Tese apresentada para obtenção do grau de Doutor em Matemática pelo
INSTITUTO DE MATEMÁTICA PURA E APLICADA

DUAS TORRES DE CORPOS DE FUNCÕES SOBRE CORPOS FINITOS E AS COTAS DE DRINFELD-VLADUT E DE T. ZINK

por
Juscelino Bezerra dos Santos

Rio de Janeiro – 24 de Março de 2004

À minha família: Gerson, Iolanda, Jacqueline, Jair, Júnior e Julio.

Agradecimentos

àquelas pessoas que ao longo desta estrada infinita que é a matemática se fizeram presentes em muitos momentos. Em especial ao Arnaldo Garcia pela orientação e pelo entusiasmo, aos professores Francisco Pimentel, Eduardo Esteves e Karl-Otto Stöhr pela minha formação em Álgebra, aos colegas algebróides Papa, Parham, Lulu, Miriam, Cleber, Tais, Juliana e Paula pelos muitos papos, aos colegas da UFC Alexandre César, Ulisses, Paulinho, Julia Toledo e Odair pela eterna força e aos colegas do IMPA Jeronimo, e Fátima por outros muitos papos. Aos colegas de república Pedro Boltz, Krerley, Perfilino, Albetã e Bruno. À Dona Ligia pelos eternos abrigo e colo. Ao Cnpq pelo essencial auxílio financeiro e finalmente agradeço ao Francisco Petrúcio pela enorme paciência em me socorrer das várias armadilhas do LaTeX.

Conteúdo

Capítulo 1

Introdução e preliminares

1.1 Introdução

"...asymptotically optimal curves yield excellent linear error-correcting codes..."[3]

O interesse de se estudar seqüências de corpos de funções sobre corpos finitos, ou geometricamente, seqüências de curvas algébricas projetivas irredutíveis e não-singulares definidas sobre um corpo finito, foi revitalizado com a construção dos códigos algébrico-geométricos por Goppa na década de 70. Com esta construção, Goppa buscava determinar uma seqüência de códigos atingindo a cota de Gilbert-Varshamov. Durante muito tempo os pesquisadores da teoria dos códigos corretores de erros foram incapazes de exibir construções de códigos com parâmetros relativos que atingissem ou superassem esta cota, o que os levou a pensar que o gráfico da função que define esta cota limitasse a região do plano real conhecida como domínio dos códigos (vide Prop. 1.2.1). Para surpresa de tais pesquisadores, Tsfasman, Vladut e Zink conseguiram uma seqüência de códigos de Goppa que superava a cota de Gilbert-Varshamov em alguns casos (vide Teor. 1.2.5). Uma tal seqüência de códigos de Goppa é construída a partir de uma seqüência de corpos de funções definidos sobre um corpo finito, chamada torre de corpos de funções. Existe um parâmetro assintótico a partir do qual se determina se uma torre de corpos dá origem, ou não, a uma boa seqüência de códigos corretores de erros. Este parâmetro, definido a partir do gênero e do número de lugares racionais de cada corpo de função que forma a torre, é chamado de limite da torre (vide Def. 1.2.6). Torres com limite positivo, conhecidas como torres assintoticamente boas, podem medir a precisão dos parâmetros relativos de códigos lineares, na medida em que melhoram a cota de Gilbert-Varshamov.

O objetivo deste trabalho é apresentar duas novas torres assintoticamente boas com novas características: são definidas recursivamente por equações racionais não-polinomiais, e têm passos com extensões não-Galois. A primeira, estudada no Cap. 2, é uma torre sobre um corpo de cardinalidade quadrada, $\mathbb{F}_{q^2}$, definida recursivamente pela equação $(y-1)/y^q = (x^q - 1)/x$ (vide Def. 1.2.8), que atinge a cota de Drinfeld-Vladut (vide Teor. 1.2.4), portanto otimal. Esta torre é uma subtorre da torre de Garcia e Stichtenoth, definida recursivamente pela equação $y^q + y = x^q/(x^{q-1} + 1)$ e otimal sobre $\mathbb{F}_{q^2}$ (vide Obs. 2.1.3), mas a determinação dos gêneros dos corpos envolvidos requer as considerações feitas no Cap. 2 (vide Obs. 2.3.7). O valor exato do gênero em cada passo desta torre é determinado e isto é muito importante em algumas aplicações (vide [1], [11]). A segunda torre, estudada no Cap. 3, é definida sobre um corpo de cardinalidade cúbica, $\mathbb{F}_{q^3}$, pela equação $(1-y)/y^q = (x^q+x-1)/x$. Nós mostramos que o limite $\lambda(\mathcal{F})$ desta torre (vide Def. 1.2.6) satisfaz $\lambda(\mathcal{F}) \geq 2(q^2-1)/(q+2)$, e este limite generaliza a cota inferior para a função $A(l)$ (vide Teo. 1.2.4), dada por Zink no caso em que l é uma potência cúbica de um primo, isto é, $l = q^3$, para q primo (vide Teor. 3.1.2). Além disso, o limite desta torre melhora a cota de Gilbert-Varshamov para $q \geq 7$ (vide Obs. 3.3.11).

Começamos o primeiro capítulo com uma abordagem rápida da teoria dos códigos corretores de erros, a principal motivação do nosso estudo, onde se destaca a cota de Gilbert-Varshamov (Prop. 1.2.1). Na seção 1.2 apresentamos o objeto fundamental que utilizamos (corpos de funções algébricas) e mostramos como construir códigos a partir desses objetos. Além disso, aparece a importante quantidade assintótica $A(q)$ (vide Teo. 1.2.4) e com o Teorema 1.2.5 desta seção melhoramos a cota de Gilbert-Varshamov se $q \geq 49$. Torres de corpos de funções algébricas aparecem na seção 1.3, juntamente com uma lista de torres que são assintoticamente boas (veja a Definição 1.2.6). Como o nosso objetivo é o cálculo do limite de torres, nós necessitamos conhecer o gênero dos corpos de funções que compõem a torre. Para isto, na seção 1.3, destacam-se teoremas sobre ramificação e sobre o cálculo do expoente da diferente que são essenciais no uso da fórmula do gênero de Riemman-Hurwitz. Para finalizar este capítulo algumas observações são colocadas na seção 1.4. Estas observações têm como objetivo conseguir, através da equação que define a torre, novos geradores para os corpos de funções envolvidos (processo de redução) de modo que tenhamos condições de aplicar o teorema de Kummer e outros resultados da seção anterior.

Os próximos dois capítulos têm basicamente o mesmo padrão. Na primeira seção (seções 2.1 e 3.1) eles apresentam a equação que define a torre em questão e discutem o comportamento de ramificação no primeiro passo da torre, isto é, na extensão F_2/F_1 (para $\mathcal{F} = (F_1, F_2, ...)$). A partir do estudo feito nesta seção inicia-se na segunda seção (seções 2.2 e 3.2) o estudo do comportamento de ramificação num passo F_n/F_{n-1} qualquer da torre. Pirâmides são utilizadas neste contexto, porém não são suficientes para o cálculo de todas as ramificações. O processo de redução se torna portanto essencial. Ainda nesta seção calculamos o expoente da diferente nos lugares que se ramificam no passo F_n/F_{n-1}. Na última seção do capítulo 2 e na penúltima do capítulo 3 (seções 2.3 e 3.3), tendo-se calculado a diferente no passo F_n/F_{n-1} na seção anterior, utiliza-se a fórmula do gênero de Riemann-Hurwitz para se calcular o valor exato do gênero de F_n, e conseqüentemente se obter o gênero das torres. Além disso, também mostramos que alguns lugares de F_1 se decompõem totalmente na torre e, para nossa sorte, estes lugares são em quantidade suficiente para que um bom limite seja alcançado. O capítulo 3 tem ainda uma última seção (seção 3.4) com a apresentação de uma torre definida sobre $K = \mathbb{F}_{q^p}$, $p = \mathrm{car}(K)$, dada recursivamente pela equação $y^q - y = x^q/(1-x)$. Esta torre é assintoticamente ruim para $q > 2$. Para $q = 2$ ela é uma torre assintoticamente otimal sobre $\mathbb{F}_4$ (vide [6]).

1.2 Códigos e corpos de funções

1.2.1 Códigos lineares

"Codes were invented to correct errors on noisy communication channels."[12]

Sejam q uma potência de um primo, $\mathbb{F}_q$ o corpo finito com q elementos e ainda $\mathbb{F}_q^n$ o $\mathbb{F}_q$-espaço vetorial formado pelas n-uplas de elementos de $\mathbb{F}_q$. Um *código linear* é um subespaço vetorial C de $\mathbb{F}_q^n$. O conjunto $\mathbb{F}_q$ é chamado de alfabeto, os elementos de $\mathbb{F}_q^n$ são chamados de palavras e o inteiro n é chamado o comprimento das palavras. Para um código C nós temos uma métrica, chamada a distância de Hamming, definida por $d(x,y) = \#\{i : 1 \leq i \leq n, x_i \neq y_i\}$, onde $x = (x_1, ..., x_n)$. O peso $w(x)$ de uma palavra x é a distância dela a origem.

Um código $C \subset \mathbb{F}_q^n$ é chamado um (n,k,d)-código se sua dimensão é k e o peso mínimo de uma palavra não-nula de C, chamado de distância mínima, é d. Um código com distância mínima d pode corrigir $\left[\frac{1}{2}(d-1)\right]$ erros. Para um (n,k,d)-código C define-se a taxa de transmissão de C por $R = R(C) = k/n$ e define-se a distância mínima relativa de C por $\delta = \delta(C) = d/n$. Um problema central na teoria dos códigos é o de achar códigos longos (comprimento grande) com transmissão de informação segura, o que se traduz em termos dos parâmetros relativos como achar códigos longos que possam corrigir uma porcentagem fixa de erros por palavra e que tenham taxa de transmissão estritamente positiva. Uma sequência de códigos (C_i) com parâmetros (n_i, k_i, d_i) tal que $n_i \to \infty$ e as razões d_i/n_i e k_i/n_i convergem para δ e R com $\delta R > 0$ é chamada uma sequência assintoticamente boa de códigos.

Seja $V_q := \{(\delta(C), R(C)) \in [0,1]^2 : C$ é um código sobre $\mathbb{F}_q\}$ e considere $U_q \subset [0,1]^2$ o conjunto dos pontos limites de V_q. A região do plano U_q é chamada de *domínio dos códigos* e é limitada no quadrado unitário pelo eixo-δ, pelo eixo-R e pelo gráfico da função contínua $\alpha_q : [0,1] \to [0,1]$ definida por

$$\alpha_q(\delta) = sup\{R : (\delta, R) \in U_q\}.$$

Esta função satisfaz $\alpha_q(0) = 1$, $\alpha_q(\delta) = 0$ para $1-q^{-1} \leq \delta \leq 1$, e α_q é decrescente no intervalo $0 \leq \delta \leq 1-q^{-1}$ (conforme [11]), porém no intervalo $0 < \delta < 1-q^{-1}$ o seu valor exato ainda é desconhecido.

Proposição 1.2.1. *(*Cota de Gilbert-Varshamov, vide [15] Prop. VII.2.3*) Para $0 \leq \delta \leq 1-q^{-1}$ a função α_q satisfaz $\alpha_q(\delta) \geq 1-H_q(\delta)$, onde $H_q : [0, 1-q^{-1}] \to \mathbb{R}$ é a função entropia definida por*

$$H_q(\delta) = \begin{cases} 0 & para\ \delta = 0 \\ \delta log_q(q-1) - \delta log_q(\delta) - (1-\delta) log_q(1-\delta) & para\ 0 < \delta \leq 1-q^{-1}. \end{cases}$$

A cota de Gilbert-Varshamov garante a existência de sequências assintoticamente boas de códigos. Durante muito tempo suspeitou-se que $\alpha_q(\delta) = 1 - H_q(\delta)$ para $0 \leq \delta \leq 1-q^{-1}$, suspeita esta que veio a ser dada como falsa com a construção dos códigos algébrico-geométricos por Tsfasman-Vladut-Zink[19] utilizando a teoria dos corpos de funções.

1.2.2 Corpos de funções e códigos de Goppa

Um *corpo de funções algébricas* (de uma variável) sobre $\mathbb{F}_q$ é uma extensão finitamente gerada de corpos $F/\mathbb{F}_q$ com grau de transcendência 1, tal que $\mathbb{F}_q$ é algebricamente fechado em F.

Para um corpo de funções $F/\mathbb{F}_q$ denotamos por $\mathbb{P}_F$ o conjunto dos lugares de $F/\mathbb{F}_q$, por $N(F)$ o número de lugares de grau um de $F/\mathbb{F}_q$ e por $g(F)$ o gênero de $F/\mathbb{F}_q$.

Seja $F/\mathbb{F}_q$ um corpo de funções algébricas de gênero $g = g(F)$. Para um conjunto $P = \{P_1, ..., P_n\}$ de n lugares de grau 1 de $F/\mathbb{F}_q$, dois a dois distintos, seja L um subespaço $\mathbb{F}_q$-linear de F tal que nenhuma função $f \in L$ tenha pólo nos lugares P_i. A aplicação $\alpha : L \to \mathbb{F}_q^n$ definida por $\alpha(f) = (f(P_1), ..., f(P_n))$ é $\mathbb{F}_q$-linear e portanto sua imagem é um código. No caso em que o conjunto L é da forma $L = L(D) = \{f \in F : div(f) + D \geq 0\}$ para algum divisor D com suporte disjunto de P, a imagem de α é o que chamamos de *código algébrico-geométrico* ou *código geométrico de Goppa*, e é denotada por $C_L(P, D)$.

Teorema 1.2.2. *(*[15] Cor.II.2.3*) Suponha que $n > deg(D)$. Então $C_L(P, D)$ é um (n, k, d)-código com $k = dimL(D) \geq deg(D) + 1 - g$ e a igualdade ocorre se $deg(D) \geq 2g-1$. Além disso, $d \geq n - deg(D)$.*

Como conseqüência do teorema acima, para se obter bons códigos algébrico-geométricos temos que construir corpos de funções com muitos lugares de grau 1. De fato, se a razão $deg(D)/n$ é fixada, então a taxa de transmissão cresce com a taxa n/g. Para se estimar, então, o número de lugares de grau 1, ou na linguagem de curvas algébricas, o número de pontos racionais de uma curva, nós temos o seguinte importante teorema (demonstrado por Hasse para o caso $g = 1$ e por Weil no caso geral):

Teorema 1.2.3. *(*Cota de Hasse-Weil,[20]*) O número $N = N(F)$ de lugares de grau 1 de um corpo de funções $F/\mathbb{F}_q$ de genêro $g = g(F)$ pode ser estimado por*

$$N \leq q + 1 + 2gq^{1/2}.$$

Esta cota, apesar de ser "sharp" (existem corpos de funções que atingem esta cota), pode ser melhorada em alguns casos. Por exemplo, se o gênero do corpo de funções é grande em relação à cardinalidade do corpo finito $\mathbb{F}_q$, esta cota pode ser melhorada de maneira significativa. Ihara [9] demonstrou que se $2g > q - q^{1/2}$, então a cota de Hasse-Weil não é atingida (vide também [17]).

Fixados q uma potência de um primo e g um inteiro não-negativo, a cota de Hasse-Weil nos permite definir a seguinte quantidade:

$$N_q(g) = max\{N(F) \text{ tal que } F/\mathbb{F}_q \text{ é um corpo de funções de genêro } g\}.$$

Teorema 1.2.4. *(*Cota de Drinfeld-Vladut,[2]*) Para cada q potência de um primo, seja $A(q)$ a quantidade assintótica definida por*

$$A(q) := \lim sup_{g\to\infty} \frac{N_q(g)}{g}.$$

Então $A(q) \leq q^{1/2} - 1$.

A função $A(q)$, introduzida por Ihara para medir o comportamento assintótico do número de pontos racionais, nos dá outra cota inferior para a função α_q. De fato, temos o seguinte teorema, provado primeiramente por Tsfasman, Vladut e Zink, relacionando comportamento assintótico de corpos de funções e de códigos:

Teorema 1.2.5. *(*[15] Prop. VII.2.5 ou [18], Corolário 3.4.2*) Se $A(q) > 1$, então $\alpha_q(\delta) \geq (1 - A(q)^{-1}) - \delta$ no intervalo $0 \leq \delta \leq 1 - A(q)^{-1}$.*

Além disso, para q um quadrado, nós temos que $A(q) = q^{1/2} - 1$ (veja por exemplo [9], [19], [4] e [5]). Logo, $\alpha_q(\delta) \geq (1 - 1/(q^{1/2} - 1)) - \delta$ e assim existe uma seqüência de códigos algébricos-geométricos sobre $\mathbb{F}_q$, q um quadrado, com um ponto limite no quadrado $[0,1]^2$ acima ou sobre a reta $R + \delta = 1 - 1/(q^{1/2} - 1)$. Para $q \geq 49$ esta reta está acima da cota de Gilbert-Varshamov em algum intervalo contendo $\delta_0 = (q-1)/(2q-1)$ (veja por exemplo [18], Teorema 3.4.4 ou [19]).

É importante mencionar que para q um não-quadrado, nenhum valor exato de $A(q)$ é conhecido. Em compensação algumas cotas inferiores são conhecidas e uma maneira de se encontrar estas cotas é através do estudo de torres de corpos de funções sobre corpos finitos.

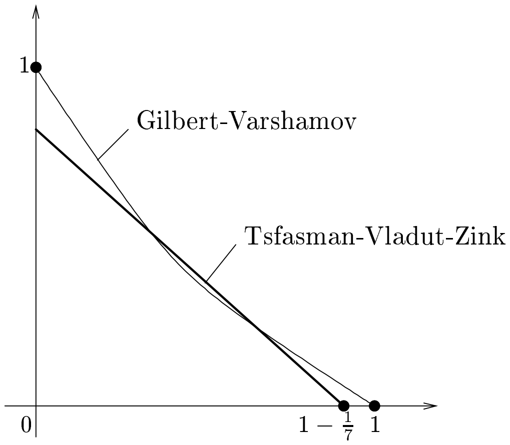

Figura 1.1: Cotas para $q = 64$

1.2.3 Torres de corpos de funções sobre corpos finitos

Uma *torre de corpos de funções* sobre $\mathbb{F}_q$ é uma seqüência infinita de corpos de funções algébricas sobre $\mathbb{F}_q$, $\mathcal{F} = (F_1, F_2, F_3, ...)$, tais que

(i) para cada $n \geq 1$ a extensão de corpos de funções F_{n+1}/F_n é finita e separável de grau $[F_{n+1} : F_n] > 1$; e

(ii) existe $n \geq 1$ tal que $g(F_n) > 1$.

Vale notar que a condição (*ii*) na definição acima e a fórmula do gênero de Hurwitz, que será apresentada na próxima seção (Teo. 1.3.2), implicam que $\lim_{n\to\infty} g(F_n) = \infty$. Salientamos ainda que $\mathbb{F}_q$ é algebricamente fechado em F_n, para todo n.

Definição 1.2.6. *Para uma torre $\mathcal{F} = (F_1, F_2, F_3, ...)$ de corpos de funções sobre $\mathbb{F}_q$, seja*

$$\lambda(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)},$$

o limite da torre $\mathcal{F}$. A torre $\mathcal{F}$ é dita assintoticamente boa (respectivamente ruim) se $\lambda(\mathcal{F}) > 0$ (respectivamente $\lambda(\mathcal{F}) = 0$).

Este limite realmente existe [7], e é óbvio que $\lambda(\mathcal{F}) \leq A(q)$. Nós dizemos que a torre $\mathcal{F}$ é otimal se $\lambda(\mathcal{F}) = A(q)$.

Torres assintoticamente boas com limite $\lambda(\mathcal{F}) > 1$ nos permitem encontrar novas cotas para a função α_q (vide Teo. 1.2.5). Em geral, não é fácil achar torres que são assintoticamente boas. A seguir, apresentaremos uma lista com algumas torres assintoticamente boas:

(1) (1982) Ihara [9] e, independentemente, Tsfasman, Vladut e Zink [21] através de curvas modulares conseguiram torres assintoticamente otimais sobre o corpo finito com q^2 elementos;

(2) (1983) Serre [14], usando métodos de corpos de classe, mostrou que existe uma constante $c > 0$ que satisfaz $A(q) \geq c\log(q)$ para qualquer q potência de primo;

(3) (1985) Zink [21], utilizando degeneração de variedades de Shimura, construiu uma torre de curvas definida sobre $\mathbb{F}_{p^3}$, para um primo p qualquer, com limite $\lambda(\mathcal{F}) \geq 2(p^2-1)/(p+2)$;

Observação 1.2.7. Torres de corpos de classe não são explícitas e torres modulares são em princípio construtivas, mas usualmente elas são muito difíceis de explicitar pois exigem o conhecimento de resultados profundos em geometria algébrica, assim como também acontece na construção feita por Zink. No entanto, na construção e no uso de códigos, precisamos ter as equações explícitas que definem os corpos de funções na torre.

Definição 1.2.8. *Seja $\mathcal{F} = (F_1, F_2, F_3, ...)$ uma torre de corpos de funções sobre $\mathbb{F}_q$ e seja $\phi(X,Y) \in \mathbb{F}_q[X,Y]$ um polinômio. Nós dizemos que a torre $\mathcal{F}$ é definida recursivamente pela equação $\phi(X,Y) = 0$, se existem elementos $x_n \in F_n$ para $n \geq 1$ tais que $F_1 = \mathbb{F}_q(x_1)$ é o corpo de funções racionais e, para todo $n \geq 1$, temos $F_n = F_{n-1}(x_n)$ com $\phi(x_{n-1}, x_n) = 0$ e, além disso, o polinômio $\phi(x_{n-1}, Y) \in F_{n-1}[Y]$ é absolutamente irredutível.*

(4) (1995) Garcia e Stichtenoth [5] apresentaram uma construção explícita de uma torre $\mathcal{F} = (F_1, F_2, F_3, ...)$ sobre $\mathbb{F}_{q^2}$ que atinge a cota de Drinfeld-Vladut, isto é, $\lambda(\mathcal{F}) = q - 1$. Ela é definida por $F_1 = \mathbb{F}_{q^2}(x_1)$, o corpo de funções racionais sobre $\mathbb{F}_{q^2}$, e para cada $n \geq 1$, $F_{n+1} = F_n(z_{n+1})$ onde $z_{n+1}^q + z_{n+1} = x_n^{q+1}$ e $x_n := z_n/x_{n-1} \in F_n$ para $n \geq 2$.

(5) (1996) Garcia e Stichtenoth [4] apresentaram outra torre otimal sobre $\mathbb{F}_{q^2}$, $\mathcal{T}$, definida recursivamente pela equação $y^q + y = x^q/(x^{q-1}+1)$, isto é, $\mathcal{T} = (T_1, T_2, T_3, ...)$ com $T_1 = \mathbb{F}_{q^2}(x_1)$, o corpo de funções racionais sobre $\mathbb{F}_{q^2}$, e para $n \geq 1$, $T_{n+1} = T_n(x_{n+1})$ onde $x_{n+1}^q + x_{n+1} = x_n^q/(x_n^{q-1}+1)$.

(6) (2002) van der Geer e van der Vlugt [8] construiram explicitamente uma torre sobre $\mathbb{F}_8$ com limite no mínimo $3/2 = 2(2^2-1)/(2+2)$ (a cota dada por Zink para $p = 2$). Esta torre é definida recursivamente pela equação $y^2 + y = x + 1 + 1/x$.

Observação 1.2.9. As torres construídas por Garcia e Stichtenoth e a torre de van der Geer e van der Vlugt acima são torres do tipo Artin-Schreier, isto é, cada passo da torre é uma extensão E/F de Galois de grau q, gerada por um elemento $y \in E$ tal que o polinômio minimal de y sobre F é da forma $P(y) = u$, onde $P(T) \in \mathbb{F}_q[T]$ é um polinômio aditivo separável de grau q e $u \in F$.

Observação 1.2.10. Com torres que são assintoticamente boas nós podemos construir outras torres que são assintoticamente boas, através da noção de subtorres. Seja $\mathcal{F} = (F_1, F_2, F_3, ...)$ uma torre de corpos de funções sobre $\mathbb{F}_q$. Uma outra torre de corpos de funções, $\mathcal{E} = (E_1, E_2, E_3, ...)$, sobre $\mathbb{F}_q$, é dita uma subtorre de $\mathcal{F}$, e denotamos por $\mathcal{E} \prec \mathcal{F}$, se para cada inteiro positivo n, existe um indice $m = m(n) \geq 1$ tal que $E_n \subset F_m$. É fácil ver que se $\mathcal{E}$ é uma subtorre de $\mathcal{F}$, então $\lambda(\mathcal{E}) \geq \lambda(\mathcal{F})$ ([4] Cor.2.4). A torre $\mathcal{T}$ no item (5) acima é uma subtorre da torre $\mathcal{F}$ no item (4) [4].

Para o estudo do limite $\lambda(\mathcal{F})$ de uma torre sobre $\mathbb{F}_q$ é conveniente considerar o comportamento assintótico do número de lugares de grau 1 e do gênero separadamente.

Teorema 1.2.11. [7] *Seja $\mathcal{F} = (F_1, F_2, F_3, ...)$ uma torre de corpos de funções sobre $\mathbb{F}_q$. Então os limites $\gamma(\mathcal{F}) := \lim_{n\to\infty} \dfrac{g(F_n)}{[F_n : F_1]}$ e $\upsilon(\mathcal{F}) := \lim_{n\to\infty} \dfrac{N(F_n)}{[F_n : F_1]}$ existem, e temos*

$$0 < \gamma(\mathcal{F}) \leq \infty \quad e \quad 0 \leq \upsilon(\mathcal{F}) \leq N(F_1) < \infty.$$

Além disso, temos que $\lambda(\mathcal{F}) = \upsilon(\mathcal{F})/\gamma(\mathcal{F})$ e portanto, a torre $\mathcal{F}$ é assintoticamente boa se, e somente se, $\upsilon(\mathcal{F}) > 0$ e $\gamma(\mathcal{F}) < \infty$.

Existe um critério simples que nos garante quando $\upsilon(\mathcal{F}) > 0$: Para uma torre $\mathcal{F} = (F_1, F_2, F_3, ...)$ de corpos de funções sobre $\mathbb{F}_q$, um lugar, racional sobre $\mathbb{F}_q$, $P \in \mathbb{P}_{F_1}$, é dito totalmente decomposto na torre $\mathcal{F}$ se P é totalmente decomposto em todas as extensões F_n/F_1 para todo $n \geq 1$, isto é, se $[F_n : F_1] = m(n)$, então existem $m(n)$ lugares racionais em F_n acima de P. Defina $t := \#\{P : P$ é um lugar de grau 1 de $F_1/\mathbb{F}_q$ que é totalmente decomposto na torre $\mathcal{F}\}$. Então temos que $\upsilon(\mathcal{F}) \geq t$. Em particular, se $t > 0$, então $\upsilon(\mathcal{F}) > 0$.

Para a análise do gênero $\gamma(\mathcal{F})$ de uma torre $\mathcal{F} = (F_1, F_2, F_3, ...)$, nós usaremos a fórmula do gênero de Hurwitz para cada extensão F_n/F_{n-1} para $n \geq 2$, o que nos pede então uma descrição da diferente de cada extensão F_n/F_{n-1}, e portanto uma descrição do divisor de ramificação de cada extensão na torre.

1.3 Resultados auxiliares

Nesta seção reveremos brevemente e sem provas alguns conceitos e resultados que serão utilizados nos próximos capítulos. Estes resultados, em especial a Proposição 1.3.5 e o Teorema 1.3.6, são a inspiração do Teorema 1.4.1 da próxima seção que serve de base para o que chamaremos de processo de redução.

Para uma extensão algébrica E/F de corpos de funções sobre $\mathbb{F}_q$, o símbolo $e(Q|P)$ denotará o índice de ramificação, $d(Q|P)$ denotará o expoente da diferente de Q sobre P, onde P é um lugar de F ($P \in \mathbb{P}_F$) e Q é um lugar de E acima de P ($Q|P$), e $\mathrm{Diff}(E/F)$ denotará a diferente da extensão E/F.

Observação 1.3.1. Sejam E/F uma extensão algébrica de corpos de funções e $P \in \mathbb{P}_F$. Então para $Q \in \mathbb{P}_E$ temos

$$Q|P \iff v_Q(x) > 0,$$

onde $x \in F$ é uma função que tenha P como único zero e onde v_Q denota a valorização associada ao lugar Q.

Para extensões separáveis E/F, existe uma fórmula importante que nos dá o gênero de E em função da diferente da extensão E/F e do gênero de F.

Teorema 1.3.2. *(Fórmula do gênero de Hurwitz,* [15] Teo. III.4.12*) Seja $F/\mathbb{F}_q$ um corpo de funções algébricas de gênero g e E um corpo de funções de gênero g' tal que E/F é uma extensão finita e separável de F . Então nós temos*

$$2g' - 2 = [E : F](2g - 2) + grau\,(\mathrm{Diff}(E/F))\,.$$

Para nos ajudar no cálculo do grau da diferente nós temos os seguintes resultados, onde se destacam lugares que não se ramificam e lugares que são totalmente ramificados.

Teorema 1.3.3. *(Teorema da Diferente de Dedekind,* [15] Teo. III.5.1*) Com a notação acima, temos*

(a) $d(Q|P) \geq e(Q|P) - 1$.

(b) $d(Q|P) = e(Q|P) - 1$ *se e somente se* $e(Q|P)$ *não é divisível pela característica de* $\mathbb{F}_q$*, isto é,* $Q|P$ *é uma ramificação moderada.*

Em particular, se P não se ramifica em E/F, então $d(Q|P) = 0$.

Para uma torre $\mathcal{F} = (F_1, F_2, F_3, ...)$ de corpos de funções nós dizemos que um lugar $P \in F_1$ se ramifica na torre, se P se ramifica na extensão F_n/F_1 para algum $n \geq 1$. O conjunto $V(\mathcal{F}) := \{P \in F_1 : P \text{ se ramifica em } \mathcal{F}\}$ é chamado de *locus de ramificação de* $\mathcal{F}$. Para uma torre moderada, de acordo com o Teorema 1.3.3, os expoentes da diferente são conhecidos imediatamente a partir dos índices de ramificação. Neste caso, se temos $s = \#V(\mathcal{F}) < \infty$ e, além disso, existem pontos na torre que se decompõem totalmente, então a torre $\mathcal{F}$ é assintoticamente boa com limite $\lambda(\mathcal{F}) \geq \dfrac{2t}{2g(F_1) + s - 2}$, onde t é o número de lugares de grau 1 de F_1 que se decompõem totalmente na torre $\mathcal{F}$ (vide [6] Teo. 2.2.4).

Proposição 1.3.4. *(*[15] Prop.III.5.12*)Sejam E/F uma extensão finita e separável de corpos de funções , $P \in \mathbb{P}_F$ e $Q \in \mathbb{P}_E$ com $Q|P$, isto é Q acima de P. Suponha que $Q|P$ é totalmente ramificado. Seja $t \in E$ um parâmetro local em Q, e considere o polinômio minimal $\varphi(T) \in F[T]$ de t sobre F. Então $d(Q|P) = v_Q(\varphi'(t))$, onde φ' denota a derivada de φ.*

Determinar o comportamento de ramificação será portanto uma ferramenta essencial no cálculo da Diff(E/F). Em alguns casos, os coeficientes do polinômio minimal da função que gera a extensão E/F nos descrevem o comportamento de ramificação em alguns lugares de F, como é o caso da seguinte proposição:

Proposição 1.3.5. *(*[15] Prop.III.1.14 *) Seja $F/\mathbb{F}_q$ um corpo de funções e seja E/F uma extensão algébrica de $F/\mathbb{F}_q$ tal que $E = F(y)$ e o polinômio minimal de y sobre F é dado por*

$$\varphi(T) = T^n + a_{n-1}T^{n-1} + ... + a_1T + a_0$$

com $a_i \in F$. Seja P um lugar de $F/\mathbb{F}_q$ tal que $v_P(a_i) \geq 0$ para $i = 1, ..., n-1$, $v_P(a_0) < 0$ e $mdc(n, v_P(a_0)) = 1$. Então P tem uma única extensão $Q \in \mathbb{P}_E$ e o índice de ramificação é $e(Q|P) = n$, isto é, $Q|P$ é totalmente ramificada.

Ainda na tentativa de analisar o polinômio minimal para descrever ramificações, temos o Teorema de Kummer abaixo que será de grande importância. Este teorema nos dá a decomposição de um lugar P do corpo F numa extensão de corpos de funções $F(y)/F$, onde y está no fecho inteiro em F do anel de valorização $\mathcal{O}_P$ do lugar P, mediante a fatoração módulo P do polinômio minimal de y sobre F. Em particular, se o polinômio minimal de y sobre F for separável módulo P, o teorema nos diz que o lugar P é não ramificado na extensão $F(y)/F$.

Teorema 1.3.6. *(Teorema de Kummer,* [15] Teo. III.3.7*). Suponha que $E = F(y)$ é uma extensão de grau n, onde y é inteiro sobre $\mathcal{O}_P$, e considere o polinômio minimal $\varphi(T) \in \mathcal{O}_P[T]$ de y sobre F. Seja $\overline{F} = \mathcal{O}_P/P$ o corpo residual de F em P e seja*

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

a fatoração de $\overline{\varphi}(T)$ em fatores irredutíveis sobre o corpo $\overline{F}$ (i.e. os polinômios $\gamma_1(T)$,...,$\gamma_r(T)$ são irredutíveis, mônicos, dois a dois distintos em $\overline{F}[T]$ e ainda $\varepsilon_i \geq 1$). Escolha polinômios mônicos $\varphi_i(T) \in \mathcal{O}_P[T]$ com

$$\overline{\varphi}_i(T) = \gamma_i(T) \ \ e \ \ deg\varphi_i(T) = deg\gamma_i(T).$$

Então, para $1 \leq i \leq r$, existem lugares distintos $Q_1, ..., Q_r \in \mathbb{P}_E$ satisfazendo

$$Q_i|P \ \ e \ \ \varphi_i(y) \in Q_i \text{ para } i = 1, ..., r.$$

Mais ainda, suponha que a seguinte hipótese é satisfeita:

$$\varepsilon_i = 1 \quad para \quad i = 1, ..., r,$$

Então existe, para $1 \leq i \leq r$, exatamente um único lugar $Q_i \in \mathbb{P}_E$ acima de P satisfazendo $\varphi_i(y) \in Q_i$. Os lugares $Q_1, ..., Q_r$ são todos os lugares de E acima de P, e temos $e(Q_i|P) = \varepsilon_i$.

Na maioria das vezes o comportamento de ramificação num lugar será determinado a partir do comportamento de ramificação de restrições deste lugar para extensões intermediárias, tal como no Lema de Abhyankar (vide [15] Prop. III.8.9). Neste sentido temos a seguinte proposição :

Proposição 1.3.7. *Seja E/F uma extensão finita e separável de corpos de funções sobre um corpo finito de característica p. Assuma que E_1 e E_2 são corpos intermediários de E/F tais que $E = E_1 \cdot E_2$. Para um lugar $Q \in \mathbb{P}_E$, seja $Q_i \in \mathbb{P}_{E_i}$ a restrição de Q a $E_i (i = 1, 2)$, e seja $P \in \mathbb{P}_F$ a restrição de Q a F. Suponha que $e(Q_1|P)$ e $e(Q_2|P)$ sejam relativamente primos, então*

(i) $e(Q|P) = e(Q_1|P).e(Q_2|P)$.

(ii) Se Q_1/P for moderado, isto é, p não divide $e(Q_1|P)$, então

$$d(Q|Q_1) = e(Q_1|P)d(Q_2|P) - (e(Q_1|P) - 1)(e(Q_2|P) - 1).$$

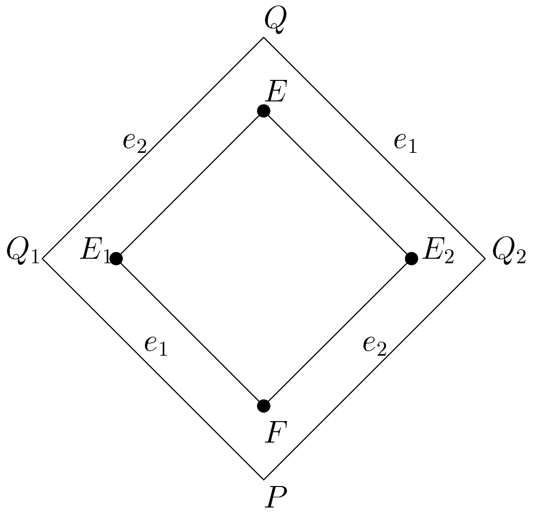

Figura 1.2: $mdc(e_1, e_2) = 1$

Demonstração: (i) Este é um caso especial do Lema de Abhyankar, veja [15] Prop. III.8.9.

(ii) Como as extensões $Q_1|P$ e $Q|Q_2$ são moderadas, nós temos pelo item anterior e pelo Teo. 1.3.3 que $d(Q_1|P) = d(Q|Q_2) = e(Q_1|P) - 1$. Usando a transitividade do expoente da diferente (conforme [15] Cor. III.4.11), nós obtemos

$$d(Q|P) = d(Q|Q_1) + e(Q_2|P) \cdot (e(Q_1|P) - 1)$$

e

$$d(Q|P) = e(Q_1|P) - 1 + e(Q_1|P) \cdot d(Q_2|P).$$

A afirmação segue então destas duas igualdades.

■

E como última observação em relação ao gênero, nós temos o seguinte teorema:

Teorema 1.3.8. *(*[15] Teo. III.6.3*) Seja $F/\mathbb{F}_q$ um corpo de funções e seja K uma extensão algébrica de $\mathbb{F}_q$. Em uma extensão algébrica por constantes $E = F \cdot K$ de $F/\mathbb{F}_q$, os seguintes itens são satisfeitos:*

(a) Os lugares de F não se ramificam na extensão E/F.

(b) E/K tem o mesmo genêro de $F/\mathbb{F}_q$.

Como corolário do item (a) do teorema anterior, temos que se existe um lugar P em $F/\mathbb{F}_q$ que é totalmente ramificado numa extensão algébrica de corpos E/F, então $\mathbb{F}_q$ é algebricamente fechado em E (conforme [15], Obs. III.7.5), e como corolário do item (b) temos que para calcular o gênero de uma torre definida sobre $\mathbb{F}_q$, podemos pensar na torre como definida sobre $\overline{\mathbb{F}}_q$, o fecho algébrico de $\mathbb{F}_q$.

1.4 Observações importantes

Consideremos uma extensão de corpos de funções E/F sobre $\mathbb{F}_q$ de grau q, onde q é uma potência de um primo, tal que $E = F(y)$ e o polinômio minimal da função y sobre F é dado por

$$\varphi(T) = T^q + aT + b, \text{ com } a, b \in F. \tag{1.1}$$

Neste caso, nós vamos dizer que a torre é do tipo especial $(*)$. As duas novas torres que serão apresentadas nos próximos dois capítulos são do tipo especial $(*)$. Note que, no caso em que $a \in \mathbb{F}_q$, a extensão E/F é uma extensão de Artin-Schreier generalizada. Vale lembrar que extensões de Artin-Schreier são extensões de Galois, e para extensões de corpos de funções E/F que são Galois, temos que para cada lugar $P \in \mathbb{P}_F$, o índice de ramificação $e(Q|P)$ independe do lugar $Q \in \mathbb{P}_E$ que está acima de P ([15] Cor. III.7.2).

Muitas vezes, a partir de extensões especiais do tipo $(*)$, nós vamos ter que mudar o gerador y destas extensões de modo que o novo gerador ainda tenha polinômio minimal do tipo (1.1) e tal que possamos usar algum dos Teoremas 1.3.4, 1.3.5 ou 1.3.6 com este polinômio (vide Lemas 2.2.3, 3.2.3 e 3.2.4). Por exemplo, para cada lugar $P \in \mathbb{P}(F)$, a função y acima que gera E pode ser tomada tal que a Equação (1.1) satisfaça $v_P(a) \geq 0$. Aplicando os Resultados 1.3.4, 1.3.5 e 1.3.6 da seção anterior para extensões do tipo especial $(*)$, nós conseguimos um resultado análogo à Proposição III.7.10 de [15], onde se faz uma análise a respeito de ramificações e diferente para extensões de Artin-Schreier:

Teorema 1.4.1. *Seja $E = F(y)$ uma extensão do corpo de funções $F/\mathbb{F}_q$ e seja $P \in \mathbb{P}_F$ um lugar tal que o polinômio minimal da função y sobre F é da forma $\varphi(T) = T^q + aT + b$, com $a, b \in F$, satisfazendo $v_P(a) \geq 0$. Para uma função $z \in F$ defina $\mathcal{P}(z) := z^q + az$. Suponha ainda que existe uma função $z \in F$ tal que*

$$v_P(b - \mathcal{P}(z)) \geq 0 \tag{1.2}$$

ou

$$v_P(b - \mathcal{P}(z)) = -m < 0, com\ mdc(m, q) = 1. \tag{1.3}$$

Defina $m_P = -1$ no caso (1.2) e $m_P = m$ no caso (1.3). Então m_P é um inteiro bem definido e valem as seguintes afirmações:

(i) Se $v_P(a) = 0$ e $m_P = -1$ então P não se ramifica na extensão E/F.

(ii) Se $m_P > 0$ então P é totalmente ramificado na extensão E/F.

(iii) Se $m_P = 1$ então o coeficiente da diferente de P na extensão E/F é igual a $d(P) = 2(q-1)$.

Demonstração: Nós provaremos inicialmente a boa definição do inteiro m_P. Assumamos que existe uma função $z \in F$ tal que $v_P(b - \mathcal{P}(z)) = -m < 0$, com $mdc(m, q) = 1$. Nós vamos mostrar que neste caso temos

$$-m = max\{v_P(b - \mathcal{P}(w)) : w \in F\}.$$

De fato, como $mdc(m, q) = 1$, para qualquer $w \in F$ temos que $q \cdot v_P(w - z) \neq -m$. Logo temos duas possibilidades:

Caso 1) $q \cdot v_P(w-z) > -m$. Então $v_P(\mathcal{P}(w-z)) = v_P((w-z)^q + a(w-z)) > -m$ e $v_P(b - \mathcal{P}(w)) = v_P(b - \mathcal{P}(z) - \mathcal{P}(w-z)) = -m$, pela desigualdade triangular.

Caso 2) $q \cdot v_P(w-z) < -m$. Então $v_P(b - \mathcal{P}(w)) = v_P(b - \mathcal{P}(z) - \mathcal{P}(w-z)) < -m$, pela desigualdade triangular novamente.

Em qualquer caso, temos $v_P(b - \mathcal{P}(w)) \leq -m$. Isto caracteriza o inteiro m_P.

Para a prova dos itens (i) e (ii) veja que para cada função $z \in F$ a função $\tilde{y} = y + z$ também é um elemento primitivo da extensão E/F e tem polinômio minimal sobre F dado por

$$\tilde{\varphi}(T) = T^q + aT + \tilde{b},$$

onde $\tilde{b} = b - \mathcal{P}(z)$.

Agora, se a função $z \in F$ nos dá $m_P = -1$, então o polinômio $\tilde{\varphi}(T)$ é separável módulo P quando $v_P(a) = 0$, e pelo Teorema 1.3.6 nós concluimos que

P é não-ramificado na extensão E/F. Por outro lado, se a função $z \in F$ nos dá $m_P > 0$, então a Proposição 1.3.5 nos permite concluir que P é totalmente ramificado na extensão E/F. Se ainda tivermos $m_P = 1$ (item (iii)), então para Q o único lugar de E acima de P, vale que

$$v_Q(\tilde{y}^q + a\tilde{y}) = v_Q(-\tilde{b}) = -q.$$

Logo, $v_Q(\tilde{y}) = -1$ e a função $\tilde{y}^{-1}$ é um parâmetro local em Q.

Da igualdade $\varphi(\tilde{y}) = 0$ nós temos que o polinômio minimal de $\tilde{y}^{-1}$ é dado por

$$\psi(T) = T^q + \frac{a}{\tilde{b}} \cdot T^{q-1} + \frac{1}{\tilde{b}}.$$

E assim, da Proposição 1.3.4 segue-se que

$$d(Q|P) = v_Q(\psi'(\tilde{y}^{-1})) = v_Q\left(\frac{a}{\tilde{b}} \cdot \tilde{y}^{-(q-2)}\right) = -v_Q(\tilde{b}) + q - 2 = 2(q-1).$$

■

O teorema acima descreve o resultado de um processso no qual a partir da Equação (1.1) com $v_P(a) \geq 0$, nós conseguimos um novo gerador $\tilde{y}$ para a extensão E/F a partir da existência da função $z \in F$ satisfazendo $v_P(b - \mathcal{P}(z)) = -m < 0$, com $mdc(m, q) = 1$, ou $v_P(b - \mathcal{P}(z)) \geq 0$. Assim o polinômio minimal de $\tilde{y} = y + z$ é da forma:

$$\varphi(T) = T^q + aT + b, \tag{1.4}$$

onde $a, b \in F$ são tais que $v_P(a) \geq 0$ e $v_P(b) = -m < 0$ com $mdc(m, q) = 1$, ou $v_P(a) \geq 0$ e $v_P(b) \geq 0$. Com Equações do tipo (1.4), nós conseguimos achar o índice de ramificação de P na extensão E/F nos seguintes casos: Caso (i) $v_P(a) = 0$ e $v_P(b) \geq 0$ ($m_P = -1$), ou no Caso (ii) $v_P(a) \geq 0$ e $v_P(b) < 0$ ($m_P > 0$), conforme a Prop. 1.3.5 e ao Teo. 1.3.6. O processo de achar este elemento z e chegar a equações que nos dão informações sobre a ramificação de P na extensão E/F, será chamado, aqui, de *Processo de Redução.*

Observação 1.4.2. Nos capítulos que seguem estaremos interessados em calcular o limite de duas torres da forma $\mathcal{F} = (F_1, F_2, F_3, ...)$ onde cada passo F_{i+1}/F_i é gerado por uma função y_i com polinômio minimal sobre F_i do tipo (1.1), isto é, $\varphi(T) = T^q + a_iT + b_i$, onde $a_i \in F_i$ e $b_i \in \{a_i, -a_i\}$. O principal problema em achar estes limites está no calculo dos gêneros $g(F_i)$. Para determinar estes gêneros utilizaremos a fórmula de Riemann-Hurwitz e, assim sendo, temos que achar a diferente das extensões F_{i+1}/F_i, e portanto o divisor de ramificação destas extensões. Do teorema anterior, segue que podemos nos restringir aos lugares que são zeros ou pólos da função a_i.

Para o processo de redução, a determinação de um parâmetro local em P se torna muito importante. Nós desenvolveremos funções como séries de potências num parâmetro local de um dado ponto e no processo de redução nós estaremos interessados somente na parte polar destas funções e iremos ignorar a parte regular da expansão em série de potências. Neste contexto, uma notação bastante utilizada será a seguinte: para funções $x, y \in F$, um lugar $P \in \mathbb{P}_F$ e um inteiro n nós vamos escrever

$$x = y + \mathcal{O}(n) \text{ em } P \qquad \text{se } v_P(x - y) \geq n.$$

Para finalizar esta seção, para uma torre $\mathcal{F} = (\mathbb{F}_q(x_1), \mathbb{F}_q(x_1, x_2), ...)$ definida recursivamente por uma equação (vide Def. 1.2.8), com a Prop. 1.3.7 nós podemos estudar o comportamento de ramificação de um lugar P do corpo de funções $F_n = \mathbb{F}_q(x_1, ..., x_n)$ na extensão F_n/F_{n-1} através do uso de pirâmides. Para um lugar P de F_n, uma pirâmide representa graficamente as ramificações das restrições de P em cada extensão da forma $\mathbb{F}_q(x_i, ..., x_{i+k})/\mathbb{F}_q(x_i, ..., x_{i+k-1})$ ou da forma $\mathbb{F}_q(x_i, ..., x_{i+k})/\mathbb{F}_q(x_{i+1}, ..., x_{i+k})$ para $1 \leq i \leq n-1$ e $1 \leq k \leq n-i$.

As arestas na pirâmide representam extensões de corpos. Cada vértice representa um corpo de funções. Os vértices na base da pirâmide representam os corpos de funções racionais $\mathbb{F}_q(x_1), \mathbb{F}_q(x_2), ..., \mathbb{F}_q(x_n)$. Os outros vértices da pirâmide representam os compósitos dos vértices que estão diretamente ligados a este por uma aresta e estão imediatamente abaixo. Nestas pirâmides os números sobre as arestas representam os índices de ramificação nas extensões de corpos correspondentes as várias restrições do lugar em questão, e muitas destas ramificações são determinadas pela Prop. 1.3.7.

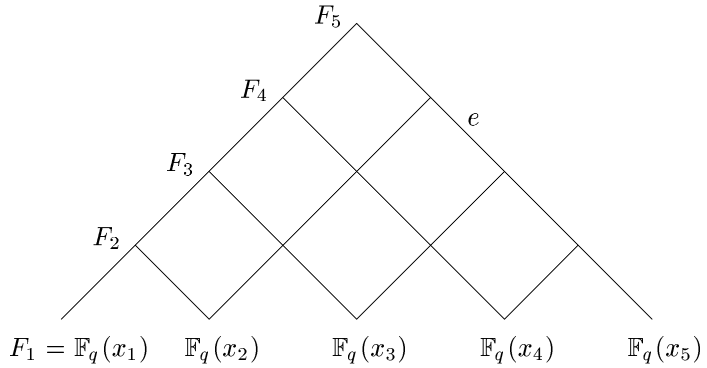

Figura 1.3: pirâmide para um lugar $P \in F_5$

A figura acima é um exemplo de uma pirâmide para um lugar $P \in F_5$. Nela o número e representa o índice de ramificação da restrição de P na extensão $\mathbb{F}_q(x_2, x_3, x_4, x_5)/\mathbb{F}_q(x_3, x_4, x_5)$.

Capítulo 2

Torre otimal não-Galois

Neste capítulo nós apresentaremos uma nova torre otimal de corpos de funções sobre o corpo finito de cardinalidade quadrada $\mathbb{F}_{q^2}$ para qualquer q potência de um primo. Esta torre, dada explicitamente e definida recursivamente por uma equação onde cada lado da igualdade é não polinomial, tem passos não-Galois quando $q \neq 2$, isto é, ela é construída com extensões não-Galois de corpos de funções.

2.1 A equação e a torre

Consideremos a equação

$$\frac{y-1}{y^q} = \frac{x^q-1}{x}. \tag{2.1}$$

Através deste capítulo K denotará o corpo finito $\mathbb{F}_{q^2}$ com q^2 elementos, k denotará o fecho algébrico de K e $\mathcal{F}$ denotará a torre $(F_1, F_2, F_3, ...)$ de corpos de funções sobre K, definida recursivamente pela Equação (2.1), isto é,

Definição 2.1.1. *Seja $F_1 := K(x_1)$ o corpo de funções racionais sobre K, isto é, a função x_1 é transcendente sobre K. Para $i \geq 1$, definimos*

$$F_{i+1} := F_i(x_{i+1}),$$

onde a função x_{i+1} satisfaz a equação abaixo:

$$\frac{x_{i+1}-1}{x_{i+1}^q} = \frac{x_i^q-1}{x_i}.$$

O principal resultado deste capítulo é o teorema seguinte, cuja demonstração será feita no final deste capítulo 2.

Teorema 2.1.2. *A torre $\mathcal{F}$ atinge a cota de Drinfeld-Vladut sobre K, isto é,*

$$\lambda(\mathcal{F}) = q - 1.$$

Observação 2.1.3. A torre $\mathcal{F}$ definida acima é uma subtorre da torre otimal $\mathcal{T}$; veja o item (5) da lista de torres assintoticamente boas na seção 1.2.3 do capítulo 1. De fato, se $T_1 = K(y_1)$ é o corpo de funções racionais e, para cada $n \geq 1$ temos $T_{n+1} = T_n(y_{n+1})$ com $y_{n+1}^q + y_{n+1} = y_n^q/(y_n^{q-1} + 1)$, tomando $x_n := 1/(1 + y_n^{q-1})$, $\forall n \in \mathbb{N}$, nós temos que $x_n \in T_n$ satisfaz a equação

$$\frac{x_{n+1} - 1}{x_{n+1}^q} = \frac{x_n^q - 1}{x_n}.$$

E portanto, pela Observação 1.2.10, isto dá uma prova de que $\lambda(\mathcal{F}) = q - 1$.

Aqui nós apresentaremos um método mais simples para o cálculo deste limite que nos leva ao cálculo exato do gênero em cada passo F_n da torre $\mathcal{F}$. Para o cálculo deste limite nós necessitamos de alguns lemas e para começar vamos enumerar algumas propriedades das extensões básicas na torre, que correspondem a base da pirâmide no estudo de ramificações.

Lema 2.1.4. *Seja $F = K(x, y)$ o corpo de funções definido pela Equacão (2.1). Então as seguintes afirmações são satisfeitas:*

1) $[F : K(x)] = [F : K(y)] = q$.

2) A função x tem um único zero P_0 em F e este lugar é totalmente ramificado na extensão $F/K(x)$ e não-ramificado na extensão $F/K(y)$.

3) A função x tem um único pólo P_∞ em F e este lugar é totalmente ramificado em $F/K(x)$ e tem índice de ramificação $q - 1$ na extensão $F/K(y)$.

4) A função $x - 1$ tem exatamente dois zeros em F a saber, o lugar Q_1 zero comum de $x - 1$ e $y - 1$ que é não-ramificado em $F/K(x)$, e o lugar Q_∞ zero comum de $x - 1$ e y^{-1} que tem índice de ramificação $q - 1$ em $F/K(x)$. Ambos estes lugares são totalmente ramificados em $F/K(y)$.

5) Os divisores principais em F das funções x, $x - 1$, y e $y - 1$ são como segue-se:

$$\begin{aligned}
(x) &= qP_0 - qP_\infty \\
(x - 1) &= Q_1 + (q - 1)Q_\infty - qP_\infty \\
(y) &= P_0 + (q - 1)P_\infty - qQ_\infty \\
(y - 1) &= qQ_1 - qQ_\infty.
\end{aligned}$$

6) Os lugares de F que são ramificados sobre $K(x)$ são exatamente os lugares P_0, P_∞ e Q_∞. Seus expoentes da diferente com respeito a extensão $F/K(x)$ são $d(P_0) = q$, $d(P_\infty) = 2(q - 1)$ e $d(Q_\infty) = q - 2$, respectivamente.

Vale notar que, como consequência do item (4) do lema, temos que $F/K(x)$ não é Galois para $q \neq 2$. Para $q = 2$, a substituição $x_i \to 1/(x_i + 1)$, para todo $i \geq 1$, transforma a equação $(x_{i+1} - 1)/x_{i+1}^2 = (x_i^2 - 1)/x_i$ na equação $x_{i+1}^2 + x_{i+1} = x_i^2/(x_i + 1)$, e esta é a torre de Artin-Schreier, e portanto com passos Galois, assintoticamente otimal sobre $\mathbb{F}_4$ em [4]. Além disso, da fórmula do gênero de Hurwitz (Teorema 1.3.2) e do item (6) do lema nós temos

$$\begin{aligned} g(F_2) &= q \cdot g(F_1) + 1 - q + \frac{1}{2} deg Diff(F_2/F_1) \\ &= 0 + 1 - q + \frac{1}{2}(q + 2(q-1) + q - 2) = q - 1 > 1 \end{aligned}$$

se $q \neq 2$. Assim, a seqüência $\mathcal{F}$ definida recursivamente pela Equação (2.1) satisfaz a condição (ii) da definição de torre dada na seção 1.2.3.

Demonstração(Lema 2.1.4): 1) Desde que a Equação (2.1) tem grau q nas variáveis x e y, é claro que $[F : K(x)] \leq q$ e $[F : K(y)] \leq q$. Seja P um lugar em F acima do único zero de x em $K(x)$. Da Equação (2.1) temos

$$v_P\left(\frac{y^q}{y-1}\right) = v_P\left(\frac{x}{x^q - 1}\right) > 0.$$

Logo, pela Observação 1.3.1, o lugar P está acima do único zero de y em $K(y)$ e assim temos

$$q v_P(y) = v_P(x) \Rightarrow v_P(x) = q \quad \text{e} \quad v_P(y) = 1.$$

Daí $e(P|P \cap K(x)) = q$ e $e(P|P \cap K(y)) = 1$, e temos

$i)$ $[F : K(x)] = q$.

$ii)$ O lugar P é totalmente ramificado na extensão $F/K(x)$ e portanto existe um único lugar P_0 em F acima do único zero da função x em $K(x)$.

$iii)$ a função y é um parâmetro local em P_0.

Analogamente, considerando-se o lugar Q acima do único pólo de y em $K(y)$, concluimos que $[F : K(y)] = q$.

Veja que aqui temos demonstrado também o item 2).

3) Seja P' um lugar em F acima do único pólo de x em $K(x)$. Da Equação (2.1) temos

$$v_{P'}\left(\frac{y^q}{y-1}\right) = v_{P'}\left(\frac{x}{x^q - 1}\right) = (q-1) v_{P'}\left(\frac{1}{x}\right) > 0.$$

Logo, pela Observação 1.3.1, o lugar P' está acima do único zero de y em $K(y)$, e assim temos

$$q v_{P'}(y) = (q-1) v_{P'}\left(\frac{1}{x}\right) \Rightarrow v_{P'}\left(\frac{1}{x}\right) = q \quad \text{e} \quad v_{P'}(y) = q - 1.$$

Daí $e(P'|P' \cap K(x)) = q$ e $e(P'|P' \cap K(y)) = q - 1$, e temos *i)* O lugar P' é totalmente ramificado na extensão $F/K(x)$ e portanto existe um único lugar P_∞ em F acima do único pólo da função x em $K(x)$.

ii) a função $t = (xy)^{-1}$ é um parâmetro local em P_∞.

4) Seja Q um lugar em F acima do único zero da função $x-1$ em $K(x)$. Da Equação (2.1) nós temos que os coeficientes do polinômio minimal do elemento primitivo de F, y^{-1}, sobre $K(x)$, dado por

$$\varphi(T) = T^q - T^{q-1} + \frac{x^q - 1}{x},$$

são inteiros sobre $\mathcal{O}_1$, o anel de valorização de $Q \cap K(x)$ em $K(x)$. Logo, pelo Teorema 1.3.6, a fatoração de $\overline{\varphi}(T) = \varphi(T)\ mod(Q \cap K(x))$, nos dá dois lugares em F acima de $Q \cap K(x)$, Q_1 e Q_∞, satisfazendo $y(Q_1) = 1$ e $y(Q_\infty) = \infty$. Além disso, da Equação (2.1) temos

$$v_{Q_\infty}\left(\frac{y-1}{y^q}\right) = v_{Q_\infty}\left(\frac{x^q-1}{x}\right) \Rightarrow (q-1)\cdot v_{Q_\infty}(y^{-1}) = q \cdot v_{Q_\infty}(x-1),$$

isto é, $v_{Q_\infty}(x-1) = q-1$ e $v_{Q_\infty}(y) = -q$. Daí temos $e(Q_\infty|Q_\infty \cap K(x)) = q-1$ e $e(Q_\infty|Q_\infty \cap K(y)) = q$. E portanto, da igualdade fundamental, nós temos que $e(Q_1|Q_1 \cap K(x)) = 1$ e estes dois lugares são os únicos zeros de $x-1$ em F. Além disso, usando a Equação (2.1) novamente segue-se que

$$v_{Q_1}\left(\frac{y-1}{y^q}\right) = v_{Q_1}\left(\frac{x^q-1}{x}\right) \Rightarrow v_{Q_1}(y-1) = q \cdot v_{Q_1}(x-1),$$

isto é, $v_{Q_1}(y-1) = q$ e portanto $e(Q_1|Q_1 \cap K(y)) = q$.

5) É consequência imediata dos itens 2), 3) e 4) e da demonstração destes itens.

6) A extensão $F/K(x)$ tem como um de seus elementos primitivos a função y cujo polinômio minimal sobre $K(x)$ é dado por

$$\varphi(T) = T^q - \frac{x}{x^q-1}T + \frac{x}{x^q-1}.$$

Do Teorema 1.3.6, as possíveis ramificações de $F/K(x)$ são os zeros e pólos da função $x(x-1)$. De fato, basta ver que o polinômio $\varphi(T)$ é separável módulo qualquer lugar que não seja nem zero e nem pólo da função $x(x-1)$.

Agora, na demonstração do item 1) nós vimos que $y \in F$ é um parâmetro local em P_0. Logo, $d(P_0) = v_{P_0}(\varphi'(y)) = v_{P_0}(x) = q$ (vide Prop.1.3.4). Analogamente, usando o parâmetro local $t = 1/xy$ em P_∞ podemos concluir que $d(P_\infty) = 2(q-1)$. De fato, da Equação (2.1) nós temos que

$$\frac{1}{y^q} - \frac{1}{y^{q-1}} - \frac{x^q-1}{x} = 0.$$

Multiplicando esta equação por $1/x^q$, nós temos que o polinômio minimal do elemento t sobre $K(x)$ é igual à

$$\varphi(T) = T^q - \frac{1}{x}T^{q-1} + \frac{x^q - 1}{x^{q+1}}.$$

Assim, $d(P_\infty) = v_{P_\infty}(\varphi'(t)) = v_{P_\infty}(1/x \cdot t^{q-2}) = q + q - 2 = 2(q-1)$. Finalmente, a afirmação $d(Q_\infty) = q - 2$ segue diretamente de Q_∞ ter ramificação moderada na extensão $F/K(x)$, com $e(Q_\infty) = q - 1$ (vide Teorema 1.3.3).

■

Na próxima seção nós vamos estudar as ramificações de um passo geral da torre $\mathcal{F}$, isto é, nas extensões F_n/F_{n-1}.

2.2 Comportamento de ramificação

Considerando a torre $\mathcal{F}$ definida pela Equação (2.1), nós temos que cada passo F_n da torre é gerado sobre F_{n-1} pela função x_n com polinômio minimal igual à

$$\varphi(T) = T^q - \frac{x_{n-1}}{x_{n-1}^q - 1}T + \frac{x_{n-1}}{x_{n-1}^q - 1}.$$

Logo, pela Observação 1.4.2, os possíveis lugares de F_n que se ramificam sobre F_{n-1} são os zeros e pólos da função $x_{n-1}/\left(x_{n-1}^q - 1\right)$. Do Item (5) do Lema 2.1.4, segue que para $n \geq 2$ e $Q \in \mathbb{P}_{F_n}$ nós temos

(1) Se $x_j(Q) = 0$ ou $x_j(Q) = \infty$ então $x_{j+1}(Q) = 0$.

(2) Se $x_j(Q) = 1$ então $x_{j+1}(Q) = 1$ ou $x_{j+1}(Q) = \infty$.

(3) Se $x_j(Q) = 0$ então $x_{j-1}(Q) = 0$ ou $x_{j-1}(Q) = \infty$.

(4) Se $x_j(Q) = 1$ ou $x_j(Q) = \infty$ então $x_{j-1}(Q) = 1$.

E assim, se $Q \in \mathbb{P}_{F_n}$ é um lugar que se ramifica na extensão F_n/F_{n-1}, então nós temos as seguintes possibilidades para este lugar:

(A) O lugar Q é zero ou pólo da função x_1 e portanto Q é um zero comum de x_i para $i = 2, ..., n$.

(B) O lugar Q é zero da função $x_n - 1$ e portanto Q é zero comum de $x_i - 1$ para $i = 1, ..., n$.

(C) Existe um inteiro $1 \leq t < n$ tal que

i) Q é zero comum de $x_1 - 1, ..., x_t - 1$;

ii) Q é pólo de x_{t+1};

iii) Q é zero de x_i para $i = t + 2, ..., n$.

Note que no Caso (C) a condição (ii) implica nas outras duas condições (i) e (iii).

O comportamento de ramificação para estas três possibilidades são bastante diferentes. Nos dois primeiros casos ele será determinado facilmente do estudo de pirâmides. Isto, juntamente com a determinação do expoente da diferente, é feito usando a Proposição 1.3.7 no seguinte lema:

Lema 2.2.1. *1)* $[F_n : K(x_i)] = q^{n-1}$ *para cada* $i = 1, ..., n$.

2) Existe um único lugar $P \in \mathbb{P}_{F_n}$ *que é zero da função* x_1. *Este lugar* P *é totalmente ramificado na extensão* F_n/F_1 *e é não-ramificado em* $F_n/K(x_n)$. *Além disso, O expoente da diferente* $d(P)$ *de* P *com respeito a extensão* F_n/F_{n-1} *é dado por* $d(P) = q$.

3) Existe um único lugar $P' \in \mathbb{P}_{F_n}$ *que é pólo da função* x_1. *Este lugar* P' *é totalmente ramificado na extensão* F_n/F_1 *e tem índice de ramificação dado por* $e(P' \mid P' \cap K(x_n)) = q - 1$ *na extensão* $F_n/K(x_n)$. *Além disso,* $d(P') = 2(q-1)$, *onde* $d(P')$ *é o expoente da diferente em* F_n/F_{n-1}.

4) Seja $Q \in \mathbb{P}_{F_n}$ *um zero de* $x_n - 1$. *O lugar* Q *é não-ramificado na extensão* F_n/F_1 *e totalmente ramificado na extensão* $F_n/K(x_n)$.

5) Seja $R \in \mathbb{P}_{F_n}$ *um lugar que não é zero e nem pólo da função* $x_1(x_1 - 1)$. *Então o lugar* R *é não-ramificado em* F_n/F_1.

Demonstração : 1) Como a Equação (2.1) tem grau q, nós temos que $[F_{i+1} : F_i] \leq q$ para cada $i \geq 1$, isto é, $[F_n : F_1] \leq q^{n-1}$. Para um lugar $P \in \mathbb{P}_{F_n}$ que é zero de x_1, isto é, um lugar do tipo (A) com $x_1(P) = 0$, a restrição de P é ramificada em F_2/F_1, com índice de ramificação q, e esta restrição é um zero simples de x_2 em F_2 (pelo Lema 2.1.4, item (5)). Além disso a função x_2 tem um único zero em $K(x_2, x_3)$ e este lugar é zero simples de x_3, assim não ramificado em $K(x_2, x_3)/K(x_3)$ (pelo Lema 2.1.4, item (5), novamente). Repetindo este argumento vemos que P é zero comum de $x_2, x_3, ..., x_n$ e que os índices de ramificação das restrições de P nas extensões $K(x_i, x_{i+1})$ sobre $K(x_i)$, respectivamente $K(x_{i+1})$, são iguais a q e 1 (vide Figura 2.1 na próxima página).

Seja então, P um lugar em F_n que é zero da função x_1. As seguintes afirmações seguem agora facilmente por indução sobre $n \geq 2$, usando o item (i) da Proposição 1.3.7:

(a) O índice de ramificação de P com respeito a extensão F_n/F_1 é q^{n-1}.

(b) $[F_n : K(x_i)] = q^{n-1}$ para $i = 1, ..., n$.

(c) P é não-ramificado sobre $K(x_n)$.

(d) O expoente da diferente de P na extensão F_n/F_{n-1} é $d(P) = q$.

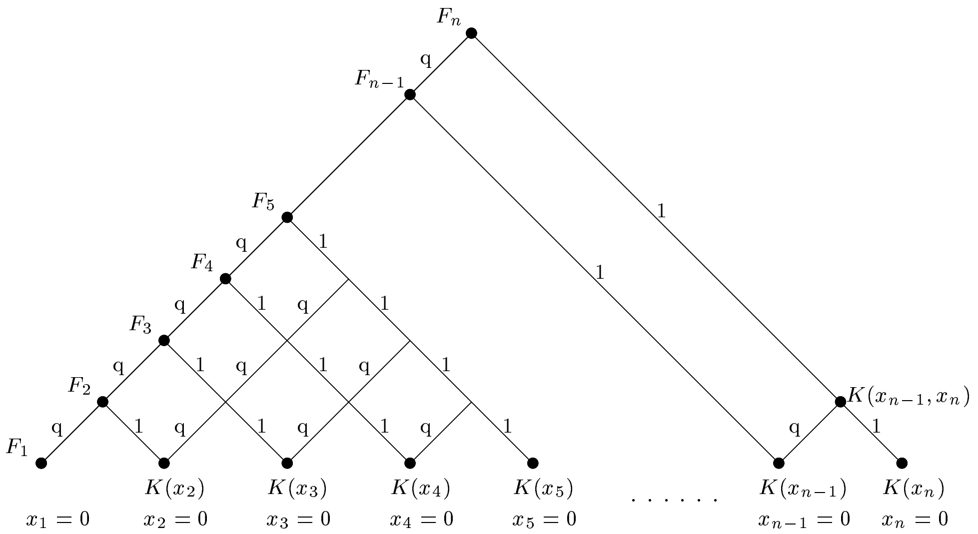

Figura 2.1: Tipo (A) com $x_1 = 0$

De fato, para $n = 2$, as afirmações já foram provadas no Lema 2.1.4. Assim nós assumimos que $n \geq 3$. Seja P_1 a restrição de P a F_{n-1}, P_2 a restrição de P a $K(x_{n-1}, x_n)$ e $\tilde{P}$ a restrição de P a $K(x_{n-1})$. Observando que o lugar P_1 é também um zero de x_1, pela hipótese de indução nós temos que $e(P_1|\tilde{P}) = 1$ e pelo Lema 2.1.4 temos que $e(P_2|\tilde{P}) = q$ e $d(P_2|\tilde{P}) = q$. Segue então da Proposição 1.3.7 que $e(P|P_1) = q$ e $d(P|P_1) = q$. Assim, $[F_n : F_{n-1}] = q$ e o lugar P é totalmente ramificado na extensão F_n/F_{n-1}. Pela hipótese de indução, novamente temos que $[F_n : K(x_i)] = q^{n-1}$ e portanto o lugar P é totalmente ramificado em F_n/F_1. O que nos leva a concluir que existe um único lugar do tipo (A) em F_n. Portanto provamos os itens (1) e (2).

3) De maneira análoga provaremos o item (3): Seja P' um lugar em $\mathbb{P}_{F_n}$ que é pólo de x_1, isto é, P' é um lugar do tipo (A) com $x_1(P) = \infty$. Então a restrição de P' é ramificada em F_2/F_1 com índice de ramificação q, e esta restrição é um zero de x_2 em F_2 com multiplicidade $q-1$ (pelo Lema 2.1.4, itens (3) e (5)). A função x_2 tem um único zero em $K(x_2, x_3)$ e este lugar é zero simples de x_3, assim não ramificado em $K(x_2, x_3)/K(x_3)$ (pelo Lema 2.1.4, itens (2) e (5)). Repetindo este argumento vemos que P' é zero comum de $x_2, x_3, ..., x_n$ e que os índices de ramificação das restrições de P' nas extensões $K(x_i, x_{i+1})$ sobre $K(x_i)$, respectivamente $K(x_{i+1})$, são iguais a q e $q-1$ se $i = 1$, e são iguais a q e 1 se $i > 1$ (como na Figura 2.2).

Assim, da Proposição 1.3.7, segue por indução sobre n que:

(a') O índice de ramificação de P' na extensão F_n/F_1 é q^{n-1}.

(b') P' se ramifica sobre $K(x_n)$ com índice de ramificação $q-1$.

(c') O expoente da diferente de P' na extensão F_n/F_{n-1} é $d(P') = 2(q-1)$.

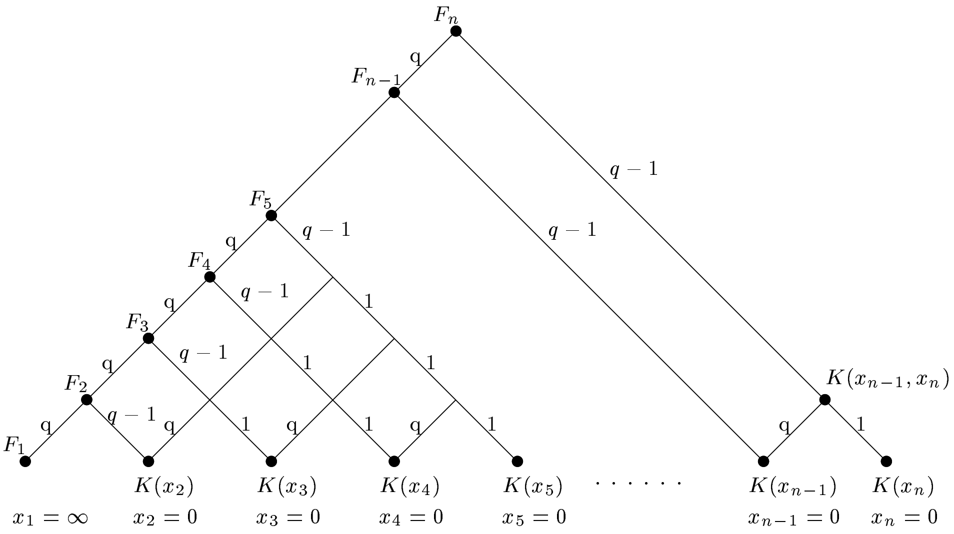

Figura 2.2: Tipo (A) com $x_1 = \infty$

Vejamos, por exemplo, como determinamos o expoente da diferente de P' na extensão F_n/F_{n-1}: Para $n = 2$, isto já foi obtido no Lema 2.1.4, item (6); assim nós assumimos que $n \geq 3$. Seja P_1' a restrição de P' a F_{n-1} e P_2' a restrição de P' a $K(x_{n-1}, x_n)$. Pelo Lema 2.1.4, item (6), o expoente da diferente de P_2' em $K(x_{n-1}, x_n)/K(x_{n-1})$ é $d(P_2') = q$, e segue agora da Proposição 1.3.7 que o expoente da diferente de P' sobre P_1' é igual a $2(q-1) = (q-1)q - (q-2)(q-1)$. Isto termina a prova do item (3).

4) Para um lugar $Q \in \mathbb{P}_{F_n}$ que é zero de $x_n - 1$, isto é, Q é um lugar do tipo (B), a restrição de Q é totalmente ramificada em $K(x_{n-1}, x_n)/K(x_n)$, e esta restrição é um zero simples de $x_{n-1} - 1$ em $K(x_{n-1}, x_n)$ (pelo Lema 2.1.4, item (5)). Além disso a função $x_{n-1} - 1$ tem um único zero em $K(x_{n-2}, x_{n-1})$ e este lugar é zero simples de $x_{n-2} - 1$, assim não ramificado em $K(x_{n-2}, x_{n-1})/K(x_{n-2})$ (pelo Lema 2.1.4, item (5), novamente). Repetindo este argumento vemos que Q é zero comum de $x_1 - 1, x_2 - 1, ..., x_n - 1$ e que os índices de ramificação das restrições de Q nas extensões $K(x_{i-1}, x_i)$ sobre $K(x_{i-1})$, respectivamente $K(x_i)$, são iguais a 1 e q.

Seja então Q um lugar de F_n que é zero de $x_n - 1$; segue por indução sobre $n \geq 2$ que:

(a'') O lugar Q é não-ramificado na extensão F_n/F_1.

(b'') O lugar Q é totalmente ramificado na extensão $F_n/K(x_n)$.

De fato, para $n = 2$, as afirmações acima já foram obtidos no Lema 2.1.4, item (5). Para $n \geq 2$ basta observar que a restrição de Q a F_{n-1}, denotada por Q_1, também é um zero de $x_{n-1} - 1$. Logo, satisfaz $e(Q_1|Q_1 \cap K(x_{n-1})) = q^{n-2}$ e $e(Q_1|Q_1 \cap F_1) = 1$. Assim, pela Proposição 1.3.7 temos $e(Q|Q \cap K(x_{n-1}, x_n)) =$

q^{n-2} e $e(Q|Q_1) = 1$. Seguem então as afirmações da transitividade dos índices de ramificação.

5) Consideremos agora um lugar $R \in \mathbb{P}_{F_n}$ que não é zero e nem pólo da função $x_1(x_1 - 1)$. Segue do Lema 2.1.4, item (5), por indução, que R não é zero e nem pólo das funções $x_i(x_i - 1)$ para $i = 1, ..., n$. Agora, o Lema 2.1.4, item (6), mostra que as restrições de R são não-ramificadas em todas as extensões $K(x_i, x_{i+1})/K(x_i)$, assim R é não-ramificado em $F_n/K(x_1)$.

■

Como consequência do item (2) do lema anterior, nós temos que a sequência (F_n) é de fato uma torre de corpos de funções sobre o corpo $K = \mathbb{F}_{q^2}$ (vide comentário após o Teorema 1.3.8).

Nosso objetivo é calcular o grau da diferente $\mathrm{Diff}(F_n/F_{n-1})$ para $n \geq 2$. Resta então, investigar os lugares Q do tipo (C), isto é, lugares $Q \in F_n$ que são pólos da função x_{t+1} para algum $1 \leq t < n$. Se $t = n - 1$, então a restrição de Q a F_{n-1} é um zero da função $x_{n-1} - 1$, logo é totalmente ramificada na extensão $F_{n-1}/K(x_{n-1})$ conforme o Item (4) do Lema 2.2.1. Além disso, a restrição de Q a $K(x_{n-1}, x_n)$ tem índice de ramificação $q - 1$ na extensão $K(x_{n-1}, x_n)/K(x_{n-1})$. Segue então da Proposição 1.3.7 que o lugar Q tem índice de ramificação $q - 1$ na extensão F_n/F_{n-1}, e consequentemente tem coeficiente da diferente igual a $d(Q) = q - 2$ (vide Figura 2.3).

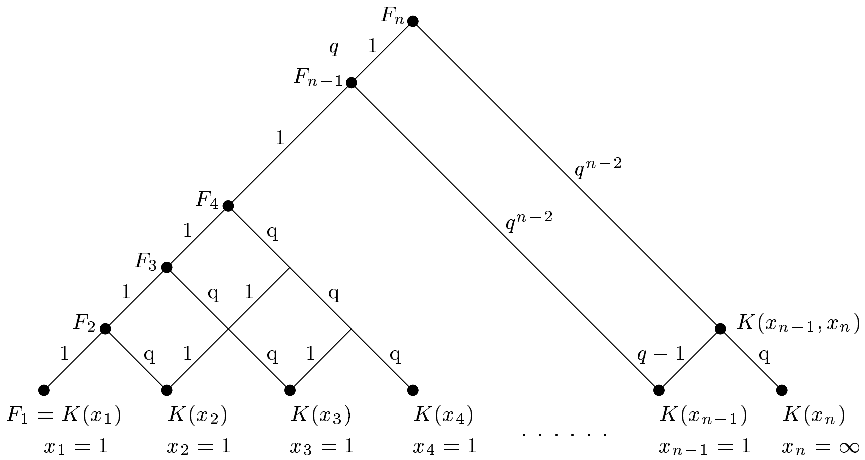

Figura 2.3: $x_n = \infty$

Suponhamos agora $1 \leq t < n - 1$. Neste caso, os índices de ramificação para as restrições de Q em $K(x_i, x_{i+1})/K(x_i)$ (respectivamente sobre $K(x_{i+1})$) para $t \leq i \leq t + 1$ são como na Figura 2.4 abaixo, conforme segue do Lema 2.1.4. Dessa figura nós não podemos deduzir os índices de ramificação de Q na extensão $F_n/K(x_j)$ para cada j. Por exemplo, qual é o índice de ramificação da restrição de Q em $K(x_t, x_{t+1}, x_{t+2})/K(x_t, x_{t+1})$? O próximo teorema nos permitirá achar este índice.

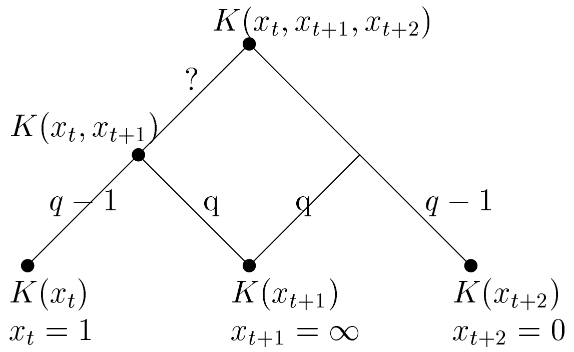

Figura 2.4: $1 < t < n-1$

Teorema 2.2.2. *Para $1 \leq k \leq t$ seja $H_k := K(x_{t+1-k}, ..., x_{t+k})$ e seja $E_k := H_k(x_{t+1+k})$. Suponha que $Q_k \in \mathbb{P}(E_k)$ é um pólo de x_{t+1}. Então o lugar Q_k é não-ramificado na extensão E_k/H_k.*

Para $k = 1$ nós temos que $H_1 = K(x_t, x_{t+1})$ e $E_1 = H_1(x_{t+2})$, e o Teorema 2.2.2 nos dá a resposta para a questão acima, isto é, podemos substituir o sinal de interrogação na Figura 2.4 por 1.

O 1 circulado na Figura 2.5 da próxima página é o objetivo do próximo lema, que é o resultado chave deste capítulo, o que nos abrirá as portas para o teorema principal. Os outros índices de ramificação da figura são obtidos no diagrama usando a Proposição 1.3.7 e o Lema 2.1.4.

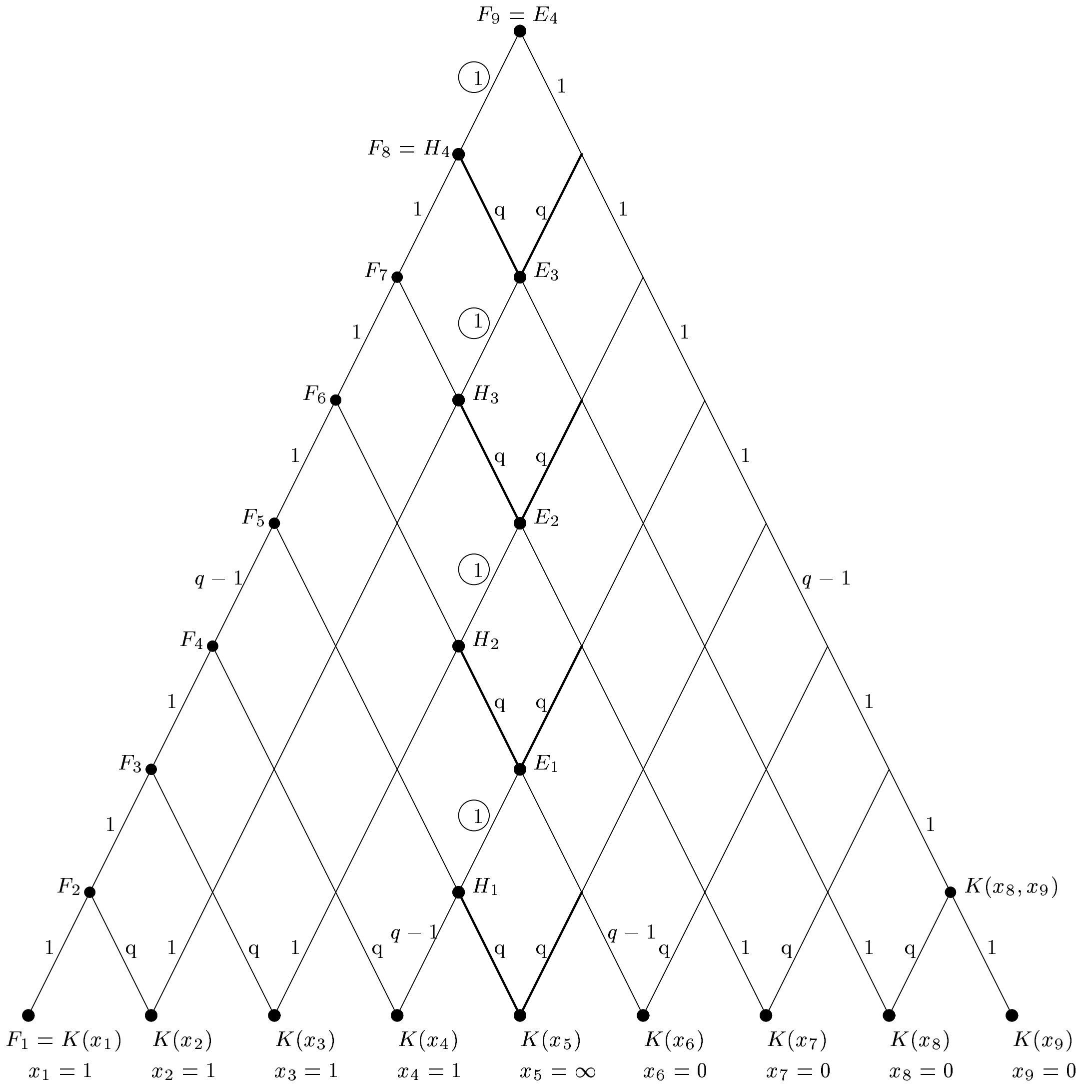

Figura 2.5: $t = 4$ e $n = 9$

Vamos fixar notação. Fixe k inteiro positivo e defina

$$X_i := \begin{cases} x_{i+t+1} - 1 & \text{para } i < 0 \\ x_{t+1}^{-1} & \text{para } i = 0 \\ -x_{i+t+1} & \text{para } i > 0; \end{cases}$$

$Y_k := \prod_{i=-k}^{-1} X_i;$

$Z_k := \prod_{i=1}^{k} X_i.$

Denotamos por $Q_0 \in \mathbb{P}_{E_0}$ com $E_0 := K(x_{t+1})$ o único pólo de x_{t+1}.

Note que o item (3) do lema abaixo prova o Teorema 2.2.2.

Lema 2.2.3. *Para um lugar Q_k como no Teorema 2.2.2 temos as seguintes afirmações :*

1)

$$v_{Q_k}(X_i) = \begin{cases} q^{k+i}(q-1) & \textit{para } i=-k,...,-1 \\ q^k & \textit{para } i=0 \\ q^{k-i}(q-1) & \textit{para } i=1,...,k; \end{cases}$$

2)

$$v_{Q_k}(\frac{X_i - X_{-i}}{X_i}) \geq q^{k-i} \qquad \text{para } i=1,...,k;$$

3) A função $f_k = \dfrac{Z_k - Y_k}{X_0} \in E_k$ é regular em Q_k e, para $P_k \in \mathbb{P}_{H_k}$ abaixo de Q_k, temos que o polinômio minimal de f_k sobre H_k é separável módulo P_k e, portanto, o lugar Q_k é não-ramificado na extensão E_k/H_k.

Demonstração: Faremos a prova por indução sobre k. Para $k=1$, temos $H_1 = \mathbb{F}_{q^2}(X_{-1}, X_0)$ e $E_1 = H_1(X_1)$. Seja $P_1 = Q_1 \cap H_1$. O lugar Q_1 é um zero comum de X_{-1}, X_0 e X_1, e temos as seguintes relações entre estas funções

$$\frac{X_1^q}{X_1+1} = \frac{X_0^{q-1}}{1-X_0^q} \tag{2.2}$$

e

$$\frac{X_{-1}^q}{X_{-1}+1} = X_0^{q-1}(1-X_0). \tag{2.3}$$

Destas relações nós temos que $v_{P_1}(X_{-1}) = q-1$, $v_{P_1}(X_0) = q$ e $e(P_1|Q_0) = q$.

Seja $f_1 = \dfrac{X_1 - X_{-1}}{X_0}$. O polinômio minimal de f_1 sobre H_1 é

$$P_{f_1|H_1}(T) = T^q - \frac{1}{1-X_0^q} \cdot T + (\frac{X_{-1}}{X_0})^q - \frac{X_{-1}+1}{(1-X_0^q)X_0}.$$

De fato, da Equação (2.2) nós temos que

$$X_1^q - \frac{X_0^{q-1}}{1-X_0^q} \cdot X_1 - \frac{X_0^{q-1}}{1-X_0^q} = 0$$

e multiplicando esta equação por $1/X_0^q$ temos

$$\left(\frac{X_1}{X_0}\right)^q - \frac{1}{1-X_0^q} \cdot \frac{X_1}{X_0} - \frac{1}{(1-X_0^q)X_0} = 0.$$

Daí segue que

$$\left(\frac{X_1}{X_0}-\frac{X_{-1}}{X_0}\right)^q+\left(\frac{X_{-1}}{X_0}\right)^q-\frac{1}{1-X_0^q}\left(\frac{X_1}{X_0}-\frac{X_{-1}}{X_0}\right)-\frac{1}{1-X_0^q}\cdot\frac{X_{-1}}{X_0}-\frac{1}{(1-X_0^q)X_0}=0.$$

Agora segue da equação (2.3) que vale

$$\left(\frac{X_{-1}}{X_0}\right)^q-\frac{X_{-1}+1}{(1-X_0^q)X_0}=\frac{(1+X_{-1})(1-X_0)}{X_0}-\frac{1+X_{-1}}{(1-X_0^q)X_0}=$$

$$\frac{1+X_{-1}}{1-X_0^q}\left(\frac{(1-X_0)^{q+1}}{X_0}-\frac{1}{X_0}\right)=\left(\frac{1+X_{-1}}{1-X_0^q}\right)(X_0^q-X_0^{q-1}-1).$$

E portanto, o polinômio minimal de f_1 sobre H_1 pode ser escrito como

$$P_{f_1|H_1}(T)=T^q-\frac{1}{1-X_0^q}\cdot T+\left(\frac{1+X_{-1}}{1-X_0^q}\right)(X_0^q-X_0^{q-1}-1).$$

Este polinômio tem coeficientes no anel de valorização de H_1 em P_1. Portanto f_1 pertence ao fecho inteiro deste anel de valorização no corpo E_1. Além disso sua redução $mod\, P_1$ nos dá $\overline{P}_{f_1|H_1}(T)=T^q-T-1$, que é separável, e assim, pelo Teorema de Kummer, concluimos que $e(Q_1|P_1)=1$. Logo temos $v_{Q_1}(X_{-1})=v_{Q_1}(X_1)=q-1$, $v_{Q_1}(X_0)=q$ e $v_{Q_1}(X_1-X_{-1})\geq v_{Q_1}(X_0)=q$. Assim $v_{Q_1}(\frac{X_1-X_{-1}}{X_1})\geq 1=q^0$ e o Lema 2.2.3 fica provado no caso $k=1$.

Seja agora $k\geq 2$ e suponha o resultado válido para $1\leq j<k$. O lugar Q_k é um zero comum de X_i para $i=-k,...,k$. Temos as seguintes relações entre X_i e X_{i+1}:

$$\frac{(1+X_{i+1})^q}{X_{i+1}}=\frac{1+X_i}{X_i^q}\ \text{ para } i=-k,...,-2 \tag{2.4}$$

$$(1-X_0)X_0^{q-1}=\frac{X_{-1}^q}{1+X_{-1}} \tag{2.5}$$

$$\frac{(1+X_1)}{X_1^q}=\frac{1-X_0^q}{X_0^{q-1}} \tag{2.6}$$

$$\frac{1+X_{i+1}}{X_{i+1}^q}=\frac{1+X_i^q}{X_i}\ \text{ para } i=1,...,k-1. \tag{2.7}$$

Da Equação (2.4) para $i=-k$ nós temos que $v_{P_k}(X_{-(k-1)})=q\cdot v_{P_k}(X_{-k})$. Logo $e(P_k|Q_{k-1})\cdot v_{Q_{k-1}}(X_{-(k-1)})=q\cdot v_{P_k}(X_{-k})$. Da hipótese de indução temos que $v_{Q_{k-1}}(X_{-(k-1)})=q-1$. De onde podemos concluir que $e(P_k\mid Q_{k-1})=q$. Assim,

$$v_{P_k}(X_j)=q\cdot v_{Q_{k-1}}(X_j)=\begin{cases} q^{k+j}(q-1) & \text{para } j=-(k-1),...,-1\\ q^k & \text{para } i=0\\ q^{k-j}(q-1) & \text{para } j=1,...,k-1.\end{cases}$$

Agora, utilizando a relação entre X_{-k} e $X_{-(k-1)}$ dada pela Equação (2.4), temos

$$v_{P_k}(X_i) = \begin{cases} q^{k+i}(q-1) & \text{para } i = -k, ..., -1 \\ q^k & \text{para } i = 0 \\ q^{k-i}(q-1) & \text{para } i = 1, ..., k-1; \end{cases} \tag{2.8}$$

Da Equação (2.7) para $i = k-1$ temos

$$X_k^q - \frac{X_{k-1}}{1+X_{k-1}^q} X_k - \frac{X_{k-1}}{1+X_{k-1}^q} = 0,$$

e multiplicando esta equação por Z_{k-1}^q / X_0^q temos

$$\left(\frac{Z_k}{X_0}\right)^q - \frac{X_{k-1} \cdot Z_{k-1}^{q-1}}{(1+X_{k-1}^q) X_0^{q-1}} \cdot \frac{Z_k}{X_0} - \frac{X_{k-1} Z_{k-1}^q}{(1+X_{k-1}^q) X_0^q} = 0.$$

Daí segue que

$$\left(\frac{Z_k}{X_0} - \frac{Y_k}{X_0}\right)^q + \left(\frac{Y_k}{X_0}\right)^q - \frac{X_{k-1} \cdot Z_{k-1}^{q-1}}{(1+X_{k-1}^q) X_0^{q-1}} \cdot \left(\frac{Z_k}{X_0} - \frac{Y_k}{X_0}\right)$$

$$- \frac{X_{k-1} \cdot Z_{k-1}^{q-1} Y_k}{(1+X_{k-1}^q) X_0^q} - \frac{X_{k-1} Z_{k-1}^q}{(1+X_{k-1}^q) X_0^q} = 0.$$

E portanto, o polinômio minimal de f_k sobre H_k é

$$P_{f_k|H_k}(T) = T^q - A_k T + B_k,$$

onde

$$A_k = \frac{X_{k-1}(Z_{k-1})^{q-1}}{(1+X_{k-1})^q \, X_0^{q-1}}$$

e

$$B_k = \left(\frac{Y_k}{X_0}\right)^q - \frac{X_{k-1}(Z_{k-1})^{q-1} Y_k}{(1+X_{k-1}^q) X_0^q} - \frac{X_{k-1}(Z_{k-1})^q}{(1+X_{k-1}^q) X_0^q}$$

Da Igualdade (2.8), é fácil ver que $v_{P_k}(Z_{k-1}) = q^k - q$ e que $v_{P_k}(A_k) = 0$. Vamos agora mostrar que $v_{P_k}(B_k) \geq 0$.

Nós podemos escrever B_k como abaixo:

$$B_k = A_k . \frac{1}{X_0} . \left(\frac{(1+X_{k-1})^q Y_k^q}{X_{k-1}(Z_{k-1})^{q-1}} - Y_k - Z_{k-1} \right).$$

Daí reduzimos a prova de que $v_{P_k}(B_k) \geq 0$ à prova de que $v_{P_k}(X_0B_k/A_k) \geq q^k$.

A hipótese de indução nos diz que $v_{P_k}(f_{k-1}) \geq 0$, isto é, nós obtemos que $Y_{k-1} = Z_{k-1} + \mathcal{O}(q^k)$ em P_k. Daí temos

$$v_{P_k}\left(\frac{Y_{k-1}^q - Z_{k-1}^q}{Z_{k-1}^{q-1}}\right) = q \cdot v_{P_k}(Y_{k-1} - Z_{k-1}) - (q-1)v_{P_k}(Z_{k-1}) \geq q^k + q^2 - q.$$

E portanto temos

$$\frac{Y_{k-1}^q}{Z_{k-1}^{q-1}} = Z_{k-1} + \mathcal{O}(q^k + q^2 - q) \text{ em } P_k. \tag{2.9}$$

Usando que $Y_k = Y_{k-1} \cdot X_{-k}$, temos

$$\frac{(1+X_{k-1})^q \cdot Y_k^q}{X_{k-1}(Z_{k-1})^{q-1}} = \frac{(1+X_{k-1})^q \cdot X_{-k}^q}{X_{k-1}} \cdot \frac{Y_{k-1}^q}{(Z_{k-1})^{q-1}} =$$

$$\left(\frac{X_{-k}^q}{X_{k-1}} + X_{k-1}^{q-1}.X_{-k}^q\right)\frac{Y_{k-1}^q}{(Z_{k-1})^{q-1}} = \left(\frac{X_{-k}^q}{X_{k-1}}\right) \cdot \frac{Y_{k-1}^q}{(Z_{k-1})^{q-1}} + \mathcal{O}(q^k) \text{ em } P_k.$$

Logo, da última igualdade e da Equação (2.9) temos

$$\frac{X_0B_k}{A_k} = \frac{X_{-k}^q}{X_{k-1}} \cdot Z_{k-1} - X_{-k} \cdot Z_{k-1} - Z_{k-1} + \mathcal{O}(q^k) \text{ em } P_k. \tag{2.10}$$

Usando a Equação (2.4) para $i = -k$, temos que

$$X_{-k}^q = \frac{(1+X_{-k})X_{-(k-1)}}{(1+X_{-(k-1)})^q}.$$

Daí temos

$$\frac{X_{-k}^q}{X_{k-1}} - X_{-k} - 1 = \left(\frac{X_{-(k-1)}}{X_{k-1}} - 1\right)(1+X_{-k}) + \mathcal{O}(q^2(q-1)) \text{ em } P_k. \tag{2.11}$$

Usando (2.10) e (2.11), a prova de que $v_{P_k}(B_k) \geq 0$ fica completa se mostramos

$$v_{P_k}\left(\frac{X_{k-1} - X_{-(k-1)}}{X_{k-1}}\right) \geq q. \tag{2.12}$$

A Equação (2.12) segue da hipótese de indução. De fato, para $i = 1, ..., k-1$ temos $v_{Q_{k-1}}\left(\dfrac{X_i - X_{-i}}{X_i}\right) \geq q^{(k-1)-i}$, e já temos observado que $e(P_k|Q_{k-1}) = q$. Terminamos então a prova de que o polinômio minimal de f_k sobre H_k tem coeficientes no anel de valorização de H_k em P_k, e é separável módulo P_k, e portanto $e(Q_k|P_k) = 1$. Agora, usando as Equações (2.4) e (2.7) para $i = -k$ e $i = k-1$, respectivamente, temos que

$$\frac{X_{-k}^q}{X_k^q} = \left(\frac{(1+X_{-k}) \cdot (1+X_{k-1})^q}{(1+X_k) \cdot \left(1+X_{-(k-1)}\right)^q} \right) \frac{X_{-(k-1)}}{X_{k-1}}.$$

Logo, temos que

$$\left(\frac{X_k - X_{-k}}{X_k} \right)^q = \frac{X_{k-1} - X_{-(k-1)}}{X_{k-1}} + \mathcal{O}(q-1) \text{ em } P_k.$$

Como já mostramos que $e(Q_k|P_k) = 1$, temos então $v_{Q_k}(\frac{X_k - X_{-k}}{X_k}) \geq 1$, e assim $v_{Q_k}(\frac{X_i - X_{-i}}{X_i}) \geq q^{k-i}$ para $i = 1, ..., k$. Assim, concluimos a prova do item 2), e portanto terminamos a prova do Lema 2.2.3.

■

Corolário 2.2.4. *Com a notação do Teorema* 2.2.2 *temos que o lugar Q_k é ramificado na extensão $E_k/K(x_{t+1+k})$ com índice de ramificação $q-1$ para $1 \leq k \leq t$.*

Isto segue diretamente do item (1) do Lema 2.2.3 (vide Figura 2.5).

2.3 O gênero da torre

Com os resultados da seção anterior estamos quase prontos para calcular o gênero de cada passo F_n da torre $\mathcal{F}$. Resta apenas calcular o grau da diferente nos lugares Q do tipo (C) e usar a fórmula do gênero de Hurwitz. Para isto, estendemos o corpo de constantes até o fecho algébrico k de $\mathbb{F}_{q^2}$. Conforme o Teorema 1.3.8, o gênero não se altera com esta mudança, e nesta seção, a menos que se mencione o contrário, denotaremos também por F_n o compositum $F_n \cdot k$. Nós também vamos precisar contar os pólos de x_{t+1} em F_n. Como uma consequência da igualdade fundamental $\sum e_i f_i = n$ temos a seguinte proposição que é consequência do Lema 2.2.2:

Proposição 2.3.1. *Com a notação do Teorema* 2.2.2*, temos que existem exatamente q^k pólos da função x_{t+1} em E_k, para cada $1 \leq k \leq t$.*

Demonstração: De fato, para cada lugar $P_k \in H_k$, pólo da função x_{t+1}, temos $e(P_k) = 1$ em E_k/H_k, conforme o Teorema 2.2.2. Além disso, como estamos trabalhando com o fecho algébrico de $\mathbb{F}_q$ como o corpo de constantes de H_k, temos que o índice de inércia é dado por $f(P) = 1$ para todo lugar P de H_k. Assim, da igualdade fundamental, segue que $\sum e(Q_k|P_k) = [E_k : H_k] = q$, e portanto existem exatamente q lugares de E_k que são pólos de x_{t+1}. O resultado segue então por indução sobre k.

■

Lema 2.3.2. *Seja $1 \leq t < n$ e seja $Q \in \mathbb{P}_{F_n}$ um lugar tal que:*
1) Q é zero de $x_1 - 1, ..., x_t - 1$;
2) Q é pólo de x_{t+1};
3) Q é zero de $x_{t+2}, ..., x_n$.
Então temos

i) Se $n \leq 2t+1$, o lugar Q é não-ramificado em F_n/F_{n-1} se $n > t+1$ e $e(Q|P) = q-1$ se $n = t+1$;

ii) Para $2t+1 < n$, o lugar Q é totalmente ramificado em F_n/F_{2t+1}, e para $2t+1 \leq s \leq n$ a restrição de Q a F_s tem índice de ramificação $q-1$ na extensão $F_s/k(x_s)$; e

iii) Se $2t+1 < n$, o expoente da diferente $d(Q)$ de Q na extensão F_n/F_{n-1} é dado por $d(Q) = 2(q-1)$.

Demonstração: O caso $t+1 = n$ já foi estudado na seção anterior. Suponhamos $t+1 < n \leq 2t+1$; então a restrição de Q a $E_k = k(x_{t+1-k}, ..., x_n)$, com $k = n-t-1$, é não-ramificada na extensão E_k/H_k, com $H_k = K(x_{t+1-k}, ..., x_{n-1})$, conforme o Teorema 2.2.2. Portanto Q é não ramificado na extensão F_n/F_{n-1}, conforme a Proposição 1.3.7 (vide Figura 2.6).

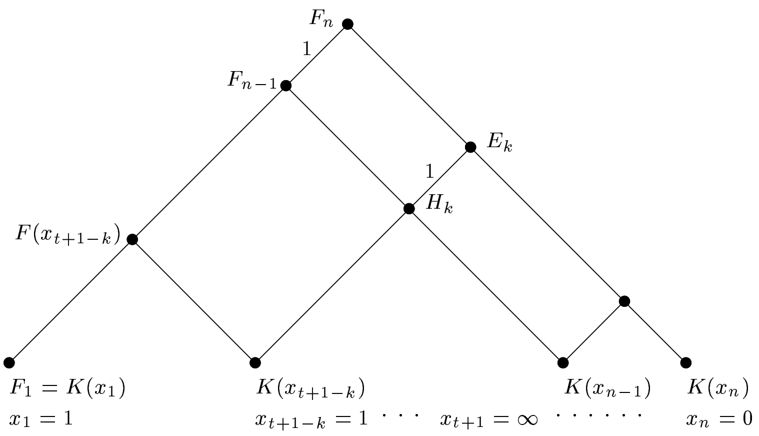

Figura 2.6: $t+1 < n \leq 2t+1$

Se $2t+1 < n$, então a restrição de Q ao corpo de funções F_{2t+1} é ramificada na extensão $F_{2t+1}/K(x_{2t+1})$ com índice de ramificação $q-1$, conforme o Corolário 2.2.4. Daí, segue por indução que a restrição Q a F_s tem índice de ramificação $q-1$ na extensão $F_s/k(x_s)$, para $2t+1 \leq s \leq n$. Os itens (ii) e (iii) seguem então da proposição 1.3.7 e do Lema 2.1.4, itens 5 e 6 (vide Figura 2.7).

■

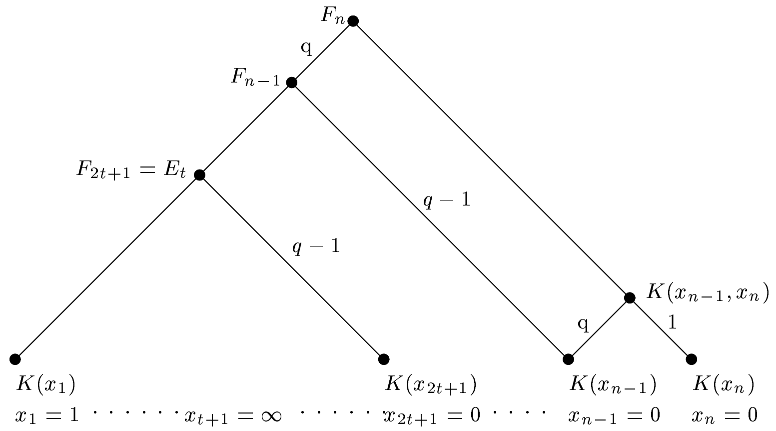

Figura 2.7: $2t + 1 < n$

Defina $A_t := \#\{Q \in \mathbb{P}_{F_n} : Q$ é pólo de $x_{t+1}\}$ e seja d_t o expoente da diferente de um lugar que é pólo de x_{t+1} na extensão F_n/F_{n-1} (Este número d_t está bem definido pois todos os lugares que são pólos de x_{t+1} em F_n têm o mesmo coeficiente da diferente na extensão F_n/F_{n-1}, vide o Lema 2.3.2). Para $1 \leq t \leq \frac{n-1}{2}$, observando que $F_{2t+1} = E_t$, nós temos do Corolário 2.3.1 e do item (ii) do lema anterior que:

Lema 2.3.3. *Seja* $1 \leq t < \dfrac{n-1}{2}$. *Então,* $A_t = q^t$.

E assim podemos obter o grau da diferente na extensãoF_n/F_{n-1}:

Lema 2.3.4. *Para* $n \geq 2$, *o grau da diferente da extensão* F_n/F_{n-1} *é dado por*

$$grau\,\mathrm{Diff}(F_n/F_{n-1}) = 2(q-1) + 2(q^{[n/2]} - 1)$$

onde $[x]$ *denota o maior inteiro menor ou igual a* x.

Demonstração: Seja $D_n = grau\,\mathrm{Diff}(F_n/F_{n-1})$. Conforme a notação do Lema 2.2.1 nós temos que $D_n = d(P) + \sum_{t=0}^{n-1} A_t d_t$. E assim, utilizando o Lema 2.2.1 e os Lemas 2.3.2 e 2.3.3 segue que

$$D_n = q + \sum_{0 \leq t < [(n-1)/2]} q^t \cdot 2(q-1) + q - 2.$$

Daí temos

$$D_n = 2(q-1)\big(1 + \sum_{0 \leq t < [(n-1)/2]} q^t\big),$$

isto é,

$$D_n = \begin{cases} 2(q-1) + 2(q^{n/2}-1) & \text{para } n \text{ par} \\ 2(q-1) + 2(q^{(n-1)/2}-1) & \text{para } n \text{ ímpar.} \end{cases}$$

■

Nós podemos facilmente determinar o gênero $g(F_n)$, usando o lema anterior e a fórmula do gênero de Hurwitz. O resultado nos dá:

Teorema 2.3.5. *Seja $g_n = g(F_n)$ o gênero do corpo de funções F_n. Então*

$$g_n = \begin{cases} (q^{n/2}-1)\left(\dfrac{q^{n/2}-1}{q-1}\right) & \textit{para } n \textit{ par} \\ \\ (q^{(n-1)/2}-1)\left(\dfrac{q^{(n+1)/2}-1}{q-1}\right) & \textit{para } n \textit{ ímpar.} \end{cases}$$

Demonstração: Da fórmula do gênero de Hurwitz (Teo. 1.3.2) e do Lema 2.3.4 segue que

$$g_n = q \cdot g_{n-1} - (q-1) + \frac{1}{2}\left(2(q-1) + 2(q^{[n/2]}-1)\right),$$

isto é,

$$g_n = q \cdot g_{n-1} + (q^{[n/2]}-1). \tag{2.13}$$

A partir da igualdade anterior vamos mostrar inicialmente o caso n par, isto é, para $k \geq 1$ nós vamos mostrar por indução que $g_{2k} = (q^k-1)\big(\frac{q^k-1}{q-1}\big)$.

Para $k = 1$ esta igualdade segue diretamente da Equação (2.13) e de $g_1 = 0$. Suponhamos então que $g_{2k} = (q^k-1)\big(\frac{q^k-1}{q-1}\big)$ para $k \geq 1$. Da Equação (2.13) segue que

$$g_{2k+1} = q \cdot g_{2k} + (q^k - 1).$$

E usando a Equação (2.13) novamente nós temos

$$g_{2(k+1)} = q^2 \cdot g_{2k} + q(q^k-1) + q^{k+1} - 1,$$

isto é,

$$\begin{aligned} g_{2(k+1)} &= q^2 \cdot (q^k-1)\big(\frac{q^k-1}{q-1}\big) + q(q^k-1) + q^{k+1} - 1 = \\ &= q(q^k-1)\left(\frac{q^{k+1}-q}{q-1} + 1\right) + q^{k+1} - 1 = \\ &= q(q^k-1)\left(\frac{q^{k+1}-1}{q-1}\right) + q^{k+1} - 1 = \\ &= (q^{k+1}-1)\left(\frac{q^{k+1}-q}{q-1} + 1\right) = (q^{k+1}-1)\left(\frac{q^{k+1}-1}{q-1}\right). \end{aligned}$$

Agora, se vale $g_{2k} = (q^k - 1)\big(\frac{q^k - 1}{q - 1}\big)$ para todo $k \geq 1$, então da Equação (2.13) nós temos que

$$\begin{aligned} g_{2k+1} &= q \cdot (q^k - 1)\big(\frac{q^k - 1}{q - 1}\big) + (q^k - 1) = \\ &= (q^k - 1) \cdot \big(\frac{q^{k+1} - q}{q - 1} + 1\big) = (q^k - 1) \cdot \big(\frac{q^{k+1} - 1}{q - 1}\big). \end{aligned}$$

■

Passamos agora a uma análise dos lugares racionais sobre $\mathbb{F}_{q^2}$:

Lema 2.3.6. *Seja $P \in \mathbb{P}_{F_1}$ zero de $x_1^q + x_1 - 1$. Então o lugar P se decompõe totalmente em F_n/F_1, para cada $n \in \mathbb{N}$.*

Demonstração: Seja então $P \in \mathbb{P}_{F_1}$ um zero de $x_1^q + x_1 - 1$. As seguintes afirmações são mostradas por indução sobre n:

a) P se decompõe totalmente em F_n/F_1;

b) Para qualquer $P' \in \mathbb{P}_{F_n}$ estando acima de P, existe $\alpha \in \mathbb{F}_{q^2}$ com $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = 1$ tal que P' é zero de $x_n - \alpha$, isto é, se $x_i^q(P') + x_i(P') = 1$, então $x_{i+1}^q(P') + x_{i+1}(P') = 1$, para cada $1 \leq i \leq n - 1$.

De fato, para $n = 2$ temos que o polinômio minimal de x_2 (gerador de F_2) sobre F_1 é dado por

$$\varphi(T) = T^q - \frac{x_1}{x_1^q - 1} \cdot T + \frac{x_1}{x_1^q - 1}.$$

Assim, a fatoração de $\varphi(T)$ módulo P é dada por $\overline{\varphi}(T) = T^q + T - 1 = \prod(T - \alpha_i)$ com $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha_i) = 1$, e do Teorema 1.3.6, segue o resultado por indução sobre n.

■

Demonstração do Teorema 2.1.2**:** Vamos utilizar aqui a notação do Teorema 1.2.11 com $\mathbb{F}_q$ substituido por $\mathbb{F}_{q^2}$.

Do Lema 2.3.6, para a torre $\mathcal{F}$ sobre $\mathbb{F}_{q^2}$ considerada, nós temos a desigualdade $N(F_n) \geq q.[F_n : F_1] = q^n$, e assim temos que:

$$\upsilon(\mathcal{F}) \geq q.$$

Do Teorema 2.3.5 temos que

$$\gamma(\mathcal{F}) = \frac{q}{q - 1}$$

e, portanto, $\lambda(\mathcal{F}) = \upsilon(\mathcal{F})/\gamma(\mathcal{F}) \geq q - 1$. O Teorema 2.1.2 agora segue do Teorema 1.2.4.

■

Observação 2.3.7. Da observação 2.1.3 nós sabemos que a torre $\mathcal{F}$ é uma subtorre da torre otimal $\mathcal{T}$ definida recursivamente pela equação

$$y^q + y = \frac{x^q}{x^{q-1}+1}.$$

Porém, se quisermos deduzir a fórmula do gênero dada acima, conforme o Teorema 2.3.5, nós devemos considerar as extensões de Kummer T_n/F_n de grau $q-1$ satisfazendo

$$T_n = F_n(y_1) \text{ com } y_1^{q-1} = \frac{1-x_1}{x_1}.$$

Logo, para deduzir o gênero de F_n do gênero de T_n nós precisamos estudar os zeros e pólos da função $(1-x_1)/x_1$ no corpo F_n, e assim não podemos evitar as considerações feitas neste capítulo.

Capítulo 3

Torre sobre $\mathbb{F}_{q^3}$

Neste capítulo nós apresentaremos uma nova torre explícita de corpos de funções sobre o corpo finito $\mathbb{F}_{q^3}$ para q qualquer potência de um primo. As características principais desta nova torre são as seguintes:

(1) Assim como a torre do Capítulo 2, ela é definida recursivamente por equações não-polinomiais e tem passos não-Galois para $q \neq 2$;

(2) A torre é assintoticamente boa e generaliza a cota inferior de Zink para uma potência q qualquer de um primo, isto é, se $\mathcal{F}$ é a torre em questão, temos

$$\lambda(\mathcal{F}) \geq \frac{2(q^2-1)}{q+2}.$$

3.1 A equação e a torre

Consideremos a equação

$$\frac{1-y}{y^q} = \frac{x^q + x - 1}{x} \tag{3.1}$$

Neste capítulo, $K = \mathbb{F}_{q^3}$ denotará o corpo finito com q^3 elementos e p a sua característica. Seja ainda $k = \overline{K}$ um fecho algébrico de K. Nós consideraremos aqui a torre $\mathcal{F} = (F_1, F_2, F_3, ...)$ de corpos de funções sobre K definida recursivamente pela Equação 3.1, isto é,

Definição 3.1.1. *Seja $F_1 := K(x_1)$ o corpo de funções racionais sobre K, isto é, a função x_1 é transcendente sobre K. Para $i \geq 1$, definimos*

$$F_{i+1} := F_i(x_{i+1}),$$

onde a função x_{i+1} satisfaz a equação abaixo:

$$\frac{1-x_{i+1}}{x_{i+1}^q} = \frac{x_i^q + x_i - 1}{x_i}. \tag{3.2}$$

Para $q = 2$, a substituição $x_i \to 1/x_i$, para cada i, transforma a Equação (3.2) na equação $x_{i+1}^2 + x_{i+1} = x_i + 1 + 1/x_i$, e esta é uma torre de Artin-Schreier, assintoticamente boa sobre $\mathbb{F}_8$, com limite $\lambda(\mathcal{F}) \geq \frac{3}{2} = 2(2^2-1)/(2+2)$ (vide [8]).

Como já foi adiantado na introdução, o principal interesse aqui é demonstrar o seguinte teorema

Teorema 3.1.2. *A torre $\mathcal{F}$ definida recursivamente como acima é assintoticamente boa com limite* $\lambda(\mathcal{F}) \geq \dfrac{2(q^2-1)}{q+2}$.

O teorema acima nos dá uma boa cota inferior para $A(q^3)$, melhorando todas as cotas inferiores até então conhecidas (vide [13]). No caso especial em que $q = p$ é um primo, o teorema acima nos dá uma nova prova para a cota inferior de Zink para $A(p^3)$ (vide [21]).

Novamente, o principal problema em achar este limite está no cálculo dos gêneros $g(F_n)$. Para isto nós estendemos o corpo de constantes até o fecho algébrico k, isto é, denotamos também por F_n o compositum $F_n.k$. A grande dificuldade está na determinação do divisor de ramificação das extensões F_{n+1}/F_n. Como veremos no Lema 3.2.1 da próxima seção, as extensões F_{n+1}/F_n têm grau q. Além disso, pela Equação (3.2), as extensões F_{n+1}/F_n são geradas por elementos $x_{n+1} \in F_{n+1}$ com polinômio minimal do tipo:

$$P_{x_{n+1}/F_n}(T) = T^q + \frac{x_n}{x_n^q + x_n - 1}T - \frac{x_n}{x_n^q + x_n - 1}. \tag{3.3}$$

Assim sendo, os possíveis lugares de ramificação na extensão F_{n+1}/F_n são os zeros e pólos da função $x_n/\left(x_n^q + x_n - 1\right)$. Para começar, nós vamos estudar as propriedades da extensão básica no próximo lema. Vale notar que como conseqüência do item (3) do lema abaixo, temos que $F/k(x)$ não é Galois para $q \neq 2$, diferindo consideravelmente do caso $q = 2$. Além disso, do item (7) do lema abaixo e da fórmula de Riemann-Hurwitz, nós temos que o gênero de F_2 é igual a $g_2 = q(q-1)/2$ e portanto $g_2 > 1$ se $q > 2$.

Lema 3.1.3. *Seja $k = \overline{\mathbb{F}_q}$ um fecho algébrico de $\mathbb{F}_q$, seja $F = k(x, y)$ o corpo de funções definido pela equação*

$$\frac{1-y}{y^q} = \frac{x^q + x - 1}{x} \tag{3.4}$$

e seja $R = \{\alpha \in k \mid \alpha^q + \alpha - 1 = 0\}$. Então as seguintes afirmações são satisfeitas:

1) $[F : k(x)] = [F : k(y)] = q$;

2) A função x tem um único zero P_0 em F e este lugar é totalmente ramificado em $F/k(x)$. A função x tem um único pólo P_∞ em F e este lugar é totalmente ramificado em $F/k(x)$;

3) *Para $\alpha \in R$ a função $x - \alpha$ tem exatamente dois zeros em F; a saber, o lugar P_α, zero comum de $x - \alpha$ e $y - 1$, que é não-ramificado em $F/k(x)$, e o lugar Q_α, zero comum de $x - \alpha$ e y^{-1}, que tem índice de ramificação $q - 1$ em $F/k(x)$;*

4) *A função $x - 1$ tem exatamente q zeros em F; a saber, para cada $\alpha \in R$ temos o lugar S_α zero comum de $x-1$ e $y-\alpha$, e este lugar é não-ramificado em $F/k(x)$;*

5) *A função y tem dois zeros em F, a saber o lugar P_0, que é não-ramificado em $F/k(y)$, e o lugar P_∞ que é ramificado em $F/k(y)$ com índice de ramificação $q - 1$. A função y tem q pólos distintos em F, a saber os lugares Q_α com $\alpha \in R$. Para $\alpha \in R$, a função $y - \alpha$ tem um único zero em F, a saber o lugar S_α, e este lugar é totalmente ramificado em $F/k(y)$. A função $y - 1$ tem q zeros em F, a saber os lugares P_α, e estes lugares são não-ramificados em $F/k(y)$.*

6) *Os divisores principais em F das funções x, $(x - 1)$, $(x - \alpha)$, y, $(y - 1)$ e $(y - \alpha)$ com $\alpha \in R$, são:*

$$
\begin{aligned}
&(x) = qP_0 - qP_\infty\\
&(x - \alpha) = P_\alpha + (q - 1)Q_\alpha - qP_\infty\\
&(x - 1) = \textstyle\sum_{\alpha\in R} S_\alpha - qP_\infty\\
&(y) = P_0 + (q - 1)P_\infty - \textstyle\sum_{\beta\in R} Q_\beta\\
&(y - \alpha) = qS_\alpha - \textstyle\sum_{\beta\in R} Q_\beta\\
&(y - 1) = \textstyle\sum_{\alpha\in R} P_\alpha - \textstyle\sum_{\beta\in R} Q_\beta;
\end{aligned}
$$

7) *Os lugares de F que são ramificados sobre $k(x)$ são exatamente os lugares P_0, P_∞ e Q_α, com $\alpha \in R$. Seus expoentes da diferente com respeito à extensão $F/k(x)$ são $d(P_0) = q$, $d(P_\infty) = 2(q - 1)$ e $d(Q_\alpha) = q - 2$, respectivamente;*

8) *Os lugares de F ramificados sobre $k(y)$ são exatamente P_∞ e S_α, com $\alpha \in R$. Seus expoentes da diferente em relação à extensão $F/k(y)$ são $q - 2$ e q, respectivamente.*

Demonstração: A prova do Lema 3.1.3 é análoga à prova do Lema 2.1.4. Vejamos neste caso.

Visto que a Equação (3.4) tem grau q nas variáveis x e y, nós claramente temos $[F : k(x)] \leq q$ e $[F : k(y)] \leq q$. Seja P_0 um lugar em F acima do único zero de x em $k(x)$. Da Equação (3.4) temos que

$$v_{P_0}\left(\frac{y^q}{1 - y}\right) = v_{P_0}(x) > 0.$$

Logo, pela Observação 1.3.1, o lugar P_0 está acima do único zero de y em $k(y)$ e assim temos

$$q \cdot v_{P_0}(y) = v_{P_0}(x) \Rightarrow e(P_0|P_0 \cap k(x)) = q \ \text{ e } \ e(P_0|P_0 \cap k(y)) = 1,$$

e estas igualdades nos permitem concluir os seguintes itens

i) P_0 é único zero de x em F, e $[F : k(x)] = q$;

ii) P_0 é não-ramificado em $F/k(y)$, e y é um parâmetro local em P_0.

Da Equação (3.4) nós temos que o polinômio minimal de y sobre $k(x)$ é igual a

$$\varphi(T) = T^q + \frac{x}{x^q + x - 1}T - \frac{x}{x^q + x - 1}.$$

Logo, da Prop. 1.3.4 segue-se que $d(P_0) = v_{P_0}(\varphi'(y)) = v_{P_0}\left(\dfrac{x}{x^q + x - 1}\right) = q.$

Analogamente, seja P_∞ um lugar em F acima do único pólo de x em $k(x)$. Da Equação (3.4) nós temos que

$$v_{P_\infty}\left(\frac{y^q}{1 - y}\right) = (q - 1) \cdot v_{P_\infty}\left(\frac{1}{x}\right) > 0.$$

Logo, pela Observação 1.3.1, o lugar P_∞ está acima do único zero de y em $k(y)$, e assim temos

$$q \cdot v_{P_\infty}(y) = (q - 1) \cdot v_{P_\infty}\left(\frac{1}{x}\right) \Rightarrow e(P_\infty|P_\infty \cap k(x)) = q \ \text{ e } \ e(P_\infty|P_\infty \cap k(y)) = q - 1,$$

e estas igualdades nos permitem concluir os seguintes itens

i') P_∞ é o único pólo de x em F;

ii') a função $t = (xy)^{-1}$ é um parâmetro local em P_∞.

Da Equação (3.4) nós temos que

$$\left(\frac{1}{y}\right)^q - \left(\frac{1}{y}\right)^{q-1} - \frac{x^q + x - 1}{x} = 0.$$

E multiplicando esta igualdade pela função $1/x^q$ nós obtemos que o polinômio minimal de t sobre $k(x)$ é igual a

$$\varphi(T) = T^q - \frac{1}{x} \cdot T^{q-1} - \frac{x^q + x - 1}{x^{q+1}}.$$

E assim, da Proposição 1.3.4, temos que

$$d(P_\infty) = v_{P_\infty}(\varphi'(t)) = v_{P_\infty}\left(\frac{1}{x} \cdot t^{q-2}\right) = q + (q - 2) = 2(q - 1).$$

Seja agora $\alpha \in R$ e seja P um zero da função $x - \alpha$ em $k(x)$. Então, o polinômio minimal da função $1/y$ sobre $k(x)$, dado por

$$\varphi(T) = T^q - T^{q-1} - \frac{x^q + x - 1}{x},$$

é inteiro sobre $\mathcal{O}_P$. Considerando a fatoração de $\varphi(T) \pmod P$ sobre $k(x)$, o Teorema 1.3.6 nos dá dois lugares em F, P_α e Q_α, ambos acima de P, com $y(P_\alpha) = 1$ e $y(Q_\alpha) = \infty$. Além disso, da Equação (3.4) nós temos que

$$(q-1) \cdot v_{Q_\alpha}(1/y) = v_{Q_\alpha}(x - \alpha) \Rightarrow e(Q_\alpha | Q_\alpha \cap k(x)) = q - 1.$$

E portanto, da igualdade fundamental, nós temos que $e(P_\alpha | P_\alpha \cap k(x)) = 1$ e estes lugares são os únicos dois zeros de $x - \alpha$ em F. Por Q_α ter ramificação moderada na extensão $F/k(x)$, segue do Teorema 1.3.3 que $d(Q_\alpha) = q - 2$.

Analogamente, para um lugar P' zero da função $x - 1$ em $k(x)$, olhando para a fatoração do polinômio minimal de y sobre o corpo $k(x)$, módulo o lugar P', nós temos, pelo Teorema 1.3.6, que para cada $\alpha \in R$ existe um único lugar S_α, acima de P', em F que é zero comum de $x - 1$ e $y - \alpha$, e que cada S_α é não-ramificado na extensão $F/k(x)$.

Veja que da Equação (3.4) nós temos que $\dfrac{1 - y - y^q}{y^q} = \dfrac{(x-1)^q}{x}$. Portanto

$$v_{S_\alpha}(y - \alpha) = q \cdot v_{S_\alpha}(x - 1).$$

E portanto, temos que $e(S_\alpha | S_\alpha \cap k(y)) = q$ e $e(S_\alpha | S_\alpha \cap k(x)) = 1$, de onde concluimos que $[F : k(y)] = q$.

Ainda do Teorema 1.3.6, nós temos que qualquer lugar S de F, que não é zero e nem pólo da função $\dfrac{x}{x^q + x - 1}$, é não-ramificado na extensão $F/k(x)$. De fato, basta ver que o polinômio minimal de y módulo $S \cap k(x)$ é separável, e portanto gera não-ramificação na extensão $F/k(x)$.

Até aqui nós provamos os itens $1), 2), 3), 4)$, parte do item $6)$, e o item $7)$. Os outros itens são provados de maneira análoga.

■

Na próxima seção nós estudaremos o comportamento de ramificação num passo geral da torre F_n/F_{n-1}.

3.2 O comportamento de ramificação

Considerando a torre $\mathcal{F}$, para cada passo F_n/F_{n-1}, os possíveis lugares de F_n que se ramificam sobre F_{n-1} são os zeros e pólos da função $x_{n-1}/\left(x_{n-1}^q + x_{n-1} - 1\right)$, conforme o Teorema 1.3.6. Do item (6) do Lema 3.1.3, segue que para $n \geq 2$ e $Q \in \mathbb{P}_{F_n}$ nós temos:

(1) Se $x_j(Q) = 0$ ou $x_j(Q) = \infty$ então $x_{j+1}(Q) = 0$.

(2) Se $x_j(Q) = \alpha$ para algum $\alpha \in R$, então $x_{j+1}(Q) = 1$ ou $x_{j+1}(Q) = \infty$.

(3) Se $x_j(Q) = 1$ então $x_{j+1}(Q) = \alpha$ para algum $\alpha \in R$.

(4) Se $x_j(Q) = 0$ então $x_{j-1}(Q) = 0$ ou $x_{j-1}(Q) = \infty$.

(5) Se $x_j(Q) = \infty$ ou $x_j(Q) = 1$ então $x_{j-1}(Q) = \alpha$ para algum $\alpha \in R$.

(6) Se $x_j(Q) = \alpha$ com $\alpha \in R$, então $x_{j-1}(Q) = 1$.

E assim, se $Q \in \mathbb{P}_{F_n}$ é um lugar que se ramifica na extensão F_n/F_{n-1}, então nós temos as seguintes possibilidades para este lugar:

(A) O lugar Q é zero ou pólo da função x_1 e portanto Q é um zero comum de x_i para $i = 2, ..., n$.

(B) O lugar Q é zero da função $x_n - 1$, e portanto existe uma $(n-1)$-upla de elementos de k, $(\alpha_1, ..., \alpha_{n-1})$, com $\alpha_{n-i} = 1$ se i é par, e $\alpha_{n-i} \in R$ caso contrário, tal que Q é zero comum das funções $x_i - \alpha_i$, para $i = 1, ..., n$.

(C) Existe um inteiro $1 \leq t' < n$ tal que

   i) Q é zero comum de $x_i - \alpha_i$, para $1 \leq i \leq t'$, onde $\alpha_{t'+1-i} \in R$ se i é ímpar, e $\alpha_{t'+1-i} = 1$ caso contrário;

   ii) Q é pólo de $x_{t'+1}$;

   iii) Q é zero de x_i para $i = t'+2, ..., n$.

Note que no Caso (C) a condição ii) implica nas outras duas condições i) e iii).

Analogamente ao estudo feito para a torre do Capítulo 2, os comportamentos de ramificação para estes três casos são bastante diferentes. Nos dois primeiros casos ele será determinado facilmente do estudo de pirâmides. Isto, juntamente com a determinação do expoente da diferente, é feito usando a Proposição 1.3.7 no seguinte lema:

Lema 3.2.1. *Para a torre $\mathcal{F}$ sobre $k = \overline{\mathbb{F}}_{q^3}$ temos:*

1) $[F_n : k(x_i)] = q^{n-1}$ *para cada* $i = 1, ..., n$.

2) Existe um único lugar $P \in \mathbb{P}(F_n)$ que é zero de x_1. O lugar P é totalmente ramificado na extensão F_n/F_1 e é não-ramificado na extensão $F_n/k(x_n)$. Além disso, o expoente da diferente $d(P)$ de P com respeito a extensão F_n/F_{n-1} é dado por $d(P) = q$.

3) Existe um único lugar $P' \in \mathbb{P}(F_n)$ que é pólo de x_1. O lugar P' é totalmente ramificado na extensão F_n/F_1 e tem índice de ramificação $q-1$ na extensão $F_n/k(x_n)$. Além disso, o expoente da diferente $d(P')$ de P' com respeito a extensão F_n/F_{n-1} é dado por $d(P') = 2(q-1)$.

4) Seja $\tilde{P} \in \mathbb{P}(F_n)$ um lugar que não é zero e nem pólo de x_n. Então o lugar $\tilde{P}$ é não-ramificado em F_n/F_1.

Demonstração: Como na demonstração do Lema 2.2.1, desde que a Equação (3.2) é uma equação de grau q para cada $i \geq 1$, nós temos que $[F_{i+1} : F_i] \leq q$ para todo $i \geq 1$, isto é $[F_n : F_1] \leq q^{n-1}$. Seja $P \in \mathbb{P}_{F_n}$ um zero de x_1, isto é, P é um lugar do tipo (A) com $x_1(P) = 0$. Então, P é um zero comum de x_i para $i = 1, ..., n$. Além disso, do Lema 3.1.3, para cada $i = 1, ..., n-1$ nós temos que os índices de ramificação das restrições de P nas extensões $K(x_i, x_{i+1})$ sobre $K(x_i)$, respectivamente sobre $K(x_{i+1})$, são iguais a q e respectivamente 1 (vide Figura 2.1 do Cap.2).

As seguintes afirmações seguem facilmente por indução sobre $n \geq 2$:

(a) O índice de ramificação de P com respeito a extensão F_n/F_1 é q^{n-1}.

(b) $[F_n : F_1] = q^{n-1}$.

(c) O lugar P é não-ramificado na extensão $F_n/k(x_n)$.

De fato, o caso $n = 2$ foi demonstrado no Lema 3.1.3. Seja agora Q um lugar em F_{n+1} zero de x_1 e sejam $P = Q \cap F_n$, $P_1 = P \cap k(x_n, x_{n+1})$ e $P_2 = P \cap k(x_n)$. Pela hipótese de indução nós temos que $e(P|P_2) = 1$ e pelo Lema 3.1.3 temos que $e(P_1|P_2) = q$ e $d(P_1|P_2) = q$. Segue então da Proposição 1.3.7 que $e(Q|P) = q$ e que $d(Q|P) = q$. Logo, com a hipótese de indução, temos $[F_{n+1} : F_1] \geq q^n$, e portanto, $[F_{n+1} : F_1] = q^n$. Assim, existe um único lugar do tipo (A) em F_n e este lugar é totalmente ramificado em F_n/F_1.

3) Seja agora $P' \in \mathbb{P}_{F_n}$ um pólo de x_1, isto é, P' é um lugar do tipo (A) com $x_1(P') = \infty$. Então, P' é um zero comum de x_i para $i = 2, ..., n$. Além disso, do Lema 3.1.3, para cada $i = 1, ..., n-1$ nós temos que os índices de ramificação das restrições de P' nas extensões $k(x_i, x_{i+1})$ sobre $k(x_i)$, respectivamente $k(x_{i+1})$, são iguais a q e $q-1$ se $i = 1$, e são iguais a q e 1 se $i > 1$ (vide Figura 2.2 do Cap.2).

As seguintes afirmações seguem facilmente por indução sobre $n \geq 2$:

(a') O lugar P' é totalmente ramificado e tem expoente da diferente na extensão F_n/F_{n-1} dado por $d(P') = 2(q-1)$.

(b') O lugar P' tem índice de ramificação $q-1$ na extensão $F_n/k(x_n)$.

De fato, o caso $n = 2$ foi demonstrado no Lema 3.1.3. Seja agora Q' um lugar em F_{n+1} pólo de x_1 e sejam $P' = Q' \cap F_n$, $P'_1 = P' \cap k(x_n, x_{n+1})$ e $P'_2 = P' \cap k(x_n)$. Pela hipótese de indução nós temos que $e(P'|P'_2) = q - 1$ e pelo Lema 3.1.3 temos que $e(P'_1|P'_2) = q$, $e(P'_1|P'_1 \cap k(x_{n+1})) = 1$ e $d(P'_1|P'_2) = q$. Segue então da Proposição 1.3.7 que $e(Q'|P') = q$, $e(Q'|P'_1) = q - 1$ e que $d(Q'|P') = 2(q-1)$. Além disso, da multiplicidade dos índices de ramificação, segue que $e(Q'|Q' \cap k(x_{n+1})) = e(Q'|P'_1) \cdot e(P'_1|P'_1 \cap k(x_{n+1})) = q - 1$.

Resta então mostrar o item 4). Do Teorema 1.3.6 e do Lema 3.1.3 basta mostrarmos que os zeros de $x_n - 1$ não se ramificam em F_n/F_1. Nós reduzimos isto a mostrar que os zeros de $x_{n-1} - \alpha$ não se ramificam na extensão F_{n-1}/F_1, para cada $\alpha \in R$, pois do Lema 3.1.3 e do item *i*) da Proposição 1.3.7 temos que tais lugares de F_{n-1} não se ramificam na extensão F_n/F_{n-1}. De um modo geral, vamos mostrar, para quaisquer $n \geq 2$ e $\alpha \in R$, que os zeros de $x_n - \alpha$ não se ramificam em F_n/F_1.

Seja $\alpha \in R$ e seja $\tilde{P} \in \mathbb{P}_{F_n}$ um zero de $x_n - \alpha$. As seguintes afirmações seguem por indução sobre $n \geq 2$:

(a") $e(\tilde{P}|\tilde{P} \cap K(x_n)) = q^{n/2}$ se n é par, e $e(\tilde{P}|\tilde{P} \cap K(x_n)) = q^{(n-1)/2}$ se n é ímpar.

(b") $e(\tilde{P}|\tilde{P} \cap K(x_1)) = 1$.

De fato, para $n = 2$, seja $\tilde{P} \in \mathbb{P}_{F_2}$ um zero de $x_n - \alpha$, para algum elemento $\alpha \in R$. Então nós temos do Lema 3.1.3 que $e(\tilde{P}|\tilde{P} \cap K(x_2)) = q = q^{2/2}$, e que $e(\tilde{P}|\tilde{P} \cap K(x_1)) = 1$. Suponhamos então que a afirmação vale para $n \geq 2$ e seja $\tilde{Q} \in \mathbb{P}_{F_{n+1}}$ um zero de $x_{n+1} - \alpha$. Aqui nós temos que analisar separadamente os casos n par e n ímpar.

Se n é par, então $n+1$ é ímpar. Logo, da hipótese de indução, a restrição $\tilde{P}$ de $\tilde{Q}$ a $K(x_2, ..., x_{n+1})$ satisfaz $e(\tilde{P}|\tilde{P} \cap K(x_{n+1})) = q^{n/2}$ e $e(\tilde{P}|\tilde{P} \cap K(x_2)) = 1$. Mas como $n+1$ é ímpar, nós temos que $x_1(\tilde{P}) = \beta \in R$ e $x_2(\tilde{P}) = 1$. Se $\tilde{P}_2$ é a restrição de $\tilde{Q}$ ao corpo de funções $K(x_1, x_2)$, novamente do Lema 3.1.3 nós temos que $e(\tilde{P}_2|\tilde{P}_2 \cap K(x_2)) = e(\tilde{P}_2|\tilde{P}_2 \cap K(x_1)) = 1$. Portanto, da Proposição 1.3.7, segue que $e(\tilde{Q}|\tilde{P}) = e(\tilde{Q}|\tilde{P}_2) = 1$, e da multiplicidade dos índices de ramificação temos que

$$e(\tilde{Q}|\tilde{Q} \cap K(x_{n+1})) = e(\tilde{Q}|\tilde{P}) \cdot e(\tilde{P}|\tilde{P} \cap K(x_{n+1})) = 1 \cdot q^{n/2} = q^{((n+1)-1)/2}$$

e

$$e(\tilde{Q}|\tilde{Q} \cap K(x_1)) = e(\tilde{Q}|\tilde{P}_2) \cdot e(\tilde{P}_2|\tilde{P}_2 \cap K(x_1)) = 1.$$

Analogamente, para o caso n ímpar, nós temos que $n+1$ é par. Logo, da hipótese de indução, a restrição $\tilde{P}$ de $\tilde{Q}$ ao corpo de funções $K(x_2, ..., x_{n+1})$ satisfaz as igualdades $e(\tilde{P}|\tilde{P} \cap K(x_{n+1})) = q^{(n-1)/2}$ e $e(\tilde{P}|\tilde{P} \cap K(x_2)) = 1$. Agora, como $n+1$ é par, nós temos que $x_1(\tilde{P}) = 1$ e $x_2(\tilde{P}) = \gamma$ para algum $\gamma \in R$. Se $\tilde{P}_2$ é a restrição de $\tilde{Q}$ ao corpo de funções $K(x_1, x_2)$, novamente do Lema 3.1.3, nós temos que $e(\tilde{P}_2|\tilde{P}_2 \cap K(x_2)) = q$ e $e(\tilde{P}_2|\tilde{P}_2 \cap K(x_1)) = 1$. Portanto, da Proposição 1.3.7, segue que $e(\tilde{Q}|\tilde{P}) = q$ e $e(\tilde{Q}|\tilde{P}_2) = 1$, e assim,

$$e(\tilde{Q}|\tilde{Q} \cap K(x_{n+1})) = e(\tilde{Q}|\tilde{P}) \cdot e(\tilde{P}|\tilde{P} \cap K(x_{n+1})) = q \cdot q^{(n-1)/2} = q^{(n+1)/2}$$

e

$$e(\tilde{Q}|\tilde{Q} \cap K(x_1)) = e(\tilde{Q}|\tilde{P}_2) \cdot e(\tilde{P}_2|\tilde{P}_2 \cap K(x_1)) = 1. \quad \blacksquare$$

Do item (2) do Lema 3.2.1 nós concluimos que a sequência (F_n) é de fato uma torre de corpos de funções (conforme o comentário após o Teorema 1.3.8). Nosso próximo passo é calcular o grau da diferente $\mathrm{Diff}(F_n/F_{n-1})$ para $n \geq 3$. Pelo Lema anterior resta investigar o comportamento dos lugares Q de F_n do tipo (C), isto é, lugares Q que são pólos de $x_{t'+1}$ para algum $1 \leq t' < n$, na extensão F_n/F_{n-1}. Como já foi observado, o lugar Q é zero comum das funções $x_i - \alpha_i$, com $\alpha_{t'+1-i} \in R$ para $i \geq 1$ ímpar, $\alpha_{t'+1-i} = 1$ para $i \geq 2$ par, e $\alpha_{t'+1+i} = 0$ para $i \geq 1$.

Se $t' = 1$, seja $r = q - 1$, segue do Lema 3.1.3, a seguinte pirâmide de ramificação para um lugar Q de F_n pólo de x_2:

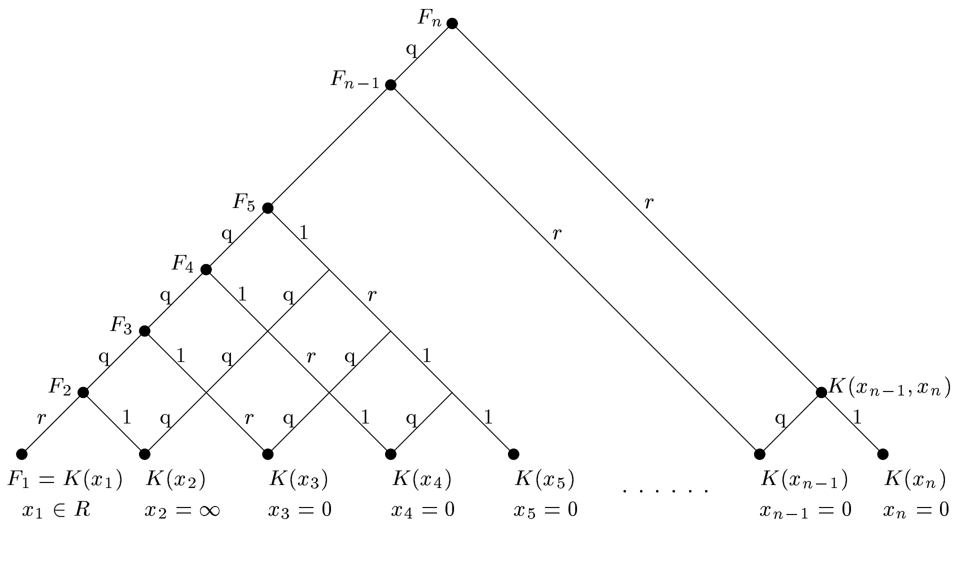

Figura 3.1: $x_2 = \infty$

Daí, usando a Proposição 1.3.7 nós temos que o lugar Q é totalmente ramificado na extensão F_n/F_{n-1} e $d(Q) = 2(q-1)$. Além disso, todo lugar Q de F_n que é pólo de x_2 tem a mesma ordem de pólo igual a q^{n-2}. Assim, se $A_{1,n}$ é a quantidade de pólos de x_2 em F_n temos da igualdade fundamental que

$$q^{n-1} = [F_n : K(x_2)] = A_{1,n} \cdot q^{n-2},$$

o que nos permite concluir que existem exatamente q pólos de x_2 em F_n para $n \geq 3$.

Se $t' = n-1$, o lugar Q é um pólo de x_n. Neste caso, a restrição P de Q a F_{n-1} é um zero da função $x_{n-1} - \alpha$ para algum elemento $\alpha \in R$ e portanto temos $e(P|P \cap K(x_1)) = 1$ e $mdc(q-1, e(P|P \cap K(x_{n-1})) = 1$, conforme a prova do Lema 3.2.1, item 4). Além disso, se P' é a restrição de Q a $K(x_{n-1}, x_n)$, então, do Lema 3.1.3, nós temos que $e(P'|P' \cap K(x_{n-1})) = q-1$ e $e(P'|P' \cap K(x_n)) = 1$. Logo, da Proposição 1.3.7 segue que $e(Q|P) = q-1$ e portanto $d(Q|P) = q-2$. Segue ainda da Proposição 1.3.7 que $e(Q|Q \cap K(x_{n-1}, x_n)) = e(P|P \cap K(x_{n-1}))$. Daí, como $e(P'|P' \cap K(x_n)) = 1$, nós temos que $e(Q|Q \cap K(x_n)) = e(P|P \cap K(x_{n-1}))$. Como isto vale para qualquer pólo Q de x_n em F_n, se $A_{n-1,n}$ é a quantidade de pólos de x_n no corpo de funções F_n, nós temos da igualdade fundamental que

$$q^{n-1} = [F_n : K(x_n)] = A_{n-1,n} \cdot e(P|P \cap K(x_{n-1})).$$

Se n é par, esta última igualdade nos dá $A_{n-1,n} = q^{n/2}$, e se n é ímpar ela nos dá $A_{n-1,n} = q^{(n-1)/2}$ (conforme a demonstração do item 4) do Lema 3.1.4).

Agora, se $1 < t' < n-1$, as ramificações para as restrições de Q em $k(x_{i-1}, x_i, x_{i+1})/k(x_i, x_{i+1})$ (resp. sobre $k(x_{i-1}, x_i)$) para $t' \leq i \leq t'+1$ são como na Figura 3.2 abaixo, conforme segue do Lema 3.1.3 e da Proposição 1.3.7. Não podemos deduzir os índices de ramificação de Q na extensão $F_n/k(x_j)$, $\forall j$, apenas da figura.

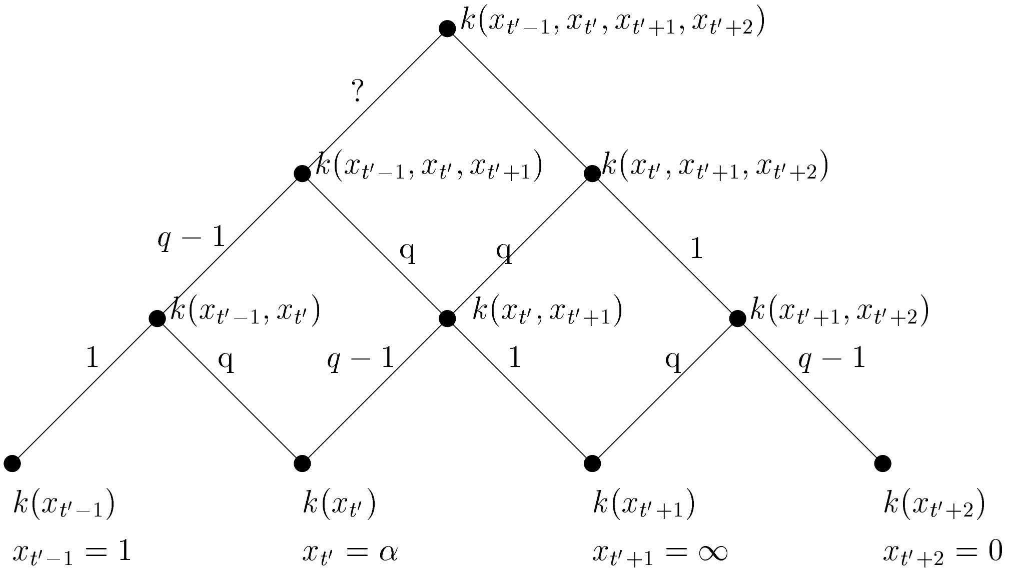

Figura 3.2: $x_{t'+1} = \infty$ com $1 < t' < n-1$

Os próximos resultados nos permitirão determinar os índices de ramificação nas extensões $F_n/k(x_j)$ através da determinação de parâmetros locais e do *Processo de Redução.* Como veremos no Teorema a seguir, o comportamento de ramificação da torre $\mathcal{F}$ irá se alternar em ramificações (total) e não-ramificações (vide Figura 3.3). Antes, porém, vamos fixar algumas notações. Seja R o conjunto $\{\alpha \in k \mid \alpha^q + \alpha - 1 = 0\}$, como no Lema 3.1.3. Fixado $t' \geq 2$, defina $t = [t'/2]$ o maior inteiro menor ou igual a $t'/2$ e seja $(\alpha_1, ..., \alpha_t)$ uma t-upla de elementos de R, nós usaremos as seguintes notações:

$$X_i := \begin{cases} x_{t'+1-i} - 1 & \text{para } i \text{ par com } 2 \leq i \leq t' \\ x_{t'+1-i} - \alpha_{\frac{i+1}{2}} & \text{para } i \text{ ímpar com } 1 \leq i \leq t'; \end{cases}$$

$Y := x_{t'+1}^{-1}$;

$Z_i := x_{t'+1+i}$ se $i \geq 1$;

$H_{i,1} := k(X_1, ..., X_{2i}, Y)$ se $1 \leq i \leq t$, onde $k = \overline{\mathbb{F}_q}$ é um fecho algébrico, e ainda, para $1 \leq j \leq i \leq t$, seja

$H_{i,j} := H_{i,1}(Z_1, ..., Z_{2(j-1)})$ para $j \geq 2$;

$E_{i,j} := H_{i,j}(Z_{2j-1})$ e $L_j := E_{j,j}(Z_{2j})$.

Nós podemos reescrever a Equação (3.2) em função de X_i, Y e Z_i, para $1 \leq i \leq t'$, e obtemos as seguintes equações:

$$\frac{X_i^q + X_i}{X_i^q + \alpha_{(i+1)/2}^q} = \frac{-X_{i+1}^q}{X_{i+1} + 1} \quad \text{se } i \text{ é ímpar} \tag{3.5}$$

$$\frac{-X_i}{X_i^q + 1} = \frac{X_{i+1}^q + X_{i+1}}{X_{i+1} + \alpha_{(i+2)/2}} \quad \text{se } i \text{ é par} \tag{3.6}$$

$$Y^q - Y^{q-1} - 1 = \frac{X_1^q - \alpha_1}{X_1 + \alpha_1} \tag{3.7}$$

$$\frac{Z_1 - 1}{Z_1^q} = \frac{Y^q - Y^{q-1} - 1}{Y^{q-1}} \tag{3.8}$$

$$\frac{1 - Z_{i+1}}{Z_{i+1}^q} = \frac{Z_i^q + Z_i - 1}{Z_i} \quad \text{para } i \geq 1. \tag{3.9}$$

Teorema 3.2.2. *Seja $P \in \mathbb{P}_{H_{i,j}}$ um zero de Y. Então P é totalmente ramificado em $E_{i,j}/H_{i,j}$. Além disso, o lugar Q acima de P em $E_{i,j}$ não se ramifica em $H_{i,j+1}/E_{i,j}$ se $j < i$ e não se ramifica em $L_j/E_{j,j}$ se $j = i$.*

O teorema 3.2.2 acima é o ponto central da determinação das diferentes $\text{Diff}(F_n/F_{n-1})$ e, portanto, da determinação dos gêneros $g(F_n), \forall n \in \mathbb{N}$. Nós dividiremos a demonstração deste Teorema em lemas que tratam separadamente do Caso $j = 1$ e do Caso $j > 1$. Em ambos os casos, o grande achado dos lemas a seguir é a determinação de parâmetros locais nos lugares P, zeros de Y, e as *Fórmulas de Redução*, que nos fornecem um novo gerador de $E_{i,j}$ sobre $H_{i,j}$ cujo o polinômio minimal é do tipo da Equação (1.4) onde podemos aplicar o Teorema 1.4.1 para obter informações sobre ramificação e diferente.

Na figura abaixo $r := q - 1$.

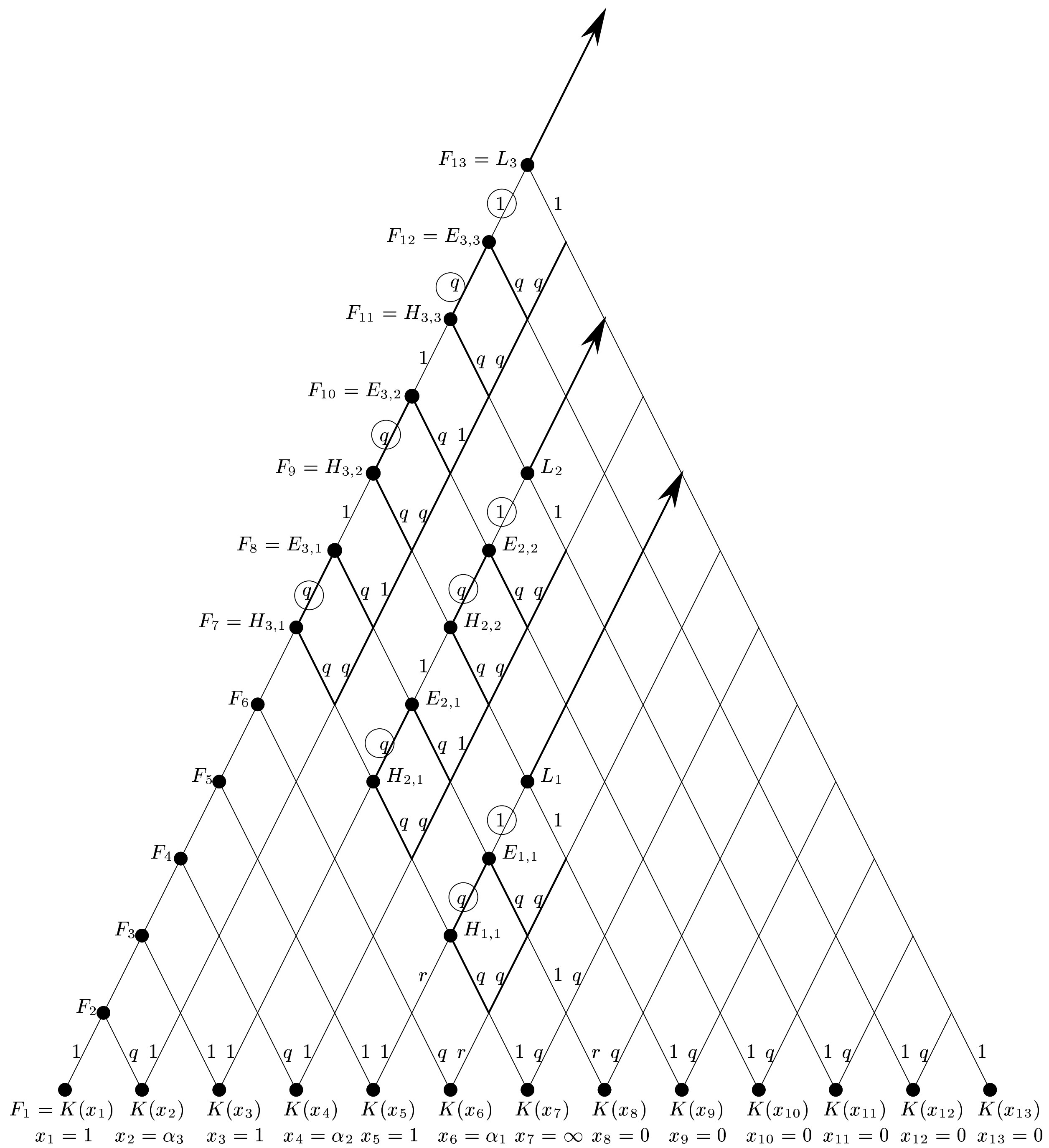

Figura 3.3: $x_7 = \infty$

Os Lemas 3.2.3 e 3.2.4 abaixo explicam os índices de ramificação circundados ① e @ na Figura 3.3. A Figura 3.3 indica que os lugares de F_{13} que são pólos da função x_7 se ramificam totalmente em F_n/F_{13} para cada $n \in \mathbb{N}$ com $n > 13$.

Lema 3.2.3. *(Caso j=1) Seja $P_i := P_{i,1} \in \mathbb{P}_{H_{i,1}}$ um zero de Y (o que implica que P_i é um zero comum de $X_1, ..., X_{2i}$). Então*

1) As ordens de zero em P_i das funções Y e X_k são $v_{P_i}(Y) = q^i$, e

$$v_{P_i}(X_k) = \begin{cases} q^{i-\frac{k-1}{2}}(q-1) & \text{para } k \text{ ímpar com } 1 \leq k \leq 2i \\ q^{i-\frac{k}{2}}(q-1) & \text{para } k \text{ par com } 1 \leq k \leq 2i. \end{cases}$$

2) Para $i \geq 1$, seja $t_i := \left(\prod_{k=1}^{i} X_{2k}\right)/Y \in H_{i,1}$ e seja $\mu_i := \dfrac{Z_1}{Y} + \sum_{k=1}^{i}(-1)^k A_k \cdot \alpha_k \cdot t_k \in E_{i,1}$, onde $A_k := \prod_{r=1}^{k} \alpha_r^{-q} \in \mathbb{F}_{q^2}$. Então

a) t_i^{-1} é parâmetro local em P_i e, para $i \geq 2$, temos

$$t_{i-1} = A_i^{q-1} \cdot t_i^q - t_i + \mathcal{O}(0) \text{ em } P_i.$$

b) $E_{i,1} = H_{i,1}(\mu_i)$, e o polinômio minimal de μ_i sobre $H_{i,1}$ é dado por

$$P_{\mu_i/H_{i,1}}(T) = T^q - (\frac{X_1 + \alpha_1}{X_1^q - \alpha_1})T + (-1)^{i+1} A_i \cdot t_i - h,$$

para alguma função $h \in H_{i,1}$ regular em P_i. Logo P_i é totalmente ramificado em $E_{i,1}/H_{i,1}$ e a função μ_i^{-1} é parâmetro local em Q_i, onde Q_i é o lugar de $E_{i,1}$ acima de P_i.

c) Para $i \geq 2$ temos a seguinte redução :

$$\mu_{i-1} = \alpha_i^q \mu_i - \alpha_i \mu_i^q + \mathcal{O}(0) \text{ em } Q_i.$$

d) Seja R_1 um lugar de L_1 acima de Q_1. A função $f_1 := Z_2\mu_1^q + c_1\mu_1 \in L_1$, com $c_1 = \alpha_1^{q-1}$, é regular em R_1 e satisfaz uma equação do tipo:

$$(Z_1^q + Z_1 - 1)f_1^q + (Z_1 \mu_1^{q(q-1)})f_1 = h,$$

para alguma função $h \in E_{1,1}$ regular em Q_1. Em particular, temos que o lugar Q_1 é não-ramificado em $L_1/E_{1,1}$ e, para $i \geq 2$, temos que o lugar Q_i é não-ramificado em $H_{i,2}/E_{i,1}$.

Demonstração: Faremos a prova para os casos $i = 1$ e $i = 2$, e continuaremos a demonstração por indução sobre i.

Para $i = 1$, temos que $v_{P_1}(X_1) = q(q-1)$, $v_{P_1}(X_2) = q - 1$ e $v_{P_1}(Y) = q$, como segue diretamente da Proposição 1.3.7 e da transitividade dos índices de ramificação (vide a Figura 3.3). Logo, $v_{P_1}(t_1) = -1$ e então $t_1^{-1} \in H_{1,1}$ é parâmetro local em P_1.

Agora veja que podemos reescrever a Equação (3.8) da seguinte forma

$$Z_1^q - (\frac{Y^{q-1}}{Y^q - Y^{q-1} - 1})Z_1 + \frac{Y^{q-1}}{Y^q - Y^{q-1} - 1} = 0. \tag{3.10}$$

Então, multiplicando esta equação por $1/Y^q$ e usando a Equação (3.7), nós obtemos

$$(\frac{Z_1}{Y} - A_1 \cdot \alpha_1 \cdot t_1)^q - (\frac{X_1 + \alpha_1}{X_1^q - \alpha_1})(\frac{Z_1}{Y} - A_1 \cdot \alpha_1 \cdot t_1) + (\alpha_1)^{q-1} \cdot t_1^q -$$
$$-(\frac{X_1 + \alpha_1}{X_1^q - \alpha_1})(\frac{1}{\alpha_1})^{q-1} \cdot t_1 + (\frac{X_1 + \alpha_1}{X_1^q - \alpha_1})\frac{1}{Y} = 0.$$

E assim, o polinômio minimal de μ_1 sobre $H_{1,1}$ é dado po

$$P_{\mu_1/H_{1,1}}(T) = T^q - (\frac{X_1 + \alpha_1}{X_1^q - \alpha_1})T + g_1,$$

onde

$$\begin{aligned} g_1 &= (\alpha_1)^{q-1} \cdot t_1^q - (\frac{X_1 + \alpha_1}{X_1^q - \alpha_1})(\frac{1}{\alpha_1})^{q-1} \cdot t_1 + (\frac{X_1 + \alpha_1}{X_1^q - \alpha_1})\frac{1}{Y} \\ &= \frac{1}{Y}\left((\alpha_1)^{q-1} \cdot \frac{X_2^q}{Y^{q-1}} - (\frac{X_1 + \alpha_1}{X_1^q - \alpha_1})\frac{X_2}{\alpha_1^{q-1}} + \frac{X_1 + \alpha_1}{X_1^q - \alpha_1}\right) \\ &= \frac{1}{Y}\left(\frac{\alpha_1^{q-1}(X_2 + 1)(1 - Y)}{(X_1 + \alpha_1)^{q-1}} - (\frac{X_1 + \alpha_1}{X_1^q - \alpha_1})\frac{X_2}{\alpha_1^{q-1}} + \frac{X_1 + \alpha_1}{X_1^q - \alpha_1}\right) \\ &= \frac{1}{Y}\left((1 + X_2) - 1 + \frac{X_2}{\alpha_1^{q-1}} + \mathcal{O}(q)\right) \quad \text{em } P_1. \end{aligned}$$

Nas igualdades acima foram usadas a Equação (3.5) para $i = 1$ e a Equação (3.7), para deduzir que $\dfrac{X_2^q}{Y^{q-1}} = \dfrac{(X_2 + 1)(1 - Y)}{(X_1 + \alpha_1)^{q-1}}$. Logo, obtemos que

$$g_1 = \frac{1}{\alpha_1^q}\frac{X_2}{Y} + \mathcal{O}(0) \quad \text{em } P_1, \text{ e}$$

$$\mu_1^q - (\frac{X_1 + \alpha_1}{X_1^q - \alpha_1}) \cdot \mu_1 + \frac{1}{\alpha_1^q} \cdot t_1 = h \quad \text{com} \quad h \in \mathcal{O}_{P_1}. \tag{3.11}$$

Como μ_1 também é um elemento primitivo de $E_{1,1}$ sobre $H_{1,1}$, nós temos que o lugar P_1 é totalmente ramificado em $E_{1,1}/H_{1,1}$ (conforme o item (ii) do Teorema 1.4.1). Além disso, da Equação (3.11) nós temos que

$$\mu_1^q + \mu_1 + A_1 \cdot t_1 = \mathcal{O}(0) \quad \text{em} \quad Q_1. \tag{3.12}$$

E isto nos dá $v_{Q_1}(\mu_1) = -1$. O que completa a prova do item b) da parte (2) do Lema 3.2.3, para o caso $i = 1$.

Para o item (d), note que da Equação (3.9), para $i = 1$, nós temos:

$$(Z_1^q + Z_1 - 1)Z_2^q + Z_1 \cdot Z_2 - Z_1 = 0.$$

Portanto, multiplicando esta equação por $\mu_1^{q^2}$ temos

$$(Z_1^q + Z_1 - 1)(Z_2\mu_1^q)^q + (Z_1\mu_1^{q^2-q})(Z_2\mu_1^q) - Z_1\mu_1^{q^2} = 0.$$

E podemos reescrever a última equação como

$$(Z_1^q + Z_1 - 1)(Z_2\mu_1^q + c_1\mu_1)^q - (Z_1^q + Z_1 - 1)c_1^q\mu_1^q + (Z_1\mu_1^{q^2-q})(Z_2\mu_1^q + c_1\mu_1)$$

$$-c_1Z_1\mu_1^{q^2-q+1} - Z_1\mu_1^{q^2} = 0.$$

com $v_{Q_1}(Z_1) = q^2 - q$ e $v_{Q_1}(\mu_1) = -1$. Daí,

$$(Z_1^q + Z_1 - 1)f_1^q + (Z_1\mu_1^{q(q-1)})f_1 - (\mu_1^{q^2} + c_1\mu_1^{q^2-q+1})Z_1 + c_1^q\mu_1^q = h_1, \tag{3.13}$$

para alguma função $h_1 \in E_{1,1}$ regular em Q_1. Vamos agora então mostrar que a função $(\mu_1^{q^2} + c_1\mu_1^{q^2-q+1})Z_1 - c_1^q\mu_1^q$ é regular em Q_1. Consideremos a equação que define a função μ_1:

$$\mu_1 = \frac{Z_1}{Y} - A_1\alpha_1t_1. \tag{3.14}$$

Da Equação (3.12) nós temos $t_1 = -\alpha_1^q\mu_1^q - \alpha_1^q\mu_1 + \mathcal{O}(0)$ em Q_1 e, substituindo na Equação (3.14), vamos ter

$$\mu_1 = \frac{Z_1}{Y} + A_1\alpha_1\big(\alpha_1^q\mu_1^q + \alpha_1^q\mu_1\big) + \mathcal{O}(0) \text{ em } Q_1,$$

isto é, vamos ter

$$\frac{Z_1}{Y} = -\alpha_1\mu_1^q + \alpha_1^q\mu_1 + \mathcal{O}(0) \text{ em } Q_1. \tag{3.15}$$

Sabendo que $v_{Q_1}(X_1) = q^2(q-1)$ (P_1 se ramifica totalmente em $E_{1,1}/H_{1,1}$), das Equações (3.7) e (3.8) nós obtemos que

$$\frac{Z_1^q}{Y^q}\Big(\frac{Y}{Z_1 - 1}\Big) = (X_1 + \alpha_1)\Big(-\frac{1}{\alpha_1}\Big) + \mathcal{O}(q^2(q-1)) \text{ em } Q_1.$$

O que implica em

$$\frac{Z_1^q}{Y^q} = \Big(-\frac{Z_1}{Y}\Big) + \frac{1}{Y} + \mathcal{O}(q^2(q-2)) \text{ em } Q_1. \tag{3.16}$$

Assim, das Equações (3.15) e (3.16) vamos ter no lugar Q_1

$$\frac{1}{Y} = -\alpha_1^q \mu_1^{q^2}\big(1-\mu_1^{-q^2+1}+\mathcal{O}(q^2)\big),$$

e portanto,

$$Y = -\frac{1}{\alpha_1^q}\cdot \mu_1^{-q^2}(1+\mu_1^{-q^2+1}+\mathcal{O}(q^2)).$$

Assim temos

$$Z_1 = \frac{Z_1}{Y}.Y = (\alpha_1^{q-1})^q\cdot \mu_1^{-q^2+q}-\mu_1^{-q^2+1}+\mathcal{O}(q^2)$$

(Aqui temos usado que $\alpha_1^{q^2-1}=1$). Logo temos que

$$(\mu_1^{q^2}+c_1\mu_1^{q^2-q+1})Z_1 - c_1^q\mu_1^q = \mathcal{O}(0) \ \text{ em } \ Q_1. \tag{3.17}$$

E das Equações (3.17) e (3.13) podemos concluir que

$$(Z_1^q+Z_1-1)f_1^q + Z_1\mu_1^{q(q-1)}f_1 = h,$$

onde $h\in\mathcal{O}_{Q_1}$. Mas $L_1 = E_{1,1}(f_1)$. Portanto, do item i) do Teorema 1.4.1, o lugar Q_1 não se ramifica em $L_1/E_{1,1}$ e concluimos a prova no Caso $i=1$.

Vejamos agora o Caso $i=2$. Novamente, da Proposição 1.3.7 e da transitividade dos índices de ramificação, nós temos que $v_{P_2}(X_1)=q^2(q-1)$, $v_{P_2}(X_2)=q(q-1)$, $v_{P_2}(X_3)=q(q-1)$, $v_{P_2}(X_4)=(q-1)$, e $v_{P_2}(Y)=q^2$. Logo $t_2=\dfrac{X_2X_4}{Y}$ satisfaz $v_{P_2}(t_2)=-1$ e então t_2^{-1} é parâmetro local em P_2.

Agora, notando que $t_2 = X_4t_1$, temos $t_1 = t_2^q/(t_2^{q-1}\cdot X_4)$. Usando as Equações (3.5), (3.6) e (3.7), obtemos

$$\frac{1}{X_4t_2^{q-1}} = \frac{Y^{q-1}}{X_2^q}\cdot\frac{X_2}{X_4^q} = \frac{(X_3+\alpha_2)^{q-1}(X_1+\alpha_1)^{q-1}(1+X_2)^{q-1}}{(1-Y)(X_4+1)}.$$

Daí, $t_1 = A_2^{q-1}(1-X_4)t_2^q+\mathcal{O}(0)$ em P_2.

Além disso, $X_4t_2^{q-1}(P_2) = (\alpha_1\alpha_2)^{1-q}$. Logo obtemos a fórmula de redução no item $2a$) para $i=2$, isto é, obtemos

$$t_1 = A_2^{q-1}\cdot t_2^q - t_2 + \mathcal{O}(0) \ \text{ em } \ P_2. \tag{3.18}$$

Das Equações (3.11) e (3.18) temos

$$\mu_1^q - \Big(\frac{X_1+\alpha_1}{X_1^q-\alpha_1}\Big)\mu_1 + \frac{1}{\alpha_1^q}\big(A_2^{q-1}\cdot t_2^q - t_2\big) = h' \in \mathcal{O}_{P_2}.$$

Assim temos

$$\big(\mu_1 + A_2\alpha_2 t_2\big)^q - (\frac{X_1+\alpha_1}{X_1^q-\alpha_1})(\mu_1 + A_2\alpha_2 t_2\big) + (\frac{X_1+\alpha_1}{X_1^q-\alpha_1})A_2\alpha_2 t_2 - \frac{1}{\alpha_1^q}\cdot t_2 = h'.$$

Pela própria definição da função μ_2 obtemos

$$\mu_2^q - (\frac{X_1+\alpha_1}{X_1^q-\alpha_1})\mu_2 - A_2 t_2 = h" \tag{3.19}$$

com $h"$ regular em P_2. Para finalizar o caso $i=2$ basta ver que a Equação (3.19) e a identidade que define μ_2, nos dão a seguinte equação:

$$\mu_1 = \alpha_2^q\mu_2 - \alpha_2\mu_2^q + \mathcal{O}(0) \ \text{ em } \ Q_2. \tag{3.20}$$

Seja agora $i \geq 2$ e suponha o resultado válido para $2 \leq k \leq i$. Vamos provar que o lema vale para $k = i+1$. O item (1) segue facilmente da hipótese de indução, do Lema de Abhyankar e da transitividade dos índices de ramificação. Para o item (2) notemos primeiramente que $t_{i+1} = X_{2(i+1)}t_i$. E portanto temos $v_{P_{i+1}}(t_{i+1}) = (q-1) - q = -1$. Assim a função t_{i+1}^{-1} é parâmetro local em P_{i+1}.

Agora veja que da hipótese de indução temos que

$$t_i \ = \ X_{2i}\cdot t_{i-1} = X_{2i}A_i^{q-1}\cdot t_i^q + \mathcal{O}(0) \ \text{ em } \ P_i$$

e, portanto, temos que

$$t_i \ = \ A_i^{q-1}\cdot\frac{X_{2i}}{X_{2(i+1)}^q}t_{i+1}^q + \mathcal{O}(0) \ \text{ em } \ P_{i+1}.$$

Das Equações (3.5) e (3.6) temos

$$\frac{X_{2i}}{X_{2(i+1)}^q} = \frac{(X_{2i}^q+1)(X_{2i+1}+\alpha_{i+1})^q}{(X_{2i+1}+\alpha_{i+1})(X_{2(i+1)}+1)}.$$

Logo $X_{2i}/X_{2(i+1)}^q = \beta_{i+1}^{q-1}(1 - X_{2(i+1)}) + \mathcal{O}(q)$ em P_{i+1} e, portanto,

$$\begin{aligned} t_i \ &= \ A_i^{q-1}\beta_{i+1}^{q-1}(1 - X_{2(i+1)})t_{i+1}^q + \mathcal{O}(0) \ \text{ em } \ P_{i+1} \text{ e, finalmente,} \\ t_i \ &= \ A_{i+1}^{q-1}t_{i+1}^q - t_{i+1} + \mathcal{O}(0) \ \text{ em } \ P_{i+1}, \end{aligned} \tag{3.21}$$

pois temos que $X_{2(i+1)}t_{i+1}^{q-1}(P_{i+1}) = \left(\frac{1}{\alpha_{i+1}}\right)^{q-1}\left(\frac{1}{\alpha_1\ldots\alpha_i}\right)^{q-1} = A_{i+1}^{1-q}$. De fato, pela indução temos

$$(X_{2i}t_i^{q-1})(P_i) = \left(\frac{1}{\alpha_1\ldots\alpha_i}\right)^{q-1}.$$

O passo inicial sai da igualdade $\dfrac{X_2^q}{Y^{q-1}} = \dfrac{(X_2+1)(1-Y)}{(X_1+\alpha_1)^{q-1}}$, que foi usada na demonstração do item $2b$) para o caso $i=1$. Agora, temos também que

$$X_{2(i+1)}t_{i+1}^{q-1} = \frac{X_{2(i+1)}^q}{X_{2i}}.(t_i^{q-1}X_{2i})$$

e ainda que $\dfrac{X_{2(i+1)}^q}{X_{2i}}(P_{i+1}) = \left(\dfrac{1}{\alpha_{i+1}}\right)^{q-1}$. Isto termina a prova do item $(2a)$.

Da hipótese de indução temos

$$\mu_i^q - \left(\frac{X_1+\alpha_1}{X_1^q-\alpha_1}\right)\mu_i + (-1)^{i+1}A_i t_i = h \in \mathcal{O}_{P_i}.$$

Da Equação (3.21) obtemos

$$\mu_i^q - \left(\frac{X_1+\alpha_1}{X_1^q-\alpha_1}\right)\mu_i + (-1)^{i+1}A_i\big(A_{i+1}^{q-1}t_{i+1}^q - t_{i+1}\big) = h' \in \mathcal{O}_{P_{i+1}}.$$

Logo,

$$\left(\mu_i + (-1)^{i+1}A_i\left(\frac{1}{\alpha_{i+1}}\right)^{q-1} t_{i+1}\right)^q - \left(\frac{X_1+\alpha_1}{X_1^q-\alpha_1}\right)\left(\mu_i + (-1)^{i+1}A_i\left(\frac{1}{\alpha_{i+1}}\right)^{q-1}\cdot t_{i+1}\right) +$$

$$+\left(\frac{X_1+\alpha_1}{X_1^q-\alpha_1}\right)(-1)^{i+1}A_i\left(\frac{1}{\alpha_{i+1}}\right)^{q-1}\cdot t_{i+1} + (-1)^i A_i\cdot t_{i+1} = h' \in \mathcal{O}_{P_{i+1}}.$$

Obtemos então que

$$\begin{aligned}\big(\mu_i + (-1)^{i+1}A_{i+1}\alpha_{i+1}t_{i+1}\big)^q - \left(\frac{X_1+\alpha_1}{X_1^q-\alpha_1}\right)\big(\mu_i + (-1)^{i+1}A_{i+1}\alpha_{i+1}t_{i+1}\big) +\\ +(-1)^{i+2}A_{i+1}t_{i+1} = h'' \in \mathcal{O}_{P_{i+1}},\end{aligned}$$

ou seja,

$$\mu_{i+1}^q - \left(\frac{X_1+\alpha_1}{X_1^q-\alpha_1}\right)\mu_{i+1} + (-1)^{i+2}A_{i+1}t_{i+1} = h'', \tag{3.22}$$

com h'' regular em P_{i+1}. Da Equação (3.22) e da identidade que define μ_{i+1} obtemos o item 2c), isto é, obtemos que

$$\mu_i = \alpha_{i+1}^q\mu_{i+1} - \alpha_{i+1}\mu_{i+1}^q + \mathcal{O}(0) \text{ em } Q_{i+1}. \tag{3.23}$$

Isto conclui a prova do Lema 3.2.3.

■

Passamos então agora ao Caso $j \geq 2$. No lema abaixo ainda vamos denotar $c_1 = \alpha_1^{q-1}$.

Lema 3.2.4. *(Caso $j \geq 2$) Seja $P_{i,j} \in \mathbb{P}_{H_{i,j}}$ um zero de Y (portanto, um zero comum de $X_1, ..., X_{2i}, Z_1, ..., Z_{2(j-1)}$), e seja $Q_{i,j} \in \mathbb{P}_{E_{i,j}}$ um lugar acima de $P_{i,j}$. Então*

1) As ordens de zero em $P_{i,j}$ das funções X_k, Y e Z_k são

$$v_{P_{i,j}}(X_k) = \begin{cases} q^{j-1} \cdot q^{i-\frac{k-1}{2}}(q-1) & \text{para } k \text{ ímpar com } 1 \leq k \leq 2i \\ q^{j-1} \cdot q^{i-\frac{k}{2}}(q-1) & \text{para } k \text{ par com } 1 \leq k \leq 2i, \end{cases}$$

$$v_{P_{i,j}}(Y) = q^{j-1} \cdot q^i \ \text{ e } \ v_{P_{i,j}}(Z_k) = q^{j-1} \cdot q^{i-k}(q-1) \text{ para } 1 \leq k \leq 2(j-1).$$

2) Defina $\xi_{i,1} := \mu_i \in E_{i,1}$ e, para $j \geq 2$, defina a função $\xi_{i,j}$ em $E_{i,j}$

$$\xi_{i,j} := \begin{cases} Z_{2j-1} \cdot \xi_{j-1,j-1} + c_1^q \cdot \alpha_2^q \cdot \xi_{j,j-1} & \text{se } i = j \\ \\ \xi_{i-1,j} + (\alpha_{i-j+1} \cdot \alpha_{i-j+2}^q / \alpha_1^q) \cdot \xi_{i,j-1} & \text{se } i > j. \end{cases}$$

Então:

a) $E_{i,j} = H_{i,j}(\xi_{i,j})$, e a função $\xi_{i,j}^{-1}$ é um parâmetro local em $Q_{i,j}$(logo também um parâmetro local em $P_{i,j+1}$ no caso $i > j$). Além disso, a função $\xi_{i,j}$ satisfaz uma equação do tipo

$$(Z_{2j-2}^q + Z_{2j-2} - 1)\xi_{i,j}^q + (Z_{2j-2} \cdot \xi_{j-1,j-1}^{q-1})\xi_{i,j} + \frac{\alpha_{i-j+2}^q}{\alpha_1} \cdot c_1^{j-2} \cdot \xi_{i,j-1} = h,$$

para alguma função $h \in H_{i,j}$ regular em $P_{i,j}$. Logo o lugar $P_{i,j}$ é totalmente ramificado na extensão $E_{i,j}/H_{i,j}$.

b) Existe $h \in E_{i+1,j}$ regular em $Q_{i+1,j}$ tal que

$$\xi_{i,j} = \alpha_{i-j+2}^q \cdot \xi_{i+1,j} - \frac{\alpha_{i-j+2}}{c_1^{j-1}} \cdot \xi_{i+1,j}^q + h.$$

c) A função $f_j := Z_{2j} \cdot \xi_{j,j}^q + c_1^j \cdot \xi_{j,j} \in L_j$ é regular nos lugares de L_j acima de $Q_{j,j}$ e satisfaz uma equação do tipo:

$$(Z_{2j-1}^q + Z_{2j-1} - 1)f_j^q + (Z_{2j-1} \cdot \xi_{j,j}^{q(q-1)})f_j = h,$$

para alguma função $h \in E_{j,j}$ regular em $Q_{j,j}$. Em particular, temos que o lugar $Q_{j,j}$ é não-ramificado em $L_j/E_{j,j}$ e, para $i \geq j+1$, temos que $Q_{i,j}$ é não-ramificado em $H_{i,j+1}/E_{i,j}$.

Demonstração: Como é de se esperar, faremos a prova do Lema 3.2.4 por indução sobre j. O passo inicial dessa indução, isto é, o caso $j = 2$, será tratado inicialmente e será demonstrado por indução em i.

Caso $j = 2$:

Novamente, para facilitar as notações, vamos denotar $P_i := P_{i,2}$, $Q_i := Q_{i,2}$ e ainda $\xi_i := \xi_{i,2}$. Note que μ_i^{-1} é parâmetro local em P_i pois P_i não se ramifica na extensão $H_{i,2}/E_{i,1}$ para $i \geq 2$ (Lema 3.2.3).

O item 1) no caso $j = 2$ e $i \geq 2$ qualquer segue diretamente do Lema 3.2.3.

Para o item 2), observemos primeiramente que segue do Lema 3.2.3 que a função $Z_2\mu_1^q + c_1\mu_1$, com $c_1 = \alpha_1^{q-1}$, é regular nos lugares de L_1 acima de $Q_{1,1}$. Logo regular também em P_2, e portanto temos $Z_2\mu_1^q = -c_1\mu_1 + \mathcal{O}(0)$ em P_2.

A Equação (3.9) para $i = 2$ nos dá

$$(Z_2^q + Z_2 - 1)Z_3^q + Z_2Z_3 - Z_2 = 0.$$

Multiplicando esta equação por μ_1^q temos

$$\begin{aligned}(Z_2^q + Z_2 - 1)(Z_3\mu_1)^q + Z_2\mu_1^{q-1}(Z_3\mu_1) - Z_2\mu_1^q = 0 \text{ , e logo}\\ (Z_2^q + Z_2 - 1)(Z_3\mu_1)^q + Z_2\mu_1^{q-1}(Z_3\mu_1) + c_1\mu_1 = h \in \mathcal{O}_{P_2}.\end{aligned}$$

Usando o item $2c$) do Lema 3.2.3 temos

$$(Z_2^q + Z_2 - 1)(Z_3\mu_1)^q + Z_2\mu_1^{q-1}(Z_3\mu_1) - c_1\alpha_2\mu_2^q + c_1\alpha_2^q\mu_2 = h', \text{com } h' \in \mathcal{O}_{P_2}.$$

Como $(Z_2^q + Z_2).\mu_2^q$ é regular em P_2, obtemos

$$\begin{aligned}(Z_2^q + Z_2 - 1)(Z_3\mu_1 + c_1^q\alpha_2^q\mu_2)^q + Z_2\mu_1^{q-1}(Z_3\mu_1 + c_1^q\alpha_2^q\mu_2) -\\ - Z_2\mu_1^{q-1}c_1^q\alpha_2^q\mu_2 + c_1\alpha_2^q\mu_2 = h'' \in \mathcal{O}_{P_2}.\end{aligned}$$

Temos $v_{P_2}(\mu_1) = -q$ e assim $v_{P_2}(Z_2\mu_1^{q-1}) = 0$. Como $(Z_2\mu_1^{q-1} + c_1)\mu_1$ é regular em P_2, temos que $(Z_2\mu_1^{q-1})(P_2) = -c_1$ e, então,

$$(Z_2^q + Z_2 - 1)\xi_2^q + Z_2\mu_1^{q-1} \cdot \xi_2 + \frac{\alpha_2^q}{\alpha_1} \cdot \mu_2 = h''', \tag{3.24}$$

com $v_{P_2}(\mu_2) = -1$ e $h''' \in \mathcal{O}_{P_2}$. Assim ξ_2^{-1} é um parâmetro local em Q_2 e concluimos o item $2a$) no caso $i = 2$. Usando novamente o fato de que $Z_2\mu_1^{q-1}(P_2) = -c_1$, temos da Equação (3.24) que

$$\alpha_2^q\mu_2 = \alpha_1\xi_2^q + \alpha_1c_1\xi_2 + \mathcal{O}(0) \text{ em } Q_2. \tag{3.25}$$

Também do Lema 3.2.3, pela *fórmula de redução* do item (c), temos a igualdade $\mu_1 = \alpha_2^q\mu_2 - (\alpha_2^q\mu_2)^q + \mathcal{O}(0)$ em Q_2. Substituindo a Equação (3.25) nesta última igualdade e na identidade que define ξ_2, temos respectivamente:

$$\mu_1 = -\alpha_1^q\xi_2^{q^2} + \alpha_1^q\xi_2 + \mathcal{O}(0) \text{ em } Q_2 \text{ e} \tag{3.26}$$

$$Z_3 \cdot \mu_1 = \alpha_1^q\xi_2 - c_1^q\alpha_1\xi_2^q + \mathcal{O}(0) \text{ em } Q_2. \tag{3.27}$$

Da Equação (3.26) temos

$$\mu_1 = -\alpha_1^q \xi_2^{q^2}\big(1 - \xi_2^{1-q^2} + \mathcal{O}(q^2)\big) \text{ em } Q_2 \text{ e, logo,}$$
$$\mu_1^{-1} = -\left(\frac{1}{\alpha_1}\right)^q \xi_2^{-q^2}\big(1 + \xi_2^{1-q^2} + \mathcal{O}(q^2)\big) \text{ em } Q_2.$$

Agora, da Equação (3.27) obtemos

$$Z_3 = (Z_3\mu_1)\mu_1^{-1} = c_1^{q-1}\xi_2^{-(q^2-q)} - \xi_2^{-(q^2-1)} + \mathcal{O}(q^2) \text{ em } Q_2. \tag{3.28}$$

Da Equação (3.9), para $i = 3$, temos que

$$(Z_3^q + Z_3 - 1)(Z_4\xi_2^q)^q + (Z_3\xi_2^{q(q-1)})(Z_4\xi_2^q) - Z_3\xi_2^{q^2} = 0.$$

Como $(Z_3^q + Z_3).\xi_2^q$ é regular em Q_2, obtemos

$$\begin{aligned}(Z_3^q + Z_3 - 1)(Z_4\xi_2^q + c_1^2\xi_2)^q + (Z_3\xi_2^{q(q-1)})(Z_4\xi_2^q + c_1^2\xi_2) + \\ + c_1^{2q}\xi_2^q - Z_3(c_1^2\xi_2^{q^2-q+1} + \xi_2^{q^2}) = h\end{aligned} \tag{3.29}$$

com $h \in \mathcal{O}_{Q_2}$. Mas, da Equação (3.28) nós temos

$$\begin{aligned} Z_3.(c_1^2\xi_2^{q^2-q+1} + \xi_2^{q^2}) &= \big[c_1^{q-1}\xi_2^{-(q^2-q)} - \xi_2^{-(q^2-1)} + \mathcal{O}(q^2)\big].(c_1^2\xi_2^{q^2-q+1} + \xi_2^{q^2}) \\ &= c_1^{q-1}\xi_2^q + \mathcal{O}(0) = (c_1^2\xi_2)^q + \mathcal{O}(0) \text{ em } Q_2. \end{aligned}$$

Logo, da Equação (3.29) temos o item $2c)$ do Lema 3.2.4, isto é,

$$(Z_3^q + Z_3 - 1)(Z_4\xi_2^q + c_1^2\xi_2)^q + \xi_2^{q(q-1)}Z_3(Z_4\xi_2^q + c_1^2\xi_2) = \tilde{h},$$

onde $\tilde{h} \in E_{2,2}$ é regular em Q_2. Daí $f_2 := Z_4\xi_2^q + c_1^2\xi_2 \in L_2$ é regular nos lugares acima de Q_2 e o lugar Q_2 é não-ramificado em $L_2/E_{2,2}$ pelo Teorema de Kummer.

A hipótese de indução nos diz que

$$(Z_2^q + Z_2 - 1)\xi_i^q + Z_2\mu_1^{q-1}\xi_i + \frac{\alpha_i^q}{\alpha_1}\mu_i = h$$

com $h \in \mathcal{O}_{P_i}$. Pelo item $2c)$ do Lema 3.2.3, temos que $\mu_i = \alpha_{i+1}^q\mu_{i+1} - \alpha_{i+1}\mu_{i+1}^q + \mathcal{O}(0)$ em P_{i+1}, para $i \geq 1$. Assim temos

$$(Z_2^q + Z_2 - 1)\xi_i^q + Z_2\mu_1^{q-1}\xi_i + \frac{\alpha_i^q}{\alpha_1}\big(\alpha_{i+1}^q\mu_{i+1} - \alpha_{i+1}\mu_{i+1}^q\big) = h' \in \mathcal{O}_{P_{i+1}}.$$

Como $(Z_2^q + Z_2).\mu_{i+1}^q$ é regular em P_{i+1}, temos

$$\begin{aligned}(Z_2^q + Z_2 - 1)\left(\xi_i + \frac{\alpha_i}{\alpha_1^q}\alpha_{i+1}^q\mu_{i+1}\right)^q + Z_2\mu_1^{q-1}\left(\xi_i + \frac{\alpha_i}{\alpha_1^q}\alpha_{i+1}^q\mu_{i+1}\right) - \\ - Z_2\mu_1^{q-1}\frac{\alpha_i}{\alpha_1^q}\alpha_{i+1}^q\mu_{i+1} + \frac{\alpha_i^q}{\alpha_1}\alpha_{i+1}^q\mu_{i+1} = h'' \in \mathcal{O}_{P_{i+1}}.\end{aligned}$$

Usando novamente que $(Z_2\mu_1^{q-1})(P_2) = -c_1$, concluimos o item $2a)$, isto é,

$$(Z_2^q + Z_2 - 1)\xi_{i+1}^q + Z_2\mu_1^{q-1}\xi_{i+1} + \frac{\alpha_{i+1}^q}{\alpha_1}\mu_{i+1} = h''' \in \mathcal{O}_{P_{i+1}}.$$

Como μ_{i+1} tem pólo simples em P_{i+1}, temos que P_{i+1} é totalmente ramificado e que ξ_{i+1}^{-1} é parâmetro local em Q_{i+1}. Logo, temos

$$\xi_{i+1}^q + c_1\xi_{i+1} - \frac{\alpha_{i+1}^q}{\alpha_1}\mu_{i+1} = \mathcal{O}(0) \text{ em } Q_{i+1}. \tag{3.30}$$

A Equação (3.25) é esta Equação (3.30) para $i = 1$.

Finalmente, da Equação (3.30) e da identidade que define ξ_{i+1} para $i \geq 2$, temos o item $2b)$ do Lema 3.2.4 no caso $j = 2$, isto é,

$$\xi_i = \alpha_i^q\xi_{i+1} - \frac{\alpha_i}{c_1}\xi_{i+1}^q + \mathcal{O}(0) \text{ em } Q_{i+1}. \tag{3.31}$$

E assim terminamos a prova do Lema 3.2.4 para o Caso $j = 2$.

Caso $j > 2$:

Como já foi mencionado, faremos a prova por indução sobre $j \geq 2$. Supomos então o lema válido para $j \geq 2$ e provamos o lema para $j+1$.

O item 1) para $j+1$ segue diretamente da hipótese de indução, mais concretamente, segue da validade do lema para j.

Também, da hipótese de indução, segue que $f_j := Z_{2j} \cdot \xi_{j,j}^q + c_1^j \cdot \xi_{j,j}$ é regular em $P_{i,j+1}$ para $i \geq j+1$, e que

$$\xi_{i,j} = \alpha_{i-j+2}^q \cdot \xi_{i+1,j} - \frac{\alpha_{i-j+2}}{c_1^{j-1}} \cdot \xi_{i+1,j}^q + \mathcal{O}(0) \text{ em } P_{i+1,j+1}.$$

Destas afirmações nós obtemos que para $i \geq j$ temos

$$Z_{2j} \cdot \xi_{j,j}^q = -c_1^j \cdot \xi_{j,j} + h \tag{3.32}$$

$$\xi_{i,j} = \alpha_{i-j+2}^q \cdot \xi_{i+1,j} - \frac{\alpha_{i-j+2}}{c_1^{j-1}} \cdot \xi_{i+1,j}^q + h', \tag{3.33}$$

com h e h' regulars em $P_{i+1,j+1}$. Da Equação (3.9) com $i = 2j$ e da Equação (3.32), temos

$$(Z_{2j}^q + Z_{2j} - 1)(Z_{2j+1} \cdot \xi_{j,j})^q + Z_{2j}\xi_{j,j}^{q-1}(Z_{2j+1} \cdot \xi_{j,j}) + c_1^j \cdot \xi_{j,j} = \mathcal{O}(0) \text{ em } P_{j+1,j+1}.$$

Usando agora a Equação (3.33) com $i = j$ temos

$$\begin{aligned}(Z_{2j}^q + Z_{2j} - 1)(Z_{2j+1} \cdot \xi_{j,j})^q + Z_{2j}\xi_{j,j}^{q-1}(Z_{2j+1} \cdot \xi_{j,j}) +& \\ + c_1^j\alpha_2^q \cdot \xi_{j+1,j} - c_1\alpha_2 \cdot \xi_{j+1,j}^q &= \mathcal{O}(0) \text{ em } P_{j+1,j+1}.\end{aligned}$$

Como $\xi_{j+1,j}$ tem pólo simples no lugar $P_{j+1,j+1}$, como a função $(Z_{2j}^q + Z_{2j})\xi_{j+1,j}^q$ é regular neste lugar e como $Z_{2j}.\xi_{j,j}^{q-1}(P_{j+1,j+1}) = -c_1^j$ temos

$$(Z_{2j}^q + Z_{2j} - 1)(Z_{2j+1} \cdot \xi_{j,j} + c_1^q \alpha_2^q \cdot \xi_{j+1,j})^q + Z_{2j}\xi_{j,j}^{q-1} \cdot (Z_{2j+1} \cdot \xi_{j,j} + c_1^q \alpha_2^q \cdot \xi_{j+1,j}) + \\ + c_1^j \alpha_2^q \cdot \xi_{j+1,j} + c_1^j c_1^q \cdot \alpha_2^q \cdot \xi_{j+1,j} = h \in \mathcal{O}_{P_{j+1,j+1}}.$$

E portanto, existe h regular em $P_{j+1,j+1}$ tal que

$$(Z_{2j}^q + Z_{2j} - 1)\xi_{j+1,j+1}^q + (Z_{2j}\xi_{j,j}^{q-1}) \cdot \xi_{j+1,j+1} + \frac{\alpha_2^q}{\alpha_1}.c_1^{j-1}.\xi_{j+1,j} = h. \tag{3.34}$$

E da Equação (3.33) nós obtemos indutivamente, para $i \geq j+1$, o item $2a$), isto é, temos a igualdade:

$$(Z_{2j}^q + Z_{2j} - 1)\xi_{i,j+1}^q + (Z_{2j}\xi_{j,j}^{q-1})\xi_{i,j+1} + \frac{\alpha_{i-j+1}^q}{\alpha_1} \cdot c_1^{j-1} \cdot \xi_{i,j} = \tilde{h},$$

onde $\tilde{h}$ é regular em $P_{i,j+1}$. De fato, da última igualdade e da Equação (3.33), nós temos que a função

$$(Z_{2j}^q + Z_{2j} - 1)\xi_{i,j+1}^q + (Z_{2j}\xi_{j,j}^{q-1})\xi_{i,j+1} + \frac{\alpha_{i-j+1}^q}{\alpha_1} c_1^{j-1}\big(\alpha_{i-j+2}^q \cdot \xi_{i+1,j} - \frac{\alpha_{i-j+2}}{c_1^{j-1}} \cdot \xi_{i+1,j}^q\big)$$

é regular em $P_{i+1,j+1}$. Daí, como $\xi_{i+1,j}$ tem pólo simples no lugar $P_{i+1,j+1}$, como a função $(Z_{2j}^q + Z_{2j})\xi_{i+1,j}^q$ é regular neste lugar e como $Z_{2j}.\xi_{j,j}^{q-1}(P_{j+1,j+1}) = -c_1^j$, rearrumando esta última equação e usando a definição da função $\xi_{i+1,j+1}$ obtemos:

$$(Z_{2j}^q + Z_{2j} - 1)\xi_{i+1,j+1}^q + (Z_{2j}\xi_{j,j}^{q-1})\xi_{i+1,j+1} + \frac{\alpha_{(i+1)-j+1}^q}{\alpha_1} \cdot c_1^{j-1} \cdot \xi_{i+1,j} = h''',$$

onde h''' é regular em $P_{i+1,j+1}$. Isto termina a prova do item $2a$).

Passamos agora ao item $2b$). Do item $2a$) e como $\xi_{i,j-1}$ tem pólo simples em $P_{i,j}$, obtemos que a função

$$\xi_{i,j}^q + c_1^{j-1} \cdot \xi_{i,j} - \frac{\alpha_{i-j+2}^q}{\alpha_1} c_1^{j-2} \cdot \xi_{i,j-1} \tag{3.35}$$

é regular em $Q_{i,j}$. Note que a Equação (3.30) é a Equação (3.35) no caso $j = 2$.

Finalmente, analogamente ao Caso $j = 2$, da Equação (3.35) com i substituido por $i+1$ e da definição de $\xi_{i+1,j}$ para $i \geq j$, concluimos a prova do item $2b$); isto é, temos que

$$\xi_{i,j} = \alpha_{i-j+2}^q \cdot \xi_{i+1,j} - \frac{\alpha_{i-j+2}}{c_1^{j-1}} \cdot \xi_{i+1,j}^q + h,$$

com h regular em $Q_{i+1,j}$.

Para facilitar as expressões que seguem vamos denotar $\eta_i := \xi_{i,i}$.

Da Equação (3.34) nós temos que $\eta_{j+1}^{-1} = \xi_{j+1,j+1}^{-1}$ é um parâmetro local em $Q_{j+1,j+1}$, e assim

$$\eta_{j+1}^q + c_1^j \cdot \eta_{j+1} - c_1^{j-1} \cdot \frac{\alpha_2^q}{\alpha_1} \cdot \xi_{j+1,j} = \tilde{h} \tag{3.36}$$

com $\tilde{h}$ regular em $Q_{j+1,j+1}$. Note que a Equação (3.25) é esta Equação (3.36) com $j = 1$. Segue também da hipótese de indução que temos a seguinte igualdade $\eta_j = \xi_{j,j} = \alpha_2^q \xi_{j+1,j} - \dfrac{\alpha_2}{c_1^{j-1}} \xi_{j+1,j}^q + h$, onde h é regular em $Q_{j+1,j+1}$. Logo, desta última igualdade e da Equação (3.36) nós obtemos

$$\begin{aligned} \eta_j &= -\alpha_1^q \cdot \eta_{j+1}^{q^2} + \alpha_1^q \cdot \eta_{j+1} + \mathcal{O}(0) \\ &= -\alpha_1^q \cdot \eta_{j+1}^{q^2}\big(1 - \eta_{j+1}^{1-q^2} + \mathcal{O}(q^2)\big) \text{ em } Q_{j+1,j+1}. \end{aligned}$$

Portanto temos

$$\eta_j^{-1} = -\frac{1}{\alpha_1^q} \cdot \eta_{j+1}^{-q^2}\big(1 + \eta_{j+1}^{1-q^2} + \mathcal{O}(q^2)\big) \text{ em } Q_{j+1,j+1}\ .$$

Como $Z_{2j+1} \cdot \eta_j = \eta_{j+1} - c_1^q \alpha_2^q \cdot \xi_{j+1,j}$ e usando a Equação (3.36) nós obtemos

$$Z_{2j+1} \cdot \eta_j = \eta_{j+1} - c_1^q \alpha_2^q \left(\frac{\alpha_1}{\alpha_2^q c_1^{j-1}} \eta_{j+1}^q + \frac{\alpha_1^q}{\alpha_2^q} \eta_{j+1} \right) + \mathcal{O}(0) \text{ em } Q_{j+1,j+1}$$

e assim temos a igualdade

$$Z_{2j+1} \cdot \eta_j = \alpha_1^q \eta_{j+1} - c_1^q \frac{\alpha_1}{c_1^{j-1}} \eta_{j+1}^q + h,$$

com h regular em $Q_{j+1,j+1}$. Multiplicando esta última igualdade por η_j^{-1} temos

$$\begin{aligned} Z_{2j+1} &= -\left(\eta_{j+1}^{1-q^2} - \frac{c_1^q}{c_1^j} \cdot \eta_{j+1}^{q-q^2} + \mathcal{O}(q^2) \right) \big(1 + \eta_{j+1}^{1-q^2} + \mathcal{O}(q^2)\big) \\ &= -\eta_{j+1}^{1-q^2} + \frac{c_1^q}{c_1^j} \cdot \eta_{j+1}^{q-q^2} + \mathcal{O}(q^2) \text{ em } Q_{j+1,j+1}. \end{aligned} \tag{3.37}$$

Agora, da Equação (3.9), para $i = 2j+1$, temos que

$$\begin{aligned} (Z_{2j+1}^q + Z_{2j+1} - 1)(Z_{2j+2} \cdot \eta_{j+1}^q)^q + (Z_{2j+1} \cdot \eta_{j+1}^{q(q-1)})(Z_{2j+2} \cdot \eta_{j+1}^q) - \\ - Z_{2j+1} \cdot \eta_{j+1}^{q^2} = 0. \end{aligned}$$

Como anteriormente obtemos

$$\begin{aligned} (Z_{2j+1}^q + Z_{2j+1} - 1)(Z_{2j+2} \cdot \eta_{j+1}^q + c_1^{j+1} \cdot \eta_{j+1})^q + (Z_{2j+1} \cdot \eta_{j+1}^{q(q-1)})\big(Z_{2j+2} \cdot \eta_{j+1}^q + \\ + c_1^{j+1} \cdot \eta_{j+1}\big) + c_1^{(j+1)q} \cdot \eta_{j+1}^q - Z_{2j+1}(c_1^{j+1} \cdot \eta_{j+1}^{q^2-q+1} + \eta_{j+1}^{q^2}) = \tilde{h} \end{aligned}$$

com $\tilde{h} \in \mathcal{O}_{Q_{j+1,j+1}}$. Mas, da Equação (3.37), se $z_{j+1} = Z_{2j+1}.(c_1^{j+1} \cdot \eta_{j+1}^{q^2-q+1} + \eta_{j+1}^{q^2})$, nós temos

$$\begin{aligned} z_{j+1} &= -\left(\eta_{j+1}^{1-q^2} - \frac{c_1^q}{c_1^j} \cdot \eta_{j+1}^{q-q^2} + \mathcal{O}(q^2)\right).(c_1^{j+1} \cdot \eta_{j+1}^{q^2-q+1} + \eta_{j+1}^{q^2}) \\ &= \frac{c_1^q}{c_1^j} \cdot \eta_{j+1}^q + \mathcal{O}(0) \text{ em } Q_{j+1,j+1}. \end{aligned}$$

Como $f_{j+1} := Z_{2j+2} \cdot \eta_{j+1}^q + c_1^{j+1} \cdot \eta_{j+1}$, temos

$$(Z_{2j+1}^q + Z_{2j+1} - 1)f_{j+1}^q + \eta_{j+1}^{q(q-1)} \cdot Z_{2j+1} \cdot f_{j+1} = h$$

com h é regular em $Q_{j+1,j+1}$. E assim, concluimos que $Q_{j+1,j+1}$ é não-ramificado em $L_{j+1}/E_{j+1,j+1}$. Terminamos assim a prova do Lema 3.2.4. ■

Com a notação do Teorema 3.2.2 temos os seguintes corolários deste teorema:

Corolário 3.2.5. *Se o lugar $R_k \in \mathbb{P}_{L_k}$ é um zero da função Y, então nós temos que $e(R_k|R_k \cap k(x_{t'+1+2k})) = q - 1$.*

Demonstração: De fato, do Lema 3.2.4 temos a igualdade $v_{P_{k,k}}(Z_{2(k-1)}) = q^{k-1} \cdot q^{k-2(k-1)}(q-1) = q(q-1)$. Assim, se $Q_{k,k} \in E_{k,k}$ é o lugar acima de $P_{k,k}$, segue ainda do Lema 3.2.4 que $v_{Q_{k,k}}(Z_{2(k-1)}) = q^2(q-1)$, e portanto obtemos que $v_{R_k}(Z_{2(k-1)}) = q^2(q-1)$. Agora, da Equação (3.9) temos que

$$\frac{1 - Z_{2k-1}}{Z_{2k-1}^q} = \frac{Z_{2k-2}^q + Z_{2k-2} - 1}{Z_{2k-2}}$$

se $k > 1$, e

$$\frac{1 - Z_{2k}}{Z_{2k}^q} = \frac{Z_{2k-1}^q + Z_{2k-1} - 1}{Z_{2k-1}}.$$

E destas igualdades concluimos que $v_{R_k}(Z_{2k-1}) = q(q-1)$ e $v_{R_k}(Z_{2k}) = q - 1$. Mas $v_{R_k}(Z_{2k}) = e(R_k|R_k \cap k(x_{t'+1+2k}))$, pois, por definição, temos $Z_{2k} = x_{t'+1+2k}$. ■

Corolário 3.2.6. *Para cada $1 \leq j \leq i$ nós temos que:*

i) Existem exatamente q^{i+j-1} pólos da função $x_{t'+1}$ em $H_{i,j}$.

ii) Existem exatamente q^{2j} pólos da função $x_{t'+1}$ em L_j.

Demonstração: De fato, seja A o número de pólos da função $x_{t'+1}$ em $H_{i,j}$. Dos Lemas 3.2.3 e 3.2.4, nós temos que todos os pólos $P_{i,j}$ de $x_{t'+1}$ em $H_{i,j}$ têm a mesma ordem de pólo igual a q^{i+j-1}. Portanto, da igualdade fundamental nós temos

$$q^{2i+2j-2} = [H_{i,j} : K(x_{t'+1})] = A \cdot e\left(P_{i,j}|P_{i,j} \cap k(x_{t'+1})\right) = A \cdot q^{i+j-1}.$$

E o item i) segue imeditamente desta última igualdade.

Para o item ii) veja que do Teorema 3.2.2, os lugares de $H_{i,j}$ que são pólos da função $x_{t'+1}$ (ou zeros da função Y) são totalmente ramificados na extensão $E_{i,j}/H_{i,j}$, o que não altera a quantidade de pólos da função $x_{t'+1}$ em $E_{i,j}$. Daí, segue do item anterior que existem exatamente q^{i+j-1} pólos da função $x_{t'+1}$ em $E_{i,j}$. Além disso, ainda do Teorema 3.2.2, segue que os pólos da função $x_{t'+1}$ em $E_{j,j}$ são não-ramificados na extensão $L_j/E_{j,j}$. E assim, existem exatamente q^{2j} pólos da função $x_{t'+1}$ em L_j. ∎

3.3 O limite da torre

3.3.1 O gênero da torre

Seguimos agora para o cálculo do gênero de cada passo F_n da torre $\mathcal{F}$ em questão. Para determinarmos o grau da diferente vamos precisar calcular a quantidade de lugares do tipo (C) e o expoente da diferente destes lugares.

Lema 3.3.1. *Seja $1 \leq t' < n$ e $Q \in \mathbb{P}_{F_n}$ um lugar do tipo* (C)*, isto é, um lugar tendo as seguintes propriedades:*

(1) Existe uma t'-upla $(\alpha_1, ..., \alpha_{t'})$ de elementos de $\mathbb{F}_{q^2}$ alternando-se $1's$ e elementos de R, com $\alpha_{t'} \in R$ e tal que o lugar Q é zero das funções $x_i - \alpha_i$ para $1 \leq i \leq t'$;

(2) Q é pólo da função $x_{t'+1}$;

(3) Q é zero das funções $x_{t'+2}, ..., x_n$.

Se $n > 2t' + 1$, então existem $q^{t'}$ lugares do tipo (C) *e cada lugar Q deste tipo é totalmente ramificado em F_n/F_{n-1}. Além disso, para $2t' + 1 \leq s \leq n$ a restrição de Q a F_s tem índice de ramificação $q - 1$ na extensão $F_s/k(x_s)$ e o expoente da diferente $d(Q)$ de Q na extensão F_n/F_{n-1} é dado por $d(Q) = 2(q - 1)$.*

Demonstração: Para provar este lema nós temos que distinguir dois casos: o caso t' par e o caso t' ímpar. Suponhamos primeiramente que $t' = 2t$ é par e provemos o resultado usando indução sobre $n \geq 2t' + 2$. Seguindo a notação do Teorema 3.2.2, temos que $F_{2t'+1} = L_t$. E portanto, do Corolário 3.2.6 e do Teorema 3.2.2, nós temos que existem q^{2t} pólos de $x_{t'+1}$ em $F_{2t'+1}$. Além disso, segue do Corolário 3.2.5 a seguinte pirâmide para a restrição de Q a $F_{2t'+2}$:

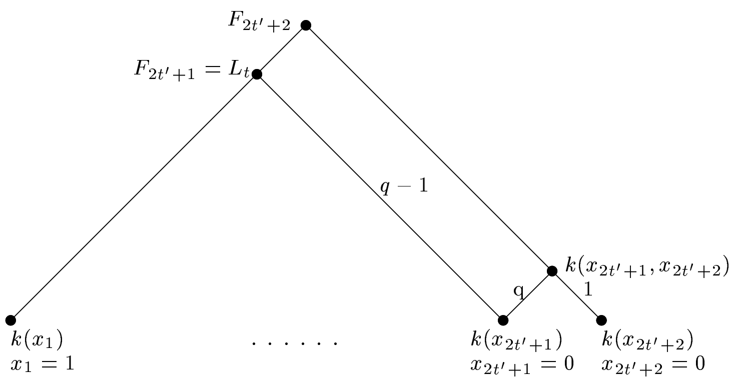

Figura 3.4: $t' = 2t$

Logo, da Proposição 1.3.7 e do Lema 3.1.3, segue o resultado para $n = 2t'+2$. Supondo agora o lema válido para $n \geq 2t' + 2$ nós temos facilmente o lema para $n + 1$ utilizando novamente a Proposição 1.3.7 e o Lema 3.1.3.

Agora, para $n > 2t' + 1$ e $t' = 2t + 1 > 1$ ímpar (o caso $t' = 1$ foi discutido após a demonstração do Lema 3.2.1), temos $k(x_2, ..., x_{4t+2}) = L_t$. Segue do caso anterior (t' par) que a restrição de Q a $k(x_2, ..., x_s)$ é totalmente ramificada na extensão $k(x_2, ..., x_s)/k(x_2, ..., x_{4t+2})$, tem índice de ramificação $q - 1$ na extensão $k(x_2, ..., x_s)/k(x_s)$, e que o expoente da diferente desta restrição na extensão $k(x_2, ..., x_n)/k(x_2, ..., x_{n-1})$ é $2(q - 1)$, para cada $2t' < s \leq n$. O resultado segue então da seguinte pirâmide:

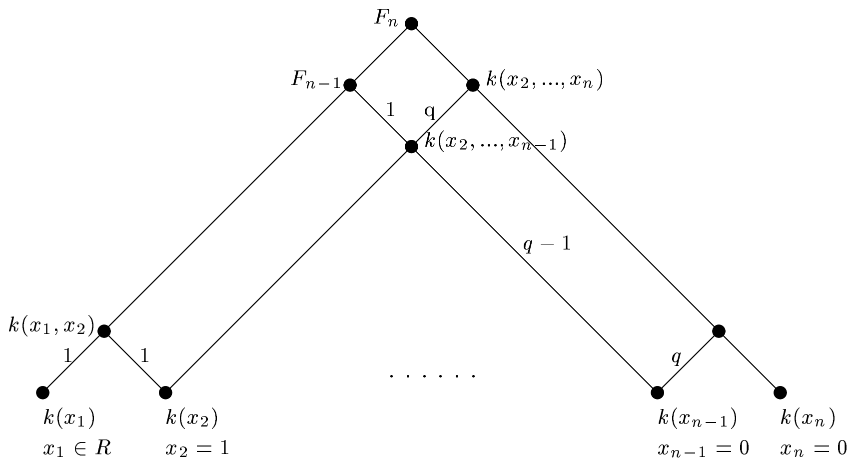

Figura 3.5: $t' = 2t + 1$

De fato, da Proposição 1.3.7, segue que o índice de ramificação e o expoente da diferente da restrição de Q na extensão F_s/F_{s-1} são iguais, respectivamente, ao índice de ramificação e ao expoente da diferente da restrição de Q na extensão $k(x_2, ..., x_s)/k(x_2, ..., x_{s-1})$, para cada $2t' < s \leq n$. Além disso, ainda da

Proposição 1.3.7, segue que a restrição de Q ao corpo de funções $k(x_2, ..., x_n)$ é não-ramificada na extensão $F_n/k(x_2, ..., x_n)$. Assim, como existem q^{2t} lugares em $k(x_2, ..., x_n)$ que são pólos de $x_{t'+1}$, existem exatamente q^{2t+1} pólos de $x_{t'+1}$ em F_n. ■

Como na demostração do lema anterior, para o caso $n \leq 2t' + 1$ nós distinguiremos os casos t' par e t' ímpar.

Lema 3.3.2. *(t' par) Ainda como no Lema* 3.3.1, *seja* $1 \leq t' < n$ *e* $Q \in \mathbb{P}_{F_n}$ *um lugar do tipo* (C). *Suponhamos que* t' *seja par e* $t' + 1 < n \leq 2t' + 1$. *Então temos:*

(i) Se n é par, existem $q^{n/2-1}$ lugares Q do tipo (C) em F_n, e estes lugares são totalmente ramificados na extensão F_n/F_{n-1} com expoente da diferente nesta extensão dado por $d(Q) = 2(q-1)$;

(ii) Se n é ímpar, existem $q^{(n-1)/2}$ lugares Q do tipo (C) em F_n, e estes lugares são não-ramificados em F_n/F_{n-1}.

Demonstração. Seja $t' = 2t$. No primeiro caso (item (i)), como n é par, temos que $n-t'-1$ é ímpar e portanto temos que $F_n = E_{t,n/2-t}$ e $F_{n-1} = H_{t,n/2-t}$. Portanto, do Teorema 3.2.2 segue que um lugar Q do tipo (C) é totalmente ramificado em F_n/F_{n-1}. Além disso, do Corolário 3.2.6 nós temos que existem exatamente $q^{n/2-1}$ lugares Q do tipo (C) em F_n. Ainda de $F_n = E_{t,n/2-t}$ e $F_{n-1} = H_{t,n/2-t}$, temos do item 2a) do Lema 3.2.4 que $F_n = F_{n-1}(\xi_{t,n/2-t})$ e que o polinômio minimal de $\xi_{t,n/2-t}$ sobre F_{n-1} nos permite aplicar o item iii) do Teorema 1.4.1 para concluir que o expoente da diferente de Q na extensão F_n/F_{n-1} é igual a $2(q-1)$. Para o item ii) veja que n ímpar nos dá que $n-t'-1$ é par, portanto $F_n = L_t$ e $F_{n-1} = E_{t,t}$ se $n = 2t' + 1$ e $F_n = H_{t,(n+1)/2-t}$ e $F_{n-1} = E_{t,(n-1)/2-t}$ se $n < 2t' + 1$. Em ambos os casos nós temos que Q é não-ramificado em F_n/F_{n-1} (conforme o Teorema 3.2.2) e temos que existem exatamente $q^{(n-1)/2}$ lugares Q do tipo (C) em F_n (conforme o Corolário 3.2.6). ■

Lema 3.3.3. *(t' ímpar) Suponhamos que t' seja ímpar, e seja $t'+1 < n \leq 2t'+1$. Então temos:*

(i) Se n é par, então existem $q^{n/2}$ lugares Q do tipo (C) em F_n, e estes lugares são não-ramificados na extensão F_n/F_{n-1}.

(ii) Se n é ímpar, existem $q^{(n-1)/2}$ lugares Q do tipo (C) em F_n, e estes lugares são totalmente ramificados na extensão F_n/F_{n-1} com expoente da diferente de Q nesta extensão dado por $d(Q) = 2(q-1)$.

Demonstração. Seja $t' = 2t+1$. No primeiro caso (item (i)), como n é par, temos que $n - t' - 1$ é par e portanto $k(x_2, ..., x_n) = L_t$ e $k(x_2, ..., x_{n-1}) = E_{t,t}$ se $n = 2t'$, e $k(x_2, ..., x_n) = H_{t,n/2-t}$ e $k(x_2, ..., x_{n-1}) = E_{t,n/2-t-1}$ se $n < 2t'$.

Em qualquer caso nós temos que a restrição de um lugar Q do tipo (C) é não-ramificado na extensão $k(x_2,...,x_n)/k(x_2,...,x_{n-1})$, e portanto Q é não ramificado na extensão F_n/F_{n-1} (conforme a figura 3.6). Além disso, do Corolário 3.2.6 existem exatamente $q^{n/2-1}$ lugares que são pólos de $x_{t'+1}$ em $k(x_2,...,x_n)$. Como cada lugar desses é não-ramificado em $F_n/k(x_2,...,x_n)$, segue que existem exatamente $q^{n/2}$ lugares Q do tipo (C) em F_n. Para o item $ii)$ como n é ímpar, temos $n-t'-1$ ímpar, logo $k(x_2,...,x_n) = E_{t,(n-1)/2-t}$ e $k(x_2,...,x_{n-1}) = H_{t,(n-1)/2-t}$. Segue então da Teorema 3.2.2 que a restrição de Q à $k(x_2,...,x_{n-1})$ é totalmente ramificada na extensão $k(x_2,...,x_n)/k(x_2,...,x_{n-1})$ e portanto é totalmente ramificada na extensão F_n/F_{n-1} (vide a figura 3.6). Além disso, do Corolário 3.2.6 existem exatamente $q^{(n-1)/2-1}$ lugares que são pólos de $x_{t'+1}$ em $k(x_2,...,x_n)$. Como cada lugar desses é não-ramificado em $F_n/k(x_2,...,x_n)$, segue que existem exatamente $q^{(n-1)/2}$ lugares Q do tipo (C) em F_n. Ainda de $k(x_2,...,x_n) = E_{t,(n-1)/2-t}$ e $k(x_2,...,x_{n-1}) = H_{t,(n-1)/2-t}$, temos do item $2a)$ do Lema 3.2.4 que $F_n = F_{n-1}(\xi_{t,(n-1)/2-t})$ e que o polinômio minimal de $\xi_{t,(n-1)/2-t}$ sobre F_{n-1} nos permite aplicar o item $iii)$ do Teorema 1.4.1 para concluir que o expoente da diferente de Q na extensão F_n/F_{n-1} é igual a $2(q-1)$.

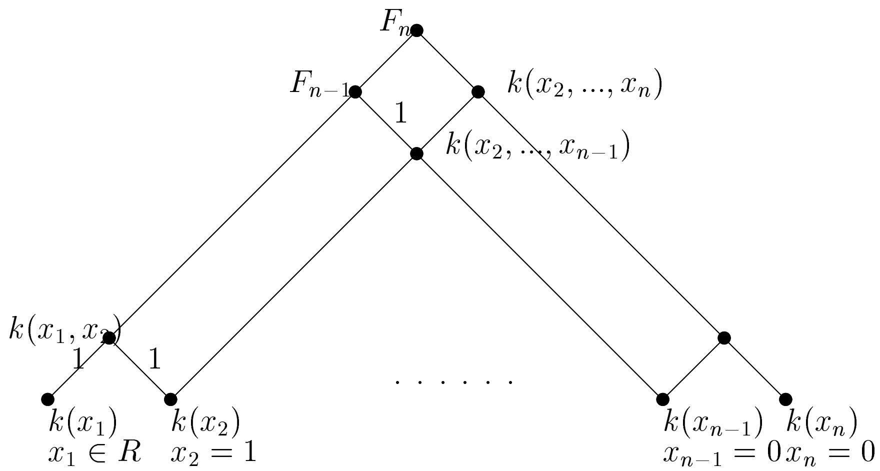

Figura 3.6: $t' = 2t+1$

■

Com estes resultados já estamos prontos para calcular o grau da diferente da extensão F_n/F_{n-1}. Para $0 \le t' < n$, seja $A_{t',n} = \#\{Q \in \mathbb{P}_{F_n} : Q$ é pólo de $x_{t'+1}\}$ e sejam $e_{t',n}$ o índice de ramificação e $d_{t',n}$ o expoente da diferente de um pólo da função $x_{t'+1}$ na extensão F_n/F_{n-1}. Do Lema 3.2.1 nós conseguimos os valores de $A_{t',n}$, $e_{t',n}$ e $d_{t',n}$ para $t'=0$. Dos comentários feitos após este lema e a partir dele nós conseguimos estes valores para $t'=1$ e $t'=n-1$. Para os outros valores de t', isto é, $1 < t' < n-1$, os valores de $A_{t',n}$, $e_{t',n}$ e $d_{t',n}$ são obtidos dos Lemas 3.3.1, 3.3.2 e 3.3.3. Com isso, nós temos, então, as seguintes tabelas para n par e n ímpar, respectivamente:

t'	$A_{t',n}$	$e_{t',n}$	$d_{t',n}$
$0 \leq t' < (n-1)/2$	$q^{t'}$	q	$2(q-1)$
$(n-1)/2 \leq t' < n-1$ t' ímpar	$q^{n/2}$	1	0
$(n-1)/2 \leq t' < n-1$ t' par	$q^{n/2-1}$	q	$2(q-1)$
$n-1$	$q^{n/2}$	$q-1$	$q-2$

Tabela 3.1: n par

t'	$A_{t',n}$	$e_{t',n}$	$d_{t',n}$
$0 \leq t' < (n-1)/2$	$q^{t'}$	q	$2(q-1)$
$(n-1)/2 \leq t' < n-1$ t' ímpar	$q^{(n-1)/2}$	q	$2(q-1)$
$(n-1)/2 \leq t' < n-1$ t' par	$q^{(n-1)/2}$	1	0
$n-1$	$q^{(n-1)/2}$	$q-1$	$q-2$

Tabela 3.2: n ímpar

Proposição 3.3.4. *Seja $D_n = grau\,(\mathrm{Diff}(F_n/F_{n-1}))$ o grau da diferente da extensão F_n/F_{n-1}. Então temos:*

(i) $D_n = q - 2 + q^{n/2+1} + \dfrac{n}{2}q^{n/2-1}(q-1)$ *se* $n \equiv 0 \pmod 4$.

(ii) $D_n = q - 2 + q^{(n+1)/2} + \frac{n-1}{2} q^{(n-1)/2}(q-1)$ *se* $n \equiv 1 \pmod 4$.

(iii) $D_n = q - 2 + q^{n/2+1} + \frac{n-2}{2} q^{n/2-1}(q-1)$ *se* $n \equiv 2 \pmod 4$.

(iv) $D_n = q - 2 + q^{(n+1)/2} + \frac{n+1}{2} q^{(n-1)/2}(q-1)$ *se* $n \equiv 3 \pmod 4$.

Demonstração: Para $0 \leq t' < n$, seja $P \in \mathbb{P}_{F_n}$ como no item 2) do Lema 3.2.1, isto é, P é zero de x_1. Deste Lema nós temos que:

$$D_n = d(P) + \sum_{t'=0}^{n-1} A_{t',n} \cdot d_{t',n}.$$

Para n par, do Lema 3.2.1 e da Tabela 3.1, segue-se que

$$D_n = q + \sum_{t'=0}^{(n-2)/2} q^{t'} \cdot 2(q-1) \quad + \sum_{(n-1)/2 \leq t', t' par}^{n-2} q^{n/2-1} \cdot 2(q-1) \quad + \quad q^{n/2} \cdot (q-2).$$

No cálculo do segundo somatório, o qual vamos chamar de S_2, nós vamos ter que distinguir dois casos. Se $n \equiv 0 \pmod 4$ então o segundo somatório começa de $\frac{n}{2}$. Enquanto se $n \equiv 2 \pmod 4$, temos que este somatório começa de $\frac{n}{2} + 1$. No primeiro caso temos

$$S_2 = q^{n/2-1} \cdot 2(q-1) \cdot \sum_{n/2 \leq t', t' par}^{n-2} 1 = q^{n/2-1} \cdot 2(q-1) \cdot \frac{n}{4};$$

enquanto que no segundo caso

$$S_2 = q^{n/2-1} \cdot 2(q-1) \cdot \sum_{n/2+1 \leq t', t' par}^{n-2} 1 = q^{n/2-1} \cdot 2(q-1) \cdot \frac{n-2}{4}.$$

Daí, se $n \equiv 0 \pmod 4$, temos que

$$\begin{aligned} D_n &= q + 2(q-1) \cdot \sum_{t'=0}^{(n-2)/2} q^{t'} \quad + q^{n/2-1} \cdot 2(q-1) \cdot \frac{n}{4} \quad + q^{n/2} \cdot (q-2) \\ &= q + 2(q-1) \cdot \frac{q^{n/2}-1}{q-1} + q^{n/2-1} \cdot 2(q-1) \cdot \frac{n}{4} + q^{n/2} \cdot (q-2) \\ &= q + 2(q^{n/2}-1) + q^{n/2-1} \cdot 2(q-1) \cdot \frac{n}{4} + q^{n/2} \cdot (q-2) \\ &= q - 2 + q^{n/2+1} + \frac{n}{2} q^{n/2-1} \cdot (q-1). \end{aligned}$$

Por outro lado, se $n \equiv 2 \pmod 4$, nós temos

$$\begin{aligned}
D_n &= q + 2(q-1)\sum_{t'=0}^{(n-2)/2} q^{t'} \quad + q^{n/2-1}\cdot 2(q-1)\cdot \frac{n-2}{4} \quad + q^{n/2}\cdot(q-2)\\
&= q + 2(q^{n/2}-1) + q^{n/2-1}\cdot 2(q-1)\cdot\frac{n-2}{4} + q^{n/2}\cdot(q-2)\\
&= q - 2 + q^{n/2+1} + \frac{n-2}{2}q^{n/2-1}\cdot(q-1).
\end{aligned}$$

O caso n ímpar é análogo. De fato, da Tabela 3.2 segue que

$$D_n = q + \sum_{t'=0}^{(n-3)/2} q^{t'}\cdot 2(q-1) \quad + \sum_{(n-1)/2\le t',t'\text{ímpar}}^{n-2} q^{(n-1)/2}\cdot 2(q-1) \quad + q^{(n-1)/2}\cdot(q-2).$$

Novamente, para o cálculo do segundo somatório, o qual vamos chamar de S_2', nós vamos ter que distinguir dois casos. Se $n \equiv 1 \pmod 4$ então o segundo somatório começa de $\frac{n+1}{2}$, enquanto que se $n \equiv 3 \pmod 4$, temos que este somatório começa de $\frac{n-1}{2}$. No primeiro caso temos

$$S_2' = q^{(n-1)/2}\cdot 2(q-1)\cdot \sum_{(n+1)/2\le t',t'\text{ímpar}}^{n-2} 1 = q^{(n-1)/2}\cdot 2(q-1)\cdot\frac{n-1}{4}.$$

No segundo caso nós temos

$$S_2' = q^{(n-1)/2}\cdot 2(q-1)\cdot \sum_{(n-1)/2\le t',t'\text{ímpar}}^{n-2} 1 = q^{(n-1)/2}\cdot 2(q-1)\cdot\frac{n+1}{4}.$$

Daí, se $n \equiv 1 \pmod 4$, temos que

$$\begin{aligned}
D_n &= q + 2(q-1)\cdot\sum_{t'=0}^{(n-3)/2} q^{t'} \quad + \quad q^{(n-1)/2}\cdot 2(q-1)\cdot\frac{n-1}{4} \quad + \quad q^{(n-1)/2}\cdot(q-2)\\
&= q + 2(q-1)\cdot\frac{q^{(n-1)/2}-1}{q-1} + q^{(n-1)/2}\cdot 2(q-1)\cdot\frac{n-1}{4} + q^{(n-1)/2}\cdot(q-2)\\
&= q + 2(q^{(n-1)/2}-1) + q^{(n-1)/2}\cdot 2(q-1)\cdot\frac{n-1}{4} + q^{(n-1)/2}\cdot(q-2)\\
&= q - 2 + q^{(n+1)/2} + \frac{n-1}{2}q^{(n-1)/2}(q-1).
\end{aligned}$$

Por outro lado, se $n \equiv 3 \pmod 4$, nós temos

$$\begin{aligned} D_n &= q + 2(q-1)\cdot \sum_{t'=0}^{(n-3)/2} q^{t'} \;+\; q^{(n-1)/2}\cdot 2(q-1)\cdot \frac{n+1}{4} \;+\; q^{(n-1)/2}\cdot(q-2) \\ &= q + 2(q^{(n-1)/2}-1) + q^{(n-1)/2}\cdot 2(q-1)\cdot\frac{n+1}{4} + q^{(n-1)/2}\cdot(q-2) \\ &= q - 2 + q^{(n+1)/2} + \frac{n+1}{2} q^{(n-1)/2}(q-1). \end{aligned}$$

■

Na proposição anterior nós vimos que o grau da diferente numa extensão F_n/F_{n-1} depende da classe de congruência de n módulo 4, o que vai se refletir no cálculo do gênero de F_n, como mostra o seguinte lema:

Lema 3.3.5. *Seja $n \geq 1$ um inteiro, e seja g_n o gênero de F_n. Então*

(i) para $n \equiv 0 \pmod 4$, temos

$$g_n = \frac{1}{2(q-1)}\cdot\left(q^{n+1} + 2q^n - 2q^{n/2+1} - 2q^{n/2} + q\right) \;-\; \frac{n}{4}\cdot q^{n/2-1}(q+1).$$

(ii) para $n \equiv 2 \pmod 4$, temos

$$g_n = \frac{1}{2(q-1)}\cdot\left(q^{n+1} + 2q^n - 4q^{n/2+1} + q\right) \;-\; \frac{n-2}{4}\cdot q^{n/2-1}(q+1).$$

(iii) para $n \equiv 1 \pmod 2$, temos

$$g_n = \frac{1}{2(q-1)}\cdot\left(q^{n+1} + 2q^n - q^{(n+3)/2} - 3q^{(n+1)/2} + q\right) \;-\; \frac{n-1}{2}\cdot q^{(n-1)/2}.$$

Demonstração: O lema é facilmente verificado para $n=1$, $n=2$, $n=3$ e $n=4$. Além disso, da fórmula do gênero de Hurwitz (conforme o Teorema 1.3.2) nós temos que

$$g_n = q\cdot g_{n-1} - (q-1) + \frac{1}{2}D_n.$$

Usando a Proposição 3.3.4, nós temos

$$(*)\quad g_n = \begin{cases} q\cdot g_{n-1} - \frac{q}{2} + \dfrac{q^{n/2-1}}{2}\cdot\left(q^2 + \dfrac{n}{2}(q-1)\right) & \text{se } n \equiv 0 \pmod 4 \\ q\cdot g_{n-1} - \frac{q}{2} + \dfrac{q^{(n-1)/2}}{2}\cdot\left(q + \dfrac{n-1}{2}(q-1)\right) & \text{se } n \equiv 1 \pmod 4 \\ q\cdot g_{n-1} - \frac{q}{2} + \dfrac{q^{n/2-1}}{2}\cdot\left(q^2 + \dfrac{n-2}{2}(q-1)\right) & \text{se } n \equiv 2 \pmod 4 \\ q\cdot g_{n-1} - \frac{q}{2} + \dfrac{q^{(n-1)/2}}{2}\cdot\left(q + \dfrac{n+1}{2}(q-1)\right) & \text{se } n \equiv 3 \pmod 4. \end{cases}$$

Primeiramente mostraremos por indução que o lema vale para $n \equiv 0 \pmod 4$. Seja então $k \geq 1$. Da Equação $(*)$ nós temos que

$$g_{4k+1} = q \cdot g_{4k} - \frac{q}{2} + \frac{q^{2k}}{2}\left(q + 2k(q-1)\right),$$

e portanto da Equação $(*)$ para $n \equiv 2 \pmod 4$ temos que

$$\begin{aligned} g_{4k+2} &= q^2 \cdot g_{4k} - \frac{q^2}{2} + \frac{q^{2k+1}}{2} \cdot \left(q + 2k(q-1)\right) - \frac{q}{2} + \frac{q^{2k}}{2} \cdot \left(q^2 + 2k(q-1)\right) \\ &= q^2 \cdot g_{4k} - \frac{q^2+q}{2} + \frac{q^{2k}}{2} \cdot \left(q^2 + 2qk(q-1) + q^2 + 2k(q-1)\right). \end{aligned}$$

Logo, da Equação $(*)$ para $n \equiv 3 \pmod 4$,

$$\begin{aligned} g_{4k+3} = q^3 \cdot g_{4k} - \frac{q^3+q^2}{2} + \frac{q^{2k+1}}{2} \cdot \left(q^2 + 2qk(q-1) + q^2 + 2k(q-1)\right) - \frac{q}{2} \\ + \frac{q^{2k+1}}{2} \cdot \left(q + (2k+2)(q-1)\right), \end{aligned}$$

isto é,

$$g_{4k+3} = q^3 \cdot g_{4k} - \frac{q^3+q^2+q}{2} + \frac{q^{2k+1}}{2} \cdot \left(2q^2 + q + 2qk(q-1) + (4k+2)(q-1)\right).$$

E assim, usando a Equação $(*)$ para $n \equiv 0 \pmod 4$, chegamos a seguinte igualdade:

$$\begin{aligned} g_{4k+4} = q^4 \cdot g_{4k} - \frac{q^4+q^3+q^2}{2} + \frac{q^{2k+2}}{2} \cdot \left(2q^2 + q + 2qk(q-1) + (4k+2)(q-1)\right) \\ - \frac{q}{2} + \frac{q^{2k+1}}{2} \cdot \left(q^2 + (2k+2)(q-1)\right), \end{aligned}$$

isto é,

$$\begin{aligned} g_{4k+4} = q^4 \cdot g_{4k} - \frac{q^4+q^3+q^2+q}{2} + \frac{q^{2k+1}}{2} \cdot \big(2q^3 + 2q^2 + 2q^2k(q-1) + \\ + (4k+2)q(q-1) + (2k+2)(q-1)\big) = \\ = q^4 g_{4k} - \frac{q^5-q}{2(q-1)} + \frac{q^{2k+1}}{2}(q+1)\left(2q^2 + 2(q-1) + 2k(q^2-1)\right). \end{aligned}$$

Conseguimos então o gênero de $F_{4(k+1)}$ em função do gênero de F_{4k}. Supondo então que o item $i)$ vale para $n = 4k$ nós temos da última igualdade que

$$\begin{aligned} g_{4k+4} = \frac{q^4}{2(q-1)}\left(q^{4k+1} + 2q^{4k} - 2q^{2k+1} - 2q^{2k} + q\right) - k \cdot q^{2k+3}(q+1) - \frac{q^5-q}{2(q-1)} \\ + \frac{q^{2k+1}}{2}(q+1)\left(2q^2 + 2(q-1) + 2k(q^2-1)\right), \end{aligned}$$

isto é,

$$g_{4k+4} = \frac{1}{2(q-1)}\left(q^{4(k+1)+1} + 2q^{4(k+1)} - 2q^{2(k+1)+1} - 2q^{2(k+1)} + q\right)$$
$$-(k+1)\cdot q^{2(k+1)-1}(q+1).$$

E com isso provamos o item $i)$. Os outros itens seguem aplicando-se a fórmula de Riemann-Hurwitz. De fato, para $n \equiv 1 \pmod 4$, temos que $n-1 \equiv 0 \pmod 4$. Daí,

$$g_{n-1} = \frac{1}{2(q-1)}\cdot\left(q^n + 2q^{n-1} - 2q^{(n+1)/2} - 2q^{(n-1)/2} + q\right) - \frac{n-1}{4}\cdot q^{(n-3)/2}\cdot(q+1).$$

E portanto, da Equação $(*)$, temos que

$$g_n = \frac{q}{2(q-1)}\cdot\left(q^n + 2q^{n-1} - 2q^{(n+1)/2} - 2q^{(n-1)/2} + q\right) - \frac{n-1}{4}\cdot q^{(n-1)/2}\cdot(q+1).$$
$$-\frac{q}{2} + \frac{q^{(n-1)/2}}{2}\cdot\left(q + \frac{n-1}{2}(q-1)\right),$$

isto é,

$$g_n = \frac{1}{2(q-1)}\cdot\left(q^{n+1} + 2q^n - q^{(n+3)/2} - 3q^{(n+1)/2} + q\right) - \frac{n-1}{2}\cdot q^{(n-1)/2}.$$

Analogamente, se temos provado o item $iii)$ para o caso $n \equiv 1 \pmod 4$, então para o caso $n \equiv 2 \pmod 4$ temos a Equação $(*)$:

$$g_n = qg_{n-1} - \frac{q}{2} + \frac{q^{n/2-1}}{2}\cdot\left(q^2 + \frac{n-2}{2}(q-1)\right).$$

Mas $n-1 \equiv 1 \pmod 4$, logo

$$g_n = \frac{q}{2(q-1)}\left(q^n + 2q^{n-1} - q^{(n+2)/2} - 3q^{n/2} + q\right) - \frac{n-2}{2}\cdot q^{n/2}$$
$$-\frac{q}{2} + \frac{q^{n/2-1}}{2}\cdot\left(q^2 + \frac{n-2}{2}(q-1)\right),$$

isto é,

$$g_n = \frac{1}{2(q-1)}\cdot\left(q^{n+1} + 2q^n - 4q^{n/2+1} + q\right) - \frac{n-2}{4}\cdot q^{n/2-1}(q+1).$$

Finalmente, se $n \equiv 3 \pmod 4$, temos da Equação $(*)$ que

$$g_n = q\cdot g_{n-1} - \frac{q}{2} + \frac{q^{(n-1)/2}}{2}\cdot\left(q + \frac{n+1}{2}(q-1)\right).$$

Mas $n-1 \equiv 2 \pmod 4$, logo

$$g_n = \frac{q}{2(q-1)}\left(q^n + 2q^{n-1} - 4q^{(n+1)/2} + q\right) - \frac{n-3}{4} \cdot q^{(n-1)/2}(q+1) - \\ -\frac{q}{2} + \frac{q^{(n-1)/2}}{2} \cdot \left(q + \frac{n+1}{2}(q-1)\right),$$

isto é,

$$g_n = \frac{1}{2(q-1)} \cdot \left(q^{n+1} + 2q^n - q^{(n+3)/2} - 3q^{(n+1)/2} + q\right) \quad - \quad \frac{n-1}{2} \cdot q^{(n-1)/2}.$$

∎

Como corolário deste lema nós temos o seguinte teorema:

Teorema 3.3.6. *O gênero da torre $\mathcal{F}$ é dado por*

$$\gamma(\mathcal{F}) = lim_{n\to\infty}\frac{g(F_n)}{q^{n-1}} = \frac{q(q+2)}{2(q-1)}.$$

3.3.2 Os lugares racionais

Para o cálculo do limite da torre $\mathcal{F}$ nós necessitamos também analisar os lugares racionais da torre sobre $\mathbb{F}_{q^3}$. Nosso objetivo nesta sessão é mostrar que certos lugares racionais de F_1 se decompõem completamente na torre $\mathcal{F}$. Estes lugares serão em quantidade suficiente para que o teorema principal seja provado. Ao contrário do Capítulo 2, aqui um estudo um pouco mais elaborado será necessário, e por isso abrimos uma seção especialmente para a contagem dos lugares racionais em cada passo da torre em questão. Vamos começar considerando as seguintes funções racionais:

$$a(T) := \frac{1-T}{T^q} \quad \text{e} \quad b(T) := \frac{T^q + T - 1}{T},$$

e consideremos os seguintes subconjuntos de $k = \overline{\mathbb{F}}_{q^3}$.

$$S := \{\gamma \in k : \gamma^{q+1} = \gamma - 1\} \text{ e } \Omega := \{w \in k : a(w) \in S\}.$$

Proposição 3.3.7. *i) Os elemetos de Ω estão em $\mathbb{F}_{q^3}$ e $\#\Omega = q(q+1)$.*

ii) Seja $\sigma \in \Omega$. Então a equação $a(\eta) = b(\sigma)$ tem exatamente q raízes η em $\mathbb{F}_{q^3}$ e todas estas raízes estão em Ω.

Esta proposição é uma consequência imediata dos dois lemas abaixo:

Lema 3.3.8. *Sejam S e Ω os conjuntos acima. Então os seguintes itens são satisfeitos:*

(i) $\#S = q+1$ *e* $\#\Omega = q(q+1)$.

(ii) Se $\gamma \in S$ *então* $\gamma^{q^2+q+1} = -1$. *Em particular, o conjunto* S *está contido em* $\mathbb{F}_{q^3}$.

(iii) O conjunto Ω *está contido em* $\mathbb{F}_{q^3}$.

Demonstração: *i*) Por definição o conjunto S consiste dos zeros do polinômio $f(T) = T^{q+1} - T + 1$ em $\overline{\mathbb{F}}_{q^3}$. Como $f'(T) = -1 \neq 0$, $f(T)$ é claramente separável e nós obtemos que $\#S = q+1$. Analogamente, o conjunto Ω consiste dos zeros dos polinômios $h_\gamma(T) := T^q + \gamma^{-1}T - \gamma^{-1}$, com $\gamma \in S$. Desde que $h'_\gamma(T) = \gamma^{-1} \neq 0$, estes polinômios são separáveis. Além disso, para $\gamma_1 \neq \gamma_2$, os polinômios h_{γ_1} e h_{γ_2} não têm raízes em comum. Portanto $\#\Omega = q(q+1)$.

ii) Se $\gamma^{q+1} = \gamma - 1$, então $\gamma^{q^2+q} = \gamma^q - 1$. Multiplicando por γ nós obtemos que $\gamma^{q^2+q+1} = \gamma^{q+1} - \gamma = -1$ e como q^2+q+1 é expoente da norma em $\mathbb{F}_{q^3}/\mathbb{F}_q$, isto nos dá elementos de $\mathbb{F}_{q^3}$.

iii) Seja $\omega \in \Omega$. Então $a(\omega) = \gamma$ para algum $\gamma \in S$; isto é, $1 - \omega = \gamma\omega^q$. Usando o item anterior nós temos que

$$\begin{aligned}
\omega^{q^3} &= -\gamma^{q^2+q+1} \cdot \omega^{q^3} = -\gamma^{q+1}(\gamma \cdot \omega^q)^{q^2} = -\gamma^{q+1}(1-\omega)^{q^2} = -\gamma^{q+1} + \gamma^{q+1} \cdot \omega^{q^2} \\
&= -\gamma^{q+1} + \gamma \cdot (\gamma \cdot \omega^q)^q = -\gamma^{q+1} + \gamma(1-\omega)^q = -\gamma^{q+1} + \gamma - \gamma \cdot \omega^q \\
&= -\gamma^{q+1} + \gamma - (1-\omega) = (-\gamma^{q+1} + \gamma - 1) + \omega = \omega,
\end{aligned}$$

desde que $\gamma \in S$. E portanto, temos $\omega \in \mathbb{F}_{q^3}$. ∎

Lema 3.3.9. *Se* $\omega \in \Omega$ *então* $b(\omega) \in S$.

Demonstração: Seja $\omega \in \Omega$. Então existe algum $\gamma \in S$ tal que $\gamma \cdot \omega^q = 1 - \omega$. Assim

$$b(\omega) = \frac{\omega^q + \omega - 1}{\omega} = \frac{\omega^q - \gamma \cdot \omega^q}{\omega} = \omega^{q-1}(1-\gamma) =: \beta,$$

e nós temos que mostrar que $\beta \in S$. De fato,

$$\begin{aligned}
\gamma \cdot \omega(\beta^{q+1} - \beta + 1) &= \gamma \cdot \omega \left((1-\gamma)^{q+1}\omega^{q^2-1} - (1-\gamma)\omega^{q-1} + 1 \right) \\
&= \gamma(1 - \gamma - \gamma^q + \gamma^{q+1})\omega^{q^2} - \gamma(1-\gamma)\omega^q + \gamma \cdot \omega \\
&= -\gamma^{q+1}\omega^{q^2} - (1-\gamma)\gamma \cdot \omega^q + \gamma \cdot \omega \\
&= -\gamma(\gamma \cdot \omega^q)^q - (1-\gamma)(1-\omega) + \gamma \cdot \omega \\
&= -\gamma(1-\omega)^q - 1 + \gamma + \omega \\
&= \gamma \cdot \omega^q - 1 + \omega = 0.
\end{aligned}$$

Assim, $\beta^{q+1} = \beta - 1$, e portanto $\beta \in S$. ∎

Agora já podemos provar a Proposição 3.3.7.

Demonstração da Prop. 3.3.7: O item $i)$ já foi provado no Lema 3.3.8. Para o item $ii)$, seja $\Lambda = \{\lambda \in k : b(\lambda) \in S\}$. Desde que $grau(b) = q$, nós temos que $\#\Lambda \leq q \cdot \#S = q(q+1)$. Além disso, pelo Lema 3.3.9 nós sabemos que $\Omega \subset \Lambda$, e desde que $\#\Omega = q(q+1)$ concluimos que $\Omega = \Lambda$. E esta igualdade entre conjuntos nos prova o item $ii)$.

■

Como consequência da Prop.3.3.7 nós temos o seguinte teorema, que é exatamente o que falta para provarmos o teorema principal deste capítulo, o Teorema 3.1.2.

Teorema 3.3.10. *Seja $\mathcal{F} = (F_1, F_2, F_3, ...)$ a torre de corpos de funções sobre $\mathbb{F}_{q^3}$ definida recursivamente pela Equação (3.1), e seja $\omega \in \Omega$. Então o lugar de F_1 que é o único zero da função $x_1 - \omega$ se decompõe totalmente na extensão F_n/F_1. Portanto, o número de lugares racionais de $F_n/\mathbb{F}_{q^3}$ satisfaz*

$$N(F_n) \geq q^{n-1} \cdot \#\Omega = q^n(q+1).$$

Demonstração: Para a demonstração deste teorema nós provaremos por indução sobre n os seguintes itens:

$i)$ O lugar de F_1 que é zero da função $x_1 - \omega$ tem exatamente q^{n-1} extensões $Q \in \mathbb{P}(F_n)$.

$ii)$ Para qualquer tal lugar Q existe algum $\omega' \in \Omega$ tal que Q é um zero da função $x_n - \omega'$.

De fato, o caso $n = 1$ é trivial, e nós assumimos que as afirmações $i)$ e $ii)$ são verdadeiras para algum $n \geq 1$. Seja $Q \in \mathbb{P}(F_n)$ um dos zeros da função $x_1 - \omega$, então Q é um zero da função $x_n - \omega'$ para algum $\omega' \in \Omega$. A função x_{n+1} satisfaz a equação $a(x_{n+1}) = b(x_n)$. Pelo Teorema 1.3.6, a cada solução η da equação $a(\eta) = b(\omega')$ corresponde um lugar $Q' \in \mathbb{P}(F_{n+1})$ com $Q'|Q$ tal que Q' é um zero da função $x_{n+1} - \eta$. Pela Prop. 3.3.7, a equação $a(\eta) = b(\omega')$ tem exatamente q raízes distintas $\eta \in \Omega$, e assim as afirmações $i)$ e $ii)$ também valem para $n+1$.

■

Demonstração do Teo. 3.1.2: Novamente nós vamos usar a notação do Teorema 1.2.11, agora substituindo $\mathbb{F}_q$ por $\mathbb{F}_{q^3}$.

Do Teo. 3.3.10, para a torre $\mathcal{F}$ sobre $\mathbb{F}_{q^3}$ considerada, temos que

$$\upsilon(\mathcal{F}) \geq lim_{n\to\infty} \frac{q^n(q+1)}{q^{n-1}} = q(q+1).$$

E do Teo. 3.3.6 temos que

$$\gamma(\mathcal{F}) = \frac{q(q+2)}{2(q-1)},$$

e, portanto, $\lambda(\mathcal{F}) = \upsilon(\mathcal{F})/\gamma(\mathcal{F}) \geq 2(q^2-1)/(q+2)$.

■

Observação 3.3.11. Como já foi observado na Seção 1.2.3 do Capítulo 1, o limite de torres assintoticamente boas sobre $\mathbb{F}_q$ dá origem a cotas inferiores para a quantidade $A(q)$. Cotas inferiores para esta quantidade por sua vez dão origem a cotas inferiores para a função $\alpha_q(\delta)$, que tem um importante papel na teoria dos códigos (conforme a Seção 1.2.1 do Capítulo 1).

Vamos agora comparar a cota dada por Tsfasman, Vladut e Zink com a cota de Gilbert-Varshamov.

A cota de Gilbert-Varshamov (Prop. 1.2.1) diz que

$$\alpha_q(\delta) \geq C_{GV}(\delta) := 1 - H_q(\delta) \text{ para todo } \delta \in [1, (q-1)/q].$$

Já a cota *Algébro-Geométrica básica* (Teo. 1.2.5) dada por Tsfasman, Vladut e Zink nos diz que

$$\alpha_q(\delta) \geq C_{TVZ}(\delta) = 1 - \delta - A^{-1} \text{ para qualquer } 0 < A \leq A(q).$$

Aqui vale a pena explicar como achamos o intervalo em que a cota C_{TVZ} melhora a cota C_{GV}. Se a reta de Goppa $R = 1 - \delta - A^{-1}$ é tangente a curva $R = C_{GV}(\delta)$ num ponto $(\delta_0, C_{GV}(\delta_0))$, então $\delta_0 = (q-1)/(2q-1)$ (basta comparar as declividades das retas em questão: a reta de Goppa e a reta tangente a curva C_{GV}). Consequentemente, nós temos que a reta $R = 1 - \delta - A^{-1}$ é tangente se $A^{-1} = H_q(\delta_0) - \delta_0 = log_q(2q-1) - 1$. Assim, como o gráfico de C_{GV} é côncavo para cima, sempre que $A^{-1} < log_q(2q-1) - 1$, existe um intervalo contendo δ_0 tal que neste intervalo a cota C_{TVZ} melhora a cota C_{GV}.

Para q substituído por q^3 nas cotas acima, nós podemos, pelo Teorema 3.1.2, escolher $A = 2(q^2-1)/(q+2)$, e calculando estas cotas em $\delta_0 = (q^3-1)/(2q^3-1)$ nós achamos que

$$1 - \delta_0 - (q+2)/2(q^2-1) > 1 - H_{q^3}(\delta_0)$$

para todo $q \geq 7$. De fato, pedir que $(q+2)/2(q^2-1) < log_{q^3}(2q^3-1) - 1$ equivale a pedir que $q^{3c} < 2q^3 - 1$, onde $c = (2q^2+q)/2(q^2-1)$, isto é,

$$q^3(q^{3(c-1)} - 2) + 1 < 0,$$

logo queremos que $q^{3(c-1)} < 2$. Uma condição suficiente para isto é pedir que $3(c-1) < 2/q$, pois para $q \geq 5$ temos $q^{2/q} < 2$. Agora, $3(c-1) < 2/q$ equivale a ter $3(q+2)/2(q^2-1) < 2/q$, e simplificando esta última desigualdade temos $-q^2+6q+4 < 0$. Calculando as raízes da equação $-x^2+6x+4 = 0$ nós vemos que a desigualdade $-x^2+6x+4 < 0$ ocorre sempre que $x < 3-\sqrt{13}$ ou $x > 3+\sqrt{13}$. Portanto a cota de Tsfasman-Vladut-Zink melhora a cota de Gilbert-Varshamov em um intervalo não-vazio contendo δ_0, para toda potência cúbica de q com $q \geq 7$.

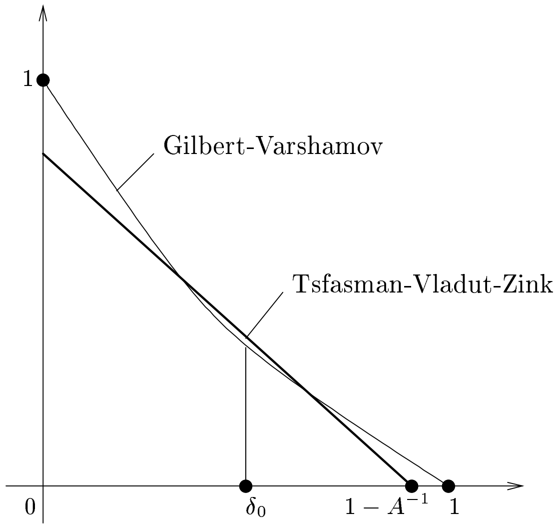

Figura 3.7: $A = \frac{2(q^2-1)}{q+2}$

3.4 Uma torre assintoticamente ruim

Antes de chegarmos às equações que nos deram torres assintoticamente boas, nós passamos, sempre na tentativa de encontrar torres com limite positivo, por algumas equações que trouxeram torres assintoticamente ruins, isto é, torres $\mathcal{F}$ com limite $\lambda(\mathcal{F}) = 0$, e por outras equações que ainda não nos permitiram nenhuma conclusão a respeito do limite da torre construída a partir de tal equação. Como apareceram estas equações? Bem, a idéia central era procurar equações que fornecessem a princípio torres com lugares totalmente decompostos (vide Teo. 1.2.11); daí se partiria para o estudo do gênero de tal torre. Esta seção finaliza o trabalho com a apresentação de uma destas equações, esboçando a razão dela originar uma torre assintoticamente ruim.

A torre que segue é uma torre sobre $\mathbb{F}_{q^p}$, onde $p = car(\mathbb{F}_q)$, do tipo Artin-Schreier (vide [15], Prop. III.7.8). Ela é otimal para $q = 2$, e somente neste caso ela é uma torre com limite positivo. As seguintes proposições são fundamentais para o nosso objetivo nesta seção, em especial a Prop. 3.4.2, que nos dá uma condição suficiente para que uma torre seja assintoticamente ruim a partir do crescimento do grau da diferente.

Proposição 3.4.1. *([15],* Prop. III.7.10*) Suponha que F/K é um corpo de funções algébricas sobre K (onde $K = \mathbb{F}_q$ é algebricamente fechado em F). Seja $w \in F$ e assuma que existe um lugar $P \in \mathbb{P}(F)$ tal que*

$$v_P(w) = -m, \quad m > 0 \;\; e \;\; mdc(m, q) = 1.$$

Então o polinômio $T^q - T - w \in F[T]$ é absolutamente irredutivel. Seja $E = F(z)$ com

$$z^q - z = w.$$

As seguintes afirmações são satisfeitas:

(i) E/F é uma extenção de Galois de grau $[E : F] = q$. O grupo de Galois de E/F é abeliano elementar de expoente $p = car\,(K)$, e K é algebricamente fechado em E.

(ii) O lugar P é totalmente ramificado em E, isto é, existe exatamente um lugar $P' \in \mathbb{P}(E)$ acima de P, e o indice de ramificação de $P' \mid P$ é $e(P' \mid P) = q$. Além disso, $degP' = degP$, e o expoente da diferente de $P' \mid P$ na extensão E/F é dado por

$$d(P' \mid P) = (q-1)(m+1).$$

(iii) Seja $R \in \mathbb{P}(F)$ e assuma que

$$w = \wp(u) + \mathcal{O}(0) \quad em \quad R,$$

para algum elemento $u \in F$, onde $\wp(u) = u^q - u$. Então, o lugar R é não-ramificado em E/F. Em particular, este é o caso se $v_R(w)$ é não-negativo.

(iv) Suponha que o lugar $Q \in \mathbb{P}(F)$ é um zero de $w - \gamma$, com $\gamma \in \mathbb{F}_q$. A equação $\alpha^q - \alpha = \gamma$ tem q raízes distintas $\alpha \in \mathbb{F}_{q^2}$, e para cada tal α existe um único lugar $Q_\alpha \in \mathbb{P}(E)$ tal que Q_α está acima de Q, e Q_α é um zero de $z - \alpha$; em particular, o lugar Q se decompõe totalmente em E.

Para uma extensão de Artin-Schreier E/F com $E = F(y)$ e $y^q - y = w$, cada vez que trocamos o gerador y desta extensão por outro da forma $\tilde{y} = y - u$ com $u \in F$ satisfazendo $v_P(w - \wp(u)) = -m < 0$ e $mdc(m, q) = 1$ (*processo de redução*, Seção 1.4), nós dizemos que estamos fazendo uma *redução de Artin-Schreier*. A contribuição para a diferente é determinada pelas ordens $m = -v_P(w*)$ para os pólos P da redução de Artin-Schreier $w* = w - \wp(u)$ da função w. O inteiro m é chamado de *ordem de redução*.

Proposição 3.4.2. *([4],* Prop. 2.5*) Seja $\mathcal{F} = (F_1, F_2, ...)$ uma torre de corpos de funções sobre $\mathbb{F}_q$. Suponha que $(\rho_2, \rho_3, ...)$ é uma sequência de números reais satisfazendo as seguintes propriedades:*

i) $\rho_2 > 0$.

ii) $\rho_{n+1} \leq grau\,(\mathrm{Diff}(F_{n+1}/F_n))$, para todo $n \geq 1$.

iii) $\rho_{n+1} \geq [F_{n+1} : F_n] \cdot \rho_n$, para todo $n \geq 2$.

Então a torre $\mathcal{F}$ é assintoticamente ruim.

Seja $K = \mathbb{F}_{q^p}$ com $p = car(\mathbb{F}_q)$, e seja k o fecho algébrico de K.

Definição 3.4.3. *Seja $F_1 := K(x_1)$ o corpo de funções racionais sobre K. Para $i \geq 1$, definimos*

$$F_{i+1} := F_i(x_{i+1}),$$

onde x_{i+1} satisfaz a equação

$$x_{i+1}^q - x_{i+1} = \frac{x_i^q}{1 - x_i} =: f(x_i). \tag{3.38}$$

Observação 3.4.4. Para $q = 2$ esta é a torre em [6], portanto assintoticamente otimal sobre $\mathbb{F}_4$.

Seja $S = \{\alpha \in k : \alpha^q = \alpha - 1\}$. É fácil ver por indução que $\alpha^{q^i} = \alpha - i$ para $i \geq 1$ (Basta elevar a igualdade $\alpha^q = \alpha - 1$ à q sucessivas vezes). Daí, para $i = p$ nós temos que $\alpha^{q^p} = \alpha$, ou seja, $\alpha \in K$.

Proposição 3.4.5. *Considere a torre $\mathcal{F}_1$ definida recursivamente pela Equação (3.42). Então, os lugares de F_1 que são zeros da funções $x_1 - \alpha$, $\alpha \in S$, se decompõem totalmente na torre $\mathcal{F}_1$.*

Esta proposição é uma consequência do Teorema 1.3.6. Ela foi o suficiente para nos levar a estudar o gênero de tal torre na tentativa de encontrar torres assintoticamente boas. Porém, isto não aconteceu.

Teorema 3.4.6. *A torre $\mathcal{F}_1$ é assintoticamente ruim.*

Este teorema é uma consequência do seguinte lema.

Lema 3.4.7. *Fixe $m \geq 1$. Então:*

(1) Existe um único lugar $P \in \mathbb{P}_{F_m}$ que é zero comum das funções $x_1, x_2, ..., x_{m-1}$ e da função $x_m - 1$.

(2) A ordem de redução em P de $f(x_m)$ em F_{m+1}/F_m é $m_P = q^{m-1} - \sum_{i=0}^{m-2} q^i$.

(3) O lugar P é totalmente ramificado na extensão F_{m+1}/F_m.

Aplicando a Prop. 3.4.1 (item *ii*)) aos resultados deste último lema, nós temos que o coeficiente da diferente de P na extensão F_{m+1}/F_m é

$$d(P) = (q^{m-1} - \frac{q^{m-1} - 1}{q - 1} + 1)(q - 1) = q^m - 2q^{m-1} + q.$$

Logo, considerando $\rho_{n+1} = q^n - 2q^{n-1}$, nós temos que a sequência $(\rho_n)_{n \geq 2}$ satisfaz as condições do Proposição 3.4.2, e usando esta proposição nós concluimos o Teorema 3.4.6.

Bibliografia

[1] S. Ballet: Curves with many points and multiplication complexity in any extension of $\mathcal{F}_q$, *Finite Fields Appl. 5* (1999), 364-377.

[2] V.G. Drinfeld, S.G. Vladut: Number of points of an algebraic curve, *Funct. Anal. 17* (1983), 53-54.

[3] Noam D. Elkies: Explicit Towers of Drinfeld Modular Curves, *European Congress of Mathematics Vol.II* (2000),189-198.

[4] A. Garcia, H. Stichtenoth: On the asymptotic behaviour of somes towers of function fields over finite fields, *J.Number Theory 61* (1996), 248-273.

[5] A. Garcia, H. Stichtenoth: A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, *Inventiones Math. 121* (1995), 211-222.

[6] A. Garcia, H. Stichtenoth: On tame towers over finite fields, *J Reine Angew. Math. 557* (2003), 53-80.

[7] A. Garcia, H. Stichtenoth, M. Thomas: On towers and composita of towers of function fields over finite fields, *Finite Fields and their applications 3* (1997), 257-274.

[8] G. van der Geer, M. van der Vlugt: An asymptotically good tower of curves over the field with eight elements, *Bull. London Math Soc. 34* (2002), 291-300.

[9] Y. Ihara: Some Remarks on the number of Rational Points of Algebraic Curves over Finite Fields, *J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28* (1981), 721-724.

[10] Manin, Y.I.: What is the maximum number of points on a curve over $\mathbb{F}_2$? *J.Fac.Sci.Univ. Tokyo 28* (1981), 715-720.

[11] R. Matsumoto: Improvement of Ashikhmin-Litsyn-Tsfasman bound for quantum codes, *IEEE Trans. Inform. Theory 48* (2002), 2122-2124.

[12] F.J. Mac Williams, N. J. Sloane: "The Theory of Error-Correcting Codes", North-Holland, 1978.

[13] H. Niederreiter, C. Xing: Curves sequences with asymptotically many rational points, *Applications of curves over finite fields, Contemporary Math. 245* (1997),3-14.

[14] J.-P. Serre: Sur le Nombre des Points Rationnels d'une Courbe Algébrique sur un Corps Fini, *C. R. Acad. Sci. Paris Sér. I Math. 296* (1983), 397-402.

[15] H. Stichtenoth: "Algebraic Function Fields and Codes". Springer Universitext, Springer-Verlag, Berlin-Heidelberg, 1993.

[16] H. Stichtenoth: Explicit Constructions of Towers of Function Fields with many Rational Places, *European Congress of Mathematics Vol.II* (2000),219-224.

[17] K.-O. Stohr, J.F. Voloch: Weierstrass points and curves over finite fields, *Proc. London Math. Soc. 52* (1986), 1-19.

[18] M.A. Tsfasman and S. G. Vladut, "Algebraic-Geometric Codes", Dordrecht, The Netherlands: Kluwer, 1991.

[19] M.A. Tsfasman, S. G. Vladut, and T. Zink: Modular Curves, Shimura Curves, and Goppa Codes, better than Varshamov-Gilbert Bound, *Math. Nachr. 109* (1982), 21-28.

[20] A. Weil:"Courbes Algébriques et Variétés Abeliennes", Hermann, Paris, 1971.

[21] T. Zink: Degeneration of Shimura Surfaces and a Problem in Coding Theory, *Fundamental of Computation Theory, Lectures Notes in Comput. Sci., 199*, Springer, Berlin, 1985, 503-511.