UNIVERSIDADE DE SÃO PAULO
Instituto de Ciências Matemáticas e de Computação

Automorfismos de curvas de Artin-Schreier

Abraham Rojas Vega

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

ICMC USP SÃO CARLOS

Abraham Rojas Vega

Automorfismos de curvas de Artin-Schreier

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

Área de Concentração: Matemática

Orientador: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
Novembro de 2021

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

Rojas Vega, Abraham
R741a Automorfismos de curvas de Artin-Schreier / Abraham Rojas Vega; orientador Herivelto Martins Borges Filho. -- São Carlos, 2022.
87 p.

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

1. Curvas algébricas. 2. Grupo de automorfismos. 3. Corpos de funções algébricas. I. Borges Filho, Herivelto Martins, orient. II. Título.

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

Abraham Rojas Vega

Automorphisms of Artin-Schreier curves

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

Concentration Area: Mathematics

Advisor: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
November 2021

AGRADECIMENTOS

Agradeço a meus pais, José e Susana, pelo amor sinceiro e incondicional que têm por mim. Agradeço que minha mãe seja uma excelente cozinheira, e que meu pai goste de falar sobre cultura na hora do almoço.

Agradeço a todos meus amigos, peruanos e estrangeiros, os que são da minha Igreja e os que são matemáticos. Sempre aprendo coisas deles, e espero me tornar uma pessoa mais sociável.
Agradeço a meu psicólogo, Otávio Beltramello, cuja ajuda não consigo expressar em poucas palavras.

Agradeço muito ao ICMC, a meu orientador, a meus professores e aos funcionários. Numa época difícil na minha vida, acredito que o ambiente da universidade me ajudou muito, acadêmica e emocionalmente. Agradeço também à CAPES pelo apoio financeiro.[1]

Ser grato dá as pessoas esperança e razões para seguir tentando melhorar. Acho que todos podemos e devemos ser mais gratos.

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

“Caminante, son tus huellas
el camino y nada más;
caminante, no hay camino,
se hace camino al andar.
Al andar se hace el camino,
y al volver la vista atrás
se ve la senda que nunca
se ha de volver a pisar.
Caminante no hay camino
sino estelas en la mar.”
(Antonio Machado)

RESUMO

ROJAS, A. **Automorfismos de curvas de Artin-Schreier**. 2021. 87 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2021.

Vamos usar a teoria de Corpos de Funções Algébricas em uma variável para estudar o grupo de automorfismos de curvas de Artin-Schreier, definidas sobre um corpo K algebricamente fechado de característica positiva. Nesse processo também estudaremos os subgrupos finitos de $\mathrm{PGL}(2,K)$.

Palavras-chave: Curvas algébricas, Grupo de automorfismos, Corpos de funções algébricas.

ABSTRACT

ROJAS, A. **Automorphisms of Artin-Schreier curves**. 2021. 87 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2021.

We use the theory of Algebraic Functions Fields in one variable to study the automorphism group of Artin-Schreier curves, defined over an algebraically closed field K of positive characteristic. In this process we also study the finite subgroups of $\mathrm{PGL}(2,K)$.

Keywords: Algebraic curves, Automorphism group, Algebraic function fields.

LISTA DE SÍMBOLOS

$\mathbb{A}^n(K)$, $\mathbb{A}^n$ — Espaço afim de dimensão n sobre o corpo K.

$\mathbb{P}^n(K)$, $\mathbb{P}^n$ — Espaço projetivo de dimensão n sobre o corpo K

$\operatorname{gr} f$ — Grau do polinômio f

$H \leqslant G$ — H é um subgrupo de G

$H \trianglelefteq G$ — H é um subgrupo normal de G

$1 \in G$ — Elemento neutro do grupo G, em muitos casos representa o mapa identidade

$|X|$ — Cardinal do conjunto X

$\mathbb{F}_q$ — Corpo finito de q elementos, onde $q = p^k$ e p é um número primo

$\overline{K}$ — Um fecho algébrico fixado do corpo K, onde estarão todas as extensões algébricas de K

$[L : K]$ — Grau (ou índice) da extensão de corpos L/K

$\operatorname{car} K$ — Característica do corpo K

F^G — Subcorpo de F fixado pelo grupo $G \leqslant \operatorname{Aut}(K)$

$F^\times$ — Grupo multiplicativo formado pelos elementos não nulos do corpo F

$ic_R(S)$ — Fecho integral do anel S no anel R

f e g são PESI — f e g são primos entre si

$\alpha = 1$ — O automorfismo α é a identidade

C_n — Grupo cíclico de ordem n

D_n — Grupo dihedral de ordem $2n$

A_n — Grupo alternante de grau n

S_n — Grupo simétrico de grau n

ζ_d — Uma raiz $d-$ésima primitiva da unidade fixada

SUMÁRIO

CAPÍTULO

1

INTRODUÇÃO

As Curvas Algébricas estão na interseção de diversas áreas da Matemática. Em Geometria Algébrica são as variedades algébricas de dimensão 1, e em Geometria Complexa são as superfícies de Riemann compactas.
Elas também são utilizadas em Criptografia, em Teoria de Códigos, e outras áreas da Ciência e da Engenharia.

Neste trabalho vamos olhar as curvas algébricas desde o ponto de vista da Geometria Algébrica. Muitos conceitos e resultados que mencionaremos têm análogos em Geometria Complexa, onde métodos da Análise (chamados de *transcendentes*) são utilizados. A Geometria Algébrica permite estender esses resultados para curvas sobre corpos distintos de $\mathbb{C}$, e tirar a hipótese de suavidade das curvas. A ideia é estudar as curvas e os mapas entre elas olhando para os corpos de funções delas e os mapas induzidos entre esses corpos. A teoria de Corpos de Funções Algébricas permite esse estudo, e também estabelece conexões com a Álgebra Comutativa e a Teoria dos Números.

O grupo de automorfismos (ou simetrias) de uma variedade (seja algébrica, diferencial, riemanianna...) determina uma grande parte da geometria dela. Em geral, objetos com mais automorfismos têm uma geometria mais rica. Por exemplo, em Topologia Algébrica existe uma correspondência entre os recobrimentos de um espaço e o grupo de automorfismos do seu recobrimento universal (uma situação análoga à Teoria de Galois para extensões de corpos).
Existe uma correspondência similar para curvas algébricas, porém nesse caso temos que considerar "morfismos fracos"(mapas racionais), que coincidem com os morfismos comuns quando as curvas são projetivas e não singulares. Além disso, os morfismos entre curvas algébricas podem ser ramificados. Um exemplo de morfismo ramificado é o mapa $z \mapsto z^n$ em $\mathbb{C}$, note que todo ponto fora da origem tem n preimagens, mas a origem só tem uma.

Entre algumas aplicações teóricas, temos que algumas famílias de curvas algébricas podem ser classificadas por seus grupos de automorfismos. Além disso, podemos achar as subex-

tensões separáveis de um corpo de funções olhando para o grupo de automorfismos (Teorema 17). Também existem aplicações práticas. Por exemplo, os Jacobianas de curvas hiperelíticas em característica dois são utilizados em sistemas criptográficos, baseados no problema do logaritmo discreto. Nessas aplicações é muito importante conhecer o grupo de automorfismos do corpo de funções da curva; a segurança oferecida pode ser reduzida se aquele grupo é muito grande (GÖB, 2004).

As curvas de Artin-Schreier são uma importante família de curvas algébricas, e têm sido muito estudadas recentemente. Algumas aplicações teóricas e práticas delas podem ser encontradas em (GÜNERI; ÖZBUDAK, 2007).
O objetivo deste trabalho é estudar a estrutura do grupo de automorfismos das curvas de Artin-Schreier utilizando a Teoria de Corpos de Funções Algébricas em uma variável.

Começaremos este capítulo mencionando os conceitos fundamentais da Geometria Algébrica, com foco em curvas algébricas. Logo apresentaremos alguns conceitos e resultados algébricos que serão necessários mais na frente.
No Capítulo 2 apresentaremos as ferramentas da Teoria de Corpos de Funções Algébricas que serão utilizadas nos próximos capítulos. No capítulo 3 mostraremos conexões entre essa teoria e a geometria das curvas algébricas, além de algumas aplicações importantes.
Os Capítulos 4 e 5 estão baseados em (VALENTINI; MADAN, 1980), onde são estudados os grupos de automorfismos de curvas de Artin-Schreier. Alguns resultados intermediários, como os subgrupos finitos de $\mathrm{PGL}(2,K)$, são muito importantes no estudo geral de curvas algébricas em característica positiva.

1.1 Curvas algébricas

Todas as definições e resultados nesta seção podem ser encontrados em (HARTSHORNE, 1977, Capítulo 1), salvo menção em contrário.

Seja K um corpo algebricamente fechado.
O **espaço afim n-dimensional** sobre K é o conjunto de n-uplas de elementos de K.
O **espaço projetivo n-dimensional** sobre K, é conjunto de classes equivalência de $A^{n+1} \setminus \{0\}$ dadas pela seguinte relação:

$$(a_0,\ldots,a_n) \sim (b_0,\ldots,b_n) \Longleftrightarrow \exists\, \lambda \in K^{\times} \text{ tal que } b_i = \lambda a_i,\ \forall\, 0 \leq i \leq n.$$

Um **conjunto algébrico afim** é o conjunto de zeros comuns em $\mathbb{A}^n(K)$ de uma família de polinômios em n variáveis.
Uma **conjunto algébrico projetivo** é o conjunto de zeros comuns em $\mathbb{P}^n(K)$ de uma família de polinômios homogêneos em $n+1$ variáveis.

A **topologia de Zariski**, em $\mathbb{A}^n(K)$ ou $\mathbb{P}^n(K)$, é a topologia cujos fechados são os conjuntos algébricos. Um conjunto algébrico é dito **irredutível** se não é união de dois subconjuntos

algébricos próprios.
Um subconjunto aberto de um conjunto algébrico afim (resp. projetivo) é um **conjunto algébrico quase-afim** (resp. **quase-projetivo**). Os conjuntos algébricos irredutíveis e seus subconjuntos abertos são chamados de **variedades algébricas**.

Dado $W \subset \mathbb{A}^n$, defina

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

Se W for uma variedade algébrica fechada então $I(W)$ é um ideal primo e o domínio $K[W] := \dfrac{K[x_1, \ldots, x_n]}{I(W)}$ é o **anel de coordenadas** de W.

Uma **curva algébrica plana afim** (resp. **projetiva**) é um conjunto algébrico em $\mathbb{A}^2$ (resp. em $\mathbb{P}^2$) que é o conjunto de zeros de um único polinômio; o **grau** da curva é definido como o grau daquele polinômio.
Uma reta é uma curva plana de grau 1. As **cônicas** são curvas planas de grau 2, as **cúbicas** têm grau 3, as **quárticas** têm grau 4, etc. Os círculos, as parábolas e as hipérbolas são cônicas.

Seja Y uma variedade quase-afim em $\mathbb{A}^n$. Uma função $f : Y \to K$ é **regular em P** $\in$ **Y** se existe um aberto $U \subset \mathbb{A}^n$ tal que $P \in U \subset Y$, e polinômios $g, h \in K[x_1, \ldots x_n]$ tais que h não se anula em U e $f = g/h$ em U. A função f é dita **regular** se for regular em todo ponto de Y.

Seja Y uma variedade quase-projetiva (em $\mathbb{P}^n$). Uma função $f : Y \to K$ é **regular em P** $\in$ **Y** se existe um aberto $U \subset \mathbb{A}^n$ tal que $P \in U \subset Y$, e polinômios homogêneos $g, h \in K[x_0, \ldots x_n]$ do mesmo grau tais que h não se anula em U e $f = g/h$ em U. A função f é dita **regular** se for regular em todo ponto de Y.

Se X e Y são variedades algébricas, um **morfismo** $\varphi : X \to Y$ é um mapa contínuo tal que para todo aberto $V \subset Y$ e toda função regular $f : V \to K$, a função $f \circ \varphi : \varphi^{-1}(V) \to K$ é regular.
Desta maneira, as variedades algébricas junto com os morfismos descritos acima formam uma categoria, que será denotada por $\mathfrak{C}$. A Geometria Algébrica é o estudo desta categoria.

Exemplo 1. 1. Seja $i = 1, \ldots, n$, o mapa

$$\varphi_i : \mathbb{A}^n \to \mathbb{P}^n \quad \varphi(a_1, \ldots, a_n) = [a_1 : \ldots 1, \ldots : a_n],$$

com 1 na $i-$ésima coordenada, é um isomorfismo sobre sua imagem, que é um aberto de $\mathbb{P}^n$. Seja $Y \subset \mathbb{P}^n$ uma variedade projetiva, temos que $\varphi_i^{-1}(Y)$ é uma variedade afim, chamada a **i−ésima carta local** de Y.

2. **O mergulho de Segre.** $\psi : \mathbb{P}^r \times \mathbb{P}^s \to \mathbb{P}^N$, $(a_0 : \ldots : a_r), (b_0, \ldots, b_s) \mapsto (\ldots, a_i b_j, \ldots)$ em ordem lexicográfica, com $N = rs + s + r$.
Ele é uma bijeção sobre sua imagem, que é uma subvariedade de $\mathbb{P}^N$. Isso permite definir uma estrutura de variedade em $\mathbb{P}^r \times \mathbb{P}^s$ (*espaço multiprojetivo*), tornando ψ num isomorfismo. Assim, $\mathfrak{C}$ admite produtos.

3. **O morfismo de Frobenius** ($\operatorname{car} K = p > 0$)**.** É um morfismo bijetivo que não é um isomorfismo, dado por

$$\varphi : \mathbb{P}^n \to \mathbb{P}^n, \quad (a_0, \ldots, a_n) \mapsto (a_0^p, \ldots, a_n^p).$$

4. Os morfismos entre variedades afins são os mapas polinomiais, i.e.,

$$f : \mathbb{A}^n \to \mathbb{A}^m, \quad f = (f_1, \ldots, f_m) \text{ tal que } f_i \in K[x_1, \ldots, x_n].$$

Seja Y uma variedade e $P \in Y$. O **anel local** de P em Y é formado pelas classes de equivalência (U, f), onde U é um aberto não vazio de Y que contém P, f é uma função regular em U, e onde (U, f) e (V, g) são equivalentes se $f = g$ em $U \cap V$.
Temos que $\mathscr{O}_P$ é de fato um anel local, cujo ideal maximal $\mathfrak{m}$ é formado pelas funções regulares que se anulam em P. O corpo residual $\mathscr{O}_P/M$ é isomorfo a K.

O **corpo de funções** $K(Y)$ de Y é o conjunto das classes de equivalência de pares (U, f), onde U é um aberto não vazio de Y, f é uma função regular em U, e onde dois pares (U, f) e (V, g) são equivalentes se $f = g$ em $U \cap V$. Os elementos de $K(Y)$ são chamados **funções racionais**, e formam um corpo.
Temos as inclusões naturais $K \hookrightarrow \mathscr{O}_P \hookrightarrow K(Y)$. Estes anéis são invariantes por isomorfismos.

A **dimensão** de uma variedade é o grau de transcendência do seu corpo de funções sobre K (veja Subseção 1.2.2).
Uma **curva algébrica** é uma variedade algébrica de dimensão 1. É fácil mostrar que toda curva algébrica plana é uma curva algébrica.

Sejam X e Y variedades algébricas. Um **mapa racional** $\varphi : X \to Y$ é uma classe de equivalência de pares (U, φ), onde U é um aberto não vazio de X, φ é um morfismo de U em Y, e onde (U, φ) e (V, ψ) são equivalentes se $\varphi = \psi$ em $U \cap V$. Um mapa racional é **dominante** se a imagem de um (e por tanto de qualquer) representante tem imagem densa no codomínio.
As variedades algébricas, junto com os mapas racionais dominantes, formam uma nova categoria, que será denotada por $\mathfrak{D}$. Os isomorfismos nessa categoria são chamados **mapas birracionais**, e as variedades isomorfas são ditas **birracionalmente equivalentes**. A partir daqui usaremos os termos **morfismos** e **isomorfismos** para morfismos e isomorfismos na categoria $\mathfrak{C}$.

Exemplo 2. 1. Seja $Y \subset \mathbb{A}^n$ uma variedade afim. Dado $P \in Y$,

$$\mathscr{O}_P = \{r \in K(X) : r = \frac{f}{g} \text{ para algum } f, g \in K[X] \text{ com } g(P) \neq 0\}.$$

O corpo de funções de Y coincide com o corpo de frações do seu anel de coordenadas.
Os mapas racionais entre variedades afins têm a forma

$$f : V \subset \mathbb{A}^n \to W \subset \mathbb{A}^m, \quad f = \left(\frac{f_1}{g_1}, \ldots, \frac{f_m}{g_m}\right) \text{ tal que } \frac{f_i}{g_i} \in K(V).$$

2. (SILVERMAN, 2009, Capítulo 1) Os anéis locais e os corpos de funções de variedades projetivas se definem como o anel correspondente à primeira carta local, que é uma variedade afim (Exemplo 1 (1)).
   Sejam V_1 e V_2 variedades projetivas. Um **mapa racional** $\phi : V_1 \to V_2$ é um mapa da forma $\phi = [\phi_0 : \ldots : \phi_n]$, onde

   a) os $\phi_i(X) \in K(V_1)$,

   b) se $\phi_0, \ldots, \phi_n \in \mathscr{O}_P$ então $[\phi_0(P) : \ldots : \phi_n(P)] \in V_2$.

   ϕ é dita **regular em P** se existe $g \in K(V_1)$ tal que $gf_i \in \mathscr{O}_P$ para todo i e $gf_i(P) \neq 0$ para algum i. Um **morfismo** é um mapa racional regular em todo ponto.

Sejam $X \subset \mathbb{A}^n$ uma variedade afim, $f_1, \ldots, f_r \in K[X]$ geradores de $I(X)$ e $P \in X$. X é **não singular em P** se $\left[\dfrac{\partial f_i}{\partial X_j}(P)\right]_{r\times n}$ tem posto $n-r$. A variedade é dita **não singular** se for não singular em cada ponto.
Um anel noetheriano local R com ideal maximal $\mathfrak{m}$ e corpo residual $k = R/\mathfrak{m}$ é dito um **anel local regular** se $\dim_k \mathfrak{m}/\mathfrak{m}^2 = \dim R$.

Teorema 3. Sejam $X \subset \mathbb{A}^n$ uma variedade afim e $P \in X$. X é regular em P se e somente se $\mathscr{O}_P$ é um anel local regular.

Seja Y uma variedade arbitrária. Y é **não singular em P** $\in$ **Y** se $\mathscr{O}_P$ é um anel local regular. Y é **não singular** se for não singular em todo ponto.

Teorema 4.
1. (SILVERMAN, 2009, Proposição II.2.1) Sejam $\mathscr{C}$ uma curva não singular, $P \in \mathscr{C}$ e $\varphi : \mathscr{C} \to \mathscr{D}$ um mapa racional. Então φ é regular em P. Em particular, se $\mathscr{C}$ é não singular então φ é um morfismo.

2. (HARTSHORNE, 1977, Proposição II.6.8) Se X e Y são curvas projetivas então todo mapa racional $\varphi : X \to Y$ é constante ou sobrejetor.

Seja $\mathscr{C}$ uma curva algébrica plana afim, dada por uma equação $f(x,y) = 0$, onde $f \in K[x,y]$ irredutível. Escreva

$$f = f_m + f_{m+1} + \cdots + f_n$$

onde os f_i são polinômios homogêneos de grau i e $f_m \neq 0$. O número m é a **multiplicidade** de X em $(0,0)$. Temos que $(0,0) \in \mathscr{C}$ se e somente se $m \geq 1$ e ele é singular se e somente se $m > 1$. No caso que se $(0,0) \in \mathscr{C}$ for singular, ainda podemos escrever

$$f_m = \prod l_i^{r_i}, \quad l_i \in K[x,y],\ \operatorname{gr} l_i = 1.$$

As retas $l_i(x,y) = 0$ são chamada de **retas tangentes** de $\mathscr{C}$ no ponto $(0,0)$. O ponto $(0,0)$ é uma **singularidade ordinária** se $\mathscr{C}$ possui m tangentes diferentes em $(0,0)$.

Os conceitos de multiplicidade, reta tangente e singularidade ordinária podem definidos em qualquer $P=(a,b)\in\mathscr{C}$, olhando para o ponto $(0,0)$ da curva $f(x+a,y+b)=0$.
Um **nó** é uma singularidade ordinária de multiplicidade 2. Por exemplo, a origem é um nodo da curva $y^2-x^2(x+1)=0$.

1.2 Tópicos de Álgebra

As definições e resultados nesta seção são clássicos e podem ser encontrados em (LANG, 2002), salvo menção em contrário.

1.2.1 Grupos e Ações

Sejam G um grupo, $N\trianglelefteq G$ e $H\leqslant G$. São equivalentes

1. Para todo $g\in G$ existem únicos $n\in N$, $h\in H$ tais que $g=nh$.
2. $G=NH=HN$, com $N\cap H=\{1\}$.
3. A composição da projeção canônica $\pi: G\to\dfrac{G}{N}$ com a inclusão $i: H\to G$ é um isomorfismo de grupos.
4. Existe um morfismo $f: G\to H$ tal que $f|_H=Id_H$ com núcleo N.

Nessa situação, diremos que G é o **produto semidireto** de N com H.

Sejam Q e N dois grupos. G é uma **extensão de Q por N** se existir uma sequência exata

$$1\longrightarrow N\longrightarrow G\longrightarrow Q\longrightarrow 1.$$

Note que se a sequência acima cinde pela direita, então a G é um produto semidireto.

Seja G um grupo e H um subgrupo. O cardinal do conjunto das classes laterais à esquerda $\{gH\mid g\in G\}$ é chamado de **índice** de H em G, e será denotado por $[G:H]$.

Observação 5. G age no conjunto das classes laterais a esquerda de H, fazendo $f\cdot gH:=(fg)H$. Seja $n=[G:H]$, temos um homomorfismo de grupos $G\to S_n$, induzido pela ação anterior, cujo núcleo é $\bigcap\limits_{g\in G} gHg^{-1}\subset H$.

O **centro** de G é o subgrupo

$$Z(G)=\{g\in G\mid gh=hg,\ \forall h\in G\}.$$

Se H é um subgrupo de ordem 2, é claro que $H \triangleleft G$ se e somente se $H \subset Z(G)$.
O **normalizador** de H em G é o subgrupo

$$N_G(H) = \{g \in G \mid gH = Hg\}.$$

Ele contém a todos os subgrupos K de G tais que $H \trianglelefteq K$, em particular $H \trianglelefteq N_G(H)$.

Seja p um fator primo de $|G|$. H é um $p-$**subgrupo** se $|H| = p^k$ para algum $k \in \mathbb{N}$; quando k é maximal, H é chamado de $p-$**subgrupo de Sylow**.

Teorema 6 (Teorema de Sylow)**.** Sejam G e p como acima. Temos:

1. Todos os $p-$subgrupos de Sylow são conjugados.
2. Todo $p-$subgrupo está contido num $p-$subgrupo de Sylow.
3. Seja n_p o número de $p-$subgrupos de Sylow, logo $n_p \equiv 1 \mod p$ e $n_p = [G : N_G(P)]$, onde P é qualquer $p-$subgrupo de Sylow.

Proposição 7. (HUNGERFORD, 1974, Capítulo II) Os subgrupos de ordem 12 são: $\mathbb{Z}_2 \times \mathbb{Z}_6$, $\mathbb{Z}_{12}$, A_4, D_6 e um grupo gerado por elementos a, b tais que $|a| = 6$, $b^2 = a^3$ e $ba = a^{-1}b$.

Proposição 8. (HUPPERT, 1967, Satz I.8.14) O único grupo simples de ordem 60 é A_5.

Grupos de matrizes

- $\mathrm{GL}(n,K)$: Matrizes quadradas invertíveis de ordem $n \times n$ sobre o corpo K.
- $\mathrm{PGL}(n,K)$: Grupo linear projetivo de dimensão n sobre o corpo K, i.e., $\mathrm{GL}(n,K)/K^\times$, onde $K^\times$ é identificado com as matrizes invertíveis de ordem $n \times n$ da forma $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, com $a \in K^\times$.
- $\mathrm{PGL}(n,q) := \mathrm{PGL}(n,\mathbb{F}_q)$, veja o Teorema 22.
- $\mathrm{PSL}(n,q)$: Grupo linear especial projetivo de dimensão n sobre $\mathbb{F}q$, i.e. o subgrupo de $\mathrm{PGL}(n,q)$ obtido ao considerar apenas matrizes com determinante 1 no quociente.
- $\mathrm{PGU}(n,q)$: Grupo unitário projetivo de dimensão n sobre $\mathbb{F}_q$, i.e., o subgrupo de $\mathrm{PGL}(n,q)$ obtido a considerar apenas matrizes ortogonais no quociente.

Proposição 9. (HUPPERT, 1967, Satz II.6.14)

1. $A_4 \simeq \mathrm{PSL}(2,3)$.
2. $S_4 \simeq \mathrm{PGL}(2,3)$.

3. $A_5 \simeq \mathrm{PGL}(2,4) \simeq \mathrm{PSL}(2,5)$.

Teorema 10. (ZASSENHAUS, 1936) Seja G um grupo de permutação $2-$transitivo de grau $n+1$, onde duas permutações são iguais se e somente coincidem em três pontos. Dados dois pontos, seja $\mathfrak{m}$ o subgrupo das permutações que fixam eles. Temos que

- $d := |\mathfrak{m}| = \dfrac{n-1}{2}$ ou $n-1$, e $|G| = d \cdot n \cdot (n+1)$.
- Se $d = \frac{n-1}{2}$ então $G \simeq \mathrm{PSL}(2,q)$, onde q é a potência de um primo impar.
- Se $d = n-1$ e $\mathfrak{m}$ é abeliano, então $G \simeq \mathrm{PGL}(2,q)$, onde q é a potência de um primo.

Seja um grupo G agindo num conjunto X. G é um **grupo de permutações** de X, e os elementos de X são chamados *pontos*. A ação será denotada por $g \cdot x$, ou por gx, onde $g \in G$ e $x \in X$. Dois pontos $x, y \in X$ são **conjugados** se existe $g \in G$ tal que $x = g \cdot x$. A **órbita** de x é o conjunto dos pontos conjugados com x.

Observação 11. $\alpha, \beta \in G$ são conjugados se existe $\omega \in G$ tais que $\omega(\alpha(P)) = \beta(\omega(P))$ para todo $P \in X$.

A ação é **transitiva** se possui uma única órbita. A ação é (**fortemente**) $k-$**transitiva** se para cada par $(x_1, \ldots, x_k), (y_1, \ldots, y_k) \in X^k$ existe (um único) $g \in G$ tal que $g \cdot x_i = y_i$ para cada $i = 1, \ldots, k$.

Dado $x \in X$, o **estabilizador** de X é o subgrupo $\mathrm{Stab}(x)$ tal que $g \cdot x = x$. O seguinte resultado, de fácil demonstração, relaciona os conceitos anteriores.

Observação 12. A ação de G sobre X é (fortemente) $k-$transitiva se e somente se a ação é transitiva e para todo $x \in G$, $\mathrm{Stab}(x)$ age (fortemente) $(k-1)-$transitivamente sobre $X \setminus \{x\}$.

1.2.2 Corpos e teoria de Galois

Proposição 13 (Decomposição em frações parciais)**.** Sejam $f(x)$ e $g(x)$ polinômios sobre um corpo K, e seja $g(x) = \prod_{i=1}^{k} p_i(x)^{n_i}$ uma descomposição de $g(x)$ em fatores irredutíveis. Existem polinômios $b(x)$ e a_{ij} sobre K com $\mathrm{gr}\, a_{ij}(x) < \mathrm{gr}\, p_i(x)$ tais que

$$\frac{f(x)}{g(x)} = b(x) + \sum_{i=1}^{k} \sum_{j=1}^{n_i} \frac{a_{ij}(x)}{p_i(x)^j}$$

Temos $b(x)$ e $a_{ij}(x)$ são os únicos polinômios com essa propriedade, e $b(x) \in K$ se $\mathrm{gr}\, f(x) \geq \mathrm{gr}\, g(x)$.

Seja F um corpo e sejam K um subcorpo e S um subconjunto de F. Definimos $K(S)$ como sendo o menor subgrupo de F que contém K e S. Em particular, se S for outro subcorpo de F, $K(S)$ é chamada a **composição** de K e S em F, e será denotado por KL.

Uma extensão algébrica L/K é dita **normal** se satisfaz uma de seguintes condições equivalentes:

- Todo polinômio sobre K se decompõe sobre L.
- L é o corpo de decomposição de uma família de polinômios sobre K. (i.e., L é a subextensão de $\overline{K}$ gerada pelas raízes daquela família de polinômios).
- Para toda extensão E/L, a imagem de todo homomorfismo de corpos $K-$linear $\sigma : L \to E$ é L.

Proposição 14. Sejam $L/E/K$ extensões algébricas. Se L/K é normal então L/E é normal.

Uma extensão algébrica L/K é dita **separável** se para todo $a \in L$, o polinômio minimal de a é um **polinômio separável**, i.e., se tem somente raízes com multiplicidade 1 em $\overline{K}$.
Um elemento $a \in L$ é dito **puramente inseparável** sobre K. se existe $n \geq 0$ tal que $a^{p^n} \in K$. A extensão L/K é dita **puramente inseparável** se todo elemento de L é puramente inseparável sobre K. Note que todo corpo é puramente inseparável sobre se mesmo.

Proposição 15. Se f é um polinômio irredutível não separável sobre K então $\operatorname{car} K = p > 0$ e f é da forma

$$c_0 + c_p T^p + c_{2p} T^{2p} + \cdots \quad \text{onde } c_i \in K.$$

Proposição 16. Sejam $K \supset E \supset L$ extensões finitas de corpos. Temos:

1. L/K é separável se e somente se L/E e E/K são separáveis.
2. (Teorema do elemento primitivo). Se L/K é separável então existe $a \in L$ tal que $L = K(a)$.

Proposição 17. Seja L/K uma extensão algébrica, existe uma único corpo S tal que $K \subset S \subset K$, S/K é separável e L/S é puramente inseparável.

Seja L/K uma extensão algébrica de característica $p > 0$. Um corpo é dito **perfeito** se não possui extensões inseparáveis além dele mesmo, ou equivalentemente se toda extensão algébrica dele é separável.

Proposição 18. Os corpos finitos, os corpos algebricamente fechados e os corpos de característica zero são perfeitos.

Seja L/K uma extensão de corpos. O grupo de automorfismos K-lineares de L será denotado por $\mathrm{Aut}(L/K)$. Seja H um subgrupo de $\mathrm{Aut}(L/K)$, o **corpo fixo de** H é o corpo

$$L^H = \{a \in L \mid \sigma(a) = a,\ \forall \sigma \in H\}.$$

L/K é **galoisiana** se for normal e separável. Uma extensão galoisiana é **cíclica** se seu grupo de Galois é cíclico.

Teorema 19 (Artin)**.** Seja L um corpo com grupo de automorfismos $\mathrm{Aut}(L)$ e G um subgrupo de ordem $n < \infty$. Seja $K = L^G$, então $[L:K] = n$, L/K é galoisiana e $G = \mathrm{Aut}(L/K)$.

Teorema 20 (Galois)**.** Seja L/K uma extensão galoisiana com grupo de Galois G.

$$\begin{array}{rcl} \{K \subset E \subset L\} & \overset{1:1}{\longleftrightarrow} & \{\text{ subgrupos } H < G\} \\ E & \overset{\phi}{\longmapsto} & \mathrm{Gal}(L/E) \\ L^H & \overset{\psi}{\longmapsfrom} & H \end{array}$$

Uma subextensão E/K é galoisiana se e somente se $H = \mathrm{Aut}(L/E)$ é normal em G. Nesse caso, $\sigma \mapsto \sigma|_E$ define um isomorfismo $G/H \xrightarrow{\sim} \mathrm{Aut}(E/K)$; assim temos uma sequência exata curta de grupos

$$0 \longrightarrow \mathrm{Gal}(L/E) \longrightarrow \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(E/K) \longrightarrow 0$$

Sejam L/K uma extensão galoisiana finita e $a \in L$. O **traço** de a é a função $\mathrm{Tr} : L \to K$ definida por $\mathrm{Tr}(a) = \sum_{\sigma \in \mathrm{Aut}(L/K)} \sigma(a)$.

Proposição 21. Tr é uma função $K-$linear.

A seguir listamos a principais propriedades dos corpos finitos.

Teorema 22. Sejam p um número primo e $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Temos:

1. Para todo $n \geq 1$, existe um único subcorpo $\mathbb{F}_{p^n}$ de $\overline{\mathbb{F}_p}$ com p^n elementos, dado pelo corpo de decomposição de $T^{p^n} - T$.

2. $\mathbb{F}_{p^n} \subset \mathbb{F}_{p^m}$ se e somente se $n|m$. Nesse caso, $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ é galoisiana e primitiva. O seu grupo de Galois é cíclico e tem ordem m/n, gerado pelo **automorfismo de Frobenius**,

$$\begin{aligned} \mathrm{Frob}_{p^n} : \mathbb{F}_{p^m} &\longrightarrow \mathbb{F}_{p^m} \\ a &\longmapsto a^{(p^n)} \end{aligned}$$

3. O grupo multiplicativo $\mathbb{F}_{p^m}^{\times}$ é cíclico de ordem $p^n - 1$.

Observação 23. Por (3) do teorema anterior, a equação $x^t = a$ tem solução em $\mathbb{F}_{p^n}$ se e somente se $\mathrm{mcd}(t, p^n - 1)$ divide $\dfrac{p^n - 1}{r}$, onde r é o mínimo inteiro positivo tal que $a^r = 1$.

Seja L/K uma extensão de corpos e $S \subset L$. S é *algebricamente dependente* sobre K se existem $n \in \mathbb{N}$, $f \in K[x_1, \ldots, x_n]$ e $s_1, \ldots, s_n \in S$ tais que $f(s_1, \ldots, s_n) = 0$. Caso contrário, S é dito **algebricamente independente**. S é uma **base de transcendência** de F sobre K se for um conjunto algebricamente independente maximal (no sentido da inclusão).

Proposição 24. Seja L/K uma extensão de corpos:

- Existe uma base de transcendência de L sobre K (poder ser vazia).
- Todo par de bases de transcendência de L sobre K têm mesma cardinalidade.
- S é uma base de transcendência de L/K se e somente se F é algébrico sobre $K(S)$

O **grau de transcendência** de L sobre K é a cardinalidade de qualquer base de transcendência de L sobre K, será denotado por $\mathrm{gr.tr}_K L$.

Teorema 25 (Normalização de Noether)**.** Seja A um domínio finitamente gerado sobre um corpo K perfeito, seja F é seu corpo de frações. Logo existe uma base de transcendência $x_1, \ldots, x_n$ sobre K tal que $F/K(x_1, \ldots, x_n)$ é uma extensão finita separável.

CAPÍTULO

2

CORPOS DE FUNÇÕES ALGÉBRICAS NUMA VARIÁVEL

Todos os resultados podem ser encontrados em (STICHTENOTH, 2009, Capítulos 3 e 4), salvo menção em contrário.

Seja K um corpo perfeito. Um **corpo de funções algébricas em uma variável** F/K é uma extensão de corpos tal que $[F : K(x)] < \infty$, para algum $x \in F$ transcendente sobre K. As vezes, F/K será denotado simplesmente por F.
Os exemplos mais simples são os **corpos de funções racionais** $F = K(x)$, com x transcendente sobre K.
Ao longo deste capítulo, O **corpo de constantes** de F/K é

$$\tilde{K} = ic_F(K) = \{z \in F \mid z \text{ é algébrico sobre } K\}.$$

Proposição 26. $[\tilde{K} : K] < \infty$

Daqui para a frente, F/K será um corpo de funções algébricas tal que K é **algebricamente fechado em F**, i.e., $K = \tilde{K}$.

Observação 27. Seja F/K um corpo de funções algébricas, temos que $z \in F$ é transcendente sobre K se e somente se $[F : K(z)] < \infty$. De fato, se z for transcendente sobre K, $\{z,x\}$ tem que ser algebricamente dependente pois $\text{gr.tr}_K F = 1$ (Proposição 24), então existe $f \in K[t_1,t_2]$ tal que $f(z,x) = 0$, logo $[K(z,x) : K(z)] \leq \deg f$ e $[F : K(z)] = [F : K(z,x)][K(z,x) : K(z)] < \infty$. A recíproca é trivial.
Em particular, se $E \subset F$ é um subcorpo tal que $[F : E] < \infty$, então E/K é um corpo de funções algébricas. De fato, existe $z \in E \setminus K$ transcendente sobre K (caso contrário, E/K e F/K são extensões algébricas), segue que $[F : K(z)] = [F : E][E : K(z)] < \infty$, logo $[E : K(z)] < \infty$. Se K é algebricamente fechado em F, o mesmo acontece em E.

2.1 Lugares, divisores e o gênero

Um **anel de valorização de** F/K é um subanel $K \subsetneq \mathcal{O} \subsetneq F$ tal que para todo $z \in F$: $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$.

Proposição 28. Seja $\mathcal{O}$ um anel de valorização de F/K:

1. $\mathcal{O}$ é um anel local, como ideal maximal $P = \mathcal{O} \setminus \mathcal{O}^{\times}$.
2. $K \subset \mathcal{O}$ e $K \cap P = \{0\}$.
3. P é um ideal principal.
4. $\mathcal{O}$ é um anel de valorização discreta.

Um **lugar** P de F/K é o ideal maximal de algum anel de valorização $\mathcal{O}$ em F/K. Um **elemento primo** $t \in P$ é um gerador de P em $\mathcal{O}$. O conjunto de lugares de F/K será denotado por $\mathbb{P}_F$.

Uma **valorização discreta em** F/K é uma função $v : F \to \mathbb{Z} \cup \{\infty\}$ satisfazendo:

1. $v(x) = \infty \iff x = 0$,
2. $v(xy) = v(x) + v(y)$ para todo $x, y \in F$,
3. $v(x+y) = \min\{v(x), v(y)\}$ se $v(x) \neq v(y)$,
4. existe $z \in F$ tal que $v(z) = 1$,
5. $v(a) = 0$ para todo $a \in K \setminus \{0\}$.

Dado $P \in \mathbb{P}_F$, a valorização discreta correspondente (Proposição 7) será denotada por v_P. Além disso, P é um **zero de ordem** n **de** z se $v_P(z) = n > 0$, e P é um **polo de ordem** n de z se $v_P(z) = -n < 0$.
O **corpo residual de** P é $F_P = \mathcal{O}_P/P$; a classe de $x \in \mathcal{O}_p$ será denotada por $x(P)$, e para $x \in F \setminus \mathcal{O}$ escrevemos $x(P) = \infty$. Assim, o corpo residual de P pode ser pensado como o conjunto de valores que pode tomar uma função racional no ponto P.

Proposição 29. Temos que $K \subset F_P$ e é uma extensão finita.

O **grau de** P é definido como $[F_P : K]$. Será denotado por $\operatorname{gr} P$.

Proposição 30.
1. Todo corpo de funções tem um número infinito de lugares.
2. Todo $x \in F \setminus K$ tem um número finito de zeros e polos.

O **grupo de divisores** $Div(F)$ de F/K é o grupo abeliano livre com base $\mathbb{P}_F$.
Dados $Q \in \mathbb{P}_F$ e $D = \sum_{P\in\mathbb{P}_F} n_P P \in Div(F)$, definimos a **valorização do divisor** D **em** Q por $v_Q(D) = n_Q$. O **grau** é o homomorfismo de grupos $Div \to \mathbb{Z}$ definido por

$$\operatorname{gr} D = \sum_{P\in\mathbb{P}_F} v_P(D) \operatorname{gr} P.$$

Vamos considerar o seguinte ordem parcial em $Div(F)$:

$$D_1 \leqslant D_2 \Longleftrightarrow v_P(D_1) \leq v_p(D_2), \forall P \in \mathbb{P}_F.$$

Um divisor A é dito **efetivo** se $A \geqslant 0$.
Sejam $x \in F^\times$ e Z (resp. N) o conjunto de zeros (resp. polos) de x. Definimos

$$\begin{aligned}
(x)_0 &= \sum_{P\in Z} v_P(x)P && \text{, o } \textbf{divisor de zeros} \text{ de } x,\\
(x)_\infty &= \sum_{P\in N} (-v_P(x))P && \text{, o } \textbf{divisor de polos} \text{ de } x,\\
(x) &= (x)_0 - (x)_\infty && \text{, o } \textbf{divisor principal} \text{ de } x.
\end{aligned}$$

Também usaremos a notação $(x)^F$, $(x)_0^F$ e $(x)_\infty^F$.
Claramente $(x)_0, (x)_\infty$ são efetivos e $(x) = \sum_{P\in\mathbb{P}_F} v_p(x)P$. Também temos: $x \in K \Longleftrightarrow (x) = 0$, sempre que $\tilde{K} = K$.

O subgrupo dos divisores principais de F/K é denotado por $\operatorname{Princ}(F)$. Estaremos interessados na relação de equivalencia

$$D \sim D' \iff \exists x \in F^\times \text{ tal que } D = D' + (x),$$

ou equivalentemente $[D] = [D'] \in Cl(F) := \operatorname{Div}(F)/\operatorname{Princ}(F)$.

Dado $A \in Div(F)$, o **espaço de Riemann-Roch** de A é o $K-$espaço vetorial

$$\mathscr{L}(A) = \{x \in F \,|\, (x) \geq -A\} \cup \{0\}.$$

Denotaremos $\dim_K(\mathscr{L}(A))$ por $l(A)$.
Se $A = \sum n_i P_i - \sum m_j Q_j \geq 0$, com $n_i, m_j > 0$, temos que $x \in \mathscr{L}(A) \Longleftrightarrow x$ tem zeros de ordem $\geq m_j$ em Q_j, e tem polos apenas em $\{P_1, \ldots, P_r\}$ de ordem $\leq n_i$.

Teorema 31. Para todo $x \in F \setminus K$,

$$\operatorname{gr}(x)_0 = \operatorname{gr}(x)_\infty = [F : K(x)].$$

Em particular, todo divisor principal tem grau zero.

Teorema 32. 1. $\mathscr{L}(A) \neq \{0\} \Longleftrightarrow A' \sim A$ com $A' \geq 0$.

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

3. Se $A \sim A'$ então $\mathscr{L}(A) = \mathscr{L}(A')$.

Proposição 33 ($g = \gamma + 1$)**.** Existe uma constante $\gamma \in \mathbb{Z}$ tal que para todo $A \in Div(F)$: $\mathrm{gr}A - l(A) \leq \gamma$.

O **gênero de** F/K está definido como

$$g = \max\{\mathrm{gr}A - l(A) + 1 \,|\, A \in Div(F)\};$$

é um inteiro não negativo; temos $l(A) \geq \mathrm{gr}A + 1 - g$.

Agora apresentaremos uma classe especial de divisores que provêm de diferenciais sobre curvas algébricas. Na seção 4 daremos outra interpretação desses conceitos.

Um **adele** de F/K é um mapa $\alpha : \mathbb{P}_F \to F$ tal que $\alpha_P := \alpha(P) \in \mathscr{O}_P$ para todo $P \in \mathbb{P}_F$ salvo em uma quantidade finita deles. O conjunto de adeles de F/K será denotado por $\mathscr{A}_F$; ele é um $K-$espaço vetorial.
O **adele principal** de $x \in F$ é a função constante $\alpha = x$ (lembre que x tem uma quantidade finita de zeros e polos). Assim obtemos um mergulho $F \hookrightarrow \mathscr{A}_F$.

Podemos estender a valorização v_p a $\mathscr{A}_F$ escrevendo $v_P(\alpha) := v_p(\alpha_P)$. Dado $A \in Div(F)$ definimos $\mathscr{A}_F(A) = \{\alpha \in \mathscr{A}_F \,|\, v_P(\alpha) \geq -v_p(\alpha)\}$, é um subespaço de $\mathscr{A}_F$.

Um **diferencial de Weil** de F/K é um mapa $K-$linear $\omega : \mathscr{A}_F \to K$ que se anula em $\mathscr{A}_F(A) + F$ para algum $A \in Div(F)$. O conjunto dos diferenciais de Weil será denotado por Ω_F. Dados $\omega \in \Omega_F$ e $A \in Div(A)$, definimos

$$\Omega_F(A) = \{\omega \in \Omega_F \,|\, \mathscr{A}_F(A) + F \subset \ker\omega\},$$
$$M(\omega) = \{A \in Div(A) \,|\, \mathscr{A}_F(A) + F \subset \ker\omega\}$$

Lema 34. Seja $\omega \in \Omega_F \setminus \{0\}$. Existe um único divisor $W \in M(\omega)$ tal que $A \leq W$ para todo $A \in M(\omega)$.

O divisor W no lema anterior é o **divisor canônico** de ω; será denotado por (ω).
Sejam $\omega \in \Omega_F \setminus \{0\}$ e $P \in \mathbb{P}_F$. Definimos $v_P(\omega) = v_P((\omega))$. Se $v_P(\omega) \geq 0$, ω é dito **regular em** P; ω é dito **regular** (ou **holomorfa**) se for regular em cada $P \in \mathbb{P}_F$.
É fácil verificar que Ω_F forma um F-espaço vetorial com a operação $x\omega : \mathscr{A}_F \to K$, $(x\omega)(\alpha) = \omega(x\alpha)$.
Temos que $\Omega_F(A) = \{\omega \in \Omega_F \,|\, \omega = 0 \text{ ou } (\omega) \geq A\}$ e $\Omega_F(0)$ é o conjunto das diferenciais holomorfas.

Proposição 35. 1. $\dim_K \Omega_F = g$.

2. Se $A \in Div(F)$: $\dim_K \Omega_F(A) = l(A) - \mathrm{gr}(A) + g - 1$.

3. Ω_F tem dimensão 1 sobre F.

4. Dados $x \in F^{\times}$ e $0 \neq \omega \in \Omega_F$: $(x\omega) = (x) + (\omega)$.

5. Todos os divisores canônicos são equivalentes entre si.

A seguir apresentaremos o Teorema de Riemann-Roch, um dos teoremas mais importantes desta teoria. Ele também pode ser provado em variedades complexas usando "métodos trascendentais"(Análise Complexa em Superfícies de Riemann).

Teorema 36 (Riemann-Roch)**.** Seja W um divisor canônico de F/K. Para todo $A \in Div(F)$:

$$l(A) = \mathrm{gr}A + 1 - g + l(W - A)$$

Corolário 37. Sejam $A, W \in Div(F)$

1. Se $\mathrm{gr}A \geq 2g-1$ então $l(A) = \mathrm{gr}A + 1 - g$.

2. W é um divisor canônico se e somente se $\mathrm{gr}W = 2g-2$ e $l(W) \geq g$ (de fato, temos a igualdade).

Seja $P \in \mathbb{P}_F$, uma **lacuna** de P é um $n \in \mathbb{N}$ tal que não existe $x \in F$ com $(x)_\infty = nP$.

Teorema 38 (Weierstrass)**.** Seja g o gênero de F/K, seja $P \in \mathbb{P}_F$:

1. O conjunto das não lacunas de um lugar forma um subsemigrupo aditivo de $\mathbb{N}$.

2. Para cada $n \geq 2g$ existe $x \in F$ com $(x)_\infty = nP$.

3. Se $\mathrm{gr}P = 1$ então existem exatamente g lacunas de P, $i_1 < \cdots < i_g$, tal que $i_1 = 1$ e $i_g \leq 2g-1$.

Observação 39. São equivalentes:

- $a+1$ é uma lacuna de P,
- $\mathscr{L}((a+1)P) = \mathscr{L}(aP)$
- $\dim_K \Omega_F((a+1)P) = \dim_K \Omega_F(aP) - 1$ (Proposição 35(2) e Teorema de Riemann-Roch),
- existe $\omega \in \Omega_F$ tal que $v_p(\omega) = a$.

Proposição 40. a é uma não lacuna do lugar P se somente se $l(aP) = l((a-1)P) + 1$.

2.2 Extensões finitas de corpos de funções

Seja F'/K' um corpo de funções. Ele é uma **extensão finita** de F/K se F'/F é finita e $K' \supset K$. *Neste caso, K'/K é finita.* Assumiremos que K e K' são algebricamente fechados em F e F' respectivamente.
Se $F' = FK'$, F'/K' é dita uma **extensão de constantes** de F/K.

Um lugar $P' \in \mathbb{P}_{F'}$ **está acima** de $P \in \mathbb{P}_F$ se $P \subset P'$; também diremos que P' é uma **extensão** de P em F'/K', ou que P' **se restringe** a P. Isso será denotado por $P'|P$. O conjunto dos lugares de F'/K' acima de P será denotado por $\mathbb{P}_{F'}(P)$.

Proposição 41. Sejam $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$. Temos:

$$P'|P \iff \mathcal{O}_P \subset \mathcal{O}_{P'} \iff \text{ existe } e \geq 1 \text{ tal que } v_{P'}|_F = e \cdot v_P.$$

Nesse caso, $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$ e $P = P' \cap F$.

O inteiro $e(P'|F) := e$ na proposição anterior é o **índice de ramificação** de P' sobre F (ou sobre P); também será denotado por $e(P'|P)$.
O inteiro $f(P'|F) := [F'_{P'} : F_P]$ é o **grau relativo** de P' sobre F (ou sobre P); também será denotado por $f(P'|P)$.

Observação 42. Sejam P' e P como acima, com a condição adicional $K' = K$. Temos que $[F'_{P'} : K] = [F_{P'} : F_P][F_P : K]$, logo

$$\operatorname{gr} P' = f(P'|P) \operatorname{gr} P.$$

Em particular, se $\operatorname{gr} P' = 1$ (como quando K é algebricamente fechado) então $f(P'|E) = 1$.

Proposição 43.

- $f(P'|P) < \infty \iff [F' : F] < \infty$.
- Para todo $P' \in \mathbb{P}_{F'}$ existe um único $P \in \mathbb{P}_F$ tal que $P'|P$.
- Para todo $P \in \mathbb{P}_F$, $\mathbb{P}_{F'}(P)$ é finito não vazio.

  Assim, denotaremos P' por P_F, onde $P = P' \cap F$.

Uma **torre de corpos de funções algébricas** é uma torre de corpos $F'' \supset F' \supset F$, onde F'', F' e F são corpos de funções algébricas com o mesmo corpo de constantes. Neste caso F' é dita uma **subextensão** de F'' que contém F.

Proposição 44 (Transitividade)**.** Seja $F'' \supset F' \supset F$ uma torre de corpos de funções algébricas, temos que

$$e\left(P''|P\right) = e\left(P''|P'\right) \cdot e\left(P'|P\right).$$
$$f\left(P''|P\right) = f\left(P''|P'\right) \cdot f\left(P'|P\right).$$

Teorema 45 (Igualdade Fundamental)**.** Seja F'/K' uma extensão finita F/K de corpos de funções, seja $P \in \mathbb{P}_F$. Então

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

Se $[F' : F] = n$, $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$:

1. P' é **ramificado** se $e(P'|F) > 1$. Diremos que P **se ramifica** quando tem pelo menos uma extensão ramificada.
2. P **se decompõe completamente** quando F'/F se $|\mathbb{P}_{F'}(P)| = n$ (i.e., para todo $P'|P$: $e(P'|F) = f(P'|F) = 1$).
3. P **se ramifica totalmente** quando $|\mathbb{P}_{F'}(P)| = 1$ e $e(P'|F) = n$. Diremos que P' é **totalmente ramificado**.

A **Conorma** $\mathrm{Con}_{F'/F} : Div(F) \to Div(F')$ é o homomorfismo de grupos definido por

$$\mathrm{Con}_{F'/F}\Big(\sum_{P \in \mathbb{P}_F} n_P \cdot P\Big) = \sum_{P \in \mathbb{P}_F} n_P \cdot \left(\sum_{P'|P} e(P'|F) P'\right)$$

Proposição 46.

- Para todo $x \in F^\times$:

$$\mathrm{Con}_{F/F'}((x)^F) = (x)^{F'}, \quad \mathrm{Con}_{F/F'}((x)_0^F) = (x)_0^F, \qquad \mathrm{Con}_{F/F'}((x)_\infty^F) = (x)_\infty^{F'}.$$

- $\mathrm{gr}(\mathrm{Con}_{F'/F}(A)) = \dfrac{[F' : F]}{[K' : K]} \mathrm{gr} A.$

A continuação vamos introduzir o Diferente de extensões separáveis. Ele aparece na fórmula do gênero de Hurwitz, na fórmula da Cotraço (seção 5), e está ligado aos tipos de ramificação (mansa e selvagem).
Seja F/K um corpo de funções, note que uma extensão finita F' de F é um corpo de funções sobre K, cujo corpo de constantes é $K' = ic_{F'}(K)$. Assumiremos que F'/F é separável.
Seja $P \in \mathbb{P}_F$, o conjunto

$$\mathscr{C}_P = \{z \in F' \mid \mathrm{Tr}_{F'/F}(z \cdot \mathscr{O}'_P) \subset \mathscr{O}_P\}$$

é o **módulo complementar** sobre $\mathscr{O}_P$, onde

$$\mathscr{O}'_P = ic_{F'}(\mathscr{O}_P) = \bigcap_{P'|P} \mathscr{O}_P$$

Teorema 47.

1. $\mathscr{C}_P$ é um $\mathscr{O}'_P-$módulo e $\mathscr{O}'_P \subset \mathscr{C}_P$.
2. Existe $t \in F'$ tal que $\mathscr{C}_P = t \cdot \mathscr{O}'_P$. Além disso, para todo $P'|P$: $v_{P'}(t) \leq 0$, e para todo $t' \in F'$: $\mathscr{C}_P = t' \cdot \mathscr{O}_P \iff v_{P'}(t') = v_{P'}(t)$ para todo $P'|P$

3. $\mathscr{C}_P = \mathscr{O}'_P$ para todo $P \in \mathbb{P}_F$ salvo uma quantidade finita.

O inteiro $d(P'|P) := -v_{P'}(t)$ é chamado de **exponente no Diferente** de P' sobre P.

O **Diferente** da extensão separável F'/F é o divisor efetivo

$$\mathrm{Diff}(F'/F) = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P) \cdot P'$$

Proposição 48 (Transitividade do Diferente)**.** Seja $F'' \supset F' \supset F$ uma torre de corpos de funções algébricas, onde todas as extensões são separáveis, temos que

- $\mathrm{Diff}(F''/F) = \mathrm{Con}_{F''/F'}(\mathrm{Diff}(F'/F)) + \mathrm{Diff}(F''/F')$.
- Para $P \in \mathbb{P}_{F''}$: $d(P|F) = e(P|F') \cdot d(P_{F'}|F) + d(P|F')$.

Teorema 49 (Fórmula do Gênero de Hurwitz)**.** Sejam F/K um corpo de funções de gênero g e F'/F uma extensão finita separável. Sejam K' o corpo de constantes de F' e g' o gênero de F'/K'. Então

$$2g' - 2 = \frac{[F' : F]}{[K' : K]}(2g-2) + \mathrm{gr}(\mathrm{Diff}(F'/F))$$

Teorema 50 (Teorema do Diferente de Dedekind)**.** Seja F'/F uma extensão finita separável de corpos de funções. Então para todo $P'|P$:

- $d(P'|P) \geq e(P'|P) - 1$.
- $d(P'|P) = e(P'|P) - 1$ se e somente se $car(k) \nmid e(P'|P)$ (em particular, se $\mathrm{car}\, K = 0$).

Seja $P' \in \mathbb{P}_{F'}$ uma extensão de $P \in \mathbb{P}_F$:

- Diremos que P' (ou P) **tem ramificação mansa** (resp. **selvagem**) se $e(P'|P) > 1$ e não é divisível por $\mathrm{car}\, K$ (resp. é divisível por $\mathrm{car}\, K$).
- Diremos que P **tem ramificação selvagem** se tem pelo menos um extensão com ramificação selvagem.

Corolário 51. 1. $P'|P$ tem ramificação selvagem $\iff d(P'|P) \geq e(P'|P)$.

2. Todo os lugares de F/K são não ramificados salvo uma quantidade finita.
3. Se $F/K(x)$ é finita separável de grau > 1 então é **ramificada** (F/K possui um lugar ramificado).

Teorema 52 (Teorema de Lurröth)**.** Todo subcorpo de um corpo de funções racional é racional, i.e., se $K \subsetneq F_0 \subset K(x)$ então $F_0 = K(y)$ para algum $y \in F_0$.

Agora daremos algumas propriedades das extensões de constantes.

Proposição 53. Seja F'/K' uma extensão de constantes de F/K.

1. F'/F é não ramificado.
2. F'/K' tem o mesmo gênero que F/K.
3. Se $P'|P$, então $F_{P'} = F_P K'$.

Um elemento $x \in F$ é um **elemento separante** de F/K se $F/K(x)$ é separável.

Proposição 54.
1. Seja $z \in F$ tal que $\operatorname{car} K \nmid v_P(z)$ para algum $P \in \mathbb{P}_F$. Então z é um elemento separante de F/K. Em particular, os elementos primos de lugares de F são separantes.
2. Existem $x, y \in F$ tal que x é um elemento separante e $F = K(x,y)$. Em particular, F está determinada por uma equação da forma $g(x,y) = 0$, onde $g \in K[x,y]$ (Teorema do elemento primitivo).
3. Para cada $n \geq 1$, o subcorpo $F^{p^n} \subset F$ (a imagem de $\text{Frob}^n : F \to F$, veja o Teorema 22) tem as seguintes propriedades:
   - $K \subset F^{p^n}$ e F/F^{p^n} é puramente inseparável de grau p^n.
   - F e F^{p^n} são isomorfos (por Frob^n), logo F^{p^n}/K e F/K têm o mesmo gênero.
   - Suponha que $K \subset F_0 \subset F$ e F/F_0 é puramente inseparável de grau p^n. Então $F_0 = F^{p^n}$.
4. $z \in F$ é um elemento separante de F/K se e somente se $z \notin F^{p^n}$.

2.3 Extensões galoisianas

O **grupo de automorfismos** de um corpo de funções algébricas F/K é o grupo $\text{Aut}(F/K)$ formado pelos automorfismos de $K-$álgebras de F.

Teorema 55. (SCHMID, 1938) Seja F/K um corpo de funções de gênero $g \geq 2$. Temos que $\text{Aut}(F/K)$ é finito.

Uma aplicação do grupo de automorfismos é conhecer os subcorpos separáveis de um corpos de funções dado.

Teorema 56. (GÖB, 2004, Teorema 1.25) Sejam F'/K e F/K corpos de funções com corpos de constantes K, tal F'/F é uma extensão separável. Se $\text{Aut}(F'/K)$ é finito então existe um subgrupo finito $U \leqslant F'/K$ tal que $F = (F')^U$.

Nos Capítulos 3 e 4 vamos focar em extensões de corpos de funções do tipo F/F^G, onde G é um subgrupo finito de $\mathrm{Aut}(F/K)$. Pelo Teorema de Artin, essas extensões serão galoisianas, e pela Observação 27, F^G/K é de fato um corpo de funções algébricas.
O seguinte teorema mostra como o grupo de automorfismo de uma extensão age nas extensões dos lugares e nos parâmetros de ramificação.

Teorema 57. Seja F^*/F uma extensão finita de corpos de funções, $P \in \mathbb{P}_F$ e $P^* \in \mathbb{P}_{F'}(P)$. Seja $\sigma \in \mathrm{Aut}(\mathrm{F}^*/\mathrm{F})$. Temos que $\sigma(P^*) \in \mathbb{P}_{F'}$ e

1. $v_{\sigma(P^*)}(y) = v_{P^*}(\sigma^{-1}(y))$ para todo $y \in F^*$, em particular $\mathrm{gr}\,\sigma(P^*) = \mathrm{gr}\,P^*$
2. $\sigma(P^*)|P$ e $\mathcal{O}_{\sigma(P^*)} = \sigma(\mathcal{O}_{P^*})$,
3. $e(\sigma(P^*)|P) = e(P^*|P)$ e $f(\sigma(P^*)|P) = f(P^*|P)$,
4. se F^* e F tem o mesmo corpo de constantes, $\mathrm{gr}\,\sigma(P^*) = P^*$ (Observação 42),
5. se F^*/F for galoisiana, $d(\sigma(P^*)|P) = d(P^*|P)$.

Observação 58.
- Revisando a prova de (1) do teorema anterior em (STICHTENOTH, 2009, Lema 3.5.2.), obtemos um fato mais geral:

$$v_P(y) = v_{\sigma(P)}(\sigma(y)), \text{ onde } \sigma \in \mathrm{Aut}(F/K),\ P \in \mathbb{P}_F \text{ e } y \in F.$$

- Seja $A \in Div(F)$ e seja $\sigma(A) \in Div(F)$ definido por $v_{\sigma(P)}(\sigma(A)) = v_P(A)$, é claro que $\sigma(\mathscr{L}(A)) = \mathscr{L}(\sigma(A))$.

Teorema 59. (ENGLER; PRESTEL, 2005, Teorema 3.2.14) Seja F'/F uma extensão normal finita de corpos de funções $P_1, P_2 \in \mathbb{P}_{F'}(P)$, existe $\sigma \in \mathrm{Aut}(F'/F)$ tal que $\sigma(P_1) = P_2$, ou seja, $\mathrm{Aut}(F'/F)$ age transitivamente em $\mathbb{P}_{F'}(P)$. Em particular, se $P_1, \ldots, P_r \in \mathbb{P}_{F'}(P)$, temos que:

- Podemos definir $e(P) := e(P_i|P) = e(P_j|P)$ e $f(P) := f(P_i|P) = e(P_j|P)$, onde $i, j = 1, \ldots, r$, similarmente com o exponente no diferente se F'/F for galoisiana.
- $e(P) \cdot f(P) \cdot r = [F' : F]$.

Nos capítulos seguintes usaremos repetidamente o teorema anterior ao estudar extensões da forma F/F^G, onde G é um subgrupo de $\mathrm{Aut}(F/K)$. Pelo Teorema de Artin, sabemos que essas são extensões galoisianas.

Observação 60. Seja N um subgrupo finito de $\mathrm{Aut}(F/K)$, e seja $H \triangleleft N$. Pelo Teorema de Galois, F^H/F^N é uma extensão normal e todo automorfismo de $\mathrm{Aut}(F^H/F^N)$ pode ser estendido a um elemento $\mathrm{Aut}(F/F^N)$. Agora, sejam P e P' lugares de F conjugados por N:

- Pelo Teorema 57 aplicado a F/F^N: $P \cap F^N = P' \cap F^N$ e $e(P|F^N) = e(P'|F^N)$.
- $P \cap F^N = (P \cap F^H) \cap F^N = (P' \cap F^H) \cap F^N$, então pelo Teorema 59 aplicado a F^H/F^N: $P \cap F^H$ e $P' \cap F^H$ são conjugados por N/H e $e(P|F^N) = e(P'|F^N)$.
- Pela Transitividade do índice de ramificação, temos que $e(P|F^H) = e(P'|F^N)$.

Agora apresentaremos os grupos de ramificação, que são ferramentas importantes para estudar ramificações selvagens.
Seja F'/F uma extensão galoisiana de corpos de funções, com $G := \mathrm{Aut}(F'/F)$. Seja $P' \in \mathbb{P}_{F'}(P)$.
O **grupo de decomposição** de P' sobre P está definido por

$$G_{-1}\left(P'|P\right) := \left\{\sigma \in G \mid \sigma\left(P'\right) = P'\right\}.$$

$F^{G_{-1}(P'|P)}$ é chamado de **corpo de descomposição** de P', as vezes é denotado por $Z(P'|P)$.
O **grupo de inércia** de P' sobre P está definido por

$$G_0(P'|P) = \{\sigma \in G \mid v_{P'}(\sigma z - z) > 0,\ \forall z \in \mathcal{O}_{P'}\}$$

$F^{G_0(P'|P)}$ é chamado de **corpo de inércia** de P', as vezes é denotado por $T(P'|P)$.

Teorema 61. 1. $|G_{-1}(P'|P)| = e(P'|P) \cdot f(P'|P)$

2. $|G_0(P'|P)| = e(P'|P)$ e $G_0(P'|P) \trianglelefteq G_{-1}(P'|P)$.

Proposição 62. Seja $F' \supset M \supset F$ uma torre de corpos de funções algébricas, onde F'/F é galoisiana. Sejam $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}(P)$. Sejam $Z(P'|P) = F^{G_{-1}(P'|P)}$ e $T(P'|P) = F^{G_0(P'|P)}$. Temos que:

1. $M \subset Z(P'|P) \iff e(P_M|P) = f(P_M|P) = 1$.
2. $M \supset Z(P'|P) \iff P'$ é o único lugar de F' sobre P_M.
3. $M \subset T(P'|P) \iff e(P_M|P) = 1$.
4. $M \supset T(P'|P) \iff P_M$ se ramifica totalmente em F'/M.

Para cada $i \geq -1$, o ***i*-ésimo grupo de ramificação** de P' sobre P está definido por

$$G_i\left(P'|P\right) := \{\sigma \in G \mid v_{P'}(\sigma z - z) \geq i+1 \text{ for all } z \in \mathcal{O}_{P'}\}$$

Também escreveremos $G_i(P'|F)$, $G_i(P')$ ou G_i. Observamos que

$$G_{-1} \supset G_0 \supset \cdots \supset G_i \supset G_{i+1} \supset \cdots$$

É claro que $G_m = 0$ para todo m suficientemente grande.

Observação 63.

$$G_i\left(\tau\left(P'\right)|P\right) = \tau G_i\left(P'|P\right)\tau^{-1}$$

i.e., lugares conjugados têm grupos de ramificação conjugados.

Observação 64. Seja $P' \in \mathbb{P}_{F'}$, temos que $G_k(P'|(F')^{G_i(P')}) = \begin{cases} G_i(P'), \text{ se } k \leq i, \\ G_k(P'), \text{ se } k > i. \end{cases}$

Teorema 65.

1. Se $\operatorname{car} K = 0$ então $G_i = \{\mathrm{id}\}$, $\forall i \geq 1$ e G_T é cíclico.
2. Se $\operatorname{car} K = p > 0$ então G_1 tem ordem uma potência de p, e G_0 é o produto semidireto de G_1 e um grupo cíclico de ordem coprimo com p.
3. $P'|P$ é mansa se e somente se G_0 é cíclico e $G_1 = \{\mathrm{id}\}$.
4. Se $\operatorname{car} K = p > 0$ então G_{i+1} é um subgrupo normal de G_i para todo $i \geq 1$, e $\dfrac{G_i}{G_{i+1}}$ é um $p-$grupo abeliano elementar.

Observação 66. Seja F/K um corpo de funções algébricas tal que K é algebricamente fechado, $\operatorname{car} K = p > 0$ $F/K(x)$ e $G := \operatorname{Aut}(F/K)$ é finito de ordem divisível por p. É sabido que existe $\alpha \in G$ de ordem p, pelo Corolário 51 (3) temos que $F/F^{\langle\alpha\rangle}$ tem um lugar ramificado, digamos $P \in \mathbb{P}_F$, logo $e(P|F^G) = p$. Pela Transitividade do índice de ramificação, P tem ramificação selvagem sobre F^G.

Teorema 67 (Teorema do Diferente de Hilbert)**.**

$$d(P'|P) = \sum_{i=0}^{\infty} (\operatorname{ord} G_i(P'|P) - 1)$$

2.4 Diferenciais

Nesta seção daremos uma interpretação das diferenciais de Weil semelhante às diferenciais em Geometria Diferencial e que facilita as contas com divisores canônicos.
Começaremos fazendo uma digressão sobre o Teorema do gênero de Hurwitz. Seja F'/F uma extensão finita separável. Defina

$$\mathscr{A}_{F'/F} = \{\alpha \in \mathscr{A}_{F'} \,|\, \alpha_{P'} = \alpha_{Q'} \text{ quando } P' \cap F = Q' \cap F\},$$

que é um subespaço de $\mathscr{A}_{F'}$. A traça $\operatorname{Tr}_{F'/F}$ pode-se estender a um mapa $\mathscr{A}_{F'/F} \to \mathscr{A}_F$ fazendo

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

para cada $\alpha \in \mathscr{A}_{F'/F}$ e $P'|P$. A boa definição é garantida pelas propriedades da traça e a seguinte proposição.

Proposição 68. Seja $R \supsetneq K$ um subanel de F/K, que não é um corpo, integralmente fechado e cujo corpo de frações é F. Seja F'/F finita e seja $z \in F'$ integral sobre R. Então $\operatorname{Tr}_{F'/F}(z) \in R$.

Teorema 69 (Fórmula do Cotraço)**.** Com as condições anteriores, para cada $\omega \in \Omega_F$ existe um único $\omega' \in \Omega_{F'}$ tal que

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

para todo $\alpha \in \mathscr{A}_{F'/F}$. Este diferencial é chamado de **Cotraço** de ω em F'/F, denotado por $\mathrm{Cotr}_{F'/F}(\omega)$. Se $\omega \neq 0$, temos que

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

Proposição 70. $\mathrm{Cotr}_{F'/F}$ é um mapa $F-$linear.

Assim, a fórmula do gênero de Hurwitz segue de tomar grau na fórmula do Cotraço, junto com a Proposição 46.
O Cotraço é a conexão entre os dois conceitos de diferencial: diferencial de Weil e derivação, .

Como antes, seja F/K um corpo de funções algébricas, onde K é um corpo perfeito. Seja M um F-espaço vetorial. Uma **derivação** de F/K é um mapa $K-$linear $\delta : F \to M$ que satisfaz a regra de Leibniz:

$$\forall u, v \in F : \quad \delta(uv) = u\delta(v) + v\delta(u),$$

Proposição 71.

- $\delta(a) = 0$ para $a \in K$.
- $\delta(z^n) = nz^{n-1}\delta(z)$ para $z \in F$ e $n \geq 0$, em particular $\delta(z^p) = 0$.
- $\delta(x/y) = (y\delta(x) - x\delta(y))/y^2$.

Proposição 72.

- Se x é um elemento separante de F/K, existe uma única derivação $\delta_x : F \to F$ de F/K tal que $\delta_x(x) = 1$.
- Se y é outro elemento separante de F/K, $\delta_y = \delta_y(x)\delta_x$.

Seja $Z = \{(u,x) \in F \times F \,|\, x \text{ é separante}\}$. Definimos a seguinte relação de equivalência:

$$(u,x) \sim (v,y) \iff v = u\delta_y(x),$$

que está bem definida pela proposição anterior. Um **diferencial** de F/K é uma das classes de equivalência obtidas. A classe de (u,x) será denotada por $u\,dx$ e a classe de $(1,x)$ será denotada por dx. Temos que

$$u\,dx = v\,dy \iff v = u\delta_y(x).$$

O conjunto dos diferenciais em F/K será denotado por Δ_F. Definimos a suma dos diferenciais $u\,dx$, $v\,dy$ da seguinte maneira: seja z um elemento separante de F/K, logo

$$u\,dx + v\,dy := (u\delta_z(x) + v\delta_z(y))dz.$$

Está bem definida pela regra da cadeia. Definimos o produto de $w \in F$ com $u\,dx$ por

$$w \cdot (u\,dx) = (wu)dx \in \Delta_F.$$

Assim, Δ_F é um F-espaço vetorial, e é chamado de **módulo de diferenciais** de F/K.
Se t é um elemento não separante, definimos $dt = 0 \in \Delta_F$.

Proposição 73. 1. Defina $dz = 0$ se $z \in F$ não for separante. O mapa $d : F \to \Delta_F$ é uma derivação sobre F/K.

2. Seja $z \in F$ separante. Temos que $dt \neq 0$ e todo diferencial $\omega \in \Delta_F$ pode ser escrito de forma única como $\omega = u\,dz$, com $u \in F$.

Exemplo 74. Suponha que $F = K(x,y)$ tal que x é um elemento separante (Proposição 54 (2)), sejam $f(x) = \sum_{i=0}^{n} a_i x^i$ e $g(x) = \sum_{j=0}^{m} b_j x^j$ em $K[x]$, definimos

$$\overline{D}_x(f(x)) = \sum_{i=1}^{n} a_i i x^{i-1}, \qquad \overline{D}_x\left(\frac{f(x)}{g(x)}\right) = \frac{g(x)\overline{D}_x(f(x) - f(x)\overline{D}_x(g(x)))}{(g(x)^2)}.$$

Assim $\overline{D}_x$ é uma derivação em $K(x)/K$ tal que $D_x(x) = 1$. Pela proposição anterior existe uma derivação $D_x : F \to F$ tal que $\delta_x(x) = 1$ e $D_x|_{K(x)} = \overline{D}_x$.

Sejam $y, z \in F$, tal que z é um elemento separante. Pela proposição anterior, podemos definir $\dfrac{dy}{dz}$ como o único elemento de F tal que $dy = \dfrac{dy}{dz} \cdot dz$.

Proposição 75 (Regra da cadeia)**.** Sejam $x, y, z \in F$, tal que z e x são elementos separantes de F/K, seja δ_z como na Proposição 72:

$$\delta_z(y) = \frac{dy}{dz}, \qquad \frac{dy}{dx} = \frac{dy}{dz} \cdot \frac{dz}{dx}$$

Observação 76. Seja $\sigma \in \mathrm{Aut}(F/K)$ e seja z um elemento primo de um lugar de F/K, pela Proposição 54 (1) e a Observação 58, z e $\sigma(z)$ são elemento separantes de F/K.
Seja $f \in F$, pela Proposição 72, $\sigma^{-1} \circ \delta_{\sigma(t)} \circ \sigma = \delta_t$ pois ambas são derivações $F \to F$ tal que $t \mapsto 1$. Então, pela regra da cadeia,

$$\frac{d\sigma(f)}{d\sigma(t)} = \delta_{\sigma(t)}\sigma(f) = \sigma(\delta_t(f)) = \sigma\left(\frac{df}{dt}\right) \implies \frac{d\sigma(f)}{dt} = \sigma\left(\frac{df}{dt}\right) \cdot \frac{d\sigma(t)}{dt}$$

Em particular, se K for algebricamente fechado, $\dfrac{d\sigma(f)}{dt} = \sigma\left(\dfrac{df}{dt}\right)$, pois todos os lugares de F tem elemento primo $t - a$ com $a \in K$, logo $\dfrac{d\sigma(t)}{dt} = 1$.

A seguir mostraremos a relação entre as duas definições de diferenciais. A seguinte proposição é a peça chave.

Proposição 77. Se $F = K(x)$, existe uma única diferencial de Weil $\eta \in \Omega_{K(x)}$ tal que

$$(\eta) = -2P_\infty \quad \text{e} \quad \eta_{P_\infty}(x^{-1}) = -1$$

Seja $x \in F$ um elemento separante de F/K, e seja $\eta \in \Omega_{K(x)}$ da proposição anterior. Definimos

$$\delta(x) = \mathrm{Cotr}_{F/K(x)}(\eta) \in \Omega_F.$$

Se $x \in F$ não é separante, definimos $\delta(x) = 0$.

Teorema 78. Seja F/K um corpo de funções algébrico sobre um corpo perfeito. Seja $x \in F$ um elemento separante.

1. A função $\delta : F \to \Omega_F$ é uma derivação sobre F/K.
2. A relação

$$\begin{aligned} \mu : \Delta_F &\longrightarrow \Omega_F \\ z\,dx &\longmapsto z \cdot \delta(x) \end{aligned}$$

   define um isomorfismo entre Δ_F e Ω_F, tal que $\mu \circ d = \delta$.
3. Se $\omega = z \cdot \delta(t) \in \Omega_F$, onde t é um elemento primo de um lugar $P \in \mathbb{P}_F$: $v_P(\omega) = v_P(z)$.

Daqui para frente, identificaremos Δ_F com Ω_F, e também $z\,dx \in \Delta_F$ com $z \cdot \delta(x)$, se x é um elemento separante de F/K.

Observação 79. Suponha que K é algebricamente fechado. Sejam $\sigma \in \mathrm{Aut}(F/K)$, $f \in F$ e t um elemento primo de um lugar de F/K, por (3) do teorema anterior e as Observação 58 e 76,

$$v_P(df) = v_P\left(\frac{df}{dt}\right) = v_{\sigma(P)}\sigma\left(\frac{df}{dt}\right) = v_{\sigma(P)}\left(\frac{d\sigma(f)}{dt}\right) \implies (d\sigma(f)) = \sigma((df)).$$

Observação 80. Seja $z\,dx \in \Omega_F$, onde x é um elemento separante de F/K. Pela definições nesta seção e a Fórmula do Cotraço, temos que:

$$\begin{aligned} (z\,dx) &= (z) + (dx) = (z) + (\mathrm{Cotr}_{F/K(x)}(\eta)) \\ &= (z) + \mathrm{Con}_{F/K(x)}(-2P_\infty) + \mathrm{Diff}(F/K(x)) \\ &= (z) - 2(x)_\infty^F + \mathrm{Diff}(F/K(x)) \end{aligned}$$

CAPÍTULO

3

EXEMPLOS DE CURVAS E CORPOS DE FUNÇÕES ALGÉBRICAS

3.1 Corpos de funções de curvas algébricas

Seja K um corpo algebricamente fechado. O seguinte teorema mostra a conexão entre a geometria das curvas algébricas sobre K e a estrutura algébrica de seus corpos de funções.

Teorema 81. (HARTSHORNE, 1977, Teorema I.4.4) O funtor $K(\cdot)$, que associa a cada variedade algébrica o seu corpo de funções, é uma equivalência contravariante, entre a categoria $\mathfrak{D}$ (veja Seção 1.1) e a categoria das extensões finitamente geradas do corpo K, junto com os morfismos de $K-$álgebras. De fato, dadas duas variedades algébricas X e Y, são equivalentes:

1. X e Y são birracionalmente equivalentes,
2. existem abertos $U \subset X$ e $V \subset Y$ tais que U é isomorfo a V,
3. $K(X) \simeq K(Y)$ como $K-$álgebras.

O teorema anterior é um dos mais importante da Geometria Algébrica. Ele indica que podemos estudar as variedades algébricas e os morfismos entre elas olhando para seus corpos de funções. Em particular, duas variedades têm o mesmo corpo de funções se e somente se forem birracionalmente equivalentes.
O Teorema 81 justifica as definições no Exemplo 2 (2), pois as variedades projetivas possuem uma cobertura aberta cujos elementos são isomorfos a variedades afins (Exemplo 1 (1)). Note que toda variedade algébrica pode ser vista como uma variedade quase-projetiva, logo podem ser cobertas também por abertos afins.

Os corpos de funções de curvas algébricas são corpos de funções algébricas em uma variável. De fato, isso é valido para curvas algébricas pelo exemplo 1 (1) e a Normalização de

Noether, e o mesmo acontece com curvas mais gerais, considerando o corpo de funções de um aberto afim dela.
Assim, podemos herdar conceitos e resultados da teoria de corpos de funções para a teoria das curvas algébricas. Por exemplo, o gênero de uma curva é definido como gênero de seu corpo de funções.

Reciprocamente, dado um corpo de funções algébricas em uma variável F/K, ele pode ser visto como o corpo de funções de uma curva algébrica plana. Isso é consequência imediata do Teorema 54 (2) (considere a curva plana definida por $g(x,y)=0$).
Em particular, tomando F como o corpo de funções de uma curva $\mathscr{C}$, temos que $\mathscr{C}$ é birracionalmente a uma curva plana. Note que todo lugar de F/K tem grau 1. Além disso, cada $x \in F$ pode ser identificado com a função $x(\cdot) : F \to K$ (veja Seção 2.1), que se corresponde com uma função racional em $K(\mathscr{C})$ pelo Teorema 81.

Teorema 82. (HARTSHORNE, 1977, Teorema IV.3.10) Toda curva é birracionalmente equivalente a uma curva plana (dita de *modelo plano*), cujas singularidades, se tiver, são nodos.

Assim o estudo das curvas algébricas, em muitas situações, se reduz ao estudo das curvas algébricas planas. Por exemplo, o seguinte resultado, que pode ser provado usando técnicas geométricas, permite obter o gênero de qualquer curva (considerando seu modelo plano).

Proposição 83. (FULTON, 2008, Proposição 8.5.) Seja $\mathscr{C}$ uma curva plana de grau n cujas singularidades são ordinárias. Temos que

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

Existe uma conexão entre os pontos das curvas e os lugares de seus corpo de funções.

Teorema 84. (HARTSHORNE, 1977, Seção 1.6)

- Sejam $\mathscr{C}$ uma curva algébrica e $P \in \mathscr{C}$. $\mathscr{C}$ é não singular em P se e somente $\mathscr{O}_P$ é um anel de valorização discreta em $K(\mathscr{C})$.
- Se $\mathscr{C}$ for não singular, existe uma correspondência entre os pontos da curva e os lugares de $K(\mathscr{C})$.
- Existe uma equivalência entre a categorias das curvas algébricas não singulares, considerando os morfismos racionais, e a categoria dos corpos de funções em uma variável, considerando os homomorfismos de $K-$álgebras.

Teorema 85. Toda curva plana é birracionalmente equivalente a uma curva projetiva não singular (pode não ser plana), única salvo isomorfismo (SILVERMAN, 2009, Teorema II.2.4).

3.2 O corpo de funções racionais $K(x)$

A referência para esta seção é (STICHTENOTH, 2009, Capítulo 1).

Seja K um corpo perfeito. Seja $p(x)$ um polinômio irredutível em $K[x]$, temos que

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ p(x) | g(x),\ p(x) \nmid g(x) \right\}$$

é um lugar de $K(x)/K$. Temos que $\operatorname{gr} P = \operatorname{gr} p(x)$ e, dado $z \in K(x)^\times$, temos que

$$z = p(x)^n \left(\frac{f(x)}{g(x)} \right) \text{ com } f(x), g(x) \in K[x] \text{ PESI},\ p(x) \nmid f(x)g(x) \Longrightarrow v_P(z) = n.$$

Além destes lugares, $K(x)/K$ possui um único lugar adicional,

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x],\ p(x) \nmid g(x),\ \operatorname{gr} f(x) < \operatorname{gr} g(x) \right\},$$

chamado de **lugar no infinito**. Temos que $\operatorname{gr} P_\infty = 1$ e

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

Observação 86.

1. Existe uma correspondência biunívoca entre os lugares de grau 1 de $K(x)$ e $\mathbb{P}^1(K)$, dada por $P_{x-a} \mapsto [a:1]$, $P_\infty \mapsto [0:1]$.
2. Vamos denotar P_{x-a} por a e P_∞ por ∞. Assim, temos que $\mathbb{P}^1 = K \cup \{\infty\}$
3. A forma de denotar estes lugares depende da escolha do gerador x. Por exemplo, o lugar no infinito respeito a $1/x$ é o lugar P_x respeito a x.

Lema 87. $K(x) = K(z)$ se e somente se

$$z = \frac{ax+b}{cx+d} \quad \text{com } a,b,c,d \in K \text{ e } ad - bc \neq 0.$$

Demonstração. Seja $z = a\dfrac{f(x)}{g(x)} \in K(x) \setminus K$, com $a \in K^\times$ e $f(x), g(x)$ PESI e mônicos. Seja $f(x) = u\prod_{i=1}^{r} p_i(x)^{n_i}$ e $g(x) = u'\prod_{i=1}^{s} q_j(x)^{m_j}$ as descomposições em fatores mônicos irredutíveis. Sejam $P_i := P_{p_i(x)}$ e $Q_j = P_{q_j(x)}$, temos que

$$(z) = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j + (\operatorname{gr} g(x) - \operatorname{gr} f(x)) P_\infty. \tag{3.1}$$

Pelo Teorema 31, temos que

$$[K(x) : K(z)] = \max\{\operatorname{gr} f(x), \operatorname{gr} g(x)\},$$

o que implica o resultado. □

Observação 88. Dado um divisor de grau zero de $K(x)$, podemos mostrar que ele é principal usando a equação 3.1, indo de trás para a frente. Isso também decorre do Corolário 37.

Proposição 89. Seja K um corpo. Temos que $\mathrm{Aut}(K(x)/K) \simeq \mathrm{PGL}(2,K)$ e é fortemente 3-transitivo sobre $\mathbb{P}^1(K)$ (e sobre os lugares de grau 1 de $K(x)$). Cada automorfismo não trivial tem no máximo dois pontos fixos. Se K é algebricamente, todo automorfismo possui um ponto fixo.

Demonstração. Seja $\alpha \in \mathrm{Aut}(K(x)/K)$, ele está determinado por su valor em x. Como $K(x) = K(\alpha(x))$ então $\alpha(x) = \dfrac{ax+b}{cx+d}$, com $a,b,c,d \in K$ e $ad-bc \neq 0$ pelo lema anterior. Por otro lado, dados a,b,c,d como antes, podemos construir um homomorfismo $K(x) \to K(x)$ dado por $\alpha(x) = \dfrac{ax+b}{cx+d}$, que será um isomorfismo pelo lema anterior, pois $K(\alpha(x)) = K(x)$.
Dado $A = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}(2,K)$, seja $\sigma_A \in \mathrm{Aut}(K(x)/K)$ definido por $\sigma_A(x) = \dfrac{ax+b}{cx+d}$. Temos que o mapa $A \mapsto \sigma_A$ é um homomorfismo sobrejetivo de grupos $\mathrm{GL}(2,K) \to \mathrm{Aut}(K(x)/K)$, cujo núcleo são as matrizes diagonais , que formam um grupo isomorfo a $K^\times$. Segue disto e do parágrafo anterior que

$$\mathrm{Aut}(K(x)/K) \simeq \mathrm{Aut}(\mathbb{P}^1(K)) \simeq \mathrm{GL}(2,K)/K^\times = \mathrm{PGL}(2,K).$$

Agora, seja $\alpha \in \mathrm{Aut}(K(x)/K)$ como no início da prova. Pelos isomorfos acima, ele age nos pontos de $\mathbb{P}^1$. Assim, dado $z \in \mathbb{P}^1$, temos que $\alpha(z) = z$ com $z \neq \infty$ se somente satisfaz

$$cz^2 + (d-a)z - b = 0,$$

. Veja que essa equação sempre tem solução se K é algebricamente fechado, também note que ∞ é ponto fixo de α se e somente se $c = 0$ e $d = 1$. Logo α tem no máximo dois pontos fixos, excepto quando $b = c = 0$ e $d = a \neq 0$, ou seja $\alpha = 1$. .
Sejam $a_1, a_2, a_3 \in \mathbb{P}^1$, se $\beta \in \mathrm{Aut}(K(x)/K)$ tal que $\alpha(a_i) = \beta(a_i)$, $i = 1,2,3$, então $\alpha \circ \beta^{-1}$ tem três pontos fixos, logo é igual a identidade. Por tanto $\alpha = \beta$.

Para provar a última afirmação, considere $a,b,c \in \mathbb{P}^1$. Defina as funções

$$\varphi_{a,b,c}(x) := \frac{x-a}{x-c} \cdot \frac{b-c}{b-a} \tag{3.2}$$

e, quando a, b ou c for ∞, o fator correspondente na expressão acima é trocado por 1, por exemplo $\varphi_{\infty,b,c}(x) = \dfrac{b-c}{x-c}$. Note que $\varphi_{a,b,c}$ faz $a \mapsto 0$, $b \mapsto 1$ e $c \mapsto \infty$. Agora, dados $a_i, b_i \in \mathbb{P}^1$, $i = 1,2,3$, $\varphi^{-1}_{b_1,b_2,b_3}(x) \circ \varphi_{a_1,a_2,a_3}$ é um automorfismo tal que $a_i \mapsto b_i$, $i = 1,2,3$. Pelo parágrafo anterior $\varphi^{-1}_{b_1,b_2,b_3}$ é o único automorfismo com essas condições. Em conclusão, $\mathrm{Aut}(K(x)/K)$ é fortemente $3-$transitivo. □

Lema 90. Seja $\alpha \in \mathrm{Aut}(K(x)/K)$ tal que $p \nmid |\langle\alpha\rangle|$, então α fixa 0 ou 2 pontos de $\mathbb{P}^1(K)$.

Demonstração. Suponha que $\alpha(z) = z$, seja $\beta \in \mathrm{Aut}(K(x)/K)$ tal que $\beta(z) = \infty$ (existe pela proposição anterior). Temos que $\beta\alpha\beta^{-1}$ fixa ∞, logo $\beta\alpha\beta^{-1}(x) = ax + b$ 3.2, onde $a, b \in K$ e $a \neq 0$. Segue que $a \neq 1$ (caso contrário $|\langle\alpha\rangle| = |\langle\beta\alpha\beta^{-1}\rangle| = p$), logo $\beta\alpha\beta^{-1}$ também fixa o ponto $\dfrac{-b}{a-1} \neq \infty$, por tanto α fixa z e $\beta^{-1}\left(\dfrac{-b}{a-1}\right) \neq z$. □

Observação 91. Seja F/K um corpo de funções algébricas definido por uma equação da forma $f(x,y) = 0$, onde x é um elemento separante (isso sempre é possível pelo Teorema 54 (2)). Sejam P_1, P_2, P_3 lugares de F, sejam $\overline{P_1}$, $\overline{P_2}$, $\overline{P_3}$ lugares de $K(x)$, e seja σ o automorfismo de $K(x)/K$ tal que

$$P_1 \cap K(x) \mapsto \overline{P}_1 \quad P_2 \cap K(x) \mapsto \overline{P}_2 \quad P_3 \cap K(x) \mapsto \overline{P}_3$$

Escolha $y' \in \overline{K(x)}$ tal que $f(y', \sigma(x)) = 0$, seja $F' = K(x', y')$, ele é claramente isomorfo a F e temos que $P_i | \overline{P}_i$, $i = i, 2, 3$ em F'/K'.

O seguinte resultado é uma consequência do Teorema de Riemann-Roch.

Teorema 92. Seja F/K um corpo de funções algébricas em uma variável. São equivalentes:

1. F/K é racional
2. F/K tem gênero 0, e existe $A \in Div(F)$ tal que $\mathrm{gr}\, A = 1$.

3.3 Corpos de funções elíticas

Seja K um corpo perfeito. Um **corpo de funções elíticas** é um corpo de funções algébricas F/K de gênero 1 que possui um divisor de grau 1. São os corpos de funções algébricas mais simples, após dos corpos de funções racionais.
Os seguintes resultados nesta seção podem ser encontrado em (STICHTENOTH, 2009, Seção 6.1)

Proposição 93. Seja F/K um corpo de funções elíticas.

1. Se $\mathrm{car}\, K \neq 2$, existem $x, y \in F$ tal que $F = K(x,y)$ e

$$y^2 = f(x) \in K[x], \text{ onde } f(x) \text{ é livre de quadrados e } \mathrm{gr}\, f = 3 \tag{3.3}$$

Reciprocamente, seja $F = K(x,y)$ um corpo de funções que satisfaz 3.3, seja $c\prod_{i=1}^{r} p_i(x)$ a decomposição de $f(x)$ em fatores irredutíveis mônicos. Seja $P_i \in \mathbb{P}_{K(x)}$ o lugar correspondem a $p_i(x)$, e P_∞ como na Seção 3.1. Temos que

- F/K é um corpo de funções elíticas com corpo de constantes K.

- A extensão $F/K(x)$ é cíclica de grau 2, os únicos lugares ramificados de $K(x)$ são os P_i e P_∞. Cada um deles possui uma única extensão de F, denotada por Q_i e Q_∞ respectivamente, totalmente ramificadas. Além disso $\operatorname{gr} Q_i = \operatorname{gr} P_i$ e $\operatorname{gr} Q_\infty = 1$.
- $\operatorname{Diff}(F/K(x)) = Q_1 + \cdots + Q_r + Q_\infty$.

2. Se $\operatorname{car} K = 2$, existem $x, y \in F$ tal que $F = K(x,y)$ e

$$y^2 + y = f(x) \in K[x] \text{ com } \operatorname{gr} f = 3, \text{ ou} \tag{3.4}$$

$$y^2 + y = x + \frac{1}{ax+b} \text{ com } a,b \in K \text{ e } a \neq 0 \tag{3.5}$$

Reciprocamente, seja $F = K(x,y)$ um corpo de funções que satisfaz 3.4 ou 3.5. Sejam $P_\infty, P_{ax+b} \in \mathbb{P}_F$ como na seção 3.1. Temos que

- F/K é um corpo de funções elíticas com corpo de constantes K.
- A extensão $F/K(x)$ é cíclica de grau 2, e os únicos lugares ramificados de $K(x)$ são P_∞ (no caso 3.4) e P_∞ e P_{ax+b} (no caso 3.5), que possuim uma única extensão em F de grau 1, Q_∞ (no caso 3.4) e Q_∞ e Q_{ax+b} (no caso 3.5).
- $\operatorname{Diff}(F/K(x)) = \begin{cases} 4Q_\infty & \text{no caso (3.4.)} \\ 2Q_\infty + 2Q' & \text{no caso (3.5.)} \end{cases}$

Proposição 94 (Lei de Grupo)**.** Seja F/K um corpo de funções elíticas, e seja $\mathbb{P}_F^{(1)}$ o conjunto de lugares de F/K de grau 1. Temos que

1. Para cada $A \in Div(F)$ com $\operatorname{gr} A = 1$ existe um único lugar $P \in \mathbb{P}_F^{(1)}$ tal que $A \simeq P$. Em particular $\mathbb{P}_F^{(1)} \neq \emptyset$.
2. Escolha $P_0 \in \mathbb{P}_F^{(1)}$. Temos uma bijeção

$$\begin{aligned} \Phi : \mathbb{P}_F^{(1)} &\longrightarrow \mathrm{Cl}^0(F) \\ P &\longmapsto [P - P_0] \end{aligned}$$

o que dota a $\mathbb{P}_F^{(1)}$ de uma estrutura de grupo abeliano, isomorfo a $Cl^0(F)$.

Seja K um corpo algebricamente fechado. Uma **curva superelítica** é uma curva plana afim dada por uma equação da forma

$$\mathscr{C}: \quad y^m = f(x)$$

onde $m \geq 2$, $f(x) \in K[x]$ e $\operatorname{gr} f(x) \geq 3$. Mais geralmente, é qualquer curva algébrica cujo corpo de funções pode ser definido pela equação acima.

Quando $m = 2$ e $d = 3$, então $\mathscr{C}$ é uma **curva elítica**. As curvas elíticas formam a família de curvas algébricas mais famosa, com muitas aplicações dentro e fora da Matemática. A

bibliografia sobre elas é muito extensa, uma introdução pode ser encontrada em (SILVERMAN, 2009).
Quando $m = 2$ e $d \geq 5$ então $\mathscr{C}$ é uma **curva hiperelítica** (veja Seção 3.5).

Um fato interessante é que a Lei de Grupo pode ser provada utilizando métodos geométricos, como o Teorema de Bezout (FULTON, 2008, Proposição 5.4)

Teorema 95. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 11.94) Seja C uma curva elítica sobre um corpo algebricamente fechado K. O grupo de automorfismos de C é infinito e age transitivamente nos pontos de C.

3.4 Extensões cíclicas

Os dois tipos principais de extensões galoisianas cíclicas são as extensões de Kummer e as extensões de Artin-Schreier.
A referência para esta seção é (STICHTENOTH, 2009, Seção 3.7.).

3.4.1 Extensões de Kummer

Proposição 96. Sejam F/K um corpo de funções algébricas e $n > 1$ tal que $\operatorname{car} K \nmid n$. Suponha que K contém as raízes $n-$ésimas da unidade. Suponha que existe $u \in F$ que satisfaz

$$u \neq w^d \quad \forall w \in F, \quad \forall d > 1 \text{ tal que } d|n, \tag{3.6}$$

Seja $F' = F(y)$ com $y^n = u$. Uma extensão F'/F que satisfaz essas condições é chamada de **extensão de Kummer**. Temos que

- $\Phi(T) = T^n - u$ é o polinômio minimal de y sobre F e F'/F é uma extensão galoisiana cíclica de grau n. Os elementos de $\operatorname{Aut}(F'/F)$ vêm dados por $\sigma(y) = \zeta y$, onde ζ é uma raiz $n-$ésima da unidade.
- Sejam $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ uma extensão de P, defina $r_P = \operatorname{mdc}(n, v_P(u))$, então

  $$e(P'|P) = \frac{n}{r_P} \quad \text{e} \quad d(P'|P) = \frac{n}{r_P} - 1$$

  Em particular, P se ramifica se e somente se $r_P < n$.
- Se K' é o corpo de constante de F' e g (resp- g') é o gênero de F/K (resp. F'/K') então

  $$g' = 1 + \frac{n}{[K' : K]}\left(g - 1 + \frac{1}{2}\sum_{P \in \mathbb{P}_F}\left(1 - \frac{r_P}{n}\right)\deg P\right)$$

Uma extensão de Kummer $F/K(x)$ sobre um corpo de funções racionais $K(x)$, com K algebricamente fechado, pode ser realizada como o corpo de funções de uma curva superelítica

(veja Seção 3.3).
Neste caso, pela proposição anterior, o gênero da extensão é

$$\frac{1}{2}\left(m(|B|-2)-\sum_{P\in B}(m,r_P)\right)+1$$

onde B é o conjunto dos lugares ramificados de F sobre $K(x)$.

Por exemplo, sabemos que a curva $\mathscr{C}: y^2-x^2(x+1)=0$ tem um nodo na origem e é uma curva superelítica. Além disso, tem gênero 0, pela fórmula acima, que coincide com o valor obtido ao aplicar a Proposição 83.

3.4.2 Extensões de Artin-Schreier

Proposição 97. Seja F/K um corpo de funções algébricas tal que $\operatorname{car} K = p > 0$. Suponha que existe $u \in F$ que satisfaz

$$u \neq w^p - w \quad \text{para todo } w \in F \tag{3.7}$$

Seja $F' = F(y)$ com $y^p - y = u$. Para cada $P \in \mathbb{P}_F$, defina

$$m_P := \begin{cases} m & \text{se } \exists z \in F \text{ tal que } v_P(u-(z^p-z)) = -m < 0 \text{ e } p \nmid m \\ -1 & \text{se } \exists z \in F \text{ tal que } v_P(u-(z^p-z)) \geq 0 \end{cases}$$

Uma extensão F'/F que satisfaz essas condições é chamada de **extensão de Artin-Schreier**. Temos que F'/F é uma extensão cíclica galoisiana de grau p, e os elementos de $\operatorname{Aut}(F'/F)$ vêm dados por $\sigma(y) = y + c$, com $c \in \mathbb{F}_p$. Além disso,

- P não se ramifica $\iff m_P = -1$. Caso contrário, P se ramifica totalmente e $d(P'|P) = (p-1)(m_P+1)$.

- Suponha que existe $Q \in \mathbb{P}_F$ tal que $m_Q > 0$. Então K é o corpo de constantes de F' e

$$g' = p\cdot g + \frac{p-1}{2}\left(-2+\sum_{P\in\mathbb{P}_F}(m_P+1)\cdot \deg P\right)$$

Uma **curva de Artin-Schreier** é uma curva plana dada por uma equação da forma

$$\mathscr{C}: \quad y^p - y = f(x)$$

onde $f(x) \in K(x)\setminus K$. Mais geralmente, é qualquer curva algébrica cujo corpo de funções pode ser definido pela equação acima. No Capítulo 5 vamos estudar o grupo de automorfismos dos corpos de funções dessas curvas.

3.5 Corpos de funções hiperelíticas

Um corpo de funções hiperelíticas é um corpo de funções de gênero $g \geq 2$ tal que existe $x \in F$ com $K(x) \subset F$ e $[F : K(x)] = 2$.

Proposição 98. (STICHTENOTH, 2009, Proposição 6.2.3)

1. Seja F/K um corpo de funções hiperelíticas de gênero g, tal que $\operatorname{gr} K > 2$. Existem $x, y \in F$ tais que $F = K(x,y)$, $F/K(x)$ é galoisiana de grau 2 e

$$y^2 = f(x) \in K[x] \text{ onde } f(x) \text{ é livre de quadrados e } \operatorname{gr} f(x) = 2g+1 \text{ e } 2g+2. \tag{3.8}$$

2. Reciprocamente, se $F = K(x,y)$ é um corpo de funções de gênero $g \geq 2$ que satisfaz 3.8 então é um corpo de funções hiperelíticas.

3. O conjunto S dos lugares de $K(x)$ que se ramificam (totalmente) em F está formado pelos zeros de $f(x)$ (em geral), mais o lugar no infinito se $\operatorname{gr} f(x)$ for impar.

Proposição 99. (STICHTENOTH, 2009, Proposição 6.2.4)

1. Todo corpos de funções algébricas de gênero 2 é hiperelítico.

2. Seja F/K um corpo de funções hiperelíticas F/K de gênero g e seja $K(x) \subset F$ tal que $[F : K(x)] = 2$. .Todos os subcorpos racionais $K(z) \subset F$ com $[F : K(z)] \geq g$ estão contidos em $K(x)$. Em particular $K(x)$ é o único subcorpo racional de F tal que $[F : K(x)] = 2$.

Observação 100. Seja F/K um corpo de funções tal que $[F : K(x)] = n$ e $K(x)$ é o único subcorpo racional $K(z)$ de F tal que $F/K(z)$ seja uma extensão normal de grau n.
Seja $\sigma \in \operatorname{Aut}(F/K)$, temos que $F/K(\sigma(x))$ também é normal de grau n. Segue que todo automorfismo de F/K leva $K(x)$ nele mesmo. Por tanto, temos a seguinte sequência exata curta:

$$0 \longrightarrow \operatorname{Aut}(F/K(x)) \longrightarrow \operatorname{Aut}(F/K) \xrightarrow{\pi} H \longrightarrow 0,$$

onde π leva automorfismos de F em sua restrição em $K(x)$ e H é um subgrupo finito de $\operatorname{Aut}(K(x)/K)$.

Em particular, temos que o grupo de automorfismos de um corpo de funções hiperelítco é uma extensão de um $\mathscr{C}_2$ por um subgrupo finito de $\operatorname{PGL}(2,K)$ (veja Seção 1.2.1).

Seja F/K um corpo de funções hiperelítico. A **involução hiperelítica** é o automorfismo de F/K definido por

$$x \mapsto x,\ y \mapsto y+1 \text{ se } \operatorname{car} K = 2; \text{ ou}$$
$$x \mapsto x,\ y \mapsto -y \text{ se } \operatorname{car} K \neq 2.$$

Note que a involução hiperelítica gera $\mathrm{Aut}(F/K(x))$.
O seguinte resultado é provado para curvas algébricas utilizando métodos geométricos, como a invariância dos pontos de Weierstrass por automorfismos.

Teorema 101. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 11.98) Seja F/K um corpo de funções hiperelítico tal que K é algebricamente fechado e $\mathrm{car}\, K \neq 2$. Temos que

1. $\mathrm{Aut}(F/K(x))$ está no centro de $\mathrm{Aut}(F/K)$.

2. Seja S como na Proposição 98 (3) e seja $G = \mathrm{Aut}(F/K)$. Temos que

$$\frac{G}{\mathrm{Aut}(F/K(x))} \simeq \mathrm{Aut}(K(x)/F^G) = W,$$

onde W é o subgrupo de $\mathrm{Aut}(K(x)/K)$ que preserva S.

3.6 Curvas dadas por polinômios separados

A referência para esta seção é (STICHTENOTH, 1973). Seja K um corpo algebricamente fechado com $\mathrm{car}\, K = p > 0$. Considere a curva $\mathscr{C}$ dada pela equação

$$\begin{aligned}
&\mathscr{C}: A(y) = B(x) \text{ com}\\
&A(y) = a_n y^{p^n} + a_{n-1} y^{p^{n-1}} + \cdots + a_1 y^p + a_0 y\\
&B(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0\\
&a_i, b_j \in K; \quad a_n, a_0, b_m \neq 0; \quad m \equiv 0 (\bmod p)\\
&n \geqq 1; \quad m \geqq 2
\end{aligned}$$

Considere as seguintes mudanças de variável:

1. $y' = cy$, $a_i' = \dfrac{a_i c^{p^n - p^i}}{a_n}$, $b_j = \dfrac{b_j c^{p^n}}{a_n}$ onde $c \in K$ tal que $c^{p^n - 1} = \dfrac{a_n}{a_0}$, o que transforma em 1 os coeficientes principal e independente de $A(y)$.

2. $x' = \sqrt[m]{b_m}x$, o que torna B mônico.

3. $x' = x + \dfrac{b_{m-1}}{m}$, o que elimina o término de ordem $m-1$ de $B(x)$.

4. $y' = y - c$, onde $c \in K$ tal que $A(x) = b_0$, o que elimina o término independente de $B(x)$.

5. Se $A(y) = y^{p^n} + y$ e $B(x) = x^{p^n+1} + b_1 x$, defina $x' = x + d$, $y' = y + bx + c$, onde $d^{p^{2n}} - d = b_1^{p^n}$, $c^{p^n} + c = d^{n^n+1}$ e $b = dp^n - b_1$. Assim obtemos $y^{p^n} + y = x^{p^n+1}$.

Teorema 102. Aplicando as mudanças anteriores, a curva C é birracionalmente a curva $\mathscr{C}'$ dada por

$$\begin{aligned}
&\mathscr{C}' : A(y) = B(x)\\
&A(y) = y^{p^n} + a_{n-1}y^{p^{n-1}} + \cdots + a_1 y^p + y\\
&B(x) = x^m + b_{m-2}x^{m-2} + \cdots + b_1 x\\
&m \equiv 0 (\bmod p), \quad m \geqq 2, \quad n \geqq 1
\end{aligned}$$

Temos que C' é irredutível. Além disso, se $F = K(C)$:

1. $\mathrm{Aut}(F/K(x))$ é um grupo abeliano elementar de ordem p^n.
2. Existe um lugar P de F que é totalmente ramificado sobre $K(x)$ e sobre $K(y)$.
3. A sequência de grupos de ramificação de P sobre $K(x)$ é

$$G_0(P) = G_1(P) = \cdots = G_m(P) = \mathrm{Aut}(F/K(x)) \text{ e } G_{m+1}(P) = \{1\}.$$

4. $\mathrm{Dif}(F/K(x)) = (p^n - 1)(m+1) \cdot P$.
5. O gênero é $\dfrac{1}{2}(p^n - 1)(m-1)$.

Teorema 103. (HIRSCHFELD; KORCHMÁROS; TORRES, 2008, Teorema 12.11) Se o grau de $\mathscr{C}$ é ≥ 4 então $\mathscr{C}$ não é uma curva elítica. Seja G o grupo de automorfismos de F (ou de $\mathscr{C}$ ou de $\mathscr{C}'$). Seja P como no teorema anterior, temos que $G = G_0(P)$, exceto nos seguintes casos:

1. $y^{p^n} + y = x^m$, com $m < p^n$, $m | p^n + 1$. Nesse caso P tem $p^n + 1$ conjugados pela ação de G e $\mathrm{Aut}(F/K)$ é uma extensão de C_m e $\mathrm{PGL}(2, p^n)$.
2. $y^{p^n} + y = x^{p^n+1}$. Nesse caso P tem $p^{3n} + 1$ conjugados pela ação de G e $\mathrm{Aut}(F/K) \simeq \mathrm{PGU}(3, q)$.

CAPÍTULO

4

SUBGRUPOS FINITOS DE $\mathrm{PGL}(2,K)$

Neste capítulo vamos aplicar a teoria desenvolvida nos capítulos anteriores para calcular os subgrupos finitos de $\mathrm{Aut}(K(x)/K)$, onde K é um corpo algebricamente fechado de característica positiva.
Este capítulo e o próximo estão baseados em (VALENTINI; MADAN, 1980).

Seja K um corpo perfeito de característica $p > 0$. Para encontrar os subgrupos finitos de $\mathrm{Aut}(K(x)/K)$, vamos estudar as ramificações que os possíveis corpos fixos por aqueles subgrupos podem ter em $K(x)$, obtendo assim o Teorema 107 . Após disso, vamos focar no caso $K = \mathbb{F}_{p^m}$, e vamos achar todos os subgrupos de $\mathrm{PGL}(2,p^m)$ (Teorema 113). Estes subgrupos podem ser considerados como subgrupos finitos de $\mathrm{Aut}(K(x)/K)$, o que implica o Teorema 114.
Os resultados do Capítulo 2 que usaremos mais frequentemente são: o Teorema 35 a Igualdade Fundamental, a Fórmula do Gênero de Hurwitz, o Teorema do Diferente de Dedekind (TDD), o Teorema do Diferente de Hilbert (TDH), o Teorema de Lurröth, o Teorema 59, o Teorema 61 e o Teorema 65.

Seja F/K um corpo de funções algébricas, e seja G um subgrupo finito de $\mathrm{Aut}(F/K)$. Seja $E = F^G$ (ou equivalente, seja F/E uma extensão galoisiana com $G = \mathrm{Aut}(F/E)$). Sabemos E/K é um corpo de funções algébricas (primeiro parágrafo da Seção 2.3). Pela fórmula do gênero de Hurwitz temos que

$$2(g_F - 1) = 2(g_E - 1)|G| + \mathrm{gr}(\mathrm{Diff}(F/E)) \tag{4.1}$$

Seja $\overline{P}$ um lugar de E de grau d que se ramifica. Seja r o número de lugares de F acima de $\overline{P}$, com índice de ramificação e, grau relativo f e exponente no Diferente δ (veja o Teorema 59). Temos que $\mathrm{gr}(\overline{P}) = fd$ (Observação 42), logo a contribuição das extensões de $\overline{P}$ no grau de $\mathrm{Diff}(F/E)$ é

$$rf\delta d = \frac{|G|}{e}\delta d \tag{4.2}$$

Sejam g_F e g_E os gêneros de F e E, respectivamente. Sejam $\overline{P}_1,\dots,\overline{P}_s$ os lugares de E que se ramificam. Usaremos a seguinte notação em todo este capítulo: para $i=1,\dots,s$, sejam $S_i=\mathbb{P}_{F/E}(\overline{P}_i)$, $d_i=\mathrm{gr}(\overline{P}_i)$ e e_i, δ_i e r_i os respectivos parâmetros de ramificação (como no parágrafo acima). Denotaremos $G_i(P|E)$ por $G_i(P)$ para $P\in\mathbb{P}_F$.
Pela fórmula do gênero de Hurwitz e a análise anterior, temos

$$2(g_F-1)=2(g_E-1)|G|+|G|\sum_{i=1}^{s}\frac{\delta_i}{e_i}d_i \tag{4.3}$$

Estudaremos o caso $F=K(x)$; logo E também é racional e $g_F=g_E=0$ (Teorema de Lüroth e o Teorema 35). Assim,

$$2-\frac{2}{|G|}=\sum_{i=1}^{s}\frac{\delta_i}{e_i}d_i \tag{4.4}$$

Podemos achar as possibilidades de G fazendo uma análise caso por caso das possíveis ramificações. Começaremos estabelecendo as principais restrições dos parâmetros.

Lema 104. Com as hipóteses anteriores:

1. Se $\overline{P}_i$ tem ramificação mansa então $\delta_i=e_i-1$.
2. Se $\overline{P}_i$ tem ramificação selvagem então $f_i=1$ e $\delta_i=e_i^*q_i+q_i-2$, onde $e_i=e_i^*q_i$, q_i é uma potência de p, $p\nmid e_i^*|q_i-1$, $d_i=1$ e $r_i\equiv 1 \mod q_i$. Se $P\in S_i$ então $\mathrm{gr}\,P=1$ e $G_2(P)=\{1\}$.
3. E tem no máximo três lugares que se ramificam. Além disso $\sum_{i=1}^{s}d_i\leq 3$.

Demonstração. (1) Teorema do Diferente de Dedekind.

(2) Seja $P\in S_i$ e seja $E'=F^{G_1(P)}$; aplicando a equação 4.1 à extensão F/E', temos que

$$2|G_1(P)|-2=\mathrm{gr}(\mathrm{Diff}(F/E')). \tag{4.5}$$

Em particular $2|G_1(P)|-2\geq d(P|E')\,\mathrm{gr}(P)$. Por outro lado, pelo Teorema do Diferente de Hilbert e a Observação 64,

$$d(P|E')=|G_1(P|E)|-1+\sum_{i=1}^{\infty}(|G_i(P|E)|-1).$$

Assim, temos que $\mathrm{gr}(P)=1=f_i=d_i$ (Observação 42), $G_{n\geq 2}(P)=\{1\}$, e P é o único lugar de F ramificado sobre E' (*).

Observação 105. Seja R uma subextensão de F que contém E. Quando $\overline{P}_i$ tem ramificação selvagem, o anterior implica, pela Observação 42 e a Proposição 44, que

$$f(P|R)=1=f(P_R|E),\ \text{onde } P\in S_i.$$

Defina $e_i^* = \dfrac{|G_0(P)|}{|G_1(P)|}$ e $q_i = |G_1(P)|$. Temos $e_i = |G_0(P|E)| = e_i^* q_i$ (Teorema 65 (2), onde q_i é uma potência de p e $p \nmid e_i^*$. Logo, pelo TDH,

$$\delta_i = |G_0(P)| - 1 + |G_1(P)| - 1 = e_i^* q_i + q_i - 2$$

Observação 106. Considere a ação de $G_1(P)$ sobre S_i. As órbitas desta ação coincidem com os lugares em F que têm a mesma restrição em E' (Teorema 59). Lugares distintos de P não são ramificados sobre E' por (*), logo suas órbitas têm comprimento $|G_1(P)| = q_i$ (Teorema 59 e Observação 105). Logo, nenhum automorfismo não trivial de $G_1(P)$ fixa lugares além de P_1. Além disso, $r_i \equiv 1 \mod q_i$.

Agora, seja $\sigma \in G_0(P)$ de ordem e_i^* (estrutura de G_0, Teorema 65). Seja $S = F^{\langle\sigma\rangle}$, temos que $S \supset F^{G_0(P)}$. Pela Proposição 62 (4), P é totalmente ramificado sobre S. Pelo Teorema de Artin temos que $[F : S] = e_i^*$, e pelo Teorema 59 e a Observação 105, $e(P|S) =$. Segue que $d(P|S) = e_i^* - 1$ pelo TDD. Como $e_i = e_i^* \cdot e(P_S|E)$ (Proposição 44) então $e(P_S|E) = q_i$. Pelo TDD, $d(P_S|E) = q_i + t$ com $t \geq 0$. Agora, pela Transitividade do Diferente temos que $d(P|E) = e(P|S) \cdot d(P_S|E) + d(P|S)$, logo

$$\delta_i = e_i^* q_i + q_i - 2 = e_i^*(q_i + t) + e_i^* - 1.$$

Simplificando, obtemos que $e_i^* | q_i - 1$.

(3) Pelo TDD: $\dfrac{\delta_i}{e_i} \geq \dfrac{e_i - 1}{e_i} \geq \dfrac{1}{2}$. Pela equação 4.1,

$$2 > 2 - \frac{2}{|G|} \geq \frac{1}{2} \sum_{i=1}^{s} d_i,$$

o que implica 3. □

Agora analisaremos cada uma das possíveis ramificações de F/E.

Caso não ramificado ($s = 0$). Da equação 4.4 segue que $G = \{1\}$, em particular $E = F$.

4.1 Um lugar ramificado

4.1.1 P_1 tem ramificação mansa.

A equação 4.4 fica

$$2 - \frac{2}{|G|} = \frac{e_1 - 1}{e_1} d_1. \tag{4.6}$$

Pelo Lema 104 (3), temos as seguintes possibilidades:

4.1.1.1 $d_1 = 1$

A equação 4.6 fica

$$1 - \frac{2}{|G|} = -\frac{1}{e_1},$$

o que é impossível pois $|G| \geq e_1 \geq 2$.

4.1.1.2 $d_1 = 2$

A equação 4.6 fica

$$1 - \frac{1}{|G|} = 1 - \frac{1}{e_1},$$

logo $|G| = e_1 = |G_0(P)|$ (Teorema 65) e G é cíclico de ordem e_1, não divisível por p.

4.1.1.3 $d_1 = 3$.

A equação 4.6 fica

$$2 - \frac{2}{|G|} = 3\left(1 - \frac{1}{e_1}\right)$$

Se $e_1 \geq 3$ então $3\left(1 - \frac{1}{e_1}\right) \geq 2$, impossível.

Assim $e_1 = 2$, logo $|G| = 4$ e é abeliano. Seja $P \in S_1$, como os grupos de inércia de lugares em S_1 são conjugados (Observação 63), todos são iguais a $G_0(P)$; note que $|G_0(P)| = e_1 = 2$ (Teorema 61). Defina $E' = F^{G_0(P)}$, pela Proposição 62 (3) temos que $e(P_{E'}|E) = 1$. Como P foi escolhido arbitrariamente, segue que E'/E é galoisiana (Teorema 20) não ramificada. O caso não ramificado mostra que $E' = E$, o que é impossível ($[F : E'] = 2$ pelo Teorema de Artin).

4.1.2 $\overline{P_1}$ tem ramificação selvagem

Pelo Lema 104 e a equação 4.4,

$$\frac{1}{e_1^*} - \frac{2}{e_1^* q_1} = 1 - \frac{2}{|G|} \geq 1 - \frac{2}{e_1^* q_1},$$

o que implica que $e_1^* = 1$ e $|G| = q_1$. Como $r_1 \equiv 1 \mod q_1$ (Lema 104 (2)) então $S_1 = \{P\}$ e $G = G_0(P) = G_1(P)$ (Teorema 65). Como $G_2(P) = \{1\}$, segue que G é um grupo abeliano p-elementar.

4.2 Dois lugares ramificados

4.2.1 $\overline{P_1}$ e $\overline{P_2}$ têm ramificação mansa

A equação 4.4 fica

$$2 - \frac{2}{|G|} = \left(1 - \frac{1}{e_1}\right) d_1 + \left(1 - \frac{1}{e_2}\right) d_2. \tag{4.7}$$

Pelo Lema 104 (3), temos as seguintes possibilidades:

4.2.1.1 $d_1 = d_2 = 1$

A equação 4.7 fica

$$\frac{2}{|G|} = \frac{1}{e_1} + \frac{1}{e_2}$$

Como $e_1, e_2 \leq |G|$ então $e_1 = e_2 = |G|$. Similar ao caso 4.1.1.2, G é cíclico de ordem não divisível por p.

4.2.1.2 $d_1 = 1$ e $d_2 = 2$

A equação 4.7 fica

$$-\frac{2}{|G|} = 1 - \frac{1}{e_1} - \frac{1}{e_2} \tag{4.8}$$

Se $e_2 \geq 4$ então $1 - \frac{1}{e_1} - \frac{1}{e_2} \geq 0$, impossível.

4.2.1.2.1 $e_2 = 2$

Pela equação 4.8, $|G| = 2e_1$. Sejam $P \in S_1$ e σ um gerador do grupo cíclico $G_0(P)$ de ordem e_1 (Teoremas 61 e 65 (3)). Como $\langle\sigma\rangle \trianglelefteq G$ (pois tem índice 2) então todos os lugares em S_1 têm o mesmo grupo de inércia $\langle\sigma\rangle$. Defina $E' = F^{\langle\sigma\rangle}$, $\overline{P_1}$ não se ramifica em E' (Proposição 62 (3)), logo $\overline{P_2}$ deve-se ramificar em E' (Corolário 51).
Seja $Q \in S_2$ tal que $Q_{E'}$ é ramificado sobre E, seja τ um gerador do grupo cíclico $G_0(Q)$ de ordem 2 (Teoremas 61 e 65 (3)). Suponha que $\tau \in \langle\sigma\rangle$ então $F \supset F^{\tau} \supset E' \supset E$, pela Proposição 62 (4) obtemos uma contradição ($\overline{P}_1$ ramificado sobre E'). Logo $\tau \notin \langle\sigma\rangle$ e $G = \langle\sigma, \tau\rangle$. Suponha que σ e τ comutam, logo $G = C_{e_1} \times C_2$ e $\langle\tau\rangle$ é normal em G; todos os lugares em S_2 têm grupo de inércia $\langle\tau\rangle$ (Observação 63). Como no parágrafo anterior, $\overline{P_1}$ é o único lugar que se ramifica em $F^{\langle\tau\rangle}/E$, que é uma extensão galoisiana pelo Teorema 20. Obtemos uma contradição pelo caso 4.1.1.1 (lembre que $d_1 = 1$). Por tanto σ e τ não comutam e $G \simeq D_{e_1}$.

4.2.1.2.2 $e_2 = 3$

A equação 4.8 fica

$$-\frac{2}{|G|} = \frac{1}{3} - \frac{1}{e_1}$$

Vemos que $e_1 < 3$, logo $e_1 = 2$ e $|G| = 12$. Suponha que existe $\sigma \in G$ de ordem 6. Seja $E' = F^{\langle\sigma\rangle}$, temos que E'/E é galoisiana (Teorema 20) de grau 2. Note que $\overline{P_2}$ não se ramifica em E' (Teorema 59), então $\overline{P_1}$ deve-se ramificar em E' (Corolário 51), o que é impossível pelo caso 4.1.1.1 (lembre que $d_1 = 1$). Pela Proposição 7 temos que $G \simeq A_4$.

4.2.2 $\overline{P_1}$ tem ramificação selvagem e $\overline{P_2}$ tem ramificação mansa

Pelo Lema 104 e a equação 4.4,

$$1-\frac{2}{|G|}=\frac{1}{e_1^*}-\frac{2}{e_1^*q_1}+\left(1-\frac{1}{e_2}\right)d_2$$

Como $\frac{1}{e_1^*}-\frac{2}{e_1^*q_1}\geq 0$ e $1-\frac{1}{e_2}\geq\frac{1}{2}$ então $d_2=1$. Assim

$$\frac{2}{|G|}=\frac{1}{e_2}-\frac{1}{e_1^*}+\frac{2}{e_1^*q_1}. \tag{4.9}$$

Como $\frac{2}{|G|}\leq\frac{2}{e_1^*q_1}$ então $e_2\geq e_1^*$.

4.2.2.1 $e_2=e_1^*$

Pela equação 4.9 e o Lema 104 (2), $|G|=e_1^*q_1=e_1$, assim $G=G_0(P)$ com $P\in S_1$ (Teorema 65); segue que G é o produto semidireto de um $p-$grupo abeliano elementar de ordem q_1 com um grupo cíclico de ordem $e_1^*|q_1-1$ (Lema 104 (2)).

4.2.2.2 $e_2>e_1^*$

Pelo Teorema 59 e a Observação 105, $|G|=e_1^*q_1r_1$. Substituindo na equação 4.9, obtemos

$$r_1=\frac{2e_2}{2e_2-(e_2-e_1^*)q_1} \tag{4.10}$$

Dado $P\in S_1$, $|G_0(P)|=|G_{-1}(P)|=e_1^*q_1$, pois $f_1=1$ (Teorema 61). Sejam $Q\in S_2$ e τ um gerador de $G_0(Q)$ (Teorema 65 (3)), pelo Teorema 61 tem ordem e_2. Vemos que $\tau\notin G_{-1}(P)$, pois tem ordem $>e_1^*$ e não divisível por p; logo τ não fixa nenhum lugar em S_1 (definição de G_{-1}).

A ação de G em S_1 associa a τ uma permutação em S_1, que pode ser escrita como um produto de ciclos disjuntos. Seja $(P_1\cdots P_t)$ um ciclo em τ de comprimento mínimo, logo $t\geq 2$ e $\tau^t\in G_{-1}(P_k)$ por definição, $k=1,\ldots,t$; note que $G_{-1}(P_k)=G_0(P_k)$ pois $f_1=1$ (Teorema 61). Pela equação 4.1, ‘

$$2|\langle\tau^t\rangle|-2=\text{gr}(\text{Diff}(F/E')),\text{ onde } E'=F^{\langle\tau^t\rangle}.$$

Temos que $F^{\langle\tau\rangle},F^{G_0(P_k)}\subset E'$, $k=1,\ldots,t$, além disso $[F:E']=|\langle\tau^t\rangle|$ (Teorema de Artin). Pela Proposição 62 (4) e o TDD, $d(Q|E')=|\langle\tau^t\rangle|-1=d(P_k|E')$, $k=1,\ldots,t$. Segue que $\text{gr}(\text{Diff}(F/E'))\geq(t+1)(|\langle\tau^t\rangle|-1)$, como $t\geq 2$, necessariamente $|\langle\tau^t\rangle|=1$, por tanto $|\langle\tau\rangle|=e_2$. Como $|S_1|=r_1\leq 2e_2$ (equação 4.10), os ciclos em τ, agindo em S_1, têm comprimento e_2, logo $e_2|r_1$. Temos dois subcasos:

4.2.2.2.1 $q_1 = 2$.

Do Lema 104 (2), $e_1^* | q_1 - 1$, logo $e_1^* = 1$. Pela equação 4.10, $r = e_2$, assim $|G| = 2r = 2e_2$. Analogamente ao caso 4.2.1.2.1 quando $e_2 = 2$, temos que $G \simeq D_{e_2}$.

4.2.2.2.2 $q_1 \geq 3$

Pela equação 4.10, $c := 2e_2 - (e_2 - e_1^*)q_1 \in \{1,2\}$, pois $e_2 | r_1$. Vamos determinar e_2, r e e_1^* em termos de q_1. Temos que

$$e_2 = \frac{e_1^* q_1 - c}{q_1 - 2}.$$

Substituindo na equação 4.10,

$$r_1 = \frac{2}{c}\frac{e_1^* q_1 - c}{q_1 - 2} = 1 + q_1 \frac{\frac{2}{c}e_1^* - 1}{q_1 - 2}.$$

Pelo Lema 104 (2), $r_1 \equiv 1 \mod q_1$, então $\frac{2}{c}e_1^* \equiv 1 \mod q_1 - 2$. Sabemos que $e_1^* | q_1 - 1$. Se $c = 1$ então $q_1 - 2 | 2e_1^* - 1$; é fácil ver que: ou $e_1^* = \frac{q_1 - 1}{2}$ e $p \neq 2$, ou $e_1^* = 2$ e $q_1 = 3$. Se $c = 2$, então pela equação 4.10, $r_1 = e_2 > e_1^* \geq 1$; usando as equações centralizadas acima, obtemos que $e_1^* = q_1 - 1$. Assim, olhando as possibilidades de e_1^*, obtemos os seguintes subcasos:

1. $q_1 = 3$, $e_1^* = 2$, $r = 10$, $e_2 = 5$, $|G| = 60$;
2. $p \neq 2$, $e_1^* = \frac{q_1 - 1}{2}$, $r_1 = q_1 + 1$, $e_2 = \frac{q_1 + 1}{2}$, $|G| = \frac{(q_1 - 1)q_1(q_1 + 1)}{2}$
3. $e_1^* = q_1 - 1$, $r_1 = q_1 + 1$, $e_2 = q_1 + 1$, $|G| = (q_1 - 1)q_1(q_1 + 1)$.

Caso 1. Neste caso $p = 3$. Seja $H \triangleleft G$ próprio e seja $E' = F^H$. Suponha que $\overline{P_2}$ não se ramifica em E', então $\overline{P_1}$ deve-se ramificar (Corolário 51). Como E'/E é galoisiana (Teorema 20) e $d_1 = 1$ (Lema 104 (2)), o caso 4.1.1.1 aplicado a E'/E implica que $\overline{P}_1$ tem ramificação selvagem em E'. Logo, o caso 4.1.2 mostra que $\overline{P_1}$ tem uma única extensão Q em E', tal que $e(Q|E) = q_1 = [E' : E] = 3$ (Teorema de Artin, note que 3 é o único divisor múltiplo de p de $|G| = [F : E]$). Pelo Teorema 59 e a Observação 42, $\overline{P}_2$ tem 1 extensão de grau 3 ou 3 extensões de grau 1 em E'; essas extensões têm que se ramificar em F, pois $e_2 > 1$ (Proposição 44). Note que a extensão de Q em F se ramifica com índice 2 (Proposição 44, lembre que $e_1 = e_1^* q_1$). Somando os graus dos lugares de F acima de Q e das extensões de $\overline{P_2}$ em E', obtemos uma contradição com o Lema 104 (3) aplicado a F/E'.
Logo $\overline{P}_2$ deve-se ramificar em E', com índice 5 (Proposição 44, note que $e_2 = 5$ é primo). Além disso, as extensões de $\overline{P}_2$ em E' não se ramificam em F, e $5 | [E' : E]$ (Teorema 59). Como $e_1 = 6$ e $f_1 = 1$ (Lema 104 (2)), $\overline{P_1}$ tem pelo menos 5 extensões em E' (Teorema 59). Pelo Lema 104 (3), essas extensões não podem ser ramificadas em F/E'. Por tanto, F/E' é não ramificado e

$H=\{1\}$ (caso não ramificado). Em conclusão, G é simples de ordem 60, e pela Proposição 8, $G\simeq A_5$.

Casos 2 e 3. Seja $S_1=\{P_1,\ldots,P_{q_1+1}\}$, pelo Teorema 59, G é um grupo de permutação sobre S_1. Seja $E'=F^{G_1(P_1)}$, pela Observação 106, P_1 é o único lugar ramificado sobre E' e P_2 tem $|G_1(P_1)|=q_1$ lugares conjugados pela ação de $G_1(P_1)$. Assim, $G_1(P_1)$ é transitivo em $\{P_2,\ldots,P_{q_1+1}\}$; pela Observação 12, G é 2-transitivo em S_1. Seja

$$H=\{\sigma\in G\,|\,\sigma(P_1)=P_1,\,\sigma(P_2)=P_2\}.$$

Temos que $H\subset G_{-1}(P_1)=G_0(P_1)$ (pois $f_1=1$, Teorema 61). Como P_2 não é fixado por nenhum elemento de $G_1(P_1)$, $H\cap G_1(P_1)=\{1\}$. Pelo Teorema 65 e a definição (4) de produto semidireto no Capítulo 1, existe um morfismo $f:G_0(P_1)\to T$, onde $T\simeq\dfrac{G_0(P_1)}{G_1(P_1)}$ cíclico, com núcleo $G_1(P_1)$. Segue que $H\overset{f}{\hookrightarrow}T$ é cíclico. Pelo Teorema 10 e a Proposição 89 temos que $|H|=d$ e $G\simeq\mathrm{PSL}(2,q_1)$ no caso II e $G\simeq\mathrm{PGL}(2,q_1)$ no caso III.

4.2.3 $\overline{P_1}$ e $\overline{P_2}$ têm ramificação selvagem

Pelo Lema 104 e a equação 4.4 fica

$$-\frac{2}{|G|}=\frac{1}{e_1^*}-\frac{2}{e_1^*q_1}+\frac{1}{e_2^*}-\frac{2}{e_2^*q_2}$$

Como $\dfrac{1}{e_1^*}-\dfrac{2}{e_1^*q_i}\geq 0$ para $i=1,2$, esta equação é impossível.

4.3 Três lugares ramificados

4.3.1 $\overline{P_1}$, $\overline{P_2}$ e $\overline{P_3}$ têm ramificação mansa

Pelo Lema 104, a equação 4.4 fica

$$1+\frac{2}{|G|}=\frac{1}{e_1}+\frac{1}{e_2}+\frac{1}{e_3}. \tag{4.11}$$

Além disso, os $d_i=1$. Por contradição, é fácil mostrar que $e_i<3$ para algum i. Assim, podemos supor que $2=e_1\leq e_2\leq e_3$. Se $e_2\geq 4$, também obtemos uma contradição. Temos então os seguintes subcasos:

4.3.1.1 $e_2=2$

Por 4.11, $|G|=2e_3$. Análogamente ao caso 4.2.1.2.1 quando $e_2=2$, $G\simeq D_{e_3}$.

4.3.1.2 $e_2 = 3$

Pela equação 4.11,

$$\frac{1}{6} + \frac{2}{|G|} = \frac{1}{e_3},$$

logo $e_3 \leq 5$. Temos as seguintes possibilidades:

4.3.1.2.1 $e_3 = 3$

Então $|G| = 12$. Analogamente ao caso 4.2.1.2.1 quando $e_2 = 3$, $G \simeq A_4$

4.3.1.2.2 $e_3 = 4$

Então $|G| = 24$. Sejam $Q \in S_2$ e $H = G_0(Q)$, logo $|H| = e_2 = 3$ (Teorema 61). Pelo Teorema de Sylow aplicado a G, H deve ter 1 ou 4 conjugados, pois H é um 3-subgrupo de Sylow. Suponha que $H \trianglelefteq G$, e seja $E' = F^H$, pelo Galois e a Proposição 16, E'/E é galoisiana. Note que $[E' : E] = 8 = |\operatorname{Aut}(E'/E)|$. Temos que $\overline{P_1}$ e $\overline{P_3}$ têm ramificação mansa em E'/E com índices < 8 (pois $e_1 = 2$ e $e_3 = 4$), mas pelo caso 4.2.1.1 isto é impossível.
Assim, H tem 4 conjugados, logo $[G : N_G(H)] = 4$ (Sylow). Seja $N = N_G(H)$, logo $|N| = 6$. Pela Observação 5, existe um homomorfismo de $G \to S_4$ com núcleo $\bigcap_{\sigma \in G} \sigma N \sigma^{-1} \subset N$. Como H tem conjugados em G fora de N (pois $H \trianglelefteq N$), então o núcleo do homomorfismo $G \to S_4$ é diferente de N, logo ele tem ordem 1 ou 2, pois H é o único subgrupo de ordem 3.
Suponha que a ordem do núcleo seja 2. Seja E' o corpo fixo pelo núcleo, temos que $[F : E'] = 2$ (Teorema de Artin) e $[E' : E] = 12$. Como $E' \triangleleft G$ então E'/E é galoisiana. Pela equação 4.4 aplicada a E'/E, $2 - \frac{1}{6} = \sum_{j=1}^{s'} \left(1 - \frac{1}{e'_j}\right)$, onde e'_j é o índice de ramificação de $\overline{P_j}$ em E' quando for ramificado; note que $e'_j | e_j$ (Proposição 44). Obtemos os seguintes casos:

1. $\overline{P}_2$ e $\overline{P}_3$ se ramificam com índice de ramificação 3 e 2 respectivamente;
2. $\overline{P}_2$ e $\overline{P}_3$ se ramificam com índice de ramificação 3 e 4 respectivamente;
3. $\overline{P}_1$, $\overline{P_2}$ e $\overline{P}_3$ se ramificam com índice de ramificação 2, 3 e 2 respectivamente.

Comparando com os resultado anteriores, nenhum desses casos é possível. Por tanto, o núcleo é trivial e $G \simeq S_4$.

4.3.1.2.3 $e_3 = 5$

Então $|G| = 60$. Analogamente ao caso 1 no final da página 50, $G \simeq A_5$.

4.3.2 $\overline{P_1}$ tem ramificação selvagem

Pelo Lema 1 e a equação 4.4, é claro que este caso é impossível.

Vamos juntar os resultados anteriores no seguinte

Teorema 107. Seja $F = K(x)$ onde K tem característica $p > 0$. Seja $G \leqslant \mathrm{Aut}(F/K)$ finito não trivial e seja $E = F^G$. Logo G é um dos seguintes grupos, tendo F/E a correspondente propriedade de ramificação:

1. C_n com $p \nmid n$, tal que
   - $s = 1$, $e_1 = |G|$, $d_1 = 2$, ou
   - $s = 2$, $e_1 = e_2 = |G|$, $d_1 = d_2 = 1$;
2. $p-$grupo abeliano elementar, com $s = 1$, $e_1 = |G|$, $d_1 = 1$;
3. D_n com
   - $p = 2$, $2 \nmid n$ $s = 2$, $e_1 = 2$, $e_2 = n$, $d_1 = d_2 = 1$, ou
   - $2 < p$, $p \nmid n$, $s = 2$, $e_1 = n$, $e_2 = 2$, $d_1 = 1$, $d_2 = 2$, ou
   - $2 < p$, $p \nmid n$, $s = 3$, $e_1 = e_2 = 2$, $e_3 = n$, $d_1 = d_2 = d_3 = 1$;
4. A_4 com
   - $p \neq 2,3$, $s = 2$, $e_1 = 2$, $e_2 = 3$, $d_1 = 1$, $d_2 = 2$, ou
   - $s = 3$, $e_1 = 2$, $e_2 = e_3 = 3$, $d_1 = d_2 = d_3 = 1$;
5. S_4 com $p \neq 2,3$, $s = 3$, $e_1 = 2$, $e_2 = 3$, $e_3 = 4$, $d_1 = d_2 = d_3 = 1$;
6. A_5 com
   - $p = 3$, $s = 2$, $e_1 = 6$, $e_2 = 5$, $d_1 = d_2 = 1$, ou
   - $p \neq 2,3,5$, $s = 3$, $e_1 = 2$, $e_2 = 3$, $e_3 = 5$, $d_1 = d_2 = d_3 = 1$;
7. um produto semidireto de um $p-$grupo abeliano elementar de ordem q com um grupo cíclico de ordem $n|q-1$, $s = 2$, $e_1 = |G|$, $e_2 = n$, $d_1 = d_2 = 1$.
8. $\mathrm{PSL}(2,q)$,com $p \neq 2$, $q = p^m$, $s = 2$, $e_1 = \dfrac{q(q-1)}{2}$, $e_2 = \dfrac{q+1}{2}$, $d_1 = d_2 = 1$, $\overline{P_1}$ tem $q+1$ extensões de grau 1 em F;
9. $\mathrm{PGL}(2,q)$ com $q = p^m$, $s = 2$, $e_1 = q(q-1)$, $e_2 = q+1$, $d_1 = d_2 = 1$, $\overline{P_1}$ tem $q+1$ extensões de grau 1 em F.

4.4 Subgrupos finitos de $\mathrm{PGL}(2,\mathbf{p^m})$

Seja $q=p^m$. Vamos aplicar o teorema anterior ao caso $K=\mathbb{F}_q$ e $F=K(x)$. Dessa forma vamos encontrar os subgrupos de $G:=\mathrm{Aut}(F/K)\simeq \mathrm{PGL}(2,q)$ (Proposição 89). O objetivo é provar o Teorema 113.

Pelo Teorema 22, se $f|m$, $\mathbb{F}_{p^m}$, $\mathbb{F}_{p^f}(x)\subset \mathbb{F}_{p^m}(x)$. Temos $\mathrm{Aut}(\mathbb{F}_{p^f}(x)/\mathbb{F}_{p^f})\hookrightarrow G$, isso implica que $\mathrm{PGL}(2,p^f)$ e $\mathrm{PSL}(2,p^f)$ são subgrupos de G.

Proposição 108. Seja $E=F^G$. Em F/E temos:

1. Todo lugar P de grau 1 em F tem ramificação selvagem, sendo $G_0(P)$ o produto semidireto de um $p-$grupo abeliano elementar de ordem $q=p^m$ com um grupo cíclico de ordem $q-1$; $G_1(P)$ é um $p-$grupo abeliano elementar de ordem q e $G_2(P)$ trivial. Todos os lugares de grau 1 de F são conjugados por G.
2. Todo lugar P de grau 2 em F tem ramificação mansa, sendo $G_{-1}(P)\simeq D_{p^m+1}$, $f(P|E)=2$ e $G_0(P)$ um grupo cíclico de ordem $q+1$. Todos os lugares de grau 2 são conjugados, e existem $\dfrac{q(q-1)}{2}$ desses lugares.
3. Os outros lugares de F são não ramificados sobre E.

Demonstração. Como $G=\mathrm{PGL}(2,q)$ então, pelo Teorema 107 (9), existem dois lugares $\overline{P_1}$ e $\overline{P_2}$ de E que se ramificam em F, com $e_1=q(q-1)$ (selvagem) e $e_2=q+1$ (mansa). Além disso, $\overline{P}_1$ tem $q+1$ extensões de grau 1 e $\overline{P_2}$ tem grau 1. Isso implica (3).

(1) F tem exatamente $q+1$ lugares de grau 1 (Observação 86), por tanto, todos aqueles lugares estão acima de $\overline{P_1}$. O resultado segue do Lema 104, do Teorema 65(2) e do Teorema 61(2).

(2) Existem q^2 polinômios mônicos e $\binom{q}{2}+q$ polinômios redutíveis mônicos de grau 2 sobre $\mathbb{F}_q$. Logo F tem $\dfrac{q(q-1)}{2}$ lugares de grau 2 (Seção 3.1.); seja P um desses lugares. Temos que $f(P|E)\leq 2$ (Observação 42) e $|G|=(q_1-1)q_1(q_1+1)=[F:E]$. Por tanto, da Igualdade Fundamental segue que $e(P|E)\geq \dfrac{|G|}{q(q-1)}=q+1$, em particular P é ramificado, está acima de $\overline{P_2}$, $e(P|F)=q+1$, $f(P|F)=2$ e $|G_Z(P)|=2(q+1)$ (Teorema 61). Observando a prova do Teorema 107, D_{q+1} é o único subgrupo tal que F/E tem um lugar com ramificação mansa e índice de ramificação $\dfrac{|G|}{2}$. Isso termina a prova. □

Vamos considerar a ação de G nos lugares de grau 1 de F, que é transitiva pela proposição anterior. Temos que $G_{-1}=G_0$ para lugares de grau 1 em F, pois o grau relativo sobre E é 1 (Observação 42 e Teorema 61). Sejam P_1 e P_2 lugares de grau 1 em F; pelo feito em 4.2.2.2.2, casos 2 e 3,

$$G_0(P_1)\cap G_0(P_2)=\langle\sigma\rangle,\ \text{de ordem } p^m-1.$$

Seja P_3 um lugar de grau 1 distinto de P_1 e P_2, pela Proposição 89,

$$\exists \lambda \in G \text{ tal que } \lambda(P_1) = P_2,\ \lambda(P_2) = P_1 \text{ e } \lambda(P_3) = P_3.$$

Observe que $\lambda^2 = 1$, pois tem três pontos fixos.

Lema 109. *D_n é um subgrupo de G se $n|p^m \pm 1$.*

Demonstração. A Proposição 108(1) implica que D_n é um subgrupo quando $n|p^m+1$.
Seja $J = \langle \sigma, \lambda \rangle$ temos que $|J| = 2(p^m-1)$. A órbita de P_1 pela ação de J é $\{P_1, P_2\}$, logo $e(P_1|F^J) = \dfrac{|J|}{2}$ (Teorema 59 e Observação 42). Assim, como na prova do item 2 da Proposição 108, $J \simeq D_{p^m-1}$. por tanto PGL$(2,p^m)$ contém D_n para $n|p^m-1$. □

Observação 110. Reordenando os lugares se for necessário, podemos supor que $P_1 = 0$, $P_2 = \infty$ e $P_3 = 1$. Seja a um gerador de $\mathbb{F}_{p^m}^{\times}$ (Teorema 22 (3)). Assim, pela equação 3.2, $\lambda(x) = \dfrac{1}{x}$ e $\sigma(x) = ax$.

Se $p > 2$, então pelo Lema 90, λ fixa mais outro lugar de grau 1, digamos P_4, distintos dos anteriores P_i. Como no parágrafo anterior, seja τ um gerador de $G_0(P_3) \cap G_0(P_4)$. Temos que $\tau^{\frac{p^m-1}{2}} = \lambda$. Seja $\gamma = \sigma^{\frac{p^m-1}{2}}$, note que $\gamma(P_i) = P_i$, com $i = 1,2$.
Pela Observação 110, $\gamma(x) = -x$, logo λ e γ comutam. Segue que $\gamma(P_3) = \gamma(\lambda(P_3)) = \lambda(\gamma(P_3))$, logo λ fixa $\gamma(P_3)$. Como γ não fixa P_3, temos que $\gamma(P_3) = P_4$. Similarmente, $\gamma(P_4) = P_3$.

Lema 111. *S_4 é um subgrupo de G se $p > 2$.*

Demonstração. Note que $4|p^m-1$ ou $4|p^m+1$. Se $4|p^m-1$, seja $H = \langle \gamma, \lambda \rangle \simeq D_2$, e seja $N = N_G(H)$. Sejam $\alpha = \sigma^{\frac{p^m-1}{4}}$ e $\beta = \tau^{\frac{p^m-1}{4}}$, vamos mostrar que eles estão em N.
Por um lado, α comuta com γ, logo $\alpha\gamma\alpha^{-1} = \gamma$. Agora vamos mostrar que $\alpha\lambda = \lambda\alpha^{-1}$. Considerando a Observação 110, defina $b = a^{\frac{p^m-1}{4}}$, temos que $\alpha(x) = bx$ e $\alpha^{-1}(x) = b^3x$, logo $\alpha(\lambda(x)) = \dfrac{b}{x} = \dfrac{1}{b^3x} = \lambda(\alpha^{-1}(x))$, o que prova o desejado. Segue que $\alpha\lambda\alpha^{-1} = \lambda\alpha^{-1}\alpha^{-1} = \lambda\gamma \in \langle \gamma, \lambda \rangle$. Temos então que $\alpha \in N$, e analogamente, $\beta \in N$.

Como $\lambda\gamma$ tem ordem 2 coprimo com p, fixa 2 lugares de grau 1, P_5 e P_6 (Lema 90), é claro que esses lugares são distintos dos P_i anteriores. Vamos mostrar que $P_1, \ldots, P_6$ são conjugados por N.
Como $H \lhd N$, γ é conjugado a λ e $\lambda\gamma$ em N. Temos que $\lambda(P_1) = P_2$. Seja $\omega \in N$ tal que $\omega\lambda = \gamma\omega$ (Observação 11), temos que $\omega(P_3) = \gamma\omega(P_3)$, logo $\omega(P_3) = P_1$ ou P_2, similarmente ocorre com P_4. Agora seja $\theta \in N$ tal que $\theta\lambda\gamma = \gamma\theta$ (Observação 11), temos que $\theta(P_5) = \gamma(\theta(P_5))$, logo $\theta(P_5) = P_1$ ou P_2, similarmente ocorre com P_6.

Agora mostraremos que $\{P_1, \ldots, P_6\}$ é uma órbita completa da ação de N. Note que para lugares de F de grau 1 distintos dos P_i, as órbitas pela ação de H tem comprimento 4, logo o Teorema 59 implica que esses lugares não podem ser ramificados sobre F^H. Por outro lado, as

órbitas dos P_i por H têm comprimento 2, o que implica que os P_i são ramificados sobre F^H. O último item da Observação 60 implica o que queríamos mostrar. Pelo Teorema 59 e o Teorema 61, $|N| = 6|e(P_1|F^N)| = 6|G_0(P_1|F^N)|$.

Sejam $J = G_0(P_1|F^N)$ e $K = G_0(P_2|F^N)$, pela Observação 63, $\lambda J = K\lambda$. Usando a definição de $N_G(H)$, temos que

$$\lambda J = \bigcup_{n\in J} Hn \setminus J = \bigcup_{n\in J} nH \setminus J = \bigcup_{n\in J} n\{\lambda, \gamma\lambda\} = K\lambda = \bigcup_{n\in K} n\{\lambda, \gamma\lambda\} \Longrightarrow J = K$$

Assim, J fixa dois lugares, então $J \cap G_1(P_1) = \{1\}$ (Observação 106). Como feito em 4.2.2.2.2, casos 2 e 3, $J \hookrightarrow C_n$, com $p \nmid n$, em particular $p \nmid e(P_1|F^N)$. Além disso, como $\alpha \in J$, $4|e(P_1|F^N)$. Examinando a lista no Teorema 107, temos que $N \simeq S_4$.

Se $4|p^m+1$, seja Q_1 um lugar de F de grau 2. Pela Proposição 108, $G_0(Q_1) = \langle\sigma\rangle$ e tem ordem $q+1$. Seja $H \leqslant G_0(P_1)$, pela Proposição 62, Q_1 é totalmente ramificado sobre F^H, logo $f_1(Q_1|F^H) = 1$ e $\mathrm{gr}(Q_1 \cap F^H) = 2$ (Observação 42). Como H é cíclico de ordem coprimo com p, o Teorema 107 mostra que Q_1 é o único lugar ramificado sobre F^H. Seja Q outro lugar de F de grau 2, pelo Teorema 59, $|H| = rf(Q|F^H)$, onde r é o número lugares conjugados com Q pela ação de H. Como $f(Q|F^H)$ divide $f(Q|E) = 2$ (Proposições 44 e 108), H fixa um lugar de grau 2 além de Q_1 somente se $|H| = 2$, i.e., $\gamma := \sigma^{\frac{q+1}{2}}$ é o único automorfismo em $G_0(Q_1)$ que pode fixar outro lugar de grau 2 além de Q_1.
Em particular, σ permuta os lugares de grau 2 distintos de Q_1 (Teorema 57(4)) em ciclos de comprimento p^m+1 ou $\dfrac{p^m+1}{2}$. Como $p^m+1 \nmid \dfrac{(p^m-2)(p^m+1)}{2}$, existe pelo menos um ciclo de comprimento $\dfrac{p^m+1}{2}$. Por tanto $\sigma^{\frac{p^m+1}{2}}$ fixa pelo menos $\dfrac{p^m+1}{2}$ lugares de grau 2 distintos de Q_1; seja Q_2 um deles. Seja τ um gerador de $G_0(Q_2)$. Defina $\lambda = \tau^{\frac{p^m+1}{2}}$, então $\langle\gamma,\lambda\rangle \simeq D_2$. Seja N o normalizador de $\langle\gamma,\lambda\rangle$ em G. Analogamente ao caso anterior, temos que $N \simeq S_4$. □

Lema 112. *A_5 é um subgrupo de G se $p = 5$ ou $5|p^{2m}-1$.*

Demonstração. Se $p = 5$, note que $A_5 \simeq \mathrm{PSL}(2,5)$, então A_5 é um subgrupo de G pelo visto no início desta seção.
Em geral, A_5 é gerado por dois elementos α e β que satisfazem as relações $\alpha^5 = \beta^2 = (\alpha\beta)^3 = 1$. Vamos produzir elementos em G satisfazendo essas relações.
Note que se $5|p^{2m}-1$ então $5|p^m-1$ ou $5|p^m+1$. Seja $q = p^m$.

Se $5|q-1$, pela Observação 23 existe uma raiz quinta da unidade a em $\mathbb{F}_{p^m}$. Seja $\alpha \in G$ definida por $\alpha(x) = ax$, ela tem ordem 5. Seja β o automorfismo definido por $\beta(x) = \dfrac{x-a^2}{cx-1}$, onde $c = a^4 - a^3 + a^2$. É claro que α e β satisfazem as condições desejadas, logo G contém A_5.

Se $5|q+1$, temos que $\mathbb{F}_{q^2}(x)/\mathbb{F}_{q^2}$ é uma extensão de constantes galoisiana de $\mathbb{F}_q(x)/\mathbb{F}_q$ de grau 2 (Teorema 22(2)). Seja $\mathrm{Aut}(\mathbb{F}_{q^2}(x)/\mathbb{F}_{q^2}(x)) = \langle\sigma\rangle$, pelo Teorema 22(2), $\sigma(y) = y^q$ se $y \in \mathbb{F}_{q^2}$. Seja $G' = \mathrm{Aut}(\mathbb{F}_{q^2}(x)/\mathbb{F}_{q^2})$, temos que G pode ser visto como o subgrupo de G' dos

elementos que comutam com σ. Seja Q um lugar de $\mathbb{F}_q(x)$ de grau 2 e P uma extensão de Q em $\mathbb{F}_{q^2}(x)$, pela Proposição 53, $\mathbb{F}_{q^2}(x)/\mathbb{F}_q(x)$ é não ramificado e, pela unicidade de $\mathbb{F}_{q^2}$ (Teorema 22(2)), o corpo residual de P é $\mathbb{F}_{q^2}$, logo $\operatorname{gr} P = 1$. Pelo Teorema 59 e a Observação 42, Q possui dois extensões P_1 e P_2 em F de grau 1, tal que $\sigma(P_1) = P_2$.

Seja $y^* \in \mathbb{F}_{q^2}(x)$ com $(y^*) = P_1 - P_2$ (Observação 88), temos que $(\sigma(y^*)) = P_2 - P_1$ (Teorema 57(1)), assim $(y^*\sigma(y^*)) = 0$, logo $y^*\sigma(y^*) \in \mathbb{F}_{q^2}$ (Proposição 30). Escolha $\varepsilon \in \mathbb{F}_{q^2}$ tal que $\varepsilon y^*\sigma(\varepsilon y^*) = \varepsilon^{q+1} y^*\sigma(y^*) = -1$ (Observação 23), defina $y = \varepsilon y^*$. Pelo Teorema 31, $\mathbb{F}_{q^2}(y) = \mathbb{F}_{q^2}(x)$ pois $\operatorname{gr}((y)_0) = 1$. Além disso $\sigma(y) = -\dfrac{1}{y}$.

Seja a um raiz quinta da unidade em $\mathbb{F}_{q^2}$ (Observação 23). Seja $\alpha \in G'$ definido por $\alpha(y) = a^2 y$, ele tem ordem 5. Seja $\beta \in G'$ definida por $\beta(y) = \dfrac{by + c}{-\sigma(c)y + \sigma(b)}$, com $b = \dfrac{1}{a - \sigma(a)}$ e $c \in \mathbb{F}_{q^2}$ que satisfaz a equação $c\sigma(c) = c^{q+1} = 1 - b\sigma(b)$ (Observação 23).
Note que $a^{q+1} = 1$, logo $\sigma(a)^2 = (a^q)^2 = \dfrac{1}{a^2}$. Segue que $\alpha\sigma(y) = -\dfrac{1}{a^2 y} = \sigma(a^2)\sigma(y) = \sigma\alpha(y)$, logo α comuta com σ. Por outro lado, é claro que $\beta^2 = (\alpha\beta)^3 = 1$, e que β comutam com σ. Isso implica que a imagem de G em G' contém A_5. □

Teorema 113. Os subgrupos de PGL$(2, p^m)$ são:

1. $p-$grupos abelianos elementares de ordem p^f com $f \geq m$;
2. C_n com $n | p^m \pm 1$
3. D_n com $n | p^m \pm 1$;
4. A_4, para $p > 2$ ou $p = 2$ e $2 | m$
5. S_4 para $p > 2$;
6. A_5 para $p = 5$ ou $5 | p^{2m} - 1$
7. produtos semidiretos de um $p-$grupo abeliano elementar de ordem p^f com um grupo cíclico de ordem n, tal que $f \leq m$, $n | p^f - 1$ e $n | p^m - 1$.
8. PSL$(2, p^f)$ e PGL$(2, p^f)$ com $f | m$.

Demonstração. Note que A_4 é o produto semidireto de um grupo elementar abeliano de ordem 4 com um grupo cíclico de ordem 3. Além disso, para $p = 2$, temos que PSL$(2, p^f) =$ PGL$(2, p^f)$. Esses fatos, junto com a Proposição 9, mostram que todos os subgrupos listados acima aparecem na lista do Teorema 107.
Por outro lado, um grupo na lista do Teorema 107 pode ser subgrupo de G somente se seu correspondente índice de ramificação divide ao índice correspondente ao caso (9) daquele teorema. Disso decorrem as restrições que aparecem na lista acima. Só falta mostrar que cada

grupo na lista acima é de fato um subgrupo de G.
No inicio desta seção mostramos a presença dos subgrupos em (8). A Proposição 108 mostra (1), (2) e (7), e os três lemas anteriores mostram (3), (5) e (6). Finalmente, observe que A_4 cai (diretamente ou como subgrupo) nos item (5) e (7) quando $p > 2$ e $p = 2$, respectivamente. □

Suponha agora que K é algebricamente fechado. Seja G um subgrupo finito de $\mathrm{Aut}(K(x)/K)$, ele tem que estar na lista do Teorema 107. O Teorema 113 mostra que todo grupo listado no Teorema 107 é um subgrupo de $\mathrm{Aut}(\mathbb{F}_{p^m}(x)/\mathbb{F}_{p^m})$ para algum m. Por outro lado, todo $\alpha \in \mathrm{Aut}(\mathbb{F}_{p^m}(x)/\mathbb{F}_{p^m})$ pode se associar ao automorfismo de $K(x)/K$ definido por $x \mapsto \alpha(x)$. Assim, todo grupo listado no Teorema 113 é um grupo finito de automorfismos de $K(x)$. Em conclusão,

Teorema 114. Seja K um corpo algebricamente fechado de característica $p > 0$. Os subgrupos finitos de $\mathrm{Aut}(K(x)/K)$ são:

1. p-grupos abelianos elementares;
2. grupos cíclicos de ordem não divisível por p;
3. D_n com $p \neq n$;
4. A_4;
5. S_4 para $p > 2$;
6. A_5;
7. produtos semidiretos de $p-$grupos abelianos elementares de ordem p^f e grupos cíclicos de ordem n com $n|p^f - 1$ e f arbitrário;
8. $\mathrm{PSL}(2, p^f)$ e $\mathrm{PGL}(2, p^f)$ com f arbitrário.

CAPÍTULO

5

AUTOMORFISMOS DE CURVAS DE ARTIN-SCHREIER

Nessa seção vamos estudar os grupos de automorfismos de extensões de Artin-Schreier da forma $F/K(x)$, onde K é um corpo algebricamente fechado de característica $p > 0$. Para isso, vamos determinar em quais casos $K(x)$ é a única subextensão racional de F tal que $F/K(x)$ é normal de grau p, pois nesse caso mostra-se que $\mathrm{Aut}(F/K)$ é uma extensão de um grupo cíclico de ordem p por um subgrupo finito de $\mathrm{Aut}(K(x)/K)$ (Observação 100). Também vamos indicar os grupos de automorfismos nos casos excepcionais.

Seja $F/K(x)$ uma extensão de Artin-Schreier sobre um corpo de funções racionais $K(x)$, onde K é um corpo algebricamente fechado de característica $p > 0$. A extensão é representada por uma equação

$$y^p - y = r(x), \text{ onde } r(x) \in K(x) \setminus K. \tag{5.1}$$

Note que se $r(x)$ for constante, então a equação $w^p - w = r(x)$ teria soluções em K, em contra da condição 3.7.
F pode ser realizada como o corpo de funções de uma curva de Artin-Schreier C, i.e., $F = K(C)$. Daqui na frente, usaremos a notação da seção 3.1. para os lugares de $K(x)$, colocando uma barra acima deles.

Proposição 115. Na equação 5.1, y e $r(x)$ podem ser escolhidos tal que $\overline{P}_\infty$ é não ramificado e

$$r(x) = \frac{f(x)}{\prod_{i=1}^{r}(x-a_i)^{\lambda_i}}$$

com $\lambda_i > 0$, $\mathrm{gr}\, f < \sum_{i=1}^{s} \lambda_i$, $(\lambda_i, p) = 1$ e f coprimo com os $(x-a_i)$.

Demonstração. Podemos assumir que $v_{P_\infty}(r(x)) \geq 0$. De fato, suponha que $v_{P_\infty}(r(x)) < 0$, seja

$r(x) = \dfrac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0}$ com $n > m$, logo

$$s(x) := r\left(\frac{1}{x}\right) = \frac{a_0 x^n + \cdots + a_n}{b_0 x^n + \cdots b_0 x^{n-m}}.$$

Seja $w = \dfrac{1}{x}$, temos que $F = K(y,w)$ e

$$y^p - y = s(w), \text{ tal que } v_{P_\infty}(s(w)) = 0.$$

Pela Proposição 97, P_∞ é não ramificado para esta equação, pois $m_p = -1$ escolhendo $z = 0$.

Seja

$$r(x) = c + \sum_{i=1}^{r} \sum_{j=1}^{\lambda_i} \frac{c_{ij}}{(x-a_i)^j}$$

uma decomposição de $r(x)$ em frações parciais(Proposição 13). Podemos supor que $c = 0$, de fato, seja $t \in K$ uma solução de $x^p - x = c$. Seja $z = y - t$, temos que $F = K(z,x)$ e

$$z^p - z = y^p - y - c = r(x) - c.$$

Suponha que $n_i = kp$. Escolha $h \in K$ tal que $h^p = c_{1j}$. Defina $z = y - \dfrac{h}{(x-a_i)^k}$, temos que

$$z^p - z = r(x) - \frac{c_{1\lambda_i}}{(x-a_i)^{\lambda_i}} + \frac{h}{(x-a_i)^k}.$$

Assim, podemos assumir que $p \nmid \lambda_i$, para cada $i = 1, \ldots, n$. Logo

$$r(x) = \frac{f(x)}{\prod_{i=1}^{r}(x-a_i)^{\lambda_i}}, \text{ onde } f(x) = \sum_{i=1}^{r} \sum_{i=1}^{\lambda_i} c_{ij}(x-a_i)^{\lambda_i - j} \prod_{k \neq i} (x-a_k)^{\lambda_i}$$

Note que $x - a_i$ divide todos os somandos em $f(x)$, exceto aquele com coeficiente $c_{i\lambda_i}$, logo $f(x)$ é coprimo com cada $(x-a_i)$; além disso $\operatorname{gr} f < \sum_{i=1}^{s} \lambda_i$. □

Daqui na frente vamos assumir que a equação 5.1 satisfaz as condições da proposição anterior. Temos que $v_{P_{(x-a_i)}}(r(x)) = -\lambda_i$ para todo $i = 1, \ldots, r$ e $v_P(r(x)) = 0$ para outros lugares de $K(x)$, logo a Proposição 97 mostra que os $\overline{P}_{x-a_i}$ são os únicos lugares de $K(x)$ que se ramificam em F.

Segue da Proposição 97 que o gênero de F é

$$g = \frac{p-1}{2}\left(\sum_{i=1}^{r}(\lambda_i + 1) - 2\right) \tag{5.2}$$

Seja P_i a extensão de $\overline{P}_{x-a_i}$ em F, temos que a Conorma é $\operatorname{Con}_{F/K(x)}(\overline{P}_{x-a_i}) = p \cdot P_i$, e o Diferente fica

$$\operatorname{Diff}(F/K(x)) = \sum_{i=1}^{r}(\lambda_i + 1)(p-1) \cdot P_i. \tag{5.3}$$

5.1 Grupo de automorfismos

Quando $g = 1$, a curva C dada pela equação 5.1 é uma curva elítica, logo $\mathrm{Aut}(F/K)$ é um grupo infinito (veja Seção 3.3).

Quando $g \leq 2$, o Teorema 55 mostra que o grupo dos automorfismos de $F = K(C)$ que fixam K, $\mathrm{Aut}(F/K)$, é finito. Estaremos interessados em encontrar esse grupo.
Vamos determinar os subcorpos racionais $K(z)$ de F tais que $F/K(z)$ é normal de grau p. No caso que $K(x)$ seja o único subcorpo com essas condições, $\mathrm{Aut}(F/K(x))$ é uma extensão de um grupo cíclico de ordem p por um subgrupo finito de $\mathrm{PGL}(2,K)$ (Observação 100).

5.1.1 Diferenciais e lacunas

Seja $K(z)$ como no parágrafo acima, pelo Corolário 51(3), pela Observação 42 e o Teorema 59, existe um lugar P de F totalmente ramificado sobre $K(z)$. Seja $\overline{P}_{z-a} = P$, seja $\tilde{z} = \dfrac{1}{z-a} \in K(z)$, então $(\tilde{z})_\infty^{K(z)} = \overline{P}$ e $K(\tilde{z}) = K(z)$. Pela Proposição 46, $(\tilde{z})_\infty^F = p \cdot P$, em particular $z \in \mathscr{L}(p \cdot P)$.
Assim, estamos interessados em subcorpos racionais de F gerados por elementos com divisor de polos em F da forma $p \cdot P$. Para isso, vamos estudar as sequências de lacunas dos lugares de F, o que pode ser feito examinando o espaço das diferenciais holomorfas (Observação 39).

Pelo algoritmo da divisão, para cada $i = 1, \ldots, r$, existem $m_i(\mu)$ e $\varepsilon_i(\mu)$ tais que

$$(p-1-\mu)\lambda_i + (p-1) = m_i(\mu)p + \varepsilon_i(\mu), \quad \text{com } 0 \leq \varepsilon_i(\mu) \leq p-1.$$

Defina

$$g_\mu(x) = \prod_{i=1}^{r} (x-a_i)^{m_i(\mu)}, \quad t(\mu) = \sum_{i=1}^{r} m_i(\mu).$$

Teorema 116. (BOSECK, 1958, Satz 15) A seguinte é uma base para o espaço das diferenciais holomorfas:

$$\{x^\nu (g_\mu(x))^{-1} y^\mu dx \,|\, t(\mu) \geq 2, 0 \leq \nu \leq t(\mu) - 2\}$$

Teorema 117. (GARCIA, 1989, pag. 235) Para todo $(a,b) \in K^2$, temos bases para o espaço das diferenciais holomorfas:

$$\{(x-a)^\nu (g_\mu(x))^{-1} (y-b)^\mu dx \,|\, t(\mu) \geq 2, 0 \leq \nu \leq t(\mu) - 2\}$$

Observação 118.

- Pela Proposição 35(1), o espaço das diferenciais tem dimensão g. Assim, as bases nos teoremas acima possuim g elementos, em particular existem g pares (μ, ν) tais que $0 \leq \mu \leq p-2, t(\mu) \geq 2, 0 \leq \nu \leq t(\mu) - 2$.
  Pelo Teorema de Weierstrass (3), todos os lugares de F possuem exatamente g lacunas.

Sejam $P \in \mathbb{P}_F$ e $\overline{P} = P \cap K(x)$ tal que $\overline{P} \neq \overline{P}_\infty$, temos que $v_P(r(x)) = e(P|\overline{P}) v_{\overline{P}}(r(x))$, pela propriedade (3) das valorizações discretas, a equação 5.1 e a Proposição 115

$$v_P(y) < 0 \iff P_i = P, \text{ para algum } i \text{ e } p v_P(y) = -p\lambda_i \tag{5.4}$$

$$v_P(y) > 0 \iff P \neq P_i, \ \forall i = 1, \ldots, r \text{ e } \overline{P} \text{ é um zero de } f(x). \tag{5.5}$$

Logo $(y) = A - \sum_{i=1}^{r} \lambda_i P_i$, onde $A \geqslant 0$ e $v_{P_i}(A) = 0$ para todo $i = 1, \ldots, r$ ($v_{\overline{P}_\infty}(y) \geq 0$ pela Proposição 115).

Seja $0 \leq \mu \leq p-2$, pela Observação 80, a Proposição 35 (4) e 5.3 temos que

$$\begin{aligned}
(y^\mu dx) &= \mu A - 2 \cdot \mathrm{Con}_{F/K(x)}(\overline{P}_\infty) + \sum_{i=1}^{r} [(p-1-\mu)\lambda_i + (p-1)] \cdot P_i, \\
(g_\mu(x)) &= -t(\mu) \cdot \mathrm{Con}_{F/K(x)}(\overline{P}_\infty) + p \sum_{i=1}^{r} m_i(\mu) P_i \\
((g_\mu(x))^{-1} y^\mu dx) &= \mu A + (t(\mu) - 2) \cdot \mathrm{Con}_{F/K(x)}(\overline{P}_\infty) + \sum_{i=1}^{r} \varepsilon_i(\mu) P_i.
\end{aligned} \tag{5.6}$$

Para cada $i = 1, \ldots, r$, o diferencial $(x-a_i)^\nu (g_\mu(x))^{-1} y^\mu dx$ é holomorfo (Teorema 117), e a valorização dele em P_i é $vp + \varepsilon_i(\mu)$. Pela Observação 39,

$$\nu p + \varepsilon_i(\mu) + 1, \ t(\mu) \geq 2 \ , 0 \leq \nu \leq t(\mu) - 2 \tag{5.7}$$

são lacunas de P_i, e pela definição de $\varepsilon_i(\mu)$, todas elas são distintas entre si. Pela Observação 118, essas são todas as lacunas de P_i.

Dado $i = 1, \ldots, r$, note que m_i é uma função decrescente, logo t também é. Se $t(p-2) \geq 2$ então, por 5.7, $\varepsilon_i(\mu) + 1$ é uma lacuna de P_i para cada $0 \leq \mu \leq p-2$. Como $\varepsilon_i(\mu)$ vai de 0 até $p-2$, P_i tem lacunas em $1, \ldots, p-1$.

Observação 119. Se $P \in \mathbb{P}_F$ tem lacunas em $1, \ldots, p-1$ (por exemplo, se $P = P_i$, $i = 1, \ldots, r$) então, pela Observação 39 e a Proposição 40,

$$1 = l(0) = l(P) = \cdots = l((p-1)P).$$

. Como $\left(\frac{1}{x-a_i}\right)_\infty^F = p \cdot P_i$, então $\mathscr{L}(p \cdot P_i) = \left\langle 1, \frac{1}{x-a_i} \right\rangle$.

Agora, seja P um lugar de F não ramificado sobre $K(x)$. Seja $e = e(P|K(y))$ e seja $\tilde{y} = y - b$ tal que $P \cap K(y) = \overline{P}_{y-b} \in \mathbb{P}_{K(y)}$,

Observação 120.

- Pela Proposição 41, $e = v_P(\tilde{y})$ e dado $Q \in \mathbb{P}_F$, $v_Q(\tilde{y}) = 0$ se $Q \cap K(y) \notin \{\overline{P}_{y-b}, \overline{P}_{\frac{1}{y-b}}\}$.
- Se $b \neq 0$, pela a propriedade (3) das valorizações e 5.4, $v_{P_i}(\tilde{y}) = v_{P_i}(y) = -\lambda_i$ para cada $i = 1, \ldots, r$, logo $P_i \cap K(y) = \overline{P}_{\frac{1}{y-b}}$, $\forall i = 1, \ldots, r$. Note que os P_i são os únicos polos de $\tilde{y}$. O mesmo acontece se $b = 0$.

Se P não está acima de $\overline{P}_\infty \in \mathbb{P}_{K(x)}$, seja $\tilde{x} = x - a$ tal que $P \cap K(x) = \overline{P}_{x-a} \in \mathbb{P}_{K(x)}$. Pelo Teorema 117, $\tilde{x}^\nu (g(x))^{-1} \tilde{y}^\mu dx$ é um diferencial holomorfo; pela Observação 120, a Proposição 35 (4) e 5.6, a sua valorização em P é $\nu + \mu e$. Logo, pelas Observações 39 e 118, segue que

$$\nu + \mu e + 1,\ 0 \leq \mu \leq p-2\ , t(\mu) \geq 2\ , 0 \leq \nu \leq t(\mu) - 2 \tag{5.8}$$

contém todas as lacunas de P.

Se P está acima de $\overline{P}_\infty$ então P é um somando de $\mathrm{Con}_{F/K(x)}(\overline{P}_\infty)$. Pela Observação 120 e 5.6, temos que $v_p(x^\nu (g(x))^{-1} \tilde{y}^\mu dx) = t(\mu) - 2 - \nu + \mu e$. Considerando a mudança de variável $\mu = t(\mu) - 2 - \nu$, observamos que 5.8 contém também todas as lacunas de P neste caso.

Agora vamos determinar os subcorpos racionais $K(z)$ tais que $F/K(z)$ é uma extensão normal de grau p. Pela análise no início desta Seção, vamos procurar $z \in F$ tal que

$$(z)_\infty^F = p \cdot P, \ \text{ com } P \text{ totalmente ramificado sobre } K(z) (\text{logo } z \in \mathscr{L}(p \cdot P)). \tag{5.9}$$

Faremos uma análise por casos.

5.1.2 $t(0) \geq p+1$

Dado $P \in \mathbb{P}_F$ não ramificado sobre $K(x)$, por 5.8, $\nu + 1$ é uma lacuna de P, $0 \leq \nu \leq t(0) - 2$. Em particular, p é uma lacuna de P, pela hipótese. Por tanto, se existe z satisfazendo 5.9, $P = P_i$ para algum i.

Observação 121. Temos que $m_i(0) = \lambda_i - \left[\frac{\lambda_i}{p}\right]$. Se $\lambda_i \geq p+2$ então $m_i(0) \geq p+1$; se $\lambda_i = p+1$ então $m_i(0) = p$; se $\lambda_i < p$ então $m_i(0) = \lambda_i$.

Pela definição de $t(\cdot)$, temos que $r \geq 2$ ou $\lambda_1 \geq p+2$. Por outro lado, $m_i(p-2) = \left[\frac{\lambda_i + p - 1}{p}\right]$. Se $\lambda_1 \geq p+2$ então $m_1(p-2) \geq 2$, logo $t(p-2) \geq 2$, como $m_i(p-2) \geq 1$, se $r \geq 2$ então de novo $t(p-2) \geq 2$.

Pela Observação 119, $\mathscr{L}(p \cdot P) = \left\langle 1, \frac{1}{x - a_i} \right\rangle$. Se existe z satisfazendo 5.9 então é da forma $\alpha + \frac{\beta}{x - a_i}$, com $\alpha, \beta \in K$ e $\beta \neq 0$. Como $K\left(\alpha + \frac{\beta}{x - a_i}\right) = K(x)$, concluímos que para $t(0) \geq p+1$, $K(x)$ é o único subcorpo racional tal que $F/K(x)$ é uma extensão normal de grau p.

Vamos focar no caso $t(0) \leq p$. Pela Observação 121, temos que: (1) $r = 1$, $\lambda_1 \leq p+1$ ou (2) $r \geq 2$, $\sum_{i=1}^{r} \lambda_i \leq p$.

5.1.3 $r \geq 3$ e $\sum_{i=1}^{r} \lambda_i \leq p$

Neste caso $m_i(p-2) = 1$ para cada i, logo $t(0) \geq t(p-2) = r \geq 3$. Se P é não ramificado sobre $K(x)$, pela Observação 5.8 temos que $\mu e + 1$ e $\mu e + 2$ são lacunas de P para $0 \leq \mu \leq p-2$, onde $e = e(P|K(y))$.
Por 5.1 e o Teorema 59,

$$1 \leq e \leq [F : K(y)] = \sum_{i=1}^{r} \lambda_i \leq p.$$

Se $e = 1$ então $p = (p-2)1 + 2$ é uma lacuna de P. Se $1 < e_P < p$, seja μ_0 tal que $\mu_0 e_P \equiv p-1 \mod p$ e $1 \leq \mu_0 \leq p-2$, logo $\mu_0 e_P + 1$ é uma lacuna de P, divisível por p. Então p deve ser uma lacuna de P, pois as não lacunas formam um semigrupo aditivo (Teorema de Weierstrass).
Por tanto, se $e(P|K(y)) < p$ para todos os lugares não ramificados sobre $K(x)$, então os P_i são os únicos lugares de F tais que p não é uma lacuna. Como feito no caso 5.1.2, temos que $K(x)$ é o único subcorpo racional de F tal que $F/K(x)$ é uma extensão racional de grau p.

Se $e(P|K(y)) = p$ para algum P não ramificado sobre $K(x)$ então $\sum_{i=1}^{r} \lambda_i = p$. Seja $\tilde{y} := y - b$ como na Observação 120, temos que $(\tilde{y})_0^F = p \cdot P$, logo $\left(\frac{1}{\tilde{y}}\right)_\infty = p \cdot P$.
Por outro lado, $m_i(0) = \lambda_i$, logo $t(0) = p \geq 2$. Então, por 5.8, $\nu + 1$ é uma lacuna de P, para $0 \leq \nu \leq p-2$; em particular p é a menor não lacuna de P.
Pela Observação 119 aplicada a nosso caso, $\mathscr{L}(p \cdot P) = \left\langle 1, \frac{1}{\tilde{y}} \right\rangle$. Assim, todo elemento de $\mathscr{L}(p \cdot P)$ com divisor de polos $p \cdot P$ é da forma $\alpha + \frac{\beta}{\tilde{y}}$ com $\alpha, \beta \in K$, $\beta \neq 0$. Como $K\left(\alpha + \frac{\beta}{\tilde{y}}\right) = K(y)$, $K(y)$ é o único subcorpo racional, além de $K(x)$, que pode satisfazer 5.9.

Suponha que $F/K(y)$ é normal de grau p. Pela Observação 120 e Teorema 59, os P_i são conjugados pela ação de $\mathrm{Aut}(F/K(y))$, $r = p$ e os $\lambda_i = 1$.

Pela Observação 91, podemos supor que P está acima de $\overline{P}_\infty \in \mathbb{P}_{K(x)}$ e que $a_1 = 0$ e $a_2 = 1$, logo a equação 5.1 fica

$$y^p - y = r(x) = \frac{f(x)}{x(x-1)\prod_{i=3}^{p}(x - a_i)}$$

Temos que $f(x) \in K^\times$. De fato, pela Proposição 41, $v_P(r(x)) = p - \mathrm{gr}\, f(x) > 0$ (Proposição 115). Por outro lado, considerando a extensão $F/K(y)$, $v_P(r(x)) = p v_{\overline{P}_{y-b}}(y^p - y)$, então $\mathrm{gr}\, f(x) = 0$, como desejado.

Seja $\sigma \in \mathrm{Aut}(F/K(y))$ tal que $\sigma(P_1) = P_2$. Pelas Observações 58 e 5.7,

$$\mathscr{L}(p \cdot P_1) = \left\langle 1, \frac{1}{x} \right\rangle \overset{\sigma}{\longmapsto} \mathscr{L}(p \cdot P_2) = \left\langle 1, \frac{1}{x-1} \right\rangle \implies K(x) \overset{\sigma}{\longrightarrow} K(x) \text{ e } \overline{P}_1 \overset{\sigma}{\longmapsto} \overline{P}_2$$

Note que σ fixa P (Teorema 59), então σ fixa $\overline{P}_\infty \in \mathbb{P}_{K(x)}$. Por tanto, σ se restringe a um automorfismo de $K(x)$ de ordem p (pois $|\mathrm{Aut}(F/K(y))| = p$) que fixa $\overline{P_\infty}$ e leva $\overline{P_1}$ em $\overline{P_2}$. Por

3.2, $\sigma(x) = x - 1$, em particular $\sigma^j(x) = x - j$ para $j = 0, \ldots, p-1$, que deve coincidir com os $(x - a_i)$ pois $\mathrm{Aut}(F/K(y)) = \langle\sigma\rangle$. Por tanto a função geradora de F fica

$$y^p - y = \frac{a}{x(x-1)\cdots(x-p+1)} = \frac{a}{x^p - x}$$

Observamos que $F/K(y)$ é uma extensão de Artin-Schreier, logo satisfaz 5.9. Por tanto, neste caso, $K(x)$ é o único subcorpo de F tal que 5.9 é satisfeito, excepto quando F é isomorfo a $y^p - y = \dfrac{a}{x^p - x}$.

5.1.4 $r = 2$ e $3 \leq \sum_{i=1}^{r} \lambda_i \leq p$

Pelo menos um $\lambda > 1$; podemos supor que $\lambda_1 \geq 2$. Olhando os m_i, é claro que $t(p-2) = 2$. Pela Observação 5.7, $\mathscr{L}(p \cdot P_1) = \left\langle 1, \dfrac{1}{x - a_1} \right\rangle$.
Suponha que $K(z) \neq K(x)$ é um subcorpo que satisfaz 5.9. Note que $z \notin \mathscr{L}(p \cdot P_1)$, pela análise no início da Seção 4.2.1., P_1 não pode ser totalmente ramificado sobre $K(z)$, e pelo Teorema 59, P_1 é não ramificado sobre $K(z)$. Além disso, P_1 possui $p \geq 3$ conjugados sobre $K(y)$, como $r = 2$ e cada lugar ramificado de $K(x)$ tem uma única extensão em F, existe $\sigma \in \mathrm{Aut}(F/K(y))$ tal que $P := \sigma(P_1)$ é não ramificado sobre $K(x)$.

Seja $w = \sigma\left(\dfrac{1}{x - a_1}\right)$; pela Observação 58 temos que $(w)_\infty^F = p \cdot P$. Sabemos que $F = K(x,y) = K(x)(y) = K(x)[y]$, além disso $\{y^i\}_{i=0}^{p-1}$ é uma base de F como $K(x)-$espaço vetorial, logo $w = \sum_{j=0}^{p-1} r_j(x) y^j$, com $r_j(x) \in K(x)$. Seja $\mathrm{Tr} : F \to K(x)$ a traça (veja Seção 1.2.2.), vamos analisar $\mathrm{Tr}(w)$.
Seja $j = 1, \ldots, p-2$, pelo Teorema 22 (3), $\mathbb{F}_p = \{b^j \mid b \in \mathbb{F}_p\}$. Logo, pela Proposição 97,

$$\mathrm{Tr}(y^j) = \sum_{b \in \mathbb{F}_p} (y+b)^j = py^j + a_{j-1}y^{j-1} \sum_{b \in \mathbb{F}_p} b + \cdots + a_1 y \sum_{b \in \mathbb{F}_p} b^{j-1} + \sum_{b \in \mathbb{F}_p} b^j = 0 = \mathrm{Tr}(1)$$

e $\mathrm{Tr}(y^{p-1}) = \sum_{b \in \mathbb{F}_p} b^{p-1} = -1$. Pela Proposição 21, $\mathrm{Tr}(w) = -r_{p-1}(x)$.

Por outro lado, se τ é gerador de $\mathrm{Aut}(F/K(x))$ então $\mathrm{Tr}(w) = \sum_{i=1}^{p-1} \tau^j(w)$. Pela Observação 58 e o Teorema 57, $v_{\tau^j(P)}(\tau^j(w)) = -p$ e os $\tau^j(P)$ estão acima de um mesmo lugar $\overline{P}$ em $K(x)$ não ramificado. Pela propriedade (3) das valorizações e a Proposição 46 segue que

$$(\mathrm{Tr}(w))_\infty^F = p \cdot \sum_{i=0}^{p-1} \tau^j(P) = \mathrm{Con}_{F/K(x)}((\mathrm{Tr}(w))_\infty^{K(x)}),$$

logo $(\mathrm{Tr}(w))_\infty^K(x) = p \cdot \overline{P} = (r_{p-1}(x))_\infty^{K(x)}$.
Os P_i não são polos de w, logo $v_{P_i}(w) \geq 0$, e são totalmente ramificados sobre $K(x)$. Por outro

lado, dado $i = 1,2$ temos que $p|v_{P_i}(f(x))$ para todo $f(x) \in K(x)$ (Proposição 41) e $(\lambda_i, p) = 1$. Dado $0 \leq j_1, j_2 \leq p-1$, se

$$v_{P_i}(r_{j_1}(x)) - j_1\lambda_i = v_{P_i}(r_{j_2}(x)) - j_2\lambda_i \implies p \left| v_{P_i}\left(\frac{r_{j_1}(x)}{r_{j_2}(x)}\right) = (j_2 - j_1)\lambda_i \implies j_1 = j_2 \right.$$

Por 5.4 e as propriedades das valorizações, $v_{P_i}(w) = \min\{v_i(r_j(x)) - j\lambda_i \,|\, 0 \leq j \leq p-1\} \geq 0$, com $i = 1,2$, em particular $v_{P_i}(r_{p-1}(x)) > (p-1)\lambda_i$. Assim, $\overline{P_i}$ é um zero de $r_{p-1}(x)$; pelo Teorema 31, $(r_{p-1}(x))^{K(x)} = \overline{P_1} + \overline{P_2} + \overline{A} - p \cdot \overline{P}$, onde $\overline{A}$ é um divisor efetivo de grau $p-2$ tal que $v_{\overline{P}}(\overline{A}) = 0$. Em particular, $r_{p-1}(x)$ não é uma potência $p-$ésima em $K(x)$.

Agora considere $dw = d\left(\sigma\left(\frac{1}{x-a_1}\right)\right)$. Pela Observação 80 e 5.3,

$$\left(d\left(\frac{1}{x-a_1}\right)\right) = -2P_1 + \mathrm{Diff}(F/K(x)) = \gamma_1 \cdot P_1 + \gamma_2 \cdot P_2,$$

onde $\gamma_1 = (\lambda_1 + 1)(p-1) - 2p \geq 0$ e $\gamma_2 = (\lambda_2 + 1)(p-1)$, logo é holomorfa. Pela Observação 79, dw também é holomorfa.
Por outro lado, pela Proposição 71 e o Exemplo 74,

$$dw = \sum_{j=0}^{p-1} [D_x(r_j(x))y^j + j r_j(x) y^{j-1} D_x(y)]dx$$

Por 5.1 temos que $D_x(y) = -D_x(r(x))$, logo

$$dw = \sum_{j=0}^{p-2} [D_x(r_j(x)) - (j+1)r_{j+1}(x)D_x(r(x))]y^j dx + D_x(r_{p-1}(x))y^{p-1}dx$$

Como $r_{p-1}(x)$ não é uma $p-$ésima potência, $D_x(r_{p-1}(x)) \neq 0$.
Observamos que o exponente de y nos elementos da base no Teorema 116 é no máximo $p-2$, logo essa base não pode gerar dw, por tanto dw não pode ser holomorfa, e temos uma contradição. Em conclusão, no caso atual, $K(x)$ é o único subcorpo racional de F que satisfaz 5.9.

5.1.5 $r = 2$, $\lambda_1 = \lambda_2 = 1$

Assumiremos que $p > 2$, pois caso contrário o gênero é 1 por 5.2.
Para encontrar os subcorpos racionais que satisfazem 5.9, vamos procurar os subgrupos de ordem p de $G := \mathrm{Aut}(F/K)$.

Pela equação 5.1 temos que F/K é um corpo de funções hiperelítico. Sejam $E = F^G$ e S o conjunto de lugares de $K(y)$ que se ramificam em F, pelo Teorema 101, $\overline{G} := \mathrm{Aut}(K(y)/E)$ coincide com o subgrupo dos automorfismos de $K(y)$ que mandam S nele mesmo.
Pelo Teorema do Diferente de Dedekind, o exponente no Diferente de $F/K(y)$ de lugares em S é 1. Então, por 4.2 temos que $\mathrm{Diff}(F/K(y)) = |S|$ (todos os lugares de F têm grau 1 pois K é algebricamente fechado), logo, pela Fórmula do Gênero de Hurwitz em $F/K(y)$,

$$2(g-1) = |S| - 4 \implies \text{por 5.2, } g = p-1 \text{ e } |S| = 2p.$$

Seja $\overline{Q} \in S$. Suponha que $G_1(P|E) \neq \{1\}$, logo $\overline{Q}$ tem ramificação selvagem sobre E (Teorema 65). Pela Observação 106, a ação de $G_1(P|E)$ em S fixa somente $\overline{Q}$ e permuta os outros lugares em ciclos de ordem $|G_1(P|E)| = p^k$. Mas isso é impossível pois $|S - \{\overline{Q}\}| = 2p-1$. Logo $\overline{Q}$ tem ramificação mansa sobre E e $G_0(\overline{Q}|E)$ é cíclico.

Se $G_0(\overline{Q}|E) = \{1\}$, note que p divide a $|\overline{G}| \leq |S|$ (Teorema 59), logo $|G| = p$ ou $2p$. Olhando para a lista no Teorema 107, $\overline{G}$ cai no caso (7). Assim, $\overline{G}$ é um grupo cíclico de ordem p ou um grupo dihedral de ordem $2p$, logo G é um grupo cíclico de ordem $2p$ ou um grupo dihedral de ordem $4p$. Em qualquer caso, G possui um único subgrupo de ordem p, que tem que ser $\mathrm{Aut}(F/K(x))$.

Assim, vamos considerar os casos onde $G_0(\overline{Q}|E) \neq \{1\}$ para todo $\overline{Q} \in S$ (pelo Teorema 65 (3) esses grupos são cíclicos). Pela Observação 66, E possui um lugar $\overline{\overline{Q}}$ com ramificação selvagem em $K(y)$. As órbitas de S por $\overline{G}$ se restringem a lugares de E com ramificação mansa, segue da Seção 4.4 que E somente tem mais um lugar ramificado distinto de $\overline{\overline{Q}}$, logo todos os lugares de S são conjugados por $\overline{G}$. Pelo Teorema 59, $|\overline{G}| = 2p|G_0(\overline{Q}|E)|$. Observando a lista do Teorema 1, isto é possível apenas nos casos (8) e (9), se $p = 3$, $|S| = 6$ e se $\overline{G}$ é isomorfo a $\mathrm{PSL}(2,3) \simeq A_4$ ou $\mathrm{PGL}(2,3) \simeq S_4$ (Teorema 9), respectivamente. Além disso, dado $\overline{G} \in S$, $|G_0(\overline{Q})| = e(\overline{Q}|E)| = 2$ ou 4, respectivamente (Teorema 61 (2)).

Vamos denotar por $\overline{Q}_a$ ao lugar de $K(y)$ associado ao polinômio $y-a$. Seja σ o automorfismo de F tal que $x \mapsto x$, $y \mapsto y-1$ e seja $\overline{\sigma} = \sigma|_{K(x)} \in \overline{G}$. Pela Observação 91 podemos assumir que $\overline{Q}_0$ se ramifica em F, logo $\overline{Q}_1$ e $\overline{Q}_2$ também se ramificam em F (Observação 58 (1)). Se $\overline{Q_b}$ é um quarto lugar em S então os lugares ramificados restantes são $\overline{Q}_{b+1}$ e $\overline{Q}_{b+2}$. A ação de $\overline{\sigma}$ em S é $(\overline{Q}_0\overline{Q}_1\overline{Q}_2)(\overline{Q}_b\overline{Q}_{b+1}\overline{Q}_{b+2})$.

Lema 122. *b pode ser escolhido como sendo $2i$, onde $i^2 = 2$. Em particular,*

$$S = \{\overline{Q}_0, \overline{Q}_1, \overline{Q}_2, \overline{Q}_{2i}, \overline{Q}_{2i+1}, \overline{Q}_{2i+2}\}.$$

Demonstração. Seja $\overline{\tau}$ o elemento de ordem 2 de $G_0(\overline{Q}_0|E)$. Como $\overline{\tau}$ age em S em ciclos disjuntos de comprimento 2, ele deve fixar um lugar $\overline{Q}_s$ em S distinto de $\overline{Q}_0$. Temos que $\overline{\sigma}\overline{\tau}(\overline{Q}_s) = \overline{Q}_{s+1}$, por outro lado $\overline{\tau}\overline{\sigma}(\overline{Q}_s) = \overline{\tau}(\overline{Q}_{s+1})$, como $\overline{\tau}$ não fixa $\overline{Q}_{s+1}$ então $\overline{\sigma}\overline{\tau} \neq \overline{\tau}\overline{\sigma}$. Em particular τ, $\overline{\sigma}\overline{\tau}\overline{\sigma}^{-1}$ e $\overline{\sigma}^2\overline{\tau}\overline{\sigma}^{-2}$ são elementos distintos dois a dois de $\overline{G}$ de ordem 2, então os dois últimos não pertencem a $G_0(\overline{Q}_0)$. Avaliando esse automorfismos em $\overline{Q}_0$, observamos que $\overline{\tau}$ não fixa $\overline{Q}_1$ nem $\overline{Q}_2$, assim podemos tomar $s = b$.

Agora vamos denotar $\overline{Q}_a$ simplesmente por a. Pelo feito no anteriormente e equação 3.2,

$$\overline{\tau}(y) = \frac{(b+q)y}{y+q}, \quad y \in K$$

Temos que $\overline{\tau}(1) = 2, b+1$ ou $b+2$. No primeiro caso, substituindo na expressão acima, temos que $b+q = -1-q$. Por outro lado, como $\overline{\tau}(2) = 1$, $-b-q = -1+q$, o que leva uma contradição. Similarmente, se $\overline{\tau}(1) = b+2$, temos que $2q = qb-1$, e como $\overline{\tau}(-1) = b+1$ então $qb = 1$,

outra contradição. Por tanto $\overline{\tau}(1) = b+1$, $\overline{b+1} = 1$ e $\overline{\tau}(2) = b+2$. Assim obtemos as equações $2q = qb-1$, $b^2+qb = 1$ e $bq = -1$, o que implica que $b^2 = q = 2$, por tanto podemos tomar $b = -i = 2i$. □

Considere o automorfismo $\overline{\lambda}(y) = \dfrac{(2i+1)y}{2y+1+i}$, ele leva S nele mesmo, logo $\overline{\lambda} \in \overline{G}$. Como $\overline{\lambda}$ tem ordem 4, $\overline{G}$ deve ser isomorfo a S_4 (Observação 100). Vamos determinar quando é que isso acontece.

Pela Observação 91, podemos assumir que $a_1 = 0$ e $a_2 = 1$, e que as extensões de $\overline{Q}_0$, $\overline{Q}_1$ e $\overline{Q}_2$ em F estão acima do lugar no infinito de $K(x)$, pois elas são conjugadas por σ . Assim, a equação de F fica $y^3 - y = \dfrac{a}{x(x-1)}$ com $a \in K$ 5.1, que pode ser escrita como $(x-2)^2 = 1 + \dfrac{a}{y^3-y} = \dfrac{y^3-y+a}{y^3-y}$. Como $F/K(y)$ é uma extensão de Kummer, o Teorema 3.6 (2) mostra que $\overline{Q}_{2i}$ se ramifica em F se e somente se $v_{\overline{Q}_{2i}} = (2i)^3 - (2i) + a = 0$, equivalentemente, se $a = i$. Assim, F tem equação $y^3 - y = \dfrac{i}{x(x-1)}$.

Por tanto, $K(x)$ é o único subcorpo racional tal que $F/K(x)$ é normal de grau p, a menos que $p = 3$ e a equação geradora de F possa ser escrita na forma $y^3 - y = \dfrac{i}{x(x-1)}$, com $i^2 = 2$.

5.1.6 $r = 1$, $\lambda_1 \leq p+1$

Podemos assumir que $a_1 = 0$ (Observação 91). Pelo Teorema 103, $G_0(P) = G_1(P_1|E) = \mathrm{Aut}(F/K(x))$, de fato $G = \mathrm{Aut}(F/K(x)) \simeq \mathscr{C}_p$, exceto no caso excepcional $y^p - y = \dfrac{1}{x^{\lambda_1}}$, com $\lambda_1 | p+1$. O grupo de automorfismos nos casos excepcionais vêm dados pelo Teorema 103.

Nos casos não excepcionais, suponha que $K(z)$ é um subcorpo de F que satisfaz 5.9. Se $F/K(z)$, pela Proposição 17 existe um corpos L tal que F/L é puramente inseparável e $L/K(z)$ é separável. Temos que $[F:L] = p$ ou $[L:K(z)] = p$, assim necessariamente $F = L$ e $L = K(z)$, logo $F/K(z)$ é puramente inseparável. Mas o Teorema 54 (3) implica que F é racional, o que não é possível. Segue que $F/K(z)$ é galoisiana, em particular $F^{\mathrm{Aut}(F/K(z))} = K(z)$ (Teorema Galois); como $\mathrm{Aut}(F/K(z)) \subset \mathrm{Aut}(F/K)$ então $F \supset K(z) \supset K(x) = F^{\mathrm{Aut}(F/K)}$, logo $K(z) = K(x)$. Por tanto, $K(x)$ é o único subcorpo racional de F que satisfaz 5.9.

Em conclusão, obtemos o seguinte teorema.

Teorema 123. Seja K um corpo algebricamente fechado de característica $p > 0$. Seja $F/K(x)$ uma extensão de Artin-Schreier com gênero maior que 1, com $F = K(x,y)$. Temos $\mathrm{Aut}(F/K)$ é uma extensão de C_p por um subgrupo finito de $\mathrm{PGL}(2,K)$, exceto nos seguintes casos:

1. $y^p - y = \dfrac{a}{x^p - x}$ com $a \in K$, logo G é o produto semidireto de um $p-$grupo abeliano elementar de ordem p^2 e D_n;
2. $y^3 - y = \dfrac{i}{x(x-1)}$ com $i^2 = -1$, logo G é a extensão de $\mathbb{Z}_2$ via S_4;

3. $y^p - y = \dfrac{1}{x^\lambda}$ com $\lambda | p+1$ e $\lambda < p+1$, logo G é a extensão de um grupo cíclico de ordem 2 via $\mathrm{PGL}(2,p)$;

4. $y^p - y = \dfrac{1}{x^{p+1}}$, logo $G \simeq \mathrm{PGU}(3,p^2)$.

Demonstração. Pela Observação 100, $G := \mathrm{Aut}(F/K)$ é uma extensão de C_p por um subgrupo finito de $\mathrm{PGL}(2,K)$, exceto nos casos não excepcionais.
O caso (2) aparece em 5.1.5 e os casos (3) e (4) aparecem no Teorema 103.

Para achar (1), considere os seguintes automorfismos de F:

$$\sigma : (x,y) \mapsto (x,y-1) \quad \tau : (x,y) \mapsto (x-1,y) \quad \lambda : (x,y) \mapsto (y,x) \quad \alpha : (x,y) \mapsto (\varepsilon x, \varepsilon^{-1} y)$$

onde ε é uma raiz $(p-1)-$ésima primitiva da unidade. Note que σ e τ geram $\mathrm{Aut}(F/K(x))$ e $\mathrm{Aut}(F/K(y))$ respectivamente, e $\langle \sigma, \tau \rangle$ é um $p-$grupo abeliano elementar de ordem p^2. Como $\lambda\alpha\lambda = \alpha^{-1}$, $\langle \alpha, \lambda \rangle$ é um grupo dihedral de ordem $2(p-1)$. Além disso, $\lambda\sigma\lambda = \tau$ e $\lambda\tau\lambda = \sigma$, e que α está no normalizador de $\mathrm{Aut}(F/K(x))$ e $\mathrm{Aut}(F/K(y))$. Assim, $\langle \sigma, \tau, \alpha, \lambda \rangle$ é o produto semidireto de um $p-$grupo abeliano elementar de ordem p^2 com um grupo dihedral de ordem $2(p-1)$.

Para mostrar que $G = \langle \sigma, \tau, \alpha, \lambda \rangle$, é suficiente mostrar que $|G| \leq 2p^2(p-1)$. Sejam $P_1, P_2, \ldots, P_p$ os lugares de F que se ramificam sobre $K(x)$. Por 5.1.3, os lugares de F tais que p é uma não-lacuna são os P_i e os lugares não ramificados sobre $K(x)$ e ramificados sobre $K(y)$. Logo, P_1 tem no máximo $2p$ conjugados. Pela Observação 119, $\mathscr{L}(p \cdot P_1) = \left\langle 1, \dfrac{1}{x-1} \right\rangle$. Assim, $G_0(P_1)/\mathrm{Aut}(F/K(x)) \hookrightarrow \mathrm{Aut}(K(x)/K)$ (correspondência de Galois) que fixa $\overline{P}_1$ e permuta $\{\overline{P}_2, \overline{P}_3, \ldots, \overline{P}_p\}$. Logo $G_0(P_1)/\mathrm{Aut}(F/K(x)) \hookrightarrow \mathrm{Aut}(K(x)/K)$ deve ser cíclico de ordem no máximo $p-1$. Assim, $|G| \leq 2p^2(p-1)$, como queríamos mostrar. □

5.2 Casos não excepcionais

Suponha que F/K está definida pela equação

$$y^p - y = f(x),\ f(x) \in K(x) \setminus K$$

tal que cai nos casos não excepcionais do teorema anterior. Seja $H = \pi(\mathrm{Aut}(F/K))$ como na Observação 100.

Lema 124. *H coincide com os automorfismos que fixam $f(x)$.*

Demonstração. ($\Longrightarrow$) Seja $\alpha \in \mathrm{Aut}(F/K)$, temos que $\alpha(y)^p - \alpha(y) = \alpha(f(x)) = f(\alpha(x))$. Temos que $\alpha(y) = y + r$, com $r \in \mathbb{F}_p$, logo $f(\alpha(x)) = \alpha(y)^p - \alpha(y) = y^p - y = f(x)$. Logo $\pi(\alpha)$ fixa $f(x)$.
($\Longleftarrow$) Se $\overline{\alpha}(x)$ é um automorfismo de $K(x)/K$ que fixa $f(x)$, então $\alpha : (x,y) \mapsto (\overline{(\alpha)(x)}, y)$ é tal que $\pi(\alpha) = \overline{\alpha}$. □

Por simplicidade, assumiremos que $f(x) \in K[x]$. Assim $\overline{P}_\infty \in \mathbb{P}_{K(x)}$ é um polo de $f(x)$, como $f(\alpha(x))$ tem polo em $\alpha^{-1}(\overline{P}_\infty)$, então $\alpha(\overline{P}_\infty) = \overline{P}_\infty$, segue que $\alpha(x) = ax+b$ (aqui temos olhado α como um automorfismo da reta projetiva). Assumiremos ainda que $f(x) = \sum_{i=0}^{N} c_i x^i$ é mônico. É claro que $a = \zeta_d^k$, com $d|N$, $p \nmid d$ e $\text{mcd}(d,k) = 1$.

Observação 125. Se $a \neq 1$, $d \neq 1$ e $p \nmid d$, então

$$f(x) = f(\alpha(x)) \iff f\left(\frac{x-b}{a-1}\right) = f\left(\frac{ax-b}{a-1}\right) \iff f\left(\frac{x-b}{a-1}\right) \in K[x^d]$$

Se $a = 1$ então $p|N$ ou $\alpha = 1$.

Se $p \nmid N$, pelo Lema 124 aplicado aos coeficiente de x^{N-1} temos que

$$c_{N-1} = \frac{Nb}{a-1},$$

o que determina $\dfrac{b}{a-1}$. Agora podemos determinar os possíveis $d|N$ tais que $f\left(\dfrac{x-b}{a-1}\right) \in K[x^d]$, o que permite a e b. É fácil ver que H é um grupo cíclico de ordem não divisível por p.

Seja $N = p^k L$, com $k, L \geq 1$ e $p \nmid L$. Primeiro considere $a = \zeta_d^k \neq 1$ com $p \nmid d|N$, logo $d|L$. Note que $(x-b)^N = (x^{p^k} - b^{p^k})^L$. Suponha $f(x) \neq x^N$, seja r o maior inteiro positivo $< \dfrac{N}{d}$ tal que $c_{rd} \neq 0$. Temos os seguintes casos:

- Se $rd > N - p^k + 1$ então $c_i = 0$ para $rd < i < N$. Pelo Lema 124,

$$\frac{b}{a-1} = \frac{c_{rd-1}}{c_{rd}(rd)}$$

- Se $rd = N - p^k + 1$, uma das restrições para $\dfrac{b}{a-1}$ é

$$L\left(\frac{b}{a-1}\right)^{p^k} + c_{N-p^k+1}(N-p^k+1)\frac{b}{a-1} - c_{N-p^k} = 0.$$

- Se $rd < N - p^k$ então

$$\left(\frac{b}{a-1}\right)^{p^k} = \frac{c_{N-p^k}}{L}.$$

Note que muitas das equações anteriores são igualdades no corpo K.
Quando $a = 1$, o seguinte resultado pode ser muito útil, especialmente quando $K = \overline{\mathbb{F}_p}$.

Proposição 126. Para $r > 0$ e $f \in \mathbb{F}_{p^r}[x]$ temos

$$f(x) = f(x+\alpha),\ \forall \alpha \in \mathbb{F}_{p^r} \iff f \in \mathbb{F}_{p^r}[x^{p^r} - x]$$

Exemplo 127.

$$F: \quad y^5 - y = (x^5 - x)^4, \quad K = \overline{\mathbb{F}_p}$$

Temos $(x^5-x)^4 = x^{20}+x^{16}+x^{12}+x^8+x^4$, logo temos que os automorfismos $\alpha(x) = x+a$, com $a \in \mathbb{F}_5$, estão em H (pela Proposição acima). Por outro lado, $N = 20$ e $L = 4$. Se $\alpha \in H$, com $\alpha(x) = ax+b$ e $a \neq 1$, temos $a = \zeta_d^k \neq 1$, com $p \nmid d | N$ e $\text{mcd}(d,k) = 1$. Segue que $d = 2$ ou 4, com raízes primitivas 4 e 2 respectivamente, e $rd = 16 = N - p^k + 1$ nos dois casos. Temos $4\left(\frac{b}{a-1}\right)^5 - 16\left(\frac{b}{a-1}\right) = 0$, logo $\left(\frac{b}{a-1}\right) \in \mathbb{F}_5$. Assim, os possíveis automorfismos neste caso são

$$\alpha_k(x) = 4x+k \qquad \beta_k(x) = 2x+k \qquad \gamma_k(x) = 3x+k \qquad k \in \mathbb{F}_5$$

Verificamos que eles são de fato elementos de H. Além disso, pela Proposição 126, também temos os automorfismos $\theta(x) = x+k$, $k \in \mathbb{F}_5$ estão em H. Temos que H é o produto semidireto de C_5 com C_4 (caso 7 no Teorema 113).

O caso geral $f \in K(x)$ é mais complexo. Ele pode ser estudado analisando os zeros e os polos de f.

Exemplo 128.

$$F: y^p + y = \frac{x^{2n}+1}{x^n}, \quad p \nmid n$$

Note que $\frac{x^{2n}+1}{x^n} = x^n + \frac{1}{x^n}$. Seja ζ uma raiz $n-$ésima primitiva da unidade, é claro que $\alpha_i(x) = \zeta^i x$ e $\beta_i(x) = \frac{\zeta^i}{x}$ estão em H, para $i = 1, \ldots, n$. Por outro lado temos que $f(\infty) = f(0) = \infty$ (olhando f como um morfismo $\mathbb{P}^1 \to \mathbb{P}^1$), logo os automorfismos em H satisfazem $\alpha(\infty) = \infty$ ou $\alpha(0) = \infty$. Assim, podemos verificar que os α_i e os β_i são todos elementos de H, e $H \simeq D_n$.

REFERÊNCIAS

BOSECK, H. Zur Theorie der Weierstraßpunkte. **Mathematische Nachrichten**, n. 19, 1958. Citado na página 75.

ENGLER, A.; PRESTEL, A. **Valued Fields**. [S.l.]: Springer, 2005. Citado na página 38.

FULTON, W. **Curve book**. [S.l.: s.n.], 2008. Citado nas páginas 46 e 51.

GARCIA, A. On Weierstrass Points on Artin-Sehreier Extensions of $K(x)$. **Mathematische Nachrichten**, n. 144, 1989. Citado na página 75.

GÖB, N. **Automorphism Groups of Hyperelliptic Function Fields**. Tese (Doutorado) — Fachbereich Mathematik der Technischen Universität Kaiserslautern, Kaiserslauter, 2004. Citado nas páginas 18 e 37.

GÜNERI, C.; ÖZBUDAK, F. Artin-schreier extensions and their applications. **Algebra and Applications**, n. 6, 2007. Citado na página 18.

HARTSHORNE, R. **Algebraic Geometry**. [S.l.]: Springer, 1977. Citado nas páginas 18, 21, 45 e 46.

HIRSCHFELD, J.; KORCHMÁROS, G.; TORRES, F. **Algebraic Curves over a Finite Field**. [S.l.]: Elsevier, 2008. Citado nas páginas 51, 54 e 55.

HUNGERFORD, T. W. **Algebra**. 1. ed. [S.l.]: Springer, 1974. Citado na página 23.

HUPPERT, B. **Endliche Gruppen**. [S.l.]: Springer, 1967. v. 1. Citado na página 23.

LANG, S. **Algebra**. [S.l.]: Springer, 2002. Citado na página 22.

SCHMID, H. Über die Automorphismen eines algebraischen Funktionenkörpers von Primzahlcharakteristik. **Journal für die Reine und Angewandte Mathematik**, n. 179, 1938. Citado na página 37.

SILVERMAN, J. H. **The Arithmetic of Elliptic Curves**. 2. ed. [S.l.]: Springer, 2009. Citado nas páginas 21, 46 e 51.

STICHTENOTH, H. Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. **Archiv der Mathematik**, n. 24, 1973. Citado na página 54.

____. **Algebraic Function Fields and Codes**. 2. ed. [S.l.]: Princeton University Press, 2009. Citado nas páginas 29, 38, 47, 49, 51 e 53.

VALENTINI, R.; MADAN, M. A hauptsatz of l.e dickson and artin-scheier extensions. **Journal für die reine und angewandte Mathematik**, n. 318, 1980. Citado nas páginas 18 e 57.

ZASSENHAUS, H. Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen. **Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg**, n. 11, 1936. Citado na página 24.


ICMC
USP
SÃO CARLOS