Classificação dos corpos de funções algébricas com Divisor Class Number igual a dois.

Josnei Antonio Novacoski

Dissertação apresentada
ao
Instituto de Matemática e Estatística
da
Universidade de São Paulo
para
obtenção do título
de
Mestre em Ciências.

Programa: Matemática
Orientador: Prof. Dr. Orlando Stanley Juriaans

Durante o desenvolvimento deste trabalho o autor recebeu auxílio financeiro do CNPq.

São Paulo, 13 de março de 2009.

Classificação dos corpos de funções algébricas com Divisor Class Number igual a dois.

Este exemplar corresponde à redação final da dissertação devidamente corrigida e defendida por Josnei Antonio Novacoski e aprovada pela Comissão Julgadora.

Banca Examinadora:

- Prof. Dr. Orlando Stanley Juriaans (orientador) - IME-USP.
- Prof. Dr. Ricardo Bianconi - IME-USP.
- Prof. Dr. Paulo Roberto Brumatti - UNICAMP.

Agradecimentos

Quero agradecer a quatro pessoas que foram de importância essencial para a obtenção deste meu título:

À minha professsora e colega Lorena, por ter me dado o direcionamento necessário para eu começar a estudar matemática.

Ao meu colega Nazar, pelas horas de discussão sobre matemática que me ajudaram a pensar certos conceitos de maneira diferente e também ser mais preciso e cuidadoso com os resultados obtidos.

Ao professor Orlando, por sempre usar sua experiência para mostrar os melhores caminhos e pela atenção que sempre teve comigo. Sou imensamente grato por ele sempre querer o melhor para mim.

Por último eu agradeço ao meu irmão Jonilso, que apesar de não ter uma participação efetiva no meu conhecimento matemático, foi quem sempre esteve ao meu lado em todos os aspectos possíveis.

Resumo

Denotemos por k o corpo finito com q elementos. Sob isomorfismo, existem exatamente 19 corpos de funções com divisor class number igual a dois tendo k como corpo de constantes, onde 11 deles são quadráticos e 8 não quadráticos.
Palavras-chave: Curvas algébricas, Corpos de funções algébricas, Corpos finitos.

Abstract

Let us denote by k a finite field with q elements. Up to isomorphism, there are exactly 11 quadratic and 8 non-quadratic algebraic function fields of one variable K/k having k for full constant field and with a divisor class number equal to two.
Keywords: Algebraic curves, Algebraic function fields, Finite fields.

Sumário

1 Introdução **1**

2 Corpos de Funções Algébricas **3**
2.1 Places 3
2.2 Corpo de Funções Racionais 5
2.3 Independência de Valorizações 6
2.4 Divisores 7
2.5 O Teorema de Riemann-Roch 10

3 Corpos de funções e Curvas algébricas **15**
3.1 Variedades Algébricas 15
3.2 Curvas Algébricas 18
3.2.1 Resolvendo singularidades 20
3.3 A Aplicação Canônica 23

4 Classificação **25**
4.1 Resultados Principais 25
4.2 Prova da Proposição 4.1.1 27
4.3 Prova do Teorema 4.1.1 32
4.3.1 Caso $g = 1$ 32
4.3.2 Caso $g \geq 2$ 33
4.4 Prova do Teorema 4.1.2 37
4.4.1 $g = 3$ 39
4.4.2 $g = 4$ 48
4.4.3 $g = 5$ 59

A Corpos de funções quadráticos **61**
A.1 Corpos de funções quadráticos 61
A.1.1 Places de um corpo de funções quadrático 62
A.1.2 Corpos de funções elípticas 62
A.1.3 Corpos de funções hiperelípticas 66

B Extensões de corpos de funções algébricas **71**
B.1 Extensões algébricas de corpos de funções 71
B.2 Anéis de corpos de funções 73
B.3 Bases Integrais Locais 75
B.4 O Cotraço de diferenciais de Weil e a fórmula do gênero de Hurwitz 77
B.5 O Diferente 80
B.6 Extensões de Corpos Constantes 82

B.7 Extensões de Galois I 83
B.8 Extensões de Galois II 87
B.9 Extensões inseparáveis 89
B.10 Estimativa do gênero de um corpo de funções 90

C Corpos de Funções sobre Corpos de Constantes Finitos **93**
C.1 A Função Zeta de Um Corpo de Funções 93
C.2 O Teorema de Hasse-Weil 101

Referências Bibliográficas **111**

Índice Remissivo **112**

Capítulo 1

Introdução

O presente trabalho baseia-se nos artigos de Dominique Le Brigand entitulados "Classification of algebraic function fields with divisor class number two"e "Quadratic function fields with ideal class number two". Também usamos resultados essenciais dos livros mencionados na bibliografia.

O trabalho tem como objetivo provar que a menos de isomorfismo, existem exatamente 11 corpos de funções algébricas quadráticos com divisor class number dois e 8 não quadráticos.

No capítulo 2, apresentamos as definições e resultados básicos sobre corpos de funções algébricas. O terceiro capítulo é destinado a apresentar alguns resultados envolvendo curvas algébricas e as relações entre corpos de funções e curvas.

O capítulo 4 é a parte central deste trabalho, onde apresentamos as provas dos resultados principais. Na prova destes resultados, usamos alguns resultados que foram omitidos da parte central por considerar que o trabalho se tornaria demasiadamente grande. Porém, como estes resultados são imprescindíveis para as provas, eles foram colocados como apêndices.

O apêndice é concebido de três capítulos, onde o primeiro deles apresenta os resultados sobre extensões de corpos, o segundo alguns resultados sobre corpos finitos, tais quais o teorema de Hasse-Weill e a cota de Hasse-Weill e no terceiro apêncdice apresentamos os resultados básicos sobre corpos de funções quadráticos que são usados na prova do teorema principal sobre corpos de funções quadráticos.

Registramos que alguns resultados, apesar de não serem triviais, serão apresentados sem demonstração, por tratarem de resultados conhecidos da teoria "standard". Porém, nestes casos, serão apresentadas as fontes onde os mesmos podem ser encontrados.

Capítulo 2

Corpos de Funções Algébricas

Neste capítulo apresentaremos as definições e os resultados básicos da teoria de corpos de funções algébricas.

2.1 Places

Definição 2.1.1. *Seja k um corpo. Um* ***corpo de funções algébricas de uma variável*** *K/k sobre k é uma extensão $K \supseteq k$, onde K é uma extensão finita de $k(x)$ para algum $x \in K$ transcendente sobre k.*

Para simplificar a notação, chamaremos K/k apenas de corpo de funções. O conjunto $\widetilde{k} := \{z \in K : z \text{ é algébrico sobre } k\}$ será chamado de **corpo das constantes de** K. Sabemos da teoria de extensões de corpos que $\widetilde{k}$ é um corpo (chamado de fecho algébrico de k em K). Como $k \subseteq \widetilde{k} \subseteq K$, é fácil ver que $K/\widetilde{k}$ é um corpo de funções sobre $\widetilde{k}$.

Observação 2.1.1. *Os elementos de K que são tanscendentes sobre k podem ser caracterizados da seguinte forma: $z \in K$ é transcendente sobre k se e somente se $[K : k(z)] < \infty$.*

Definição 2.1.2. *Um* ***anel de valorização*** *de um corpo de funções K/k é um anel $\mathcal{O} \subset K$ que possui as seguintes propriedades:*

1. $k \subsetneqq \mathcal{O} \subsetneqq K$, *e*
2. $z \in K \Longrightarrow z \in \mathcal{O}$ *ou* $z^{-1} \in \mathcal{O}$.

Proposição 2.1.1. *Seja $\mathcal{O}$ um anel de valorização do corpo de funções K/k. Então:*

(a) *$\mathcal{O}$ é um anel local, isto é, $\mathcal{O}$ tem um único ideal maximal $P = \mathcal{O} \backslash \mathcal{O}^*$, onde $\mathcal{O}^*$ é o grupo das unidades de $\mathcal{O}$;*

(b) *Se $0 \neq x \in K$, então $x \in P \Longleftrightarrow x^{-1} \notin \mathcal{O}$;*

(c) *Se $\widetilde{k}$ é o corpo das constantes de K/k, então $\widetilde{k} \subseteq \mathcal{O}$ e $P \cap \widetilde{k} = \{0\}$.*

Teorema 2.1.1. *Seja $\mathcal{O}$ um anel de valorização de K/k e P seu ideal maximal. Então:*

(a) *P é um ideal principal;*

(b) *Se $P = t\mathcal{O}$, então todo $0 \neq z \in K$ tem uma única representação na forma $z = t^n u$, para algum $n \in \mathbb{Z}$ e algum $u \in \mathcal{O}^*$;*

(c) *$\mathcal{O}$ é um domínio de ideais principais; mais precisamente, se $P = t\mathcal{O}$ e $\{0\} \neq I \subseteq \mathcal{O}$ é um ideal, então $I = t^n\mathcal{O}$ para algum $n \in \mathbb{N}$.*

Um anel com as propridades acima é chamado de **anel de valorização discreta**.

Definição 2.1.3. (a) *Um "**Place**" P de um corpo de funções K/k é o ideal maximal de algum anel de valorização $\mathcal{O}$ de K/k. Um elemento $t \in P$ tal que $P = t\mathcal{O}$ é chamado de **elemento primo de** P.*

(b) $\mathbb{P}(K) := \{P : P$ *é Place de* $K/k\}$.

Se $\mathcal{O}$ é um anel de valorização de K/k, e P o seu ideal maximal, então, pelo item (b) da proposição 2.1.1, $\mathcal{O}$ está unicamente determinado por P, a saber $\mathcal{O} := \{z \in K : z^{-1} \notin P\} \cup \{0\}$. Portanto, $\mathcal{O}_P := \mathcal{O}$ será chamado **anel de valorização do Place** P.

Definição 2.1.4. *Uma **valorização discreta** de K/k é uma função sobrejetora $v : K \longrightarrow \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades:*

1. $v(x) = \infty \Longleftrightarrow x = 0$;
2. $v(xy) = v(x) + v(y)$, $\forall x, y \in K$;
3. $v(x + y) \geq min\{v(x), v(y)\}$, $\forall x, y \in K$;
4. $v(a) = 0$, $\forall a \in k^*$.

A propriedade (3) acima é chamada de **desigualdade triangular**. No seguinte lema, apresentamos uma versão mais forte dessa propriedade, versão essa que nos será muito útil no decorrer do trabalho.

Lema 2.1.1 (Desigualdade triangular estrita). *Seja v uma valorização discreta de K/k, e $x, y \in K$ com $v(x) \neq v(y)$. Então $v(x + y) = min\{v(x), v(y)\}$.*

Definição 2.1.5. *A cada Place $P \in \mathbb{P}(K)$ associamos a função $v_P : \mathbb{Z} \cup \{\infty\}$, da seguinte forma: vimos que se $0 \neq z \in K$, então z é unicamente representado na forma $z = t^n u$, para algum $n \in \mathbb{Z}$ e algum $u \in \mathcal{O}^*$; assim, definimos $v_P(z) := n$ e $v_P(0) := \infty$.*

Teorema 2.1.2. *Seja K/k um corpo de funções.*

(a) *Para todo Place $P \in \mathbb{P}(K)$, a função definida acima é uma valorização discreta; ademais, temos que:*

$$\mathcal{O}_P = \{z \in K : v_P(z) \geq 0\},$$
$$\mathcal{O}_P^* = \{z \in K : v_P(z) = 0\},$$
$$P = \{z \in K : v_P(z) > 0\},$$
$$z \text{ é um elemento primo de } P \Longleftrightarrow v_P(x) = 1.$$

(b) *Reciprocamente, suponhamos que v seja uma valorização discreta de K/k. Então o conjunto $P := \{z \in K : v(z) > 0\}$é um Place de K/k, e $\mathcal{O}_P = \{z \in K : v(z) \geq 0\}$ é o anel de valorização correspondente.*

(c) *Todo anel de valorização de K/k é um subanel de K.*

Seja P um Place de K/k e $\mathcal{O}_P$ seu anel de valorização. Como P é um ideal maximal de $\mathcal{O}_P$, temos que o quociente $\mathcal{O}_P/P$ é um corpo. Para $x \in \mathcal{O}_P$, definimos $x(P) \in \mathcal{O}_P/P$ como sendo a classe de resíduos de x módulo P. Para $x \in K \backslash \mathcal{O}_P$, definimos $x(P) := \infty$. Assim, pelo ítem (c) da proposição 2.1.1 temos de maneira imediata uma imersão $k \hookrightarrow \mathcal{O}_P/P$. Portanto, vamos considerar daqui para frente k como um subcorpo de $\mathcal{O}_P/P$. De maneira análoga, concluímos que $\widetilde{k}$ também é um subcorpo de $\mathcal{O}_P/P$.

Definição 2.1.6. *Seja $P \in \mathbb{P}(K)$.*

(a) *$K_P := \mathcal{O}_P/P$ é chamado* ***corpo residual*** *de P. A aplicação $x \mapsto x(P)$ de K para $K_P \cup \{\infty\}$ é chamada* ***função de classe de resíduo com respeito a*** *P. Em alguns momentos, usaremos a notação $x + P := x(P)$ para $x \in \mathcal{O}_P$.*

(b) *$degP := [K_P : k]$ é chamado* ***grau*** *de P.*

Proposição 2.1.2. *Se P é um Place de K/k e $0 \neq x \in P$, então $degP \leq [K : k(x)] < \infty$. Portanto, K_P é uma extensão finita de k.*

Corolário 2.1.1. *Supondo $\mathbb{P}(K) \neq \emptyset$, temos que $\widetilde{k}$ é uma extensão finita de k.*

Observação 2.1.2. *Se $degP = 1$, então $K_P = k$. Se k é algebricamente fechado, temos obviamente que todo Place de K/k tem grau 1.*

Definição 2.1.7. *Seja $z \in K$ e $P \in \mathbb{P}(K)$. Dizemos que P é um* ***zero*** *de z se e somente se $v_P(z) > 0$; P é um* ***pólo*** *de z se e somente se $v_P(z) < 0$. Se $v_P(z) = m > 0$, P é um* ***zero de z de ordem m****; se $v_P(z) = m < 0$, P é um* ***pólo de z de ordem m****.*

Observe que, até agora, nada nos assegurou a existência de anéis de valorização e, portanto, de Places em um corpo de funções. O próximo resultado irá nos garantir tal existência.

Teorema 2.1.3. *Seja K/k um corpo de funções e R um subanel de K com $k \subsetneq R \subseteq K$. Suponha que $\{0\} \neq I \subsetneq R$ seja um ideal próprio de R. Então existe um place $P \in \mathbb{P}(K)$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$.*

Corolário 2.1.2. *Seja K/k um corpo de funções, $z \in K$ transcendente sobre k. Então z tem pelo menos um zero e um pólo. Em particular, $\mathbb{P}(K) \neq \emptyset$.*

Demonstração. Considere o anel $k[z]$ e o ideal $z \cdot k[z]$. Pelo teorema anterior, existe um Place $P \in \mathbb{P}(K)$ tal que $z \cdot k[z] \subseteq P \Longrightarrow z \in P$; logo z é um zero de P. Analogamente, prova-se que z^{-1} tem um zero $Q \in \mathbb{P}(K)$. Logo Q é um pólo de z. □

2.2 Corpo de Funções Racionais

Veremos nesta seção o exemplo mais simples de corpo de funções algébricas.

Definição 2.2.1. *Um corpo de funções K/k é chamado de* ***corpo de funções racionais*** *se $K = k(x)$ para algum $x \in K$ transcendente sobre k.*

Dado um polinômio irredutível $p(x) \in k[x]$, é fácil verificar que o conjunto

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \ : \ f(x), g(x) \in k[x] \text{ e } p(x) \nmid g(x) \right\} \tag{2.1}$$

é um anel de valorização de $k(x)/k$, e que

$$P_{p(x)} := \left\{ \frac{f(x)}{g(x)} \ : \ f(x), g(x) \in k[x], \text{ onde } p(x) \nmid g(x) \text{ e } p(x) | f(x) \right\} \tag{2.2}$$

é o Place associado a $\mathcal{O}_{p(x)}$. No caso particular em que $p(x)$ é linear, isto é, $p(x) = x - \alpha$, com $\alpha \in k$, abreviamos para $P_\alpha := P_{x-\alpha} \in \mathbb{P}(k(x))$.

Existe outro anel de valorização em $k(x)/k$, a saber

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \ : \ f(x), g(x) \in k[x], \ e \ deg(g(x)) \geq deg(f(x)) \right\} \tag{2.3}$$

cujo ideal maximal associado é:

$$P_\infty := \left\{ \frac{f(x)}{g(x)} \ : \ f(x), g(x) \in k[x], \ e \ deg(g(x)) > deg(f(x)) \right\}. \tag{2.4}$$

Este último é denominado **Place infinito** de $k(x)/k$.

Proposição 2.2.1. *Seja $K = k(x)$ um corpo de funções racionais.*

(a) *Seja $P = P_{p(x)} \in \mathbb{P}(k(x))$, onde $p(x) \in k[x]$ é um polinômio irredutível. Então $p(x)$ é um elemento primo de P, e a valorização discreta associada a P pode ser descrita da seguinte forma: se $z \in k(x)\backslash\{0\}$ é escrito da forma $z = p(x)^n \left(\frac{f(x)}{g(x)}\right)$, com $n \in \mathbb{Z}$, $f(x), g(x) \in k[x]$, $p(x) \nmid f(x)$ e $p(x) \nmid g(x)$, então $v_P(z) = n$. O corpo residual $k(x)_P = \mathcal{O}_P/P$ é isomorfo a $k[x]/\langle p(x) \rangle$, e tal isomorfismo é dado por:*

$$\begin{array}{rccc} \phi \ : & k[x]/\langle p(x) \rangle & \longrightarrow & k(x)_P \\ & f(x) \ mod \ p(x) & \longmapsto & f(x)(P). \end{array}$$

Consequentemente, $degP = deg(p(x))$.

(b) *Considere $P_\infty \in \mathbb{P}(k(x))$ definido em 2.4. Então $degP_\infty = 1$. Um elemento primo de P_∞ é $t = \frac{1}{x}$. A valorização discreta v_∞ é dada por:*

$$v_\infty \left(\frac{f(x)}{g(x)} \right) = deg(g(x)) - deg(f(x)).$$

(c) *k é o corpo das constantes de $k(x)/k$.*

Teorema 2.2.1. *Não existem outros Places em $k(x)/k$ que não sejam do tipo $P_{p(x)}$ ou P_∞, definidos em 2.2 e 2.4.*

Corolário 2.2.1. *Os Places de grau 1 de $k(x)/k$ estão em correspondência biunívova com $k \cup \{\infty\}$.*

2.3 Independência de Valorizações

Teorema 2.3.1 (Aproximação Fraca). *Seja K/k um corpo de funções e $P_1, P_2, \ldots, P_n \in \mathbb{P}(K)$ Places dois a dois distintos de K/k. Se $x_1, x_2, \ldots, x_n \in K$ e $r_1, r_2, \ldots, r_n \in \mathbb{Z}$, então existe $0 \neq x \in K$ tal que*

$$v_{P_i}(x - x_i) = r_i \ para \ todo \ i = 1, 2, \ldots, n.$$

Corolário 2.3.1. *Todo corpo de funções K/k tem infinitos Places.*

Demonstração. Suponha por absurdo que $|\mathbb{P}(K)| = n < \infty$. Tome $r_1, r_2, \ldots, r_n \in \mathbb{Z}$ tais que $r_i > 0$ para todo $i = 1, 2, \ldots, n$. Pelo Teorema da Aproximação Fraca, existe $0 \neq x \in K$ tal que $v_{P_i}(x).0$ para todo $i = 1, \ldots, n$. Em outras palavras, x é transcendente e não possui nenhum pólo, o que contradiz o corolário 2.1.2. □

Proposição 2.3.1. *Seja K/k um corpo de funções e $P_1, P_2, \ldots, P_r$ zeros de um elemento $x \in K$. Então*

$$\sum_{i=1}^{r} v_{P_i} \cdot deg(P_i) \leq [K : k(x)]$$

Corolário 2.3.2. *Em um corpo de funções K/k, todo elemento $0 \neq x \in K$ tem um número finito de zeros e pólos.*

2.4 Divisores

De agora em diante, consideraremos que k seja o corpo das constantes de K/k, ou seja, k é algebricamente fechado em K.

Definição 2.4.1. *O grupo (aditivo) abeliano gerado pelos Places de K/k será chamado de* ***grupo dos divisores*** *de K/k, e será denotado por $\mathcal{D}_K$.*

Os elementos de $\mathcal{D}_K$ serão chamados de **divisores** de K/k. Em outras palavras, um divisor $D \in \mathcal{D}_K$ é dado por

$$D = \sum_{P \in \mathbb{P}(K)} n_P P$$

com $n_P \in \mathbb{Z}$ e $n_P = 0$ para quase todo $P \in \mathbb{P}(K)$. Apresentemos agora algumas definições e fatos com respeito a divisores:

- Um divisor da forma $D = P \in \mathbb{P}(K)$ é chamado **divisor primo**.
- Se $D = \sum n_P P$ e $D' = \sum n'_P P$, então $D + D' = \sum (n_P + n'_P) P$.
- O elemento nulo do grupo $\mathcal{D}_K$ é o divisor

  $$0 := \sum_{P \in \mathbb{P}(K)} r_P P$$

  onde $r_P = 0$ para todo $P \in \mathbb{P}(K)$
- Se $Q \in \mathbb{P}(K)$ e $D = \sum n_P P$, definimos

  $$v_Q(D) := n_Q \quad e \quad suppD := \{P \in \mathbb{P}(K) \ : \ v_P(D) \neq 0\},$$

  sendo este último chamado de **suporte de** D.
- Definimos uma ordem parcial em $\mathcal{D}_K$ da seguinte forma:

  $$D_1 \leq D_2 \Longleftrightarrow v_P(D_1) \leq v_P(D_2), \forall P \in \mathbb{P}(K)$$

  Um divisor $D \geq 0$ é dito **positivo** ou **efetivo**.

- O **grau** de um divisor é definido por

$$degD := \sum_{P \in \mathbb{P}(K)} v_P(D) \cdot degP$$

originando um homomorfismo de grupos $deg : \mathcal{D}_K \longrightarrow \mathbb{Z}$.

Pelo corolário 2.3.2, todo elemento $0 \neq x \in K$ tem um número finito de zeros e pólos. Logo, a próxima definição faz sentido.

Definição 2.4.2. *Seja $0 \neq x \in K$, e Z e N os conjuntos de zeros e pólos de x em $\mathbb{P}(K)$, respectivamente. Então difinimos:*

$$(x)_0 = \sum_{P \in Z} v_P(x)P, \text{ o divisor zero de } x,$$

$$(x)_\infty = \sum_{P \in N} -v_P(x)P, \text{ o divisor pólo de } x$$

$$(x) = (x)_0 - (x)_\infty, \text{ o divisor principal de } x.$$

Obviamente, temos $(x)_0 \geq 0$, $(x)_\infty \geq 0$ e

$$(x) = \sum_{P \in \mathbb{P}(K)} v_p(x)P. \tag{2.5}$$

Os elementos $0 \neq x \in K$ que são constantes são caracterizados por

$$x \in k \Longleftrightarrow (x) = 0.$$

Definição 2.4.3. *$\mathcal{P}_K := \{(x) \ : \ 0 \neq x \in K\}$ é chamado de **grupo dos divisores principais** de K/k. Ele é um subgrupo de $\mathcal{D}_K$, uma vez que para $0 \neq x, y \in K$, $(xy) = (x) + (y)$, por 2.5. O grupo quociente $\mathcal{C}_K := \mathcal{D}_K/\mathcal{P}_K$ é chamado de **grupo de classes de divisor**. Para um divisor $D \in \mathcal{D}_K$, o elemento correspondente em $\mathcal{C}_K$ é denotado po $[D]$, e chamado de **classe do divisor** D. Dois divisores $D, D' \in \mathcal{D}_K$ são ditos **equivalentes** (notação: $D \sim D'$), se $[D] = [D']$, isto é, $D = D' + (x)$ para algum $x \in K \backslash \{0\}$.*

Definição 2.4.4. *Para um divisor $A \in \mathcal{D}_K$, definimos*

$$\mathcal{L}(A) := \{x \in K \ : \ (x) \geq -A\} \cup \{0\}.$$

Esta definição tem a seguinte interpretação: se

$$A = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$$

com $n_i > 0$, $m_j > 0$ então $\mathcal{L}(A)$ consiste de todos os elementos $x \in K$ tais que

1. Q_j é zero de x com ordem maior ou igual a m_j para $j = 1, \ldots, s$;
2. $P_1, \ldots, P_r$ são os únicos possíveis pólos de x, cuja ordem de pólo é menor ou igual à n_i, para $i = 1, \ldots, r$.

Lema 2.4.1. *Seja $A \in \mathcal{D}_K$. Então:*

(a) $x \in \mathcal{L}(A) \Longleftrightarrow v_P(x) \geq -v_P(A) \forall P \in \mathbb{P}(K)$.

(b) $\mathcal{L}(A) \neq \{0\} \Longleftrightarrow$ *existe um divisor* $A' \sim A$ *com* $A' \geq 0$.

(c) $\mathcal{L}(A)$ *é um espaço vetorial sobre* k.

(d) *se* $A' \sim A$ *então* $\mathcal{L}(A) \simeq \mathcal{L}(A')$ *(isomorfismo de espaços vetoriais sobre* k*).*

(e) $\mathcal{L}(0) = k$.

(f) *se* $A < 0$ *então* $\mathcal{L}(A) = \{0\}$

(g) $k \subset \mathcal{L}(A) \Longleftrightarrow A \geq 0$

Lema 2.4.2. *Sejam* A, B *divisores de* K/k *com* $A \leq B$. *Então temos que* $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ *e* $dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq degB - degA$.

Proposição 2.4.1. *Se* $A \in \mathcal{D}_K$, *então* $\mathcal{L}(A)$ *é um espaço vetorial de dimenão finita sobre* k. *Mais precisamente: Se* $A = A_+ - A_-$, *com* A_+ *e* A_- *divisores positivos, então*

$$dim\mathcal{L}(A) \leq degA_+ + 1$$

Demonstração. Como $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$, é suficiente mostrar que $dim\mathcal{L}(A_+) \leq degA_+ + 1$. Como $0 \leq A_+$, o Lema 2.4.2 nos fornece que $dim(\mathcal{L}(A_+)/\mathcal{L}(0)) \leq degA_+$. Como $\mathcal{L}(0) = k$, temos que $dim\mathcal{L}(A_+) = dim(\mathcal{L}(A_+)/\mathcal{L}(0)) = 1$. □

Definição 2.4.5. *Se* $A \in \mathcal{D}_K$, *o número inteiro* $dimA := dim\mathcal{L}(A)$ *é chamado a* ***dimensão*** *do divisor* A.

Teorema 2.4.1. *Todo divisor principal tem grau zero. Mais precisamente: Seja* $x \in K \backslash k$ *e* $(x)_0$ *e* $(x)_\infty$ *os divisores zero e pólo de* x, *respectivamente. Então*

$$deg(x)_0 = deg(x)_\infty = [F : k(x)].$$

Corolário 2.4.1. (a) *Sejam* A, A' *divisores tais que* $A \sim A'$. *Então* $dimA = dimA'$ *e* $degA = degA'$.

(b) *Se* $degA < 0$ *então* $dimA = 0$.

(c) *Para um divisor* A *de grau zero, as seguintes afirmações são equivalentes:*

1. A *é principal.*
2. $dimA \geq 1$.
3. $dimA = 1$

Proposição 2.4.2. *Seja* K/k *um corpo de funções. Então existe* $\gamma \in \mathbb{Z}$, *dependendo apenas de* K/k, *tal que para todo divisor* $A \in \mathcal{D}_K$ *temos:*

$$degA - dimA \leq \gamma.$$

Definição 2.4.6. *O* ***gênero*** *de* K/k *é definido por*

$$g := max\{degA - dimA + 1 \ : \ A \in \mathcal{D}_K\}$$

Observe que a Proposição 2.4.2 nos garante que essa definição é consistente. Veremos ao longo do trabalho que o gênero é um dos invariantes mais importantes de um corpo de funções.

Observação 2.4.1. *O gênero de K/k é um inteiro não-negativo, uma vez que, tomando $A = 0$, temos $g \geq deg(0) - dim(0) + 1 = 0$.*

Teorema 2.4.2 (Teorema de Riemann). *Seja K/k um corpo de funções de gênero g.*

(a) *Para todo divisor $A \in \mathcal{D}_K$, temos que*

$$dimA \geq degA + 1 - g.$$

(b) *Existe um inteiro c, dependendo de K/k tal que*

$$dimA = degA + 1 - g$$

para todo $A \in \mathcal{D}_K$ tal que $degA \geq c$.

Demonstração. (a) Imediato da definição de gênero.
(b) Tome um divisor A_0 tal que $g = degA_0 - dimA_0 + 1$ e defina $c := degA_0 + g$. Daí, se $degA \geq c$, então

$$\begin{array}{rcl} dim(A - A_0) & \geq & deg(A - A_0) + 1 - g \\ & = & degA - degA_0 + 1 - g \\ & \geq & c - degA_0 + 1 - g \geq 1 \end{array}$$

Logo, existe $0 \neq z \in \mathcal{L}(A - A_0)$, e assim $(z) \geq A_0 - A$. Considere o divisor $A' := A + (z)$. Dai $A' \geq A_0$ e temos

$$\begin{array}{rcccl} degA - dimA & = & degA' & - & dimA' \quad \text{(pelo Corolário 2.4.1)} \\ & \geq & degA_0 & - & dimA_0 \quad \text{(pelo Lema 2.4.2)} \\ & = & g - 1. & & \end{array}$$

Portanto $dimA \leq degA + 1 - g$. □

Corolário 2.4.2. *O corpo de funções racionais $k(x)/k$ tem gênero $g = 0$.*

2.5 O Teorema de Riemann-Roch

Nesta seção, K/k denotará um corpo de funções de gênero g.

Definição 2.5.1. *Para $A \in \mathcal{D}_K$,*

$$i(A) := dimA - degA + g - 1$$

*é chamado o **índice de especialidade** de A.*

O teorema de Riemman nos garante que $i(A) \geq 0$ e, $i(A) = 0$ para $degA$ suficientemente grande.

Definição 2.5.2. *Uma **adele** de K/k é uma função.*

$$\alpha : \left\{ \begin{array}{ccc} \mathbb{P}(K) & \longrightarrow & K \\ P & \longmapsto & \alpha_P \end{array} \right.$$

*onde $\alpha_P \in \mathcal{O}_P$ para quase todo $P \in \mathbb{P}(K)$. O conjunto $\mathcal{A}_K := \{\alpha \ : \ \alpha$ é uma adele de $F/K\}$ é chamado **espaço das adeles** de K/k. É fácil verificar que $\mathcal{A}_K$ é um espaço vetorial sobre k.*

Uma **adele principal** de um elemento $x \in K$ é aquela cujas componentes são todas iguais a x (note que essa definição é consistente, uma vez que todo $x \in K$ tem um número finito de pólos em $\mathbb{P}(K)$). Assim, temos automaticamente uma imersão $K \hookrightarrow \mathcal{A}_K$. A valorização v_P de K/k pode ser estendida a $\mathcal{A}_K$ fazendo $v_P(\alpha) = v_P(\alpha_P)$, onde α_P é a P-ésima componente da adele α. Logo, por definição, $v_P(\alpha) \geq 0$ pra quase todo $P \in \mathbb{P}(K)$.

Definição 2.5.3. *Se $A \in \mathcal{D}_K$, definimos $\mathcal{A}_K(A) := \{\alpha \in \mathcal{A}_K \ : \ v_P(\alpha) \geq -v_P(A), \forall \ P \in \mathbb{P}(K)\}$, que é, naturalmente, um k-subespaço vetorial de $\mathcal{A}_K$.*

Teorema 2.5.1. *Para todo divisor A, o índice de especialidade é $i(A) = dim(\mathcal{A}_K/(\mathcal{A}_K(A) + K))$.*

Definição 2.5.4. *Um **diferencial de Weil** de K/k é uma aplicação k-linear $\omega : \mathcal{A}_K \longrightarrow k$ que se anula em $\mathcal{A}_K(A) + K$ para algum $A \in \mathcal{D}_K$. Denominamos o conjunto*

$$\Omega_K := \{\omega \ : \ \omega \text{ é uma diferencial de Weil de } K/k\}$$

*de **módulo dos diferenciais de Weil** de K/k. De maneira natural, Ω_K pode ser visto como um espaço vetorial sobre k.*

Gostaríamos de associar a cada $0 \neq \omega \in \Omega_K$ um divisor $W \in \mathcal{D}_K$. Para isso, consideremos o conjunto

$$M(\omega) := \{A \in \mathcal{D}_K \ : \ \omega \text{ se anula em } \mathcal{A}_K(A) + K\}.$$

Lema 2.5.1. *Seja $0 \neq \omega \in \Omega_K$. Então existe um único divisor $W \in M(\omega)$ tal que $A \leq W$ para todo $A \in M(\omega)$.*

Definição 2.5.5. *Seja $0 \neq \omega \in \Omega_K$. O divisor*

$$(\omega) := W = max\{A \in \mathcal{D}_K \ : \ \omega \text{ se anula em } \mathcal{A}_K(A) + K\}$$

*é chamado um **divisor canônico** de K/k (Observe que o Lema anterior da consistência a essa definição). Um divisor canônico positivo é chamado um divisor canônico de primeiro tipo de K/k.*

Definição 2.5.6. *Sejam $\omega, \omega' \in \Omega_K$ diferenciais de Weil não nulos de K/k. Então existe um elemento $x \in K$ tal que $\omega = x \cdot \omega'$. Tal elemento x é chamado a **razão entre os diferenciais** ω e ω'. Se os divisores canônicos associados à ω e ω' forem positivos, então diremos que o elemento x é uma **razão de diferenciais de primeiro tipo**.*

Teorema 2.5.2. *Sejam A um divisor arbitrário e $W = (\omega)$ um divisor canônico de K/k. Então $i(A) = dim(W - A)$.*

Teorema 2.5.3 (Teorema de Riemann-Roch). *Seja W um divisor canônico de K/k. Então, para todo $A \in \mathcal{D}_K$, temos*

$$dimA = degA + 1 - g + dim(W - A).$$

Proposição 2.5.1. *Um divisor B é canônico se e somente se $degB = 2g - 2$ e $dimB \geq g$.*

Do Teorema de Riemann, vimos que existe uma constante c tal que $i(A) = 0$ se $degA \geq c$. O próximo teorema nos dá um valor mais preciso à essa constante.

Teorema 2.5.4. *Se A é um divisor de K/k tal que $degA \geq 2g - 1$, então $dimA = degA + 1 - g$.*

Observe que a cota $2g - 1$ do teorema anterior é a melhor possível, uma vez que, se W é um divisor canônico, temos que $dimW > degW + 1 - g$, pela proposição 2.5.1.

Proposição 2.5.2. *Para um corpo de funções K/k, as seguintes condições são equivalentes:*

1. *K/k é racional, isto é, $K = k(x)$ para algum x transcendente sobre k.*
2. *K/k tem gênero 0, e existe um divisor $A \in \mathcal{D}_K$ com $degA = 1$.*

Os próximos dois resultados são importantes conseqüências do Teorema de Riemann-Roch.

Teorema 2.5.5 (Aproximação Forte). *Seja $S \subsetneq \mathbb{P}(K)$ um subconjunto próprio de $\mathbb{P}(K)$ e $P_1, \ldots, P_r \in S$. Suponha que são dados $x_1, \ldots, x_r \in K$ e $n_1, \ldots, n_r \in \mathbb{Z}$. Então existe $x \in K$ tal que*

$$v_{P_i}(x - x_i) = n_i \text{ para } i = 1, \ldots, r \text{ e}$$
$$v_P(x) \geq 0 \text{ para todo } P \in S \backslash \{P_1, \ldots, P_r\}.$$

Proposição 2.5.3. *Seja $P \in \mathbb{P}(K)$. Então, para $n \geq 2g$, existe um elemento $x \in K$ cujo divisor pólo é $(x)_\infty = nP$.*

Definição 2.5.7. *Seja $P \in \mathbb{P}(K)$. Um inteiro $n \geq 0$ é chamado* ***número pólo*** *de P se existir um elemento $x \in K$ com $(x)_\infty = nP$. Caso contrário, n é chamado uma* ***lacuna*** *de P.*

Teorema 2.5.6 (Teorema da lacuna de Weierstrass). *Suponha que K/k tem gênero $g > 0$ e P é um Place de grau um. Então existem exatamente g lacunas $i_1 < \ldots < i_g$ de P. Ademais,*

$$i_1 = 1 \quad e \quad i_g \leq 2g - 1.$$

Definição 2.5.8. *Um divisor $A \in \mathcal{D}_K$ é dito* ***não-especial*** *se $i(A) = 0$; caso contrário, A é dito* ***especial****.*

Proposição 2.5.4. (a) *A é não-especial $\Longleftrightarrow dimA = degA + 1 - g$.*

(b) *$degA > 2g - 2 \Longrightarrow A$ é não-especial.*

(c) *A propriedade de um divisor A ser especial ou não-especial depende apenas da classe $[A]$ de A no grupo de classes do divisor.*

(d) *Divisores canônicos são especias.*

(e) *Todo divisor A com $dimA > 0$ e $degA < g$ é especial.*

(f) *Se A é não-especial e $B \geq A$, então B é não-especial.*

Demonstração. (a) é apenas a definição de $i(A)$.

(b) Imediato de teorema 2.5.4.

(c) Segue do fato de que $dimA$ e $degA$ dependem apenas da classe $[A]$ do divisor A.

(d) Pelo teorema 2.5.2, temos que se W é um divisor canônico, então $i(W) = dim(W - W) = dim(0) = 1$. Portanto, W é especial.

(e) $1 \leq dimA = degA + 1 - g + i(A) \Longrightarrow i(A) \geq g - degA > 0$, uma vez que $degA < g$. Logo A é especial.

(f) Pelo teorema 2.5.1, temos que A é não-especial se e somente se $\mathcal{A}_K = \mathcal{A}_K(A) + K$. Como $B \geq A$, é fácil ver que $\mathcal{A}_K(A) \subseteq \mathcal{A}_K(B)$. Dai segue o resultado.

□

Como vimos, se A é um divisor tal que $degA > 2g - 2$, conseguimos determinar sua dimensão, no caso, $dimA = degA + 1 - g$. Em princípio, não é possível determinar a dimensão de um divisor A tal que $0 \leq degA \leq 2g - 2$. Finalizaremos este capítulo com um teorema que nos fornece uma cota superior para a dimensão do divisor A nesses casos.

Teorema 2.5.7 (Teorema de Clifford). *Se A é um divisor tal que $0 \leq degA \leq 2g - 2$, então*

$$dimA \leq 1 + \frac{1}{2} \cdot degA.$$

Capítulo 3

Corpos de funções e Curvas algébricas

3.1 Variedades Algébricas

Definição 3.1.1. (a) *Seja k um corpo, então $\mathbb{A}^n(k) = \{(x_1, ..., x_n) | x_i \in k\}$ é chamado o* ***espaço afim de dimensão n sobre o corpo k****.*

(b) *Seja $X \subset \mathbb{A}^n(k), I(X) := \{f(x_1, ..., x_n) \in k[x_1, ...x_n] | f(P) = 0, \forall P \in X\}$.*

(c) *Seja $T \subset k[x_1, ...x_n], V(T) := \{P \in \mathbb{A}^n(k) | f(P) = 0, \forall f \in T\}$.*

(d) *Um* ***conjunto algébrico*** *é um conjunto $V \subseteq \mathbb{A}^n(k)$ tal que existe $T \subseteq k[x_1, ..., x_n]$ com $V = V(T)$. É fácil ver, que a reunião de dois conjuntos algébricos é um conjunto algébrico e que intersecções arbitrárias de conjuntos algébricos ainda é um conjunto algébrico. Além disso, $\emptyset = V(1)$ e $\mathbb{A}^n(k) = V(0)$.*

(e) *A* ***topologia de Zariski*** *em $\mathbb{A}^n(k)$ é definida por: $A \subseteq \mathbb{A}^n(k)$ é aberto se $\mathbb{A}^n(k) \backslash A$ é um conjunto algébrico.*

(f) *Um subconjunto não vazio $Y \subseteq \mathbb{A}^n(k)$ é* ***irredutível*** *se não existem $Y_1 \neq \emptyset \neq Y_2$ fechados em Y tais que $Y = Y_1 \cup Y_2$.*

(g) *Uma* ***variedade "algébrica"afim*** *é um subconjunto fechado e irredutível de $\mathbb{A}^n(k)$.*

(h) *Seja $X \subseteq k[x_1, ..., x_n]$, definimos o* ***radical de*** *X por $rad(X) = \{f(x_1, ..., x_n) \in k[x_1, ...x_n] | f^r \in X$ para algum $r > 0\}$.*

Teorema 3.1.1. *(Nullstellensatz de Hilbert) Seja k um corpo algebricamente fechado e seja $Y \subseteq k[x_1, .., x_n]$ um ideal e seja $f(x_1, ..., x_n) \in k[x_1, ..., x_n]$ um polinômio que zera todo elemento de $V(Y)$. Então existe $r > 0$ tal que $f^r \in Y$, ou seja, $I(V(Y)) = rad(Y)$.*

Corolário 3.1.1. *Existe uma bijeção entre os ideais radicais ($rad(I) = I$) de $k[x_1, ..., x_n]$ e os conjuntos algébricos de $\mathbb{A}^n(k)$. Além disso, Y é irredutível se e somente se $I(Y)$ é um ideal primo. Se $Y \subseteq \mathbb{A}^n(k)$ é um conjunto algébrico afim, definimos o* ***Anel Coordenado Afim de Y*** *por*

$$\Gamma(Y) = \frac{k[x_1, ..., x_n]}{I(Y)}.$$

Observação 3.1.1. *Se $V \subseteq \mathbb{A}^n(k)$ é uma variedade afim, então $I(V)$ é primo e $\Gamma(V)$ é um domínio.*

Definição 3.1.2. *O corpo $k(V) := Frac(\Gamma(V))$ é chamado o* ***Corpo das Funções Racionais da variedade*** *V. Os elementos de $k(V)$ são chamados de* ***funções racionais de*** *V. Prova-se que $k(V)$ é uma extensão finitamente gerada de k. Definimos assim a* ***dimensão de*** *V como o grau de transcendência da extensão $k(V)/k$*

Definição 3.1.3. *Seja*

$$\phi : V \subseteq \mathbb{A}^n \longrightarrow W \subseteq \mathbb{A}^m$$

uma aplicação entre variedades afins. Então ϕ é chamada **polinomial** *se existem polinômios $T_1, \cdots, T_m \in k[x_1, \cdots, x_n]$ tais que*

$$\phi(a_1, \cdots, a_n) = (T_1(a_1, \cdots, a_n), \cdots, T_m(a_1, \cdots, a_n))$$

para todo $(a_1, \cdots, a_n) \in V$.

Definição 3.1.4. (a) *Seja f uma função racional em V e $P \in V$. Dizemos que f* **está definida em** *P se para algum $a, b \in \Gamma(V)$, $f = a/b$ e $b(P) \neq 0$. Definimos assim*

$$\mathcal{O}_{P,V} := \{f \in k(V) | f \text{ está definida em } P\}.$$

$\mathcal{O}_{P,V}$ é chamado o **anel local de** *V* **em** *P.*

(b) *O conjunto dos pontos $P \in V$ tal que f não está definida em P é chamado o* **conjunto pólo de** *f.*

(c) *Seja $\psi : \mathcal{O}_{P,V} \longrightarrow k$ definida por $\psi(a/b) := a(P)/b(P)$. Então $M_{P,V} := Ker(\psi)$ é chamado o* **ideal maximal de** *V* **em** *P.*

(d) *Seja R um domínio que não é corpo. Se existe um elemento $t \in R$ irredutível tal que todo elemento não nulo $z \in R$ pode ser escrito unicamente da forma $z = ut^n$, com u unidade de R e n um inteiro não negativo, então R é chamado um* **anel de valorização discreta (AVD)**.

(e) *Seja R um AVD e $K = Frac(R)$, então qualquer elemento $z \in K$ não nulo se escreve de maneira única como $z = ut^n$, onde u é uma unidade de R e $n \in \mathbb{Z}$. O inteiro n é chamado a ordem de z e escrito $n = ord(z)$. Definimos $ord(0) := \infty$. Trivialmente temos*

$$R = \{z \in K | ord(z) \geq 0\}$$

e ainda

$$M = \{z \in K | ord(z) > 0\}$$

é seu único ideal maximal.

Definição 3.1.5. *Seja k um corpo. Definimos o* **n-espaço projetivo sobre** *k e denotamos por $\mathbb{P}^n(k)$ como o conjunto de todas as linhas de $\mathbb{A}^{n+1}(k)$ passando por $(0, \cdots, 0) \in \mathbb{A}^{n+1}(k)$. Assim,*

$$\mathbb{P}^n(K) = (\mathbb{A}^{n+1}(k) \backslash \{(0, \cdots, 0)\}) / \sim,$$

onde

$$(a_1, \cdots, a_{n+1}) \sim (b_1, \cdots, b_{n+1}) \Longleftrightarrow \exists \lambda \in k | (a_1, \cdots, a_{n+1}) = \lambda(b_1, \cdots, b_{n+1}).$$

Um ponto de $(a_1 : \cdots : a_{n+1}) \in \mathbb{P}^n(k)$ é a classe de equivalência à qual o elemento $(a_1, \cdots, a_{n+1})$ pertence.

Definição 3.1.6. *Seja $f(x_1, \cdots, x_n) \in k[x_1, \cdots, x_n]$ um polinômio qualquer. Definimos o* ***polinômio homogêneo*** *$F(x_1, \cdots, x_{n+1}) \in k[x_1, \cdots, x_{n+1}]$* ***associado à*** *$f$ como*

$$F(x_1, \cdots, x_{n+1}) := f(x_1/x_{n+1}, \cdots, x_n/x_{n+1})(x_{n+1})^{\partial(f)}.$$

Analogamente, dado um polinômio homogêneo $F(x_1, \cdots, x_{n+1}) \in k[x_1, \cdots, x_{n+1}]$, definimos sua ***desomogeinização*** *em x_{n+1} $f(x_1, \cdots, x_n) \in k[x_1, \cdots, x_n]$ por*

$$f(x_1, \cdots, x_n) := F(x_1, \cdots, x_n, 1).$$

Definição 3.1.7. *Seja $P = (a_1 : \cdots : a_{n+1}) \in \mathbb{P}^n(k)$. Então o conjunto $\{f \in k[x_1, \cdots, x_{n+1}] | f(P) = 0\}$ não está definido. Mas o conjunto*

$$\{F \in k[x_1, \cdots, x_{n+1}] | F \text{ é homogêneo e } F(P) = 0\}$$

está. Assim, podemos fazer as definições projetivas feitas para o caso afim trocando "polinômio"por "polinômio homogêneo".

Definição 3.1.8. *Sejam U e V variedades (afins ou projetivas). Um* ***morfismo de*** *U* ***para*** *V é uma função $\phi : U \longrightarrow V$ tal que:*

(1) *ϕ é contínua (na topologia de Zariski).*

(2) *Para cada conjunto aberto $V' \subseteq V$, se $f \in \Gamma(V')$, então*

$$\widetilde{\phi}(f) := f \circ \phi \in \Gamma(\phi^{-1}(V')).$$

Um isomorfismo de U para V é um morfismo ϕ de U para V tal que existe ϕ^{-1} de V para U tal que $\phi^{-1} \circ \phi = Id_U$ e $\phi \circ \phi^{-1} = Id_V$.

Proposição 3.1.1. *Sejam U e V variedades afins. Então existe uma correspondência biunívoca entre morfismos*

$$\phi : U \longrightarrow V$$

e homomorfismos

$$\widetilde{\phi} : \Gamma(V) \longrightarrow \Gamma(U),$$

ou seja, o funtor

$$\mathcal{F} : \mathcal{V} \longrightarrow \mathcal{D}$$

entre a categoria de variedades afins e morfismos de variedades afins e a categoria de domínios com homomorfismos de domínios dado por

$$U \longmapsto \mathcal{F}(U) := \Gamma(U)$$

e

$$\phi \longmapsto \mathcal{F}(\phi) := \widetilde{\phi}$$

é um funtor contravariante, fiel e pleno.

Definição 3.1.9. *Sejam U e V variedades. Dois morfismos $f_i : U_i \longrightarrow V$ de subvariedades abertas U_i de U para V são ditas equivalentes se suas restrições a $U_1 \cap U_2$ são iguais. Uma classe de equivalência de tais morfismos é chamada uma* **aplicação racional de** U **para** V. *Uma aplicação racional $F : U \longrightarrow V$ é dita* **dominante** *se $f(U')$ é denso em V, onde f é um morfismo qualquer que representa a aplicação F ($f : U' \subseteq U \longrightarrow V$ que não pode ser estendido). Uma aplicação racional $F : U \longrightarrow V$ é dita* **birracional** *se existem conjuntos $U' \subseteq U$ e $V' \subseteq V$ e um isomorfismo $f : U' \longrightarrow V'$ que representa F.*

Proposição 3.1.2. *Duas variedades são birracionalmente equivalentes se e somente se seus corpos de funções são isomorfos, ou seja, existe um funtor fiel e pleno entre a categoria variedades e aplicações racionais e a categoria de corpos e homomorfismos.*

3.2 Curvas Algébricas

Uma **curva algébrica afim (projetiva)** é uma variedade afim (projetiva) de dimensão 1. Vamos estudar o caso plano, ou seja, em $\mathbb{A}^2(k)$ ($\mathbb{P}^2(k)$), onde k não é necessariamente algebricamente fechado.

Seja k um corpo e considere $f \in k[x, y]$ um polinômio qualquer. Definimos a curva algébrica plana afim

$$C := V(f) = \{(a, b) \in \mathbb{A}^2(\overline{k}) | f(a, b) = 0\}.$$

A curva algébrica plana projetiva associada à C será

$$C' := V(F) = \{(a : b : c) \in \mathbb{P}^2(\overline{k}) | F(a, b, c) = 0\}$$

onde F é a homogeinização de f.

Definição 3.2.1. *Seja $P = (a, b) \in \overline{k}^2$ (onde $\overline{k}$ denota o fecho algébrico de k) e escreva*

$$f_P(x, y) := f(a - x, b - y) = f_0(x, y) + f_1(x, y) + \cdots + f_r(x, y),$$

onde $\partial(C) := \partial(f) = r$ e $f_i(x, y)$ é um polinômio homogêneo de grau i.

(a) *Definimos $m = ord_P(f) := min\{i | f_i \neq 0\}$ e tal f_m será chamado a* **forma inicial de** f **em** P. *Temos que*

$$P \in C \Longleftrightarrow ord_P(f) > 0 \Longleftrightarrow f_0 = 0.$$

(b) *A forma inicial f_m se escreve como*

$$f_m = \prod_{j=1}^{m} (a_j x + b_j y)$$

onde $a_j, b_j \in \overline{k}$. As retas $a_j x + b_j y \in \overline{k}[x, y]$ são chamadas as **retas tangentes de** C **em** P *de inclinação ∞ se $a_j = 0$ e b_j/a_j se $a_j \neq 0$.*

(c) *Dizemos que um ponto $P \in C$ é* **simples (não-singular)** *se $ord_P(f) = 1$ e* **singular** *se $ord_P(f) > 1$. Se P é ponto simples de f, então f tem uma única reta tangente em P, a saber, $l = V(f_1)$. Uma curva algébrica plana afim é* **suave** *(não-singular) se todos os seus pontos são simples.*

(d) *Um ponto singular $P \in C$ é dito* **ordinário** *se as tangentes de C em P são distintas entre si, ou seja, cada duas delas se intersectam transversalmente em P.*

Definição 3.2.2. *Seja $C = V(f)$ ($C' = V(F)$) uma curva algébrica irredutível plana afim (projetiva). Definimos*

$$k(C) := \left\{ \frac{g(x,y)}{h(x,y)} \in k(x,y) | f \nmid h \right\}$$

$$(k(C') := \left\{ \frac{G(x,y,z)}{H(x,y,z)} \in k(x,y,z) | G, H \text{ são homogêneos}, \right.$$
$$\left. \partial(G) = \partial(H) \text{ e } F \nmid H \right\}).$$

Seja $P = (\alpha, \beta) \in C$ ($P' = (a : b : c) \in C'$), então

$$\mathcal{O}_{C,P} := \left\{ \frac{g}{h} \in k(C) | h(P) \neq 0 \right\}$$

$$(\mathcal{O}_{C',P'} := \left\{ \frac{G}{H} \in k(C') | H(P') \neq 0 \right\}).$$

Observação 3.2.1. (i) *As definições dadas acima representam um abuso de linguagem, já que a definição formal é a dada na seção anterior, ou seja, o corpo $k(C)$ é tomado sob a equivalência dada por $(f) \subseteq k[x,y]$, o ideal gerado por f.*

(ii) *Os corpos $k(C)$ e $k(C')$ dados acima são isomorfos. Por isso vamos tratar apenas do caso afim.*

Lema 3.2.1. *Seja*

$$\begin{array}{rccl} \phi : & \mathcal{O}_{C,P} & \longrightarrow & k(P) := k(\alpha, \beta) \\ & g/h & \longmapsto & \phi(g/h) := \dfrac{g(P)}{h(P)}. \end{array}$$

Pelo Lema de Zorn, existe prolongamento maximal(não necessariamente único) de ϕ dado por

$$\widetilde{\phi} : \widetilde{\mathcal{O}}_{C,P} \longrightarrow \overline{k}.$$

Teorema 3.2.1. (i) *$k(C)/k$ é um corpo de funções algébricas;*

(ii) *$\widetilde{\mathcal{O}}_{C,P}$ é um anel de valorização de $k(C)/k$;*

(iii) *$\widetilde{P} := ker\widetilde{\phi}$ é o place associado à $\widetilde{\mathcal{O}}_{C,P}$;*

(iv) *$\widetilde{\mathcal{O}}_{C,P} = \mathcal{O}_{C,P} \Longleftrightarrow P$ é não singular;*

(v) *Se P é não singular, então $deg\widetilde{P} = [k(\alpha, \beta) : k]$.*

Demonstração. [8] □

Definição 3.2.3. *Seja K/k um corpo de funções algébricas. Definimos a* ***superfície abstrata de Riemann associada a*** *K/k por*

$$\mathbb{S}_{K/k} := \{ \text{ anéis de valorização } K/k\}.$$

Em particular, dada uma curva C, teremos que a Superfície abstrata de Riemann associada à C será $\mathbb{S}_{k(C)/k}$. No caso em que a curva é não singular, pelo teorema acima temos que existe uma bijeção $C \longleftrightarrow \mathbb{S}_{k(C)/k}$.

Definição 3.2.4. *Definimos uma topologia em $\mathbb{S}_{K/k}$ tomando para fechados subconjuntos finitos e o espaço todo. Se $U \subseteq \mathbb{S}_{K/k}$ é um subconjunto aberto, então definimos o* ***anel das funções regulares em*** *U como sendo $\Gamma(U) := \bigcap_{P \in U} P$.*

Definição 3.2.5. *Seja K/k é um corpo de funções algébricas. Uma* ***curva abstrata não singular*** *é um subconjunto aberto $U \subseteq \mathbb{S}_{K/k}$ com a topologia induzida e a noção de função regular em seus subconjuntos abertos.*

Teorema 3.2.2. *Seja F uma aplicação racional de uma curva C' para uma curva projetiva C. Se f é um morfismo que representa F, então o domínio de f inclui todos os pontos simples da curva C'. Se C' é não singular, então F é um morfismo.*

Corolário 3.2.1. *Duas curvas projetivas não singulares são isomorfas se e somente se seus corpos de funções são isomorfos.*

Observação 3.2.2. *Note que no teorema e corolário acima não estamos considerando apenas o caso plano.*

3.2.1 Resolvendo singularidades

Pela seção anterior, vemos que se uma curva é não singular, para tratar da curva precisamos apenas olhar para seu corpo de funções e vice-versa. Nesta seção queremos analizar a curva nos pontos que ela tem problemas, ou seja, em suas singularidades.

A abordagem pode ser dadas de várias maneiras, por exemplo definindo os ramos da curva e provar que existe uma bijeção entre a superfície de Riemann abstrata de uma curva e os ramos da mesma. Essa abordagem é mais completa, porém é demasiada trabalhosa, tendo em vista que temos de trabalhar as propriedades do anel das séries formais de potência. Aqui vamos usar a teoria de "Blow-Ups", ou seja, resolver as singularidades via Transformações Monoidais.

Vamos assumir por enquanto que k é algebricamente fechado. Seja

$$\begin{array}{rccc} \psi: & \mathbb{A}^2(k) & \longrightarrow & \mathbb{A}^2(k) \\ & (a,c) & \longmapsto & (a,ac). \end{array}$$

Para cada ponto $(a,b) \in \mathbb{A}^2(k)$ consideremos a fibra

$$\psi^{-1}(a,b) = \begin{cases} (a, b/a) & \text{se } a \neq 0 \\ \emptyset & \text{se } a = 0 \text{ e } b \neq 0 \\ \{(0,c) | c \in k\} & \text{se } (a,b) = (0,0) \end{cases}$$

Assim, a origem $(0,0)$ foi "esplodida"em uma reta.

Definição 3.2.6. *Seja $C = V(f)$ uma curva plana irredutível. Suponha que $(0,0) \in C$ e $C \neq V(x)$. Seja m a multiplicidade de C em $(0,0)$ e n o grau de C. Escrevemos $f = \sum_{i=m}^{n} f_i$, onde f_i é uma forma (polinômio homogêneo) de grau i em $k[x,y]$ e $f_m \neq 0 \neq f_n$. Então*

$$\begin{aligned} f(x, xz) &= \sum_{i=m}^{n} f_i(x, xz) \\ &= \sum_{i=m}^{n} x^i f_i(1, z) \\ &= x^m f^{(1)}(x, z) \end{aligned}$$

onde

$$f^{(1)} := \sum_{i=m}^{n} x^{i-m} f_i(1, z) \in k[x, z].$$

O conjunto $C^{(1)} \cup \{(0,c) | c \in k\}$ é chamado o ***"Blow-up"de*** *C ou a* ***trasformada estrita de*** *C.*

Lema 3.2.2. **(i)** *$f^{(1)}$ e logo $C^{(1)} = V(f^{(1)})$ é irredutível.*

(ii) *C possui na origem uma reta tangente de inclinação finita c se e somente se $(0,c) \in C^{(1)}$. Em particular, $(0,0) \in C^{(1)}$ se e somente se o eixo horizontal $V(y)$ é tangente de C em $(0,0)$.*

Proposição 3.2.1. *Com as definições acima temos que C e $C^{(1)}$ são birracionalmente equivalentes, mais ainda, $k(C) = k(C^{(1)})$.*

Corolário 3.2.2. *Seja $P \in C$ um ponto singular ordinário, onde C é uma curva algébrica afim irredutível sobre um corpo k algebricamente fechado. Então existe uma curva C' e uma aplicação birracional $\phi : C' \longrightarrow C$ tal que $|\phi^{(-1)}(P)| = ord_P(C)$ e para todo $Q \in \phi^{(-1)}(P)$, Q é um ponto simples de C'.*

Corolário 3.2.3. *Seja $P \in C$ um ponto racional da curva C sobre o corpo k (não necessariamente algebricamente fechado). Considere a forma inicial f_m da curva em P, onde m é a multiplicidade do ponto P. Então existe uma extensão finita de k, digamos k', tal que os pontos obtidos de P pelo Blow-up do lema acima são racionais sobre k'. A saber, esse corpo é dado por $k' = k(a_1, \cdots, a_m, b_1, \cdots, b_m)$ onde $a_i x + b_i y$ são as retas tangentes de C no ponto P.*

Teorema 3.2.3. *Toda curva algébrica (plana) irredutível é birracionalmente equivalente a uma curva algébrica plana, cujos pontos singulares são todos ordinários.*

Demonstração. [8] □

Teorema 3.2.4. *Toda curva algébrica projetiva plana é birracionalmente equivalente a uma curva algébrica projetiva não singular (não necessariamente plana).*

Demonstração. [8] □

Observação 3.2.3. *Dada uma curva algébrica plana C, construímos uma curva algébrica plana C' birracionalmente equivalente a C tendo apenas pontos singulares ordinários. Podemos resolver localmente com um Blow-up cada singularidade, porém este Blow-up pode mexer nas outras singulariades. Assim, para provar o teorema acima, temos de considerar a curva dada no teorema anterior e fazer um Blow-up simultâneo em todas as singularidades. Mas isto não pode ser necessariamente feito em $\mathbb{P}^2(k)$, e sim em um espaço de dimensão maior.*

Corolário 3.2.4. *Seja K/k um corpo de funções algébricas. Então existe uma curva algébrica $C_K \subseteq \mathbb{P}^n$ não singular tal que $k(C_K) = K$.*

Definição 3.2.7. *Seja C uma curva algébrica plana. Então a curva algébrica projetiva dada pelo teorema acima será chamada o* ***modelo não singular da curva*** *C.*

Apesar de não conseguirmos achar um modelo não singular plano para a curva plana dada, é interessante resolvermos cada singularidade apenas e obter informações sobre ela.

Definição 3.2.8. *Seja C uma curva algébrica afim irredutível e $P \in C$.*

(a) *Dizemos que um ponto $Q \in C'$ está* ***infinitesimamente próximo de*** *P se C' é obtido de C por uma sequência finita de Blow-ups e Q é obtido de P por essa sequência. Definimos o conjunto $Inf(P) := \{Q \in \mathbb{A}^2(k) | Q$ está infinitesimamente próximo de $P\}$.*

(b) *O* ***δ-invariante*** *do ponto P é definido como*

$$\delta_P := \sum_{Q \in Inf(P)} \frac{r_Q(r_Q - 1)}{2},$$

onde $r_Q := ord_Q(C')$.

Observação 3.2.4. *A definição acima, é uma equivalência da definição dada em termos de ramos da curva em questão. Naquele caso, prova-se facilmente a finitude de δ_P. Da definição dada acima, verifica-se facilmente que $\delta_P = 0$ para todo $P \in C$ não singular e sendo o número de pontos singulares finito, temos que*

$$\sum_{p \in C} \delta_P < \infty.$$

Definição 3.2.9. *Seja C uma curva projetiva plana e seja $\phi : C' \longrightarrow C$ a aplicação birracional do modelo não singular C' de C para C. Seja $Q \in C'$ tal que $\phi(Q) = P \in C$. Para qualquer curva plana $G(V(G))$ (possivelmente redutível) escrevemos $G_* := G/L^{\partial(G)}$ onde L é uma linha em $\mathbb{P}^2(k)$. Seja f a imagem de G_* em $\mathcal{O}_{P,\mathbb{P}^2(k)} \subseteq k(C) = k(C')$, então definimos $ord_Q(G) := ord_Q(f)$.*

Definição 3.2.10. *Seja C uma curva algébrica plana irredutível e $\phi : C' \longrightarrow C$ a aplicação birracional do seu modelo não singular.*

(a) *Um divisor em C' é uma soma formal $\sum_{Q \in C'} n_Q Q$ onde $\{n_Q\}_{Q \in C'}$ é uma família quase nula.*

(b) *Seja G uma curva plana que não contém C como componente. Definimos o divisor de G, $div(G) := \sum_{Q \in C'} ord_Q(G) Q$.*

(c) *Para qualquer $z = G/H \in k(C')$ definimos $div(z) := div(G) - div(H)$.*

(d) *Dado z como acima, definimos o divisor zero de z como $(z)_0 := div(G)$ e o divisor pólo de z como $(z)_\infty := div(H)$.*

(e) *Seja $C = V(F)$ uma curva projetiva plana não singular e seja G um polinômio homogêneo em $k[x, y, z]$. Definimos o divisor intersecção de C com a curva $V(G)$ e representamos por $(F)(G)$ ao divisor $\sum_{P \in C} m_P P$, onde m_P denota a multiplicidade de intersecção das curvas C e $V(G)$ em P.*

Observação 3.2.5. *Como a curva C' é não singular, pela bijeção $C' \longleftrightarrow \mathbb{S}_{k(C')/k} = \mathbb{S}_{k(C)/k}$, existe uma bijeção entre os divisores em C' e os divisores de $k(C)$ definido no capítulo anterior, assim como entre divisores canônicos, zero e pólo. As definições feitas no capítulo anterior podem então serem carregadas para a curva em questão e falaremos de divisor de uma curva e de seu corpo de funções como sendo a mesma coisa.*

Teorema 3.2.5. *Seja C uma curva plana, n o grau de C e $r_P = ord_P(C)$. Então o gênero g de C é dado pela fórmula*

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

Corolário 3.2.5. *Seja C uma curva plana com somente pontos ordinários como singularidades. Seja n o grau da curva C e $r_P = ord_P(C)$. Então o gênero g de C é dado pela fórmula*

$$g = \frac{(n-1)(n-2) - deg(E)}{2},$$

onde $E := \sum_{P \in C} r_P(r_P - 1)P$.

Proposição 3.2.2. *Seja C uma curva plana de grau $n \geq 3$ com somente pontos ordinários como singularidades. Seja G qualquer curva plana de grau $n-3$. Então $div(G) - E$ é um divisor canônico.*

3.3 A Aplicação Canônica

Seja K/k um corpo de funções algébricas e seja $\phi : C_K \longrightarrow \mathbb{P}^n$ uma aplicação regular. Suponha que $H \subset \mathbb{P}^n$ é um plano racional definido por um polinômio homogêneo L de grau 1 e fixemos um ponto $P \in C_K$. Escolhemos outro polinômio homogêneo M de grau 1 que não zera $\phi(P)$ e considere $h = (L/M) \circ \phi$, definida em uma vizinhança de P. Definimos o valor $\phi^*(H)(P) := ord_P(h)$ que é não negativo e será positivo se e somente se $\phi(P) \in H$.

Definição 3.3.1. *A construção acima define um divisor $\phi^*(H)$ em C_K que será chamado o* ***divisor hiperplano*** *para a aplicação ϕ.*

Lema 3.3.1. *Seja $\phi : C_K \longrightarrow \mathbb{P}^n$ uma aplicação regular. Então o conjunto $\{\phi^*(H)\}$ dos divisores hiperplanos é um sistema linear, que será denotado por $|\phi|$.*

Proposição 3.3.1. *Seja $|D|$ um sistema linear completo livre de ponto base e de dimensão n em um corpo de funções K/k. Então existe uma aplicação regular $\phi : C_K \longrightarrow \mathbb{P}^n$ tal que $|D| = |\phi|$. Mais ainda, ϕ é única a menos de escolha de coordenadas em $\mathbb{P}^n$.*

Dado um divisor D com $|D|$ livre de ponto base, denotamos por ϕ_D a aplicação regular associada com o sistema linear completo $|D|$.

Proposição 3.3.2. *Seja D um divisor em um corpo de funções K/k. Então o sistema linear completo $|D|$ não tem ponto base se e somente se para cada $P \in C_K$, $dim|D - P| = dim|D| - 1$;*

Definição 3.3.2. *Quando a aplicação ϕ_D é birracional em sua imagem dizemos que ele é um mergulho. Um divisor D tal que $|D|$ não tem ponto base e ϕ_D é um mergulho é chamado de um divisor* ***"very ample"****.*

Proposição 3.3.3. *Seja K/k um corpo de funções algébricas e seja D um divisor em K/k com $|D|$ livre de pontos base. Então ϕ_D é uma aplicação birracional em sua imagem se e somente se para cada P e Q em C_K, tivermos que $dim(L(D - P - Q)) = dim(L(D)) - 2$.*

Corolário 3.3.1. *Seja D um divisor em um corpo de funções K/k de gênero g.*

(a) *Se $deg(D) \geq 2g$, então $|D|$ não tem ponto base.*

(b) *Se $deg(D) \geq 2g+1$, então D é "very ample".*

Lema 3.3.2. *O sistema linear canônico $|K|$ em um corpo de funções algébricas K/k de gênero $g \geq 1$ é livre de ponto base.*

Seja K/k um corpo de funções algébricas de gênero $g \geq 3$ e seja K um divisor canônico em C_K. Pelo lema 3.3.2 temos que $|K|$ é um sistema linear completo sem ponto base. Por isso, a aplicação $\phi_K : C_K \longrightarrow \mathbb{P}^{g-1}$ está definida. Esta aplicação é chamada a **aplicação canônica para** K/k.

Pela proposição 3.3.3, temos que a aplicação ϕ_K não é um mergulho se e somente se existirem pontos P e Q em C_K tal que

$$dim(L(K-P-Q)) \neq dim(L(K)) - 2.$$

Isso só pode acontecer se $dim(L(K-P-Q)) = dim(L(K)) - 1 = g-1$, pois $|K|$ não tem ponto base. Usando Riemann-Roch, temos que

$$\begin{aligned} dim(L(K-P-Q)) &= deg(K-P-Q) + 1 - g + dim(L(p+q)) \\ &= g - 3 + dim(L(p+q)). \end{aligned}$$

Por isso, a aplicação canônica será um mergulho se e somente se existem pontos $P, Q \in C_K$ tal que $dim(P+Q) = 2$.

Proposição 3.3.4. *Seja K/k um corpo de funções algébricas de gênero $g \geq 3$. Então a aplicação canônica é um mergulho se e somente se K/k não é hiperelíptico. Se K/k não é hiperelíptico, a imagem de C_K pela aplicação canônica é uma curva projetiva não de grau $2g-2$ em $\mathbb{P}^{g-1}$. Mais ainda, dois corpos de funções algébricas não hiperelípticos são isomorfos se e somente se seus modelos canônicos são isomorfos por mudança de coordenadas em $\mathbb{P}^{g-1}$.*

Capítulo 4

Classificação

4.1 Resultados Principais

Neste capítulo enunciaremos os resultados principais deste trabalho, assim como apresentaremos suas provas. O primeiro resultado, que será chamado de Proposição 4.1.1, nos dá condições necessárias e suficientes para que um corpo de funções algébricas tenha divisor class number igual a dois. Estas condições são impostas sobre o gênero, o número de elementos de k e os valores dos n_i. Os outros dois teoremas apresentam a classificação destes corpos, onde o primeiro teorema trata dos corpos de funções algébricas quadráticos e o segundo teorema dos não quadráticos.

Alguns dos objetos e resultados que aparecem neste capítulo não foram definidos nos capítulos anteriores. Esses resultados fazem parte dos apêndices deste trabalho, onde apresentamos os conceitos básicos que cercam este capítulo.

Proposição 4.1.1. *Seja K/k um corpo de funções de gênero $g > 0$ tendo o corpo finito k com q elementos como corpo de constantes. Então $h = 2$ se e somente se*

$$\begin{array}{lll}
g=1, & 2 \leq q \leq 5, & n_1 = 2; \\
g=2, & q=2, & n_1 = 0, n_2 = 4 \text{ ou } n_1 = 1, n_2 = 3 \text{ ou } n_1 = 2, n_2 = 1; \\
g=2, & q=3, & n_1 = 0, n_2 = 5; \\
g=3, & q=2, & n_1 = 0, n_3 = 2 \text{ ou } n_1 = 1, n_3 = 3 - n_2; \\
g=4, & q=2, & n_1 = n_2 = 0, 0 \leq n_3 \leq 6, n_4 = 2 \text{ ou} \\
 & & n_1 = 0, n_2 = 1, 0 \leq n_3 \leq 3, n_4 = 3 \text{ ou} \\
 & & n_1 = n_3 = 0, n_2 = 2, n_4 = 3; \\
g=5, & q=2, & n_1 = n_2 = n_4 = 0, n_3 = 1, n_5 = 4 \text{ ou} \\
 & & n_1 = n_2 = n_3 = 0, 0 \leq n_4 \leq 3, n_5 = 2.
\end{array}$$

Teorema 4.1.1. *A menos de isomorfismo, existem apenas 11 corpos de funções algébricas quadráticos K/k de gênero $g \geq 1$, tendo corpo de constantes k, o corpo finito com q elementos e tal que $h = 2$. Eles são obtidos para $K = k(x, y)$ com:*

- $g = 1$

$$\begin{array}{llll}
q=2, & y^2 + xy & = x^3 + x^2 + 1 & n_1 = 2 \quad (r) \\
q=3, & y^2 & = x^3 + 2x^2 + 2 & n_1 = 2 \quad (r) \\
q=4, & y^2 + xy & = x^3 + ax^2 + 1 (*) & n_1 = 2 \quad (r) \\
q=5, & y^2 & = x^3 + 2x^2 & n_1 = 2 \quad (r)
\end{array}$$

- $g = 2$

$$q = 2, \quad y^2 + y = \frac{x^3 + x + 1}{x^2 + x + 1} \qquad n_1 = 1, n_2 = 3 \quad (r)$$

$$y^2 + y = \frac{x^4 + x + 1}{x} \qquad n_1 = 2, n_2 = 1 \quad (r)$$

$$q = 3, \quad y^2 = 2(x^2 + 1)(x^4 + 2x^3 + x + 1) \quad n_1 = 0, n_2 = 5 \quad (r)$$

- $g = 3$

$$q = 2, \quad y^2 + y = \frac{x^4 + x^3 + x^2 + x + 1}{x^3 + x + 1} \quad n_1 = 1, n_2 = 2, n_3 = 1 \quad (r)$$

$$y^2 + y = \frac{x^5 + x^2 + 1}{x^2 + x + 1} \qquad n_1 = 1, n_2 = 3, n_3 = 0 \quad (r)$$

$$y^2 + y = \frac{x^6 + x + 1}{(x^2 + x + 1)^3} \qquad n_1 = 0, n_2 = 4, n_3 = 2$$

$$y^2 + y = \frac{x^4 + x^3 + 1}{x^4 + x + 1} \qquad n_1 = 0, n_2 = 3, n_3 = 2$$

$(*)$ *onde a é um gerador de $\mathbb{F}_4$.*

Teorema 4.1.2. *A menos de isomorfismo, existem apenas 8 corpos de funções algébricas não quadráticos K/k tendo gênero $g \geq 1$ e corpo de constantes k, o corpo finito com q elementos e divisor class number 2. Eles são obtidos para $k = \mathbb{F}_2$ e $K = k(x, y)$ com*

- $g = 3$

$$y^4 + xy^3 + (x + 1)y + (x^4 + x^2 + 1) = 0, \quad n_1 = 0, n_2 = 2, n_3 = 2;$$

$$y^3 + (x^2 + x + 1)y + (x^4 + x^3 + 1) = 0, \quad n_1 = 1, n_2 = 0, n_3 = 3;$$

$$y^3 + y + (x^4 + x^3 + 1) = 0, \quad n_1 = 1, n_2 = 2, n_3 = 2;$$

- $g = 4$

$$y^3 + (x^4 + x^3 + 1)y + (x^6 + x^3 + 1) = 0, \quad n_1 = 0, n_2 = 0, n_3 = 4, n_4 = 2;$$

$$y^3 + (x^4 + x^2 + 1)y + (x^6 + x^5 + 1) = 0, \quad n_1 = 0, n_2 = 0, n_3 = 4, n_4 = 2;$$

$$y^3 + (x^4 + x^3 + 1)y + (x^6 + x + 1) = 0, \quad n_1 = 0, n_2 = 1, n_3 = 3, n_4 = 3;$$

$$y^6 + xy^5 + (x + 1)y^4 + (x^3 + x)y^3 + x^3y^2 + (x^5 + x^3 + x^2)y + (x^6 + x^5 + x^3 + x + 1) = 0, \quad n_1 = 0, n_2 = 1, n_3 = 1, n_4 = 3;$$

$$y^6 + xy^5 + (x + 1)y^4 + x^3y^3 + x^2y^2 + (x^5 + x^3 + x^2 + x)y + (x^6 + x^5 + x^3 + x + 1) = 0, \quad n_1 = 0, n_2 = 1, n_3 = 2, n_4 = 3;$$

4.2 Prova da Proposição 4.1.1

Lema 4.2.1. *Seja K/k um corpo de funções de gênero g e com corpo de constantes k onde $2 \leq |k| = q$. Então seu divisor class number é maior que 2 se qualquer uma das seguites condições valem:*

$$\begin{array}{lll} (i) & q \geq 6 & g \geq 1. \\ (ii) & q = 4, 5 & g \geq 2. \\ (iii) & q = 3 & g \geq 3. \\ (iv) & q = 2 & g \geq 6. \end{array}$$

Demonstração. Usando o teorema de Hasse-Weil temos que

$$L(u) = \prod_{j=1}^{g} (1 - q^{1/2} e^{i\theta_j} u)(1 - q^{1/2} e^{-i\theta_j} u). \tag{4.1}$$

Como $h = L(1)$ obtemos a desigualdade

$$h \geq (q^{1/2} - 1)^{2g}$$

e consequentemente obtemos (i).

Seja agora K'/k' a extensão constante de K/k de grau $2g-1$. Se $\overline{n}_1$ denota o número de places de grau um em K'/k', então temos pela cota de Hasse-Weil que

$$\overline{n}_1 \geq q^{2g-1} + 1 - 2g \cdot q^{(2g-1)/2}$$

(onde usamos que o gênero de K'/k' é igual ao de K/k pois a extensão é uma extensão constante). Mas cada place de grau um em K'/k' está sobre um place de grau n em K/k onde $n \mid 2g-1$. Assim, o número de divisores positivos de grau $2g-1$ em K/k é maior ou igual ao número de places de grau um em K'/k' dividido por $2g-1$, ou seja, se a_{2g-1} denota o número de divisores de grau $2g-1$ em K/k, temos que

$$a_{2g-1} \geq \frac{\overline{n}_1}{2g-1} \geq \frac{q^{2g-1} + 1 - 2g \cdot q^{(2g-1)/2}}{2g-1}.$$

Por outro lado, sabemos que

$$a_{2g-1} \leq h(q^g - 1)/(q-1),$$

pois do teorema de Riemann-Roch temos que se $D \in \mathcal{D}(K)$ tem grau $2g-1$ então $dim(D) = g$ e então $|\{D' \in \mathcal{D}(K) | D \sim D'\}| = (q^g - 1)/(q-1)$ e temos a desigualdade da definição de h.

Assim, temos que se

$$\frac{q^{2g-1} + 1 - 2g \cdot q^{(2g-1)/2}}{2g-1} > 2 \cdot \frac{q^g - 1}{q-1}$$

então $h > 2$.

Definimos agora

$$S(q,g) := \frac{q^{2g-1} + 1 - 2g \cdot q^{(2g-1)/2}}{2g-1} - 2 \cdot \frac{q^g - 1}{q-1}.$$

Então $S(q,g) > 0 \Longrightarrow h > 2$.

Uma conta rápida mostra que $S(q,g) > 0$ para os casos $(ii), (iii)$ e (iv), pois fixado $q \geq 2$ então $R(g) := S(q,g)$ é crescente e logo basta verificar que $S(4,2), S(5,2), S(3,3)$ e $S(2,6) > 0$. □

Demonstração. (*Da proposição* 4.1.1)

Casos:

(a) $q = 3$ e $g = 2$.

Temos que

$$\begin{aligned} 2 = L(1) &= (1+q^g) + (1+q^{g-1})a_1 + \cdots + (1+q)a_{g-1} + a_g \\ &= 10 + 4a_1 + a_2 \\ &= 10 + 4(n_1 - 4) + \frac{n_1^2 - 7n_1 + 2n_2 + 6}{2} \\ &= \frac{-6 + n_1^2 + n_1 + 2n_2}{2} \end{aligned}$$

Portanto, $n_1^2 + n_1 + 2n_2 = 10$.

Da equação 4.1 temos:

$$\begin{aligned} L(u) &= \prod_{j=1}^{2}(1 - \sqrt{3}e^{i\theta_j}u)(1 - \sqrt{3}e^{-i\theta_j}u) \\ &= \prod_{j=1}^{2}(1 - 2\sqrt{3}\cos(\theta_j)u + 3u^2) \\ &= (1 - 2\sqrt{3}\cos(\theta_1)u + 3u^2)(1 - 2\sqrt{3}\cos(\theta_2)u + 3u^2) \\ &= 1 - 2\sqrt{3}(\cos(\theta_1) + \cos(\theta_2))u + (12\cos(\theta_1)\cos(\theta_2) - 6)u^2 \\ &\quad -6\sqrt{3}(\cos(\theta_1) + \cos(\theta_1))u^3 + 9u^4 \\ &= 1 + a_1u + a_2u^2 + 3a_1u^3 + 9u^4 \end{aligned}$$

Segue-se que $a_2 = 12\cos(\theta_1)\cos(\theta_2) - 6$ e $a_1 = -2\sqrt{3}(\cos(\theta_1) + \cos(\theta_2))$.

Substituindo os valores de a_i obtemos os seguintes valores para $\cos(\theta_1)\cos(\theta_2)$ e $\cos(\theta_1) + \cos(\theta_2)$:

$$\begin{aligned} \cos(\theta_1)\cos(\theta_2) &= \frac{a_2 - 6}{12} \\ &= \frac{n_1^2 - 7n_1 + 2n_2 + 6 - 12}{24} \\ &= \frac{10 - n_1 - 2n_2 - 7n_1 + 2n_2 - 6}{24} \\ &= \frac{1 - 2n_1}{6} \end{aligned}$$

$$\begin{aligned}\cos(\theta_1)+\cos(\theta_2) &= \frac{-a_1}{2\sqrt{3}}\\ &= \frac{-(n_1-4)}{2\sqrt{3}}\\ &= \frac{(4-n_1)\cdot\sqrt{3}}{6}\end{aligned}$$

Assim, o polinômio que tem $\cos(\theta_1)$ e $\cos(\theta_2)$ como raízes será:

$$f(x)=x^2+\frac{(4-n_1)\cdot\sqrt{3}}{6}x+\frac{1-2n_1}{6}.$$

Aplicando o polinômio $f(x)$ em 1, obtemos

$$6f(1)=7-4\sqrt{3}+(\sqrt{3}-2)n_1$$

Suponha que $n_1 \geq 1$, então da equação acima temos que $f(1) < 0$. Como $f(x)$ tem grau positivo, então $f(x) \longrightarrow \infty$ quando $x \longrightarrow \infty$, consequentemente f tem uma raíz maior que 1, ou seja, $\cos(\theta_j) > 1$. O que é um absurdo.

Portanto, $h=2, g=2$ e $q=3 \Longleftrightarrow n_1=0$ e $n_2=5$.

(b) $q=2, g=2$

Como no item anterior temos que

$$h=\frac{n_1^2+n_1+2n_2-4}{2}$$

e então temos que

$$h=2 \Longleftrightarrow n_1^2+n_1+2n_2=8.$$

Portanto,

$$\begin{aligned}h=2, q=2 \text{ e } g=2 \quad \Longleftrightarrow \quad & n_1=0 \text{ e } n_2=4 \text{ ou}\\ & n_1=1 \text{ e } n_2=3 \text{ ou}\\ & n_1=2 \text{ e } n_2=1.\end{aligned}$$

(c) $q=2, g=3$

Pelo mesmo argumento temos

$$h=\frac{-10n_1+3n_1^2+n_1^3+6n_1n_2+6n_3}{6},$$

ou seja,

$$h=2 \Longleftrightarrow n_1^3+3n_1^2-10n_1+6n_1n_2+6n_3=12.$$

Procedendo como em (a) temos as seguintes relações:

$$\begin{aligned}
-\sum \cos(\theta_i) &= \frac{a_1\sqrt{2}}{4} \\
\sum \cos(\theta_i)\cos(\theta_j) &= \frac{a_2-6}{8} \\
-\cos(\theta_1)\cos(\theta_2)\cos(\theta_3) &= \frac{a_3-4a_1}{32}\sqrt{2}
\end{aligned}$$

Assim, o polinômio que tem $\cos(\theta_1), \cos(\theta_2)$ e $\cos(\theta_3)$ como raízes é

$$f(x) = x^3 + \frac{a_1\sqrt{2}}{4}x^2 + \frac{a_2-6}{8}x + \frac{a_3-4a_1}{32}\sqrt{2}.$$

Por isso,

$$32f(1) = 8 + 4a_2 + \sqrt{2}a_3 + 4a_1\sqrt{2}.$$

Suponha que $n_1 = 2$. Substituindo os valores de a_i teremos

$$\begin{aligned}
32f(1) &= 8 + 4(n_2-1) + \sqrt{2}(1-3n_2) - 4\sqrt{2} \\
&= 4 - 3\sqrt{2} + n_2(4-3\sqrt{2}) \qquad < 0.
\end{aligned}$$

O que é um absurdo.

Portanto

$$h = 2, q = 2 \text{ e } g = 3 \iff \begin{array}{l} n_1 = 0 \text{ e } n_3 = 2 \text{ ou} \\ n_1 = 1 \text{ e } n_3 = 2 - n_2. \end{array}$$

(d) $q = 2, g = 4$.

O class number é dado por

$$h = 17 + 9a_1 + 5a_2 + 3a_3 + a_4.$$

Assim,

$$h = 2 \iff 15 + 9a_1 + 5a_2 + 3a_3 + a_4 = 0 \iff n_2^2 = 3n_2 - 2n_4 + 4.$$

Obtemos assim

$$\begin{aligned}
-\sum \cos(\theta_i) &= \frac{a_1\sqrt{2}}{4}, \\
\sum \cos(\theta_i)\cos(\theta_j) &= \frac{a_2-8}{8}, \\
-\sum \cos(\theta_i)\cos(\theta_j)\cos(\theta_k) &= \frac{a_3-6a_1}{32}\sqrt{2}, \\
\cos(\theta_1)\cos(\theta_2)\cos(\theta_3)\cos(\theta_4) &= \frac{a_4-4a_2+8}{64}.
\end{aligned}$$

Com isso, o polinômio tendo como raízes $\cos(\theta_i)$ é

$$\begin{aligned} f(x) &= x^4 + \frac{a_1\sqrt{2}}{4}x^3 + \frac{a_2-8}{8}x^2 \\ &\quad + \frac{(a_3-6a_1)\sqrt{2}}{32}x + \frac{a_4-4a_2+8}{64} \end{aligned}$$

e então

$$\begin{aligned} 64f(1) &= 64 - 48\sqrt{2} + 8n_2 - 48 + 36\sqrt{2} \\ &\quad +2\sqrt{2}n_3 - 6\sqrt{2}n_2 - 3n_3 + 2 \\ &= (18 - 12\sqrt{2}) + (8 - 6\sqrt{2})n_2 + (2\sqrt{2} - 3)n_3 \end{aligned}$$

quando $n_1 = 0$. Nos casos em que $n_1 > 0$ o polinômio $f(x)$ tem raíz maior que 1. Temos assim,

$$\begin{aligned} h = 2, q = 2 \text{ e } g = 4 \iff & \; n_1 = n_2 = 0, 0 \leq n_3 \leq 6 \text{ e } n_4 = 2 \text{ ou} \\ & \; n_1 = 0, n_2 = 1, 0 \leq n_3 \leq 3 \text{ e } n_4 = 3 \text{ ou} \\ & \; n_1 = n_3 = 0, n_2 = 2 \text{ e } n_4 = 3. \end{aligned}$$

(e) $q = 2, g = 5$.

Neste caso temos que a fórmula do divisor class number é dada por

$$h = 33 + 17a_1 + 9a_2 + 5a_3 + 3a_4 + a_5.$$

donde

$$h = 2 \iff 33 + 17a_1 + 9a_2 + 5a_3 + 3a_4 + a_5 = 2.$$

Comparando os coeficientes como nos items anteriores, temos as seguintes relações:

$$\begin{aligned} -\sum \cos(\theta_i) &= \frac{a_1\sqrt{2}}{4} \\ \sum \cos(\theta_i)\cos(\theta_j) &= \frac{a_2-10}{8} \\ -\sum \cos(\theta_i)\cos(\theta_j)\cos(\theta_k) &= \frac{(a_3-8a_1)\sqrt{2}}{32} \\ \sum \cos(\theta_i)\cos(\theta_j)\cos(\theta_k)\cos(\theta_l) &= \frac{a_4-6a_2+20}{64} \\ -\cos(\theta_1)\cos(\theta_2)\cos(\theta_3)\cos(\theta_4)\cos(\theta_5) &= \frac{(a_5-4a_3+8a_1)\sqrt{2}}{256} \end{aligned}$$

Por isso, $\cos(\theta_i)$ são as raízes do polinômio

$$\begin{aligned} f(x) = x^5 &+ \frac{a_1\sqrt{2}}{4}x^4 + \frac{a_2-10}{8}x^3 + \frac{(a_3-8a_1)\sqrt{2}}{32}x^2 \\ &+ \frac{a_4-6a_2+20}{64}x + \frac{(a_5-4a_3+8a_1)\sqrt{2}}{256}. \end{aligned}$$

Substituindo os valores de $a_i, i = 1, \cdots, 5$ no polinômio acima temos que

$$\begin{aligned} n_1 = 0 &\implies n_5 - 2n_3 + n_2n_3 = 2 \\ n_1 = 1 &\implies n_5 + n_4 + n_2n_3 - n_3 + \frac{n_2^2 - n_2}{2} = 3. \end{aligned}$$

Usando isto, obtemos

$$\begin{aligned} 256f(1) = (16 - 13\sqrt{2}) + n_2(10 - \frac{17\sqrt{2}}{2}) + n_3(5\sqrt{2} - 8) \\ + n_4(4 - 3\sqrt{2}) + \frac{n_2^2}{2}(4 - 3\sqrt{2}) \end{aligned}$$

e então $f(1) < 0$. Similarmente para $n_1 = 2$ obtemos

$$n_5 + 2n_4 + n_3 + n_2n_3 + n_2^2 + n_2 = 4$$

e por isso

$$\begin{aligned} 256f(1) = (4 - 9\sqrt{2}) + n_2(6 - \frac{13}{2}\sqrt{2}) + n_2^2(4 - \frac{3\sqrt{2}}{2}) \\ + n_3(2\sqrt{2} - 4) + n_4(4 - 3\sqrt{2}). \end{aligned}$$

Por isso, $f(1) < 0$ e este caso também não ocorre.

Portanto

$$\begin{aligned} h = 2, q = 2 \text{ e } g = 5 \iff & n_1 = n_2 = n_4 = 0, n_3 = 1 \text{ e } n_5 = 4 \text{ ou} \\ & n_1 = n_2 = n_3 = 0, 0 \leq n_4 \leq 3 \text{ e } n_5 = 2. \end{aligned}$$

□

4.3 Prova do Teorema 4.1.1

Nesta seção usaremos os resultados construídos no apêndice A para classificar os corpos de funções quadráticos com $h = 2$. Dividiremos a prova do teorema 4.1.1 em casos:

4.3.1 Caso $g = 1$

Pela definição de corpos de funções elípticas, temos que K/k é elíptico ($g = 1$ e existe place de grau 1 pois k é finito). Temos ainda que o divisor class number h é igual a n_1 o número de places de grau um de K/k. Assim, pelo apêndice sobre funções elípticas temos que $K = k(x, y)$ com $F(x, y) = 0$ onde F é uma equação de Weierstrass com invariante $\Delta \neq 0$. Da seção A.1.2 do apêndice A temos as seguintes possibilidades para F em termos de $p := car(k)$:

$$\begin{array}{llrcll} 1^a) & p = 2 & y^2 + xy & = & x^3 + a_2x^2 + a_6, & \Delta = a_6 \\ 1^b) & p = 2 & y^2 + a_3y & = & x^3 + a_4x + a_6, & \Delta = a_3^4 \\ 2^a) & p = 3 & y^2 & = & x^3 + a_2x^2 + a_6, & \Delta = -a_2^3a_6 \\ 2^b) & p = 3 & y^2 & = & x^3 + a_4x + a_6, & \Delta = -a_4^3 \\ 3) & p = 5 & y^2 & = & x^3 + a_4x + a_6, & \Delta = a_4^3 - 2a_6^2 \end{array}$$

A curva algébrica afim com equação $F(x, y) = 0$ deve ter apenas um único ponto racional (pois tem apenas dois places de grau 1 e um deles é correspondente ao ponto infinito da curva). Mas os

casos 1^b ($a_3 = 0 \Longrightarrow \Delta = 0$, $a_6 = 0 \Longrightarrow x^3 + a_4x$ não é livre de quadrados e $a_3 = a_4 = a_6 = 1 \Longrightarrow$ a curva afim não tem pontos racionais) e 2^b (pelas mesmas razões) não atendem às propriedades exigidas para K/k. Nos outros casos, podemos encontrar uma única solução a menos de isomorfismo para cada $q = 2, 3, 4, 5$ que são dadas por:

$$\begin{array}{lrcl} p = 2, & y^2 + xy & = & x^3 + x^2 + 1 \\ p = 3, & y^2 & = & x^3 + 2x + 2 \\ p = 4, & y^2 + xy & = & x^3 + ax^2 + 1(*) \\ p = 5, & y^2 & = & x^3 + 2x \end{array}$$

$(*)$ onde a é um gerador de $\mathbb{F}_4$.

4.3.2 Caso $g \geq 2$

Neste caso K/k é um corpo de funções hiperelípticas. Se $k = \mathbb{F}_2$ o corpo de funões $k(x)$ tem 3 places de grau um (incluindo o place infinito) e um place P_0 de grau 2 associado ao polinômio $x^2 + x + 1$. Teremos então o seguinte resultado:

Lema 4.3.1. *Assuma que $k = \mathbb{F}_2$ e seja K/k um corpo de funções hiperelípticas de genêro g tal que, para algum $x \in K$, a extensão $K/k(x)$ é imaginária. Denotemos por n_1 (resp. n_2) o número de places de grau um (resp. dois) de K.*

1. *Se $n_1 = 0$, temos $n_2 = 3, 4$ ou 5 (se $g = 2, n_2 = 3$ ou 5).*

2. *Se $n_1 = 1$, temos $n_2 = 2, 3$ ou 4.*

3. *Se $n_1 = 2$, temos $n_2 = 1, 2$ ou 3 no caso ramificado (se $g = 2, n_2 = 1$ ou 3) e $n_2 = 2, 3$ ou 4 no caso inerte (se $g = 2, n_2 = 2$ ou 4).*

Demonstração. Seja $K = k(x, y)$ e $F(x, y) = y^2 + h(x)y + f(x) = 0$ como na proposição A.1.5.

1. Se $n_1 = 0$ estamos no caso inerte. Temos pela Proposição A.1.6 que o polinômio $h(x)$ não tem raízes em k, seu grau é igual a $g + 1$ e $f(0) = f(1) = 1$. Existe um place de grau dois sobre cada place de grau um de $k(x)/k$ um mais sobre P_0 se e somente se $x^2 + x + 1$ divide $h(x)$ e 0 ou 2 places sobre P_0 caso contrário. Se $g = 2$ então $h(x)$ é irredutível de grau 3 e é primo com $x^2 + x + 1$.

2. Se $n_1 = 1$ podemos estar no caso ramificado. O place de K sobre o place infinito de $k(x)$ é o único place de grau 1 e então $h(x)$ não tem raízes em k, $deg(h) \leq g$ e $f(0) = f(1) = 1$. Temos um place de grau 2 sobre cada place finito de grau 1 de $k(x)/k$, um mais sobre P_0 se e somente se $x^2 + x + 1$ divide $h(x)$ e 0 ou 2 caso contrário.

3. Se $n_1 = 2$ ambos os casos (ramificado e inerte) podem ocorrer. No caso ramificado dois places de grau um de $k(x)$ ramificam: o place infinito e o um dos places finitos. A conclusão se dá como anteriormente.

□

$g = 2$

1. Se $q = 2$ devemos ter $n_1 = 0$, $n_2 = 4$ ou $n_1 = 1, n_2 = 3$ ou $n_1 = 2, n_2 = 1$ pela Proposição 4.1.1.

(a) Se $n_1 = 0, n_2 = 4$ não temos nenhuma solução devido ao Lema 4.3.1.

(b) Se $n_1 = 1, n_2 = 3$ usando o Lema 4.3.1 devemos ter $h(x) = x^2 + x + 1$ e $f(0) = f(1) = 1$. O polinômio $f(x)$ é mônico de grau 5. Temos então que o corpo de funções é dado por

$$y^2 + (x^2 + x + 1) = q(x) \cdot (x^2 + x + 1)$$

ou na forma normal de Hasse

$$Y^2 + Y = \frac{q(x)}{x^2 + x + 1}$$

onde $q(x)$ é um polinômio mônico irredutível de grau 3. Mas as duas possibilidades para $q(x)$ são $x^3 + x^2 + 1$ e $x^3 + x + 1$ e nestes casos seus corpos de funções são isomorfos sob a aplicação $x \longmapsto x + 1$. Assim, a menos de isomorfismo a única solução neste caso é dada por

$$Y^2 + Y = \frac{x^3 + x + 1}{x^2 + x + 1}.$$

(c) Se $n_1 = 2, n_2 = 1$ de acordo com o lema 4.3.1 devemos estar no caso ramificado. Então $deg(f) = 5$, $deg(h) \leq 2$ e $h(x)$ tem um único zero em k. Então temos que

$$h(x) = x, x^2, (x + 1) \text{ ou } (x + 1)^2.$$

a menos de isomorfismo temos uma única solução que é dada por

$$y^2 + xy = x(x^4 + x + 1) \text{ ou } Y^2 + Y = \frac{x^4 + x + 1}{x}.$$

2. Se $q = 3, n_1 = 0, n_2 = 5$ estamos no caso inerte e $y^2 = f(x)$ com

$$f(x) = 2x^6 + c_1x^5 + c_2x^4 + c_3c^3 + c_4x^2 + c_5x + c_6$$

pois 2 é o único elemento de k que não é um quadrado. Além disso $f(x)$ deve ser livre de quadrados e como $n_1 = 0$ temos que

$$f(a) = 2, \forall a \in k.$$

Sobre os places de grau um de $k(x)$ existem 4 places de grau dois em K e ainda temos que $n_2 = 5$, ou seja, $f(x)$ deve ser o produto de dois polinômios irredutíveis tendo grau igual a dois e a quatro. Usando isomorfismos da forma $x \longmapsto x + 1$ e $x \longmapsto 1/x$ reduzimos para a equação

$$y^2 = 2(x^2 + 1) \cdot q(x)$$

com $q(x)$ irredutível de grau 4. Como $q(0) = 1$ ficamos apenas com duas possibilidades para $f(x)$, a saber

$$2(x^2 + 1)(x^4 + x^3 + 2x + 1) \text{ ou } 2(x^2 + 1)(x^4 + 2x^3 + x + 1).$$

Como estes dois casos são isomorfos via isomorfismo $x \longmapsto 2x$ temos que a única solução a menos de isomorfismo é dada por

$$y^2 = 2(x^4 + 2x^3 + x + 1)(x^2 + 1).$$

$g = 3$

Então $q = 2$ e $n_1 = 1, n_2 + n_3 = 3$ ou $n_1 = 0, n_3 = 2$.

1. Se $n_1 = 1, n_2 + n_3 = 3$, estamos no caso ramificado e usando o lema 4.3.1,temos duas possibilidades:

$$\begin{cases} n_1 = 1 & n_2 = 2 & n_3 = 1 \\ n_1 = 1 & n_2 = 3 & n_3 = 0 \end{cases}$$

Temos $y^2 + h(x)y = f(x)$ onde $deg(f) = 7$, $deg(h) \leq 3$ e como $n_1 = 1$, f e h não tem raízes em k. Os possíveis valores de $h(x)$ são:

$$h_1 = 1, h_2 = x^2 + x + 1, h_3 = x^3 + x + 1, h_4 = x^3 + x^2 + 1.$$

Como $h_3(x+1) = h_4(x)$, os polinômios h_3 e h_4 definem corpos de funções isomorfos. O corpo $k(x)$ tem dois places de grau 3, a saber os places P_1 e P_2 associados respectivamente aos polinômios irredutíveis $p_1(x) = x^3 + x + 1$ e $p_2 = x^3 + x^2 + 1$. Se b é uma raíz primitiva de p_1 então $b + 1$ é raíz primitiva de p_2.

(a) Se $h(x) = 1$ temos $n_2 = 2$. Os places P_i não ramificam, e não podemos ter $n_3 = 1$.

(b) Se $h(x) = x^2 + x + 1$ o place P_0 associado ao polinômio $h(x)$ ramifica e então $n_2 = 3$. Para obter $n_3 = 0$ os places P_i devem estar inertes e então

$$\begin{cases} tr_{k_3/k}(f(b)/h(b)^2) & = & tr_{k_3/k}(b^4 f(b)) = 1 \\ tr_{k_3/k}(f(b+1)/h(b+1)^2) & = & tr_{k_3/k}(b^4 f(b+1)) = 1. \end{cases}$$

Seja

$$f(x) = (x^2 + x + 1)(x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + 1)$$

com

$$\sum_{i=1}^{4} c_i = 1.$$

Obtemos então

$$\begin{cases} c_2 = 1 \\ c_3 = 0 \\ c_4 = c_1. \end{cases}$$

Como anteriormente, podemos encontrar uma única solução, a menos de isomorfismo dada por

$$y^2 + (x^2 + x + 1)y = (x^5 + x^2 + 1)(x^2 + x + 1)$$

ou

$$Y^2 + Y = \frac{x^5 + x^2 + 1}{x^2 + x + 1}.$$

(c) Se $h = x^3 + x + 1$ então P_1 ramifica, P_0 não ramifica e então $n_2 \neq 3$. Seja a umja raíz de $x^2 + x + 1$. Então as condições $n_2 = 2$ e $n_3 = 1$ são equivalentes a

$$\begin{cases} tr_{k_2/k}(f(a)/h(a)^2) & = & tr_{k_2/k}(af(a)) = 1 \\ tr_{k_3/k}(f(b+1)/h(b+1)^2) & = & tr_{k_3/k}(b^6 f(b+1)) = 1. \end{cases}$$

Seja

$$f(x) = (x^3 + x + 1)(x^4 + c_3x^3 + c_2x^2 + c_1x + 1)$$

com

$$\sum_{i=1}^{3} c_i = 1.$$

Obtemos então $c_1 = c_2 = c_3 = 1$. Existe uma única solução:

$$y^2 + (x^3 + x + 1)y = (x^4 + x^3 + x^2 + x + 1)(x^3 + x + 1)$$

ou

$$Y^2 + Y = \frac{x^4 + x^3 + x^2 + x + 1}{x^3 + x + 1}.$$

2. Se $n_1 = 0, n_3 = 2$ estamos no caso inerte e $y^2 + h(x)y = f(x)$ onde $deg(f) = 8, deg(h) = 4, h(x)$ não tem raízes em k e $f(0) = f(1) = 1$ Os possíveis valores para h são:

$$\begin{cases} h_1 &= (x^2 + x + 1)^2, \\ h_2 &= x^4 + x + 1, \\ h_3 &= x^4 + x^3 + 1, \\ h_4 &= x^4 + x^3 + x^2 + x + 1; \end{cases}$$

como $h_3(x + 1) = h_4(x)$ os polinômios h_3 e h_4 definem corpos de funções isomorfos. Ainda, as raízes de h_3 são recíprocas das raízes de h_2, e então seus correspondentes corpos de funções são isomorfos.

(a) Se $h(x) = (x^2 + x + 1)^2$ P_0 ramifica e então $n_2 = 4$ e se

$$f(x) = (x^2 + x + 1)(x^6 + c_5x^5 + c_4x^4 + c_3x^3 + c_2x^2 + c_1x + 1)$$

com

$$\sum_{i=1}^{5} c_i = 1$$

então $n_3 = 0$ é equivalente a

$$\begin{cases} tr_{k_2/k}(f(b)/h(b)^2) &= tr_{k_2/k}(bf(b)) &= 1 \\ tr_{k_3/k}(f(b+1)/h(b+1)^2) &= tr_{k_3/k}(bf(b+1)) &= 0 \end{cases} \text{ou} \quad \begin{matrix} 0 \\ 1. \end{matrix}$$

Obtemos dois casos

$$\begin{cases} c_1 + c_4 &= 1 \\ c_3 &= 0 \\ c_5 &= c_2 \end{cases}$$

ou

$$\begin{cases} c_1 + c_4 &= 0 \\ c_3 &= 0 \\ c_5 &= c_2 + 1. \end{cases}$$

A menos de isomorfismo existe uma única solução:

$$y^2 + (x^2 + x + 1)^2 y = (x^6 + x + 1)(x^2 + x + 1),$$

ou

$$Y^2 + Y = \frac{x^6 + x + 1}{(x^2 + x + 1)^3}.$$

(b) Se $h(x) = x^4 + x + 1$, escrevemos

$$f(x) = h(x)(x^4 + c_3x^3 + c_2x^2 + c_1x + 1)$$

com

$$\sum_{i=1}^{3} c_i = 1.$$

Temos

$$\begin{array}{rcl} n_2 = 3 & \Longleftrightarrow & c_1 + c_2 = 0 \\ n_2 = 5 & \Longleftrightarrow & c_1 + c_2 = 1 \end{array}$$

e

$$n_3 = 2 \Longleftrightarrow c_2 = c_1 = 0 \text{ ou } c_2 = c_1 = 1.$$

Então $n_2 = 5$ é impossível. Para $n_2 = 3$ temos uma única solução:

$$y^2 + (x^4 + x + 1)^2 y = (x^4 + x^3 + 1)(x^4 + x + 1),$$

ou

$$Y^2 + Y = \frac{x^4 + x^3 + 1}{x^4 + x + 1}.$$

$g \geq 4$

Usando a Proposição 4.1.1 e o Lema 4.3.1 temos imediatamente que não existem soluções para este caso.

4.4 Prova do Teorema 4.1.2

Seja K/k um corpo de funções algébricas não quadrático (não hiperelíptico) e seja C_K a curva algébrica não singular (Corolário 3.2.4) associada à K/k. Então pela Proposição 3.3.4 temos que a aplicação $\phi_{|k|} : C_K \longrightarrow \mathbb{P}^{g-1}$ é um mergulho e ainda $\mathcal{C} := \phi_{|k|}(C_K) \subseteq \mathbb{P}^{g-1}$ é uma curva algébrica absolutamente irredutível (consequência de ser suave), suave e de grau $2g - 2$ que será chamado o modelo canônico de K/k. Assim, pelo Corolário 3.2.1 temos que dois corpos de funções são isomorfos se e somente se seus modelos canônicos são isomorfos via um automorfismo projetivo de $\mathbb{P}^{g-1}$.

Lema 4.4.1. *Se existe um g^1_m em K/k livre de pontos base, então existem $x, y \in K$ tal que $K = k(x, y)$, x é transcendente, $[K : k(x)] = m$ e existe uma equação polinomial mônica de grau m com coeficientes em $k[x]$ zerando y.*

Demonstração. Vamos mostrar que existe $x \in K$ transcendente, tal que $[K : k(x)] = m$ e que ele é um elemento separante de K/k.

Sejam $D, D' \in g_m^1$ divisores positivos de grau m e $l(D) = 2$. Então existe $x \in K$ tal que $(x) = D' - D$ e então $\{1, x\}$ é uma base de $\mathcal{L}(D)$. Vamos mostrar que se

$$P \in supp(D') \cap supp(D) \Longrightarrow P \in \bigcap_{D'' \in g_m^1} supp(D''),$$

ou seja, P é ponto base de g_m^1, o que é um absurdo.

Mas da definição de $\mathcal{L}(D)$ temos

$$P \in supp(D') \cap supp(D) \text{ e } (x) = D' - D \Longrightarrow v_P(x) > -v_P(D).$$

Seja D'' outro divisor em g_m^1 e $y \in K$ tal que $(y) = D'' - D$. Mas então $y \in \mathcal{L}(D)$, ou seja, $y = ax + b$ com $a, b \in k$ e temos

$$v_P(y) = v_P(ax + b) \geq min\{v_P(ax), v_P(b)\} > -v_P(D).$$

Consequentemente $P \in supp(D'')$ e como D'' foi tomado qualquer temos $P \in \bigcap_{D'' \in g_m^1} supp(D'')$.

Como o sistema é livre de pontos base, provamos acima que $supp(D) \cap supp(D') = \emptyset$ e então $(x)_\infty = D$. Portanto temos

$$[K : k(x)] = deg((x)_\infty) = deg(D) = m.$$

Falta mostrar então que x é um elemento separante de K/k. Suponha que $r = mdc\{v_P(x) | P \in supp(D)\} \neq 1$, então temos que

$$\mathcal{L}(D) \ni D/r = (x)_\infty/r = (\sqrt[r]{x})_\infty \Longrightarrow \sqrt[r]{x} = ax + b \Longrightarrow x = (ax + b)^r.$$

Absurdo, pois x é um transcendente sobre k. Assim, existe $P \in \mathbb{P}(K)$ tal que $v_P(x) \not\equiv 0 (mod\ p)$ e então x é um elemento separante pela Proposição B.9.1. □

Como $h = 2$ temos que, dados dois divisores positivos de mesmo grau D_1 e D_2, então

$$2D_1 \sim 2D_2.$$

O conjunto $\mathcal{D}_i^+$ dos divisores positivos de grau i será dividido em no máximo dois conjuntos distintos

$$\mathcal{D}_i^+ = \mathcal{D}_{i,1}^+ \sqcup \mathcal{D}_{i,2}^+,$$

onde todos os elementos de $\mathcal{D}_{i,1}^+$ ($\mathcal{D}_{i,2}^+$) serão equivalentes e nenhum elemento de $\mathcal{D}_{i,1}^+$ será equivalente a algum de $\mathcal{D}_{i,2}^+$.

Afirmação. Se $i = 2$ então $|\mathcal{D}_{i,1}^+|, |\mathcal{D}_{i,2}^+| \leq 1$.

Demonstração. Suponha que D_1 e D_2 são divisores de grau 2 tal que $(x) = D_1 - D_2$. Então

$$D_i \in \{2P_1, 2P_2, Q_i\}$$

onde P_i são os dois places de grau 1 e Q_i são os places de grau 2. Daí

$$(x)_0 = D_1 \text{ e } [K : k(x)] = deg(D_1) = 2.$$

O que é um absurdo, pois K/k é não hiperelíptico. □

Assim $A_2 = |\mathcal{D}_{i,1}^+| + |\mathcal{D}_{i,2}^+| \leq 2$ e se $n_1 = 0$ e $n_2 = 2$ então esses dois places não são equivalentes. Vamos dividir a prova nos casos $g = 3, 4$ e 5.

4.4.1 $g = 3$

Pela Proposição 4.1.1 basta apenas estudarmos os casos em que $k = \mathbb{F}_2$ e:

(i) $n_1 = 0, n_3 = 2$;

(ii) $n_1 = 1, n_3 = 3 - n_2$.

Caso **(i)**
Se $n_1 = 0$ e $n_3 = 2$ temos que

$$L(t) = 1 - 3t + (n_2 + 2)t^2 + (2 - 3n_2)t^3 + 2(n_2 + 2)t^4 - 12t^5 + 8t^6.$$

Podemos excluir o caso em que $n_2 = 0$ ou 1, pois para estes valores L teria 4 raízes com valores absolutos ao quadrado diferente de $1/2$. O caso $n_2 \geq 3$ pode ser excluído também pois isso implicaria que existiriam dois places de grau 2 equivalentes e consequentemente K/k seria hiperelíptico.

O único caso a ser estudado então é quando $n_1 = 0, n_2 = 2$ e $n_3 = 2$. Denotemos por Q_1 e Q_2 os dois places de grau 2. Temos então

$$Q_1 \nsim Q_2 \text{ e } 2Q_1 \sim 2Q_2 \nsim Q_1 + Q_2.$$

Assim, a classe canônica contém um dos divisores $2Q_i, i = 1, 2$ ou $Q_1 + Q_2$. Como a classe canônica contém

$$\frac{q^{l(k)} - 1}{q - 1} = \frac{2^3 - 1}{2 - 1} = 7$$

elementos, temos que existem pelo menos 5 places de grau 4 distintos na classe canônica. Seja F_1 um desses places, e considere então a base $\{1, x, y\}$ de $\mathcal{L}(F_1)$.

Da definição de $\mathcal{L}(F_1)$ temos que

$$z \in \mathcal{L}(F_1) \Longrightarrow v_P(z) \geq -v_P(F_1) \forall P \in \mathbb{P}(K),$$

ou seja,

$$v_Q(x), v_Q(y) \geq 0 = -v_Q(F_1) \forall Q \neq F_1$$

e ainda

$$v_{F_1}(x), v_{F_1}(y) \geq -1 = -v_{F_1}(F_1).$$

Mas temos que x e y são transcendentes sobre k e então

$$supp((x)_\infty) \neq \emptyset \neq supp((y)_\infty),$$

ou seja,

$$v_{F_1}(x), v_{F_1}(y) < 0.$$

Logo $v_{F_1}(x) = v_{F_1}(y) = -1$.

Assim temos que $(z) \geq -4F_1$ para todo

$$z \in \mathcal{B} := \{1, x, x^2, x^3, x^4, y, y^2, y^3, y^4, xy, xy^2, xy^3, x^2y, x^2y^2, x^3y\}.$$

Mas esse conjunto tem 15 elementos e

$$l(4F_1) = deg(4F_1) - g + 1 = 4 \cdot 4 - 3 + 1 = 14$$

pois $deg(4F_1) = 16 \geq 5 = 2g - 1$.

Assim, existe uma combinação linear não nula do conjunto $\mathcal{B}$. Seja $f(x, y)$ o polinômio dado por essa combinação.

Seja z uma razão de diferenciais de primeiro tipo em K/k (Definição 2.5.6), então existem D_1, D_2 elementos em $|C|$ a classe canônica de K/k tal que

$$(z) = D_1 - D_2 = (D_1 - F_1) + (F_1 - D_2) = (z') - (z'') = (z'/z'').$$

Assim, temos que $z = az'/z''$ onde $z', (z'')^{-1} \in \mathcal{L}(P) \subseteq k(x, y)$ e $a \in k$.

Portanto, $z \in k(x, y)$, ou seja, o corpo $K' \supseteq k$ gerado pelas razões de diferenciais de primeiro tipo está contido em $k(x, y)$.

Se $K \neq k(x, y) \supseteq K'$, então pela definição de corpo de funções hiperelípticas (definição A.1.6) teríamos que K/k o é, o que é um absurdo. Portanto $K = k(x, y)$.

Assim, a curva algébrica afim associada à K/k será a curva dada por $V(f)$. Pela fórmula do gênero em termos dos δ-invariantes, temos que

$$g = \frac{(n-1)(n-2)}{2} - \sum_{P \in C} \delta_P,$$

ou seja, $\delta_P = 0 \forall P \in C$ pois a curva acima tem gênero $g = 3$ e grau $n = 4$. Temos então que a curva não tem singularidades e consequentemente o polinômio $f(x, y)$ é absolutamente irredutível.

Construímos o polinômio homogêneo $F(X, Y, Z)$ associado à f, e esse definirá o modelo canônico de K/k em $\mathbb{P}^2(k)$.

Como as imposições sobre x e y são apenas que $\{1, x, y\}$ seja uma base de $\mathcal{L}(F_1)$, podemos tomar x e y de modo que

$$(x) = F_2 - F_1 \text{ e } (y) = F_0 - F_1$$

onde F_2 é outro place de grau 4 e $F_0 = 2Q_1$ ou $Q_1 + Q_2$.

Como da Proposição 3.2.2, os divisores canônicos de K/k são a intersecção da curva com as retas racionais de $\mathbb{P}^2(k)$, então podemos considerar, fazendo transformação projetiva se necessário, que

$$F_2 = (F)(X),\ F_1 = (F)(Z) \text{ e } F_0 = (F)(Y).$$

Seja

$$\begin{aligned} F(X, Y, Z) = \ & eY^4 + (a_1X + a_0Z)Y^3 + (b_2X^2 + b_1XZ + b_0Z^2)Y^2 \\ & +(c_3X^3 + c_2X^2Z + c_1XZ^2 + c_0Z^3)Y \\ & +(d_4X^4 + d_3X^3Z + d_2X^2Z^2 + d_1XZ^3 + d_0Z^4). \end{aligned}$$

Como o divisor $(F)(Z)$ é um place de grau 4, temos que o polinômio

$$F_Z(X, Y) := F(X, Y, 0) = eY^4 + a_1XY^3 + b_2X^2Y^2 + c_3X^3Y + d_4X^4$$

é absolutamente irredutível, ou seja, as únicas possibilidades para F_Z são

$$\begin{aligned} F_Z = \ & Y^4 + XY^3 + X^2Y^2 + X^3Y + X^4 \text{ ou} \\ & Y^4 + X^3Y + X^4 \text{ ou} \\ & Y^4 + XY^3 + X^4. \end{aligned}$$

Analogamente, temos que

$$\begin{aligned} F_X = \; & Y^4 + ZY^3 + Z^2Y^2 + Z^3Y + Z^4 \text{ ou} \\ & Y^4 + Z^3Y + Z^4 \text{ ou} \\ & Y^4 + ZY^3 + Z^4. \end{aligned}$$

Como F_0 foi tomado com sendo $2Q_1$ ou $Q_1 + Q_2$ temos que o polinômio

$$F_Y = X^4 + d_3X^3Z + d_2X^2Z^2 + d_1XZ^3 + Z^4$$

se decompõe como um produto de dois polinômios irredutíveis de grau 2, sendo que eles são distintos se $F_0 = Q_1 + Q_2$ ou iguais se $F_0 = 2Q_1$.

Mas o único polinômio irredutível de grau 2 nesse caso é $G(X, Z) = X^2 + XZ + Z^2$, ou seja,

$$F = 2Q_1 \text{ e } F_Y(X, Z) = X^4 + X^2Z^2 + Z^4.$$

Assim, temos 36 possibilidades para $F(X, Y, Z)$ que são representadas na Tabela 4.1 como o elemento

$$(a_1, a_0, b_2, b_1, b_0, c_3, c_2, c_1, c_0) \in \mathbb{F}_2^9,$$

tendo em vista que os elementos

$$e = 1, d_4 = 1, d_3 = 0, d_2 = 1, d_1 = 0 \text{ e } d_0 = 1$$

não variam.

Tabela 4.1: $(a_1, a_0, b_2, b_1, b_0, c_3, c_2, c_1, c_0)$

1.	(1, 1, 1, 0, 1, 1, 0, 1, 1)	19.	(0, 1, 0, 0, 0, 1, 1, 0, 0)
2.	(1, 1, 1, 1, 1, 1, 0, 0, 1)	20.	(0, 1, 0, 1, 0, 1, 1, 1, 0)
3.	(1, 1, 1, 0, 1, 1, 1, 0, 1)	21.	(0, 0, 0, 0, 0, 1, 0, 1, 1)
4.	(1, 1, 1, 1, 1, 1, 1, 1, 1)	22.	(0, 0, 0, 1, 0, 1, 0, 0, 1)
5.	(1, 1, 1, 0, 0, 1, 0, 1, 0)	23.	(0, 0, 0, 0, 0, 1, 1, 0, 1)
6.	(1, 1, 1, 1, 0, 1, 0, 0, 0)	24.	(0, 0, 0, 1, 0, 1, 1, 1, 1)
7.	(1, 1, 1, 0, 0, 1, 1, 0, 0)	25.	(1, 1, 0, 0, 1, 0, 0, 1, 1)
8.	(1, 1, 1, 1, 0, 1, 1, 1, 0)	26.	(1, 1, 0, 1, 1, 0, 0, 0, 1)
9.	(1, 0, 1, 0, 0, 1, 0, 1, 1)	27.	(1, 1, 0, 0, 1, 0, 1, 0, 1)
10.	(1, 0, 1, 1, 0, 1, 0, 0, 1)	28.	(1, 1, 0, 1, 1, 0, 1, 1, 1)
11.	(1, 0, 1, 0, 0, 1, 1, 0, 1)	29.	(1, 1, 0, 0, 0, 0, 0, 1, 0)
12.	(1, 0, 1, 1, 0, 1, 1, 1, 1)	30.	(1, 1, 0, 1, 0, 0, 0, 0, 0)
13.	(0, 1, 0, 0, 1, 1, 0, 1, 1)	31.	(1, 1, 0, 0, 0, 0, 1, 0, 0)
14.	(0, 1, 0, 1, 1, 1, 0, 0, 1)	32.	(1, 1, 0, 1, 0, 0, 1, 1, 0)
15.	(0, 1, 0, 0, 1, 1, 1, 0, 1)	33.	(1, 0, 0, 0, 0, 0, 0, 1, 1)
16.	(0, 1, 0, 1, 1, 1, 1, 1, 1)	34.	(1, 0, 0, 1, 0, 0, 0, 0, 1)
17.	(0, 1, 0, 0, 0, 1, 0, 1, 0)	35.	(1, 0, 0, 0, 0, 0, 1, 0, 1)
18.	(0, 1, 0, 1, 0, 1, 0, 0, 0)	36.	(1, 0, 0, 1, 0, 0, 1, 1, 1)

Apresentamos na Tabela 4.2 as classes de isomorfismos das curvas dadas em 4.1, onde

$$(a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}, a_{31}, a_{32}, a_{33}) \in \mathbb{F}_2^9$$

Tabela 4.2: $T := (a_{11}, a_{12}, a_{13}, a_{21}, a_{22}, a_{23}, a_{31}, a_{32}, a_{33})(V(F)) = N$ de 4.1

$y^4 + xy^3 + (x+1)y$	(0, 0, 1, 1, 0, 1, 1, 1, 1)	4
$+(x^4 + x^2 + 1)$	(0, 0, 1, 0, 1, 0, 1, 1, 1)	5
	(0, 1, 1, 1, 1, 0, 1, 0, 0)	6
	(0, 1, 1, 1, 1, 1, 1, 0, 1)	12
	(0, 0, 1, 1, 1, 1, 1, 0, 1)	16
	(0, 0, 1, 0, 1, 0, 1, 0, 1)	17
	(0, 0, 1, 1, 1, 0, 1, 0, 0)	18
	(0, 0, 1, 0, 1, 0, 1, 0, 0)	19
	(0, 1, 1, 1, 0, 1, 1, 1, 1)	24
	(1, 0, 1, 0, 1, 1, 0, 0, 1)	26
	(1, 0, 0, 0, 1, 0, 1, 1, 1)	27
	(1, 0, 1, 0, 1, 0, 0, 0, 1)	29
	(1, 0, 1, 0, 1, 0, 1, 0, 0)	31
	(1, 0, 0, 0, 1, 0, 0, 0, 1)	33
	(1, 0, 0, 0, 1, 1, 0, 0, 1)	34
	(1, 0, 0, 0, 1, 0, 1, 0, 1)	35
$y^4 + xy^3 + (x+1)y$	(0, 0, 1, 0, 1, 1, 1, 1, 1)	1
$+(x^4 + x^3 + 1)$	(0, 1, 1, 0, 0, 1, 1, 1, 0)	3
	(0, 1, 1, 0, 0, 1, 1, 1, 1)	9
	(0, 0, 1, 0, 1, 1, 1, 1, 0)	11
	(0, 0, 1, 0, 1, 1, 1, 0, 1)	13
	(0, 0, 1, 0, 1, 1, 1, 0, 0)	15
	(0, 1, 1, 0, 0, 1, 1, 0, 1)	21
	(0, 1, 1, 0, 0, 1, 1, 0, 0)	23
$y^4 + xy^3 + xy^2 + (x^2 + x + 1)y$	(0, 0, 1, 0, 1, 0, 1, 1, 0)	8
$+(x^4 + x^2 + 1)$	(0, 0, 1, 0, 1, 0, 1, 1, 1)	10
	(0, 0, 1, 0, 1, 0, 1, 0, 1)	14
	(0, 0, 1, 0, 1, 0, 1, 0, 0)	20
	(1, 0, 0, 0, 1, 0, 0, 1, 1)	28
	(1, 0, 0, 0, 1, 0, 0, 0, 1)	36
$y^4 + (x+1)y^3 + x^2y^2 + (x^3 + x^2)y$	(0, 1, 0, 1, 0, 1, 0, 1, 1)	7
$+(x^4 + x^2 + 1)$	(0, 0, 1, 1, 1, 1, 0, 1, 1)	25
	(0, 0, 1, 0, 1, 1, 1, 0, 0)	30
$y^4 + xy^2 + (x^3 + 1)y$	(0, 0, 1, 0, 1, 0, 1, 1, 0)	2
$+(x^4 + x^2 + 1)$	(0, 0, 1, 0, 1, 0, 1, 0, 0)	22
	(0, 0, 1, 1, 0, 1, 0, 1, 1)	32

representa o automorfismo projetivo de $\mathbb{P}^2(\mathbb{F}_2)$ que leva a curva $V(F)$ dada à esquerda para a curva dada na direita pelo número correspondente à Tabela 4.1.

Vamos mostrar que a primeira classe de curvas dada na Tabela 4.2 é a única que atende as propriedades requeridas para $V(F)$, onde na segunda classe temos que $n_2 < 2$ e as três últimas são redutíveis sobre $\mathbb{F}_4$. Chamemos de $h_i, i = 1, \cdots, 5$ os polinômios dados na tabela 4.2 e $H_i, i = 1, \cdots, 5$ suas homogeinizações.

Como todas as curvas não tem pontos racionais e n_3 depende de n_2, basta mostrar que a primeira tem dois places de grau 2 e a segunda menos que dois. Como descrito anteriormente, a classe dos divisores canônicos é dada por

$$\{2Q_1, 2Q_2, F_i\}, i = 1, \cdots, 5$$

se tiverem dois places de grau dois e

$$\{2Q_1, F_i\}, i = 1, \cdots, 6 \text{ ou } \{F_i\}, i = 1, \cdots, 7$$

se o corpo de funções tiver apenas um ou nehum place de grau 2. Mas os divisores canônicos são dados pelas intersecções das sete retas racionais de $\mathbb{P}^2(\mathbb{F}_2)$ com a curva.

Assim, basta verificar se o polinômio obtido restringindo F à equação dessas retas é irredutível ou o quadrado de um irredutível de grau dois. Nas Tabelas 4.3 e 4.4 damos as retas e a restrição de F a cada uma delas.

Tabela 4.3: Divisores canônicos de $V(H_1)$

$L_1 = X + Y + Z$	$H_1(L_1) = X^4 + XY^3 + Y^4$
$L_2 = X + Y$	$H_1(L_2) = X^4 + XZ^3 + Z^4$
$L_3 = X + Z$	$H_1(L_3) = X^4 + XY^3 + Y^4$
$L_4 = Y + Z$	$H_1(L_4) = X^4 + X^2Y^2 + Y^4$
$L_5 = X$	$H_1(L_5) = Y^4 + YZ^3 + Z^4$
$L_6 = Y$	$H_1(L_6) = X^4 + X^2Z^2 + Z^4$
$L_7 = Z$	$H_1(L_7) = X^4 + XY^3 + Y^4$

Tabela 4.4: Divisores canônicos de $V(H_2)$

$L_1 = X + Y + Z$	$H_2(L_1) = X^4 + X^3Y + X^2Y^2 + XY^3 + Y^4$
$L_2 = X + Y$	$H_2(L_2) = X^4 + X^3Y + X^2Z^2 + XZ^3 + Z^4$
$L_3 = X + Z$	$H_2(L_3) = X^4 + XY^3 + Y^4$
$L_4 = Y + Z$	$H_2(L_4) = X^4 + X^3Y + Y^4$
$L_5 = X$	$H_2(L_5) = Y^4 + YZ^3 + Z^4$
$L_6 = Y$	$H_2(L_6) = X^4 + X^3Z + Z^4$
$L_7 = Z$	$H_2(L_7) = X^4 + XY^3 + Y^4$

Na Tabela 4.3, vemos que os polinômios

$$H_1(L_4) = X^4 + X^2Y^2 + Y^4 = (X^2 + XY + Y^2)^2 \text{ e}$$
$$H_1(L_6) = X^4 + X^2Z^2 + Z^4 = (X^2 + XZ + Z^2)^2$$

correspondem aos divisores $2Q_1$ e $2Q_2$ e consequentemente o corpo de funções associado à $V(H_1)$ tem dois places de grau dois.

Por outro lado, todos os polinômios da Tabela 4.4 são irredutíveis e logo o corpo de funções associado à $V(H_2)$ tem menos de dois places de grau 2.

Falta mostrar que os polinômios $H_i, i = 3, 4, 5$ são redutíveis sobre $\mathbb{F}_4$. Mas seja α um gerador de $\mathbb{F}_4$, então a Tabela 4.5 mostra decomposições dos h_i.

Tabela 4.5: Decomposições dos $h_i, i = 3, 4, 5$

$h_3 = y^4 + xy^3 + xy^2 + (x^2 + x + 1)y$ $+(x^4 + x^2 + 1)$	$(y^2 + (1 + \alpha x)y + \alpha x^2 + \alpha^2)$ $(y^2 + (1 + \alpha^2 x)y + \alpha^2 x^2 + \alpha)$
$h_4 = y^4 + (x + 1)y^3 + x^2y^2$ $+(x^3 + x^2)y + (x^4 + x^2 + 1)$	$(y^2 + (\alpha x + \alpha)y + x^2 + \alpha)$ $(y^2 + (\alpha^2 x + \alpha^2)y + x^2 + \alpha^2)$
$h_5 = y^4 + xy^2 + (x^3 + 1)y$ $+(x^4 + x^2 + 1)$	$(y^2 + (1 + x)y + \alpha^2 x^2 + \alpha^2 x + \alpha^2)$ $(y^2 + (1 + x)y + \alpha x^2 + \alpha x + \alpha)$

Provamos assim, que a menos de isomorfismo, existe um único corpo de funções algébricas com $h = 2, g = 3$ e $n_1 = 0$ e ele é dado por

$$K = k(x, y) \text{ com } y^4 + xy^3 + (x + 1)y + (x^4 + x^2 + 1) = 0.$$

Caso **(ii)**
Como $n_1 = 1, n_3 = 3 - n_2, 0 \leq n_2 \leq 3$ temos que

$$L(t) = 1 - 2t - n_2t^2 + (3 - 3n_2)t^3 + 2n_2t^4 - 8t^5 + 8t^6.$$

Como antes, podemos excluir os casos $n_2 = 2$ ou 3. Ficamos assim com

$$n_1 = 1, n_2 = 0, n_3 = 3 \text{ ou } n_1 = 1, n_2 = 1, n_3 = 2.$$

Denotemos por P o único ponto racional do modelo canônico de K/k. Como K/k é não hiperelíptico, temos pelas proposições 3.3.2, 3.3.3 e 3.3.4 que

$$l(k - P) = l(k) - 1 = g - 1 = 2 \text{ e } l(k - 2P) = l(k) - 2 = 1.$$

(Obs. Estamos denotando por k um divisor canônico genérico e o corpo k, porém fica claro quando estamos falando do corpo ou do divisor). Assim, existem dois divisores D_1, D_2 de grau 3 mutuamente equivalentes e um divisor D de grau 2 tais que

$$k \sim D_1 + P \sim D_2 + P \sim D + 2P.$$

- $n_1 = 1, n_2 = 0, n_3 = 3.$

  Como $n_2 = 0$, o único D tal que

  $$k \sim D + 2P$$

  é $2P$ e temos que $l(4P) = 3$ e $l(3P) = 2$. Então $|k - P|$ tem três $((q^{l(k-P)} - 1)/q - 1 = 3)$ elementos, ou seja,

  $$|k - P| = \{3P, T_1, T_2\}$$

  onde T_1, T_2 são places de grau 3.

Assim, podemos escolher $x \in K$ de modo que $(x) = T_1 - 3P$ e então $\{1, x\}$ será uma base de $\mathcal{L}(3P)$. Seja então $\{1, x, y\}$ uma base de $\mathcal{L}(4P)$ e então y tem um pólo em P de ordem exatamente 4, pois

$$-4 = -v_P(4P) \leq v_P(y) < -v_P(3P) = -3 \Longrightarrow v_P(y) = -4.$$

Como $deg(12P) = 12 \geq 5 = 2g - 1$ temos que

$$l(12P) = deg(12P) - g + 1 = 12 - 3 + 1 = 10.$$

Além disso, os 11 elementos

$$\{1, x, x^2, x^3, x^4, y, xy, x^2y, y^2, xy^2, y^3\}$$

estão em $\mathcal{L}(12P)$, ou seja, existe uma relação

$$y^3 + \phi_1(x)y^2 + \phi_2(x)y + \phi_4(x) = 0,$$

onde $\phi_i \in k[x], i = 1, 2$ e 4, $deg(\phi_1) \leq 1, deg(\phi_2) \leq 2$ e $deg(\phi_4) = 4$, pois x^3 e y^4 são as únicas funções tendo um pólo de ordem 12 em P, já que

$$[K : k(x)] = deg((x)_\infty) = deg(3P) = 3$$

e

$$[K : k(y)] = deg((y)_\infty) = deg(4P) = 4.$$

Fazendo a mudança de variável

$$y + \phi_1(x) \longmapsto y,$$

a equação se torna

$$y^3 + (a_2x^2 + a_1x + a_0)y + (x^4 + b_3x^3 + b_2x^2 + b_1x + b_0) = 0.$$

Procedendo de maneira análoga ao caso anterior podemos supor $(x) = T_1 - 3P$ onde T_1 é um place de grau 3 e

$$(y) = Q - 4P = (F)(Y) - (F)(X),$$

onde Q é um place de grau 4. Assim, temos que

$$F(0, Y, Z) = Y^3Z + a_0YZ^3 + b_0Z^4 = Z(Y^3 + a_0YZ^2 + b_0Z^3),$$

ou seja, $a_0 = b_0 = 1$. Do fato de

$$F(X, 0, Z) = X^4 + b_3X^3Z + b_2X^2Z^2 + b_1XZ^3 + b_0Z^4$$

ser irredutível, temos que

$$\begin{aligned} F(X, 0, Z) = \; & X^4 + XZ^3 + Z^4, \\ & X^4 + X^3Z + Z^4 \text{ ou} \\ & X^4 + X^3Z + X^2 + Z^2 + XZ^3 + Z^4. \end{aligned}$$

Tabela 4.6: $(a_2, a_1, b_3, b_2, b_1)$

1. (1, 1, 1, 1, 1)	7. (0, 1, 0, 0, 1)
2. (1, 0, 1, 1, 1)	8. (0, 0, 0, 0, 1)
3. (0, 1, 1, 1, 1)	9. (1, 1, 1, 0, 0)
4. (0, 0, 1, 1, 1)	10. (1, 0, 1, 0, 0)
5. (1, 1, 0, 0, 1)	11. (0, 1, 1, 0, 0)
6. (1, 0, 0, 0, 1)	12. (0, 0, 1, 0, 0)

A Tabela 4.6 apresenta as possibilidades para

$$(a_2, a_1, b_3, b_2, b_1) \in \mathbb{F}_2^5.$$

Os casos 2., 3., 6., 7., 10. e 11. não servem, pois do contrário o ponto $(1:1:1) \in \mathbb{P}^2(k)$ seria outro ponto racional, onde sabemos que o único ponto racional da curva é $(0:1:0)$. Prova-se, usando argumentos semelhantes aos usados anteriormente, que existe uma única solução a menos de isomorfismo, a saber,

$$K = k(x, y) \text{ com } y^3 + (x^2 + x + 1)y + (x^4 + x^3 + 1) = 0$$

para o caso em que $n_1 = 1, n_2 = 0, n_3 = 3$.

- $n_1 = 1, n_2 = 1, n_3 = 2$.

  Sabemos que existe um divisor positivo de grau 2 tal que $k \sim D + 2P$. Duas coisas podem acontecer: $D = 2P$ ou $D = Q$, onde Q é o único place de grau 2. Em qualquer caso,

  $$2P \nsim Q \text{ e } 4P \sim 2Q.$$

  1. $4P$ é canônico.
     Então $l(4P) = 3$ e $l(3P) = 2$ e

     $$|k - P| = \{3P, T_1, T_2\}$$

     onde T_1 e T_2 são places de grau 3 e

     $$|k| = \{4P, T_1 + P, T_2 + P, F_1, F_2, F_3\},$$

     onde F_1, F_2 e F_3 são places de grau 4. Escolhemos $x, y \in K$ de modo que

     $$(x) = T_1 - 3P \text{ e } (y) = F_1 - 4P.$$

     Por isso, $\{1, x\}$ é uma base de $\mathcal{L}(3P)$ e $\{1, x, y\}$ base de $\mathcal{L}(4P)$. Procedendo de maneira análoga aos casos anteriores, temos que a menos de isomorfismo, existe uma única solução, a saber,

     $$K = k(x, y) \text{ com } y^3 + y + (x^4 + x^3 + 1) = 0$$

     para $n_1 = 1, n_2 = 1$ e $n_3 = 2$.

2. $2P + Q$ é canônico.
Temos então

$$l(2P + Q) = 3 \text{ e } l(P + Q) = 2.$$

Ainda

$$|k - P| = \{P + Q, T_1, T_2\}$$

e

$$|k| = \{2P + Q, P + T_1, P + T_2, F_1, \cdots, F_4\},$$

onde T_i são places de grau 3 e F_j são places de grau 4. Escolhemos $x, y \in K$ de modo que

$$(x) = 2P + Q - F_1 \text{ e } (y) = F_2 - F_1.$$

Então $\{1, x, y\}$ é base de $\mathcal{L}(F_1)$. Procedemos como anteriormente obtemos o polinômio homogêneo

$$\begin{aligned} F(X,Y,Z) = \; & eY^4 + (a_1X + a_0Z)Y^3 + (b_2X^2 + b_1XZ + b_0Z^2)Y^2 \\ & +(c_3X^3 + c_2X^2Z + c_1XZ^2 + c_0Z^3)Y \\ & +(d_4X^4 + d_3X^3Z + d_2X^2Z^2 + d_1XZ^3 + d_0Z^4). \end{aligned}$$

Considerando

$$(x) = (F)(X) - (F)(Z) \text{ e } (y) = (F)(Y) - (F)(Z)$$

temos que

$$F(X,0,Z) = d_4X^4 + d_3X^3Z + d_2X^2Z^2 + d_1XZ^3 + d_0Z^4$$

é irredutível, ou seja,

$$\begin{aligned} F(X,0,Z) \in \{ & X^4 + X^3Z + Z^4, X^4 + XZ^3 + Z^4, \\ & X^4 + X^3Z + X^2Z^2 + XZ^3 + Z^4\}. \end{aligned}$$

Ainda

$$\begin{aligned} F(X,Y,0) &= eY^4 + a_1XY^3 + b_2X^2Y^2 + c_3X^3Y + X^4 \\ &\in \{X^4 + X^3Y + Y^4, X^4 + XY^3 + Y^4, \\ &\quad X^4 + X^3Y + X^2Y^2 + XY^3 + Y^4\}. \end{aligned}$$

Como $(F)(X) = 2P + Q$, o polinômio $F(0,Y,Z)$ é o produto de um polinômio de grau 2 irredutível por um de grau 1 ao quadrado, ou seja,

$$\begin{aligned} Y^4 + a_0ZY^3 + b_0Y^2Z^2 + c_0YZ^3 + Z^4 &= (Y^2 + YZ + Z^2)(Y^2 + Z^2) \\ &= Y^4 + YZ^3 + Y^3Z + Z^4. \end{aligned}$$

Usando argumentos como os usados anteriormente, prova-se que tal situação não é possível.

Concluímos assim, que as únicas possibilidades para K/k ter gênero $g = 3$ e $h = 2$ é para $K = k(x, y)$ com:

$$\begin{array}{ll} y^4 + xy^3 + (x+1)y + (x^4 + x^2 + 1) = 0, & n_1 = 0, n_2 = 2, n_3 = 2; \\ y^3 + (x^2 + x + 1)y + (x^4 + x^3 + 1) = 0, & n_1 = 1, n_2 = 0, n_3 = 3; \\ y^3 + y + (x^4 + x^3 + 1) = 0, & n_1 = 1, n_2 = 2, n_3 = 2; \end{array}$$

4.4.2 $g = 4$

Da proposição 4.1.1, temos que $h = 2$ é equivalente a $n_1 = 0$ e $n_2^2 = 3n_2 - 2n_4 + 4$. Assim, temos que

$$L(t) = 1 + a_1 t + a_2 t^2 + a_3 t^3 + a_4 t^4 + 2a_3 t^5 + 4a_2 t^6 + 8a_1 t^7 + 16t^8,$$

onde

$$\begin{cases} a_1 = -3 \\ a_2 = n_2 + 2 \\ a_3 = n_3 - 3n_2 \\ a_4 = 4n_2 - 3n_3 + 2 \end{cases}$$

Nos casos em que $n_1 = n_2 = 0, 0 \leq n_3 \leq 2, n_4 = 2$ e $n_1 = 0, n_2 = 1, n_3 = 0, n_4 = 3$ temos que L tem 4 raízes com quadrado absoluto diferente de $1/2$. Assim, os casos possíveis são:

(i) $n_1 = n_2 = 0, 3 \leq n_3 \leq 6, n_4 = 2$.

(ii) $n_1 = 0, n_2 = 1, 1 \leq n_3 \leq 3, n_4 = 3$.

(iii) $n_1 = 0, n_2 = 2, n_3 = 0, n_4 = 3$.

A função zeta é então dada por

$$Z(t) = 1 + n_2 t^2 + n_3 t^3 + \frac{n_4 + n_2(n_2+1)}{2} t^4 + 6t^5 + 22t^6 + O(t^7).$$

Teorema 4.4.1. *Seja K/k um corpo de funções não hiperelíptico de gênero $g = 4$ e $\mathcal{C}$ seu modelo canônico em $\mathbb{P}^3(k)$. Então $\mathcal{C}$ é a intersecção completa de uma única quádrica completamente irredutível $\mathcal{D}$ e uma superfície cúbica $\mathcal{E}$ que pode ser escolhida racionalmente sobre k.*

Demonstração. [5] □

Teorema 4.4.2. *A menos de isomorfismo, as únicas superfícies quádricas $\mathcal{D}$ absolutamente irredutíveis sobre $\mathbb{F}_q$ são as seguintes:*

- *$x^2 + yz = 0$. A superfície singular $\mathcal{D}$ é um cone com $(q^2 + q + 1)$ pontos racionais sobre k. Existe um único sistema gerador racional, a saber, as linhas racionais através do vértice.*
- *$xy + \gamma(z, t) = 0$, onde $\gamma(z, t)$ é uma forma binária irredutível. $\mathcal{D}$ é uma quádrica elíptica. Se $k = \mathbb{F}_2$, temos $\gamma(z, t) = z^2 + zt + t^2$. $\mathcal{D}$ é suave com $(q^2 + 1)$ pontos racionais sobre k e não contém linhas racionais.*

- $xy + zt = 0$. *$\mathcal{D}$ é uma quádrica hiperbólica suave com $(q+1)^2$ pontos racionais sobre k. Ela tem dois conjuntos de geradores racionais.*

Demonstração. [6] □

Lema 4.4.2. *Seja K/k um corpo de funções não hiperelíptico de gênero $g = 4$ e seja $\mathcal{C}$ seu modelo canônico em $\mathbb{P}^3(k)$. Se denotarmos por N o número de sistemas lineares g_3^1 de K/k, então temos que $0 \leq N \leq 2$ e:*

(1) *$N = 0$ se e somente se $\mathcal{C}$ está em uma quádrica elíptica.*

(2) *$N = 1$ se e somente se $\mathcal{C}$ está em um cone.*

(3) *$N = 2$ se e somente se $\mathcal{C}$ está em uma quádrica hiperbólica.*

Demonstração. Vamos mostrar que os únicos sistemas lineares g_3^1 de $\mathcal{C}$ são obtidos por

$$\{(\mathcal{C})(L_i)|i = 1, 2, 3\}$$

onde $\{L_i|i = 1, 2, 3\}$ é um sistema gerador de $\mathcal{D}$. Assim, temos que N é igual ao número de conjuntos geradores de $\mathcal{D}$ e pelo Teorema 4.4.2 temos provado o lema.

Suponha que existe um g_3^1 em K/k e seja $D \in g_3^1$. Pelo teorema de Riemann-Roch temos que

$$l(k - D) - l(D) = deg(D) + 1 - g = 3 + 1 - 4 = 0,$$

ou seja, $l(k - D) = l(D) = 2$. Assim, temos dois divisores distintos $D_1, D_2 \in \mathcal{D}_K$ tal que

$$k \sim D + D_1 \sim D + D_2.$$

Mas os divisores canônicos de K/k são obtidos pela intersecção dos planos racionais de $\mathbb{P}^3(k)$ com o modelo canônico de K/k, ou seja,

$$D + D_i = (V_i)(\mathcal{C}), i = 1, 2.$$

Seja L a intersecção dos planos V_1 e V_2. Então temos que

$$D + D_1 = (V_1)(\mathcal{C}) = (L)(\mathcal{C}) + D_1'$$

e

$$D + D_2 = (V_2)(\mathcal{C}) = (L)(\mathcal{C}) + D_2',$$

onde $supp(D_1') \cap supp(D_2') = \emptyset$.

Portanto,

$$D \leq (L)(\mathcal{C}), \text{ ou seja, } supp(D) \subseteq L.$$

Vamos mostrar inicialmente que $\{(\mathcal{C})(L_i)|i = 1, 2, 3\}$ é um g_3^1. Sejam V_1 o plano gerado por L_1 e L_2, V_2 gerado por L_2 e L_3 e V_3 por L_3 e L_1. Como estes planos são gerados por linhas racionais eles também o são. Assim, $(V_i)(\mathcal{C})$ é um divisor canônico para $i = 1, 2, 3$, ou seja,

$$(V_i)(\mathcal{C}) \sim (V_j)(\mathcal{C}) \text{ para todo } 1 \leq i, j \leq 3.$$

Mas

$$\begin{aligned}(V_1)(\mathcal{C}) &= (L_1)(\mathcal{C}) + (L_2)(\mathcal{C})\\ (\text{resp. } (V_2)(\mathcal{C}) &= (L_2)(\mathcal{C}) + (L_3)(\mathcal{C}))\\ (\text{resp. } (V_3)(\mathcal{C}) &= (L_3)(\mathcal{C}) + (L_1)(\mathcal{C})).\end{aligned}$$

Assim,

$$\begin{aligned}(V_1)(\mathcal{C}) \sim (V_2)(\mathcal{C}) &\Longrightarrow (L_1)(\mathcal{C}) + (L_2)(\mathcal{C}) \sim (L_2)(\mathcal{C}) + (L_3)(\mathcal{C})\\ &\Longrightarrow (L_1)(\mathcal{C}) \sim (L_3)(\mathcal{C})\\ &\text{e}\\ (V_1)(\mathcal{C}) \sim (V_3)(\mathcal{C}) &\Longrightarrow (L_1)(\mathcal{C}) + (L_2)(\mathcal{C}) \sim (L_3)(\mathcal{C}) + (L_1)(\mathcal{C})\\ &\Longrightarrow (L_2)(\mathcal{C}) \sim (L_3)(\mathcal{C}).\end{aligned}$$

Portanto,

$$(L_1)(\mathcal{C}) \sim (L_2)(\mathcal{C}) \sim (L_3)(\mathcal{C}).$$

Considere $D = (L_1)(\mathcal{C})$. Temos então que

$$l(k - D) - l(D) = deg(D) + 1 - g = 0,$$

ou seja,

$$l(D) = l(k - D) \leq l(k - P - Q) = l(k) - 2 = 2,$$

onde $P, Q \in supp(D)$ e usamos que K/k é não hiperelíptico para termos que

$$l(k - P - Q) = l(k) - 2.$$

Mas assim temos que

$$3 \leq (q^{l(D)} - 1)/(q - 1) \leq 3 \Longrightarrow l(D) = 2.$$

Portanto $\{(\mathcal{C})(L_i) | i = 1, 2, 3\}$ é um g_3^1.

Por outro lado, vimos que cada divisor em um g_3^1 está contido em uma reta racional. Além disso, se escrevermos

$$D = P_1 + P_2 + P_3$$

temos que esses pontos estão em uma reta. Mas uma reta que não está em $\mathcal{D}$ intersecta $\mathcal{D}$ (consequentemente $\mathcal{C}$) em no máximo dois pontos. Assim, cada g_3^1 forma um conjunto gerador para $\mathcal{D}$. □

Sejam K_1/k e K_2/k corpos de funções algébricas de gênero $g = 4$ e $\mathcal{C}_1$ e $\mathcal{C}_2$ seus modelos canônicos. Assuma que

$$\mathcal{C}_1 = \mathcal{D} \cap \mathcal{E}_1 \text{ e } \mathcal{C}_2 = \mathcal{D} \cap \mathcal{E}_2$$

para alguma quádrica $\mathcal{D}$. Como $\mathcal{C}_1$ e $\mathcal{C}_2$ são canônicos, então seus corpos de funções serão k-isomorfos se e somente se existe um automorfismo projetivo σ de $\mathbb{P}_3(k)$ fixando a quádrica $\mathcal{D}$ e tal que $\sigma(\mathcal{E}_1) = \mathcal{E}_2$.

Vamos dividir o estudo em dois casos:

- K/k tem um sistema linear g_3^1. Isto implica que existe $x \in K$ transcendente sobre k tal que $[K : k(x)] = 3$.
- K/k não tem sistema linear do tipo g_3^1. Isto implica que para todo $x \in K$ transcendente sobre k temos que $[K : k(x)] > 3$.

Existe um g^1_3

Lema 4.4.3. *Seja K/k um corpo de funções não hiperelíptico de gênero $g = 4$ e tal que $h = 2$. Se existe ao menos um sistema linear do tipo g^1_3, então existe um place T de grau 3 tal que $l(T) = 2$ e $l(2T) = 4$. Neste caso, existe exatamente um sistema linear do tipo g^1_3.*

Demonstração. Como $h = 2$ temos que K/k atende a uma das condições **(i)**,**(ii)**,**(iii)**. Mas em todos esses casos os únicos divisores positivos de grau 3 são os próprios places. Assim, temos que a existência de um g^1_3 é equivalente a termos $n_3 \geq 3$. Estamos assim na situação **(i)** ou no caso **(iii)** com $n_3 \geq 3$. Assim, o sistema g^1_3 é dado por

$$\mathcal{D}^+_{3,1} = \{T_1, T_2, T_3\}$$

onde $T_1 \sim T_2 \sim T_3$ com $l(T_i) = 2, i = 1, 2, 3$. Se $n_3 \geq 4$ temos que

$$\mathcal{D}^+_{3,2} = \{T_4, \cdots, T_{n_3}\}$$

é o conjunto de divisores de grau 3, onde

$$T_i \nsim T_j \text{ se } 1 \leq i \leq 3 \text{ e } 4 \leq j \leq n_3.$$

Se $n_3 \geq 5$ temos que $l(T_4) = 2$ pois

$$2 \leq ||T_4|| = (q^{l(T_4)} - 1)/(q - 1) = 2^{l(T_4)} - 1 \Longrightarrow l(T_4) \geq 2$$

e logo igual a dois, pois $n_3 \leq 6$, ou seja, $\mathcal{D}^+_{3,2}$ seria outro g^1_3. Vamos mostrar que isso é impossível.

Temos que $A_6 = n_3(n_3 + 1)/2 + n_6$ e pelos coeficientes da função zeta, obtemos que esse valor é igual a 22, ou seja, n_6 deve ser igual a 1 (seja P este place). Consideremos os seguintes conjuntos de places formados pela forma $T_i + T_j, 1 \leq i, j \leq 6$:

(a) $C_1 = \{T_i + T_j | i, j = 1, 2, 3\}$. Este conjunto tem 6 elementos.

(b) $C_2 = \{T_i + T_j | i, j = 4, 5, 6\}$. Este conjunto tem 6 elementos.

(c) $C_3 = \{T_i + T_j | i = 1, 2, 3 \text{ e} j = 4, 5, 6\}$. Este conjunto tem 9 elementos.

Pela construção dos conjuntos, nenhum elemento de C_1 ou C_2 é equivalente a algum de C_3. Mas a classe canônica contém

$$15 = 2^4 - 1 = (q^g - 1)/(q - 1) \text{ elementos,}$$

mas isso é impossível, pois os únicos conjuntos com divisores de grau 6 equivalentes entre si são possivelmente $C_1 \cup C_2 \cup \{P\}$ ou $C_3 \cup \{P\}$ e o primeiro tem 13 elementos enquanto que o segundo tem 10 elementos.

Assim, estamos no caso em que $k = \mathbb{F}_2$ e

$$n_1 = n_2 = 0, n_3 = 3, 4, n_4 = 2 \text{ ou } n_1 = 0, n_2 = 1, n_3 = 3, n_4 = 3.$$

Agora temos que os elementos de C_1 são equivalentes entre si, ou seja,

$$2T_1 \sim T_1 + T_2.$$

Mas $T_i = (\mathcal{C})(L_i), i = 1, 2$ onde L_i são retas racionais distintas de $\mathcal{D}$. Mas daí que o plano V gerado pelas retas L_1 e L_2 é racional, ou seja,

$$T_1 + T_2 = (\mathcal{C})(L_1) + (\mathcal{C})(L_2) = (\mathcal{C})(V)$$

é um divisor canônico. Portanto $deg(2T_1) = g = 4$ pois este é canônico.

Portanto,

$$l(T_1) = 2,\ l(2T_1) = 4 \text{ e } \{T_1, T_2, T_3\} \text{ é o único } g_3^1 \text{ de } K/k.$$

□

Seja T um place de grau 3 de K/k tal que $l(T) = 2$ e $l(2T) = 4$ e seja $\{1, x\}$ uma base de $\mathcal{L}(T)$. Então $(x)_\infty = T$ e $[K : k(x)] = 3$. Como $l(2T) = 4$ existe $y \in \mathcal{L}(2T)\backslash\mathcal{L}(T)$ tal que $\{1, x, x^2, y\}$ é uma base de $\mathcal{L}(2T)$. Temos então que $(y)_\infty = 2T$ e $k(x, y) = K$. Além disso, o conjunto

$$C = \{1, x, \cdots, x^6, y, xy, \cdots, x^4y, y^2, xy^2, x^2y^2, y^3\}$$

está em $\mathcal{L}(6T)$. Porém $\mathcal{L}(6T)$ é um k-espaço vetorial de dimensão 15 e o conjunto C tem 16 elementos, ou seja, existe uma relação

$$F(x, y) := y^3 + \phi_2(x)y^2 + \phi_4(x)y + \phi_6(x) = 0 \tag{4.2}$$

onde $\phi_i(x) \in k[x]$ e $deg(\phi_i) \leq i, i = 2, 4, 6$. Seja $v = y + \phi_2(x)$. Então temos que

$$k(x) \subseteq k(x, v) \subseteq k(x, y),$$

ou seja, $k(x, v) = k(x, y) = K$, pois do contrário $y + \phi_2(x) \in k(x) \Longrightarrow y \in k(x)$. Da equação 4.2 temos que

$$v^3 + \psi_4(x)v + \psi_6(x) = 0, \tag{4.3}$$

onde $\psi_i(x) \in k[x]$ e $deg(\psi_i(x)) \leq i, i = 4, 6$. Escrevemos

$$\begin{aligned} \psi_4(x) &= a_4x^4 + \cdots + a_0 \\ \psi_6(x) &= b_6x^6 + \cdots + b_0. \end{aligned}$$

Agora, as funções v^3, x^4v e x^6 são as únicas tendo um pólo de ordem 6 em T, por isso, $a_4 \neq 0$ ou $a_6 \neq 0$. Substituindo $u = 1/x$ em 4.3 e multiplicando por u^6 temos

$$(u^2v)^3 + (a_4 + \cdots + a_0u^4)(u^2v) + (b_6 + \cdots + b_0u^6) = 0. \tag{4.4}$$

Substituindo $t = u^2v$ em 4.4 obtemos a equação

$$F_1(u, t) := t^3 + (a_4 + \cdots + a_0u^4)t + (b_6 + \cdots + b_0u^6) = 0. \tag{4.5}$$

Os corpos de funções $k(x, y)/k$ com $F(x, y) = 0$ e $k(u, t)/k$ com $F_1(u, t) = 0$ são iguais e o place infinito α de $k(x)/k$ corresponde ao place finito (u) de $k(u)/k$(pois $u = 1/x$). Assim, temos que $F(0, t)$ é um polinômio irredutível, ou seja,

$$F(0, t) = t^3 + a_4t + b_6 = t^3 + t + 1$$

pois $a_4 = 1$ ou $b_6 = 1$, se um deles não fosse igual a 1, então o polinômio $F(0, t)$ seria redutível sobre $\mathbb{F}_2$.

Homogeinizando a equação 4.5 em z temos

$$F_1'(u, t, z) = t^3z^3 + (z^5 + \cdots + a_0u^4z)t + (z^6 + \cdots + b_0u^6), \tag{4.6}$$

donde claramente o ponto infinito $P = (0 : 1 : 0)$ é singular. Vamos mostrar que $\delta_P = 6$, e da fórmula do gênero teremos que este é o único ponto singular da curva $V(F_1')$, ou seja, a curva afim $C = V(F_1)$ é não singular. Desomogeinizando $F_1'(u,t,z)$ em t temos

$$F_2(u,z) := F_1'(u,1,z) = z^3 + (z^5 + \cdots + a_0u^4z) + (z^6 + \cdots + b_0u^6). \tag{4.7}$$

Fazendo um Blow-up em F_2 temos

$$\begin{aligned} F_2(u,uz) &= u^3z^3 + (u^5z^5 + \cdots + a_0u^5z) + (u^6z^6 + \cdots + b_0u^6) \\ &= u^3(z^3 + (u^2z^5 + \cdots + a_0u^2z) + (u^3z^6 + \cdots + b_0u^3)) \\ &= u^3F_3(u,z). \end{aligned}$$

obtendo assim um novo ponto Q de ordem 3. Fazendo um novo Blow-up em F_3 desingularizamos o ponto Q e da definição de δ_P temos que

$$\delta_P = r_P(r_P - 1)/2 + r_Q(r_Q - 1)/2 = 3(3-1)/2 + 3(3-1)/2 = 6.$$

Ficamos com 12 possibilidades no caso **(i)** com $n_3 = 4$, 12 possibilidades para o caso **(ii)** com $n_3 = 3$ e nenhuma solução para **(i)** com $n_3 = 3$. Usando isomorfismos do tipo $x \longmapsto x+1$ e $x \longmapsto 1/x$, existem 3 soluções dadas por $K = k(x,y)$ e

$$\begin{aligned} &y^3 + (x^4 + x^3 + 1)y + (x^6 + x^3 + 1) = 0, \quad n_1 = 0, n_2 = 0, n_3 = 4, n_4 = 2; \\ &y^3 + (x^2 + x + 1)^2y + (x^6 + x^5 + 1) = 0, \quad n_1 = 0, n_2 = 0, n_3 = 4, n_4 = 2; \\ &y^3 + (x^4 + x^3 + 1)y + (x^6 + x + 1) = 0, \quad n_1 = 0, n_2 = 1, n_3 = 3, n_4 = 3; \end{aligned}$$

Vamos mostrar que as duas primeiras não são isomorfas. Sabemos que os modelos canônicos de K_1/k e K_2/k podem ser vistos como intersecção da quádrica $f(x,y,z,t) = x^2 + zt = 0$ com cúbicas $\mathcal{E}_1$ e $\mathcal{E}_2$. Desomogeinizando f em z temos que $t = x^2$. Substituindo na equação de K_1/k (resp. K_2/k) temos que

$$\begin{aligned} y^3 + (t^2 + tx + 1)y + (t^3 + tx + 1) &= 0 \\ (\text{resp. } y^3 + (t^2 + t + 1)y + (t^3 + t^2x + 1) &= 0). \end{aligned}$$

Homogeinizando em z temos que $C_i = V(s_i), i = 1, 2$ com

$$\begin{aligned} s_1 &= y^3 + (t^2 + tx + z^2)y + (t^3 + txz + z^3) \\ (\text{resp. } s_2 &= y^3 + (t^2 + tz + z^2)y + (t^3 + t^2x + z^3). \end{aligned}$$

Temos que mostrar que não existe automorfismo de $\mathbb{P}^4(k)$ fixando a quádrica e tal que aplica s_1 em $s_2 + l \times f$ onde f é uma forma de grau 1(pois se $\sigma(s_1) = s_2 + l \times f$ então temos que $\sigma(V(s_1)) = V(s_2 + l \times f) = V(s_2)$).

Mas o grupo dos automorfismos de $\mathbb{P}^4(k)$ fixando o cone $(V(x^2 + zt))$ tem 48 elementos, cuja forma geral é

$$\sigma = \begin{pmatrix} 1 & 0 & c_1c_3 & c_2c_4 \\ a_1 & 1 & a_2 & a_3 \\ 0 & 0 & c_1 & c_2 \\ 0 & 0 & c_3 & c_4 \end{pmatrix}$$

onde os coeficientes a_i e c_j pertencem a k e $c_1c_4 + c_2c_3 = 1$. Usando argumentos computacionais, mostra-se que nenhum desses automorfismos envia s_1 em $s_2 + l \times f$, ou seja, K_1/k não é k-isomorfo a K_2/k.

Portanto, a menos de isomorfismo os únicos corpos de funções de gênero 4 e $h = 2$ tendo um sistema g_3^1 são dados por

$$\begin{array}{ll} y^3 + (x^4 + x^3 + 1)y + (x^6 + x^3 + 1) = 0, & n_1 = 0, n_2 = 0, n_3 = 4, n_4 = 2; \\ y^3 + (x^2 + x + 1)^2 y + (x^6 + x^5 + 1) = 0, & n_1 = 0, n_2 = 0, n_3 = 4, n_4 = 2; \\ y^3 + (x^4 + x^3 + 1)y + (x^6 + x + 1) = 0, & n_1 = 0, n_2 = 1, n_3 = 3, n_4 = 3. \end{array}$$

Não existe um g_3^1

Neste caso devemos ter $n_3 < 3$, pois do contrário teríamos dois places de grau 2 equivalentes e então existiria $x \in K$ tal que $[K : k(x)] = 3$. Estamos então nos casos **(ii)** com

$$n_1 = 0, n_2 = 1, 1 \leq n_3 \leq 2, n_4 = 3$$

ou no caso **(iii)** com

$$n_1 = 0, n_2 = 2, n_3 = 0, n_4 = 3.$$

- Caso $n_1 = 0, n_2 = 1, 1 \leq n_3 \leq 2, n_4 = 3$.

  Seja $\mathcal{C} = \mathcal{D} \cap \mathcal{E}$ o modelo canônico de K/k. Podemos escolher coordenadas homogêneas em $\mathbb{P}^3(k)$, $(x : y : z : t)$, de modo que a equação de $\mathcal{D}$ é dada por

  $$f(x, y, z, t) = xy + z^2 + zt + t^2 = 0$$

  Uma superfície cúbica $\mathcal{E}$ tem a equação da forma

  $$s_0(x, y, z, t) = \sum_{i+j+k+l=3} d_{i,j,k,l} x^i y^j z^k t^l = 0$$

  Existem 20 monômios de grau 3 em 4 indeterminadas. Seja l uma forma de grau 1 em (x, y, z, t), ou seja, $l(x, y, z, t) = ax + by + cz + dt$. Então temos que

  $$l \times f(x, y, z, t) = ax^2y + bxy^2 + cxyz + dxyt + H(x, y, z, t).$$

  Assim, podemos tomar l de tal modo que

  $$s(x, y, z, t) = s_0(x, y, z, t) - l \times f(x, y, z, t)$$

  não depende dos monômios x^2y, xy^2, xyz e xyt. Assim, podemos considerar que a equação de $\mathcal{E}$ é da forma

  $$\begin{array}{rl} s(x, y, z, t) = & c_1x^2z + c_2x^2t + c_3xz^2 + c_4xt^2 + c_5xzt \\ & +c_6y^2z + c_7y^2t + c_8yz^2 + c_9yzt + c_{10}yt^2 \\ & +c_{11}zt^2 + c_{12}z^2t + c_{13}z^3 + c_{14}t^3 + c_{15}x^3 + c_{16}y^3 \quad = 0 \end{array}$$

  As coordenadas dos 5 pontos racionais de $\mathcal{D}$ são

  $$\begin{array}{l} P_1 = (1 : 0 : 0 : 0) \\ P_2 = (0 : 1 : 0 : 0) \\ P_3 = (1 : 1 : 0 : 1) \\ P_4 = (1 : 1 : 1 : 0) \\ P_5 = (1 : 1 : 1 : 1). \end{array}$$

Com $n_1 = 0$ e $\mathcal{C} = \mathcal{D} \cap \mathcal{E}$ temos que nenhum desses pontos está em $\mathcal{E}$, ou seja,

$$\begin{cases} c_{16} = 1 \\ c_{15} = 1 \\ c_{14} = 1 + c_{10} + c_7 + c_4 + c_2 \\ c_{13} = 1 + c_8 + c_6 + c_3 + c_1 \\ c_{12} = 1 + c_{11} + c_9 + c_5. \end{cases}$$

Seja P o place de grau 2 de $K/\mathbb{F}_2$, então $Q = Con_{\mathbb{F}_4/\mathbb{F}_2}(P) = \overline{P}_1 + \overline{P}_2$, onde $\overline{P}_1, \overline{P}_2$ são places de grau 1 de $\mathbb{F}_4K/\mathbb{F}_4$. Assim. as possibilidades para Q são

$$\begin{aligned} Q_1 &= (\alpha : \alpha^2 : 0 : 1) + (\alpha^2 : \alpha : 0 : 1) \\ Q_2 &= (\alpha : \alpha^2 : 1 : 0) + (\alpha^2 : \alpha : 1 : 0) \\ Q_3 &= (\alpha : \alpha^2 : 1 : 1) + (\alpha^2 : \alpha : 1 : 1) \\ Q_4 &= (0 : 1 : 1 : \alpha) + (0 : 1 : 1 : \alpha^2) \\ Q_5 &= (1 : 0 : 1 : \alpha) + (1 : 0 : 1 : \alpha^2) \\ Q_6 &= (0 : 0 : 1 : \alpha) + (0 : 0 : 1 : \alpha^2) \\ Q_7 &= (0 : 1 : \alpha : 1) + (0 : 1 : \alpha^2 : 1) \\ Q_8 &= (0 : \alpha^2 : \alpha : 1) + (0 : \alpha : \alpha^2 : 1) \\ Q_9 &= (1 : 0 : \alpha : 1) + (0 : 0 : \alpha^2 : 1) \\ Q_{10} &= (\alpha^2 : 0 : \alpha : 1) + (\alpha : 0 : \alpha^2 : 1) \end{aligned}$$

onde α é um elemento gerador de $\mathbb{F}_4$. Temos por exemplo

$$\begin{aligned} Q_1 = Q \iff & \begin{cases} s(\alpha, \alpha^2, 0, 1) = 0 \\ s(\alpha^2, \alpha, 0, 1) = 0 \end{cases} \\ \iff & \begin{cases} (c_4 + c_7)\alpha + (c_2 + c_{10})\alpha^2 + c_{14} = 0 \\ (c_2 + c_{10})\alpha + (c_4 + c_7)\alpha^2 + c_{14} = 0 \end{cases} \\ \iff & \begin{cases} c_4 + c_7 = 1 \\ c_2 + c_{10} = 1 \end{cases}. \end{aligned}$$

Prova-se que o subgrupo $\mathcal{G}$ do grupo de automorfismos de $\mathbb{P}^3(k)$ fixando $\mathcal{D}$ é isomorfo à S_5, o grupo de permutações de 5 elementos. Esse isomorfismo pode ser dado explicitamente considerando esses elementos como os pontos 5 racionais de $\mathcal{D}$, ou seja,

$$\mathcal{G} = \{\sigma \in Aut(\mathbb{P}^3(k)) | \sigma \text{ permuta } P_1, \cdots, P_5\}.$$

Todos os places Q_i pertencem à mesma órbita sob $\mathcal{G}$. Ainda temos que o subgrupo de $\mathcal{G}$ fixando Q_1 tem 12 elementos. Se considerarmos as cúbicas que contenham Q_1 e nenhum outro $Q_j, j = 2, \cdots, 10$ teremos que existem 12 soluções isomorfas em cada um dos casos

$$n_1 = 0, n_2 = 1, n_3 = 1, n_4 = 3$$

e

$$n_1 = 0, n_2 = 1, n_3 = 2, n_4 = 3.$$

Assim, a menos de isomorfismo, existem apenas duas soluções, que são

1. $n_1 = 0, n_2 = 1, n_3 = 1, n_4 = 3$

$$\begin{cases} f(x,y,z,t) = xy + z^2 + zt + t^2 = 0 \\ s_1(x,y,z,t) = x^3 + x^2t + xz^2 + xt^2 + y^3 + zt^2 + t^3 = 0. \end{cases}$$

2. $n_1 = 0, n_2 = 1, n_3 = 2, n_4 = 3$

$$\begin{cases} f(x,y,z,t) = & xy + z^2 + zt + t^2 = 0 \\ s_1(x,y,z,t) = & x^3 + x^2t + xz^2 + xzt + y^3 \\ & +y^2t + yzt + zt^2 + t^3 = 0. \end{cases}$$

Queremos obter um modelo plano para cada uma dessas curvas, para tal, vamos criar uma projeção de $\mathbb{P}^3(k)$ em $\mathbb{P}^2(k)$ e considerarmos a curva plana que é imagem das curvas acima. Considere então as coordenadas homogêneas de $\mathbb{P}^2(k)$ dadas por $(u : v : w)$ e os abertos

$$U := \{(x : y : z : w) \in \mathbb{P}^3(k) | y \neq 0\} \subseteq \mathbb{P}^3(k)$$

e

$$V := \{(u : v : w) \in \mathbb{P}^2(k) | w \neq 0\} \subseteq \mathbb{P}^2(k).$$

Consideramos o morfismo de V para U dado por

$$(u : v : 1) \longmapsto (u^2 + uv + v^2 : 1 : v : u).$$

Assim, as soluções para K/k são com $K = k(u, v)$ onde

1. $n_1 = 0, n_2 = 1, n_3 = 1, n_4 = 3$ e

$$\begin{aligned} &v^6 + uv^5 + (u+1)v^4 + (u^3+u)v^3 + u^3v^2 + (u^5+u^3+u^2)v \\ &+u^6 + u^5 + u^3 + u + 1 = 0; \end{aligned}$$

2. $n_1 = 0, n_2 = 1, n_3 = 2, n_4 = 3$ e

$$\begin{aligned} &v^6 + uv^5 + (u+1)v^4 + u^3v^3 + u^3v^2 + (u^5+u^3+u^2+u)v \\ &+u^6 + u^5 + u^3 + u + 1 = 0; \end{aligned}$$

- $n_1 = 0, n_2 = 2, n_3 = 0, n_4 = 3$.
  Vamos mostrar que este caso é impossível. Temos

$$22 = A_6 = n_2(n_2+1)(n_2+2)/6 + n_2n_4 + n_6 = 4 + 6 + n_6.$$

Então temos que $n_6 = 12$. Sejam Q_1 e Q_2 os dois places de grau 2. Então

$$2Q_1 \sim 2Q_2 \text{ e } Q_1 \nsim Q_2$$

pois K/k é não hiperelíptico. Assim

$$3Q_1 \sim Q_1 + 2Q_2 \nsim Q_2 + 2Q_1 \sim 3Q_2,$$

ou seja, $3Q_1$ ou $3Q_2$ é um divisor canônico pois $h = 2$. Suponhamos sem perda de generalidade que $3Q_1$ é canônico. Seja $\mathcal{C}$ o modelo canônico de K/k em $\mathbb{P}^3(k)$. Temos que os divisores canônicos $Q_1 + 2Q_2$ e $3Q_3$ são a intersecção dos planos racionais V_1 e V_2 com $\mathcal{C}$, os quais se

intersectam em uma reta racional L_1 que passa por Q_1. Além disso, o plano V_2 é gerado por L_1 e uma outra reta racional que passa por Q_2, ou seja, existe um ponto P que está em ambas as retas. Consideremos a projeção de $\mathcal{C}$ para $\mathbb{P}^2(k)$ através de P. Temos então uma curva plana $C := \pi(\mathcal{C})$ que tem dois pontos singulares racionais obtidos pelas imagens de Q_1 e Q_2. Como essa projeção é uma aplicação birracional, temos que os corpos $K = k(\mathcal{C})$ e $k(\pi(\mathcal{C}))$ são k-isomorfos.

Podemos supor, fazendo transformação projetiva se necessário, que

$$\pi(V_1) = V(x),\ \pi(V_2) = V(y)$$

e que os pontos singulares associados a Q_1 e Q_2 são respectivamente $P_1 = (0:0:1)$ e $P_2 = (1:0:0)$. Seja $F(x,y,z) = 0$ a equação de $\pi(C)$ que é um polinômio homogêneo de grau 6. Então $F(0,y,z) = y^6$, pois V_1 intersecta $\mathcal{C}$ em $3Q_1$ e $F(x,0,z) = x^2z^4$, pois V_2 intersecta $\mathcal{C}$ em $Q_1 + 2Q_2$. Assim temos que

$$F(x,y,z) = x^2z^4 + y^6 + xyH(x,y,z),$$

onde H é um polinômio homogêneo de grau 4. Escrevemos

$$\begin{aligned} F(x,y,z) &= x^2z^4 + y^6 + a_1xyz^4 + a_2x^2yz^3 + a_3xy^2z^3 \\ &+a_4x^3yz^2 + a_5x^2y^2z^2 + a_6xy^3z^2 + a_7x^4yz \\ &+a_8x^3y^2z + a_9x^2y^3z + a_{10}xy^4z + a_{11}x^5y \\ &+a_{12}x^4y^2 + a_{13}x^3y^3 + a_{14}x^2y^4 + a_{15}xy^5. \end{aligned}$$

Desomogeinizando a curva em z, obtemos a equação da curva em P_1, que será

$$F(x,y,1) = x^2 + xyH(x,y,1) + y^6, \tag{4.8}$$

donde temos $ord_{P_1}(C) = 2$.

Suponha que $a_1 = 1$, então a Equação 4.8 se tornaria

$$F(x,y,1) = x^2 + xy + G(x,y) + y^6 = x(x+y) + G(x,y) + y^6, \tag{4.9}$$

onde a forma inicial de $G(x,y)$ tem grau maior que dois. Dando um Blow-up em 4.9 teríamos dois pontos racionais associados aos pontos $(0,0)$ e $(0,1)$, mas isso é um absurdo. Consequentemente $a_1 = 0$.

Assim, a equação 4.8 é da forma

$$F(x,y,1) = x^2 + a_2x^2y + a_3xy^2 + a_6xy^3 + \cdots + y^6. \tag{4.10}$$

Dando um Blow-up em 4.10 temos

$$\begin{aligned} F(xy,y,1) &= y^2(x^2 + a_2x^2y + a_3xy + a_6xy^2 + \cdots + y^4) \\ &= y^2g(x,y). \end{aligned} \tag{4.11}$$

Assim, existe um único ponto infinitesimamente próximo de P por esse Blow-up que chamemos de Q. Pela mesma razão usada em 4.9, devemos ter $a_3 = 0$. Fazendo um novo Blow-up em g temos

$$\begin{aligned} g(xy,y) &= y^2(x^2 + a_2x^2y + a_6xy + \cdots + y^2) \\ &= y^2g_1(x,y). \end{aligned} \tag{4.12}$$

Obtemos assim um novo ponto R de multiplicidade 2. Suponha que $a_6 = 0$, então a forma inicial de g seria $x^2+y^2 = (x+y)^2$ e dando um Blow-up teríamos um ponto racional associado a $(0,0)$,o que é um absurdo. Portanto $a_6 = 1$.

Assim, a forma inicial de g é dada por $x^2+xy+y^2 = (x+\alpha^2 y)(x+\alpha y)$ onde α é um gerador de $\mathbb{F}_4$. Obtemos assim, por um último Blow-up o place Q_1.

Usando a fórmula para δ_{P_1}, obtemos

$$\delta_P = \frac{m_{P_1}(m_{P_1}-1)+m_Q(m_Q-1)+m_R(m_R-1)}{2} = 3.$$

Repetindo o processo, obtemos como equação para P_2

$$F(1,y,z) = a_{11}y + a_{12}y^2 + a_7yz + a_4yz^2 + a_8y^2z + a_{13}y^3 + \cdots + z^4 + y^6.$$

Como P_2 é singular, então $a_{11} = 0$. Ainda, P_2 tem multiplicidade 2 e é não ordinário, ou seja,

$$F(1,y,z) = y^2 + a_4yz^2 + a_8y^2z + a_{13}y^3 + \cdots + z^4 + y^6. \tag{4.13}$$

Fazendo um Blow-up em 4.13 obtemos

$$F(1,yz,z) = z^2(y^2 + a_4yz + \cdots + z^2 + y^6z^4) = z^2g_2(yz). \tag{4.14}$$

Como anteriormente, devemos ter $a_4 = 1$ e por Blow-up, obtemos Q_2. Assim, $\delta_{P_2} = 2$ e usando a fórmula do gênero, obtemos

$$4 = g(C) = \frac{(n-1)(n-2)}{2} - \sum_{P\in C}\delta_P = \frac{5\cdot 4}{2} - \sum_{P\in C}\delta_P = 10 - \sum_{P\in C}\delta_P.$$

Assim, temos que

$$\sum_{P\in C\setminus\{P_1,P_2\}}\delta_P = 6-5 = 1,$$

ou seja, existe outro ponto $P \in C$ não singular. Este ponto deve ser racional de multiplicidade 2. Se o ponto fosse ordinário, com um único Blow-up obteríamos um outro place de grau 2 e se esse ponto fosse não ordinário, obteríamos um place de grau 1. Ambos os casos não podem ocorrer pelas condições sobre n_1 e n_2.

Concluímos assim, que a menos de isomorfismo, existem exatamente 5 corpos de funções não hiperelípticos K/k com $g = 4$ e $h = 2$, eles são dados por $K = k(x,y)$ e

$$\begin{array}{ll}
y^3 + (x^4+x^3+1)y + (x^6+x^3+1) = 0, & n_1 = 0, n_2 = 0, n_3 = 4, n_4 = 2; \\
y^3 + (x^4+x^2+1)y + (x^6+x^5+1) = 0, & n_1 = 0, n_2 = 0, n_3 = 4, n_4 = 2; \\
y^3 + (x^4+x^3+1)y + (x^6+x+1) = 0, & n_1 = 0, n_2 = 1, n_3 = 3, n_4 = 3; \\
y^6 + xy^5 + (x+1)y^4 + (x^3+x)y^3 + x^3y^2 + & n_1 = 0, n_2 = 1, n_3 = 1, n_4 = 3; \\
(x^5+x^3+x^2)y + (x^6+x^5+x^3+x+1) = 0, & \\
 & \\
y^6 + xy^5 + (x+1)y^4 + x^3y^3 + x^2y^2 + (x^5+ & n_1 = 0, n_2 = 1, n_3 = 2, n_4 = 3. \\
x^3+x^2+x)y + (x^6+x^5+x^3+x+1) = 0, &
\end{array}$$

4.4.3 $g = 5$

Temos que

$$\begin{aligned} L(t) = \; & 1 + a_1 t + a_2 t^2 + a_3 t^3 + a_4 t^4 + a_5 t^5 + 2a_4 t^6 + 4a_3 t^7 \\ & + 8a_2 t^8 + 16 a_1 t^9 + 32 t^{10}, \end{aligned}$$

onde

$$\begin{cases} a_1 = -3 \\ a_2 = 2 \\ a_3 = n_3 \\ a_4 = n_4 - 3n_3 \\ a_5 = 4n_3 - 3n_4 + 2 \end{cases}$$

Pela Proposição 4.1.1 temos que estudar os casos

(i) $n_1 = n_2 = n_4 = 0, n_3 = 1$ e $n_5 = 4$

Neste caso

$$\begin{aligned} L(t) = \; & 1 - 3t + 2t^2 + t^3 - 3t^4 + 6t^5 \\ & -6t^6 + 4t^7 + 16t^8 - 48t^9 + 32t^{10}. \end{aligned} \tag{4.15}$$

(ii) $n_1 = n_2 = n_3 = 0, 0 \leq n_4 \leq 3$ e $n_5 = 2$

Neste caso

$$\begin{aligned} L(t) = \; & 1 - 3t + 2t^2 + n_4 t^4 + (2 - 3n_4) t^5 \\ & + 2n_4 t^6 + 16t^8 - 48t^9 + 32t^{10}. \end{aligned} \tag{4.16}$$

Em todos os casos $L(t)$ tem 4 zeros com quadrado absoluto diferente de $1/2$. Portanto, não existem soluções para K/k não hiperelíptico com $g = 5$ e $h = 2$.

Apêndice A

Corpos de funções quadráticos

Seja K/k um corpo de funções sobre $k = \mathbb{F}_q$ o corpo com q elementos de gênero $g \leq 1$ com k como corpo de constantes. O corpo K é uma extensão algébrica e finita de $k(x)$ para algum $x \in K$ que é transcendente sobre k.

Definição A.0.1. *Denotamos por:*

- *h o divisor class number de K/k;*
- *S_x o conjunto dos places de K/k sobre o place infinito $(1/x)$ de $k(x)/k$;*
- *R_x o fecho integral de $k[x]$ em k;*
- *h_x a ordem do ideal class group de R_x; chamaremos h_x o **ideal class number**;*
- *$\mathcal{D}_0(S_x)$ o grupo dos divisores de grau zero de k com suporte em S_x;*
- *$\mathcal{P}(S_x)$ o grupo dos divisores principais com suporte em S_x.*

Temos a fórmula dada por

$$h_x \cdot r_x = h \cdot n_x \tag{A.1}$$

onde $n_x := mdc\{deg(P) | P \in S_x\}$ e $r_x := ord(\mathcal{D}_0(S_x)/\mathcal{P}(S_x))$.

Definição A.0.2. *Seja K/k um corpo de funções algébricas com gênero $g > 0$.*

- *K/k é **quadrático** se existe $x \in K$ transcendente sobre k tal que $[K : k(x)] = 2$.*
- *Se existe $x \in K$ transcendente tal que $[K : k(x)] = 2$ e $|S_x| = 1$, dizemos que $K/k(x)$ é uma **extensão quadrática imaginária**.*
- *Se existe $x \in K$ tal que $[K : k(x)] = 2$ e $|S_x| = 2$, dizemos que $K/k(x)$ é uma **extensão quadrática real**.*

A.1 Corpos de funções quadráticos

Seja K/k um corpo de funções quadrático. Para algum $x \in K$ temos $[K : k(x)] = 2$ e $deg(x)_\infty = 2$, onde $(x)_\infty$ denota o divisor pólo de x. Então $K = k(x, y)$, onde $F(x, y) = 0$, com $F \in k(x)[y]$ e $deg_y(F) = 2$. K/k é um corpo de funções elíptico se $g = 1$ e um corpo de funções hiperelíptco se $g \geq 2$.

A.1.1 Places de um corpo de funções quadrático

Os places finitos de $k(x)/k$ são classificados pelos polinômios mônicos irredutíveis de $k[x]$ e temos ainda o place infinito correspondendo à $(1/x)$. Seja $P \in \mathbb{P}(k(x))$ um place qualquer. Como $[K : k(x)] = 2$ existem no máximo dois places distintos sobre P e seus graus são divisíveis pelo grau de P. Temos então que

$$\sum_{P'|P} f(P'|P) \cdot e(P'|P) = [K : k(x)] = 2 \tag{A.2}$$

Três possibilidades podem ocorrer:

Definição A.1.1. *1. Se existe somente um place P' sobre P com $deg(P') = deg(P)$, $f(P'|P) = 1$ e $e(P'|P) = 2$ então dizemos que P* ***ramifica.***

2. Se existe somente um place P' sobre P com $deg(P') = 2 \cdot deg(P)$, $f(P'|P) = 2$ e $e(P'|P) = 1$ então dizemos que P ***está inerte.***

3. Se existem dois places P', P'' sobre P com $deg(P'') = deg(P') = deg(P)$, $f(P''|P) = f(P'|P) = 1$ e $e(P''|P) = e(P'|P) = 1$ então dizemos que o place ***cinde.***

Aplicamos então este resultado para o place infinito P de $k(x)/k$ usando a notação da equação A.1. Temos então:

1. Se P ramifica, existe um único place P' sobre P, $deg(P') = 1$, $n_x = 1$, $r_x = 1$ e $h_x = h$. A extensão quadrática $K/k(x)$ é imaginária.

2. Se P está inerte, existe um único place P' sobre P, $deg(P') = 2$, $n_x = 2$, $r_x = 1$ e $h_x = 2h$. A extensão quadrática $K/k(x)$ é imaginária.

3. Se P cinde, existem dois places P', P'' sobre P, $deg(P') = deg(P'') = 1$, $n_x = 1$ e $r_x \geq 2$. A extensão quadrática $K/k(x)$ é real.

Observação A.1.1. *Para estudar o caso onde a extensão $K/k(x)$ é quadrática imaginária temos de estudar as duas seguintes situações:*

1. K/k tem um place P de grau um tal que $(x)_\infty = 2P$ e $h = 2$.

2. K/k tem um place Q de grau dois tal que $(x)_\infty = Q$ e $h = 1$.

A.1.2 Corpos de funções elípticas

Definição A.1.2. *Um corpo de funções K/k (onde k é o corpo das constantes de K) é dito um* ***corpo de funções elípticas*** *se possui as seguintes propriedades:*

1. O gênero de K/k é $g = 1$.

2. Existe um divisor $A \in \mathcal{D}_K$ com $degA = 1$.

Repare que a condição 2 dessa definição é atendida se k é algebricamente fechado ou um corpo finito.

Proposição A.1.1. *Seja K/k um corpo de funções elípticas.*

(a) *Se* $car(k) \neq 2$, *existem* $x, y \in K$ *tais que* $K = k(x, y)$ *e*

$$y^2 = f(x) \in k[x] \tag{A.3}$$

com um polinômio livre de quadrados $f(x) \in k[x]$ *de grau 3.*

(b) *Se* $car(k) = 2$, *existem* $x, y \in F$ *tais que* $K = k(x, y)$ *e*

$$y^2 + y = f(x) \in k[x] \text{ com } deg f(x) = 3, \tag{A.4}$$

ou

$$y^2 + y = x + \frac{1}{ax + b} \quad \text{com } a, b \in k \text{ e } a \neq 0. \tag{A.5}$$

Demonstração. Escolha um divisor A de grau um. Pelo teorema de Riemann-Roch, $dim(A) = deg(A) + 1 - g = 1$ ($deg(A) = 1 > 0 = 2g - 2$). Por isso, A é equivalente a um divisor $A' \geq 0$ de grau um. Mas então $A' = P$ é um place de $\mathbb{P}(K)$. Consideremos agora a sequência de espaços vetoriais

$$k = \mathcal{L}(0) \subseteq \mathcal{L}(P) \subseteq \mathcal{L}(2P) \subseteq \cdots \subseteq \mathcal{L}(nP) \subseteq \cdots. \tag{A.6}$$

Como $2g - 2 = 0$ e $deg(iP) = i$ temos que $\mathcal{L}(P) = k$ e $\mathcal{L}((i+1)P) \supsetneq \mathcal{L}(iP)$ para $i > 0$. Escolhemos então elementos $x_1, y_1 \in K$ de modo que $x_1 \in \mathcal{L}(2P) \backslash \mathcal{L}(P)$ e $y_1 \in \mathcal{L}(3P) \backslash \mathcal{L}(2P)$. Seus divisores pólos são

$$(x_1)_\infty = 2P, (y_1)_\infty = 3P. \tag{A.7}$$

Como $[K : k(x_1)] = deg(x_1)_\infty = deg(2P) = 2$ e $[K : k(y_1)] = deg(y_1)_\infty = deg(3P) = 3$ temos que $K = k(x_1, y_1)$.

Os 7 elementos $1, x_1, y_1, x_1^2, x_1y_1, x_1^3, y_1^2$ estão em $\mathcal{L}(6P)$ e $dim(6P) = 6$, ou seja, existem $a_1, b_1, c_1, d_1, e_1, f_1, g_1 \in k$ tal que

$$a_1y_1^2 + b_1x_1y_1 + c_1y_1 = d_1x_1^3 + e_1x_1^2 + f_1x_1 + g_1 \tag{A.8}$$

O coeficiente $a_1 \neq 0$, pois do contrário $y_1 \in k(x_1)$ e da mesma forma $d_1 \neq 0$ pois do contrário $[K : k(y_1)] < 3$. Multiplicando a equação A.8 por $a_1^3d_1^2$ e tomando $y_2 := a_1^2d_1y_1$ e $x_2 := a_1d_1x_1$ obtemos que $K = k(x_2, y_2)$ e

$$y_2^2 + (b_2x_2 + c_2)y_2 = x_2^3 + e_2x_2^2 + f_2x_2 + g_2 \tag{A.9}$$

onde $b_2, c_2, e_2, f_2, g_2 \in k$. Dividimos agora nos casos em que $car(k) = 2$ e $car(k) \neq 2$.

(a) $car(k) \neq 2$.
Consideramos $y := y_2 + (b_2x_2 + c_2)/2$ e $x := x_2$ e teremos $K = k(x, y)$ e

$$y^2 = x^3 + ax^2 + bx + c = f(x) \in k[x] \tag{A.10}$$

com $a, b, c \in k$. Falta mostrar que $f(x)$ é livre de quadrados. Suponha o contrário, então $f(x) = (x - \alpha)^2(x - \beta)$ com $\alpha, \beta \in k$. Considere então o elemento $z := y/(x - \alpha)$. Então $z^2 = x - \beta$ e $K = k(x, z) = k(z)$. Então K/k é racional, o que é um absurdo.

(b) $car(k) = 2$.
Af. $b_2x_2 + c_2 \neq 0$.
De fato, se $b_2x_2 + c_2 = 0$ então $y_2^2 \in k(x_2)$, isto é, $K/k(x_2)$ é puramente inseparável de grau 2. Mas sabemos que o único corpo intermediário $k \subseteq K_0 \subseteq K$ tal que K/K_0 é puramente

inseparável de grau p é o corpo K^p, então $k(x_2) = K^p$. Entretanto, o gênero de $k(x_2)/k$ é zero e o gênero de K^p/k é um. Esta contradição prova a afirmação.

Considere agora $y_3 := y_2(b_2 + c_2)^{-1}$. Então $K = k(x_2, y_3)$ e

$$y_3^2 + y_3 = (b_2x_2 + c_2)^{-2}(x_2^3 + e_2x_2^2 + f_2x_2 + g_2). \tag{A.11}$$

Se $b_2 = 0$, o lado direito de A.11 é o polinômio $f(x_2) \in k[x_2]$ de grau 3 e temos o caso A.4.

Se $b_2 \neq 0$ o lado direito de A.11 pode ser escrito da forma

$$vx_2 + u + \frac{w}{(b_2x_2 + c_2)^2} + \frac{w'}{b_2x_2 + c_2} \tag{A.12}$$

com $u, v, w, w' \in k$ e $v \neq 0$. Como k é perfeito, $w = w''^2$ para algum $w'' \in k$ e o elemento $y_4 := y_3 + w''(b_2x_2 + c_2)^{-1}$ satisfaz a equação

$$y_4^2 + y_4 = v_2x_2 + u_2 + \frac{w_1}{b_2x_2 + c_2} \tag{A.13}$$

com $v_2, u_2, w_2 \in k$ e $v_2 = v \neq 0$. Também, o coeficiente $w_2 \neq 0$ (pois do contrário $K = k(x_2, y_4)$ seria racional). Tomando $y := y_4$ e $x := v_2x_2 + u_2$ obtemos $K = k(x, y)$ com

$$y^2 + y = x + \frac{1}{ax + b} \tag{A.14}$$

com $a, b \in k$ e $a \neq 0$.

□

A próxima proposição nos diz que cada uma das equações A.3, A.4 e A.5 definem um corpo de funções elípticas.

Proposição A.1.2. **(a)** *$car(k) \neq 2$. Suponha que $K = k(x, y)$ com*

$$y^2 = f(x) \in k[x], \tag{A.15}$$

onde $f(x)$ é um polinômio livre de quadrados de grau 3. Considere a decomposição $f(x) = c\prod_{i=1}^{r} p_i(x)$ de $f(x)$ em um produto de polinômios mônicos irredutíveis $p_i(x) \in k[x]$ com $0 \neq c \in k$. Denote por $P_i \in \mathbb{P}(k(x))$ o place de $k(x)$ correspondente a $p_i(x)$, e $P_\infty \in \mathbb{P}(k(x))$ o pólo de x. Então valem as seguintes afirmações:

1. *k é o corpo as constantes de K, e K/k é um corpo de funções elípticas.*
2. *A extensão $K/k(x)$ é cíclica de grau 2. Os places $P_1, \ldots, P_r$ e P_∞ são ramificados em $K/k(x)$; cada um deles tem exatamente uma extensão em k, digamos $Q_1, \ldots, Q_r$ e Q_∞, e temos que $e(Q_j \mid P_j) = e(Q_\infty \mid P_\infty) = 2$, $degQ_j = degP_j$ e $degQ_\infty = 1$.*
3. *$P_1, \ldots, P_r$ e P_∞ são os únicos places de $k(x)$ que são ramificados em $K/k(x)$, e o diferente de $K/k(x)$ é*
$$Diff(K/k(x)) = Q_1 + \ldots + Q_r + Q_\infty.$$

(b) *$car(k) = 2$. Suponha que $K = k(x, y)$ com*

$$y^2 + y = f(x) \in k[x] \text{ com } degf(x) = 3, \tag{A.16}$$

ou

$$y^2 + y = x + \frac{1}{ax + b} \quad \text{com } a, b \in k \text{ e } a \neq 0. \tag{A.17}$$

Denote por $P_\infty \in \mathbb{P}(k(x))$ o pólo de x em $k(x)$ e por $P' \in \mathbb{P}(k(x))$ o zero de $ax + b$ em $k(x)$ (no caso A.17). Então valem as seguintes afirmações:

1. *k é o corpo das constantes de K, e K/k é um corpo de funções elípticas.*
2. *A extensão $K/k(x)$ é cíclica de grau 2. Os únicos places de $k(x)$ que ramificam em $K/k(x)$ são*
   - *P_∞, no caso (A.16);*
   - *P_∞ e P', no caso (A.17).*

   Seja Q_∞ (respectivamente Q' no caso (A.17)) a extensão de P_∞ (respectivamente P') em K/k. Então $degQ_\infty = degQ' = 1$ e

$$Diff(K/k(x)) = \begin{cases} 4Q_\infty & \text{no caso (A.16)} \\ 2Q_\infty + 2Q' & \text{no caso (A.17)} \end{cases}$$

Definição A.1.3. *A equação A.9 escrita como*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{A.18}$$

é chamada a ***equação de Weierstrass*** *do corpo de funções elípticas K/k.*

Definição A.1.4. *A partir dos valores $a_1, a_2, a_3, a_4, a_6, a_8 \in k$ definidos em A.1.3 definimos os seguintes valores:*

- $b_2 := a_1^2 + 4a_2$;
- $b_4 := 2a_4 + a_1a_3$;
- $b_6 := a_3^2 + 4a_6$;
- $b_8 := a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$;
- $c_4 := b_2^2 - 24b_4$;
- $c_6 := b_2^3 + 36b_2b_4 - 216b_6$;
- $\Delta := -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$;
- $j := c_4^3/\Delta$.

O valor Δ é chamado o discriminante da equação de Weierstrass de K/k e o valor j é chamado o j-invariante do corpo de funções K/k.

Definição A.1.5. *Considere a curva algébrica plana afim C, dada por $F(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x + a_6) = 0$. Esta é chamada a* ***curva elíptica associada à*** *K/k.*

Proposição A.1.3. (a) *A curva C pode ser caracterizada como segue:*

(i) *C é não singular se e somente se $\Delta \neq 0$.*

(ii) *C tem um nó (ponto singular ordinário) se e somente se $\Delta = 0$ e $c_4 \neq 0$.*

(iii) *C tem uma cúspide se e somente se $\Delta = c_4 = 0$.*

(b) *Duas curvas elípticas são isomorfas (sobre $\overline{k}$) se e somente se elas têm o mesmo j-invariante.*

(c) *Dado $j_0 \in \overline{k}$ existe uma curva elíptica (definida sobre $k(j_0)$), com j-invariante igual a j_0.*

A.1.3 Corpos de funções hiperelípticas

Definição A.1.6. *Um corpo de funções K/k é chamado hiperelíptico se o corpo K' gerado pelas razões de diferenciais de primeiro tipo é diferente de K.*

Teorema A.1.1. *Um corpo de funções K/k com $g > 1$ é hiperelíptico se e somente se existe um corpo $k \subseteq K_0 \subseteq K$ tal que K_0/k é um corpo de funções de gênero 0 e $[K : K_0] = 2$. Em particular, se k é finito temos que K/k é hiperelíptico se e somente se existe $x \in K$ tal que $[K : k(x)] = 2$.*

Observação A.1.2. *A partir de agora, consideramos como definição de corpo de funções hiperelípticas um corpo de funções K/k de gênero $g \geq 2$ que contém um corpo de funções racionais $k(x) \subseteq K$ com $[K : k(x)] = 2$, onde $k = \mathbb{F}_q$ é o corpo finito com q elementos.*

Lema A.1.1. (a) *Um corpo de funções K/k de gênero $g \geq 2$ é hiperelíptico se, e somente se, existe um divisor $A \in \mathcal{D}_K$ com $degA = 2$ e $dimA \geq 2$.*

(b) *Todo corpo de funções K/k de gênero 2 é hiperelíptico.*

Da definição de divisor especial, temos que o divisor obtido acima o é, por isso, seu sistema linear é um g_2^1. De fato, um corpo de funções hiperelíptico tem exatamente um sistema linear g_2^1 (D pertence a ele) que é livre de pontos base. Se $g = 2$, o sistema canônico é um g_2^1 e K/k é hiperelíptico (exatamente o que diz o segundo item do Lema anterior). Seja $g \geq 2$ e D qualquer divisor em g_2^1, então D é chamado de **divisor hiperelíptico**. Se $D = 2P$, onde P é um place de grau um, então dizemos que P é um **ponto hiperelíptico** e se $D = Q$, onde Q é um place de grau dois, então dizemos que Q é um **place hiperelíptico**.

Então existe um $x \in K$ tal que $K/k(x)$ é quadrática imaginária se e somente se K/k tem um place hiperelíptico ou um ponto hiperelíptico.

Observação A.1.3. *Como $[K : k(x)] = 2$, o número n_1 de places de grau um de qualquer corpo hiperelíptico K/k é no máximo $2(q+1)$. Observe que, se $n_1 < 2(q+1)$, K/k tem um ponto hiperelíptico ou um place hiperelíptico e se n_1 é ímpar, então K/k tem um ponto hiperelíptico. Então, se K/k é hiperelíptico tal que $n_1 < 2(q+1)$, existe um $x \in K$ tal que $K/k(x)$ é uma extensão quadrática imaginária.*

Definição A.1.7. *Seja $K/k(x)$ uma extensão quadrática e seja P o place infinito de $k(x)/k$.*

(a) *Se P ramifica, então $(x)_\infty = 2P'$, onde P' é um ponto hiperelíptico. Para qualquer inteiro $n, 0 \leq n \leq 2g$ temos*

$$l(nP') = dim_k \mathcal{L}(nP') = \lfloor n/2 \rfloor + 1 \tag{A.19}$$

*Chamaremos este caso de **caso ramificado**.*

(b) *Se P não ramifica, então $(x)_\infty = Q_\infty$, onde Q_∞ é um place hiperelíptico ou é igual a $P_1 + P_2$. Para um inteiro $n, 0 \leq n \leq g$ temos*

$$l(nQ_\infty) = dim_k \mathcal{L}(nQ_\infty) = n + 1. \tag{A.20}$$

*Se P está inerte, chamaremos este caso de **caso inerte**.*

Se K/k é hiperelíptico e $k(x)$ é um subcorpo de K com $[K : k(x)] = 2$, a extensão é separável. Portanto $K/k(x)$ é uma extensão cíclica de grau 2. Para o caso em que $car(k) \neq 2$, temos a seguinte proposição.

Teorema A.1.2. *Seja K/k um corpo de funções hiperelíptico de gênero g. Então existem $x, y \in K$ tal que $K = k(x, y)$ e*

(a) *Se $car(k) = 2$*

$$F(x, y) = y^2 + \Phi_1(x)y + \Phi_2(x) = 0 \tag{A.21}$$

onde $\Phi_i \in k[x], deg(\Phi_i) \leq i(g+1)$ para $i = 1, 2$.

(b) *Se $car(k) \neq 2$*

$$F(x, y) = y^2 - f(x) = 0 \tag{A.22}$$

onde $f \in k[x], deg(f) = 2g + 1$ ou $2g + 2$ e f é livre de quadrados.

No caso em que $car(k) \neq 2$, temos o seguinte e mais preciso resultado:

Teorema A.1.3. *Assuma que $car(k) \neq 2$.*

(a) *Seja K/k um corpo de funções hiperelíplticas de gênero g. Então existem $x, y \in K$ tais que $K = k(x, y)$ e*

$$y^2 = f(x) \in k[x], \tag{A.23}$$

para um polinômio livre de quadrados $f(x)$ de grau $2g + 1$ ou $2g + 2$.

(b) *Reciprocamente, se $K = k(x, y)$ e $y^2 = f(x) \in k[x]$ para um polinômio livre de quadrados $f(x)$ de grau $m > 4$, então K/k é hiperelíptico de gênero*

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

(c) *Seja $K = k(x, y)$ com $y^2 = f(x)$ como em (A.23). Então os places $P \in \mathbb{P}(k(x))$ que ramificam em $K/k(x)$ são os seguintes:*

- *todos os zeros de $f(x)$ se $degf(x) \equiv 0(mod\ 2)$,*
- *todos os zeros de $f(x)$ e o pólo de x se $degf(x) \equiv 1(mod\ 2)$.*

Portanto, se $f(x)$ se decompõe em fatores lineares, exatamente $2g + 2$ places em $k(x)$ são ramificados em $K/k(x)$.

Vamos agora caracterizar as extensões quadráticas imaginárias.

Característica de k não é igual a 2.

Nesta seção assumimos que $car(k) \neq 2$. Seja K/k um corpo de funções hiperelípticas de gênero g tal que $K = k(x, y)$ e $y^2 = f(x)$ como em A.23.

Lema A.1.2. (a) *Seja $q \in k[x]$ um polinômio mônico e irredutível e seja $Q = (q)$ o place finito de $k(x)/k$ associado à q.*

(i) *Q ramifica se e somente se $q|f$;*

(ii) *Q cinde se e somente se $mdc(q, f) = 1$ e $f(x)$ é um quadrado mod.q em $k[x]$;*

(iii) *Q está inerte se e somente se $mdc(q, f) = 1$ e $f(x)$ não é um quadrado mod.q em $k[x]$.*

(b) *Seja $P = (1/x)$ o place infinito de $k(x)/k$.*

(i) *P ramifica se e somente se $deg(f) = 2g + 1$;*

(ii) *P cinde se e somente se $deg(f) = 2g+2$ e o coeficiente de x^{2g+2} em $f(x)$ é um quadrado em k;*

(iii) *P está inerte se e somente se $deg(f) = 2g + 2$ e o coeficiente de x^{2g+2} em $f(x)$ não é um quadrado em k.*

Proposição A.1.4. *Assuma que $car(k) \neq 2$.*

(a) *Seja K/k um corpo de funções hiperelípticas de gênero g tal que $K/k(x)$ é uma extensão imaginária para algum $x \in K$. Então existe $y \in K$ tal que $K = k(x, y)$ e*

$$F(x, y) = y^2 - f(x) = 0 \tag{A.24}$$

com um polinômio livre e quadrados $f \in k[x]$ de grau $2g + 1$ ou $2g + 2$;

(i) *No caso ramificado $deg(f) = 2g + 1$ e f é mônico;*

(ii) *No caso inerte $deg(f) = 2g + 2$ e o coeficiente de x^{2g+2} não é um quadrado.*

(b) *Reciprocamente, seja $g \geq 2$ um inteiro e seja $K = k(x, y)$ com $F(x, y) = 0$ como em (A.24). Se $deg(f) = 2g + 1$ (resp. $2g + 2$ e o coeficiente de x^{2g+2} não é um quadrado em k) então $K/k(x)$ é uma extensão quadrática imaginária e o place infinito de $k(x)/k$ ramifica (resp. está inerte) em K/k; o gênero de K/k é igual a g.*

Característica de k é igual a 2.

Nesta seção assumimos que $car(k) = 2$. Se tomarmos $Y = y/\Phi_1(x)$ em (A.1.2) obtemos

$$Y^2 + Y = \frac{\Phi_2(x)}{\Phi_1(x)^2} = u(x) \in k(x). \tag{A.25}$$

Então $K = k(x, y)$ é uma extensão de Artin-Schreier de grau 2 se $u \neq w^2 + w$ para todo $w \in k(x)$.

Seja K/k um corpo de funções hiperelípticas tal que $K = k(x, y)$ e $y^2 + h(x)y = f(x)$, onde

$$f(x) = \sum_{i=0}^{2m+1} b_i x^i + bx^{2m+2} \tag{A.26}$$

$$h(x) = \sum_{i=0}^{m} a_i x^i + ax^{m+1}. \tag{A.27}$$

Lema A.1.3. (a) *Seja $q \in k[x]$ um polinômio mônico e irredutível de grau r, c uma raíz de q e k_r a extensão de grau r de k. Tomemos $k_0 = \mathbb{F}_2$ e denote por tr_{k_r/k_0} o traço usual de k_r sobre k_0. Seja Q o place de $k(x)/k$ associado à q.*

(i) *Q ramifica se e somente se q divide $h(x)$.*

(ii) *Q cinde se e somente se $mdc(q, h) = 1$ e $tr_{k_r/k_0} \dfrac{f(c)}{h(c)^2} = 0$.*

(iii) *Q está inerte se e somente se $mdc(q, h) = 1$ e $tr_{k_r/k_0} \dfrac{f(c)}{h(c)^2} = 1$.*

(b) *Suponha que $deg(h) = m + 1$ ou $deg(f) > 2m$. Seja $P = (1/x)$ o place infinito de $k(x)/k$.*

(i) *P ramifica se e somente se $deg(h) \leq m$.*

(ii) *P cinde se e somente se $deg(h) = m+1$ e $t^2 + at + b$ é redutível sobre $k[t]$.*

(iii) *P está inerte se e somente se $deg(h) = m+1$ e $t^2 + at + b$ é irredutível sobre $k[t]$.*

Proposição A.1.5. *Assuma que $car(k) = 2$.*

(a) *Seja K/k um corpo de funções hiperelípticas de gênero g. Então existem $x, y \in K$ tal que $K = k(x,y)$ e*

$$F(x,y) = y^2 + h(x)y + f(x) = 0 \tag{A.28}$$

com os polinômios $f, h \in k[x]$ tal que todos os zeros de $h(x)$ em $\overline{k}$ são zeros simples de $f(x)$ e

$$deg(h) \leq g \text{ e } deg(f) = 2g+1 \tag{A.29}$$

ou

$$deg(h) = g+1 \text{ e } deg(f) \leq 2g+2. \tag{A.30}$$

(b) *Reciprocamente, seja g um inteiro tal que $g \geq 2$. Se $K = k(x,y)$ e $y^2 + h(x)y + f(x) = 0$ com polinômios $f(x), h(x)$ como em (A.28), então K/k é um corpo de funções hiperelíptico de gênero g.*

(c) *Seja $K = k(x,y)$ e $y^2 + h(x)y + f(x) = 0$ como em (A.28). Então os places de $k(x)/k$ que ramificam em K/k são*

- *todos os zeros de $h(x)$ se $deg(h) = g+1$,*
- *todos os zeros de $h(x)$ e o pólo de x se $deg(h) \leq g$.*

Se tomarmos $Y = y/h(x)$ em (A.28), obtemos uma nova equação:

$$G(x,Y) = Y^2 + Y + \frac{f(x)}{h(x)^2} = 0. \tag{A.31}$$

Os corpos de funções $k(x,y)/k$ e $k(x,Y)/k$ são isomorfos. Se fatorarmos $h(x)$ sobre $k[x]$, obtemos

$$h(x) = h_1(x)^{\lambda_1} \cdots h_l(x)^{\lambda_l} \tag{A.32}$$

e se todos os zeros de $h(x)$ em $\overline{k}$ são zeros simples de $f(x)$ então temos $f(x) = f_1(x)h_1(x)\cdots h_l(x)$ onde f_1 é primo com $h_i, i = 1, \cdots, l$. Por expansão via frações parciais, obtemos

$$Y^2 + Y = \frac{g_1(x)}{h_1(x)^{2\lambda_1 - 1}} + \cdots + \frac{g_l(x)}{h_l(x)^{2\lambda_1 - 1}} + g(x), \tag{A.33}$$

com polinômios $g_i, h_i, g \in k[x]$ tais que:

- $h_1, \cdots, h_l$ são irredutíveis, dois a dois distintos,
- $deg(g_i) < deg(h_i^{2\lambda_i - 1})$ e $mdc(g_i, h_i) = 1$, para $i = 1, \ldots, l$,
- $g(x) \equiv 0$ ou $deg(g) \equiv 1 \ mod\ 2$.

A equação (A.33) é a forma normal de Hasse.

Proposição A.1.6. *Assuma que $car(k) = 2$.*

(a) *Seja K/k um corpo de funções hiperelípticas de gênero g tal que $K/k(x)$ é uma extensão quadrática imaginária para algum $x \in K$. Então existe $y \in K$ tal que $K = k(x, y)$ e*

$$F(x, y) = y^2 + h(x)y + f(x) = 0 \tag{A.34}$$

com polinômios $f(x), h(x) \in k[x]$ tal que todos os zeros de $h(x)$ em $\overline{k}$ são zeros simples e $f(x)$ é mônico de grau $\leq 2g + 2$. Mais precisamente

(i) *no caso ramificado $deg(f) = 2g + 1$ e $deg(h) \leq g$;*

(ii) *no caso inerte $deg(f) = 2g + 2$, $deg(h) = g + 1$ e o coeficiente a de x^{g+1} em $h(x)$ é tal que $t^2 + at + 1$ é um polinômio irredutível de $k[t]$.*

(b) *Reciprocamente, seja $g \geq 2$ um inteiro e $K = k(x, y)$ com $F(x, y) = 0$ como em (A.34). Se $deg(f) = 2g + 1$ e $deg(h) \leq g$ (resp. $deg(f) = 2g + 2, deg(h) = g + 1$ e o coeficiente a de x^{g+1} em $h(x)$ é tal que $t^2 + at + 1$ é um polinômio irredutível em $k[t]$), então $K/k(x)$ é uma extensão quadrática imaginária e o place infinito de $k(x)/k$ ramifica (resp. está inerte) em K/k. O gênero de K/k é igual a g.*

Apêndice B

Extensões de corpos de funções algébricas

K/k denota um corpo de funções algébricas com corpo de constantes k. Assumimos que o corpo k é perfeito. Consideramos o corpo de funções K'/k' (onde k' é o corpo de constantes de K') tal que $K' \supseteq K$ é uma extensão algébrica e $k' \supseteq k$. Por conveniência fixamos algum corpo algebricamente fechado $\Phi \supseteq K$ e consideramos somente extensões $K' \supseteq K$ com $K' \subseteq \Phi$.

B.1 Extensões algébricas de corpos de funções

Definição B.1.1. (a) *Um corpo de funções algébricas K'/k' é chamado uma* ***extensão algébrica de*** *K/k se $K' \supseteq K$ é uma extensão algébrica e $k' \supseteq k$.*

(b) *A extensão algébrica K'/k' de K/k é chamada uma* ***extensão constante de corpos*** *se $K' = Kk'$, o corpo composto de K e k'.*

(c) *A extensão algébrica K'/k' de K/k é chamada uma* ***extensão finita*** *se $[K' : K] < \infty$.*

Lema B.1.1. *Seja K'/k' uma extensão algébrica de K/k. Então vale as seguintes afirmações:*

(a) *K'/K é algébrico, e $K \cap k' = k$.*

(b) *K'/k' é uma extensão finita de K/k se e somente se $[K' : k] < \infty$.*

(c) *Seja $K_1 := Kk'$. Então K_1/k' é um extenão constante de corpos e K'/k' é uma extensão finita de K_1/k'(tendo o mesmo corpo de constantes).*

Definição B.1.2. *Considere uma extensão algébrica K'/k' de K/k. Um place $P' \in \mathbb{P}(K')$ está sobre $P \in \mathbb{P}(K)$ se $P \subseteq P'$. Também dizemos que P'* ***é uma extensão de*** *P ou que P* ***está sob*** *P' e escrevemos $P'|P$.*

Proposição B.1.1. *Seja K'/k' uma extensão algébrica de K/k. Suponha que P(resp. P') é um place de K/k (resp. K'/k'), seja $\mathcal{O}_P \subseteq K$ (resp. $\mathcal{O}_{P'} \subseteq K'$) o anel de valorização correspondente e v_P (resp. $v_{P'}$) a valorização discreta correspondente. Então são equivalentes:*

(1) *$P'|P$.*

(2) *$\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.*

(3) *Existe um inteiro $e \geq 1$ tal que $v_P(x) = e \cdot v_{P'}(x)$ para todo $x \in K$. Mais ainda, se $P'|P$ então*

$$P = P' \cap K \text{ e } \mathcal{O}_P = \mathcal{O}_{P'} \cap K.$$

Definição B.1.3. *Seja K'/k' uma extensão algébrica de K/k e seja $P' \in \mathbb{P}(K')$ um place de K'/k' sobre $P \in \mathbb{P}(K)$.*

(a) *O inteiro* $e(P'|P) := e$ *com*

$$v_{P'}(x) = e \cdot v_P(x) \text{ para qualquer } x \in F$$

é chamado o ***índice de ramificação de*** P' ***sobre*** P. *Dizemos que* $P'|P$ *é ramificado se* $e(P'|P) > 1$ *e não ramificado se* $e(P'|P) = 1$.

(b) $f(P'|P) := [K'_{P'} : K_P]$ *é chamado o* ***grau relativo de*** P' ***sobre*** P.

Proposição B.1.2. *Seja* K'/k' *uma extensão algébrica de* K/k *e* P' *um place de* K'/k' *sobre* $P \in \mathbb{P}(K)$. *Então:*

(a) $f(P'|P) < \infty \Longleftrightarrow [K' : K] < \infty$.

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

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

Proposição B.1.3. *Seja* K'/k' *uma extensão algébrica de* K/k.

(a) *Para qualquer place* $P' \in \mathbb{P}(K')$ *existe exatamente um place* $P \in \mathbb{P}(K)$ *tal que* $P'|P$, *a saber* $P = P' \cap K$.

(b) *Reciprocamente qualquer place* $P \in \mathbb{P}(K)$ *tem ao menos um e no máximo um número finito de extensões* $P' \in \mathbb{P}(K')$.

Definição B.1.4. *Seja* K'/k' *uma extensão algébrica de* K/k. *Para um place* $P \in \mathbb{P}(K)$ *definimos sua* ***conorma*** *(com respeito a* K'/K*) por*

$$Con_{K'/K}(P) := \sum_{P'|P} e(P'|P) \cdot P',$$

onde a soma percorre todos os places $P' \in \mathbb{P}(K')$ *sobre* P. *A aplicação conorma é estendida a um homomorfismo de* $\mathcal{D}_K$ *para* $\mathcal{D}_{K'}$ *por*

$$Con_{K'|K}(\sum n_P \cdot P) := \sum n_P \cdot Con_{K'/K}(P).$$

Proposição B.1.4. *Seja* K'/k' *uma extensão algébrica do corpo de funções* K/k. *Para* $0 \neq x \in K$ *seja* $(x)_0^K$, $(x)_\infty^K$, $(x)^K$ *resp.* $(x)_0^{K'}$, $(x)_\infty^{K'}$, $(x)^{K'}$ *seu divisor zero, polo e divisor principal em* $\mathcal{D}_K$ *resp. em* $\mathcal{D}_{K'}$. *Então* $Con_{K'/K}((x)_0^K) = (x)_0^{K'}$, $Con_{K'/K}((x)_\infty^K) = (x)_\infty^{K'}$ *e* $Con_{K'/K}((x)^K) = (x)^{K'}$.

Por esta proposição, conorma induz um homomorfismo (novamente denotado por conorma) dos grupos de classes de divisores $Con_{K'/K} : \mathcal{C}_K \longrightarrow \mathcal{C}_{K'}$. Esta aplicação não é em geral injetiva ou sobrejetiva (onde a aplicação $Con_{K'/K} : \mathcal{D}_K \longrightarrow \mathcal{D}_{K'}$ é trivialmente injetiva).

Lema B.1.2. *Seja* K'/K *uma extensão finita de corpos e* x *um transcendente sobre* K. *Então*

$$[K'(x) : K(x)] = [K' : K].$$

Teorema B.1.1. *Seja K'/k' uma extensão finita de K/k, P um place de K/k e $P_1, P_2, \cdots, P_m$ todos os places de K'/k' sobre P. Seja $e_i := e(P_i|P)$ os índices de ramificação e $f_i := f(P_i|P)$ os graus relativos de $P_i|P$. Então*

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

Corolário B.1.1. *Seja K'/k' uma extensão finita de K/k e $P \in \mathbb{P}(K)$. Então:*

(a) $|\{P' \in \mathbb{P}_{K'} : P' \text{ está sobre } P\}| \leq [K' : K]$.

(b) *Se $P' \in \mathbb{P}_{K'}$ está sobre P então $e(P'|P) \leq [K' : K]$ e $f(P'|P) \leq [K' : K]$.*

Corolário B.1.2. *Seja K'/k' uma extensão finita de K/k. Então para qualquer divisor $A \in \mathcal{D}_K$,*

$$deg(Con_{K'/K}(A)) = \frac{[K' : K]}{[k' : k]} \cdot deg(A).$$

Proposição B.1.5. *Considere um corpo de funções K/k e um polinômio*

$$\phi(T) = a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0$$

com coeficientes $a_i \in K$. Assuma que existe um place $P \in \mathbb{P}(K)$ tal que uma das seguintes condições vale:

(1) $v_P(a_n) = 0, v_P(a_i) \geq v_P(a_0) > 0$ *para* $i = 1, \cdots, n-1$ *e* $mdc(n, v_P(a_0)) = 1$.

(2) $v_P(a_n) = 0, v_P(a_i) \geq 0$ *para* $i = 1, \cdots, n-1$, $v_P(a_0) < 0$ *e* $mdc(n, v_P(a_0)) = 1$.

Então $\phi(T)$ é irredutível em $K[T]$. Se $K' = K(y)$ onde y é uma raíz de $\phi(T)$, então P tem uma única extensão $P' \in \mathbb{P}(K')$ e temos que $e(P'|P) = n$ e $f(P'|P) = 1$.

B.2 Anéis de corpos de funções

Definição B.2.1. *Um* ***subanel de*** *K/k é um anel R tal que $k \subseteq R \subseteq K$ e R não é um corpo.*

Definição B.2.2. *Para $\emptyset \neq S \subsetneq \mathbb{P}(K)$ seja*

$$\mathcal{O}_S := \{z \in K : v_P(z) \geq 0, \forall P \in S\}$$

a intersecção de todos os anéis de valorização $\mathcal{O}_P$ com $P \in S$. Qualquer anel $R \subseteq K$ que é da forma $R = \mathcal{O}_S$ para algum $S \subsetneq \mathbb{P}(K)$ e $S \neq \emptyset$ é chamado um ***anel holomórfico de*** *K/k.*

Lema B.2.1. (a) *Qualquer anel de valorização $\mathcal{O}_P$ é um anel holomórfico, a saber $\mathcal{O}_P = \mathcal{O}_S$ com $S = \{P\}$.*

(b) *Qualquer anel holomórfico $\mathcal{O}_S$ é um subanel de K/k.*

(c) *Para* $P \in \mathbb{P}(K)$ *e* $\emptyset \neq S \subsetneq \mathbb{P}(K)$ *temos*

$$\mathcal{O}_S \subseteq \mathcal{O}_P \Longleftrightarrow P \in S.$$

Consequentemente $\mathcal{O}_S = \mathcal{O}_T \Longleftrightarrow S = T$.

Definição B.2.3. *Seja* R *um subanel de* K/k.

(a) *Um elemento* $z \in K$ *é dito* ***integral sobre*** R *se* $f(z) = 0$ *para algum polinômio mônico* $f(X) \in R[X]$, *isto é, existem* $a_0, a_1, \cdots, a_{n-1} \in R$ *tais que*

$$z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0 = 0.$$

Tal equação é chamada uma equação integral para z *sobre* R.

(b) *O conjunto*

$$ic_K(R) := \{z \in K | z \text{ é integral sobre } R\}$$

é chamado o ***fecho integral de*** R ***em*** K.

(c) *Seja* $K_0 \subseteq K$ *o corpo quociente de* R. *O anel* R *é chamado integralmente fechado se* $ic_{K_0}(R) = R$, *isto é, qualquer* $z \in K_0$ *que é integral sobre* R *já está em* R.

Proposição B.2.1. *Seja* $\mathcal{O}_S$ *um anel holomórfico de* K/k. *Então*

(a) K *é o corpo quociente de* $\mathcal{O}_S$.

(b) $\mathcal{O}_S$ *é integralmente fechado.*

Teorema B.2.1. *Seja* R *um subanel de* K/k *e*

$$S(R) := \{P \in \mathbb{P}(K) | R \subseteq \mathcal{O}_P\}.$$

Então vale:

(a) $\emptyset \neq S \subsetneq \mathbb{P}(K)$.

(b) *O fecho integral de* R *em* K *é* $ic_K(R) = \mathcal{O}_{S(R)}$. *Em particular,* $ic_K(R)$ *é um subanel integralmente fechado de* K/k *com corpo quociente* K.

Corolário B.2.1. *Um subanel de* K/k *com corpo quociente* K *é integralmente fechado se e somente se* R *é um anel holomórfico.*

Proposição B.2.2. *Seja $\mathcal{O}_S$ um anel holomórfico de K/k. Então existe uma correspondência biunívoca entre S e o conjunto de ideais maximais de $\mathcal{O}_S$, dado por*

$$P \longrightarrow M_P := P \cap \mathcal{O}_S \text{ (para } P \in S).$$

Mais ainda, a aplicação

$$\begin{array}{ccc} \mathcal{O}_S/M_P & \longrightarrow & K_P = \mathcal{O}_P/P \\ x + M_P & \longmapsto & x + P \end{array}$$

é um isomorfismo.

Proposição B.2.3. *Se $S \subseteq \mathbb{P}(K)$ é um subconjunto não vazio de places de K/k, então $\mathcal{O}_S$ é um domínio de ideais principais.*

B.3 Bases Integrais Locais

Nesta seção K/k é um corpo de funções com corpo de constantes k e $K' \supseteq K$ é uma extensão finita (o corpo de constantes k' de K' pode ser maior que k).

Proposição B.3.1. *Seja R um subanel integralmente fechado de K/k tal que K é o corpo quociente de R. Para $z \in K'$ seja $\phi(T) \in K[T]$ seu polinômio minimal sobre K. Então temos que*

$$z \text{ é integral sobre } R \Longleftrightarrow \phi(T) \in R[T].$$

Corolário B.3.1. *Seja R um subanel integralmente fechado de K/k tal que K é o corpo quociente de R. Seja $Tr_{K'/K} : K' \longrightarrow K$ a aplicação traço de K' para K e $x \in K'$ integral sobre R. Então $Tr_{K'/K}(x) \in R$.*

Proposição B.3.2. *Seja M/L uma extensão de corpos finita e separável e considere a base $\{z_1, \cdots, z_n\}$ de M/L. Então existem elementos $\{z_1^*, \cdots, z_n^*\} \in M$ unicamente determinados, tal que*

$$Tr_{M/L}(z_i z_j^*) = \delta_{ij}.$$

O conjunto $\{z_1^*, \cdots, z_n^*\}$ é uma base de M/L que é chamada **base dual de** *$\{z_1, \cdots, z_n\}$(com respeito ao traço).*

Teorema B.3.1. *Seja R um subanel integralmente fechado de K/k com corpo de quocientes K e K'/K uma extensão separável de grau n. Seja $R' = ic_{K'}(R)$ o fecho integral de R em K'. Então temos:*

(a) *Para qualquer base $\{x_1, \cdots, x_n\}$ de K'/K, existem elementos $a_i \in R\backslash\{0\}$ tais que*

$$a_1 x_1, \cdots, a_n x_n \in R'.$$

Consequentemente, existe uma base de K'/K que está contida em R'.

(b) *Se $\{z_1, \cdots, z_n\} \subseteq R'$ é uma base de K'/K e $\{z_1^*, \cdots, z_n^*\}$ é sua base dual com respeito ao traço, então*

$$\sum_{i=1}^{n} Rz_i \subseteq R' \subseteq \sum_{i=1}^{n} Rz_i^*.$$

(c) *Se em adição R é um domínio de ideais principais, então existe uma base $\{u_1, \cdots, u_n\}$ de K'/K com a propriedade*

$$R' = \sum_{i=1}^{n} Ru_i.$$

Corolário B.3.2. *Seja K'/K uma extensão finita e separável do corpo de funções K/k e $P \in \mathbb{P}(K)$ um place de K/k. Então o fecho integral $\mathcal{O}'_P$ de $\mathcal{O}_P$ em K' é*

$$\mathcal{O}'_P = \bigcap_{P'|P} \mathcal{O}_{P'}.$$

Existe uma base $\{u_1, \cdots, u_n\}$ de K'/K tal que

$$\mathcal{O}'_P = \sum_{i=1}^{n} \mathcal{O}_P \cdot u_i.$$

Tal base é chamada uma ***base integral de $\mathcal{O}'_P$ sobre $\mathcal{O}_P$.***

Teorema B.3.2. *Seja K/k um corpo de funções, K'/K uma extensão finita e separável de corpos. Então qualquer base $\{z_1. \cdots, z_n\}$ de K'/K é uma base integral para quase todos os places $P \in \mathbb{P}(K)$.*

Notação B.3.1. **(i)** *$\overline{K} := K_P$ o corpo das classes residuais de P.*

(ii) *$\overline{a} := a(P) \in \overline{K}$ a classe residual de $a \in \mathcal{O}_P$.*

(iii) *Se $\psi(T) = \sum c_i T^i$ é um polinômio com coeficientes $c_i \in \mathcal{O}_P$, definimos*

$$\overline{\psi}(T) := \sum \overline{c_i} T^i \in \overline{K}[T].$$

Teorema B.3.3. ***(Kummer).*** *Suponha que $K' = K(y)$ onde y é integral sobre $\mathcal{O}_P$ e considere o polinômio minimal $\phi(T) \in \mathcal{O}_P[T]$ de y sobre K. Seja*

$$\overline{\phi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\epsilon^i}$$

a decomposição de $\overline{\phi}(T)$ sobre $\overline{K}$. Escolha polinômios mônicos

$$\phi_i(T) \in \mathcal{O}_P[T] \text{ com } \overline{\phi}_i(T) = \gamma_i(T) \text{ e } deg\phi_i(T) = deg\gamma_i(T).$$

Então para $1 \leq i \leq r$ existem places $P_i \in \mathbb{P}(K')$ satisfazendo

$$P_i|P,\ \phi_i(y) \in P_i \text{ e } f(P_i|P) \geq deg\gamma_i(T).$$

Mais ainda, $P_i \neq P_j$ para $i \neq j$. Sob hipóteses adicionais, prova-se mais: Suponha que ao menos uma das hipóteses (*) ou (**) são verificadas:

(*) $\epsilon_i = 1$ *para* $i = 1, \cdots, r$, *ou*

(**) $\{1, y, \cdots, y^{n-1}\}$ *é uma base integral para* P.

Então existe, para $1 \leq i \leq r$, *exatamente um place* $P_i \in \mathbb{P}(K')$ *com* $P_i|P$ *e* $\phi_i(y) \in P_i$. *Os places* $P_1, \cdots, P_r$ *são todos os places de* K' *sobre* P *e temos*

$$Con_{K'/K}(P) = \sum_{i=1}^{r} \epsilon_i P_i,$$

isto é, $\epsilon_i = e(P_i|P)$. *A classe residual* $K'_{P_i} = \mathcal{O}_{P_i}/P_i$ *é isomorfa a* $\overline{K}[T]/(\gamma_i(T))$ *e* $f(P_i|P) = deg\gamma_i(T)$.

Corolário B.3.3. *Seja* $\phi(T) = T^n + f_{n-1}(x)T^{n-1} + \cdots + f_0(x) \in k(x)[T]$ *um polinômio irredutível sobre o corpo de funções racionais* $k(x)$. *Consideremos o corpo de funções* $k(x, y)/k$ *onde* y *satisfaz a equação* $\phi(y) = 0$ *e um elemento* $\alpha \in k$ *tal que* $f_j(\alpha) \neq \infty$ *para qualquer* $j, 0 \leq j \leq n-1$. *Denote por* $P_\alpha \in \mathbb{P}(k(x))$ *o zero de* $x - \alpha$ *em* $k(x)$. *Suponha que o polinômio*

$$\phi_\alpha(T) := T^n + f_{n-1}(\alpha)T^{n-1} + \cdots + f_0(\alpha) \in k[T]$$

tem a seguinte decomposição no anel de polinômios $k[T]$:

$$\phi_\alpha(T) = \prod_{i=1}^{r} \psi_i(T)$$

com polinômios $\psi_i(T) \in k[T]$ *mônicos, irredutíveis e distintos entre si. Então temos:*

(a) *Para qualquer* $i = 1, \cdots, r$, *existe um place* $P_i \in \mathbb{P}(k(x, y))$ *tal que* $x - \alpha \in P_i$ *e* $\psi_i(y) \in P_i$. *O elemento* $x - \alpha$ *é um elemento primo de* P_i *e o corpo das classes residuais de* P_i *é isomorfo a* $k[T]/(\psi_i(T))$. *Por isso* $f(P_i|P) = deg\psi_i(T)$.

(b) *Se* $deg\psi_i(T) = 1$ *para ao menos um* $i \in \{1, \cdots, r\}$, *então* k *é o corpo de constantes de* $k(x, y)$.

(c) *Se* $\phi_\alpha(T)$ *tem* $n = deg\phi(T)$ *raízes distintas em* k, *então existe para cada* β *com* $\phi_\alpha(\beta) = 0$ *um único place* $P_{\alpha,\beta} \in \mathbb{P}(k(x, y))$ *tal que*

$$x - \alpha \in P_{\alpha,\beta} \text{ e } y - \beta \in P_{\alpha,\beta}.$$

$P_{\alpha,\beta}$ *é um place de* $k(x, y)$ *de grau* 1.

B.4 O Cotraço de diferenciais de Weil e a fórmula do gênero de Hurwitz

Nesta seção, vamos considerar K/k um corpo de funções, K'/K uma extensão finita e separável e k' corpo de constantes de K'. Claramente, k'/k é uma extensão finita e separável.

Definição B.4.1. *Para* $P \in \mathbb{P}(K)$, *seja* $\mathcal{O}'_P := ic_{K'}(\mathcal{O}_P)$ *o fecho integral de* $\mathcal{O}_P$ *em* K'. *Então o conjunto*

$$\mathcal{C}_P := \{z \in K' | Tr_{K'/K}(z \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P\}$$

é chamado o ***módulo complementar*** *sobre* $\mathcal{O}_P$.

Proposição B.4.1. *Com as notações da definição B.4.1, vale:*

(a) $\mathcal{C}_P$ *é um* $\mathcal{O}'_P$*-módulo e* $\mathcal{O}'_P \subseteq \mathcal{C}_P$.

(b) *Se* $\{z_1, \cdots, z_n\}$ *é uma base integral de* $\mathcal{O}'_P$ *sobre* $\mathcal{O}_P$*, então*

$$\mathcal{C}_P = \sum_{i=1}^{n} \mathcal{O}_P \cdot z_i^*,$$

onde $\{z_1^*, \cdots, z_n^*\}$ *é a base dual de* $\{z_1, \cdots, z_n\}$.

(c) *Existe um elemento* $t \in K'$ *(dependendo de* P*) tal que* $\mathcal{C}_P = t \cdot \mathcal{O}'_P$*. Mais ainda,*

$$v_{P'}(t) \leq 0 \text{ para todo } P'|P,$$

e se $t' \in K'$*, então*

$$\mathcal{C}_P = t' \cdot \mathcal{O}'_P \Longleftrightarrow v_{P'}(t') = v_{P'}(t), \forall P'|P.$$

(d) $\mathcal{C}_P = \mathcal{O}'_P$ *para quase todo* $P \in \mathbb{P}(K)$.

Definição B.4.2. *Considere um place* $P \in \mathbb{P}(K)$ *e o fecho integral* $\mathcal{O}'_P$ *de* $\mathcal{O}_P$ *em* K'*. Seja* $\mathcal{C}_P = t' \cdot \mathcal{O}'_P$ *o módulo complementar sobre* $\mathcal{O}_P$*. Então definimos, para* $P'|P$*, o* ***expoente diferente*** *de* P' *sobre* P *por*

$$d(P'|P) := -v_{P'}(t).$$

Pela proposição B.4.1, $d(P'|P)$ *está bem definido e* $d(P'|P) \geq 0$*. Mais ainda,* $d(P'|P) = 0$ *vale para quase todo* $P \in \mathbb{P}(K)$ *e* $P'|P$*, pois* $\mathcal{C}_P = 1 \cdot \mathcal{O}'_P$ *para quase todo* P*. Portanto, podemos definir o divisor*

$$Diff(K'/K) := \sum_{P \in \mathbb{P}(K)} \sum_{P'|P} d(P'|P) \cdot P'$$

que será chamado o ***diferente de*** K'/K.

Observação B.4.1. *Temos a seguinte e útil caracterização do módulo complementar* $\mathcal{C}_P$*, que segue diretamente das definições. Para* $z \in K'$*, temos*

$$z \in \mathcal{C}_P \Longleftrightarrow v_{P'}(z) \geq -d(P'|P) \text{ para todo } P'|P.$$

Definição B.4.3. *Seja*

$$\mathcal{A}_{K'/K} := \{\alpha \in \mathcal{A}_K | \alpha_{P'} = \alpha_{Q'} \text{ sempre que } P' \cap K = Q' \cap K\}.$$

Então $\mathcal{A}_{K'/K}$ *é um* k'*-subespaço de* $\mathcal{A}'_K$*. A aplicação* $Tr_{K'/K} : K' \longrightarrow K$ *pode ser estendida para uma aplicação* K*-linear de* $\mathcal{A}_{K'/K}$ *para* $\mathcal{A}_K$ *por*

$$(Tr_{K'/K}(\alpha))_P := Tr_{K'/K}(\alpha_{P'}), \text{ para } \alpha \in \mathcal{A}_{K'/K},$$

onde P' é qualquer place de K' sobre P. Claramente o traço de um adele principal $z \in K'$ é o adele principal de $Tr_{K'/K}(z)$. Para um divisor $A' \in \mathcal{D}_{K'}$, definimos

$$\mathcal{A}_{K'/K}(A') := \mathcal{A}_{K'}(A') \cap \mathcal{A}_{K'/K}.$$

Teorema B.4.1. *Como na situação precedente, para cada diferencial de Weil ω de K/k, existe um único diferencial de Weil ω' de K'/k', tal que*

$$Tr_{K'/K}(\omega'(\alpha)) = \omega(Tr_{K'/K}(\alpha))$$

para todo $\alpha \in \mathcal{A}_{K'/K}$. Este diferencial é chamado o **cotraço de** ω **em** K'/K *e é denotado por $Cotr_{K'/K}(\omega)$. Se $\omega \neq 0$ e $(\omega) \in \mathcal{D}_K$ é o divisor de ω, então*

$$(Cotr_{K'/K}(\omega)) = Con_{K'/K}((\omega)) + Diff(K'/K).$$

Observação B.4.2. *Usando as notações de componentes locais de um diferenciais de Weil, a equação anterior pode ser substituída pela seguinte condição local: para qualquer place $P \in \mathbb{P}(K)$ e $y \in K'$,*

$$\omega_P(Tr_{K'/K}(y)) = Tr_{K'/K}\left(\sum_{P'|P} \omega'_{P'}(y)\right).$$

Lema B.4.1. *Para qualquer $C' \in \mathcal{D}_{K'}$, temos $\mathcal{A}_{K'} = \mathcal{A}_{K'/K} + \mathcal{A}_{K'}(C')$.*

Lema B.4.2. *Seja M/L uma extensão de corpos finita e separável, V um espaço vetorial sobre M e $\mu : V \longrightarrow L$ uma aplicação L-linear. Então existe uma única aplicação M-linear $\mu' : V \longrightarrow M$ tal que $Tr_{M/L} \circ \mu' = \mu$.*

Proposição B.4.2. **(a)** *Se ω, ω_1 e ω_2 são diferenciais de Weil de K/k e $x \in K$, então*

$$Cotr_{K'/K}(\omega_1 + \omega_2) = Cotr_{K'/K}(\omega_1) + Cotr_{K'/K}(\omega_2)$$

e

$$Cotr_{K'/K}(x\omega) = x \cdot Cotr_{K'/K}(\omega).$$

(b) *Seja K''/K' outra extensão finita e separável. Então*

$$Cotr_{K''/K'}(\omega) = Cotr_{K''/K'}(Cotr_{K'/K}(\omega))$$

para qualquer diferencial de Weil ω de K/k.

Corolário B.4.1. *Em uma torre $K'' \supseteq K' \supseteq K$ de extensões finitas e separáveis, vale:*

(a) $Diff(K''/K) = Con_{K''/K'}(Diff(K'/K)) + Diff(K''/K')$.

(b) $d(P''/P) = e(P''|P') \cdot d(P'|P) + d(P''|P')$, *se P'' (resp. P', P) são places de K'' (resp. K', F) com $P'' \supseteq P' \supseteq P$.*

Teorema B.4.2. ***(Fórmula do gênero de Hurwitz).*** *Seja K/k um corpo de funções algébricas de gênero g e K'/K uma extensão finita e separável. Seja k' o corpo de constantes de K' e g' o gênero de K'/k'. Então temos que*

$$2g' - 2 = \frac{[K' : K]}{[k' : k]}(2g - 2) + deg(Diff(K'/K)).$$

B.5 O Diferente

Consideramos uma extensão finita e separável K'/K onde K/k e K'/k' são corpos de funções com corpos de constantes k e k', respectivamente. Como sempre, k (por isso k') é assumido como sendo perfeito.

Teorema B.5.1. ***(Teorema do Diferente de Dedekind).*** *Com as notações como anteriormente, temos para todo $P'|P$:*

(a) $d(P'|P) \geq e(P'|P) - 1$.

(b) $d(P'|P) = e(P'|P) - 1$ *se e somente se $e(P'|P)$ não é divisível por $car(k)$. Em particular, se $car(k) = 0$ então $d(P'|P) = e(P'|P) - 1$.*

Lema B.5.1. *Seja K^*/K uma extensão algébrica de corpos de funções, $P \in \mathbb{P}(K)$ e $P^* \in \mathbb{P}(K^*)$ com $P^*|P$. Considere um automorfismo σ de K^*/K. Então $\sigma(P^*) := \{\sigma(z)|z \in P^*\}$ é um place de K^* e temos:*

(a) $v_{\sigma(P^*)}(y) = v_{P^*}(\sigma^{-1}(y))$ *para todo $y \in K^*$.*

(b) $\sigma(P^*)|P$.

(c) $e(\sigma(P^*)|P) = e(P^*|P)$ *e* $f(\sigma(P^*)|P) = f(P^*|P)$.

Lema B.5.2. *Sejam $P \in \mathbb{P}(K)$ e $P_1, \cdots, P_r \in \mathbb{P}(K')$ todas as extensões de P em K'/K. Considere o corpo das classes residuais $\overline{k} := \mathcal{O}_P/P$ resp. $\overline{k}_i := \mathcal{O}_{P_i}/P_i \supseteq \overline{k}$ e as correspondentes aplicações residuais $\pi : \mathcal{O}_P \longrightarrow \overline{k}$ resp. $\pi_i : \mathcal{O}_{P_i} \longrightarrow \overline{k}_i$ (para $i = 1, \cdots, r$). Então temos para qualquer $u \in \mathcal{O}'_P$ (o fecho integral de $\mathcal{O}_P$ em K'),*

$$\pi(Tr_{K'/K}(u)) = \sum_{i=1}^{r} e(P_i|P) \cdot Tr_{\overline{k}_i/\overline{k}}(\pi_i(u)).$$

Definição B.5.1. *Sejam K'/K uma extensão de corpos de funções e $P \in \mathbb{P}(K)$.*

(a) *Uma extensão P' de P em K' é dita* ***domesticamente (selvagemente) ramificada*** *se $e(P'|P) > 1$ e $car(k)$ não divide $e(P'|P)$ (resp. $e(P'|P) > 1$ e $car(k)$ divide $e(P'|P)$)).*

(b) *Dizemos que P é* ***ramificado (resp. não ramificado)*** *em K'/K se existe ao menos um $P' \in \mathbb{P}(K')$ sobre P tal que $P'|P$ é ramificado(resp. se $P'|P$ é não ramificado para todo $P'|P$). O place P é* ***domesticamente ramificado*** *em K'/K se é ramificado em K'/K e nenhuma extensão de P é selvagemente ramificada. Se existe ao menos uma place selvagemente ramificado $P'|P$, dizemos que P é* ***selvagemente ramificado em*** *K'/K.*

(c) *P é* ***totalmente ramificado*** *em K'/K se existe somente uma extensão $P' \in \mathbb{P}(K')$ de P em K' e o índice de ramificação é $e(P'|P) = [K' : K]$.*

(d) *K'/K é dita* ***ramificada (resp. não ramificada)*** *se ao menos um $P \in \mathbb{P}(K)$ é ramificado em K'/K (resp. se todos os places $P \in \mathbb{P}(K)$ são não ramificados em K'/K).*

(e) *K'/K é dita* ***doméstica*** *se nenhum place $P \in \mathbb{P}(K)$ é selvagemente ramificado em K'/K.*

Corolário B.5.1. *Seja K'/K uma extensão finita e separável de corpos de funções.*

(a) *Se $P \in \mathbb{P}(K)$ e $P' \in \mathbb{P}(K')$ tal que $P'|P$, então $P'|P$ é ramificada se e somente se $P' \leq Diff(K'/K)$. Se $P'|P$ é ramificada, então*

$$d(P'|P) = e(P'|P) - 1 \Longleftrightarrow P'|P \text{ é domesticamente ramificado,}$$

$$d(P'|P) \geq e(P'|P) \Longleftrightarrow P'|P \text{ é selvagemente ramificado.}$$

(b) *Quase todos os places $P \in \mathbb{P}(K)$ são não ramificados em K'/K.*

Corolário B.5.2. *Suponha que K'/K é uma extensão finita e separável de corpos de funções, tendo o mesmo corpo de constantes k. Seja g (resp. g') o gênero de K/k (resp. K'/k). Então*

$$2g' - 2 \geq [K' : K] \cdot (2g - 2) + \sum_{P \in \mathbb{P}(K)} \sum_{P'|P} (e(P'|P) - 1) \cdot deg(P').$$

A igualdade vale se e somente se K'/K é doméstico, o que é o caso quando $car(k) = 0$.

Corolário B.5.3. *Suponha que K'/K é uma extensão finita e separável de corpos de funções, tendo o mesmo corpo de constantes k. Seja g (resp. g') o gênero de K/k (resp. K'/k). Então $g \leq g'$.*

Corolário B.5.4. *Seja $K/k(x)$ uma extensão finita e separável do corpo de funções racionais de grau $[K : k(x)] > 1$ tal que k é o corpo de constantes de K. Então $K/k(x)$ é ramificado.*

Proposição B.5.1. ***(Teorema de Luroth).*** *Qualquer subcorpo de um corpo de funções racionais é racional, isto é, se $k \subsetneq K_0 \subseteq k(x)$ então $K_0 = k(y)$ para algum $y \in K_0$.*

Teorema B.5.2. *Suponha que $K' = K(y)$ é uma extensão finita e separável de um corpo de funções K de grau $[K' : K] = n$. Seja $P \in \mathbb{P}(K)$ tal que o polinômio minimal $\phi(T)$ de y sobre K tem os coeficientes em $\mathcal{O}_P$ (isto é, y é integral sobre $\mathcal{O}_P$), e sejam $P_1, \cdots, P_r \in \mathbb{P}(K')$ todos os places de K' sobre P. Então o seguinte vale:*

(a) *$d(P_i|P) \leq v_{P_i}(\phi'(y))$ para $1 \leq i \leq r$.*

(b) $\{1, y, \cdots, y^{n-1}\}$ *é uma base integral de* K'/K *no place* P *se e somente se* $d(P_i|P) = v_{P_i}(\phi'(y))$ *para* $1 \leq i \leq r$.

(Aqui, $\phi'(T)$ *denota a derivada de* $\phi(T)$ *no anel dos polinômios* $K[T]$*.)*

Corolário B.5.5. *Seja* $K' = K(y)$ *uma extensão finita e separável de corpos de funções de grau* $[K' : K] = n$ *e seja* $\phi(T) \in K[T]$ *o polinômio minimal de* y *sobre* K*. Suponha que* $P \in \mathbb{P}(K)$ *satisfaz*

$$\phi(T) \in \mathcal{O}_P[T] \text{ e } v_{P'}(\phi'(y)) = 0$$

para todo $P' \in \mathbb{P}(K')$ *com* $P'|P$*. Então* P *é não ramificado em* K'/K *e* $\{1, y, \cdots, y^{n-1}\}$ *é uma base integral para* K'/K *em* P*.*

Proposição B.5.2. *Seja* K'/K *uma extensão finita e separável de corpos,* $P \in \mathbb{P}(K)$ *e* $P' \in \mathbb{P}(K')$ *com* $P'|P$*. Suponha que* $P'|P$ *é totalmente ramificado, isto é,* $e(P'|P) = [K' : K] = n$*. Seja* $t \in K'$ *um* P'*-elemento primo e considere o polinômio minimal* $\phi(T) \in K[T]$ *de* t *sobre* K*. Então* $d(P'|P) = v_{P'}(\phi'(t))$ *e* $\{1, t, \cdots, t^{n-1}\}$ *é uma base integral para* K'/K *sobre* P*.*

B.6 Extensões de Corpos Constantes

Seja $K' \supseteq K$ uma extensão algébrica de corpos (com $K' \subseteq \Phi$). O compositum $K' := Kk'$ é um corpo de funções sobre k' e seu corpo de constantes é uma extensão finita de k'. Entretanto (isto não é claro a priori) K' é o corpo de funções de Kk'.

Proposição B.6.1. *Seja* $K' = Kk'$ *uma extensão algébrica constante de* K/k *(de grau finito ou infinito). Então temos:*

(a) k' *é o corpo de constantes de* K'*.*

(b) *Qualquer subconjunto de* K *que é linearmente independente sobre* k *também o é sobre* k'*.*

(c) $[K : k(x)] = [K' : K'(x)]$ *para qualquer* $x \in K \setminus k$*.*

Lema B.6.1. *Suponha que* $\alpha \in \Phi$ *é algébrico sobre* k*. Então* $[k(\alpha) : k] = [K(\alpha) : K]$*.*

Teorema B.6.1. *Em uma extensão de corpos constante* $K' = Kk'$ *de* K/k*, o seguinte vale:*

(a) K'/K *é não ramificado (isto é,* $e(P'|P) = 1$ *para todo* $P \in \mathbb{P}(K)$ *e* $P' \in \mathbb{P}(K')$ *com* $P'|P$*).*

(b) K'/k' *tem o mesmo gênero de* K/k*.*

(c) *Para qualquer divisor* $A \in \mathcal{D}_K$*, temos* $deg(Con_{K'/K}(A)) = deg(A)$*.*

(d) *Para qualquer divisor* $A \in \mathcal{D}_K$*,*

$$dim(Con_{K'/K}(A)) = dim(A).$$

Mais precisamente: Qualquer base de $\mathcal{L}(A)$ *é uma base de* $\mathcal{L}(Con_{K'/K}(A))$ *também. (Note que* $\mathcal{L}(A) \subseteq K$ *é um* k*-espaço vetorial, enquanto que* $\mathcal{L}(Con_{K'/K}(A))$ *é um* k'*- espaço vetorial.)*

(e) *Se* W *é um divisor canônico de* K/k *então* $Con_{K'/K}(W)$ *é um divisor canônico de* K'/k'*.*

(f) *A aplicação conorma* $Con_{K'/K} : \mathcal{C}_K \longrightarrow \mathcal{C}_{K'}$ *do grupo das classes de divisores de* K/k *na de* K'/k' *é injetiva.*

(g) *O corpo das classes residuais* $K'_{P'}$ *de qualquer place* $P' \in \mathbb{P}(K')$ *é o compositum* $K_P K'$ *de* K' *e o corpo das classes residuais* K_P, *onde* $P = P' \cap K$.

(h) *Se* K'/K *é de grau finito, qualquer base de* K'/K *é uma base integral de* K'/K *para todo* $P \in \mathbb{P}(K)$.

Corolário B.6.1. *Seja* K'/K *uma extensão algébrica de* K/k*(não necessariamente uma extensão de corpos constante). Então temos, para qualquer divisor* $A \in \mathcal{D}_K$ *que*

$$deg(Con_{K'/K}(A)) = [K' : Kk'] \cdot deg(A).$$

Corolário B.6.2. *Seja* $P \in \mathbb{P}(K)$ *um place de* K/k *de grau* r *e* $\overline{K} = K\overline{k}$ *a extensão de corpos constante de* K/k *com o fecho algébrico* $\overline{k}$ *de* k. *Então*

$$Con_{\overline{K}/K}(P) = \overline{P}_1 + \cdots + \overline{P}_r$$

com places dois a dois distintos $\overline{P}_i \in \mathbb{P}(\overline{K})$.

Proposição B.6.2. *Seja* K/k *um corpo de funções com corpo de constantes* k. *Suponha que* K'/K *é uma extensão finita com corpo de constantes* k'. *Seja* $\overline{k} \subseteq \Phi$ *o fecho algébrico de* k. *Então*

$$[K' : K] = [K'\overline{k} : K\overline{k}] \cdot [k' : k].$$

No caso especial em que $K' = K(y)$ *obtemos: se* $\phi(T) \in K[T]$ *é o polinômio minimal de* y *sobre* K, *as seguintes condições são equivalentes:*

(1) $k' = k$.

(2) $\phi(T)$ *é irredutível em* $K\overline{k}[T]$.

Corolário B.6.3. *Seja* $K = k(x, y)$ *um corpo de funções e* $\phi(T) \in k(x)[T]$ *o polinômio minimal de* y *sobre* $k(x)$. *Então as seguintes condições são equivalentes:*

(1) k *é o corpo de constantes de* K.

(2) $\phi(T)$ *é absolutamente irredutível, isto é, é irredutível sobre* $\overline{k}(x)[T]$.

B.7 Extensões de Galois I

Definição B.7.1. *Uma extensão finita de corpos* M/L *é dita de Galois se o grupo dos automorfismos* $Aut(M/L) = \{\sigma : M \longrightarrow M | \sigma$ *é um isomorfismo com* $\sigma(a) = a, \forall a \in L\}$ *tem ordem* $[M : L]$. *Neste caso, chamamos* $Aut(M/L)$ *o grupo de Galois de* M/L *e escrevemos* $Gal(M/L) := Aut(M/L)$. *Uma extensão* K'/k' *de um corpo de funções* K/k *é de Galois se* K'/K *é de Galois de grau finito.*

Teorema B.7.1. *Seja* K'/k' *uma extensão de Galois de* K/k *e* $P_1, P_2 \in \mathbb{P}(K')$ *extensões de* $P \in \mathbb{P}(K)$. *Então* $P_2 = \sigma(P_1)$ *para algum* $\sigma \in Gal(K'/K)$. *Em outras palavras, o grupo de Galois age transitivamente no conjunto das extensões de* P.

Corolário B.7.1. *Com as notações do teorema B.7.1. Sejam $P_1, \cdots, P_r$ todas as extensões de P em K'. Então temos:*

(a) *$e(P_i|P) = e(P_j|P)$ e $f(P_i|P) = f(P_j|P)$ para todos i, j. Por isso, definimos*

$$e(P) := e(P_i|P) \text{ e } f(P) := f(P_i|P)$$

e chamamos $e(P)$ (resp.$f(P)$) o ***índice de ramificação (resp. grau relativo) de P em*** *K'/K.*

(b) *$e(P) \cdot f(P) \cdot r = [K' : K]$. Em particular $e(P), f(P)$ e r dividem o grau $[K' : K]$.*

(c) *Os expoentes diferente $d(P_i|P)$ e $d(P_j|P)$ são o mesmo para todos i, j.*

Proposição B.7.1. ***(Extensões de Kummer)*** *. Seja K/k um corpo de funções em que k contém uma n-ésima raíz primitiva da unidade (com $n > 1$ a n relativamente primo com $car(k)$). Suponha que $u \in K$ é um elemento satisfazendo*

$$u \neq w^d \text{ para todo } w \in K \text{ e } d|n, d > 1.$$

Seja

$$K' = K(y) \text{ com } y^n = u.$$

Uma extensão como tal é chamada uma ***Extensão de Kummer****. Temos:*

(a) *O polinômio $\phi(T) = T^n - u$ é o polinômio minimal de y sobre K (em particular, Φ é irredutível sobre K). A extensão K'/K é Galois de grau n, seu grupo é cíclico e todos os automorfismos de K'/K são dados por $\sigma(y) = \zeta y$, onde $\zeta \in k$ é uma n-ésima raíz da unidade.*

(b) *Seja $P \in \mathbb{P}(K)$ e $P' \in \mathbb{P}(K')$ uma extensão de P. Então*

$$e(P'|P) = n/r_P \text{ e } d(P'|P) = n/r_P - 1,$$

onde

$$r_P := mdc(n, v_P(u)) > 0,$$

o máximo divisor comum de n e $v_P(u)$.

(c) *Se k' denota o corpo de constantes de K' e g (resp. g') o gênero de K/k (resp. K'/k'), então*

$$g' = 1 + \frac{n}{[k' : k]}\Big(g - 1 + \frac{1}{2}\sum_{P \in \mathbb{P}(K)} (1 - \frac{r_P}{n}) deg(P)\Big).$$

Corolário B.7.2. *Seja K/k um corpo de funções e $K' = K(y)$ com $y^n = u \in K$, onde $n \not\equiv 0(mod(car(k)))$ e k contém uma n-ésima raíz primitiva da unidade. Assuma que existe um place $Q \in \mathbb{P}(K)$ tal que $mdc(v_Q(u), n) = 1$. Então k é o corpo de constantes de K', a extensão K'/K é cíclica de grau n e*

$$g' = 1 + n(g-1) + \frac{1}{2} \sum_{P \in \mathbb{P}(K)} (n - r_P) deg(P).$$

Lema B.7.1. *Seja K/k um corpo de funções algébricas de característica $p > 0$. Dado um elemento $u \in K$ e um place $P \in \mathbb{P}(K)$ uma das seguintes afirmações é válida:*

(a) *Existe um elemento $z \in K$ tal que $v_P(u - (z^p - z)) \geq 0$, ou;*

(b) *Para algum $z \in K$,*

$$v_P(u - (z^p - z)) = -m < 0 \text{ com } m \not\equiv 0(mod(p)).$$

No último caso, o inteiro m é unicamente determinao por u e P, a saber,

$$-m = max\{v_P(u - (w^p - w)) | w \in K\}.$$

Proposição B.7.2. ***(Extensões de Artin-Schreier).*** *Seja K/k um corpo de funções de característica $p > 0$. Suponha que $u \in K$ é um elemento que satisfaz a seguinte condição:*

$$u \neq w^p - w \text{ para todo } w \in K.$$

Seja

$$K' = K(y) \text{ com } y^p - y = u. \tag{B.1}$$

Uma tal extensão é chamada ***Extensão de Artin-Schreier de*** *K. Para $P \in \mathbb{P}(K)$ definimos o inteiro m_P por*

$$m_p := \begin{cases} m & \text{se existe um elemento } z \in K \text{ satisfazendo} \\ & v_P(u - (z^p - z)) = -m < 0 \text{ e } m \not\equiv 0(mod(p)), \\ -1 & \text{se } v_P(u - (z^p - z)) \geq 0 \text{ para algum } z \in K. \end{cases}$$

(Observe que m_P está bem definido). Temos então:

(a) *K'/K é uma extensão de Galois cíclica de grau p. Os automorfismos de K'/K são dados por $\sigma(y) = y + \nu$, onde $\nu = 0, 1, \cdots, p-1$.*

(b) *P é não ramificado em K'/K se e somente se $m_P = -1$.*

(c) *P é totalmente ramificado em K'/K se e somente se $m_P > 0$. Denote por P' o único place de K' sobre P. Então o expoente diferente $d(P'|P)$ é dado por*

$$d(P'|P) = (p-1)(m_P + 1).$$

(d) *Se ao menos um place $Q \in \mathbb{P}(K)$ satisfaz $m_Q > 0$, então k é algebricamente fechado em K' e*

$$g' = p \cdot g + \frac{p-1}{2}\Big(-2 + \sum_{P \in \mathbb{P}(K)} (m_P + 1) \cdot deg(P)\Big),$$

onde g' (resp. g) é o gênero de K'/k' (resp. K/k).

Observação B.7.1. (a) *Nas notações de B.7.2, suponha que existe um place $Q \in \mathbb{P}(K)$ com*

$$v_Q(u) < 0 \text{ e } v_Q(u) \not\equiv 0(mod(p)).$$

Então u satisfaz $u \neq w^p - w$ para todo $w \in K$. Por isso, a proposição B.7.2 se aplica a este caso.

(b) *Todas as extensões K'/K de grau $[K' : K] = p = car(k)$ são de Artin-Schreier.*

Proposição B.7.3. *Considere um corpo de funções K/k com corpo de constantes k de característica $p > 0$ e um polinômio aditivo separável $\alpha(T) \in k[T]$ (isto é, $\alpha(T) = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \cdots + a_1 T^p + a_0 T$) de grau p^n que tem todas as raízes em k. Seja $u \in K$. Suponha que para qualquer $P \in \mathbb{P}(K)$ existe um elemento $z \in K$ (dependendo de P) tal que*

$$v_P(u - \alpha(z)) \geq 0$$

ou

$$v_P(u - \alpha(z)) = -m \text{ com } m > 0 \text{ e } m \not\equiv 0(mod(p)).$$

Define $m_P := -1$ no primeiro caso e $m_P = m$ no segundo. Então m está bem definido. Considere a extensão de corpos $K' = K(y)$ de K, onde y satisfaz a equação $\alpha(y) = u$. Se existe ao menos um place $Q \in \mathbb{P}(K)$ com $m_Q > 0$, o seguinte vale:

(a) *K'/K é Galois, $[K' : K] = p^n$ e o grupo de Galois de K'/K é isomorfo ao grupo aditivo $\{a \in k | \alpha(a) = 0\}$, por isso, isomorfo à $(\mathbb{Z}/p\mathbb{Z})^n$. (Tal grupo é chamado grupo abeliano elementar de expoente p e grau p^n.)*

(b) *k é algebricamente fechado em K'.*

(c) *Qualquer $P \in \mathbb{P}(K)$ com $m_P = -1$ é não ramificado em K'/K.*

(d) *Qualquer* $P \in \mathbb{P}(K)$ *com* $m_P > 0$ *é totalmente ramificado em* K'/K *e o expoente diferente* $d(P'|P)$ *da extensão* P' *de* P *em* K' *é*

$$d(P'|P) = (p^n - 1)(m_P + 1).$$

(e) *Seja* g' *(resp.* g*) o gênero de* K'*(resp.* K*). Então*

$$g' = p^n \cdot g + \frac{p^n - 1}{2}\Big(-2 + \sum_{P \in \mathbb{P}(K)} (m_P - 1) \cdot deg(P)\Big).$$

B.8 Extensões de Galois II

Consideremos uma extensão de Galois K'/K de corpos de funções algébricas com grupo de Galois $G := Gal(K'/K)$. Seja P um place de K e P' uma extensão de P em K'.

Definição B.8.1. (a) $G_Z(P'|P) := \{\sigma \in G | \sigma(P') = P'\}$ *é chamado o* ***grupo decomposição de*** P' ***sobre*** P.

(b) $G_T := (P'|P) := \{\sigma \in G | v_{P'}(\sigma(z) - z) > 0$ *para todo* $z \in \mathcal{O}_{P'}\}$ *é chamado o* ***grupo de inércia de*** $P'|P$.

(c) *O corpo fixado* $Z := Z(P'|P)$ *(resp.* $T := T(P'|P)$*) de* $G_Z(P'|P)$ *(resp.* $G_T(P'|P)$*) é chamado o* ***corpo decomposição*** *(resp.* ***corpo de inércia****) de* P' *sobre* P.

Teorema B.8.1. *Com as notações como anteriormente, temos:*

(a) *O grupo decomposição* $G_Z(P'|P)$ *tem ordem* $e(P'|P) \cdot f(P'|P)$.

(b) *O grupo de inércia* $G_T(P'|P)$ *é um subgrupo normal de* $G_Z(P'||P)$ *de ordem* $e(P'|P)$.

(c) *A extensão das classes residuais* $K'_{P'}/K_P$ *é uma extensão de Galois. Qualquer automorfismo* $\sigma \in G_Z(P'|P)$ *induz um automorfismo* $\overline{\sigma}$ *de* $K'_{P'}$ *sobre* K_P *dada por* $\overline{\sigma}(z(P')) = \sigma(z)(P')$ *para* $z \in \mathcal{O}_{P'}$. *A aplicação*

$$\begin{array}{ccc} G_Z(P'|P) & \longrightarrow & Gal(K'_{P'}/K_P) \\ \sigma & \longmapsto & \overline{\sigma} \end{array},$$

é um homomorfismo sobrejetivo, cujo kernel é o grupo de inércia $G_T(P'|P)$. *Em particular* $Gal(K'_{P'}/K_P)$ *é isomorfo a* $G_Z(P'|P)/G_T(P'/P)$.

(c) *Denotemos por* P_Z *(resp.* P_T*) a restrição de* P' *ao corpo decomposição* $Z = Z(P'|P)$ *(resp. ao corpo de inércia* $T = T(P'|P)$*). Então temos a seguinte situação:*

$$\begin{array}{ccl}
K' & P' & e(P'|P_T) = e(P'|P) = [K' : T], f(P'|P_T) = 1 \\
| & | & \\
T & P_T & f(P_T|P_Z) = f(P'|P) = [T : Z], e(P_T|P_Z) = 1 \\
| & | & \\
Z & P_Z & e(P_Z|P) = f(P_Z|P) = 1 \\
| & | & \\
F & P &
\end{array}$$

Teorema B.8.2. *Considere uma extensão de Galois K'/K de corpos de funções algébricas, um place $P \in \mathbb{P}(K)$ e uma extensão P' de P em K'. Para um corpo intermediário $K \subseteq M \subseteq K'$, denotemos por $P_M := P' \cap M$ a restrição de P' à M. Então temos:*

(a) $M \subseteq Z(P'|P) \Longleftrightarrow e(P_M|P) = f(P_M|P) = 1$.

(b) $M \supseteq Z(P'|P) \Longleftrightarrow P'$ *é o único place de* K' *sobre* P_M.

(c) $M \subseteq T(P'|P) \Longleftrightarrow e(P_M|P) = 1$.

(d) $M \supseteq T(P'|P) \Longleftrightarrow P_M$ *é totalmente ramificado em* K'/M.

Corolário B.8.1. *Suponha que K'/K é uma extensão finita e separável de corpos de funções. Sejam K_1, K_2 corpos intermediários de K'/K tal que $K' = K_1K_2$ é o compositum de K_1 e K_2. Então temos, para um place $P \in \mathbb{P}(K)$:*

(a) *Se P é completamente decomponível (isto é, $e(Q|P) = f(Q|P) = 1$ para todas as extensões Q de P) em K_1/K e K_2/K, então P é completamente decomponível em K'/K.*

(b) *Se P é não ramificado em K_1/K e K_2/K, então é não ramificado em K'/K.*

Definição B.8.2. *Seja K'/K uma extensão de Galois de corpos de funções algébricas com grupo de Galois $G = Gal(K'/K)$. Considere um place $P \in \mathbb{P}(K)$ e uma extensão P' de P em K'. Para qualquer $i \geq -1$ definimos o i-ésimo grupo de ramificação de $P'|P$ por*

$$G_i(P'|P) := \{\sigma \in G | v_{P'}(\sigma(z) - z) \geq i + 1 \text{ para todo } z \in \mathcal{O}_{P'}\}.$$

Proposição B.8.1. *Com as notações como anteriormente, temos:*

(a) $G_{-1} = G_Z(P'|P)$ *e* $G_0 = G_T(P'|P)$. *Em particular,* $ord(G_0) = e(P'|P)$.

(b) $G_{-1} \supseteq G_0 \supseteq \cdots \supseteq G_i \supseteq G_{i+1} \supseteq \cdots$ *e* $G_m = \{id\}$ *para m suficientemente grande.*

(c) *Seja $\sigma \in G_0$, $i \geq 0$ e t um P'-elemento primo, isto é, $v_{P'}(t) = 1$. Então,*

$$\sigma \in G_i \Longleftrightarrow v_{P'}(\sigma(t) - t) \geq i + 1.$$

(d) *Se $car(k) = 0$ então $G_i = \{id\}$ para todo $i \geq 1$ e $G_0 = G_T(P'|P)$ é cíclico.*

(e) *Se* $car(k) = p > 0$ *então* G_1 *é um subgrupo normal de* G_0. *A ordem de* G_1 *é uma potência de* p *e o grupo quociente* G_0/G_1 *é cíclico de ordem relativamente prima com* p.

(f) *Se* $car(k) = p > 0$ *então* G_{i+1} *é um subgrupo normal de* G_i *(para qualquer* $i \geq 1$*) e* G_i/G_{i+1} *é isomorfo ao subgrupo aditivo do corpo das classes residuais* $K'_{P'}$ *(por isso,* G_i/G_{i+1} *é um* p*-grupo abeliano elementar de expoente* p*).*

Corolário B.8.2. *Suponha que* K'/K *é uma extensão de corpos de funções de Galois e característica* $p > 0$. *Seja* $P \in \mathbb{P}(K)$ *e* $P' \in \mathbb{P}(K')$ *uma extensão de* P *em* K' *e considere o corpo fixado* $V_1(P'|P)$ *do primeiro grupo de ramificação* $G_1(P'|P)$. *Denote por* P_M *a restrição de* P' *no corpo intermediário* M, $K \subseteq M \subseteq K'$. *Então o seguinte vale:*

(a) $M \subseteq V_1(P'|P) \Longleftrightarrow e(P'|P)$ *é primo com* p.

(b) $M \supseteq V_1(P'|P) \Longleftrightarrow P_M$ *é totalmente ramificado em* K'/M *e* $e(P'|P_M)$ *é uma potência de* p.

Teorema B.8.3. ***(Fórmula do Diferente de Hilbert).*** *Considere uma extensão de corpos de funções de Galois* K'/K, *um place* $P \in \mathbb{P}(K)$ *e um place* $P' \in \mathbb{P}(K')$ *sobre* P. *Então o expoente diferente* $d(P'|P)$ *é*

$$d(P'|P) = \sum_{i=0}^{\infty}(ordG_i(P'|P) - 1)$$

(Note que isto é finito, já que $G_i(P'|P) = \{id\}$ *para* $i \geq m$*).*

Proposição B.8.2. ***(Lema de Abhyankar).*** *Seja* K'/K *uma extensão finita e separável de corpos. Suponha que* $K' = K_1K_2$ *é o compositum de dois corpos intermediários* $K \subseteq K_1, K_2 \subseteq K'$. *Seja* $P' \in \mathbb{P}(K')$ *uma extensão de* $P \in \mathbb{P}(K)$ *e* $P_i := P' \cap F_i$ *para* $i = 1, 2$. *Assuma que ao menos uma das extensões* $P_1|P$ *ou* $P_2|P$ *é doméstica (isto é* $e(P_i|P)$ *é relativamente primo com* $car(k)$*). Então*

$$e(P'|P) = mmc\{e(P_1|P), e(P_2|P)\}.$$

Lema B.8.1. *Seja* G *um grupo finito e* $U \subseteq G$ *um subgrupo normal tal que* $ord(U) = p^n$ *(com* $p = 1$ *ou* p *um número primo) e* G/U *é cíclico de ordem relativamente prima com* p. *Suponha que* H_1 *é um subgrupo de* G *com* $p^n|orh(H_1)$. *Então para qualquer outro* $H_2 \subseteq G$, *temos*

$$ord(H_1 \cap H_2) = mmc(ord(H_1), ord(H_2)).$$

B.9 Extensões inseparáveis

Qualquer extensão algébrica de corpos de funções pode ser quebrada em uma extensão separável K_S/K e uma puramente inseparável K'/K_S. Como estudamos o caso separável, vamos agora estudar o caso puramente inseparável. Através desta seção, k será um corpo perfeito de característica $p > 0$ e K/k um corpo de funções com corpo constante k.

Lema B.9.1. *Suponha que* K'/K *é uma extensão puramente inseparável de corpos de grau* p. *Então* k *é o corpo de constante de* K' *também. Qualquer place* $P \in \mathbb{P}(K)$ *tem somente uma extensão* $P' \in \mathbb{P}(K')$, *a saber,*

$$P' = \{z \in K' | z^p \in P\}.$$

O correspondente anel de valorização é

$$\mathcal{O}_{P'} = \{z \in K' | z^p \in \mathcal{O}_P\}.$$

Temos ainda $e(P'|P) = p$ *e* $f(P'|P) = 1$.

Definição B.9.1. *Um elemento* $x \in K$ *é chamado um elemento separante para* K/k *se* $K/k(x)$ *é uma extensão finita e separável.* K/k *é dito separavelmente gerada se existe um elemento separante para* K/k.

Proposição B.9.1. (a) *Assuma que* $z \in K$ *satisfaz* $v_P(z) \not\equiv 0(mod(P))$ *para algum* $P \in \mathbb{P}(K)$. *Então* z *é um elemento separante para* K/k. *Em particular,* K/k *é separavelmente gerada.*

(b) *Existem* $x, y \in K$ *tal que* $F = k(x, y)$.

(c) *Para* $n \geq 1$, *o conjunto* $K^{p^n} := \{z^{p^n} | z \in K\}$ *é um subcorpo de* K. *Este tem as seguintes propriedades:*

(1) $k \subseteq K^{p^n} \subseteq K$ *e* K/K^{p^n} *é puramente inseparável de grau* p^n.

(2) *A* ***aplicação de Forbenius*** $\phi_n : K \longrightarrow K$ *definida por* $\phi_n(z) := z^{p^n}$ *é um isomorfismo de* K *para* K^{p^n}. *Por isso, o corpo de funções* K^{p^n}/K *tem o mesmo gênero que* K/k.

(3) *Suponha que* $k \subseteq K_0 \subseteq K$ *e* K/K_0 *é puramente inseparável de grau* $[K : K_0] = p^n$. *Então* $K_0 = K^{p^n}$.

(d) *Um elemento* $z \in K$ *é um elemento separante para* K/k *se e somente se* $z \notin K^p$.

B.10 Estimativa do gênero de um corpo de funções

Proposição B.10.1. *Seja* K_1/k *um subcorpo de* K/k *e* $[K : K_1] = n$. *Assuma que* $\{z_1, \cdots, z_n\}$ *é uma base de* K/K_1 *tal que* $z_i \in \mathcal{L}(C), \forall i = 1, \cdots, n$, *onde* $C \in \mathcal{D}_K$ *é um divisor de* K/k. *Então*

$$g \leq 1 + n(g_1 - 1) + deg(C),$$

onde g *(resp.* g_1*) denota o gênero de* K/k *(resp.* K_1/k*).*

Lema B.10.1. *Assuma que* k *é algebricamente fechado e considere um subcorpo* K_1/k *de* K/k *tal que* K/K_1 *é separável de grau* $[K : K_1] = n > 1$. *Seja* $y \in K$ *um elemento com* $K = K_1(y)$. *Então quase todo* $P \in \mathbb{P}(K_1)$ *tem as seguintes propriedades:*

(a) P *tem* n *extensões distintas* $P_1, \cdots, P_n$ *em* K/k.

(b) *As restrições* $P_1 \cap k(y), \cdots, P_n \cap k(y)$ *são places dois a dois distintos em* $k(y)$.

Teorema B.10.1. ***(Desigualdade de Castelnuovo).*** *Seja* K/k *um corpo de funções com corpo de constantes* k. *Suponha que são dados dois subcorpos* K_1/k *e* K_2/k *de* K/k *satisfazendo*

(1) $K = K_1K_2$ *é o compositum de* K_1 *e* K_2.

(2) $[K : K_i] = n_i$ *e* K_i/k *tem gênero* g_i *(i=1,2).*

Então o gênero g *de* K/k *é limitado por*

$$g \leq n_1 g_1 + n_2 g_2 + (n_1 - 1)(n_2 - 1).$$

Corolário B.10.1. ***(Desigualdade de Riemann).*** *Suponha que* $K = k(x, y)$. *Então temos a seguinte estimativa para o gênero* g *de* K/k*:*

$$g \leq ([K : k(x)] - 1) \cdot ([K : k(y)] - 1).$$

Proposição B.10.2. *Considere um corpo de funções algébricas* $K = k(x, y)$ *sobre* k, *onde a equação irredutível para* y *sobre* $k(x)$ *tem a forma*

$$y^n + f_1(x) y_{n-1} + \cdots + f_{n-1}(x) y + f_n(x) = 0$$

com $f_i(x) \in k[x]$ *e* $deg(f_j(x)) \leq j, \forall j = 1, \cdots, n$. *Então o gênero* g *de* K/k *satisfaz a desigualdade* $g \leq \frac{1}{2}(n-1)(n-2)$.

Apêndice C

Corpos de Funções sobre Corpos de Constantes Finitos

Estabelecemos aqui que ao longo de todo esse capítulo, a menos de menção contrária, $K/\mathbb{F}_q$ denotará um corpo de funções de gênero g cujo corpo das constantes é o corpo finito $\mathbb{F}_q$.

C.1 A Função Zeta de Um Corpo de Funções

Lema C.1.1. *Para todo $n \geq 0$, em $K/\mathbb{F}_q$ existe um número finito de divisores positivos de grau n.*

Demonstração. Um divisor positivo é a soma de divisores primos; logo é suficiente provar que o conjunto $S := \{P \in \mathbb{P}(K) \ : \ degP \leq n\}$ é finito. Escolhemos um elemento $x \in K \backslash \mathbb{F}_q$, e consideramos o conjunto $S_0 := \{P_0 \in \mathbb{P}(\mathbb{F}_q(x)) \ : \ degP_0 \leq n\}$. Como $K/\mathbb{F}_q$ é extensão algébrica de $\mathbb{F}_q(x)/\mathbb{F}_q$, temos que para todo $P \in S$, $P \cap \mathbb{F}_q(x) \in S_0$, e, além disso, todo $P_0 \in S_0$ tem um número finito de extensões em K. Sendo assim, precisamos apenas mostrar que S_0 é finito. Como os places de $\mathbb{F}_q(x)$ (com excecão do polo de x) correspondem a polinômios mônicos irredutíveis $p(x) \in \mathbb{F}_q[x]$ do mesmo grau, temos que S_0 é finito. □

Recordemos a notação de capítulos anteriores: $\mathcal{D}_K$ é o grupo dos divisores de $K/\mathbb{F}_q$, $\mathcal{P}_K$ é o subgrupo de $\mathcal{D}_K$ formado pelos divisores principais $(x) = \sum_{P \in \mathbb{P}(K)} v_P(x)P$ (com $0 \neq x \in K$) e o grupo quociente $\mathcal{C}_K = \mathcal{D}_K/\mathcal{P}_K$ é o grupo de classes de divisor de $K/\mathbb{F}_q$. A classe de um divisor A em $\mathcal{C}_K$ é denotada por $[A]$. Como divisores equivalentes têm o mesmo grau e a mesma dimensão, temos que

$$deg[A] := degA \text{ e } dim[A] := dimA$$

estão bem definidos para $[A] \in \mathcal{C}_K$.

Definição C.1.1. *O conjunto*

$$\mathcal{D}_K^0 := \{A \in \mathcal{D}_K \ : \ degA = 0\},$$

que é obviamente um subgrupo de $\mathcal{D}_K$, é chamado ***grupo dos divisores de grau zero****, e*

$$\mathcal{C}_K^0 := \{[A] \in \mathcal{C}_K \ : \ deg[A] = 0\}$$

é o ***grupo de classes de divisor de grau zero.***

Proposição C.1.1. *$\mathcal{C}_K^0$ é um grupo finito.*

Demonstração. Escolha um divisor de grau $\geq g$, digamos $n = degB$; considere o conjunto de classes

$$\mathcal{C}_K^n := \{[C] \in \mathcal{C}_K \ : \ deg[C] = n\}.$$

A aplicação

$$\begin{array}{ccc} \mathcal{C}_K^0 & \longrightarrow & \mathcal{C}_K^n \\ [\mathrm{A}] & \longmapsto & [\mathrm{A+B}] \end{array}$$

é claramente bijetora e, sendo assim, precisamos apenas verificar que $\mathcal{C}_K^n$ é finito.
Afirmação: para todo $[C] \in \mathcal{C}_K^n$, existe $A \in [C]$ tal que $A \geq 0$.
De fato: Como $degC = n \geq g$, temos $dim[C] \geq n + 1 - g \geq 1$ (pelo Teorema de Riemann-Roch). daí $\mathcal{L}(C) \geq 1$ e logo, pelo lema 2.4.1, existe $A \sim C$ com $A \geq 0$, e a afirmação está provada.

Como vimos no lema anterior, existe um número finito de divisores $A \geq 0$ de grau n. Com isso e com a afirmação, concluímos que $\mathcal{C}_K^n$ é finito. □

Definição C.1.2. *A ordem do grupo $\mathcal{C}_K^0$ é chamado* ***"Divisor Class Number"****, e será denotada por $h = h_K$. Em outras palavras,*

$$h := h_K := \left|\mathcal{C}_K^0\right|.$$

Definimos agora o inteiro $\partial > 0$ por

$$\partial := min\{degA \ : \ A \in \mathcal{D}_K \ e \ degA > 0\}. \tag{C.1}$$

A imagem da função grau $deg : \mathcal{D}_K \longrightarrow \mathbb{Z}$ é um subgrupo de $\mathbb{Z}$ gerado por ∂, e o grau de qualquer divisor é um múltiplo de ∂.

Para todo $n \geq 0$, cosideremos o conjunto

$$\mathbb{A}_n := \{A \in \mathcal{D}_K \ : \ A \geq 0 \ e \ degA = n\}. \tag{C.2}$$

Definimos então

$$A_n := |\mathbb{A}_n|. \tag{C.3}$$

No que segue, vamos estudar os números A_n. É fácil ver que $A_0 = 1$ e A_1 é o número de places $P \in \mathbb{P}(K)$ de grau um.

Lema C.1.2. **(a)** *$A_n = 0$ se $\partial \nmid n$.*

(b) *Fixada uma classe $[C] \in \mathcal{C}_K$, temos*

$$|\{A \in [C] \ : \ A \geq 0\}| = \frac{q^{dim[C]} - 1}{q - 1}.$$

(c) *Para todo inteiro $n > 2g - 2$ com $\partial | n$,*

$$A_n = \frac{h}{q-1}(q^{n+1-g} - 1).$$

Demonstração. **(a)** Direto da definição de ∂.

(b) As condições $A \in [C]$ e $A \geq 0$ são equivalentes a

$$A = (x) + C \text{ para algum } x \in K \text{ com } (x) \geq -C,$$

isto é, $x \in \mathcal{L}(C)\backslash\{0\}$. Como $\mathcal{L}(C)$ é um espaço vetorial sobre $\mathbb{F}_q$, temos que $|\mathcal{L}(C)| = q^{dim[C]}$ e logo $|\mathcal{L}(C)\backslash\{0\}| = q^{dim[C]} - 1$. Além disso, dados dois elementos $x, y \in \mathcal{L}(C)\backslash\{0\}$, temos que $(x) + C = (y) + C \iff (x) = (y) \iff y = \alpha x$ para algum $0 \neq \alpha \in \mathbb{F}_q$. Daí temos o resultado.

(c) Existem $h = h_K$ classes de divisores de grau n, digamos $[C_1], \ldots, [C_h]$. Daí, por (b) e pelo Teorema de Riemann-Roch temos

$$|\{A \in [C_j] \ : \ A \geq 0\}| = \frac{q^{dimC_j} - 1}{q-1} = \frac{q^{n+1-g} - 1}{q-1}.$$

Todo divisor de grau n está em apenas uma das classes $[C_1], \ldots, [C_h]$, logo

$$A_n = \sum_{j=1}^{h} |\{A \in [C_j] \ : \ A \geq 0\}| = \frac{h}{q-1}(q^{n+1-g} - 1).$$

□

Definição C.1.3. *A série de potências*

$$Z(t) := Z_K(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]]$$

(onde A_n é o definido em C.3) é chamada a ***função Zeta*** *de $K/\mathbb{F}_q$.*

Proposição C.1.2. *A série de potências $Z(t) = \sum_{n=0}^{\infty} A_n t^n$ é convergente para $|t| < q^{-1}$. Mais precisamente, temos para $|t| < q^{-1}$:*

(a) *Se $K/\mathbb{F}_q$ tem gênero $g = 0$, então*

$$Z(t) = \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right).$$

(b) *Se $g \geq 1$, então $Z(t) = F(t) + G(t)$, onde*

$$F(t) = \frac{1}{q-1} \sum_{0 \leq deg[C] \leq 2g-2} q^{dim[C]} \cdot t^{deg[C]},$$

(onde $[C]$ percorre todas as classes de divisores $[C] \in \mathcal{C}_K$ tais que $0 \leq deg[C] \leq 2g-2$) e

$$G(t) = \frac{h}{q-1}\left(q^{1-g}(qt)^{2g-2+\partial}\frac{1}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right).$$

Demonstração. (a) Primeiro, mostraremos que um corpo de funções de gênero zero tem número de classe de divisor $h = 1$, isto é, todo divisor de A de grau zero é principal. De fato: Pelo Teorema de Riemann-Roch, como $0 > 2g - 2$, temos que $dimA = degA + 1 - g = 1$. Logo, existe um elemento $x \neq 0$ tal que $(x) \geq -A$, onde ambos os divisores têm grau zero. Daí, como $deg((x) + A) = 0$ e $(x) + A \geq 0$, então $(x) + A = 0$ e portanto $A = -(x) = (x^{-1})$ é principal. Assim, aplicando o lema C.1.2 temos

$$\begin{aligned}
\sum_{n=0}^{\infty} A_n t^n &= \sum_{n=0}^{\infty} A_{\partial n} t^{\partial n} = \sum_{n=0}^{\infty} \frac{1}{q-1}(q^{\partial n+1} - 1)t^{\partial n} \\
&= \frac{1}{q-1}\left(q\sum_{n=0}^{\infty}(qt)^{\partial n} - \sum_{n=0}^{\infty} t^{\partial n}\right) \\
&= \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right)
\end{aligned}$$

para $|qt| < 1$.

(b)

$$\sum_{n=0}^{\infty} A_n t^n = \sum_{deg[C]\geq 0} |\{A \in [C] \ : \ A \geq 0\}| \cdot t^{deg[C]}$$

$$= \sum_{deg[C]\geq 0} \frac{q^{dim[C]}-1}{q-1} \cdot t^{deg[C]} = \frac{1}{q-1} \sum_{0\leq deg[C]\leq 2g-2} q^{dim[C]} \cdot t^{deg[C]}$$

$$+\frac{1}{q-1} \sum_{deg[C]>2g-2} q^{deg[C]+1-g} \cdot t^{deg[C]} - \frac{1}{q-1} \sum_{deg[C]\geq 0} t^{deg[C]}$$

$= F(t) + G(t)$, onde

$$F(t) = \frac{1}{q-1} \sum_{0\leq deg[C]\leq 2g-2} q^{dim[C]} \cdot t^{deg[C]}$$

e

$$\begin{aligned}(q-1)G(t) &= \sum_{n=((2g-2)/\partial)+1}^{\infty} hq^{n\partial+1-g} \cdot t^{n\partial} - \sum_{n=0}^{\infty} ht^{n\partial} \\ &= hq^{1-g}(qt)^{2g-2+\partial}\frac{1}{1-(qt)^{\partial}} - h\frac{1}{1-t^{\partial}}.\end{aligned}$$

□

Corolário C.1.1. *$Z(t)$ pode ser estendida a uma função racional em $\mathbb{C}$ que tem um pólo simples em $t = 1$.*

Proposição C.1.3 (Produto de Euler). *Para $|t| < q^{-1}$, a função Zeta pode ser representada por um produtório absolutamente convergente*

$$Z(t) = \prod_{P\in\mathbb{P}(K)} (1 - t^{degP})^{-1}. \tag{C.4}$$

Em particular, $Z(t) \neq 0$ para $|t| < q^{-1}$.

No que segue, fixaremos um fecho algébrico $\bar{\mathbb{F}}_q$ de $\mathbb{F}_q$ e consideramos a extensão do corpo das constantes $\bar{F} = F\bar{\mathbb{F}}_q$ de $K/\mathbb{F}_q$. Para todo $r \geq 1$ existe uma única extensão $\mathbb{F}_{q^r}/\mathbb{F}_q$ de grau r com $\mathbb{F}_{q^r} \subseteq \bar{\mathbb{F}}_q$, e definimos

$$K_r := K\mathbb{F}_{q^r} \subseteq \bar{K}.$$

Lema C.1.3. **(a)** *K_r/K é uma extensão cíclica de grau r (isto é, K_r/K é Galois com um grupo de Galois cíclico de ordem r). O grupo de Galois $Gal(K_r/K)$ é gerado pelo automorfismo de Forbenius σ que atua em $\mathbb{F}_{q^r}$ por $\sigma(\alpha) = \alpha^q$.*

(b) *$\mathbb{F}_{q^r}$ é o corpo das constantes de K_r.*

(c) *$K_r/\mathbb{F}_{q^r}$ tem o mesmo gênero que $K/\mathbb{F}_q$.*

(d) *Seja $P \in \mathbb{P}(K)$ um place de grau m. Então $Con_{K_r/K}(P) = P_1 + \ldots + P_d$ com $d := mdc(m, r)$ places dois a dois distintos $P_i \in \mathbb{P}(K_r)$ e $degP_i = m/d$.*

Demonstração. (a) É sabido que $\mathbb{F}_{q^r}/\mathbb{F}_q$ é cíclico de grau r e seu grupo de Galois é gerado pela aplicação de Forbenius $\beta \mapsto \beta^q$. Como $\mathbb{F}_q$ é perfeito, existe $\alpha \in \mathbb{F}_{q^r}$ tal que $\mathbb{F}_{q^r} = \mathbb{F}_q(\alpha)$. Daí temos que $K_r = K\mathbb{F}_q(\alpha) = K(\alpha)$. Pelo lema B.6.1, $[K_r : K] = [K(\alpha) : K] = [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = r$; além disso, no mesmo lema vimos que o polinômio minimal de α sobre $\mathbb{F}_q$ é o mesmo de α sobre K. Logo o automorfismo $\alpha \mapsto \alpha^q$ gera $Gal(K_r/K)$.

(b) e (c) saem da proposição B.6.1 e do teorema B.6.1.

(d) P é não-ramificado em K_r/K conforme teorema B.6.1. Considere um place $P' \in \mathbb{P}(K_r)$ pat que $P'|P$. Pelo teorema B.6.1 (g), o corpo resídual de P' é o compositum de $\mathbb{F}_{q^r}$ com o corpo residual K_P de P. Seja $l = mmc(m, r)$. Como $degP = m$, temos que $[K_P : \mathbb{F}_q] = m$; logo $K_P = \mathbb{F}_{q^m}$ e o compositum citado acima é

$$\mathbb{F}_{q^m}\mathbb{F}_{q^r} = \mathbb{F}_{q^l}.$$

Portanto

$$degP' = [\mathbb{F}_{q^l} : \mathbb{F}_{q^r}] = m/d.$$

Como $deg(Con_{K_r/K}(P)) = degP = m$ (pelo teorema B.6.1 (c)), concluímos que $Con_{K_r/K}(P) = P_1 + \ldots + P_r$ com places P_i de grau m/d.

□

Na próxima proposição precisaremos da seguinte identidade polinomial: se $m \geq 1$ e $r \geq 1$ são inteiros e $d = mdc(m, r)$, então

$$(X^{r/d} - 1)^d = \prod_{\zeta^r=1} (X - \zeta^m) \tag{C.5}$$

onde ζ percorre todas as raízes r-ésimas da unidade em $\mathbb{C}$. Substituindo $X = t^{-m}$ em C.5 e multiplicando por t^{mr} obtemos

$$(1 - t^{mr/d})^d = \prod_{\zeta^r=1} (1 - (\zeta t)^m). \tag{C.6}$$

Proposição C.1.4. *Seja $Z(t)$ (resp. $Z_r(t)$) a função Zeta de K (resp. de K_r). Então*

$$Z_r(t^r) = \prod_{\zeta^r=1} (\zeta t) \tag{C.7}$$

para todo $t \in \mathbb{C}$ (ζ percorrendo as raízes r-ésimas da unidade).

Demonstração. É suficiente provar C.7 para $|t| < q^{-1}$. Nesta região, a representaç ão como produto de Euler nos dá

$$Z_r(t^r) = \prod_{P \in \mathbb{P}(K)} \prod_{P'|P} (1 - t^{r \cdot degP'})^{-1} \tag{C.8}$$

Para um place $P \in \mathbb{P}(K)$ fixado, chame $m = degP$ e $d = mdc(r, m)$; daí

$$\prod_{P'|P} (1 - t^{r \cdot degP'})^{-1} = (1 - t^{rm/d})^d$$

$$= \prod_{\zeta^r=1} (1 - (\zeta t)^m) = \prod_{\zeta^r=1} (1 - (\zeta t)^{degP}),$$

pelo ítem (d) do lema C.1.3 e por C.6. Assim, por C.8 obtemos

$$Z_r(t^r) = \prod_{\zeta^r=1} \prod_{P\in\mathbb{P}(K)} (1-(\zeta t)^{degP})^{-1} = \prod_{\zeta^r=1} Z(\zeta t).$$

□

Corolário C.1.2 (F.K. Schmidt). $\partial = 1$.

Demonstração. Para $\zeta^\partial = 1$, temos

$$Z(\zeta t) = \prod_{P\in\mathbb{P}(K)} (1-(\zeta t)^{degP})^{-1} = \prod_{P\in\mathbb{P}(K)} (1-t^{degP})^{-1} = Z(t),$$

uma vez que ∂ divide o grau de P para todo $P \in \mathbb{P}(K)$. Logo $Z_\partial(t^\partial) = Z(t)^\partial$ pela proposição C.1.4. A função racional $Z_\partial(t^\partial)$ tem um pólo simples em $t = 1$ pelo corolário C.1.1, e $Z(t)^\partial$ tem um pólo de ordem ∂ em $t = 1$. Portanto $\partial = 1$. □

Corolário C.1.3. (a) *Todo corpo de funções $K/\mathbb{F}_q$ de gênero $g = 0$ é racional, e sua função Zeta é*

$$Z(t) = \frac{1}{(1-t)(1-qt)}.$$

(b) *Se $K/\mathbb{F}_q$ tem gênero $g \geq 1$, sua função Zeta pode ser escrita da forma $Z(t) = F(t) + G(t)$, onde*

$$F(t) = \frac{1}{q-1} \sum_{0\leq deg[C]\leq 2g-2} q^{dim[C]} \cdot t^{deg[C]}$$

e

$$G(t) = \frac{h}{q-1}\left(q^g t^{2g-1}\frac{1}{1-qt} - \frac{1}{1-t}\right).$$

Demonstração. Um corpo de funções de gênero 0 que possui um divisor de grau 1 é racional (proposição 2.5.2). O restante segue imediatamente de proposição C.1.2 e $\partial = 1$. □

Não demonstraremos a próxima proposição; sua prova pode ser encontrada em [17] (página 165).

Proposição C.1.5 (Equação Funcional da Função Zeta). *A função Zeta de $K/\mathbb{F}_q$ satisfaz a seguinte equação funcional:*

$$Z(t) = q^{g-1}t^{2g-2}Z\left(\frac{1}{qt}\right).$$

Definição C.1.4. *O polinômio*

$$L(t) := L_K(t) := (1-t)(1-qt)Z(t)$$

é chamado ***L-polinômio*** *de $K/\mathbb{F}_q$.*

Pelo Corolário C.1.3 é óbvio que $L(t)$ é um polinômio de grau $\leq 2g$. Observe também que $L(t)$ contém todas as informações sobre os números A_n. $n \geq 0$, pois

$$L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n. \tag{C.9}$$

Teorema C.1.1. (a) *$L(t) \in \mathbb{Z}[t]$ e $degL(t) = 2g$.*

(b) *(Equação funcional) $L(t) = q^g t^{2g} L(1/qt)$*

(c) *$L(1) = h$, o número de classe de divisor de $K/\mathbb{F}_q$.*

(d) *Escreva $L(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g}$. Temos:*

1. *$a_0 = 1$ e $a_{2g} = q^g$.*
2. *$a_{2g-i} = q^{g-i} a_{2g}$ para $0 \leq i \leq g$.*
3. *$a_1 = N - (q+1)$, onde N é o número de places $P \in \mathbb{P}(K)$ de grau um.*

(e) *$L(t)$ fatora-se em $\mathbb{C}$ na forma*

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t). \tag{C.10}$$

Os números complexos $\alpha_1, \ldots, \alpha_{2g}$ são inteiros algébricos, e eles podem ser arranjados de tal forma que $\alpha_i \alpha_{g+i} = q$ para todo $i = 1, \ldots, g$.

(f) *Se $L_r(t) := (1-t)(1-qt)Z_r(t)$ denota o L-polinômio da extensão do corpo das constantes $K_r = K\mathbb{F}_{q^r}$, então*

$$L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t),$$

onde os α_i são os dados em C.10.

Demonstração. Todas as afirmações são triviais para $g = 0$. Assumiremos então $g \geq 1$.

(a) Já sabemos que $L(t)$ é um polinômio de grau $\leq 2g$. No ítem (d) veremos que seu coeficiente dominante é q^g, donde $degL(t) = 2g$. A afirmação $L(t) \in \mathbb{Z}[t]$ segue de C.9 comparando os coeficientes.

(b) Direto da proposição C.1.5.

(c) Com a notação co corolário C.1.3, temos

$$L(t) = (1-t)(1-qt)F(t) + \frac{h}{q-1}(q^g t^{2g-1}(1-t) - (1-qt)).$$

Logo $L(1) = h$.

(d) Escreva $L(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g}$. Da equação funcional (b) temos

$$L(t) = q^g t^{2g} L(\frac{1}{qt}) = \frac{a_{2g}}{q^g} + \frac{a_{2g-1}}{q^{g-1}} + \ldots + q^g a_0 t^{2g}.$$

Portanto $a_{2g-i} = q^{g-i} a_i$ para $i = 1, \ldots, g$ e a afirmação *2* está provada. Comparando os coeficientes de t^0 e t^1 em C.9 temos que $a_0 = A_0$ e $a_1 = A_1 - (q+1)A_0$. Como $A_0 = 1$ e $A_1 = N$, temos que $a_0 = 1$ e $a_1 = N - (q+1)$. Fimalmente, $a_{2g} = q^g a_0 = q^g$ por *2*.

(e) Considere o polinômio recíproco

$$L^{\perp}(t) := t^{2g}L(\frac{1}{t}) = a_0t^{2g} + a_1t^{2g-1} + \ldots + a_{2g} = t^{2g} + a_1t^{2g-1} + \ldots + q^g. \tag{C.11}$$

$L^{\perp}$ é um polinômio mônico com coeficientes em $\mathbb{Z}$, donde suas raízes $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$ são inteiros algébricos, e $L^{\perp}(t) = \prod_{i=1}^{2g}(t - \alpha_i)$. Logo

$$L(t) = t^{2g}L^{\perp}(\frac{1}{t}) = \prod_{i=1}^{2g}(1 - \alpha_i t).$$

Observe que as raízes α_i de $L^{\perp}(t)$ são as inversas das raízes de $L(t)$, pois $L(\alpha_i^{-1}) = 0$. Da equação funcional (b) temos que $L^{\perp}(\alpha) = 0$ se, e somente se, $L^{\perp}(q/\alpha) = 0$. Daí arranjamos as raízes de $L^{\perp}(t)$ como

$$\alpha_1, \frac{q}{\alpha_1}, \ldots, \alpha_k, \frac{q}{\alpha_k}, q^{1/2}, \ldots, q^{1/2}, -q^{1/2}, \ldots, -q^{1/2},$$

onde $q^{1/2}$ ocorre m vezes e $-q^{1/2}$ ocorre n vezes. Por C.11,

$$\alpha_1 \cdot \frac{q}{\alpha_1} \cdot \ldots \cdot \alpha_k \cdot \frac{q}{\alpha_k} \cdot (q^{1/2})^m \cdot (-q^{1/2})^n = q^g.$$

Portanto n é par. Como $m + n + 2k = 2g$, m também é par, e assim podemos rearranjar $\alpha_1, \ldots, \alpha_{2g}$ tal que $\alpha_i\alpha_{g+i} = q$ para todo $i = 1, \ldots, g$.

(f) Usando a proposição C.1.4 obtemos

$$L_r(t^r) = (1 - t^r)(1 - q^rt^r)Z_r(t^r) = (1 - t^r)(1 - q^rt^r)\prod_{\zeta^r=1} Z(\zeta t)$$

$$= (1 - t^r)(1 - q^rt^r)\prod_{\zeta^r=1}\frac{L(\zeta t)}{(1 - \zeta t)(1 - q\zeta t)} = \prod_{\zeta^r=1} L(\zeta t)$$

$$= \prod_{i=1}^{2g}\prod_{\zeta^r=1}(1 - \alpha_i\zeta t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t^r).$$

Portanto $L_r(t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t)$.

□

O teorema acima mostra que o número

$$N(F) := N = |\{P \in \mathbb{P}(K) \ : \ degP = 1\}| \tag{C.12}$$

pode ser facilmente calculado se o L-polinômio $L(t)$ de $K/\mathbb{F}_q$ for conhecido. Mais ainda, consideramos para $r \geq 1$ o número

$$N_r := N(F_r) = |\{P \in \mathbb{P}(F_r) \ : \ degP = 1\}|, \tag{C.13}$$

onde $K_r = K\mathbb{F}_{q^r}$ é a extensão do corpo das constantes de $K/\mathbb{F}_q$ de grau r. Segue agora um resultado de papel essencial para o próximo capítulo.

Corolário C.1.4. *Para todo $r \geq 1$,*

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r,$$

onde $\alpha_1, \ldots, \alpha_2 g \in \mathbb{C}$ são as recíprocas das raízes de $L(t)$. Em Particular, como $N_1 = N(F)$, temos

$$N(F) = q + 1 - \sum_{i=1}^{2g} \alpha_i.$$

Demonstração. Pelo ítem (d) do teorema C.1.1, $N_r - (q+1)$ é o coeficiente de t no L-polinômio $L_r(t)$. Por outro lado, como $L_r(t) = \prod_{i=1}^{2g}(1 - \alpha_i^r t)$, temos que esse coeficiente é $-\sum_{i=1}^{2g} \alpha_i^r$. □

C.2 O Teorema de Hasse-Weil

Nesta seção demonstraremos o resultado mais importante de capítulo, que é o seguinte

Teorema C.2.1 (Hasse-Weil). *As recíprocas das raízes de $L_K(t)$ satisfazem*

$$|\alpha_i| = q^{1/2} para\ i = 1, \ldots, 2g.$$

Antes de prová-lo, vejamos alguns resultados que nos guiarão a uma estratégia para tal prova.

Lema C.2.1. *Seja $m \geq 1$. Então o teorema de Hasse-Weil é válido para $K/\mathbb{F}_q$ se, e somente se, ele é válido para a extensão do corpo das constantes $K_m/\mathbb{F}_{q^m}$.*

Demonstração. As recíprocas das raízes de $L_K(t)$ são $\alpha_1, \ldots, \alpha_2 g$. Pelo teorema C.1.1 (f), as recíprocas das raízes de $L_m(t)$ são $\alpha_1^m, \ldots, \alpha_2 g^m$. Assim, o resultado segue imediatamente, pois $|\alpha_i| = q^{1/2} \iff |\alpha_i^m| = (q^m)^{1/2}$. □

Lema C.2.2. *Suponha que existe $c \in \mathbb{R}$ tal que para todo $r \geq 1$,*

$$|N_r - (q^r + 1)| \leq c q^{r/2}. \tag{C.14}$$

Então o Teorema de Hasse-Weil vale para $K/\mathbb{F}_q$.

Demonstração. Pelo corolário C.1.4, temos $N_r - (q^r + 1) = -\sum_{i=1}^{2g} \alpha_i^r$, logo C.14 nos fornece que

$$\left| \sum_{i=1}^{2g} \alpha_i^r \right| \leq c q^{1/2} \tag{C.15}$$

para todo $r \geq 1$. Considere a função meromorfa

$$H(t) := \sum_{i=1}^{2g} \frac{\alpha_i t}{1 - \alpha_i t}. \tag{C.16}$$

Seja $\delta := min\{|\alpha_i^{-1}| \ : \ 1 \leq i \leq 2g\}$. O raio de convergência da expansão em série de potências de $H(t)$ em torno de 0 é precisamente δ (pois $\alpha_1^{-1}, \ldots, \alpha_2 g^{-1}$ são as únicas singularidades de $H(t)$). Por outro lado, temos para $|t| < \delta$ que

$$H(t) = \sum_{i=1}^{2g} \sum_{r=1}^{\infty} (\alpha_i t)^r = \sum_{r=1}^{\infty} \left(\sum_{i=1}^{2g} \alpha_i^r \right) t^r. \tag{C.17}$$

Suponha $|t| < q^{-1/2}$. Daí $\left|q^{1/2}t\right| < 1 \Longrightarrow \sum_{r=i}^{\infty} q^{r/2}t^r < +\infty \Longrightarrow \sum_{r=i}^{\infty}(cq^{r/2})t^r < +\infty$. Logo por C.15 temos que C.17 converge quando $|t| < q^{-1/2}$. Portanto $q^{1/2} \leq \delta$. Isso implica que $q^{1/2} \geq |\alpha_i|$ para todo $i = 1, \ldots, 2g$. Como $\prod_{i=1}^{2g} \alpha_i = q^g$ (teorema C.1.1 (e)), temos que $|\alpha_i| = q^{1/2}$. □

Observe que a desigualdade C.14 é equivalente a uma cota superior e uma cota inferior para N_r: existem constantes $c_1 > 0$ e $c_2 > 0$ tais que

$$N_r \leq q^r + 1 + c_1 q^{r/2} \tag{C.18}$$

e

$$N_r \geq q^r + 1 - c_2 q^{r/2} \tag{C.19}$$

para todo $r \geq 1$. Pelo Lema C.2.1, o teorema de Hasse-Weil vale para $K/\mathbb{F}_q$ se ele vale para alguma extensão do corpo das constantes de K. Sendo assim, é suficiente provar C.18 e C.19 sob hipóteses adicionais que podem serem feitas em uma extensão finita do corpo das constantes apropriada.

Proposição C.2.1. *Suponha que $K/\mathbb{F}_q$ satisfaz as seguintes hipóteses:*

1. *q é um quadrado;*
2. *$q > (g+1)^4$.*

Então o número $N = N(F)$ de places de grau 1 de $K/\mathbb{F}_q$ pode ser estimado por

$$N < (q+1) + (2g+1)q^{1/2}.$$

Demonstração. Podemos assumir que existe um place $Q \in \mathbb{P}(K)$ de grau 1 (caso contrário, teríamos $N = 0$ e a proposição seria trivial). Sejam

$$q_0 := q^{1/2}, \quad m := q_0 - 1 \quad e \quad n := 2g + q_0.$$

Daí temos que

$$r := q - 1 + (2g+1)q^{1/2} = m + nq_0. \tag{C.20}$$

Dado um place P, um inteiro positivo i é chamado número pólo de P se existir um elemento $x \in K$ com o divisor pólo $(x)_\infty = iP$ (definição 2.5.7). Seja $T := \{i \ : \ 0 \leq i \leq m$, e i é um número pólo de $Q\}$. Para cada $i \in T$, escolha um elemento $u_i \in F$ com divisor pólo iQ (ou seja, $(u_i)_\infty = iQ$). Daí o conjunto $\{u_i \ : \ i \in T\}$ é uma base de $\mathcal{L}(mQ)$. De fato: Primeiro, temos que $\mathcal{L}(Q) = \mathcal{L}(0) = \mathbb{F}_q$, pois se por absurdo existisse $x \in (K \backslash \mathbb{F}_q) \cap \mathcal{L}(Q)$, teríamos que $(x)_\infty = Q$, um absurdo, pois 1 é lacuna (Teorema 2.5.6). Considere a seqüência

$$\mathbb{F}_q = \mathcal{L}(Q) \subseteq \mathcal{L}(2Q) \subseteq \ldots \subseteq \mathcal{L}(mQ).$$

É fácil ver que i é lacuna $\Longleftrightarrow \mathcal{L}((i-1)Q) = \mathcal{L}(iQ)$ e i é número pólo $\Longrightarrow dim(iQ) = dim((i-1)Q) + 1$. Logo, como $dimQ = 1$ e em cada passo da seqüência acima subimos a dimensão em 0 (se i é lacuna) ou 1 (se i é número pólo), temos que $dim(mQ) = |\{u_i \ : \ i \in T\}|$. Pela desigualdade triângular estrita temos que $\{u_i \ : \ i \in T\}$ é lineramente independente, donde temos o resultado.

Agora considere o espaço

$$\mathcal{L} := \mathcal{L}(mQ) \cdot \mathcal{L}(nQ)^{q_0} \subseteq \mathcal{L}(rQ)$$

Por definição, $\mathcal{L}$ consiste de todas as somas finitas $\sum x_\nu y_\nu^{q_0}$ com $x_\nu \in \mathcal{L}(mQ)$ e $y_\nu \in \mathcal{L}(nQ)$; óbviamente $\mathcal{L}$ é um $\mathbb{F}_q$-espaço vetorial e $\mathcal{L} \subseteq \mathcal{L}(rQ)$ por C.20.

Queremos construir um elemento $0 \neq x \in \mathcal{L}$ tal que

$$x(P) = 0 \quad \forall \quad P \in \mathbb{P}(K) \quad com \quad degP = 1 \quad e \quad P \neq Q. \tag{C.21}$$

Suponha que encontramos tal elemento x. Então todos os places de grau 1 (exceto Q) são zeros de x e assim, o divisor zero $(x)_0$ tem grau

$$deg(x)_0 \geq N - 1.$$

Como $\mathcal{L} \subseteq \mathcal{L}(rQ)$, temos que

$$deg(x)_0 = deg(x)_\infty \leq r = q - 1 + (2g+1)q^{1/2}.$$

Combinando essas duas desigualdades obtemos $N \leq q + (2g+1)q^{1/2}$, o que prova a proposição.
Afirmação 1: Todo $y \in \mathcal{L}$ pode ser escrito de maneira única na forma

$$y = \sum_{i \in T} u_i z_i^{q_0} \quad com \quad z_i \in \mathcal{L}(nQ) \tag{C.22}$$

(onde $\{u_i \ : \ i \in T\}$ é a base de $\mathcal{L}(mQ)$ encontrada acima).
De fato: Dado $y \in \mathcal{L}$, temos que $y = \sum x_\nu y_\nu^{q_0}$, com $x_\nu \in \mathcal{L}(mQ)$ e $y_\nu \in \mathcal{L}(nQ)$. Sendo assim, temos que $x_\nu = \sum_{i \in T} \alpha_i u_i$, com $\alpha_i \in \mathbb{F}_q = \mathbb{F}_{q_0^2}$ $\forall i \in T$. Substituindo e reagrupando, obtemos

$$y = \sum_{i \in T} u_i \left(\sum_\nu \alpha_{i_\nu} y_\nu^{q_o} \right).$$

Como

$$\begin{array}{rcl} \sigma : \mathbb{F}_{q_o^2} & \longrightarrow & \mathbb{F}_{q_o^2} \\ \beta & \longmapsto & \beta^{q_0} \end{array}$$

é um automorfismo em $\mathbb{F}_q$ (automorfismo de Forbenius), $\alpha'_{i_\nu} \in \mathbb{F}_q$ tais que $\alpha_{i_\nu} = (\alpha'_{i_\nu})^{q_0}$. Como q_0 é uma potência da característica de $\mathbb{F}_q$, temos que para todo $i \in T$, $\sum_\nu \alpha_{i_\nu} y_\nu^{q_0} = z_i^{q_0}$ para algum $z_i \in \mathcal{L}(nQ)$. Logo, y é da forma sugerida em C.22. Resta então apenas provarmos a unicidade.

Suponha por absurdo que existe uma equação

$$\sum_{i \in T} u_i x_i^{q_0} = 0 \tag{C.23}$$

com $x_i \in \mathcal{L}(nQ)$ não todos nulos. Para cada $i \in T$, com $x_i \neq 0$, temos

$$v_Q(u_i x_i^{q_0}) \equiv v_Q(u_i) \equiv -i (mod\ q_0).$$

Como $m = q_0 - 1$, os números $i \in T$ são dois a dois distintos módulo q_0. Daí, da desigualdade triangular estrita temos

$$v_Q\left(\sum_{i \in T} u_i x_i^{q_0} \right) = min\{v_Q(u_i x_i^{q_0}) \ : \ i \in T\} \neq \infty,$$

contradizendo C.23. Logo a afirmação 1 está provada.

Considere agora a aplicação $\lambda : \mathcal{L} \longrightarrow \mathcal{L}((q_0m+n)Q)$ dada por

$$\lambda\left(\sum_{i\in T} u_i z_i^{q_0}\right) := \sum_{i\in T} u_i^{q_0} z_i,$$

com $z_i \in \mathcal{L}(nQ)$. Pela afirmação 1, λ está bem definida; observe que λ não é $\mathbb{F}_q$-linear, mas é um homomorfismo de grupo aditivo.

Afirmação 2: $ker(\lambda) \neq \{0\}$.
De fato: Como λ é um homomorfismo de $\mathcal{L}$ em $\mathcal{L}((q_0m+n)Q)$ e ambos são $\mathbb{F}_q$-espaços vetoriais de dimensão finita (logo ambos são conjuntos finitos), basta mostrar que

$$dim\mathcal{L} > \mathcal{L}((q_0m+n)Q). \tag{C.24}$$

Pela afirmação 1 e pelo teorema de Riemann-Roch, temos

$$dim\mathcal{L} = dim(mQ)\cdot dim(nQ) \geq (m+1-g)(n+1-g).$$

Por outro lado, como

$$q_0m+n = q_0(q_0-1)+(2g+q_0) = 2g+q,$$

obtemos

$$dim\mathcal{L}((q_0m+n)Q) = (2g+q)+1-g = g+q+1.$$

Logo, C.24 é verdadeiro se conseguirmos provar

$$(m+1-g)(n+1-g) > g+q+1. \tag{C.25}$$

Considere então as seguintes equivalências

$$\begin{aligned}
&(m+1-g)(n+1-g) > g+q+1\\
&\Longleftrightarrow (q_0-g)(2g+q_0+1-g) > g+q+1\\
&\Longrightarrow q-g^2+q_0-g > g+q+1\\
&\Longrightarrow q_o > g^2+2g+1 = (g+1)^2\\
&\Longrightarrow q > (g+1)^4.
\end{aligned}$$

Como a última desigualdade é assumida por hipótese, temos o resultado da afirmação 2.

Afirmação 3: Seja $0 \neq x \in ker(\lambda) \subseteq \mathcal{L}$ e $P \neq Q$ um place de grau 1. Então $x(P) = 0$.
De fato: Note que $y(P) \neq \infty$ para todo $y \in \mathcal{L}$, uma vez que Q é o único pólo de y. Além disso, como $degP = 1$, temos que $\mathbb{F}_q$ é o corpo residual de P, donde $y(P)^q = y(P)$. Agora, considere um elemento $x \in \mathcal{L}$ com $\lambda(x) = 0$. escrevendo $x = \sum_{i\in T} u_i z_i^{q_0}$, obtemos

$$\begin{aligned}
x(P)^{q_0} &= \left(\sum_{i\in T} u_i(P)\cdot z_i(P)^{q_0}\right)^{q_0}\\
&= \sum_{i\in T} u_i^{q_0}(P)\cdot z_i(P)^q\\
&= \left(\sum_{i\in T} u_i^{q_0} z_i\right)(P) = \lambda(x)(P) = 0.
\end{aligned}$$

Assim, a afirmação 3 está provada e, portanto, a proposição está provada. □

A proposição anterior nos fornece uma cota superior C.18 aos números N_r (se for tomada uma extensão do corpo das constantes apropriada). A seguir, queremos obter uma cota inferior. Começaremos com um lema de teoria dos grupos.

Lema C.2.3. *Considere um grupo G' que é o produto direto*

$$G' = \langle\sigma\rangle \times G \tag{C.26}$$

de um subgrupo cíclico $\langle\sigma\rangle$ e um subgrupo $G \subseteq G'$ tal que $|G| = m$, $ord(\sigma) = n$ e m divide n. Suponha que $H \subseteq G'$ é um subgrupo de G' com

$$|H| = ne \quad e \quad |H \cap G| = e. \tag{C.27}$$

Então existem exatamente e subgrupos $U \subseteq H$ com as seguintes propriedades:

$$U \text{ é cíclico de ordem } n, \text{ e } U \cap G = \{1\}. \tag{C.28}$$

Demonstração. Para $\tau \in G$, considere o grupo cíclico $\langle\sigma\tau\rangle \subseteq G'$. Como $\sigma\tau = \tau\sigma$ (por C.26), $ord(\sigma) = n$ e $ord(\tau)|m$, concluímos que $ord(\sigma\tau) = n$. Além disso, $\langle\sigma\tau\rangle \cap G = \{1\}$ e $\langle\sigma\tau\rangle \neq \langle\sigma\tau'\rangle$ para $\tau \neq \tau'$ (tudo isso segue de C.26, uma vez que os elementos $\lambda \in G'$ têm uma única representação $\lambda = \sigma^i\delta$, com $0 \leq i \leq n$ e $\delta \in G$). Logo, encontramos $m = |G|$ subgrupos distintos $U \subseteq G'$ com as propriedades C.28.

Por C.26, temos também que $G \subseteq G'$ é um subgrupo normal; logo $H/H \cap G \simeq HG/G$. Por C.27, isso implica que $HG = G'$ e $H/H \cap G \simeq G'/G$ é cíclico de grau n. Tome um elemento $\lambda_0 \in H$ tal que $ord(\lambda_0(H \cap G)) = n$, isto é, $\langle\lambda_0(H \cap G)\rangle = H/H \cap G$. Escreva $\lambda_0 = \sigma^a\tau'$, com $\tau' \in G$ e $a \in \mathbb{Z}$. Temos que $mdc(a, n) = 1$ (pois caso contrário, existiria um inteiro $1 \leq d \leq n$ tal que $n|ad$ e logo $\sigma^{ad} = 1 \Longrightarrow \lambda_0^d = \tau'^d \in H \cap G$, donde teríamos que a ordem de λ_0 módulo $H \cap G$ seria menor que n). Assim, existem $t, r \in \mathbb{Z}$ tais que $ta = 1 + rn$.Daí

$$\lambda := \lambda_0^t = \sigma^{ta}\tau'^t = \sigma^{1+rn}(\tau')^t = \sigma\tau'^t.$$

Assim, obtivemos $\lambda = \sigma\tau_0$, com $\tau_0 := \tau'^t \in G$, onde λ também tem ordem n módulo $H \cap G$. Seja $H \cap G = \{\psi_1, \ldots, \psi_e\}$. Definimos

$$U^{(j)} := \langle\sigma\tau_0\psi_j\rangle, \quad j = 1, \ldots, e.$$

Como vimos no começo dessa demosntração, os subgrupos $U^{(j)} \subseteq H$ são cíclicos de ordem n, são distintos dois a dois e $U^{(j)} \cap G = \{1\}$.

Resta apenas mostrar que H não possui nenhum outro subgrupo cíclico U de ordem n com $U \cap G = \{1\}$. De fato, seja $U \subseteq H$ um subgrupo satisfazendo C.28. Como fizemos acima, podemos encontrar um gerador de U da forma $\sigma\tau_1$ com $\tau_1 \in G$. Como $\sigma\tau_1 \in H$ e $\sigma\tau_0 \in H$, temos

$$\tau_0^{-1}\tau_1 = (\sigma\tau_0)^{-1}(\sigma\tau_1) \in H \cap G = \{\psi_1, \ldots, \psi_e\}.$$

Logo $\tau_1 = \tau_0\psi_j$ para algum j, e $U = \langle\sigma\tau_1\rangle = \langle\sigma\tau_0\psi_j\rangle = U^{(j)}$. □

A próxima proposição é o passo essencial para a prova de uma cota inferior para N_r. Consideremos a seguinte situação: E/L é uma extensão de Galois de corpos de funções de grau $[E : L] = m$, e é assumido que $\mathbb{F}_q$ é o corpo das constantes de E e de L. Tome um inteiro $n > 0$ com $m|n$ e seja $E' := E\mathbb{F}_{q^n}$ (respectivamente $L' := L\mathbb{F}_{q^n}$) a correspondente extensão do corpo das constantes de grau n. Seja $G := Gal(E'/L') \simeq Gal(E/L)$. Sabemos que $Gal(E'/E) = \langle\sigma\rangle$, onde σ é o

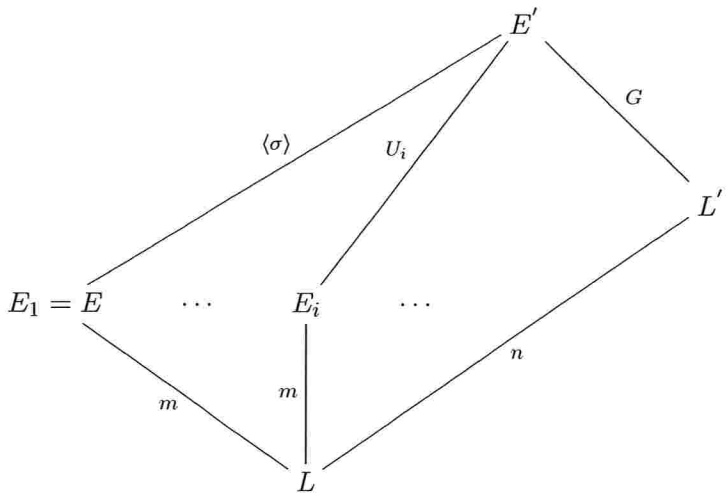
automorfismo de Forbenius de E'/E (isto é, $\sigma(z) = z$ para $z \in E$ e $\sigma(\alpha) = \alpha^q$ para $\alpha \in \mathbb{F}_{q^n}$). Temos que E'/L é Galois e , se $G' = Gal(E'/L)$, temos que $G' = \langle\sigma\rangle \times G$. De fato: primeiro, $[E' : L] = mn \Longrightarrow \left|G'\right| = mn$. Além disso, $\sigma \in G'$ e $G \subseteq G'$. É fácil provar que $\sigma\tau = \tau\sigma$ para todo $\tau \in G$. Também, $EL' = EL\mathbb{F}_{q^n} = E\mathbb{F}_{q^n} = E'$. Daí, pela teoria de Galois,

$$\{1\} = Gal(E'/E') = Gal(E'/EL') = Gal(E'/E) \cap Gal(E'/L') = \langle\sigma\rangle \cap G.$$

Logo $|\langle\sigma\rangle \times G| = nm = \left|G'\right|$. Portanto $G' = \langle\sigma\rangle \times G$.

Assim, pelo lema anterior, G' possui exatamente m subgrupos cíclicos $U \subseteq G'$ com $|U| = n$ e $U \cap G = \{1\}$, digamos $U_1, \ldots, U_m$. Podemos assumir $U_1 = \langle\sigma\rangle$.

Seja E_i o corpo fixado por U_i $(i = 1, \ldots, m)$. Então $E_1 = E$ e temos o seguinte diagrama:



Denote por $g(E_i)$ o gênero de E_i, e por $N(E_i)$ (respectivamente $N(L)$) o número de places de grau um de E_i (respectivamente L).

Proposição C.2.2. *Sob as hipóteses acima, temos:*

(a) $\mathbb{F}_q$ *é o corpo das constantes de* E_i, *para* $1 \leq i \leq m$.

(b) $E' = E_i\mathbb{F}_{q^n}$ *e* $g(E_i) = g(E)$ *para* $1 \leq i \leq m$.

(c) $m \cdot N(L) = \sum_{i=1}^{m} N(E_i)$.

Demonstração. (a), (b) Note que $U_i \cap G = \{1\}$. Daí, pela teoria de Galois, E' é o compositum de E_i e L', logo $E' = E_iL' = E_iL\mathbb{F}_{q^n} = E_i\mathbb{F}_{q^n}$ é a extensão do corpo das constantes de E_i com $\mathbb{F}_{q^n}$. Como $[E' : E_i] = |U_i| = n$, temos que $\mathbb{F}_q$ é o corpo das constantes de E_i. Como o gênero é invariante sob extensão do corpo das constantes, temos que $g(E_i) = g(E') = g(E)$, para $i = 1, \ldots, m$.

(c) Considere os conjuntos $X := \{P \in \mathbb{P}(L) \ : \ degP = 1\}$ e para $i = 1, \ldots, m$, $X_i := \{Q \in \mathbb{P}(E_i) \ : \ degQ = 1\}$. Temos que provar o seguinte:

$$\left|\bigcup_{i=1}^{m} X_i\right| = m \cdot |X|. \tag{C.29}$$

Seja $P \in X$. Escolha um place $P' \in \mathbb{P}(E')$ tal que $P'|P$, e chame $P_1 := P' \cap E$. Como E/L é Galois, temos que o grau relativo $f(P_1|P)$ divide m. Portanto $f(P_1|P)$ divide n e o corpo residual de P' é $\mathbb{F}_{q^n}$, pelo teorema B.6.1(g). Isso significa que o grau relativo de $P'|P$ é $f(P'|P) = n$. Denote por $e := e(P'|P)$ o índice de ramificação de P em E'/L e por r o número de places em $\mathbb{P}(E')$ que são extensões de P (como E'/L é Galois, e depende apenas de P.). Obtemos

$$m \cdot n = [E' : L] = e(P'|P) \cdot f(P'|P) = e \cdot n \cdot r.$$

Portanto $m = e \cdot r$, e C.29 se reduz às seguintes afirmações:

Afirmação 1: Para todo $Q \in X_i$ com $Q|P$, existe exatamente um place $Q' \in \mathbb{P}(E')$ que estende Q.

Afirmação 2: Para todo $Q' \in \mathbb{P}(E')$ com $Q'|P$, existem exatamente e places distintos $Q \in \cup_{i=1}^{m} X_i$ tais que $Q'|Q$.

Prova da afirmação 1. Se $Q' \in \mathbb{P}(E')$ é tal que $Q'|Q \in X_i$ e $Q|P$, então

$$f(Q'|Q) = f(Q'|Q) \cdot f(Q|P) = f(Q'|P) = n.$$

Logo $f(Q'|Q) = [E' : E_i] = n$, o que significa que Q' é a única extensão de Q em E'/E_i.

Prova da afirmação 2. Tome um place $Q' \in \mathbb{P}(E')$ com $Q'|P$. Seja $H \subseteq Gal(E'/L)$ o grupo de composição de Q' sobre P, $Z \subseteq E'$ o corpo fixado por H e $P_Z := Q' \cap Z$. Então

$$|H| = e(Q'|P) \cdot f(Q'|P) = e \cdot n$$

e $f(P_Z|P) = 1$, pelo teorema B.8.1. Em particular, se $\widetilde{k}$ é o corpo das constantes de Z, sabemos que

$$\widetilde{k} \hookrightarrow K_{P_Z} \Longrightarrow [\widetilde{k} : \mathbb{F}_q] \leq [K_{P_Z} : \mathbb{F}_q] = 1 \Longrightarrow \widetilde{k} = \mathbb{F}_q,$$

ou seja,

$$\mathbb{F}_q \text{ é o corpo das constantes de } Z \tag{C.30}$$

Pela teoria de Galois, o corpo fixado por $H \cap G$ é ZL'. Temos que $ZL' = ZL\mathbb{F}_{q^n} = Z\mathbb{F}_{q^n}$ e $[Z\mathbb{F}_{q^n} : Z] = n$ (por C.30). Portanto

$$|H \cap G| = \frac{[E' : Z]}{[ZL' : Z]} = \frac{ne}{n} = e.$$

Como P_Z é não-ramificado em $ZL' = Z\mathbb{F}_{q^n}$ (pelo teorema B.6.1(a)), temos que $T := ZL'$ é o corpo de inércia e $H \cap G$ é o grupo de inércia de $Q'|P$ (pelo teorema B.8.2 (c) e (d), com ZL' fazendo o papel de M).

Agora aplicamos o lema C.2.3 novamente: Exatamente e dos grupos cíclicos $U_1, \ldots, U_m \subseteq Gal(E'/L)$ de ordem n com $U_i \cap G = \{1\}$ estão contidos em H, digamos $U_{i_1}, \ldots, U_{i_e}$. Seja $Q_{i_j} := Q' \cap E_{i_j}$. Como $U_{i_j} \subseteq H$, temos que $Z \subseteq E_{i_j}$; logo, pelo teorema B.8.2(b), Q' é o único place de E' que estende Q_{i_j}. Por outro lado, $e(Q'|Q_{i_j}) = 1$, pois E' é a extensão do corpo das constantes de E_{i_j} (por(b)). Daí temos que $n = [E' : E_{i_j}] = f(Q'|Q_{i_j}) \cdot e(Q'|Q_{i_j}) = f(Q'|Q_{i_j})$. Como $n = f(Q'|P)$, temos que $f(Q'|Q_{i_j}) = f(Q'|P)$. Logo $degQ_{i_j} = 1$. Assim, encontramos e places distintos $Q_{i_j} \in \cup_{i=1}^{m} X_i$ tais que $Q'|Q_{i_j}$.

Reciprocamente, tome $Q \in X_i$ para algum $i \in \{1, \ldots, m\}$ e $Q'|Q$. Daí $f(Q'|Q) = n$. Pela afirmação 1, Q' é a única extensão de Q em E'. Novamente pelo teorema B.8.2(b), $Z \subseteq E_i$ e logo $U_i \subseteq H$. Assim, U_i é um dos grupos U_{i_j} citados acima e Q é o place Q_{i_j} correspondente. Isso prova a afirmação 2 e, portanto, finaliza a prova da proposição C.2.2. □

Demonstração. **(Final do teorema de Hasse-Weil 4.2.1:)** Como já mencionado, resta estabelecermos uma cota inferior C.19 para $N_r = N(F_r)$. Procederemos da seguinte maneira. Escolha um subcorpo racional $K_0 = \mathbb{F}_q(t) \subseteq K$ tal que K/K_0 é separável, e uma extensão finita $E \supseteq K$ tal que E/K_0 é Galois (observe que existe um elemeto separante t, pela proposição B.9.1). É possível que o corpo das constantes de E seja uma extensão própria $\mathbb{F}_{q^d}$ de $\mathbb{F}_q$. Nesse caso, consideramos os corpos $K\mathbb{F}_{q^d}$ e $K_0\mathbb{F}_{q^d} = \mathbb{F}_{q^d}(t)$ no place de K e K_0 respectivamente. A extensão $E/K_0\mathbb{F}_{q^d}$ é Galois, e é suficiente provar o teorema de Hasse-Weil para $K\mathbb{F}_{q^d}/\mathbb{F}_{q^d}$ (pelo lema C.2.1). Sendo assim, podemos assumir do começo que $\mathbb{F}_q$ é também o corpo das constantes de E. Além disso, podemos assumir que

$$q \text{ é um quadrado, e } q > (g(E)+1)^4. \tag{C.31}$$

Sejam $m = [E : K]$ e $n = [E : K_0]$, e considere as extensões do corpo das constantes $E' = E\mathbb{F}_{q^n}$, $K' = K\mathbb{F}_{q^n}$ e $K_0' = K_0\mathbb{F}_{q^n}$. Pelo lema C.2.3, existem exatamente m subgrupos cíclicos distintos $V_1, \ldots, V_m \subseteq Gal(E'/K)$ de ordem n tais que $V_i \cap Gal(E'/K') = \{1\}$. Por outro lado, existem n subgrupos cíclicos $U_1, \ldots, U_n \subseteq Gal(E'/K_0)$ de ordem n tais que $U_j \cap Gal(E'/K_0') = \{1\}$. Temos também que $V_i \cap Gal(E'/K_0') = \{1\}$. De fato: como $V_i \subseteq Gal(E'/K)$, temos que, se D_i é o corpo fixado por V_i, então $K \subseteq D_i$; assim, tome $\alpha \in V_i \cap Gal(E'/K_0')$. Daí α fixa D_i e $K_0' \Longrightarrow \alpha$ fixa K e $K_0' \Longrightarrow \alpha$ fixa $KK_0' = KK_0\mathbb{F}_{q^n} = K\mathbb{F}_{q^n} = K'$. Logo $\alpha \in V_i \cap Gal(E'/K')$ e assim, $\alpha = 1$.

Logo, podemos assumir que $V_i = U_i$ para $i = 1, \ldots, m$. Denote por E_i o corpo fixado por U_i, $i = 1, \ldots, n$. A proposição C.2.2 diz que

$$m \cdot N(F) = \sum_{i=1}^{m} N(E_i) \tag{C.32}$$

e

$$n \cdot N(F_0) = \sum_{i=1}^{n} N(E_i). \tag{C.33}$$

Com a hipótese assumida em C.31, temos a cota superior

$$N(E_i) \leq q + 1 + (2g(E)+1)q^{1/2}$$

para $1 \leq i \leq n$, pela proposição C.2.1. Os places de grau um de $K_0 = \mathbb{F}_q(t)$são o pólo de t e o zero de $t - \alpha$ para todo $\alpha \in \mathbb{F}_q$. Logo $N(K_0) = q + 1$. Combinando isso com C.32 e C.33, obtemos

$$\begin{aligned} m \cdot N(K) &= n \cdot N(K_0) + \sum_{i=1}^{m} N(E_i) - \sum_{i=1}^{n} N(E_i) \\ &= n(q+1) - \sum_{i=m+1}^{n} N(E_i) \\ &\geq n(q+1) - (n-m)(q+1+(2g(E)+1)q^{1/2}) \\ &= m(q+1) - (n-m)(2g(E)+1)q^{1/2}. \end{aligned}$$

Logo

$$N(K) \geq q + 1 - \frac{n-m}{m}(2g(E)+1)q^{1/2}.$$

Observe que os números m, n e $g(E)$ são invariantes sob extensões de corpo das constantes; logo, estabelecemos uma cota inferior

$$N_r \geq q^r + 1 - c_2 q^{r/2},$$

com $c_2 > 0$. □

Encerraremos esse capítulo com uma importante conseqüência do teorema de Hasse-Weil.

Teorema C.2.2 (Cota de Hasse-Weil). *O número $N = N(F)$ de places de grau um de $K/\mathbb{F}_q$ pode ser estimado por*

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

Demonstração. O corolário C.1.4 nos fornece

$$N - (q+1) = -\sum_{i=1}^{2g} \alpha_i,$$

onde α_i são as recíprocas das raízes do L-polinômio de $K/\mathbb{F}_q$. Daí, usando o teorema de Hasse-Weil,

$$|N - (q+1)| = \left|\sum_{i=1}^{2g} \alpha_i\right| \leq \sum_{i=1}^{2g} |\alpha_i| = 2gq^{1/2}.$$

□

Note que o teorema C.2.2, aplicado ao corpo de funções $K_r/\mathbb{F}_{q^r}$ fornece

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

para todo $r \geq 1$.

Referências Bibliográficas

[1] D. Le Brigand, Classification of algebraic function fields with divisor class number two, Finite Fields and Apll. **2** (1996) 153-172.

[2] D. Le Brigand, Quadratic algebraic function fields with ideal class number two, in "Arithmetic Geometry and Coding Theory-4, Luminy, 1993", de Gruyter, Berlim, 1996.

[3] M.L. Madan and C.S. Queen, Algebraic function fields of class number one. Acta Arithmetica **20** (1972), 423-432.

[4] J.R.C. Leitzel, M.L. Madan and C.S. Queen, Algebraic function fields with small class number, J. Number Theory **7** (1975), 11-27.

[5] R. Hartshorne, "Algebraic Geometry", Springer-Verlag, Berlin/New York, 1977.

[6] J.W.P. Hirschfeld, "Finite Projective Spaces of Three Dimensions", Oxford Math. Monographs, Oxford University, New York, 1985.

[7] H. Stichtenoth, "Algebraic Function Fields and Codes", Universitext, Springer-Verlag, Berlin/New York, 1993.

[8] W. Fulton, "Algebraic Curves", W.A. Benjamin, New York, 1969.

[9] R. Miranda, "Algebraic Curves and Riemann Surfaces", A.M.S. Bookstore, 1995.

[10] C. Chevalley, "Introduction to the Theory of Algebraic Functions of One Variable", A.M.S., Providence, 1951.

Índice Remissivo

δ-invariante, 22
Índice de especialidade, 10

Adele, 10
  principal, 11
Anel coordenado afim, 15
Anel de valorização, 3
  discreta, 4
  do Place P, 4
Anel local de P em V, 16

Base dual, 75
Base integral, 76
Blow-up, 21

Caso inerte, 66
Caso ramificado, 66
Classe do divisor, 8
Conjunto algébico, 15
  radical de um, 15
Corpo das constantes de K, 3
Corpo das Funções Racionais
  de uma variedade, 15
Corpo de funções algébricas, 3
  anel holomórfico de um, 73
  subanel de um, 73
    elemento integral de um, 74
Corpo de funções elípticas, 62
Corpo de funções quadrático, 61
Corpo de funções racionais, 5
Corpo de inércia de P' sobre P, 87
Corpo decomposição de P' sobre P, 87
Corpo residual, 5
Cota de Hasse-Weil, 109
Cotraço de ω, 79

Desigualdade de Castelnuovo, 90
Desigualdade de Riemann, 91
Desigualdade triangular, 4
  estrita, 4
Diferencial de Weil, 11
Diferente de K'/K, 78
Dimensão de um divisor, 9
Divisor
  conorma de um, 72
  canônico, 11
  efetivo, 7
  especial, 12
  não-especial, 12
  positivo, 7
  primo, 7
  suporte de um, 7
Divisor Class Number, 94
Divisor hiperelíptico, 66
Divisores, 7
  equivalentes, 8

Elemento primo de P, 4
Elemento separante para K/k, 90
equação de Weierstrass, 65
Espaço afim, 15
Espaço das adeles, 10
Expoente diferente, 78
Extensão algébrica
  constante, 71
  de K/k, 71
  de places, 71
    índice de ramificação, 72
    grau relativo, 72
  finita, 71
  ramificada, 81
Extensão de Artin-Schreier de K, 85
Extensão de Kummer, 84
Extensão de places
  domesticamente (selvagemente) ramificada, 80
Extensão quadrática imaginária, 61
Extensão quadrática real, 61

Fórmula do Diferente de Hilbert, 89
Forma normal de Hasse, 69
Função
de classe de resíduo, 5
Zeta, 95

Gênero, 9
Grau
de um Place, 5
de um divisor, 8
Grupo
de classes de divisor, 8
de classes de divisores de grau zero, 93
dos divisores de grau zero, 93
dos divisores principais, 8
Grupo de inércia de P' sobre P, 87
Grupo decomposição de P' sobre P, 87
Grupo dos divisores, 7

Lacuna, 12
Lema de Abhyankar, 89

Módulo complementar, 77
Módulo dos diferenciais de Weil, 11

Número pólo, 12
Nullstellensatz de Hilbert, 15

Pólo, 5
Place, 4
conorma de um, 72
ramificado, 72
domesticamente ramificado, 81
infinito, 6
ramificado, 81
totalmente ramificado, 81
Place hiperelíptico, 66
Ponto hiperelíptico, 66
Produto de Euler, 96

razão de diferenciais de primeiro tipo, 11
Razão entre os diferenciais ω e ω', 11

Subconjunto irredutível, 15

Teorema
da aproximação forte, 12
da aproximação fraca, 6
da lacuna de Weiestrass, 12
de Clifford, 13
de F.K. Schmidt, 98
de Hasse-Weil, 101
de Riemann, 10
de Riemann-Roch, 11
Topologia de Zariski, 15

Valorização discreta, 4
Variedade
dimensão de uma, 15
Variedade algébrica, 15
Variedades
aplicação polinomial entre, 16
aplicação racional entre, 18
morfismo entre, 17

Zero, 5