2
Preliminares

Neste capítulo daremos algumas definições e resultados que serão utilizados no percorrer deste trabalho.

2.1
Pontos de Weierstrass

Seja C uma curva algébrica não singular completa de gênero g sobre um corpo k de característica $p > 0$ e seja $K = k(C)$ o corpo de funções algébricas de C. Para cada ponto $P \in C$ existe uma seqüência de números $1 = l_1(P) < l_2(P) < \cdots < l_g(P) \leq 2g - 1$ tal que $\dim \mathcal{L}(l_i(P)P) = \dim \mathcal{L}((l_i(P) - 1)P)$, denominada *seqüência de lacunas do ponto* P. Por outro lado, existe uma seqüência $L = \{l_1, l_2, \ldots, l_g\}$ tal que $L = L(P)$, onde $L(P) = \{l_1(P), l_2(P), \ldots, l_g(P)\}$, para todo ponto $P \in C$ salvo um número finito. Um ponto $Q \in C$ é um *Ponto de Weierstrass* se $L(Q) \neq L$. O *semigrupo de Weierstrass do ponto* P é o conjunto $\mathbb{N} \setminus L(P)$.
Seja $|\mathcal{K}|$ o sistema linear canônico de C. Temos que $|\mathcal{K}|$ define um morfismo

$$f_{|\mathcal{K}|} : C :\longrightarrow \mathbb{P}^{g-1}(k),$$

onde $f_{|\mathcal{K}|} = (f_0 : f_1 : \cdots : f_{g-1})$ com $f_0, f_1, \ldots, f_{g-1} \in k(C)$.
Seja $P \in C$ e t uma variável separante. Pelo teorema 1.1 de [[10], p. 4], existem inteiros $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{g-1}$ com $0 = \varepsilon_0 < \varepsilon_1 < \cdots < \varepsilon_{g-1}$ tais que o Wronskiano

$$\det \left(D_t^{(\varepsilon_i)}(f_j) \right)_{i,j=0,\ldots,g-1}$$

não é identicamente nulo, onde $D_t^{(\varepsilon_i)}$ é a derivada de Hasse. A escolha dos inteiros $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{g-1}$ é feita mínima na ordem lexicográfica. Agora, a proposição 1.4, de [[10], p. 5], afirma que os inteiros ε_i dependem somente da escolha do sistema linear canônico $|\mathcal{K}|$, e são chamados de ordens do morfismo $f_{|\mathcal{K}|}$.
Além do mais, temos que o *divisor de ramificação* do sistema linear canônico

PUC-Rio - Certificação Digital Nº 9816063/CA

$|\mathcal{K}|$ é

$$\mathcal{R} = \text{div}\left(D_t^{(\varepsilon_i)}(f_j)\right) + (\varepsilon_1 + \cdots + \varepsilon_{g-1})\text{div}(dt) + g\mathcal{K},$$

e,

$$\text{grau}(\mathcal{R}) = (\varepsilon_1 + \cdots + \varepsilon_{g-1})(2g-2) + g(2g-2).$$

Pelo Teorema 1.5 de [[10], p. 6], um ponto $P \in C$ é um ponto de Weierstrass se, e somente se, $v_P(\mathcal{R}) > 0$, onde o inteiro $v_P(\mathcal{R})$ é o peso do ponto P. Temos que $v_P(\mathcal{R}) > \sum_{i=0}^{n}(l_i(P) - 1 - \varepsilon_i)$ e a igualdade vale se, e somente se, $\det \begin{pmatrix} l_i(P) - 1 \\ \varepsilon_r \end{pmatrix} \not\equiv 0 \mod (p)$.

2.2
Operador de Cartier

Seja $K|k$ um corpo de funções de gênero g sobre um corpo perfeito k de característica $p > 0$. Seja x uma variável separante de $K|k$. Temos que $\{1, x, x^2, \ldots, x^{p-1}\}$ é uma base de K sobre K^p e logo podemos escrever todo $z \in K$ como

$$z = a_0^p + a_1^p x + \cdots + a_{p-1}^p x^{p-1},$$

onde os $a_i \in K$ para $i = 0, 1, \ldots, (p-1)$. Seja $\Omega_1(0)$ o espaço das formas diferenciais regulares e seja $\omega \in \Omega_1(0)$, então $\omega = zdx$, para algum $z \in K$. Definimos o *Operador de Cartier* para diferenciais regulares por

$$\mathcal{C}(\omega) = a_{p-1}dx,$$

onde $z = \sum_{i=0}^{p-1} a_i^p x^i$. Pelo Corolário 1.4 de [[11], p. 53], temos que $\mathcal{C}$ independe da escolha da variável separante x. Seja $y \in K$ tal que $K = k(x, y)$ e $f \in k[X, Y]$ polinômio irredutível tal que $f(x, y) = 0$. Logo, $K|k$ é o corpo de funções da curva plana projetiva dada pela equação afim

$$f(x, y) = 0.$$

Se a curva é não singular temos que

$$\omega = \frac{dx}{f_y(x, y)}$$

PUC-Rio - Certificação Digital Nº 9816063/CA

é uma diferencial regular. Logo, neste caso, as diferenciais regulares são da forma

$$h(x,y)\omega,$$

onde $h(x,y) \in K[x,y]$ é o polinômio adjunto de grau formal $\partial f - 3$. Então,

$$\mathcal{L}(div(\omega)) = \{h \in K[x,y] \ / \ \partial h \leq \partial f - 3\}.$$

Observe que como o operador de Cartier age sobre as diferenciais regulares, ele age, também, sobre os polinômios adjuntos de grau formal $\partial f - 3$. Pelo Teorema 1.1, de [[11], p. 50], temos que

$$\mathcal{C}(h\omega) = \left(\frac{\partial^{2p-2}}{\partial x^{p-1}\partial y^{p-1}}(f^{p-1}h)\right)^{\frac{1}{p}} \omega, \text{ onde } \omega = \frac{dx}{f_y(x,y)}$$

Em particular, para corpos de característica dois, temos

$$\mathcal{C}(h\omega) = \left(\frac{\partial^2}{\partial x \partial y}hf\right)^{\frac{1}{2}} \omega.$$

O operador de Cartier satisfaz:

(i) $\mathcal{C}$ independe da escolha da variável separante.

(ii) $\mathcal{C}(\omega_1 + \omega_2) = \mathcal{C}(\omega_1) + \mathcal{C}(\omega_2)$, para $\omega_1, \omega_2 \in \Omega_1(0)$

(iii) $\mathcal{C}(a^p\omega) = a\mathcal{C}(\omega)$ para $a \in K$ e $\omega \in \Omega_1(0)$.

2.3
Matriz e Invariante de Hasse-Witt

Seja C uma curva algébrica não singular completa de gênero g sobre um corpo algebricamente fechado de característica $p > 0$. Seja $\{\omega_1, \omega_2, \ldots, \omega_g\}$ uma base do espaço $\Omega_1(0)$ das diferenciais regulares. Para cada i, podemos escrever

$$\mathcal{C}(\omega_i) = \sum_{j=1}^{g} a_{ij}\omega_j, \tag{2-1}$$

onde $a_{ij} \in k$.
A matriz $H = (a_{ij}^p)$, onde a_{ij} é definido em (2-1), é chamada a *Matriz de Hasse-Witt*, em relação à base $\{\omega_1, \omega_2, \ldots, \omega_g\}$.

PUC-Rio - Certificação Digital Nº 9816063/CA

Se $\{\omega'_1, \omega'_2, \ldots, \omega'_g\}$ é outra base de $\Omega_1(0)$ e se

$$\mathcal{C}(\omega'_i) = \sum_{j=1}^{g} b_{ij}\omega_j,$$

com $(b_{ij}) \in GL_g(k)$, então a matriz de Hasse-Witt em relação à base $\{\omega'_1, \omega'_2, \ldots, \omega'_g\}$ é dada por

$$(b_{ij})H(b_{ij}^p)^{-1}.$$

O *Invariante de Hasse-Witt*, denotado por σ, é definido como o posto da matriz $(h_{ij})(h_{ij}^p)\cdots(h_{ij}^{p^{g-1}})$, onde $H = (h_{ij})$ é a matriz de Hasse-Witt. Isto é,

$$\sigma = \text{posto}\left((h_{ij})(h_{ij}^p)\cdots(h_{ij}^{p^{g-1}})\right).$$

2.4
Característica Teta em característica dois

Seja C uma curva algébrica não singular completa de gênero g sobre um corpo k algebricamente fechado de característica 2 e seja $K = k(C)$ o corpo de funções de C. Uma *Característica Teta* é definida como uma classe de divisores Θ tal que 2Θ é a classe canônica.
Seja x uma variável separante, isto é, $x \in K \setminus K^2$. Desenvolvendo x, localmente, como uma série de potências, em termos de um parâmtero local, temos que dx tem polos e zeros de ordem 2, ou seja,

$$(dx) = 2\mathcal{D}_0,$$

para algum divisor $\mathcal{D}_0$.
Consideremos $x_1, x_2 \in K \setminus K^2$, temos que $\{1, x_2\}$ é uma base de K sobre K^2, e então, $x_1 = a_0^2 + a_1^2 x_2$, com $a_0, a_1 \in K$. Logo, $dx_1 = a_1 dx_2$ e assim os divisores D_1 e D_2 de x_1 e x_2, respectivamente, satisfazem

$$\mathcal{D}_1 = (a_1) + \mathcal{D}_2,$$

onde (a_1) é o divisor de a_1. Podemos concluir que a classe de $\mathcal{D}_0$ independe de x. A classe de $\mathcal{D}_0$ é uma Característica Teta, chamada de *Característica Teta canônica*, e é denotada por Θ_0.

Observação 2.1 *Uma diferencial (em característica p) é exata se, e somente se, ela pertence ao núcleo do operador de Cartier.*

PUC-Rio - Certificação Digital Nº 9816063/CA

Os seguintes resultados e suas respectivas demonstrações podem ser encontrados em [11], páginas 59 e 60.

Proposição 2.1 *Existe uma bijeção $\frac{1}{2}$-linear do espaço de diferenciais regulares exatas sobre $\mathcal{L}(\Theta_0)$.*

Corolário 2.1 *Em característica dois a matriz de Hasse-Witt tem posto $\geq \frac{g-1}{2}$. A desigualdade é estrita se a curva é não hiperelítica de gênero $g \geq 3$.*

Observe que uma Característica Teta Θ pode ser escrita da forma $\Theta = \Theta_0 + \gamma$, onde γ é um ponto de torsão 2 na Jacobiana.

Observação 2.2 *Uma diferencial (em característica p) é logarítmica se, e somente se, ela é invariante sob o operador de Cartier.*

Proposição 2.2 *Existe uma bijeção canônica entre o conjunto de diferenciais regulares logarítmicas não nulas e o conjunto de características teta não canônicas, que associa ω à classe de $\frac{1}{2}(\omega)$.*

Por outro lado, temos que o número de Características Teta não canônicas é igual a p^σ, onde $0 \leq \sigma \leq g$ é o invariante de Hasse-Witt.
Pela Proposição 2.2 temos que cada Característica Teta não canônica é representada por um divisor positivo. No caso de característica Teta canônica isto é verdade se, e somente se, o posto da matriz de Hasse-Witt é menor que g.
Para uma curva não hiperelítica C de gênero $g = 3$, identificando-a com sua imagem pelo morfismo canônico, temos que ela é uma quártica projetiva plana não singular. Como os divisores canônicos neste caso são os divisores de interseção de C com as retas projetivas, temos que os divisores positivos que representam uma Característica Teta correspondem bijetivamente às bitangentes da quártica C.

PUC-Rio - Certificação Digital Nº 9816063/CA

2.5
Pontos Galoisianos

Seja C uma curva algébrica não singular completa de gênero g definida sobre um corpo de constantes k algebricamente fechado e seja $K = k(C)$ o corpo de funções racionais de C.
Sejam $Q \in C$ e d_Q a primeira não lacuna positiva em Q, então, existe uma função f_Q em K que possui um polo em Q de ordem d_Q, isto é, $\mathrm{div}_\infty(f_Q) = d_Q Q$.

Definição 2.1 *O ponto Q é um ponto Galoisiano se a extensão $k(C)|k(f_Q)$ é uma extensão Galoisiana de corpos.*

A função meromorfa f_Q é única a menos de uma transformação do tipo $f_Q \mapsto \alpha f_Q + \beta$ com $\alpha \neq 0$, e logo a extensão $k(C)|k(f_Q)$ é bem definida: uma transformação $f_Q \mapsto \alpha f_Q + \beta$ com $\alpha \neq 0$ resulta no mesmo subcorpo de $k(C)$ com um gerador que difere do original por um automorfismo de $k(f_Q)$ (que fixa o ponto infinito de $k(f_Q)$, do qual Q é uma extensão).
Seja Q um ponto de Galois da curva C, então o grupo de Galois $\mathrm{Gal}(k(C)|k(f_Q))$ fixa a função f_Q e logo fixa também o ponto Q e os espaços $\mathcal{L}(nQ)$, isto é,

$$\mathrm{Gal}(k(C)|k(f_Q)) \subset G_Q := \{\sigma \in \mathrm{Aut}(C) \,/\, \sigma(Q) = Q\},$$

onde G_Q é o subgrupo do grupo dos automorfismos $\mathrm{Aut}(C)$ de C que fixam o ponto Q. Segue que

$$\mathrm{Gal}(k(C)|k(f_Q)) \subset G_Z := \{\sigma \in \mathrm{Gal}(k(C)|k(f_Q)) \,/\, \sigma(Q) = Q\},$$

onde G_Z é o grupo de decomposição de $Q|P$ na extensão $k(C)|k(f_Q)$, (ver ([9], Def. III.8.1, p. 118). Se Q é um ponto de Galois, o grupo G_Q é não trivial. A recíproca não é verdadeira. Seja Q_∞ o ponto no infinito da curva

$$y^{p^n} + y = x^m + x,$$

definida sobre um corpo de característica positiva $p > 0$. Para $p \nmid m < p^n$ o grupo G_{Q_∞} consiste dos automorfismos

$$\begin{array}{rccc} \sigma_b : & x & \mapsto & x \\ & y & \mapsto & y + b, \end{array}$$

PUC-Rio - Certificação Digital Nº 9816063/CA

com $b^{p^n} = b$, ver ([8], Teil II, p. 621), mas y é a função com ordem de polo mínima em Q_∞, que é fixa apenas por $\sigma_0 = \mathrm{Id} \in G_{Q_\infty}$. Segue

$$Gal(k(C)|k(f_Q)) = G_Z = \{\ \sigma\ \in Gal(k(C)|k(f_Q)) \mid \sigma(Q) = Q\ \}$$

Se o corpo de constantes k for algebricamente fechado então os graus de inércia são triviais, e logo $G_Z = G_T$, onde

$$G_T := \{\ \sigma\ \in Gal_{k(C)|k(f_Q)} \mid v_Q(\sigma(z) - z) > 0 \text{ para todo } z \in \mathcal{O}_Q\ \},$$

com $\mathcal{O}_Q = \{z \in k(C)\ /\ v_Q(z) \geq 0\}$, é o *grupo de inércia* de $Q|P$ na extensão $k(C)|k(f_Q)$ ([9], Teo. III.8.1, p. 119).

Se $\pi \in k(C)$ é um parâmetro local em Q então a série de grupos de ramificação de $Q|P$ na extensão $k(C)|k(f_Q)$ é definida por

$$G_i := \{\ \sigma \in Gal_{k(C)|k(f_Q)} \mid v_Q(\sigma(\pi) - \pi) > i\ \},$$

e o expoente da diferente $\delta_{Q|P}$ é dado em termos destes grupos pela fórmula da diferente de Hilbert

$$\delta_{Q|P} = \sum_{i \geq 0} card(G_i).$$

O grupo $G_0 = G_T$ é o grupo de inércia de $Q|P$. Ver, por exemplo, ([9], Prop. III.8.6, p. 122 e 124). Se a característica de $k(C)$ é $p > 0$, então G_1 é um subgrupo normal de G_0,

$$card(G_1) = p^e, \qquad \text{para algum inteiro} \quad e,$$

e G_0/G_1 é cíclico de ordem relativamente prima com p. Além disso, G_{i+1} é um subgrupo normal de G_i, para cada $i \geq 1$, e G_i/G_{i+1} é isomorfo a um subgrupo aditivo do corpo residual $k_Q = \mathcal{O}_Q/\mathcal{M}_Q$ de Q ([9], Prop. III.8.6, p. 122). A postulação de um ponto Q determina:

i. O sistema linear do tipo $g^1_{d_Q}$

$$|d_Q Q| = \{\ \alpha f_Q + \beta \mid \alpha, \beta \in k,\ \alpha \neq 0\ \}.$$

ii. A extensão $k(C)|k(\alpha f_Q + \beta) = k(C)|k(f_Q)$ que tem grau d_Q.

PUC-Rio - Certificação Digital Nº 9816063/CA

iii. O fecho normal $k(E_Q)|k(f_Q)$ de $k(C)|k(f_Q)$. O ponto Q é de Galois se, e só se, $k(E_Q) = k(C)$.

iv. O grupo de Galois

$$G_Q := Gal_{k(E_Q)|k(f_Q)},$$

e o subgrupo $H_Q := Hom_{k(f_Q)}(k(C), k(C)) \subset G_Q$ correspondente pela teoria de Galois à extensão $k(C)|k(f_Q)$.
Se o ponto Q é ponto de Galois e a característica de k é zero, caso originalmente tratado em [7], o grupo de Galois $G_Q = Gal_{k(E_Q)|k(f_Q)}$ é sempre cíclico.

v. A diferente $Diff_{k(E_Q)|k(f_Q)}$, que é um divisor na superfície de Riemann associada a $k(E_Q)$, sua norma

$$\mathcal{N}_{k(E_Q)|k(f_Q)}(Diff_{k(E_Q)|k(f_Q)}),$$

que é o discriminante da extensão $k(E_Q)|k(f_Q)$, é também um divisor na superfície de Riemann associada a $k(f_Q)$, e a conorma

$$Con_{k(C)|k(f_Q)}(\mathcal{N}_{k(E_Q)|k(f_Q)}(Diff_{k(E_Q)|k(f_Q)})),$$

é um divisor na superfície de Riemann associada a $k(C)$.
Como

$$\mathrm{div}_\infty(f_Q) = \begin{cases} d_Q Q & \text{em} \quad k(C) \\ \\ P := Q|_{k(f_Q)} & \text{em} \quad k(f_Q), \end{cases}$$

temos que $e_{Q|P} = d_Q$, isto é, $Q|P$ é totalmente ramificado na extensão $k(C)|k(f_Q)$.

Na torre de extensões e grupos correspondentes

$$\begin{array}{cc} k(E_Q) & G_Q \\ \uparrow & \uparrow \\ k(C) & H_Q \\ \uparrow d_Q & \uparrow \\ k(f_Q) & \{id\} \end{array}$$

temos (por exemplo, ([9], Cor. III.4.11, p. 88))

$$Diff_{k(E_Q)|k(f_Q)} = Con_{k(E_Q)|k(C)}(Diff_{k(C)|k(f_Q)}) + Diff_{k(E_Q)|k(C)}.$$

PUC-Rio - Certificação Digital Nº 9816063/CA

Como consequência do teorema da diferente de Dedekind (por exemplo, ([9], Teo. III.5.1, p. 89)) se a característica p não divide d_Q então

$$v_Q(Diff_{k(C)|k(f_Q)}) = d_Q - 1,$$

de modo que se R for um ponto acima de Q na superfície de Riemann associada a $k(E_Q)$, então

$$v_R(Diff_{k(E_Q)|k(f_Q)}) = e_{R|Q}(d_Q - 1) + v_R(Diff_{k(E_Q)|k(C)}).$$

Se a característica p também não dividir $e_{R|Q}$ — o que necessariamente ocorre, por exemplo, se $p > d_Q$ — então

$$v_R(Diff_{k(E_Q)|k(C)}) = e_{R|Q}-1, \quad \text{e logo} \quad v_R(Diff_{k(E_Q)|k(f_Q)}) = e_{R|Q}\cdot d_Q-1.$$

vi. O índice de ramificação $e_{R|Q}$ da extensão de Q a $k(E_Q)$ é independente de R porque a extensão $k(E_Q)|k(C)$ é de Galois.

vii. O gênero g_Q de $k(E_Q)$.

PUC-Rio - Certificação Digital Nº 9816063/CA