UNIVERSIDADE DE SÃO PAULO

Instituto de Ciências Matemáticas e de Computação

Corpos de funções algébricas sobre corpos finitos

Alex Freitas de Campos

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

SERVIÇO DE PÓS-GRADUAÇÃO DO ICMC-USP

Data de Depósito:

Assinatura: _____

Alex Freitas de Campos

Corpos de funções algébricas sobre corpos finitos

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. *VERSÃO REVISADA*

Área de Concentração: Matemática

Orientador: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
Fevereiro de 2018

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

d278c de Campos, Alex Freitas
Corpos de funções algébricas sobre corpos finitos
/ Alex Freitas de Campos; orientador Herivelto
Martins Borges Filho. -- São Carlos, 2018.
148 p.

Dissertação (Mestrado - Programa de Pós-Graduação
em Matemática) -- Instituto de Ciências Matemáticas
e de Computação, Universidade de São Paulo, 2018.

1. Álgebra. 2. Corpos globais. 3. Curvas
algébricas. I. Borges Filho, Herivelto Martins,
orient. II. Título.

Alex Freitas de Campos

Algebraic function fields over finite fields

Master dissertation submitted to the Institute of Mathematics and Computer Sciences – ICMC-USP, in partial fulfillment of the requirements for the degree of the Master Program in Mathematics. *FINAL VERSION*

Concentration Area: Mathematics

Advisor: Prof. Dr. Herivelto Martins Borges Filho

USP – São Carlos
February 2018

AGRADECIMENTOS

Em proêmio, urge fazer apoteose a meus pais pela vida, em sentido lato e estrito, que me deram. O que sou é indissociável deles. Não menos dignos de mérito são meus familiares mais próximos.

Do mesmo modo, insta expressar profunda estima e admiração, respeito e consideração àquele que considero ser o indivíduo fulcral para minha formação profissional e pessoal, a saber, meu egrégio orientador, o Professor Doutor Herivelto Martins Borges Filho.

Ademais, faz-se mister agradecer todos os que, direta e indiretamente, contribuíram de alguma forma e estiveram envolvidos na produção do presente trabalho: professores, funcionários e amigos.

Por fim, agradeço a Deus, cujo entendimento me é vago, mas cuja existência tenho certa e dá meios, fins e, acima de tudo, sentido a minha própria.

RESUMO

DE CAMPOS, A. F. **Corpos de funções algébricas sobre corpos finitos**. 2018. 148 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2018.

Este trabalho é essencialmente sobre pontos racionais em curvas algébricas sobre corpos finitos ou, equivalentemente, lugares racionais em corpos de funções algébricas em uma variável sobre corpos finitos. O objetivo é a demonstração da existência de constantes a_q e $b_q \in \mathbb{R}_{>0}$ tais que se $g \geq a_q \cdot N + b_q$, então existe uma curva sobre $\mathbb{F}_q$ de gênero g com N pontos racionais.

Palavras-chave: Extensões de Artin-Schreier, Corpos finitos, Pontos racionais.

ABSTRACT

DE CAMPOS, A. F. **Algebraic function fields over finite fields**. 2018. 148 p. Dissertação (Mestrado em Ciências – Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos – SP, 2018.

This work is essentially about rational points on algebraic curves over finite fields or, equivalently, rational places on algebraic function fields of one variable over finite fields. The aim is the proof of the existence of constants a_q and $b_q \in \mathbb{R}_{>0}$ such that if $g \geq a_q \cdot N + b_q$ then there exists a curve over $\mathbb{F}_q$ of genus g with N rational points.

Keywords: Artin-Schreier extensions, Finite fields, Rational points.

SUMÁRIO

1	UMA EXPOSIÇÃO INTRODUTÓRIA	13
2	“PROLEGÔMENOS”	19
2.1	Lugares	19
2.2	O corpo de funções racional	24
2.3	Independência das valorizações	26
2.4	Divisores	27
2.5	O teorema de Riemann-Roch e suas principais consequências	32
3	EXTENSÕES ALGÉBRICAS DE CORPOS DE FUNÇÕES	35
3.1	A igualdade fundamental	35
3.2	Subaneis de corpos de funções	46
3.3	Base Integral local	50
3.4	O cotraço das diferenciais de Weil e a fórmula do gênero de Hurwitz	61
3.5	O diferente	65
3.6	Extensões de corpo de constantes	71
3.7	Extensões Galoisianas	75
4	O TEOREMA DE HASSE-WEIL	91
4.1	A função zeta de um corpo de funções	91
4.2	O teorema de Hasse-Weil	100
4.3	Melhoramentos da cota de Hasse-Weil	107
4.4	A constante de Ihara	112
5	CORPOS DE FUNÇÕES COM UM NÚMERO PRESCRITO DE LUGARES RACIONAIS	117
5.1	Lemas preliminares	117
5.2	Corpos de funções com um número prescrito de lugares racionais	122
5.3	O caso q quadrado	127
5.4	O caso $q = 2$	135
5.5	Curvas com um número prescrito de pontos de grau maior	137
5.6	Desigualdades para os coeficientes de $L(t)$	142
5.7	Curvas com os coeficientes de $L(t)$ prescritos	144

REFERÊNCIAS 147

UMA EXPOSIÇÃO INTRODUTÓRIA

O presente trabalho é baseado em [Stichtenoth e Anbar \(2013\)](#).

De grande interesse aplicacional, especialmente para a teoria de códigos corretores de erros, são as curvas algébricas sobre corpos finitos com muitos pontos racionais. Tal interesse vem da construção, feita primeiramente por [Goppa \(1981\)](#), de códigos bons valendo-se de tais curvas. Tal construção, bem como uma introdução à teoria de códigos, não será apresentada neste texto pois foge ao escopo do mesmo. Não obstante, recomendamos aos leitores interessado que confirmem [Stichtenoth \(2009\)](#).

A fim de esclarecer brevemente os principais resultados do artigo no qual este trabalho baseia-se, façamos algumas considerações.

Ao longo do texto, C sempre denotará uma curva projetiva não singular e absolutamente irredutível definida sobre o corpo finito $\mathbb{F}_q$ ($q = p^n$) e $g(C)$ e $N(C)$ denotarão, respectivamente, o gênero e o número de pontos $\mathbb{F}_q$ -racionais de C . Como usaremos predominantemente a “linguagem” de corpos de funções, $F/\mathbb{F}_q$ denotará, analogamente, um corpo de funções algébricas em uma variável sobre $\mathbb{F}_q$ e $g(F)$ e $N(F)$ denotarão o gênero e o número de lugares racionais de $F/\mathbb{F}_q$, respectivamente. Sejam

$$\mathcal{M}_q(g) \doteq \{N \in \mathbb{Z}_{\geq 0} \mid \text{existe } C \text{ de gênero } g \text{ com} \\ \text{exatamente } N \text{ pontos racionais}\}$$

e

$$N_q(g) \doteq \max \mathcal{M}_q(g)$$

Pela [COTA DE HASSE-WEIL](#) (hipótese de **Riemann** para corpos finitos) temos que $|N_q(g) - (q+1)| \leq 2g\sqrt{q}$. Mais do que $N_q(g)$, estuda-se o seu comportamento assintótico dado em termos da chamada constante de **Ihara** $A(q)$:

$$A(q) \doteq \limsup_{g \rightarrow \infty} \frac{N_q(g)}{g}$$

Tal constante é mais simples de ser estudada do que os números $N_q(g)$ em si e, além disso, ela “contem” informações qualitativas a respeito de $N_q(g)$ (para g suficientemente grande). Notemos que, novamente pela [COTA DE HASSE-WEIL](#), temos que $A(q) \leq 2\sqrt{q}$. Um melhoramento significativo da cota anterior é dado pela [COTA DE DRINFEL'D-VLĂDUȚ](#):

$$A(q) \leq \sqrt{q} - 1$$

No caso de q ser um quadrado, [Ihara \(1981\)](#) e [Tsfasman, Vlăduț e Zink \(1982\)](#) mostraram que a desigualdade anterior é na verdade uma igualdade e, mais tarde, [Garcia e Stichtenoth \(1995\)](#) construíram explicitamente uma sequência de curvas sobre $\mathbb{F}_q$ (com q quadrado) que atinge a cota anterior. No caso de q não ser quadrado, o valor exato de $A(q)$ ainda é desconhecido. Não obstante, [Serre \(1982-1983\)](#) mostrou a existência de $c \in \mathbb{R}_{>0}$ independente de q tal que

$$A(q) \geq c \cdot \log q$$

Serre também propôs o estudo do seguinte limite inferior

$$A^-(q) \doteq \liminf_{g \rightarrow \infty} \frac{N_q(g)}{g}$$

e levantou a questão sobre a positividade de $A^-(q)$. Tal questionamento foi respondido afirmativamente 20 anos depois por [Elkies et al. \(2004\)](#). Mais precisamente, foi demonstrado o seguinte

Teorema 1. Existe uma constante $d > 0$ tal que para todo q e qualquer inteiro positivo g vale

$$N_q(g) \geq d \log q \cdot g$$

Em outras palavras, para cada $g \geq 0$ existe uma curva C sobre $\mathbb{F}_q$ com $g(C) = g$ e $N(C) \geq \gamma_q \cdot g$, onde $\gamma_q = d \log q > 0$. ■

Antes desse resultado, nada se sabia a respeito de $A^-(q)$ e mesmo a seguinte afirmação mais fraca

$$N_q(g) \xrightarrow{g \rightarrow \infty} \infty$$

foi demonstrada (KRESCH; WETHERELL; ZIEVE, 2002) pouco antes do resultado anterior.

O [teorema anterior](#) mostra que podemos prescrever o gênero g e “encontrar” uma curva com pelo menos $\gamma_q \cdot g$ pontos racionais. Será que podemos prescrever números N e g (que queremos que sejam o número de pontos racionais e o gênero respectivamente) e ainda assim encontrar uma curva C de gênero $g(C) = g$ e com $N(C) = N$ pontos racionais? Definindo

$$\mathcal{M}_q \doteq \{(N, g) \mid \text{existe } C \text{ de gênero } g(C) = g \text{ com exatamente } N(C) = N \text{ pontos racionais}\}$$

o resultado principal de [Stichtenoth e Anbar \(2013\)](#), cujo enunciado é dado a seguir, nos dá condições suficientes para que a resposta à pergunta anterior seja afirmativa.

Teorema 2. Para todo q , existem constantes $a_q, b_q > 0$ tais que

$$\{(N, g) \mid g \geq a_q \cdot N + b_q\} \subset \mathcal{M}_q$$

■

“Isolando” N na desigualdade anterior, o teorema anterior nos diz simplesmente que o “intervalo discreto” $[0, a_q^{-1}g - a_q^{-1}b_q] \cap \mathbb{Z}$ está contido em $\mathcal{M}_q(g)$ (com a seguinte convenção: se $r < 0$ então $[0, r] = \{0\}$), i.e., existe uma curva C sobre $\mathbb{F}_q$ tal que seus gênero e número de pontos racionais são dados, respectivamente, por g e N . As ilustrações abaixo nos ajudam a entender um pouco melhor o que acontece.

A reta acima da qual os pontos estão azuis é a reta $a_q N + b_q$, e o [teorema](#) nos garante que todos os pontos azuis pertencem ao conjunto $\mathcal{M}_q$.

Aqui, simplesmente invertamos os papéis de N e g no diagrama anterior. Agora, a reta abaixo da qual os pontos estão vermelhos é a reta $a_q^{-1}g - a_q^{-1}b_q$ e o teorema mais uma vez nos garante que todos os pontos vermelhos pertencem ao conjunto $\mathcal{M}_q$. Os diagramas anteriores são meramente ilustrativos: não estão de acordo com os valores típicos (aproximados) de a_q e b_q .

O [teorema anterior](#) também generaliza o seguinte resultado ([STICHTENOTH, 2011](#))

Teorema. Dados um corpo finito $\mathbb{F}_q$ e um inteiro $N \geq 0$, existe um inteiro g_0 tal que para todo $g \geq g_0$ existe uma curva sobre $\mathbb{F}_q$ de gênero g e com N pontos racionais. ■

O [Teorema 2](#) é generalizado da seguinte maneira

Teorema. Seja $\mathbb{F}_q$ um corpo finito e sejam $b_1, \dots, b_m$ inteiros não negativos. Então existe um inteiro $g_0 \geq 0$ com a seguinte propriedade

para todo $g \geq g_0$ existe uma curva C sobre $\mathbb{F}_q$ de gênero $g(C) = g$ e tal que C possui exatamente b_r pontos de grau r para $r = 1, \dots, m$.

■

Os resultados anteriores podem e serão formulados em termos da teoria dos corpos de funções algébricas. No lugar de curvas sobre corpos finitos usaremos corpo de funções algébricas cujo corpo de constantes é um corpo finito. Daí, no lugar de pontos racionais

da curva teremos lugares racionais do corpo de funções e no lugar do gênero da curva teremos o gênero do corpo de funções. E é nessa linguagem, puramente algébrica, que este texto foi escrito.

A demonstração detalhada do [Teorema 2](#) é dada no capítulo [5](#). O leitor com conhecimento suficiente da teoria de corpos de funções pode começar a leitura a partir de tal capítulo. Para os demais leitores, os capítulos [2](#), [3](#) e [4](#) contem os conceitos e resultados básicos que serão utilizados no capítulo [5](#).

Uma sugestão. É preferível que o texto seja lido na versão digital porquanto as referências estão *linkadas* e faço uso de sinais em cores em alguns trechos. Caso o leitor não abra mão da leitura em versão impressa, sugiro que a impressão seja em cores, caso contrário o entendimento dos trechos com sinais em cores citados anteriormente será comprometido.

Por fim, dúvidas, críticas, comentários e sugestões são sempre muito bem-vindas. Essa versão não é de todo definitiva: está sujeita a modificações e acrescentamentos. Para obter a última versão do texto ou enviar uma nota para o autor, entre em contato através do endereço alex.freitas.campos@usp.br.

“PROLEGÔMENOS”

Este capítulo é um “apanhado geral” dos objetos com os quais a teoria de corpos de funções algébricas lida. A maioria dos resultados é apresentada sem demonstração. Tenha o leitor em mente que uma exibição mais completa do que a feita aqui pode ser encontrada em [Stichtenoth \(2009\)](#).

2.1 Lugares

Seja K um corpo qualquer e seja x transcendente sobre K . Considere a seguinte torre de corpos

$$\begin{array}{c} F \\ | \\ K(x) \\ | \\ K \end{array} \begin{array}{l} \\ < \infty \\ \text{tr deg} = 1 \end{array}$$

Nesse caso dizemos que F/K , ou simplesmente F quando K estiver subentendido, é um corpo de funções algébricas em uma variável sobre K . O fecho algébrico de K em F (que é um subcorpo de F) será denotado por $\tilde{K}$ e será chamado de **corpo de constantes** de F . É claro que $F/\tilde{K}$ é também um corpo de funções algébricas. No caso de K ser algebricamente fechado em F diremos que K é **todo o corpo de constantes** de F . Por simplicidade, na maioria dos casos chamaremos F/K simplesmente de corpo de funções.

Observação 3. Observemos também que $z \in F$ é transcendente sobre K se, e somente se, $[F : K(z)] < \infty$. ■

Definição 4. Um anel de valorização do corpo de funções F/K é um anel $O \subset F$ com as seguintes propriedades:

1. $K \subsetneq O \subsetneq F$, e
2. para todo $z \in F$, ou $z \in O$ ou $z^{-1} \in O$. ■

Proposição 5. Seja O um anel de valorização do corpo de funções F/K . Então

1. O é um anel local, cujo único ideal maximal será denotado por $P \doteq O \setminus O^\times$, e onde $O^\times = \{z \in O \mid \exists w \in O \text{ tal que } zw = 1\}$ é o grupo das unidades de O .
2. Seja $0 \neq x \in F$. Então $x \in P \Leftrightarrow x^{-1} \notin O$.
3. Sendo $\tilde{K}$ o corpo de constantes de F/K , temos que $\tilde{K} \subset O$ e $\tilde{K} \cap P = \{0\}$. ■

Teorema 6. Seja O um anel de valorização do corpo de funções F/K e P seu único ideal maximal. Então

1. P é um ideal principal.
2. Se $P = tO$ então todo $0 \neq z \in F$ admite uma única representação na forma $z = t^n u$ para algum $n \in \mathbb{Z}$ e $u \in O^\times$.
3. O é um domínio de ideais principais: se $P = tO$ e $\{0\} \neq I \subset O$ é um ideal então $I = t^n O$ para algum $n \in \mathbb{Z}_{\geq 1}$. ■

Um anel com as propriedades acima é denominado **anel de valorização discreta**.

Definição 7. Um **lugar** do corpo de funções F/K é o ideal maximal de algum anel de valorização de F/K . Um gerador de P será chamado de elemento primo de P (outras denominações usadas são parâmetro local ou de uniformização). O conjunto de todos os lugares de F/K será denotado por $\mathbb{P}_F$. ■

Observemos que pelo item 2 da [Teorema 5](#), o anel de valorização O fica unicamente determinado pelo seu ideal maximal P : $O = \{z \in F \mid z^{-1} \notin P\} \cup \{0\}$. Portanto, de agora em diante denotaremos o anel de valorização associado ao lugar P por O_P .

Definição 8. Uma valorização discreta de F/K é uma função $v : F \rightarrow \mathbb{Z} \cup \{\infty\}$ que satisfaz

1. $v(x) = \infty \Leftrightarrow x = 0$
2. $v(xy) = v(x) + v(y)$, $\forall x, y \in F$
3. $v(x + y) \geq \min\{v(x), v(y)\}$, $\forall x, y \in F$

$$4. \exists z \in F \text{ tal que } v(z) = 1$$

$$5. v(a) = 0 \forall 0 \neq a \in K$$

■

Observemos que pelos itens 2 e 4, v é sobrejetora. O símbolo ∞ denota uma entidade que não um número inteiro sujeita a $\infty + \infty = \infty + n = n + \infty = \infty$ e $\infty > m$ quaisquer que sejam $m, n \in \mathbb{Z}$. A propriedade 3 é chamada de *desigualdade triangular*.

Notemos que $v(ay) = v(y)$ para $0 \neq a \in K$, e em particular $v(-y) = v(y)$. Suponhamos que $v(x) \neq v(y)$, digamos $v(x) < v(y)$. Se $v(x+y) \neq \min\{v(x), v(y)\}$, então por 3 (desigualdade triangular), $v(x+y) > v(x)$. Daí obtemos $v(x) = v((x+y) - y) \geq \min\{v(x+y), v(y)\} > v(x)$, uma contradição. Com isso, acabamos de mostrar a seguinte versão mais forte da desigualdade triangular:

Lema 9 (DESIGUALDADE TRIANGULAR ESTRITA). Sejam v uma valorização discreta de F/K e $x, y \in F$ tais que $v(x) \neq v(y)$. Então $v(x+y) = \min\{v(x), v(y)\}$. ■

Definição 10. A cada lugar $P = tO_P \in \mathbb{P}_F$ vamos associar uma função $v_P : F \rightarrow \mathbb{Z} \cup \{\infty\}$ da seguinte maneira: $v_P(0) \doteq \infty$ e para $0 \neq z \in F$ escrevemos $z = t^n \cdot u$, com $u \in O_P^\times$ e $n \in \mathbb{Z}$, e colocamos $v_P(z) \doteq n$. ■

A função v_P definida anteriormente independe da escolha de elemento primo de P . Ora, se t e t' são elementos primos de P , então $t = t' \cdot w$, para algum $w \in O_P^\times$. De fato, de $P = tO_P = t'O_P$ (pois t e t' são elementos primos de P), segue que $t = t' \cdot \alpha$ para algum $\alpha \in O_P$ e $t' = t \cdot \beta$ para algum $\beta \in O_P$. Daí $t = t\beta\alpha \Rightarrow \beta\alpha = 1 \Rightarrow \alpha, \beta \in O_P^\times$. Daí, se $z = t^n u$ então $z = (t'w)^n u = t'^n (w^n u)$ com $w^n u \in O_P^\times$.

Teorema 11. Seja F/K um corpo de funções. Então

1. Para todo $P \in \mathbb{P}_F$ a função v_P é uma valorização discreta de F/K . Mais ainda

$$\begin{aligned} O_P &= \{z \in F \mid v_P(z) \geq 0\} \\ O_P^\times &= \{z \in F \mid v_P(z) = 0\} \\ P &= \{z \in F \mid v_P(z) > 0\} \end{aligned} \tag{2.1}$$

2. Reciprocamente, suponhamos que v seja uma valorização discreta de F/K . Então o conjunto $P = \{z \in F \mid v(z) > 0\}$ é um lugar de F/K e $O_P = \{z \in F \mid v_P(z) \geq 0\}$ é o correspondente anel de valorização.
3. Um elemento $x \in F$ é um elemento primo de P se, e somente se, $v_P(x) = 1$.
4. Todo anel de valorização de F/K é um subanel (próprio) maximal de F . ■

O teorema anterior nos diz que lugares, anéis de valorização e valorizações discretas do corpo de funções F/K são, essencialmente, a mesma coisa: dado um dos três objetos anteriores, os outros dois ficam unicamente determinados.

Aneis de valorização $\longleftrightarrow$ Lugares $\longleftrightarrow$ Valorizações discretas

O leitor perceberá ao longo do texto o papel fundamental que esses objetos desempenharão em tudo que será desenvolvido.

Como $P \in \mathbb{P}_F$ é um (na verdade, o) ideal maximal de $\mathcal{O}_P$, temos que o quociente $\mathcal{O}_P/P$ é um corpo. Para $x \in \mathcal{O}_P$ denotaremos por $x(P)$ classe de equivalência de x em $\mathcal{O}_P/P$ e para $x \in F \setminus \mathcal{O}_P$ definimos $x(P) \doteq \infty$. O item 2 da [Teorema 5](#) nos dá uma imersão canônica $K \hookrightarrow \mathcal{O}_P/P$. Logo, consideramos K como subcorpo de $\mathcal{O}_P/P$, o mesmo podendo ser feito com $\tilde{K}$.

$$\begin{array}{c} \mathcal{O}_P/P \\ \downarrow \\ \tilde{K} \\ \downarrow \\ K \end{array} \quad \left. \vphantom{\begin{array}{c} \mathcal{O}_P/P \\ \downarrow \\ \tilde{K} \\ \downarrow \\ K \end{array}} \right\} \deg P$$

Definição 12. Seja $P \in \mathbb{P}_F$.

1. $F_P \doteq \mathcal{O}_P/P$ é denominado **corpo residual de P** . O mapa $x \mapsto x(P)$ é dito **mapa de classe de resíduos com respeito a P** . Quando for conveniente, usaremos a notação $x + P$ no lugar de $x(P)$, para $x \in \mathcal{O}_P$.
2. $\deg P \doteq [F_P : K]$ é chamado de **grau** do lugar P . Um lugar de grau um é chamado de **lugar racional**. ■

Proposição 13. Se $P \in \mathbb{P}_F$ e $0 \neq x \in P$ então

$$\deg P \leq [F : K(x)] < \infty$$

Com isso temos que a extensão F_P/K é finita para todo $P \in \mathbb{P}_F$. ■

Corolário 14. Se $\mathbb{P}_F \neq \emptyset$, então $[\tilde{K} : K] < \infty$. ■

Demonstração. Seja $P \in \mathbb{P}_F$. O resultado segue da [Teorema 13](#) e da seguinte torre de corpos:

$$\begin{array}{c} F_P \\ | \\ \tilde{K} \\ | \\ K \end{array} \left. \vphantom{\begin{array}{c} F_P \\ | \\ \tilde{K} \\ | \\ K \end{array}} \right\} < \infty$$

□

A demonstração anterior depende da existência de lugares. Isso é tratado adiante, no [Teorema 17](#).

Observação 15. Observe que se F/K tiver pelo menos um lugar racional, então $\tilde{K} = K = F_P$, i.e., K é todo o corpo de constantes de F/K . Ainda nesse caso, temos que o mapa de classe de resíduos mapeia F em $K \cup \{\infty\}$. No caso de K ser algebricamente fechado, todo lugar é racional e podemos “ler” um elemento $z \in F$ como uma função

$$z : \begin{cases} \mathbb{P}_F & \rightarrow K \cup \{\infty\} \\ P & \mapsto z(P) \end{cases} \quad (2.2)$$

E é por isso que F/K é chamado de corpo de funções. Notemos também que os elementos de K , vistos como funções no sentido anterior, são funções constantes. E é por isso também que K é dito corpo de constantes de F . ■

As seguintes terminologias ainda são motivadas por [2.2](#).

Definição 16. Seja $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um zero de z se $v_P(z) > 0$. Caso $v_P(z) < 0$, diremos que P é pólo de z . Caso $v_P(z) = m > 0$, diremos que P é zero de z de ordem m e caso $v_P(z) = -m < 0$, diremos que P é pólo de z de ordem m . ■

Ainda não nos preocupamos com a questão da existência ou não de anéis de valorização e, conseqüentemente, de lugares. Com relação a isso temos o seguinte

Teorema 17. Sejam F/K um corpo de funções e R um subanel de F tal que $K \subset R \subset F$. Suponha que $\{0\} \neq I \subsetneq R$ é um ideal próprio de R . Então existe um lugar $P \in \mathbb{P}_F$ tal que $P \subset I$ e $R \subset \mathcal{O}_P$. ■

Um tal anel R como no enunciado do teorema acima sempre existe: basta tomar $z \in F$ transcendente sobre K e considerar $R = K[z]$ e $I = (z)$. Aplicando o teorema anterior nesse caso, concluímos que existe um zero P de z . Repetindo o argumento para z^{-1} , concluímos que z tem, também, um pólo Q (que é zero de z^{-1}). Isso mostra então o seguinte

Corolário 18. Seja F/K um corpo de funções algébricas e seja $z \in F$ transcendente sobre K . Então z possui pelo menos um zero e pelo menos um pólo. Em particular $\mathbb{P}_F \neq \emptyset$. ■

2.2 O corpo de funções racional

Definição 19. Seja F/K um corpo de funções. Se $F = K(x)$ para algum x transcendente sobre K , então F/K será chamado de corpo de funções racional. ■

O estudo do corpo de funções racional é de grande auxílio no entendimento de corpos de funções arbitrários. Assim sendo, vamos analisar os lugares de um corpo de funções racional, bem como os correspondentes anéis de valorização e valorizações discretas.

Seja $p(x) \in K[x]$ um polinômio irreduzível e mônico. Consideremos o seguinte conjunto

$$\mathcal{O}_{p(x)} \doteq \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \text{ com } p(x) \nmid g(x) \right\}$$

É de verificação imediata que $\mathcal{O}_{p(x)}$ é um anel de valorização de $K(x)/K$. É fácil ver também, pelo item 2 da [Teorema 5](#) que o correspondente lugar é dado por

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \text{ com } p(x) \nmid g(x) \text{ e } p(x) \nmid f(x) \right\} \in \mathbb{P}_{K(x)}$$

Caso $p(x) = x - \alpha$, $\alpha \in K$, tenha grau 1 escreveremos, por simplicidade, $\mathcal{O}_\alpha \doteq \mathcal{O}_{x-\alpha}$ e $P_\alpha \doteq P_{x-\alpha}$.

Existe um outro anel de valorização em $K(x)/K$ que é distinto dos anteriores, a saber

$$\mathcal{O}_\infty \doteq \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \text{ com } \deg f(x) \leq \deg g(x) \right\}$$

cujo correspondente ideal maximal é

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in K[x] \text{ com } \deg f(x) \leq \deg g(x) \right\}$$

Esse lugar é chamado de lugar infinito de $K(x)$. Note que os índices dependem da escolha de x (por exemplo o lugar infinito de $K(1/x)$ é o lugar P_0 de $K(x)$).

Proposição 20. Seja $K(x)/K$ um corpo de funções racional.

1. Seja $P_{p(x)} \in \mathbb{P}_{K(x)}$. Então $p(x)$ é um elemento primo de $P_{p(x)}$ e a correspondente valorização discreta é dada como a seguir. Seja $0 \neq z \in K(x)$ e escrevamos z como

$$z = p(x)^n \frac{f(x)}{g(x)}$$

com $n \in \mathbb{Z}$ e $f(x), g(x) \in K[x]$ tais que $p(x) \nmid f(x) \cdot g(x)$, então $v_{P_{p(x)}} = n$ (compare com o item 1 do Teorema 11).

O corpo residual $K(x)_{p(x)} = \mathcal{O}_{p(x)} / P_{p(x)}$ é isomorfo a $K[x] / ((p(x)))$ (onde $(p(x))$ é o ideal gerado por $p(x)$), com isomorfismo dado por

$$\phi : \begin{cases} K[x] / ((p(x))) & \rightarrow K(x)_{p(x)} \\ f(x) \bmod p(x) & \mapsto f(x)(P) \end{cases}$$

Como consequência imediata disso, temos que $\deg P = \deg p(x)$.

2. No caso especial em que $p(x) = x - \alpha$ com $\alpha \in K$, temos que o lugar P_α é racional e o mapa de classe de resíduos é dado por

$$z(P_\alpha) = z(\alpha) \doteq \begin{cases} f(\alpha)/g(\alpha) & \text{se } g(\alpha) \neq 0 \\ \infty & \text{se } g(\alpha) = 0 \end{cases}$$

onde escrevemos $z = f(x)/g(x)$ com $f(x), g(x) \in K[x]$ coprimos.

3. Temos que P_∞ também é um lugar racional, e um elemento primo de tal lugar é $t = 1/x$. A valorização discreta correspondente é dada por

$$v_\infty(f(x)/g(x)) = \deg(g(x)) - \deg(f(x))$$

Escrevendo

$$z = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0}$$

com $a_n, b_m \neq 0$, temos que o mapa de classe de resíduos com respeito a P_∞ é dado por

$$z(P_\infty) = z(\infty) \doteq \begin{cases} a_n/b_m & \text{se } n = m \\ 0 & \text{se } n < m \\ \infty & \text{se } n > m \end{cases}$$

4. K é todo o corpo de constantes de $K(x)/K$. ■

Teorema 21. Os únicos lugares do corpo de funções racional $K(x)/K$ são o lugar infinito P_∞ e os lugares da forma $P_{p(x)}$, com $p(x) \in K[x]$ irredutível e mônico. ■

Com o teorema anterior e o item 2 da proposição acima, segue o seguinte

Corolário 22. Os lugares racionais de $K(x)/K$ estão bijeção com $K \cup \{\infty\}$:

$$\begin{array}{ccc} \{\text{Lugares racionais de } K(x)/K\} & \longleftrightarrow & K \cup \{\infty\} \\ P_\alpha & \longleftrightarrow & \alpha \end{array}$$

■

2.3 Independência das valorizações

Teorema 23 (APROXIMAÇÃO FRACA). Seja F/K um corpo de funções e $P_1, \dots, P_n \in \mathbb{P}_F$ lugares dois a dois distintos de F/K . Sejam também $x_1, \dots, x_n \in F$ e $r_1, \dots, r_n \in \mathbb{Z}$. Então existe $x \in F$ tal que

$$v_{P_i}(x - x_i) = r_i \text{ para } i = 1, \dots, n$$

■

O teorema anterior também é conhecido como teorema da independência. O termo *independência* é justificado da seguinte maneira. Suponhamos que, dados n lugares distintos $P_1, \dots, P_n$, o valor de $v_{P_n}(z)$ dependa apenas dos valores $v_{P_1}(z), \dots, v_{P_{n-1}}(z)$. Sob essa hipótese, é claro que se $v_{P_i}(y) = v_{P_i}(z)$ para $i = 1, \dots, n-1$ então $v_{P_n}(y) = v_{P_n}(z)$. Daí, se usarmos a [APROXIMAÇÃO FRACA](#) com $P_1, \dots, P_n, x_i = 0$ e $r_i = v_{P_i}(z)$ para $i = 1, \dots, n-1$, $x_n \in F$ qualquer e $r_n \in \mathbb{Z}$ tal que $r_n < \min\{v_{P_n}(z), v_{P_n}(x_n)\}$, temos garantida a existência de $y \in F$ tal que $v_{P_i}(y) = v_{P_i}(z)$ para $i = 1, \dots, n-1$ (de modo que $v_{P_n}(y) = v_{P_n}(z)$) e $v_{P_n}(y - x_n) = r_n$. Ora, mas pela [desigualdade triangular](#) temos que $v_{P_n}(y - x_n) \geq \min\{v_{P_n}(y) = v_{P_n}(z), v_{P_n}(x_n)\}$. Por outro lado $v_{P_n}(y - x_n) = r_n < \min\{v_{P_n}(z), v_{P_n}(x_n)\}$. Essa contradição nos leva a concluir que o valor $v_{P_n}(z)$ *independe* dos outros $n-1$ valores $v_{P_i}(z)$.

Para uma justificação do termo *aproximação*, o leitor pode conferir [Niederreiter e Xing \(2001, p. 5\)](#).

Corolário 24. Todo corpo de funções possui infinitos lugares. ■

Demonstração. Suponhamos que $\mathbb{P}_F = \{P_1, \dots, P_n\}$ seja finito. Vamos aplicar o teorema anterior para $P_1, \dots, P_n$ com $x_i = 0$ e $r_i > 0 \forall i$. Então existe $x \in F$ tal que $v_{P_i}(x) > 0 \forall i$. Com isso, temos que x é transcendente sobre K . Mas x não possui pólos, o que contraria o [Teorema 18](#).

□

Proposição 25. Seja F/K um corpo de funções e sejam $P_1, \dots, P_n$ zeros de um elemento $x \in F$. Então

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

■

Corolário 26. Em um corpo de funções F/K , qualquer elemento $0 \neq x \in F$ possui apenas um número finito de zeros e pólos. ■

Demonstração. Se $x \in \tilde{K}$, então x não possui nem zeros nem pólos. Caso x seja transcendente sobre K seu número de zeros é $\leq [F : K(x)] < \infty$ pela [Teorema 25](#). Daí, aplicando o mesmo argumento para x^{-1} , concluímos que o número de pólos de x também é $\leq [F : K(x^{-1})] < \infty$.

□

2.4 Divisores

Sem perda de generalidade, vamos supor de agora em diante que K é todo o corpo de constantes de F .

Definição 27. O grupo abeliano livre gerado pelos lugares de F/K é chamado de **grupo dos divisores** de F/K e denotado por $\text{Div}(F)$. Os elementos de $\text{Div}(F)$ são ditos **divisores** de F/K . Em outras palavras, um divisor é uma soma formal

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

com $n_P \in \mathbb{Z}$ e $n_P = 0$ para quase todo $P \in \mathbb{P}_F$, i.e., $n_P \neq 0$ apenas para um número finito de lugares.

O suporte de D é definido como

$$\text{supp } D \doteq \{P \in \mathbb{P}_F \mid n_P \neq 0\}$$

Às vezes será conveniente escrevermos

$$D = \sum_{P \in S} n_P P$$

onde $S \subset \mathbb{P}_F$ é um conjunto finito que contem o suporte de D .

Um divisor da forma $D = P$ com $P \in \mathbb{P}_F$ será chamado de **divisor primo**. A adição de dois divisores $D = \sum_{P \in \mathbb{P}_F} n_P P$ e $D' = \sum_{P \in \mathbb{P}_F} n'_P P$ é feita coeficiente a coeficiente:

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P)P$$

O zero do grupo de divisores $\text{Div}(F)$ é o divisor

$$0 \doteq \sum_{P \in \mathbb{P}_F} r_P P, \text{ com } r_P = 0 \text{ para todo } P$$

Para $Q \in \mathbb{P}_F$ e $D = \sum_{P \in \mathbb{P}_F} n_P P \in \text{Div}(F)$ definimos $v_Q(D) \doteq n_Q$. Com isso podemos escrever

$$\text{supp } D \doteq \{P \in \mathbb{P}_F \mid v_P(D) \neq 0\} \quad \text{e} \quad D = \sum_{P \in \text{supp } D} v_P(D)P$$

Podemos definir uma ordem parcial em $\text{Div}(F)$ da seguinte maneira

$$D_1 \leq D_2 \Leftrightarrow v_P(D_1) \leq v_P(D_2) \quad \forall P \in \mathbb{P}_F$$

Caso $D_1 \leq D_2$ e $D_1 \neq D_2$, também escreveremos $D_1 < D_2$. Um divisor $D \geq 0$ é chamado de **positivo** ou **efetivo**.

Finalmente o grau de um divisor é definido como

$$\deg D \doteq \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \deg P$$

de modo que temos um homomorfismo de grupos $\deg : \text{Div}(F) \rightarrow \mathbb{Z}$. ■

Uma vez que todo elemento não nulo possui apenas um número finito de zeros e pólos (confira o [Teorema 26](#)), faz sentido definirmos os divisores a seguir.

Definição 28. Seja $0 \neq x \in F$ e denotemos por Z e N o conjunto dos zeros e dos pólos, respectivamente, de x em $\mathbb{P}_F$. Então colocamos

$$\begin{aligned} (x)_0 &\doteq \sum_{P \in Z} v_P(x)P, & \text{o divisor zero de } x, \\ (x)_\infty &\doteq \sum_{P \in N} (-v_P(x))P, & \text{o divisor pólo de } x, \\ (x) &\doteq (x)_0 - (x)_\infty, & \text{o divisor principal de } x \end{aligned}$$
■

Claramente os divisores zero e pólo de qualquer elemento $0 \neq x \in F$ são efetivos e

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x)P$$

É claro também (confira o [Teorema 18](#)) que

$$x \in K \Leftrightarrow (x) = 0$$

Definição 29. O conjunto de divisores

$$\text{Princ}(F) \doteq \{(x) \mid 0 \neq x \in F\}$$

é chamado **grupo dos divisores principais** de F/K . Temos que $\text{Princ}(F)$ é subgrupo de $\text{Div}(F)$ uma vez que, para $0 \neq x, y \in F$, $(xy) = (x) + (y)$. O grupo quociente

$$\text{Cl}(F) \doteq \text{Div}(F)/\text{Princ}(F)$$

é chamado de grupo das classes de divisores de F/K . A classe de um divisor $D \in \text{Div}(F)$ em $\text{Cl}(F)$ será denotada por $[D]$ e chamada de classe do divisor D . Diremos que dois divisores D e D' são **equivalentes**, e denotaremos isso por

$$D \sim D'$$

se $[D] = [D']$, i.e., se $D = D' + (x)$, para algum $0 \neq x \in F$. ■

Definição 30. Para um divisor $A \in \text{Div}(F)$, o espaço de Riemann-Roch associado ao divisor A é definido como

$$\mathcal{L}(A) \doteq \{x \in F \mid (x) \geq -A\} \cup \{0\}$$

■

Essa definição tem a seguinte interpretação em termos dos zeros e pólos de uma função $x \in F$. Escrevendo A como

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

com $n_i, m_j \in \mathbb{Z}_{>0}$, então $\mathcal{L}(A)$ consiste dos elementos de F que satisfazem as duas condições a seguir

1. x tem zeros de ordem $\geq m_j$ em Q_j para $j = 1, \dots, s$ e
2. x pode possuir pólos somente em $P_1, \dots, P_r$, com as respectivas ordens dos pólos sendo no máximo $n_1, \dots, n_r$.

Vale também observar que

1. $x \in \mathcal{L}(A) \Leftrightarrow v_P(x) \geq v_P(A) \forall P \in \mathbb{P}_F$ e
2. $\mathcal{L}(A) \neq \{0\}$ se, e somente se, existir $A' \in \text{Div}(F)$ tal que $A' \sim A$ e $A' \geq 0$, pois daí teremos que existe $0 \neq x \in F$ tal que $A + (x) = A' \geq 0$, ou seja $x \in \mathcal{L}(A)$.

Lema 31. Sejam A e $B \in \text{Div}(F)$. Então

1. $\mathcal{L}(A)$ é um K -espaço vetorial.
2. Se $A \sim B$, então $\mathcal{L}(A) \simeq \mathcal{L}(B)$ (como K -espaços vetoriais).
3. $\mathcal{L}(0) = K$.
4. Se $A < 0$, então $\mathcal{L}(A) = \{0\}$.
5. Se $A \leq B$, então $\mathcal{L}(A) \subset \mathcal{L}(B)$ e $\dim_K(\mathcal{L}(B)/\mathcal{L}(A)) \leq \deg B - \deg A$. ■

Proposição 32. Para todo $A \in \text{Div}(F)$, temos que $\mathcal{L}(A)$ é um K -espaço vetorial de dimensão finita. Mais explicitamente, escrevendo $A = A_+ - A_-$, onde A_+ e A_- são divisores efetivos, então

$$\dim_K(\mathcal{L}(A)) \leq \deg A_+ + 1$$

■

Demonstração. Como $A_+ \geq A$, temos que $\mathcal{L}(A) \subset \mathcal{L}(A_+)$ pelo item 2 do Teorema 31, portanto, basta mostrarmos que $\dim_K \mathcal{L}(A_+) \leq \deg A_+ + 1$.

Ora, também temos que $A_+ \geq 0$, logo, pelos itens 3 e 5 do Teorema 31,

$$\dim_K \mathcal{L}(A) = \dim_K(\mathcal{L}(A)/\mathcal{L}(0)) + 1 \leq \deg A_+ + 1$$

□

Definição 33. Para $A \in \text{Div}(F)$ o inteiro $\ell(A) \doteq \dim_K \mathcal{L}(A)$ é dito ser a dimensão do divisor A . ■

O teorema a seguir diz, essencialmente, que qualquer função $0 \neq x$ em F/K possui o “mesmo número” de zeros e pólos.

Teorema 34. Qualquer divisor principal tem grau zero. Mais precisamente, para $x \in F \setminus K$ vale

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

■

Teorema 35. Seja F/K um corpo de funções. Então existe $\gamma \in \mathbb{Z}$, que depende *apenas* de F/K , tal que, para qualquer divisor A vale

$$\deg A - \ell(A) \leq \gamma$$

■

O teorema anterior dá sentido à seguinte

Definição 36. O gênero g de F/K é definido como

$$g \doteq \max\{\deg A - \ell(A) + 1 \mid A \in \text{Div}(F)\} \quad (2.3)$$

■

Observação 37. O gênero de um corpo de funções F/K é um inteiro não negativo. De fato, tomando $A = 0$, temos que

$$g \geq \deg 0 - \ell(0) + 1 = 0 - 1 + 1 = 0$$

■

Teorema 38 (TEOREMA DE RIEMANN). Seja F/K um corpo de funções de gênero g . Então

1. se $A \in \text{Div}(F)$, então $\ell(A) \geq \deg A + 1 - g$ e
2. existe um inteiro c , que depende *apenas* de F/K , tal que se $\deg A \geq c$ então $\ell(A) = \deg A + 1 - g$.

■

Demonstração. O item 1 segue da definição de gênero dada anteriormente. Para o item 2 tomemos $A_0 \in \text{Div}(F)$ tal que $g = \deg A_0 - \ell(A_0) + 1$ e coloquemos $c \doteq \deg A_0 + g$. Se $\deg A \geq c$, então por 1 temos

$$\ell(A - A_0) \geq \deg(A - A_0) + 1 - g \geq c - \deg A_0 + 1 - g = 1$$

Com isso, temos que existe $0 \neq z \in \mathcal{L}(A - A_0)$. Consideremos então o divisor $A' = A + (z) \geq A_0$. Temos que

$$\begin{aligned}
\deg A - \ell(A) &= \deg A' - \ell(A') && \text{pois } A \sim A' \\
&\geq \deg A_0 - \ell(A_0) && \text{pelo item 5 do Teorema 31} \\
&= g - 1
\end{aligned}$$

Daí, $\ell(A) \leq \deg A + 1 - g$ e do item 1 segue a igualdade.

□

Corolário 39. Qualquer corpo de funções racional possui gênero zero. ■

Demonstração. Seja P_∞ o divisor (primo) pólo de x , onde $F = K(x)$. Para $r \geq 0$ consideremos o espaço $\mathcal{L}(rP_\infty)$. Da definição do espaço de Riemann-Roch, é fácil ver que $1, x, \dots, x^r \in \mathcal{L}(rP_\infty)$. Daí, para r suficientemente grande,

$$r + 1 \leq \ell(rP_\infty) = \deg rP_\infty + 1 - g = r + 1 - g \quad (2.4)$$

Ou seja, $g \leq 0$. Mas como $g \geq 0$ qualquer que seja o corpo de funções F/K (confira a Teorema 37), concluímos que, nesse caso do corpo de funções racional, $g = 0$.

□

2.5 O teorema de Riemann-Roch e suas principais consequências

Começamos essa seção com a seguinte

Definição 40. Para $A \in \text{Div}(F)$, o inteiro

$$i(A) \doteq \ell(A) - \deg A + g - 1$$

é chamado de **índice de especialidade** do divisor A . ■

Nesses termos, o **TEOREMA DE RIEMANN** nos diz que $i(A) \geq 0$ para todo $A \in \text{Div}(F)$ e que, se $\deg A$ é suficientemente grande, então $i(A) = 0$. É comum encontrarmos na literatura o termo *divisor não especial* para um divisor cujo índice de especialidade é nulo.

Definição 41. Um **adele** de F/K é uma função

$$\alpha : \begin{cases} \mathbb{P}_F & \rightarrow F \\ P & \mapsto \alpha_P \end{cases}$$

tal que $\alpha_P \in \mathcal{O}_P$ para quase todo (a menos de um número finito) $P \in \mathbb{P}_F$. Olhando um adele como elemento do produto direto $\prod_{P \in \mathbb{P}_F} F$, podemos (e vamos) usar a notação $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ ou $\alpha = (\alpha_P)$. O conjunto de todos os adeles de F/K será denotado por $\mathcal{A}_F$ e chamado de **espaço adele** de F/K . É de verificação imediata que $\mathcal{A}_F$ é um K -espaço vetorial.

Para $x \in F$ definimos o adele principal de x como sendo o adele cujas componentes são todas iguais a x . Tal definição faz sentido, tendo em mente o [Teorema 26](#). Isso nos dá uma imersão $F \hookrightarrow \mathcal{A}_F$, e denotaremos também por F o espaço dos adeles principais (ficará claro pelo contexto quando F é o espaço dos adeles principais e quando é o corpo de funções). As valorizações de F/K se estendem naturalmente a $\mathcal{A}_F$: colocamos $v_P(\alpha) \doteq v_P(\alpha_P)$, onde α_P é a “ P -ésima componente” do adele α (notemos que, pela definição de adele, temos que $v_P(\alpha) \geq 0$ para quase todo $P \in \mathbb{P}_F$). ■

Definição 42. Para $A \in \text{Div}(F)$ definimos

$$\mathcal{A}_F(A) \doteq \{\alpha \in \mathcal{A}_F \mid v_P(\alpha) \geq -v_P(A) \forall P \in \mathbb{P}_F\}$$

É fácil ver que $\mathcal{A}_F(A)$ é um subespaço vetorial de $\mathcal{A}_F$ e que se nos restringirmos aos adeles principais recuperamos $\mathcal{L}(A)$. ■

Definição 43. Uma **diferencial de Weil** de F/K é uma transformação K -linear $\omega : \mathcal{A}_F \rightarrow K$ que se anula em $\mathcal{A}_F(A) + F$ para algum $A \in \text{Div}(F)$, i.e., tal que $\text{Ker}(\omega) \supset \mathcal{A}_F(A) + F$ para algum $A \in \text{Div}(F)$. O conjunto de todas as diferenciais de Weil de F/K será denotado por Ω_F e será chamado de o **módulo das diferenciais de Weil** de F/K . É claro que Ω_F pode ser visto como K -espaço vetorial. ■

Para cada $\omega \in \Omega_F$ vamos associar um divisor $W \in \text{Div}(F)$. Fixada uma diferencial de Weil ω , consideremos o seguinte conjunto

$$M(\omega) \doteq \{A \in \text{Div}(F) \mid \omega \text{ se anula em } \mathcal{A}_F(A) + F\}$$

Proposição 44. Seja $0 \neq \omega \in \Omega_F$. Então existe um único $W \in M(\omega)$ tal que $A \leq W$ para todo $A \in M(\omega)$. ■

A proposição anterior nos permite denotar, fixada uma diferencial de Weil ω , o divisor W por (ω) . Se $W \in \text{Div}(F)$ é tal que $W = (\omega)$ para alguma $\omega \in \Omega_F$, diremos que W é um **divisor canônico**.

Teorema 45. Sejam $A \in \text{Div}(F)$ um divisor qualquer e $W = (\omega)$ um divisor canônico. Então

$$i(A) = \ell(W - A)$$

■

Teorema 46 (TEOREMA DE RIEMANN-ROCH). Seja W um divisor canônico de F/K . Então para qualquer $A \in \text{Div}(F)$ temos

$$\ell(A) = \deg A + 1 - g + \ell(W - A)$$

■

Demonstração. Basta usar o teorema anterior e a definição de índice de especialidade.

□

Corolário 47. Qualquer divisor canônico W de F/K tem grau $\deg W = 2g - 2$ e dimensão $\ell(W) = g$.

■

Demonstração. Basta usar o [TEOREMA DE RIEMANN-ROCH](#) para $A = 0$ e, em seguida, para $A = W$.

□

Os próximos resultados são consequência do [TEOREMA DE RIEMANN-ROCH](#) e de grande utilidade ao longo do texto.

Proposição 48. Para um corpo de funções F/K as seguintes condições são equivalentes

1. F/K é racional, i.e., $F = K(x)$ para algum x transcendente sobre K .
2. F/K tem gênero 0 e existe um divisor $A \in \text{Div}(F)$ tal que $\deg A = 1$.

■

Teorema 49 (TEOREMA DA APROXIMAÇÃO FORTE). Seja $S \subsetneq \mathbb{P}_F$ um subconjunto próprio e não vazio de $\mathbb{P}_F$ e $P_1, \dots, P_r \in S$. Supondo que nos sejam dados $x_1, \dots, x_r \in F$ e $n_1, \dots, n_r \in \mathbb{Z}$. Então existe $x \in F$ tal que

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

■

Proposição 50. Seja $P \in \mathbb{P}_F$. Então para cada $n \geq 2g$, existe $x \in F$ tal que $(x)_\infty = nP$.

■

Com a proposição acima somos capazes de, dado um lugar, obter uma função cujo único pólo (ou zero) seja o lugar em questão.

EXTENSÕES ALGÉBRICAS DE CORPOS DE FUNÇÕES

Neste capítulo estudaremos extensões de corpos do tipo F'/F onde F' e F são corpos de funções. Antes de iniciarmos, convencionaremos algumas coisas.

F/K denotará um corpo de funções algébricas em uma variável tal que K é todo o corpo de constantes de F . Vamos assumir também que K é perfeito. Consideramos corpos de funções F'/K' onde $F' \supseteq F$ é uma extensão algébrica e $K' \supseteq K$. Fixamos um corpo algebricamente fechado $\Phi \supseteq F$ e, sem perda de generalidade, consideraremos apenas extensões $F' \supseteq F$ tais que $F' \subseteq \Phi$.

3.1 A igualdade fundamental

Começamos com algumas definições básicas.

Definição 51. Seja F/K um corpo de funções .

1. Um corpo de funções algébricas F'/K' é dito ser uma extensão algébrica de F/K se $F \subseteq F'$ for uma extensão algébrica de corpos e se $K \subseteq K'$.
2. A extensão algébrica F'/K' de F/K é dita ser uma extensão de corpo de constantes se $F' = FK'$, onde FK' é o compósito de F e K' .
3. A extensão algébrica F'/K' de F/K é dita ser finita se $[F' : F] < \infty$. ■

É claro que podemos considerar extensões arbitrárias (não necessariamente algébricas) de corpos de funções. Entretanto, restringimo-nos às extensões algébricas visto elas serem, de longe, as de maior importância para o nosso estudo.

Algumas consequências simples da definição anterior são dadas pelo seguinte

Lema 52. Seja F'/K' uma extensão algébrica de F/K . Então vale o seguinte:

1. K'/K é algébrica e $K = F \cap K'$.
2. F'/K' é uma extensão finita de F/K se, e somente se, $[K' : K] < \infty$.
3. Seja $\bar{F} = FK'$. Então $\bar{F}/K'$ é uma extensão de corpo de constantes de F/K , e F'/K' é uma extensão finita de $\bar{F}/K'$ (tendo o mesmo corpo de constantes). ■

Demonstração.

1. Na torre de corpos a seguir as linhas vermelhas representam extensões transcendentais (com grau de transcendência exatamente 1) e a azul, uma extensão que é algébrica por hipótese.

A linha de K a K' também é azul, ou seja, K'/K também é algébrica. De fato, como o grau de transcendência é aditivo, basta olharmos para a extensão F'/K de duas maneiras distintas: $F' \supset F \supset K$ e $F' \supset K' \supset K$. Como F'/F é algébrica e F/K tem grau de transcendência 1, F'/K tem grau de transcendência 1. Mas daí, como F'/K' já

tem grau de transcendência 1, K'/K não pode ser transcendente, logo deve ser algébrica.

Para a segunda afirmação, basta mostrarmos que $K \supset K' \cap F$ (a outra inclusão é clara). Seja $z \in K' \cap F$. Como $K \subset K(z) \subset K'$ e como K'/K é algébrica, temos que $F \ni z$ é algébrico sobre K . Como K é todo o corpo de constantes de F , $z \in K$.

2. Primeiro, suponhamos que F'/K' seja extensão finita de F/K . Então, como $K \subseteq K'$, F' pode ser visto como corpo de funções algébricas sobre K . Como K' é todo corpo de constantes de F' , pela nossa suposição inicial, temos que F'/K é um corpo de funções com corpo de constantes $\tilde{K} = K'$. Portanto, pelo [Teorema 14](#), temos que $[\tilde{K} : K] = [K' : K] < \infty$.

Agora, suponhamos que K'/K seja finita. Seja $x \in F \setminus K$. Pela [Teorema 3](#), temos que x é transcendente sobre K . Ora, uma vez que $F \subseteq F'$ temos que $x \in F'$. Temos que x também é transcendente sobre K' , caso contrário $x \in K'$ e, por K'/K ser algébrica, teríamos que x seria algébrico sobre K . Daí, novamente pela [Teorema 3](#), temos que $[F' : K'(x)] < \infty$. Além disso, temos, uma vez que existe elemento primitivo $\alpha \in K'$ tal que $K' = K(\alpha)$ (lembramos que supomos K perfeito no início do capítulo),

$$[K'(x) : K(x)] \leq [K' : K] < \infty \quad (3.1)$$

Daí, na torre de corpos a seguir, as linhas verdes representam extensões que já sabemos serem finitas.

Portanto $[F' : K(x)] = \underbrace{[F' : K'(x)]}_{<\infty} \cdot \underbrace{[K'(x) : K(x)]}_{<\infty \text{ por 3.1}} < \infty$. Por outro lado $\underbrace{[F' : K(x)]}_{<\infty} = \underbrace{[F' : F]}_{<\infty} \cdot \underbrace{[F : K(x)]}_{<\infty} \Rightarrow [F' : F] < \infty$.

3. Temos a seguinte torre:

$$\begin{array}{ccccc}
 & & \bar{F} = FK' & - & F' \\
 & \swarrow & | & & | \\
 F & & & & K' \\
 | & & & & | \\
 K & & & & K'
 \end{array}$$

Temos que, pela definição de extensão de corpo de constantes, $\bar{F}/K'$ é extensão de corpo de constantes de F/K . Pelo item anterior concluímos que F'/K' é extensão finita de $\bar{F}/K'$, pois $[K' : K'] = 1 < \infty$. Temos que K' é todo o corpo de constantes de F'/K' . Vamos mostrar que K' também é todo o corpo de constantes de $\bar{F}/K'$. Para isso, basta mostrarmos que se $x \in \bar{F}$ é algébrico sobre K' , então $x \in K'$. Ora, se $x \in \bar{F}$ então $x \in F'$, logo, se x é algébrico sobre K' , então $x \in K'$.

□

Observação 53. A desigualdade 3.1 na verdade é uma igualdade (STICHTENOTH, 2009, p. 73), porém não a demonstraremos aqui. ■

Vamos estudar agora a relação entre os lugares de F e os de F' .

Definição 54. Considere uma extensão algébrica F'/K' de F/K . Dizemos que um lugar $P' \in \mathbb{P}_{F'}$ **está acima** de $P \in \mathbb{P}_F$ se $P \subseteq P'$. Também dizemos que P' é uma extensão de P ou que P está abaixo de P' e denotamos isso por $P'|P$. ■

Proposição 55. Seja F'/K' uma extensão algébrica de F/K . Suponha que P (resp. P') é um lugar de F/K (resp. F'/K'), e seja $\mathcal{O}_P \subset F$ (resp. $\mathcal{O}_{P'} \subset F'$) o anel de valorização correspondente e v_P (resp. $v_{P'}$) a valorização discreta correspondente. Então as seguintes afirmações são equivalentes:

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

Mais ainda, se $P'|P$ então $P = P' \cap F$ e $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$. Por essa razão, P é dito ser a restrição de P' em F . ■

Demonstração. $1 \Rightarrow 2$. Suponha que $P'|P$, mas que $\mathcal{O}_P \not\subseteq \mathcal{O}_{P'}$. Então existe algum $u \in F$ com $v_P(u) \geq 0$ e $v_{P'}(u) < 0$. Como $P \subseteq P'$, concluímos que $v_P(u) = 0$ (caso contrário $v_P(u) > 0 \Rightarrow u \in P \subseteq P' \Rightarrow v_{P'}(u) > 0$). Seja t um elemento primo de P , ou seja, $v_P(t) = 1$. Então $t \in P \subseteq P'$ e $r = v_{P'}(t) \geq 1$. Consequentemente,

$$v_P(u^r t) = r v_P(u) + v_P(t) = 0 + 1 = 1 \Rightarrow u^r t \in P$$

e

$$v_{P'}(u^r t) = r v_{P'}(u) + v_{P'}(t) \leq -r + r = 0 \Rightarrow u^r t \notin P'$$

que contradiz $P \subseteq P'$.

Antes de mostrarmos que $2 \Rightarrow 1$, vamos mostrar o seguinte:

$$O_P \subseteq O_{P'} \Rightarrow O_P = O_{P'} \cap F \quad (3.2)$$

Claramente, $F \cap O_{P'}$ é um subanel de F tal que $O_P \subseteq F \cap O_{P'}$ (pois $O_P \subset F$ e $O_P \subseteq O_{P'}$). Então, pelo [Item 4](#) do [Teorema 11](#), temos que ou $F \cap O_{P'} = O_P$ ou $F \cap O_{P'} = F$. Suponhamos que o segundo caso acontece, ou seja, que $F \subset O_{P'}$ e escolhamos $z \in F' \setminus O_{P'}$. Como F'/F é algébrica, temos que existem $c_0, \dots, c_{n-1} \in F$ tais que

$$z^n + c_{n-1}z^{n-1} + \dots + c_1z + c_0 = 0 \quad (3.3)$$

Uma vez que $z \notin O_{P'}$, temos que $v_{P'}(z^n) = n \cdot v_{P'}(z) < 0$ e daí

$$v_{P'}(z^n) < v_{P'}(c_v z^v) \quad \text{para } v = 0, \dots, n-1$$

Com isso, uma aplicação da [DESIGUALDADE TRIANGULAR ESTRITA](#) resulta em

$$v_{P'}(z^n + c_{n-1}z^{n-1} + \dots + c_1z + c_0) = n \cdot v_{P'}(z) \neq \infty = v_{P'}(0) \quad (3.4)$$

contradizendo a [Equação 3.3](#) e, portanto, provando [3.2](#).

[2](#) $\Rightarrow$ [1](#). Suponhamos que $O_P \subset O_{P'}$. Dado $y \in P$, a o item [2](#) da [Teorema 5](#) nos diz que $y^{-1} \notin O_P$ e portanto $y^{-1} \notin O_{P'}$ por [3.2](#) (note que $y^{-1} \in F$). Com mais uma aplicação do item [2](#) da [Teorema 5](#) obtemos $y = (y^{-1})^{-1} \in P'$. Logo $P \subseteq P'$.

[2](#) $\Rightarrow$ [3](#). Seja $u \in F$ tal que $v_P(u) = 0$. Então u e $u^{-1} \in O_P$ e, pelo item [2](#), u e $u^{-1} \in O_{P'}$ também. Logo $v_{P'}(u) = 0$. Agora seja $t \in F$ um elemento primo de P e coloquemos $e \doteq v_{P'}(t)$. De $P \subseteq P'$ segue que $e \geq 1$. Seja $0 \neq x \in F$ e $v_P(x) \doteq r \in \mathbb{Z}$. Então $v_P(xt^{-r}) = 0$ e portanto

$$v_{P'}(x) = v_{P'}(xt^{-r}) + v_{P'}(t^r) = 0 + r \cdot v_{P'}(t) = e \cdot v_{P'}(x)$$

[3](#) $\Rightarrow$ [2](#). Temos

$$x \in \mathcal{O}_P \Rightarrow v_P(x) \geq 0 \Rightarrow v_{P'}(x) = \overset{\geq 1}{e} \cdot v_P(x) \geq 0 \Rightarrow x \in \mathcal{O}_{P'}$$

Então mostramos que $1 \Leftrightarrow 2 \Leftrightarrow 3$ e que $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$ se $P'|P$ ($\Leftrightarrow \mathcal{O}_P \subset \mathcal{O}_{P'}$ pelo item 2).

Para $P = F \cap P'$, basta mostrar $P' \cap F \subset P$. Sendo $x \in P' \cap F$, temos que $v_{P'}(x) > 0$ e pelo 3 $e \cdot v_P(x) = v_{P'}(x) > 0 \Rightarrow v_P(x) > 0 \Rightarrow x \in P$. Isso finaliza a demonstração. $\square$

Se $P'|P$, como consequência da Teorema 55 anterior temos um mergulho canônico do corpo residual $F_P = \mathcal{O}_P/P$ no corpo residual $F'_{P'} = \mathcal{O}_{P'}/P'$ dado por

$$x(P) \mapsto x(P') \quad \text{para } x \in \mathcal{O}_P$$

e podemos considerar F_P como subcorpo de $F'_{P'}$, como na torre de corpos a seguir

$$\begin{array}{ccc} & & F'_{P'} \\ & \swarrow f(P'|P) & \downarrow \deg P' \\ & F_P & \\ \downarrow \deg P & & \downarrow \\ & K & \swarrow \\ & & K' \end{array}$$

Definição 56. Sejam F'/K' uma extensão algébrica de F/K e $P' \in \mathbb{P}_{F'}$ um lugar de F'/K' acima de $P \in \mathbb{P}_F$.

1. O inteiro $e(P'|P) \doteq e$ tal que $v_{P'}(x) = e \cdot v_P(x)$ para todo $x \in F$ é chamado de **índice de ramificação** de P' sobre P . Dizemos que a extensão $P'|P$ é **ramificada** se $e(P'|P) > 1$ e **não-ramificada** caso contrário.
2. O inteiro $f(P'|P) \doteq [F'_{P'} : F_P]$ é chamado de **grau relativo** de P' sobre P . $\blacksquare$

Apesar de $e(P'|P)$ ser *sempre* um inteiro ≥ 1 , nada podemos afirmar sobre a finitude de $f(P'|P)$. Não obstante, temos a seguinte útil igualdade

$$f(P'|P) \cdot \deg P = [K' : K] \cdot \deg P' \quad (3.5)$$

Proposição 57. Sejam F'/K' uma extensão algébrica de F/K e $P' \in \mathbb{P}_{F'}$ um lugar de F'/K' acima de $P \in \mathbb{P}_F$. Então

1. $f(P'|P) < \infty \Leftrightarrow [F' : F] < \infty (\Leftrightarrow [K' : K] < \infty$ pelo Item 2 do Teorema 52)

2. Se F''/K'' é uma extensão algébrica de F'/K' e $P'' \in \mathbb{P}_{F''}$ está acima de P' , então

$$\begin{aligned} e(P''|P) &= e(P''|P') \cdot e(P'|P) \\ f(P''|P) &= f(P''|P') \cdot f(P'|P) \end{aligned} \quad (3.6)$$

■

Demonstração. O item 1 é imediato da torre de corpos anterior e do fato de serem os graus de quaisquer lugares finitos (confira a [Teorema 13](#)).

Para 2, a igualdade para os índices de ramificação segue da própria definição de índice de ramificação: basta tomar t um elemento primo de P e calcular as valorizações de t nos lugares P' e P'' . Para a igualdade dos graus relativos basta considerar as extensões $F_P \subset F'_{P'} \subset F''_{P''}$ e usar a multiplicatividade do grau de extensões de corpos.

□

O próximo resultado mostra que existem, de fato, lugares acima de um lugar $P \in \mathbb{P}_F$ numa extensão de F e reciprocamente.

Proposição 58. Seja F'/K' uma extensão algébrica de F/K .

1. Para cada lugar $P' \in \mathbb{P}_{F'}$, existe *exatamente um* lugar $P \in \mathbb{P}_F$ tal que $P'|P$, a saber $P = P' \cap F$.
2. Reciprocamente, cada lugar $P \in \mathbb{P}_F$ possui *pelo menos uma*, mas *sempre um número finito* de extensões $P' \in \mathbb{P}_{F'}$.

■

Demonstração. Dado $P' \in \mathbb{P}_{F'}$, afirmamos que existe $z \in F$ tal que $v_{P'}(z) \neq 0$. Suponhamos que a afirmação anterior seja falsa. Escolhamos $t \in F'$ tal que $v_{P'}(t) > 0$. Sendo F'/F algébrica temos que existem $c_0, \dots, c_n \in F$ com c_0 e c_n não nulos tais que

$$c_n t^n + c_{n-1} t^{n-1} + \dots + c_1 t + c_0 = 0$$

Por hipótese, temos que $v_{P'}(c_0) = 0$ e $v_{P'}(c_{i+1} t^{i+1}) = v_{P'}(c_{i+1}) + (i+1)v_{P'}(t) > i v_{P'}(t) = v_{P'}(c_i t^i)$ para $i = 0, \dots, n-1$. “Aplicando” $v_{P'}$ dos dois lados da [igualdade anterior](#) obtemos uma contradição com a [DESIGUALDADE TRIANGULAR ESTRITA](#) como na demonstração da [Teorema 55](#).

Coloquemos $\mathcal{O} \doteq \mathcal{O}_{P'} \cap F$ e $P \doteq P' \cap F$. Vamos mostrar que $\mathcal{O}$ é um anel de valorização de F . Pela afirmação feita no início, existe $0 \neq z \in F$ tal que $v_{P'}(z) \neq 0$. Se $v_{P'}(z) < 0$, então pela primeira das relações [2.1](#), $z \notin \mathcal{O}_{P'}$. Com isso temos que existe $z \in F \setminus \mathcal{O}_{P'}$ e daí $\mathcal{O} \subsetneq F$. Temos que $v_{P'}(z^{-1}) > 0$ e portanto, pelo [Teorema 18](#), z é transcendente sobre K' , logo sobre K (se fosse z algébrico sobre K' , z não teria nenhum zero nem nenhum

pólo). Com isso temos que $K \subsetneq \mathcal{O}$. Caso o z da afirmação seja tal que $v_{P'}(z) > 0$, então basta trocarmos z por z^{-1} e repetirmos os argumentos anteriores. Isso mostra o item 1 da Teorema 4. Para o item 2 basta notar, que caso $z \in F \setminus \mathcal{O}$ então $z^{-1} \in \mathcal{O}_{P'}$ e, portanto, $z^{-1} \in \mathcal{O}$. Sabendo então que $\mathcal{O}$ é um anel de valorização de F/K , é claro, pela última afirmação feita na Teorema 55, que o lugar associado a $\mathcal{O}$ é $P \doteq P' \cap F$. Isso mostra o item 1.

Para o item 2, seja $P \in \mathbb{P}_F$. Escolhamos $x \in F \setminus K$ cujo único zero seja P (tal escolha é possível pela Teorema 50). Afirmamos que, para $P' \in \mathbb{P}_{F'}$ vale o seguinte

$$P'|P \Leftrightarrow v_{P'}(x) > 0 \quad (3.7)$$

Daí o resultado segue do Teorema 26: x possui apenas um número finito de zeros em F'/K' .

Vamos, então, mostrar a afirmação. Se $P'|P$ então $v_{P'}(x) = e \cdot v_P(x) > 0$. Reciprocamente, suponhamos $v_{P'}(x) > 0$. Seja Q o lugar, dado pelo item 1, abaixo de P' . Então $v_Q(x) > 0$ e daí $Q = P$ pois P é o único zero de x em F/K .

□

O resultado anterior é ilustrado abaixo.

O item 2 da proposição anterior dá sentido à seguinte

Definição 59. Seja F'/K' uma extensão algébrica de F/K . Dado uma lugar $P \in \mathbb{P}_F$, a **conorma** de P (em relação à F'/F) é definida como

$$\text{Con}_{F'/F}(P) \doteq \sum_{P'|P} e(P'|P) \cdot P'$$

onde a soma anterior é “feita” sobre todos os lugares $P' \in \mathbb{P}_{F'}$ acima do lugar $P \in \mathbb{P}_F$ em questão. Podemos estender a definição de conorma a qualquer divisor $D \in \text{Div}(F)$. Basta colocarmos, para $D = \sum n_P P$,

$$\text{Con}_{F'/F}\left(\sum n_P P\right) \doteq \sum n_P \text{Con}_{F'/F}(P) \in \text{Div}(F')$$

■

A conorma é “bem comportada” em torres de corpos $F'' \supset F' \supset F$: do item 2 da Teorema 57 resulta que

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

para qualquer divisor $A \in \text{Div}(F)$. Outra boa propriedade da conorma é que ela leva divisores principais de F/K em divisores principais de F'/K' como diz, mais precisamente, a seguinte

Proposição 60. Seja F'/K' uma extensão algébrica do corpo de funções F/K . Para $0 \neq x \in F$, sejam $(x)_0^F$, $(x)_\infty^F$, $(x)^F$, $(x)_0^{F'}$, $(x)_\infty^{F'}$ e $(x)^{F'}$ os divisores zero, pólo e principal, respectivamente, de x em $\text{Div}(F)$ e em $\text{Div}(F')$, respectivamente. Então

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

■

Demonstração. Da definição cla de divisor principal de x segue que

$$\begin{aligned}(x)^{F'} &= \sum_{P' \in \mathbb{P}_{F'}} v_{P'}(x) \cdot P' = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} e(P'|P) \cdot v_P(x) \cdot P' \\ &= \sum_{P \in \mathbb{P}_F} v_P(x) \cdot \text{Con}_{F'/F}(P) = \text{Con}_{F'/F} \left(\sum_{P \in \mathbb{P}_F} v_P(x) \cdot P \right) \\ &= \text{Con}_{F'/F}((x)^F)\end{aligned}\tag{3.8}$$

Daí, se considerarmos apenas as partes positiva (zeros) e negativa (pólos) do divisor principal, obtemos os correspondentes resultados para os divisores zero e pólo, respectivamente, de x .

□

A seguir, o resultado mais importante desta seção.

Teorema 61 (IGUALDADE FUNDAMENTAL). Sejam F'/K' uma extensão finita de F/K , P um lugar de F/K e $P_1, \dots, P_m$ todos os lugares de F'/K' acima de P . Coloquemos $e_i \doteq e(P_i|P)$ e $f_i \doteq f(P_i|P)$ para $i = 1, \dots, m$. Então

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

■

Demonstração. Escolhamos $x \in F$ tal que o único zero de x em F/K seja P (confira a [Teorema 50](#)) e coloquemos $r \doteq v_P(x) > 0$. Então os lugares $P_1, \dots, P_m$ acima de P são exatamente todos os zeros de x em F'/K' por [3.7](#). Vamos calcular o número $[F' : K(x)]$ de duas maneiras distintas. Daí o teorema ficará demonstrado depois que compararmos os resultados tais cálculos.

Por um lado, temos

$$\begin{aligned}
 [F' : K(x)] &= [F' : K'(x)] \cdot [K'(x) : K(x)] \\
 &= \left(\sum_{i=1}^m v_{P_i}(x) \cdot \deg P_i \right) \cdot [K' : K] \\
 &= \sum_{i=1}^m v_{P_i}(x) \cdot \deg P_i \cdot [K' : K] \\
 &= \sum_{i=1}^m e_i \cdot v_P(x) \cdot f_i \cdot \deg P \\
 &= r \cdot \deg P \cdot \sum_{i=1}^m e_i f_i
 \end{aligned}$$

Confira a [Teorema 53](#). Por outro lado, temos que

$$[F' : K(x)] = [F' : F] \cdot [F : K(x)] = [F' : F] \cdot r \cdot \deg P \quad (3.9)$$

a última igualdade anterior segue do [Teorema 34](#) por ser $rP = (x)_0 \in \text{Div}(F)$. Daí é claro que $\sum_{i=1}^m e_i f_i = [F' : F]$.

□

O corolário a seguir é uma consequência imediata da igualdade fundamental.

Corolário 62. Seja F'/K' uma extensão finita de F/K e $P \in \mathbb{P}_F$. Então

1. $|\{P' \in \mathbb{P}_{F'} \mid P'|P\}| \leq [F' : F]$
2. Se $P' \in \mathbb{P}_{F'}$ está acima de P , então $e(P'|P) \leq [F' : F]$ e $f(P'|P) \leq [F' : F]$. ■

Definição 63. Seja, como de costume, F'/K' uma extensão de F/K de grau $[F' : F] = n$ e seja $P \in \mathbb{P}_F$.

1. Diremos que P se **decompõe completamente** em F'/F se o número de lugares $P' \in \mathbb{P}_{F'}$ acima de P é exatamente n , o que acontece se, e somente se, $e(P'|P) = f(P'|P) = 1$ para todo $P'|P$.
2. Dizemos que P é **totalmente ramificado** em F'/F se existir um lugar $P' \in \mathbb{P}_{F'}$ acima de P com índice de ramificação máximo $e(P'|P) = n$. Nesse P' será o único lugar acima de P e $f(P'|P) = 1$. ■

Outra consequência direta da igualdade fundamental é o seguinte

Corolário 64. Seja F'/K' uma extensão finita de F/K . Então para cada divisor $A \in \text{Div}(F)$ vale

$$\deg \text{Con}_{F'/F}(A) = \frac{[F' : F]}{[K' : K]} \cdot \deg A$$

■

Demonstração. Basta mostrarmos o resultado para divisores primos $A = P \in \mathbb{P}_F$. Daí o resultado geral segue de ser $\deg$ um homomorfismo. Temos que

$$\begin{aligned}
 \deg \text{Con}_{F'/F}(P) &= \deg \left(\sum_{P'|P} e(P'|P) \cdot P' \right) \\
 &= \sum_{P'|P} e(P'|P) \cdot [F'_{P'} : K'] \\
 &= \sum_{P'|P} e(P'|P) \cdot \frac{[F'_{P'} : K]}{[K' : K]} \\
 &= \frac{1}{[K' : K]} \cdot \sum_{P'|P} e(P'|P) \cdot [F'_{P'} : F_P] \cdot [F_P : K] \\
 &= \frac{1}{[K' : K]} \cdot \left(\sum_{P'|P} e(P'|P) f(P'|P) \right) \cdot \deg P \\
 &= \frac{[F' : F]}{[K' : K]} \cdot \deg P
 \end{aligned}$$

□

Proposição 65. Consideremos um corpo de funções F/K e um polinômio

$$\varphi(T) = a_n T^n + a_{n-1} T^{n-1} + \dots + a_1 T + a_0 \quad (3.10)$$

com coeficientes $a_i \in F$. Suponhamos que exista um lugar $P \in \mathbb{P}_F$ tal que uma das seguintes condições seja válida

1. $v_P(a_n) = 0$, $v_P(a_i) \geq v_P(a_0) > 0$ para $i = 1, \dots, n-1$ e n e $v_P(a_0)$ são coprimos.
2. $v_P(a_n) = 0$, $v_P(a_i) \geq 0$ para $i = 1, \dots, n-1$, $v_P(a_0) < 0$ e n e $v_P(a_0)$ são coprimos.

Então $\varphi(T)$ é irredutível em $F[T]$. Se $F' = F(y)$, onde y é uma raiz de $\varphi(T)$, então P tem uma única extensão $P' \in \mathbb{P}_{F'}$, e temos que $e(P'|P) = n$ e $f(P'|P) = 1$ (i.e., P é totalmente ramificado em $F(y)/F$). ■

3.2 Subaneis de corpos de funções

Definição 66. Um **subanel** de F/K é um anel R tal que $K \subseteq R \subseteq F$ e que não é corpo. ■

Já vimos exemplos de subaneis de F/K : os aneis de valorização do [Capítulo 2](#). Notemos que se R é subanel de F/K , então $K \subsetneq R \subsetneq F$.

Definição 67. Para $\emptyset \neq S \subseteq \mathbb{P}_F$, definimos

$$\mathcal{O}_S \doteq \bigcap_{P \in S} \mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0 \forall P \in S\}$$

Um conjunto como dessa forma será chamado de **anel de holomorfia** de F/K . ■

Lema 68.

1. Todo anel de valorização $\mathcal{O}_P$ é um anel de holomorfia de F/K , a saber $\mathcal{O}_P = \mathcal{O}_S$ com $S = \{P\}$.
2. Todo anel de holomorfia de F/K é subanel de F/K .
3. Para $P \in \mathbb{P}_F$ e $\emptyset \neq S \subseteq \mathbb{P}_F$ temos que

$$\mathcal{O}_S \subseteq \mathcal{O}_P \Leftrightarrow P \in S$$

Disso, segue que $\mathcal{O}_S = \mathcal{O}_T \Leftrightarrow S = T$. ■

Demonstração. O item 1 é óbvio pela definição de anel de holomorfia. Para o item 2, basta mostrarmos que $\mathcal{O}_S$ não é corpo, pois é claro que $\mathcal{O}_S$ é anel tal que $K \subset \mathcal{O}_S \subset F$. Dado $P_1 \in S$ o [TEOREMA DA APROXIMAÇÃO FORTE](#) nos garante a existência de $0 \neq x \in F$ tal que

$$v_{P_1}(x) > 0 \quad \text{e} \quad v_P(x) \geq 0, \quad \forall P \in S \setminus \{P_1\}$$

Em particular $x \in \mathcal{O}_S$, mas

$$v_{P_1}(x^{-1}) < 0 \Rightarrow x^{-1} \notin \mathcal{O}_{P_1} \Rightarrow x^{-1} \notin \mathcal{O}_S$$

o que mostra que $\mathcal{O}_S$ não é um corpo. Para o item 3, é claro que $P \in S \Rightarrow \mathcal{O}_S \subset \mathcal{O}_P$. Então basta mostrarmos que $P \notin S \Rightarrow \mathcal{O}_S \not\subset \mathcal{O}_P$. Suponhamos então que $P \notin S$. Novamente, o **TEOREMA DA APROXIMAÇÃO FORTE** nos garante a existência de $z \in F$ tal que

$$v_P(z) < 0 \text{ e } v_Q(z) \geq 0, \quad \forall Q \in S \quad (3.11)$$

De fato, caso $S \cup \{P\} \neq \mathbb{P}_F$, a existência de um z como acima é clara pelo **TEOREMA DA APROXIMAÇÃO FORTE**. Agora caso $S \cup \{P\} = \mathbb{P}_F$, basta tomarmos $z \in \mathcal{O}_S$ tal que $v_Q(z) > 0$ para pelo menos um $Q \in S$. Daí, pelo **Teorema 18** e por $z \in \mathcal{O}_S$, temos necessariamente que P será pólo de z , i.e., $v_P(z) < 0$. Cada elemento $z \in \mathcal{O}_S$ que satisfaz 3.11, é tal que $z \in \mathcal{O}_S$ mas $z \notin \mathcal{O}_P$. Ou seja $P \notin S \Rightarrow \mathcal{O}_S \not\subset \mathcal{O}_P$. Para a última afirmação do 3, basta observar que se $\mathcal{O}_S = \mathcal{O}_T$, temos que $P \in S \Rightarrow \mathcal{O}_S \subset \mathcal{O}_P \Rightarrow \mathcal{O}_T \subset \mathcal{O}_P$ e, pela primeira parte do 3, $P \in T$. Logo $S \subset T$. Invertendo os papeis de S e de T , obtemos $S = T$.

□

Definição 69. Seja R um subanel de F/K .

1. Um elemento $z \in F$ é dito ser **inteiro** sobre R se z é raiz de algum polinômio mônico em uma variável com coeficientes em R . Ou seja, z é inteiro sobre R se

$$f(z) = z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0 = 0$$

com $a_{n-1}, \dots, a_0 \in R$. Uma tal equação é chamada de **equação integral** para z sobre R .

2. O conjunto

$$\text{ic}_F(R) \doteq \{z \in F \mid z \text{ é inteiro sobre } R\}$$

é chamado de **fecho inteiro** de R em F .

3. Seja $F_0 \subseteq F$ o corpo quociente de R . Diremos que o anel R é **integralmente fechado** se $\text{ic}_{F_0}(R) = R$, ou seja, se todo elemento $z \in F_0$ que for inteiro sobre R já estiver em R . ■

É importante enfatizar que, para nós, a noção de ser integralmente fechado depende apenas do anel R em questão: um anel R é integralmente fechado se o fecho inteiro de R no seu corpo de frações (que depende apenas de R) é o próprio R . Assim, um anel R tal que $R \subsetneq \text{ic}_F(R)$ não necessariamente é não integralmente fechado.

Proposição 70. Seja $\mathcal{O}_S$ um anel de holomorfia de F/K . Então

1. F é o corpo de frações de $\mathcal{O}_S$ e
2. $\mathcal{O}_S$ é integralmente fechado. ■

Demonstração. Seja $0 \neq x \in F$. Vamos mostrar que x pode ser expresso como um quociente de dois elementos de $\mathcal{O}_S$, $x = y/z$, y e $z \in \mathcal{O}_S$. Escolhamos $P_0 \in S$. Afirmamos que existe $z \in F$ tal que

$$v_{P_0}(z) = \max\{0, v_{P_0}(x^{-1})\} \quad \text{e} \quad v_P(z) \geq \max\{0, v_P(x^{-1})\}, \quad \forall P \in S$$

Vejamos. Sabemos que x possui apenas um número finito de zeros e pólos, que denotaremos por $\{Q_1, \dots, Q_r\}$. Seja $T \doteq \{Q_1, \dots, Q_r\} \cap S$. Se $T = \emptyset$, então $v_P(x^{-1}) = 0$ para todo $P \in S$, e a existência de z segue imediatamente do [TEOREMA DA APROXIMAÇÃO FORTE](#). Caso $T \neq \emptyset$, basta tomarmos, no [TEOREMA DA APROXIMAÇÃO FORTE](#) (aqui Q_{i_j} denotam os lugares de T), $n_j = \max\{0, v_{Q_{i_j}}(x^{-1})\}$ e $x_j = 0$ para $j = 1, \dots, |T|$. Caso $P_0 \notin T$ acrescentamos $n_0 = \max\{0, v_{P_0}(x^{-1})\}$ e $x_0 = 0$. Daí, em ambos os casos $P_0 \in T$ e $P_0 \notin T$, o [TEOREMA DA APROXIMAÇÃO FORTE](#) nos garante novamente a existência de z como acima.

Notemos que $z \in \mathcal{O}_S$. Além disso, $z \neq 0$ pois $v_{P_0}(z) < \infty$. Definamos $y \doteq zx$. Temos que $v_P(y) \geq 0$ para qualquer $P \in S$. Daí $y \in \mathcal{O}_S$ e também $y \neq 0$ (pois ambos z e x são não nulos). Daí $x = yz^{-1} \in \text{Frac}(\mathcal{O}_S)$. Com isso mostramos o 1.

Agora seja $u \in \mathcal{O}_S$ tal que

$$u^n + a_{n-1}u^{n-1} + \dots + a_1u + a_0 = 0 \tag{3.12}$$

com $a_i \in \mathcal{O}_S$ para $i = 0, \dots, n-1$. Então para mostrarmos 2, basta mostrarmos que $v_P(u) \geq 0$ qualquer que seja $P \in S$. Suponhamos que $v_P(u) < 0$ para algum $P \in S$. Uma vez que $v_P(a_i) \geq 0$ temos que

$$v_P(u^n) = n \cdot v_P(u) < v_P(a_i u^i) \tag{3.13}$$

para $i = 0, \dots, n-1$. Daí “aplicando” v_P aos dois lados da [Equação 3.12](#) e usando a [DESIGUALDADE TRIANGULAR ESTRITA](#) (que é possível por [3.13](#)), obtemos uma contradição. □

Teorema 71. Sejam R um subanel de F/K e

$$S(R) \doteq \{P \in \mathbb{P}_F \mid R \subseteq \mathcal{O}_P\}$$

Então valem

1. $\emptyset \neq S(R) \subsetneq \mathbb{P}_F$.
2. O fecho inteiro de R em F é $\text{ic}_F(R) = \mathcal{O}_{S(R)}$. Em particular, $\text{ic}_F(R)$ é um subanel integralmente fechado e de holomorfia de F/K cujo corpo quociente é F . ■

Demonstração. Por R não ser um corpo, existe um ideal próprio $\{0\} \neq I \subsetneq R$. Daí, pelo [Teorema 17](#), existe $P \in \mathbb{P}_F$ tal que $I \subseteq P$ e $R \subseteq \mathcal{O}_P$ e, portanto, $S(R) \neq \emptyset$. Por outro lado, temos que existe $x \in R$ que é transcendente sobre K . De fato, como R é subanel e como K é todo o corpo de constantes de F , de $K \subsetneq R$, temos que existe um elemento $x \in R \setminus K$ e tal elemento é transcendente sobre K . Como x tem pelo menos um pólo pelo [Teorema 18](#), e como qualquer pólo de x não está em $S(R)$, segue que $S(R) \subsetneq \mathbb{P}_F$. Com isso temos o item 1.

Da definição de $S(R)$ temos que $R \subseteq \mathcal{O}_{S(R)}$. Como $\mathcal{O}_{S(R)}$ é integralmente fechado, pela [proposição anterior](#), temos que $\text{ic}_F(R) \subseteq \mathcal{O}_{S(R)}$. Para mostrar a inclusão $\supseteq$, seja $z \in \mathcal{O}_{S(R)}$ e vamos mostrar que existe uma equação integral para z sobre R , i.e., que z é integral sobre R . Para tal, afirmamos que

$$z^{-1} \cdot R[z^{-1}] = R[z^{-1}] \quad (3.14)$$

onde $z^{-1} \cdot R[z^{-1}]$ é o ideal, em $R[z^{-1}]$, gerado por z^{-1} . Suponha que a [igualdade anterior](#) não seja válida, i.e., que $z^{-1}R[z^{-1}]$ é um ideal próprio de $R[z^{-1}]$. Nessas condições o [Teorema 17](#) nos dá um lugar $Q \in \mathbb{P}_F$ tal que

$$R \subset R[z^{-1}] \subseteq \mathcal{O}_Q \quad \text{e} \quad z^{-1} \in Q$$

Da parte em vermelho acima segue que $Q \in S(R)$ e da parte em azul segue que $z \notin Q$, e isso contradiz $z \in \mathcal{O}_{S(R)}$ e mostra a afirmação. Da afirmação cla, obtemos

$$1 = z^{-1} \cdot \sum_{i=0}^s a_i (z^{-1})^i \quad (3.15)$$

com $a_0, \dots, a_s \in R$. Multiplicando a [equação anterior](#) cla por z^{s+1} temos

$$z^{s+1} - \sum_{i=0}^s a_i z^{s-i} = 0$$

que é uma equação integral para z sobre R . Isso finaliza a demonstração do item 2. □

Corolário 72. Um subanel R de F/K com corpo quociente igual a F é integralmente fechado se, e somente se, R é um anel de holomorfia. ■

Demonstração. Se R é anel de holomorfia, então pela [Teorema 70](#), R é integralmente fechado. Reciprocamente, se R é integralmente fechado, então pelo [teorema anterior](#), $R = i_{CF}(R) = O_{S(R)}$ e, portanto, R é de holomorfia. □

Proposição 73. Seja O_S um anel de holomorfia de F/K . Então existe uma correspondência biunívoca entre S e o conjunto dos ideais maximais de O_S dada por

$$S \ni P \mapsto M_P \doteq P \cap O_S$$

Mais ainda, o mapa

$$\varphi : \begin{cases} O_S/M_P & \rightarrow F_P = O_P/P \\ x + M_P & \mapsto x + P \end{cases}$$

é um isomorfismo. ■

Proposição 74. Seja $S \subseteq \mathbb{P}_F$ um conjunto não vazio e finito de lugares de F/K . Então O_S é um domínio de ideais principais. ■

3.3 Base Integral local

O principal resultado dessa seção é um [teorema](#) devido a **Kummer** sobre ramificação de lugares em uma extensão finita F'/F do tipo $F' = F(y)$. Nessa seção F'/F será uma extensão finita e separável de corpos de funções.

Proposição 75. Seja R um subanel integralmente fechado de F/K cujo corpo quociente é F (ou seja, pelo [Teorema 72](#), R é um anel de holomorfia de F/K). Para $z \in F'$, seja $\varphi(T) \in F[T]$ seu polinômio minimal sobre F . Então

$$z \text{ é integral sobre } R \Leftrightarrow \varphi(T) \in R[T]$$

■

Demonstração. Da definição de elemento inteiro sobre R , é claro que $\varphi(T) \in R[T] \Rightarrow z$ é inteiro sobre R .

Para a recíproca, não podemos de imediato concluir que $\varphi(T) \in R[T]$: o polinômio minimal de z sobre F pode não nos dar uma equação integral para z sobre R . Para

concluirmos isso, vamos usar a hipótese de R ser integralmente fechado e ter corpo de frações igual a F o que, pelo Teorema 72, é equivalente a R ser um anel de holomorfia de F/K . Seja $f(T) \in R[T]$ tal que $f(z) = 0$. Como $\varphi(T) \in F[T]$ é o polinômio minimal de z sobre F , e como $f(z) = 0$, temos que $\varphi(T) | f(T)$ em $F[T]$, ou seja, existe $\psi(T) \in F[T]$ tal que $f(T) = \varphi(T) \cdot \psi(T)$. Seja $F'' \supseteq F'$ uma extensão finita de F contendo todas as raízes de $\varphi(T)$ e seja $R'' \doteq \text{ic}_{F'}(R)$ o fecho inteiro de R sobre F'' . Uma vez que qualquer raiz de $\varphi(T)$ é também uma raiz de $f(T)$, temos que todas as raízes de $\varphi(T)$ estão em R'' . Agora, sendo os coeficientes de $\varphi(T)$ dados por expressões polinomiais (simétricas) de suas raízes, temos que $\varphi(T) \in R''$. Por outro lado, $\varphi(T) \in F[T]$. Disso, concluimos que $\varphi(T) \in R''[T] \cap F[T]$. Ora, mas $R'' \cap F = R$ pois R é integralmente fechado (lembramos que seu corpo de frações que é F). Daí $\varphi(T) \in R[T]$.

□

Corolário 76. Nas mesmas hipóteses da proposição anterior, seja $\text{Tr}_{F'/F} : F' \rightarrow F$ o mapa traço de F' para F e seja $x \in F'$ inteiro sobre R . Então $\text{Tr}_{F'/F}(x) \in R$. ■

Antes de mostrarmos esse resultado, vale a pena recapitular a definição de mapa traço de uma extensão, bem como suas principais propriedades, que serão usadas ao longo do texto.

Seja M/L uma extensão finita de grau n . Caso M/L não seja separável, o mapa traço $\text{Tr}_{M/L} : M \rightarrow L$ é o mapa identicamente nulo. Então seja M/L uma extensão separável. Nesse caso o mapa traço $\text{Tr}_{M/L} : M \rightarrow L$ é uma transformação L -linear que não é identicamente nula e que descreveremos da seguinte maneira. Fixemos um corpo algebricamente fechado $\Psi \subseteq L$. Como M/L é separável e de grau n , existem n mergulhos de M/L em Ψ , i.e., n morfismos de corpos $\sigma_i : M \rightarrow \Psi$, $i = 1, \dots, n$, tais que $\sigma(a) = a$ para todo $a \in L$. Daí, para $x \in M$ temos que

$$\text{Tr}_{M/L}(x) = \sum_{i=1}^n \sigma_i(x) \quad (3.16)$$

Se $\varphi(T) = T^r + a_{r-1}T^{r-1} + \dots + a_1T + a_0 \in L[T]$ é o polinômio minimal de x sobre L , então

$$\text{Tr}_{M/L}(x) = -sa_{r-1} \quad (3.17)$$

onde $s \doteq [M : L(x)] = n/r$. O traço é “bem comportado” em torres de corpos:

$$\text{Tr}_{H/L}(x) = \text{Tr}_{M/L}(\text{Tr}_{H/M}(x)) \quad (3.18)$$

sempre que $H \supseteq M \supseteq L$.

Demonstração. [do Teorema 76]

Como x é inteiro sobre R e R é integralmente fechado, temos que o polinômio minimal $\varphi(T)$ de x sobre F é tal que $\varphi(T) \in R[T]$. Daí, de 3.17, fica claro que $\text{Tr}_{F'/F}(x) \in R$.

□

Proposição 77. Sejam M/L uma extensão de corpos finita e separável e $\{z_1, \dots, z_n\}$ uma base de M/L . Então existem elementos $z_1^*, \dots, z_n^*$ tais que

$$\text{Tr}_{M/L}(z_i z_j^*) = \delta_{ij}$$

(o δ_{ij} aqui usado denota o **delta de Kronecker**). Temos que $\{z_1^*, \dots, z_n^*\}$ é também uma base de M/L , chamada de base dual de $\{z_1, \dots, z_n\}$ com respeito ao traço. ■

Teorema 78. Sejam R um subanel integralmente fechado de F/K cujo corpo quociente é F e F'/F uma extensão de corpos finita de grau n . Seja $R' = \text{ic}_{F'}(R)$ o fecho inteiro de R em F' . Então

1. Para cada base $\{x_1, \dots, x_n\}$ de F'/F existem elementos $a_1, \dots, a_n \in R \setminus \{0\}$ tais que $a_1 x_1, \dots, a_n x_n \in R'$. Consequentemente, existem bases de F'/F que estão contidas em R' .
2. Se $\{z_1, \dots, z_n\} \subseteq R'$ é uma base de F'/F e $\{z_1^*, \dots, z_n^*\}$ denota sua base dual com respeito ao traço então

$$\sum_{i=1}^n R z_i \subseteq R' \subseteq \sum_{i=1}^n R z_i^*$$

3. Se além disso R for um domínio de ideais principais, então existe uma base $\{u_1, \dots, u_n\}$ de F'/F tal que

$$R' = \sum_{i=1}^n R u_i$$

■

Corolário 79. Sejam F'/F uma extensão de corpos finita e separável de F/K e $P \in \mathbb{P}_F$. Então o fecho inteiro $\mathcal{O}'_P$ de $\mathcal{O}_P$ em F' é

$$\mathcal{O}'_P = \bigcap_{P'|P} \mathcal{O}_{P'} \quad (3.19)$$

Existe uma base $\{u_1, \dots, u_n\}$ de F'/F tal que

$$\mathcal{O}'_P = \sum_{i=1}^n \mathcal{O}_P \cdot u_i \quad (3.20)$$

Uma base que satisfaz a [equação anterior](#) é dita ser uma **base integral** de $\mathcal{O}'_P$ sobre $\mathcal{O}_P$. Também diremos que $\{u_1, \dots, u_n\}$ é uma **base integral local** de F'/F para o lugar P .

Demonstração. Para a [primeira afirmação](#) basta notarmos que $S(\mathcal{O}_P) = \{P' \in \mathbb{P}_{F'} \mid P' \mid P\}$ (para notação, confira o [Teorema 71](#)) e que, pelo item 2 do [Teorema 71](#), $\text{ic}_{F'}(\mathcal{O}_P) = \mathcal{O}_{S(\mathcal{O}_P)}$. Daí, pelas definições de $\mathcal{O}_{S(\mathcal{O}_P)}$ e de $\mathcal{O}'_P$ segue que

$$\mathcal{O}'_P = \bigcap_{P' \mid P} \mathcal{O}_{P'}$$

A segunda afirmação segue do fato de $\mathcal{O}_P$ ser domínio de ideais principais (confira a [Teorema 74](#)) e do item [Item 3](#) do [Teorema 78](#).

□

Teorema 80. Seja F/K um corpo de funções e F'/F uma extensão de corpos finita e separável. Então cada base $\{z_1, \dots, z_n\}$ de F'/F é uma base integral local para quase todo (isto é, a menos de um número finito) de lugares $P \in \mathbb{P}_F$. ■

Observemos que o [Teorema 79](#) nos diz que dado um lugar $P \in \mathbb{P}_F$, existe uma base integral local de F'/F para P . O [teorema anterior](#) nos diz que dada a base, existe (na verdade existem infinitos) $P \in \mathbb{P}_F$ para o qual a base em questão é integral local para P .

Para o teorema a seguir, que é utilíssimo nas aplicações que faremos, usaremos as seguinte notações:

1. $\bar{F} \doteq F_P$ é o corpo residual de P .
2. $\bar{a} \doteq a(P)$ é a classe residual de $a \in \mathcal{O}_P$.
3. Se $\psi(T) = \sum c_i T^i$ é um polinômio com coeficientes em $\mathcal{O}_P$, colocamos

$$\bar{\psi}(T) \doteq \sum \bar{c}_i T^i \in \bar{F}[T]$$

Teorema 81 (TEOREMA DE KUMMER). Seja $F' = F(y)$ onde o elemento y é inteiro sobre $\mathcal{O}_P$ e denotemos por $\varphi(T) \in \mathcal{O}_P[T]$ (a pertinência anterior segue da [Teorema 75](#)) o polinômio minimal de y sobre F . Seja

$$\bar{\varphi}(T) = \prod_{i=1}^r \gamma_i(T)^{\varepsilon_i}$$

a decomposição de $\bar{\varphi}(T)$ em fatores irredutíveis sobre $\bar{F}$ (ou seja, os polinômios γ_i são irredutíveis, mônicos, dois a dois distintos em $\bar{F}[T]$ e $\varepsilon_i \geq 1$ para $i = 1, \dots, r$). Escolhamos polinômios mônicos $\varphi_i(T) \in O_P[T]$ tais que

$$\bar{\varphi}_i(T) = \gamma_i(T) \quad \text{e} \quad \deg \phi_i(T) = \deg \gamma_i(T)$$

(Notemos que tal escolha é claramente possível). Então para $1 \leq i \leq r$, existem lugares $P_i \in \mathbb{P}_{F'}$ satisfazendo

1. $P_i | P$,
2. $\varphi_i(y) \in P_i$ e
3. $f(P_i | P) \geq \deg \gamma_i(T)$.

Mais ainda: $P_i \neq P_j$ se $i \neq j$.

Sob hipóteses adicionais, temos mais resultados. Suponhamos que pelo menos umas das duas hipóteses abaixo sejam satisfeitas

$$\varepsilon_i = 1 \quad \text{para} \quad i = 1, \dots, r \tag{3.21}$$

ou

$$\{1, y, \dots, y^{n-1}\} \quad \text{é uma base integral local para} \quad P \tag{3.22}$$

Então existe, para $1 \leq i \leq r$, exatamente um lugar $P_i \in \mathbb{P}_{F'}$ com $P_i | P$ e $\varphi_i(y) \in P_i$. Os lugares $P_1, \dots, P_r$ são todos os lugares de F' acima de P e temos que

$$\text{Con}_{F'/F}(P) = \sum_{i=1}^r \varepsilon_i P_i$$

i.e., $\varepsilon_i = e(P_i | P)$. O corpo residual $F'_{P_i} = O_{P_i}/P_i$ é isomorfo a $\bar{F}[T]/(\gamma_i(T))$, logo $f(P_i | P) = \deg \gamma_i(T)$. ■

Demonstração. Colocamos $\bar{F}_i \doteq \bar{F}[T]/((\gamma_i(T)))$. Como os γ_i 's são irredutíveis, $\bar{F}_i/\bar{F}$ é uma extensão de corpos de grau

$$[\bar{F}_i : \bar{F}] = \deg \gamma_i(T) \tag{3.23}$$

Consideremos o anel $\mathcal{O}_P[y] = \sum_{i=0}^{n-1} \mathcal{O}_P y^i$ onde $n = \deg \varphi(T) = [F' : F]$. Temos os seguintes homomorfismos de aneis:

$$\rho : \begin{cases} \mathcal{O}_P[T] & \rightarrow & \mathcal{O}_P[y] \\ \sum c_j T^j & \mapsto & \sum c_j y^j \end{cases}$$

e

$$\pi_i : \begin{cases} \mathcal{O}_P[T] & \rightarrow & \bar{F}_i \\ \sum c_j T^j & \mapsto & \sum \bar{c}_j(T^j \bmod \gamma_i(T)) \end{cases}$$

para $i = 1, \dots, r$. O núcleo de ρ é o ideal (em $\mathcal{O}_P[T]$) gerado por $\varphi(T)$. Como

$$\pi_i(\varphi(T)) = \bar{\varphi}(T) \bmod \gamma_i(T) = 0$$

(pois $\gamma_i(T) | \bar{\varphi}(T)$ em $\bar{F}[T]$), vemos que $\text{Ker}(\rho) = \varphi(T) \cdot \mathcal{O}_P[T] \subseteq \text{Ker}(\pi_i)$. Com isso, temos que existe um único homomorfismo $\sigma_i : \mathcal{O}_P[y] \rightarrow \bar{F}_i$ que faz o seguinte diagrama comutar

$$\begin{array}{ccc} \mathcal{O}_P[T] & \xrightarrow{\pi_i} & \bar{F}_i \\ & \searrow \rho \quad \nearrow \sigma_i & \\ & \mathcal{O}_P[y] & \end{array}$$

De fato, para $z \in \mathcal{O}_P[y]$, temos, uma vez que ρ é claramente sobrejetor, que existe $f \in \mathcal{O}_P[T]$ tal que $\rho(f) = z$. Daí definimos

$$\sigma_i(z) \doteq \pi_i(f)$$

Temos que σ_i está bem definido pois $\text{Ker}(\rho) \subseteq \text{Ker}(\pi_i)$. É claro que σ_i é um homomorfismo e é o único que satisfaz $\pi_i = \sigma_i \circ \rho$. Temos que σ_i é dado explicitamente por

$$\sigma_i : \begin{cases} \mathcal{O}_P[y] & \rightarrow & \bar{F}_i \\ \sum c_j y^j & \mapsto & \sum \bar{c}_j(T^j \bmod \gamma_i(T)) \end{cases}$$

Disso é claro que σ_i é um epimorfismo, i.e., um homomorfismo sobrejetor. Afirmamos que

$$\text{Ker}(\sigma_i) = P \cdot \mathcal{O}_P[y] + \varphi_i(y) \cdot \mathcal{O}_P[y] \quad (3.24)$$

onde $P \cdot \mathcal{O}_P[y]$ é o ideal, em $\mathcal{O}_P[y]$, gerado por $P \subseteq \mathcal{O}_P$ e analogamente para $\varphi_i(y) \cdot \mathcal{O}_P[y]$. Ora, a inclusão $\text{Ker}(\sigma_i) \supseteq P \cdot \mathcal{O}_P[y] + \varphi_i(y) \cdot \mathcal{O}_P[y]$ é trivial uma vez que $\sigma_i(\varphi_i(y)) = \bar{\varphi}_i(T) \bmod \gamma_i(T) = 0 \bmod \gamma_i(T)$ e $\sigma_i(z) = \bar{z} = 0$ para $z \in P$ pois $\bar{F} = F_P \subset \bar{F}_i$.

Para mostrarmos a outra inclusão, tomemos um elemento $\sum_{j=0}^{n-1} c_j y^j \in \text{Ker}(\sigma_i)$. Então $\sigma_i(\sum_{j=0}^{n-1} c_j y^j) = \sum_{j=0}^{n-1} \bar{c}_j T^j \bmod \gamma_i(T) = 0$ em $\bar{F}_i[T] \Rightarrow \sum_{j=0}^{n-1} \bar{c}_j T^j = \bar{\varphi}_i(T) \bar{\psi}(T)$ em $\bar{F}[T]$ para algum $\psi(T) \in \mathcal{O}_P[T]$, lembrando que $\bar{\varphi}_i(T) = \gamma_i(T)$. Daí

$$\sum_{j=0}^{n-1} \bar{c}_j T^j - \bar{\varphi}_i(T) \bar{\psi}(T) = 0$$

em $\mathcal{O}_T/T$, ou seja

$$\sum_{j=0}^{n-1} c_j T^j - \varphi_i(T) \psi(T) \in P \cdot \mathcal{O}_P[T]$$

Fazendo $T = y$ na [expressão anterior](#) obtemos

$$\sum_{j=0}^{n-1} c_j y^j - \varphi_i(y) \psi(y) \in P \cdot \mathcal{O}_P[y]$$

e “passando” o termo contendo $\varphi_i(y)$ para o outro lado obtemos [3.24](#), como afirmamos.

Com isso, temo, pelo [Teorema 17](#), que existe um lugar $P_i \in \mathbb{P}_{F'}$ tal que $\text{Ker}(\sigma_i) \subseteq P_i$ e $\mathcal{O}_P[y] \subseteq \mathcal{O}_{P_i}$, pois $\mathcal{O}_P[y]$ é um subanel de F' (“vemos” F' como corpo de funções sobre K , i.e., o corpo de funções em questão é F'/K) tal que $K \subseteq \mathcal{O}_P[y] \subseteq F'$ e $\{0\} \neq P \cdot \mathcal{O}_P[y] + \varphi_i(y) \cdot \mathcal{O}_P[y]$ é um ideal próprio de $\mathcal{O}_P[y]$. De fato, para ver que $\text{Ker}(\sigma_i) = P \cdot \mathcal{O}_P[y] + \varphi_i(y) \cdot \mathcal{O}_P[y]$ é um ideal próprio de $\mathcal{O}_P[y]$, basta notar que se não fosse esse o caso, então $\sigma_i(z) = 0$ para todo $z \in \mathcal{O}_P[y]$. Mas $\sigma_i(1) = 1 \neq 0$.

Logo, como $P \subseteq \text{Ker}(\sigma_i) \subseteq P_i$, temos que $P_i|P$ e é claro que $\varphi_i(y) = 0 + \varphi_i(y) \cdot 1 \in P_i$. O corpo residual $\mathcal{O}_{P_i}/P_i$ contém $\mathcal{O}_P[y]/\text{Ker}(\sigma_i)$ pois $\mathcal{O}_P[y] \subset \mathcal{O}_{P_i}$ e $\text{Ker}(\sigma_i) \subset P_i$. Ora mas $\mathcal{O}_P[y]/\text{Ker}(\sigma_i) \simeq \bar{F}_i$. Daí, por [3.23](#) temos que

$$f(P_i|P) \geq [\bar{F}_i : \bar{F}] = \deg \gamma_i(T)$$

Mais do que isso, $\deg \gamma_i(T) | f(P_i|P)$.

$$f(P_i|P) \left[\begin{array}{c} F'_{P_i} = \mathcal{O}_{P_i}/P_i \\ | \\ \bar{F}_i = \bar{F}[T]/((\gamma_i(T))) \simeq \mathcal{O}_P[y]/\text{Ker}(\sigma_i) \\ | \\ \bar{F} = F_P \end{array} \right] \left[\begin{array}{l} [\bar{F}_i : \bar{F}] = \\ = \deg \gamma_i(T) \end{array} \right]$$

Para $i \neq j$ os polinômios $\gamma_i(T) = \bar{\varphi}_i(T)$ e $\gamma_j = \bar{\varphi}_j(T)$ são coprimos em $\bar{F}[T]$, logo podemos escrever

$$1 = \bar{\varphi}_i(T)\bar{\lambda}_i(T) + \bar{\varphi}_j(T)\bar{\lambda}_j(T)$$

para alguns $\lambda_i(T)$ e $\lambda_j(T) \in \mathcal{O}_P[T]$. Isso implica que (alguns T 's foram omitidos)

$$\begin{aligned} \overline{\varphi_i \lambda_i + \varphi_j \lambda_j - 1} = 0 \text{ em } \mathcal{O}_T/T &\Rightarrow \varphi_i \lambda_i + \varphi_j \lambda_j - 1 \in P \cdot \mathcal{O}_P[T] \Rightarrow \\ &\Rightarrow \varphi_i(y) \lambda_i(y) + \varphi_j(y) \lambda_j(y) - 1 \in P \cdot \mathcal{O}_P[y] \end{aligned}$$

Disso e de 3.24 concluímos que $1 \in \text{Ker}(\sigma_i) + \text{Ker}(\sigma_j)$. Como $\text{Ker}(\sigma_i) \subseteq P_i$ e $\text{Ker}(\sigma_j) \subseteq P_j$, temos que $1 \in P_i + P_j$, logo $P_i \neq P_j$ para $i \neq j$ (caso contrário, $1 \in P_i + P_j = P_i = P_j$ e $P_i = P_j$ não seria ideal maximal de $\mathcal{O}_{P_i} = \mathcal{O}_{P_j}$).

Agora suponhamos que valha a hipótese 3.21, i.e., que

$$\bar{\varphi}(T) = \prod_{i=1}^r \gamma_i(T)$$

onde, lembremos, os polinômios γ_i são irredutíveis e distintos. Temos então que

$$\begin{aligned} [F' : F] = \deg \varphi(T) &= \sum_{i=1}^r \overbrace{\deg \gamma_i(T)}^{=\deg \varphi_i(T)} \\ &\leq \sum_{i=1}^r f(P_i|P) \leq \sum_{i=1}^r e(P_i|P) f(P_i|P) \\ &\leq \sum_{P'|P} e(P'|P) f(P'|P) = [F' : F] \end{aligned}$$

A desigualdade em vermelho foi [demonstrada anteriormente](#). A igualdade em verde é a [IGUALDADE FUNDAMENTAL](#). Então todas as desigualdades anteriores são igualdades e,

mais do que isso, para $i = 1, \dots, r$ temos $e(P_i|P) = 1 = \varepsilon_i$, $f(P_i|P) = \deg \varphi_i(T)$ e os P_i 's, $i = 1, \dots, r$ são *todos* os lugares em F' acima de P .

Observemos que de $P_i \neq P_j$ para $i \neq j$, temos que $\varphi_i(y) \notin P_j$. Suponhamos que não, i.e., que $\varphi_i(y) \in P_j$ para algum $j \neq i$. Então temos que $\overline{\varphi_i(y)} = 0$ tanto em F_{P_i} quanto em F_{P_j} . Como F_{P_i} e F_{P_j} são iguais a $\bar{F}[T]/((\gamma_i(T)))$ e $\bar{F}[T]/((\gamma_j(T)))$, respectivamente, concluimos que y é raiz tanto de $\gamma_i(T)$ quanto de $\gamma_j(T)$, contradizendo o fato de serem $\gamma_i(T)$ e $\gamma_j(T)$ polinômios irredutíveis e distintos. Isso nos diz que para cada $i = 1, \dots, r$ existe exatamente um lugar $P_i|P$ tal que $\varphi_i(y) \in P_i$.

Finalmente, suponhamos que valha a hipótese 3.22. Como anteriormente escolhemos $P_i \in \mathbb{P}_{F'}$ tal que $P_i|P$ e $\varphi_i(y) \in P_i$, o que é possível pela “primeira parte” da demonstração. Afirmamos que $P_1 \dots, P_r$ são os únicos lugares em F' acima de P .

Seja $P' \in \mathbb{P}_{F'}$ com $P'|P$. Uma vez que

$$0 = \varphi(y) \equiv \prod_{i=1}^r \varphi_i(y)^{\varepsilon_i} \pmod{P \cdot \mathcal{O}_P[y]}$$

obtemos

$$\prod_{i=1}^r \varphi_i(y)^{\varepsilon_i} \in P'$$

De fato, como, por 3.22, $\{1, y, \dots, y^{n-1}\}$ é base integral de P , temos que $\mathcal{O}'_P = \sum_{i=0}^{n-1} \mathcal{O}_P y^i = \mathcal{O}_P[y]$ e como $\mathcal{O}'_P = \bigcap_{P'|P} \mathcal{O}_{P'}$ (confira o Teorema 79), temos que $\mathcal{O}_P[y] \subset \mathcal{O}_{P'}$ para todo $P'|P$. Logo $P \cdot \mathcal{O}_P[y] \subset P \mathcal{O}_{P'} \subset P' \mathcal{O}_{P'} = P'$ para todo $P'|P$. Agora, como P' é um ideal primo de $\mathcal{O}_{P'}$, temos que a equação anterior implica que $\varphi_i(y) \in P'$ para algum $i \in \{1, \dots, r\}$ e

$$P \cdot \mathcal{O}_P[y] + \varphi_i(y) \mathcal{O}_P[y] \subseteq P' \cap \mathcal{O}_P[y]$$

O lado esquerdo dessa inclusão é um ideal maximal de $\mathcal{O}_P[y]$ por 3.24 (pois $P \cdot \mathcal{O}_P[y] + \varphi_i(y) \mathcal{O}_P[y] = \text{Ker}(\sigma_i)$ e $\mathcal{O}_P[y]/\text{Ker}(\sigma_i) \simeq \bar{F}_i = \bar{F}[T]/((\gamma_i(T)))$ é um corpo). Logo, vale a igualdade em 3.3. Pela própria definição de P_i vista na “primeira parte” da demonstração, temos também que

$$P' \cap \mathcal{O}_P[y] = P_i \cap \mathcal{O}_P[y] = \varphi_i(y) \cdot \mathcal{O}_P[y] + P \cdot \mathcal{O}_P[y] \quad (3.25)$$

Uma vez que $\mathcal{O}_P[y]$ é o fecho inteiro de $\mathcal{O}_P$ em F' pela hipótese 3.22, a proposição Teorema 73 nos mostra que $P' = P_i$. De fato, temos que $\mathcal{O}_P[y] = \mathcal{O}'_P = \bigcap_{P'|P} \mathcal{O}_{P'} = \mathcal{O}_S$ com $S = \{P' \in \mathbb{P}_{F'} \mid P'|P\}$ é anel de holomorfia, e como $P' \cap \mathcal{O}_P[y]$ e $P_i \cap \mathcal{O}_P[y]$ são ambos ideais maximais, temos, pela Teorema 73, que $P' = P_i$.

Como consequência imediata da afirmação anterior e do [Teorema 79](#), vemos que

$$\mathcal{O}_P[y] = \bigcap_{i=1}^r \mathcal{O}_{P_i} \quad (3.26)$$

Pela [APROXIMAÇÃO FRACA](#), existem elementos $t_1, \dots, t_r \in F'$ tais que

$$v_{P_i}(t_j) = \delta_{ij}$$

(basta tomar, com a notação como no enunciado da [APROXIMAÇÃO FRACA](#), $x_{ik} = 0$ e $n_{ik} = \delta_{ik}$ para $k = 1, \dots, r$ e fazer isso para $i = 1, \dots, r$). Seja $t \in F$ um elemento primo de P , i.e., $P = (t)$ em $\mathcal{O}_P$. Então

$$t_i \in \mathcal{O}_P[y] \cap P_i = \varphi_i(y) \cdot \mathcal{O}_P[y] + t \cdot \mathcal{O}_P[y]$$

por [3.26](#) e [3.25](#). Então t_i pode ser escrito como

$$t_i = \varphi_i(y) \cdot a_i(y) + t \cdot b_i(y)$$

com $a_i(y)$ e $b_i(y) \in \mathcal{O}_P[y]$. Disso obtemos (o (y) foi omitido)

$$t_i^{\varepsilon_i} = (\varphi_i a_i + t b_i)^{\varepsilon_i} = \varphi_i^{\varepsilon_i} a_i^{\varepsilon_i} + t \tilde{b}_i$$

onde $\tilde{b}_i \in \mathcal{O}_P[y]$. Daí

$$\begin{aligned} \prod_{i=1}^r t_i^{\varepsilon_i} &= \prod_{i=1}^r (\varphi_i^{\varepsilon_i} a_i^{\varepsilon_i} + t \tilde{b}_i) = \prod_{i=1}^r a_i^{\varepsilon_i} \cdot \prod_{i=1}^r \varphi_i^{\varepsilon_i} + t \cdot b \\ &= a(y) \cdot \prod_{i=1}^r \varphi_i(y)^{\varepsilon_i} + t \cdot b(y) \end{aligned} \quad (3.27)$$

com $a(y)$ e $b(y) \in \mathcal{O}_P[y]$. Como

$$\prod_{i=1}^r \varphi_i(y)^{\varepsilon_i} \equiv \varphi(y) \pmod{P \cdot \mathcal{O}_P[y]} = t \cdot \mathcal{O}_P[y]$$

e como $\varphi(y) = 0$, temos que [3.27](#) implica (lembrando que $P \cdot \mathcal{O}_P[y] = t \mathcal{O}_P[y]$)

$$\prod_{i=1}^r t_i^{\varepsilon_i} = t \cdot u(y)$$

para algum $u(y) \in \mathcal{O}_P[y]$. Logo

$$\varepsilon_i = v_{P_i} \left(\prod_{j=1}^r t_j^{\varepsilon_j} \right) = v_{P_i}(t \cdot u(y)) = v_{P_i}(t) + v_{P_i}(u(y)) \geq v_{P_i}(t) = e(P_i|P) \quad (3.28)$$

(observe que de $u(y) \in \mathcal{O}_P[y] \subseteq \mathcal{O}_{P_i}$ temos que $v_{P_i}(u(y)) \geq 0$). Por outro lado, temos que

$$f(P_i|P) = \deg \gamma_i(T) \quad (3.29)$$

por 3.23, 3.24, 3.25 e pela Teorema 73 (notemos que a hipótese 3.22 é fundamental para que possamos usar a Teorema 73: ela garante que $\mathcal{O}_P[y]$ é anel de holomorfia). Daí, segue por 3.28, 3.29 e pela IGUALDADE FUNDAMENTAL que

$$[F' : F] = \sum_{i=1}^r e(P_i|P) f(P_i|P) \leq \sum_{i=1}^r \varepsilon_i \deg \gamma_i(T) = \deg \varphi(T) = [F' : F] \quad (3.30)$$

Portanto a desigualdade anterior é uma igualdade e segue que $\varepsilon_i = e(P_i|P)$ para $i = 1, \dots, r$ (e como anteriormente, temos que $\varphi_i(y) \notin P_j$ para $i \neq j$).

□

Observação 82. Notemos que dada uma extensão do tipo $F' = F(y)$, com y algébrico sobre F , sempre é possível “encontrarmos” um lugar P tal que o polinômio minimal de y sobre F , $\varphi(T) \in F[T]$ esteja em $\mathcal{O}_P[T]$, ou, equivalentemente, um lugar P tal que y seja inteiro sobre P . De fato, o polinômio minimal de y possui um número finito de coeficientes $a_0, \dots, a_{n-1}$. Cada um destes coeficientes, por sua vez, possui um número finito de zeros e pólos pelo Teorema 26. Se existir um lugar P que é zero de todos os coeficientes, podemos tomar este lugar para ser o lugar sobre o qual y é inteiro. Mas daí, $v_P(a_i) > 0 \Rightarrow a_i(P) = 0$ em F_P para $i = 0, \dots, n-1$ e nesse caso o polinômio $\bar{\varphi}(T)$ do TEOREMA DE KUMMER é identicamente nulo e não nos diz nada sobre a ramificação de P . Entretanto, independente de existir um lugar que seja zero de todos os coeficientes, podemos fazer o seguinte. Como cada coeficiente possui um número finito de zeros e pólos, o conjunto S de todos os zeros e todos os pólos de todos os coeficientes do polinômio minimal é finito. Mas, pelo Teorema 24, o conjunto $\mathbb{P}_F$ dos lugares de F é infinito. Então qualquer lugar $Q \in \mathbb{P}_F \setminus S \neq \emptyset$ é tal que $v_Q(a_i) = 0 \Rightarrow a_i(P) \neq 0$ em F_P para $i = 0, \dots, n-1$. Daí, para esses (infinitos) Q 's, o TEOREMA DE KUMMER nos diz muito sobre a ramificação de Q , desde que saibamos a fatoração de $\bar{\varphi}(T)$ em $F_Q[T]$. Por exemplo, se $\bar{\varphi}(T)$ “continuar” irredutível em $F_Q[T]$, então Q terá, pela IGUALDADE FUNDAMENTAL, apenas uma extensão cujo grau relativo é máximo.

3.4 O cotraço das diferenciais de Weil e a fórmula do gênero de Hurwitz

Nessa seção, F'/F denotará uma extensão finita e separável de corpos de funções. É claro que a respectiva extensão dos corpos de constante K'/K também é separável.

Vamos associar para cada diferencial de Weil de F/K uma diferencial de Weil de F'/K' . Essa associação nos levará a uma **fórmula utilíssima** que relaciona os gêneros de F e F' em termos dos graus das extensões F'/F e K'/K e do grau de um **divisor especial** de F' denominado o **diferente** da extensão F'/F . Como assumimos que F'/F é separável, o mapa traço $\text{Tr}_{F'/F}$ não é identicamente nulo.

Definição 83. Para $P \in \mathbb{P}_F$, seja $\mathcal{O}'_P \doteq \text{ic}_{F'}(\mathcal{O}_P)$ o fecho inteiro de $\mathcal{O}_P$ em F' . Então o conjunto

$$C_P \doteq \{z \in F' \mid \text{Tr}_{F'/F}(z \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P\} \quad (3.31)$$

é chamado de **módulo complementar sobre $\mathcal{O}_P$** . ■

Proposição 84. Com a notação como na definição anterior, temos que

1. C_P é um $\mathcal{O}'_P$ -módulo e $\mathcal{O}'_P \subseteq C_P$.
2. Se $\{z_1, \dots, z_n\}$ é uma base integral de $\mathcal{O}'_P$ sobre $\mathcal{O}_P$, então

$$C_P = \sum_{i=1}^n \mathcal{O}_P \cdot z_i^* \quad (3.32)$$

onde $\{z_1^*, \dots, z_n^*\}$ é a base dual de $\{z_1, \dots, z_n\}$.

3. Existe um elemento $t \in F'$ (dependendo de P) tal que $C_P = t \cdot \mathcal{O}'_P$. Mais ainda,

$$v_{P'}(t) \leq 0 \quad \forall P' \mid P \quad (3.33)$$

e para todo $t' \in F'$ temos que

$$C_P = t' \cdot \mathcal{O}'_P \Leftrightarrow v_{P'}(t') = v_{P'}(t) \quad \forall P' \mid P \quad (3.34)$$

4. $C_P = \mathcal{O}'_P$ para quase todo $P \in \mathbb{P}_F$. ■

Demonstração.

1. Que C_P é um $\mathcal{O}'_P$ -módulo é trivial. Uma vez que o traço de qualquer elemento $y \in \mathcal{O}'_P$ está em $\mathcal{O}_P$, pelo [Teorema 76](#), temos que $\mathcal{O}'_P \subseteq \mathcal{O}_P$.
2. Primeiramente, consideremos um elemento $z \in C_P$. Uma vez que $\{z_1^*, \dots, z_n^*\}$ é também uma base de F'/F (confira a [Teorema 77](#)), existem $x_1, \dots, x_j \in F$ tais que $z = \sum_{i=1}^n x_i z_i^*$. Para mostrarmos a inclusão $\subseteq$, basta mostrarmos que $x_j \in \mathcal{O}_P$ para $i = 1, \dots, n$. Ora, uma vez que $z \in C_P$ e $z_1, \dots, z_n \in \mathcal{O}'_P$, segue que $\text{Tr}_{F'/F}(zz_j) \in \mathcal{O}_P$ para $j = 1, \dots, n$. Mas também temos que

$$\text{Tr}_{F'/F}(zz_j) = \text{Tr}_{F'/F}\left(\sum_{i=1}^n x_i z_i^* z_j\right) = \sum_{i=1}^n x_i \cdot \text{Tr}_{F'/F}(z_i^* z_j) = x_j$$

ou seja, $x_j \in \mathcal{O}_P$ e portanto $z \in \sum_{i=1}^n \mathcal{O}_P z_i^*$.

Reciprocamente, seja $z \in \sum_{i=1}^n \mathcal{O}_P z_i^*$ e $u \in \mathcal{O}'_P$, digamos, $z = \sum_{i=1}^n x_i z_i^*$ e $u = \sum_{j=1}^n y_j z_j$ com x_i e $y_j \in \mathcal{O}_P$. Então

$$\begin{aligned} \text{Tr}_{F'/F}(zu) &= \text{Tr}_{F'/F}\left(\sum_{i,j=1}^n x_i y_j z_i^* z_j\right) \\ &= \sum_{i,j=1}^n x_i y_j \cdot \text{Tr}_{F'/F}(z_i^* z_j) = \sum_{i=1}^n x_i y_i \in \mathcal{O}_P \end{aligned}$$

de modo que $z \in C_P$.

3. Pelo resultado do [item anterior](#) e pelo [Teorema 79](#) sabemos que $C_P = \sum_{i=1}^n \mathcal{O}_P u_i$ para elementos $u_i \in F'$ apropriados. Escolhamos $x \in F$ tal que

$$v_P(x) \geq v_{P'}(u_i)$$

para todo $P'|P$ e para $i = 1, \dots, n$ (tal escolha é obviamente possível: basta tomarmos uma potência suficientemente grande de um elemento primo de P). Então

$$v_{P'}(xu_i) = e(P'|P) \cdot v_P(x) + v_{P'}(u_i) \geq 0$$

para todo $P'|P$ e para $i = 1, \dots, n$. Daí $x \cdot C_P \subseteq \mathcal{O}'_P$, desde que lembremos que $\mathcal{O}'_P = \{u \in F' \mid v_{P'} \geq 0 \forall P'|P\}$ pelo [Teorema 79](#). Mais do que $x \cdot C_P \subseteq \mathcal{O}'_P$, temos que $x \cdot C_P$ é um ideal de $\mathcal{O}'_P$ e, como $\mathcal{O}'_P$ é um domínio de ideais principais (confira a [Teorema 74](#)), temos que $x \cdot C_P = y \cdot \mathcal{O}'_P$ para algum $y \in \mathcal{O}'_P$. Colocando $t \doteq x^{-1}y$ temos que $C_P = t \cdot \mathcal{O}'_P$. Como $1 \in C_P$, pelo [Teorema 76](#) e pela [própria definição](#) de C_P , temos que $1 = t \cdot a$, donde vem que $-v_{P'}(t) = v_{P'}(a) \geq 0$, para todo $P'|P$, ou seja $v_{P'}(t) \leq 0$, para todo lugar de F' acima de P . Finalmente, temos, para $t' \in F'$

$$\begin{aligned}
t \cdot \mathcal{O}'_P = t' \mathcal{O}'_P &\Leftrightarrow tt'^{-1} \text{ e } t^{-1}t' \in \mathcal{O}'_P \\
&\Leftrightarrow v_{P'}(tt'^{-1}) \text{ e } v_{P'}(t^{-1}t') \geq 0 \quad \forall P'|P \\
&\Leftrightarrow v_{P'}(t) = v_{P'}(t') \quad \forall P'|P
\end{aligned}$$

onde, na equivalência em vermelho, usamos o fato que $v_{P'}(tt'^{-1}) = -v_{P'}(t^{-1}t')$ pois $tt'^{-1} = (t^{-1}t')^{-1}$, donde segue, pela afirmação verde, que $v_{P'}(tt'^{-1}) = 0 = v_{P'}(t^{-1}t')$.

4. Escolhamos uma base $\{z_1, \dots, z_n\}$ de F'/F . Pelo Teorema 80, $\{z_1, \dots, z_n\}$ e $\{z_1^*, \dots, z_n^*\}$ são bases integrais locais para quase todos os lugares $P \in \mathbb{P}_F$. Daí, usando o resultado do item anterior, vemos que $C_P = \mathcal{O}'_P$ para quase todo $P \in \mathbb{P}_F$.

□

Definição 85. Consideremos um lugar $P \in \mathbb{P}_F$ e o fecho inteiro $\mathcal{O}'_P$ de $\mathcal{O}_P$ em F' . Seja $C_P = t \cdot \mathcal{O}'_P$ o módulo complementar sobre $\mathcal{O}_P$. Então, para $P'|P$, definimos o expoente do (divisor) diferente de P' sobre P por

$$d(P'|P) \doteq -v_{P'}(t) \quad (3.35)$$

Pela Teorema 84, $d(P'|P)$ está bem definido e $d(P'|P) \geq 0$. Pelo item 4 da mesma proposição, temos que $d(P'|P) = 0$ para quase todo $P \in \mathbb{P}_F$ (e qualquer que seja $P'|P$), pois $C_P = \mathcal{O}'_P \Rightarrow v_{P'}(t) = v_{P'}(1) = 0$ qualquer que seja $P'|P$. Com isso, podemos definir o seguinte divisor

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

Tal divisor será chamado de **diferente** de F'/F . Notemos que o diferente é um divisor efetivo. ■

Vale a pena comentar que o expoente do diferente *não necessariamente* é igual para lugares $P'|P$ e $P''|P$ distintos, i.e., não necessariamente temos $d(P'|P) = d(P''|P)$ para lugares P' e P'' acima de P distintos.

Observação 86. Das definições anteriores, é fácil ver que para todo $z \in F'$ temos

$$z \in C_P \Leftrightarrow v_{P'}(z) \geq -d(P'|P) \quad \forall P'|P$$

Nesse ponto, aconselhamos o leitor a relembrar as definições 41, 42 e 43 do capítulo 2.

Definição 87. Seja

$$\mathcal{A}_{F'/F} \doteq \{\alpha \in \mathcal{A}_{F'} \mid \alpha_{P'} = \alpha_Q \text{ sempre que } P' \cap F = Q' \cap F\}$$

Notemos que a condição $P' \cap F = Q' \cap F$ significa que P' e Q' estão acima do mesmo lugar de F . $\mathcal{A}_{F'/F}$ é um F' -subespaço de $\mathcal{A}_{F'}$. Extendemos o mapa traço $\text{Tr}_{F'/F} : F' \rightarrow F$ a uma transformação F -linear (que denotaremos por $\text{Tr}_{F'/F}$) de $\mathcal{A}_{F'/F}$ para $\mathcal{A}_F$ bastando para isso colocar

$$(\text{Tr}_{F'/F}(\alpha))_P \doteq \text{Tr}_{F'/F}(\alpha_{P'}) \text{ para } \alpha \in \mathcal{A}_{F'/F}$$

onde P' é qualquer lugar de F' acima de P . Note que tal definição é consistente com as definições de adele do capítulo 2. Temos então que $\text{Tr}_{F'/F}(\alpha)$ é um adele de F/K e, claramente, o traço do adele principal $z \in F'$ é o adele principal de $\text{Tr}_{F'/F}(z)$.

Finalmente, definimos para $A' \in \text{Div}(F')$

$$\mathcal{A}_{F'/F}(A') \doteq \mathcal{A}_{F'}(A') \cap \mathcal{A}_{F'/F}$$

■

Teorema 88. Com a notação como na [definição anterior](#), temos que para cada diferencial de Weil ω de F/K existe uma única diferencial de Weil ω' de F'/K' tal que

$$\text{Tr}_{K'/K}(\omega'(\alpha)) = \omega(\text{Tr}_{F'/F}(\alpha)), \forall \alpha \in \mathcal{A}_{F'/F}$$

Tal diferencial ω' será denominada **cotraço** de ω em F'/F e denotada por $\text{Cotr}_{F'/F}(\omega)$.

Se $0 \neq \omega \in \Omega_F$ e $(\omega) \in \text{Div}(F)$ é seu correspondente divisor canônico, então vale

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

■

Proposição 89.

1. Se ω, ω_1 e ω_2 são diferenciais de Weil de F/K e $x \in F$, então

$$\text{Cotr}_{F'/F}(\omega_1 + \omega_2) = \text{Cotr}_{F'/F}(\omega_1) + \text{Cotr}_{F'/F}(\omega_2)$$

e

$$\text{Cotr}_{F'/F}(x\omega) = x \cdot \text{Cotr}_{F'/F}(\omega)$$

2. Seja F''/F' outra extensão de corpos finita e separável. Então

$$\text{Cotr}_{F''/F}(\omega) = \text{Cotr}_{F''/F'}(\text{Cotr}_{F'/F}(\omega))$$

qualquer que seja a diferencial de Weil ω de F/K .

Corolário 90 (TRANSITIVIDADE DO DIFERENTE). Se $F'' \supseteq F' \supseteq F$ são extensões de corpos finitas e separáveis, então valem

1. $\text{Diff}(F''/F) = \text{Con}_{F''/F'}(\text{Diff}(F'/F)) + \text{Diff}(F''/F')$
2. $d(P''|P) = e(P''|P) \cdot d(P'|P) + d(P''|P')$, sendo $P'' \supseteq P' \supseteq P$ lugares de F'' , F' e F , respectivamente.

Teorema 91 (FÓRMULA DO GÊNERO DE HURWITZ). Seja F/K um corpo de funções algébricas de gênero g e seja F'/F uma extensão de corpos finita e separável. Seja K' o corpo das constantes de F' e g' o gênero de F'/K' . Então temos que

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

Demonstração. Escolhamos uma diferencial de Weil $\omega \neq 0$ de F/K . Segue do [Teorema 88](#) que

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

O grau de qualquer divisor canônico é $2g - 2$ pelo [Teorema 47](#). Obtemos, daí, pela [equação anterior](#) e pelo [Teorema 64](#)

$$\begin{aligned} 2g' - 2 &= \deg \text{Con}_{F'/F}((\omega)) + \deg \text{Diff}(F'/F) \\ &= \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg \text{Diff}(F'/F) \end{aligned} \tag{3.36}$$

□

3.5 O diferente

Nessa seção, como na anterior, as extensões tratadas serão finitas e separáveis. Lembremos que também assumimos que o corpo K é perfeito.

Para $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ com $P'|P$, definimos (confira as definições 56 e 85) o índice de ramificação $e(P'|P)$ e o expoente do diferente $d(P'|P)$. O seguinte teorema apresenta uma relação entre estes dois números.

Teorema 92 (TEOREMA DO DIFERENTE DE DEDEKIND). Com a notação como acima, temos, para todo $P'|P$

1. $d(P'|P) \geq e(P'|P) - 1$
2. $d(P'|P) = e(P'|P) - 1$ se, e somente se, $e(P'|P)$ não é divisível por $\text{char } K$. Em particular, se $\text{char } K = 0$, então $d(P'|P) = e(P'|P) - 1$. ■

Observação 93. Pelo [teorema anterior](#), temos que se $P'|P$ é não ramificado, ou seja se $e(P'|P) = 1$, então P' não está no suporte do diferente. Isso nos ajuda a calcular o gênero de F' com a [FÓRMULA DO GÊNERO DE HURWITZ](#). ■

Para a demonstração do item 1, precisaremos do seguinte

Lema 94. Sejam F^*/F uma extensão algébrica de corpos de funções, $P \in \mathbb{P}_F$ e $P^* \in \mathbb{P}_{F^*}$. Seja, também, σ um automorfismo de F^*/F . Então, $\sigma(P^*) \doteq \{\sigma(z) \mid z \in P^*\}$ é um lugar de F^* e temos que

1. $v_{\sigma(P^*)}(y) = v_{P^*}(\sigma^{-1}(y))$ para todo $y \in F^*$,
2. $\sigma(P^*)|P$ e
3. $e(\sigma(P^*)|P) = e(P^*|P)$ e $f(\sigma(P^*)|P) = f(P^*|P)$. ■

Demonstração. [do item 1 do [TEOREMA DO DIFERENTE DE DEDEKIND](#)]

Pela [Teorema 86](#), temos que $t \in C_P \Leftrightarrow d(P'|P) \geq -v_{P'}(t)$ para todo $P'|P$, onde C_P denota o módulo complementar sobre $\mathcal{O}_P$. Então, se conseguirmos mostrar que existe um elemento $t \in F'$ tal que $t \in C_P$ e tal que $v_{P'}(t) = 1 - e(P'|P)$ para todo $P'|P$, a equivalência anterior nos garantirá que o item 1 é válido. Ora, a [APROXIMAÇÃO FRACA](#) garante que existe um elemento $t \in F'$ tal que $v_{P'}(t) = 1 - d(P'|P)$ para todo $P'|P$. Resta mostrarmos que $t \in C_P$, ou seja, que $\text{Tr}_{F'/F}(t \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P$, onde, como de costume, $\mathcal{O}'_P$ denota o fecho inteiro de $\mathcal{O}_P$ em F' .

Para isso, consideramos uma extensão de Galois finita F^*/F tal que $F \subseteq F' \subseteq F^*$. Como F'/F é finita e separável, dos $[F^* : F]$ F -automorfismos, temos $[F' : F] = n$ cujas restrições a F' são distintas entre si e que denotaremos por $\sigma_1, \dots, \sigma_n$. Daí, para $z \in \mathcal{O}'_P$, temos que

$$\text{Tr}_{F'/F}(tz) = \sum_{i=1}^n \sigma_i(tz) \quad (3.37)$$

Seja P^* um lugar de F^* acima de P e coloquemos $P_i^* \doteq \sigma_i^{-1}(P^*)$ e $P'_i \doteq P_i^* \cap F'$. É claro que P_i^* e, portanto, P'_i estão acima de P . Notemos que, por $z \in \mathcal{O}'_P$ temos que $\sigma_i(z) \in \mathcal{O}'_P$ também. De fato, se $f(z)$ é uma equação integral para z sobre $\mathcal{O}_P$ então $\sigma_i(f(z)) = f(\sigma_i(z)) = 0$. Com isso, $v_{P^*}(z) \geq 0$. Daí

$$\begin{aligned}
 v_{P^*}(\sigma_i(tz)) &= v_{P^*}(\sigma_i(t)) + v_{P^*}(\sigma_i(z)) \\
 &\geq v_{P^*}(\sigma_i(t)) = v_{P_i^*}(t) && \text{pelo Teorema 94} \\
 &= e(P_i^*|P'_i) \cdot v_{P'_i}(t) \\
 &= e(P_i^*|P'_i) \cdot (1 - e(P'_i|P)) \\
 &> -e(P_i^*|P'_i) \cdot e(P'_i|P) \\
 &= -e(P_i^*|P) \\
 &= -e(P^*|P) && \text{pelo Teorema 94}
 \end{aligned}$$

Daí, usando 3.37, e a desigualdade triangular, temos que

$$-e(P^*|P) < v_{P^*}(\text{Tr}_{F'/F}(tz)) = e(P^*|P) \cdot v_P(\text{Tr}_{F'/F}(tz)) \quad (3.38)$$

o que implica que $\text{Tr}_{F'/F}(tz) \geq 0$, ou seja, $\text{Tr}_{F'/F}(tz) \in \mathcal{O}_P$. Como $z \in \mathcal{O}'_P$ foi escolhido arbitrariamente, temos que $\text{Tr}_{F'/F}(t \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P$.

□

Já para o item 2, usaremos o seguinte

Lema 95. Seja $P \in \mathbb{P}_F$ e $P_1, \dots, P_r \in \mathbb{P}_{F'}$ todos os lugares acima de P . Consideremos os corpos residuais $k \doteq \mathcal{O}_P/P$ e $k_i \doteq \mathcal{O}_{P_i}/P_i \supseteq k$ e as correspondentes projeções $\pi : \mathcal{O}_P \rightarrow k$ e $\pi_i : \mathcal{O}_{P_i} \rightarrow k_i$. Então, sendo $\mathcal{O}'_P$ o fecho inteiro de $\mathcal{O}_P$ em F' , temos para todo $u \in \mathcal{O}'_P$

$$\pi(\text{Tr}_{F'/F}(u)) = \sum_{i=1}^r e(P_i|P) \cdot \text{Tr}_{k_i/k}(\pi_i(u)) \quad (3.39)$$

■

Notemos que as extensões k_i/k são separáveis uma vez que K é perfeito.

Demonstração. [do item 2 do TEOREMA DO DIFERENTE DE DEDEKIND]

Mantemos a notação do lema anterior e colocamos $e_i \doteq e(P_i|P)$, $P' \doteq P_1$ e $e \doteq e(P'|P) = e_1$. Devemos mostrar que

$$d(P'|P) = e - 1 \Leftrightarrow \text{char } K \nmid e$$

Primeiramente, vamos mostrar $\Leftarrow$. Então suponhamos que $\text{char } K \nmid e$ e que $d(P'|P) \geq e$. Se “chegarmos” a uma contradição, o item 1 nos dará $d(P'|P) = e - 1$. Como $d(P'|P) \geq e$, a [Teorema 86](#) nos diz que existe algum $w \in F'$ tal que

$$v_{P'}(w) \leq -e \quad \text{e} \quad \text{Tr}_{F'/F}(w \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P \quad (3.40)$$

Como a extensão k_1/k é separável, existe $y_0 \in \mathcal{O}_{P'}$ tal que $\text{Tr}_{k_1/k}(\pi_1(y_0)) \neq 0$. Pela [APPROXIMAÇÃO FRACA](#), existe $y \in F'$ tal que

$$v_{P'}(y - y_0) > 0 \quad (3.41)$$

e, para $i = 2, \dots, r$

$$v_{P_i}(y) \geq \max\{1, e_i + v_{P_i}(w)\} > 0 \quad (3.42)$$

Temos que $y \in \mathcal{O}'_P$ e, pelo [Teorema 95](#)

$$\begin{aligned} \pi(\text{Tr}_{F'/F}(y)) &= e \cdot \text{Tr}_{k_1/k}(\pi_1(y)) + \sum_{i=2}^r e_i \cdot \overbrace{\text{Tr}_{k_i/k}(\pi_i(y))}^{=0 \text{ por 3.42}} \\ &= e \cdot \text{Tr}_{k_1/k} \underbrace{(\pi_1(y_0))}_{=\pi_1(y) \text{ por 3.41}} \neq 0 \end{aligned}$$

Na última desigualdade anterior, usamos o fato que $\text{char } K \nmid e$, i.e., $e \neq 0$ em k . Disso concluímos que

$$v_P(\text{Tr}_{F'/F}(y)) = 0$$

Agora, tomemos $x \in F$ com $v_P(x) = 1$, i.e., um elemento primo de P . Então

$$\text{Tr}_{F'/F}(x^{-1}y) = \underbrace{x^{-1}}_{\notin \mathcal{O}_P} \cdot \overbrace{\text{Tr}_{F'/F}(y)}^{\in \mathcal{O}_P} \notin \mathcal{O}_P \quad (3.43)$$

Por outro lado temos que $x^{-1}yw^{-1} \in \mathcal{O}'_{P'}$, pois

$$v_{P'}(x^{-1}yw^{-1}) = -e + v_{P'}(y) - v_{P'}(w) \geq 0$$

e

$$v_{P_i}(x^{-1}yw^{-1}) = v_{P_i}(y) - (e_i + v_{P'}(w)) \geq 0$$

para $i = 2, \dots, r$ por 3.40 e 3.42. Segue então que $x^{-1}y \in w \cdot \mathcal{O}'_P$ e que $\text{Tr}_{F'/F}(x^{-1}y) \in \mathcal{O}_P$, por 3.40. Mas isso contradiz 3.43 e termina a demonstração de $\Leftarrow$.

Para $\Rightarrow$, supomos que $\text{char } K \mid e$. Daí, basta mostrarmos que $d(P'|P) \geq e$. Escolhamos $u \in F'$, usando a APROXIMAÇÃO FRACA, tal que

$$v_{P'}(u) = -e \quad \text{e} \quad v_{P_i}(u) \geq -e_i + 1$$

para $i = 2, \dots, r$. Como anteriormente, $x \in F$ será um elemento primo de P . Para cada $z \in \mathcal{O}'_P$ temos que

$$v_{P'}(xuz) \geq 0 \quad \text{e} \quad v_{P_i}(xuz) > 0$$

para $i = 2, \dots, r$. Daí $xuz \in \mathcal{O}'_P$ e pelo Teorema 95

$$\begin{aligned} \pi(\text{Tr}_{F'/F}(xuz)) &= e \cdot \text{Tr}_{k_1/k}(\pi_1(xuz)) + \sum_{i=2}^r e_i \cdot \overbrace{\text{Tr}_{k_i/k}(\pi_i(xuz))}^{=0} \\ &= e \cdot \text{Tr}_{k_1/k}(\pi_1(xuz)) = 0 \end{aligned}$$

Com isso concluímos que $x \cdot \text{Tr}_{F'/F}(uz) = \text{Tr}_{F'/F}(xuz) \in P = x \cdot \mathcal{O}_P$ e, daí, $\text{Tr}_{F'/F}(uz) \in \mathcal{O}_P$, qualquer que seja $z \in \mathcal{O}'_P$. Logo, $u \in C_P$ e, pela Teorema 86, $-e = v_{P'}(u) \geq -d(P'|P)$.

□

Definição 96. Seja F'/F uma algébrica de corpos de funções e $P \in \mathbb{P}_F$.

1. Diremos que uma extensão de lugares $P'|P$ é ramificada se $e(P'|P) > 1$. Caso contrário, diremos que a extensão $P'|P$ é não ramificada.
2. Diremos que P é **ramificado** em F'/F se existir pelo menos um lugar $P' \in \mathbb{P}_{F'}$ acima de P tal que $e(P'|P) > 1$. Diremos ainda que a ramificação de P é **mansa** caso $\text{char } K \nmid e(P'|P)$ e que a ramificação de P é **selvagem** caso contrário.
3. Diremos que P é não ramificado em F'/F se $e(P'|P) = 1$ qualquer que seja $P'|P$, com $P' \in \mathbb{P}_{F'}$.
4. Diremos que P é totalmente ramificado em F'/F se existir apenas um lugar $P' \in \mathbb{P}_{F'}$ acima de P cujo índice de ramificação seja, pela IGUALDADE FUNDAMENTAL, $e(P'|P) = [F' : F]$.
5. Diremos que F'/F é ramificada, respectivamente não ramificada, se pelo menos um $P \in \mathbb{P}_F$ é ramificado em F'/F , respectivamente todo $P \in \mathbb{P}_F$ é não ramificado em

F'/F . Caso F'/F seja ramificada, diremos que F'/F é mansa se nenhum dos $P \in \mathbb{P}_F$ que são ramificados for de ramificação selvagem. ■

O corolário a seguir pode ser visto como uma reformulação do **TEOREMA DO DIFERENTE DE DEDEKIND**.

Corolário 97. Seja F'/F uma extensão de corpos finita e separável de corpos de funções algébricas.

1. Se $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ é tal que $P'|P$, então $P'|P$ é ramificada se, e somente se, $P' \leq \text{Diff}(F'/F)$. (Lembremos que o divisor $\text{Diff}(F'/F)$ é efetivo). Se $P'|P$ é ramificado, então

$$\begin{aligned} d(P'|P) = e(P'|P) - 1 &\Leftrightarrow P'|P \text{ é mansamente ramificado} \\ d(P'|P) \geq e(P'|P) &\Leftrightarrow P'|P \text{ é selvagemmente ramificado} \end{aligned}$$

2. Quase todos os lugares $P \in \mathbb{P}_F$ são não ramificados em F'/F . Mais precisamente, todo lugar fora do suporte de $\text{Diff}(F'/F)$ é não ramificado. ■

Corolário 98. Seja F'/F uma extensão de corpos finita e separável de corpos de funções algébricas cujos corpos de constantes sejam iguais. Sejam g e g' os gêneros de F/K e de F'/K , respectivamente. Então

$$2g' - 2 \geq [F' : F] \cdot (2g - 2) + \sum_{P \in \mathbb{P}_F} \sum_{P'|P} (e(P'|P) - 1) \cdot \deg P'$$

Além disso, a igualdade é válida se, e somente se, F'/F é mansa (por exemplo, se K for de característica 0). ■

Corolário 99. Seja F'/F uma extensão finita e separável de corpos de funções cujos corpos de constantes sejam iguais. Sejam g e g' os gêneros de F/K e F'/K , respectivamente. Então $g' \geq g$. ■

Proposição 100 (TEOREMA DE LÜROTH). Todo subcorpo de um corpo de funções racional $K(x)/K$ é um corpo de funções racional, i.e., se $K \subsetneq F_0 \subsetneq K(x)$, então $F_0 = K(y)$ para algum $y \in F_0$. ■

O próximo resultado é útil para o cálculo do diferente de uma extensão F'/F .

Teorema 101. Seja $F' = F(y)$ uma extensão de corpos finita e separável de um corpo de funções F de grau $[F' : F] = n$. Seja $P \in \mathbb{P}_F$ tal que o polinômio minimal de y sobre F , $\varphi(T)$, esteja em $\mathcal{O}_P[T]$ (ou seja, y é inteiro sobre $\mathcal{O}_P$; confira a **Teorema 82**) e sejam $P_1, \dots, P_r \in \mathbb{P}_{F'}$ todos os lugares de F' acima de P . Então vale o seguinte

1. $d(P_i|P) \leq v_{P_i}(\varphi'(y))$ para $1 \leq i \leq r$.
2. $\{1, y, \dots, y^{n-1}\}$ é uma base integral de F'/F para o lugar P se, e somente se, $d(P_i|P) = v_{P_i}(\varphi'(y))$ para $1 \leq i \leq r$.

Aqui, $\varphi'(T)$ denota a derivada (formal) do polinômio $\varphi(T)$. ■

A próxima proposição oferece um critério que nos permite saber quando as potências de um dado elemento formam uma base integral local para um dado lugar P .

Proposição 102. Seja F'/F uma extensão finita e separável de corpos de funções algébricas, $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ com $P'|P$. Suponha que $P'|P$ é totalmente ramificada, i.e., $e(P'|P) = [F' : F] = n$. Seja $t \in F'$ um elemento primo de P' e consideremos o polinômio minimal $\varphi(T) \in F[T]$ de t sobre F . Então $d(P'|P) = v_{P'}(\varphi'(t))$ e $\{1, t, \dots, t^{n-1}\}$ é uma base integral local de F'/F para P . ■

A [proposição acima](#) juntamente com o item 2 do [Teorema 101](#), é uma poderosa ferramenta para o cálculo do diferente.

3.6 Extensões de corpo de constantes

Lembremos que $\Phi \supseteq F$ é um corpo algebricamente fechado fixado. Seja K'/K uma extensão algébrica (com $K' \subseteq \Phi$). O compósito $F' \doteq FK'$ é um corpo de funções sobre K' e, portanto, seu corpo de constantes é uma extensão finita de K' (confira o [Teorema 14](#)). Mas na verdade vale a seguinte

Proposição 103. Seja $F' = FK'$ uma extensão algébrica de corpo de constantes de F/K (de grau finito ou infinito). Então temos que:

1. K' é todo o corpo de constantes de F' .
2. Qualquer subconjunto linearmente independente sobre K continua linearmente independente sobre K' .
3. $[F : K(x)] = [F' : K'(x)]$ para qualquer elemento $x \in F \setminus K$. (Note que, como K'/K é algébrica, se x é transcendente sobre K , x também será sobre K'). ■

Para a demonstração da [proposição anterior](#) usaremos o seguinte

Lema 104. Suponha que $\alpha \in \Phi$ é algébrico sobre K . Então $[K(\alpha) : K] = [F(\alpha) : F]$.

Demonstração. [da [Teorema 103](#)]

1. Seja $\gamma \in F'$ algébrico sobre K' . Então, γ é algébrico sobre K e como $\gamma \in F' = FK'$ podemos escrever

$$\gamma = \frac{\sum_{i=1}^r a_i b_i}{\sum_{j=1}^s c_j d_j} \quad (3.44)$$

onde os a_i 's e os c_j 's pertencem a K' e os b_i 's e os d_j 's pertencem a F . Com isso, vemos que $\gamma \in F(a_1, \dots, a_r, c_1, \dots, c_s)$. Como K é perfeito e K'/K é algébrica, a extensão $K(a_1, \dots, a_r, c_1, \dots, c_s)/K$ é finita e separável daí, pelo teorema do elemento primitivo, $K(a_1, \dots, a_r, c_1, \dots, c_s) = K(\alpha)$ para algum $\alpha \in K'$. Agora, γ é algébrico sobre K' e, conseqüentemente, sobre K , a extensão $K(\alpha, \gamma)/K$ também é finita e separável daí, novamente pelo teorema do elemento primitivo, $K(\alpha, \gamma) = K(\beta)$ para algum $\beta \in F'$. Disso segue que $F(\alpha, \gamma) = F(\beta)$. Ora, mas como $\gamma \in F(a_1, \dots, a_r, c_1, \dots, c_s) = F(\alpha)$, temos que $F(\alpha)F(\beta)$. Daí pelo [lema anterior](#), segue que

$$[K(\beta) : K] = [F(\beta) : F] = [F(\alpha) : F] = [K(\alpha) : K]$$

e disso segue imediatamente que $K(\alpha) = K(\beta)$ e portanto, $\gamma \in K(\beta) = K(\alpha) \subseteq K'$.

2. Sejam $y_1, \dots, y_r \in F$ linearmente independentes sobre K e

$$\sum_{i=1}^r \gamma_i y_i = 0 \quad (3.45)$$

com $\gamma_i \in K'$. Queremos mostrar que $\gamma_i = 0$ para $i = 1, \dots, r$. Para isso, seja $\alpha \in K'$ tal que $\gamma_1, \dots, \gamma_r \in K(\alpha)$ e escrevamos

$$\gamma_i = \sum_{j=0}^{n-1} c_{ij} \alpha^j$$

com $c_{ij} \in K$ e onde $n = [K(\alpha) : K]$. De [3.45](#) obtemos

$$\sum_{i=1}^r \left(\sum_{j=0}^{n-1} c_{ij} \alpha^j \right) y_i = \sum_{j=0}^{n-1} \left(\sum_{i=1}^r c_{ij} y_i \right) \alpha^j$$

Observemos que $\sum c_{ij} y_i \in F$. Como $[F(\alpha) : F] = [K(\alpha) : K]$, pelo [lema anterior](#), temos que $1, \alpha, \dots, \alpha^{n-1}$ são linearmente independentes sobre F e, portanto, a [equação anterior](#) implica

$$\sum_{i=1}^r c_{ij} y_i = 0$$

para $j = 0, \dots, n-1$. Agora, como os y_i 's são linearmente independentes sobre K , temos que todos os osc_{ij} 's são nulos e, consequentemente, todos os γ_i 's são nulos.

3. Como $F' = FK' = FK'(x)$ e como $[F : K(x)] < \infty$, temos que $[F' : K'(x)] \leq [F : K(x)]$.

Para mostrar que $[F' : K'(x)] \geq [F : K(x)]$, vamos mostrar que qualquer subconjunto $\{z_1, \dots, z_s\}$ de F que é linearmente independente sobre $K(x)$ é um subconjunto de F' que é linearmente independente sobre $K'(x)$. Suponhamos que não. Seja então

$$\sum_{i=1}^s f_i(x) z_i = 0$$

com $f_i(x) \in K'(x)$ e pelo menos um deles não nulo. Multiplicando por um fator conveniente, podemos supor que $f_i(x) \in K'[x]$ para $i = 1, \dots, s$. Com isso, a [equação anterior](#) nos mostra que o conjunto $\{x^j z_i \mid 1 \leq i \leq s, 0 \leq j \leq N\} \subset F$ (onde N é o máximo dos graus dos f_i 's) é linearmente dependente sobre K' . Daí, pelo item [2](#), temos que esse mesmo conjunto é linearmente dependente sobre K . Logo os elementos $z_1, \dots, z_s$ são linearmente dependentes sobre $K(x)$. Essa contradição finaliza a demonstração.

□

O teorema a seguir é um “apanhado” das principais propriedades de extensões do corpo de constantes.

Teorema 105. Para uma extensão de corpo de constantes de F/K , $F' = FK'$, vale o seguinte

1. F'/F é não ramificada, ou seja, $e(P'|P) = 1$ para todo $P \in \mathbb{P}_F$ e todo $P' \in \mathbb{P}_{F'}$ com $P'|P$.
2. Os gêneros de F/K e de F'/K' são iguais.
3. Para cada divisor $A \in \text{Div}(F)$ temos que $\deg \text{Con}_{F'/F}(A) = \deg A$.
4. Para cada divisor $A \in \text{Div}(F)$,

$$\ell(\text{Con}_{F'/F}(A)) = \ell(A)$$

Mais precisamente (e mais “fortemente” na verdade): toda base de $\mathcal{L}(A)$ é também uma base de $\mathcal{L}(\text{Con}_{F'/F}(A))$ (note que $\mathcal{L}(A) \subseteq F$ é um K -espaço vetorial, enquanto que $\mathcal{L}(\text{Con}_{F'/F}(A))$ é um K' -espaço vetorial).

5. Se W é um divisor canônico de F/K então $\text{Con}_{F'/F}(W)$ é também um divisor canônico de F'/K' .

6. O mapa conorma $\text{Con}_{F'/F} : \text{Cl}(F) \rightarrow \text{Cl}(F')$ do grupo das classes de divisores de F/K para o grupo das classes de divisores de F'/K' é injetor.
7. O corpo residual F'_P , de cada lugar $P' \in \mathbb{P}_{F'}$ é o compósito $F_P K'$ de K' e do corpo residual F_P , onde $P = P' \cap F$.
8. Se K'/K é finita, **toda** base de K'/K é uma base integral local de F'/F para **todo** lugar $P \in \mathbb{P}_F$. ■

Combinando o item 1 do [teorema anterior](#) com o [Teorema 64](#), obtemos uma fórmula para o grau da conorma de uma divisor numa extensão algébrica *arbitrária*.

Corolário 106. Seja F'/K' uma extensão algébrica de F/K (não necessariamente uma extensão de corpo de constantes). Então para cada divisor $A \in \text{Div}(F)$ temos

$$\deg \text{Con}_{F'/F}(A) = [F' : FK'] \cdot \deg A$$

Demonstração. Pelo item 3 do [Teorema 52](#), sabemos que $[F' : FK'] < \infty$ e que FK'/K' é uma extensão de corpo de constantes de F/K . Uma vez que

$$\text{Con}_{F'/F}(A) = \text{Con}_{F'/FK'}(\text{Con}_{FK'/F}(A))$$

segue que

$$\deg \text{Con}_{F'/F}(A) = [F' : FK'] \cdot \deg \text{Con}_{FK'/F}(A) = [F' : FK'] \deg A$$

pelos [Teorema 64](#) e item 1 do [Teorema 105](#). □

Corolário 107. Seja $P \in \mathbb{P}_F$ um lugar de F/K de grau r e seja $\bar{F} = F\bar{K}$ a extensão de corpo de constantes de F/K com o fecho algébrico $\bar{K}$ de K . Então

$$\text{Con}_{\bar{F}/F}(P) = \bar{P}_1 + \dots + \bar{P}_r$$

onde os lugares $\bar{P}_i \in \mathbb{P}_{\bar{F}}$ são dois a dois distintos. ■

Proposição 108. Seja F/K um corpo de funções cujo corpo de constantes é K . Suponha que F'/F é uma extensão de corpos finita cujo corpo de constantes é K' . Seja $\bar{K} \subseteq \Phi$ o fecho algébrico de K . Então

$$[F' : F] = [F'\bar{K} : F\bar{K}] \cdot [K' : K] \quad (3.46)$$

No caso particular em que $F' = F(y)$, temos que se $\varphi(T) \in F[T]$ é o polinômio minimal de y sobre F , as seguintes condições são equivalentes:

1. $K' = K$
2. $\varphi(T)$ é irredutível sobre $F\bar{K}[T]$ ■.

3.7 Extensões Galoisianas

Uma extensão F'/K' de F/K é dita **Galoisiana** (ou **de Galois**) se F'/F é uma extensão de corpos finita de Galois, ou seja, se o grupo dos automorfismos de F' que fixam F

$$\text{Aut}(F'/F) \doteq \{\sigma : F' \rightarrow F' \mid \sigma|_F = \text{id}_F\}$$

tem ordem $[F' : F]$. Nesse caso dizemos que $\text{Aut}(F'/F)$ é o grupo de Galois da extensão F'/F e o denotamos por $\text{Gal}(F'/F) \doteq \text{Aut}(F'/F)$.

As extensões Galoisianas apresentam várias propriedades boas. Por exemplo, veremos a seguir que os índice de ramificação e grau relativo de uma extensão $P'|P$ de lugares, com $P' \in \mathbb{P}_{F'}$ e $P \in \mathbb{P}_F$ e onde F'/F é de Galois, não dependem do lugar P' acima de P .

Seja $P \in \mathbb{P}_F$. Então $\text{Gal}(F'/F)$ age no conjunto $\{P' \in \mathbb{P}_{F'} \mid P'|P\}$ das extensões de P em F' “via” $\sigma(P') = \{\sigma(x) \mid x \in P'\}$, e vimos no [Teorema 94](#) que a valorização correspondente é dada por

$$v_{\sigma(P')}(y) = v_{P'}(\sigma^{-1}(y))$$

qualquer que seja $y \in F'$.

Teorema 109. Sejam F'/K' uma extensão Galoisiana de F/K e $P_1, P_2 \in \mathbb{P}_{F'}$ extensões de $P \in \mathbb{P}_F$. Então $P_2 = \sigma(P_1)$ para algum $\sigma \in \text{Gal}(F'/F)$. Em outras palavras: a ação descrita anteriormente é transitiva. ■

Demonstração. Vamos supor que $\sigma(P_1) \neq P_2$ qualquer que seja $\sigma \in G \doteq \text{Gal}(F'/F)$. A [APROXIMAÇÃO FRACA](#) nos garante a existência de $z \in F'$ tal que $v_{P_2}(z) > 0$ e $v_Q(z) = 0$ para todo $Q|P$ e distinto de P_2 . Consideremos agora o mapa norma $N_{F'/F} : F' \rightarrow F$. É bem sabido que

$$N_{F'/F}(z) = \prod_{\sigma \in G} \sigma(z)$$

Daí temos que

$$\begin{aligned}
v_{P_1}(N_{F'/F}(z)) &= v_{P_1}\left(\prod_{\sigma \in G} \sigma(z)\right) = \sum_{\sigma \in G} v_{P_1}(\sigma(z)) \\
&= \sum_{\sigma \in G} v_{\sigma^{-1}(P_1)}(z) = \sum_{\sigma \in G} v_{\sigma(P_1)}(z) = 0
\end{aligned}$$

onde a última igualdade segue da nossa hipótese de $\sigma(P_1) \neq P_2$ para todo $\sigma \in G$ e da nossa “escolha” de z . Por outro lado, temos que

$$v_{P_2}(N_{F'/F}(z)) = \sum_{\sigma \in G} v_{\sigma(P_2)}(z) > 0 \quad (3.47)$$

onde a desigualdade no final segue da nossa “escolha” de z . Ora mas $\zeta \doteq N_{F'/F}(z) \in F$ qualquer que seja $z \in F'$. Daí $v_{P_1}(\zeta) = 0 \Leftrightarrow v_P(\zeta) = 0 \Leftrightarrow v_{P_2}(\zeta) = 0$, o que contradiz 3.47 e finaliza a demonstração. $\square$

Corolário 110. Com a notação como no [teorema anterior](#), sejam $P_1, \dots, P_r$ todos os lugares de F' acima de P . Temos então que

1. $e(P_i|P) = e(P_j|P)$ e $f(P_i|P) = f(P_j|P)$ quaisquer que sejam i, j . Assim sendo, definimos

$$e(P) \doteq e(P_i|P) \quad \text{e} \quad f(P) \doteq f(P_i|P)$$

e diremos que $e(P)$ e $f(P)$ são, respectivamente, os índices de ramificação de grau relativo de P em F'/F .

2. $e(P) \cdot f(P) \cdot r = [F' : F]$. Em particular, $e(P)$, $f(P)$ e r dividem o grau $[F' : F]$ da extensão $F' : F$.
3. Os expoentes do diferente $d(P_i|P)$ e $d(P_j|P)$ são os mesmos quaisquer que sejam i, j . $\blacksquare$

Demonstração. O item 1 é uma consequência imediata do [Teorema 109](#) e do item 3 do [Teorema 94](#). O item 2 também segue imediatamente do item 1 e da [IGUALDADE FUNDAMENTAL](#). Para o item 3, consideraremos (confira as seções 3.2, 3.3 e 3.4 deste capítulo) o fecho inteiro $\mathcal{O}'_P$ de $\mathcal{O}_P$ em F'

$$\mathcal{O}'_P = \bigcap_{i=1}^r \mathcal{O}_{P_i} \quad (3.48)$$

e o módulo complementar sobre O_P

$$C_P = \{z \in F' \mid \text{Tr}_{F'/F}(z \cdot O'_P) \subseteq O_P\} \quad (3.49)$$

Seja $\sigma \in \text{Gal}(F'/F)$. Temos que $\sigma(O'_P) = O'_P$. De fato, dado $z \in O'_P$, temos que $v_{P_i}(z) \geq 0$ para $i = 1, \dots, r$. Daí $v_{P_i}(\sigma(z)) = v_{\sigma^{-1}(P_i)}(z) = v_{P_j}(z) \geq 0$ para $i = 1, \dots, r$. Isso mostra que $\sigma O'_P \subseteq O'_P$. Agora dado $z \in O'_P$, como σ é sobrejetor, existe $w \in F'$ tal que $z = \sigma(w)$. Mas, mais do que $w \in F'$, temos $w \in O'_P$. De fato, como σ é bijetor, $w = \sigma^{-1}(z)$, e, como $\sigma^{-1} \in \text{Gal}(F'/F)$ e $z \in O'_P$, segue da “parte” anterior que $w \in O_P$. Com isso temos que $z \in \sigma(O'_P)$ o que mostra que $O'_P \subseteq \sigma(O'_P)$.

Temos também que $\sigma(C_P) = C_P$. Isso segue da igualdade $\sigma(O'_P) = O'_P$ do parágrafo anterior e do simples fato que $\sigma(\text{Tr}_{F'/F}(u)) = \text{Tr}_{F'/F}(\sigma(u)) = \text{Tr}_{F'/F}(u)$ qualquer que seja $u \in F'$. Então, escrevendo $C_P = t \cdot O'_P$ obtemos $\sigma(t)O'_P = \sigma(C_P) = C_P = t \cdot O'_P$. Daí, pelo item 3 da [Teorema 84](#) e pela [definição do expoente do diferente](#), temos que

$$-d(P_i|P) = v_{P_i}(t) = v_{P_i}(\sigma(t))$$

para $i = 1, \dots, r$. Sejam P_i e P_j dois lugares acima de P e seja $\sigma \in \text{Gal}(F'/F)$ tal que $\sigma(P_j) = P_i$. Então, usando a [equação anterior](#), temos que

$$-d(P_i|P) = v_{P_i}(\sigma(t)) = v_{\sigma^{-1}(P_i)}(t) = v_{P_j}(t) = -d(P_j|P)$$

e isso finaliza a demonstração. □

Vamos discutir agora dois tipos específicos de extensões Galoisianas de corpos de funções, a saber, **extensões de Kummer** e **extensões de Artin-Schreier**.

Proposição 111 (EXTENSÕES DE KUMMER). Seja F/K um corpo de funções algébricas tal que K contem uma raiz primitiva n -ésima da unidade (com $n > 1$ e n coprimo com a característica de K). Suponha que $u \in F$ é um elemento que satisfaz

$$u \neq w^d \quad \text{para todo } w \in F \text{ e } d|n, d > 1 \quad (3.50)$$

Seja

$$F' = F(y) \quad \text{com } y^n = u \quad (3.51)$$

Uma tal extensão F'/F é dita ser uma **extensão de Kummer** de F . Temos que

1. O polinômio $\Phi(T) = T^n - u$ é o polinômio minimal de y sobre F (em particular, tal polinômio é irredutível sobre F). A extensão F'/F é galoisiana de grau $[F' : F] = n$. Seu grupo de Galois é cíclico e os automorfismos de F'/F são dados por $\sigma(y) = \sigma_\zeta(y) = \zeta y$, onde $\zeta \in K$ é uma raiz n -ésima da unidade.
2. Seja $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ um lugar acima de P . Então

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

onde

$$r_P \doteq (n, v_P(u)) > 0$$

é o máximo divisor comum entre n e $v_P(u)$ (de agora em diante, (a, b) sempre denotará, para a e $b \in \mathbb{Z}$, o máximo divisor comum entre a e b).

3. Se K' denota o corpo das constantes de F' e g e g' os gêneros de F/K e F'/K' , respectivamente, então

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

onde r_P é como no [item anterior](#). ■

Demonstração.

1. Notemos primeiramente que $f(T) \doteq T^n - u \in F[T]$ é separável pois os únicos fatores de $f'(T) = nT^{n-1}$ são da forma T^i com $i = 1, \dots, n-1$. Como $T^i \nmid T^n - u$ para nenhum $i = 1, \dots, n-1$, temos que $f(T)$ e $f'(T)$ são coprimos e portanto $f(T)$ é separável (observemos que $f'(T)$ não é ideticamente nulo pois n e $\text{char } K$ são primos entre si).

Se y é uma raiz de $T^n - u$, então para qualquer raiz primitiva n -ésima da unidade ζ (lembremos que, por hipótese, K contem todas as raízes n -ésimas da unidade, ou seja, $\zeta \in K$), temos que $(\zeta \cdot y)^n - u = \zeta^n \cdot y^n - u = y^n - u = 0$. Isso mostra que $\zeta \cdot y$ também é raiz de $T^n - u$, qualquer que seja $\zeta \in K$ com $\zeta^n = 1$. Daí, temos que as n raízes distintas de $f(T)$ são $\zeta_1 y, \dots, \zeta_n y \in F'$, onde $\zeta_1, \dots, \zeta_n \in K$ são todas as n raízes n -ésimas da unidade (distintas), ou seja, F'/F é normal. É claro que os automorfismos de F' são dados por $\sigma_i(y) = \zeta_i \cdot y$ (lembremos que as raízes n -ésimas da unidade são fixadas por todos automorfismos uma vez que estão no corpo base). Daí é claro que $f(T)$ é irredutível pois, como vimos anteriormente, $f(T)$ é separável e o grupo de Galois de F'/F age transitivamente nas raízes de $f(T)$. As outras afirmações são claras.

2. Vamos analisar o caso $r_P = 1$ primeiro. De 3.51 obtemos

$$n \cdot v_{P'}(y) = v_{P'}(y^n) = v_{P'}(u) = e(P'|P) \cdot v_P(u) \quad (3.52)$$

Disso, concluímos que $e(P'|P) = n$, uma vez que, por $r_P = 1$, n e $v_P(u)$ são coprimos. Como n não é divisível por $\text{char } K$, o **TEOREMA DO DIFERENTE DE DEDEKIND**, nos dá que o expoente do diferente é $d(P'|P) = n - 1$.

Agora, vamos analisar o caso $r_P = n$, ou seja, $v_P(u) = l \cdot n$ para algum $l \in \mathbb{Z}$. Escolhamos $t \in F$ tal que $v_P(t) = l$ e sejam $y_1 \doteq t^{-1}y \in F'$ e $u_1 \doteq t^{-n}u \in F$. Então,

$$y^n = u \Rightarrow y_1^n = u_1 \Rightarrow n \cdot v_{P'}(y_1) = e(P'|P)v_P(u_1) = e(P'|P) \cdot (-nl + v_P(u)) = 0$$

Logo $v_{P'}(y_1) = v_P(u_1) = 0$. Além disso o polinômio minimal de y_1 sobre F é

$$\psi(T) = T^n - u_1 \in F[T]$$

De fato, suponhamos que $\psi(T)$ fosse redutível em $F[T]$, i.e., que $T^n - u_1 = f(T)g(T)$. Então $(t^{-1}T)^n - u_1 = f(t^{-1}T)g(t^{-1}T) \Rightarrow T^n - t^n u_1 = T^n - u = t^n f(t^{-1}T)g(t^{-1}T)$, que contradiz o fato de $T^n - u$ ser irredutível sobre $F[T]$. Com isso, temos que y_1 é inteiro sobre $\mathcal{O}_P$ e o **Teorema 101** implica em

$$0 \leq d(P'|P) \leq v_{P'}(\psi'(y_1))$$

Temos que $\psi'(y_1) = n \cdot y_1^{n-1}$, de modo que $v_{P'}(\psi'(y_1)) = (n-1) \cdot v_{P'}(y_1) = 0$. Logo $d(P'|P) = 0$ e o **TEOREMA DO DIFERENTE DE DEDEKIND** nos dá $e(P'|P) = 1$.

Finalmente vamos analisar o caso $1 < r_P < n$. Consideremos o corpo intermediário $F_0 \doteq F(y_0)$ onde $y_0 \doteq y^{n/r_P}$. Temos que $T^{r_P} - u$ é o polinômio minimal de y_0 sobre F , logo $[F_0 : F] = r_P$ e $[F' : F_0] = n/r_P$.

$$n \left[\begin{array}{c} F' \\ | \\ F_0 \\ | \\ F \end{array} \right] \begin{array}{l} n/r_P \\ \\ r_P \end{array}$$

Seja $P_0 \doteq P' \cap F_0$, de modo que P_0 também é uma extensão de P (mas em F_0). Observemos que, pela **definição de r_P** , temos que $(r_P, v_P(u)) = r_P$ e que F_0/F é também uma extensão de Kummer (ainda temos que $u \neq w^d$ para todo $w \in F$ com

$d|r_P$ e $d > 1$, pois todo divisor de n é também divisor de r_P e temos a mesma condição válida com n no lugar de r_P). Como $[F_0 : F] = r_P$, temos que $r_{P_0} = r_P = [F_0 : F]$ e o último caso que consideramos se aplica nessa situação com r_P no lugar de n e $r_{P_0} = r_P$ no lugar de r_P . Então $e(P_0|P) = 1$. Como $y_0^{r_P} = u$, temos que

$$r_{P_0} \cdot v_{P_0}(y_0) = e(P_0|P) \cdot v_P(u) \Rightarrow v_{P_0}(y_0) = \frac{v_P(u)}{r_P}$$

Notemos que como $y^{n/r_P} = y_0$, temos que $F' = F_0(y)/F_0$ é também uma extensão de Kummer. Ora, como $(n, v_P(u)) = r_P$ temos que $(n/r_P, v_P(u)/r_P) = 1$ e agora, o primeiro caso que consideramos se aplica nessa situação com n/r_P no lugar de n e 1 no lugar de r_P . Consequentemente, temos que

$$e(P'|P) = e(P'|P_0) \cdot e(P_0|P) = n/r_P$$

e a igualdade para o expoente do diferente segue diretamente do [TEOREMA DO DIFERENTE DE DEDEKIND](#) (notemos que uma vez que n é suposto não ser divisível pela característica do corpo, temos que os números r_P e n/r_P também não o serão).

3. O grau do diferente $\text{Diff}(F'/F)$ é (usando o resultado do [item anterior](#))

$$\begin{aligned} \deg \text{Diff}(F'/F) &= \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P) \cdot \deg P' \\ &= \sum_{P \in \mathbb{P}_F} \left(\frac{n}{r_P} - 1 \right) \cdot \sum_{P'|P} \deg P' \end{aligned} \tag{3.53}$$

Lembrando que, pelo item 1 do [Teorema 110](#), o índice de ramificação $e(P)$ numa extensão de Galois não depende da escolha do lugar P' acima de P , temos que

$$\begin{aligned} \sum_{P'|P} \deg P' &= \frac{1}{e(P)} \cdot \deg \left(\sum_{P'|P} e(P'|P) \cdot P' \right) \\ &= \frac{1}{e(P)} \cdot \deg \text{Con}_{F'/F}(P) = \frac{r_P}{n} \cdot \frac{n}{[K' : K]} \cdot \deg P \\ &= \frac{r_P}{[K' : K]} \cdot \deg P \end{aligned}$$

pelo [Teorema 64](#). Substituindo a expressão acima em [3.53](#) obtemos o seguinte para o grau de $\text{Diff}(F'/F)$

$$\begin{aligned} \deg \text{Diff}(F'/F) &= \sum_{P \in \mathbb{P}_F} \frac{n - r_P}{r_P} \cdot \frac{r_P}{[K' : K]} \cdot \deg P \\ &= \frac{n}{[K' : K]} \cdot \sum_{P \in \mathbb{P}_F} \left(1 - \frac{r_P}{n}\right) \deg P \end{aligned}$$

O resultado agora segue substituindo a expressão acima na [FÓRMULA DO GÊNERO DE HURWITZ](#).

□

Vale a pena notarmos o seguinte caso particular da proposição anterior.

Corolário 112. Seja F/K um corpo de funções e $F' = F(y)$ onde $y^n = u \in F$ e $n \not\equiv 0 \pmod{\text{char } K}$. Suponhamos também que K contenha uma raiz primitiva n -ésima da unidade e que existe um lugar $Q \in \mathbb{P}_F$ tal que $(v_Q(u), n) = 1$. Então K é todo o corpo de constantes de F' , a extensão F'/F é cíclica de grau n e

$$g' = 1 + n(g - 1) + \frac{1}{2} \sum_{P \in \mathbb{P}_F} (n - r_P) \deg P \quad (3.54)$$

■

Demonstração. Da condição $(v_Q(u), n) = 1$ segue que u satisfaz a condição 3.50. De fato, se fosse $u = w^d$ para algum $w \in F$ e algum $d|n$, $d > 1$, teríamos que $v_Q(u) = d \cdot v_Q(w)$ e daí, como $d|n$, n e $v_Q(u)$ não seriam coprimos. Notemos que essa condição é equivalente a $r_Q = 1$. A expressão para o gênero de F' seguirá do item 3 uma vez que mostrarmos que K' , o corpo de constantes de K , não é “maior” que K , e é exatamente isso que faremos agora. Escolhamos um lugar $Q' \in \mathbb{P}_{F'}$ acima de Q . O item 2 nos mostra que

$$e(Q'|Q) = [F' : F] = n$$

Isso implica que Q' é o único lugar acima de Q . Suponhamos que $[K' : K] > 1$ e consideremos o corpo intermediário $F_1 K' \supsetneq F$ e o lugar $Q_1 \doteq Q' \cap F_1$. Temos que Q_1 também será o único lugar de $\mathbb{P}_{F_1}$ acima de Q pela [Teorema 58](#). Por 3.7, temos que $e(Q_1 : Q) = [F_1 : F] > 1$. Por outro lado, por F_1/F se tratar de uma extensão de corpo de constantes, temos que $e(Q_1 : Q) = 1$ (confira o [Teorema 105](#)). Essa contradição mostra que $[K' : K] = 1$, i.e., que $K' = K$.

□

Observação 113. Observemos que basta K conter uma raiz primitiva n -ésima da unidade para que contenha, na verdade, todas as raízes n -ésimas da unidade. Nas demonstrações

anteriores “quase” não usamos a hipótese de K conter uma raiz primitiva n -ésima da unidade (i.e., não usamos o fato de F'/F ser de Galois). Logo, as afirmações dos itens 2 e 3 da [Teorema 111](#) e o [Teorema 112](#) continuam válidos caso K não contenha todas as raízes n -ésimas da unidade com uma única exceção: $F(y)/F$ não será mais galoisiana. ■

Podemos agora dar um exemplo de um corpo de funções de gênero $g > 0$ usando os resultados anteriores.

Exemplo 114. Suponha que $\text{char } K \neq 2$. Seja $F = K(x, y)$ com

$$y^2 = f(x) = p_1(x) \cdot \dots \cdot p_s(x) \in K[x]$$

onde $p_1(x), \dots, p_s(x)$ são polinômios mônicos irreduzíveis e distintos e $s \geq 1$. Seja $m = \deg f(x)$. Então K é o corpo de constantes de F , e F/K tem gênero

$$g = \begin{cases} (m-1)/2 & \text{se } m \equiv 1 \pmod{2} \\ (m-2)/2 & \text{se } m \equiv 0 \pmod{2} \end{cases}$$

De fato, temos que $F = F_0(y)$, onde $F_0 \doteq K(x)$ é um corpo de funções racional. Seja $P_i \in \mathbb{P}_{K(x)}$ o zero de $p_i(x)$ e P_∞ o pólo de x em $K(x)$ (confira a seção 2.2). Temos que $v_{P_i}(f(x)) = 1$ e $v_{P_\infty}(f(x)) = -m$. Do [corolário anterior](#), obtemos que F/F_0 é uma extensão cíclica de grau 2 (lembremos que $\text{char } K \neq 2$) e que K é o corpo de constantes de F . Os números r_P são dados por

P 's	r_P 's
$P_1, \dots, P_s$	1
P_∞	1 se $m \equiv 1 \pmod{2}$ 2 se $m \equiv 0 \pmod{2}$
$P \notin \{P_1, \dots, P_s, P_\infty\}$	2

Caso $m \equiv 1 \pmod{2}$, o gênero de F será, pelo [Teorema 112](#), com $g = g(K(x)) = 0$

$$\begin{aligned} g' &= 1 + 2(0-1) + \frac{1}{2} \sum_{P \in \mathbb{P}_F} (2 - r_P) \deg P = -1 + \frac{1}{2} \left(\sum_{i=1}^s \deg p_i(x) + \color{red}{1} \right) \\ &= -1 + \frac{1}{2}(m + \color{red}{1}) = \frac{m-1}{2} \end{aligned}$$

Caso $m \equiv 0 \pmod{2}$, $r_{P_\infty} = 2$ e o número 1 em vermelho na expressão anterior deverá ser substituído por $2 - 2 = 0$, de modo que obtemos, nesse caso,

$$g' = \frac{m-2}{2}$$

Finalmente, é claro que K é o corpo de constantes de F , pelo [Teorema 112](#). ■

Agora, trataremos das **extensões de Artin-Schreier**. Para isso, precisaremos do seguinte

Lema 115. Seja F/K um corpo de funções algébricas de característica $p > 0$. Dado um elemento $u \in F$ e um lugar $P \in \mathbb{P}_F$, vale o seguinte

1. ou existe um elemento $z \in F$ tal que

$$v_P(u - (z^p - z)) \geq 0, \quad (3.55)$$

2. ou então, para algum $z \in F$,

$$v_P(u - (z^p - z)) = -m < 0 \text{ com } m \not\equiv 0 \pmod{p} \quad (3.56)$$

Nesse último caso, o inteiro m é unicamente determinado por u e por P , a saber

$$-m = \max\{v_P(u - (w^p - w)) \mid w \in F\} \quad (3.57)$$

Demonstração. Vamos começar mostrando que se x_1 e $x_2 \in F \setminus \{0\}$ e $v_P(x_1) = v_P(x_2)$, então existe $y \in F$ tal que

$$v_P(y) = 0 \quad \text{e} \quad v_P(x_1 - y^p x_2) > v_P(x_1) \quad (3.58)$$

De fato, a classe residual $(x_1/x_2)(P) \in \mathcal{O}_P/P$ é não nula, pois $v_P(x_1/x_2) = v_P(x_1) - v_P(x_2) = 0$ e (é claro) $x_1/x_2 \neq 0$. Logo $(x_1/x_2)(P) = (y(P))^p$ para algum $y \in \mathcal{O}_P \setminus P$, pois $\mathcal{O}_P/P$ é perfeito (lembramos que $\mathcal{O}_P/P$ é uma extensão finita de K e que supomos K perfeito). Como $(y(P))^p = (x_1/x_2)(P) \neq 0$, temos que $y(P) \neq 0$ e portanto $y \in \mathcal{O}_P \setminus P$, ou seja, $v_P(y) = 0$. Além disso, como $(y(P))^p = y^p(P)$, temos que $(x_1/x_2 - y^p)(P) = 0$ e, portanto, $v_P(x_1/x_2 - y^p) > 0 \Rightarrow v_P(x_1 - y^p x_2) > v_P(x_2) = v_P(x_1)$.

Agora, vamos mostrar que se $v_P(u - (z_1^p - z_1)) = -lp < 0$, então existe $z_2 \in F$ tal que

$$v_P(u - (z_2^p - z_2)) > -lp \quad (3.59)$$

Para isso, escolhamos $t \in F$ tal que $v_P(t) = -l$, de modo que podemos escrever

$$v_P(u - (z_1^p - z_1)) = v_P(t^p) \quad (3.60)$$

Por 3.58, com $u - (z_1^p - z_1)$ no lugar de x_1 e t^p no lugar de x_2 , podemos “encontrar” $y \in F$ tal que $v_P(y) = 0$ e

$$v_P(u - (z_1^p - z_1) - (yt)^p) > -lp \quad (3.61)$$

Uma vez que $v_P(yt) = v_P(t) = -l > -lp$, segue dessas duas últimas desigualdades e da **desigualdade triangular** que

$$v_P(u - (z_1^p - z_1) - ((yt)^p - yt)) > -lp \quad (3.62)$$

Daí, colocando $z_2 \doteq z_1 + yt$ obtemos 3.59 (lembramos que $z_2^p = (z_1 + yt)^p = z_1^p + (yt)^p$).

De 3.59, segue a existência de um elemento $z \in F$ para o qual ou vale o item 1 ou o item 2. De fato, se existir z para o qual $v_P(u - (z^p - z)) = -m < 0$ com $m \not\equiv 0 \pmod{p}$, já temos que vale o item 2. Caso seja $v_P(u - (z_1^p - z_1))$ negativo e múltiplo de p , então 3.59 nos diz que existe z_2 tal que $v_P(u - (z_2^p - z_2)) > v_P(u - (z_1^p - z_1))$. Caso $v_P(u - (z_2^p - z_2)) \geq 0$, temos que vale o item 1. Caso contrário, temos um de dois casos possíveis: ou $v_P(u - (z_2^p - z_2))$ não é múltiplo de p , e daí temos que vale o item 2, ou $v_P(u - (z_2^p - z_2))$ é múltiplo de p . No último caso, podemos repetir o raciocínio e “encontrar” z_3 tal que $v_P(u - (z_3^p - z_3)) > v_P(u - (z_2^p - z_2))$. É claro que esse processo eventualmente acaba, i.e. eventualmente teremos $v_P(u - (z_k^p - z_k)) \geq 0$ ou $v_P(u - (z_k^p - z_k))$ negativo e não múltiplo de p , pois as desigualdades $v_P(u - (z_{i+1}^p - z_{i+1})) > v_P(u - (z_i^p - z_i))$ são estritas.

Resta mostrarmos a caracterização 3.57 de m do no caso de termos o item 2. Por hipótese, temos que $v_P(u - (z^p - z)) = -m < 0$ com $m \not\equiv 0 \pmod{p}$. Para todo $w \in F$, temos que $p \cdot v_P(w - z) \neq -m$, pois o $p \cdot v_P(w - z)$ é múltiplo de p e o m não. Daí temos dois casos a considerar: $p \cdot v_P(w - z) > -m$ e $p \cdot v_P(w - z) < -m$.

Primeiramente, $p \cdot v_P(w - z) > -m$. Temos que $v_P((w - z)^p - (w - z)) > -m$. De fato, se $v_P(w - z) \geq 0$, é claro, pela **desigualdade triangular**, que $v_P((w - z)^p - (w - z)) \geq 0 > -m$ e se $v_P(w - z) < 0$, temos que $-m < p \cdot v_P(w - z) = v_P((w - z)^p) < v_P(w - z) < 0$ e pela **DESIGUALDADE TRIANGULAR ESTRITA**, segue que $v_P((w - z)^p - (w - z)) = \min\{v_P((w - z)^p), v_P(w - z)\} = p \cdot v_P(w - z) > -m$. Com isso temos que

$$v_P(u - (w^p - w)) = v_P(\overbrace{u - (z^p - z)}^{=-m} - \underbrace{((w - z)^p - (w - z))}_{> -m}) = -m \quad (3.63)$$

onde, na última igualdade usamos a **DESIGUALDADE TRIANGULAR ESTRITA**.

Agora, consideremos o caso $p \cdot v_P(w - z) < -m$. É claro, pela **DESIGUALDADE TRIANGULAR ESTRITA** que $v_P((w - z)^p - (w - z)) = v_P((w - z)^p) = p \cdot v_P(w - z) < -m$. Daí temos que,

como anteriormente,

$$v_P(u - (w^p - w)) = v_P(\overbrace{u - (z^p - z)}^{=-m} - \underbrace{((w - z)^p - (w - z))}_{< -m}) < -m \quad (3.64)$$

Em ambos os casos, vemos que $v_P(u - (w^p - w)) \leq -m$, para todo $w \in F$. Isso mostra 3.57.

□

Observação 116. Na demonstração anterior, fica claro que as relações 3.55 e 3.56 são mutuamente excludentes, i.e., para todo $u \in F$ e para todo $P \in \mathbb{P}_F$, um, e apenas um, dos itens 1 ou 2 é satisfeito. De fato, se tivermos 3.56 então, como vimos no final da demonstração, $v_P(u - (w^p - w)) \leq -m < 0$ para todo $w \in F$ e, portanto nunca acontecerá 3.55. E, se tivermos 3.55, pelo mesmo motivo nunca acontecerá 3.56. ■

Proposição 117 (EXTENSÕES DE ARTIN-SCHREIER). Seja F/K um corpo de funções algébricas de característica $p > 0$. Suponha que $u \in F$ é um elemento tal que

$$u \neq w^p - w \quad \text{para todo } w \in F \quad (3.65)$$

Seja

$$F' = F(y) \quad \text{com} \quad y^p - y = u \quad (3.66)$$

Uma tal extensão é chamada de **extensão de Artin-Schreier** de F . Para $P \in \mathbb{P}_F$, o lema anterior nos permite definir o inteiro m_P da seguinte maneira (confira a Teorema 116)

$$m_P \doteq \begin{cases} m & \text{se 3.56} \\ -1 & \text{se 3.55} \end{cases} \quad (3.67)$$

Temos então que

1. F'/F é uma extensão galoisiana cíclica de grau p . Os automorfismos de F'/F são dados por $\sigma(y) = \sigma_v(y) = y + v$, com $v \in \mathbb{F}_p$.
2. P é não ramificado em F'/F se, e somente se, $m_P = -1$.
3. P é totalmente ramificado em F'/F se, e somente se, $m_P > 0$. Denotando por P' o único lugar de F' acima de P , temos que o expoente do diferente $d(P'|P)$ é dado por

$$d(P'|P) = (p - 1)(m_P + 1)$$

4. Se pelo menos um lugar $Q \in \mathbb{P}_F$ satisfaz $m_Q > 0$, então K algebricamente fechado em F' e

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

onde g' e g denotam, como de costume, os gêneros de F'/K e F/K , respectivamente.

■

Demonstração. Para o item 1 notemos primeiramente que o polinômio $T^p - T - u \in F[T]$ é claramente separável (note que sua derivada é constante igual a -1). Se y é como no enunciado, i.e., uma raiz de $T^p - T - u$, então qualquer que seja $v \in \mathbb{F}_p$ vale

$$(y+v)^p - (y+v) = y^p + v^p - y - v = y^p - y + \overbrace{v^p - v}^{=0 \text{ (} v^p=v \text{)}} = y^p - y = u \quad (3.68)$$

Isso mostra que $y+v$ é também uma raiz, qualquer que seja $v \in \mathbb{F}_p$. Como temos p elementos em $\mathbb{F}_p$, temos que as $p = \deg(T^p - T - u)$ raízes distintas de $T^p - T - u$ são exatamente $y+0, y+1, \dots, y+(p-1) \in F' = F(y)$, de modo que F'/F é normal. É claro que os automorfismos de F' são dados por $\sigma(y) = \sigma_v(y) = y+v$, para cada $v \in \mathbb{F}_p$, de modo que $\text{Gal}(F'/F) \simeq \mathbb{Z}/p\mathbb{Z}$ (a composição de automorfismos em $\text{Gal}(F'/F)$ é “dada” pela adição em $\mathbb{Z}/p\mathbb{Z}$). Em resumo, F'/F é Galoisiana cíclica de grau p .

Vamos agora mostrar os itens 2 e 3. Consideremos primeiramente o caso $m_P = -1$, i.e., $v_P(u - (z^p - z)) \geq 0$ para algum $z \in F$. Sejam $y_1 = y - z$ e $u_1 = u - (z^p - z)$. Então, é claro que $F' = F(y) = F(y - z) = F(y_1)$ e que $\varphi_1(T) = T^p - T - u$ é o polinômio minimal de y_1 sobre F , pela Teorema 65. Uma vez que $v_P(u_1) \geq 0$, temos que y_1 é integral sobre o anel de valorização $\mathcal{O}_P$ e o expoente do diferente $d(P'|P)$ de um lugar P' acima de P satisfaz, pelo Teorema 101

$$0 \leq d(P'|P) \leq v_{P'}(\varphi'_1(y_1)) = 0 \quad (3.69)$$

pois $\varphi'_1(T) = -1$. Daí $d(P'|P) = 0$ e, pelo TEOREMA DO DIFERENTE DE DEDEKIND, $e(P'|P) = 1$, ou seja, $P'|P$ é não ramificada.

Agora, consideremos o caso $m_P > 0$. Escolhamos $z \in F$ tal que $v_P(u - (z^p - z)) = -m_P$. Sejam y_1 e u_1 como anteriormente. Temos novamente que $F' = F(y_1)$ e que $\varphi_1(T) = T^p - T - u_1$ é o polinômio minimal de y_1 sobre F . Seja $P' \in \mathbb{P}_{F'}$ um lugar acima de $P \in \mathbb{P}_F$. Uma vez que $y_1^p - y_1 = u_1$, obtemos

$$v_{P'}(u_1) = e(P'|P) \cdot v_P(u_1) = -m_P \cdot e(P'|P) \quad (3.70)$$

e

$$0 > v_{P'}(u_1) = v_{P'}(y_1^p - y_1) = v_{P'}(y_1^p) = p \cdot v_{P'}(y_1) \quad (3.71)$$

pela **DESIGUALDADE TRIANGULAR ESTRITA**. Logo $p \cdot v_{P'}(y_1) = -m_P e(P'|P)$. Como p e m_P são coprimos, temos que $p|e(P'|P)$. Mas $e(P'|P) \leq [F':F] = p$. Logo, temos que

$$e(P'|P) = p \quad \text{e} \quad v_{P'}(y_1) = -m_P \quad (3.72)$$

Ou seja, P é totalmente ramificado em F'/F .

Agora, vejamos como são os expoentes do diferente. Seja $x \in F$ um elemento primo de P . Escolhamos inteiros i e $j \geq 0$ tais que $1 = ip - jm_P$. Tal escolha é obviamente possível, uma vez que p e m_P são coprimos e positivos. Temos então que o elemento $t = x^i y_1^j$ é um elemento primo de P' (onde, como mostramos anteriormente, P' é o único lugar de F' acima de P), pois $v_{P'}(t) = i \cdot v_{P'}(x) + j \cdot v_{P'}(y_1) = ip - jm_P = 1$. Pela **Teorema 102** temos que o expoente do diferente $d(P'|P)$ é

$$d(P'|P) = v_{P'}(\psi'(t)) \quad (3.73)$$

onde $\psi(T) \in F[T]$ é o polinômio minimal de t sobre F . Seja $G \doteq \text{Gal}(F'/F)$ o grupo de Galois de F'/F . É claro que

$$\psi(T) = \prod_{\sigma \in G} (T - \sigma(t)) = (T - t) \cdot h(T) \quad (3.74)$$

onde

$$h(T) = \prod_{\sigma \neq \text{id}} (T - \sigma(t)) \in F'[T] \quad (3.75)$$

Então, $\psi'(T) = h(T) + (T - t) \cdot h'(T)$ e, portanto, $\psi'(t) = h(t)$. Disso concluímos que

$$d(P'|P) = v_{P'}\left(\prod_{\sigma \neq \text{id}} (t - \sigma(t))\right) = \sum_{\sigma \neq \text{id}} v_{P'}(t - \sigma(t)) \quad (3.76)$$

Ora, cada $\sigma \in G \setminus \{\text{id}\}$ tem a forma $\sigma(y_1) = y_1 + \mu$ para algum $\mu \in \{1, \dots, p-1\}$ (notemos que $\mu = 0$ corresponde justamente a $\sigma = \text{id}$). Daí, lembrando que como $x \in F$ temos que $\sigma(x) = x$ para todo $\sigma \in G$, obtemos

$$t - \sigma(t) = x^i y_1^j - x^i (y_1 + \mu)^j = -x^i \cdot \sum_{l=1}^j \binom{j}{l} y_1^{j-l} \mu^l \quad (3.77)$$

Como $v_{P'}(y_1^{j-1}) < v_{P'}(y_1^{j-l})$ para $l \geq 2$, e como $v_{P'}(\mu) = 0$ para qualquer $\mu \in \mathbb{F}_p^*$, a **DESIGUALDADE TRIANGULAR ESTRITA** nos dá

$$\begin{aligned} v_{P'}(t - \sigma(t)) &= v_{P'}(x^i) + v_{P'}(\textcolor{red}{j} \mu y_1^{j-1}) = ip + (j-1) \cdot (-m_P) \\ &= ip - jm_P + m_P = m_P + 1 \end{aligned} \quad (3.78)$$

O j em vermelho na igualdade anterior vem do coeficiente binomial $\binom{j}{1} \in K$. Observemos que esse j é não nulo em K pois $ip - jm_P \equiv -jm_P \equiv 1 \pmod{p}$, ou seja $j \not\equiv 0 \pmod{p}$, de modo que $v_{P'}(j \mu y_1^{j-1}) \neq \infty$. Uma substituição direta de 3.78 em 3.76 nos dá $d(P'|P) = (p-1)(m_P+1)$. E com isso terminamos de mostrar os itens 2 e 3.

Suponhamos agora que $m_Q > 0$ para pelo menos um lugar $Q \in \mathbb{P}_F$. Do item 3, temos que Q é totalmente ramificado. A demonstração de que K é o corpo de constantes de F' é idêntica à demonstração dada no **Teorema 112**.

A igualdade para o gênero

$$g' = p \cdot g + \frac{p-1}{2} \left(-2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \cdot \deg P \right) \quad (3.79)$$

é uma consequência imediata dos itens 2 e 3 e da **FÓRMULA DO GÊNERO DE HURWITZ**.

Antes de finalizarmos a demonstração, notemos que a soma que aparece na última igualdade é “feita sobre” todos os lugares $P \in \mathbb{P}_F$, e não sobre os lugares $P' \in \mathbb{P}_{F'}$. De fato, nesse tipo de extensão um lugar $P \in \mathbb{P}_F$ ou é não ramificado ($m_P = -1$), de modo que o expoente do diferente é nulo ($m_P + 1 = 0$) pelo **Teorema 97**, ou P é totalmente ramificado, de modo que só existe um lugar P' acima de P de grau $\deg P' = f(P'|P) \cdot \deg P = \deg P$ e cujo expoente do diferente é dado pelo item 3. Em qualquer um dos dois casos, m_P positivo ou negativo, temos que o expoente do diferente é dado por $d(P'|P) = (p-1)(m_P+1)$ (é exatamente para que isso aconteça que definimos $m_P = -1$ caso tenhamos 3.56).

□

Observação 118. Com a notação como na **proposição anterior**, supondo que exista um lugar $Q \in \mathbb{P}_F$ tal que

$$v_Q(u) < 0 \quad \text{e} \quad v_Q(u) \not\equiv 0 \pmod{p} \quad (3.80)$$

então u satisfaz a condição 3.65 pela **DESIGUALDADE TRIANGULAR ESTRITA**. De fato, se fosse $u = w^p - w$ para algum $w \in F$, então $v_Q(u) = v_Q(w^p - w) < 0 \Rightarrow v_Q(w^p - w) = v_Q(w^p) =$

$p \cdot v_Q(w) \equiv 0 \pmod{p}$. Com isso, temos que a [proposição anterior](#) se aplica nesse caso, i.e., no caso de u ter um pólo de ordem não múltipla de p .

Além disso, qualquer extensão de corpos F'/F cíclica de grau $[F' : F] = p = \text{char } F > 0$ é uma extensão de Artin-Schreier (confira cla). ■

Os argumentos usados na demonstração da proposição anterior se aplicam num cenário mais geral. Um polinômio da forma

$$a(T) = a_n T^{p^n} + a_{n-1} T^{p^{n-1}} + \dots + a_1 T^p + a_0 T \in K[T]$$

onde $p = \text{char } K > 0$ é chamado de polinômio aditivo (ou linearizado) sobre K . Lembrando que $a(T)$ é separável se, e somente se, $a(T)$ e sua derivada $a'(T)$ não possuem um fator (de grau > 0) em comum, vemos que polinômios aditivos são separáveis se, e somente se, $a'(T) = a_0 \neq 0$.

Os polinômios aditivos satisfazem a seguinte notabilíssima propriedade

$$a(u + v) = a(u) + a(v)$$

quaisquer que sejam os elementos u e v em qualquer extensão de K . Em particular, se $a(T)$ é um polinômio aditivo e separável em $K[T]$ que possui todas as suas raízes em K , então o conjunto dessas raízes é um subgrupo do grupo aditivo de K de ordem $p^n = \deg a(T)$.

O cenário mais geral no qual valem os argumentos usados na demonstração anterior é o seguinte.

Proposição 119. Consideremos um corpo de funções algébricas F/K cujo corpo das constantes K é de característica $p > 0$ e um polinômio aditivo e separável $a(T) \in K[T]$ de grau p^n que possui todas as suas raízes em K . Seja $u \in F$ e suponhamos que para cada $P \in \mathbb{P}_F$ existe um elemento $z \in F$ (que dependerá de P) tal que

$$v_P(u - a(z)) \geq 0 \tag{3.81}$$

ou tal que

$$v_P(u - a(z)) = -m \quad \text{com } m > 0 \text{ e } m \not\equiv 0 \pmod{p} \tag{3.82}$$

Defina $m_P \doteq -1$ caso [3.81](#) e $m_P \doteq m$ caso [3.82](#). Então m_P é um inteiro bem definido*. Consideremos a extensão de corpos $F' = F(y)$ de F onde y satisfaz a equação

* De fato, basta verificarmos que as duas condições anteriores [3.81](#) e [3.82](#) são mutuamente excludentes, i.e., se uma ocorre a outra não poderá ocorrer. A demonstração disse segue as

$$a(y) = u$$

Se existir pelo menos um lugar $Q \in \mathbb{P}_F$ com $m_Q > 0$ (essa é uma condição suficiente para que $u \neq a(z)$ para todo $z \in F$, ou seja, para que o polinômio $a(T) - u \in F[T]$ seja irredutível), então vale o seguinte

1. F'/F é galoisiana de grau $[F' : F] = p^n$ e o grupo de Galois de F'/F é isomorfo ao subgrupo aditivo $\{\alpha \in K \mid a(\alpha) = 0\}$, logo é isomorfo a $(\mathbb{Z}/p\mathbb{Z})^n$ (tais grupos são chamados de grupos abelianos elementares de expoente p , e portanto F'/F é dita ser uma extensão abeliana elementar de expoente p e grau p^n).
2. K é algebricamente fechado em F' .
3. Cada $P \in \mathbb{P}_F$ com $m_P = -1$ é não ramificado em F'/F .
4. Cada $P \in \mathbb{P}_F$ com $m_P > 0$ é totalmente ramificado em F'/F e o expoente do diferente $d(P'|P)$ da extensão P' de P em F' é

$$d(P'|P) = (p^n - 1)(m_P + 1)$$

5. Sejam g' e g os gêneros de F' e F , respectivamente. Então

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

A demonstração desse “cenário” mais geral é *idêntica* (feitas as modificações necessárias) à demonstração da [Teorema 117](#), para o caso particular do polinômio $a(T) = T^p - T$.

mesmas linhas do final da demonstração do [Teorema 115](#): pode-se mostrar que se $v_P(u - a(z)) = -m < 0$ com $m \not\equiv 0 \pmod{p}$, então para todo $w \in F$, $v_P(u - a(w)) \leq -m$. Daí, as duas condições [3.81](#) e [3.82](#) são mutuamente excludentes (a [Teorema 116](#) se aplica nesse caso com as modificações necessárias). Notemos que a primeira parte da demonstração do [Teorema 115](#) foi a existência de z tal que ou [3.81](#) ou [3.82](#) para o particular polinômio aditivo $T^p - T$. Aqui supomos que ou [3.81](#) ou [3.82](#) é válida para o polinômio $a(T)$.

O TEOREMA DE HASSE-WEIL

O corpo de constantes do corpo de funções F/K era um corpo perfeito arbitrário, no capítulo anterior. Neste capítulo consideraremos em maior detalhe o caso de um corpo de funções cujo corpo de constantes é finito. Como corpos finitos são perfeitos, os resultados obtidos e as considerações feitas anteriormente se aplicam nesse caso. O principal resultado do capítulo é o [TEOREMA DE HASSE-WEIL](#) que tem como consequência (na verdade veremos que são [equivalentes](#)) a célebre [COTA DE HASSE-WEIL](#) para o número de lugares racionais de $F/\mathbb{F}_q$. O [TEOREMA DE HASSE-WEIL](#) também é conhecido como **hipótese de Riemann para corpos de funções** (confira a [Teorema 138](#)), nomenclatura esta para a qual daremos sentido quando enunciarmos o teorema.

4.1 A função zeta de um corpo de funções

De agora em diante, F será um corpo de funções algébricas de gênero g cujo corpo de constantes é o corpo finito $\mathbb{F}_q$.

Lema 120. Para todo $n \geq 0$ existe apenas um número finito de divisores positivos de grau n . ■

Demonstração. Um divisor positivo é uma soma de divisores primos. Então para mostrarmos que o conjunto dos divisores positivos de grau n é finito, basta mostrarmos que o conjunto S dos lugares de grau $\leq n$ é finito. De fato, esses lugares, vistos como divisores primos, são precisamente os divisores que podem aparecer como “parcelas” na representação de um divisor positivo como soma de divisores primos. Escolhamos $x \in F \setminus \mathbb{F}_q$ e consideremos o conjunto S_0 dos lugares de $\mathbb{F}_q(x)$ de grau $\leq n$. É claro que $P \cap \mathbb{F}_q(x) \in S_0$ para todo $P \in S$, pois $\deg P = \deg(P \cap \mathbb{F}_q(x)) \cdot f(P|(P \cap \mathbb{F}_q(x)))$, e, além disso, cada $P_0 \in S_0$ possui apenas um número finito de extensões em F (confira o item 2 da [Teorema 58](#)). Sendo assim, basta mostrarmos que o conjunto S_0 é finito. Ora, mas

como os lugares de $\mathbb{F}_q(x)$ correspondem (exceto pelo pólo de x) a polinômios mônicos irreduzíveis $p(x) \in \mathbb{F}_q[x]$ de mesmo grau que o lugar (confira o [Teorema 21](#)), a finitude de S_0 segue da finitude do número de polinômios de grau $\leq n$ em $\mathbb{F}_q[x]$. $\square$

Definição 121. O conjunto

$$\text{Div}^0(F) = \{A \in \text{Div}(F) \mid \deg A = 0\}$$

é chamado de grupo dos divisores de grau zero. Analogamente,

$$\text{Cl}^0(F) = \{[A] \in \text{Cl}(F) \mid \deg[A] = 0\}$$

é chamado de grupo das classes de divisores de grau zero. Observemos que ambos são, de fato, subgrupos de $\text{Div}(F)$ e de $\text{Cl}(F)$, respectivamente. $\blacksquare$

Proposição 122. $\text{Cl}^0(F)$ é um grupo finito cuja ordem, denotada por $h = h_F$, é chamada de **número de classe** de $F/\mathbb{F}_q$. $\blacksquare$

Demonstração. Consideremos um divisor B de grau $\deg B \doteq n \geq g$ e definamos $\text{Cl}^n(F)$ de modo análogo a $\text{Cl}^0(F)$. O mapa

$$\begin{aligned} \text{Cl}^0(F) &\rightarrow \text{Cl}^n(F) \\ [A] &\mapsto [A + B] \end{aligned}$$

é claramente bijetor (qualquer que seja $n \geq 0$) e $\text{Cl}^n(F)$ é finito. De fato, dado $[C] \in \text{Cl}^n(F)$, como $\deg[C] = n \geq g$, temos, pelo [TEOREMA DE RIEMANN-ROCH](#)

$$\ell([C]) = \ell(C) \geq n + 1 - g \geq 1$$

Para a igualdade em vermelho, confira o item 2 do [Teorema 31](#). Com isso, temos, por 2, que para qualquer classe $[C] \in \text{Cl}^n(F)$ existe um divisor positivo A tal que $A \in [C]$. Logo, a ordem de $\text{Cl}^n(F)$ é menor ou igual que o número de divisores de grau n (pode ser menor pois pode ser que dois divisores positivos distintos de mesmo grau sejam equivalentes). Uma vez que o número de divisores positivos de grau n é finito pelo [Teorema 120](#), segue que $\text{Cl}^n(F)$ é finito. A finitude de $\text{Cl}^n(F)$ juntamente com o fato de o mapa considerado anteriormente ser bijetor implicam na finitude de $\text{Cl}^0(F)$. $\square$

Definição 123. Definimos o inteiro $\partial > 0$ por

$$\partial = \min\{\deg A \mid A \in \text{Div}(F) \text{ e } \deg A > 0\}$$

Notemos que a imagem do homomorfismo $\deg: \text{Div}(F) \rightarrow \mathbb{Z}$ é o subgrupo de $\mathbb{Z}$ gerado por ∂ . Logo o grau de qualquer divisor de $F/\mathbb{F}_q$ é múltiplo de ∂ . O inteiro ∂ é chamado de **índice** de $F/\mathbb{F}_q$.

Definimos também, para $n \in \mathbb{Z}$

$$A_n = |\{A \in \text{Div}(F) \mid A \geq 0 \text{ e } \deg A = n\}|$$

■

Então, por exemplo, $A_0 = 1$ (só existe um divisor efetivo de grau zero, a saber, o divisor zero) e A_1 é o número de lugares racionais de F .

Lema 124.

1. $A_n = 0$ se $\partial \nmid n$.
2. Para uma classe de divisores $[C]$ fixa temos

$$|\{A \in [C] \mid A \geq 0\}| = \frac{q^{\ell([C])} - 1}{q - 1}$$

3. Para cada inteiro $n > 2g - 2$ tal que $\partial \mid n$ temos

$$A_n = \frac{h \cdot (q^{n+1-g} - 1)}{q - 1}$$

■

Definição 125. A série de potências

$$Z(t) \doteq Z_F(t) \doteq \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]] \quad (4.1)$$

é chamada de **função Zeta** de $F/\mathbb{F}_q$.

■

Proposição 126. A série de potências $Z(t) = \sum_{n=0}^{\infty} A_n t^n$ converge para $|t| < q^{-1}$. Mais precisamente, para $|t| < q^{-1}$ temos

1. Se o gênero g de $F/\mathbb{F}_q$ é $g = 0$ então

$$Z(t) = \frac{1}{q-1} \left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}} \right)$$

2. Se $g \geq 1$, então $Z(t) = F(t) + G(t)$ com

$$F(t) = \frac{1}{1-q} \sum_{0 \leq \deg[C] \leq 2g-2} q^{\ell([C])} \cdot t^{\deg[C]}$$

(onde a soma anterior é “feita sobre” todas as classes distintas de divisores $[C] \in \text{Cl}(F)$ tais que $0 \leq \deg[C] \leq 2g-2$) e

$$G(t) = \frac{h}{q-1} \left(q^{1-g} (qt)^{2g-2+\partial} \frac{1}{1-(qt)^\partial} - \frac{1}{1-t^\partial} \right)$$

■

Como consequência [dessa proposição](#), temos que a função Zeta pode ser estendida a uma função racional em $\mathbb{C}$ que, em particular, possui um pólo simples em 1.

É conveniente termos uma representação de $Z(t)$ como um produto infinito de modo a estudar seu comportamento sob uma extensão de corpo de constantes finita de $F/\mathbb{F}_q$. Dizemos que um produto infinito $\prod_{i=1}^{\infty} (1+a_i)$ (com $-1 \neq a_i \in \mathbb{C}$) converge para $a \in \mathbb{C}$ se $\lim_{n \rightarrow \infty} \prod_{i=1}^n (1+a_i) = a \neq 0$. Dizemos que o produto converge absolutamente se $\sum_{i=1}^{\infty} |a_i| < \infty$. “Da análise”, sabemos que convergência absoluta implica convergência, e que o limite de um produto absolutamente convergente independe da ordem dos fatores (observemos que um produto infinito $\prod_{i=1}^{\infty} a_i$ com $0 \neq a_i \in \mathbb{C}$ pode ser estudado em termos da série $\sum_{i=1}^{\infty} \log(a_i)$). Se o produto $\prod_{i=1}^{\infty} (1+a_i) = a$ é absolutamente convergente, então $\prod_{i=1}^{\infty} (1+a_i)^{-1}$ também converge absolutamente com limite a^{-1} .

Proposição 127 (PRODUTO DE EULER). Para $|t| < q^{-1}$ a função Zeta pode ser representada como o seguinte produto absolutamente convergente

$$Z(t) = \prod_{P \in \mathbb{P}_F} (1 - t^{\deg P})^{-1}$$

Em particular, $Z(t) \neq 0$ para $|t| < q^{-1}$. ■

Fixamos um fecho algébrico $\overline{\mathbb{F}_q}$ de $\mathbb{F}_q$ e consideramos a extensão de corpo de constantes $\bar{F} = F\overline{\mathbb{F}_q}$. Para cada $r \geq 1$ existe exatamente uma extensão $\mathbb{F}_{q^r}/\mathbb{F}_q$ de grau r tal que $\mathbb{F}_{q^r} \subseteq \overline{\mathbb{F}_q}$. Daí, colocamos

$$F_r = F\mathbb{F}_{q^r} \subset \bar{F}$$

Lema 128.

1. F_r/F é uma extensão galoisiana cíclica de grau r . O grupo de Galois $\text{Gal}(F_r/F)$ é gerado pelo automorfismo de Frobenius dado por $\sigma(\alpha) = \alpha^q$ para $\alpha \in \mathbb{F}_q$.

2. $\mathbb{F}_{q^r}$ é todo o corpo de constantes de F_r .
3. $F_r/\mathbb{F}_{q^r}$ tem o mesmo gênero de $F/\mathbb{F}_q$
4. Seja $P \in \mathbb{P}_F$ um lugar de grau m . Então $\text{Con}_{F_r/F}(P) = P_1 + \dots + P_d$, com $d = (m, r)$ lugares $P_i \in \mathbb{P}_{F_r}$ dois a dois distintos e tais que $\deg P_i = m/d$. ■

Na demonstração da [próxima proposição](#) usaremos a seguinte identidade polinomial. Se $m \geq 1$ e $r \geq 1$ são inteiros e $d = (m, r)$, então

$$(X^{r/d} - 1)^d = \prod_{\zeta^r=1} (X - \zeta^m)$$

onde ζ “percorre” todas as raízes r -ésimas da unidade em $\mathbb{C}$. De fato, observemos que os polinômios dos dois lados da [igualdade anterior](#) são mônicos de grau r . Além disso, é fácil ver que as raízes do polinômio do lado esquerdo são as raízes (r/d) -ésimas da unidade (em $\mathbb{C}$), cada uma com multiplicidade d . Para vermos que as raízes do polinômio do lado direito são também as raízes (r/d) -ésimas da unidade com multiplicidade d cada, basta notar o seguinte. Como $d = (m, r)$, temos que existem a e $b \in \mathbb{Z}$ tais que $ak + b(r/d) = 1$, com $k = m/d$. Além disso, temos que $\zeta_r^m = \zeta_{r/d}^k$, onde ζ_r e $\zeta_{r/d}$ são raízes r -ésima e (r/d) -ésima, respectivamente, primitivas da unidade. Daí os fatores do polinômio do lado direito são $(X - \zeta_{r/d}^{i \cdot k})$ com $i = 1, \dots, r$. Como $ak \equiv 1 \pmod{(r/d)}$, e como temos $r = (r/d) \cdot d$, temos que cada raiz (r/d) -ésima da unidade aparecerá exatamente d vezes no polinômio do lado direito, e portanto os polinômios dos lados esquerdo e direito coincidem.

Fazendo $X = t^{-m}$ na equação anterior e multiplicando ambos os lados por t^{mr} , obtemos

$$(1 - t^{mr/d})^d = \prod_{\zeta^r=1} (1 - (\zeta t)^m) \quad (4.2)$$

Proposição 129. Sejam $Z(t)$ e $Z_r(t)$ as funções Zeta de F e F_r respectivamente. Então

$$Z_r(t^r) = \prod_{\zeta^r=1} Z(\zeta t) \quad (4.3)$$

para todo $t \in \mathbb{C}$. ■

Demonstração. É suficiente mostrar [4.3](#) para $|t| < q^{-1}$. De fato, supondo [4.3](#) válida para $|t| < q^{-1}$ temos, temos para $|t| < R$

$$Z_r(t^r) = Z_r(R^r q^r (t/Rq)^r) = R^r q^r Z_r((t/Rq)^r) = R^r q^r \prod_{\zeta^r=1} Z(\zeta t/Rq) = \prod_{\zeta^r=1} Z(\zeta t)$$

A igualdade em vermelho segue de 4.1 Para $|t| < q^{-1}$, a representação de Z_r através do PRODUTO DE EULER nos dá

$$Z_r(t^r) = \prod_{P \in \mathbb{P}_F} \prod_{P' | P} (1 - t^{r \cdot \deg P'})^{-1} \quad (4.4)$$

Para um lugar $P \in \mathbb{P}_F$ fixado colocamos $m \doteq \deg P$ e $d \doteq (r, m)$. Daí

$$\prod_{P' | P} (1 - t^{r \cdot \deg P'}) = (1 - t^{rm/d})^d$$

Na igualdade em vermelho, usamos o item 4 do Teorema 128. Por outro lado, por 4.2, temos

$$(1 - t^{rm/d})^d = \prod_{\zeta^r=1} (1 - (\zeta t)^m) = \prod_{\zeta^r=1} (1 - (\zeta t)^{\deg P}) \quad (4.5)$$

Finalmente, por 4.4 e 4.5, temos

$$Z_r(t^r) = \prod_{\zeta^r=1} \prod_{P \in \mathbb{P}_F} (1 - (\zeta t)^{\deg P})^{-1} = \prod_{\zeta^r=1} Z(\zeta t) \quad (4.6)$$

Observemos que a convergência absoluta do PRODUTO DE EULER nos permite trocar a ordem do produto em 4.4.

□

Corolário 130 (FRIEDRICH KARL SCHMIDT). $\partial = 1$. ■

Demonstração. Sendo ζ_∂ uma raiz ∂ -ésima da unidade, temos que

$$Z(\zeta_\partial t) = \prod_{P \in \mathbb{P}_F} (1 - (\zeta_\partial t)^{\deg P})^{-1} = \prod_{P \in \mathbb{P}_F} (1 - t^{\deg P})^{-1} = Z(t)$$

pois $\partial | \deg P$ para todo $P \in \mathbb{P}_F$. Daí, pela proposição anterior, $Z_\partial(t^\partial) = Z(t)^\partial$. Ora, a função racional $Z_\partial(t^\partial)$ possui um pólo simples em $t = 1$, como já foi observado. Por outro lado, $Z(t)^\partial$ possui um pólo de ordem ∂ em $t = 1$. Logo, como as ordens dos pólos devem ser iguais, $\partial = 1$.

□

Observação 131. Note que o resultado anterior não implica na existência de lugares racionais, mas de divisores de grau 1 e, portanto, de qualquer grau. Com isso, temos que *todo* corpo de funções $F/\mathbb{F}_q$ de gênero $g = 0$ é racional, pela Teorema 48.

Proposição 132 (EQUAÇÃO FUNCIONAL DA FUNÇÃO ZETA). A função Zeta de $F/\mathbb{F}_q$ satisfaz a equação funcional

$$Z(t) = q^{g-1} t^{2g-2} Z\left(\frac{1}{qt}\right)$$

■

Definição 133. O polinômio $L(t) = L_F(t) = (1-t)(1-qt)Z(t)$ é chamado de L -polinômio de $F/\mathbb{F}_q$.

■

É claro que, pela [Teorema 126](#) e por ser $\partial = 1$, $L(t)$ é um polinômio de grau $\leq 2g$. Observemos que ele contém toda e qualquer informação sobre os números A_n , com $n \geq 0$, uma vez que

$$L(t) = (1-t)(1-qt) \sum_{n=0}^{\infty} A_n t^n \quad (4.7)$$

Teorema 134.

1. $L(t) \in \mathbb{Z}[t]$ e $\deg L(t) = 2g$.
2. (EQUAÇÃO FUNCIONAL) $L(t) = q^g t^{2g} L(1/qt)$.
3. $L(1) = h$, o número de classe de $F/\mathbb{F}_q$.
4. Escrevendo $L(t) = a_0 + a_1 t + \dots + a_{2g} t^{2g}$, temos que $a_0 = 1$ e $a_{2g} = q^g$, $a_{2g-i} = q^{g-i} a_i$ para $0 \leq i \leq g$ e $a_1 = N - (q+1)$, onde N é o número de lugares racionais de F .
5. $L(t)$ se fatora em $\mathbb{C}[t]$ da seguinte maneira

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t) \quad (4.8)$$

Os números complexos $\alpha_1, \dots, \alpha_{2g}$ são inteiros algébricos que podem ser arranjados de tal forma que $\alpha_i \alpha_{g+i} = q$ para $1 \leq i \leq g$.

6. Se $L_r(t) = (1-t)(1-q^r t)Z_r(t)$ denota o L -polinômio da extensão de corpo de constantes $F_r = F\mathbb{F}_{q^r}$, então

$$L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t) \quad (4.9)$$

onde os α_i 's são os mesmos do [item anterior](#).

■

Demonstração. Para gênero zero, pode-se mostrar usando o item 1 da Teorema 126 e a Teorema 133, que nesse caso o L -polinômio é constante igual a 1. Disso, seguem imediatamente todos os itens, exceto os itens 3 e 6. Para o item 3, vamos mostrar que qualquer que seja o corpo de funções $F/\mathbb{F}_q$ de gênero 0, seu número de classe é igual a 1, ou equivalentemente, que todo divisor de grau zero é principal. Mas isso é uma consequência do TEOREMA DE RIEMANN-ROCH. De fato, dado $A \in \text{Div}(F)$ de grau zero, como $0 > 2g - 2 = -2$, temos que $\ell(A) = \deg A + 1 - g = 1$, e daí podemos “encontrar” um elemento $0 \neq x$ tal que $(x) \geq -A$. Ambos esses divisores, (x) e A tem grau zero, logo a desigualdade anterior é na verdade uma igualdade e, portanto, $A = -(x) = (x^{-1})$ é principal. Já para o item 6, basta observarmos que se F tem gênero zero, então F_r também terá gênero zero (sendo uma extensão de corpo de constantes), qualquer que seja r (confira o item 3 do Teorema 128).

Com isso podemos supor que $g \geq 1$.

1. Já foi observado que $L(t)$ tem gênero $\leq 2g$. Veremos adiante que o coeficiente líder de $L(t)$ é q^g , de modo que $\deg L(t) = 2g$. A afirmação $L(t) \in \mathbb{Z}[t]$ segue de 4.7 se compararmos os coeficientes dos dois lados.
2. Segue da EQUAÇÃO FUNCIONAL DA FUNÇÃO ZETA.
3. Com notação como na Teorema 126, e usando o fato que $\partial = 1$, temos que

$$L(t) = (1-t)(1-qt)F(t) + \frac{h}{q-1}(q^g t^{2g-1}(1-t) - (1-qt))$$

Daí, por substituição direta, temos $L(1) = h$.

4. Escrevamos $L(t) = a_0 + a_1 t + \dots + a_{2g} t^{2g}$. Usando a equação funcional, obtemos

$$a_{2g} t^{2g} + a_{2g-1} t^{2g-1} + \dots + a_1 t + a_0 L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right) = \frac{a_{2g}}{q^g} + \frac{a_{2g-1}}{q^{g-1}} t + \dots + q^g a_0 t^{2g}$$

Daí, $a_{2g-1} = q^{g-1} a_1$ para $i = 0, \dots, g$. Comparando os coeficientes de t^0 e de t^1 em 4.7, temos que $a_0 = A_0$ e $a_1 = A_1 - (q+1)A_0$. Uma vez que $A_0 = 1$ e $A_1 = N$, obtemos $a_0 = 1$ e $a_1 = N - (q+1)$. Finalmente $a_{2g} = q^g a_0 = q^g$.

5. Consideremos o “polinômio inverso”

$$L^\perp(t) \doteq t^{2g} L\left(\frac{1}{t}\right) = a_0 t^{2g} + a_1 t^{2g-1} + \dots + a_{2g} = t^{2g} + a_1 t^{2g-1} + \dots + q^g$$

Temos que $L^\perp(t)$ é um polinômio mônico com coeficientes em $\mathbb{Z}$ (pois $L(t) \in \mathbb{Z}[t]$), logo, suas raízes são inteiros algébricos. Escrevamos

$$L^\perp(t) = \prod_{i=1}^{2g} (t - \alpha_i)$$

com $\alpha_i \in \mathbb{C}$. Temos então que

$$L(t) = t^{2g} L^\perp\left(\frac{1}{t}\right) = \prod_{i=1}^{2g} (1 - \alpha_i t)$$

Observemos que $L(\alpha_i^{-1}) = 0$ para $i = 1, \dots, 2g$ e que

$$\prod_{i=1}^{2g} \alpha_i = a_{2g} = q^g \quad (4.10)$$

Substituindo $t = qu$ e usando a [equação funcional](#), obtemos

$$\begin{aligned} \prod_{i=1}^{2g} (t - \alpha_i) &= L^\perp(t) = t^{2g} L\left(\frac{1}{t}\right) \\ &= q^{2g} u^{2g} L\left(\frac{1}{qu}\right) = q^g L(u) = q^g \cdot \prod_{j=1}^{2g} (1 - \alpha_j u) \\ q^g \cdot \prod_{j=1}^{2g} \left(1 - \frac{\alpha_j}{q} t\right) &= q^g \cdot \prod_{j=1}^{2g} \left(\frac{\alpha_j}{q} t - 1\right) = q^g \cdot \underbrace{\prod_{j=1}^{2g} \frac{\alpha_j}{q}}_{=1 \text{ por 4.10}} \cdot \prod_{j=1}^{2g} \left(t - \frac{q}{\alpha_j}\right) \\ &= \prod_{j=1}^{2g} \left(t - \frac{q}{\alpha_j}\right) \end{aligned} \quad (4.11)$$

Disso, vemos que podemos ordenar as raízes de $L^\perp(t)$ da seguinte maneira

$$\alpha_1, \frac{q}{\alpha_1}, \dots, \alpha_k, \frac{q}{\alpha_k}, q^{1/2}, \dots, q^{1/2}, -q^{1/2}, \dots, -q^{1/2} \quad (4.12)$$

onde $q^{1/2}$ “ocorre” m vezes e $-q^{1/2}$ “ocorre” n vezes. Por [4.10](#), temos que

$$\alpha_1 \cdot \frac{q}{\alpha_1} \cdot \dots \cdot \alpha_k \cdot \frac{q}{\alpha_k} \cdot (q^{1/2})^m \cdot (-q^{1/2})^n = q^g$$

Daí, temos que n é par, pois o lado direito da [equação anterior](#) é positivo. Como $n + m + 2k = 2g = \deg L^\perp(t)$, temos que m também é par e portanto podemos ordenar todas as raízes $\alpha_1, \dots, \alpha_{2g}$ de tal forma que $\alpha_i \alpha_{g+i} = q$ para $i = 1, \dots, g$ (basta “parearmos”, em [4.12](#), os elementos de mesma cor entre si, i.e., os vermelhos com

os vermelhos e os verdes com os verdes e, para os restantes, “pareamos” o α_i com o respectivo $q/\alpha\alpha_i$.

6. Usando a [Teorema 129](#) e a [definição](#) do L -polinômio obtemos

$$\begin{aligned} L_r(t^r) &= (1-t^r)(1-q^r t^r) Z_r(t^r) = (1-t^r)(1-q^r t^r) \prod_{\zeta^r=1} Z(\zeta t) \\ &= (1-t^r)(1-q^r t^r) \prod_{\zeta^r=1} \frac{L(\zeta t)}{(1-\zeta t)(1-q\zeta t)} = \prod_{\zeta^r=1} L(\zeta t) \\ &= \prod_{i=1}^{2g} \prod_{\zeta^r=1} (1-\alpha_i \zeta t) = \prod_{i=1}^{2g} (1-\alpha_i^r t^r) \end{aligned}$$

$$\text{Logo } L_r(t) = \prod_{i=1}^{2g} (1-\alpha_i^r t).$$

□

Corolário 135. Sendo N_r o número de lugares racionais do corpo de funções $F_r/\mathbb{F}_{q^r}$, temos, para todo $r \geq 1$

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r \quad (4.13)$$

onde os α_i 's são, como no [teorema anterior](#), os inversos das raízes do L -polinômio de $F/\mathbb{F}_q$. ■

Corolário 136. Seja $L(t) = \sum_{i=0}^{2g} a_i t^i$ o L -polinômio de $F/\mathbb{F}_q$ e sejam $S_r \doteq N_r - (q^r + 1)$. Temos então que

$$1. \quad L'(t)/L(t) = \sum_{r=1}^{\infty} S_r t^{r-1}$$

$$2. \quad a_0 = 1 \text{ e}$$

$$i a_i = S_i a_0 + S_{i-1} a_1 + \dots + S_1 a_{i-1} \quad (4.14)$$

4.2 O teorema de Hasse-Weil

O teorema a seguir, conjecturado por **Emil Artin** na década de 1920, foi mostrado primeiramente por **Helmut Hasse** no caso $g = 1$ na década de 1930. O caso geral foi mostrado por **André Weil** na década de 1940.

Teorema 137 (TEOREMA DE HASSE-WEIL). Os inversos das raízes de $L_F(t)$ satisfazem

$$|\alpha_i| = q^{1/2}$$

Observação 138. O [TEOREMA DE HASSE-WEIL](#) é também chamado de hipótese de Riemann para corpos de funções. Vejamos o porquê.

Podemos enxergar a função Zeta $Z_F(t)$ de um corpo de funções $F/\mathbb{F}_q$ como um “análogo” da função ζ de Riemann clássica

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

(com $s \in \mathbb{C}$ e $\text{Re}(s) > 1$) da seguinte maneira. Definimos a norma absoluta de um divisor $A \in \text{Div}(F)$ por

$$\mathcal{N}(A) \doteq q^{\deg A}$$

Para um divisor primo $P \in \mathbb{P}_F$, por exemplo, a norma absoluta $\mathcal{N}(P)$ é a cardinalidade do seu corpo residual F_P .

Daí, a função

$$\zeta_F(s) \doteq Z_F(q^{-s})$$

pode ser escrita como

$$\zeta_F(s) = \sum_{n=0}^{\infty} A_n q^{-sn} = \sum_{A \in \text{Div}(F), A \geq 0} \mathcal{N}(A)^{-s}$$

e esse é o análogo “apropriado” da função ζ clássica. É sabido que a função ζ clássica se estende analiticamente a uma função meroforma em $\mathbb{C}$. A hipótese de Riemann clássica afirma que, a não ser pelos zeros triviais, todos os zeros de $\zeta(s)$ são tais que $\text{Re}(s) = 1/2$.

No caso de corpos de funções, o [TEOREMA DE HASSE-WEIL](#) afirma que

$$\zeta_F(s) = 0 \Rightarrow Z_F(q^{-s}) = 0 \Rightarrow |q^{-s}| = q^{-1/2}$$

Notemos que na implicação anterior, usamos o fato de os zeros de $L(t)$ e $Z(t)$ coincidirem, pela [definição do \$L\$ -polinômio](#). (notemos também que, pelo item 3 do [Teorema 134](#), temos que $L(1) = h \geq 1$ e pela [equação funcional](#) “aplicada” em $t = 1/q$, temos que $L(1/q) = h/q^g \neq 0$). Como $|q^{-s}| = q^{-\text{Re}(s)}$, isso significa que

$$\zeta_F(t) = 0 \Rightarrow \operatorname{Re}(s) = 1/2$$

Daí o **TEOREMA DE HASSE-WEIL** pode ser visto como um análogo da hipótese de Riemann clássica. ■

O seguinte resultado, a célebre **COTA DE HASSE-WEIL**, é uma consequência imediata do **TEOREMA DE HASSE-WEIL** e do **Teorema 135**. Além disso, veremos **adiante** que o **TEOREMA DE HASSE-WEIL** em si é equivalente à existência de uma cota como esta.

Corolário 139 (COTA DE HASSE-WEIL). O número $N = N(F)$ de lugares racionais de $F/\mathbb{F}_q$ satisfaz a seguinte desigualdade

$$|N - (q + 1)| \leq 2gq^{1/2}$$

■

É claro que, usando o item 6 do **Teorema 134** e o **Teorema 135**, obtemos

$$|N_r - (q^r + 1)| \leq 2gq^{r/2} \quad (4.15)$$

Em lugar de demonstrar detalhadamente o **TEOREMA DE HASSE-WEIL**, faremos um roteiro da demonstração devida a **Enrico Bombieri**, enunciando resultados sem demonstrar.

Lema 140. O **TEOREMA DE HASSE-WEIL** é válido para $F/\mathbb{F}_q$ se, e somente se, o for para $F_m/\mathbb{F}_{q^m}$, para um dado $m \geq 1$. ■

Lema 141. Suponha que exista uma constante $c \in \mathbb{R}$ tal que para todo $r \geq 1$ seja válida a seguinte desigualdade

$$|N_r - (q^r + 1)| \leq cq^{1/2}$$

Então o **TEOREMA DE HASSE-WEIL** é válido para $F/\mathbb{F}_q$. ■

Observemos que a hipótese do **lema anterior** é equivalente à existência de uma cota inferior e de uma cota superior para os números N_r , i.e., à existência de números c_1 e $c_2 \in \mathbb{R}_{>0}$ tais que

$$N_r \leq q + 1 + c_1q^{1/2} \quad (4.16)$$

e

$$N_r \geq q + 1 - c_2q^{1/2} \quad (4.17)$$

para todo $r \geq 1$.

O Teorema 140 nos garante a validade do TEOREMA DE HASSE-WEIL para $F/\mathbb{F}_q$ uma vez que mostrarmos a sua validade em $F_m/\mathbb{F}_{q^m}$ para algum m apropriado. A validade do TEOREMA DE HASSE-WEIL para $F_m/\mathbb{F}_{q^m}$, por sua vez, será garantida se mostrarmos as desigualdades 4.16 e 4.17 para todo $r \geq 1$ (com q^m no lugar de q). Isso nos permite assumir, sem perda de generalidade, que q é um quadrado tal que $q > (g+1)^4$ (lembremos que o gênero é invariante por extensões do corpo das constantes). Sob essas suposições temos garantida a existência de c_1 como em 4.16, segundo a seguinte

Proposição 142. Seja $F/\mathbb{F}_q$ um corpo de funções tal que q é um quadrado e $q > (g+1)^4$, onde g é o gênero de $F/\mathbb{F}_q$. Então o número $N = N(F)$ de lugares racionais de $F/\mathbb{F}_q$ pode ser estimado por

$$N < (q+1) + (2g+1)q^{1/2}$$

■

Note que, se $F/\mathbb{F}_q$ é como anteriormente, para qualquer $r \geq 1$, q^r será um quadrado tal que $q^r > q > (g+1)^4 = (g_r+1)^4$, onde g_r denota o gênero de $F_r/\mathbb{F}_{q^r}$. Daí, a estimativa anterior também é válida, com N_r no lugar de N e q^r no lugar de q , para todo $r \geq 1$.

Resta agora mostrarmos a existência de c_2 . Feito isso, o TEOREMA DE HASSE-WEIL seguirá.

Para tal, consideremos uma extensão galoisiana E/L de corpos de funções de grau $[E:L] = m$ e tal que $\mathbb{F}_q$ é todo o corpo das constantes de L e de E . Seja $n > 0$ um inteiro divisível por m e sejam $E' \doteq E\mathbb{F}_{q^n}$ e $L' \doteq L\mathbb{F}_{q^n} \subset E'$. Então E'/L é de Galois com grupo de Galois $G' = \langle \sigma \rangle \times G$, onde $G \doteq \text{Gal}(E'/L') \simeq \text{Gal}(E/L)$ e σ é o automorfismo de Frobenius de E'/E (i.e., $\sigma(z) = z$ para $z \in E$ e $\sigma(\alpha) = \alpha^q$ para $\alpha \in \mathbb{F}_{q^n}$).

Para um grupo G' que é dado pelo produto direto

$$G' = \langle \sigma \rangle \times G$$

de um subgrupo cíclico $\langle \sigma \rangle$ de ordem n e de um subgrupo $G \geq G'$ de ordem m , com n divisível por m , temos que existem m subgrupos distintos de G' que denotaremos por U_i , $i = 1, \dots, m$, tais que cada U_i é cíclico de ordem n e tais que $U_i \cap G = \{1\}$, a identidade de G' . Além disso, se H é um subgrupo de G' de ordem $n \cdot e$ e tal que a ordem de $H \cap G$ é e , então H contém e dos m subgrupos U_i anteriores.

Voltando às extensões de corpos de funções, a discussão anterior pode ser aplicada ao grupo de Galois G' da extensão E'/L : G' contém exatamente m subgrupos cíclicos de ordem n que interceptam G apenas na identidade, que denotaremos por U_i , $i = 1, \dots, m$.

Tomemos $U_1 = \langle \sigma \rangle$. Denotemos por E_i o corpo fixo correspondente a U_i , para $i = 1, \dots, m$. Então $E_1 = E$ e a situação pode ser melhor entendida através do diagrama a seguir.

Denotemos por $g(E_i)$ e por $N(E_i)$ os gênero e número de lugares racionais de E_i , respectivamente. Denotemos, também, por $N(L)$ o número de lugares racionais de L .

Proposição 143. Na situação descrita anteriormente, temos que

1. $\mathbb{F}_q$ é todo o corpo das constantes de E_i , para $i = 1, \dots, m$.
2. $E' = E_i\mathbb{F}_{q^n}$ e $g(E_i) = g(E)$, para $i = 1, \dots, m$.
3. $m \cdot N(L) = \sum_{i=1}^m N(E_i)$

Para mostrar a existência da constante c_2 que dá a [cota inferior](#) para os números N_r , vamos usar a [proposição anterior](#) para dois casos: E'/F e E'/F_0 com $F_0 \subset F$. Daí o item 3 da [mesma proposição](#) nos permitirá comparar o número de lugares racionais de F com o número de lugares racionais de F_0 e, desde que escolhamos F e F_0 “bem”, teremos a cota inferior 4.17. Então, começamos com um corpo de funções $F/\mathbb{F}_q$, para o qual queremos mostrar a cota cla. Podemos escolher um subcorpo racional $F_0 = \mathbb{F}_q(t) \subset F$ tal que F/F_0 é separável. Escolhemos também uma extensão finita $E \supset F$ tal que E/F_0 é de Galois (se o leitor duvidar que um tal F_0 exista, recomendamos que confira sitchtenoth seção 3.10 cla). É possível que o corpo de constantes de E seja uma extensão própria $\mathbb{F}_{q^d}$ de $\mathbb{F}_q$. Se for este o caso, consideramos $F\mathbb{F}_{q^d}$ e $F_0\mathbb{F}_{q^d} = \mathbb{F}_{q^d}(t)$ no lugar de F e F_0 , respectivamente. Nesse caso, a extensão $E/F_0\mathbb{F}_{q^d}$ continua sendo de Galois e, como [já foi observado anteriormente](#), basta mostrarmos a validade do [TEOREMA DE HASSE-WEIL](#) para o corpo de funções $F\mathbb{F}_{q^d}/\mathbb{F}_{q^d}$. Com isso em mente, supomos, sem perda de generalidade, que $\mathbb{F}_q$ é todo o corpo das constantes de E e também que q é um quadrado tal que $q > (g(E) + 1)^4$ (como na [Teorema 142](#)).

Seja $m \triangleq [E : F]$ e $n \triangleq [E : F_0]$, de modo que n é divisível por m , e consideremos as extensões de corpo de constantes $E' \triangleq E\mathbb{F}_{q^n}$, $F' \triangleq F\mathbb{F}_{q^n}$ e $F'_0 \triangleq F_0\mathbb{F}_{q^n}$. Observe as torres de extensões de corpos a seguir.

Vamos usar a [Teorema 143](#) nas extensões da esquerda e da direita anteriores. Observe que, para a extensão da direita temos que os números m e n da [proposição](#) são ambos iguais a n . Para a extensão da esquerda, como foi discutido anteriormente, temos que existem exatamente m subgrupos cíclicos $V_1, \dots, V_m \subset \text{Gal}(E'/F)$ de ordem n cada e tal que cada um intercepta $\text{Gal}(E'/L') \simeq \text{Gal}(E/L)$ na identidade. Por outro lado, para a extensão da direita, temos que existem exatamente n subgrupos cíclicos $U_1, \dots, U_n \subset \text{Gal}(E'/F_0)$ de ordem n cada e tal que cada U_i intercepta $\text{Gal}(E'/F'_0)$ na identidade. Notando que o compósito de E' e F'_0 é o corpo fixo correspondente a V_i , para $i = 1, \dots, m$, concluímos que cada V_i também intercepta $\text{Gal}(E'/F'_0)$ apenas na identidade. Logo m dos n subgrupos U_i são os subgrupos V_i , e podemos supor que $V_i = U_i$, para $i = 1, \dots, m$. Denotemos por E_i o corpo correspondente a U_i , para $i = 1, \dots, n$. O item 3 da [Teorema 143](#) aplicado à extensão da esquerda nos diz que

$$m \cdot N(F) = \sum_{i=1}^m N(E_i) \quad (4.18)$$

e o mesmo resultado aplicado à extensão da direita nos dá

$$n \cdot N(F_0) = \sum_{i=1}^n N(E_i) \quad (4.19)$$

Como as hipóteses da [Teorema 142](#) são satisfeitas, temos que a seguinte desigualdade (lembremos que $g(E_i) = g(E)$ para todo i)

$$N(E_i) \leq q + 1 + (2g(E) + 1)q^{1/2}$$

é válida para todo $i = 1, \dots, n$. Como $F_0 = \mathbb{F}_q(t)$ é um corpo de funções racionais, temos que $N(F_0) = q + 1$: q polinômios mônicos lineares distintos mais o pólo de t (também podemos ver isso pelo Teorema 134). Daí, combinando 4.18 e 4.19, obtemos

$$\begin{aligned} m \cdot N(F) &= n \cdot N(F_0) + \sum_{i=1}^m N(E_i) - \sum_{i=1}^n N(E_i) \\ &= n(q+1) - \sum_{i=m+1}^n N(E_i) \\ &\geq n(q+1) - (n-m)(q+1 + (2g(E)+1)q^{1/2}) \\ &= m(q+1) - (n-m)(2g(E)+1)q^{1/2} \end{aligned}$$

Daí

$$N(F) \geq q+1 - \frac{n-m}{m}(2g(E)+1)q^{1/2}$$

Lembremos que os números n , m e $g(E)$ são invariantes por extensões de corpo de constantes. Assim sendo, mostramos a existência de uma constante $c_2 > 0$ tal que, para todo $r \geq 1$, temos

$$N_r \geq q^r + 1 - c_2 q^{r/2}$$

a saber, $c_2 = \frac{n-m}{m}(2g(E)+1)$. Disso e de toda a discussão anterior segue o **TEOREMA DE HASSE-WEIL**.

Observemos que se $n = m$, então $F = F_0$, ou seja F , e portanto todos os F_r , serão racionais, logo $N_r = q + 1$. Observemos também que temos uma certa liberdade para escolher os números n , m e $g(E)$, de modo que, escolhendo valores apropriados, podemos obter cotas inferiores boas.

Vamos introduzir uma quantidade e mostrar uma relação que voltará a aparecer no capítulo seguinte.

Definição 144. Dado um corpo de funções $F/\mathbb{F}_q$ definimos

$$B_r \doteq B_r(F) \doteq |\{P \in \mathbb{P}_F \mid \deg P = r\}|$$

Vejamos que os números B_r são distintos dos números A_n introduzidos na Teorema 123. Notemos também que $B_1 = N(F)$. É uma consequência direta do item 4 do Teorema 128

a seguinte relação

$$N_r = \sum_{d|r} d \cdot B_d \quad (4.20)$$

onde a soma é feita sobre os inteiros $d \geq 1$ que dividem r . A fórmula de inversão de Möbius converte 4.20 em

$$r \cdot B_r = \sum_{d|r} \mu\left(\frac{r}{d}\right) \cdot N_d \quad (4.21)$$

onde $\mu : \mathbb{Z}_{\geq 1} \rightarrow \{-1, 0, 1\}$ é a função de Möbius.

O resultado a seguir é uma consequência imediata de 4.21 e 4.15.

Corolário 145.

1. A seguinte estimativa

$$\left| B_r - \frac{q^r}{r} \right| \leq \left(\frac{q}{q+1} + 2g \frac{q^{1/2}}{q^{1/2}-1} \right) \cdot \frac{q^{r/2}-1}{r} < (2+7g) \cdot \frac{q^{r/2}}{r}$$

é válida para todo $r \geq 1$ (exceto para $(q, g, r) = (2, 0, 1)$).

2. Se $g = 0$ então $B_r \geq 1$ para todo $r \geq 1$.

3. Para cada r tal que $2g+1 \leq q^{(r-1)/2}(q^{1/2}-1)$, existe pelo menos um lugar de grau r . Em particular, se $r \geq 4g+3$ então $B_r \geq 1$. ■

4.3 Melhoramentos da cota de Hasse-Weil

Denotando por $\lfloor x \rfloor$ a parte inteira de um número real x , é claro que, sendo N e q números inteiros, a seguinte estimativa vale

$$|N - (q+1)| \leq \lfloor 2gq^{1/2} \rfloor$$

Fixado q , o crescimento da função $\lfloor 2gq^{1/2} \rfloor$ é da ordem $2q^{1/2}$. O seguinte resultado, cuja demonstração é, na opinião do autor, apoteótica, nos diz que na verdade a quantidade $|N - (q+1)|$ pode ser limitada por uma função (em g) de crescimento $\lfloor 2q^{1/2} \rfloor$, que é substancialmente melhor no caso de q não ser um quadrado.

Teorema 146 (COTA DE SERRE). Para um corpo de funções $F/\mathbb{F}_q$ de gênero g o número de lugares racionais é limitado por

$$|N - (q + 1)| \leq g \lfloor 2q^{1/2} \rfloor$$

■

Demonstração. Seja $\mathbb{A} \subset \mathbb{C}$ o conjunto dos inteiros algébricos, i.e., $\mathbb{A}$ consiste de todas as raízes de todos os polinômios mônicos com coeficientes em $\mathbb{Z}$. “Da teoria dos números”, sabemos que $\mathbb{A}$ é um subanel de $\mathbb{C}$ e que $\mathbb{A} \cap \mathbb{Q} = \mathbb{Z}$. Vamos supor, sem perda de generalidade, que $g \geq 1$. Seja $L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t)$ o L -polinômio de $F/\mathbb{F}_q$. Nas seções anteriores vimos que os números complexos $\alpha_1, \dots, \alpha_{2g}$ são inteiros algébricos (confira o item 5 do Teorema 134) de módulo $|\alpha_i| = q^{1/2}$ (confira o TEOREMA DE HASSE-WEIL. Vimos também que podemos indexá-los de forma que $\alpha_i \alpha_{g+i} = q$, ou seja, tal que $\overline{\alpha_i} = \alpha_{g+i} = q/\alpha_i$ (aqui $\bar{z}$ denota o conjugado z) para $1 \leq i \leq g$. Coloquemos

$$\gamma_i \doteq \alpha_i + \overline{\alpha_i} + \lfloor 2q^{1/2} \rfloor + 1 \quad (4.22)$$

e

$$\delta_i \doteq -(\alpha_i + \overline{\alpha_i}) + \lfloor 2q^{1/2} \rfloor + 1 \quad (4.23)$$

Como $\mathbb{A}$ é subanel de $\mathbb{C}$, γ_i e δ_i são inteiros algébricos reais para $i = 1, \dots, g$. Além disso, como $|\alpha_i + \overline{\alpha_i}| \leq 2q^{1/2} < \lfloor 2q^{1/2} \rfloor + 1$, temos que $\gamma_i > 0$ e $\delta_i > 0$.

Cada mergulho $\sigma : \mathbb{Q}(\alpha_1, \dots, \alpha_{2g}) \rightarrow \mathbb{C}$ é uma permutação do conjunto $\{\alpha_1, \dots, \alpha_{2g}\}$. De fato, os α_i 's são raízes do polinômio $L^\perp(t) = t^{2g} L(1/t) = \prod_{i=1}^{2g} (t - \alpha_i) \in \mathbb{Z}[t]$. Mais ainda, notemos que se $\sigma(\alpha_i) = \alpha_j$ então

$$\sigma(\overline{\alpha_i}) = \sigma(q/\alpha_i) = q/\sigma(\alpha_i) = \overline{\sigma(\alpha_i)} = \overline{\alpha_j} \quad (4.24)$$

Logo $\sigma(\gamma_i) = \gamma_j$ e $\sigma(\delta_i) = \delta_j$. Definimos $\gamma \doteq \prod_{i=1}^g \gamma_i$ e $\delta \doteq \prod_{i=1}^g \delta_i$. É claro que γ e δ são inteiros algébricos. Mais ainda, eles são fixos por todos os mergulhos de $\mathbb{Q}(\alpha_1, \dots, \alpha_{2g})$ em $\mathbb{C}$, ou seja, γ e δ pertencem ao corpo fixo por $\text{Gal}(\mathbb{Q}(\alpha_1, \dots, \alpha_{2g})/\mathbb{Q})$ que é $\mathbb{Q}$. Logo, $\gamma, \delta \in \mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$. Como cada γ_i e cada δ_i é estritamente positivo, γ e δ são estritamente positivos. Sendo, também, γ e δ inteiros, temos que $\prod_{i=1}^g \gamma_i \geq 1$ e $\prod_{i=1}^g \delta_i \geq 1$. Usando a conhecida desigualdade entre as médias aritmética e geométrica, temos que

$$\frac{1}{g} \sum_{i=1}^g \gamma_i \geq \left(\prod_{i=1}^g \gamma_i \right)^{1/g} \geq 1$$

Logo

$$g \leq \left(\sum_{i=1}^g (\alpha_i + \bar{\alpha}_i) \right) + g \lfloor 2q^{1/2} \rfloor + g = \sum_{i=1}^{2g} \alpha_i + g \lfloor 2q^{1/2} \rfloor + g$$

Na última igualdade, usamos o fato que $\bar{\alpha}_i = \alpha_{g+i}$. Ora, o [Teorema 135](#) nos diz que $\sum_{i=1}^{2g} \alpha_i = q + 1 - N$. Com isso, a última expressão se torna

$$N \leq q + 1 + g \lfloor 2q^{1/2} \rfloor$$

Repetindo o raciocínio anterior para δ_i no lugar de γ_i , obtemos

$$N \geq q + 1 + g \lfloor 2q^{1/2} \rfloor$$

□

Os números γ e δ que apareceram na demonstração não são “piores” do que os números

$$\gamma' = \sum_{i=1}^g \gamma_i$$

e

$$\delta' = \sum_{i=1}^g \delta_i$$

Então, se usarmos γ' e δ' no lugar de γ e δ , obtemos novas estimativas para N . Entretanto, se observarmos que

$$\gamma' = \sum_{i=1}^g \gamma_i \geq \frac{1}{g} \sum_{i=1}^g \gamma_i$$

e analogamente para δ' , vemos porque a escolha de γ e δ é preferível.

A [COTA DE HASSE-WEIL](#) não pode ser melhorada em geral: existem corpos de funções $F/\mathbb{F}_q$ tais que $N(F) = q + 1 + 2g\sqrt{q}$. Tais corpos são chamados de maximais. O próximo resultado nos diz que para que um corpo de funções seja maximal seu gênero não pode ser grande em comparação com q .

Proposição 147 (YASUTAKA IHARA). Suponha que $F/\mathbb{F}_q$ seja um corpo de funções maximal. Então $g \leq (q - q^{1/2})/2$. ■

Demonstração. Supondo $F/\mathbb{F}_q$ maximal, temos que $N = q + 1 + 2gq^{1/2}$. Por outro lado, pelo [Teorema 135](#), também temos que $N = q + 1 - \sum_{i=1}^{2g} \alpha_i$, onde $|\alpha_i| = q^{1/2}$. Com isso, temos que $\sum_{i=1}^{2g} \alpha_i = -2gq^{1/2}$. Daí, devemos ter

$$\alpha_i = -q^{1/2} \quad (4.25)$$

Sendo N_2 o número de lugares racionais da extensão do corpo de constantes $F\mathbb{F}_{q^2}/\mathbb{F}_{q^2}$, temos novamente pelo [Teorema 135](#) e por 4.25

$$N_2 = q + 1 - \sum_{i=1}^{2g} \alpha_i^2 = q + 1 + 2gq$$

Ora, mas como $N \leq N_2$, por 4.20, o resultado segue substituindo os valores de N e N_2 na desigualdade $N \leq N_2$.

□

A estimativa anterior também não pode ser melhorada, existem corpos de funções maximais cujo gênero é $(q - q^{1/2})/2$.

A demonstração anterior pode ser “refinada” de modo a obtermos outras cotas para o número de lugares racionais de $F/\mathbb{F}_q$. O “refinamento” apresentado a seguir foi feito primeiramente por **Jean-Pierre Serre**.

Seja N_r como no [Teorema 135](#). Para $i = 1, \dots, 2g$, definamos

$$\omega_i \doteq \alpha_i q^{-1/2} \quad (4.26)$$

onde os α_i 's são, como sempre, os inversos das raízes do L -polinômio de $F/\mathbb{F}_q$. Pelo [TEOREMA DE HASSE-WEIL](#), temos que os ω_i 's são números complexos de módulo 1. Além disso, podemos supor, como na demonstração da [COTA DE SERRE](#), que

$$\omega_{g+i} = \bar{\omega}_i = \omega_i^{-1}$$

Pelo [Teorema 135](#) e pela [equação anterior](#), temos que

$$N_r q^{-r/2} = q^{r/2} + q^{-r/2} - \sum_{i=1}^g (\omega_i^r + \omega_i^{-r}) \quad (4.27)$$

Dados m números reais $c_1, \dots, c_m$, multiplicando 4.27 por c_r , obtemos

$$N_1 c_r q^{-r/2} = c_r q^{r/2} + c_r q^{-r/2} - \sum_{i=1}^g c_r (\omega_i^r + \omega_i^{-r}) - (N_r - N_1) c_r q^{-r/2} \quad (4.28)$$

Definindo

$$\lambda_m(t) \doteq \sum_{r=1}^m c_r t^m \quad (4.29)$$

e

$$f_m(t) \doteq 1 + \lambda_m(t) + \lambda_m t^{-1} \quad (4.30)$$

para $t \in \mathbb{C} \setminus \{0\}$, temos, somando as equações 4.28 para $r = 1, \dots, m$

$$N_1 \lambda_m(q^{-1/2}) = \lambda_m(q^{1/2}) + \lambda_m(q^{-1/2}) + g - \sum_{i=1}^g f_m(\omega_i) - \sum_{i=1}^m (N_r - N_1) c_r q^{-r/2} \quad (4.31)$$

Notemos que $f_m(t) \in \mathbb{R}$ se $|t| = 1$. A equação anterior nos permitirá obter estimativas boas para $N = N_1$ desde que escolhamos apropriadamente as constantes c_r .

Proposição 148 (FÓRMULAS EXPLÍCITAS DE SERRE). Suponhamos que $c_1, \dots, c_m \in \mathbb{R}$ satisfaçam as seguintes condições

1. $c_r \geq 0$ para $r = 1, \dots, m$ e $c_i \neq 0$ para pelo menos um i .
2. $f_m(t) \geq 0$ para todo $t \in \mathbb{C}$ com $|t| = 1$, onde $f_m(t)$ é como em 4.30.

Então o número de lugares racionais de $F/\mathbb{F}_q$ é limitado da seguinte maneira

$$N \leq \frac{g}{\lambda_m(q^{-1/2})} + \frac{\lambda_m(q^{1/2})}{\lambda_m(q^{-1/2})} + 1$$

onde $\lambda_m(t)$ é como em 4.29. ■

Demonstração. Como $N_1 \leq N_r$ para todo $r \geq 1$, a equação 4.31 juntamente com as condições 1 e 2 implicam

$$N \cdot \lambda_m(q^{-1/2}) \leq \lambda_m(q^{1/2}) + \lambda_m(q^{-1/2}) + g$$

Dividindo ambos os lados da desigualdade anterior por $\lambda_m(q^{-1/2})$ (que é um número real positivo pela condição 1), resulta na desigualdade do enunciado. □

4.4 A constante de Ihara

Vimos na [Teorema 147](#) que um corpo de funções pode atingir a [COTA DE HASSE-WEIL](#) somente se $g \leq (q - q^{1/2})/2$. É natural nos perguntarmos como N , o número de lugares racionais de um corpo de funções $F/\mathbb{F}_q$ de gênero g , se comporta com relação à g (fixado q). Para uma tal investigação é conveniente definirmos as seguintes quantidades que voltarão a aparecer no capítulo 5.

Definição 149. Para cada inteiro $g \geq 0$, definimos

$$N_q(g) \doteq \max\{N(F) \mid F \text{ é um corpo de funções de gênero } g \text{ sobre } \mathbb{F}_q\} \quad (4.32)$$

O número real

$$A(q) \doteq \limsup_{g \rightarrow \infty} \frac{N_q(g)}{g} \quad (4.33)$$

é chamado de constante de Ihara. ■

A [COTA DE SERRE](#) nos dá trivialmente a limitação $0 \leq A(q) \leq \lfloor 2q^{1/2} \rfloor$. Fazendo uso das [FÓRMULAS EXPLÍCITAS DE SERRE](#), temos o seguinte importante resultado

Teorema 150 (COTA DE DRINFEL'D-VLĀDUŢ). A constante de Ihara $A(q)$ é limitada superiormente por

$$A(q) \leq q^{1/2} - 1$$

Demonstração. Dado um inteiro $m \geq 1$, coloquemos

$$c_r \doteq 1 - \frac{r}{m} \quad \text{para } r = 1, \dots, m$$

Então é claro que $c_r \geq 0$ para todo r e nem todos c_r 's são nulos. Ou seja, temos válida a condição 1 da [Teorema 148](#). As funções λ_m são, então

$$\lambda_m(t) = \sum_{r=1}^m \left(1 - \frac{r}{m}\right) t^r$$

Para verificarmos a condição 2 da [Teorema 148](#), consideremos a função

$$u(t) \doteq \sum_{r=1}^m t^r = \frac{t^{m+1} - t}{t - 1}$$

De $u'(t) = \sum_{r=1}^m r t^{r-1}$, temos que

$$\frac{t \cdot u'(t)}{m} = \sum_{r=1}^m \frac{r}{m} t^r$$

Daí, depois de algumas manipulações algébricas, podemos escrever as funções λ_m da seguinte maneira

$$\begin{aligned} \lambda_m(t) &= \sum_{r=1}^m \left(1 - \frac{r}{m}\right) t^r = u(t) - \frac{t \cdot u'(t)}{m} \\ &= \frac{t}{t-1} (t^m - 1) - \frac{t}{m} \cdot \frac{(t-1)((m+1)t^m - 1) - (t^{m+1} - t)}{(t-1)^2} \\ &= \frac{t}{(t-1)^2} \left(\frac{t^m - 1}{m} + 1 - t \right) \end{aligned}$$

Substituindo a expressão acima para $\lambda_m(t)$ em $f_m(t) = 1 + \lambda_m(t) + \lambda_m(t^{-1})$, vemos que aparecerão os termos

$$\frac{t}{(t-1)^2} (1-t) = -\frac{t}{t-1}$$

e

$$\frac{t^{-1}}{(t^{-1}-1)^2} (1-t^{-1}) = -\frac{t^{-1}}{t^{-1}-1} = +\frac{1}{t-1}$$

Daí

$$1 - \frac{t}{t-1} + \frac{1}{t-1} = 0$$

e obtemos para $f_m(t)$ a seguinte expressão

$$f_m(t) = \frac{1}{m} \left(\frac{t(t^{-1}-1)^2(t^m-1) + t^{-1}(t-1)^2(t^{-m}-1)}{(t-1)^2(t^{-1}-1)^2} \right)$$

Ora mas $t(t^{-1}-1)^2 = (1-t)(t^{-1}-1) = (1-t^{-1})(t-1) = t^{-1}(t-1)^2$, logo

$$f_m(t) = \frac{2 - (t^m + t^{-m})}{m(t-1)(t^{-1}-1)}$$

Sabendo que $t^{-1} = \bar{t}$ para $t = \exp(i\theta)$, temos finalmente que

$$f_m(t) = f_m(\theta) = \frac{1}{m} \frac{1 - \cos(m\theta)}{1 - \cos(\theta)}$$

Da [equação anterior](#), fica fácil ver que $f_m(t) \geq 0$ para todo $t \in \mathbb{C}$ com $|t| = 1$ (se $t = 1$, o limite da equação anterior quando θ vai pra zero é m que é igual ao valor de $f_m(t)$ fazendo $t = 1$ nas [expressões para \$\lambda_m\(t\)\$](#)). Ou seja, temos válida a condição 2 das [FÓRMULAS EXPLÍCITAS DE SERRE](#).

Uma vez que as condições para aplicação das [FÓRMULAS EXPLÍCITAS DE SERRE](#) são satisfeitas, a desigualdade [148](#) aplicada nesse caso nos fornece

$$\frac{N}{g} \leq \frac{1}{\lambda_m(q^{-1/2})} + \frac{1}{g} \left(1 + \frac{\lambda_m(q^{1/2})}{\lambda_m(q^{-1/2})} \right) \quad (4.34)$$

onde N é o número de lugares racionais de um corpo de funções $F/\mathbb{F}_q$ arbitrário de gênero g . De [4.11](#), temos

$$\lambda_m(q^{-1/2}) \xrightarrow{m \rightarrow \infty} \frac{q^{-1/2}}{(q^{-1/2} - 1)^2} (1 - q^{-1/2}) = \frac{1}{q^{1/2} - 1}$$

Uma vez que a sequência $\lambda_m(q^{-1/2})$ converge para $1/(q^{1/2} - 1)$, a sequência dos inversos, $\lambda_m(q^{-1/2})^{-1}$ também converge e para $q^{1/2} - 1$. Logo, para qualquer $\varepsilon > 0$, existe $m_0 \in \mathbb{Z}_{\geq 1}$ tal que

$$\lambda_{m_0}(q^{-1/2})^{-1} < q^{1/2} - 1 + \varepsilon/2$$

Como

$$\frac{1}{g} \left(1 + \frac{\lambda_m(q^{1/2})}{\lambda_m(q^{-1/2})} \right) \xrightarrow{g \rightarrow \infty} 0$$

existe $g_0 \in \mathbb{Z}_{\geq 1}$ tal que para todo $g \geq g_0$ vale

$$\frac{1}{g} \left(1 + \frac{\lambda_{m_0}(q^{1/2})}{\lambda_{m_0}(q^{-1/2})} \right) < \frac{\varepsilon}{2}$$

Daí, usando [4.34](#), temos

$$\frac{N}{g} < q^{1/2} - 1 + \varepsilon$$

para todo $g \geq g_0$ e para todos os corpos de funções $F/\mathbb{F}_q$ de gênero g , em particular para um que tenha $N_q(g)$ lugares racionais. Isso finaliza a demonstração. □

A seguir, estão listados alguns fatos sobre a constante de Ihara $A(q)$.

1. $A(q) > 0$ para todas as potências de números primos, i.e., para todo número $q = p^n$ com p um número primo e $n \in \mathbb{Z}_{\geq 1}$. Mais precisamente, $A(q) \geq c \cdot \log q$ para todo q . Esse resultado é devido à [Serre \(1983\)](#)
2. Se $q = \ell^2$ é um quadrado então $A(q) = q^{1/2} - 1$, ou seja, no caso de q ser uma potência par de um número primo a [COTA DE DRINFEL'D-VLĂDUȚ](#) é atingida. Essa igualdade foi primeiramente demonstrada por [Ihara \(1981\)](#) e depois por [Tsfasman, Vlăduț e Zink \(1982\)](#) usando a teoria de curvas modulares. Uma demonstração mais elementar e prática foi dada por [Garcia e Stichtenoth \(1996\)](#).
3. Se $q = \ell^3$ é um cubo, então $A(q) \geq 2(\ell^2 - 1)/(\ell + 2)$. Para ℓ um número primo, este resultado foi mostrado por [Zink \(1985\)](#). Para um ℓ arbitrário, a cota anterior foi demonstrada primeiramente por [Bezerra, Garcia e Stichtenoth \(2005\)](#) e depois foi simplificada por [Bassa, Garcia e Stichtenoth \(2008\)](#).
4. O valor exato de $A(q)$ não é conhecido para nenhum q que não é quadrado.

CORPOS DE FUNÇÕES COM UM NÚMERO PRESCRITO DE LUGARES RACIONAIS

5.1 Lemas preliminares

Definição 151. Dada uma potência q de um número primo, colocamos

$$\mathcal{M}_q = \{(N, g) \mid \exists F/\mathbb{F}_q \text{ de gênero } g \text{ com } N \text{ lugares racionais}\}$$

■

Lema 152. Seja E um corpo de funções sobre $\mathbb{F}_q$ de gênero $g(E) \geq 2$, e seja r um inteiro tal que $r \geq 2g(E) + 1$. Então existe (pelo menos) um lugar $\mathbb{P}_E$ de grau r . ■

Demonstração. Usando a notação introduzida no [Teorema 135](#) e na [Teorema 144](#), e colocando $g \doteq g(E)$ (aqui ainda não precisaremos de $g(E) \geq 2$) vamos mostrar, primeiramente, que para todo $d \geq 1$ temos que

$$B_d > (q^d - (6g + 3)q^{d/2})/d \quad (5.1)$$

Para isso, vamos usar a [COTA DE HASSE-WEIL](#) (na forma [4.15](#)) em [4.21](#) para cada m que divide d . Como $\mu(k) \geq -1$ para todo $k \in \mathbb{Z}$ e como $\mu(1) = \mu(d/d) = 1$, temos então que

$$d \cdot B_d \geq q^d + 1 - 2gq^{d/2} - \sum_{\substack{m|d \\ 1 \leq m < d}} (q^m + 1 + 2gq^{m/2}) \quad (5.2)$$

Para todo $d \geq 1$ temos que

$$q + q^2 + \dots + q^{\lfloor d/2 \rfloor} < 2q^{d/2} \quad (5.3)$$

De fato, para $d = 1$, 5.3 é trivial: $q^{\lfloor 1/2 \rfloor} = q^0 = 1 < 2q^{1/2}$. Para $d \geq 2$, temos

$$q + q^2 + \dots + q^{\lfloor d/2 \rfloor} = q(1 + q + \dots + q^{\lfloor d/2 \rfloor - 1}) = \frac{q(q^{\lfloor d/2 \rfloor} - 1)}{q - 1} \leq \frac{2(q - 1)(q^{\lfloor d/2 \rfloor} - 1)}{q - 1} < 2q^{\lfloor d/2 \rfloor} \quad (5.4)$$

Daí, 5.3 é válida para todo $d \geq 1$. Com isso, podemos estimar a soma que aparece em 5.2 da seguinte maneira

$$\sum_{\substack{m|d \\ 1 \leq m < d}} (q^m + 1 + 2gq^{m/2}) < \sum_{1 \leq m \leq d/2} ((2g + 1)q^m + 1) < (4g + 2)q^{d/2} + d/2 \quad (5.5)$$

Na desigualdade em vermelho, usamos $q^{m/2} < q^m$ e o fato que se $m|d$ e $m < d$ então $m \leq d/2$. Já na desigualdade em verde, usamos 5.3. Daí, substituindo 5.5 em 5.2, obtemos

$$\begin{aligned} d \cdot B_d &> q^d + 1 - 2gq^{d/2} - (4g + 2)q^{d/2} - d/2 \\ &= q^d - (6g + 2)q^{d/2} - d/2 + 1 > q^d - (6g + 3)q^{d/2} \end{aligned} \quad (5.6)$$

onde, na desigualdade em vermelho, usamos o fato que $d/2 - 1 < d/2 < q^{d/2}$ (lembrando que $q \geq 2$). Daí, dividindo ambos os lados de 5.6 por d , temos 5.1.

Agora, suponhamos que $g \geq 2$ e que $r \geq 2g + 1$. Suponhamos, primeiramente que $q \geq 3$. Temos então que

$$q^{r/2} \geq q^{(g+1)/2} \geq 3^{(g+1)/2} \quad (5.7)$$

onde a última desigualdade segue do fato de $q^{g+1/2}$ ser crescente (como função de q). Vamos mostrar que $3^{(g+1)/2} > 6g + 3$. Juntando isso com 5.7 teremos, depois de multiplicar por $q^{r/2}$, $q^r - (6g + 3)q^{r/2} > 0$. Daí, usando 5.1, obteremos $B_r > 0$. Temos que $((2 + 1)/2) \cdot \log(3) - \log(6 \cdot 2 + 3) > 0$ e, como a função $((g + 1)/2) \cdot \log(3) - \log(6 \cdot g + 3)$ é crescente para $g \geq 2$ (pois sua derivada, $(\log(3))/2 + \frac{1}{g+(1/2)}$, é estritamente positiva para $g \geq 2$), temos que

$$\begin{aligned} ((g + 1)/2) \cdot \log(3) - \log(6 \cdot g + 3) &\geq ((2 + 1)/2) \cdot \log(3) - \log(6 \cdot 2 + 3) \\ &> 0 \Rightarrow 3^{(g+1)/2} > 6 \cdot g + 3 \end{aligned}$$

Logo, pela discussão anterior, temos $B_r > 0$. Falta considerarmos o caso $q = 2$. Caso $g \geq 5$, podemos repetir o último argumento e concluir que $2^{r/2} \geq 2^{(g+1)/2} > 6 \cdot g + 3$. Caso $2 \leq g \leq 4$, mas $r \geq g + 6^*$, temos que $2^{r/2} \geq 2^{g/2+3}$ e a desigualdade $2^{g/2+3} > 6 \cdot g + 3$ é

* Observemos que, nesse caso, ainda temos $r \geq 2 \cdot g + 1$.

válida para $g = 2, 3$ e 4 . Então caso $g \geq 5$ ou $r \geq g + 6$, temos que $2^{r/2} > 6 \cdot g + 3$ e, como anteriormente, $B_r > 0$ vale.

Resta verificarmos que $B_r > 0$ para seis pares (r, g) , a saber: $(5, 2)$, $(6, 2)$, $(7, 2)$, $(7, 3)$, $(8, 3)$ e $(9, 4)$. Vamos analisar o par $(5, 2)$. Por 4.21, temos que $5 \cdot B_5(\mathbb{F}_2) = N(\mathbb{F}_{2^5}) - N(\mathbb{F}_2)$. Pela COTA DE SERRE, $|N(\mathbb{F}_{2^5}) - (2^5 + 1)| = |N(\mathbb{F}_{2^5}) - 33| \leq 2 \cdot \lfloor 2\sqrt{2^5} \rfloor = 22$, logo $N(\mathbb{F}_{2^5}) \geq 11$. Analogamente (mas usando a cota superior no lugar da inferior), $-N(\mathbb{F}_2) \geq -7$. Portanto $5 \cdot B_5(\mathbb{F}_2) \geq 11 - 7 = 4$, ou seja $B_5(\mathbb{F}_2) \geq 4/5 > 0$. Portanto o resultado continua válido nesse caso. Procedendo de maneira análoga, temos que o resultado também vale para os outros pares (r, g) . A tabela[†] a seguir resume as contas para todos os pares.

(r, g)	$r \cdot B_r$	Cotas	$B_r \geq$
$(5, 2)$	$N_5 - N_1$	$11 - 7$	$4/5$
$(6, 2)$	$N_6 - N_3 - N_2 + N_1$	$33 - 19 - 13 + 0$	$1/6$
$(7, 2)$	$N_7 - N_1$	$85 - 7$	$78/7$
$(7, 3)$	$N_7 - N_1$	$63 - 9$	$54/7$
$(8, 3)$	$N_8 - N_4$	$161 - 41$	$120/8 = 15$
$(9, 4)$	$N_9 - N_3$	$333 - 29$	$304/9$

Tabela 1 – “Subcasos” do caso $q = 2$.

Isso finaliza a demonstração.

□

Observação 153. Para gênero zero, dado $r \geq 1$, sempre existe um lugar de grau r . De fato, pela Teorema 131, temos que todo corpo de funções de gênero zero sobre um corpo finito é racional e como num corpo de funções racional $\mathbb{F}_q(x)$ os lugares, exceto pelo pólo de x , estão em bijeção com polinômios em uma variável com coeficientes em $\mathbb{F}_q$, temos que a existência de lugares de grau qualquer segue da existência de polinômios irreduzíveis em $\mathbb{F}_q[x]$ de grau qualquer (confira o item 2 do Teorema 145).

Para gênero 1, 5.1 nos dá $B_d > (q^d - 9q^{d/2})/d$, então para que $B_d > 0$, basta termos $q^d - 9q^{d/2} = q^{d/2}(q^{d/2} - 9) > 0$, ou seja, basta termos (lembrando que $q \geq 2$) $q^{d/2} - 9 > 2^{d/2} - 9 > 0$. Isso nos dá $d > 2\log(9)/\log(2) \approx 6.34$. Com isso, para $d \geq 7 = 2 \cdot 1 + 5$, temos que $B_d > 0$ num corpo de funções de gênero 1.

A estimativa anterior pode ser melhorada ainda mais: se $d \geq 2g + 3$ então $B_d > 0$. Novamente, basta verificarmos a desigualdade $B_d > 0$ apenas para $g = 1$ e para $d = 5$ e 6 (e q qualquer). Essa verificação é feita como no caso $q = 2$ do Teorema 152 e está resumida na tabela a seguir.

[†] No caso do par $(6, 2)$ usamos a cota trivial $N_1 \geq 0$ e no caso dos pares $(8, 3)$ e $(9, 4)$, temos que $\mu(8/2) = \mu(8/1) = \mu(9/1) = 0$.

r	$r \cdot B_r$	$r \cdot B_r \geq$
5	$N_5 - N_1$	$q^5 - q - \lfloor 2\sqrt{q^5} \rfloor - \lfloor 2\sqrt{q} \rfloor > 0$
6	$N_6 - N_3 - N_2 + N_1$	$q^6 - 3q^3 - q^2 - q - \lfloor 2\sqrt{q^3} \rfloor - \lfloor 2\sqrt{q} \rfloor > 0$

Ainda com $g = 1$, para $r = 3$ temos que

$$3 \cdot B_3 = N_3 - N_1 \geq q^3 + 1 - \lfloor 2\sqrt{q^3} \rfloor - q - 1 - \lfloor 2\sqrt{q} \rfloor$$

A expressão em vermelho é > 0 para $q \geq 3$, mas é $= -1$ para $q = 2$. Isso não impede que fosse $B_3 > 0$ para $q = 2$. Mas na verdade, um dentre os dois corpos de funções sobre $\mathbb{F}_2$ de gênero 1 é tal que $B_3 = 0$. Um tal corpo de funções é dado por $F = \mathbb{F}_2(x, y)$ onde $y^2 + y = x + 1/x$.

Para $r = 4$, temos também que $B_4 > 0$ para $q \geq 3$, mas $B_4 = 0$ para $q = 2$. Novamente, um dentre os dois corpos de funções de gênero 1 sobre $\mathbb{F}_2$ é tal que $B_4 = 0$: o corpo de funções dado por $F = \mathbb{F}_2(x, y)$ onde $y^2 + y = x^3$.

Sendo assim, a cota $d \geq 2g + 3$ não pode ser melhorada.

Juntando o resultado do [Teorema 152](#) aos dessa observação, temos o seguinte resultado

Para qualquer corpo de funções $E/\mathbb{F}_q$ e para qualquer $d \geq 2 \cdot g(E) + 3$ temos que $B_d > 0$, ou seja, E possui um lugar de grau d .

■

Lema 154. Seja $E/\mathbb{F}_q$ um corpo de funções de gênero $g(E)$ e N um inteiro tal que $0 \leq N \leq N(E)$, e escrevamos $N(E) = N + s$. Denotemos por $P_1, \dots, P_N, Q_1, \dots, Q_s$ os lugares racionais distintos de E . Seja r um inteiro tal que $r \geq 2g(E) + 3 + s$, e seja $\alpha \in \mathbb{F}_q$. Então existe um elemento $x \in E$ e um lugar $P \in \mathbb{P}_E$ com as seguintes propriedades:

1. $\deg P = r$,
2. os únicos pólos de x são $P_1, \dots, P_N$ e P e eles são todos simples, e
3. $x(Q_i) = \alpha^\dagger$ para $i = 1, \dots, s$.

■

Demonstração. Primeiramente escolhamos um lugar P de E de grau r usando a [Teorema 153](#). Temos que

† Confira a discussão da [Teorema 15](#).

$$\begin{aligned}
\deg(P - \sum_{i=1}^s Q_i) &= \deg P - \deg(\sum_{i=1}^s Q_i) = \deg P - \sum_{i=1}^s \deg Q_i \\
&= r - \sum_{i=1}^s 1 = r - s \geq 2g(E) + 3 + s - s > 2g(E) - 1
\end{aligned} \tag{5.8}$$

Logo, pelo [TEOREMA DE RIEMANN-ROCH](#), temos

$$\begin{aligned}
\ell(P - \sum_{i=1}^s Q_i) &= \deg(P - \sum_{i=1}^s Q_i) + 1 - g(E) = r - s + 1 - g(E) \\
&\geq 2g(E) + 3 + s - s + 1 - g(E) > 0
\end{aligned} \tag{5.9}$$

Portanto, existe $0 \neq u \in \mathcal{L}(P - \sum_{i=1}^s Q_i)$. De $\ell(P + P_j - \sum_{i=1}^s Q_i) = \ell(P - \sum_{i=1}^s Q_i) + 1$, pois $\deg(P + P_j - \sum_{i=1}^s Q_i) = \deg(P - \sum_{i=1}^s Q_i) + 1$ (e pelo [TEOREMA DE RIEMANN-ROCH](#)), temos que existem elementos $x_1, \dots, x_N$ com $x_j \in \mathcal{L}(P + P_j - \sum_{i=1}^s Q_i) \setminus \mathcal{L}(P - \sum_{i=1}^s Q_i)$ para $j = 1, \dots, N$. A pertinência anterior pode ser reescrita como

$$(x_j) \geq -P - P_j + \sum_{i=1}^s Q_i \quad \text{e} \quad (x_j) \not\geq -P + \sum_{i=1}^s Q_i \tag{5.10}$$

Isso é possível somente se $v_{P_j}(x_j) = -1$, ou seja, somente se P_j é pólo simples de x_j , $j = 1, \dots, N$. Observemos também que todos os Q_i 's, $i = 1, \dots, s$, são zeros de cada x_j . O elemento $w \doteq \sum_{j=1}^N x_j$ tem, pela [DESIGUALDADE TRIANGULAR ESTRITA](#) (note que, pela forma como x_j foi escolhido, $v_{P_j}(x_i) = \delta_{ij}$), pólos simples em $P_1, \dots, P_N$ e zeros em $Q_1, \dots, Q_s$. Para cada $j = 1, \dots, N$, se P for pólo de x_j , então ele será pólo simples. Por essa razão, e pela [DESIGUALDADE TRIANGULAR ESTRITA](#), se P for pólo de w , então ele será pólo simples. Colocamos

$$\tilde{x} \doteq \begin{cases} w & \text{se } P \text{ é pólo de } w \\ w + u & \text{caso contrário} \end{cases} \tag{5.11}$$

Agora é fácil ver que o elemento $x := \tilde{x} + \alpha$ satisfaz as propriedades desejadas (lembrando que, caso P não seja pólo de w , P será pólo simples de $\tilde{x} = w + u$, pela [DESIGUALDADE TRIANGULAR ESTRITA](#), pois P é pólo simples de u).

□

5.2 Corpos de funções com um número prescrito de lugares racionais

A seguinte proposição é o resultado principal deste capítulo: dela decorrem todos os outros que enunciaremos. Dito de maneira simples, vamos construir (e essa construção depende da existência de um elemento que satisfaz as conclusões do [Teorema 154](#)) um corpo de funções com um número “quase” prescrito de lugares racionais.

Proposição 155. Sejam $E/\mathbb{F}_q$ um corpo de funções de gênero $h = g(E)$, e N um inteiro tal que $0 \leq N \leq N(E)$. Suponhamos que g seja um inteiro que satisfaz as seguintes condições (onde $p = \text{char } \mathbb{F}_q$):

1. $g \equiv h \pmod{p-1}$, e
2. $g \geq (3p-2)h + (p-1)(N(E)+2)$.

Então $(N, g) \in \mathcal{M}_q$. ■

Demonstração. Como a condição 1 voltará a aparecer no texto, vale a pena notar agora que ela não diz nada caso $p = 2$.

Denotemos por $P_1, \dots, P_N, Q_1, \dots, Q_s$ todos os lugares racionais de E , onde $s = N(E) - N$. Escolhamos $\alpha \in \mathbb{F}_q \setminus \wp(\mathbb{F}_q)$, onde $\wp$ é o mapa de Artin-Schreier de $\mathbb{F}_q$ para $\mathbb{F}_q$ dado por $\beta \mapsto \beta^p - \beta$ ($p = \text{char } \mathbb{F}_q$). Tal escolha é possível pelo teorema do núcleo e da imagem, uma vez que $\wp$ é $\mathbb{F}_p$ -linear e $\mathbb{F}_p \subset \text{Ker}(\wp)$. Das condições 1 e 2, podemos escrever $g = (3p-2)h + (p-1)(N(E)+2) + j(p-1)$ para algum inteiro $j \geq 0$ (notemos que $3p-2 = p-1+p-1+p \equiv 0+0+1 \equiv 1 \pmod{p-1}$). Pelo [Teorema 154](#), existe um elemento $x \in E$ e um lugar $P \in \mathbb{P}_E$ de grau $2h+3+s+j$ ($\geq 2h+3+s$) com $(x)_\infty = P + P_1 + \dots + P_N$ e $x(Q_i) = \alpha$, para $i = 1, \dots, s$. Definamos $F \doteq E(y)$, onde y é uma raiz de $T^p - T - x \in E[T]$. Como x possui um pólo simples, a [Teorema 118](#) garante que a extensão F/E é Galoisiana de grau $[F : E] = p$ com as seguintes propriedades:

- 1.

Os lugares $P_1, \dots, P_N$ e P são totalmente ramificados e todos os outros lugares de E são não ramificados.

De fato, como $v_{P_1}(x) = \dots = v_{P_N}(x) = v_P(x) = -1 \not\equiv 0 \pmod{p}$, temos que os lugares $P_1, \dots, P_N$ e P satisfazem [3.56](#) (com $z = 0$) e qualquer outro lugar Q satisfaz [3.57](#) (também com $z = 0$).

- 2.

Os expoentes do diferente dos lugares acima de $P_1, \dots, P_N, P$ em F/E são todos iguais a $d = 2(p - 1)$.

Com efeito, como foi observado acima, $P_1, \dots, P_N$ e P satisfazem 3.56 com $m = 1$, logo $m_{P_1} = \dots = m_{P_N} = m_P = 1$ e, pelo item 3 da Teorema 117 o expoente do diferente é exatamente $d(\tilde{P}_1|P_1) = \dots = d(\tilde{P}_N|P_N) = d(\tilde{P}|P) = 2(p - 1)$ (onde denotamos por $\tilde{P}_i$, resp. por $\tilde{P}$, o único lugar acima de P_i , resp. de P , para $i = 1, \dots, N$).

3.

Os lugares $Q_1, \dots, Q_s$ são inertes em F/E , i.e., só existe um lugar $\tilde{Q}_j$ em F acima de Q_j , para cada $j = 1, \dots, s$, com grau relativo $f(\tilde{Q}_j|Q_j)$ máximo ($= p$).

Isso não é tão claro à primeira vista. Vejamos o porquê. Como $e(\tilde{Q}_j|Q_j) = 1$, o item 2 do Teorema 110 nos dá, denotando por r_j o número de lugares acima de Q_j em F , $r_j \cdot f(\tilde{Q}_j|Q_j) = p$, ou seja, $f(\tilde{Q}_j|Q_j) = 1$ ou p . Mas a condição 3 do Teorema 154 (que ainda não foi “usada”), juntamente com o TEOREMA DE KUMMER e com a nossa escolha de α , implicará que $f(\tilde{Q}_j|Q_j) = p$. De fato, temos que, no corpo residual $E_{Q_j} = \mathbb{F}_q$ (essa igualdade vale pois Q_j é racional) o polinômio $T^p - T - x$ é $T^p - T - \alpha$. Daí, como α não está na imagem do mapa de Artin-Schreier, o polinômio $T^p - T - \alpha \in E_{Q_j}[T] = \mathbb{F}_T$ é irreduzível. Daí o TEOREMA DE KUMMER nos garante que $f(\tilde{Q}_j|Q_j) = p$ (confira também a Teorema 82).

Dos itens 1 e 3 acima, podemos concluir que $N(F) = N$ (pela condição 3, os lugares $\tilde{Q}_j$ terão grau exatamente p e portanto não serão mais racionais). Do item 2, e da FÓRMULA DO GÊNERO DE HURWITZ (confira também o item 4 da Teorema 117), temos

$$\begin{aligned}
 2g(F) - 2 &= p \cdot (2h - 2) + \deg \text{Diff}(F/E) \\
 &= p \cdot (2h - 2) + \left(\sum_{i=1}^N \overbrace{d(\tilde{P}_i|P_i)}^{=2(p-1)} \underbrace{\deg P_i}_{=1} \right) + \overbrace{d(\tilde{P}|P)}^{=2(p-1)} \underbrace{\deg P}_{2h+3+s+j} \\
 &= p \cdot (2h - 2) + 2(p - 1)(2h + 3 + j + \underbrace{s + N}_{=N(E)})
 \end{aligned} \tag{5.12}$$

Logo $g(F) = (3p - 2)h + (p - 1)(N(E) + 2) + j(p - 1) = g$. Ou seja, o corpo de funções F tem N lugares racionais e gênero g , logo $(N, g) \in \mathcal{M}_q$.

□

Observação 156. Se “pedirmos”, no Teorema 154 e na Teorema 155, que $g(E)$ seja ≥ 2 , podemos substituir a desigualdade $r \geq 2g(E) + 3 + s$ que aparece no Teorema 154

por $r \geq 2g(E) + 1 + s$ tendo em mente o Teorema 152 e, da mesma forma, podemos substituir a desigualdade $g \geq (3p - 2)g(E) + (p - 1)(N(E) + 2)$ que aparece no item 2 da Teorema 155 por $g \geq (3p - 2)g(E) + (p - 1)N(E)$. O leitor interessado não terá dificuldades em repetir a demonstração da Teorema 155 com essas pequenas alterações tendo em vista o Teorema 154 “modificado” bem como o Teorema 152. ■

Agora daremos o passo de “quase prescrito” para “prescrito” apenas. Para isso, o Teorema 1 será como uma borracha que apagará o “quase”.

Teorema 157. Para qualquer potência de qualquer número primo $q = p^n$ existem constantes $a_q, b_q > 0$ tais que

$$\{(N, g) \mid g \geq a_q \cdot N + b_q\} \subset \mathcal{M}_q$$

■

Demonstração. Definamos a_q e b_q por

$$a_q \doteq \gamma_q^{-1}(3p - 2 + 2(p - 1)\sqrt{q}) > 0 \quad (5.13)$$

e

$$b_q \doteq (p - 1)(q + 2(p - 1)\sqrt{q} + 3p + 1) > 0 \quad (5.14)$$

onde γ_q é a constante introduzida no Teorema 1.

Dados N e g com

$$g \geq a_q \cdot N + b_q \quad (5.15)$$

nosso objetivo é “construir” um corpo de funções $F/\mathbb{F}_q$ com $g(F) = g$ e $N(F) = N$.

Existe um único inteiro h tal que $g \equiv h \pmod{p - 1}$ e

$$\frac{N}{\gamma_q} \leq h < \frac{N}{\gamma_q} + (p - 1) \quad (5.16)$$

De fato, o intervalo $[N/\gamma_q, N/\gamma_q + (p - 1))$ contem exatamente $p - 1$ inteiros consecutivos de modo que exatamente um deles será $\equiv g \pmod{p - 1}$. Então $N \leq \gamma_q \cdot h$ e, pelo Teorema 1, existe um corpo de funções $E/\mathbb{F}_q$ de gênero $g(E) = h$ com $N(E) (\geq h \cdot \gamma_q \geq N)$ lugares racionais. De 5.15,

$$\begin{aligned}
g &\geq \overbrace{(3p-2+2(p-1)\sqrt{q})\gamma_q^{-1}N}^{a_q} \\
&\quad + \underbrace{(p-1)(q+2(p-1)\sqrt{q}+3p+1)}_{b_q} \\
&> (h-(p-1))(3p-2+2(p-1)\sqrt{q}) \\
&\quad + (p-1)(q+2(p-1)\sqrt{q}+3p-1+2) \\
&= (3p-2)h + (p-1)(q+1+2h\sqrt{q}+2) \\
&\geq (3p-2)h + (p-1)(N(E)+2)
\end{aligned} \tag{5.17}$$

A desigualdade em vermelho segue de 5.16: $N\gamma_q^{-1} > (h-(p-1))$. Já a última desigualdade segue da COTA DE HASSE-WEIL.

Logo, pela Teorema 155 existe um corpo de funções F sobre $\mathbb{F}_q$ com $N(F) = N$ e $g(F) = g$ e terminamos.

□

Vamos discutir agora algumas consequências do teorema anterior. Seja

$$\mathcal{M}_q(g) \doteq \{N \mid \exists F/\mathbb{F}_q \text{ de gênero } g \text{ com } N \text{ lugares racionais}\} \subset \mathbb{Z}_{\geq 0} \tag{5.18}$$

Pela COTA DE HASSE-WEIL temos que $\mathcal{M}_q(g)$ está contido no intervalo $[0, q+1+2g\sqrt{q}]$. O corolário a seguir é uma consequência da COTA DE DRINFEL'D-VLĂDUȚ e do Teorema 157.

Corolário 158. Existe uma constante $\varepsilon_q > 0$ (que depende apenas de q) tal que para todo g suficientemente grande temos

$$[0, \varepsilon_q \cdot g] \cap \mathbb{Z}_{\geq 0} \subseteq \mathcal{M}_q(g) \subseteq [0, \sqrt{q} \cdot g] \cap \mathbb{Z}_{\geq 0} \tag{5.19}$$

Demonstração. A COTA DE DRINFEL'D-VLĂDUȚ nos diz que

$$A(q) = \limsup_{g \rightarrow \infty} \frac{N_q(g)}{g} \leq \sqrt{q} - 1 \tag{5.20}$$

onde $N_q(g) = \max \mathcal{M}_q(g)$ (confira 4.32). Portanto existe n_1 (que depende apenas de q) tal que o seguinte vale para $N \in \mathcal{M}_q(g)$

$$g \geq n_1 \Rightarrow \frac{N_q(g)}{g} \leq \sqrt{q} \Rightarrow N \leq N_q(g) \leq \sqrt{q} \cdot g$$

Ou seja, $\mathcal{M}_q(g) \subseteq [0, \sqrt{q} \cdot g] \cap \mathbb{Z}_{\geq 0}$. Suponhamos agora que $n_1 > b_q$ e seja $0 < \delta_q < 1$ tal que $\delta_q n_1 = b_q$ (i.e., $\delta_q = b_q/n_1$). Daí, $g > \delta_q \cdot g \geq \delta_q n_1 = b_q \Rightarrow -b_q \geq -\delta_q \cdot g$. Logo $\frac{g-b_q}{a_q} \geq g \cdot \frac{1-\delta_q}{a_q} \geq 0$ e, portanto, $0 \leq N \leq \frac{1-\delta_q}{a_q} \cdot g \Rightarrow N \in \mathcal{M}_q(g)$, ou seja, $[0, \varepsilon_q \cdot g] \cap \mathbb{Z}_{\geq 0} \subseteq \mathcal{M}_q(g)$, onde $\varepsilon_q = \frac{1-\delta_q}{a_q} > 0$.

Caso $n_1 \leq b_q$, basta tomarmos n_2 (que, também, só depende de q) o menor inteiro (≥ 0) tal que $n_2(> n_1) > b_q$ e repetirmos o que foi feito acima.

Observemos que caso $n_1 > b_q$, o “suficientemente grande” do enunciado é $g \geq n_1$. Caso $n_1 \leq b_q$, o “suficientemente grande” passa a ser $g \geq n_2 > n_1$, onde ambas as inclusões 5.19 do enunciado são válidas. Observemos também que a estimativa $[0, \sqrt{q}g] \cap \mathbb{Z}_{\geq 0}$ pode ser “trocada” (caso q não seja um quadrado) por $[0, (\lceil \sqrt{q} \rceil - 1 + 1)g] \cap \mathbb{Z}_{\geq 0}$ (quando q é quadrado, $\lceil \sqrt{q} \rceil - 1 + 1 = \sqrt{q}$).

□

Observação 159. Notemos que o [corolário anterior](#) nos diz que para g suficientemente grande, $\mathcal{M}_q(g)$ contem um “intervalo” de números $\in \mathbb{Z}_{\geq 0}$ não trivial. Entretanto, o conjunto $\mathcal{M}_q(g)$ em geral (para g não suficientemente grande) *não* é um intervalo de números $\in \mathbb{Z}_{\geq 0}$. ■

Vamos considerar agora “limites” de corpos de funções sobre $\mathbb{F}_q$. Definimos

$$L_q \doteq \{ \alpha \in \mathbb{R} \mid \exists \text{ uma sequência de corpos de funções } (F_i)_{i \geq 0} \text{ sobre } \mathbb{F}_q \text{ tal que } g(F_i) \xrightarrow{i \rightarrow \infty} \infty \text{ e } N(F_i)/g(F_i) \xrightarrow{i \rightarrow \infty} \alpha \} \quad (5.21)$$

Temos que $A(q) = \sup L_q$. De fato, seja $\alpha \in L_q$ e seja $(F_i)_{i \geq 0}$ uma sequência de corpos de funções sobre $\mathbb{F}_q$ tal que $g(F_i) \rightarrow \infty$ e $N(F_i)/g(F_i) \rightarrow \alpha$ com $i \rightarrow \infty$. Temos que $N_q(g(F_i))/g(F_i) \geq N(F_i)/g(F_i)$. Logo

$$A(q) = \limsup_{g \rightarrow \infty} \frac{N_q(g)}{g} \geq \limsup_{i \rightarrow \infty} \frac{N_q(g(F_i))}{g(F_i)} \geq \limsup_{i \rightarrow \infty} \frac{N(F_i)}{g(F_i)} = \lim_{i \rightarrow \infty} \frac{N(F_i)}{g(F_i)} = \alpha \quad (5.22)$$

Ou seja, $A(q) \geq \alpha$ para qualquer $\alpha \in L_q$. Logo $A(q) \geq \sup L_q$. Para mostrar a desigualdade contrária, $\sup L_q \geq A(q)$, vamos usar a [COTA DE DRINFEL'D-VLĂDUȚ](#). Sabemos que $A(q) \in [0, \sqrt{q} - 1]$, ou seja, $\limsup_{i \rightarrow \infty} N_q(g(F_i))/g(F_i) \in [0, \sqrt{q} - 1]$. Logo existe n^* , tal que para todo $g \geq n^*$, temos $N_q(g)/g \in [0, \sqrt{q}]$. Como $[0, \sqrt{q}] \subseteq \mathbb{R}$ é compacto, temos que existe uma subsequência convergente da sequência $\{N_q(g)/g\}_{g \geq n^*}$. Mais do que isso, como $\limsup_{i \rightarrow \infty} N_q(g)/g = A(q)$, existe uma subsequência $N_q(g_i)/g_i$ que converge para $A(q)$ (obviamente $g_i \rightarrow \infty$ com $i \rightarrow \infty$ pois $g \rightarrow \infty$). Seja $F_i/\mathbb{F}_q$ um corpo de funções de gênero

g_i com $N_q(g_i)$ lugares racionais (um tal corpo de funções existe pela própria definição de $N_q(g)$). Então

$$\frac{N_q(g(F_i))}{g(F_i)} = \frac{N_q(g_i)}{g_i} \xrightarrow{i \rightarrow \infty} A(q) \quad (5.23)$$

Logo $A(q) \in L_q$ e portanto $A(q) \leq \sup L_q$.

O próximo resultado nos diz que L_q possui uma infinidade de números reais.

Corolário 160. Existe $\delta_q > 0$ tal que $[0, \delta_q] \subseteq L_q$.

Demonstração. Pelo [Teorema 157](#), temos que se $g \geq a_q \cdot N + b_q$, então existe um corpo de funções F sobre $\mathbb{F}_q$ de gênero g com N lugares racionais. Seja $\beta \leq a_q^{-1}$ e suponhamos, inicialmente, que β é racional. Escrevendo $\beta = n/d$, com n e d coprimos, temos que $\beta = n/d \leq a_q^{-1} \Rightarrow n \leq a_q^{-1} \cdot d$. Logo, para qualquer $j \in \mathbb{Z}_{\geq 1}$, temos

$$\beta = \frac{j \cdot n}{j \cdot d} \leq a_q^{-1} \Rightarrow j \cdot n \leq a_q^{-1} \cdot (dj) \Rightarrow j \cdot (n - a_q^{-1} \cdot d) \leq 0 \quad (5.24)$$

Suponhamos também que $\beta < a_q^{-1}$, de modo que $(n - a_q^{-1} \cdot d) < 0$ e, portanto, $j(n - a_q^{-1} \cdot d) \rightarrow -\infty$ para $j \rightarrow \infty$. Daí, temos que existe $j^* \in \mathbb{Z}_{\geq 0}$ tal que

$$j \geq j^* \Rightarrow j(n - a_q^{-1} \cdot d) \leq -\frac{b_q}{a_q} \Rightarrow 0 \leq j \cdot n \leq a_q^{-1}(d \cdot j - b_q) \quad (5.25)$$

Logo, pelo [Teorema 157](#), existe um corpo de funções $F/\mathbb{F}_q$ com $j \cdot n$ lugares racionais e de gênero $j \cdot d$, para todo $j \geq j^*$. Definimos então, para $k \in \mathbb{Z}_{\geq 1}$, $N_k \doteq (j^* + k) \cdot n$ e $g_k = (j^* + k) \cdot d$. Temos então que

$$\frac{N_k}{g_k} = \frac{(j^* + k) \cdot n}{(j^* + k) \cdot d} = \frac{n}{d} \xrightarrow{k \rightarrow \infty} \frac{n}{d} = \beta \quad (5.26)$$

Se β é um irracional em $[0, a_q^{-1}]$ ou se $\beta = a_q^{-1} \in \mathbb{Q}$, aproximamos β por racionais e repetimos, para cada racional dessa aproximação, o argumento anterior (note que, por [5.26](#), a razão N_k/g_k é constante e igual ao número racional em questão). Por fim, note que podemos tomar o δ_q do enunciado como sendo a_q^{-1} .

□

5.3 O caso q quadrado

Essa seção contém um aprimoramento do [Teorema 157](#) no caso de q ser um quadrado. Ao longo dessa seção escreveremos, portanto,

$$q = \ell^2$$

Alguns dos resultados de [Garcia e Stichtenoth \(1995\)](#) são essenciais. De fato, começamos com a torre $\mathcal{H} = (H_0 \subset H_1 \subset H_2 \dots)$ sobre $\mathbb{F}_q$ que lá foi introduzida. Essa torre é definida recursivamente (para a definição de torre e de torre recursivamente definida, confira [Stichtenoth \(2009, p. 246\)](#)) da seguinte maneira: $H_0 = \mathbb{F}_q(x_0)$ é o corpo de funções racional, e para $i \geq 0$, $H_{i+1} = H_i(x_{i+1})$ onde

$$x_i^{\ell-1}x_{i+1}^\ell + x_{i+1} = x_i^\ell. \quad (5.27)$$

Todas as extensões intermediárias $H_i \subset H_{i+1}$ são extensões de Galois de grau ℓ . De fato, o polinômio $x_i^{\ell-1}T^\ell + T - x_i^\ell$ é separável e dada uma raiz $y \in H_{i+1} \setminus H_i$ as outras raízes são dadas por $y + \alpha_j/x_i$ onde $\alpha_j, j = 1, \dots, \ell$ são as raízes de $T^\ell + T \in \mathbb{F}_q[T]$, raízes essas que pertencem a $\mathbb{F}_q$.

Podemos “refinar” essas extensões H_{i+1}/H_i em “passos” de grau p :

$$\begin{array}{ccc} & H_{i+1} & - F_{(i+1)n} \\ & \downarrow & \downarrow p \\ & & \vdots \\ \ell = p^n & \downarrow & \downarrow p \\ & & F_{in+1} \\ & & \downarrow p \\ H_i & - & F_{in} \end{array}$$

Esse “refinamento” é feito da seguinte maneira. Uma vez que cada extensão da torre $\mathcal{H}$ é abeliana elementar de expoente p (e de grau p^n), a existência de subgrupos de ordem p^k de $\text{Gal}(H_{i+1}/H_i)$, $k = 1, \dots, n-1$, é garantida. Fixando um subgrupo de cada ordem, basta então tomarmos o corpo fixo por cada um desses subgrupos. Dessa maneira obtemos uma torre $\mathcal{F} = (F_0 = H_0 \subset F_1 \subset \dots \subset F_n = H_1 \subset \dots)$ como no diagrama anterior.

A seguir listamos algumas propriedades da torre $\mathcal{F}$ que serão usadas ao longo da seção.

Lema 161. A torre $\mathcal{F}$ possui as seguintes propriedades:

1. $F_0 = \mathbb{F}_q(x_0)$ é um corpo de funções racional, e todas as extensões F_{n+1}/F_n são galoisianas de grau $[F_{n+1} : F_n] = p$.

2. O lugar P_∞ de F_0 , que é o pólo de x_0 em F_0 , é totalmente ramificado em todas as extensões F_n/F_0 .
3. Denotando por P_n o único lugar de F_n acima de P_∞ , temos que o expoente do diferente de P_{n+1} sobre P_n é $d(P_{n+1}|P_n) = (p-1)(\ell+2)$.
4. Para todo n , $g(F_{n+1}) \geq p \cdot g(F_n) + \ell(p-1)/2$.
5. Os lugares de F_0 que são zeros de $x_0 - \alpha$ com $0 \neq \alpha \in \mathbb{F}_q$ decompõem-se completamente em todas as extensões F_n/F_0 .
6. Para todo $n \geq 0$, $p^n(q-1) \leq N(F_n) \leq p^n q + 1$.
7. $\lim_{n \rightarrow \infty} N(F_n)/g(F_n) = \ell - 1 = \sqrt{q} - 1$.
8. Para todo $n \geq 0$,

$$N(F_n)/g(F_n) > N(F_{n+1})/g(F_{n+1}) > \ell - 1. \quad (5.28)$$

9. $2g(F_n) \equiv 0 \pmod{p-1}$, para todo $n \geq 0$.

Demonstração. O item 1 é claro da maneira como a torre $\mathcal{F}$ é construída. Os itens 2, 3, 5, 7, são demonstrados em Garcia e Stichtenoth (1995) para a torre $\mathcal{H}$, e não é difícil mostrar que eles continuam válidos na torre $\mathcal{F}$. O item 4 segue do item 3 e da FÓRMULA DO GÊNERO DE HURWITZ aplicada à extensão F_{n+1}/F_n lembrando que o item 3 nos dá $\deg \text{Diff}(F_{n+1}/F_n) \geq (p-1)(\ell+2)$. O item 6 segue dos itens 2 e 5. De fato, o item 5 nos dá a cota inferior $p^n(q-1)$, pois os $q-1$ lugares racionais de F_0 que são zeros de $x_0 - \alpha$, com $0 \neq \alpha \in \mathbb{F}_q$ (um lugar para cada α), decompõem-se completamente em $p^n = [F_n : F_0]$ lugares racionais em F_n . Já o item 2 juntamente com o fato de que os únicos lugares racionais de F_0 são o pólo de x_0 (que é totalmente ramificado em todas as extensões) e os q lugares racionais $P_{x_0-\alpha}$, $\alpha \in \mathbb{F}_q$, nos dá um máximo de $qp^n + 1$ lugares racionais em F_n . A monotonicidade da sequência $N(F_n)/g(F_n)$ segue do item 4 e da desigualdade $N(F_{n+1}) \leq p \cdot N(F_n)$, e a última desigualdade do item 8 vem do item 7. O item 9 segue por indução na FÓRMULA DO GÊNERO DE HURWITZ para a extensão F_{n+1}/F_n e do fato que o grau do diferente numa extensão de Artin-Schreier é múltiplo de $p-1$, pois os expoentes do diferente o são (confira a Teorema 117).

□

Lema 162. Para cada inteiro $j \geq 0$ existe uma torre $\mathcal{E} = (E_0 \subset E_1 \subset \dots)$ de corpos de funções sobre $\mathbb{F}_q$ tal que para todo $n \geq 0$ o seguinte é válido

1. E_{n+1}/E_n é galoisiana de grau p .

2. $g(E_n) \equiv j \pmod{p-1}$.
3. $(q-1)p^n \leq N(E_n) \leq 2(1+qp^n)$ e $g(E_n) = 2g(F_n) - 1 + (j+1)p^n$, onde F_n é o n -ésimo corpo de funções da torre $\mathcal{F}$ do lema anterior.

Demonstração. Para $p = 2$ basta tomarmos $E_n = F_n(y)$ com $y^2 + y = x_n^{(j+1)p^{n+1}-1}$, onde $P_n = (x_n)$ (P_n denota, como anteriormente, o único lugar em F_n acima de $P_\infty \in \mathbb{P}_{F_0}$). Suponhamos então que $p \neq 2$. Tomemos a torre $\mathcal{F}$ do Teorema 161 e escolhamos um polinômio irreduzível $f(x) \in \mathbb{F}_q[x]$ de grau $\deg f(x) = 2j+2$ (não necessariamente mônico) com a propriedade a seguir.

Para pelo menos $(q-1)/2$ elementos $0 \neq \alpha \in \mathbb{F}_q$ o valor $f(\alpha)$ é um quadrado em $\mathbb{F}_q$.

Se um polinômio irreduzível $g(x)$ de grau $2j+2$ não satisfizer a condição anterior, basta multiplicarmos $g(x)$ por um não quadrado (lembremos que $\mathbb{F}_q^\times$ possui $(q-1)/2$ quadrados e $(q-1)/2$ não quadrados). Consideremos agora o corpo de funções $E_0 = F_0(y)$ onde y satisfaz a equação $y^2 = f(x_0)$ e a torre de *composita* $\mathcal{E} = (E_0 \subset E_1 \subset E_2 \subset \dots)$, i.e., $E_n = F_n \cdot E_0$ para todo $n \geq 0$.

Claramente, E_{n+1}/E_n é extensão de Galois de grau p para todo n . Temos que

$$(q-1)p^n \leq N(E_n) \leq 2N(F_n) \leq 2(1+qp^n). \quad (5.29)$$

Na desigualdade em vermelho, usamos o fato que $f(\alpha)$ é quadrado para pelo menos $(q-1)/2$ elementos de $\mathbb{F}_q^\times$. Isso, juntamente com o TEOREMA DE KUMMER, nos diz que pelo menos $(q-1)/2$ dos $q+1$ lugares racionais do corpo de funções racional F_0 dão origem a $2 = [E_0 : F_0]$ lugares racionais de E_0 . Daí, $N(E_0) \geq [E_0 : F_0] \cdot (q-1)/2 = 2 \cdot (q-1)/2 = q-1$. A desigualdade em vermelho segue então de ser $[E_n : E_0] = p^n$. Já a desigualdade em azul segue do item 6 do Teorema 161.

O gênero de E_n pode ser calculado através da [FÓRMULA DO GÊNERO DE HURWITZ](#) para a extensão E_n/F_n , lembrando que, como $p \neq 2$, tal extensão é de Kummer (confira a [Teorema 111](#)):

$$2g(E_n) - 2 = 2(2g(F_n) - 2) + (2j + 2)p^n \quad (5.30)$$

O termo $(2j + 2)p^n$ que aparece na igualdade acima é o grau do diferente da extensão E_n/F_n . O cálculo do diferente da extensão E_n/F_n é um pouco delicado, de modo que uma explicação detalhada se faz necessária. Procedemos então com uma tal explicação.

Ora, da forma como E_n foi definido, temos que $E_n = F_n(y)$ onde y é uma raiz de $T^2 = f(x_0)$, com $f(x_0)$ visto agora como elemento de F_n . No que segue, vamos denotar por P_0 o único zero de $f(x_0)$ em $F_0 = \mathbb{F}_{\ell^2}(x_0)$ (lembremos que o polinômio $f(T)$ é irredutível).

Da proposição sobre [EXTENSÕES DE KUMMER](#), temos que os lugares P de F_n que estão no suporte de $\text{Diff}(E_n/F_n)$ são aqueles para os quais $(2, v_P(f(x_0))) = 1$, ou seja são os lugares que são zeros ou pólos de ordem ímpar da função $f(x_0) \in F_n$. É de verificação imediata que o lugar $P_n \in \mathbb{P}_{F_n}$ acima do pólo $P_\infty \in \mathbb{P}_{F_0}$ de x_0 é tal que $v_{P_n}(f(x_0)) = -(2j + 2)p^n$, pois $v_{P_\infty}(f(x_0)) = -2j + 2 = -\deg f(T)$ e a extensão $P_n|P_\infty$ é totalmente ramificada. Logo P_n não está no suporte do diferente de E_n/F_n . Os lugares de F_n que **não** estão acima de P_0 também não estão no suporte do diferente de E_n/F_n , pois $v_P(f(x_0)) = 0$. Já os lugares de F_n que estão acima de P_0 são tais que $v_P(f(x_0)) = p^{i_n}$, onde $0 \leq i_n \leq n$ para todo n . De fato, temos que

$$v_P(f(x_0)) = \overbrace{e(P|P \cap F_{n-1})}^{1 \text{ ou } p} \cdot \overbrace{e(P \cap F_{n-1}|P \cap F_{n-2})}^{1 \text{ ou } p} \cdots \overbrace{e(P \cap F_1|P \cap F_0)}^{1 \text{ ou } p} \underbrace{v_{P \cap F_0}(f(x_0))}_1$$

O índice de ramificação $e(P \cap F_{i+1}|P \cap F_i)$ é sempre 1 ou p pois cada extensão F_{i+1}/F_i é de Artin-Schreier, e em extensões desse tipo as respectivas extensões de lugares ou são não ramificadas ou são totalmente ramificadas (lembremos também que $[F_{i+1} : F_i] = p$).

Para um lugar P de F_n acima de P_0 temos, novamente pela proposição sobre [EXTENSÕES DE KUMMER](#), que o índice de ramificação $e(P)$ (que não depende da particular extensão de P em E_n uma vez que E_n/F_n é galoisiana) é exatamente $2 = [E_n : F_n]$, ou seja P é totalmente ramificado em E_n/F_n de que modo que P possui uma única extensão P' em E_n . Também, o expoente do diferente $d(P)$ será exatamente 1. Daí, o grau do diferente de E_n/F_n será dado por $\deg \text{Diff}(E_n/F_n) = \sum_{P|P_0} \deg P$ e, portanto, precisamos verificar que $\sum_{P|P_0} \deg P = (2j + 2)p^n$.

Denotemos por $Q_1, \dots, Q_s$ todas as extensões de P_0 em F_n . O divisor principal de $f(x_0)$ em F_n é dado por $(f(x_0))^{F_n} = p^{i_1}Q_1 + \dots + p^{i_s}Q_s - (2j + 2)p^n P_n$, com $0 \leq i_j \leq n$. Sendo

$(f(x_0))^{F_n}$ um divisor principal, o [Teorema 34](#) garante que $\sum_{l=1}^s p^{i_l} \deg P_l = (2j+2)p^n$. Com isso, para verificarmos que $\sum_{P|P_0} \deg P = (2j+2)p^n$, basta verificarmos que $i_l = 0$ para todo $l = 1, \dots, s$ (independente de n). O coeficiente p^{i_l} é justamente o índice de ramificação da extensão $P_l|P_0$, de modo que $i_l = 0$ para todo l (independente de n) se, e somente se, P_0 é não ramificado na torre $\mathcal{F}$. Como a torre $\mathcal{F}$ é uma subtorre da torre $\mathcal{H}$, P_0 é não ramificado na torre $\mathcal{F}$ se, e somente se, o for na torre $\mathcal{H}$. Para verificar que P_0 é não ramificado na torre $\mathcal{H}$, vamos usar agora a [Teorema 119](#). Como $H_i = H_{i-1}(x_i)$, com $x_{i-1}^{\ell-1}x_i^\ell + x_i = x_{i-1}^\ell$ para $i \geq 1$, basta verificarmos, dado um lugar P_i de H_i acima de P_0 , que $v_{P_i}(x_i) = 0$, pois daí o item 3 da [Teorema 119](#) nos garante que P_i será não ramificado em H_{i+1}/H_i . Vamos supor que $v_{P_i \cap H_{i-1}}(x_{i-1}) = 0$. Temos então que

$$0 = \ell \cdot e(P_i|P_i \cap H_{i-1})v_{P_i \cap H_{i-1}}(x_{i-1}) = v_{P_i}(x_{i-1}^\ell) = v_{P_i}(x_{i-1}^{\ell-1}x_i^\ell + x_i) \quad (5.31)$$

Pela [desigualdade triangular](#), temos

$$\begin{aligned} v_{P_i}(x_{i-1}^{\ell-1}x_i^\ell + x_i) &\geq \min\{(\ell-1)e(P_i|P_i \cap H_{i-1})\overbrace{v_{P_i \cap H_{i-1}}(x_{i-1})}^0 + \ell v_{P_i}(x_i), v_{P_i}(x_i)\} \\ &= \min\{\ell v_{P_i}(x_i), v_{P_i}(x_i)\} \end{aligned}$$

Se fosse $v_{P_i}(x_i) \neq 0$, a [DESIGUALDADE TRIANGULAR ESTRITA](#) nos daria $v_{P_i}(x_{i-1}^{\ell-1}x_i^\ell + x_i) = \ell v_{P_i}(x_i)$ ou $v_{P_i}(x_i)$, dependendo do sinal de $v_{P_i}(x_i)$. Em ambos os casos teríamos $v_{P_i}(x_{i-1}^{\ell-1}x_i^\ell + x_i) \neq 0$, contradizendo [5.31](#). Falta mostrarmos então que a nossa suposição de que $v_{P_i \cap H_{i-1}}(x_{i-1}) = 0$ é válida. Mas para isso, é suficiente mostrarmos que $v_{P_i \cap H_0}(x_0) = v_{P_0}(x_0) = 0$, o que é claro pois P_0 não é zero de x_0 (em H_0).

A conclusão que tiramos da digressão anterior é que o grau do diferente da extensão E_n/F_n é de fato $(2j+2)p^n$. Simplificando agora [5.30](#) obtemos

$$g(E_n) = 2g(F_n) - 1 + (j+1)p^n. \quad (5.32)$$

Pelo item 9 do [Teorema 161](#) vemos que $g(E_n) \equiv j \pmod{p-1}$.

□

Agora estamos em posição de mostrar um melhoramento quantitativo do [Teorema 157](#) no caso de q ser um quadrado.

Proposição 163. Seja q um quadrado, $p = \text{char } \mathbb{F}_q$. Assuma que $N \geq (q-1)/p$, e

$$g \geq \frac{2q}{q-1}p(p+4.5)N + p + 6$$

Então $(N, g) \in \mathcal{M}_q$. ■

Demonstração. Escolhamos j tal que $0 \leq j \leq p-2$ e $j \equiv g \pmod{p-1}$ e consideremos a torre $\mathcal{E} = (E_0 \subset E_1 \subset \dots)$ do Teorema 162. Escolhamos $i \geq -1$ tal que

$$p^i(q-1) \leq N < p^{i+1}(q-1) \quad (5.33)$$

e tomemos $E \doteq E_{i+1}$. Nosso objetivo é aplicar a Teorema 155 nessa situação. Observemos que $N \leq N(E)$ por 5.29 e 5.33. Na expressão a seguir, o corpo F_{i+1} denota o $(i+1)$ -ésimo corpo da torre $\mathcal{F}$ do Teorema 161. Temos que

$$\begin{aligned} g(E) &= 2g(F_{i+1}) - 1 + (j+1) \cdot p^{i+1} && \text{pelo Teorema 162} \\ &\leq 2g(F_{i+1}) - 1 + (p-1)p^{i+1} && \text{pois } j+1 \leq p-1 \\ &< \frac{2}{\ell-1}(1+p^{i+1}q) - 1 + (p-1)p^{i+1} && \text{pelos itens 6 e 8 do Teorema 161} \\ &= \frac{2}{\ell-1} - 1 + p^{i+1} \left(\frac{2q}{\ell-1} + p - 1 \right) \end{aligned} \quad (5.34)$$

e por 5.29

$$(p-1)(N(E)+2) \leq (p-1)(2p^{i+1}q+4), \quad (5.35)$$

Daí

$$(3p-2)g(E) + (p-1)(N(E)+2) < \left(\frac{6p-4}{\ell-1} + p - 2 \right) + p^{i+1} \left(\frac{2q(3p-2)}{\ell-1} + (p-1)(3p+2q-2) \right)$$

Segue de 5.33 que $p^{i+1} \leq pN/(q-1)$ e daí

$$(3p-2)g(E) + (p-1)(N(E)+2) \leq A + BpN, \quad (5.36)$$

com

$$A \doteq \frac{6p-4}{\ell-1} + p - 2 \quad (5.37)$$

e

$$B \doteq \frac{1}{q-1} \left(\frac{2q(3p-2)}{\ell-1} + (p-1)(3p+2q-2) \right) < \frac{2q}{q-1}(p+4.5) \quad (5.38)$$

Para verificar a desigualdade em vermelho basta verificarmos que para $p \geq 2$ vale

$$\frac{3p-2}{p-1} + \frac{(p-1)(3p-2)}{2p^2} < 5.5 \quad (5.39)$$

A função $f(p) \doteq (3p-2)/(p-1)$ é decrescente e $\leq f(2) = 4$, para $p \geq 2$. Já a função $g(p) = (p-1)(3p-2)/2p^2$ é crescente e $< 3/2 = \lim_{p \rightarrow \infty} g(p)$. Logo $f(p) + g(p) < 4 + 3/2 = 5.5$ e 5.39 é válida.

A constante A é $\leq p+6$ pois $\frac{6p-4}{\ell-1} \leq 8$. Com isso, a desigualdade

$$A + BpN \leq \frac{2q}{q-1}p(p+4.5)N + p+6 \quad (5.40)$$

é válida para $\ell \geq 2$.

Segue agora da Teorema 155 que existe um corpo de funções $F/\mathbb{F}_q$ com $g(F) = g$ e $N(F) = N$.

□

A Teorema 163 não se aplica para $N < (q-1)/p$. Nesse caso temos uma condição ligeiramente diferente, como diz a seguinte

Observação 164. Seja q um quadrado, $p = \text{char } \mathbb{F}_q$. Assuma que $N < (q-1)/p$ e $g \geq 2q(p-1) + 3p^2 - 4p$. Então $(N, g) \in \mathcal{M}_q$.

Demonstração. Primeiramente consideremos $p \neq 2$. Escolhamos j tal que $0 \leq j \leq p-2$ e $j \equiv g \pmod{p-1}$, e consideremos o corpo $E \doteq \mathbb{F}_q(x, y)$ com $y^2 = f(x)$, onde $f(x)$ é um polinômio irredutível de grau $2j+2$ e $f(\alpha)$ é um quadrado em $\mathbb{F}_q$ para pelo menos $(q-1)/2$ elementos $0 \neq \alpha \in \mathbb{F}_q$ (como na demonstração do Teorema 162). Então $g(E) = j \geq 2$ e $N < (q-1)/p < q-1 \leq N(E) \leq 2q+2$, e daí

$$\begin{aligned} (3p-2) \overbrace{g(E)}^{=j \leq p-2} + (p-1)(N(E)+2) &\leq (3p-2)(p-2) + (p-1)(2q+4) \\ &= 2q(p-1) + 3p^2 - 4p \end{aligned} \quad (5.41)$$

E agora a afirmação segue da Teorema 155.

Para $p = 2$, como a equivalência $\text{mod } (p-1)$ é irrelevante, basta considerarmos o corpo de funções racional $\mathbb{F}_q(x)$ e aplicar a Teorema 155, lembrando que $N(\mathbb{F}_q(x)) = q+1$, de modo que $N < (q-1)/p < N(\mathbb{F}_q(x))$ e $(3p-2)g(\mathbb{F}_q(x)) + (p-1)(N(\mathbb{F}_q(x))+2) = q+3 \leq 2q+4$. Com isso, vemos que podemos “trocar”, nesse caso do primo 2, a desigualdade $g \geq 2q(p-1) + 3p^2 - 4p = 2q+4$ por $g \geq q+3$.

□

5.4 O caso $q = 2$

Se q não é um quadrado ainda somos capazes de melhorar as constantes a_q e b_q do [Teorema 157](#) desde que tenhamos uma “boa” sequência de corpos de funções $(F_n/\mathbb{F}_q)_{n \geq 0}$ com o limite $\lim_{n \rightarrow \infty} N(F_n)/g(F_n) > 0$ suficientemente grande. Ilustramos isso no caso $q = 2$. Em [Duursma e Mak \(2011, p. 17\)](#) é dada uma torre de corpos de funções $\mathcal{F} = (F_0 \subset F_1 \subset \dots)$ sobre $\mathbb{F}_2$ tal que $g(F_0) = 0$, $g(F_1) = 2$ e para todo $n \geq 0$

$$N(F_n) = 3 \cdot 2^n \quad \text{e} \quad g(F_n) \leq \gamma \cdot N(F_n) \quad (5.42)$$

onde $\gamma \approx 3.154582$. O valor exato de γ (na verdade de γ^{-1}) é dado em [Duursma e Mak \(2011, p. 19\)](#). Note que γ^{-1} é uma cota inferior para $A(2)$, a melhor conhecida, ou seja o limite $\lim_{n \rightarrow \infty} N(F_n)/g(F_n)$ é “suficientemente grande”.

Tomemos N e g satisfazendo

$$N \geq 3 \quad \text{e} \quad g \geq (8\gamma + 2)N \quad (5.43)$$

Escolhamos i tal que

$$3 \cdot 2^i \leq N \leq 3 \cdot 2^{i+1} \quad (5.44)$$

e seja $E \doteq F_{i+1}$. Notemos que $g \geq 2$ ([STICHTENOTH, 2009, p. 246](#)) e que $N \leq N(E) = N(F_{i+1}) = 3 \cdot 2^{i+1}$, mas $2N \geq N(E)$. Com isso obtemos

$$\begin{aligned} (3p - 2)g(E) + (p - 1)N(E) &\leq 4g(E) + N(E) \\ &\leq (4\gamma + 1)N(E) \\ &\leq (4\gamma + 1) \cdot 2N \\ &\leq g \end{aligned} \quad (5.45)$$

Pela [Teorema 156](#) segue que $(N, g) \in \mathcal{M}_2$.

Para todo $g \geq 1$, o corpo de funções $F = \mathbb{F}_2(x, y)$ com

$$y^2 + y = x^{2g}(x + 1) + 1 \quad (5.46)$$

tem gênero $g(F) = g$ e $N(F) = 1$. De fato, sendo P_∞ o lugar infinito de $\mathbb{F}_2(x)$, temos que $v_{P_\infty}(x^{2g}(x + 1) + 1) = -2g - 1 \not\equiv 0 \pmod{2}$ e é claro que $-2g - 1 < 0$. Além disso, fazendo uso do [Teorema 21](#), temos que $v_P(x^{2g}(x + 1) + 1) \geq 0$ para todo lugar $P \in \mathbb{P}_{\mathbb{F}_2(x)}$ distinto P_∞ . Daí, pela [Teorema 117](#) temos que P_∞ é totalmente ramificado em $\mathbb{F}_2(x, y)/\mathbb{F}_2(x)$ e

todos os outros lugares são não ramificados. Com isso, uma aplicação da [FÓRMULA DO GÊNERO DE HURWITZ](#) fornece

$$\begin{aligned}
 2g(F) - 2 &= 2 \cdot \overbrace{(2g(\mathbb{F}_2(x)) - 2)}^0 + \deg \text{Diff}(\mathbb{F}_2(x, y)/\mathbb{F}_2(x)) \\
 &= -4 + \overbrace{(2g + 2)}^{m_{P_\infty} + 1} \cdot \underbrace{1}_{2-1} \cdot \deg P_\infty \\
 &= 2g - 2 \Rightarrow g(F) = g
 \end{aligned} \tag{5.47}$$

O lugar P'_∞ acima de P_∞ continua racional em $\mathbb{F}_2(x, y)$. Os únicos outros lugares de $\mathbb{F}_2(x, y)$ que “tem chance” de serem racionais são os lugares acima de $P_0 = P_{x=0}$ e de $P_1 = P_{x=1}$. Para vermos que esses lugares não são racionais, vamos mostrar que o grau relativo de ambos é exatamente 2.

Com efeito, temos que $\overline{x^{2g}(x+1)+1} = 1$ em $\mathcal{O}_{P_0}/P_0 = \mathbb{F}_2 = \mathcal{O}_{P_1}/P_1$ (essas duas últimas igualdades seguem do fato de P_0 e P_1 serem racionais). Daí, $\overline{T^2 + T - x^{2g}(x+1)+1} = T^2 + T + 1$ em $\mathcal{O}_{P_0}/P_0[T] = \mathbb{F}_2[T] = \mathcal{O}_{P_1}/P_1[T]$. O polinômio $T^2 + T + 1$ é irredutível em $\mathbb{F}_2[T]$, daí, pelo [Teorema 81](#), temos que $f(P'_0|P_0) = f(P'_1|P_1) = 2$, onde P'_0 denota o lugar de $\mathbb{F}_2(x, y)$ acima de P_0 e analogamente para P_1 . Isso, então, mostra que $N(F) = 1$.

Já o corpo de funções $E/\mathbb{F}_2$ definido pela equação

$$y^2 + y = x^{2g-1} + 1/(x+1) \tag{5.48}$$

tem gênero $g(E) = g$ e $N(E) = 2$. Nesse caso, os únicos lugares de $\mathbb{F}_2(x)$ que serão totalmente ramificados serão P_∞ e P_1 . De modo análogo ao que foi feito anteriormente, pode-se mostrar que o gênero de $\mathbb{F}_2(x, y)$ é exatamente g e que o lugar P'_∞ acima de P_∞ e o lugar P'_1 acima de P_1 serão os únicos lugares racionais de $\mathbb{F}_2(x, y)$.

Não existe corpo de funções de gênero 1 (sobre $\mathbb{F}_2$) sem lugares racionais. De fato, o [Teorema 130](#) nos diz que todo corpo de funções sobre $\mathbb{F}_q$ tem um divisor de grau 1. Logo, todo corpo de funções sobre $\mathbb{F}_q$ de gênero 1 é elíptico ([STICHTENOTH, 2009](#), p. 217)) e a afirmação segue do primeiro resultado em [Stichtenoth \(2009, p. 218\)](#). Não obstante, para todo $g \geq 2$ a equação

$$y^2 + y = \frac{u(x)}{v(x)}, \tag{5.49}$$

com polinômios $u(x), v(x) \in \mathbb{F}_2[x]$ distintos e tais que $\deg u(x) = \deg v(x) = 2g + 1$, $u(0) = u(1) = 1$ e tal que $v(x)$ seja irredutível, nos dá um corpo de funções $H/\mathbb{F}_2$ de gênero $g(H) = g$ e $N(H) = 0$. A verificação disso segue as mesmas linhas dos casos em [5.46](#) e [5.48](#).

Com tudo isso, mostramos a seguinte

Proposição 165.

1. Para todo $g \geq 1$, existe uma curva sobre $\mathbb{F}_2$ de gênero g com exatamente um ponto racional.
2. Para todo $g \geq 1$, existe uma curva sobre $\mathbb{F}_2$ de gênero g com exatamente 2 pontos racionais.
3. Para todo $g \geq 2$, existe uma curva sobre $\mathbb{F}_2$ de gênero g sem pontos racionais.
4. Para todo (N, g) com $N \geq 3$ e $g \geq (8\gamma + 2)N (\approx 27.237N)$, existe uma curva sobre $\mathbb{F}_2$ de gênero g com exatamente N pontos racionais. ■

5.5 Curvas com um número prescrito de pontos de grau maior

Nessa seção vamos provar o seguinte

Teorema 166. Seja $\mathbb{F}_q$ um corpo finito, e sejam $b_1, \dots, b_m$ inteiros não negativos. Então existe um inteiro $g_0 \geq 0$ com a seguinte propriedade: para todo $g \geq g_0$ existe uma curva C sobre $\mathbb{F}_q$ de gênero $g(C) = g$ tal que C tem exatamente b_r pontos de grau r , para $r = 1, \dots, m$. ■

Antes de demonstrá-lo, precisamos de alguns resultados auxiliares. Lembremo-nos que $B_r(F)$ denota o número de lugares de grau r do corpo de funções $F/\mathbb{F}_q$. Em particular, $B_1(F) = N(F)$ (confira a [Teorema 144](#)). O próximo lema segue imediatamente do [Teorema 157](#).

Lema 167. Para todo $h \in \{0, \dots, q-2\}$ e para todo $c > 0$ existe um corpo de funções $F/\mathbb{F}_q$ com $g(F) \equiv h \pmod{q-1}$ e com $B_1(F) \geq c$. ■

Demonstração. Dado $c > 0$, seja $N \geq c$. O [Teorema 157](#) nos diz que se $g \geq a_q N + b_q$ então $(N, g) \in \mathcal{M}_q$. Seja $g_1 = \lceil a_q N + b_q \rceil$. Se $g_1 \equiv h \pmod{q-1}$, “acabou”. Caso contrário, se $g_1 \not\equiv h \pmod{q-1}$, seja $g_2 > g_1$ com $g_2 \equiv h \pmod{q-1}$. Então $g_2 > g_1 \geq a_q N + b_q$ e portanto $(N, g_2) \in \mathcal{M}_q$. □

Lema 168. Para todo $h \in \{0, \dots, q-2\}$ e toda lista $(c_1, \dots, c_m) \in \mathbb{Z}_{\geq 0}^m$ existe um corpo de funções $F/\mathbb{F}_q$ com $g(F) \equiv h \pmod{q-1}$ e $B_1(F) \geq c_1, \dots, B_m(F) \geq c_m$. ■

Demonstração. Procedemos por indução em m . O caso $m = 1$ é o conteúdo do [lema anterior](#). Agora suponhamos que o resultado é válido para $m - 1 \geq 1$, e consideremos uma lista $(c_1, \dots, c_m) \in \mathbb{Z}_{\geq 0}^m$. Podemos assumir que pelo menos um dos c_i 's é estritamente positivo (caso contrário, o resultado é obviamente válido). Seja $c := \max\{c_1, \dots, c_m\}$. Pela hipótese de indução existe um corpo de funções $E/\mathbb{F}_q$ com $g(E) \equiv h \pmod{q-1}$ e com $B_i(E) \geq c$ para $i = 1, \dots, m-1$. Coloquemos

$$S := \{P \in \mathbb{P}_E \mid \deg P \leq m-1\} \quad (5.50)$$

Vamos analisar a ramificação dos lugares de S numa extensão de corpos de funções do corpo E apropriada. Para isso (e também para o próximo resultado), será indispensável o [TEOREMA DE KUMMER](#).

Escolhamos um lugar $Q \in \mathbb{P}_E$ de grau suficientemente grande de modo que $\ell(Q - \sum_{P \in S} P) \geq 1$. A existência de um tal lugar é garantida pelo [Teorema 152](#). Tomemos, então, um elemento não nulo $x \in \mathcal{L}(Q - \sum_{P \in S} P)$. Consideremos a extensão F/E dada por $F = E(y)$ com

$$y^{q^m} - y = x \quad (5.51)$$

Pelo item 5 da [Teorema 119](#), o gênero de F é congruente a $g(E)$ módulo $(q-1)$ (notemos que $(q^m - 1) = (q-1)(q^{m-1} + \dots + 1)$). Todo lugar $P \in S$ é um zero de x em E . O polinômio $y^{q^m} - y \in \mathbb{F}_q[y]$ se fatora em fatores irredutíveis distintos (pois é separável) sobre $\mathbb{F}_q[y]$. Dentre estes estão fatores de grau 1 (correspondendo aos elementos de $\mathbb{F}_q$). Portanto existem lugares $R \in \mathbb{P}_F$ acima de P com grau relativo $f(R|P) = 1$, logo $\deg R = \deg P$. Daí temos que $B_j(F) \geq B_j(E) \geq c \geq c_j$ para $j = 1, \dots, m-1$. Agora seja $P \in S$ tal que $\deg P = 1$ (tal lugar existe pois mostramos anteriormente que $B_1(E) = N(E) \geq c > 0$). O polinômio $y^{q^m} - y$ tem um fator de grau m . De fato o corpo de raízes de $y^{q^m} - y$ é $\mathbb{F}_{q^m}$ e a extensão $\mathbb{F}_{q^m}/\mathbb{F}_q$ é de Galois. Logo pelo teorema do elemento primitivo $\mathbb{F}_{q^m} = \mathbb{F}_q(\alpha)$, com α raiz de um certo polinômio mônico irredutível $f(x) \in \mathbb{F}_q[x]$ e $\deg f = m = [\mathbb{F}_{q^m} : \mathbb{F}_q]$. Como $\mathbb{F}_{q^m}/\mathbb{F}_q$ é normal, todas as raízes de f estão em $\mathbb{F}_{q^m}$ e, logo, são raízes de $y^{q^m} - y \in \mathbb{F}_q[y]$. Portanto $f \mid y^{q^m} - y$ em $\mathbb{F}_q[y]$, ou seja, $y^{q^m} - y$ possui um fator irredutível de grau m em $\mathbb{F}_q[y] = F_P[y]$. Logo, existe pelo menos um lugar $R \in \mathbb{P}_F$, $R|P$ com $\deg R = \deg P \cdot f(R|P) = \deg f(x) = m$. Portanto $B_m(E) \geq B_1(F) \geq c \geq c_m$.

□

Lema 169. Para todo $h \in \{0, 1, \dots, q-2\}$ e toda lista $(c_1, \dots, c_m) \in \mathbb{Z}_{\geq 0}^m$, existe um corpo de funções $F/\mathbb{F}_q$ com $g(F) \equiv h \pmod{q-1}$ e $B_1(F) = c_1, \dots, B_m(F) = c_m$. ■

Demonstração. Pelo lema anterior, existe $F_0/\mathbb{F}_q$ com $g_0 = g(F_0) \equiv h \pmod{q-1}$ e $B_j(F_0) \geq c_j$, $j = 1, \dots, m$. Escolhamos $S_1 \subset \mathbb{P}_{F_0}$ tal que S_1 tenha exatamente c_i lugares de grau i para

$i = 1, \dots, m$. Seja $S_2 = \{R \in \mathbb{P}_{F_0} \mid \deg R \leq m \text{ e } R \notin S_1\}$. É claro que se $S_2 = \emptyset$ então não há nada a fazer, i.e., F_0 já é tal que $B_i(F_0) = c_i$. Caso contrário, para cada $R \in S_2$ escolhemos $a_R \in \mathcal{O}_R/R = F_R$ tal que a equação $T^q - T = a_R$ não possui soluções em F_R . Isso é possível pois o mapa $\mathbb{F}_q$ -linear $\tau : F_R \rightarrow F_R$ dado por $\tau(v) = v^q - v$ possui núcleo não trivial (temos que $\mathbb{F}_q$ está contido no núcleo de τ), logo não é sobrejetor. Escolhamos também um lugar $Q \in \mathbb{P}_{F_0}$ com $\deg Q > m$ (observemos que $Q \notin S_1 \cup S_2$) e tal que $\deg(Q - \sum_{R \in S_2} R) \geq 2g_0$ (novamente, tal escolha é possível graças ao [Teorema 152](#)). Além disso, para cada $P \in S_1$ fixemos $t_P \in F_0$ tal que $P = (t_P)$.

Consideremos a seguinte aplicação $\mathbb{F}_q$ -linear (lembremo-nos que o corpo residual de qualquer lugar é uma extensão finita de, nesse caso, $\mathbb{F}_q$)

$$\begin{aligned} \psi : \mathcal{L}(Q + \sum_{P \in S_1} P) &\rightarrow \bigoplus_{P \in S_1} \mathcal{O}_P/P \oplus \bigoplus_{R \in S_2} \mathcal{O}_R/R \\ u &\mapsto ((t_P \cdot u)_{P \in S_1}, (u)_{R \in S_2}) \end{aligned} \quad (5.52)$$

O núcleo de ψ é $\mathcal{L}(Q - \sum_{R \in S_2} R) \subset \mathcal{L}(Q + \sum_{P \in S_1} P)$. Antes de mostrarmos isso, notemos que, sendo $A \doteq Q - \sum_{R \in S_2} R$ e $B \doteq Q + \sum_{P \in S_1} P$, temos que $A \leq B$ (como divisores) e portanto $\mathcal{L}(A) \subset \mathcal{L}(B)$, o que mostra que a afirmação anterior faz sentido. Notemos também que $u \in \mathcal{L}(B) \Rightarrow v_P(u) \geq -1$, ou seja, $u = t_P^k \cdot w$, com $k \geq -1$ e $w \in \mathcal{O}_P^\times$. A partir dessas duas observações, é fácil perceber que $u \in \text{Ker}(\psi)$ se, e somente se, forem satisfeitas $v_P(u) \geq 0 \forall P \in S_1$ e $v_R(u) \geq 1 \forall R \in S_2$. Mas os elementos que satisfazem as duas condições anteriores são precisamente os elementos de $\mathcal{L}(A)$.

Temos então, pelo teorema do núcleo e da imagem,

$$\begin{aligned} \dim \text{Im}(\psi) &= \ell(Q + \sum_{P \in S_1} P) - \ell(Q - \sum_{R \in S_2} R) \\ &= \deg(Q + \sum_{P \in S_1} P) - \deg(Q - \sum_{R \in S_2} R) \\ &= \sum_{P \in S_1} \deg P + \sum_{R \in S_2} \deg R \\ &= \dim_{\mathbb{F}_q} \left(\bigoplus_{P \in S_1} \mathcal{O}_P/P \oplus \bigoplus_{R \in S_2} \mathcal{O}_R/R \right) \end{aligned} \quad (5.53)$$

A segunda igualdade segue do [TEOREMA DE RIEMANN-ROCH](#) e do fato que $\deg(Q - \sum_{R \in S_2} R) \geq 2g(F_0)$. A última igualdade nos diz que ψ é sobrejetor. Com isso, é garantida a existência de um elemento $x_1 \in \mathcal{L}(Q + \sum_{P \in S_1} P)$ tal que x_1 possui pólos simples em P , para todo $P \in S_1$ e tal que $x_1 \bmod R = a_R$, para todo $R \in S_2$. De fato basta tomar um elemento na pré imagem de $((1 \bmod P)_{P \in S_1}, (a_R \bmod R)_{R \in S_2})$. Se Q também for pólo (no caso de ser, deverá ser simples) de x_1 , definimos $x \doteq x_1$. Caso contrário, definimos $x \doteq x_1 + z$ com $0 \neq z \in \text{Ker}(\psi)$. Em ambos os casos, x tem pólos simples em Q e em cada $P \in S_1$, e $x \bmod R = a_R$ para cada $R \in S_2$. No segundo caso, o fato de $z \in \text{Ker}(\psi) = \mathcal{L}(Q - \sum_{R \in S_2} R)$ garante que $v_Q(z) = -1$, pois z deve ter pólo (uma vez que possui zeros nos lugares de

S_2), e esse pólo deverá ser Q . Agora consideremos a extensão

$$F_1 \doteq F_0(y) \quad \text{com} \quad y^q - y = x \quad (5.54)$$

Todos os lugares $P \in S_1$ são totalmente ramificados em F_1/F_0 (confira a [Teorema 119](#)). Com isso obtemos pelos menos c_j lugares de grau j , $j = 1, \dots, m$, em F_1 . O lugar Q também é totalmente ramificado, porém ele não entra nas nossas considerações pois $\deg Q > m$. Agora, qualquer lugar R' acima de algum $R \in S_2$ é tal que $\deg R' > \deg R$, pois $T^q - T - a_R \in F_R[T]$ não possui fatores irredutíveis de grau 1 em $F_R[T]$ por não possuir soluções em F_R . Logo, não existe nenhum R'/R com $\deg R' = 1$. Portanto $B_1(F_1) = c_1$. Repetindo esse “processo” (se necessário), teremos F_2 com $B_1(F_2) = c_1$ e $B_2(F_2) = c_2$. É evidente que após um número finito de repetições do processo teremos F_k , $k \leq m$, com $B_j(F_k) = c_j$, $j = 1, \dots, m$. Aplicações sucessivas da [FÓRMULA DO GÊNERO DE HURWITZ](#) nos dá $g(F_k) \equiv g(F_{k-1}) \equiv \dots \equiv g(F_0) \equiv h \pmod{q-1}$.

□

Finalmente, podemos demonstrar o [Teorema 166](#).

Demonstração. [do [Teorema 166](#)]

Lembremos que os números $b_1, \dots, b_m \geq 0$ são *dados*. Ora, o número b_k de lugares $\mathbb{F}_{q^k}$ -racionais está relacionado com os números c_r de lugares de grau r , $r \leq k$, números esses que aparecem nos resultados anteriores, através da expressão [4.20](#):

$$b_k = \sum_{r|k} r \cdot c_r \quad (5.55)$$

Usando a fórmula de inversão de Möbius na expressão anterior (confira [4.21](#)), dada uma lista $(b_1, \dots, b_m) \in \mathbb{Z}_{\geq 0}^m$ obtemos outra lista $(c_1, \dots, c_m) \in \mathbb{Z}_{\geq 0}^m$ e podemos, então, fazer uso dos resultados anteriores. Dito isso, agora é suficiente mostrarmos que para todo $h \in \{0, \dots, q-2\}$, existe um inteiro positivo $g_h \equiv h \pmod{q-1}$ com a seguinte propriedade:

para todo $g \geq g_h$ tal que $g \equiv g_h \pmod{q-1}$ existe um corpo de funções de gênero g com exatamente c_j lugares de grau j , para $j = 1, \dots, m$.

O teorema fica demonstrado tomando o máximo dos g_h 's, para $h = 0, \dots, q-2$.

Começamos então com um corpo de funções F_0 sobre $\mathbb{F}_q$ de gênero $g_0 \doteq g(F_0) \equiv h \pmod{(q-1)}$ tal que $B_j(F_0) = c_j$, $j = 1, \dots, m$. Isso é possível pelo [Teorema 169](#). Para cada inteiro $r \geq 2g_0 + 5$, existe, pela [Teorema 153](#), um lugar $Q \in \mathbb{P}_{F_0}$ tal que $\deg Q = r$. Sejam

$$S \doteq \{P \in \mathbb{P}_{F_0} \mid \deg P \leq m\} \quad \text{e} \quad D \doteq \sum_{P \in S} P \quad (5.56)$$

e

$$g_h \doteq g_0 + (q-1)(\deg D + 3g_0 + 4) \quad (5.57)$$

É claro que $g_h \equiv g_0 \equiv h \pmod{(q-1)}$. Basta, então, construirmos para cada $g = g_h + (q-1)r_h$ (os g 's tais que $g \geq g_h$ e $g \equiv g_h \pmod{(q-1)}$ são todos dessa forma), com $r_h \geq 0$, um corpo de funções $F/\mathbb{F}_q$ de gênero g com $B_j(F) = c_j$, $j = 1, \dots, m$. Essa construção é feita da seguinte maneira. Escolhamos um lugar $Q \in \mathbb{P}_{F_0}$ de grau $r \doteq 2g_0 + 5 + r_h$. Para cada $P \in S$ vale

$$\ell(Q+P) > \ell(Q) > 1 \quad (5.58)$$

pelo [TEOREMA DE RIEMANN-ROCH](#). Escolhamos um elemento $x_P \in \mathcal{L}(Q+P) \setminus \mathcal{L}(Q)$ e coloquemos $x_1 \doteq \sum_{P \in S} x_P$. Todos os lugares $P \in S$ são pólos simples de x_1 , pois a condição imposta a cada x_P , a saber $x_P \in \mathcal{L}(Q+P) \setminus \mathcal{L}(Q)$, “força” $v_P(x_P) = -1$ e $v_{P'}(x_P) \geq 0$ para $P \neq P' \in S$. Daí a [DESIGUALDADE TRIANGULAR ESTRITA](#) implica que cada $P \in S$ é pólo simples de x_1 . Se Q também for pólo de x_1 , colocamos $x \doteq x_1$, caso contrário colocamos $x \doteq x_1 + z$ com $z \in \mathcal{L}(Q)$ não constante, i.e. $z \notin \mathbb{F}_q$, (o que “força” a ser $v_Q(z) = -1$). Em todo caso, x possui pólos simples em Q e nos lugares $P \in S$ e nenhum outro pólo.

Seja $F \doteq F_0(y)$ com $y^q - y = x$. Todos os lugares de S são totalmente ramificados em F/F_0 , daí $B_j(F) = B_j(F_0) = c_j$, $j = 1, \dots, m$. A [FÓRMULA DO GÊNERO DE HURWITZ](#) nos dá

$$2g(F) - 2 = q(2g_0 - 2) + \deg \text{Diff}(F/F_0) = q(2g_0 - 2) + 2(q-1)\deg(D+Q) \quad (5.59)$$

logo

$$g(F) = g_0 + (q-1)(\deg D + 3g_0 + 4 + r_h) = g_h + (q-1)r_h = g \quad (5.60)$$

Isso finaliza a demonstração.

□

5.6 Desigualdades para os coeficientes de $L(t)$

A definição e as principais propriedades do L -polinômio, $L^{(F)}(t)$, de um corpo de funções $F/\mathbb{F}_q$ foram dadas na seção 4.1 do capítulo 4.

Denotaremos $L^{(F)}(t)$ por $L(t)$ e escreveremos

$$L(t) = 1 + a_1 t + \dots + a_{2g} t^{2g} \quad (5.61)$$

onde $g = g(F)$.

O objetivo dessa seção é demonstrar que os coeficientes a_i de $L(t)$ satisfazem certas desigualdades. De modo a formular os resultados, introduzamos certos polinômios com coeficientes em $\mathbb{Z}$. Colocamos

$$\sigma_0 \doteq 0 \quad (5.62)$$

e para todo $r \geq 1$

$$\sigma_r(T_1, \dots, T_r) \doteq rT_r - \sum_{j=1}^{r-1} \sigma_{r-j}(T_1, \dots, T_{r-j}) \cdot T_j \quad (5.63)$$

Daí definimos

$$\beta_r(T_1, \dots, T_r) \doteq \sum_{d|r} \mu\left(\frac{r}{d}\right) \sigma_d(T_1, \dots, T_d) + \sum_{d|r} \mu\left(\frac{r}{d}\right) (q^d + 1) \quad (5.64)$$

onde $\mu: \mathbb{Z} \rightarrow \{-1, 0, 1\}$ denota a função de Möbius. Segue das duas definições anteriores que

$$\varphi_r(T_1, \dots, T_{r-1}) \doteq rT_r - \beta_r(T_1, \dots, T_r) \quad (5.65)$$

é um polinômio em $T_1, \dots, T_{r-1}$.

As seguintes fórmulas foram vistas no item 2 do Teorema 136

$$a_1 = N - (q + 1) = S_1, \quad (5.66)$$

$$ra_r = S_r + \sum_{j=1}^{r-1} S_{r-j} a_j \quad \text{para } r = 1, \dots, g \quad (5.67)$$

Substituindo $N_d = S_d + q^d + 1$ em 4.21, obtemos

$$rB_r = \sum_{d|r} \mu\left(\frac{r}{d}\right) \cdot (q^d + 1 + \sigma_d(a_1, \dots, a_d)) = \beta_r(a_1, \dots, a_r) = ra_r - \varphi_r(a_1, \dots, a_{r-1}) \quad (5.68)$$

Pela definição dos polinômios σ_r segue que $\sigma_1(a_1) = a_1 = S_1$ e daí, fazendo uso de 5.63 e de 5.67, segue, por uma simples indução, que

$$\sigma_r(a_1, \dots, a_r) = S_r \quad \text{para } r = 1, \dots, g \quad (5.69)$$

Então, a partir de 5.68, 5.69, 5.64 e 5.65, obtemos, para $r = 1, \dots, g$,

$$\begin{aligned} rB_r &= \sum_{d|r} \mu\left(\frac{r}{d}\right) \cdot (q^d + 1 + \sigma_d(a_1, \dots, a_d)) \\ &= \beta_r(a_1, \dots, a_r) = ra_r - \varphi_r(a_1, \dots, a_{r-1}) \end{aligned} \quad (5.70)$$

Logo, temos que

$$ra_r = \varphi_r(a_1, \dots, a_{r-1}) + rB_r \quad \text{para } 1 \leq r \leq g \quad (5.71)$$

Como B_r denota o número de lugares de grau r , B_r é não negativo. Daí, a última igualdade prova a seguinte

Proposição 170. Seja $F/\mathbb{F}_q$ um corpo de funções de gênero $g \geq 1$ e seja $L(t) = 1 + a_1t + \dots + a_{2g}t^{2g}$ o seu L -polinômio. Então valem as seguintes desigualdades

$$ra_r \geq \varphi_r(a_1, \dots, a_r) \quad (5.72)$$

para $r = 1, \dots, g$, onde os $\varphi_r(T_1, \dots, T_{r-1})$'s foram definidos em 5.65.

Por exemplo, usando as fórmulas para φ_r dadas na Tabela 2, obtemos (para todo $g \geq 5$)

$$\begin{aligned} a_1 &\geq -(q+1), \\ 2a_2 &\geq a_1^2 + a_1 - (q^2 - q), \\ 3a_3 &\geq -a_1^3 + a_1 + 3a_1a_2 - (q^3 - q), \\ 4a_4 &\geq a_1^4 - a_1^2 - 4a_1^2a_2 + 4a_1a_3 + 2a_2^2 + 2a_2 - (q^4 - q^2), \\ 5a_5 &\geq -a_1^5 + 5a_1^3a_2 - 5a_1^2a_3 - 5a_1a_2^2 + 5a_1a_4 + 5a_2a_3 + a_1 - (q^5 - q). \end{aligned} \quad (5.73)$$

r	Polinômios
1	$\sigma_1 = T_1$
	$\beta_1 = T_1 + q + 1$
	$\varphi_1 = -q - 1$
2	$\sigma_2 = -T_1^2 + 2T_2$
	$\beta_2 = -T_1^2 + q^2 - T_1 + 2T_2 - q$
	$\varphi_2 = T_1^2 - q^2 + T_1 + q$
3	$\sigma_3 = T_1^3 - 3T_1T_2 + 3T_3$
	$\beta_3 = T_1^3 + q^3 - 3T_1T_2 - T_1 + 3T_3 - q$
	$\varphi_3 = -T_1^3 - q^3 + 3T_1T_2 + T_1 + q$
4	$\sigma_4 = -T_1^4 + 4T_1^2T_2 - 4T_1T_3 - 2T_2^2 + 4T_4$
	$\beta_4 = -T_1^4 + q^4 + 4T_1^2T_2 + T_1^2 - 4T_1T_3 - 2T_2^2 - q^2 - 2T_2 + 4T_4$
	$\varphi_4 = T_1^4 - q^4 - 4T_1^2T_2 - T_1^2 + 4T_1T_3 + 2T_2^2 + q^2 + 2T_2$
5	$\sigma_5 = T_1^5 - 5T_1^3T_2 + 5T_1^2T_3 + 5T_1T_2^2 - 5T_1T_4 - 5T_2T_3 + 5T_5$
	$\beta_5 = T_1^5 + q^5 - 5T_1^3T_2 + 5T_1^2T_3 + 5T_1T_2^2 - 5T_1T_4 - 5T_2T_3 - T_1 + 5T_5 - q$
	$\varphi_5 = -T_1^5 - q^5 + 5T_1^3T_2 - 5T_1^2T_3 - 5T_1T_2^2 + 5T_1T_4 + 5T_2T_3 + T_1 + q$

Tabela 2 – Os σ 's, β 's e φ 's.

5.7 Curvas com os coeficientes de $L(t)$ prescritos

Nessa seção consideraremos a seguinte questão: dadas uma lista de m números inteiros $(a_1, \dots, a_m)$ que satisfazem as desigualdades da [Teorema 170](#) e um inteiro $g \geq m$, existe um corpo de funções $F/\mathbb{F}_q$ de gênero $g(F) = g$ cujo L -polinômio tenha a seguinte forma

$$L(t) = 1 + a_1t + \dots + a_mt^m + \dots? \quad (5.74)$$

Veremos que em geral a resposta é “não” pois os coeficientes do L -polinômio de um corpo de funções de gênero g satisfazem algumas propriedades a mais, por exemplo

$$|a_r| \leq \binom{2g}{r} \cdot \sqrt{q}^r \quad \text{para } r = 1, \dots, g \quad (5.75)$$

Essas desigualdades seguem do [TEOREMA DE HASSE-WEIL](#) (e do fato de serem os coeficientes de um polinômio dados por expressões polinomiais simétricas elementares de suas raízes), uma vez que o L -polinômio se fatora, em $\mathbb{C}[t]$, como

$$L(t) = \prod_{k=1}^{2g} (1 - \omega_k t) \quad \text{com } |\omega_k| = \sqrt{q} \quad \forall k \quad (5.76)$$

Entretanto, mostraremos que a questão colocada no início da seção possui resposta afirmativa caso g seja suficientemente grande em relação a m . Lembremos que, para polinômios $f(t), h(t) \in \mathbb{Z}[t]$ e um inteiro $m \geq 0$, a congruência $f(t) \equiv h(t) \pmod{t^m}$ significa que $f(t) = h(t) + t^m \cdot u(t)$, para algum polinômio $u(t) \in \mathbb{Z}[t]$.

Teorema 171. Sejam $a_1, \dots, a_m$ inteiros que satisfazem as desigualdades

$$ra_r \geq \varphi_r(a_1, \dots, a_{r-1}) \quad (5.77)$$

para $r = 1, \dots, m$. Então existe um inteiro $g_0 \geq m$ com a seguinte propriedade: para todo $g \geq g_0$ existe um corpo de funções $F/\mathbb{F}_q$ cujo L -polinômio satisfaz a congruência

$$L(t) \equiv 1 + a_1 t + \dots + a_m t^m \pmod{t^{m+1}} \quad (5.78)$$

■

A condição $g_0 \geq m$ garante que o L -polinômio terá pelo menos m coeficientes.

Vamos demonstrar, juntamente com o teorema anterior, o seguinte

Lema 172. Para todo $m \geq 2$ e todo $(c_1, \dots, c_{m-1}) \in \mathbb{Z}^{m-1}$ vale $\varphi_m(c_1, \dots, c_{m-1}) \equiv 0 \pmod{m}$.

■

Demonstração. Procedemos por indução em m . Para $m = 1$, o lema anterior é trivial (para $m = 1$ o polinômio φ_1 é constante igual a $-(q+1)$ e a congruência módulo 1 não diz essencialmente nada). Vamos agora mostrar que o teorema anterior é válido para $m = 1$. A suposição $ma_m \geq \varphi_m(a_1, \dots, a_{m-1})$ significa, nesse caso, apenas que $a_1 \geq -(q+1)$. Definamos $b_1 \doteq a_1 + (q+1) \geq 0$. Pelo [Teorema 166](#), existe um inteiro $g_1 \geq m = 1$ tal que para todo $g \geq g_1$ existe um corpo de funções $F/\mathbb{F}_q$ de gênero $g(F) = g$ e tal que $B_1(F) = b_1$. Por [5.71](#), o coeficiente do monômio de grau um do L -polinômio de F que, digamos, se escreve da seguinte maneira

$$L^{(F)}(t) = 1 + \alpha_1 t + \alpha_2 t^2 + \dots \quad (5.79)$$

é dado por

$$\alpha_1 = \varphi_1 + B_1(F) = -(q+1) + b_1 = -(q+1) + a_1 + (q+1) = a_1 \quad (5.80)$$

Isso mostra, então, que

$$L^{(F)}(t) \equiv 1 + a_1 t \pmod{t^2} \quad (5.81)$$

Agora, suponhamos que o [Teorema 171](#) o [Teorema 172](#) são válidos para $1 \leq k \leq m$. Primeiramente, vamos mostrar que o [lema](#) é também válido para $m+1$. São dados m inteiros $c_1, \dots, c_m$. Escolhamos outros m inteiros $d_1, \dots, d_m$ tais que

$$c_r \equiv d_r \pmod{m+1} \quad \text{e} \quad rd_r \geq \varphi(d_1, \dots, d_{r-1}) \quad \text{para} \quad 1 \leq r \leq m \quad (5.82)$$

Vamos usar o [Teorema 171](#) no caso m : pela hipótese de indução, existe um corpo de funções $F^*/\mathbb{F}_q$ cujo L -polinômio $L^{(F^*)}(t)$ satisfaz

$$L^{(F^*)}(t) \equiv 1 + d_1 t + \dots + d_m t^m \pmod{t^{m+1}} \quad (5.83)$$

Por [5.71](#), o coeficiente d_{m+1} do monômio de grau $m+1$ de $L^{(F^*)}(t)$ é dado por

$$d_{m+1} = \frac{\varphi_{m+1}(d_1, \dots, d_m)}{m+1} + B_{m+1}(F^*) \quad (5.84)$$

Logo $\varphi_{m+1}(d_1, \dots, d_m) \equiv 0 \pmod{m+1}$ e daí, uma vez que $c_i \equiv d_i \pmod{m+1}$ para $1 \leq i \leq m$, concluimos que

$$\varphi_{m+1}(c_1, \dots, c_m) \equiv \varphi_{m+1}(d_1, \dots, d_m) \equiv 0 \pmod{m+1} \quad (5.85)$$

E isso finaliza a demonstração do [lema](#). Agora vamos finalizar a demonstração do [teorema](#). São dados $m+1$ inteiros $a_1, \dots, a_{m+1}$ que satisfazem as desigualdades $ra_r \geq \varphi_r(a_1, \dots, a_{r-1})$ para $r = 1, \dots, m+1$. Ora, acabamos de mostrar que as congruências $\varphi_r(a_1, \dots, a_{r-1}) \equiv 0 \pmod{r}$ são válidas para $r = 1, \dots, m+1$. Então os números

$$b_r \doteq a_r - \frac{\varphi_r(a_1, \dots, a_{r-1})}{r} \quad (5.86)$$

são *inteiros* não negativos. Logo, pelo [Teorema 166](#) existe um inteiro $g_1 \geq m+1$ com a seguinte propriedade: para cada $g \geq g_1$ existe um corpo de funções $F/\mathbb{F}_q$ com $B_r(F) = b_r$ para $1 \leq r \leq m+1$. Novamente por [5.71](#), o L -polinômio $L^{(F)}(t)$ de F satisfaz a congruência

$$L^{(F)}(t) \equiv 1 + a_1 t + \dots + a_{m+1} t^{m+1} \pmod{t^{m+2}} \quad (5.87)$$

E com isso acabamos.

□

REFERÊNCIAS

- BASSA, A.; GARCIA, A.; STICHTENOTH, H. A new tower over cubic finite fields. **Moscow Mathematical Journal**, v. 8, n. 3, p. 401–418, 2008. Citado na página 115.
- BEZERRA, J.; GARCIA, A.; STICHTENOTH, H. An explicit tower of function fields over cubic finite fields and zink's lower bound. **Journal für die reine und angewandte Mathematik**, v. 589, p. 159–199, 2005. Citado na página 115.
- DUURSMA, I.; MAK, K.-H. On lower bounds for the ihara constants $a(2)$ and $a(3)$. 2011. Disponível em: <<https://arxiv.org/abs/1102.4127>>. Citado na página 135.
- ELKIES, N. D.; HOWE, E. W.; KRESCH, A.; POONEN, B.; WETHERELL, J. L.; ZIEVE, M. E. Curves of every genus with many points, ii: Asymptotically good families. **Duke Mathematical Journal**, v. 122, n. 1, p. 399–422, 2004. Citado na página 14.
- GARCIA, A.; STICHTENOTH, H. A tower of artin-schreier extensions of function fields attaining the drinfeld-vlăduț bound. **Inventiones mathematicae**, v. 121, p. 211–222, 1995. Citado nas páginas 14, 128 e 129.
- _____. On the asymptotic behavior of some towers of function fields over finite fields. **Journal of Number Theory**, v. 61, p. 248–273, 1996. Citado na página 115.
- GOPPA, V. D. Codes on algebraic curves. **Soviet Mathematics Doklady**, v. 24, n. 1, p. 170–172, 1981. Citado na página 13.
- IHARA, Y. Some remarks on the number of rational points of algebraic curves over finite fields. **Journal of the Faculty of Science, the University of Tokyo. Sect. 1 A, Mathematics**, v. 28, p. 721–724, 1981. Citado nas páginas 14 e 115.
- KRESCH, A.; WETHERELL, J. L.; ZIEVE, M. E. Curves of every genus with many points, i: Abelian and toric families. **Journal of Algebra**, v. 250, p. 353–370, 2002. Citado na página 15.
- NIEDERREITER, H.; XING, C. **Rational Points on Curves over Finite Fields: Theory and Applications**. [S.l.]: Cambridge University Press, 2001. (London Mathematical Society Lecture Note Series, v. 285). Citado na página 26.
- SERRE, J.-P. **Nombres de points des courbes algébriques sur $\mathbb{F}_q$** . 1982–1983. In Séminaire de Théorie des Nombres de Bordeaux. Exposé n. 22. Citado na página 14.
- _____. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. **Comptes rendus de l'Académie des sciences. Série I, Mathématique**, v. 296, p. 397–402, 1983. Citado na página 115.
- STICHTENOTH, H. **Algebraic Function Fields and Codes**. 2. ed. [S.l.]: Springer-Verlag, 2009. (Graduate Texts in Mathematics, v. 254). Citado nas páginas 13, 19, 38, 128, 135 e 136.

_____. Curves with a prescribed number of rational points. **Finite Fields and Their Applications**, v. 17, p. 552–559, 2011. Citado na página 16.

STICHTENOTH, H.; ANBAR, N. Curves of every genus with a prescribed number of rational points. **Bulletin of the Brazilian Mathematical Society**, v. 44, n. 2, p. 173–193, 2013. Citado nas páginas 13 e 15.

TSFASMAN, M. A.; VLADUȚ, S. G.; ZINK, T. Modular curves, shimura curves and goppa codes better than the varshamov-gilbert bound. **Mathematische Nachrichten**, v. 109, p. 21–28, 1982. Citado nas páginas 14 e 115.

ZINK, T. Degeneration of shimura surfaces and a problem in coding theory. In: BUDACH, L. (Ed.). **Fundamentals of Computation Theory**. [S.l.]: Springer-Verlag, 1985. (Lecture Notes in Computer Science, v. 199), p. 503–511. Citado na página 115.