sum_{i=1}^{m}(2-1)\text{grau}(P_i) & se \quad m \equiv 0 \mod 2. \end{cases}$$

Lembremos que o gênero do corpo de funções racionais, g, é zero; como $\text{grau}(P_i) = \text{grau}(p_i(x)) = 1$ e $\text{grau}(P_\infty) = 1$, concluímos o requerido.

2. Outro exemplo de extensão de Kummer sobre $K(x)$ é o corpo de funções do *tipo Fermat*, que são os corpos de funções $F = K(x,y)$ definidos pela equação

$$ax^n + by^n = c,$$

com $a, b, c \in K\backslash\{0\}$ e $\text{char}K \nmid n$. Em particular, se $a = b = c = 1$, temos que F é o corpo associado ao modelo não singular da curva projetiva de Fermat $\mathcal{F}_n$.

Considere o corpo de funções $F(y,w)$ representado pela curva de Hurwitz dada pela equação:

$$y^3w + w^3 + y = 0. \tag{3.3}$$

Multiplicando (3.3) por y^6 obtemos:

$$y^7(1 + y^2w) + (y^2w)^3 = 0,$$

fazendo $x = -y^2w$, obtemos

$$y^7 = x^3(1-x)^{-1}. \tag{3.4}$$

De (3.4), segue que para $\text{char}K \neq 7$, o corpo de funções $F(x,y)$ com esta equação é uma extensão tipo Kummer.
Observe que quando $\text{char}K = 7$, a curva dada pela equação (3.3), é singular.

4 Operador de Cartier

Neste capítulo vamos considerar o corpo de funções algébricas de uma variável F/K de gênero g, sendo K um corpo perfeito de característica $p > 0$, algebricamente fechado.

4.1 Definição e propriedades

Seja L um corpo de característica $p > 0$. Seja x um elemento algébrico puramente inseparável sobre L tal que $x \notin L$ e $x^p \in L$, neste caso, o polinômio mínimo $f(X) \in L[X]$ de x é dado por $f(X) = X^p - c$ onde $x^p = c \in L$, assim, $[L(x) : L] = \deg(f(X)) = p$ e temos que

$$L(x) = \{\alpha_0 + \alpha_1 x + \cdots + \alpha_{p-1}x^{p-1} \mid \alpha_i \in L\};$$

logo, para todo $y \in L(x)$ temos que

$$y = y_0 + y_1 x + \cdots + y_{p-1}x^{p-1},$$

onde $y_i \in L$.

Definição 4.1.1. A função

$$\begin{array}{rccc} S_x & : & L(x) & \longrightarrow & L \\ & & y & \longmapsto & y_{p-1} \end{array}$$

que a cada elemento de $L(x)$ atribui o coeficiente da potência x^{p-1} na sua decomposição na base $\{1, x, x^2, \ldots, x^{p-1}\}$ é denominada *traço de Tate*.

Seja $\delta : L(x) \longrightarrow L(x)$ tal que $f(x) \longmapsto f'(x)$ sendo f' a derivada formal do polinômio $f(X) \in L[X]$. Observe que δ está bem definida, de fato, se $h = f - g \in L[X]$ e $h(x) = 0$, temos que $(X^p - c)|h$, pois $X^p - c$ é o polinômio mínimo de x, isso significa que $h'(X) = (X^p - c)q(X)$ e assim, $h'(x) = 0$, portanto, $\delta(f(x)) = \delta(g(x))$. É fácil ver que δ é uma derivação (segue do fato que a derivada formal é uma derivação). Observe que $\delta(x) = 1$, pois nesse caso, o polinômio a derivar é $f(X) = X$, assim, $f'(X) \equiv 1$, isto é, $f'(x) = 1$. Como x é separante para $L(x)/L$ e antes vimos que a derivação com respeito a x é única, então, δ é a derivação com respeito a x. Denotemos $\delta = D_x$. Segue que se $y \in L(x)$ é tal que $y = y_0 + y_1 x + \cdots + y_{p-1}x^{p-1}$, então,

$$D_x(y) = y_1 + 2y_2 x + \cdots + (p-1)y_{p-1}x^{p-2}. \tag{4.1}$$

Lema 4.1.1. *Seja $y \in L(x)$, considere a representação de y na base $\{1, x, \ldots, x^{p-1}\}$ como acima. Então, $y = D_x(z)$ para algum $z \in L(x)$ se e somente se $y_{p-1} = 0$.*

Demonstração. Se $y = D_x(z)$ para algum z, então da equação (4.1) temos que

$$y = z_1 + 2z_2 + \cdots + (p-1)z_{p-1}x^{p-2},$$

segue que o coeficiente de x^{p-1} é zero, isto é, $y_{p-1} = 0$. Reciprocamente, suponha que $y_{p-1} = 0$. Construímos $z \in L(x)$ assim:

$$z = y_0 x + \left(\frac{y_1}{2}\right) x^2 + \cdots + \left(\frac{y_{p-2}}{p-1}\right) x^{p-1}.$$

Segue que $D_x(z) = y$. ■

Neste caso dizemos que y é *integrável*.

Propriedades do traço de Tate

Claramente a função S_x é L-linear.

1. $S_x D_x \equiv 0$.

   Se $y \in L(x)$, então, $y = y_0 + y_1 x + \cdots + y_{p-1}x^{p-1}$ e

   $$D_x(y) = y_1 + 2y_2 x + \cdots + (p-1)y_{p-1}x^{p-2} + 0 \cdot x^{p-1},$$

   segue por definição que $S_x(D_x y) = 0$.

2. $S_x(y^{p-1}D_x y) = (D_x y)^p$.

   Observe que a igualdade acima é equivalente a

   $$S_x(D_x y/y) = (D_x y/y)^p.$$

   Com efeito, $S_x(y^{p-1}D_x y) = S_x(y^p y^{-1} D_x y)$; como $x^p \in L$, então, $y^p \in L$, assim, $S_x(y^{p-1}D_x y) = y^p S_x(D_x y/y)$ e da igualdade no enunciado segue que $S_x(D_x y/y) = (D_x y/y)^p$.
   Agora, vamos mostrar a veracidade do enunciado fazendo uso da equivalência acima. Seja R o conjunto de elementos de $L(x)$ satisfazendo a equação no enunciado, isto é,

   $$R = \{y \in L(x) \ : \ S_x(D_x y/y) = (D_x y/y)^p\}$$

   Vamos mostrar que R é um subcorpo de $L(x)$ que contém x.

- $(R\backslash\{0\}, \cdot)$ é um grupo abeliano.

  Sejam $y, z \in R\backslash\{0\}$.

$$\begin{aligned} S_x(D_x(yz)/yz) &= S_x((yD_xz + zD_xy)/yz) \\ &= S_x(D_xz/z) + S_x(D_xy/y) \\ &= (D_xz/z)^p + (D_xy/y)^p \\ &= \left(\frac{yD_xz + zD_xy}{yz}\right)^p \\ &= (D_x(yz)/yz)^p. \end{aligned}$$

  Assim, $yz \in R$. Observe que 1_L é o elemento unidade de R, pois $D_x(1_L) = 0$, assim, $1_L \in R$ trivialmente; Do fato de ser $L(x)$ um corpo, se satisfazem as demais propriedades de grupo abeliano para $R\backslash\{0\}$.

- Se $y \in R$, então $y + 1 \in R$.

  Seja $w = (y+1)^{p-1}D_xy - y^{p-1}D_xy$, como os dois termos em w são integráveis, então w é integrável e temos que $S_x(w) = 0$ (propriedade 1), assim,

$$\begin{aligned} S_x((y+1)^{p-1}D_xy - y^{p-1}D_xy) = 0 &\Leftrightarrow S_x((y+1)^{p-1}D_xy) - S_x(y^{p-1}D_xy) = 0 \\ &\Leftrightarrow S_x((y+1)^{p-1}D_xy) = S_x(y^{p-1}D_xy) \\ &\Leftrightarrow S_x((y+1)^{p-1}D_xy) = (D_xy)^p \end{aligned}$$

  Como D_x é uma derivação, $D_x(1) = 0$ e temos que $D_x(y+1) = D_xy$, assim,

$$S_x((y+1)^{p-1}D_xy) = (D_x(y+1))^p,$$

  portanto, $y + 1 \in R$.

- $(R, +)$ é um grupo abeliano.

  Sejam $y, z \in R$. Vamos mostrar que $y + z \in R$; podemos supor ambos elementos não nulos (no caso contrário a conclusão é imediata).
  Observe que $y + z = z(yz^{-1} + 1)$; $yz^{-1} \in R$ por ser R um grupo multiplicativo, assim, pelo mostrado acima, $yz^{-1} + 1 \in R$, concluindo que $y + z \in R$. Claramente $0_L \in R$ e novamente, as demais propriedades de grupo são herdadas do corpo $L(x)$.

- $x \in R$.

$D_x x = 1$ implica que $S_x(x^{p-1} D_x x) = S_x(x^{p-1}) = 1$, por outra parte, é evidente que $(D_x x)^p = 1$, assim, $x \in R$.

Lembremos que $L(x)$ é o menor corpo contendo L e x, evidentemente, $L \subseteq R$, assim, $R = L(x)$.

3. Seja $L(x) = L(w)$. Então, $S_w(z) = S_x(z(D_x w)^{1-p})$ para todo $z \in L(x)$. Em termos equivalentes,

$$S_x(zD_x w) = S_w(z)(D_x w)^p.$$

Primeiro, vamos ver que as duas expressões acima são equivalentes. Com efeito, $S_x(z(D_x w)^{1-p}) = (D_x w)^{-p} S_x(zD_x w)$ pois $(D_x w)^p \in L$, assim, $(D_x w)^{-p} S_x(zD_x w) = S_w z$, o que significa $S_x(zD_x w) = (D_x w)^p S_w(z)$.

Como ambos lados da expressão no enunciado acima são lineares com respeito a z (pois, $z = \sum_{i=0}^{p-1} z_i w^i$ onde $z_i \in L$), basta provar a igualdade $S_x(w^i D_x w) = (D_x w)^p S_w(w^i)$ com $i \neq 1$.
Suponha $i < p-1$; observe que $D_x\left(\frac{w^{i+1}}{i+1}\right) = w^i D_x(w)$, isto é, $w^i D_x w$ é integrável, portanto, $S_x(w^i D_x w) = 0$.
Por outra parte, em $L(w)$, $w^i = 0 + 0 \cdot w + \cdots + 1 \cdot w^i + \cdots + 0 \cdot w^{p-1}$, segue que $S_w(w^i) = 0$, obtendo a igualdade desejada.
Suponha $i = p-1$; temos que $S_w(w^{p-1}) = 1$, assim, $(D_x w)^p S_w(w^{p-1}) = (D_x w)^p = S_x(w^{p-1} D_x w)$ (propriedade 2), obtendo a igualdade desejada.

A definição do operador de Cartier pode ser feita a partir da função S_x, mais ainda, sua definição em termos desta função permite mostrar que a ação deste operador sobre uma diferencial é independente da representação desta diferencial em qualquer base do espaço Ω_F, como veremos a continuação.

Do Teorema 1.1.8 (c) sabemos que $K \subseteq F^p \subseteq F$ e $[F : F^p] = p$. Se $x \notin F^p$, então $F^p \subseteq F^p(x) \subseteq F$, assim, $p = [F : F^p(x)][F^p(x) : F^p]$, e temos que $[F : F^p(x)] = 1$ ou $[F^p(x) : F^p] = 1$; como $x \notin F^p$ concluímos que $[F : F^p(x)] = 1$ e $[F^p(x) : F^p] = p$, assim, $F = F^p(x)$.
Por outra parte, do Teorema 1.1.8 (d) sabemos que se $x \notin F^p$, então x é separante, isso significa que podemos considerar a derivação com respeito a x e para todo $\omega \in \Omega_F$ podemos escrever $\omega = ydx$ onde $y \in F$.

Como $[F^p(x) : F^p] = p$, temos que

$$F^p(x) = \{\alpha_0 + \alpha_1 x + \cdots + \alpha_{p-1}x^{p-1} \mid \alpha_i \in F^p\}.$$

Assim, para todo $y \in F = F^p(x)$ temos que

$$y = y_0^p + y_1^p x + \cdots + y_{p-1}^p x^{p-1}, \tag{4.2}$$

onde $y_i \in F$ para todo i com $0 \leqslant i \leqslant p-1$. Logo, para todo $\omega \in \Omega_F$, temos:

$$\omega = ydx = (y_0^p + y_1^p x + \cdots + y_{p-1}^p x^{p-1})dx.$$

Definição 4.1.2. O operador

$$\begin{array}{rcl} \mathcal{C} : \Omega_F & \longrightarrow & \Omega_F \\ ydx & \longmapsto & y_{p-1}dx \end{array}$$

onde y tem a representação dada na equação (4.2), é denominado o *operador de Cartier*.

Em termos do traço de Tate temos que $\mathcal{C}(ydx) = S_x(y)^{1/p}dx$, pois por definição de S_x, temos que $S_x(y) = y_{p-1}^p$.

Proposição 4.1.1. *$\mathcal{C}(\omega)$ é independente da representação de ω, isto é, se $w \notin F^p$ é tal que $ydx = zdw$, então $\mathcal{C}(ydx) = \mathcal{C}(zdw)$.*

Demonstração. Como $x, w \notin F^p$ e $K \subseteq F^p$, temos que x e w são transcendentes sobre K ($K = \tilde{K}$), assim, $F^p(x) = F^p(w)$, e pela propriedade 3 do traço de Tate temos que $S_w(z) = S_x(zD_x w)(D_x w)^{-p}$. Lembremos que para todo $t \in F$, $dt = D_x(t)dx$, em particular, $dw = D_x(w)dx$, assim, $dw/dx = D_x(w)$. Por outra parte, como $ydx = zdw$, temos que $dw/dx = yz^{-1}$, isso significa que $zD_x(w) = y$, logo, $S_w(z) = S_x(y)(D_x w)^{-p}$, assim, $S_w(z)^{1/p} = S_x(y)^{1/p}(D_x w)^{-1}$, que implica que $S_w(z)^{1/p}(D_x w)dx = S_x(y)^{1/p}dx$, isto é, $S_w(z)^{1/p}dw = S_x(y)^{1/p}dx$, concluindo que $\mathcal{C}(ydx) = \mathcal{C}(zdw)$. ■

Propriedades básicas do operador de Cartier

É claro que $\mathcal{C}$ é aditivo.

C1. $\mathcal{C}(z^p\omega) = z \cdot \mathcal{C}(\omega)$ para todo $z \in F$.

Observe que podemos definir a função traço de Tate no corpo F^p, pois $\mathrm{char}F^p = p$, $[F^p(x) : F^p] = p$ e x é puramente inseparável sobre F^p, isso significa que S_x é F^p-linear; segue que se $\omega = ydx$, então,

$$\mathcal{C}(z^p\omega) = S_x(z^p y)^{1/p}dx = (z^p S_x(y))^{1/p}dx = zS_x(y)^{1/p}dx = z \cdot \mathcal{C}(\omega).$$

Da aditividade e propriedade C1 de $\mathcal{C}$ dizemos que $\mathcal{C}$ é $1/p$-linear.

C2. $\mathcal{C}(dz) = 0$ para todo $z \in F$.

Se $z \in F^p$, então z não é separante e assim $dz = 0$, segue que $\mathcal{C}(dz) = 0$.
Se $z \notin F^p$, então z é separante e assim, dz gera Ω_F, isso significa que $dz = 1 \cdot dz$ de onde $1 = 1 + 0 \cdot z + \cdots + 0 \cdot z^{p-1}$, assim, $\mathcal{C}(dz) = 0 \cdot dz = 0$.

C3. $\mathcal{C}(z^{p-1}dz) = dz$ para todo $z \in F$.

Se $z \in F^p$, sabemos que $dz = 0$ e assim, $z^{p-1}dz = 0$, logo a igualdade em C3 se satisfaz.
Suponha que $z \notin F^p$, então, em $F^p(z)$ temos que $z^{p-1} = 0 + 0 \cdot z + \cdots + 1 \cdot z^{p-1}$ e por definição de $\mathcal{C}$ concluímos que $\mathcal{C}(z^{p-1}dz) = 1 \cdot dz = dz$.

C4. $\mathcal{C}\left(\dfrac{dz}{z}\right) = \dfrac{dz}{z}$, para todo $z \in F\backslash\{0\}$.

Suponha que $z \notin F^p$. Da propriedade C3 temos que $\mathcal{C}(z^{p-1}dz) = dz$, mas, $\mathcal{C}(z^{p-1}dz) = \mathcal{C}\left(z^p\dfrac{dz}{z}\right) = z \cdot \mathcal{C}\left(\dfrac{dz}{z}\right)$, isso significa que $z \cdot \mathcal{C}\left(\dfrac{dz}{z}\right) = dz$, portanto, $\mathcal{C}\left(\dfrac{dz}{z}\right) = \dfrac{dz}{z}$.

C5. Para todo inteiro positivo n tal que $p \nmid n$ temos que $\mathcal{C}(z^{n-1}dz) = 0$.

Observe que

$$z^{n-1}dz = \frac{n}{n}z^{n-1}dz = \frac{1}{n}d(z^n) = d\left(\frac{z^n}{n}\right).$$

(aqui, entende-se n/n como $n \cdot 1_K/n \cdot 1_K$). Fazendo $y = \dfrac{z^n}{n}$, temos que $\mathcal{C}(z^{n-1}dz) = \mathcal{C}(dy) = 0$ pela propriedade C2.

Proposição 4.1.2. *Seja $P \in \mathbb{P}_F$. Se ω é regular em P, então $\mathcal{C}(\omega)$ também é regular em P.*

Demonstração. Seja x um parâmetro local para P e suponha que $\omega = ydx$, então, $v_P(\omega) = v_P(y)$. Por hipótese temos que $v_P(\omega) \geqslant 0$, o que significa que $v_P(y) \geqslant 0$, assim, se

$$y = \sum_{i=0}^{p-1} y_i^p x^i,$$

então,

$$v_P\left(\sum_{i=0}^{p-1} y_i^p x^i\right) \geqslant 0.$$

Observe que $v_P(y_i^p x^i) = p \cdot v_P(y_i) + i$ para todo i com $0 \leqslant i \leqslant p-1$.
Vamos ver que se $i \neq j$, então $v_P(y_i^p x^i) \neq v_P(y_j^p x^j)$ para todo par i, j com $0 \leqslant i, j \leqslant p-1$.
Suponha que $i \neq j$ e que $v_P(y_i^p x^i) = v_P(y_j^p x^j)$; sem perda de generalidade suponha $i < j$, então $p \cdot v_P(y_i) + i = p \cdot v_P(y_j) + j$, isto é,

$$p \cdot v_P(y_i y_j^{-1}) = j - i.$$

Como $0 \leqslant i, j \leqslant p-1$, então, $0 \leqslant j - i \leqslant p-1$, o que significa que $p \nmid (j-i)$, assim, a única forma que a equação acima seja válida é que $v_P(y_i y_j^{-1}) = 0$, concluindo que $j - i = 0$, contrariando a hipótese.
Da desigualdade triangular estrita e da hipótese segue que:

$$v_P(y) = v_P\left(\sum_{i=0}^{p-1} y_i^p x^i\right) = \min\{v_P(y_i^p x^i) \mid 0 \leqslant i \leqslant p-1\} \geqslant 0,$$

isso significa que $v_P(y_i^p x^i) \geqslant 0$ para todo i com $1 \leqslant i \leqslant p-1$, em particular, $v_P(y_{p-1}^p x^{p-1}) \geqslant 0$. Segue que $v_P(y_{p-1}) \geqslant 0$, portanto, $v_P(y_{p-1}dx) \geqslant 0$. ■

Observe que se $0 \leqslant i \leqslant p-2$, então $z = y_i^p x^i$ é integrável, pois,

$$z = 0 + 0 \cdot x + \cdots + y_i^p x^i + \cdots + 0 \cdot x^{p-1},$$

assim, para cada i com $0 \leqslant i \leqslant p-2$ existe w_i tal que $y_i^p x^i = D_x(w_i)$. Seja $\omega = ydx$, então,

$$\begin{aligned}
\omega &= (y_0^p + y_1^p x + \cdots + y_{p-1}^p x^{p-1})dx \\
&= y_0^p dx + y_1^p x dx + \cdots + y_{p-2}^p x^{p-2} dx + y_{p-1}^p x^{p-1} dx \\
&= D_x(w_0)dx + D_x(w_1)dx + \cdots + D_x(w_{p-2})dx + (y_{p-1}x)^p x^{-1} dx \\
&= dw_0 + \cdots + dw_{p-2} + (y_{p-1}x)^p dx/x \\
&= d(w_0 + \cdots + w_{p-2}) + (y_{p-1}x)^p dx/x \\
&= df + g^p dx/x,
\end{aligned}$$

onde $f = w_0 + \cdots + w_{p-2}$ e $g = y_{p-1}x$.

Do anterior temos que para todo $\omega \in \Omega_F$ existe uma representação de ω da forma:

$$\omega = df + g^p \frac{dx}{x}, \tag{4.3}$$

com $f, g \in F$.

Se ω tem a representação dada na equação (4.3), então,

$$\begin{aligned}\mathcal{C}(\omega) &= \mathcal{C}\left(df + g^p\frac{dx}{x}\right)\\ &= \mathcal{C}(df) + \mathcal{C}\left(g^p\frac{dx}{x}\right)\\ &= g\cdot\mathcal{C}\left(\frac{dx}{x}\right)\end{aligned}$$

isto é,

$$\mathcal{C}(\omega) = g\frac{dx}{x}. \tag{4.4}$$

A anterior visualização para ω é útil em vários casos, como veremos.

Observe que como consideramos K algebricamente fechado, então todos os lugares de F são de grau um, assim, poderemos considerar as expansões em série de potências dos elementos de F e os seus resíduos.

Proposição 4.1.3. *Seja $P \in \mathbb{P}_F$, então,*

$$res_P(\omega) = (res_P(\omega))^{1/p}.$$

Demonstração. Seja x um parâmetro local para P, da dedução da equação (4.3) temos que é possível representar a forma ω por $\omega = df + g^p x^p\frac{dx}{x}$, desta forma $\mathcal{C}(\omega) = gdx$.
Considerando a expansão em séries de potência de g:

$$g = \sum_{i=m}^{\infty} c_i x^i$$

temos que $\mathrm{res}_P(\mathcal{C}\omega) = c_{-1}$. Por outra parte, $\mathrm{res}_P(\omega) = \mathrm{res}_P(df + g^p x^{p-1}dx) = c_{-1}^p$. ■

Teorema 4.1.1. *Seja $\omega \in \Omega_F$ não nula, então,*

(i) $\mathcal{C}(\omega) = 0$ *se e somente se existe* $z \in F$ *tal que* $\omega = dz$.

(ii) $\mathcal{C}(\omega) = \omega$ *se e somente se existe* $z \in F$ *tal que* $\omega = dz/z$.

Demonstração. Observe que nos dois casos a implicação '($\Leftarrow$)' foi provada em C2 e C4 respectivamente, assim, resta provar a implicação '($\Rightarrow$)' em ambos casos.

(i) Suponha que $\mathcal{C}(\omega) = 0$ e escreva $\omega = df + g^p dx/x$, então, $\mathcal{C}(\omega) = gdx/x$, isso significa que $gdx/x = 0$ e como $x \notin F^p$, temos que tanto x quanto dx são não nulos, portanto $g = 0$ e em (4.3) temos que $\omega = df$.

(ii) A demonstração requer de dois lemas técnicos. Como neste caso nosso interesse não está centrado nas diferenciais logarítmicas, omitiremos a demonstração; o leitor interessado pode consultar (LANG, 1987).

■

4.2 A matriz de Cartier-Manin

Como vimos na Proposição 4.1.2,

$$\mathcal{C}(\Omega_F(0)) \subseteq \Omega_F(0).$$

Seja $\mathcal{B} = \{\omega_1, \omega_2 \ldots, \omega_g\}$ uma base para $\Omega_F(0)$. Considere o operador de Cartier restrito a $\Omega_F(0)$. Se $A_{\mathcal{C}}$ é a matriz associada ao operador de Cartier, sabemos que para toda diferencial $\omega \in \Omega_F(0)$,

$$\mathcal{C}(\omega) = A_{\mathcal{C}} \cdot \omega.$$

Assim, se $\omega = \sum_{i=1}^{g} c_i\omega_i$ e $\mathcal{C}(\omega_i) = \sum_{j=1}^{g} a_{ij}\omega_j$ então

$$\mathcal{C}(\omega) = \sum_{i=1}^{g} c_i^{1/p}\mathcal{C}(\omega_i) = \sum_{i=1}^{g}\sum_{j=1}^{g} c_i^{1/p}a_{ij}\omega_j = \sum_{i,j=1}^{g} b_{ij}\omega_j$$

onde $b_{ij} = c_i^{1/p}a_{ij}$, portanto, $A_{\mathcal{C}} = (b_{ij})$.

Definição 4.2.1. A matriz $A = (b_{ij}^{1/p})$ de tamanho $g \times g$, onde a matriz (b_{ij}) é a matriz associada ao operador de Cartier, é denominada *matriz de Cartier-Manin*.

Exemplo. Seja K um corpo com $\mathrm{char}K = p > 2$. Considere o corpo de funções hiperelíptico $F = K(x, y)$, de gênero g, dado pela equação:

$$y^2 = \prod_{i=1}^{2g+1}(x - a_i) = G(x)$$

onde $a_i \in K$ e $a_i \neq a_j$ para todo $i \neq j$.

Por simplicidade, suponha que x é um elemento separante de F. Das propriedades do operador de Cartier segue que:

$$\mathcal{C}(x^j dx) = \begin{cases} 0 & \text{se} \quad p \nmid j+1 \\ x^{s-1}dx & \text{se} \quad j+1 = ps \end{cases}$$

Com efeito, se $p \nmid j+1$, então, $d\left(\dfrac{x^{j+1}}{j+1}\right) = x^j dx$, assim, se $z = \dfrac{x^{j+1}}{j+1}$, então, $dz = x^j dx$ e $\mathcal{C}(x^j dx) = \mathcal{C}(dz) = 0$. Se $j+1 = ps$, então $x^j dx = x^{j+1}\dfrac{dx}{x} = x^{ps}\dfrac{dx}{x}$, logo,

$$\mathcal{C}(x^j dx) = x^s\mathcal{C}\left(\frac{dx}{x}\right) = x^s\frac{dx}{x} = x^{s-1}dx.$$

Isso mostra que $\mathcal{C}(x^j dx) \neq 0$ se e só se $j \equiv -1 \mod p$.

Neste caso, uma base para $\Omega_F(0)$ está dada por:

$$\mathcal{B} = \left\{ \omega_i = x^{i-1}\frac{dx}{y} \ : \ 1 \leqslant i \leqslant g \right\},$$

Como $y^2 = G(x)$, então,

$$y^{p-1} = G(x)^{\frac{p-1}{2}} = \sum_{j=0}^{N} c_j x^j$$

de onde $N = \dfrac{p-1}{2}(2g+1)$, segue que,

$$\begin{aligned}
\mathcal{C}(\omega_i) &= \mathcal{C}(x^{i-1}y^{-1}dx) = \mathcal{C}(y^{-p}x^{i-1}y^{p-1}dx) = y^{-1}\mathcal{C}(x^{i-1}y^{p-1}dx) \\
&= y^{-1}\mathcal{C}\left(\sum_{j=0}^{N} x^{i+j-1}dx\right) = y^{-1}\sum_{j=0}^{N} c_j^{1/p}\mathcal{C}(x^{i+j-1}dx) \\
&= \sum_{s} c_{p(s+1)-i}^{1/p}\ x^s\frac{dx}{y}.
\end{aligned}$$

Agora, como $0 \leqslant j \leqslant N$, temos que $0 \leqslant p(s+1) - i \leqslant N$, que é equivalente a $0 \leqslant s \leqslant \dfrac{N+i}{p} - 1$, e como $i \leqslant g$, temos que $\dfrac{N+i}{p} - 1 \leqslant g - \dfrac{1}{2} - \dfrac{1}{2p} < g - \dfrac{1}{2}$, segue que $0 \leqslant s \leqslant g-1$; finalmente,

$$\mathcal{C}(\omega_i) = \sum_{s=0}^{g} c_{p(s+1)-i}^{1/p}\ \omega_{s+1}.$$

Assim, a matriz do operador de Cartier neste caso está dada por:

$$A_{\mathcal{C}} = \begin{pmatrix}
c_{p-1}^{1/p} & c_{p-2}^{1/p} & \cdots & c_{p-g}^{1/p} \\
c_{2p-1}^{1/p} & c_{2p-2}^{1/p} & \cdots & c_{2p-g}^{1/p} \\
\vdots & \vdots & & \vdots \\
c_{gp-1}^{1/p} & c_{gp-2}^{1/p} & \cdots & c_{gp-g}^{1/p}
\end{pmatrix}$$

4.3 Ação do operador de Cartier sobre adjuntas canônicas

Seja $y \in F$ tal que $F = K(x, y)$, seja $f \in K[X, Y]$ um polinômio irredutível tal que $f(x, y) = 0$. F é o corpo de funções da curva plana projetiva cuja equação afim é $f(x, y) = 0$.

Seja C a curva projetiva plana cuja equação afim é $f(x, y) = 0$. Assuma que C tem só pontos múltiplos ordinários e que X é um modelo não singular de C cujo morfismo birracional é $q : X \longrightarrow C$. Para cada $Q \in X$, seja $r_Q = m_{q(Q)}(C)$. Definimos o divisor:

$$E = \sum_{Q \in X} (r_Q - 1)Q.$$

E está bem definido, pois qualquer curva irredutível tem finitos pontos múltiplos, assim, $m_P(C) = 1$ para quase todo $P \in C$.

Sejam $P_1, P_2, \ldots, P_l$ os pontos múltiplos de C; para cada j com $1 \leqslant j \leqslant l$, considere o conjunto das pre-imagens por meio de q de P_j, então, para cada Q_{ij} nesse conjunto temos $r_{Q_{ij}} \geqslant 2$, assim,

$$E = \sum_{Q_{ij}} (r_{Q_{ij}} - 1)Q_{ij} \geqslant 0,$$

isto é, E é um divisor efetivo.

Definição 4.3.1. Sejam C e E como acima. Qualquer curva projetiva plana G tal que

$$\mathrm{div}(G) \geqslant E$$

é denominada *adjunta* de C.

Observação 4.3.1. Se C é uma curva não singular, então qualquer curva é uma adjunta de C.
Isso segue do fato que $\mathrm{div}(G)$ é um divisor de grau mn (obs 1.2.4) onde m é o grau da curva G e n é o grau de C, ou seja, $\mathrm{div}(G)$ é um divisor efetivo para toda curva G; portanto, se C é não singular, tem-se $E = 0$ e a condição para ser adjunta de C se satisfaz trivialmente.

Definição 4.3.2. Seja C uma curva projetiva plana de grau $n > 3$ com pontos múltiplos ordinários. As adjuntas de C de grau $n - 3$ são denominadas *adjuntas canônicas* de C.

Proposição 4.3.1. *((HIRSCHFELD; KORCHMáROS; TORRES, 2008), Proposition 6.55). Seja C uma curva projetiva plana com pontos múltiplos ordinários. Existem g adjuntas canônicas de C linearmente independentes.*

O seguinte teorema é muito útil para o calculo de bases das diferenciais regulares sobre uma curva dada; sua demonstração foi dada por David Gorenstein.

Teorema 4.3.1. *((GORENSTEIN, 1952), Theorem 12). Seja C uma curva como acima com equação afim $f(x,y)=0$. $\omega \in \Delta_F$ é regular se e somente se $\omega = \dfrac{h(x,y)}{f_y}dx$, onde $h(x,y)=0$ é a equação afim de uma adjunta canônica H de C.*

Corolário. *Se $\mathcal{X}$ é uma curva plana não singular de grau n com equação afim $f(x,y)=0$, então,*

$$\mathcal{B}' = \left\{ \frac{x^i y^j}{f_y} dx \ : \ 0 \leqslant i+j \leqslant n-3 \right\}$$

é uma base para as diferenciais regulares sobre $\mathcal{X}$.

Demonstração. Como $\mathcal{X}$ é não singular, qualquer curva plana é adjunta de $\mathcal{X}$, em particular, se $\mathcal{H}$ é uma curva de grau formal $n-3$, $\mathcal{H}$ é uma adjunta canônica.
Sabemos que o conjunto das curvas de grau formal $n-3$ (o também denominadas formas) formam um espaço vetorial sobre K e que os monômios de grau $n-3$ formam uma base para este espaço. (Na verdade, este espaço coincide -pode ser identificado- com o espaço projetivo $\mathbb{P}^{n(n-3)/2}$, isso significa que podemos tratar cada uma dessas curvas como um ponto no espaço projetivo $\mathbb{P}^{n(n-3)/2}$).
Um monômio de grau $n-3$ é da forma:

$$x^{s_0} y^{s_1} z^{s_2} \qquad \text{onde} \qquad s_0+s_1+s_2 = n-3;$$

assim, dada uma curva de grau $n-3$, os monômios de sua equação afim ($z=1$) são da forma:

$$x^{s_0} y^{s_1} \qquad \text{onde} \qquad 0 \leqslant s_0+s_1 \leqslant n-3$$

isso significa que qualquer polinômio em duas variáveis de grau menor ou igual a $n-3$ é uma representação afim de uma adjunta canônica. Como o conjunto

$$\mathcal{B} = \{ x^i y^j \ : \ 0 \leqslant i+j \leqslant n-3 \}$$

é uma base para os polinômios de grau menor ou igual a $n-3$, então, $\mathcal{B}$ é uma base para as curvas afim das canônicas adjuntas de $\mathcal{X}$.
Segue do teorema anterior que

$$\mathcal{B}' = \left\{ \frac{x^i y^j}{f_y} dx \ : \ 0 \leqslant i+j \leqslant n-3 \right\}$$

é um conjunto de diferenciais regulares sobre $\mathcal{X}$.
Queremos mostrar que $\mathcal{B}'$ é uma base para as diferenciais regulares.
Observe que para $i=0$ existem $n-2$ possibilidades para y^j de tal forma que $xy^j \in \mathcal{B}'$;

para $i = 1$, existem $n-3$ possibilidades para y^j de tal forma que $xy^j \in \mathcal{B}'$; continuando com esse raciocínio encontramos que há

$$(n-2) + (n-3) + \cdots + 2 + 1 = \frac{1}{2}(n-2)(n-1)$$

elementos em $\mathcal{B}'$. Por outra parte, como $\mathcal{X}$ é não singular, então $g(\mathcal{X}) = (n-1)(n-2)/2$, isto é, $\mathcal{B}'$ tem g elementos; como o espaço das diferenciais regulares sobre $\mathcal{X}$ tem dimensão g, basta mostrar que os elementos de $\mathcal{B}'$ são linearmente independentes, mas, isso segue do fato de ser $\mathcal{B}$ uma base. ■

Sabemos, da Proposição 4.1.2 que o operador de Cartier envia diferenciais regulares em diferenciais regulares, além disso, do Teorema 4.3.1 temos que

$$\mathcal{C}\left(h_0(x,y)\frac{dx}{f_y}\right) = h_1(x,y)\frac{dx}{f_y},$$

onde h_0 e h_1 são equações afim de algum par de adjuntas canônicas da curva. O anterior significa que o operador de Cartier também envia adjuntas canônicas em adjuntas canônicas; o seguinte teorema mostra a forma explícita de h_1 e como ela depende de h_0; a formula dada pelo teorema é de extrema utilidade para os cálculos que faremos no final deste documento, foi provado por Stöhr e Voloch.

Teorema 4.3.2. *((STöHR; VOLOCH, 1987), Theorem 1.1). Seja C uma curva projetiva plana com equação afim $f(x,y) = 0$. Para cada $h \in F = K(x,y)$ tem-se:*

$$\mathcal{C}\left(h\frac{dx}{f_y}\right) = \left(\frac{\partial^{2p-2}}{\partial x^{p-1}\partial y^{p-1}}(f^{p-1}h)\right)^{\frac{1}{p}}\frac{dx}{f_y}. \tag{4.5}$$

Como mencionamos antes, fazendo

$$\nabla = \frac{\partial^{2p-2}}{\partial x^{p-1}\partial y^{p-1}},$$

do teorema acima segue que a ação do operador de Cartier $\mathcal{C}$ sobre as adjuntas canônicas é dada por:

$$h \longmapsto (\nabla(f^{p-1}h))^{\frac{1}{p}}.$$

Para finalizar, vamos analisar a ação do operador ∇ descrito acima sobre os polinômios em $K[X,Y]$.

Seja $G = G(X, Y) \in K[X, Y]$. Vamos considerar o caso em que G é um monômio, isto é,

$$G = a_{i,j} X^i Y^j,$$

onde $a_{ij} \in K$. Vamos calcular ∇G:

Como $i = pq_1 + k_1$ e $j = pq_2 + k_2$ onde $0 \leqslant k_1, k_2 \leqslant p-1$, então vamos considerar dois casos:

(i) $k_1 \neq p-1$ ou $k_2 \neq p-1$.

(ii) $k_1 = k_2 = p-1$.

No primeiro caso, vamos supor que $i \equiv k \mod p$ para $k \neq p-1$. Então,

$$\frac{\partial^{k+1} G}{\partial X^{k+1}} = (i-k)(i-(k-1)) \cdots (i-1) i a_{i,j} X^{i-(k+1)} Y^j = 0,$$

pois $p \mid (i-k)$ e $\mathrm{char} K = p$.
O mesmo raciocínio aplica para o caso em que $j \equiv k \mod p$ para $k \neq p-1$.

Segue que:

$$\nabla G = 0,$$

quando $i \equiv k \mod p$ ou $j \equiv k \mod p$ para $k \neq p-1$.

Para o segundo caso, se $i \equiv p-1 \mod p$ e $j \equiv p-1 \mod p$, então,

$$\frac{\partial^{p-1} G}{\partial X^{p-1}} = \frac{i!}{(i-(p-1))!} a_{i,j} X^{i-(p-1)} Y^j,$$

assim,

$$\frac{\partial^{2p-2} G}{\partial X^{p-1} Y^{p-1}} = b_{ij} a_{i,j} X^{i-(p-1)} Y^{j-(p-1)},$$

onde $b_{ij} = \dfrac{i!j!}{(i-(p-1))!(j-(p-1))!}$ é não nulo.

Como p divide a $i-(p-1)$ e a $j-(p-1)$, existem $r, s \in \mathbb{Z}$ tal que

$$\begin{aligned} i-(p-1) &= pr, \\ j-(p-1) &= ps, \end{aligned}$$

portanto,

$$\nabla G = b_{ij} a_{pr+p-1,ps+p-1} X^{pr} Y^{ps}.$$

Agora consideremos

$$G = \sum_{i,j} a_{i,j} X^i Y^j.$$

Como o operador ∇ é linear, temos que:

$$\nabla G = \sum_{i,j} a_{i,j} \nabla(X^i Y^j);$$

do anterior, sabemos que só "sobrevivem" os termos de G para os quais $i, j \equiv p-1 \mod p$, desta forma,

$$\nabla \left(\sum_{i,j} a_{i,j} X^i Y^j \right) = \sum_{r,s} b_{ij} a_{pr+p-1,ps+p-1} X^{pr} Y^{ps}, \tag{4.6}$$

onde b_{ij} é como acima, $i-(p-1) = pr$ e $j-(p-1) = ps$.

5 O a-número e p-posto de uma curva

Dada uma curva algébrica $\mathcal{X}$ sobre um corpo K de característica $p > 0$ existem dois importantes invariantes birracionais sobre a curva, denominados a-número e p-posto e denotados por $a(\mathcal{X})$ e $\gamma(\mathcal{X})$ respectivamente. Antes de introduzir tais conceitos, vamos caracterizar dois subespaços importantes do espaço das diferenciais regulares.

O seguinte teorema foi demonstrado por Hasse-Witt em (HASSE; WITT, 1936).

Teorema 5.0.1. *Seja V um espaço vetorial finito dimensional sobre um corpo algebricamente fechado K de característica $p > 0$. Seja $f : V \longrightarrow V$ uma aplicação $1/p$-linear. Então existem dois subespaços V° e V^s de V satisfazendo as seguintes condições:*

1. *V^s é gerado por elementos que são invariantes sob f.*
2. *Cada $y \in V^\circ$ é anulado por alguma iteração de f.*
3. *$V = V^s \oplus V^\circ$.*

V^s é denominado o *subespaço semisimples* de V (suprimindo a dependência de f quando o contexto seja claro).

Denotemos por $H^0(\mathcal{X}, \Omega_F)$ o espaço das diferenciais regulares sobre $F = K(\mathcal{X})$, isto é,

$$H^0(\mathcal{X}, \Omega_F) := \Omega_F(0) = \Delta_F(0);$$

Aplicando o teorema anterior ao operador de Cartier e o espaço $H^0(\mathcal{X}, \Omega_F)$, temos:

$$H^0(\mathcal{X}, \Omega_F) = H^0(\mathcal{X}, \Omega_F)^s \oplus H^0(\mathcal{X}, \Omega_F)^\circ,$$

e o seguinte corolário (SUBRAO, 1975)

Corolário. *(i) $H^0(\mathcal{X}, \Omega_F)^s$ é o espaço gerado pelas diferenciais logarítmicas (isso pode-se concluir devido ao Teorema 4.1.1)*

(ii) O p-posto de $\mathcal{X}$ coincide com a dimensão do subespaço semisimples das diferenciais regulares.

Assim, temos a seguinte definição:

Definição 5.0.1. Definimos o p-posto da curva $\mathcal{X}$, $\gamma(\mathcal{X})$, por:

$$\gamma(\mathcal{X}) = \dim_K H^0(\mathcal{X}, \Omega_F)^s.$$

Observação 5.0.1. O corolário acima diz que o p-posto "coincide" com a dimensão do subespaço semisimples das diferenciais regulares, isso é porque o p-posto é definido de forma mais geral, no contexto das variedades abelianas sobre um corpo K; aqui precisamos de uma definição que esteja relacionada com o operador de Cartier, logo, a definição acima é a indicada. A definição geral para o p-posto de uma curva é a seguinte (TAFAZOLIAN, 2008):
Seja A uma variedade abeliana sobre um corpo K de característica $p > 0$, o p-posto de A é a quantidade de cópias de $\mathbb{Z}/p\mathbb{Z}$ no grupo de pontos de ordem p em $A(\bar{K})$. Assim, se define o p-posto de uma curva $\mathcal{X}$, $\gamma(\mathcal{X})$, como sendo o p-posto do seu Jacobiano.

Observe do Teorema 4.1.1 que

$$\ker(\mathcal{C}) = \{\omega \in H^0(\mathcal{X}, \Omega_F) \ : \ \omega \text{ é exata } \}.$$

Definição 5.0.2. Definimos o *a-número* da curva $\mathcal{X}$, $a(\mathcal{X})$, por:

$$a(\mathcal{X}) := \dim_K(\ker \mathcal{C})$$

Como vimos no final da seção 2.1, as diferenciais exatas formam um K-espaço vetorial, assim, o a-número $a(\mathcal{X})$ está bem definido.

Observação 5.0.2. Como acontece com o p-posto, o a-número também é definido em forma geral no contexto das variedades abelianas, como segue (GEER; VLUGT, 1992):
Seja A uma variedade abeliana sobre um corpo K de característica $p > 0$, fazendo:

$$\alpha_p := Spec(K[x]/(x^p))$$

Se define o a-número $a(A)$ de A por:

$$a(A) := \dim_K \hom(\alpha_p, A).$$

Como dito na observação anterior, precisamos relacionar o a-número com o operador de Cartier, assim, a nossa definição é a mais útil nesse contexto.

Lembrando que $\dim_K H^0(\mathcal{X}, \Omega_F) = g(\mathcal{X})$, como $H^0(\mathcal{X}, \Omega_F) = H^0(\mathcal{X}, \Omega_F)^s \oplus H^0(\mathcal{X}, \Omega_F)^\circ$ e $\ker(\mathcal{C}) \subseteq H^0(\mathcal{X}, \Omega_F)^\circ$ (segue do Teorema 5.0.1), temos que

$$0 \leqslant a(\mathcal{X}) + \gamma(\mathcal{X}) \leqslant g(\mathcal{X}).$$

No caso em que $H^0(\mathcal{X}, \Omega_F)$ é representado pela base $\mathcal{B} = \{\omega_1, \ldots, \omega_g\}$ e $A(\mathcal{X}) = (a_{ij})$ é a matriz de Cartier-Manin de $\mathcal{X}$, temos que o a-número $a(\mathcal{X})$ coincide com o co-posto de $A(\mathcal{X})$, isto é,

$$a(\mathcal{X}) = g(\mathcal{X}) - \text{posto}(A(\mathcal{X})),$$

para toda curva $\mathcal{X}$ definida sobre um corpo K de característica $p > 0$.

Devido à $1/p$-linearidade, o operador $\mathcal{C}^n$ é representado com respeito a $\mathcal{B}$ pela matriz:

$$(a_{ij})(a_{ij}^{1/p}) \cdots (a_{ij}^{1/p^{n-1}})$$

elevando os coeficientes das matrizes acima à p^n-ésima potência, obtemos a matriz:

$$(a_{ij}^{p})(a_{ij}^{p^2}) \cdots (a_{ij}^{p^n})$$

Se $n \geqslant g$, então o posto da matriz acima não depende de n, aliás, coincide com o p-posto $\gamma(\mathcal{X})$ da curva.

Observação 5.0.3. o p-posto de uma curva é também conhecido como o invariante de Hasse-Witt da curva.

6 Calculando o a-número de algumas curvas

Neste capitulo vamos considerar um corpo K algebricamente fechado e de característica $p > 0$, onde cada uma das curvas que vamos estudar está definida sobre K e tem gênero g.

6.1 Curvas hiperelípticas

Lembremos que o conjunto:

$$\mathcal{B} = \{\omega_i = \frac{x^{i-1}}{y}dx \ : \ 1 \leqslant i \leqslant g\},$$

é uma base para as diferenciais regulares sobre uma curva hiperelíptica.

Também, como vimos atrás,

$$\mathcal{C}(x^k dx) = \begin{cases} 0 & \text{se} \quad p \nmid (k+1) \\ x^{s-1}dx & \text{se} \quad k+1 = ps \end{cases}$$

A continuação vamos calcular o a-número de infinitas curvas pertencentes a duas famílias de curvas hiperelípticas.

6.1.1 Curva $\mathbf{y^2 = x^m + 1}$

Seja $\mathcal{X}$ a curva hiperelíptica com equação afim $y^2 - x^m - 1 = 0$.

Proposição 6.1.1. *O posto do operador de Cartier sobre a curva hiperelíptica $\mathcal{X}$ corresponde à quantidade de $i's$ com $1 \leqslant i \leqslant g$ (ou, equivalentemente, de $\omega_i's$ da base $\mathcal{B}$) tais que a equação módulo p:*

$$i + mj \equiv 0 \tag{6.1}$$

tem solução j, com $0 \leqslant j \leqslant \dfrac{p-1}{2}$.

Demonstração. Temos que

$$\mathcal{C}(\omega_i) = \mathcal{C}(x^{i-1}y^{-1}dx) = \mathcal{C}(x^{i-1}y^{-1}y^p y^{-p}dx) = y^{-1}\mathcal{C}(x^{i-1}y^{p-1}dx).$$

Como $y^2 = x^m + 1$, então,

$$y^{p-1} = (y^2)^{\frac{p-1}{2}} = (x^m + 1)^{\frac{p-1}{2}}$$

onde:

$$(x^m+1)^{\frac{p-1}{2}} = \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} x^{mj}$$

Assim,

$$\begin{aligned} \mathcal{C}(\omega_i) &= y^{-1}\mathcal{C}\left(\sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} x^{mj+i-1}dx\right) \\ &= y^{-1}\sum_j a_j^{1/p}\mathcal{C}(x^{mj+i-1}dx) \end{aligned}$$

onde $a_j = \binom{\frac{p-1}{2}}{j}$.

Se $\mathcal{C}(\omega_i) = 0$, então $\omega_i \in \ker(\mathcal{C})$, assim, se $\mathcal{C}(\omega_i) \neq 0$, existe pelo menos um j com $0 \leqslant j \leqslant \dfrac{p-1}{2}$ tal que $\mathcal{C}(x^{mj+i-1}dx) \neq 0$ e sabemos que isso é possível só se

$$mj + i - 1 \equiv -1 \mod p$$

isto é,

$$mj + i \equiv 0 \mod p$$

O anterior não é suficiente, pois poderia acontecer que alguma das diferenciais $\mathcal{C}(\omega_r)$ seja linearmente dependente das demais diferenciais $\mathcal{C}(\omega_i)$ obtendo nesse caso que o posto da matriz do operador de Cartier é estritamente menor do previsto. Vamos mostrar então que para cada par $\omega_i \neq \omega_r$ onde ambas, $\mathcal{C}(\omega_i)$ e $\mathcal{C}(\omega_r)$, são diferenciais não nulas, tem-se que estas ultimas são linearmente independentes.
Suponha que $\mathcal{C}(\omega_i) = \lambda\mathcal{C}(\omega_r)$ para algum $\lambda \in K$ não nulo, então, para cada j com $0 \leqslant j \leqslant \dfrac{p-1}{2}$ existe j_0 com as mesmas condições tal que

$$x^{mj+i-1} = x^{mj_0+r-1}$$

de onde, $mj + i - 1 = mj_0 + r - 1$, isto é,

$$mj + i = mj_0 + r \tag{6.2}$$

Sem perda de generalidade podemos supor $r > i$, assim, em (6.2) temos que $r-i = m(j-j_0)$. Observe que $g < m$ sem importar se m é par ou ímpar, além disso, $r - i \leqslant g$, assim, se $j - j_0 > 0$ teríamos que $r - i \geqslant m > g$, por outra parte, se $j - j_0 < 0$, então $r - i < 0$ contrariando o suposto inicial $r > i$; logo, a única opção possível é $j = j_0$, mas, nesse caso, teríamos $r = i$. O anterior implica que para cada j com $0 \leqslant j \leqslant \dfrac{p-1}{2}$ não existe uma solução j_0 tal que a igualdade em (6.2) seja válida, portanto, $\mathcal{C}(\omega_i)$ e $\mathcal{C}(\omega_r)$ são linearmente independentes. ■

Seja $A_m := A(\mathcal{X}) = (a_{ij})$ onde $(a_{ij}^{1/p})$ é a matriz de Cartier-Manin da curva $\mathcal{X}$.

Teorema 6.1.1. *Seja $m = sp + 1$, com $s \geqslant 1$, então,*

1. *Se $s = 2k + 1$, (equivalentemente, se m é par) então o a-número da curva $\mathcal{X}$ é:*

$$a(\mathcal{X}) = \frac{1}{2}(k + 1)(p - 1).$$

2. *Se $s = 2k$, (equivalentemente, se m é ímpar) então o a-número da curva $\mathcal{X}$ é:*

$$a(\mathcal{X}) = \frac{1}{2}k(p - 1).$$

Demonstração. Observe que se j é uma solução da equação (6.1), então existe h com $\frac{p-1}{2} \leqslant h \leqslant p - 1$ tal que $m(p - 1 - h) + i \equiv 0 \mod p$, assim, encontrar as soluções j da equação (6.1) é equivalente a encontrar as soluções h da equação módulo p:

$$m(p - 1 - h) + i \equiv 0 \tag{6.3}$$

onde $\frac{p-1}{2} \leqslant h \leqslant p - 1$. Como neste caso $m = sp + 1$, a equação (6.3) é equivalente à equação módulo p:

$$i \equiv h + 1. \tag{6.4}$$

É importante observar que esta equação não depende da variável k.

Se $h \geqslant 0$ é uma solução da equação acima para $1 \leqslant i \leqslant g$, então existe $\ell \in \mathbb{Z}$ tal que:

$$i = p\ell + h + 1$$

Como i e h são estritamente positivos, então $\ell \geqslant 0$. Assim, para o nosso propósito, é suficiente considerar $\ell \in \mathbb{Z}_0^+$.

Para a primeira parte do teorema, vamos mostrar por indução sobre k que

$$\text{posto}(A_m) = \frac{1}{2}k(p + 1),$$

via a proposição 6.1.1. Como neste caso m é par, então $g = (m - 2)/2$.

- Caso $k = 0$: Neste caso temos que $m = p + 1$ e $g = \frac{1}{2}(p - 1)$. Supondo ℓ como antes, se $1 \leqslant p\ell + h + 1 \leqslant \frac{1}{2}(p - 1)$, então, quando $h \geqslant 0$, $p\ell + h + 1 > p\ell$, assim, se $\ell > 0$, $p\ell + h + 1 > p > g$, e como procuramos soluções h para (6.4) com $0 < \frac{1}{2}(p - 1) \leqslant h \leqslant p - 1$, a única opção possível é $l = 0$.
  Se $\ell = 0$, então,

$$i = h + 1,$$

assim, $1 \leqslant i \leqslant g$ implica $1 \leqslant h+1 \leqslant \frac{1}{2}(p-1)$, isto é, $0 \leqslant h \leqslant \frac{1}{2}(p-1)-1$ e essas soluções não satisfazem a condição da proposição 6.1.1, portanto, $\text{posto}(A_{p+1}) = 0$.

- Caso $k = 1$: Aqui, $m = 3p+1$ e $g = \frac{1}{2}(3p-1)$. Como a equação (6.4) não depende de k, as soluções encontradas para valores menores de k são as mesmas (neste caso, não há), assim, é suficiente achar as possíveis soluções para $\frac{1}{2}(p+1) \leqslant i \leqslant \frac{1}{2}(3p-1)$, isto é, estamos interessados nas soluções h com $\frac{1}{2}(p-1) \leqslant h \leqslant p-1$ para as quais:

$$\frac{1}{2}(p+1) \leqslant p\ell + (h+1) \leqslant \frac{1}{2}(3p-1), \tag{6.5}$$

onde $\ell \in \mathbb{Z}_0^+$. Como $h+1 > 0$, então,

$$p\ell < p\ell + (h+1) \leqslant \frac{1}{2}(3p-1) < \frac{3}{2}p$$

assim, $0 \leqslant l < 3/2$, isto é, os possíveis valores para ℓ são: $\ell = 0$ e $\ell = 1$.

Se $\ell = 0$, em (6.5) tem-se:

$$\frac{1}{2}(p-1) \leqslant h \leqslant \frac{3}{2}(p-1)$$

Assim, as possíveis soluções satisfazendo as condições requeridas são:

$$\left\{ h = \frac{p-1}{2} + r \ : \ 0 \leqslant r \leqslant \frac{p-1}{2} \right\}.$$

Se $\ell = 1$ em (6.5) tem-se:

$$-\frac{1}{2}(p+1) \leqslant h \leqslant \frac{1}{2}(p-1)-1,$$

portanto, para este caso não há soluções com as condições procuradas.

Segue que para $\frac{1}{2}(p+1) \leqslant i \leqslant \frac{1}{2}(3p-1)$, a equação (6.4) tem $\frac{p+1}{2}$ soluções h; como a cada solução corresponde um único i, segue da proposição 6.1.1 que:

$$\text{posto}(A_{3p+1}) = \frac{1}{2}(p+1)$$

- Caso geral: Suponha que $k \geqslant 2$ e

$$\text{posto}(A_{(2k-1)p+1}) = \frac{(k-1)(p+1)}{2}.$$

Pelo mesmo argumento exposto no caso anterior, é suficiente achar as soluções da equação (6.4) para $\frac{(2k-1)p+1}{2} \leqslant i \leqslant \frac{(2k+1)p-1}{2}$, pois, a quantidade de soluções quando $1 \leqslant i \leqslant \frac{(2k-1)p-1}{2}$ está consignada na hipótese indutiva acima.

O anterior significa que estamos interessados nas soluções h com $\frac{1}{2}(p-1) \leqslant h \leqslant p-1$ para as quais:

$$\frac{(2k-1)p+1}{2} \leqslant p\ell + (h+1) \leqslant \frac{(2k+1)p-1}{2}, \tag{6.6}$$

onde $\ell \in \mathbb{Z}_0^+$. Como $h+1 > 0$, então,

$$p\ell < p\ell + (h+1) \leqslant \frac{(2k+1)p-1}{2} < \frac{(2k+1)p}{2},$$

logo, $\ell < \frac{2k+1}{2}$. Por outra parte,

$$\frac{2k-1}{2}p < \frac{(2k-1)p+1}{2} \leqslant p\ell + (h+1),$$

de onde,

$$\frac{2k-1}{2}p - (h+1) < p\ell,$$

assim, como $h+1 \leqslant p$, então, $\frac{2k-3}{2}p = \frac{2k-1}{2}p - p < p\ell$, portanto, $\ell > \frac{2k-3}{2}$. Como $\frac{2k-3}{2}$ e $\frac{2k-1}{2}$ não são inteiros, concluímos que $k-1 \leqslant \ell \leqslant k$, isto é, $\ell \in \{k-1, k\}$.

Se $\ell = k-1$, em (6.6) tem-se:

$$\frac{1}{2}(p-1) \leqslant h \leqslant \frac{3}{2}(p-1),$$

como $p-1 < \frac{3}{2}(p-1)$, h pode tomar todos os valores entre $\frac{1}{2}(p-1)$ e $p-1$, isso significa que para este caso há $\frac{1}{2}(p+1)$ soluções da equação inicial.

Se $\ell = k$, em (6.6) tem-se:

$$-\frac{1}{2}(p+1) \leqslant h \leqslant \frac{1}{2}(p-1) - 1,$$

portanto, para este caso não há soluções com as condições procuradas.

Segue que para $\frac{(2k-1)p+1}{2} \leqslant i \leqslant \frac{(2k+1)p-1}{2}$, a equação (6.4) tem $\frac{p+1}{2}$ soluções h; da hipótese indutiva e da proposição 6.1.1 concluímos que:

$$\operatorname{posto}(A_{(2k+1)p+1}) = \frac{(k-1)(p+1)}{2} + \frac{1}{2}(p+1) = \frac{k(p+1)}{2}.$$

Como $a(\mathcal{X}) = g(\mathcal{X}) - \operatorname{posto}(A_m)$, então,

$$a(\mathcal{X}) = \frac{(2k+1)p-1}{2} - \frac{k(p+1)}{2} = \frac{(k+1)(p-1)}{2}.$$

Para a segunda parte do teorema, vamos mostrar por indução sobre k que novamente

$$\text{posto}(A_m) = \frac{1}{2}k(p+1),$$

via a proposição 6.1.1. Como neste caso m é ímpar, então $g = (m-1)/2$.

- Caso $k = 1$: para $k = 1$ temos que $m = 2p+1$ e $g = p$. Lembremos que buscamos as soluções h de (6.4) com $\frac{1}{2}(p-1) \leqslant h \leqslant p-1$ para as quais $1 \leqslant i \leqslant g$, assim, se $\ell \in \mathbb{Z}_0^+$ é tal que $i = p\ell + (h+1)$, então,

  $$1 \leqslant p\ell + (h+1) \leqslant p.$$

  Se $h+1 > 0$, para que a desigualdade acima seja válida, a única opção possível é $\ell = 0$, o que implica $0 \leqslant h \leqslant p-1$, logo, para este caso, há $\frac{1}{2}(p+1)$ soluções h da equação inicial, isto é,

  $$\text{posto}(A_{2p+1}) = \frac{1}{2}(p+1).$$

- Caso $k = 2$: Aqui, $m = 4p+1$ e $g = 2p$; sob o mesmo argumento usado na primeira parte do teorema, vemos que é suficiente buscar as soluções da equação (6.4) para as que $p+1 \leqslant i \leqslant 2p$, isto é,

  $$p+1 \leqslant p\ell + (h+1) \leqslant 2p. \tag{6.7}$$

  Se $h+1 > 0$, temos que $p\ell < p\ell + (h+1) < 2p$, assim, $\ell < 2$, portanto, $\ell \in \{0, 1\}$.

  Se $\ell = 0$, segue de (6.7) que $p \leqslant h \leqslant 2p-1$, logo, neste caso não há soluções com as condições procuradas.

  Se $\ell = 1$, segue de (6.7) que

  $$0 \leqslant h \leqslant p-1,$$

  Obtendo, como no caso anterior, $\frac{1}{2}(p+1)$ soluções h da equação inicial; logo,

  $$\text{posto}(A_{4p+1}) = \frac{1}{2}(p+1) + \frac{1}{2}(p+1) = p+1.$$

- Caso geral: Suponha que $k \geqslant 3$ e

  $$\text{posto}(A_{2(k-1)p+1}) = \frac{1}{2}(k-1)(p+1).$$

  Observe que se $m = 2kp+1$, então $g = kp$. Pela hipótese indutiva, basta encontrar as soluções h de (6.4) para $(k-1)p+1 \leqslant i \leqslant kp$, isto é, queremos saber quantos valores h com $\frac{1}{2}(p-1) \leqslant h \leqslant p-1$ satisfazem:

  $$(k-1)p+1 \leqslant p\ell + (h+1) \leqslant kp. \tag{6.8}$$

Se $h+1>0$, então,

$$p\ell < p\ell + (h+1) \leqslant kp,$$

segue que $\ell < k$. Por outra parte,

$$(k-1)p < (k-1)p + 1 \leqslant p\ell + (h+1),$$

de onde,

$$(k-1)p - (h+1) < p\ell,$$

assim, como $h+1 \leqslant p$, então, $(k-2)p = (k-1)p - p < p\ell$, portanto, $\ell > k-2$, o que significa que $\ell = k-1$.
Com o anterior, segue de (6.8) que $0 \leqslant h \leqslant p-1$, obtendo, como no caso anterior, $\frac{1}{2}(p+1)$ soluções. Finalmente, do anterior e a hipótese indutiva concluímos que:

$$\text{posto}(A_{2kp+1}) = \frac{1}{2}(k-1)(p+1) + \frac{1}{2}(p+1) = \frac{1}{2}k(p+1).$$

Como $a(\mathcal{X}) = g(\mathcal{X}) - \text{posto}(A_m)$, então,

$$a(\mathcal{X}) = kp - \frac{k(p+1)}{2} = \frac{k(p-1)}{2}.$$

■

6.1.2 Curva $\mathbf{y^2 = x^m + x}$

Agora seja $\mathcal{X}$ a curva hiperelíptica com equação afim $y^2 - x^m - x = 0$.

Proposição 6.1.2. *O posto do operador de Cartier sobre a curva hiperelíptica $\mathcal{X}$ corresponde à quantidade de $i's$ com $1 \leqslant i \leqslant g$ (ou, equivalentemente, de $\omega_i's$ da base $\mathcal{B}$) tais que a equação módulo p:*

$$(m-1)j + i \equiv 0 \tag{6.9}$$

tem solução j, com $0 \leqslant j \leqslant \frac{p-1}{2}$.

Demonstração. Análogo ao feito na proposição 6.1.1 vemos que se $\omega_i \in \mathcal{B}$, então $\mathcal{C}(\omega_i) = y^{-1}\mathcal{C}(x^{i-1}y^{p-1}dx)$ onde,

$$y^{p-1} = x^{\frac{p-1}{2}}(x^m+1)^{\frac{p-1}{2}},$$

portanto,

$$\mathcal{C}(\omega_i) = y^{-1}\sum_{j=0}^{\frac{p-1}{2}} b_j \mathcal{C}(x^{(m-1)j+i-1}dx).$$

Se $\mathcal{C}(\omega_i) \neq 0$, existe pelo menos um j com $0 \leqslant j \leqslant \frac{p-1}{2}$ tal que $\mathcal{C}(x^{(m-1)j+i-1}dx) \neq 0$ e sabemos que isso é possível só se

$$(m-1)j + i - 1 \equiv -1 \mod p$$

isto é,

$$(m-1)j + i \equiv 0 \mod p$$

Falta mostrar que se ω_i e ω_r são elementos distintos de $\mathcal{B}$, para os que $\mathcal{C}(\omega_i)$ e $\mathcal{C}(\omega_r)$ são diferenciais não nulas, então estas ultimas são linearmente independentes.
Suponha que existe $\lambda \in K$ não nulo tal que $\mathcal{C}(\omega_i) = \lambda\mathcal{C}(\omega_r)$, então, para cada j com $0 \leqslant j \leqslant \dfrac{p-1}{2}$ existe j_0 com as mesmas condições tal que

$$x^{(m-1)j+i-1} = x^{(m-1)j_0+r-1}$$

de onde, $(m-1)j + i - 1 = (m-1)j_0 + r - 1$, isto é,

$$(m-1)j + i = (m-1)j_0 + r \tag{6.10}$$

Como $m > 1$, um argumento idêntico ao da proposição 6.1.1 mostra que não é possível encontrar j_0 que valide a equação (6.10) para cada j, portanto, $\mathcal{C}(\omega_i)$ e $\mathcal{C}(\omega_r)$ são linearmente independentes. ■

Seja $A_m := A(\mathcal{X}) = (a_{ij})$ onde $(a_{ij}^{1/p})$ é a matriz de Cartier-Manin da curva $\mathcal{X}$.

Teorema 6.1.2. *Se $m = sp$ com $s \geqslant 1$, então o a-número da curva $\mathcal{X}$ é:*

$$a(\mathcal{X}) = \frac{1}{2}(k+1)(p-1).$$

Demonstração. Vamos mostrar o teorema quando m é par, isto é, quando $s = 2k$ com $k \geqslant 1$, a prova do caso m ímpar é completamente análoga.

Observe que para $m = sp$ a equação (6.9) na proposição anterior é equivalente à equação módulo p:

$$i \equiv j \tag{6.11}$$

Se j é uma solução desta equação, então existe $\ell \in \mathbb{Z}$ tal que:

$$i = p\ell + j$$

para $i \geqslant 0$, tem-se $j \geqslant p(-\ell)$, assim, se $\ell < 0$, então $j \geqslant p$; como buscamos as soluções com $0 \leqslant j \leqslant \dfrac{1}{2}(p-1)$, então podemos considerar $\ell \in \mathbb{Z}_0^+$.

- Caso $k = 1$: Aqui, $m = 2p$ e $g = p - 1$. Procuramos as soluções j da equação (6.11) com $0 \leqslant j \leqslant \dfrac{p-1}{2}$ para as quais $1 \leqslant i \leqslant g$, assim, se ℓ é como acima, queremos que

$$1 \leqslant p\ell + j \leqslant p - 1$$

Como $j \geqslant 0$, temos que

$$p\ell \leqslant p\ell + j \leqslant p - 1 < p$$

assim, $\ell < 1$, isso significa que $\ell = 0$.
Se $\ell = 0$, temos que $i = j$, logo $\mathcal{C}(x^{(m-1)i+i-1}) \neq 0$, isto é, $\mathcal{C}(x^{mi-1}) \neq 0$, que contradiz a propriedade C5 do operador de Cartier $\mathcal{C}$. Concluímos que não existem soluções da equação na proposição 6.1.2 com as condições requeridas, assim, a mesma proposição permite afirmar que $\text{posto}(A_{2p}) = 0$.

- Caso $k = 2$: para este caso, $m = 4p$ e $g = 2p - 1$. Como a equação que estamos analisando não depende da variável k, as soluções encontradas atrás continuam sendo soluções para este caso, assim, é suficiente encontrar a quantidade de soluções satisfazendo:

$$p \leqslant p\ell + j \leqslant 2p - 1; \tag{6.12}$$

Como $j \geqslant 0$, temos que $p\ell < 2p$, assim, $\ell < 2$.
Observe que se $\ell = 0$, de acordo com (6.12) as soluções j satisfazem $p \leqslant j \leqslant 2p - 1$, portanto não são de nosso inteires. Falta analisar que acontece quando $\ell = 1$; neste caso, em (6.12) teríamos:

$$0 \leqslant j \leqslant p - 1,$$

obtendo $\frac{1}{2}(p + 1)$ possíveis soluções j.

- Caso geral: Suponha que $k \geqslant 3$ e que

$$\text{posto}(A_{2(k-1)p}) = \frac{1}{2}(k - 2)(p + 1)$$

pelo argumento dado no caso anterior, é suficiente encontrar as soluções de (6.11) para as quais:

$$(k - 1)p \leqslant p\ell + j \leqslant kp - 1; \tag{6.13}$$

para $j \geqslant 0$, tem-se $p\ell \leqslant p\ell + j < kp$, assim, $\ell < k$.
Observe que se $\ell < k - 1$, então $k - 1 - \ell > 0$ e de (6.13) segue que

$$p < (k - 1 - \ell)p \leqslant j \leqslant (k - \ell)p - 1$$

o que significa que podemos descartar esses valores de ℓ, logo, $\ell = k - 1$ é a única opção possível; de acordo com (6.13), quando $\ell = k-1$, temos $0 \leqslant j \leqslant p-1$, obtendo $\frac{1}{2}(p + 1)$ possíveis soluções j com as condições desejadas.
Da hipótese indutiva segue que:

$$\text{posto}(A_m) = \frac{1}{2}(k - 2)(p + 1) + \frac{1}{2}(p + 1) = \frac{1}{2}(k - 1)(p + 1).$$

Como $a(\mathcal{X}) = g(\mathcal{X}) - \text{posto}(A_m)$ e $g = \frac{1}{2}(m - 2)$, então,

$$a(\mathcal{X}) = (kp - 1) - \frac{(k - 1)(p + 1)}{2} = \frac{(k + 1)(p - 1)}{2}.$$

■

6.2 Curva de Fermat

Como foi demonstrado no corolário 4.3, para as curvas planas não singulares com equação afim $f(x, y) = 0$, o conjunto:

$$\mathcal{B}' = \left\{ \frac{x^i y^j}{f_y} dx \ : \ 0 \leqslant i + j \leqslant n - 3 \right\}$$

é uma base para as diferenciais regulares sobre a curva.

Como vimos no primeiro capitulo, $\mathcal{F}_n$ é uma curva não singular com equação afim:

$$F : X^n + Y^n - 1 = 0,$$

assim, o conjunto

$$\mathcal{B}_F = \left\{ \frac{x^i y^j}{n y^{n-1}} dx \ : \ 0 \leqslant i + j \leqslant n - 3 \right\}$$

é uma base para as diferenciais regulares sobre $\mathcal{F}_n$.

Proposição 6.2.1. *O posto do operador de Cartier sobre a curva de Fermat $\mathcal{F}_n$ corresponde ao número de pares (i, j) com $i + j \leqslant n - 3$ tal que o sistema de congruências módulo p:*

$$\begin{cases} n(p - 1 - h) + i \equiv p - 1 \\ nk + j \equiv p - 1 \end{cases} \tag{6.14}$$

tem uma solução (h, k) para $0 \leqslant h \leqslant p - 1$ e $0 \leqslant k \leqslant h$.

Demonstração. Seja $\omega_{i,j}$ um elemento da base $\mathcal{B}_F$. Suponha que $\mathcal{C}(\omega_{i,j}) \neq 0$.
Como $\omega_{i,j} = (h/F_y)dx$ onde $h = x^i y^j$, então, $\mathcal{C}(\omega_{i,j}) = \nabla(F^{p-1}h)^{1/p} dx/F_y$ e segue que

$$\mathcal{C}(\omega_{i,j}) \neq 0 \ \Leftrightarrow \ \nabla(F^{p-1}h) \neq 0. \qquad (*)$$

Temos que $F^{p-1}h = (x^n + y^n - 1)^{p-1} x^i y^j$, onde:

$$\begin{aligned} (x^n + y^n - 1)^{p-1} &= \sum_{h=0}^{p-1} \binom{p-1}{h} x^{n(p-1-h)} (y^n - 1)^h \\ &= \sum_{h=0}^{p-1} \sum_{k=0}^{h} \binom{p-1}{h} \binom{h}{k} (-1)^{h-k} x^{n(p-1-h)} y^{nk} \end{aligned}$$

Assim,

$$\nabla((x^n + y^n - 1)^{p-1} x^i y^j) = \sum_{i,j} b_{i,j} x^{n(p-1-h)+i-(p-1)} y^{nk+j-(p-1)}$$

logo, de $(*)$ segue que existem $s, r \in \mathbb{Z}$ tal que

$$\begin{cases} n(p-1-h)+i-(p-1) = ps \\ nk+j-(p-1) = pr \end{cases}$$

que é equivalente a

$$\begin{cases} n(p-1-h)+i \equiv p-1 \mod p \\ nk+j \equiv p-1 \mod p \end{cases}$$

onde $0 \leqslant h \leqslant p-1$ e $0 \leqslant k \leqslant h$.

Falta provar que se $(i,j) \neq (i_0,j_0)$ são tais que $\mathcal{C}(\omega_{i,j}) \neq 0$ e $\mathcal{C}(\omega_{i_0,j_0}) \neq 0$, então, $\mathcal{C}(\omega_{i,j}) \neq \lambda \mathcal{C}(\omega_{i_0,j_0})$ para todo $\lambda \in K\backslash\{0\}$.

Suponha que $\mathcal{C}(\omega_{i,j}) = \lambda \mathcal{C}(\omega_{i_0,j_0})$ para algum $\lambda \in K$ não nulo. Como ambos $\mathcal{C}(\omega_{i,j})$ e $\mathcal{C}(\omega_{i_0,j_0})$ são não nulas, existem soluções (h,k) e (h_0,k_0) do sistema de congruências acima, para (i,j) e (i_0,j_0) respectivamente. Por outra parte, como $\mathcal{C}(\omega_{i,j}) = \nabla(F^{p-1}x^iy^j)^{1/p}dx/F_y = \lambda\nabla(F^{p-1}x^{i_0}y^{j_0})^{1/p}dx/F_y$, então,

$$\nabla(F^{p-1}x^iy^j)dx/F_y = \lambda^p\nabla(F^{p-1}x^{i_0}y^{j_0})dx/F_y$$

isso significa que

$$x^{n(p-1-h)+i-(p-1)} = x^{n(p-1-h_0)+i_0-(p-1)} \quad \text{e} \quad y^{nk+j-(p-1)} = y^{n_0k+j_0-(p-1)}$$

portanto,

$$\begin{cases} i-nh = i_0-nh_0 & (1) \\ nk+j = nk_0+j_0 & (2) \end{cases}$$

como $(i,j) \neq (i_0,j_0)$, existem três possibilidades:

(I) $i = i_0$ e $j \neq j_0$.

(II) $i \neq i_0$ e $j = j_0$.

(III) $i \neq i_0$ e $j \neq j_0$.

Para (I), temos que $h \neq h_0$, assim, podemos supor $h > h_0$; na equação (1) temos que $i - i_0 = n(h-h_0) \geqslant n$, mas sabemos que $i - i_0 \leqslant n-3$.
Para (II), temos que $k \neq k_0$; supondo $k > k_0$, da equação (2) segue que $j - j_0 = n(k-k_0) \geqslant n$ e sabemos que $j - j_0 \leqslant n-3$.
Para (III), suponha $h > h_0$; da equação (2) segue que $k - k_0 < 0$. Somando as equações (1) e (2) obtemos:

$$i+j = n(h-h_0)+n(k_0-k)+i_0+j_0$$

onde $h - h_0 > 0$, $k_0 - k > 0$ e $i_0 + j_0 \geqslant 0$, assim, $i + j \geqslant 2n$ e sabemos que $i + j \leqslant n - 3$. Concluímos que não existem duplas (h_0, k_0) com $0 \leqslant k_0 \leqslant h_0 \leqslant p - 1$ satisfazendo as equações (1) e (2), assim, $\mathcal{C}(\omega_{i,j})$ e $\mathcal{C}(\omega_{i_0,j_0})$ são linearmente independentes, concluindo que a cada solução (h, k) do sistema no enunciado corresponde uma única dupla (i, j) com $i + j \leqslant n - 3$, isto prova a proposição. ■

Teorema 6.2.1. *Se $n = sp + 1$, com $s \geqslant 1$, o a- número da curva de Fermat é:*

$$a(\mathcal{F}_n) = \frac{1}{4}s(s+1)p(p-1).$$

Demonstração. Seja A_{sp+1} a p-ésima potência da matriz de Cartier-Manin da curva de Fermat $\mathcal{F}_{sp+1}$. Fazendo uso da proposição 6.2.1, vamos mostrar que

$$\text{posto}(A_{sp+1}) = \frac{1}{4}s(s-1)p(p+1)$$

por meio da indução sobre $s \geqslant 1$.
Antes de começar o procedimento, observe que para $n = sp + 1$, o sistema de congruências em (6.14) é equivalente ao sistema módulo p:

$$\begin{cases} i \equiv h \\ j \equiv p - 1 - k \end{cases} \tag{6.15}$$

e esse sistema não depende da variável s.
Se as equações do sistema (6.15) tem solução para $0 \leqslant k \leqslant h \leqslant p - 1$, então existem $\ell, m \in \mathbb{Z}$ tais que

$$\begin{aligned} i &= p\ell + h \\ j &= p(m+1) - k - 1 \end{aligned}$$

Como $i, j \geqslant 0$, temos que $h \geqslant p(-\ell)$ e $-(k+1) \geqslant -p(m+1)$, assim, se $\ell < 0$ teríamos que $h \geqslant p(-\ell) \geqslant p$, da mesma forma, se $m < 0$, teríamos $-(k+1) \geqslant -p(m+1) \geqslant 0$ e esse valores não correspondem aos valores que podem tomar h e k como soluções do sistema de congruências acima; dessa forma, de existir as soluções ao sistema, vamos considerar sempre $\ell, m \in \mathbb{Z}_0^+$.

- Caso $s = 1$. Aqui, $n = p + 1$ e de acordo com a proposição 6.2.1, procuramos a quantidade de pares (i, j) com $0 \leqslant i + j \leqslant p - 2$ tais que o sistema (6.15) tem solução (h, k) módulo p para $0 \leqslant k \leqslant h \leqslant p - 1$.
  Observe que se $\ell > 0$, como $h \geqslant 0$, então $p\ell + h \geqslant p$, isto é, $i \geqslant p$, da mesma forma, se $m > 0$, $p(m+1) - (k+1) \geqslant pm \geqslant p$, isso significa que $j \geqslant p$, e como procuramos os pares (i, j) com $i + j \leqslant p - 2$, concluímos que a única opção possível é $\ell = m = 0$.
  Se $\ell = m = 0$, então,

$$\begin{cases} i &= h \\ j &= p - k - 1 \end{cases}$$

e nesse caso temos que

$$i + j = (p - 1) + (h - k)$$

Como precisamos que $i + j \leqslant p - 2$, então,

$$i + j = (p - 1) + (h - k) \leqslant p - 2$$

isso implica

$$h - k \leqslant -1$$

e o conjunto solução que procuramos satisfaz $h - k \leqslant 0$, assim, o sistema de congruências (6.15) não possui soluções nos intervalos requeridos. Portanto, posto$(A_p) = 0$ como queríamos mostrar.

Vamos ilustrar mais um caso particular.

- Caso $s = 2$. Aqui temos $n = 2p + 1$ e $i + j \leqslant 2p - 2$. Como mencionamos antes, o sistema acima não depende de s, isso implica que na medida que s varia, as soluções achadas para valores menores de n (que depende de s) não são afetadas por essa variação, assim, como no caso anterior vimos que o sistema não tem soluções para $i + j \leqslant p - 2$, basta determinar se tem soluções para $p - 1 \leqslant i + j \leqslant 2p - 2$, e, no caso de ter, contar quantas há.

Consideremos o sistema (6.15), e sejam $\ell, m \in \mathbb{Z}_0^+$ tais que

$$\begin{aligned} i &= p\ell + h \\ j &= p(m + 1) - k - 1 \end{aligned}$$

então, $i + j = (\ell + m + 1)p + h - k - 1$; como só procuramos as soluções para as quais $p - 1 \leqslant i + j \leqslant 2p - 2$, então,

$$p \leqslant (\ell + m + 1)p + (h - k) \leqslant 2p - 1. \tag{6.16}$$

Como $h - k \geqslant 0$, então,

$$(\ell + m + 1)p \leqslant (\ell + m + 1)p + (h - k) \leqslant 2p - 1 < 2p$$

e segue que $\ell + m < 1$; por outra parte, como $\ell, m \in \mathbb{Z}_0^+$, temos que $\ell + m \geqslant 0$, assim, neste caso só é possível $\ell + m = 0$, o que significa que $\ell = m = 0$.
De acordo ao anterior, em (6.16) temos que

$$p \leqslant p + (h - k) \leqslant 2p - 1,$$

de onde, $0 \leqslant h-k \leqslant p-1$; segue que h e k podem tomar todos os valores para os que $0 \leqslant k \leqslant h \leqslant p-1$. Observe que para cada $0 \leqslant r \leqslant p-1$ tal que $h = r$, podemos encontrar $r+1$ possíveis valores para k satisfazendo $0 \leqslant h-k \leqslant p-1$, assim, encontramos $1+2+\cdots+p = p(p+1)/2$ possíveis duplas (h,k) que satisfazem o sistema (6.15), e claramente, para cada uma dessas soluções existe uma única dupla (i,j) satisfazendo as condições da proposição 6.2.1, isso permite concluir que

$$\text{posto}(A_{2p+1}) = \frac{1}{2}p(p+1)$$

.

- Caso geral: suponha $s \geqslant 3$. Vamos tomar como hipótese indutiva que

$$\text{posto}(A_{kp+1}) = \frac{1}{4}k(k-1)p(p+1)$$

para todo $k \leqslant s-1$ e vamos mostrar que

$$\text{posto}(A_{sp+1}) = \frac{1}{4}s(s-1)p(p+1)$$

usando o mesmo argumento do caso $s = 2$ vemos que é suficiente encontrar as soluções do sistema (6.15) quando $(s-1)p-1 \leqslant i+j \leqslant sp-2$.
Sejam $\ell, m \in \mathbb{Z}_0^+$ tais que

$$\begin{aligned} i &= p\ell + h \\ j &= p(m+1) - k - 1 \end{aligned}$$

Segue que

$$(s-1)p \leqslant (\ell+m+1)p + (h-k) \leqslant sp-1. \tag{6.17}$$

Como $h-k \leqslant p-1$, então, $(s-1)p-(h-k) \geqslant (s-1)p-(p-1)$, assim,

$$(s-2)p < (s-1)p-(h-k) \leqslant (\ell+m+1)p$$

e temos que $\ell+m \geqslant s-2$. Por outra parte, como $h-k \geqslant 0$, então,

$$(\ell+m+1)p \leqslant (\ell+m+1)p + (h-k) \leqslant sp-1 < sp$$

assim, $\ell+m+1 < s$, isto é, $\ell+m \leqslant s-2$. Concluímos que $\ell+m = s-2$.
Substituindo o valor de $\ell+m$ em (6.17) temos

$$(s-1)p \leqslant (s-1)p + (h-k) \leqslant sp-1$$

segue que $0 \leqslant h-k \leqslant p-1$. O anterior significa que para cada par (ℓ,m) com $\ell+m = s-2$, todos os possíveis pares (h,k) com $0 \leqslant k \leqslant h \leqslant p-1$ satisfazem o sistema (6.15); assim, se (ℓ,m) é um desses pares, ele tem associados $\frac{1}{2}p(p+1)$ pares (a mesma contagem feita para o caso s=2 com $(\ell,m) = (0,0)$). Falta saber quantos possíveis pares (ℓ,m) podem-se formar com a condição $\ell+m = 2$, vejamos:

ℓ	m
0	$s-2$
1	$s-1$
$\vdots$	$\vdots$
$s-2$	0

Isso significa que temos $s-1$ possíveis pares (ℓ, m) com $\ell, m \in \mathbb{Z}_0^+$ satisfazendo a condição desejada, portanto, existem $\frac{1}{2}(s-1)p(p+1)$ pares (h,k) que são solução do sistema (6.15) com $(s-1)p-1 \leqslant i+j \leqslant sp-2$.
Fazendo uso da hipótese indutiva concluímos que:

$$\text{posto}(A_{sp+1}) = \frac{1}{4}(s-1)(s-2)p(p+1) + \frac{1}{2}s(s-1)p(p+1) = \frac{1}{4}s(s-1)p(p+1)$$

Agora, por definição sabemos que $a(\mathcal{F}_n) = g(\mathcal{F}_n) - \text{posto}(A_n)$, assim,

$$\begin{aligned} a(\mathcal{F}_{sp+1}) &= \frac{1}{2}sp(sp-1) - \frac{1}{4}sp(s-1)(p+1) \\ &= \frac{1}{4}s(s+1)p(p-1) \end{aligned}$$

■

Teorema 6.2.2. *Se $n = sp-1$, com $s \geqslant 1$, o a-número da curva de Fermat, $\mathcal{F}_n$ é:*

$$a(\mathcal{F}_n) = \frac{1}{4}s(s-1)p(p-1).$$

Demonstração. Seja A_{sp-1} a p-ésima potência da matriz de Cartier-Manin da curva de Fermat $\mathcal{F}_{sp-1}$. Vamos mostrar que

$$\text{posto}(A_{sp-1}) = \begin{cases} \frac{1}{2}(p-2)(p-3), & s=1, \\ \frac{1}{2}(p-2)(p-3) + p(p-2), & s=2, \\ 3(p-1)^2 + \frac{1}{4}p[(p+1)s^2 + (p-11)s - 12(p-2)], & s \geqslant 3. \end{cases}$$

O último desses casos por indução sobre s.

Se $n = sp-1$, o sistema de equações na proposição 6.2.1 é equivalente ao sistema módulo p:

$$\begin{cases} i \equiv -(h+2) \\ j \equiv k-1 \end{cases} \tag{6.18}$$

Se o sistema acima tem solução, então existem $\ell, m \in \mathbb{Z}$ tais que:

$$\begin{aligned} i &= p\ell - (h+2) \\ j &= pm + k - 1 \end{aligned}$$

Como $i, j \geqslant 0$, temos que $h+2 \leqslant p\ell$ e $k-1 \geqslant p(-m)$, assim, se $\ell \leqslant 0$ e $m < 0$ então, $h+2 < 0$ e $k-1 \geqslant p$, assim, para o nosso propósito consideramos $\ell \in \mathbb{Z}^+$ e $m \in \mathbb{Z}_0^+$.

- $s = 1$. Neste caso, $n = p-1$ e $0 \leqslant i+j \leqslant p-4$.

  Sejam $\ell \in \mathbb{Z}^+$ e $m \in \mathbb{Z}_0^+$ satisfazendo as equações acima; Observe que se $k \geqslant 0$, então, $j = pm + k - 1 \geqslant pm - 1$, assim, se $m > 0$, então, $j \geqslant p-1 > p-4$. Analogamente, se $h \leqslant p-1$, temos que $-(h+2) \geqslant -(p+1)$ e $i = p\ell - (h+2) \geqslant p(\ell-1)+1$, assim, se $\ell \geqslant 2$, temos que $i \geqslant p-1 > p-4$; com isso, podemos descartar esses valores de ℓ e m, obtendo como única possível dupla $(\ell, m) = (1, 0)$. Segue que

  $$\begin{aligned} i &= p - (h+2) \\ j &= k - 1 \end{aligned}$$

  Assim, se $i + j \leqslant p-4$, então, $0 \leqslant p - (h-k+1) \leqslant p-4$, que é equivalente a que $3 \leqslant h-k \leqslant p-1$. Se $3 \leqslant r \leqslant p-1$ é tal que $h = r$, então temos $r-2$ possíveis valores para k que satisfazem $3 \leqslant h-k \leqslant p-1$, isso significa que há $1 + 2 + \cdots + p - 3 = \frac{1}{2}(p-3)(p-2)$ duplas (h, k) com essa propriedade. Como a cada dupla (h, k) corresponde uma única dupla (i, j), concluímos que

  $$\operatorname{posto}(A_p - 1) = \frac{1}{2}(p-3)(p-2).$$

  Segue que

  $$a(\mathcal{F}_{p-1}) = 0.$$

- $s = 2$. Neste caso, $n = 2p-1$. Queremos achar as soluções do sistema (6.18) para $p-3 \leqslant i+j \leqslant 2p-4$. considere $\ell \in \mathbb{Z}^+$ e $m \in \mathbb{Z}_0^+$ como acima. Se $\ell \geqslant 3$, então $i \geqslant 2p-1 > 2p-4$, que não satisfazem o procurado; segue que $\ell \in \{1, 2\}$. Analogamente, se $m \geqslant 2$, então $j \geqslant 2p-1 > 2p-4$, portanto, $m \in \{0, 1\}$.
  Como $i + j = p(\ell + m) - (h-k) - 3$, precisamos para (h, k):

  $$p \leqslant p(\ell+m) - (h-k) \leqslant 2p-1, \tag{6.19}$$

  onde os possíveis valores para $\ell + m$ são: $\ell + m = 1$, $\ell + m = 2$ e $\ell + m = 3$.
  Vamos estudar a possível quantidade de pares de soluções (h, k) (com sua respectiva restrição) para cada um dos casos anteriores:

1. $\ell + m = 3$: Neste caso, a desigualdade (6.19) é equivalente à desigualdade:

$$p + 1 \leqslant h - k \leqslant 2p,$$

e sabemos que as soluções procuradas satisfazem $0 \leqslant h - k \leqslant p - 1$.

2. $\ell + m = 2$: Aqui, a desigualdade em (6.19) é equivalente a:

$$1 \leqslant h - k \leqslant p,$$

as possíveis duplas (ℓ, m) são $(1, 1)$ e $(2, 0)$.
No caso $(\ell, m) = (1, 1)$ temos que $i = p-(h+2)$; observe que se $h = p-1$, então $i = -1$, assim, os possíveis valores para h que satisfazem a desigualdade acima estão entre $1 \leqslant h \leqslant p - 2$ e não temos restrições para k, assim, quando $h = r$ (com $1 \leqslant r \leqslant p-2$), existem r valores possíveis para k tal que $1 \leqslant h-k \leqslant p-2$, obtendo $\frac{1}{2}(p-2)(p-1)$ possíveis soluções ao sistema inicial.
No caso $(\ell, m) = (2, 0)$, temos $i = 2p - (h + 2)$ e $j = k - 1$, assim, se $h = 1$, então $i = 2p - 3$ e precisamos as soluções para as que $i, j \leqslant 2p - 4$, assim, podemos considerar $2 \leqslant h \leqslant p-1$, além do anterior, se $k = 0$, teríamos $j = -1$, assim, só consideramos os valores de k para os quais $1 \leqslant k \leqslant h-1$, encontrando $\frac{1}{2}(p-2)(p-1)$ possíveis soluções para o sistema inicial. Portanto, para o caso $\ell + m = 2$, existem $(p-2)(p-1)$ duplas (h, k) que são solução do sistema inicial sob a respectivas restrições.

3. $\ell + m = 1$: neste caso, a desigualdade (6.19) é equivalente a

$$-(p-1) \leqslant h - k \leqslant 0$$

deixando como única opção possível aquelas duplas (h, k) onde $h = k$. Observe que $\ell+m = 1$ implica que $(\ell, m) = (1, 0)$, assim, como vimos acima, as restrições para h e k são $0 \leqslant h \leqslant p - 2$ e $1 \leqslant k \leqslant p - 1$ respectivamente. Com isso, obtemos $p - 2$ possíveis duplas (h, k) com $h = k$.

Dos três casos acima obtemos um total de $(p-1)(p-2)+(p-2) = p(p-2)$ soluções (h, k) para o sistema (6.18) com $p - 3 \leqslant i + j \leqslant 2p - 4$, sabemos que a cada uma dessas duplas corresponde uma única dupla (i, j) com a restrição acima; logo, com as soluções encontradas no caso $s = 1$, obtemos, via a proposição 6.2.1 que:

$$\text{posto}(A_{2p-1}) = \frac{1}{2}(p-2)(p-3) + p(p-2)$$

Logo,

$$\begin{aligned} a(\mathcal{F}_{2p-1}) &= \frac{1}{2}(2p-2)(2p-3) - \frac{1}{2}(p-2)(p-3) - p(p-2) \\ &= \frac{1}{2}p(p-1). \end{aligned}$$

Finalmente, vamos mostrar usando indução que para todo $s \geqslant 3$, tem-se:

$$\text{posto}(A_{sp-1}) = 3(p-1)^2 + \frac{1}{4}p[(p+1)s^2 + (p-11)s - 12(p-2)].$$

Como caso inicial mostramos que o resultado é válido para $s = 3$: Precisamos encontrar as soluções para o sistema (6.18) onde $2p-3 \leqslant i+j \leqslant 3p-4$ (lembramos que o sistema não depende da variação de s, isso significa que as soluções encontradas nos casos anteriores continuam sendo válidas).
Sejam, $\ell \in \mathbb{Z}^+$ e $m \in \mathbb{Z}_0^+$ como antes. Aqui temos que $i, j \leqslant 3p-4$, assim, se $m \leqslant 3$ temos que $j = pm + (k-1) \geqslant pm - 1 \geqslant 3p - 1 > 3p - 4$; da mesma forma, se $\ell \geqslant 4$, então, $i = p\ell - (h+2) \geqslant p\ell - (p+1) \geqslant 3p - 1 > 3p - 4$. Segue que $\ell \in \{1, 2, 3\}$ e $m \in \{0, 1, 2\}$. Como $i + j = p(\ell + m) - (h - k) - 3$, precisamos para (h, k):

$$2p \leqslant p(\ell + m) - (h - k) \leqslant 3p - 1, \tag{6.20}$$

Sabemos que $\ell + m \in \{1, 2, 3, 4, 5\}$. Queremos analisar as possibilidades para h, k em (6.20) dependendo do valor de $\ell + m$.
Se $\ell + m = 5$ ou $\ell + m = 4$, em (6.20) queda que

$$2p + 1 \leqslant h - k \leqslant 3p$$

e

$$p + 1 \leqslant h - k \leqslant 2p,$$

respectivamente, e sabemos que as soluções procuradas satisfazem $0 \leqslant h - k \leqslant p - 1$.
Se $\ell + m = 3$, em (6.20) temos que

$$1 \leqslant h - k \leqslant p$$

As possíveis duplas (ℓ, m) são: $(1, 2)$, $(2, 1)$ e $(3, 0)$. Vamos analisar os possíveis valores para h e k nesses três casos:

- $(\ell, m) = (1, 2)$; para esse caso, $i = p - (h + 2)$ e $j = 2p + k - 1$, um raciocínio similar ao do caso $s = 2$ (especificamente quando $\ell + m = 2$) mostra que $1 \leqslant h \leqslant p - 2$ e $0 \leqslant k \leqslant p - 3$. Logo, a quantidade de possíveis soluções do sistema inicial para este caso é: $\frac{1}{2}(p-2)(p-1)$.
- $(\ell, m) = (2, 1)$; aqui, $i = 2p - (h + 2)$ e $p + k - 1$, é fácil ver que neste caso não temos restrições tanto para h quanto para k. Logo, a quantidade de possíveis soluções do sistema inicial para este caso é: $\frac{1}{2}p(p-1)$.
- $(\ell, m) = (3, 0)$; neste caso, $i = 3p - 4$ e $j = k - 1$, assim, o mesmo raciocínio que nos anteriores casos mostra que $2 \leqslant h \leqslant p - 1$ e $1 \leqslant k \leqslant h - 1$. Logo, a quantidade de possíveis soluções do sistema inicial para este caso é: $\frac{1}{2}(p-2)(p-1)$.

Se $\ell + m = 2$, em (6.20) temos que

$$-(p-1) \leqslant h - k \leqslant 0$$

As possíveis duplas (ℓ, m) são: $(1,1)$ e $(2,0)$. Vamos analisar os possíveis valores para h e k nesses dois casos:

- $(\ell, m) = (1,1)$, nesse caso $i = p - (h+2)$ e $p + k - 1$; segue que $0 \leqslant h \leqslant p-2$ e não há restrições para k. Logo a quantidade de possíveis soluções do sistema inicial para este caso é: $p - 1$.
- $(\ell, m) = (2,0)$: aqui temos $i = 2p - (h+2)$ e $j = k - 1$,; segue que $1 \leqslant k \leqslant p-1$ e não há restrições para h. Logo a quantidade de possíveis soluções do sistema inicial para este caso é: $p - 1$.

Se $\ell + m = 1$, em (6.20) temos que

$$-(2p-1) \leqslant h - k \leqslant -p,$$

e sabemos que as soluções procuradas satisfazem $0 \leqslant h - k \leqslant p - 1$.

Vamos fazer a contagem das soluções obtidas:

Para $\ell + m = 3$ obtivemos $(p-1)(p-2) + \frac{1}{2}p(p-1)$ soluções e para $\ell + m = 2$ obtivemos $2(p-1)$ soluções, o que significa que obtivemos um total de $2(p-1)+(p-1)(p-2)+\frac{1}{2}p(p-1)$ soluções para o sistema inicial com as restrições requeridas. Segue que

$$\begin{aligned} \text{posto}(A_{3p-1}) &= \frac{1}{2}(p-2)(p-3) + p(p-2) + 2(p-1) + (p-1)(p-2) + \frac{1}{2}p(p-1) \\ &= 3(p-1)^2. \end{aligned}$$

Agora, suponha $s \geqslant 4$. Vamos tomar como hipótese indutiva que

$$\text{posto}(A_{kp-1}) = 3(p-1)^2 + \frac{1}{4}p[(p+1)k^2 + (p-11)k - 12(p-2)],$$

para todo $k \leqslant s-1$ e vamos mostrar que

$$\text{posto}(A_{sp-1}) = 3(p-1)^2 + \frac{1}{4}p[(p+1)s^2 + (p-11)s - 12(p-2)].$$

Vamos contar as soluções do sistema (6.18) quando $(s-1)p - 3 \leqslant i + j \leqslant sp - 4$.
Sejam ℓ, m como antes; Como $i + j = p(\ell + m) - (h - k)$, então, precisamos:

$$(s-1)p \leqslant p(\ell + m) - (h - k) \leqslant sp - 1, \tag{6.21}$$

Observe que como $h-k \geqslant 0$, então,

$$p(\ell+m) \geqslant p(\ell+m)-(h-k) \geqslant (s-1)p,$$

de onde temos que $\ell+m \geqslant s-1$. Por outra parte, como $h-k \leqslant p-1$, então,

$$p(\ell+m)-(h-k) \geqslant p(\ell+m-1)+1,$$

assim, $sp-1 \geqslant p(\ell+m-1)+1$, e segue que $p(\ell+m-1) \leqslant sp-2 < sp$, portanto, $\ell+m \leqslant s$. Concluímos que $\ell+m \in \{s-1, s\}$.
Como $i, j \leqslant sp-4$, então $\ell \leqslant s$ e $m \leqslant s-1$. Vamos analisar as possibilidades para as soluções (h,k) mediante o estudo da desigualdade (6.21) para os dois possíveis valores de $\ell+m$:

- $\ell+m=s-1$: Neste caso, a desigualdade em (6.21) é equivalente a:

  $$-(p-1) \leqslant h-k \leqslant 0,$$

  assim, as únicas soluções não descartáveis são aquelas para as que $h=k$. Neste caso, as possíveis duplas (ℓ, m) são descritas mediante o conjunto:

  $$\{(\ell, s-(\ell+1)) \ : \ 1 \leqslant \ell \leqslant s\},$$

  para as duplas $(1, s-2)$ e $(s-1, 0)$ temos as restrições $0 \leqslant h \leqslant p-2$ e $1 \leqslant k \leqslant p-1$ respectivamente, para as demais duplas do conjunto acima não há restrições sobre os valores que podem tomar h e k. O anterior implica que podemos encontrar $2(p-1)+(s-3)p$ soluções para o sistema inicial.

- $\ell+m=s$: Aqui, a desigualdade em (6.21) é equivalente a:

  $$1 \leqslant h-k \leqslant p.$$

  Neste caso, as possíveis duplas (ℓ, m) são descritas mediante o conjunto

  $$\{(\ell, s-\ell) \ : \ 1 \leqslant \ell \leqslant s\},$$

  para a dupla $(1, s-1)$ temos que $1 \leqslant h \leqslant p-2$ e $0 \leqslant k \leqslant p-3$.
  Para a dupla $(s, 0)$ temos que $2 \leqslant h \leqslant p-1$ e $1 \leqslant k \leqslant p-2$.
  Para as demais duplas do conjunto acima não há restrições sobre os valores que podem tomar h e k sempre que $1 \leqslant h-k \leqslant p-1$. O anterior significa que para esse caso há $(p-2)(p-1)+\frac{1}{2}(s-2)(p-1)p$ soluções para o sistema inicial.

Segue que para $(s-1)p-3 \leqslant i+j \leqslant sp-4$, o sistema (6.18) tem

$$2(p-1)+(s-3)p+(p-2)(p-1)+\frac{1}{2}(s-2)(p-1)p = \frac{1}{2}p(sp+s-6)$$

soluções (h,k) satisfazendo $0 \leqslant k \leqslant h \leqslant p-1$; sabemos que cada uma dessas soluções tem associado um e só um par (i,j), assim, fazendo uso da hipótese indutiva temos que:

$$\begin{aligned}\text{posto}(A_{sp-1}) &= \text{posto}(A_{(s-1)p-1}) + \frac{1}{2}p(sp+s-6)\\ &= 3(p-1)^2 + \frac{1}{4}p[(p+1)(s-1)^2 + (p-11)(s-1) - 12(p-2)]\\ &\qquad + \frac{1}{2}p(sp+s-6)\\ &= 3(p-1)^2 + \frac{1}{4}p[(p+1)s^2 + (p-11)s - 12(p-2)].\end{aligned} \tag{6.22}$$

Com o anterior, sabendo que $a(\mathcal{F}_{sp-1}) = g(\mathcal{F}_{sp-1}) - \text{posto}(A_{sp-1})$ concluímos que

$$a(\mathcal{F}_{sp-1}) = \frac{1}{4}s(s-1)p(p-1)$$

Como queríamos mostrar. ■

6.3 Curva de Hurwitz

Novamente, como a curva de Hurwitz dada pela equação afim:

$$F : X^nY + Y^n + X = 0,$$

é uma curva não singular, via o corolário 4.3 temos que o conjunto:

$$\mathcal{B}_H = \left\{ \frac{x^iy^j}{x^n + ny^{n-1}}dx \ : \ 0 \leqslant i+j \leqslant n-2 \right\},$$

é uma base para as diferenciais regulares sobre $\mathcal{H}_n$.

Proposição 6.3.1. *O posto do operador de Cartier $\mathcal{C}$ sobre a curva de Hurwitz $\mathcal{H}_n$ corresponde à quantidade de pares (i,j) com $i+j \leqslant n-2$ tais que o sistema de congruências módulo p*

$$\begin{cases} nk - h + i \equiv 0 \\ n(h-k) + k + j \equiv p-1 \end{cases} \tag{6.23}$$

tem uma solução (h,k) para $0 \leqslant h \leqslant p-1$ e $0 \leqslant k \leqslant h$.

Demonstração. Seja $\omega_{i,j}$ um elemento da base $\mathcal{B}_H$. Se $\mathcal{C}(\omega_{i,j}) = 0$, então $\omega_{i,j} \in \ker(\mathcal{C})$. Suponha que $\mathcal{C}(\omega_{i,j}) \neq 0$; assim, como $\omega_{i,j} = (h/F_y)dx$ onde $h = x^iy^j$, então, $\mathcal{C}(\omega_{i,j}) = \nabla(F^{p-1}h)^{1/p}dx/F_y$ e segue que

$$\mathcal{C}(\omega_{i,j}) \neq 0 \ \Leftrightarrow \ \nabla(F^{p-1}h) \neq 0. \qquad (*)$$

Temos que $F^{p-1}h = (x^n y + y^n + x)^{p-1} x^i y^j$ onde:

$$\begin{aligned}(x^n y + y^n + x)^{p-1} &= \sum_{h=0}^{p-1} \binom{p-1}{h} (x^n y + y^n)^h x^{p-1-h} \\ &= \sum_{h=0}^{p-1} \sum_{k=0}^{h} \binom{p-1}{h}\binom{h}{k} (x^n y)^k (y^n)^{h-k} x^{p-1-h} \\ &= \sum_{h=0}^{p-1} \sum_{k=0}^{h} \binom{p-1}{h}\binom{h}{k} x^{nk-h+p-1} y^{n(h-k)+k}\end{aligned}$$

Assim,

$$\nabla((x^n y + y^n + x)^{p-1} x^i y^i) = \sum_{i,j} b_{i,j} x^{(nk-h+i+p-1)-(p-1)} y^{(n(h-k)+k+j)-(p-1)}$$

logo, de $(*)$ segue que existem $s, r \in \mathbb{Z}$ tal que

$$\begin{cases} (nk-h+i+p-1)-(p-1) = ps \\ (n(h-k)+k+j)-(p-1) = pr \end{cases}$$

que é equivalente a

$$\begin{cases} nk-h+i \equiv 0 \mod p \\ n(h-k)+k+j \equiv p-1 \mod p \end{cases}$$

onde $0 \leqslant h \leqslant p-1$ e $0 \leqslant k \leqslant h$.

Falta provar que se $(i,j) \neq (i_0, j_0)$ são tais que $\mathcal{C}(\omega_{i,j}) \neq 0$ e $\mathcal{C}(\omega_{i_0,j_0}) \neq 0$, então, $\mathcal{C}(\omega_{i,j}) \neq \lambda \mathcal{C}(\omega_{i_0,j_0})$ para todo $\lambda \in K \backslash \{0\}$.

Suponha que $\mathcal{C}(\omega_{i,j}) = \lambda \mathcal{C}(\omega_{i_0,j_0})$ para algum $\lambda \in K$ não nulo. Como ambos $\mathcal{C}(\omega_{i,j})$ e $\mathcal{C}(\omega_{i_0,j_0})$ são não nulas, existem soluções (h,k) e (h_0,k_0) do sistema de congruências acima, para (i,j) e (i_0,j_0) respectivamente. Por outra parte, como $\mathcal{C}(\omega_{i,j}) = \nabla(F^{p-1}x^i y^j)^{1/p} dx/F_y = \lambda \nabla(F^{p-1}x^{i_0}y^{j_0})^{1/p} dx/F_y$, então,

$$\nabla(F^{p-1}x^i y^j) dx/F_y = \lambda^p \nabla(F^{p-1}x^{i_0}y^{j_0}) dx/F_y$$

isso significa que

$$x^{nk-h+i} = x^{nk_0-h_0+i_0} \quad \text{e} \quad y^{n(h-k)+k+j-(p-1)} = y^{n(h_0-k_0)+k_0+j_0-(p-1)}$$

portanto,

$$\begin{cases} nk-h+i = nk_0-h_0+i_0 & (1) \\ n(h-k)+k+j = n(h_0-k_0)+k_0+j_0 & (2) \end{cases}$$

Observe que se $(h,k) = (h_0,k_0)$, então $(i,j) = (i_0,j_0)$, assim, se $(i,j) \neq (i_0,j_0)$ tem-se $(h,k) \neq (h_0,k_0)$ e para isso há três casos:

1. $h = h_0$ e $k \neq k_0$,
2. $h \neq h_0$ e $k = k_0$,
3. $h \neq h_0$ e $k \neq k_0$.

No primeiro caso, sem perda de generalidade podemos supor $k > k_0$; da equação (1) segue que $n(k - k_0) = i_0 - i$, como $i_0 - i \leqslant n - 2$, concluímos que $n(k - k_0) \leqslant n - 2$, que não pode acontecer quando $k - k_0 > 0$.
No segundo caso, podemos supor $h > h_0$ e da equação (2) obter $n(h - h_0) = j_0 - j$; um argumento análogo ao do caso anterior mostra que isso também não é possível.
No último caso, vamos supor $h > h_0$. Na equação (1) obtemos:

$$i - i_0 = (h - h_0) + n(k_0 - k) \leqslant n - 2$$

Como $h - h_0 > 0$, se $k_0 - k > 0$ teríamos que $i - i_0 > n$, assim, $k_0 < k$; desta forma, $k_0 - k \leqslant -1$ e

$$-(n-2) \leqslant i - i_0 = (h - h_0) + n(k_0 - k) \leqslant h - h_0 - n,$$

de onde $h - h_0 \geqslant 2$. Agora, somando as equações (1) e (2), obtemos:

$$(n-1)h + k + i + j = (n-1)h_0 + k_0 + i_0 + j_0,$$

assim,

$$j - j_0 = (n-1)(h_0 - h) + (k_0 - k) + (i_0 - i).$$

Usando os fatos: $h - h_0 \geqslant 2$, $k_0 - k < 0$ e $i_0 - i \leqslant n - 2$ obtemos:

$$j - j_0 < 2(1 - n) + (n - 2) = -n$$

de onde $j_0 - j > n$. Absurdo.

O anterior mostra que não existem duplas (h_0, k_0) com $0 \leqslant k_0 \leqslant h_0 \leqslant p - 1$ satisfazendo as equações (1) e (2), isso significa que $\mathcal{C}(\omega_{i,j})$ e $\mathcal{C}(\omega_{i_0,j_0})$ são linearmente independentes, concluindo que a cada solução (h, k) do sistema no enunciado corresponde uma única dupla (i, j) com $i + j \leqslant n - 2$, isto prova a proposição.

■

Seja $A_n := A(\mathcal{H}_n) = (a_{ij})$ onde $(a_{ij}^{1/p})$ é a matriz de Cartier-Manin da curva $\mathcal{H}_n$.

Teorema 6.3.1. *Se $n = sp$, com $s \geqslant 1$, então o a-número da curva de Hurwitz, $\mathcal{H}_{sp}$, é:*

$$a(\mathcal{H}_{sp}) = \frac{1}{4}s(s+1)p(p-1).$$

Demonstração. Vamos mostrar por indução sobre s que:

$$\text{posto}(A_{sp}) = \frac{1}{4}s(s-1)p(p+1).$$

Observe que neste caso ($n = sp$), o sistema (6.23) é equivalente ao sistema módulo p:

$$\begin{cases} i \equiv h \\ j \equiv -k-1 \end{cases} \tag{6.24}$$

que não depende da variável s. Se as equações do sistema (6.24) tem solução para $0 \leqslant k \leqslant h \leqslant p-1$, então existem $\ell, m \in \mathbb{Z}$ tais que:

$$\begin{aligned} i &= p\ell + h \\ j &= pm - k - 1 \end{aligned}$$

Como $i, j \geqslant 0$, então $h \geqslant p(-\ell)$ e $k+1 \leqslant pm$, logo, se $\ell < 0$ e $m \leqslant 0$ teríamos $h \geqslant p$ e $k+1 \leqslant 0$, portanto, podemos assumir $\ell \in \mathbb{Z}_0^+$ e $m \in \mathbb{Z}^+$.

Queremos encontrar as soluções (h,k) módulo p do sistema (6.24) para as quais $0 \leqslant k \leqslant h \leqslant p-1$ e para as que $i + j \leqslant sp - 2$.

- Caso $s = 1$: Aqui, $0 \leqslant i + j \leqslant p-2$, assim, $i, j \leqslant p-2$. Sejam ℓ e m como acima; se $\ell \geqslant 1$ e $h \geqslant 0$, então $i \geqslant p + h > p - 2$. Por outra parte, se $k \leqslant p-1$, então $j = pm - (k+1) \geqslant p(m-1)$, segue que se $m \geqslant 2$, então $j \geqslant p$, logo, a única possibilidade para (ℓ, m) é $\ell = 0$ e $m = 1$, assim,

  $$\begin{aligned} i &= h, \\ j &= p - k - 1, \end{aligned}$$

  Como precisamos $i + j \leqslant p-2$, deveríamos ter $h + (p-k-1) \leqslant p-2$, isto é, $h - k \leqslant -1$; o anterior implica que não existem soluções (h,k) para o sistema inicial com $0 \leqslant k \leqslant h \leqslant p-1$, segue, via a proposição anterior que $\text{posto}(A_p) = 0$.

- Caso $s = 2$: queremos encontrar os pares (i,j) com $p-1 \leqslant i+j \leqslant 2p-2$ para os quais $\mathcal{C}(\omega_{i,j}) \neq 0$.
  Sejam ℓ, m como antes; como $p-1 \leqslant i+j \leqslant 2p-2$, precisamos:

  $$p \leqslant p(\ell+m) + (h-k) \leqslant 2p-1 \tag{6.25}$$

  Observe que como $h - k \geqslant 0$, então,

  $$p(\ell+m) \leqslant p(\ell+m) + (h-k) \leqslant 2p-1 < 2p,$$

de onde temos que $\ell + m < 2$. Por outra parte, como $\ell \geqslant 0$ e $m > 0$, temos que $\ell + m \geqslant 1$, portanto, $\ell + m = 1$, isto é, $(\ell, m) = (0, 1)$. Segue da desigualdade (6.25) que

$$0 \leqslant h - k \leqslant p - 1$$

obtendo $\frac{1}{2}p(p+1)$ possíveis duplas (h, k), portanto, sabendo que para $0 \leqslant i+j \leqslant p-2$ não há soluções do sistema inicial, concluímos que:

$$\text{posto}(A_{2p}) = \frac{1}{2}p(p+1).$$

- Caso geral: Suponha que $s \geqslant 3$. Vamos tomar como hipótese indutiva que

$$\text{posto}(A_{kp}) = \frac{1}{4}k(k-1)p(p+1),$$

para todo $k \leqslant s-1$ e vamos mostrar que

$$\text{posto}(A_{sp}) = \frac{1}{4}s(s-1)p(p+1).$$

Como sempre, é suficiente encontrar as soluções do sistema (6.24) para $(s-1)p-1 \leqslant i+j \leqslant sp-2$. Considerando ℓ e m como antes e sabendo que $(s-1)p-1 \leqslant i+j \leqslant sp-2$, observamos que é necessário que

$$(s-1)p \leqslant p(\ell + m) + (h - k) \leqslant sp - 1 \tag{6.26}$$

Um argumento similar ao do caso anterior mostra que $\ell + m \leqslant s - 1$; por outra parte, se $h - k \leqslant p - 1$, então,

$$(s-1)p \leqslant p(\ell + m) + (h - k) \leqslant p(\ell + m + 1) - 1 < p(\ell + m + 1)$$

e temos que $\ell + m \geqslant s - 1$, portanto, $\ell + m = s - 1$.
Com o anterior, de (6.26) segue que

$$0 \leqslant h - k \leqslant p - 1$$

assim, para cada dupla (ℓ, m) com $\ell + m = s - 1$ existem $\frac{1}{2}p(p+1)$ duplas (h, k) satisfazendo (6.24).
Todas as possibilidades para (ℓ, m) estão consignadas na seguinte tabela:

ℓ	m
0	$s-1$
1	$s-2$
$\vdots$	$\vdots$
$s-2$	1

Concluímos que existem $\frac{1}{2}(s-1)p(p+1)$ soluções (h,k) com as condições requeridas. Fazendo uso da hipótese indutiva temos que:

$$\begin{aligned}\text{posto}(A_{sp}) &= \frac{1}{4}(s-1)(s-2)p(p+1)+\frac{1}{2}(s-1)p(p+1)\\ &= \frac{1}{4}s(s-1)p(p+1).\end{aligned}$$

Segue que $a(\mathcal{H}_{sp}) = g(\mathcal{H}_{sp}) - \text{posto}(A_{sp})$, isto é,

$$\begin{aligned}a(\mathcal{H}_{sp}) &= \frac{1}{2}sp(sp-1)-\frac{1}{4}s(s-1)p(p+1)\\ &= \frac{1}{4}s(s+1)p(p-1)\end{aligned}$$

■

Teorema 6.3.2. *Se $n = sp+1$, com, $s \geqslant 1$, então o a-número da curva de Hurwitz é:*

$$a(\mathcal{H}_{sp}) = \frac{1}{4}s(s-1)p(p-1).$$

A demonstração deste teorema é bastante similar às demonstrações dos teoremas anteriores, a diferencia encontra-se especificamente nas contas, como nos teoremas anteriores foram detalhadas a maioria delas, aqui omitiremos bastantes desses detalhes para não torná-lo mais repetitivo.

Demonstração. Neste caso, o sistema (6.23) é equivalente ao sistema módulo p:

$$\begin{cases} i \equiv h-k \\ j \equiv -h-1 \end{cases} \tag{6.27}$$

■

Se existem soluções (h,k) deste sistema sob as restrições da proposição 6.3.1, então existem $\ell, m \in \mathbb{Z}$ tais que:

$$\begin{aligned} i &= p\ell + h - k\\ j &= pm - h - 1\end{aligned}$$

Segue que $\ell \in \mathbb{Z}_0^+$ e $m \in \mathbb{Z}^+$.

Queremos, como sempre, usar a proposição 6.3.1 para mostrar por indução que:

$$\text{posto}(A_{sp+1}) = \frac{1}{4}s(s+1)p(p+1).$$

- Caso $s = 1$: Aqui, $n = p + 1$ e precisamos que $0 \leqslant i + j \leqslant p - 1$, assim, $i, j \leqslant p - 1$, de onde temos que $\ell = 0$ e $m = 1$, logo,

$$\begin{aligned} i &= h - k, \\ j &= p - h - 1, \end{aligned}$$

assim, $i+j = p-1-k$ e como $0 \leqslant k \leqslant p-1$, temos que cada para (h, k) com $0 \leqslant k \leqslant h$ é uma solução do sistema. Portanto, existem $\frac{1}{2}p(p+1)$ soluções com as condições requeridas, assim, a proposição 6.3.1 permite concluir que $\text{posto}(A_{p+1}) = \frac{1}{2}p(p+1)$.

- Caso $s = 2$: Neste caso $n = 2p + 1$. Novamente, o sistema (6.27) não depende de s, assim, basta encontrar as soluções para as quais $p \leqslant i + j \leqslant 2p - 1$.
Sejam ℓ, m como antes, então,

$$p \leqslant p(\ell + m) - (k + 1) \leqslant 2p - 1 \tag{6.28}$$

segue que $1 \leqslant \ell+m < 3$. Se $\ell+m = 1$, então de (6.28) tem-se que $-(p-1) \leqslant k+1 \leqslant 0$, assim, neste caso não temos soluções com as condições desejadas.
Se $\ell + m = 2$, então de (6.28) tem-se que $0 \leqslant k \leqslant p - 1$. Temos duas possibilidades para (ℓ, m):

1. $(\ell, m) = (0, 2)$,
2. $(\ell, m) = (1, 1)$.

Nos dois casos não existem restrições tanto para h quanto para k, isso significa que há $\frac{1}{2}p(p+1)$ soluções para cada dupla (ℓ, m). Portanto,

$$\text{posto}(A_{2p+1}) = \frac{1}{2}p(p+1) + p(p+1) = \frac{3}{2}p(p+1).$$

- Caso geral: Suponha $s \geqslant 3$; vamos tomar como hipótese indutiva que

$$\text{posto}(A_{kp+1}) = \frac{1}{4}k(k+1)p(p+1),$$

para todo $k \leqslant s - 1$ e vamos mostrar que

$$\text{posto}(A_{sp+1}) = \frac{1}{4}s(s+1)p(p+1).$$

Como sempre, é suficiente encontrar as soluções do sistema (6.27) para $(s-1)p \leqslant i+j \leqslant sp-1$. Considerando ℓ e m como antes e sabendo que $(s-1)p \leqslant i+j \leqslant sp-1$, temos:

$$(s-1)p \leqslant p(\ell + m) - (k + 1) \leqslant sp - 1 \tag{6.29}$$

Para que a desigualdade anterior seja válida, é necessário que $\ell + m = s$, assim, de (6.29) segue que $0 \leqslant k \leqslant p-1$; isso significa que para cada dupla (ℓ, m) existem $\frac{1}{2}p(p+1)$ soluções, portanto, há $\frac{1}{2}sp(p+1)$ soluções sob a restrição inicial. Assim,

$$\begin{aligned} \text{posto}(A_{sp+1}) &= \frac{1}{4}s(s-1)p(p+1) + \frac{1}{2}sp(p+1) \\ &= \frac{1}{4}s(s+1)p(p+1). \end{aligned}$$

Finalmente,

$$\begin{aligned} a(\mathcal{H}_{sp+1}) &= \frac{1}{2}sp(sp+1) - \frac{1}{4}s(s+1)p(p+1) \\ &= \frac{1}{4}s(s-1)p(p-1). \end{aligned}$$

Referências

FULTON, W. *Algebraic Curves, an introduction to algebraic geometry*. 2008. Citado 2 vezes nas páginas 13 e 30.

GEER, G. Van der; VLUGT, M. Van der. Reed-muller codes and supersingular curves. *Compositio Mathematica*, v. 84, p. 333–367, 1992. Citado na página 78.

GORENSTEIN, D. An arithmetic theory of adjoint plane curves. *American Mathematical Society*, v. 72, p. 414–436, 1952. Citado na página 73.

HASSE, H.; WITT, E. Zyklische unverzweigte erweiterungskörper vom primzahlgrade p über einen algebraischen funktionenkörper der characteristik p. *Monatshefte Math. Phys*, v. 43, p. 477–492, 1936. Citado na página 77.

HIRSCHFELD, J.; KORCHMáROS, G.; TORRES, F. *Algebraic Curves over a Finite Field*. Princeton, New Yersey: Princeton University Press, 2008. Citado na página 72.

LANG, S. *Elliptic Functions*. Second edition. New York: Springer-Verlag, 1987. Citado na página 70.

MONTANUCCI, M.; SPEZIALI, P. The a-numbers of fermat and hurwitz curves. *Journal of Pure and Applied Algebra*, v. 222, p. 477–488, 2017. Citado na página 11.

MORANDI, P. *Field and Galois theory*. New York: Springer-Verlag, 1996. Citado na página 59.

NOUROZI, V.; RAHMATI, F.; TAFAZOLIAN, S. The a-number of certain hyperelliptic curves. ArXiv: 1902.03672v2. 2019. Citado na página 11.

STICHTENOTH, H. *Algebraic function fields and codes*. San Francisco: Springer-Verlag, 2008. Citado 5 vezes nas páginas 13, 52, 56, 57 e 60.

STöHR, K.; VOLOCH, J. A formula for the cartier operator on plane algebraic curves. *J. Reine Angew Math*, v. 377, p. 49–64, 1987. Citado 2 vezes nas páginas 12 e 74.

SUBRAO, D. The p-rank of artin-schreier curves. *Manuscripta math*, v. 16, p. 169–193, 1975. Citado na página 77.

TAFAZOLIAN, S. *On supersingular curves over finite fields*. Tese (Doctoral Thesis) — IMPA, 2008. Citado na página 78.