UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

Alessandro Rezende de Macedo

Corpos de funções de curvas algébricas sobre um corpo algebricamente fechado: seu grupo de automorfismos e uma família de curvas com grupo de automorfismos trivial

RIO DE JANEIRO

2011

Alessandro Rezende de Macedo

Corpos de funções de curvas algébricas sobre um corpo algebricamente fechado: seu grupo de automorfismos e uma família de curvas com grupo de automorfismos trivial

Dissertação de Mestrado submetida ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Orientador: Luciane Quoos Conte

Rio de Janeiro

Novembro de 2011

Macedo, Alessandro Rezende de

Corpos de funções de curvas algébricas sobre um corpo algebricamente fechado: seu grupo de automorfismos e uma família de curvas com grupo de automorfismos trivial/ Alessandro Rezende de Macedo. – Rio de Janeiro: UFRJ/ IM, 2011.

xiv, 90 p.; 31 cm

Orientador: Luciane Quoos Conte.

Dissertação (Mestrado) – UFRJ/ IM/ Programa de Pós-Graduação em Matemática, 2011.

1. Corpos de funções. 2. Curvas algébricas. I. Conte, Luciane Quoos. II. Universidade Federal do Rio de Janeiro, Instituto de Matemática, Programa de Pós-Graduação em Matemática. III. Título.

Corpos de funções de curvas algébricas sobre um corpo algebricamente fechado: seu grupo de automorfismos e uma família de curvas com grupo de automorfismos trivial

por

Alessandro Rezende de Macedo
Orientador: Luciane Quoos Conte

Dissertação de Mestrado submetida ao Programa de Pós-graduação do Instituto de Matemática, da Universidade Federal do Rio de Janeiro - UFRJ, como parte dos requisitos necessários à obtenção do título de Mestre em Matemática.

Aprovada por:

Luciane Quoos Conte
IM - UFRJ - Presidente

Severino Collier Coutinho
IM - UFRJ

Herivelto Martins Borges Filho
ICMC - USP

Francesco Noseda
IM - UFRJ

Guilherme Augusto de La Rocque Leal
IM - UFRJ - Suplente

Rio de Janeiro

Novembro de 2011

Agradecimentos

Obrigado meus pais e ancestrais
pois, sem vocês, não existiria.
Sem seus incentivos fundamentais
tudo mais difícil ficaria.

Por servir de modelo para mim,
Professora Luciane Conte,
muito obrigado! Você para mim
foi uma ajuda sem precedente .

Agradeço ao CNPQ
pelo seu apoio financeiro
e aos colegas do IM que
me escutavam o dia inteiro.

Por fim, devo agradecer a Deus, pois tudo que aprendi,
supostamente, não haveria sido possível sem Ti.

Resumo

Estudamos a estrutura do grupo de automorfismos de curvas algébricas não singulares sobre um corpo algebricamente fechado. Classificamos este grupo para curvas de gênero zero e fazemos breves comentários para o caso de curvas de gênero um. Nosso principal objetivo é definir o grupo de decomposição de um lugar, mostrar sua finitude para curvas de gênero positivo e provar que o grupo de automorfismos de uma curva de gênero maior que um é finito, utilizando um resultado sobre a ordem de grupos irredutíveis de transformações lineares. Por fim, exibimos uma família explícita de curvas planas cujos corpos de funções possuem grupo de automorfismos trivial.

Palavras-Chaves: curva algébrica, corpo de função, grupo de automorfismos.

Abstract

We study the structure of the automorphism group of nonsingular algebraic curves over an algebraically closed field. We classify this group for genus zero curves and we make brief comments on the case of genus one curves. Our main goal is to define the decomposition group of a place, to prove its finiteness for curves of positive genus and to prove that the automorphism group of a curve of genus greater than one is finite, using a result on the order of irreducible groups of linear transformations. Finally, we exhibit an explicit family of plane curves whose function fields have trivial automorphism group.

Key-words: algebraic curve, function field, automorphism group.

Introdução

No final do século XIX, Poincaré provou, utilizando métodos analíticos, que uma superfície de Riemann de gênero maior que um possui grupo de automorfismos finito e, não muito depois, Hurwitz provou o mesmo resultado utilizando métodos mais algébricos. Mais precisamente, se X é uma curva não singular de gênero $g > 1$ definida sobre os complexos, Hurwitz mostrou que uma cota superior para seu grupo de automorfismos é $84(g-1)$ (ver [7]). Seu método se baseava na existência de "pontos de Weierstrass" e podia ser generalizado para curvas não singulares sobre corpos de característica 0. O caso de curvas de gênero maior que um sobre um corpo de característica positiva foi primeiramente resolvido em 1938 por H. L. Schmid (ver [12]), utilizando uma generalização devida a F. K. Schmidt para a teoria de pontos de Weierstrass. Alguns anos depois, Iwasawa e Tamagawa mostraram em [8] que o estudo da ação do grupo de automorfismos no conjunto das diferenciais holomorfas do corpo de funções dessas curvas também permite concluir a finitude desse grupo.

Posteriormente, em 1961, Baily provou em [3] que uma curva genérica de gênero maior que dois (sobre os complexos) possui grupo de automorfismos trivial, mas seu método não fornecia um exemplo concreto de tal curva. A primeira família de equações explícitas com grupo de automorfismos trivial foi dada por Turbek em [15].

Nesta dissertação, nosso principal objetivo é provar os resultados devido a Iwasawa e Tamagawa em[8] e de Turbek em [15], sendo estes investigados nos capítulos 3 e 4, respectivamente. Nos capítulos 1 e 2, definimos com precisão os conceitos de curvas algébricas e corpos de funções em uma variável. Como estamos mais interessados em utilizar suas propriedades para obter os resultados no capítulo 3 e 4 e a fim de manter o foco desta dissertação, nos capítulos 1 e 2 omitimos as demonstrações de certos lemas e teoremas clássicos, mas sempre fornecemos referências para mais detalhes.

Mais precisamente, no primeiro capítulo, a fim de definir o conceito de curva algébrica, apresentamos mais geralmente as noções de variedades algébricas afins e projetivas sobre um corpo algebricamente fechado e os conceitos de morfismos e aplicações racionais entre tais objetos. Definimos também o corpo de funções de uma variedade algébrica e provamos, por exemplo, o resultado clássico de que duas variedades sobre K são birracionalmente equivalentes se, e só se, seus corpos de funções são K-isomorfos. Encerramos

o capítulo definindo o conceito de curva algébrica e singularidade em curvas algébricas e exploramos suas principais propriedades, como, por exemplo, a existência de modelos planos e um modelo projetivo não singular. A demonstração desses resultados bem como mais detalhes podem ser encontrados em Hartshorne [6], Fulton [4], Atiyah-Macdonald [1] ou Matsumura [10].

No segundo capítulo, motivados pelo fato de que a geometria birracional de uma curva é traduzida pelo seu corpo de funções, definimos a noção de um corpo de funções em uma variável sobre um corpo algebricamente fechado K. Definimos também o conceito de gênero de um corpo de funções e provamos o teorema de Riemann-Roch (teorema 2.4) seguindo a demonstração apresentada em Stichtenoth [14], que não utilizará o fato de K ser algebricamente fechado. Encerramos o capítulo estudando extensões algébricas de corpos de funções sobre um corpo algebricamente fechado, que aparecerão naturalmente no capítulo 3.

No terceiro capítulo, definimos o grupo de automorfismos de um corpo de funções sobre um corpo algebricamente fechado e estudamos sua ação natural no conjunto de divisores e diferenciais de Weil. Em seguida, consideramos o caso de corpos de funções de gênero zero, classificando seu grupo de automorfismos e fornecendo explicitamente a ação desse grupo nos lugares desses corpos de funções. Em seguida, com base no artigo de Iwasawa e Tamagawa, definimos o conceito de grupo de decomposição de um lugar, provamos sua finitude para corpos de funções de gênero positivo e, utilizando esse fato bem como um resultado devido a Burnside (lema 3.6), provamos que o grupo de automorfismos de um corpo de funções de gênero maior que um sobre um corpo algebricamente fechado é finito. Na última seção, fazemos breves comentários sobre a estrutura do grupo de automorfismos de corpos de funções de gênero um.

No quarto e último capítulo, investigamos a família de curvas planas afins consideradas por Turbek e provamos que seu corpo de funções possui grupo de automorfismos trivial. Para tal, construímos o modelo projetivo não singular dessas curvas e estudamos a sequência de lacunas em cada um de seus pontos.

Sumário

Capítulo 1

Variedades

Nesse capítulo, investigamos a categoria das variedades sobre um corpo algebricamente fechado K e seus morfismos. Definimos também a noção de uma aplicação racional dominante entre variedades e consideramos a categoria das variedades aplicações racionais dominantes. Mostramos que essa última categoria é equivalente à categoria das extensões de K finitamente geradas e, por fim, consideramos os principais objetos dessa dissertação, as curvas algébricas, que são as variedades de dimensão 1. Provamos alguns resultados, mas omitimos as demonstrações de certos lemas e teoremas clássicos. Suas provas bem como mais detalhes podem ser encontrados, por exemplo, em Hartshorne [6], Fulton [4], Atiyah-Macdonald [1] ou Matsumura [10].

1.1 Conjuntos algébricos afins

Ao longo de toda a dissertação, K denota um corpo algebricamente fechado. Definimos o *n-espaço afim sobre* K, denotado por $\mathbb{A}^n(K)$ (ou simplesmente $\mathbb{A}^n$ caso não haja dúvida de que seja sobre K), como o produto cartesiano de n cópias de K, isto é,

$$\mathbb{A}^n(K) = K \times ... \times K, \quad n \text{ vezes}$$

Definição 1.1. Seja $S \subseteq K[x_1, ..., x_n]$. O *conjunto algébrico afim de* S é o conjunto

$$\mathrm{Z}(S) = \{x \in \mathbb{A}^n \mid f(x) = 0, \forall f \in S\}.$$

Se I é o ideal gerado pelos elementos de $S \subseteq K[x_1, ..., x_n]$, então é claro que $\mathrm{Z}(S) = \mathrm{Z}(I)$ e, portanto, pensamos em V como uma aplicação sobrejetiva do conjunto de ideais de $K[x_1, ..., x_n]$ na classe dos conjuntos algébricos afins. Quanto à notação, se I é gerado por elementos $f_1, ..., f_r$, escrevemos $\mathrm{Z}(f_1, ..., f_r)$ ao invés de $\mathrm{Z}(I)$.

As seguintes propriedades são imediatas da definição de Z:

Proposição 1.1.

(a) *Para todo* $k \in K\backslash\{0\}$, $m \in \mathbb{N}\backslash\{0\}$ *e* $f \in K[x_1, ..., x_n]$, $\mathrm{Z}(f) = \mathrm{Z}(kf) = \mathrm{Z}(f^m)$;

(b) *Se* $I \subseteq J$ *são ideais de* $K[x_1, ..., x_n]$, *então* $\mathrm{Z}(I) \supseteq \mathrm{Z}(J)$;

(c) *Se* $\{I_\lambda\}_\lambda$ *é uma família de ideais de* $K[x_1, ..., x_n]$, *então* $\mathrm{Z}(\bigcup_\lambda I_\lambda) = \bigcap \mathrm{Z}(I_\lambda)$;

(d) *Se* I *e* J *são ideais de* $K[x_1, ..., x_n]$, *então* $\mathrm{Z}(I) \cup \mathrm{Z}(J) = \mathrm{Z}(IJ)$

(e) $\mathrm{Z}(0) = \mathbb{A}^n(K)$ *e* $\mathrm{Z}(1) = \emptyset$;

As propriedades em (c) e (d) nos permitem concluir que interseções arbitrárias de conjuntos algébricos bem como uniões finitas de conjuntos algébricos são ainda conjuntos algébricos. Como o conjunto vazio e $\mathbb{A}^n$ também são conjuntos algébricos pela propriedade em (e), vemos que $\mathbb{A}^n$ possui estrutura de espaço topológico, definindo os fechados como os conjuntos algébricos afins. Essa topologia em $\mathbb{A}^n$ é denominada *topologia de Zariski*.

Exemplo 1.1. Os conjuntos algébricos de $\mathbb{A}^1$ são os conjuntos de zeros de polinômios em $K[x]$, que são precisamente os conjuntos finitos. Logo, os abertos não vazios de $\mathbb{A}^1$ são os conjuntos de complementar finito.

Em contraposição ao conceito de conjunto algébrico de um ideal de polinômios, temos o conceito de ideal de um conjunto de pontos de $\mathbb{A}^n$:

Definição 1.2. Seja X um subconjunto de $\mathbb{A}^n(K)$, o *ideal de* X é o conjunto

$$\mathrm{I}(X) = \{f \in K[x_1, ..., x_n] \mid f(x) = 0, \forall x \in X\}.$$

Observe que, de fato, o ideal de um subconjunto de $\mathbb{A}^n$ é um ideal de $K[x_1, ..., x_n]$, justificando a nomenclatura dessa aplicação. Provamos que:

Proposição 1.2.

(a) *Se* $X \subseteq Y$ *são subconjuntos de* $\mathbb{A}^n(K)$, *então* $\mathrm{I}(X) \supseteq \mathrm{I}(Y)$;

(b) $\mathrm{I}(\emptyset) = K[x_1, ..., x_n]$;

(c) $\mathrm{I}(\mathbb{A}^n(K)) = \{0\}$;

(d) $\mathrm{I}(\mathrm{Z}(S)) \supseteq S$, *para todo* $S \subseteq K[x_1, ..., x_n]$.

(e) $\mathrm{Z}(\mathrm{I}(X)) \supseteq X$, *para todo* $X \subseteq \mathbb{A}^n(K)$.

Demonstração. A única afirmação que não é imediata da definição é a propriedade em (c). Provaremos esse resultado por indução em n. A veracidade para o caso $n = 1$ decorre do fato de que um polinômio não nulo em uma variável possui apenas um número finito de raízes e do fato de que K é um conjunto infinito, pois assumimos K um corpo algebricamente fechado. Supondo então que o resultado valha para $n-1$, seja $f \in \mathrm{I}(\mathbb{A}^n)$, escrevemos $f = f_0 + f_1 x_n + ... + f_m x_n^m$, com $f_i \in K[x_1, ..., x_{n-1}]$. Se f é não nulo, então algum f_i é não nulo e, pela hipótese de indução, existe $(a_1, ..., a_{n-1}) \in \mathbb{A}^{n-1}$ tal que $f_i(a_1, ..., a_{n-1}) \neq 0$. Nesse caso, temos que $f(a_1, ..., a_{n-1}, x_n)$ é um polinômio não nulo em uma variável. No entanto, como $f \in \mathrm{I}(\mathbb{A}^n)$, o polinômio $f(a_1, ..., a_{n-1}, x_n)$ deve possuir infinitas raízes, um absurdo!

□

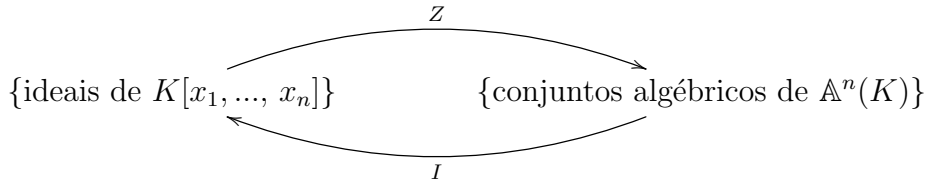
Utilizando as propriedades acima, podemos provar que:

Corolário 1.1. *Seja $X \subseteq \mathbb{A}^n(K)$, então $\mathrm{I}(X) = \mathrm{I}(\overline{X})$, onde $\overline{X}$ denota o fecho de X em $\mathbb{A}^n(K)$ (munido da topologia de Zariski).*

Demonstração. Por um lado, como $X \subseteq \overline{X}$, temos que $\mathrm{I}(X) \supseteq \mathrm{I}(\overline{X})$, pelo item (a). Por outro lado, pelo item (e), $X \subseteq \mathrm{Z}(\mathrm{I}(X))$ e, como $\mathrm{Z}(\mathrm{I}(X))$ é fechado na topologia de Zariski, temos que $\overline{X} \subseteq \mathrm{Z}(\mathrm{I}(X))$. Finalmente, segue pelos itens (a) e (d) que $\mathrm{I}(\overline{X}) \supseteq \mathrm{I}(\mathrm{Z}(\mathrm{I}(X))) \supseteq \mathrm{I}(X)$.

□

Logo, a dinâmica entre I e Z pode ser resumida no diagrama



Ingenuamente poderíamos sugerir que tais operações são inversas. No entanto, a propriedade (a) da proposição 1.1 nos fala que Z nem é injetiva! Uma pergunta natural é qual o resultado das composições $\mathrm{Z} \circ \mathrm{I}$ e $\mathrm{I} \circ \mathrm{Z}$. A resposta da primeira é simples:

Proposição 1.3. *Seja $X \subseteq \mathbb{A}^n$ um conjunto algébrico, então $\mathrm{Z}(\mathrm{I}(X)) = X$.*

Demonstração. A proposição 1.2.(e) nos garante a inclusão $\mathrm{Z}(\mathrm{I}(X)) \supseteq X$. Para verificar a inclusão contrária, escreva $X = \mathrm{Z}(J)$, para algum ideal J de $K[x_1, ..., x_n]$. Pela proposição 1.2.(d), temos que $\mathrm{I}(X) \supseteq J$ e, portanto, pela proposição 1.2.(a), $\mathrm{Z}(\mathrm{I}(X)) \subseteq \mathrm{Z}(J) = X$.

□

A composição $\mathrm{I} \circ \mathrm{Z}$ não é tão simples. Sua resposta é conhecida como o teorema dos zeros de Hilbert:

Teorema 1.1 (**Teorema dos zeros de Hilbert**). *Seja I um ideal de $K[x_1, ..., x_n]$. Se K é algebricamente fechado, então*

$$\mathrm{I}(\mathrm{Z}(I)) = \sqrt{I},$$

onde $\sqrt{I}$ denota o radical de I, isto é, o conjunto de todos os $f \in K[x_1, ..., x_n]$ para os quais existe um natural m com $f^m \in I$.

Demonstração. Ver Fulton [[4], Seção 1.7, página 10].

□

Observe que a hipótese de K ser algebricamente fechado é essencial para a validade desse teorema. De fato, se, por exemplo, $K = \mathbb{R}$, o ideal I gerado por $x^2 + y^2 + 1$ em $\mathbb{R}[x, y]$ é primo e, portanto, $\sqrt{I} = I$, mas $\mathrm{Z}(I)$ é obviamente vazio e, portanto, $\mathrm{I}(\mathrm{Z}(I)) = K[x_1, ..., x_n]$.

1.2 Variedades afins

Um espaço topológico X é dito *irredutível* se ele não pode ser escrito como a união de dois fechados próprios. Convencionamos que $\emptyset$ não é irredutível.

Definição 1.3. Uma *variedade afim* é um conjunto algébrico afim irredutível. Uma *variedade quase afim* é um aberto não vazio de uma variedade afim.

Em outras palavras, um subconjunto $X \subseteq \mathbb{A}^n$ é uma variedade quase afim se existem um aberto U de $\mathbb{A}^n$ e uma variedade afim $V \subseteq \mathbb{A}^n$ tais que $X = V \cap U$. Em particular, toda variedade afim é uma variedade quase afim, pois $\mathbb{A}^n$ é aberto. Além disso, note que todo aberto não vazio de uma variedade afim é denso:

Proposição 1.4. *Se U é um aberto não vazio de uma variedade afim V, então $\overline{U} = V$.*

Demonstração. Por um lado, $\overline{U} \subseteq \overline{V} = V$. Por outro lado, se $\overline{U} \neq V$, então podemos escrever $V = \overline{U} \cup (V \backslash U)$, o que contraria o fato de V ser irredutível.

□

Um bom critério para decidir quando um conjunto algébrico afim é uma variedade afim é olhar para seu ideal:

Proposição 1.5. *Um conjunto algébrico não vazio $V \subseteq \mathbb{A}^n$ é uma variedade afim se, e só se,* $\mathrm{I}(V)$ *é um ideal primo.*

Demonstração. Suponha que $\mathrm{I}(V)$ não seja um ideal primo e sejam f, g polinômios em $K[x_1, ..., x_n]$ tais que $fg \in \mathrm{I}(V)$, mas f, $g \notin \mathrm{I}(V)$. É claro que

$$V = (V \cap \mathrm{Z}(f)) \cup (V \cap \mathrm{Z}(g)).$$

Afirmamos que $V \cap \mathrm{Z}(f) \neq V$. De fato, se $V \cap \mathrm{Z}(f) = V$, teríamos que $V \subseteq \mathrm{Z}(f)$ e, nesse caso, $\mathrm{I}(V) \supseteq \mathrm{I}(\mathrm{Z}(f)) \supseteq (f)$, implicando $f \in \mathrm{I}(V)$, um absurdo! Pelos mesmos argumentos, temos que $V \cap \mathrm{Z}(g) \neq V$ e, portanto, V é redutível. Para mostrar a recíproca, suponha que existam conjuntos algébricos V_1, $V_2 \neq V$ tais que $V = V_1 \cup V_2$. Nesse caso, $\mathrm{I}(V_i) \supsetneq \mathrm{I}(V)$, para todo i, e podemos escolher $f \in \mathrm{I}(V_1)$, $g \in \mathrm{I}(V_2)$ tais que f, $g \notin \mathrm{I}(V)$, mas $fg \in \mathrm{I}(V)$, o que nos mostra que $\mathrm{I}(V)$ não é um ideal primo.

□

Exemplo 1.2. $\mathbb{A}^n$ e qualquer conjunto do tipo $\{(a_1, ..., a_n)\}$ são variedades afins, pois seus ideais são, respectivamente, $\{0\}$ e $(x_1 - a_1, ..., x_n - a_n)$, que são primos.

Exemplo 1.3. Toda hipersuperfície $\mathrm{Z}(f)$, com $f \in K[x_1, ..., x_n]$ irredutível, é uma variedade afim, pois seu ideal é $\sqrt{(f)} = (f)$, que é primo.

Exemplo 1.4. As únicas variedades de $\mathbb{A}^1$ são os conjuntos unitários e $\mathbb{A}^1$. No entanto, não é difícil ver que em $\mathbb{A}^2$ as variedades são, além dos conjuntos unitários e o próprio $\mathbb{A}^2$, os conjuntos do tipo $\mathrm{Z}(f)$, para algum $f \in K[x_1, x_2]$ irredutível.

Um *espaço topológico noetheriano* é um espaço topológico que satisfaz a condição de cadeia descendente para fechados, isto é, para toda cadeia de fechados $X_1 \supseteq X_2 \supseteq ...$ existe um natural n tal que $X_n = X_{n+1} = ...$ Por exemplo, $\mathbb{A}^n$ munido da topologia de Zariski é noetheriano, uma vez que a cada cadeia de conjuntos algébricos

$$V_1 \supseteq V_2 \supseteq ...$$

podemos associar a cadeia de ideais

$$\mathrm{I}(V_1) \subseteq \mathrm{I}(V_2) \subseteq ...,$$

que é estacionária, pois $K[x_1, ..., x_n]$ é um anel noetheriano, pelo teorema da base de Hilbert (ver Atiyah-Macdonald [[1], Teorema 7.5, página 81]). Em particular, todo subconjunto de um espaço topológico noetheriano é noetheriano e, portanto, toda variedade quase afim é um espaço topológico noetheriano munido da topologia de Zariski induzida.

Definimos a dimensão de uma variedade quase afim da seguinte maneira:

Definição 1.4. A *dimensão* de uma variedade quase afim X, denotada por $\dim X$, é o supremo dos inteiros n para os quais existe uma cadeia $X_0 \subsetneq ... \subsetneq X_n$ de fechados irredutíveis de X.

Exemplo 1.5. Todo conjunto unitário de $\mathbb{A}^n$ possui trivialmente dimensão zero. Reciprocamente, se $X \neq \emptyset$ é uma variedade quase afim de dimensão zero, então, dado $Q \in X$, como $\{Q\}$ é um fechado irredutível de X, a inclusão $\{Q\} \subseteq X$ implica $X = \{Q\}$, e, assim, concluímos que as variedades de dimensão zero são precisamente os conjuntos unitários.

Exemplo 1.6. Como as variedades de $\mathbb{A}^1$ são os conjuntos unitários e o próprio $\mathbb{A}^1$, a cadeia mais longa possível de variedades de $\mathbb{A}^1$ deve ser da forma $\{a\} \subsetneq \mathbb{A}^1$. Com isso, concluímos que $\dim \mathbb{A}^1 = 1$. Veremos a seguir que, mais geralmente, $\dim \mathbb{A}^n = n$.

Até agora, discutimos essencialmente as propriedades topológicas de variedades afins. Mostraremos como essas propriedades topológicas podem ser traduzidas algebricamente:

Definição 1.5. Seja $X \subseteq \mathbb{A}^n$ uma variedade afim, o *anel de coordenadas* de X é o conjunto

$$\Gamma(X) = \frac{K[x_1, ..., x_n]}{\mathrm{I}(X)}.$$

Pela proposição 1.5, $\mathrm{I}(X)$ é um ideal primo e, portanto, $\Gamma(X)$ é um domínio de integridade. A noção de dimensão de uma variedade afim pode ser traduzida para o contexto algébrico através da noção de dimensão de Krull de um anel:

Definição 1.6. A *altura* de um ideal primo P de um anel R, denotada por $h(P)$, é o supremo dos inteiros n para os quais existe uma cadeia $P_0 \subsetneq ... \subsetneq P_n = P$ de ideais primos de R. A *dimensão (de Krull)* de R é

$$\dim R = \sup\{h(P) \mid P \text{ ideal primo de } R\}.$$

Teorema 1.2. *Seja X uma variedade afim, então* $\dim X = \dim \Gamma(X)$.

Demonstração. Pela proposição 1.5 e pelo teorema dos zeros de Hilbert, os fechados irredutíveis de X estão em bijeção com os ideais primos de $K[x_1, ..., x_n]$ que contêm $\mathrm{I}(X)$, que, por sua vez, correspondem aos ideais primos de $\Gamma(X)$. Logo, $\dim X$ é o tamanho da maior cadeia possível de ideais primos de $\Gamma(X)$, que é igual a $\dim \Gamma(X)$.

□

Enunciamos a seguir um clássico resultado de Álgebra Comutativa:

Teorema 1.3. *Seja R um domínio que é uma K-álgebra finitamente gerada. Então,* $\dim R$ *é igual ao grau de transcendência do corpo de frações de R sobre K.*

Demonstração. Ver Matsumura [[10], Corolário 1, página 91].

□

Corolário 1.2. $\dim \mathbb{A}^n = n$

Demonstração. Pelo teorema 1.2, $\dim \mathbb{A}^n = \dim K[x_1, ..., x_n]$. Por sua vez, pelo teorema 1.3, temos que $\dim K[x_1, ..., x_n]$ é igual ao grau de transcendência de $K(x_1, ..., x_n)$ sobre K, que é igual a n.

□

1.3 Conjuntos algébricos projetivos

Se estamos interessados em discutir propriedades de interseção entre duas variedades, o espaço afim não é o melhor ambiente para fazê-lo. Definimos o n-espaço projetivo como o conjunto de "retas passando pela origem" em $\mathbb{A}^{n+1}$. Mais precisamente:

Definição 1.7. Sejam $(a_0, ..., a_n), (b_0, ..., b_n) \in \mathbb{A}^{n+1}(K)$, escrevemos

$$(a_0, ..., a_n) \sim (b_0, ..., b_n)$$

se existe $\lambda \in K\backslash\{0\}$ tal que $a_i = \lambda b_i$, para todo i. Essa relação é de equivalência e definimos o *n-espaço projetivo sobre K* como

$$\mathbb{P}^n(K) = \frac{\mathbb{A}^{n+1}\backslash\{(0, ..., 0)\}}{\sim}.$$

Quando estiver subentendido que o espaço é sobre K, escreveremos simplesmente $\mathbb{P}^n$. Denotamos a classe de equivalência de um elemento $(\alpha_0, ..., \alpha_n) \in \mathbb{A}^{n+1}\backslash\{(0, ..., 0)\}$ por $[\alpha_0 : ... : \alpha_n]$ e dizemos que $[\alpha_0 : ... : \alpha_n]$ são as *coordenadas homogêneas* de $(\alpha_0, ..., \alpha_n)$.

Construiremos uma topologia em $\mathbb{P}^n$ de maneira similiar à topologia de Zariski em $\mathbb{A}^n$, onde os fechados são os conjuntos algébricos. No entanto, para definir a noção de conjunto algébrico projetivo, precisamos dizer o que significa um ponto em $\mathbb{P}^n$ ser zero de um polinômio. Naturalmente, diremos que $\alpha \in \mathbb{P}^n$ é *raiz* de $f \in K[x_0, ..., x_n]$ se todo representante $Q \in \alpha$ é uma raiz de f no sentido usual.

Um polinômio não nulo em $K[x_0, ..., x_n]$ é dito *homogêneo de grau* $i \geq 0$ se é uma soma de monômios de grau i. Equivalentemente, um polinômio não nulo $f \in K[x_0, ..., x_n]$ é homogêneo de grau i, se, para todo $\lambda \in K$, temos que

$$f(\lambda x_0, ..., \lambda x_n) = \lambda^i f(x_0, ..., x_n).$$

É claro que um polinômio $f \in K[x_0, ..., x_n]$ de grau $m \geq 0$ pode ser escrito unicamente na forma $f = f_0 + ... + f_m$, onde $f_i = 0$ ou é homogêneo de grau i. Nesse caso, se $\alpha \in \mathbb{P}^n$ é raiz de f, concluímos que α é raiz de cada um dos f_i. De fato, se α não é raiz de um

algum f_i e $(a_0, ..., a_n) \in \mathbb{A}^n$ é um elemento da classe de α, então o polinômio

$$f(xa_0, ..., xa_n) = f_0(a_0, ..., a_n) + xf_1(a_0, ..., a_n) + ... + x^m f_m(a_0, ..., a_n)$$

é não nulo mas possui infinitas raízes, um absurdo. Assim, vemos que $\alpha \in \mathbb{P}^n$ é raiz de um polinômio se, e só se, esse polinômio é soma de polinômios homogêneos que são zerados por α e, com isso, somos motivados a definir:

Definição 1.8. Seja S um conjunto de polinômios homogêneos de $K[x_0, ..., x_n]$, o *conjunto algébrico projetivo de* S é o conjunto

$$\mathrm{Z}(S) = \{x \in \mathbb{P}^n \mid f(x) = 0, \forall f \in S\}.$$

Observação 1.1. Estamos utilizando a mesma notação para conjuntos algébricos afins e projetivos. Quando necessária uma distinção, escreveremos Z_a (resp. Z_p) para a aplicação afim (resp. projetiva).

Assim como no caso afim, se I é o ideal gerado pelos elementos de S, então facilmente se verifica que $\mathrm{Z}(S) = \mathrm{Z}(I)$ e, portanto, podemos pensar na aplicação Z definida no conjunto de ideais homogêneos de $K[x_0, ..., x_n]$, isto é, no conjunto dos ideais que são gerados por polinômios homogêneos. Além disso, as propriedades da proposição 1.1 com devidas alterações também são satisfeitas pela aplicação Z e podemos construir a *topologia de Zariski* em $\mathbb{P}^n$: os fechados de $\mathbb{P}^n$ são os conjuntos algébricos projetivos.

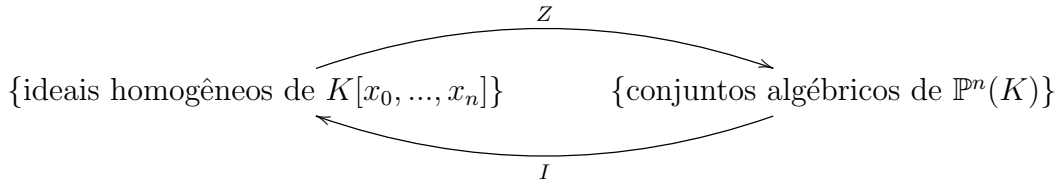
Em contraposição ao conceito de conjunto algébrico projetivo, temos a noção de ideal de um conjunto de pontos de $\mathbb{P}^n$:

Definição 1.9. Seja X um subconjunto de $\mathbb{A}^n(K)$, o *ideal homogêneo de* X é o ideal homogêneo $\mathrm{I}(X)$ de $K[x_0, ..., x_n]$ gerado pelo conjunto de polinômios

$$\{f \in K[x_0, ..., x_n] \mid f \text{ é homogêneo e } f(x) = 0, \forall x \in X\}.$$

Observação 1.2. Estamos utilizando o mesmo símbolo para o ideal de subconjuntos de $\mathbb{A}^n$ e $\mathbb{P}^n$. Quando necessária uma distinção, escreveremos I_a (resp. I_p) para a aplicação afim (resp. projetiva).

As propriedades da proposição 1.2 com devidas alterações são ainda satisfeitas por I. Além disso, utilizando argumentos análogos aos da demonstração do corolário 1.1, vemos que podemos encarar I como uma aplicação definida na classe dos conjuntos algébricos de $\mathbb{P}^n$:



As composições $\mathrm{I} \circ \mathrm{Z}$ e $\mathrm{Z} \circ \mathrm{I}$ no caso projetivo se comportam de forma similar ao caso afim:

Teorema 1.4. *Sejam $X \subseteq$ um conjunto algébrico e I um ideal homogêneo de $K[x_0, ..., x_n]$ com $\mathrm{Z}(I) \neq \emptyset$, então:*

(a) $\mathrm{Z}(\mathrm{I}(X)) = X$;

(b) $\mathrm{I}(\mathrm{Z}(I)) = \sqrt{I}$.

Demonstração. Para provar a primeira igualdade, antes de mais nada note que, pela definição de Z e I, temos que $\mathrm{Z}(\mathrm{I}(X)) \supseteq X$. Por outro lado, escrevendo $X = \mathrm{Z}(J)$, para algum ideal homogêneo J de $K[x_0, ..., x_n]$, temos que $\mathrm{I}(X) \supseteq J$ e, portanto, $\mathrm{Z}(\mathrm{I}(X)) \subseteq \mathrm{Z}(J) = X$.

Para provar a segunda igualdade, observe que

$$\begin{aligned} \mathrm{I}_p(\mathrm{Z}_p(I)) &= \mathrm{I}_a(\{(\alpha_0, ..., \alpha_n) \in \mathbb{A}^{n+1} \mid [\alpha_0 : ... : \alpha_n] \in V_p(I)\} \cup \{(0, ..., 0)\}) \\ &= \mathrm{I}_a(\mathrm{Z}_a(I)). \end{aligned}$$

Pelo teorema dos zeros de Hilbert, temos a igualdade do enunciado.

□

1.4 Variedades projetivas

Estaremos interessados em estudar conjuntos algébricos projetivos irredutíveis.

Definição 1.10. Uma *variedade projetiva* é um conjunto algébrico projetivo irredutível. Uma *variedade quase projetiva* é um aberto não vazio de uma variedade projetiva.

Como no caso afim, todo aberto não vazio de uma variedade projetiva é denso. Além disso, a irredutibilidade de um conjunto algébrico projetivo se traduz na primalidade de seu ideal homogêneo:

Proposição 1.6. *Um conjunto algébrico $X \subseteq \mathbb{P}^n$ é uma variedade se, e somente se,* $\mathrm{I}(X)$ *é um ideal primo de $K[x_0, ..., x_n]$.*

Demonstração. Segue utilizando argumentos similares aos da demonstração da proposição 1.5 e do fato de que, para checar se um ideal homogêneo I é primo, basta verificar se para quaisquer elementos homogêneos a e b, o produto $ab \in I$ implica $a \in I$ ou $b \in I$.

□

Como a toda cadeia descendente de fechados de $\mathbb{P}^n$ podemos associar uma cadeia ascendente de ideais de $K[x_0, ..., x_n]$, pelo teorema da base de Hilbert, concluímos que $\mathbb{P}^n$ munido da topologia de Zariski, assim como $\mathbb{A}^n$, é um espaço topológico noetheriano. Podemos também definir a noção de dimensão de uma variedade quase projetiva como no caso afim:

Definição 1.11. A *dimensão* de uma variedade quase projetiva X, denotada por $\dim X$, é o supremo dos inteiros n para os quais existe uma cadeia $X_0 \subsetneq ... \subsetneq X_n$ de fechados irredutíveis de X.

Uma maneira de traduzir algebricamente essa noção de dimensão é considerar o anel de coordenadas homogêneas de uma variedade projetiva:

Definição 1.12. Seja $X \subseteq \mathbb{P}^n$ uma variedade projetiva. O *anel de coordenadas homogêneas* de X é o conjunto

$$\Gamma(X) = \frac{K[x_0, ..., x_n]}{\mathrm{I}(X)}.$$

Observação 1.3. Como o contexto sempre deixará claro quando uma variedade está em $\mathbb{P}^n$ ou em $\mathbb{A}^n$, não deverá haver ambiguidade no uso do símbolo Γ.

Pela proposição 1.6, temos que o conjunto $\Gamma(X)$ é um domínio de integridade. Podemos calcular a dimensão de X a partir da dimensão de Krull de $\Gamma(X)$.

Teorema 1.5. *Seja X uma variedade projetiva, então* $\dim X = \dim \Gamma(X) - 1$.

Demonstração. Para cada $i = 0, ..., n$, podemos considerar a variedade quase projetiva

$$U_i = \{[\alpha_0 : ... : \alpha_n] \in \mathbb{P}^n \mid \alpha_i \neq 0\}$$

e a aplicação

$$\varphi_i : [\alpha_0 : ... : \alpha_n] \in U_i \mapsto \left(\alpha_0/\alpha_i, , ..., \widehat{\alpha_i/\alpha_i}, ..., \alpha_n/\alpha_i\right) \in \mathbb{A}^n,$$

onde $\widehat{\cdot}$ indica a omissão do i-ésimo termo. Essa função é um homeomorfismo (ver Hartshorne [[6], Proposição 2.2, página 10]) e, como a família $\{U_i\}$ obviamente cobre $\mathbb{P}^n$, vemos que

$$\dim X = \sup_i \{\dim \tilde{X}_i \mid \tilde{X}_i \neq \emptyset\} = \sup_i \{\dim X_i \mid X_i \neq \emptyset\},$$

onde $\tilde{X}_i$ e X_i denotam $X \cap U_i$ e $\varphi_i(X \cap U_i)$, respectivamente.

Observe que existe i tal que $\tilde{X}_i \neq \emptyset$. Para tal i, vemos que $x_i \notin \mathrm{I}(X)$ e, assim, podemos considerar a localização de $\Gamma(X)$ no conjunto de classes $\{1+\mathrm{I}(X),\ x_i+\mathrm{I}(X),\ x_i^2+\mathrm{I}(X),\ ...\}$, denotada por $\Gamma(X)_{x_i}$. Provaremos que

$$\Gamma(X)_{x_i} \cong \Gamma(X_i)[x_i,\ x_i^{-1}],$$

onde enxergamos os elementos de $\Gamma(X_i)$ como classes de polinômios nas variáveis x_j, $j \neq i$.

Primeiramente, note que, como $\mathrm{I}(X)$ é um ideal homogêneo, o quociente $\Gamma(X) = K[x_0, ...,\ x_n]/\mathrm{I}(X)$ possui naturalmente uma graduação, e, seja

$$(\Gamma(X)_{x_i})_0 = \left\{ \frac{f + \mathrm{I}(X)}{x_i^n + \mathrm{I}(X)} \mid n \in \mathbb{N},\ \mathrm{grau}(f + \mathrm{I}(X)) = n \right\}$$

o anel dos elementos de grau 0 da localização $\Gamma(X)_{x_i}$, temos que

$$\Gamma(X)_{x_i} = (\Gamma(X)_{x_i})_0[x_i + \mathrm{I}(X),\ x_i^{-1} + \mathrm{I}(X)].$$

Logo, para obter o isomorfismo desejado, basta mostrar que $(\Gamma(X)_{x_i})_0 \cong \Gamma(X_i)$. Para obter esse último isomorfismo, note que, por um lado, temos o homomorfismo $\psi_1 : (\Gamma(X)_{x_i})_0 \to \Gamma(X_i)$, dado por $\psi_1(x_i + \mathrm{I}(X)) = 1 + \mathrm{I}(X_i)$ e $\psi_1(x_j + \mathrm{I}(X)) = x_j + \mathrm{I}(X_i)$, $j \neq i$, e, por outro lado, temos o homomorfismo $\psi_2 : \Gamma(X_i) \to (\Gamma(X)_{x_i})_0$, dado por $\psi_2(x_j + \mathrm{I}(X_i)) = (x_j + \mathrm{I}(X))(x_i + \mathrm{I}(X))^{-1}$, $j \neq i$. É imediato verificar que as aplicações ψ_1 e ψ_2 são inversas uma da outra.

Por fim, observe que, pelo isomorfismo acima e pelos teoremas 1.2 e 1.3, se $X \cap U_i \neq \emptyset$, então

$$\dim X_i = \dim \Gamma(X_i) = \dim \Gamma(X_i)[x_i,\ x_i^{-1}] - 1 = \dim \Gamma(X)_{(x_i)} - 1 = \dim \Gamma(X) - 1$$

e isso conlui a demonstração.

□

Corolário 1.3. *Seja X uma variedade projetiva e sejam U_i, φ_i e X_i como na demonstração acima. Se $X_i \neq \emptyset$, então* $\dim X = \dim X_i$.

Corolário 1.4. $\dim \mathbb{P}^n = n$

Demonstração. Pelos teoremas 1.5 e 1.3,

$$\dim \mathbb{P}^n = \dim \Gamma(\mathbb{P}^n) - 1 = \dim K[x_0, ...,\ x_n] - 1 = n.$$

□

1.5 Morfismos

A partir de agora, utilizaremos o termo *variedade (sobre K)* para designar uma variedade afim, quase afim, projetiva ou quase projetiva (sobre K). Quando necessária a distinção, será especificado o tipo de variedade. Nosso objetivo é finalizar a construção da categoria das variedades definindo os morfismos dessa categoria. Para tal, introduzimos o conceito de função regular, primeiramente no caso afim e em seguida no caso projetivo:

Definição 1.13. Seja $X \subseteq \mathbb{A}^n$ uma variedade quase afim, uma função $f : X \to K$ é dita *regular em* $P \in X$ se existe um aberto $U \subseteq X$ com $P \in U$ e polinômios g, $h \in K[x_1, ..., x_n]$ tais que $h(Q) \neq 0$, para todo $Q \in U$, e $f = g/h$ em U. Diremos simplesmente que f é *regular* se o for em todo ponto de X.

Definição 1.14. Seja $X \subseteq \mathbb{P}^n$ uma variedade quase projetiva, uma função $f : X \to K$ é dita *regular em* $P \in X$ se existe um aberto $U \subseteq X$ com $P \in U$ e polinômios homogêneos g, $h \in K[x_1, ..., x_n]$ de mesmo grau tais que $h(Q) \neq 0$, para todo $Q \in U$, e $f = g/h$ em U. Diremos simplesmente que f é *regular* se o for em todo ponto de X.

Observação 1.4. Em geral dado um polinômio homogêneo a função de avaliação desse polinômio em um ponto de $\mathbb{P}^n$ não está bem-definida. No entanto, se g e h são polinômios homogêneos de mesmo grau, a função que associa cada $\alpha \in \mathbb{P}^n$ ao elemento $\mapsto g(\alpha)/h(\alpha) \in K$ está bem definida.

Se identificarmos K com $\mathbb{A}^1(K)$, temos que toda função regular em uma variedade é, em particular, contínua:

Proposição 1.7. *Seja X uma variedade. Se $f : X \to K$ é regular, então f é contínua.*

Demonstração. Suponha X uma variedade quase afim e seja Y um fechado de K. Vimos no exemplo 1.1 que Y é finito e, dessa forma, para ver que f é contínua, basta mostrar que, dado $a \in Y$, a imagem inversa $f^{-1}(a)$ é um fechado de X. De fato, como f é regular, para cada ponto $P \in X$ existe um aberto $U_P \subseteq X$ com $P \in U_P$ e polinômios g, h tais que h não se anula em U_P e $f = g/h$ em U_P e, nesse caso, temos que

$$f^{-1}(a) \cap U_P = \{Q \in U_P \mid g(Q)/h(Q) = a\} = \mathrm{Z}(g - ah) \cap U_P$$

é fechado em U_P. Por fim, como a família $\{U_P \mid P \in X\}$ é uma cobertura aberta de X, concluímos que $f^{-1}(a)$ é fechado em X.

A demonstração para o caso em que X é uma variedade quase projetiva é análoga.

□

Observação 1.5. Em particular, isso nos mostra que, sejam X uma variedade e U_1, U_2 abertos de X, se duas funções regulares $f_1 : U_1 \to K$ e $f_2 : U_2 \to K$ coincidem em algum

aberto não vazio $V \subseteq U_1 \cap U_2$, como todo aberto não vazio de uma variedade é denso e f_1 e f_2 são contínuas pela proposição acima, devemos ter que $f_1 = f_2$ em $U_1 \cap U_2$.

Definição 1.15. Sejam X e Y variedades, uma aplicação $\varphi : X \to Y$ será dita um *morfismo* se φ é contínua e, para todo aberto $U \subseteq Y$ e para toda função regular $f : U \to K$, a composição $f \circ \varphi : \varphi^{-1}(U) \to K$ é regular.

Em particular, a identidade $id_X : \alpha \in X \to \alpha \in X$ é um morfismo. Além disso, a composição de morfismos é ainda um morfismo e, portanto, a classe das variedades juntamente com a classe de morfismos entre essas variedades como definidos acima constitui, de fato, uma categoria. Nesse caso, temos a noção de isomorfismo:

Definição 1.16. Um morfismo de variedades $\varphi : X \to Y$ é dito um *isomorfismo* se existe um morfismo $\psi : Y \to X$ tal que $\varphi \circ \psi = id_Y$ e $\psi \circ \varphi = id_X$. Se, mais ainda, $X = Y$, dizemos que φ é um *automorfismo*. O conjunto de todos os automorfismos de X forma um grupo munido da composição de funções, o qual será denotado por $\mathrm{Aut}(X)$.

Até agora definimos e investigamos as propriedades topológicas dos morfismos entre variedades. Nosso próximo passo será traduzir essas propriedades algebricamente:

Definição 1.17. Seja X uma variedade, denotaremos por $\mathcal{O}(X)$ o anel das funções regulares em X. Sejam $P \in X$ e U_1, U_2 abertos de X contendo P, identificamos duas funções regulares $f_1 : U_1 \to K$ e $f_2 : U_2 \to K$ se $f_1 = f_2$ em $U_1 \cap U_2$. Nesse caso, escrevemos $f_1 \sim f_2$ e $\sim$ é uma relação de equivalência pela observação 1.5. Definimos o *anel local* de X em P como

$$\mathcal{O}_P(X) = \frac{\{f \text{ regular em uma vizinhança aberta de } P \text{ em } X\}}{\sim}.$$

Quando X estiver subentendida, escreveremos apenas $\mathcal{O}$ e $\mathcal{O}_P$ para denotar $\mathcal{O}(X)$ e $\mathcal{O}_P(X)$, respectivamente. Observe que, de fato, $\mathcal{O}_P$ é um anel. Além disso, se um elemento $f \in \mathcal{O}_P$ é invertível, então obviamente $f(P) \neq 0$. Reciprocamente, se $f(P) \neq 0$, como uma função regular é contínua, deve existir uma vizinhança aberta de U contendo P na qual f não se anula e, portanto, f é invertível. É imediato verificar que

$$\mathfrak{m}_P = \mathcal{O}_P \backslash \mathcal{O}_P^* = \{f \in \mathcal{O}_P \mid f(P) = 0\}$$

é um ideal de $\mathcal{O}_P$. Em particular, como todo ideal próprio está contido em $\mathcal{O}_P \backslash \mathcal{O}_P^* = \mathfrak{m}_P$, vemos que $\mathfrak{m}_P$ é maximal; mais ainda, é o único ideal maximal de $\mathcal{O}_P$, de onde segue que $\mathcal{O}_P$ é um anel local.

Exemplo 1.7. Se $X \subseteq \mathbb{A}^n$ é uma variedade afim, então $\mathcal{O}(X) \cong \Gamma(X)$. Além disso, para cada $P \in X$, temos que $\mathcal{O}(X)_P \cong \Gamma(X)_{M_P}$, onde M_P denota o ideal maximal das classes $f + \mathrm{I}(X) \in \Gamma(X)$ tais que $f(P) = 0$ (ver Hartshorne [[6], Teorema 3.2, página 17]).

Exemplo 1.8. Se $X \subseteq \mathbb{P}^n$ é uma variedade projetiva, então $\mathcal{O}(X) = K$, onde um elemento de K é identificado com uma função constante. Além disso, para cada $P \in X$, temos que $\mathcal{O}_P(X) \cong (\Gamma(X)_{M_P})_0$ onde M_P denota o ideal primo homogêneo gerado pelos elementos homogêneos $f + \mathrm{I}(X) \in \Gamma(X)$ tais que $f(P) = 0$ e $(\Gamma(X)_{M_P})_0$ denota o anel dos elementos homogêneos de grau zero da localização $\Gamma(X)_{M_P}$ (ver Hartshorne [[6], teorema 3.4, página 18]).

Finalmente, observe que, se duas variedades X e Y são isomorfas, então $\mathcal{O}(X)$ e $\mathcal{O}(Y)$ são ismomorfos como K-álgebras. De fato, se existe um isomorfismo $\varphi : X \to Y$, as aplicações $f \in \mathcal{O}(Y) \mapsto f \circ \varphi \in \mathcal{O}(X)$ e $f \in \mathcal{O}(X) \mapsto f \circ \varphi^{-1} \in \mathcal{O}(Y)$ são K-homomorfismos, um inverso do outro. No entanto, a recíproca é falsa em geral. Por exemplo, um subconjunto unitário de $\mathbb{P}^1$ e $\mathbb{P}^1$ são obviamente não isomorfos, mas seus anéis de funções regulares são ambos iguais a K, como mencionado no exemplo 1.8.

Um caso em que a recíproca é verdadeira é quando as variedades são afins. Mais geralmente:

Teorema 1.6. *Sejam X uma variedade qualquer e $Y \subseteq \mathbb{A}^n$ uma variedade afim. A aplicação $\alpha : \mathrm{Hom}(X, Y) \to \mathrm{Hom}_K(\Gamma(Y), \mathcal{O}(X))$, dada por $\alpha(\varphi) : f \in \Gamma(Y) \mapsto f \circ \varphi \in \mathcal{O}(X)$, é uma bijeção entre o conjunto dos morfismos de X em Y e o conjunto dos K-homomorfismos de $\Gamma(Y)$ em $\mathcal{O}(X)$.*

Demonstração. A aplicação α está bem-definida, pois Y é afim e, portanto, $\mathcal{O}(Y) \cong \Gamma(Y)$ (ver exemplo 1.7). Vamos construir uma inversa β para essa aplicação. Mais precisamente, dado um K-homomorfismo $f : \Gamma(Y) \to \mathcal{O}(X)$, denotamos $\xi_i = f(x_i)$ e definimos $\beta(f)$ como a aplicação de X em $\mathbb{A}^n$ dada por $\beta(f)(P) = (\xi_1(P), ..., \xi_n(P))$.

Afirmamos que $\beta(f)$ possui imagem em Y e é um morfismo. Para provar o primeiro fato, como $Y = \mathrm{Z}(\mathrm{I}(Y))$, basta mostrar que, para todo $P \in X$ e $h \in \mathrm{I}(Y)$, vale

$$h(\beta(f)(P)) = h(\xi_1(P), ..., \xi_n(P)) = 0,$$

mas isso realmente ocorre, pois f é K-homomorfismo e, portanto,

$$h(\xi_1(P), ..., \xi_n(P)) = f(h(x_1, ..., x_n))(P) = 0.$$

Por último, $\beta(f)$ é um morfismo, pois cada função coordenada ξ_i é regular (ver Hartshorne [[6], Lema 3.6, página 20]).

Finalmente, é fácil ver que, de fato, α e β são inversas uma da outra.

□

Corolário 1.5. *Duas variedades afins X e Y são isomorfas se e, só se, $\Gamma(X) \cong_K \Gamma(Y)$.*

Demonstração. Já vimos que, se X e Y são isomorfas, então $\mathcal{O}(X) \cong \mathcal{O}(Y)$. Como X e Y são afins, $\mathcal{O}(X) \cong \Gamma(X)$ e $\mathcal{O}(Y) \cong \Gamma(Y)$ e, portanto, $\Gamma(X) \cong \Gamma(Y)$.

Reciprocamente, seja $\varphi : \Gamma(X) \to \Gamma(Y)$ um K-isomorfismo, consideramos os morfismos $\alpha^{-1}(\varphi) : Y \to X$ e $\alpha^{-1}(\varphi^{-1}) : X \to Y$, onde α é a bijeção do teorema 1.6. Obviamente, um é inverso do outro e, portanto, X e Y são isomorfas.

□

1.6 Aplicações racionais

Na seção anterior, vimos que podemos associar a uma variedade afim um domínio que é uma K-álgebra finitamente gerada, a saber seu anel de coordenadas, e essa associação é funtorial no sentido de que duas variedades afins são isomorfas se, e só se, seus anéis de coordenadas são K-isomorfos. No entanto, o grupo $\mathrm{Aut}(X)$ de uma variedade qualquer não permite recuperar a variedade a menos de isomorfismo. Nessa seção, consideramos certas classes de equivalência de morfismos, as chamadas aplicações racionais dominantes, e veremos que a uma variedade qualquer podemos associar um corpo que é uma extensão finitamente gerada sobre K, o denominado corpo de funções da variedade, e essa construção é funtorial no sentido de que duas variedades são birracionalmente equivalentes se, e só se, seus corpos de funções são K-isomorfos.

Sejam X e Y variedades, consideramos o conjunto de todos os morfismos $f : U \to Y$, onde U é um aberto não vazio de X. Identificaremos morfismos $f_1 : U_1 \to Y$ e $f_2 : U_2 \to Y$ se $f_1 = f_2$ em $U_1 \cap U_2$ e, nesse caso, escreveremos $f_1 \sim f_2$. Observe que essa relação é de equivalência. De fato, pela definição, $f_1 \sim f_1$ e, se $f_1 \sim f_2$, então $f_2 \sim f_1$. Por fim, se $f_1 \sim f_2$ e $f_2 \sim f_3$, onde $f_3 : U_3 \to Y$, então $f_1 = f_3$ em $U_1 \cap U_2 \cap U_3$ e o lema abaixo garante que $f_1 = f_3$ em $U_1 \cap U_3$:

Lema 1.1. *Se dois morfismos $f, g : X \to Y$ coincidem em um aberto $U \subseteq X$, então $f = g$.*

Demonstração. Ver Hartshorne [[6], Lema 4.1, página 24].

□

Definição 1.18. Uma *aplicação racional* de X em Y é uma classe de equivalência definida acima. Seja φ um morfismo representante, denotamos essa classe por $\varphi : X \dashrightarrow Y$. Diremos que uma aplicação racional é *dominante* se, para algum aberto U no qual φ está definida, seu morfismo representante $\varphi : U \to Y$ possui imagem $\varphi(U)$ densa em Y.

Em particular, pelo lema acima, se algum representante da classe tiver imagem densa em Y, então qualquer outro representante possui essa propriedade. Além disso, observe que, em geral, a composição de duas aplicações racionais não está bem definida, mas a

composição de aplicações racionais dominantes está bem-definida e é ainda uma aplicação racional dominante. Dessa forma, faz sentido pensar na categoria constituída pelas variedades e as aplicações racionais dominantes.

Definição 1.19. Um isomorfismo na categoria das variedades e aplicações racionais dominantes é dito uma *aplicação birracional*. Um morfismo não constante no sentido da seção anterior será dito um *morfismo birracional* se sua aplicação racional dominante associada é birracional.

Observação 1.6. Para evitar confusões, a partir de agora, no contexto das variedades, reservaremos os termos morfismos, isomorfismos e automorfismos apenas para as aplicações definidas na seção anterior.

Para traduzir o conceito de aplicação racional algebricamente, precisamos introduzir a noção de corpo de funções de uma variedade:

Definição 1.20. Seja X uma variedade, identificamos duas funções regulares $f_1 : U_1 \to K$ e $f_2 : U_2 \to K$ se $f_1 = f_2$ em $U_1 \cap U_2$, onde U_1 e U_2 são abertos não vazios de X. Essa relação é de equivalência e seja $f : U \to K$ uma função regular, denotamos sua classe de equivalência por $f : X \dashrightarrow K$. Uma classe de equivalência é denominada uma *função racional* em X e o conjunto de todas as funções racionais em X é denominado o *corpo de funções* de X e será denotado por $\mathrm{K}(X)$.

Observação 1.7. Pela definição acima, para todo aberto não vazio $U \subseteq X$, devemos ter $\mathrm{K}(U) = \mathrm{K}(X)$.

Observe que $\mathrm{K}(X)$ possui uma estrutura natural de anel. Mais ainda, seja $f \neq 0$ uma função racional, onde $f : U \to K$ é uma função regular representante de sua classe, existe um aberto não vazio $V \subseteq U$ tal que f não se anula em V e, assim, vemos que $1/f$ é regular em V e, portanto, sua função racional associada é um inverso para f em $\mathrm{K}(X)$. Isso nos mostra que $\mathrm{K}(X)$ possui estrutura de corpo, como sugerido pelo seu nome.

Exemplo 1.9. Se X é uma variedade afim, então $\mathrm{K}(X) \cong \mathrm{Frac}(\Gamma(X))$, que é uma extensão finitamente gerada sobre K com grau de transcendência igual a $\dim X$ (ver Hartshorne [[6], Teorema 3.2, página 17]).

Exemplo 1.10. Se X é uma variedade projetiva, então $\mathrm{K}(X) \cong (\mathrm{Frac}(\Gamma(X)))_0$, que é uma extensão finitamente gerada sobre K com grau de transcendência igual a $\dim X$ (ver Hartshorne [[6], Teorema 3.4, página 18]).

Genericamente, diremos que uma variedade (não necessariamente no espaço afim) é afim se é isomorfa a uma variedade afim no sentido usual. Toda variedade possui uma cobertura aberta de variedades afins (ver Hartshorne [[6], Proposição 4.3, página 25]) e,

portanto, a demonstração de muitos resultados se reduz ao caso das variedades afins. Utilizaremos esse fato, por exemplo, para provar um análogo do teorema 1.6 para a categoria das variedades e as aplicações racionais dominantes:

Teorema 1.7. *Sejam X, Y variedades. A aplicação*

$$\alpha : \{\textit{aplicações racionais } X \dashrightarrow Y \textit{ dominantes}\} \to \mathrm{Hom}_K(\mathrm{K}(Y), \mathrm{K}(X))$$

dada por $\alpha(\varphi) : f \in \mathrm{K}(Y) \mapsto f \circ \varphi \in K(X)$ é uma bijeção.

Observação 1.8. A aplicação acima está bem-definida. De fato, para cada função racional $f : Y \dashrightarrow K$ e aplicação racional dominante $\varphi : X \dashrightarrow Y$, escolhendo uma função regular representante $f : V \to K$ e um morfismo representante $\varphi : U \to Y$, como φ é dominante, $\varphi^{-1}(V)$ é não vazio e $f \circ \varphi : \varphi^{-1}(V) \to K$ é uma função regular, de forma que temos uma função racional associada $f \circ \varphi \in \mathrm{K}(X)$.

Demonstração. Supomos primeiramente que Y é uma variedade afim. Como na demonstração do teorema 1.6, vamos construir uma inversa β para α, isto é, dado um K-homomorfismo $f : \mathrm{K}(Y) \to \mathrm{K}(X)$, vamos definir uma aplicação racional dominante $\beta(f) : X \to Y$. Sejam $y_1, ..., y_n$ os geradores de $\Gamma(Y)$ como K-álgebra, $f(y_1), ..., f(y_n) \in K(X)$ e existe um aberto $U \subseteq X$ tal que cada $f(y_i)$ é regular em U. Assim, f define um K-homomorfismo injetivo $f : \Gamma(Y) \to \mathcal{O}(U)$ que, pelo teorema 1.6, corresponde a um morfismo $\beta(f) : U \to Y$ e, portanto, a uma aplicação racional dominante $\beta(f) : X \dashrightarrow Y$. Obviamente, β e α como definidas são inversas uma da outra.

Para o caso geral, isto é, o caso em que Y não necessariamente é uma variedade afim, já observamos que podemos considerar uma cobertura aberta $\{Y_\lambda\}$ de Y, onde cada Y_λ é uma variedade afim. Fixado algum aberto Y_λ dessa cobertura, para cada aplicação racional $\alpha : X \dashrightarrow Y$, escolhendo um morfismo representante $\varphi : V \to Y$, onde V é um aberto de X, como φ é dominante, $\varphi(V) \cap Y_\lambda \neq \emptyset$ e, portanto, φ se restringe a um morfismo $\tilde{\varphi} : \varphi^{-1}(Y_\lambda) \to Y_\lambda$, que corresponde a uma aplicação racional (dominante) $\varphi_\lambda : X \dashrightarrow Y_\lambda$. Esse procedimento define uma aplicação sobrejetiva

$$\{\text{ap. racionais } X \dashrightarrow Y \text{ dominantes}\} \to \{\text{ap. racionais } X \dashrightarrow Y_\lambda \text{ dominantes}\},$$

que pelo lema 1.2 deve também ser injetiva. Por fim, pelo que provamos inicialmente e pelo fato de que $\mathrm{K}(Y) = \mathrm{K}(Y_\lambda)$ (ver observação 1.6), concluímos que existe uma bijeção entre o conjunto à direita e $\mathrm{Hom}_K(\mathrm{K}(Y), \mathrm{K}(X))$.

□

Corolário 1.6. *Duas variedades X e Y são birracionalmente equivalentes se, e só se,* $\mathrm{K}(X) \cong_K \mathrm{K}(Y)$.

Demonstração. Se existe uma aplicação birracional $\varphi : X \dashrightarrow Y$, pelo teorema acima, existem K-homomorfismos $\alpha(\varphi) : \mathrm{K}(Y) \to \mathrm{K}(X)$ e $\alpha(\varphi^{-1}) : \mathrm{K}(X) \to \mathrm{K}(Y)$, os quais são inversos um do outro e, portanto, $\mathrm{K}(Y) \cong_K \mathrm{K}(X)$. Reciprocamente, se existe um K-isomorfismo $f : \mathrm{K}(Y) \to \mathrm{K}(X)$, seja β como definida na demonstração do teorema acima, temos aplicações racionais $\beta(f) : X \dashrightarrow Y$ e $\beta(f^{-1}) : Y \dashrightarrow X$, que são inversas uma da outra, implicando X e Y birracionalmente equivalentes.

□

1.7 Curvas algébricas

A partir de agora, consideraremos uma classe especial de variedades:

Definição 1.21. Um *curva algébrica* é uma variedade $\mathcal{C}$ de dimensão 1. Se $\mathcal{C}$ for afim (resp. projetiva), diremos que $\mathcal{C}$ é uma *curva algébrica afim* (resp. *curva algébrica projetiva*).

Exemplo 1.11. Pelo corolário 1.4, $\mathbb{P}^1$ é uma curva algébrica, denominada *reta projetiva*.

Exemplo 1.12. Uma variedade da forma $\mathrm{Z}(f) \subseteq \mathbb{A}^2$, para algum $f \in K[X, Y]$ irredutível, é uma curva, dita uma *curva algébrica plana afim*.

Exemplo 1.13. Uma variedade da forma $\mathrm{Z}(F) \subseteq \mathbb{P}^2$, para algum $F \in K[X, Y, Z]$ homogêneo e irredutível, é uma curva, dita uma *curva algébrica plana projetiva*.

O corpo de funções de uma curva $\mathcal{C}$ é uma extensão finitamente gerada de K com grau de transcendência $\dim \mathcal{C} = 1$, e toda extensão de corpos finitamente gerada de um corpo perfeito (em particular, de um corpo algebricamente fechado) é separavelmente gerada (ver Matsumura [[10], Corolário, página 194]), isto é, existe $x \in \mathrm{K}(\mathcal{C})$ tal que $\mathrm{K}(\mathcal{C})/K(x)$ é uma extensão finita e separável. Dessa forma, pelo teorema do elemento primitivo, existe $y \in \mathrm{K}(\mathcal{C})$ algébrico sobre $\mathrm{K}(x)$ tal que $K(\mathcal{C}) = K(x, y)$ e, nesse caso, x e y satisfazem $f(x, y) = 0$, para algum polinômio irredutível f em duas variáveis com coeficientes em K. Isso implica

$$\mathrm{K}(\mathcal{C}) = K(x, y) \cong_K \mathrm{Frac}(\Gamma(\mathrm{Z}(f))) = \mathrm{K}(\mathrm{Z}(f)).$$

O corolário 1.6 nos fornece então que:

Proposição 1.8. *Toda curva algébrica é birracionalmente equivalente a uma curva plana afim.*

Dada uma curva algébrica plana afim $\mathcal{C} = \mathrm{Z}(f)$, $f \in K[X, Y]$, podemos considerar seu *fecho projetivo*, isto é, a curva algébrica plana projetiva $\overline{\mathcal{C}} = \mathrm{Z}(F)$, onde

$$F = Z^{\mathrm{grau}(f)} f(X/Z, Y/Z) \in K[X, Y, Z]$$

é a *homogeneização* de f. Podemos enxergar $\mathrm{K}(\mathcal{C}) = K(x, y)$, com $f(x, y) = 0$, e $\mathrm{K}(\overline{\mathcal{C}}) = K(x, y, z)$, com $F(x, y, z) = 0$. A aplicação $\mathrm{K}(\mathcal{C}) \to \mathrm{K}(\overline{\mathcal{C}})$, dada por $x \mapsto X/Z$ e $y \mapsto Y/Z$, define um isomorfismo $\mathrm{K}(\mathcal{C}) \cong_K \mathrm{K}(\overline{\mathcal{C}})$ e, pelo corolário 1.6, concluímos que:

Proposição 1.9. *Toda curva algébrica plana afim $\mathcal{C}$ é birracionalmente equivalente a seu fecho projetivo $\overline{\mathcal{C}}$.*

Observação 1.9. Reciprocamente, começando com uma curva algébrica plana projetiva $\mathrm{Z}(F)$, com $F \in K[X_1, X_2, X_3]$ homogêneo irredutível, podemos considerar, para cada variável X_i, sua *desomogeneização* $\mathrm{Z}(f_i)$, onde f_i é obtido fazendo $X_i = 1$ na expressão de F. Se $\mathrm{Z}(F) \neq \mathrm{Z}(X_i)$, então $\mathrm{Z}(f_i)$ é uma curva algébrica plana afim, cujo fecho projetivo é precisamente $\mathrm{Z}(F)$.

Definimos a noção de singularidade de uma curva algébrica plana de maneira análoga à definição de singularidade na topologia diferencial:

Definição 1.22. Seja $\mathcal{C} = \mathrm{Z}(f)$ uma curva algébrica plana afim, dizemos que $P \in \mathcal{C}$ é um ponto *singular* de $\mathcal{C}$ se $f_X(P) = f_Y(P) = 0$. Caso contrário, dizemos que P é *não singular*. Finalmente, diremos que $\mathcal{C}$ é não singular se todo ponto de $\mathcal{C}$ é não singular.

Podemos estender a noção de singularidade para uma curva algébrica plana projetiva da seguinte maneira: dizemos que $P \in \mathrm{Z}(F) \subseteq \mathbb{P}^2$, com $F \in K[X_1, X_2, X_3]$ homogêneo irredutível, é singular se $F_{X_1}(P) = F_{X_2}(P) = F_{X_3}(P) = 0$. Obviamente, se $P \notin \mathrm{Z}(X_i)$, então P é singular em $\mathrm{Z}(F)$ se, e só se, $\varphi_i(P)$ é singular em $\mathrm{Z}(f_i)$, com φ_i como no corolário 1.3,. Além disso, $\mathrm{Z}(F)$ é não singular se, e só se, cada desomogeneização $\mathrm{Z}(f_i)$ é não singular.

Um *domínio de valorização discreta* é um domínio de ideais principais R que também é um anel local, mas não é um corpo. Nesse caso, um gerador t de seu único ideal maximal $\mathfrak{m}$ é dito um *parâmetro local* e é fácil ver que todo elemento não nulo $z \in \mathrm{Frac}(R)$ pode ser escrito unicamente na forma $z = ut^n$, com $u \in R^*$ e $n \in \mathbb{Z}$ (ver Fulton [[4], Proposição 4, página 22]). Com isso, temos uma função, dita uma valorização discreta, $v : \mathrm{Frac}(R) \to \mathbb{Z} \cup \{\infty\}$, dada por $v(z) = n$, se $z = ut^n$, e $v(0) = \infty$. É imediato de sua definição que $v(ab) = v(a) + v(b)$ e que

$$v(a + b) \geq \min\{v(a), v(b)\}$$

Mais ainda, não é difícil verificar que, se $v(a) \neq v(b)$, então vale a igualdade na expressão acima. Por fim, notamos que

$$R = \{z \in \mathrm{Frac}(R) \mid v(z) \geq 0\},$$
$$R^* = \{z \in \mathrm{Frac}(R) \mid v(z) = 0\},$$
$$\mathfrak{m} = \{z \in \mathrm{Frac}(R) \mid v(z) > 0\}.$$

A não singularidade de um ponto P de uma curva algébrica plana afim $\mathcal{C}$ pode ser traduzida pelo anel local $\mathcal{O}_P(\mathcal{C})$ da seguinte forma:

Proposição 1.10. *Seja $\mathcal{C}$ uma curva algébrica plana afim. Um ponto $P \in \mathcal{C}$ é não singular se, e só se, $\mathcal{O}_P(\mathcal{C})$ é um domínio de valorização discreta.*

Demonstração. Ver Fulton [[4], Teorema 1, página 34].

□

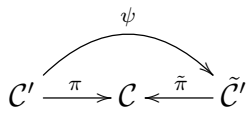
Esse resultado nos motiva a estender a noção de singularidade para uma curva algébrica qualquer da seguinte maneira:

Definição 1.23. Seja $\mathcal{C}$ uma curva algébrica, dizemos que $P \in \mathcal{C}$ é um ponto *não singular* de $\mathcal{C}$ se $\mathcal{O}_P(\mathcal{C})$ é um domínio de valorização discreta. Diremos que $\mathcal{C}$ é não singular se todo ponto for não singular.

Já vimos que estudar curvas algébricas sobre K a menos de equivalência birracional é estudar extensões de K finitamente geradas com grau de transcendência igual a 1. O que não é tão óbvio é que toda extensão finitamente gerada de K com grau de transcendência igual a 1 é K-isomorfa ao corpo de funções de alguma curva algébrica projetiva não singular:

Teorema 1.8. *Dada uma curva algébrica plana projetiva $\mathcal{C}$, existem uma curva algébrica projetiva não singular $\mathcal{C}'$ e um morfismo birracional $\pi : \mathcal{C}' \to \mathcal{C}$. Mais ainda, π é sobrejetivo e o par $(\mathcal{C}', \pi)$ é único no seguinte sentido: para todo outro par $(\tilde{\mathcal{C}}', \tilde{\pi})$, existe um único isomorfismo $\psi : \mathcal{C}' \to \tilde{\mathcal{C}}'$ tal que $\tilde{\pi} \circ \psi = \pi$.*

Demonstração. A unicidade segue do fato de que toda aplicação racional $X \dashrightarrow Y$, onde X é um curva não singular e Y é projetiva, se estende a um único morfismo $X \to Y$ (ver Fulton [[4], corolário 1, página 82]). De fato, dado um outro par $(\tilde{\mathcal{C}}', \tilde{\pi})$, existe uma equivalência birracional entre $\tilde{\mathcal{C}}'$ e $\mathcal{C}'$, que, pelo fato mencionado, se estende a um único isomorfismo $\psi : \mathcal{C}' \to \tilde{\mathcal{C}}'$ que faz o diagrama abaixo comutar:



A existência pode ser obtida, por exemplo, via *blow-up* (ver Fulton [[4], seção 7.3 e teorema 3, página 92]). □

A curva $\mathcal{C}'$ é dita um modelo projetivo não singular de $\mathcal{C}$. Para cada ponto $P \in \mathcal{C}$ não singular, existe um único $Q \in \mathcal{C}'$ tal que $\pi(Q) = P$. Isso, em geral, não é verdade para os pontos singulares de $\mathcal{C}$. Seja $P \in \mathcal{C}$ um ponto singular, dizemos que $Q \in \mathcal{C}'$ está *acima* de P, se $\pi(Q) = P$. É possível provar que acima de qualquer ponto singular de $\mathcal{C}$ existe no máximo um número finito de pontos de $\mathcal{C}'$. De fato, seja $f \in \mathcal{O}_P$ não nula com $f(P) = 0$, então, para todo ponto Q acima de P, como π é um morfismo, devemos ter que $f \circ \pi \in \mathcal{O}_Q \backslash \{0\}$ e $(f \circ \pi)(Q) = 0$. O resultado segue então do fato de que uma função racional não nula possui um número finito de zeros (ver proposição 2.1). Logo, podemos escrever

$$\mathcal{C}' = (\mathcal{C} - \{\text{pontos singulares}\}) \cup \{Q_1, ..., Q_n\}$$

onde Q_i são os pontos acima dos pontos singulares de $\mathcal{C}$.

Capítulo 2

Corpos de funções em uma variável

No capítulo anterior, vimos que duas curvas algébricas são birracionalmente equivalentes se, e só se, seus corpos de funções são K-isomorfos. Dessa forma, muitas respostas para perguntas sobre curvas e muitos invariantes birracionais de curvas podem ser obtidos estudando seus corpos de funções. Como um corpo de função de uma curva é uma extensão de corpos finitamente gerada F/K com grau de transcendência igual a 1, nesse capítulo investigamos os principais resultados sobre extensões desse tipo. Provaremos a maior parte dos resultados, apenas omitindo a demonstração de certos lemas ou resultados clássicos cujas demonstrações sejam muito longas. Nesse caso, fornecemos referências para suas provas e mais detalhes.

2.1 Corpos de funções e curvas algébricas

Lembramos que K denota um corpo algebricamente fechado fixo.

Definição 2.1. Um *corpo de funções em uma variável sobre* K (que, por simplicidade, chamaremos de um *corpo de funções*) é uma extensão F/K tal que $F/K(x)$ é uma extensão finita, para algum $x \in F \backslash K$. Um elemento de F é dito uma *função* e as funções $x \in K$ são ditas *constantes*. Dizemos que K é o corpo de constantes de F.

Em particular, $F/K(x)$ é finita para todo $x \in F$ transcendente sobre K. Mais ainda, isso caracteriza os elementos transcendentes sobre K, isto é, $x \in F$ é transcendente sobre K se, e só se, $F/K(x)$ é uma extensão finita.

A noção de corpo de funções acima está intimamente relacionada com a noção de corpo de funções de uma curva algébrica. Por um lado, já vimos que o corpo de funções de uma curva algébrica é um corpo de funções no sentido da definição acima. Por outro lado, se F/K é um corpo de funções em uma variável sobre K, como K é algebricamente fechado já havíamos observado que existem elementos $x, y \in F$ tais que $F = K(x, y)$ e $f(x, y) = 0$, para algum polinômio f em duas variáveis sobre K e, nesse caso, F é o

corpo de funções da curva algébrica plana $\mathrm{Z}(f) \subseteq \mathbb{A}^2$. Em particular, tomando o modelo projetivo não singular do fecho projetivo $\overline{\mathrm{Z}(f)}$, temos que todo corpo de funções F/K como na definição acima é o corpo de funções de alguma curva algébrica projetiva não singular X.

Essa construção garante uma equivalência entre a categoria das curvas algébricas projetivas não singulares e morfismos não constantes e a categoria dos corpos de funções em uma variável e K-homomorfismos. Dessa forma, vários conceitos e resultados podem ser traduzidos de uma categoria para a outra. Por exemplo, existe uma bijeção entre o conjunto dos pontos $P \in X$ e o conjunto dos ideais maximais dos anéis de valorização $\mathcal{O}_P$ de F/K, o qual sabemos serem anéis de valorização discreta (ver Fulton [[4], Corolário 4, página 82]).

Por simplicidade, denotaremos esses ideais maximais também por P e diremos que P é um *lugar* de F/K. Para cada lugar P de F/K, temos uma valorização discreta $v_P : F \to \mathbb{Z} \cup \{\infty\}$, definida como antes. Lembramos que temos as caracterizações:

$$\mathcal{O}_P = \{x \in F \mid v_P(x) \geq 0\},$$
$$P = \{x \in F \mid v_P(x) > 0\}.$$

Vamos fixar alguns termos novos:

Definição 2.2. Diremos que um lugar P é um *zero* de $x \in F$ se $v_P(x) > 0$. Se $v_P(x) < 0$, diremos que P é um *polo* de x.

Uma consequência do lema de Zorn é que toda função não constante $x \in F$ possui pelo menos um zero e um polo (ver Stichtenoth [[14], corolário I.1.19, página 8]). Por outro lado, toda função não nula deve ter no máximo um número finito de polos e zeros. Mais precisamente, não é difícil provar que:

Proposição 2.1. *Sejam $P_1, ..., P_n$ zeros distintos de $x \in F$. Então,*

$$\sum_{i=1}^{n} v_{P_i}(x) \leq [F : K(x)].$$

Demonstração. Ver Stichtenoth [[14], proposição I.3.3, página 13].

□

Mais a frente, provaremos que, se $P_1, ..., P_n$ são todos os zeros de x, vale a igualdade.

2.2 Divisores

Consideraremos certas somas formais entre os lugares de um certo corpo de funções F/K. No contexto de curvas, esses elementos são somas formais entre os pontos de um

modelo projetivo não singular X com corpo de funções $\mathrm{K}(X) = F$. Utilizaremos esses objetos para definir um importante invariante birracional de uma curva algébrica, seu gênero.

Definição 2.3. Definimos o *grupo de divisores* de F/K, denotado por $\mathrm{Div}(F/K)$, como o grupo abeliano livre gerado pelos lugares de F/K. Um elemento $D \in \mathrm{Div}(F/K)$, dito um *divisor* de F/K, é, portanto, uma soma formal

$$D = \sum_{P \text{ lugar}} n_P P,$$

onde $n_P \in \mathbb{Z}$ e $n_P = 0$, para quase todos os (isto é, todos exceto uma quantidade finita de) lugares P. Definimos seu *grau* como

$$\operatorname{grau} D = \sum_{P \text{ lugar}} n_P.$$

O elemento neutro de $\mathrm{Div}(F/K)$ será denotado por 0 e corresponde ao divisor com $n_P = 0$, para todo lugar P. Um divisor da forma $D = P$, para algum lugar P, é dito um *divisor primo*.

Como toda função não nula $x \in F$ possui um número finito de zeros e polos (ver proposição 2.1), podemos associar a x um divisor

$$(x) = \sum_{P \text{ lugar}} v_P(x) P.$$

Um divisor $D \in \mathrm{Div}(F/K)$ da forma $D = (x)$, para alguma função não nula $x \in F$, é dito um *divisor principal*. Sem dificuldades, se verifica que o conjunto dos divisores principais juntamente com o divisor nulo forma um subgrupo $\mathcal{P}(F/K)$ de $\mathrm{Div}(F/K)$. O quociente $\mathrm{Div}(F/K)/\mathcal{P}(F/K)$ é conhecido como o *grupo de classes de divisores* de F/K. A classe de cada divisor D nesse quociente será denotada por $[D]$ e escreveremos $D_1 \sim D_2$ se $[D_1] = [D_2]$.

Para introduzir o conceito de gênero de um corpo de funções, precisamos definir um novo objeto:

Definição 2.4. Sejam $D_1 = \sum n_P P$ e $D_2 = \sum m_P P$ divisores de F/K, escreveremos $D_1 \geq D_2$ se $n_P \geq m_P$, para todo lugar P. Para cada $D \in \mathrm{Div}(F/K)$, definimos

$$L(D) = \{x \in F \backslash \{0\} \mid (x) + D \geq 0\} \cup \{0\}.$$

É imediato da definição acima que se $D = \sum n_P P$, então $x \in F$ não nulo é um elemento de $L(D)$ se, e somente se, $v_P(x) \geq -n_P$, para todo lugar P. Em particular,

com isso vemos que, para um divisor primo P e um natural positivo n, $L(nP)$ consiste da função nula e de todas as funções $x \in F$ tais que x possui polo apenas em P com $v_P(x) \geq -n$. Além disso, como toda função não constante deve ter um polo, temos que $L(0) = K$ e $L(A) = \{0\}$, para todo $A < 0$.

Observe também que o conjunto $L(D)$ como definido acima possui estrutura de K-subespaço de F. De fato, $L(D) \neq \emptyset$ e, para quaisquer duas funções $x, y \in L(D)$ e $k \in K$, temos que, para todo lugar P, $v_P(x-y) \geq \min\{v_P(x), v_P(y)\} \geq -n_P$ e $v_P(kx) = v_P(k)+v_P(x) = v_P(x) \geq -n_P$. Mais ainda, provamos que $L(D)$ é um espaço de dimensão finita, a qual denotaremos por $l(D)$.

Lema 2.1. *Sejam D_1, D_2 divisores em F/K:*

(a) *Se $D_1 \sim D_2$, então $L(D_1) \cong_K L(D_2)$;*

(b) *Se $D_1 \leq D_2$, então $L(D_1) \subseteq L(D_2)$ e $\dim(L(D_2)/L(D_1)) \leq \operatorname{grau} D_2 \operatorname{grau} D_1$.*

Demonstração. Para provar o item (a), observe que, pondo $D_1 = D_2 + (x)$, para alguma função não nula $x \in F$, temos que, para toda função $y \in L(D_1)$, a função $xy \in F$ satisfaz $(xy) + D_2 = (y) + (x) + D_2 = (y) + D_1 \geq 0$. Assim, temos uma aplicação $y \in L(D_1) \mapsto xy \in L(D_2)$, a qual verifica-se imediatamente ser o K-isomorfismo desejado.

A inclusão $L(D_1) \subseteq L(D_2)$ do item (b) é óbvia. Para provar a última desigualdade, podemos assumir $D_2 = D_1 + Q$, para algum divisor primo Q e o caso geral segue por indução. Escrevendo $D_2 = \sum n_P P$ e $D_1 = \sum m_P P$, podemos tomar $t \in F$ com $v_Q(t) = n_Q = m_Q + 1$ e, nesse caso, para cada $x \in L(D_1)$, temos que $v_Q(xt) = v_Q(x) + v_Q(t) = v_Q(x) + n_Q \geq 0$. Dessa forma, obtemos uma aplicação K-linear $x \in L(D_2) \mapsto xt + Q \in \mathcal{O}_Q/Q$. Seu núcleo é o conjunto das funções $x \in L(D_2)$ com $v_Q(xt) > 0$, o qual verifica-se facilmente ser $L(D_1)$. Finalmente, como K é algebricamente fechado e $\mathcal{O}_Q/Q$ é uma K-álgebra finitamente gerada e um corpo contendo uma cópia de K, temos que $\mathcal{O}_Q/Q \cong K$ (ver Fulton [[4], Proposição 4, página 15]) e consequentemente

$$\dim(L(D_1)/L(D_2)) \leq \dim \mathcal{O}_Q/Q = 1 = \operatorname{grau} D_2 - \operatorname{grau} D_1.$$

□

Proposição 2.2. *Seja D um divisor em F/K, existem únicos divisores D_+, $D_- \geq 0$ tais que $D = D_+ - D_-$ e, nesse caso,*

$$l(D) \leq \operatorname{grau} D_+ - 1.$$

Demonstração. A existência e unicidade da escrita $D = D_+ - D_-$ é óbvia. Para provar a desigualdade do enunciado, observe que, como $D \leq D_+$, pelo lema anterior, $L(D) \subseteq$

$L(D_+)$ e, portanto, basta mostrar que $l(D_+) \leq \text{grau}(D_+) + 1$. De fato, ainda pelo lema anterior, temos que

$$l(D_+) - 1 = \dim(L(D_+)/L(0)) \leq \text{grau}\, D_+.$$

□

No caso em que $D = (x)$ é um divisor principal, vamos denotar D_+ e D_- por $(x)_0$ e $(x)_\infty$, respectivamente. Diremos que $(x)_\infty$ e $(x)_0$ são respectivamente o divisor de zeros e o divisor de polos de x em F/K.

Observe que a proposição 2.1 nos informa que $\text{grau}(x)_0$, $\text{grau}(x)_\infty \leq [F : K(x)]$. A seguir, provamos que, para uma função não constante, vale a igualdade:

Teorema 2.1. *Seja $x \in F\backslash K$, então* $\text{grau}(x)_0 = \text{grau}(x)_\infty = [F : K(x)]$.

Demonstração. Como $(x)_0 = (x^{-1})_\infty$, basta mostrar que para uma função não constante $x \in F$, vale a igualdade $\text{grau}(x)_\infty = [F : K(x)]$. Além disso, observe que, pela proposição 2.1, já temos a desigualdade $\text{grau}(x)_\infty \leq [F : K(x)]$ e, portanto, falta mostrar que $\text{grau}(x)_\infty \geq [F : K(x)]$.

Para tal, sejam $n = [F : K(x)]$ e $\{x_1, ..., x_n\}$ uma base F sobre $K(x)$, consideramos um divisor $D \geq 0$ tal que $(x_i) \geq -D$, para todo i. Observe que, para todo natural m, os elementos $x^i x_j \in L((x^m)_\infty + D)$, com $i = 0, ..., m$ e $j = 1, ..., n$, são linearmente independentes sobre K, uma vez que os x_j são linearmente independentes sobre $K(x)$, e, portanto:

$$l((x^m)_\infty + D) \geq (m + 1)n.$$

Mais ainda, pela proposição 2.2, para todo natural m temos a desigualdade

$$\text{grau}(x^m)_\infty + \text{grau}(D) + 1 \geq (m + 1)n,$$

que pode ser reescrita como

$$m(\text{grau}(x)_\infty - n) \geq n - \text{grau}(D) - 1.$$

Por fim, como a desigualdade acima vale para todo natural m, fazendo $m \to \infty$, concluímos que $\text{grau}(x)_\infty - n \geq 0$.

□

Como consequência desse teorema, temos que todo divisor principal possui grau 0 e, portanto, se $D_1 \sim D_2$, não só temos que $l(D_1) = l(D_2)$, mas também $\text{grau}\, D_1 = \text{grau}\, D_2$. Isso, por exemplo, nos permite provar que:

Corolário 2.1. *Se* $\operatorname{grau} D < 0$*, então* $l(D) = 0$.

Demonstração. De fato, se $l(D) > 0$, existe $x \in L(D)$, $x \neq 0$ tal que $D' := (x) + D \geq 0$. Nesse caso, $D' \sim D$ e, pelo que já observamos, $\operatorname{grau}(D) = \operatorname{grau}(D') \geq 0$.

□

Finalmente, definimos a noção de gênero de um corpo de funções e provamos o teorema de Riemann, um primeiro passo importante para a demonstração de um dos principais teoremas desse capítulo, o teorema de Riemann-Roch.

Definição 2.5. Definimos o *gênero* de um corpo de funções F/K como

$$g = \sup\{\operatorname{grau}(D) - l(D) + 1 \mid D \in \operatorname{Div}(F/K)\}.$$

Observação 2.1. Antes de mais nada, observe que esse valor é sempre não negativo, uma vez que $\operatorname{grau}(0) - l(0) + 1 = 0$. Não é difícil mostrar também que g é sempre finito (ver Stichtenoth [[14], proposição I.4.14, página 20]).

Teorema 2.2 (**Teorema de Riemann**)**.** *Seja* F/K *um corpo de funções de gênero* g*. Então,* $l(D) \geq \operatorname{grau} D + 1 - g$*, para todo divisor* D*, e existe um natural* $c \in \mathbb{N}$ *(que depende de* F/K*) tal que*

$$l(D) = \operatorname{grau} D + 1 - g,$$

para todo $D \in Div(F/K)$ *com* $\operatorname{grau} D \geq c$.

Demonstração. A primeira desigualdade segue imediatamente da definição de g. Para provar a segunda afirmação, observe que, como g é finito, podemos escolher um divisor D_0 tal que $l(D_0) = \operatorname{grau} D_0 + 1 - g$. Nesse caso, tome $c = \operatorname{grau} D_0 + g$ e, pela definição do gênero, precisamos mostrar que, se D é um divisor com $\operatorname{grau} D > c$, então $l(D) \leq \operatorname{grau} D + 1 - g$. Para tal, primeiramente, note que

$$l(D - D_0) \geq \operatorname{grau}(D - D_0) + 1 - g \geq c - \operatorname{grau} D_0 + 1 - g = 1.$$

Portanto, existe uma função não nula $x \in L(D - D_0)$ e, pondo $D' = D + (z) \geq D_0$, obtemos que

$$\operatorname{grau} D - l(D) = \operatorname{grau} D' - l(D') \geq \operatorname{grau} D_0 - l(D_0) = g - 1,$$

como queríamos mostrar.

□

2.3 Divisores canônicos e o teorema de Riemann-Roch

Nessa seção, consideramos uma importante classe de divisores, que nos permitirá obter uma expressão para a dimensão $l(D)$ em função do grau de D e o gênero g, bem como o menor valor da constante c do teorema de Riemann.

Definição 2.6. Um *adele* de F/K é uma aplicação $\alpha : \{\text{lugares de } F/K\} \to F$ tal que $\alpha(P) \in \mathcal{O}_P$, para quase todos os lugares P de F/K. Por simplicidade, escreveremos $\alpha = (\alpha_P)$ para denotar o adele $\alpha : P \mapsto \alpha_P$.

Observe que o conjunto dos adeles de F/K, denotado por $\mathcal{A}_F$, possui naturalmente uma estrutura de K-espaço vetorial onde $k(\alpha_P)$, com $k \in K$ é definido como a aplicação $P \mapsto k\alpha_P$, que, de fato, é um adele, pois, se $\alpha_P \in \mathcal{O}_P$, como $v_P(k) = 0$, devemos ainda ter $k\alpha_P \in \mathcal{O}_P$. Mais ainda, como uma função $x \in F$ possui um número finito de polos, a multiplicação $x(\alpha_P)$ pode ser definida da mesma forma e ainda será um adele, de onde segue que $\mathcal{A}_F$ também possui estrutura de F-espaço vetorial. O mesmo argumento também nos permite ver que a aplicação constante $P \mapsto x$ é um adele, dito um *adele principal*, e, assim, temos uma inclusão $F \hookrightarrow \mathcal{A}_F$.

Definição 2.7. Para cada lugar P e adele α, definimos $v_P(\alpha) = v_P(\alpha_P)$. Para cada divisor $D = \sum n_P P$, definimos

$$\mathcal{A}_F(D) = \{\alpha \in \mathcal{A}_F \mid v_P(\alpha) + n_P \geq 0\}.$$

Observe que $\mathcal{A}_F(D)$ é um K-subespaço de $\mathcal{A}_F$. A seguir, mostramos que podemos interpretar o gênero como a dimensão sobre K de $\mathcal{A}_F/(\mathcal{A}_F(0) + F)$.

Lema 2.2.

(a) *Sejam D_1 e D_2 divisores com $D_1 \leq D_2$. Então, $\mathcal{A}_F(D_1) \subseteq \mathcal{A}_F(D_2)$ e*

$$\dim\left(\frac{\mathcal{A}_F(D_2) + F}{\mathcal{A}_F(D_1) + F}\right) = (\text{grau}(D_2) - l(D_2)) - (\text{grau}(D_1) - l(D_1)).$$

(b) *Se D é um divisor com $l(D) = \text{grau}\, D + 1 - g$, então $\mathcal{A}_F = \mathcal{A}_F(D) + F$.*

Demonstração. Ver Stichtenoth [[14], teorema I.5.4, página 23].

□

Teorema 2.3. *Para todo divisor D, temos que*

$$l(D) - \text{grau}\, D + g - 1 = \dim\left(\frac{\mathcal{A}_F}{\mathcal{A}_F(D) + F}\right).$$

Demonstração. Seja D um divisor qualquer, pelo teorema de Riemann, existe um divisior $D_0 \geq D$ tal que $l(D_0) = \text{grau}\, D_0 + 1 - g$. Pelo lema anterior, $\mathcal{A}_F = \mathcal{A}_F(D_0) + F$ e

$$\begin{aligned}\dim\left(\frac{\mathcal{A}_F}{\mathcal{A}_F(D)+F}\right) &= (\text{grau}\, D_0 - l(D_0)) - (\text{grau}\, D - l(D)) \\ &= l(D) - \text{grau}\, D + g - 1.\end{aligned}$$

□

Finalmente, introduzimos o conceito de uma diferencial de Weil e associamos a cada um desses objetos um divisor:

Definição 2.8. Uma *diferencial de Weil* de F/K é uma aplicação K-linear $\omega : \mathcal{A}_F \to K$ que se anula em $\mathcal{A}_F(D) + F$, para algum divisor D. Denotamos o conjunto de todas as diferenciais de Weil de F/K por Ω_F.

Se ω_1 e ω_2 são diferenciais de Weil, digamos se anulando em $\mathcal{A}_F(D_1)+F$ e $\mathcal{A}_F(D_2)+F$, respectivamente, e $k \in K$, então $k\omega_1 - \omega_3$ é uma diferencial de Weil, que se anula em $\mathcal{A}_F(D_3) + F$, para qualquer divisor D_3 com $D_3 \leq D_1$ e $D_3 \leq D_2$. Assim, vemos que Ω_F possui estrutura natural de K-espaço vetorial.

Além disso, para cada divisor D, o conjunto

$$\Omega_F(D) = \{\omega \in \Omega_F \mid \omega \text{ se anula em } \mathcal{A}_F(D) + F\}$$

é um K-subespaço de Ω_F naturalmente isomorfo ao dual de $\mathcal{A}_F/(\mathcal{A}_F(D)+F)$ e, portanto, de dimensão $l(D) - \text{grau}\, D + g - 1$. Em particular, o conjunto $\Omega_F(0)$, cujos elementos são denominados *diferenciais holomorfas*, é um K-espaço vetorial de dimensão g. Isso nos fornece uma nova interpretação para o gênero.

Observe também que Ω_F possui estrutura de F-espaço vetorial, definindo o produto $x\omega$ como a aplicação dada por $x\omega(\alpha) = \omega(x\alpha)$. De fato, se uma diferencial de Weil ω se anula em $\mathcal{A}_F(D) + F$, para algum divisor D, então $x\omega$ é uma aplicação K-linear que se anula em $\mathcal{A}_F(D + (x)) + F$. Não é difícil mostrar que:

Proposição 2.3. *Ω_F é um F-espaço vetorial de dimensão* 1.

Demonstração. Ver Stichtenoth [[14], proposição I.5.9, página 26].

□

Provamos a seguir um importante fato que nos motivará a associar a cada diferencial de Weil um divisor de F/K:

Proposição 2.4. *Para cada $\omega \in \Omega_F$ não nula, o conjunto*

$$M(\omega) = \{D \in \text{Div}(F/K) \mid \omega \textit{ se anula em } \mathcal{A}_F(D) + F\}$$

é não vazio e existe um divisor $W \in M(\omega)$ tal que $D \leq W$, para todo $D \in M(\omega)$.

Demonstração. Pela definição de diferencial de Weil, o conjunto $M(\omega)$ é não vazio. Seja c a constante do teorema de Riemann, observe que, para todo divisor $D \in M(\omega)$, devemos ter grau $D < c$, pois, caso contrário, pelo teorema de Riemann, $\dim(\mathcal{A}_F/(\mathcal{A}_F(D)+F)) = l(D) - \text{grau}\, D + g - 1 = 0$ e $D \notin M(\omega)$. Logo, podemos escolher um divisor $W \in M(\omega)$ de grau máximo e afirmamos que W possui a propriedade desejada.

De fato, escreva $W = \sum n_P P$ e suponha que exista $D \in M(\omega)$, digamos $D = \sum m_P P$, tal que $m_Q > n_Q$, para algum lugar Q. Consideramos um adele $\alpha = (\alpha_P) \in \mathcal{A}_F(W+Q)$ e decompomos $\alpha = \alpha_1 + \alpha_2$, onde α_1 (resp. α_2) é o adele dado por $\alpha_1(Q) = 0$ (resp. $\alpha_2(Q) = \alpha_Q$) e $\alpha_1(P) = \alpha_P$ (resp. $\alpha_2(P) = 0$), para lugares $P \neq Q$. É imediato ver que $\alpha_1 \in \mathcal{A}_F(W)$ e $\alpha_2 \in \mathcal{A}_F(D)$ e, portanto, $\omega(\alpha) = \omega(\alpha_1) + \omega(\alpha_2) = 0$. Em particular, isso nos mostra que $W + Q \in M(\omega)$, contradizendo a maximalidade do grau de W.

□

Claramente o divisor da proposição acima é único e, assim, a cada diferencial de Weil não nula ω, associamos o divisor W como no enunciado da proposição acima, o qual será denotado por (ω). Um divisor da forma (ω) para alguma diferencial de Weil não nula ω é dito um *divisor canônico*. Se $(\omega) = \sum n_P P$, definimos, para cada lugar P, $v_P(\omega) = n_P$ e dizemos que P é um zero (resp. polo) de ω se $v_P(\omega) > 0$ (resp. < 0).

Podemos verificar que:

Lema 2.3.

(a) $\Omega_F(D) = \{\omega \in \Omega \mid \omega = 0 \text{ ou } (\omega) \geq D\}$;

(b) $(x\omega) = (x) + (\omega)$, *para todo* $x \in F\backslash\{0\}$ *e* $\omega \in \Omega_F\backslash\{0\}$;

(c) *Se* W_1 *e* W_2 *são divisores canônicos, então* $W_1 \sim W_2$.

Demonstração. As afirmações em (a) e (b) decorrem da definição do divisor associado a uma diferencial de Weil. Para provar a propriedade em (c), basta observar que, escrevendo $W_1 = (\omega_1)$ e $W_2 = (\omega_2)$, para certas diferenciais de Weil não nulas ω_1 e ω_2, como Ω_F é um espaço de dimensão 1 sobre F, existe $x \in F$ não nulo tal que $\omega_1 = x\omega_2$. Nesse caso, pela propriedade em (b), vemos que

$$W_1 = (\omega_1) = (x\omega_2) = (x) + \omega_2 = (x) + W_2,$$

isto é, $W_1 \sim W_2$.

□

Finalmente, provamos o teorema de Riemann-Roch:

Teorema 2.4 (**Teorema de Riemann-Roch**). *Sejam D um divisor de F/K e W um divisor canônico, então*

$$l(D) = \text{grau}(D) + 1 - g + l(W - D).$$

Demonstração. Como $l(D) - \text{grau}(D) - 1 + g$ é a dimensão sobre K de $\Omega_F(D)$, basta mostrar que $L(W-D) \cong_K \Omega_F(D)$. Para construir esse isomorfismo, como W é um divisor canônico, considere primeiramente uma diferencial de Weil ω tal que $W = (\omega)$ e observe que, se $x \in L(W - D)$, $x \neq 0$, então

$$(xw) = (x) + (\omega) = (x) + W \geq D$$

implicando $x\omega \in \Omega_F(D)$. Assim, temos a aplicação $\varphi : L(W - D) \to \Omega_F(D)$ dada por $\varphi(x) = x\omega$. Essa aplicação é obviamente K-linear e injetiva. Para verificar sua sobrejetividade, note que, dada uma diferencial de Weil $\omega' \in \Omega_F(D)$, como Ω_F é um espaço vetorial de dimensão 1 sobre F, devemos ter que $\omega' = x\omega$, para algum $x \in F$. Finalmente, como

$$(x) + W = (x) + (\omega) = (x\omega) = (\omega') \geq D,$$

vemos que $x \in L(W - D)$ e, portanto, $\omega' = \varphi(x)$.

□

Corolário 2.2. *Um divisor W de F/K é um divisor canônico se, e só se,*

$$\text{grau}\, W = 2g - 2 \quad e \quad l(W) = g.$$

Demonstração. Por um lado, se W é canônico, então pelo teorema de Riemann-Roch, temos que:

$$l(W) = l(W - 0) = l(0) - \text{grau}\, 0 - 1 + g = g,$$
$$\text{grau}\, W = l(W) - 1 + g - l(W - W) = 2g - 2.$$

Reciprocamente se W é um divisor com $\text{grau}\, W = 2g-2$ e $l(W) = g$, então, consideramos um divisor canônico W' de F/K e, pelo teorema de Riemann-Roch, vemos que

$$l(W - W') = l(W) - \text{grau}\, W + g - 1 = 1.$$

Nesse caso, existe uma função não nula $x \in L(W - W')$ satisfazendo $(x) + W - W' \geq 0$.

Como

$$\text{grau}((x) + W - W') = \text{grau}\, W - \text{grau}\, W' = 0,$$

concluímos que $(x) + W - W' = 0$, isto é, $W = W' + (x^{-1})$. Escrevendo $W' = (\omega)$, para alguma diferencial de Weil não nula, vemos que $W = (x^{-1}\omega)$ e, portanto, W é um divisor canônico.

□

Corolário 2.3. *Seja D um divisor de F/K. Se* $\text{grau}\, D \geq 2g - 1$*, então*

$$l(D) = \text{grau}\, D + 1 - g.$$

Demonstração. Se $\text{grau}\, D \geq 2g-1$, para qualquer divisor canônico W, temos que $\text{grau}\, W - D \leq 2g-2-2g+1 = -1$. Pelo corolário 2.1, vemos que $l(W-D) = 0$ e, assim, o teorema de Riemann-Roch aplicado ao divisor D se reduz à expressão do enunciado.

□

2.4 Uma aplicação: a sequência de lacunas em um lugar

O teorema de Riemann-Roch é sem dúvidas um dos mais importantes teoremas que provamos nesse capítulo e são inúmeras suas consequências. Nessa seção investigaremos uma delas, a saber a existência de uma sequência de lacunas em cada lugar P de um corpo de funções de gênero positivo.

Proposição 2.5. *Seja P um lugar de F/K. Para todo natural $n \geq 2g$, existe um elemento $x \in F$ com $(x)_\infty = nP$.*

Demonstração. Seja $n \geq 2g$, já vimos que, pelo teorema de Riemann-Roch, como ambos os graus de $(n-1)P$ e nP são maiores ou iguais a $2g-1$, devemos ter $l((n-1)P) = n - 1 + 1 - g = n - g$ e $l(nP) = n + 1 - g$. Isso nos mostra que $L((n-1)P) \subsetneq L(nP)$ e, portanto, existe $x \in L(nP) \backslash L((n-1)P)$ e $(x)_\infty = nP$.

□

Definição 2.9. Seja P um lugar de F/K. Dizemos que um natural n é uma *lacuna* em P se não existe uma função $x \in F$ com $(x)_\infty = nP$.

Em particular, a proposição que acabamos de provar mostra que toda lacuna deve ser menor que $2g$. Note também que o conjunto das não lacunas em um lugar P é um subsemigrupo aditivo de $\mathbb{N}$. De fato, se n_1 e n_2 não são lacunas, então existem funções

x_1, $x_2 \in F$ com $(x_i)_\infty = n_i P$, $i = 1, 2$, e, nesse caso, vemos que $n_1 + n_2$ não é lacuna, pois $(x_1 x_2)_\infty = (n_1 + n_2)P$.

Dado um lugar P, podemos considerar os espaços $L(nP)$ e eles nos fornecem a seguinte caracterização de quando um natural é uma lacuna em P:

Lema 2.4. *Seja P um lugar de F/K. Um natural n é uma lacuna em P se, e só se, $l((n-1)P) = l(nP)$.*

Demonstração. Por um lado, se $l((n-1)P) \neq l(nP)$, então $L((n-1)P) \subsetneq L(nP)$ e existe $x \in L(nP) \backslash ((n-1)P)$, o qual obviamente satisfaz $(x)_\infty = nP$ e isso nos mostra que n não é lacuna em P. Reciprocamente, se n não é lacuna em P, existe $x \in F$ com $(x)_\infty = nP$ e, nesse caso, vemos que $x \in L(nP)$, mas $x \notin L((n-1)P$. Isso nos mostra que $l((n-1)P \neq l(nP)$.

□

Finalmente, provamos que em qualquer corpo de funções de gênero $g \neq 0$ existem exatamente g lacunas em cada lugar P. Mais adiante veremos que as sequências de lacunas são preservadas por automorfismos e no capítulo 4 utilizaremos esse fato para obter a estrutura do grupo de automorfismos de certos corpos de funções.

Teorema 2.5 (**Teorema das lacunas de Weierstrass**)**.** *Sejam F/K um corpo de funções de gênero $g \neq 0$ e P um lugar de F/K. Então existem g lacunas $n_1 < ... < n_g$ em P. Mais ainda, $n_1 = 1$ e $n_g \leq 2g - 1$.*

Demonstração. Consideramos a sequência de K-espaços vetoriais

$$K = L(0) \subseteq L(P) \subseteq L(2P) \subseteq ... \subseteq L((2g-1)P).$$

Pelo lema 2.1, devemos ter que $l(nP) = l((n-1)P)$ ou $l(nP) = l((n-1)P) + 1$. Como $l(0) = 1$ e, pelo teorema de Riemann-Roch, $l((2g-1)P) = g$, cada caso deve ocorrer precisamente g vezes. Pelo lema 2.4, isso corresponde à existência de g lacunas $n_1 < ... < n_g \leq 2g - 1$ em P. Em particular, como não existem lacunas maiores ou iguais a $2g$ pela proposição 2.5, $n_1, ..., n_g$ são todas as lacunas em P. Falta provar que $n_1 = 1$. Para tal supomos que 1 não fosse lacuna. Nesse caso, como o grupo das não lacunas forma um subsemigrupo aditivo de $\mathbb{N}$ e 1 gera $\mathbb{N}$ como semigrupo, teríamos que não existem lacunas em P, mas isso contradiz o fato de que existem $g > 0$ lacunas em P.

□

2.5 Extensões de corpos de funções

Seja F/K um corpo de funções, por definição, existe $x \in F \backslash K$ tal que o grau $[F : K(x)]$ é finito. O corpo $K(x)$ também é um corpo de funções sobre K e gostaríamos de relacionar

os lugares e divisores de $K(x)$ com os lugares e divisores de F, por exemplo. De uma forma mais geral, fazemos essa relação em extensões algébricas de corpos de funções:

Definição 2.10. Uma *extensão algébrica de corpos de funções (sobre K)* F'/F são dois corpos de funções F'/K e F/K tais que a extensão de corpos F'/F é algébrica.

Observe antes de mais nada que:

Proposição 2.6. *Se F'/F é uma extensão algébrica de corpos de funções, então $[F' : F] < \infty$.*

Demonstração. Seja $x \in F \backslash K$, então $x \in F' \backslash K$ e, portanto, $[F' : K(x)] < \infty$. Como $F' \supseteq F \supseteq K(x)$, vemos que F'/F é uma extensão finita de corpos.

□

Para estudar a relação entre os lugares de F' e os lugares de F, introduzimos a noção de estar *acima*:

Definição 2.11. Dizemos que um lugar P' de F' está *acima* de um lugar P de F se $P \subseteq P'$. Nesse caso, escrevemos $P'|P$.

Proposição 2.7. *Sejam F'/F uma extensão algébrica de corpos de funções e P' e P lugares de F' e F, respectivamente. São equivalentes:*

(a) *$P'|P$;*

(b) *$\mathcal{O}_P \subseteq \mathcal{O}_{P'}$;*

(c) *Existe um natural $e(P'|P) \geq 1$ tal que $v_{P'}(x) = e(P'|P)v_P(x)$, para todo $x \in F$.*

Além disso, se $P'|P$, então $P = P' \cap F$ e $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$.

Demonstração. Para ver que (a) implica (b), suponha que exista $x \in F$ com $v_P(x) \geq 0$, mas $v_{P'}(x) \leq -1$. Como $P \subseteq P'$, devemos ter $x \notin P$, isto é, $v_P(x) = 0$. Seja $t \in F$ com $v_P(t) = 1$, como $P \subseteq P'$, vemos que $v_{P'}(t) > 0$. Nesse caso, observe que

$$v_P(x^{v_{P'}(t)}t) = v_{P'}(t)v_P(x) + v_P(t) = 1$$

mas

$$v_P(x^{v_{P'}(t)}t) = v_{P'}(t)v_{P'}(x) + v_{P'}(t) \leq -v_{P'}(t) + v_{P'}(t) = 0,$$

isto é $x^{v_{P'}(t)}t \in P \backslash P'$, contradizendo a hipótese de $P \subseteq P'$.

Vamos mostrar agora que (b) implica (a). Supondo que $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$, observe primeiramente que $\mathcal{O}_P = F \cap \mathcal{O}_{P'}$. De fato, $F \cap \mathcal{O}_{P'}$ é um subanel de F contendo $\mathcal{O}_P$ e como $\mathcal{O}_P$

é um subanel maximal de F (ver Stichtenoth [[14], teorema I.1.12, página 5]), devemos ter $F \cap \mathcal{O}_{P'} = \mathcal{O}_P$ ou $F \cap \mathcal{O}_{P'} = F$. Para ver que o último caso não ocorre, suponha que $F \cap \mathcal{O}_{P'} = F$ (isto é, $F \subseteq \mathcal{O}_{P'}$) e tome um elemento $x \in F' \backslash \mathcal{O}_{P'}$. Como a extensão F'/F é algébrica, existem $a_0, ..., a_{n-1} \in F$ tais que

$$x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 = 0.$$

Como $v_{P'}(x) < 0$ e $v_{P'}(a_i) \geq 0$, para todo i, vemos que na soma acima a parcela x^n possui ordem em P' estritamente menor que as ordens das outras parcelas em P'. Logo,

$$v_{P'}(0) = v_{P'}(x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0) = v_{P'}(x^n) = nv_{P'}(x)$$

mas isso não é possível. Assim concluímos que $\mathcal{O}_P = F \cap \mathcal{O}_{P'}$ e falta mostrar que $P \subseteq P'$. De fato, seja $y \in P$, então $v_P(y^{-1}) < 0$ e, portanto, $y^{-1} \notin \mathcal{O}_P$. Em particular, pela igualdade que acabamos de provar, $y^{-1} \notin \mathcal{O}_{P'}$, mas isso implica $v_{P'}(y^{-1}) < 0$ ou, equivalentemente, $v_{P'}(y) > 0$, isto é, $y \in P'$.

Finalmente mostramos que (c) é equivalente às duas primeiras afirmações. Por um lado, supondo que $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$, note primeiramente que se $z \in F$ possui ordem $v_P(z) = 0$, então z, $z^{-1} \in \mathcal{O}_P \subseteq \mathcal{O}_{P'}$ e, portanto, $v_{P'}(z) = 0$. Defina $e(P' \mid P) = v_{P'}(t)$, onde t é um parâmetro local em P, isto é, $v_P(t) = 1$. Em particular, observe que, como $P \subseteq P'$, devemos ter $e(P' \mid P) \geq 1$. Nesse caso, seja $x \in F$ não nulo, $v_P(xt^{-v_P(x)}) = 0$ e, portanto, pela observação que fizemos,

$$v_{P'}(x) = v_{P'}(xt^{-v_P(x)}) + v_{P'}(t^{v_P(x)}) = e(P' \mid P)v_P(x).$$

A recíproca é óbvia, pois dado $x \in \mathcal{O}_P$, então $v_P(x) \geq 0$ e, portanto, $v_{P'}(x) = e(P' \mid P)v_P(X) \geq 0$, isto é, $x \in \mathcal{O}_{P'}$. Dessa forma, estabelecemos a equivalência entre (a), (b) e (c) e provamos que $\mathcal{O}_P = F \cap \mathcal{O}_{P'}$. A igualdade $P = F \cap P'$ segue imediatamente de (c). □

Obviamente, o natural positivo $e(P'|P)$ da proposição acima é único. Dizemos que $e(P'|P)$ é o *índice de ramificação* de P' sobre P e, quando P' e P estiverem subentendidos escreveremos simplesmente e ao invés de $e(P'|P)$. Note também que, se temos extensões algébricas de corpos de funções F''/F' e F'/F, a extensão F''/F é algébrica e se P'', P', P são lugares de F''/K, F'/K, F/K, respectivamente, com $P'' \supseteq P' \supseteq P$, então, pela definição do índice de ramificação, temos que

$$e(P''|P) = e(P''|P')e(P'|P).$$

A seguir provamos um teorema sobre a relação entre os lugares de F' e F:

Teorema 2.6. *Seja F'/F uma extensão algébrica de corpos de funções sobre K. Para cada lugar P' de F'/K, existe um único lugar P de F/K, a saber $P = F \cap P'$, tal que $P'|P$. Reciprocamente, para cada lugar P de F/K, existe pelo menos um mas no máximo um número finito de lugares P' de F'/K com $P'|P$.*

Demonstração. Seja P' um lugar de F'/K, se P é um lugar de F com $P'|P$, pela proposição 2.8, temos que $P = P' \cap F$ e, portanto, para provar a primeira afirmação do teorema, basta mostrar que $P' \cap F$ é um lugar de F. Para isso, vamos mostrar que $\mathcal{O} = F \cap \mathcal{O}_{P'}$ é um anel de valorização discreta de F. Note primeiramente que existe $x \in F$, $x \neq 0$, com $v_P(x) \neq 0$. De fato, seja $t \in F'$ com $v_{P'}(t) > 0$, como F'/F é uma extensão algébrica, existem $a_0, ..., a_{n-1} \in F$, $c_0 \neq 0$, satisfazendo

$$t^n + a_{n-1}t^{n-1} + ... + a_1 t + a_0$$

e, nesse caso, se todo elemento não nulo de F tivesse ordem em P' igual a 0, teríamos que a parcela a_0 possui ordem em P' estritamente menor que a ordem de qualquer outra parcela da soma acima em P'. Isso implica que

$$v_{P'}(0) = v_{P'}(t^n + a_{n-1}t^{n-1} + ... + a_1 t + a_0) = v_{P'}(a_0) = 0,$$

o que é um absurdo! Como todo elemento de K possui ordem em P' igual a 0, essa observação nos mostra que $K \subsetneq \mathcal{O}$ e, em particular, deve existir $x \in F$ com $v_P(x) < 0$, implicando também que $\mathcal{O} \subsetneq F$. Finalmente, se $z \in F \backslash \mathcal{O}$, então $v_{P'}(z) < 0$ e, portanto, $v_{P'}(z^{-1}) > 0$ e, portanto, $z^{-1} \in \mathcal{O}$. Isso nos mostra que $\mathcal{O}$ é um anel de valorização de F/K e, portanto, é um anel de valorização discreta (ver Stichtenoth [[14], teorema I.1.6, página 3]). Seu único ideal maximal é obviamente $P = P' \cap F$ e também é claro que $P'|P$.

Seja agora P um lugar de F, consideramos um elemento $x \in F$ com zero apenas em P (ver proposição 2.5). Como x deve possuir pelo menos um mas no máximo um número finito de zeros em F'/K, a última afirmação do teorema segue imediatamente se provarmos que um lugar P' de F'/K está acima de P se, e só se, $v_{P'}(x) > 0$. Para provar esse fato, observe que, por um lado, se $P'|P$, então, pela proposição 2.7, $v_{P'}(x) = e(P'|P)v_P(x) > 0$. Por outro lado, se P' é um zero de x em F'/K, já provamos que existe um lugar P_0 de F/K com $P'|P_0$ e, nesse caso, $v_{P_0}(x) = e(P'|P_0)^{-1}v_{P'}(x) > 0$, implicando $P_0 = P$, uma vez que o único zero de x em F/K é P. Logo, temos que $P'|P$.

□

Finalmente, consideramos a relação entre divisores de F'/K e F/K e provamos a igualdade fundamental, que relaciona, para cada lugar P de F/K, o grau da extensão F'/F e os índices de ramificação $e(P'|P)$, para cada lugar P' de F'/K acima de P:

Definição 2.12. Seja $D = \sum_P n_P P$ um divisor de F/K, definimos sua *conorma* com

respeito à extensão F'/F como o divisor de F'/K dado por

$$\text{Con}_{F'/F}(D) = \sum_P \sum_{P'|P} e(P'|P) n_P P'.$$

Observação 2.2. A aplicação $\text{Con}_{F'/F} : \text{Div}(F/K) \to \text{Div}(F'/K)$ é obviamente um homomorfismo de grupos. Além disso, pela multiplicatividade do índice de ramificação, temos que se F''/F' e F'/F são extensões de corpos de funções, então, para todo divisor D de F/K,

$$\text{Con}_{F''/F}(D) = \text{Con}_{F''/F'}(\text{Con}_{F'/F}(D).$$

Lema 2.5. *Sejam F'/F uma extensão de corpos de funções sobre K e $x \in F$. Denotando por (x), $(x)_0$, $(x)_\infty$ (resp. $(x)'$, $(x)'_0$, $(x)'_\infty$) os respectivos divisores principal, de zeros e de polos de x em $\text{Div}(F/K)$ (resp. $\text{Div}(F'/K)$), então*

$$\begin{aligned}(x)' &= \text{Con}_{F'/F}((x)),\\ (x)'_0 &= \text{Con}_{F'/F}((x)_0),\\ (x)'_\infty &= \text{Con}_{F'/F}((x)_\infty).\end{aligned}$$

Demonstração. Seja P um zero de x em F/K, para cada lugar P' de F'/K acima de P, temos que $v_{P'}(x) = e(P'|P)v_P(x) > 0$ e, portanto, P' é um zero de x em F'/K. Mais ainda, cada zero P' de x em F'/K está acima de um zero P de (x) F/K, uma vez que, se $v_{P'}(x) > 0$, então $v_P(x) = e(P'|P)^{-1}v_{P'}(x) > 0$. Assim, vemos que

$$\begin{aligned}(x)'_0 &= \sum_{v_{P'}(x)>0} e(P'|P' \cap F) v_P(x)\\ &= \sum_{v_P(x)>0} \sum_{P'|P} e(P'|P) v_P(x)\\ &= \text{Con}_{F'/F}((x)_0).\end{aligned}$$

De maneira análoga, mostramos que $(x)'_\infty = \text{Con}_{F'/F}((x_\infty)$ e finalmente temos que

$$\begin{aligned}(x)' = (x)'_0 - (x)'_\infty &= \text{Con}_{F'/F}((x)_0) - \text{Con}_{F'/F}((x)_\infty)\\ &= \text{Con}_{F'/F}((x)_0 - (x)_\infty = \text{Con}_{F'/F}((x)).\end{aligned}$$

□

Teorema 2.7 (Igualdade Fundamental). *Seja F'/F uma extensão algébrica de corpos*

de funções sobre K e seja P um lugar de F/K. Então,

$$[F' : F] = \sum_{P'|P} e(P'|P).$$

Demonstração. Considere um elemento $x \in F$ que possua zero apenas em P (ver Proposição 2.5). Seja $(x)'_0$ o divisor de zeros de x em F'/K, por um lado, pelos teorema 2.1 e lema 2.5, temos que

$$[F' : K(x)] = \text{grau}(x)'_0 = \sum_{P'|P} e(P'|P) v_P(x) = v_P(x) \sum_{P'|P} e(P'|P).$$

Por outro lado, novamente pelo teorema 2.1, temos que

$$[F' : K(x)] = [F' : F][F : K(x)] = [F' : F] v_P(x).$$

Igualando os dois valores obtidos para $[F' : K(x)]$, obtém-se a igualdade fundamental.

□

Corolário 2.4. *Seja F'/F uma extensão algébrica de corpos de funções sobre K. Então:*

(a) *Para todo lugar P de F/K, $\#\{$lugares P' de F'/K acima de $P\} \leq [F' : F]$;*

(b) *Para todo lugar P de F/K e P' de F'/K com $P'|P$, $e(P'|P) \leq [F' : F]$;*

(c) *Para todo $D \in \text{Div}(F/K)$, $\text{grau}(\text{Con}_{F'/F}(D)) = [F' : F] \,\text{grau}\, D$.*

Demonstração. As afirmações nos itens (a) e (b) são imediatas da igualdade fundamental. Para provar a afirmação em (c), escreva $D = \sum_P n_P P$ e observe que, pela igualdade fundamental

$$\begin{aligned}
\text{grau}(\text{Con}_{F'/F}(D)) &= \sum_P \sum_{P'|P} e(P'|P) n_P \\
&= \sum \left(n_P \sum_{P'|P} e(P'|P) \right) \\
&= [F' : F] \sum_P n_P \\
&= [F' : F] \,\text{grau}\, D.
\end{aligned}$$

□

Fixamos, por último, alguns novos termos, que aparecerão com frequência na próxima seção e no próximo capítulo:

Definição 2.13. Seja F'/F uma extensão algébrica de corpos de funções sobre K e seja P um lugar de F/K. Diremos que P se *ramifica* na extensão F'/F se $e(P'|P) > 1$, para algum lugar P' de F'/K acima de P. Em particular, P não se ramifica se, e só se, existem $[F' : F]$ lugares de F'/K acima de P. Por fim, diremos que P se *ramifica totalmente* na extensão F'/F se existe um único lugar P' de F'/K acima de P. Em particular, isso ocorre se, e só se, $e(P'|P) = [F' : F]$.

2.6 Extensões separáveis de corpos de funções

Nessa seção, consideramos extensões algébricas F'/F de corpos de funções sobre K tais que as extensões de corpos F'/F são também separáveis. Da teoria de corpos, sabemos que essa hipótese garante que a função traço $\mathrm{Tr}_{F'/F} : F' \to F$ com respeito à extensão F'/F não é identicamente nula. Utilizaremos a seguir o traço de F'/F para construir um divisor $\mathrm{Diff}_{F'/F}$ de F'/K, dito a *diferente* de F'/F, que, de certa forma, contém informações importantes sobre a ramificação dos lugares de F/K na extensão F'/F.

Lembramos antes que numa extensão separável de corpo, toda base possui uma base dual com respeito ao traço da extensão:

Lema 2.6. *Seja F'/F uma extensão algébrica e separável de corpos (de funções sobre K). Então, a função traço $\mathrm{Tr}_{F'/F} : F' \to F$ induz uma forma bilinear $T : L \times L \to K$ não degenerada dada por $T(x, y) = \mathrm{Tr}_{F'/F}(x, y)$. Em particular, vemos que, dada uma F-base $\{x_1, ..., x_n\}$ de F', existe uma única F-base $\{x_1^*, ..., x_n^*\}$ de F', dita a base dual de $\{x_1, ..., x_n\}$, com $T(x_i x_j) = \delta_{ij}$, onde por δ_{ij} denotamos o delta de Kronecker.*

Demonstração. Ver Stichtenoth [[14], proposição III.3.3, página 73].

□

Lema 2.7. *Sejam F'/F uma extensão algébrica de corpos de funções sobre K e R um domínio integralmente fechado com corpo de frações $F \neq R$ contendo K. Se $x \in F'$ é inteiro sobre R, então $\mathrm{Tr}_{F'/F}(x) \in R$.*

Demonstração. Ver Stichtenoth [[14]Corolário III.3.2, página 72].

□

Provamos a seguir a existência de bases integrais para lugares de F'/F:

Definição 2.14. Seja F'/F uma extensão algébrica e separável de corpos de funções sobre K, dizemos que uma base $\{x_1, ..., x_n\}$ de F'/F é uma *base integral* para um lugar P de F/K se $\{x_1, ..., x_n\}$ é uma base para o fecho inteiro de $\mathcal{O}_P$ em F' visto como $\mathcal{O}_P$-módulo.

Teorema 2.8. *Seja F'/F uma extensão algébrica e separável de corpos de funções sobre K e seja R um domínio integralmente fechado contendo K e com corpo de frações $F \neq R$. Se R' denota o fecho inteiro de R em F', então:*

(a) *Seja $x \in F'$, existe $a \in R$ não nulo tal que $ax \in R'$. Em particular, existem bases de F'/F contidas em R';*

(b) *Seja $\{x_1, ..., x_n\}$ uma base de F'/F contida em R' e seja $\{x_1^*, ..., x_n^*\}$ sua base dual, temos que*

$$Rx_1 + ... + Rx_n \subseteq R' \subseteq Rx_1^* + ... + Rx_n *\,.$$

(c) *Se R é um domínio de ideais principais, então R' é um R-módulo livre e existe uma base $\{x_1, ..., x_n\}$ de F'/F tal que*

$$R' = Rx_1 + ... + Rx_n.$$

Demonstração.

(a) Seja $x \in F'$, como F'/F é uma extensão algébrica, existem $a_{m-1}, ..., a_0 \in F$ tais que

$$x^m + a_{m-1}x^{m-1} + ...a_1x + a_0 = 0.$$

Escrevendo $a_i = \alpha_i\beta_i^{-1}$, com α_i, $\beta_i \in R$, defina $a = \beta_1...\beta_{m-1} \in \mathbb{R}$ e observe que

$$(ax)^m + aa_{m-1}(ax)^{m-1} + ... + a^{m-1}a_1(ax) + a^m a_0 = 0,$$

de onde segue que $ax \in R'$. Por fim, seja agora $\{x_1, ..., x_n\}$ uma base de F'/F, como vimos existem elementos $b_1, ..., b_n \in R$ não nulos tais que $b_ix_i \in R'$, para todo i. Obviamente, $\{b_1x_1, ..., b_nx_n\}$ é uma base de F'/F contida em R'.

(b) A primeira desigualdade é imediata. Seja então $x \in R'$, em particular, $x \in F'$ e, portanto, existem elementos $a_1, ..., a_n \in F$ tais que

$$x = a_1x_1^* + ... + a_nx_n^*.$$

Por hipótese, $x_i \in R'$, para todo i, e, assim, temos que $xx_i \in R$. Pelo lema 2.7, para cada i, devemos ter que

$$\mathrm{Tr}_{F'/F}(xx_i) = \sum_{j=1}^{n} a_j \,\mathrm{Tr}_{F'/F}(x_j^*x) = a_i \in R.$$

Logo, $x \in Rx_1^* + ... + Rx_n^*$.

(c) Começamos com uma base $\{z_1, ..., z_n\}$ de F'/F com $R' \subseteq Rz_1 + ... + Rz_n$, o que é possível pelo item (b) que acabamos de provar. Para cada $j = 1, ..., n$, definimos

$R_j = R' \cap \sum_{i=1}^{j} Rz_i$. Vamos mostrar que, para cada j, existem $x_1, ..., x_n \in R'$ tais que $R_j = Rx_1 + ... + Rx_j$. Em particular, isso conlui a demonstração, pois, para $j = n$, vemos que $R' = R_n = Rx1 + ... + Rx_n$ e $x_1, ..., x_n$ são linearmente independentes sobre F, pois R' contém alguma base de F'/F.

Para $j = 1$, considere o conjunto

$$I_1 = \{a \in F \mid az_1 \in R'\},$$

e observe que $I_1 \subseteq R$. De fato, para cada $a \in I_1$, $az_1 \in R' \subseteq Rz_1 + ... + Rz_n$ e, como $z_1, ..., z_n$ são linearmente independentes sobre F, concluímos que $a \in R$. Mais ainda, é imediato ver que I_1 é um ideal de R e, portanto, como supomos R um domínio de ideais principais, existe $a_1 \in R$ tal que $I_1 = Ra_1$. Dessa forma, definimos $x_1 = a_1 z_1$ e vemos que $R_1 = Rx_1$. De fato, por um lado, dado $x \in R_1 = R' \cap Rz_1$, então $xz^{-1} \in R$ e, mais precisamente, como $xz^{-1}z_1 = x \in R'$, temos que $xz_1 \in I_1 = Ra_1$. Logo, $x \in Rz_1a_1 = Rx_1$. A inclusão $R_1 \supseteq Rx_1$ é imediata.

Finalmente, supomos que, para $j \in \{2, ..., n\}$, encontramos $x_1, ..., x_{j-1}$ tais que $R_{j-1} = Rx_1 + ... + Rx_{j-1}$. Considere o conjunto

$$I_j = \{a \in F \mid \exists b_1, ..., b_{j-1} \in R \text{ com } b_1z_1 + ... + b_{j-1}z_{j-1} + az_j \in R'\},$$

o qual, utilizando argumentos análogos ao do caso $j = 1$, vemos ser um ideal de R, digamos $I_j = Ra_j$, para algum $a_j \in I_j$. Sejam $b_1, ..., b_{j-1} \in R$ tais que $b_1z_1 + ... + b_{j-1}z_{j-1} + a_jz_j \in R'$, defina u_j como

$$x_j = b_1z_1 + ... + b_{j-1}z_{j-1} + a_jz_j \in R'$$

Por um lado, imediatamente vemos que

$$R_j = R' \cap \sum_{i=1}^{j} Rz_j \supseteq R_{j-1} + (R' \cap Rz_j) \supseteq R_1x_1 + ... + Rx_j$$

Por outro lado, seja $x \in R_k$, existem $c_1, ..., c_j \in R$ tais que

$$x = c_1z_1 + ... + c_jz_j$$

e, nesse caso, vemos que $c_j \in I_j$ e, portanto, $c_j = a_jc$, para algum $c \in R$. Assim, concluímos que

$$x - cx_k = (c_1 - cb_1)z_1 + ... + (c_{j-1} - cb_{j-1})z_{j-1} \in R_{j-1} = Rx_1 + ... + Rx_{j-1},$$

de onde segue que $x \in Rx_1 + ... + Rx_j$.

□

Corolário 2.5. *Sejam F'/F uma extensão algébrica e separável de corpos de funções sobre K. Todo lugar de F/K admite uma base integral no sentido da definição 2.14. Mais ainda, qualquer base de F'/F é uma base integral para quase todo lugar de F/K.*

Demonstração. A primeira afirmação segue imediatamente do item (c) do teorema 2.8, visto que, para todo lugar P de F/K, o anel $\mathcal{O}_P$ é um anel de valorização discreta e, em particular, um domínio de ideais principais. Provamos então a última afirmação e, para tal, seja $\{x_1, ..., x_n\}$ uma base arbitrária de F'/F, consideramos sua base dual $\{x_1^*, ..., x_n^*\}$ e os coeficientes dos polinômios mínimos (mônicos) de cada x_i e x_i^*. Existe um conjunto finito S de polos de tais coeficientes em F. Seja P um lugar de F/K com $P \notin S$, então os coeficientes dos polinômios mínimos de cada x_i e x_i^* são elementos de $\mathcal{O}_P$, de onde segue que $x_i,\ x_i^* \in \mathcal{O}'_P$, para todo i, onde denotamos por $\mathcal{O}'_P$ o fecho inteiro de $\mathcal{O}_P$ em F'. Logo, pelo item (b) do teorema 2.8 e pelo fato de que $\{x_1, ..., x_n\}$ é a base dual de $\{x_1^*, ..., x_n^*\}$,

$$\sum_{i=1}^{n} \mathcal{O}_P x_i \subseteq \mathcal{O}'_P \subseteq \sum_{i=1}^{n} \mathcal{O}_P x_i^* \subseteq \mathcal{O}'_P \subseteq \sum_{i=1}^{n} \mathcal{O}_P x_i,$$

de onde segue que $\mathcal{O}'_P = \mathcal{O}_P x_1 + ... + \mathcal{O}_P x_n$.

□

Finalmente, utilizando as propriedades do traço mencionadas acima e a existência de bases integrais para lugares de F/K, provamos um resultado que nos motivará a definir a diferente da extensão algébrica e separável F'/F:

Lema 2.8. *Sejam P um lugar de F/K e $\mathcal{O}'_P$ o fecho inteiro de $\mathcal{O}_P$ em F', então*

$$\mathcal{O}'_P = \{x \in F' \mid v_{P'}(x) \geq 0, \text{ para todo } P'|P\}.$$

Além disso, $\mathcal{O}'_P$ é um domínio de ideais principais.

Demonstração. Ver Stichtenoth [[14], corolário III.3.5, página 75]

□

Proposição 2.8. *Sejam P um lugar de F/K e $\mathcal{O}'_P$ o fecho inteiro de $\mathcal{O}_P$ em F', considere o conjunto $\mathcal{C}_P = \{x \in F' \mid \mathrm{Tr}_{F'/F}(x\mathcal{O}'_P) \subseteq \mathcal{O}_P\}$. Então:*

(a) *$\mathcal{C}_P$ é um $\mathcal{O}'_P$-módulo com $\mathcal{O}'_P \subseteq \mathcal{C}_P$;*

(b) *Se $\{x_1, ..., x_n\}$ é uma base integral para o lugar P, então $\mathcal{C}_P = \mathcal{O}_P x_1^* + ... + \mathcal{O}_P x_n^*$;*

(c) *Existe* $t \in F'$ *tal que* $\mathcal{C}_P = t\mathcal{O}'_P$ *e, para todo lugar* P' *de* F'/K *acima de* P*, temos que* $v_{P'}(t) \leq 0$*. Além disso,* $\mathcal{C}_P = t'\mathcal{O}'_P$*, para outro* $t' \in F'$ *se, e só se,* $v_{P'}(t') = v_{P'}(t)$*, para todo* $P'|P$*;*

(d) $\mathcal{C}_Q = \mathcal{O}'_Q$*, para quase todo lugar* Q *de* F/K*.*

Demonstração.

(a) A primeira afirmação é óbvia pela definição de $\mathcal{C}_P$ e a segunda afirmação segue diretamente do lema 2.7.

(b) Por um lado, seja $x \in \mathcal{C}_P$, em particular, $x \in F'$ e, portanto, existem $a_1, ..., a_n \in F$ tais que $x = a_1x_1^* + ... + a_nx_n^*$. Como $x_i \in \mathcal{O}'_P$, para todo i, e $x \in \mathcal{C}_P$, vemos que, para cada i,

$$\mathrm{Tr}_{F'/F}(xx_i) = \sum_{j=1}^{n} a_j \,\mathrm{Tr}_{F'/F}(x_j^* x_i) = a_i \in \mathcal{O}_P$$

e, assim, concluímos que $x \in \mathcal{O}_P x_1^* + ... + \mathcal{O}_P x_n^*$.

Por outro lado, seja agora $x = a_1x_1^* + ... + a_nx_n^*$, com $a_i \in \mathcal{O}_P$, devemos mostrar que $\mathrm{Tr}_{F'/F}(xy) \in \mathcal{O}_P$, para todo $y \in \mathcal{O}'_P$. De fato, seja $y \in \mathcal{O}'_P$, existem $b_1, ..., b_n \in \mathcal{O}_P$ tais que $y = b_1x_1 + ... + b_n$ e, nesse caso, vemos que

$$\mathrm{Tr}_{F'/F}(xy) = \sum_{i,\,j=1}^{n} a_i b_j \,\mathrm{Tr}_{F'/F}(x_i^* b_j) = \sum_{i=1}^{n} a_i b_i \in \mathcal{O}_P.$$

(c) Pelo item (b), existem elementos $x_1, ..., x_n \in F'$ tais que $\mathcal{C}_P = \mathcal{O}_P x_1 + ... + \mathcal{O}_P x_n$. Seja $x \in \mathcal{O}_P$ com $v_P(x) \geq v_{P'}(x_i)$, para todo $P'|P$ e i, observe que $x\mathcal{C})P \subseteq \mathcal{O}'_P$. De fato, dado $y \in \mathcal{C}_P$, existem $a_1, ..., b_n \in \mathcal{O}_P$ tais que $y = a_1x_1 + ... + a_nx_n$ e, assim, temos que, para todo lugar $P'|P$

$$v_{P'}(xy) \geq \min\{e(P'|P)v_P(a_1) + e(P'|P)v_P(x_1) + v_{P'}(x_i)\} \geq 0,$$

o que implica $xy \in \mathcal{O}'_P$, pelo lema 2.8. Além disso, pelo item (a), concluímos que $x\mathcal{C}_P$ é um ideal de $\mathcal{O}'_P$ e, portanto, pelo lema 2.8, existe $z \in x\mathcal{C}_P$ tal que $x\mathcal{C}_P = z\mathcal{O}'_P$. Dessa forma, pondo $t = zx^{-1}$, vemos que $\mathcal{C}_P = t\mathcal{O}'_P$ e, como $1 \in \mathcal{C}_P$, devemos ter $t^{-1} \in \mathcal{O}'_P$, isto é, $v_{P'}(t) \leq 0$, para todo $P'|P$. Finalmente, note que $t\mathcal{O}'_P = t'\mathcal{O}'_P$, para outro $t' \in F'$ se, e só se, ambos $t't^{-1}$ e $(t't^{-1})^{-1}$ são elementos de $\mathcal{O}'_P$. Pelo lema 2.8, isto equivale a dizer que $v_{P'}(t't^{-1}) = 0$, para todo $P'|P$, isto é, $v_{P'}(t) = v_{P'}(t')$, para todo $P'|P$.

(d) Seja $\{x_1, ..., x_n\}$ uma base de F'/F, sua base dual $\{x_1^*, ..., x_n^*\}$ é uma base de F'/F, pelo coroário 2.5, $\mathcal{O}'_Q = \mathcal{O}_Q x_1^* + ... + \mathcal{O}_Q x_n^*$, para quase todo lugar Q de F/K. Pelo item (b), concluímos que $\mathcal{C}_Q = \mathcal{O}'_Q$ para tais lugares Q de F/K.

□

Definição 2.15. Seja F'/F uma extensão algébrica e separável de corpos de funções sobre K. Para cada lugar P de F/K e P' de F'/K acima de P, definimos $d(P'|P) = -v_{P'}(t)$, onde t é um elemento de F' tal que $\mathcal{C}_P = t\mathcal{O}_P$. A *diferente* da extensão F'/F é o divisor

$$\text{Diff}(F'/F) = \sum_P \sum_{P'|P} d(P'|P)P'.$$

Observação 2.3. O valor $d(P'|P)$ está bem definido em virtude do item (b) da proposição acima. Mais ainda, pelo mesmo item, $d(P'|P) \geq 0$ e, portanto, $\text{Diff}(F'/F) \geq 0$. Finalmente, note que a soma na expressão da diferente é finita, pois pelo item (c) da proposição acima $d(P'|P) = -v_{P'}(1) = 0$, para quase todo lugar P de F/K e P' de F'/K acima de P.

Como mencionado anteriormente, a diferente da extensão separável F'/F traz certas informações relevantes sobre a ramificação dos lugares de F/K. Isso se deve à existência de uma íntima relação entre os números $d(P'|P)$ e $e(P'|P)$. Essa relação é resumida abaixo em um teorema clássico conhecido como o teorema da diferente de Dedekind:

Teorema 2.9 (**Teorema da Diferente de Dedekind**). *Seja F'/F uma extensão algébrica e separável de corpos de funções sobre K. Sejam P um lugar de F/K e P' um lugar de F'/K acima de P, então:*

(a) $d(P'|P) \geq e(P'|P) - 1$*;*

(b) $d(P'|P) = e(P'|P) - 1$ *se, e só se, a característica de K não divide $e(P'|P)$.*

Demonstração. Ver Stichtenoth [[14], teorema III.5.1, página 89].

□

Finalmente, investigamos a relação entre os gêneros $g_{F'}$ e g_F de F'/K e F/K, respectivamente. Essa relação se baseia na existência do *cotraço* de uma diferencial de Weil de F/K:

Definição 2.16. Seja F'/F uma extensão algébrica e separável de corpos de funções sobre K, definimos

$$\mathcal{A}_{F'/F} = \{\alpha \in \mathcal{A}_{F'} \mid \alpha_{P'} = \alpha_{P''} \text{ se } P' \cap F = P'' \cap F\}$$

o qual obviamente é um F'-subespaço do espaço de adeles de F'/K. Lembramos que identificamos um elemento de F' com um adele principal associado a esse elemento e é claro que um adele principal é um elemento de $\mathcal{A}_{F'/F}$. Estendemos o traço $\mathrm{Tr}_{F'/F}$ a uma aplicação F-linear $\mathrm{Tr}_{F'/F} : \mathcal{A}_{F'/F} \to \mathcal{A}_F$ dada por

$$(\mathrm{Tr}_{F'/F}(\alpha))_P = \mathrm{Tr}_{F'/F}(\alpha_{P'}),$$

onde P' é qualquer lugar de F'/K acima de P.

Observação 2.4. A extensão do traço definida acima está bem definida. De fato, para cada lugar P de F/K, o valor $\alpha_{P'}$ é o mesmo para todo lugar $P'|P$, pela definição de $\mathcal{A}_{F'/F}$, e, portanto, $(\mathrm{Tr}_{F'/F}(\alpha))_P$ independe da escolha de P'. Além disso, $\alpha_Q \in \mathcal{O}_Q$, para quase todo lugar Q de F'/K e, portanto, para quase todo lugar P de F/K, devemos ter $\alpha_{P'} \in \bigcap_{Q|P} \mathcal{O}_Q = \mathcal{O}'_P$, onde P' é um lugar de F'/K acima de P. Logo, pelo lema 2.7, para quase todo lugar P de F/K, devemos ter $\mathrm{Tr}_{F'/F}(\alpha_{P'}) \in \mathcal{O}_P$, e, assim, concluímos que $\mathrm{Tr}_{F'/F}(\alpha)$ é, de fato, um adele de F/K.

Lema 2.9. *Para todo $D' \in \mathrm{Div}(F'/K)$, temos que $\mathcal{A}_{F'} = \mathcal{A}_{F'/F} + \mathcal{A}_{F'}(D')$.*

Demonstração. Ver Stichtenoth [[14], lema III.4.8, página 84].

□

Teorema 2.10. *Seja ω uma diferencial de Weil de F/K, existe única diferencial de Weil ω' de F'/K tal que*

$$\omega'(\alpha) = \omega(\mathrm{Tr}_{F'/F}(\alpha)),$$

para todo $\alpha \in \mathcal{A}_{F'/F}$. Essa única diferencial de Weil é denominada cotraço *de ω (com respeito à extensão F'/F) e será denotada por $\mathrm{Cotr}_{F'/F}(\omega)$. Mais ainda, se $\omega \neq 0$, então*

$$(\mathrm{Cotr}_{F'/F}(\omega)) = \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F).$$

Demonstração. Mostramos primeiramente a existência do cotraço. Se $\omega = 0$, obviamente tomamos $\omega' = 0$. Caso contrário, consideramos o divisor $W' = \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F)$. Definimos, primeiramente, $\omega_1 : \mathcal{A}_{F'/F} \to K$ dada por $\omega_1 = \omega \circ \mathrm{Tr}_{F'/F}$ e verifica-se que (ver Stichtenoth [[14], teorema III.4.6, página 85])

(1) ω_1 é K-linear e se anula em $(\mathcal{A}_{F'/F} \cap \mathcal{A}_{F'}(W')) + F'$;

(2) W' é um elemento maximal do conjunto

$$M(\omega_1) = \{D' \in \mathrm{Div}(F'/K) \mid \omega_1 \text{ se anula em } (\mathcal{A}_{F'}(D') \cap \mathcal{A}_{F'/F}) + F'\}.$$

Finalmente, definimos $\omega' : \mathcal{A}_{F'} \to K$, utilizando o lema 2.9: dado $\alpha \in \mathcal{A}_{F'}$, existem $\beta \in \mathcal{A}_{F'/F}$ e $\gamma \in \mathcal{A}_{F'}(W')$ tais que $\alpha = \beta + \gamma$ e, nesse caso, definimos $\omega'(\alpha) = \omega_1(\beta)$. Observe que a aplicação ω' está bem definida, pois se α também se escreve como $\beta' + \gamma'$, para outros $\beta' \in \mathcal{A}_{F'/F}$ e $\gamma' \in \mathcal{A}_{F'}(W')$, então

$$\beta - \beta' = \gamma - \gamma' \in \mathcal{A}_{F'}(W') \cap \mathcal{A}_{F'/F}$$

e, portanto, pela propriedade (1) de ω_1, temos que $\omega_1(\beta - \beta') = 0$, isto é, $\omega_1(\beta) = \omega_1(\beta')$. Além disso, obviamente ω' é K-linear e pelas propriedades (1) e (2) de ω_1, vemos que

(3) ω' se anula em $\mathcal{A}_{F'}(W') + F'$;

(4) W' é um elemento maximal do conjunto

$$M(\omega') = \{D' \in \mathrm{Div}(F'/K) \mid \omega' \text{ se anula em } \mathcal{A}_{F'}(D') + F'\}.$$

Observe que a propriedade em (3) nos informa que $\omega' \in \Omega_{F'}$ e a propriedade em (4) nos diz que W' é o divisor de ω', isto é, $(\omega') = W' = \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F)$. Por fim, pela construção de ω', temos que, para $\alpha \in \mathcal{A}_{F'/F}$,

$$\omega'(\alpha) = \omega_1(\alpha) = \omega(\mathrm{Tr}_{F'/F}(\alpha)).$$

Só falta provar a unicidade do cotraço. Para tal, suponha que ω' e ω'' são duas diferenciais de Weil de F'/K com $\omega' = \omega''$ em $\mathcal{A}_{F'/F}$. Como $\omega' - \omega''$ é uma diferencial de Weil de F'/K, existe $D' \in \mathrm{Div}(F'/K)$ tal que $\omega' - \omega''$ se anula em $\mathcal{A}_{F'}(D')$ e, nesse caso, $\omega' = \omega''$ em $\mathcal{A}_{F'}(D')$. Pelo lema 2.9, concluímos que $\omega' = \omega''$ em $\mathcal{A}_{F'} = \mathcal{A}_{F'/F} + \mathcal{A}_{F'}(D')$ e, portanto, ω' e ω'' são uma mesma diferencial de Weil.

□

Corolário 2.6 (**Fórmula de Hurwitz**). *Seja F'/F uma extensão algébrica e separável de corpos de funções sobre K. Então,*

$$2g_{F'} - 2 = [F' : F](2g_F - 2) + d(F'/F)$$

onde $g_{F'}$, g_F e $d(F'/F)$ denotam, respectivamente, o gênero de F'/K, o gênero de F/K e o grau da diferente de F'/F.

Demonstração. Seja ω uma diferencial de Weil nao nula de F/K, pelo teorema 2.10,

$$(\mathrm{Cotr}_{F'/F}(\omega)) = \mathrm{Con}_{F'/F}((\omega)) + \mathrm{Diff}(F'/F). \tag{2.1}$$

Observe que $(\mathrm{Cotr}_{F'/F}(\omega))$ e (ω) são divisores canônicos de F'/K e F/K, respectivamente, e, portanto, possuem graus $2g_{F'} - 2$ e $2g_F - 2$, respectivamente. Além disso, pelo item (c) do corolário 2.4, o grau da conorma de (ω) é $[F' : F]\,\mathrm{grau}(\omega) = [F' : F](2g_F - 2)$ e, portanto, a igualdade do enunciado segue se tomarmos os graus na expressão (2.1).

□

Capítulo 3

Grupo de Automorfismos de Corpos de Funções

Nesse capítulo, discutimos questões sobre a ordem do grupo de automorfismos de um corpo de funções F/K de gênero $g \neq 1$, onde K como nos capítulos anteriores é um corpo algebricamente fechado. Na primeira seção, estudamos a ação natural desse grupo no conjunto dos divisores de F/K e, na segunda seção, determinamos explicitamente todos os automorfismos de um corpo de funções de gênero 0. No entanto, o principal objetivo desse capítulo está na seção 4, onde mostramos que, se $g \geq 2$, então o grupo de automorfismos de F/K é finito e, para tal, na seção 3, introduzimos a noção de grupo de decomposição de um lugar e provamos sua finitude. A demonstração desse fato será baseada em Iwasawa-Tamagawa [8]. O caso de corpos de funções de gênero 1 é também conhecido e faremos breves comentários na última seção, fornecendo referências para mais detalhes.

3.1 Automorfismos de corpos de funções

Lembramos que um corpo de funções F/K é antes de mais nada uma extensão de corpos F/K e por $\mathrm{Aut}(F/K)$ denotamos seu grupo de automorfismos, isto é, o conjunto de todos os automorfismos do corpo F que deixam cada elemento de K fixo. Seja F'/F uma extensão de corpos de funções sobre K, é conveniente considerar também o grupo dos automorfismos da extensão de corpos F'/F, denotado por $\mathrm{Aut}(F'/F)$, o qual claramente é um subgrupo de $\mathrm{Aut}(F'/K)$.

Investigaremos primeiramente a ação do grupo $\mathrm{Aut}(F/K)$ no conjunto dos lugares de F/K:

Proposição 3.1. *Sejam P um lugar de F/K e $\sigma \in \mathrm{Aut}(F/K)$, então $\sigma(P)$ é um lugar de F/K. Mais ainda, $\sigma(\mathcal{O}_P) = \mathcal{O}_{\sigma(P)}$ e $v_{\sigma(P)} = v_P \circ \sigma^{-1}$.*

Demonstração. Observe primeiramente que $\sigma(\mathcal{O}_P)$ é um anel de valorização. De fato, esse anel não é um corpo e, se $x \in F$ não é um elemento de $\sigma(\mathcal{O}_P)$, então $\sigma^{-1}(x)$ não é um elemento de $\mathcal{O}_P$ e, portanto, $(\sigma^{-1}(x))^{-1} = \sigma^{-1}(x^{-1}) \in \mathcal{O}_P$, implicando $x^{-1} \in \sigma(\mathcal{O}_P)$. Nesse caso, vemos que seu lugar associado é $\sigma(\mathcal{O}_P)\backslash\sigma(\mathcal{O}_P)^* = \sigma(\mathcal{O}_P\backslash\mathcal{O}_P^*) = \sigma(P)$.

Falta verificar que $v_{\sigma(P)} = v_P \circ \sigma^{-1}$. Para tal, considere t um parâmetro local em P, isto é, t é um gerador do ideal P de $\mathcal{O}_P$, e então $\sigma(t)$ é claramente um gerador do ideal $\sigma(P)$ de $\sigma(\mathcal{O}_P) = \mathcal{O}_{\sigma(P)}$. Nesse caso, se $x \in F\backslash\{0\}$ se escreve na forma $u\sigma(t)^n$, para $u \in \mathcal{O}^*_{\sigma(P)}$, então $v_{\sigma(P)}(x) = n$ e

$$v_P(\sigma^{-1}(x)) = v_P(\sigma^{-1}(u)t^n) = n = v_{\sigma(P)}(x),$$

uma vez que $\sigma^{-1}(u) \in \sigma^{-1}(\mathcal{O}^*_{\sigma(P)}) = \mathcal{O}_P^*$.

□

Corolário 3.1. *Sejam F'/F uma extensão algébrica de corpos de funções sobre K, P um lugar de F/K e $\sigma \in \mathrm{Aut}(F'/K)$ tal que $\sigma(F) = F$. Então, para todo lugar P' de F'/K acima de P, temos que $\sigma(P')|\sigma(P)$ e $e(P'|P) = e(\sigma(P')|\sigma(P))$.*

Demonstração. Pela proposição 3.1, $\sigma(P')$ é um lugar de F'/K e $\sigma(P)$ é um lugar de F/K e, como $\sigma(P') \supseteq \sigma(P)$, concluímos que $\sigma(P')|\sigma(P)$. Finalmente, se t é um parâmetro local em P, pela proposição 3.1, $\sigma(t)$ é um parâmetro local em $\sigma(P)$, e, mais ainda,

$$e(\sigma(P')|\sigma(P)) = v_{\sigma(P')}(\sigma(t)) = v_{P'}(\sigma^{-1}(\sigma(t))) = v_{P'}(t) = e(P'|P).$$

□

Observação 3.1. Mais ainda, no caso especial em que F'/F é uma extensão Galois, para todo lugar P de F/K, temos que o grupo de Galois $\mathrm{Aut}(F'/F)$ age transitivamente sobre o conjunto das extensões $P'|P$, isto é, dados lugares P_1 e P_2 de F'/K acima de um lugar P de F/K, existe $\sigma \in \mathrm{Aut}(F'/F)$ tal que $P_1 = \sigma(P_2)$ (ver Stichtenoth [[14], Teorema III.7.1, página 109]). Em particular, vemos que, se Q é um lugar de F'/K acima de um lugar P de F/K e $\sigma(Q) = Q$, para todo $\sigma \in \mathrm{Aut}(F'/F)$, então Q é totalmente ramificado na extensão F'/F.

A proposição 3.1 nos motiva a definir a seguinte ação do grupo $\mathrm{Aut}(F/K)$ no conjunto dos divisores de F/K:

Definição 3.1. Seja $D = \sum n_p P$ um divisor de F/K, para cada $\sigma \in \mathrm{Aut}(F/K)$, definimos

$$\sigma(D) = \sum n_P \sigma(P).$$

Note que D e $\sigma(D)$ possuem o mesmo grau. Além disso, se $D = (x)$, para alguma função x não nula, então $\sigma(D) = (\sigma(x))$ e isso nos mostra que, para um divisor arbitrário A, os espaços $L(A)$ e $L(\sigma(A))$ são K-isomorfos. De fato, se $A = \sum n_P P$, então $\sigma(A) = \sum n_P \sigma(P)$ e, para todo $x \in L(A)$ não nulo, temos que

$$v_{\sigma(P)}(\sigma(x)) + n_P = v_P(\sigma^{-1}(\sigma(x))) + n_P = v_P(x) + n_P \geq 0,$$

o que nos mostra que $\sigma(x) \in L(\sigma(A))$. A aplicação $x \in L(A) \mapsto \sigma(x) \in L(\sigma(A))$ é naturalmente um K-isomorfismo.

Por sua vez, o corolário 3.1 nos informa que, se F'/F é uma extensão algébrica de corpos de funções sobre K, então, para todo $\sigma \in \mathrm{Aut}(F'/K)$ tal que $\sigma(F) = F$, temos que $\mathrm{Con}_{F'/F}(\sigma(D)) = \sigma(\mathrm{Con}_{F'/F}(D))$. Supondo F'/F separável, investigamos o que ocorre com a diferente da extensão F'/F:

Proposição 3.2. *Sejam F'/F uma extensão algébrica e separável de corpos de funções sobre K, então, para todo $\sigma \in \mathrm{Aut}(F'/K)$ tal que $\sigma(F) = F$, temos que*

$$\sigma(\mathrm{Diff}(F'/F)) = \mathrm{Diff}(F'/F).$$

Demonstração. Em virtude do corolário 3.1, notamos que o resultado segue se provarmos que, para cada $P'|P$, temos a igualdade $d(P'|P) = d(\sigma(P')|\sigma(P))$. Sejam $\mathcal{C}_P$, $\mathcal{O}'_P$ como na definição 2.15 e $t \in F'$ tal que $\mathcal{C}_{\sigma(P)} = t\mathcal{O}'_{\sigma(P)}$, pela caracterização de $\mathcal{O}'_P$ no lema 2.8 e pela definição de $\mathcal{C}_P$, é imediato que $\sigma(\mathcal{C}_P) = \mathcal{C}_{\sigma(P)}$ e $\sigma(\mathcal{O}'_P) = \mathcal{O}'_{\sigma(P)}$. Pela definição de t, vemos então que $\mathcal{C}_P = \sigma^{-1}(t)\mathcal{O}'_P$ e, assim, concluímos que

$$d(P'|P) = -v_{P'}(\sigma^{-1}(t)) = -v_{\sigma(P')}(t) = d(\sigma(P')|\sigma(P)).$$

□

Observamos também que a sequência de lacunas em lugares de um corpo de funções F/K de gênero positivo é preservada por isomorfismos. Mais precisamente:

Proposição 3.3. *Sejam F/K um corpo de funções de gênero positivo e $\sigma \in \mathrm{Aut}(F/K)$. Então, para todo lugar P de F/K, a sequência de lacunas em P e $\sigma(P)$ são iguais.*

Demonstração. Observe que se n não é lacuna em P, então existe uma função $x \in F$ tal que $(x)_\infty = nP$. Nesse caso, vemos que $\sigma(x)$ possui divisor de polos $n\sigma(P)$ e, portanto, n também não é lacuna em $\sigma(P)$. Reciprocamente, se n não é lacuna em $\sigma(P)$, pelos mesmos argumentos, devemos ter que n não é lacuna em $\sigma^{-1}(\sigma(P)) = P$.

□

Finalmente, terminamos a seção, definindo a ação de $\mathrm{Aut}(F/K)$ no conjunto das diferenciais de Weil de F/K. Para tal, seja $\alpha = (\alpha_P)$ um adele de F/K, definimos $\sigma(\alpha)$ como o adele cuja P-ésima componente é $\sigma(\alpha_{\sigma^{-1}(P)})$. De fato, $\sigma(\alpha)$ é um adele, pois, se $\sigma(\alpha_{\sigma^{-1}(P)}) \notin \mathcal{O}_P$, então $\alpha_{\sigma^{-1}(P)} \notin \sigma^{-1}(\mathcal{O}_P) = \mathcal{O}_{\sigma^{-1}(P)}$ e isso ocorre apenas para um número finito de lugares P, pois (α_P) é um adele.

Definição 3.2. Sejam $\sigma \in \mathrm{Aut}(F/K)$ e $\omega \in \Omega_F$, definimos $\sigma(\omega)$ como a diferencial de Weil dada por $\sigma(\omega)(\alpha) = \omega(\sigma^{-1}(\alpha))$, para todo adele $\alpha \in \mathcal{A}_F$.

Observamos que $\sigma(\omega)$ como definida acima é realmente uma diferencial de Weil de F/K, pois $\sigma(\omega)$ é um funcional K-linear e, se ω se anula em $\mathcal{A}_F(D) + F$, para o divisor $D = \sum n_P P$, então, $\sigma(\omega)$ se anula em $\mathcal{A}_F(\sigma(D)) + F$. De fato, se $\alpha = (\alpha_P) \in \mathcal{A}_F(\sigma(D))$, então $v_P(\sigma^{-1}(\alpha_{\sigma(P)})) + n_P \geq 0$ e $\sigma^{-1}(\alpha) \in \mathcal{A}_F(D)$, pois, pela proposiçao 3.1,

$$v_P(\sigma^{-1}(\alpha_{\sigma(P)})) + n_P = v_{\sigma(P)}(\alpha_{\sigma(P)}) + n_P \geq 0$$

e, portanto,

$$\sigma(\omega)(\alpha + x) = \omega(\sigma^{-1}(\alpha) + \sigma^{-1}(x)) = 0,$$

para todo adele principal $x \in F$.

Em particular, a construção e discussão acima nos fornecem que:

Proposição 3.4. *Sejam $\sigma \in \mathrm{Aut}(F/K)$ e D um divisor de F/K. Então $\Omega_F(D)$ e $\Omega_F(\sigma(D))$ são K-isomorfos. Além disso, $(\sigma(\omega)) = \sigma((\omega))$, para toda $\omega \in \Omega_F \backslash \{0\}$.*

Demonstração. A aplicação dada por $\omega \in \Omega_F(D) \mapsto \sigma(\omega) \in \Omega_F(\sigma(D))$ com inversa dada por $\omega \in \Omega_F(\sigma(D)) \mapsto \sigma^{-1}(\omega) \in \Omega_F(D)$ nos fornece o K-isomorfismo do enunciado. Por fim, consideramos os conjuntos

$$M(\omega) = \{D \in \mathrm{Div}(F/K) \mid \omega \text{ se anula em } \mathcal{A}_F(D) + F\},$$
$$M(\sigma(\omega)) = \{D \in \mathrm{Div}(F/K) \mid \sigma(\omega) \text{ se anula em } \mathcal{A}_F(D) + F\}.$$

Já vimos que σ induz uma bijeção $D \in M(\omega) \mapsto \sigma(D) \in M(\sigma(\omega))$ e é imediato verificar que essa bijeção preserva ordem em $\mathrm{Div}(F/K)$. Em particular, a cota superior de $M(\omega)$ é levada na cota superior de $M(\sigma(\omega))$ e, pela definição do divisor de uma diferencial, isso equivale a dizer que $(\sigma(\omega)) = \sigma((\omega))$.

□

3.2 Automorfismos de corpos de funções de gênero zero

Dizemos que um corpo de funções F/K é *racional* se existe $x \in F\backslash K$ tal que $F = K(x)$.

Proposição 3.5. *Um corpo de funções (sobre um corpo algebricamente fechado) tem gênero 0 se, e só se, é um corpo de funções racional.*

Demonstração. Por um lado, se F/K tem gênero 0, seja P um lugar de F/K, como $\text{grau}\, P = 1 \geq -1 = 2g - 1$, concluímos, pelo corolário 2.3, que

$$l(P) = 1 + 1 - g = 2.$$

Nesse caso, vemos que $L(P)$ contém uma função $x \in F\backslash K$ e essa função possui divisor de polos $(x)_\infty = P$. Dessa forma, temos que

$$[F : K(x)] = \text{grau}(x)_\infty = 1$$

e, portanto, $F = K(x)$.

Por outro lado, se $F = K(x)$, para alguma função $x \in F$ não constante, como

$$1 = [F : K(x)] = \text{grau}(x)_\infty$$

concluímos que $(x)_\infty = P$, para algum lugar P de F/K. Seja r um natural positivo, como as funções $1, x, ..., x^r$ estão em $L(rP)$ e são linearmente independentes sobre K (pois possuem ordens distintas em P), vemos que $l(rP) \geq r + 1$. Para $r \geq 2g - 1$, obtemos que

$$r + 1 \leq l(rP) = r + 1 - g$$

e, finalmente, como $g \geq 0$, concluímos que $g = 0$.

□

Estamos, então, interessados em calcular o grupo de automorfismos de um corpo de funções F/K de gênero 0 e, pela proposição acima, podemos escrever $F = K(x)$, para alguma função $x \in F\backslash K$.

Teorema 3.1. *Sejam $F = K(x)$ um corpo de funções racional e $\sigma \in \text{Aut}(K(x)/K)$. Então, existem a, b, c, $d \in K$ tais que $ad - bc \neq 0$ e*

$$\sigma(x) = \frac{ax + b}{cx + d}.$$

Demonstração. Sejam $\sigma \in \mathrm{Aut}(K(x)/K)$ e $y = \sigma(x)$, então $K(x) = K(y)$ e $[K(x) : K(y)] = 1$. Vamos mostrar que, por outro lado, escrevendo $y = f/g$, para certos $f, g \in K[x]$, com $g \neq 0$ e f, g primos entre si, devemos ter

$$[K(x) : K(y)] = \max\{\mathrm{grau}(f), \mathrm{grau}(g)\}.$$

Note que, isso implica f e g de grau no máximo 1, isto é, $f = ax + b$ e $g = cx + d$, para certos $a, b, c, d \in K$ sendo a ou c não nulos. Juntamente com o fato de f e g serem primos entre si, isso é equivalente à condição $ad - bc \neq 0$.

Para provar que $[K(x) : K(y)] = \max\{\mathrm{grau}(f), \mathrm{grau}(g)\}$, observamos primeiramente que, como $y = f/g$, x é raiz do polinômio

$$h = f(X) - yg(X) \in K(y)[X].$$

Dessa forma, o fato que queremos mostrar segue da irredutibilidade desse polinômio sobre $K(y)$. Mais ainda, pelo lema de Gauss, sabemos que basta checar sua irredutibilidade como polinômio em $K[X, Y]$. No entanto, como polinômio na variável Y, h possui grau 1, e, então, se h fosse redutível, deveria ter um fator $p \in K[X]$ de grau maior ou igual a 1. Nesse caso, p deve dividir ambos f e g, o que contraria a hipótese de f e g serem primos entre si.

□

Observe que, por outro lado, à matriz

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, K)$$

podemos associar a aplicação

$$\begin{array}{rccc} \sigma : & K(x) & \longrightarrow & K(x) \\ & \frac{f(x)}{g(x)} & \mapsto & \frac{f((ax+b)/(cx+d))}{g((ax+b)/(cx+d))} \end{array}$$

que é um K-automorfismo de $K(x)$. Não é difícil ver que essa associação define um homomorfismo de $GL(2, K)$ em $\mathrm{Aut}(K(x)/K)$ e, mais ainda, pelo teorema que acabamos de provar, sabemos que esse homomorfismo é sobrejetivo. O núcleo desse homomorfismo consiste das matrizes

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, K)$$

tais que

$$\frac{ax+b}{cx+d} = x$$

o que implica $c = b = 0$ e $a = d$. Logo, pelo teorema dos isomorfismos,

$$\mathrm{Aut}(K(x)/K) \cong \frac{GL(2,K)}{\left\{ \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix} \mid k \in K^* \right\}}.$$

O grupo quociente no isomorfismo acima é conhecido como o *grupo linear geral projetivo*, denotado por $PGL(2,K)$.

Terminamos essa seção mostrando como esse grupo age nos lugares de $K(x)$ e, para tal, determinamos primeiramente quem são os lugares de $K(x)$. Antes de mais nada, observe que podemos pensar em $K(x)$ como o corpo de funções da reta afim $V_a(y)$ em $\mathbb{A}^2$ (ver exemplo 1.9) ou de seu fecho projetivo $V_p(y)$, que é uma curva não singular. Nesse caso, como observado no começo do capítulo 2, os lugares de $K(x)$ correspondem aos pontos de $\mathrm{Z}_p(y) = \mathrm{Z}_a(y) \cup \{(1:0:0)\}$ e $x : V_p(y) \dashrightarrow K$ é a função racional associada à função regular $x : V_a(y) \to K$ dada por $x(k,0) = k$.

Se $P_a = (a,\, 0)$ é um ponto afim, então vimos no exemplo 1.7 que

$$\mathcal{O}_{P_a} = \{f/g \in K(x) \mid g(a) \neq 0\}$$

e seu respectivo lugar, também denotado por P_a, é

$$P_a = \{f/g \in K(x) \mid f(a) = 0,\, g(a) \neq 0\}$$

No entanto, um polinômio em uma variável sobre K possui a como raiz se, e só se, $x - a$ divide esse polinômio e, portanto, podemos reescrever

$$\begin{aligned} \mathcal{O}_{P_a} &= \{f/g \in K(x) \,:\, x - a \nmid g\} \\ P_a &= (x-a)\mathcal{O}_{P_a} \end{aligned}$$

Em particular, acabamos de ver que $x - a$ é um parâmetro local em P_a. Por fim, seja P_∞ o lugar correspondente ao ponto no infinito $(1:0:0)$, como

$$\mathrm{grau}(x)_\infty = [K(x) : K(x)] = 1$$

e x não possui polos em $V_a(y)$, concluímos que $(x)_\infty = P_\infty$ e, portanto, x^{-1} é um parâmetro local em P_∞.

Proposição 3.6. *Seja $K(x)$ um corpo de funções racional e sejam P_k, $k \in K \cup \{\infty\}$, os lugares de $K(x)$ como acima. Se $\sigma \in \mathrm{Aut}(K(x)/K)$ é dado por $\sigma(x) = (ax+b)/(cx+d)$, com a, b, c, $d \in K$ e $ad - bc \neq 0$, então $\sigma(P_k) = P_{-(b-dk)/(a-ck)}$ para $k \in K$ e $\sigma(P_\infty) = P_{-d/c}$, onde definimos $1/0 = \infty$.*

Demonstração. Se $k \in K$, então $x - k$ é um parâmetro local em P_k e na demonstração da proposição 3.1, vimos que $\sigma(x-k)$ é um parâmetro local em $\sigma(P_k)$. Além disso, observe que $K(x) = K(x-k) = K(\sigma(x-k))$ e, portanto, pelo teorema 2.1, devemos ter que $\sigma(x-k)$ possui apenas um zero, a saber $\sigma(P_k)$. Assim, como

$$\sigma(x-k) = \frac{(a-ck)x + (b-dk)}{cx+d}$$

possui zero em $P_{-(b-dk)/(a-ck)}$, concluímos que $\sigma(P_k) = P_{-(b-dk)/(a-ck)}$.

Finalmente, se $k = \infty$, temos que x^{-1} é parâmetro local em P_∞ e devemos determinar o zero de $\sigma(x^{-1})$. Como

$$\sigma(x^{-1}) = \frac{cx+d}{ax+b}$$

possui zero em $P_{-d/c}$, concluímos que $\sigma(P_k) = P_{-d/c}$.

□

Corolário 3.2. *Seja $K(x)/K$ um corpo de funções racional. Se $\sigma \in \mathrm{Aut}(K(x)/K)$ fixa três lugares distintos, então σ é a identidade.*

Demonstração. Digamos que $\sigma(x) = (ax+b)/(cx+d)$, para a, b, c, $d \in K$ com $ad-bc = 0$ e que σ fixa os lugares P_{k_1}, P_{k_2}, P_{k_3}, onde k_1, k_2, k_3 são elementos distintos entre si de $K \cup \{\infty\}$. Supomos inicialmente que k_1, k_2, $k_3 \in K$ e, pela proposição 3.6, devemos ter

$$k_i = -\frac{b-dk_i}{a-ck_i}, \qquad i = 1,\, 2,\, 3$$

Assim, vemos que k_1, k_2, k_3 são três raízes distintas do polinômio

$$cX^2 + (d-a)X - b$$

Como um polinômio não nulo de grau até 2 deve possuir até no máximo duas raízes, concluímos que $a = d$ e $c = b = 0$ e, portanto, $\sigma(x) = x$, isto é, σ é a identidade em $K(x)$.

Supomos por fim que um dos lugares, digamos P_{k_3}, seja P_∞ e, então, pela proposição 3.6, devemos ter $c = 0$. Além disso, utilizando os mesmos argumentos de acima para os lugares P_{k_1} e P_{k_2}, concluímos que k_1, k_2 são duas raízes distintas do polinômio $(a-d)X - b$ e, portanto, $a = d$ e $b = 0$, o que nos fornece $\sigma(x) = x$.

□

3.3 Os grupos de decomposição e ramificação de um lugar

Seja P um lugar de F/K, definimos o *grupo de decomposição* de P sobre K como

$$G(P) = \{\sigma \in \mathrm{Aut}(F/K) \mid \sigma(P) = P\},$$

e o *primeiro grupo de ramificação* de P sobre K como

$$N(P) = \{\sigma \in G(P) \mid \sigma(t) \equiv t (\mathrm{mod}\ P^2)\},$$

onde t é um parâmetro local em P. Observamos antes de mais nada que:

Proposição 3.7. *A definição de $N(P)$ não depende da escolha do parâmetro local t, $N(P)$ é um subgrupo normal de $G(P)$ e $G(P)/N(P) \hookrightarrow (\mathcal{O}_P/P)^* \cong K^*$.*

Demonstração. Seja t' outro parâmetro local em P, sabemos que existe $u \in \mathcal{O}_P^*$ tal que $t' = ut$ e precisamos mostrar que

$$ut \equiv \sigma(u)\sigma(t) (\mathrm{mod}\ P^2)$$

ou equivalentemente que

$$1 \equiv \frac{\sigma(u)}{u}\frac{\sigma(t)}{t} (\mathrm{mod}\ P)$$

para todo $\sigma \in N(P)$. De fato, por um lado, como K é algebricamente fechado e $\mathcal{O}_P/P$ é uma extensão algébrica da cópia de K nesse quociente (ver Fulton [[4], Proposição 4, página 15]), temos que $\mathcal{O}_P/P \cong K$ e, mais precisamente, existe $k \in K^*$ tal que $u \equiv k (\mathrm{mod}\ P)$. Nesse caso, como todo automorfismo $\sigma \in N(P)$ é a identidade em K e fixa P, vemos que $\sigma(u) \equiv u (\mathrm{mod}\ P)$, isto é, $\sigma(u)/u \equiv 1 (\mathrm{mod}\ P)$. Finalmente, como $\sigma \in N(P)$ fixa t módulo P^2, devemos ter que $\sigma(t)/t \equiv 1 (\mathrm{mod}\ P)$.

Para provar que $N(P) \triangleleft G(P)$, consideramos a aplicação

$$\theta : \sigma \in G(P) \mapsto \frac{\sigma(t)}{t} + P \in (\mathcal{O}_P/P)^*,$$

onde t é um parâmetro local em P. Os argumentos acima nos mostram que θ não depende da escolha de t e afirmamos que θ é um homomorfismo de grupos. De fato, sejam σ_1, $\sigma_2 \in G(P)$, temos que

$$\frac{(\sigma_1 \circ \sigma_2)(t)}{t} = \frac{\sigma_1(\sigma_2(t))}{\sigma_2(t)}\frac{\sigma_2(t)}{t}$$

e, como $\sigma_2(t)$ é parâmetro local em P, já vimos que

$$\frac{\sigma_1(\sigma_2(t))}{\sigma_2(t)} \equiv \frac{\sigma_1(t)}{t} (\text{mod } P).$$

Por fim, note que $N(P) = \ker(\theta)$ e, portanto, $N(P)$ é um subgrupo normal de $G(P)$ e temos o homomorfismo injetivo $G(P)/N(P) \hookrightarrow (\mathcal{O}_P/P)^*$.

□

Mostraremos nessa seção que:

Teorema 3.2. *Seja P um lugar de um corpo de funções F/K de gênero $g \geq 1$ e seja p a característica de K.*

(a) *$G(P)/N(P)$ é um grupo cíclico finito de ordem limitada por uma constante que depende apenas de g e p;*

(b) *Se $p = 0$, então $N(P) = \{id\}$;*

(c) *Se $p > 0$, então $N(P)$ é um p-subgrupo de $G(P)$ com $|N(P)| \leq p^2(g+1)(2g-1)^2$.*

Note que esse teorema implica imediatamente a finitude de $G(P)$:

Corolário 3.3. *Se $p = 0$, $G(P)$ é um grupo cíclico finito e, mais geralmente, para qualquer valor de p, temos que $G(P)$ é um grupo finito de ordem limitada superiormente por uma constante que depende apenas de g e p.*

Provaremos os itens (a), (b) e (c) em sequência. A grande chave para essa demonstração será considerar uma representação de $G(P)$ no espaço das transformações linear de $L((2g+1)P)$ e utilizar certas propriedades de matrizes e grupos nilpotentes.

Para provar o item (a), utilizaremos também o seguinte resultado de teoria de grupos:

Lema 3.1. *Sejam L um corpo e G um subgrupo do grupo multiplicativo L^*. Se $r = \sup\{o(g) \mid g \in G\} < \infty$, então G é um grupo cíclico de ordem $|G| = r$.*

Demonstração. Seja r como no enunciado, sabemos da teoria de grupos que a ordem de todo elemento do grupo abeliano G deve dividir r (ver Garcia-Lequain [[5], Proposição V.3.11, página 135]. Logo, todo elemento de G é raiz do polinômio $x^r - 1 \in L[x]$ e, portanto, G deve ser um grupo finito de ordem menor ou igual a r. Como existe um elemento $g \in G$ de ordem $o(g) = r$, vemos por outro lado que $|G| \geq r$ e, com isso, concluímos que $|G| = r$. Em particular, $G = \langle g \rangle$.

□

Dessa forma, como $G(P)/N(P) \hookrightarrow (\mathcal{O}_P/P)^* \cong K^*$, a demonstração de que $G(P)/N(P)$ é um grupo cíclico finito está concluída se mostrarmos, por exemplo, que o supremo das ordens dos elementos de $G(P)$ é finito, o que será feito na proposição 3.9. Construímos agora a representação mencionada acima.

Observamos que, pelo teorema de Riemann-Roch, $L((2g+1)P)$ possui dimensão $g+2$ sobre K e, então, podemos escolher uma base $\{x_1, ..., x_{g+2}\}$, de forma que, para cada $i = 1, ..., g+2$, o conjunto $\{x_i, ..., x_{g+2}\}$ seja uma base para algum $L(n_iP) \subseteq L((2g+1)P)$, com $n_i \leq 2g+1$. Nesse caso, como cada $\sigma \in G(P)$ fixa P e, portanto, induz um automorfismo K-linear de $L(nP)$, para todo natural n, temos que

$$\sigma(x_i) = a_i x_i + \sum_{j>i} a_{ji} x_j,$$

para certos $a_i \in K^*$ e $a_{ji} \in K$. Matricialmente:

$$(\sigma(x_1), ..., \sigma(x_{g+2})) = (x_1, ..., x_{g+2}) A_\sigma,$$

onde

$$A_\sigma = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ * & & a_{g+2} \end{pmatrix}$$

é uma matriz triangular inferior com autovalores $a_1, ..., a_{g+2}$. Observe que, de fato, esses autovalores são não nulos, pois A_σ é um automorfismo K-linear de $L((2g+1)P)$ e, portanto, $\det A_\sigma \neq 0$.

Proposição 3.8. *A aplicação $\rho : \sigma \in G(P) \mapsto A_\sigma \in GL(g+2, K)$ é uma representação fiel de $G(P)$.*

Demonstração. É imediato verificar que ρ é um homomorfismo de grupos. Seja $\sigma \in \ker(\rho)$, então A_σ é a matriz identidade, ou, equivalentemente,

$$\sigma(x_i) = x_i, \qquad i = 1, ..., g+2.$$

Em particular, temos que σ é a identidade em $K(x_1)$, $K(x_2)$ e $K(x_1, x_2)$. Queremos mostrar que σ é a identidade em F e, para tal, é suficiente mostrar que $K(x_1, x_2) = F$. Por um lado, note que $[F : K(x_1, x_2)]$ é um divisor comum de $[F : K(x_1)]$ e $[F : K(x_2)]$, mas, por outro lado, como $x_1 \in L((2g+1)P) \backslash L(2gP)$ e $x_2 \in L(2gP) \backslash L((2g-1)P)$, temos

que

$$[F : K(x_1)] = \text{grau}(x_1)_\infty = 2g + 1,$$
$$[F : K(x_2)] = \text{grau}(x_2)_\infty = 2g$$

são primos entre si.

□

Essa representação nos ajudará a obter uma cota dependendo apenas de g e p para a ordem dos elementos de $G(P)$.

Lema 3.2. *Seja $\sigma \in \text{Aut}(F/K)$ tal que $\sigma(K(x)) = K(x)$, para algum $x \in F\backslash K$. Se $p = char(K)$ não divide $n = [F : K(x)]$, então σ possui ordem finita, limitada por uma constante dependendo apenas de g, p e n.*

Demonstração. Consideramos primeiramente o caso em que $p = 0$. Nesse caso, sejam $P_1, ..., P_r$ os lugares de F que aparecem na expressão da diferente da extensão $F/K(x)$, digamos acima dos lugares $Q_1, ..., Q_s$ de $K(x)$. Cada Q_i possui conorma

$$e_1 P_{i_1} + ... + e_{t_i} P_{i_{t_i}}$$

e, pelo teorema da diferente de Dedekind, contribui com

$$(e_1 - 1)P_{i_1} + ... + (e_{t_i} - 1)P_{i_{t_i}}$$

na expressão da diferente. Pela igualdade fundamental, o grau dessa contribuição é $\sum_j (e_j - 1) = n - t_i \leq n - 1$. Como, pela fórmula de Hurwitz para a extensão $F/K(x)$, o grau de $\text{Diff}(F/K(x))$ é

$$d = 2g + 2n - 2 > 2n - 2 = 2(n - 1),$$

concluímos que existem pelo menos três e no máximo d lugares entre os Q_i.

Além disso, como σ permuta os conjuntos $\{P_i\}$ e $\{Q_i\}$, mantendo a diferente fixa (ver proposição 3.2), concluímos que existe alguma potência σ^l, com

$$l \leq d(d - 1)(d - 2)$$

tal que σ^l fixa três dos P_i e, consequentemente, três dos Q_i. Pelo corolário 3.2, temos que σ^l é a identidade em $K(x)$ e, por fim, como $n = [F : K(x)]$, concluímos que a ordem de σ satisfaz

$$o(\sigma) \leq nl \leq nd(d - 1)(d - 2).$$

Suponha, então, $p \neq 0$, e, pela forma canônica de Jordan, como $\mathrm{Aut}(K(x)/K) \cong PGL(2, K)$, basta considerar os casos em que $\sigma(x) = x + a$ e $\sigma(x) = ax$, para $a \in K^*$. No primeiro caso, $\sigma^p(x) = x$ e, portanto, σ^p é a identidade em $K(x)$. Como $[F : K(x)] = n$, concluímos que

$$o(\sigma) \leq pn.$$

O segundo caso requer cuidado. Primeiramente, supomos que o divisor de x com respeito à extensão F/K seja da forma $nP - nQ$, onde P e Q são lugares de $K(x)$ totalmente ramificados em F. Nesse caso, como $p \nmid n$, pelo teorema da diferente de Dedekind, as contribuições de P e Q para a expressão da diferente são respecitvamente $(n-1)P$ e $(n-1)Q$. Como, pela fórmula de Hurwitz, $d > 2(n-1)$, concluímos que existe um terceiro lugar de $K(x)$ contribuindo para a expressão da diferente. Utilizando os mesmos argumentos do caso $p = 0$, concluímos então que

$$o(\sigma) \leq nd(d-1)(d-2).$$

Suponha agora que o divisor dos zeros ou o divisor dos polos de x possua dois lugares $P_1 \neq P_2$ em sua expressão. Digamos que isso ocorra no divisor dos polos. Primeiramente, como σ fixa o divisor de polos de x permutando os lugares em sua expressão, existe uma potência σ^l, com $l \leq n = \mathrm{grau}(x)_\infty$, tal que σ^l fixe P_1 e, nesse caso, seja $r \leq g + 1$ o menor natural para o qual $L(rP) \neq K$, isto é, a primeira não lacuna em P, então $L(rp)$ possui dimensão 2 e existe $y \in L(rP_1) \backslash K$ tal que $\sigma^l(y) = by + c$, para certos b, $c \in K$. Se $b = 1$, então σ^{pl} é a identidade em $K(y)$ e, portanto, como $[F : K(y)] = \mathrm{grau}(y)_\infty = r$, concluímos que

$$o(\sigma) \leq plr \leq pn(g+1).$$

Finalmente, consideramos o caso em que $b \neq 1$ e podemos assumir $\sigma^l(y) = by$, pois, para todo $i \geq 1$,

$$\sigma^{li}(y) = b^i y + \frac{c(b^i - 1)}{b - 1}.$$

Seja $H = \sum a_{ij} X^i Y^j \in K[X, Y]$ irredutível tal que $H(x, y) = 0$, então $H(a^l x, by) = H(\sigma^l(x), \sigma^l(y)) = 0$ e, portanto, existe $k \in K$ tal que

$$\sum a_{ij} a^{li} b^j X^i Y^j = H(a^l X, bY) = kH(X, Y) = \sum k a_{ij} X^i Y^j.$$

Como H é irredutível, existem pelo menos dois coeficientes a_{ij} e a_{st} não nulos e, comparando coeficientes de $X^i Y^j$ e $X^s Y^t$, vemos que $a^{li} b^j = k = a^{ls} b^t$. Logo, $a^{l(i-s)} b^{j-t} = 1$ e,

isso nos mostra, por exemplo, que a função racional $z = x^{i-s}y^{j-t}$ é fixada por σ^l. Observe também que essa função não é constante, pois x possui polo em P_2, mas y apenas possui polo apenas em P_1. Mais ainda, como H é um polinômio de grau menor ou igual a $[F : K(y)] = \text{grau}(y)_\infty$ na variável X e de grau menor ou igual a $[F : K(x)] = \text{grau}(x)_\infty$ na variável Y, vemos que

$$|i - s| \leq \text{grau}(y)_\infty = r \leq g + 1,$$
$$|j - t| \leq \text{grau}(x)_\infty = n.$$

Dessa forma, pela expressão de z, temos que

$$[F : K(z)] = \text{grau}(z)_\infty \leq \text{grau}(x)_\infty |i - s| + \text{grau}(y)_\infty |j - t| \leq 2n(g + 1).$$

Por fim, como σ^l é a identidade em $K(z)$, vemos que

$$o(\sigma) \leq l[F : K(z)] \leq 2n^2(g + 1).$$

□

Proposição 3.9. $\sup\{o(\sigma) \mid \sigma \in G(P)\} < M$, *onde* M *é uma constante que depende apenas de* g *e* p.

Demonstração. Seja $\sigma \in G(P)$, buscamos uma função $x \in F$ nas condições do lema 3.2 e, para tal, utilizaremos a representação ρ da proposição 3.8. Supomos primeiramente que a matriz $A_\sigma = \rho(\sigma)$ seja diagonalizável e, nesse caso, mudando a base se necessário, podemos supor que $\sigma(x_i) = a_i x_i$. Lembramos que, pela construção de nossa base, $\{x_i, ..., x_{g+2}\}$ é uma base de $L(n_i P)$, para $n_i \leq 2g + 1$. Em particular, $\sigma(K(x_1)) = K(x_1)$ e $\sigma(K(x_2)) = K(x_2)$. Se

$$[F : K(x_1)] = \text{grau}(x_1)_\infty = 2g + 1$$

não for divisível por p, então σ e x_1 estão nas condições do lema 3.2 e conseguimos obter uma cota para a ordem de σ que depende apenas de g e p. Se esse grau for divisível por p, então observamos que

$$[F : K(x_2)] = \text{grau}(x_2)_\infty = 2g$$

não o é e, portanto, σ e x_2 estão nas condições do lema 3.2 e obtemos uma cota para a ordem de σ dependendo apenas de g e p.

Finalmente, consideramos o caso em que a matriz A_σ não é diagonalizável. Em particular, pela forma canônica de Jordan, existem autovalores $a_i = a_j$, $i \neq j$, e elementos

x, y_0 linearmente independentes tais que

$$\sigma(x) = a_i x,$$
$$\sigma(y_0) = x + a_i y_0.$$

Escolhendo $y = x + a_i y_0$, vemos que

$$\sigma(y) = 2a_i x + a_i^2 y_0 = a_i(x + y)$$

e, portanto, tomando $z = y/x$, temos que

$$\sigma(z) = \frac{a_i(x+y)}{a_i x} = z + 1.$$

Logo, $\sigma(K(z)) = K(z)$ e, se $p = 0$, o lema 3.2 nos garante que σ possui ordem finita. Por sua vez, se $p > 0$, então σ^p é a identidade em $K(z)$ e, portanto, como $\text{grau}(z)_\infty \leq \text{grau}(x)_\infty + \text{grau}(y)_\infty \leq 2(2g+1)$, pois x, $y \in L((2g+1)P)$, concluímos que

$$o(\sigma) \leq p[F : K(z)] = p\,\text{grau}(z)_\infty \leq 2p(2g+1).$$

□

Dessa forma, como mencionado anteriormente, em virtude do lema 3.1, concluímos que $G(P)/N(P)$ é um grupo finito cíclico; mais ainda, sua ordem é limitada superiormente por uma constante que depende apenas de p e g.

O próximo passo na demonstração do teorema 3.2 consiste em mostrar que $N(P)$ é um grupo finito, provando os itens (b) e (c) do enunciado. A demonstração do item (b) é simples e será feita na proposição 3.10. A prova do item é mais envolvente: será feita na proposição 3.11 com a ajuda dos lemas 3.3, 3.4 e 3.5 bem como de alguns resultados sobre grupos nilpotentes. Definições e propriedades gerais de grupos nilpotentes podem ser encontradas em [11].

A estratégia será ainda considerar a representação ρ mas agora restrita ao grupo $N(P)$. Note que, se $\sigma \in N(P)$ e t é um parâmetro local em P, então, para cada $i = 1, ..., g+2$, existe $u_i \in \mathcal{O}_P^*$ e $n_i \in \mathbb{N}$ tais que $x_i = u_i t^{-n_i}$ e, nesse caso, como já discutido na demonstração da proposição 3.7, devemos ter

$$\frac{\sigma(x_i)}{x_i} \equiv \frac{\sigma(u_i)}{u_i}\frac{t^{n_i}}{\sigma(t)^{n_i}} \equiv 1 (\text{mod } P).$$

Logo, existem $v_i \in \mathcal{O}_P^* \cup \{0\}$ e um natural positivo m_i tais que

$$\sigma(x_i) = x_i + v_i t^{m_i} x_i.$$

Claramente, o termo $v_i t^{m_i} x_i = v_i u_i t^{m_i - n_i}$ é elemento de um espaço $L(s_i P) \subsetneq L(n_i P)$ e, assim, vemos que o autovalor a_i é igual a 1. Isso nos fornece que, para um elemento $\sigma \in N(P)$, a matriz A_σ é unitriangular inferior, isto é, da forma

$$A_\sigma = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ * & & 1 \end{pmatrix}.$$

Estamos prontos para provar o item (a) do teorema 3.2:

Proposição 3.10. *Se $p = 0$, então $N(P) = \{id\}$.*

Demonstração. Seja $\sigma \in N(P)$, a matriz A_σ possui todos autovalores iguais a 1 e, portanto, A_σ é diagonalizável se, e só se, A_σ é a matriz identidade, isto é, se, e só se, $\sigma = id$, uma vez que a representação ρ é fiel (ver proposição 3.7). Logo, supondo $p = 0$, basta mostrar que A_σ é diagonalizável, para todo $\sigma \in N(P)$.

De fato, se A_σ não fosse diagonalizável, então pela forma canônica de Jordan, A_σ seria equivalente a uma matriz contendo pelo menos um bloco de Jordan com autovalor 1 e com pelo menos duas linhas. Seja $J(n)$ um bloco de Jordan de tamanho n, então $J(n) = I_n + M_n$, onde I_n é a matriz identidade n por n e M_n é a matriz nilpotente com 1 na diagonal abaixo da diagonal principal e 0 nas demais entradas. Nesse caso, vemos que

$$J(n)^k = (I_n + M_n)^k = I_n + \binom{k}{1} M_n + \binom{k}{2} M_n^2 + \cdots + \binom{k}{k-1} M_n^{k-1} + M_n^k$$

não se anula para nenhum valor de $k \in \mathbb{N}$ em característica $p = 0$. No entanto, isso contradiz o fato de que todo $\sigma \in N(P)$ (e, portanto, toda matriz A_σ) possui ordem finita! □

O caso em que $p > 0$ requer mais cuidado. Primeiramente, note que em característica positiva, seja $J(n)$ um bloco de Jordan como na demonstração acima, sua p^n-ésima potência é igual a I_n, uma vez que os coeficientes binomiais se anulam e a n-ésima potência da matriz nilpotente M_n é a matriz nula. Logo, a ordem de toda matriz A_σ, para $\sigma \in N(P)$ é uma potência de p e, portanto, $N(P)$ é um p-subgrupo de $G(P)$. Observamos também que, como $N(P)$ é isomorfo, via a representação ρ, a um grupo de matrizes unitriangulares inferiores e o grupo das matrizes unitriangulares inferiores é nilpotente, então $N(P)$ é um grupo nilpotente.

Provamos agora os lemas que nos ajudarão a garantir a finitude de $N(P)$:

Lema 3.3. *Seja G um grupo de ordem maior ou igual a um natural n contendo um subgrupo central N de ordem p (primo) tal que o quociente G/N é abeliano e tal que todo*

elemento de G/N diferente do elemento neutro possua ordem p. Então G contém um subgrupo abeliano de ordem pelo menos $\sqrt{pn}$.

Demonstração. Observe antes de mais nada que podemos supor G finito, pois, caso contrário, como N é finito e todo elemento diferente do neutro de G/N possui ordem p, temos que G/N é naturalmente um espaço vetorial sobre $\mathbb{Z}/p\mathbb{Z}$ de dimensão infinita. Nesse caso, seja m um natural tal que $p^m \geq n$, escolhemos $m-1$ elementos linearmente independentes de G/N sobre $\mathbb{Z}/p\mathbb{Z}$ e o subgrupo (de ordem p^{m-1}) gerado por esses elementos é da forma $G'N/N$ para algum subgrupo $G' \leq G$. Assim, trocamos G por $G'N$, que é um grupo finito de ordem maior ou igual a $p^m \geq n$ e satisfaz as demais hipóteses do enunciado.

Supondo então G finito, consideramos U um subgrupo normal abeliano maximal de G contendo o centro de G e observamos que, como N é central, $N \leq Z(G) \leq U$ e o quociente $U/N \leq G/N$ possui a propriedade de que todo elemento diferente do neutro possui ordem p. Também existem elementos $\sigma_1, ..., \sigma_r \in U$ tais que suas classes módulo N formam uma base de U/N sobre $\mathbb{Z}/p\mathbb{Z}$. Mostraremos que U é um subgrupo de ordem maior ou igual a $\sqrt{pn}$.

Denotamos por $[a, b]$ o comutador entre a e b, isto é, $[a, b] = aba^{-1}b^{-1}$. Note que, como G/N é abeliano, temos que $[\sigma, \sigma_i] \in N$, para todo $\sigma \in G$ e para todo i. Isso nos permite construir uma aplicação de G em N^r dada por

$$\sigma \mapsto ([\sigma, \sigma_1], ..., [\sigma, \sigma_r]).$$

Note que a aplicação acima é um homomorfismo de grupos, pois, se ψ, $\sigma \in G$, então

$$[\sigma\psi, \sigma_i] = \sigma[\psi, \sigma_i]\sigma^{-1}[\sigma, \sigma_i] = [\psi, \sigma_i][\sigma, \sigma_i],$$

uma vez que $[\psi, \sigma_i] \in N \subseteq Z(G)$, para todo i.

Por fim, note que o núcleo desse homomorfismo contém U e é um subgrupo abeliano normal de G, de modo que deve ser o próprio grupo U. Em particular, isso nos mostra que o quociente G/U tem no máximo p^r elementos. Como, por outro lado, U/N possui p^r elementos, concluímos que U possui p^{r+1} elementos (pois N possui p elementos) e

$$n \leq |G| = |U||G/U| \leq p^{2r+1}$$

e, portanto, $|U| = p^{r+1} \geq \sqrt{pn}$.

□

Lema 3.4. *Seja H é um grupo abeliano tal que todo elemento possua ordem dividindo p^2. Se H possui um único subgrupo U de ordem p, então H é cíclico de ordem p ou p^2.*

Demonstração. Por hipótese, a ordem de qualquer elemento diferente do neutro é p ou p^2 e, como H possui um subgrupo U de ordem p, devemos ter que $|H| \geq p$. Supomos inicialmente que todo elemento possua ordem p. Se H possuísse ordem maior que p, então existiria $y \in H \backslash U$ e, nesse caso, o grupo gerado por y seria um subgrupo de H de ordem p distinto de U, um absurdo. Dessa forma, concluímos que H possui ordem p e, portanto, é cíclico.

Supomos por fim que existe $x \in H$ de ordem p^2 e note que, em particular, o grupo gerado por x contém um subgrupo de ordem p, que deve ser igual a U. Afirmamos que H é o grupo gerado por x, implicando H cíclico de ordem p^2. De fato, se não o fosse, existiria $y \in H \backslash \langle x \rangle$ e observamos que y deve possuir ordem p^2, pois, caso contrário, possuiria ordem p e, portanto, estaria contido em $U \subseteq \langle x \rangle$. Além disso, note que, como o grupo gerado por y possui um elemento de ordem p, devemos ter $U \subseteq \langle y \rangle$ e, portanto, $\langle x \rangle \cap \langle y \rangle = U$. Isso implica que o grupo gerado por x e y tem ordem

$$\frac{|\langle x \rangle||\langle y \rangle|}{|\langle x \rangle \cap \langle y \rangle|} = p^3.$$

Como H possui apenas um subgrupo de ordem p, pelo teorema da estrutura dos grupos abelianos finitamente gerados, vemos que o grupo gerado por x e y deve ser isomorfo a $\mathbb{Z}/p^3\mathbb{Z}$, que possui um elemento de ordem p^3, contradizendo o fato de que a ordem de todo elemento de H divide p^2.

□

Lema 3.5. *Se F/K é um corpo de funções de gênero $g > 0$ e H é um subgrupo abeliano de* $\mathrm{Aut}(F/K)$ *tal que:*

(a) *Todo elemento de H possui ordem potência de p;*

(b) *Todo elemento de H fixa um lugar P;*

(c) *Para todo subgrupo finito $U \leq H$, seu corpo fixo F^U é um corpo de funções racional;*

Então, H é um grupo cíclico de ordem 1, *p ou p^2. Além disso, mesmo se retirada a hipótese (c), ainda garantimos que H é um grupo finito, de ordem menor ou igual a $p^2(2g-1)$.*

Demonstração. Suponha que H seja um grupo abeliano satisfazendo as hipóteses (a), (b) e (c) do enunciado e suponha que H não seja trivial. Então, pela hipótese (a), existe um elemento de H de ordem p^n, para algum natural positivo n, e o subgrupo de H gerado por esse elemento contém um subgrupo U de ordem p, o qual deve ser cíclico, digamos gerado por σ.

Seja F^U o subcorpo de F fixo pelo subgrupo U, pela hipótese (c), existe $x \in F$ tal que $F^U = K(x)$. Observe que, pelo teorema 2.1, o divisor de x com respeito ao corpo de funções $K(x)/K$ deve possuir divisor de polos de grau $[K(x) : K(x)] = 1$ e, trocando x por x^{-1} ou por $x - k$, para algum $k \in K$, podemos supor que esse divisor seja $P \cap K(x)$ (ver descrição dos lugares de $K(x)/K$ na seção 3.2), onde P é o lugar fixado pelos elementos de H da hipótese (b). Nesse caso, como F/F^U é uma extensão Galois de grau $|U| = p$ e P é totalmente ramificado nessa extensão de corpos de funções, pois é fixo por todo elemento de $\mathrm{Aut}(F/F^U) = U$ (ver observação 3.1), temos que $(x)_\infty = pP$.

Para mostrar que H é cíclico de ordem p ou p^2, utilizamos o lema 3.4, bastando mostrar então que todo elemento de H possui ordem no máximo p^2 e que U é o único subgrupo de ordem p de H. Para mostrar esse primeiro fato, observe que como o grupo H é abeliano, por teoria de Galois, todo automorfismo $\tau \in H$ se restringe a um automorfismo de $F^U = K(x)$. Além disso, pela hipótese (b), τ fixa P, que é precisamente o divisor de polos de x no corpo de funções $K(x)/K$ e, assim, a proposição 3.6 nos permite concluir que

$$\tau(x) = ax + b$$

para certos a, $b \in K$. Como a ordem de τ é p^m, para algum natural positivo m, temos que $a^{p^m} = 1$ e, consequentemente, $a = 1$. Nesse caso, vemos que $\tau^p(x) = x$ e, portanto, a ordem de τ é no máximo $p[F : K(x)] = p^2$.

Suponha por fim que exista outro subgrupo V de H de ordem p e então V é cíclico gerado por um automorfismo ψ e $V \cap U = \{id\}$. Pelos mesmos argumentos utilizados acima, vemos também que existe $y \in F$ tal que o subcorpo F^V de F fixo por V seja da forma $K(y)$ com $(y)_\infty = pP$. Vimos também que $\psi(x) = x + a$, para algum $a \in K$ e, como $\psi \notin U$, devemos ter $a \neq 0$. Trocando x por x/a, podemos supor que $\psi(x) = x + 1$. Analogamente, como $y \notin U$, podemos supor que $\sigma(y) = y + 1$. Nesse caso, como $\sigma(x) = x$ e $\psi(y) = y$, vemos que $x^p - x$, $y^p - y \in F^{UV} = K(x) \cap K(y)$. Como os divisores de polos desses elementos são ambos iguais a p^2P e F/F^{UV} é uma extensão Galois de grau $|UV| = p^2$, vemos que $K(x^p - x) = K(y^p - y)$ e, portanto, existe $\tau \in \mathrm{Aut}(K(x^P - x)/K)$ tal que $y^p - y = \tau(x^p - x)$ e, pela proposição 3.6, temos que

$$y^p - y = c(x^p - x) + d$$

para certos c, $d \in K$.

Definimos $z = y - c^{1/p}x$, de forma que

$$z^p - z = (c^{1/p} - c)x + d$$

e observamos que, se $c^{1/p}-c \neq 0$, então $x \in K(z)$ e, portanto, $y \in K(z)$, pois $y = z+c^{1/p}x$. No entanto, como $V \cap U = \{id\}$, devemos ter que $F = F^{V \cap U} = K(x, y) \subseteq K(z)$, implicando que F é um corpo de funções racional, o que é um absurdo pois supomos $g > 0$. Finalmente, se $c^{1/p} - c = 0$, então $z \in K$ e, portanto, $K(x) = K(y)$, o que contradiz $V \cap U = \{id\}$.

Mostraremos agora que se H satisfaz apenas as hipóteses (a) e (b), então H é finito de ordem não excedendo $p^2(2g-1)$. Para tal, escolha um subgrupo finito $N \leq H$ ordem n (que existe pela hipótese (a)) maximal com a propriedade de que F^N não seja racional. Afirmamos que $n < 2g$. De fato, a extensão F/F^N é Galois de grau n e, pela fórmula de Hurwitz para essa extensão, o gênero g' de F^N se relaciona com o gênero g de F através da equação

$$2g - 2 = (2g' - 2)n + d$$

onde d é o grau da diferente da extensão F/F^N. Como pela hipótese (b), o lugar P se ramifica totalmente na extensão F/F^N com índice de ramificação $e(P|P \cap F^N) = [F : F^N] = n$, pelo teorema da diferente de Dedekind, sua contribuição na expressão da diferente é de pelo menos $n - 1$ e, portanto

$$2g - 2 \geq (2g' - 2)n + n - 1 > -n - 1.$$

Se $n \geq 2g$, então $2g' - 2 < 0$ e, consequentemente, $g' = 0$, um absurdo!

Finalmente, como o grupo H é abeliano, podemos considerar o quociente H/N, que ainda é um grupo abeliano. Além disso, H/N é o grupo de automorfismos da extensão F^N/F^H, que é um subgrupo do grupo de automorfismos da extensão F^N/K, e claramente satisfaz as hipóteses (a) e (b) do enunciado substituindo o lugar P por $P \cap F^N$. Como todo subgrupo de H/N corresponde a um subgrupo de H contendo N, pela maximalidade de N, conluímos que o corpo fixo por todo subgrupo de H/N é um corpo de funções racionais e, portanto, H/N satisfaz a hipótese (c) do enunciado. Pelo que acabamos de provar, devemos então ter $|H/N| \leq p^2$ e, consequentemente,

$$|H| \leq p^2|N| \leq p^2(2g - 1).$$

□

Proposição 3.11. *Se $p > 0$, então $N(P)$ é um p-grupo de ordem menor ou igual a $p^2(g+1)(2g-1)^2$.*

Demonstração. Considere o elemento $x = x_{g+1}$ da base $\{x_1, ..., x_{g+2}\}$ de $L((2g+1)P)$ e observe que x é um elemento do espaço $L(nP)$, onde $n \leq g+1$ é o primeiro natural tal que $L(nP) \supsetneq K$, isto é, é a primeira não lacuna em P. Logo, para $\sigma \in N(P)$, vemos que

existe único $\gamma_\sigma \in K$ tal que $\sigma(x) = x + \gamma_\sigma$ e a aplicação dada por $\sigma \mapsto \gamma_\sigma$ é claramente um homomorfismo do grupo $N(P)$ no grupo aditivo K. Denotaremos por N_0 o núcleo desse homomorfismo, de forma que temos um mergulho $N(P)/N_0 \hookrightarrow K$. Em particular, $N(P)/N_0$ é abeliano e a ordem de todo elemento diferente do elemento neutro é p. Além disso, como, para todo $\sigma \in N_0$, devemos ter $\sigma(x) = x$, vemos que $N_0 \subseteq \mathrm{Aut}(F/K(x))$ é um grupo finito de ordem menor ou igual a $[F : K(x)] = \mathrm{grau}(x)_\infty = n$.

Observe agora que, como $N(P)$ é um p-grupo nilpotente, podemos encontrar um subgrupo N_1 de N_0 normal em $N(P)$ e de índice p em N_0 e tal que $N_0/N_1 \leq Z(N(P)/N_1)$ (ver [[11], exercício 3, página 98]). Se F' é o corpo fixo pelo subgrupo N_1, devemos ter

$$p[F : F'] = [N_0 : N_1]|N_1| = |N_0| \leq |\,\mathrm{Aut}(F/K(x))| \leq n$$

e, portanto, F' possui gênero $g' > 0$. De fato, se $g' = 0$, pela proposição 3.5, existiria $y \in F\backslash K$ tal que $F' = K(y)$ e, como na demonstração do lema 3.4, podemos supor $(y)_\infty = n'P$, onde $n' = [F : F'] \leq n/p < n$. Isso no entanto, contradiz a minimalidade de n.

Como todo elemento distinto do neutro de

$$\frac{N(P)}{N_0} \cong \frac{N(P)/N_1}{N_0/N_1}$$

possui ordem p e o subgrupo N_0/N_1 de $N(P)/N_1$ é central de ordem p, concluímos, pelo lema 3.3, que, se $|N(P)/N_1| = m$, então $N(P)/N_1$ contém um subgrupo abeliano U de ordem pelo menos $\sqrt{pm}$. Por outro lado, como $N(P)/N_1$ pode ser visto como um subgrupo de $\mathrm{Aut}(F'/K)$, $g' > 0$ e todo subgrupo abeliano de $N(P)/N_1$ (e, em particular, U) obviamente satisfaz as hipóteses (a) e (b) do lema 3.5 para o lugar $P \cap F'$, sabemos que qualquer tais grupos possuem ordem limitada por $p^2(2g' - 1)$. Consequentemente, devemos ter

$$\sqrt{pm} \leq p^2(2g' - 1)$$

ou, equivalentemente, $m \leq p^3(2g' - 1)^2$. Isso nos mostra que $|N(P)/N_0| \leq p^2(2g' - 1)^2$.

Dessa forma, temos que

$$|N(P)| \leq |N_0|p^2(2g' - 1)^2 \leq np^2(2g' - 1)^2 \leq p^2(g + 1)(2g' - 1)^2.$$

Como desejamos uma cota superior que dependa apenas de g e p, observamos que a extensão F/F' é Galois e então podemos relacionar a quantidade $2g' - 1$ na expressão

acima com a quantidade $2g-1$ pela fórmula de Hurwitz para a extensão F/F':

$$2g-2=(2g'-2)[F:F']+d,$$

onde d é o grau da diferente da extensão F/F'. Como na demonstração do lema 3.3., o lugar P contribui com pelo menos $([F:F']-1)P$ na expressão da diferente e, portanto,

$$2g-1\geq(2g'-1)[F:F']\geq 2g'-1.$$

□

3.4 Automorfismos de um corpo de funções com $g>1$

Supomos nessa seção que F/K é um corpo de funções de gênero $g>1$ e, utilizando o fato de que $G(P)$ é finito para todo lugar P de F/K, mostraremos que $\mathrm{Aut}(F/K)$ é um grupo finito. Observe que a hipótese de $g>1$ nos garante que existem diferenciais holomorfas não nulas, pois $\Omega_F(0)$ possui dimensão g, e, mais ainda, como um divisor canônico possui grau $2g-2$, qualquer $\omega\in\Omega_F(0)$ não nula deve possuir pelo menos um zero.

Em particular, seja $\sigma\in\mathrm{Aut}(F/K)$, como σ induz um transformação K-linear em $\Omega_F(0)$ (ver proposição 3.4), também denotada por σ, podemos obter uma diferencial $\omega\in\Omega_F(0)$ não nula e $k\in K$, a saber um autovetor de σ e seu correspondente autovalor, tais que

$$\sigma(\omega)=k\omega.$$

Nesse caso, σ permuta os zeros de ω e, como ω possui $2g-2$ zeros (não necessariamente distintos entre si), concluímos que existe um natural positivo $n\leq 2g-2$ tal que σ^n fixa pelo menos um dos zeros de ω. Seja P tal zero, temos então que $\sigma^n\in G(P)$, o que nos permite concluir que σ possui ordem

$$o(\sigma)\leq(2g-2)|G(P)|<\infty.$$

Mais ainda, como σ foi tomado genericamente, vemos que

Proposição 3.12. *Todo elemento do grupo de automorfismos possui ordem finita e essas ordens são limitadas superiormente por uma constante que depende apenas de g e da característica p de K.*

Precisamos agora de alguns resultados sobre representações de grupos em espaços de transformações lineares. Seja V um espaço vetorial (de dimensão finita), denotamos por

$GL(V)$ o grupo de suas transformações lineares e, seja $\pi : H \to GL(V)$ uma representação de grupo, dizemos que um subespaço $W \leq V$ é invariante com respeito a π se $\pi(h)(w) \in W$, para todo $h \in H$ e $w \in W$. Nesse caso, temos uma representação $\pi_W : H \to GL(W)$, dada por $\pi_W(h) = \pi(h)$, que dizemos ser uma subrepresentação de π. Se os únicos subespaços de V invariantes com respeito a π são V e $\{0\}$, dizemos que π é uma representação irredutível. Observe que todo espaço vetorial de dimensão finita possui um subespaço invariante não nulo cuja subrepresentação associada é irredutível. Por fim, diremos que um grupo $K \leq GL(V)$ é irredutível se os únicos subespaços $W \leq V$ com $\sigma(W) \subseteq W$, para todo $\sigma \in K$, são os triviais e notamos que, se $\pi : H \to GL(V)$ é uma representação irredutível, então a imagem $\pi(H)$ é um grupo irredutível, dito o grupo irredutível associado a essa representação.

Lema 3.6 (**Burnside**). *Seja G um grupo irredutível de transformações lineares de um espaço de dimensão finita n. Se a ordem de todo elemento de G é limitada superiormente por uma constante $M > 0$, então o grupo G é finito. Mais ainda, sua ordem é limitada superiormente por uma constante dependendo de n e M.*

Demonstração. Ver Burnside [[2], Nota J, página 491].

□

Teorema 3.3. *O grupo de automorfismos de um corpo de funções F/K de gênero $g > 1$ é finito. Mais ainda, sua ordem é limitada superiormente por uma constante dependendo apenas de g e da característica p de K.*

Demonstração. Consideramos a representação de $\mathrm{Aut}(F/K)$ no conjunto das transformações K-lineares de $\Omega_F(0)$ e W um subespaço invariante cuja subrepresentação associada é irredutível. Sejam G_0 o núcleo dessa subrepresentação e G o grupo irredutível associado a essa subrepresentação, pelo teorema dos isomorfismos, temos que $G \cong \mathrm{Aut}(F/K)/G_0$. Observe que, como a ordem de todo elemento de $\mathrm{Aut}(F/K)$ possui uma cota superior, temos que a ordem de todo elemento de G é limitada superiormente por essa mesma cota e o lema acima nos fornece que G é um grupo finito com ordem limitada superiormente por uma constante dependendo apenas de g e p. Dessa forma, para provar que $\mathrm{Aut}(F/K)$ é finito e, mais ainda, que uma cota superior para essa ordem depende apenas de g e p, basta mostrar que G_0 é finito de ordem limitada superiormente por uma constante dependendo de g e p.

Seja $\omega \in W$ uma diferencial holomorfa não nula, pela definição de G_0, devemos ter

$$\sigma(\omega) = \omega$$

para todo $\sigma \in G_0$ e, assim, σ permuta os zeros de ω. Seja P um zero de ω, como ω possui $2g - 2$ zeros (não necessariamente distintos), consideramos o subgrupo $G_1 \leq G_0$

dos elementos de G_0 que fixam P e afirmamos que $[G_0 : G_1] \leq 2g - 2$. De fato, observe que, se duas classes laterais $\sigma_1 G_1$ e $\sigma_2 G_1$ são distintas, então $\sigma_1(P)$ e $\sigma_2(P)$ são zeros distintos de ω, mas ω possui no máximo $2g - 2$ zeros distintos.

Finalmente, como $G_1 \subseteq G(P)$, temos que G_1 possui ordem finita limitada superiormente por uma constante $m = m(g, p)$. Logo,

$$|G_0| \leq (2g - 2)m(g, p)$$

e isso conclui a demonstração.

□

3.5 Automorfismos de corpos de funções de gênero um

Discutimos até agora automorfismos de corpos de funções de gênero $g = 0$ e $g \geq 2$. Naturalmente, nos perguntamos qual a estrutura do grupo de automorfismos de um corpo de funções F/K de gênero 1. Existe uma teoria específica sobre corpos de funções desse tipo e para não perdermos o foco dessa dissertação, nessa seção, daremos apenas uma ideia da estrutura do grupo de automorfismos de tais corpos de funções. Omitimos então a demonstração de alguns resultados clássicos e, para mais detalhes, por exemplo, ver [13].

A estratégia é similar ao caso em que $g = 0$: mostramos que existem elementos $x, y \in F$ satisfazendo certa relação e tais que $F = K(x, y)$; em seguida, utilizamos essa descrição para estudar a estrutura do corpo de funções e classificar seus automorfismos.

Lema 3.7 (**Forma de Weierstrass**). *Seja F/K um corpos de funções de gênero 1. Existem $x, y \in F \backslash K$ e $a_1, a_2, a_4, a_5, a_6 \in K$ tais que*

$$y^2 + a_1xy + a_2y = x^3 + a_4x^2 + a_5x + a_6$$

e $F = K(x, y)$.

Demonstração. Ver Silverman [[13], Proposição 3.1, página 63].

□

Ao corpo de funções F estamos associando então uma curva de equação

$$Y^2 + a_1XY + a_2Y = X^3 + a_4X^2 + a_5X + a_6,$$

que podemos provar ser não singular, uma vez que se trata de uma cúbica de gênero 1. Estudar os automorfismos de F é então o mesmo que estudar os automorfismos dessa curva. Vamos mostrar a seguir apenas que tal grupo de automorfismos é infinito.

Para tal, precisamos do fato de que toda cúbica não singular E possui uma lei de grupo abeliano natural, isto é, existem morfismos $m : E \times E \to E$ e $i : E \to E$ e um ponto $0 \in E$ tais que

(a) $m(a, b) = m(b, a)$,

(b) $m(m(a, b), c) = m(a, m(b, c))$,

(c) $m(0, a) = m(a, 0) = a$,

(d) $m(i(a), a) = m(a, i(a)) = 0$,

para todo x, y, $z \in E$. Por conveniência, escrevemos $a + b = m(a, b)$ e $-a = i(a)$.

Uma construção geométrica dessa lei de grupo, utilizando interseção de curvas, pode ser encontrada em Fulton [[4], Proposição 4, página 63]. Para uma construção explícita utilizando a forma de Weierstrass, ver Silverman [[13], Algoritmo da Lei de Grupo 2.3, página 58]. A construção explícita, por exemplo, nos mostra imediatamente que a soma e a operação de inverso são morfismos.

Vamos mostrar aqui como fazer essa construção algebricamente:

Lema 3.8. *Seja F/K um corpo de funções de gênero $g = 1$. Se as classes de lugares $[P]$ e $[Q]$ são iguais, então $P = Q$.*

Demonstração. Se $[P] = [Q]$, então existe $x \in F$ tal que $P = Q + (x)$ e, nesse caso, vemos que $x \in L(Q)$. Pelo teorema de Riemann-Roch, como $g = 1$, temos que $l(Q) = 1$. Logo, $x \in L(Q) = K$ e, portanto, $(x) = 0$, o que conclui a demonstração.

□

Proposição 3.13. *Denotamos por $Pic^0(F/K)$ o grupo de classes de divisores de grau zero e seja Q um lugar qualquer de F/K. Então, existe uma bijeção entre os lugares de F/K e $Pic^0(F/K)$ dada por $P \mapsto [P] - [Q]$.*

Demonstração. Denotemos por $\mathcal{P}$ o conjunto dos lugares de F/K e $\mathrm{Div}^0(F/K)$ o grupo dos divisores de grau 0. Dado $D \in \mathrm{Div}^0(F/K)$, notamos primeiramente que existe único $P \in \mathcal{P}$ tal que $[D] = [P] - [Q]$. De fato, como F/K possui gênero 1, pelo teorema de Riemann-Roch, temos que $L(D + Q) = 1$ e, seja $x \in L(D + Q)$ não nulo, temos que

$$0 \leq (x) + Q + D = Q + D.$$

Como D tem grau zero, devemos ter $Q + D = P$, para algum lugar P. Pelo lema acima, esse é o único lugar de F/K tal que $[D] = [P] - [Q]$.

Dessa forma, acabamos de construir uma aplicação $\sigma : \mathrm{Div}^0(F/K) \to \mathcal{P}$, que imediatamente vemos ser sobrejetiva. Afirmamos que $\sigma(D_1) = \sigma(D_2)$ se, e só se, $[D_1] = [D_2]$. De fato, por um lado, pela definição de σ, temos que

$$[\sigma(D_1)] - [\sigma(D_2)] = [D_1] - [D_2]$$

e, portanto, imagens iguais implicam $[D_1] = [D_2]$. Por outro lado, se as classes $[D_1]$ e $[D_2]$ coincidem, então $[\sigma(D_1)] = [\sigma(D_2)]$, o que implica $\sigma(D_1) = \sigma(D_2)$, pelo lema acima.

Logo, a aplicação σ induz uma bijeção $\tau : Pic^0(F/K) \to \mathcal{P}$, cuja inversa é dada por

$$\tau(P) = [P] - [Q].$$

□

Utilizamos a bijeção da proposição acima e a estrutura de grupo de $Pic^0(F/K)$ para definir a lei de grupo no conjunto dos lugares de F/K (ou, equivalentemente, no conjunto dos pontos da cúbica não singular associada a F/K). Pode-se provar que, tomando o lugar Q na proposição acima como o lugar associado ao ponto no infinito da cúbica na forma de Weierstrass, essa lei de grupo construída é a mesma lei de grupo geométrica que comentamos acima (ver Silverman [[13], Proposição 3.4, página 66]).

Finalmente, provamos que:

Teorema 3.4. $\mathrm{Aut}(F/K)$ *possui infinitos automorfismos.*

Demonstração. Vamos exibir uma classe de infinitos automorfismos da cúbica singular E associada a esse corpo de funções. Como a lei de grupo é um morfismo de E, dado um ponto $A \in E$, temos a *translação* por A

$$\begin{array}{rccc} \tau_A : & E & \to & E \\ & P & \mapsto & P + A \end{array},$$

que é um automorfismo de E. Seja B um outro ponto de E, então imediatamente verifica-se que $\tau_B = \tau_A$ se, e só se, $A = B$. Como existem infinitos pontos em uma curva sobre um corpo algebricamente fechado, concluímos que existem infinitos automorfismos de translação, o que conclui a prova.

□

Vale a pena mencionar que se sabem mais fatos sobre a estrutura do grupo de automorfismos. Por exemplo, se E uma cúbica não singular, segue de um famoso Lema de Rigidez que todo automorfismo de E é a composição entre um automorfismo de E

como grupo e de uma translação. Observe que um automorfismo de E como grupo fixa o lugar Q - o elemento neutro do grupo - e, portanto, uma descrição do grupo total parece necessitar conhecer o grupo de decomposição de Q, que já vimos ser um grupo finito na seção 3.3. No caso de $g = 1$, sua cardinalidade exata é conhecida (ver Silverman [[13], Teorema 10.1, página 103]).

Capítulo 4

Curvas com grupo de automorfismos trivial

No capítulo anterior, determinamos uma cota superior para a ordem do grupo de automorfismos de um corpo de funções de gênero maior que 1. Uma questão natural é encontrar uma cota inferior para essa ordem. Em 1961, Bayly mostrou em [3] que uma curva genérica de gênero maior que 2 possui grupo de automorfismos trivial mas sua demonstração não fornecia uma equação explícita para alguma curva com essa propriedade. Nesse capítulo, estudamos uma família de equações polinomiais, construídas por Turbek em [15], que definem curvas cujo grupo de automorfismos é trivial.

4.1 A equação da curva

Sejam m, n naturais primos entre si com $n > m + 1 > 3$, nesse capítulo daremos um exemplo de uma equação que define uma curva de gênero $g = (m-1)(n-1)/2$ cujo grupo de automorfismos é trivial. Mais precisamente, seja K um corpo algebricamente fechado de característica p como nos capítulos anteriores, supomos que $p \nmid nm(m-1)$ e, dados A, $B \in K\backslash\{0\}$, consideraremos a curva afim $\mathcal{C}$ de equação

$$f(x, y) = x^n + y^m + Axy + Bx = 0.$$

Calculamos suas derivadas parciais

$$f_x = nx^{n-1} + Ay + B,$$
$$f_y = my^{m-1} + Ax$$

e observamos que podemos escolher A e B de forma que $\mathcal{C}$ seja não singular, isto é, f_x e f_y não sejam simultaneamente zero em nenhum ponto de $\mathcal{C}$. De fato, seja $(x, y) \in \mathcal{C}$, se

$f_x(x,y) = f_y(x,y) = 0$ então, como $A \neq 0$, temos que

$$x = -\frac{my^{m-1}}{A}.$$

Também, como $f(x,y) = 0$, vemos que

$$(n-1)x^n - y^m = xf_x(x,y) - f(x,y) = 0.$$

Logo, y é uma das raízes $y_1, ..., y_r$ do polinômio

$$(n-1)(-1)^n \frac{m^n y^{n(m-1)}}{A^n} - y^m$$

e, portanto, os pontos singulares devem ser da forma

$$\left(-\frac{my_i^{m-1}}{A}, y_i\right).$$

Dessa forma, se para cada i, definirmos

$$B_i = \frac{(-1)^{n-1}m^{n-1}n}{A^{n-1}} y_i^{(m-1)(n-1)} + Ay_i$$

então tomando $B \in K\backslash\{-B_1, ..., -B_r\}$, vemos que

$$f_x\left(-\frac{my^{m-1}}{A}, y\right) = \frac{(-1)^{n-1}m^{n-1}n}{A^{n-1}} y^{(m-1)(n-1)} + Ay + B$$

não se anula na curva.

Provaremos nesse capítulo que:

Teorema 4.1. *Sejam A, $B \in K\backslash\{0\}$ escolhidos de forma que $\mathcal{C}$ seja não singular, então seu modelo projetivo não singular $\mathcal{C}'$ é uma curva de gênero $g = (m-1)(n-1)/2$ com grupo de automorfismos trivial.*

4.2 O modelo projetivo não singular de $\mathcal{C}$

Nessa seção, construímos o modelo projetivo não singular de $\mathcal{C}$, o qual será denotado por $\mathcal{C}'$, e calcularemos seu gênero. Por último, estudaremos algumas propriedades de seu corpo de funções $\mathrm{K}(\mathcal{C})$, que serão utilizadas nas seções subsequentes.

Para construir $\mathcal{C}'$, consideramos primeiramente o fecho projetivo de $\mathcal{C}$, denotado por

$\overline{\mathcal{C}}$, definido pela homogeneização de f:

$$F(X,Y,Z) = X^n + Y^m Z^{n-m} + AXYZ^{n-2} + BXZ^{n-1} = 0.$$

Nesse caso, vemos que $\overline{\mathcal{C}}$ possui um único ponto no infinito, a saber o ponto $P = [0:1:0]$. Além disso, como as derivadas parciais de F são

$$\begin{aligned} F_X &= nX^{n-1} + AYZ^{n-2} + BZ^{n-1}, \\ F_Y &= mY^{m-1}Z^{n-m} + AXZ^{n-2}, \\ F_Z &= (n-m)Y^m Z^{n-m-1} + (n-2)AXYZ^{n-3} + (n-1)BXZ^{n-2}, \end{aligned}$$

temos que P é um ponto singular, em particular, o único ponto singular de $\overline{\mathcal{C}}$. Dessa forma, já vimos que, se $\pi : \mathcal{C}' \to \overline{\mathcal{C}}$ é um morfismo birracional de $\mathcal{C}'$ em $\overline{\mathcal{C}}$, construir $\mathcal{C}'$ consiste em determinar os pontos $Q \in \mathcal{C}'$ acima do ponto P, isto é, tais que $\pi(Q) = P$:

Proposição 4.1. *Existe um único ponto $Q \in \mathcal{C}'$ acima de P.*

Demonstração. Escreva $\mathrm{K}(\mathcal{C}) = K(x,y)$ com x e y satisfazendo $f(x,y) = 0$. Os lugares de $\mathrm{K}(\mathcal{C})$ correspondem aos pontos do modelo projetivo não singular de $\mathcal{C}$, isto é, aos pontos de $\mathcal{C}$ e aos pontos acima de P. Além disso, as funções x e y são regulares em $\mathcal{C}$ e vamos mostrar que possuem polo em todo ponto acima de P. De fato, $\mathrm{K}(\overline{\mathcal{C}}) = K(X,Y,Z)$, com X , Y e Z satisfazendo $F(X, Y, Z) = 0$, e $\mathrm{K}(\mathcal{C}) \cong_K \mathrm{K}(\overline{\mathcal{C}})$ via a aplicação definida por $x \mapsto X/Z$ e $y \mapsto Y/Z$. A função Z/Y se anula em P e, assim, como $\pi : \mathcal{C}' \to \overline{\mathcal{C}}$ é um morfismo birracional, vemos que a função correspondente a Z/Y em $\mathrm{K}(\mathcal{C}')$ possui zero em todo ponto acima de P. Logo, $v_Q(y) < 0$ para todo Q acima de P e, como $x^n + y^m + Axy + Bx = 0$, concluímos que x também possui polo em Q. De fato, seja Q um ponto acima de P, se $v_Q(x) \geq 0$, teríamos que as funções x^n, y^m e xy possuem ordens distintas em Q e, portanto, pela expressão $f(x,y) = 0$ e como $v_Q(y) < 0$, deveríamos ter

$$v_Q(x) = \min\{nv_Q(x),\, mv_Q(y),\, v_Q(x) + v_Q(y)\} = mv_Q(y) < 0,$$

um absurdo.

Seja Q um ponto de $\mathcal{C}'$ acima de P, como $f(x,y) = 0$, temos que

$$\frac{x^n}{y^m} + A\frac{x}{y^{m-1}} + B\frac{x}{y^m} = -1$$

e, assim, aplicando a valorização v_Q na expressão acima, obtém-se que

$$\min\{n(v_Q(x)) - mv_Q(y), v_Q(x) - (m-1)v_Q(y), v_Q(x) - mv_Q(y)\} \leq 0.$$

Como $v_Q(x)$, $v_Q(y) < 0$, os valores no membro esquerdo da inequação acima são todos

distintos e vale a igualdade, o que implica

$$nv_Q(x) = mv_Q(y).$$

Da condição de $\text{mdc}(m, n) = 1$, conclui-se que $m \mid v_Q(x)$ e $n \mid v_Q(y)$ e, consequentemente, $|v_Q(x)| \geq m$ e $|v_Q(y)| \geq n$. Logo, se existisse mais de um ponto $Q \in \mathcal{C}'$ acima de P, teríamos que

$$\text{grau}(x)_\infty \geq 2m,$$
$$\text{grau}(y)_\infty \geq 2n.$$

No entanto, pelo critério de Eisenstein, verifica-se que $f(x, y)$ é irredutível como polinômio na variável y e, portanto, $[\text{K}(\mathcal{C}) : K(x)] = m$. Por sua vez, pelo teorema 2.1, tem-se que $\text{grau}(x)_\infty = [\text{K}(\mathcal{C}) : K(x)] = m$, o que contradiz as desigualdades acima.

□

Dessa forma, podemos enxergar $\mathcal{C}' = \mathcal{C} \cup \{Q\}$, onde Q é o único ponto acima de $[0 : 1 : 0]$, e, além disso, como esse ponto distinto é o único polo de x e $[\text{K}(\mathcal{C}) : K(x)] = m$, temos que $v_Q(x) = -m$. Da expressão $mv_Q(y) = nv_Q(x)$ provada acima, concluímos então que $v_Q(y) = -n$ e, portanto, $[K(\mathcal{C}) : K(y)] = \text{grau}(y)_\infty = n$. Em particular, isso nos mostra que f também é irredutível como polinômio na variável x. Como claramente f não é o produto entre um polinômio na variável x e um polinômio na variável y, concluímos mais ainda que f, como polinômio em duas variáveis, é irredutível.

Como a característica p não divide $m = [F : K(x)]$, vemos que a extensão $F/K(x)$ é separável. Seja $P_{x,\infty}$ o divisor de polos de x em $K(x)/K$ (ver seção 3.2), o corolário 2.2 nos mostra que $-2P_{x,\infty}$ é um divisor canônico e, pode-se provar que existe uma única diferencial η_x do corpo de funções $K(x)/K$ tal que $(\eta_x) = -2P_{x,\infty}$ e $\eta_x(1_{P_{x,\infty}}(x^{-1})) = -1$, onde $1_{P_{x,\infty}}(x^{-1})$ é o adele de $K(x)/K$ dado por $1_{P_{x,\infty}}(x^{-1})(P_{x,\infty}) = x^{-1}$ e $1_{P_{x,\infty}}(x^{-1})(P) = 0$, para todo lugar $P \neq P_{x,\infty}$ de $K(X)/K$ (ver Stichtenoth [[14], Proposição I.7.4, página 37]). Definimos

$$dx = \text{Cotr}_{F/K(x)}(\eta_x)$$

e, analogamente, definimos η_y e, como p não divide $n = [F : K(y)]$, a extensão $F/K(y)$ é separável e consideramos

$$dy = \text{Cotr}_{F/K(y)}(\eta_y).$$

Observação 4.1. A notação dx similar a de 1-formas é justificada. De fato, é possível definir a noção de 1-formas em um corpo de funções F/K e o conjunto das 1-formas,

denotado por Δ_F, é um F-espaço vetorial de dimensão 1, de forma que, dado um elemento separante z, isto é, um elemento $z \in F$ tal que $F/K(z)$ é uma extensão finita e separável, então toda 1-forma pode ser escrita na forma $g\,dz$, para alguma função $g \in F$. Além disso, $dz \neq 0$ se, e só se, z é separante e, nesse caso, definimos o quociente de 1-formas dw/dz como a única função $g \in F$ satisfazendo $dw = g\,dz$. Em particular, é possível com essa definição provar a regra da cadeia

$$\frac{dw}{dz} = \frac{dw}{dk}\frac{dk}{dz}$$

para todo elemento $k \in F$ separante. Por fim, observamos que, se $z \in F$ é separante, então a correspondência $g\,dz \mapsto g\,\mathrm{Cotr}_{F/K(z)}(\eta_z)$, onde η_z é diferencial de Weil como acima, define um F-isomorfismo entre Δ_F e o conjunto das diferenciais de Weil Ω_F. Em particular, seja P um lugar de F/K, podemos definir $v_P(g\,dz) = v_P(g\,\mathrm{Cotr}_{F/K(z)}(\eta_z))$. Para demonstrações e mais detalhes sobre esses fatos, ver, por exemplo, Stichtenoth [[14], Seções IV.1 e IV.3].

Para calcular o gênero de $\mathrm{K}(\mathcal{C})$, vamos avaliar o grau da diferencial

$$\omega = \frac{1}{f_y}dx = -\frac{1}{f_x}dy$$

de duas maneiras distintas.

Lema 4.1. *Se $v_P(z) \neq 0$ para algum lugar P de um corpo de funções F/K, então $v_P(g\,dz) = v_P(g) + v_P(z) - 1$, para toda função $g \in F$*

Demonstração. Como $v_P(g\,dz) = v_P(g) + v_P(dz)$, basta mostrar que $v_P(dz) = v_P(z) - 1$. Seja t um parâmetro local em P, utilizando a expansão P-ádica, não é difícil provar que, se $v_P(z) \neq 0$, então $v_P(dz/dt) = v_P(z) - 1$ (ver Stichtenoth [[14], Proposição IV.2.7, página 145]). Como pela regra da cadeia, $dz = (dz/dt)\,dt$, nosso problema se reduz a mostrar que $v_P(dt) = 0$.

Como t é um parâmetro local em P, devemos ter $v_P(t) = 1$ e, portanto, como $e(P|P \cap K(t))$ divide $v_P(t) = 1$, vemos que P é não ramificado na extensão $F/K(t)$. Além disso, como $dt \neq 0$, devemos ter $F/K(t)$ separável e, pelo teorema 2.10, sabemos que

$$(dt) = \mathrm{Con}_{F/K(t)}(-2(t)_\infty) + \mathrm{Diff}(F/K(t)).$$

Por um lado, pelo teorema da diferente de Dedekind, como a característica de F não divide $e(P|P \cap K(t)) = 1$, a contribuição de P na expressão da diferente é $d(P|P \cap K(t)) = e(P|P \cap K(t)) - 1 = 0$. Por outro lado, como P não é um polo de t, vemos que P não aparece na expressão da conorma de $-2(t)_\infty$. Assim, pela expressão de (dt), concluímos que $v_P(dt) = 0$.

□

Lema 4.2. *Seja $g \in K[x, y]$ um polinômio irredutível não constante, $l \in K[x, y]$ um polinômio de grau 1 e X e L as curvas plana definidas por $g = 0$ e $l = 0$, respectivamente. Se $P = (a, b)$ é um ponto não singular de X, denotamos por*

$$T_P(X) = \mathrm{Z}(f_x(P)(x - a) + f_y(P)(y - b))$$

a reta tangente a X em P e, nesse caso, temos que $L \neq T_P(X)$ se, e só se, a função racional definida por l é um parâmetro local em P.

Demonstração. Decorre essencialmente do fato de que na curva X, como P é simples, P corresponde a um lugar de $\mathrm{K}(X)$ e l é um parâmetro local em P se, e só se, $v_P(l) = 1$ e, por sua vez, $v_P(l) = 1$ se, e só se, L não é a reta tangente em P (ver Fulton [[4], teorema 1 e comentário subsequente, páginas 34 e 35]).

□

Proposição 4.2. *A curva $\mathcal{C}'$ possui gênero $g = (m - 1)(n - 1)/2$.*

Demonstração. Seja $P = (a, b) \in \mathcal{C}$, como $\mathcal{C}$ é não singular, $f_x(a, b) \neq 0$ ou $f_y(a, b) \neq 0$. No primeiro caso, o lema 4.2 nos fornece que $y - b$ é um parâmetro local em P e, portanto, pelo lema 4.1, temos que

$$v_P(\omega) = v_P\left(-\frac{1}{f_x}dy\right) = v_P(dy) = v_P(d(y - b)) = 0.$$

Analogamente, no segundo caso, vemos que $x - a$ é um parâmetro local em P e

$$v_P(\omega) = v_P\left(-\frac{1}{f_y}dx\right) = v_P(dx) = v_P(d(x - a)) = 0.$$

Logo, ω possui ordem nula em todo lugar correspondente aos pontos de $\mathcal{C}$.

Por sua vez, como $f_y = my^{m-1} + Ax$, $v_Q(y) = -n$ e $v_Q(x) = -m$, mais uma aplicação do lema 4.1 nos fornece

$$v_Q\left(\frac{1}{f_y}\,dx\right) = -\min\{-n(m - 1), -m\} + (-m - 1) = n(m - 1) - m - 1.$$

Assim, vemos que

$$\mathrm{grau}(\omega) = v_Q(\omega) + \sum_{P \in \mathcal{C}} v_P(\omega) = n(m - 1) - m - 1.$$

Por outro lado, como o divisor (ω) é canônico, possui grau $2g - 2$. Igualando o valor

obtido acima a $2g-2$, concluímos que

$$g = \frac{-m+1+n(m-1)}{2} = \frac{(n-1)(m-1)}{2}.$$

□

Observação 4.2. Até o final desse capítulo o divisor canônico $(\omega) = (2g-2)Q$ será denotado por W.

Encerramos a seção calculando as ordens de algumas funções de $\mathrm{K}(\mathcal{C})$ em pontos afins:

Lema 4.3. *Seja $P = (a,b) \in \mathcal{C}$:*

(a) *Se $P = (0,0)$, então $v_P(x) = m$ e $v_P(y) = 1$;*

(b) *Se $P \neq (0,0)$, então $v_P(x-a) = 1$ ou 2.*

Demonstração.

(a) Como $f_x(0,0) \neq 0$, y é parâmetro local em $P = (0,0)$ e, portanto $v_P(y) = 1$. A mesma técnica não se aplica a x, uma vez que $f_y(0,0) = 0$. Para resolver esse problema, observe, então, que o único zero de x ocorre em $P = (0,0)$, de forma que seu divisor de zeros é $(x)_0 = v_P(x)P$. Por sua vez, pelo teorema 2.1, $m = [K(C) : K(x)] = \mathrm{grau}(x)_0 = v_P(x)$.

(b) Basta mostrar que $v_P(x-a) = 2$, quando $x-a$ não é um parâmetro local em $P = (a,b) \neq (0,0)$, isto é, quando $f_y(a,b) = 0$, pelo lema 4.2. Para tal, calcularemos o grau de dx, vendo a contribuição de cada ponto de $\mathcal{C}'$.

Por um lado, como $v_P(dx) = v_P(d(x-a)) = v_P(x-a) - 1 = 0$ nos pontos $P = (a,b)$ em que $x-a$ é uniformizante local, vemos que

$$\mathrm{grau}(dx) = v_Q(dx) + \sum_P v_P(dx),$$

onde o somatório é sobre todos os pontos $P = (a,b)$ de $\mathcal{C}$ nos quais $x-a$ não é um parâmetro local. Note que esses pontos são precisamente os pontos na interseção das curvas definidas por $f = 0$ e de $f_y = 0$.

Pela expressão de f_y e f, tem-se que esses pontos são do tipo $(-my^{m-1}/A, y)$ e y é raiz de

$$h(y) = f\left(-\frac{my^{m-1}}{A}, y\right).$$

A derivada de h é dada por

$$h'(y) = -\frac{m(m-1)y^{m-2}}{A} f_x\left(-\frac{my^{m-1}}{A}, y\right) + f_y\left(-\frac{my^{m-1}}{A}, y\right).$$

Observando que a característica de K não divide $m(m-1)$, por hipótese, e que f_x não se anula em um ponto do tipo $(-my^{m-1}/A, y)$, pois $(-my^{m-1}/A, y)$ é um ponto não singular de $\mathcal{C}$ e f_y já se anula nesse ponto, concluímos que a única raiz múltipla de h é 0, de multiplicidade $m-1$.

Logo, como h é um polinômio de grau $n(m-1)$, existem $n(m-1)-(m-1) = 2g$ outros pontos $P = (a,b) \neq (0,0)$ onde $x-a$ não é uniformizante local. Nesse caso, supondo a existência de algum ponto desse tipo com $v_P(x-a) > 2$, tem-se que nesse mesmo ponto a ordem de dx é maior que 1 e, portanto:

$$\text{grau}(dx) \geq v_Q(dx) + v_{(0,0)}(dx) + 2g + 1 = (-m-1) + (m-1) + 2g + 1 = 2g - 1.$$

No entanto, isso contraria o fato de que o grau de um divisor canônico é $2g-2$.

□

4.3 A sequência de lacunas em pontos de $\mathcal{C}'$

Sabemos pela proposição 3.3 que, dado $\sigma \in \text{Aut}(\mathcal{C}')$, os lugares P e $\sigma(P)$ possuem a mesma sequência de lacunas. Nessa seção, mostraremos que Q sempre possui uma sequência de lacunas distinta da sequência em qualquer outro ponto de $\mathcal{C}$, exceto possivelmente em $(0,0)$. Dessa maneira, poderemos concluir que qualquer automorfismo de $\mathcal{C}'$ deve fixar Q ou, no máximo, trocar Q e $(0,0)$.

Para estudar a sequência de lacunas em Q, construiremos uma base para $L((m-1)nQ)$, que, em particular, contém os espaços $L(W) = L((2g-2)Q)$ e $L(W+Q) = L((2g-1)Q)$. Para ajudar nesse processo fornecemos dois lemas com propriedades da função "parte inteira":

Lema 4.4. *Sejam n e m inteiros positivos primos entre si. Então:*

$$\sum_{k=1}^{m-1} \left\lfloor \frac{kn}{m} \right\rfloor = \frac{(n-1)(m-1)}{2}.$$

Demonstração. Denote por $\{x\}$ a parte fracionária do número real x. Então, para $k \in$

$\{1, ..., m-1\}$, obviamente

$$\left\{\frac{nk}{m}\right\} + \left\{\frac{n(m-k)}{m}\right\} = 1$$

e, portanto:

$$m - 1 = \sum_{k=1}^{m-1} \left\{\frac{nk}{m}\right\} + \left\{\frac{n(m-k)}{m}\right\} = 2\sum_{k=1}^{m-1} \left\{\frac{nk}{m}\right\}.$$

Como para um número real x, $x = \lfloor x \rfloor + \{x\}$, segue que:

$$\sum_{k=1}^{m-1} \left\lfloor \frac{nk}{m} \right\rfloor = \sum_{k=1}^{m-1} \frac{nk}{m} - \sum_{k=1}^{m-1} \left\{\frac{nk}{m}\right\} = \frac{n(m-1)}{2} - \frac{m-1}{2} = \frac{(n-1)(m-1)}{2}.$$

□

Lema 4.5. *Sejam $n > m$ inteiros positivos tais que $m \nmid n$. Então,*

$$\left\lfloor \frac{n}{m} \right\rfloor = \#\{k \in \mathbb{N} \mid k < n \text{ com } k \equiv n (\text{mod } m)\}.$$

Demonstração. Considere a divisão euclidiana de n por m: existem q, $r \in \mathbb{N}$ tais que $n = qm + r$ e $r < m$. Por um lado, tem-se que $\lfloor n/m \rfloor = q$. Por outro lado, existem exatamente q naturais menores que n congruentes a n módulo m, a saber, r, $r + m$, ..., $r + (q-1)m$.

□

Proposição 4.3. *Uma base para o espaço $L((m-1)nQ)$ é*

$$\{x^i y^j \mid i, j \in \mathbb{N} \text{ com } mi + nj \leq (m-1)n\}.$$

Demonstração. Primeiramente, observe que, aplicando o teorema de Riemann-Roch para o divisor $(m-1)nQ$, como seu grau é maior que $2g-1$, conclui-se que

$$l((m-1)nQ) = (m-1)n + 1 - g.$$

Nesse caso, como o conjunto

$$T_Q = \{x^i y^j \mid i, j \in \mathbb{N} \text{ com } mi + nj \leq (m-1)n\}$$

está obviamente contido em $L((m-1)nQ)$, a tese segue se for provado que T_Q é linearmente independente e possui $(m-1)n + 1 - g$ elementos.

Para fazer essa contagem, introduzimos os conjuntos

$$A = \{0, 1, ..., (m-1)n\},$$
$$B = \{c \in A \mid c = mi + nj, \text{ para certos } i, j \in \mathbb{N}\}.$$

Note agora que $-v_Q$ é uma função sobrejetiva de T_Q em B. Mais ainda, é fácil verificar que é injetiva. De fato, se $mi + nj = -v_Q(x^i y^j) = -v_Q(x^{i'} y^{j'}) = mi' + nj'$, então

$$nj \equiv nj' (\text{mod } m) \quad \therefore \quad j \equiv j' (\text{mod } m)$$
$$mi \equiv mi' (\text{mod } n) \quad \therefore \quad i \equiv i' (\text{mod } n)$$

Por sua vez, como $mi + nj$ e $mi' + nj$ são ambos menores ou iguais a $(m-1)n$, tem-se que

$$0 \leq i, i' < n$$
$$0 \leq j, j' < m$$

e, portanto, as congruências acima implicam nas igualdades $i = i'$ e $j = j'$, de onde segue a injetividade da função $-v_Q$ em T_Q.

Logo, mostrar que T_Q possui $(m-1)n + 1 - g$ elementos equivale a mostrar que $\#B = (m-1)n+1-g$. Para tal, contamos o número de elementos de $A \backslash B$. Observe que, como m e n são primos entre si, para cada elemento de $a \in A$ existe um único elemento $0 \leq k < m$ tal que $a \equiv kn (\text{mod } m)$ e, nesse caso:

$$a \in A \backslash B \quad \iff \quad a < kn.$$

Para verificar a afirmação acima, escreva $a = kn + mw$, para certo $w \in \mathbb{Z}$. Por um lado, se $a \geq kn$, então $w \geq 0$ e, portanto, $a \in B$. Por outro lado, se $a \in B$, então existem $i, j \in \mathbb{N}$ tais que $a = mi + nj$, de forma que $k \equiv j (\text{mod } m)$ e, em particular, já vimos acima que, como $j < m$, devemos ter $k = j$. Nesse caso, $a - kn = mi \geq 0$.

Pelo lema 4.5, o número de inteiros não negativos menores que kn congruentes a kn módulo m é $\lfloor kn/m \rfloor$ e, portanto, pelo lema 4.4 e pela observação acima, o número de elementos em $A \backslash B$ é

$$\sum_{k=1}^{m-1} \left\lfloor \frac{kn}{m} \right\rfloor = \frac{(n-1)(m-1)}{2} = g.$$

Consequentemente, $\#B = \#A - \#A \backslash B = (m-1)n + 1 - g$, como queríamos provar.

Falta mostrar que T_Q é linearmente independente sobre K. No entanto, isso segue do fato de que as ordens dos elementos $x^i y^j$ em Q são $-(mi + nj)$, todas distintas entre si.

□

Como observado anteriormente, $L(W)$ e $L(W+Q)$ são subespaços de $L((m-1)n)$ e, portanto, como as ordens dos elementos em $\{x^iy^j \mid i,j \in \mathbb{N} \text{ com } mi+nj \leq (m-1)n\}$ são todas distintas em Q, segue imediatamente da proposição 4.3 que:

Corolário 4.1. *Os espaços vetoriais $L(W)$ e $L(W+Q)$ possuem respectivamente bases*

$$\{x^iy^j \mid i,j \in \mathbb{N} \text{ com } mi+nj \leq 2g-2\} \text{ e } \{x^iy^j \mid i,j \in \mathbb{N} \text{ com } mi+nj \leq 2g-1\}.$$

Estamos aptos para estudar as sequências de lacunas em Q:

Proposição 4.4. *Sejam $q, r \in \mathbb{N}$ com $n = qm - r$ e $0 \leq r < m$. Então, m não é lacuna em Q e, se $r \neq 1$, $n+r-1$ é lacuna em Q.*

Demonstração. Como $(x)_\infty = mQ$, m não é lacuna em Q. Considere agora $n+r-1 = qm-1$ e observe que $n+r-1 < 2n$ e $m \nmid n+r-1$. Já vimos que se $n+r-1$ não fosse lacuna, então existiriam $i,j \in \mathbb{N}$ tais que $n+r-1 = mi+nj$, e, nesse caso, pelas duas propriedades de $n+r-1$ mencionadas, teríamos $n+r-1 \equiv n (\text{mod } m)$, o que é um absurdo supondo $r \neq 1$.

□

Consideramos agora o estudo de lacunas em pontos afins de $\mathcal{C}'$:

Lema 4.6. *Seja $P \in \mathcal{C}$, então t é lacuna em P se, e só se, existe $h \in L(W)$ com $v_P(h) = t-1$.*

Demonstração. Aplicando o teorema de Riemann-Roch para os divisores tP e $(t-1)P$, obtém-se que

$$\begin{aligned} l(tP) &= t+1-g+l(W-tP), \\ l((t-1)P) &= t-1+1-g+l(W-(t-1)P) \end{aligned}$$

e, portanto:

$$l(tP) - l((t-1)P) = 1 + l(W-tP) - l(W-(t-1)P).$$

Vimos no lema 2.4 que t é lacuna em P se e, só se, $l(tP) = l((t-1)P)$ e a expressão acima nos mostra que isso ocorre se, e só se, $l(W-tP) < l(W-(t-1)P)$.

Como $L(W-tP) \subseteq L(W-(t-1)P)$, isso equivale a dizer que existe $h \in L(W-(t-1)P) \backslash L(W-tP)$, que é caracterizado pela propriedade do enunciado.

□

Proposição 4.5. *Sejam $P \in \mathcal{C}$ e $q, r \in \mathbb{N}$ com $n = qm - r$ e $r < m$:*

(a) *Se $P \neq (0,0)$, então m é lacuna em P;*

(b) *Se $P = (0,0)$, então $n + r - 1$ não é lacuna em P.*

Demonstração.

(a) Seja $P = (a,b)$, pelo lema 4.3, $v_P(x-a) = 1$ ou 2. No primeiro caso, a função $(x-a)^{m-1}$ possui ordem $m-1$ em P e, além disso, pela caracterização de $L(W)$ no corolário 4.1, conclui-se que $(x-a)^{m-1} \in L(W)$. Finalmente, o lema 4.6 garante que m é lacuna em P.

Por sua vez, se $v_P(x-a) = 2$, consideramos a divisão euclidiana de $m-1$ por 2: existem $s, t \in \mathbb{N}$ com $m-1 = 2s+t$ e $t \in \{0,1\}$. Nesse caso, já vimos que $f_y(a,b) = 0$ e, portanto, $f_x(a,b) \neq 0$, implicando que $y-b$ é um parâmetro local em P. Logo, a função $(x-a)^s(y-b)^t$ goza da propriedade de estar em $L(W)$ e possuir ordem $m-1$ em P e, mais uma vez, o lema 4.6 nos garante que m é lacuna em P.

(b) Observe que, pelo lema 4.3, a função $h = y/x^q$ possui polo apenas em $P = (0,0)$, de ordem $1 - qm = -(n+r-1)$. Dessa forma, $(h)_\infty = (n+r-1)P$ e, portanto, $n+r-1$ não é lacuna em $P = (0,0)$.

□

Um corolário imediato das proposições 4.4 e 4.5 é que:

Corolário 4.2. *Seja $P \in \mathcal{C}$, então os pontos Q e P possuem sequências de lacunas distintas, exceto possivelmente se $P = (0,0)$. Nesse caso, devemos ter $n \equiv -1 (\mathrm{mod}\ m)$.*

4.4 O grupo de automorfismos de $\mathcal{C}'$

Pela proposição 3.3, um ponto de $\mathcal{C}'$ e sua imagem por um elemento de $\mathrm{Aut}(\mathcal{C}')$ devem possuir as mesmas sequências de lacunas e, assim, o corolário 4.2 nos fornece que:

Proposição 4.6. *Seja $\sigma \in \mathrm{Aut}(\mathcal{C}')$, então $\sigma(Q) = Q$ ou $\sigma(Q) = (0,0)$. Mais ainda, se $\sigma(Q) = (0,0)$, então $n \equiv -1 (\mathrm{mod}\ m)$.*

Finalmente, o teorema 4.1 segue se provarmos que o único automorfismo com as propriedades acima é a identidade:

Proposição 4.7. *O único automorfismo de $\mathcal{C}'$ que preserva Q é a identidade.*

Demonstração. Seja $\sigma \in \mathrm{Aut}(\mathcal{C}')$ tal que $\sigma(Q) = Q$, denotamos por σ^* o K-automorfismo de $\mathrm{K}(\mathcal{C})$ induzido por σ. Por sua vez, x' e y' denotarão as imagens de x e y por σ^*, respectivamente.

Como x (resp. y) possui polo apenas em Q, de ordem $-m$ (resp. $-n$), temos que x' (resp. y') também possui polo apenas em Q, de ordem $-m$ (resp. $-n$). Nesse caso, concluímos que x', $y' \in L(W)$ e, portanto, pelo corolário 4.1, x' e y' podem ser escritos na forma

$$x' = \sum a_{ij} x^i y^j,$$
$$y' = \sum b_{ij} x^i y^j,$$

onde as somas acima são sobre os pares de naturais (i, j) com $mi+nj \leq 2g-2$. Para que x' (resp. y') possua polo em Q de ordem $-m$ (resp. $-n$), como $n > m$ e $v_Q(x^i y^j) = -mi-nj$, vemos que os únicos possíveis termos da forma $x^i y^j$ na expressão de x' (resp. y')acima são x e 1 (resp. y, x^q, ..., x e 1, onde q é o quociente da divisão euclidiana de n por m). Em outras palavras, existem a, $b \in K\backslash\{0\}$ e a_0, b_0, b_1, ..., $b_q \in K$ tais que

$$x' = ax + a_0$$
$$y' = by + b_0 + b_1 x + ...b_q x^q.$$

Por conveniência, escrevemos $h(x) = b_0 + ... + b_q x^q \in K[x]$.

Por sua vez, como x e y satisfazem $f(x, y) = 0$, temos que $f(x', y') = 0$, isto é:

$$g(x, y) = (ax + a_0)^n + (by + h(x))^m + A(ax + a_0)(by + h(x)) + B(ax + a_0) = 0$$

Podemos enxergar g como um polinômio na variável y, que possui grau m, coeficiente líder $b^m \in K\backslash\{0\}$ e satisfaz $g(x, y) = 0$. Como f possui grau m, é mônico, é irredutível como polinômio na variável y e também satisfaz $f(x, y) = 0$, concluímos que $g(x, y) = b^m f(x, y)$. No entanto, o coeficiente de y^{m-1} na expressão de g é $mb^{m-1}h(x)$, de onde obtemos que $h(x) = 0$. Da mesma forma, como o coeficiente de y na expressão de g é $Ab(ax + a_0)$, concluímos que $a = b = 1$ e $a_0 = 0$.

Logo, acabamos de provar que $x' = x$ e $y' = y$, de onde segue que σ é a identidade.

□

Proposição 4.8. *Não existe um automorfismo σ de $\mathcal{C}'$ tal que $\sigma(Q) = (0, 0)$.*

Demonstração. Suponha que exista um automorfismo σ de $\mathcal{C}'$ tal que $\sigma(Q) = (0, 0)$ e já vimos que, nesse caso, podemos supor $n \equiv -1 (\mathrm{mod}\ m)$. Denotaremos o ponto $(0, 0)$ por P e, assim como na demonstração anterior, denotaremos por σ^* o K-automorfismo de $\mathrm{K}(C)$ induzido por σ. Observe que, em virtude do corolário 4.2, o único possível ponto

que tem Q como imagem por σ é P e vice-versa. Em particular, isso nos mostra que σ possui ordem 2.

Procedemos de maneira análoga à demonstração da proposição 4.7. Para tal, observe que uma base para o espaço $L((2g-1)P)$ é

$$\{x^{-i}(y/x^q)^j \mid mi + nj \leq 2g-1\},$$

onde q é o único inteiro tal que $n = qm - 1$. De fato, note que, pelo lema 4.2,

$$v_P(x^{-i}(y/x^q)^j) = v_Q(x^i y^j)$$

e, assim, basta aplicar o mesmo argumento utilizado para obter o corolário 4.1. Sejam x' e y' as imagens de x e y por σ, respectivamente, então x', $y' \in L((2g-1)P)$ possuem respectivos divisores de polos mP e nP. Pela descrição de $L((2g-1)P)$ acima, concluímos como na demonstração da proposição 4.7 que existem $a, b \in K\backslash\{0\}$, $a_0 \in K$ e um polinômio h em uma variável sobre K tais que

$$\begin{aligned} x' &= ax^{-1} + a_0, \\ y' &= b(y/x^q) + h(x^{-1}). \end{aligned}$$

Como σ^2 é a identidade, devemos ter

$$x = \sigma^*(x') = \frac{a}{a/x + a_0} + a_0,$$

de onde segue que $a_0 = 0$. Por sua vez, como x e y satisfazem $f(x, y) = 0$, temos que $f(x', y') = 0$, isto é:

$$(a/x)^n + (h(1/x) + by/x^q)^m + A(a/x)(h(1/x) + by/x^q) + B(a/x) = 0.$$

Como na demonstração da proposição 4.7, podemos ver que $h(1/x) = 0$ e, portanto,

$$(a/x)^n + (by/x^q)^m + A(a/x)(by/x^q) + B(a/x) = 0.$$

Multiplicando por $x^{n+1} = x^{qm}$, obtemos que

$$a^n x + (by)^m + Aabyx^{n-q} + Bax^n = 0$$

o que, mais uma vez pela irredutibilidade de f, implica $n - q = 1$. No entanto, $n = mq - 1$ e, portanto, $(m-1)q = 2$, um absurdo, pois $n > m > 2$.

□

Bibliografia

[1] Atiyah, M.F. and Macdonald, I.G.. *Introduction to Commutative Algebra*. Reading: Addison-Wesley, 1963. 128 p.

[2] Burnside, W.. *Theory of Groups of Finite Order*. 2a. edição. London: Cambridge University Press, 1911. 512 p.

[3] Baily, W. L.. On the automorphism group of a generic curve of genus > 2. *J. Math. Kyoto Univ.*, v. 1, n.1, p. 101-108, 1961.

[4] Fulton, W.. *Algebraic Curves: an Introduction to Algebraic Geometry*. Disponível em: http://www.math.lsa.umich.edu/∼wfulton/CurveBook.pdf.

[5] Garcia, A. e Lequain, Y.. *Elementos de Álgebra*. 4a. edição. Rio de Janeiro: IMPA, 2006. 326 p.

[6] Hartshorne, R.. *Algebraic Geometry*. New York: Springer-Verlag, 1977. 496 p.

[7] Hurwitz, A.. Uber algebraische Gebilde mit Eindeutigen Transformationen in sich. *Mathematische Annalen*, v.41, n. 3, p. 403-442, 1893.

[8] Iwasawa, K. and Tamagawa, T.. On the group of automorphisms of a function field. *J. Math. Soc. Japan*, v. 3, n. 1, p. 137-147, mai. 1951.

[9] Iwasawa, K. and Tamagawa, T.. Correction: On the paper "On the group of automorphisms of a function field". *J. Math. Soc. Japan*, v. 4, n. 2, p. 203-204, out. 1952.

[10] Matsumura, H.. *Commutative Algebra*. 2a. edição. Reading: The Benajamin/Cummings Publishing Company, Inc, 313 p.

[11] Milies, C.P.. Grupos Nilpotentes: uma introdução. *Matemática Universitária*, n.34, p. 55-100, jun. 2003.

[12] Schmid, H.L.. Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik. *Crelles Journal*, v. 179, p. 5-15, jan. 1938.

[13] Silverman, J.H.. *The Arithmetic of Elliptic Curves*. 1a. edição. New York: Springer-Verlag, 400 p.

[14] Stichtenoth, H.. *Algebraic Function Fields and Codes*. 1a. edição. Berlin: Springer-Verlag, 260 p.

[15] Turbek, P.. An explicit family of curves with trivial automorphism groups. *Proceeding of the American Mathematical Society*, v. 122, n.3, p. 657-664, nov. 1994.