Universidade Federal do Rio de Janeiro

POLINÔMIOS DE CHEBYSHEV E CURVAS MAXIMAIS

Raquel Tavares Scarpelli

Dissertação apresentada para obtenção do grau de Mestre em Matemática, pela Universidade Federal do Rio de Janeiro.

Orientadora: Luciane Quoos Conte

Rio de Janeiro
Maio de 2007

RESUMO

POLINÔMIOS DE CHEBYSHEV E CURVAS MAXIMAIS

Raquel Tavares Scarpelli

Orientadora: Luciane Quoos Conte

Este trabalho, baseado no artigo *"On Chebyshev Polinomials and Maximal Curves"*, de Arnaldo Garcia e Henning Stichtenoth, tem como objetivo estudar algumas subextensões $E_i^{\omega}/\mathbb{F}_{q^2}$ ($q = p^n$, para algum primo ímpar p), $i = 1, 2$, do corpo de funções Hermitiano $\mathcal{H}/\mathbb{F}_{q^2}$, onde $E_i = \mathcal{H}^{\langle\lambda\rangle}$ para certos automorfismos λ e ω de $\mathcal{H}/\mathbb{F}_{q^2}$. Caracterizaremos, por meio de resultados sobre polinômios de Chebyshev, os lugares que se ramificam em E_1/E_1^{ω}, bem como o gênero do corpo de funções $E_2^{\omega}/\mathbb{F}_{q^2}$. Novamente utilizando resultados sobre polinômios de Chebyshev, encontraremos fórmulas explícitas (nas quais tais polinômios aparecem) para as equações das curvas maximais que envolvem os geradores de E_i^{ω}, $i = 1, 2$.

Palavras-chave: corpo de funções Hermitiano, gênero de um corpo de funções, polinômios de Chebyshev, curvas maximais.

ABSTRACT

CHEBYSHEV POLYNOMIALS AND MAXIMAL CURVES

Raquel Tavares Scarpelli

Advisor: Luciane Quoos Conte

The present work, based on the paper *"On Chebyshev Polinomials and Maximal Curves"*, by Arnaldo Garcia and Henning Stichtenoth, is devoted to the study of some subextensions $E_i^{\omega}/\mathbb{F}_{q^2}$ ($q = p^n$, for some odd prime p), $i = 1, 2$, of the Hermitian function field $\mathcal{H}/\mathbb{F}_{q^2}$, where $E_i = \mathcal{H}^{\langle\lambda\rangle}$ for some automorphisms λ and ω of $\mathcal{H}/\mathbb{F}_{q^2}$. We characterize, by means of results about Chebyshev polynomials, the places which ramify in E_1/E_1^{ω}, as well as the genus of the function field $E_2^{\omega}/\mathbb{F}_{q^2}$. Using again some results on Chebyshev polynomials, we find explicit formulae (in which such polynomials appear) for the equations of the maximal curves involving the generators of E_i^{ω}, $i = 1, 2$.

Keywords: Hermitian function field, genus of a function field, Chebyshev polynomials, maximal curves.

Ao Carlinhos

AGRADECIMENTOS

Deixo aqui meus agradecimentos às pessoas que, de uma forma ou de outra, contribuíram para que este trabalho fosse possível.

Agradeço:

- Ao Carlinhos, por sua dedicação e paciência (infinitas!).
- Ao Sr. Carlos e à Sra. Anna Lúcia, pelo carinho com que me receberam.
- Ao Centro Nacional de Desenvolvimento Científico e Tecnológico - CNPq.
- A todos os professores e pesquisadores da UFRJ que, seja em cursos, seja em conversas, ajudaram-me a aprender a pouquíssima matemática que eu sei. Em particular, agradeço à Luciane, que me orientou nesse trabalho, e é, portanto, uma das principais responsáveis por ele (pelo que há de bom nele — pelos erros, a responsável sou eu).
- À Míriam Abdón e a Adilson Gonçalves, que aperfeiçoaram este trabalho com suas correções.
- À minha família, que soube compreender meu gosto pela matemática, e a todos os amigos de BH.
- Ao Sr. Rogério e ao colega Marcelo Tavares, pela assitência técnica.

Jogue o corpo para lá
Jogue o corpo para cá
O corpo e...
Tudo legal pra começar

Jadir de Castro e Daniel Marechal, " Lição de Baião "

Sumário

Introdução

Uma curva algébrica (projetiva, não-singular e irredutível) cujo modelo afim é dado por $f(x,y) = 0$ sobre um corpo finito $\mathbb{F}_{q^2}$, onde $q = p^n$ para algum primo p, é maximal se $\mathcal{N}_{\mathbb{F}_{q^2}}\mathbb{F}_{q^2}(x,y) = q^2 + 1 + 2gq$, onde $\mathcal{N}_{\mathbb{F}_{q^2}}\mathbb{F}_{q^2}(x,y)$ é o número dos lugares racionais de $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}$ e g é o gênero desse corpo de funções. Nesse caso, também dizemos que o corpo de funções $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}$ é maximal ou que o corpo $\mathbb{F}_{q^2}(x,y)$ é maximal sobre $\mathbb{F}_{q^2}$.

Gilles Lachaud provou (Proposição 6, [L]) que se $f(x,y)$ é uma curva maximal sobre um corpo finito $\mathbb{F}_{q^2}$ e L é um subcorpo de $\mathbb{F}_{q^2}(x,y)$, então $L/\mathbb{F}_{q^2}$ é também maximal. Isso equivale a dizer que o corpo de funções $L/\mathbb{F}_{q^2}$ é gerado por funções que satisfazem uma equação de um modelo afim de uma curva maximal.

Dentre muitos problemas envolvendo curvas maximais $f(x,y) = 0$ sobre $\mathbb{F}_{q^2}$ está a obtenção de equações explícitas para tais subcorpos L de $\mathbb{F}_{q^2}(x,y)$. Este é um dos principais objetivos desta dissertação. Para alguns desses subcorpos, mostraremos que essas equações envolvem de maneira natural polinômios de Chebyshev. Além disso, usaremos propriedades algébricas desses polinômios para caracterizar os lugares que se ramificam em certas extensões de tais subcorpos.

A curva $x^{q+1} = y^q + y$ sobre $\mathbb{F}_{q^2}$ é uma curva maximal, como veremos no final do Capítulo 1. Ela é chamada curva Hermitiana e seu corpo de funções correspondente $\mathcal{H}/\mathbb{F}_{q^2}$, onde $\mathcal{H} = \mathbb{F}_{q^2}(x,y)$, é denominado corpo de funções Hermitiano. Neste trabalho, baseado no artigo "On Chebyshev Polinomials and Maximal Curves"([G-S]) de Arnaldo Garcia e Henning Stichtenoth, definiremos certos subgrupos do grupo de automorfismos de $\mathcal{H}$ e olharemos para alguns corpos fixos L por tais subgrupos.

O primeiro capítulo destina-se a apresentar ao leitor os principais resultados da Teoria de Corpos de Funções Algébricas que usaremos no texto. Merecem destaque o Teorema de Kummer e o Teorema 1.3.24 (para extensões de Kummer), os quais serão largamente utilizados no Capítulo 3.

O Capítulo 2 tem como objetivo definir polinômios de Chebyshev e apresentar propriedades a eles relacionados. Foram incluídos certos resultados sobre esses polinômios, os quais não aparecem no artigo original. Isso foi feito para que pudéssemos caracterizar

os lugares que se ramificam nas extensões dos subcorpos com os quais vamos trabalhar usando apenas os Capítulos 1, 2 e 3 (contrariamente ao artigo, que faz uso de resultados do paper "*On subfields of the Hermitian function field*", Compositio Math., de A. Garcia, H. Stichtenoth e C. P. Xing), além de permitir a generalização dos Teoremas 6.1 e 6.2 de [G-S]. O leitor perceberá também que substituímos o Teorema 3.1 e a Nota 3.2 de [G-S] pela Proposição 2.1.4, que já é suficiente para provarmos o Teorema 3.2.5 (Teorema 4.1 de [G-S]).

O Capítulo 3 desenvolve o artigo citado acima, na tentativa de obter, entre outras questões, equações explícitas para curvas maximais sobre $\mathbb{F}_{q^2}$ (q ímpar). Dado um divisor m de q^2-1, analisaremos o caso em que m divide $(q-1)$ e o caso em que m é divisor de $(q+1)$. Em ambos os casos, obteremos as equações das curvas maximais estudadas por meio de resultados relacionados a polinômios de Chebyshev, os quais aparecerão (como já era de se esperar) nas fórmulas das curvas. Para o caso em que m divide $(q+1)$, será possível, inclusive, calcular o gênero de alguns corpos de funções (em geral, essa é uma tarefa árdua). Ressaltamos a prova do Teorema 4.1 de [G-S], onde analisamos todos os casos.

É importante mencionar que alguns teoremas, lemas e proposições do Capítulo 1 terão suas demonstrações omitidas, a fim de não alongarmos o texto demasiadamente. Para tais, recomendamos [S].

Capítulo 1

Corpos de Funções Algébricas

1.1 Corpos de Funções Algébricas e Valorações

Definição 1.1.1. Um corpo de funções algébricas F/K em uma variável sobre K é uma extensão de corpos $F \supseteq K$ tal que F é uma extensão finita de $K(x)$ para algum $x \in F$ transcendente sobre K.

O corpo $\tilde{K} = \{z \in F;\ z \text{ é algébrico sobre } K\}$ é chamado o corpo de constantes de F/K.

Exemplo 1. O corpo de funções algébricas F/K onde $F = K(x)$ para algum $x \in F \backslash \tilde{K}$ é chamado de *corpo de funções racionais*.

Exemplo 2. Sejam K um corpo, x transcendente sobre K e $f(x, y) = 0$ um modelo afim de uma curva algébrica (projetiva, não-singular e irredutível) sobre K. $F = K(x, y)/K$ é um corpo de funções algébricas. Em particular, se $K = \mathbb{F}_{q^2}$ (onde $q = p^n$, p primo) e $x^{q+1} = y^q + y$, temos que $\mathcal{H}/K$ é o *corpo de funções Hermitiano*, onde $\mathcal{H} = K(x, y)$. A curva projetiva cujo modelo afim é dado pela equação $x^{q+1} = y^q + y$ é chamada *curva Hermitiana*.

Definição 1.1.2. Um anel de valoração do corpo de funções F/K é um anel O com as seguintes propriedades:

(*i*) $K \subsetneq O \subsetneq F$;

(*ii*) Para cada $z \in F$, $z \in O$ ou $z^{-1} \in O$.

O anel $P = O \backslash O^*$, onde $O^* = \{z \in O; \exists \omega \in O \text{ tal que } z.\omega = 1\}$, é o único ideal maximal próprio de O e é chamado um lugar de F/K. O anel quociente $O/P = F_P$ é o corpo residual em P e definimos $deg\, P = [F_P : K]$. Dado x em F, $x(P) := x\,(mod\, P)$ é a classe de x em F_P.

Os lugares de F/K de grau 1 são denominados *lugares racionais* de F/K.

O conjunto $\mathbb{P}_F = \{P; P \text{ é lugar de } F/K\}$ é o conjunto dos lugares de F/K. Ele é um conjunto infinito, conforme veremos no final da Seção 2.

Exemplo 3. Dado um polinômio não constante, mônico e irredutível $p(x) \in K[x]$, o conjunto $O_{p(x)} := \{\frac{f(x)}{g(x)};\ f(x), g(x) \in K[x] \ e\ p(x) \nmid g(x)\}$ é um anel de valoração do corpo de funções $K(x)/K$. De fato, $K \subsetneq O_{p(x)}$, já que $p(x) \in O_{p(x)} \backslash K$. Além disso, $O_{p(x)} \subsetneq K(x)$, pois $p(x)^{-1} \in K(x) \backslash O_{p(x)}$. Seja $q(x)/h(x) \in K(x)$. Sem perda de generalidade, podemos supor que $q(x)$ e $h(x)$ não têm fatores em comum. Assim, $p(x)$ não pode dividir ambos os polinômios ao mesmo tempo. Caso $p(x)$ não divida $h(x)$, temos que $q(x)/h(x)$ pertence a $O_{p(x)}$. E se $p(x)$ divide $h(x)$, então $[q(x)/h(x)]^{-1} \in O_{p(x)}$. Portanto, $O_{p(x)}$ é um anel de valoração de $K(x)/K$.

O conjunto $O_\infty := \{\frac{f(x)}{g(x)};\ f(x), g(x) \in K[x],\ \partial\, f(x) \leq \partial\, g(x)\}$ é também um anel de valoração do corpo de funções $K(x)/K$. Com efeito, $K \subsetneq O_\infty$, já que $p(x)^{-1} \in O_\infty \backslash K$. Além disso, $O_\infty \subsetneq K(x)$, já que $p(x) \in K(x) \backslash O_\infty$. Seja $q(x)/h(x) \in K(x)$; se $\partial\, q(x) \leq \partial\, h(x)$, então $q(x)/h(x) \in O_\infty$. Caso contrário, temos que $[q(x)/h(x)]^{-1} \in O_\infty$. Portanto, O_∞ é um anel de valoração de $K(x)/K$.

Veremos mais tarde que, de fato, esses são os únicos anéis de valoração do corpo de funções racionais.

A próxima Proposição mostra que um anel de valoração pode ser unicamente determinado por seu ideal maximal P.

Proposição 1.1.3. *Seja O um anel de valoração de F/K e P seu ideal maximal. Então:*

(i) $x \in F \setminus \{0\}$, $x \in P \iff x^{-1} \notin O$;

(ii) Para o corpo de constantes $\tilde{K}$ de F/K temos $\tilde{K} \subseteq O$ e $\tilde{K} \cap P = \{0\}$.

Demonstração. (*i*) Suponhamos que $x \in \mathrm{F}\backslash\{0\}$ e $x \in P$. Como P é um ideal próprio de O, temos que x^{-1} não pertence a O. Reciprocamente, se x^{-1} não pertence a O para

algum x pertencente a F, então x pertence O, pois O é um anel de valoração. Além disso, como x^{-1} não pertence a O^*, temos que x não pertence a O^*. Portanto, x pertence a P.

(ii) Seja $z \in \tilde{K}$. Suponhamos, por absurdo, que $z \notin O$. Logo, $z^{-1} \in O$. Como z é algébrico sobre K, z^{-1} também o é. Portanto, existem $a_i \in K$, $i = 1, \cdots, r$, tais que $a_r(z^{-1})^r + a_{r-1}(z^{-1})^{r-1} + \cdots + a_1 z^{-1} + 1 = 0$. Assim, $z^{-1}[a_r(z^{-1})^{r-1} + a_{r-1}(z^{-1})^{r-2} + \cdots + a_1] = -1$. Logo, $z = -[a_r(z^{-1})^{r-1} + a_{r-1}(z^{-1})^{r-2} + \cdots + a_1] \in K[z^{-1}] \subseteq O$. Então $z \in O$ e temos uma contradição. Agora provemos que $\tilde{K} \cap P = \{0\}$. Obviamente, $0 \in \tilde{K} \cap P$. Suponhamos que exista $y \neq 0$ tal que $y \in \tilde{K} \cap P$. Como $y \in P$, $y^{-1} \notin O$. Mas $y^{-1} \in F \cap \tilde{K} \subseteq \tilde{K} \subseteq O$. Contradição.

∎

Desse modo, O é unicamente determinado por P já que $O = \{z \in F;\ z^{-1} \notin P\}$ e escrevemos $O =: O_P$, que passa a ser chamado de *anel de valoração do lugar P*.

Proposição 1.1.4. *Seja F/K um corpo de funções algébricas. Então $z \in F$ é transcendente sobre K se, e somente se, [F:K(z)] $< \infty$.*

Demonstração. Como F/K é um corpo de funções, existe x em F transcendente sobre K tal que $F/K(x)$ é finita. Logo, z é algébrico sobre $K(x)$ e temos $p(z) = 0$ para algum $p(u) \in K(x)[u]$ não nulo. Como z não é algébrico sobre K, $p(u) \notin K[u]$. Logo, x é algébrico sobre $K(z)$ e $[K(x,z) : K(z)] \leq \partial\, p(z)$. Por outro lado, como $F/K(x)$ é finita, $F/K(x,z)$ também o é. Conseqüentemente, $F/K(z)$ é uma extensão finita.

Reciprocamente, se $F/K(z)$ é finita, então $F/K(z)$ é algébrica e como F/K é transcendente, z é transcendente sobre K. ∎

Proposição 1.1.5. *Se P é um lugar de F/K e $0 \neq x \in P$, então $deg\,(P) \leq [F : K(x)] < \infty$.*

Demonstração. Em primeiro lugar, notemos que $x \notin \tilde{K}$, pela Proposição 1.1.3(ii). E pela Proposição 1.1.4, $[F : K(x)] < \infty$. Assim, basta provarmos que se $z_1(P), z_2(P), ...,$ $z_n(P) \in F_P$ são linearmente independentes sobre K, então $z_1, , z_2, \cdots, z_n$ são também linearmente independentes sobre $K(x)$.

Sejam $z_1(P), z_2(P), ..., z_n(P)$ linearmente independentes sobre K. Suponha que exista $\phi_i \neq 0$ tal que $\sum_{i=1}^{n} \phi_i z_i = 0$, com $\phi_i \in K(x)$ para todo $i = 1, \cdots, n$. Sem perda de

generalidade, podemos supor que $\phi_i \in K[x]$ para $i = 1, 2, ..., n$ e que existe $j \in \{1, 2, ..., n\}$ tal que $x \nmid \phi_j$. Em outras palavras, $\phi_i = a_i + xg_i$ com $a_i \in K$ e $g_i \in K[x]$ e $a_j \neq 0$ para algum j. Como $x \in P$ e $g_i \in O_P$, temos $\phi_i(P) = a_i(P)$. Assim:

$$0(P) = \sum_{i=1}^{n} \phi_i(P)z_i(P) = \sum_{i=1}^{n} a_i(P)z_i(P) = a_j(P)z_j(P) + \sum_{i \neq j} a_i(P)z_i(P),$$

contradizendo a independência linear de $\{z_i(P)\}_{i=1,2,...,n}$ sobre K. ∎

Definição 1.1.6. Uma valoração discreta normalizada de F/K é uma função $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ com as seguintes propriedades:

(i) $v(x) = \infty \iff x = 0$;

(ii) $v(xy) = v(x) + v(y)$ $\forall x, y \in F$;

(iii) $v(x + y) \geq \text{mín}\{v(x), v(y)\}$ $\forall x, y \in F$;

(iv) $\exists z \in F$ com $v(z) = 1$;

(v) $v(a) = 0$ $\forall a \in K \backslash \{0\}$.

Proposição 1.1.7. *Seja v uma valoração discreta normalizada de F/K e x,y ∈ F com v(x)≠ v(y). Então v(x+y)= mín {v(x),v(y)}.*

Demonstração. Como $v(x) \neq v(y)$, pelo menos uma das valorações é finita. Podemos assumir, sem perda de generalidade, que $v(x) < v(y)$. Se $v(x + y) > \text{mín}\ \{v(x), v(y)\} = v(x)$, temos então que $v(x) = v((x + y) - y) \geq \text{mín}\{v(x + y), v(-y)\} = \text{mín}\{v(x + y), v(y)\} > v(x)$, uma contradição. ∎

Agora veremos como se relacionam os anéis de valoração de um corpo de funções F/K com as valorações discretas desse mesmo corpo.

Lema 1.1.8. *Sejam $P \in \mathbb{P}_F$, O_P seu anel de valoração, $0 \neq x \in P$ e $x_1, x_2, ..., x_n \in P$ tais que $x_1 = x$ e $x_i \in x_{i+1}P$ para $i = 1, 2, ..., n - 1$. Então $n \leq [F : K(x)] < \infty$.*

Demonstração. Como $0 \neq x \in P$, temos que $x \notin \tilde{K}$, pela Proposição 1.1.3(ii). Portanto, $[F : K(x)] < \infty$ (Proposição 1.1.4). Basta-nos então mostrar que o conjunto $\{x_i \in F;$ $i = 1, 2, ..., n\}$ é linearmente independente sobre $K(x)$. Suponha que exista $i \in \{1, \cdots, n\}$ tal que $0 \neq \phi_i \in K(x)$ e $\sum_{i=1}^{n} \phi_i x_i = 0$. Sem perda de generalidade, podemos assumir

que cada $\phi_i \in K[x]$ e que existe $j \in \{1, 2, ..., n\}$ tal que $x \nmid \phi_j$. Sejam $a_i := \phi_i(0)$ e $j := \text{máx}\{r \in \{1, 2, ..., n\}; a_r \neq 0\}$.

Como $x_i \in x_j P$ e $\phi_i = xg_i$ para $i > j$ e para algum $g_i \in K[x]$, temos que

$$-\phi_j x_j = \sum_{i \neq j} \phi_i x_i \quad e \quad -\phi_j = \sum_{i<j} \phi_i \frac{x_i}{x_j} + \sum_{i>j} \frac{x}{x_j} g_i x_i.$$

Logo, $\phi_j \in P$. E como $a_j = \phi_j - xg_j$ para algum $g_j \in K[x] \subset O$, temos que $a_j \in P$, contradizendo o item (ii) da Proposição 1.1.3.

∎

Teorema 1.1.9. *Sejam O um anel de valoração de F/K e P seu ideal maximal. Então:*

(i) P é um ideal principal;

(ii) Se $P = tO$, então qualquer $0 \neq z \in F$ pode ser escrito de maneira única como $z = t^n u$ para certos $u \in O^*$, $n \in \mathbb{Z}$. Nesse caso, t é chamado elemento primitivo (ou uniformizante local) de P.

Demonstração. (i) Suponhamos que P não seja um ideal principal de O. Assim, $P \neq xO$ para todo $x \in P$. Em particular, existe $0 \neq x_1 \in P$ tal que $P \neq x_1 O$. Conseqüentemente, existe $x_2 \in P \backslash x_1 O$. Assim, $x_2 x_1^{-1} \notin O$. Pelo item (i) da Proposição 1.1.3 segue que $x_2^{-1} x_1 \in P$. Portanto, $x_1 \in x_2 P$. Analogamente, $P \neq x_2 O$ e existe $x_3 \in P \backslash x_2 O$ tal que $x_2 \in x_3 P$. Indutivamente, obtemos uma seqüência x_1, x_2, x_3, ... em P satisfazendo $x_i \in x_{i+1} P$ para todo i ≥ 1. Assim, obtivemos uma infinidade de funções em F linearmente independentes sobre $K(x)$, contradizendo o Lema 1.1.8.

(ii) Primeiro provemos a unicidade da representação.

Seja $z \in F \setminus \{0\}$ e suponha que $z = t^n u$, para algum $n \in \mathbb{Z}$ e $u \in O^*$, e $z = t^m v$ para algum $m \in \mathbb{Z}$ e $v \in O^*$. Se $m = n$, o resultado é imediato. Suponha, sem perda de generalidade, que $m > n$. Temos então que $t^{m-n} = uv^{-1} \in O^*$, o que é um absurdo. Logo, $m = n$, donde segue que $u = v$.

Para provarmos a existência, consideremos $0 \neq z \in F$. Assumiremos, sem perda de generalidade, que $z \in O$. Se $z \in O^*$, então $z = t^0 z$. Basta, portanto, considerarmos $z \in P = tO$. Como $z \neq 0$, $z \notin \tilde{K}$ e, portanto, $[F : K(z)] < \infty$. Temos $tO \supset t^2 O \supset ... \supset t^n O \supset ...$ e, desse modo, a seqüência $x_1 = z$, $x_j = t^{m-(j-1)}$ para $j \in \mathbb{N}$ satisfaz $x_j \in t^{m-j+1} O = t^{m-j} P = x_{j+1} P$ para todo $j \in \mathbb{N}$ e pelo Lema 1.1.8, existe $m \geq 1$ máximo

com a propriedade $z \in t^m O$. Então, $z = t^m u$ para algum $u \in O$. Se $u \in P$, $u = t\omega$ para algum $\omega \in O$. Assim: $z = t^{m+1}\omega \in t^{m+1}O$, contrariando a maximalidade de m. Concluímos que $u \in O \backslash P = O^*$. ∎

Definição 1.1.10. Para qualquer lugar $P \in \mathbb{P}_F$ associamos uma função $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ do seguinte modo: escolha um elemento primitivo de P. Dado $z \in F \backslash \{0\}$, existe uma única representação $z = t^n u$ para algum $n \in \mathbb{Z}$ e $u \in O^*$. Definimos $v_P(z) = n$ e $v_P(0) = \infty$ (observe que tal Definição independe da escolha de t).

Agora já temos condições de relacionar um anel de valoração de F/K com uma valoração do mesmo.

O Teorema seguinte nos ajudará a mostrar como são os lugares do corpo de funções $K(x)/K$.

Teorema 1.1.11. *Seja F/K um corpo de funções.*

(i) Para cada $P \in \mathbb{P}_F$, a função v_P definida em (1.1.10) é uma valoração discreta normalizada de F/K. Além disso, $O_P = \{z \in F;\, v_P(z) \geq 0\}$, $O_P^* = \{z \in F;\, v_P(z) = 0\}$ e $P = \{z \in F;\, v_P(z) > 0\}$. Um elemento $x \in F$ é um elemento primitivo de P se, e somente se, $v_P(x) = 1$;

(ii) Reciprocamente, se v é uma valoração discreta normalizada de F/K, o conjunto $P := \{z \in F;\, v(z) > 0\}$ é um lugar de F/K e $O_P = \{z \in F;\, v(z) \geq 0\}$ é o anel de valoração correspondente.

(iii) Qualquer anel de valoração $O \subset F/K$ é um subanel próprio maximal de F.

Demonstração. Seja t um elemento primitivo de P.

(i) Obviamente, v_P satisfaz as propriedades (i), (ii), (iv) e (v) da Definição 1.1.6. Para provarmos a propriedade (iii), consideremos $x, y \in F$ com $v_P(x) = n$ e $v_P(y) = m$. Podemos supor $n < m < \infty$ (de fato, se $n = m = \infty$, teríamos $x = y = 0$ e a propriedade (iii) estaria provada e se $n < m = \infty$, teríamos $y = 0$ e a propriedade (iii) mais uma vez seria verificada). Sejam $x = t^n u_1$ e $y = t^m u_2$ com $u_1, u_2 \in O_P^*$, então $x + y = t^n(u_1 + t^{m-n}u_2) = t^n z$ com $z := u_1 + t^{m-n}u_2 \in O_P$. Logo, $v_P(x + y) = n.v_P(t) + v_P(z) = n + v_P(z) \geq n = \text{mín}\{m, n\} = \text{mín}\{v_P(x), v_P(y)\}$. Logo, v_P é uma valoração discreta normalizada de F/K. As demais asserções seguem imediatamente do Teorema 1.1.9(ii) e da Definição 1.1.10.

(*ii*) O_P é subanel de F (de fato, dados $x, y \in O_P$, temos $v(x+y) \geq 0$, $v(xy) \geq 0$ e que $0 \in O_P$). Além disso, dado $z \in F$ temos $v(z^{-1}) = -v(z)$. Portanto, $z^{-1} \in O_P$ ou $z \in O_P$. Resta-nos mostrar que $K \subsetneq O_P \subsetneq F$. Obviamente, $K \subset O_P$. No entanto, $K \neq O_P$ pois $v(t) = 1 \neq 0$, o que implica que $t \notin K$. Também temos, por definição, que $O_P \subset F$. Mas $O_P \neq F$ já que $v(t^{-1}) = -1$, e, portanto, $t^{-1} \notin O_P$. Assim, O_P é um anel de valoração de F/K. Agora mostremos que P é o lugar de F/K correspondente, ou seja, que $P = O_P \backslash O_P^*$. Obviamente, $P \subset O_P$. Se $z \in O_P^*$, existe $w \in O_P$ com $zw = 1$. Como $0 = v(1) = v(zw) = v(z) + v(w)$, temos que $0 \leq v(w) = -v(z)$ e $z \notin P$. Logo, $O_P^* \subset O_P \setminus P$. Reciprocamente, se $z \in O_P \setminus P$, temos $v(z) = v(z^{-1}) = 0$, donde $z^{-1} \in O_P$. Como O_P é um anel, $zz^{-1} = 1 \in O_P$ e $z \in O_P^*$. Portanto, $O_P \setminus P \subset O_P^*$ e está provado (*ii*).

(*iii*) Sejam O_P um anel de valoração de F/K e P seu lugar correspondente. Precisamos provar que se $z \in F \backslash O_P$ (portanto, $z^{-1} \in O_P$), então $O_P[z] = F$. Basta mostrarmos que $F \subset O_P[z]$, pois a outra inclusão é imediata. Seja $y \in F$. Temos para $s \in \mathbb{N}$ suficientemente grande que $v_P(yz^{-s}) = v_P(y) - s.v_P(z) \geq 0$. Portanto, $yz^{-s} \in O_P$ e temos que $y \in O_P[z]$. ∎

Definição 1.1.12. Sejam $z \in F$ e $P \in \mathbb{P}_F$. Dizemos que P é um *zero de ordem m* (resp. *pólo de ordem m*) de z se $v_P(z) = m \ > 0$ (resp. se $v_P(z) = -m \ < 0$).

Exemplo 4. Vimos que dado um polinômio não constante, mônico e irredutível $p(x) \in K[x]$, os conjuntos $O_{p(x)} := \{\frac{f(x)}{g(x)};\ f(x), g(x) \in K[x] \text{ e } p(x) \nmid g(x)\}$ e $O_\infty := \{\ \frac{f(x)}{g(x)};\ f(x), g(x) \in K[x],\ deg\, f(x) \leq deg\, g(x)\}$ são anéis de valoração do corpo de funções $K(x)/K$ (veja Exemplo 3). Os conjuntos $P_{p(x)} := \{\ \frac{f(x)}{g(x)};\ p(x), g(x) \in K[x],\ p(x) \mid f(x) \text{ e } p(x) \nmid g(x)\ \}$ e $P_\infty := \{\ \frac{f(x)}{g(x)};\ f(x), g(x) \in K[x],\ deg\, f(x) \ > deg\, g(x)\ \}$ são, respectivamente, seus lugares correspondentes (Proposição 1.1.3(*i*)). O lugar P_∞ é chamado lugar no infinito de $K(x)$. Se $p(x) = x + a$, $a \in K$, denotamos $P_{p(x)}$ por P_a.

Temos também que $p(x)$ é um elemento primitivo de $P = P_{p(x)}$ e a valoração discreta normalizada correspondente v_P é assim definida: se $z \in K(x)\backslash\{0\}$ é dada por $z = p(x)^n.(f(x)/g(x))$ com $n \in \mathbb{Z}$, $f(x), g(x) \in K[x]$ com $p(x) \nmid f(x)$ e $p(x) \nmid g(x)$, então $v_P(z) = n$. Além disso, $K(x)_P = O_P/P \simeq K[x]/\langle p(x)\rangle$. Consequentemente, $deg\, P = deg\, p(x)$.

Para o lugar no infinito, temos $deg\, P_\infty = 1$, já que $P_\infty = x^{-1}O_\infty$. A valoração

discreta normalizada v_∞ correspondente é dada da seguinte forma: $v_\infty(f(x)/g(x)) = deg\, g(x) - deg\, f(x)$, onde $f(x), g(x) \in K[x]$.

Teorema 1.1.13. *Seja $x \in F$ transcendente sobre K. Todo lugar de $K(x)/K$ assume uma das formas dadas no Exemplo* 4.

Demonstração. Vamos supor que $P \in \mathbb{P}_F \backslash \{P_\infty\}$ e que O_P seja o anel de valoração correspondente.

(a) Suponhamos que $x \in O_P$. Nesse caso, $K[x] \subset O_P$ e $J = K[x] \cap O_P$ é um ideal primo de $K[x]$. A aplicação de classes residuais induz uma injeção $K[x]/J \longmapsto [K(x)]_P$. Como $deg\,(P) < \infty$, temos $J \neq \{0\}$ e, portanto, existe $p(x) \in K[x]$ mônico e irredutível tal que $J = p(x)K[x]$. Qualquer $g(x) \in K[x]$ tal que $p(x) \nmid g(x)$ não está em J e, portanto, $g(x) \notin P$. Assim, $1/g(x) \in O_P$ e concluímos que:

$$O_{p(x)} = \{\frac{f(x)}{g(x)}; f(x), g(x) \in K[x], p(x) \nmid g(x)\} \subset O_P.$$

Como anéis de valoração são subanéis próprios maximais de F, temos que $O_{p(x)} = O_P$.

(b) Suponha que $x \notin O_P$. Concluímos que $K[x^{-1}] \subset O_P$, $x^{-1} \in P \cap K[x^{-1}]$ e, portanto, $P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$. Como em (a),

$$O_P \supseteq O_P \cap K[x^{-1}] \supseteq \{\frac{f(x^{-1})}{g(x^{-1})}; f(x^{-1}), g(x^{-1}) \in K[x^{-1}], x^{-1} \nmid g(x^{-1})\}$$

$$= \{\frac{a_0 + ... + a_n x^{-n}}{b_0 + ... + b_m x^{-m}}; b_0 \neq 0\}$$

$$= \{\frac{a_0 x^{m+n} + ... + a_n x^m}{b_0 x^{m+n} + ... + b_m x^n}; b_0 \neq 0\}$$

$$= \{\frac{h(x)}{l(x)}; deg(l(x)) \geq deg(h(x))\} = O_\infty.$$

Repetindo o argumento de (a), obtemos $O_P = O_\infty$ e $P = P_\infty$. ∎

Veremos agora que dado o corpo de funções F/K, temos $\mathbb{P}_F \neq \varnothing$. Em seguida, mostraremos que todo elemento de F transcendente sobre K possui pelo menos um pólo e um zero em F. Isso será importante quando provarmos que F/K possui um número infinito de lugares.

Teorema 1.1.14. *Seja F/K um corpo de funções e $R \subset F$ subanel de F com $R \supset K$. Se existe um ideal $\{0\} \neq I \subsetneq R$, então existe um lugar $P \in \mathbb{P}_F$ tal que $I \subset P$ e $R \subset O_P$.* ∎

Corolário 1.1.15. *Se $z \in F$ é transcendente sobre K, então z tem ao menos um zero e um pólo em F.*

Demonstração. Basta considerar o ideal $I = zK[z] \subsetneq K[z]$. Pelo Teorema 1.1.14, seque que existe $P \in \mathbb{P}_F$ tal que $z \in P$ e existe P' tal que $z^{-1} \in P'$. Portanto, P e P' são um zero e um pólo de z, respectivamente. ∎

Lema 1.1.16. *Sejam F/K um corpo de funções e P_1, ..., P_n zeros de uma função $x \in F$. Então:*

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

∎

Proposição 1.1.17. *Em um corpo de funções F/K, qualquer função $x \in F\backslash\{0\}$ tem somente um número finito de zeros e pólos.*

Demonstração. Se $x \in \tilde{K} \setminus \{0\}$, a Proposição 1.1.3 garante que para todo $P \in \mathbb{P}_F$ tem-se $\tilde{K} \setminus \{0\} \subset O_P$ e $(\tilde{K} \setminus \{0\}) \cap P = \varnothing$. Conseqüentemente, $v_P(x) = 0$ para todo x em $\tilde{K} \setminus \{0\}$ e $P \in \mathbb{P}_F$. Portanto, x não possui nem zeros e nem pólos em F/K.

Se x é transcendente sobre K, o número de zeros é menor ou igual a $[F : K(x)]$, pelo Lema 1.1.16. E como x é transcendente sobre K, temos que $[F : K(x)] < \infty$. Isso prova que o número de zeros de x é finito. O mesmo argumento usado para x^{-1} mostra que o número de pólos de x é finito. ∎

1.2 Divisores e o gênero de um corpo de funções

O principal objetivo desta seção é definir o gênero de um corpo de funções.

Iniciemos esta seção definindo o que é um divisor de F/K.

Definição 1.2.1. O grupo de divisores $\mathcal{D}_F$ de F/K é o grupo livre (aditivo) gerado pelos lugares de F/K. Seus elementos são chamados divisores de F/K, isto é, se $D \in \mathcal{D}_F$, então $D = \sum_{P \in \mathbb{P}_F} n_P.P$, onde $n_P \in \mathbb{Z}$ e $n_P = 0$ para quase todo P.

Se $D = \sum_{P\in\mathbb{P}_F} n_P.P$ e $D' = \sum_{P\in\mathbb{P}_F} n'_P.P$, definimos a soma de D e D' como $D+D' = \sum_{P\in\ \mathbb{P}_F} (n_P + n'_P).P$ e o zero do grupo $\mathcal{D}_F$ como o divisor $D:= 0$, no qual $n_P = 0$ para todo $P \in \mathbb{P}_F$.

Para $Q \in \mathbb{P}_F$ e $D = \sum_{P\in\mathbb{P}_F} n_P.P$, definimos $v_Q(D) := n_Q$. Uma ordenação parcial em $\mathcal{D}_F$ é definida por $D_1 \leq D_2$ se, e somente se, $v_P(D_1) \leq v_P(D_2)$ para todo $P \in \mathbb{P}_F$. Finalmente, definimos o grau de um divisor como $deg\, D = \sum_{P\in\mathbb{P}_F} v_P(D).deg\, P$ e induzimos um homomorfismo $deg : \mathcal{D}_F \longrightarrow \mathbb{Z}$.

Definição 1.2.2. Sejam $x \in F\backslash\{0\}$ e Z (resp.N) o conjunto dos zeros (resp. de pólos) de x em $\mathbb{P}_F$. Definimos:

$$(x)_0 := \sum_{P\in Z} v_P(x).P \text{ o divisor de zeros de } x \ ;$$

$$(x)_\infty := \sum_{P\in N} -v_P(x).P \text{ o divisor de pólos de } x \ ,$$

$$(x) := (x)_0 - (x)_\infty \text{ o divisor principal de } x \ .$$

Concluímos então que $x \in \tilde{K}\backslash\{0\}$ se, e somente se, $(x) = 0$.

Dizemos que D e D' são equivalentes (notação: $D \sim D'$) se $D = D' + (x)$ para algum $x \in F\backslash\{0\}$.

Para um divisor $A \in \mathcal{D}_F$, definimos $\mathcal{L}(A):= \{\ x \in F; (x) \geq -A\} \cup \{0\}$.

Proposição 1.2.3. *Sejam F/K um corpo de funções algébricas e A um divisor de F/K. Valem as seguintes afirmativas:*

(i) $x \in \mathcal{L}(A)$ se, e somente se, $v_P(x) \geq -v_P(A)$ para todo $P \in \mathbb{P}_F$;

(ii) $\mathcal{L}(A) \neq \{0\}$ se, e somente se, existe um divisor $A' \geq 0$ tal que $A' \sim A$;

(iii) $\mathcal{L}(A)$ é um espaço vetorial sobre K e definimos $dim\,(A):= dim\,(\mathcal{L}(A))$.

(iv) $\mathcal{L}(A) \simeq \mathcal{L}(A')$ sempre que $A' \sim A$; ∎

Teorema 1.2.4. *Sejam A, B divisores de F/K com $A \leq B$. Então $\mathcal{L}(A) \subset \mathcal{L}(B)$ e $dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq$ deg B - deg A.*

Demonstração. Seja $x \in \mathcal{L}(A)$, então $(x) \geq -A \geq -B$, logo $x \in \mathcal{L}(B)$, ou seja, $\mathcal{L}(A) \subset L(B)$. Como $A \leq B$, podemos supor $B = A + P$ (o caso geral, segue por indução). Tome $y \in F$ tal que $v_P(y)= 1$ e defina $t:= y^{v_P(B)}$. Temos $v_P(t) = v_P(B)=$

$v_P(A) + 1$. Para $x \in \mathcal{L}(B)$, temos $v_P(x) \geq -v_P(B) = -v_P(t)$. Portanto, $xt \in O_P$. Definindo $\psi : \mathcal{L}(B) \longrightarrow F_P$ como $\psi(x)= (xt)(P)$, temos que ψ é linear e que $Ker(\psi)= \{x \in \mathcal{L}(B);\ xt \in P\}= \{x \in \mathcal{L}(B);\ v_P(x) > -v_P(t)\ \}= \{x \in \mathcal{L}(B);\ v_P(x) \geq -v_P(t) + 1\}= \{x \in \mathcal{L}(B);\ v_P(x) \geq -v_P(A)\}= \mathcal{L}(A)$. Assim, existe um isomorfismo $\phi : \mathcal{L}(B)/\mathcal{L}(A) \longrightarrow Im\,(\psi)$ e, portanto:

$$dim\,(\mathcal{L}(B)/\mathcal{L}(A)) \leq dim F_P = deg\,B - deg\,A.$$

∎

Proposição 1.2.5. *Qualquer divisor principal tem grau zero, ou seja, $deg(x)_0= deg(x)_\infty=$ [F: K(x)], $x \in F \setminus \tilde{K}$.* ∎

Teorema 1.2.6. *Sejam $A, A' \in \mathcal{D}_F$ com $A \sim A'$. Então $dim(A) = dim(A')$ e $deg(A) = deg(A')$.*

Demonstração. O resultado segue da Proposição 1.2.5 e da Proposição 1.2.3(iv). ∎

A próxima Proposição é o último passo para a definição do gênero de F/K.

Proposição 1.2.7. *Existe uma constante $\lambda \in \mathbb{Z}$ tal que, para todo $A \in \mathcal{D}_F$, deg A - dim A $\leq \lambda$.*

Demonstração. Primeiro observemos que se $A_1 \leq A_2$, então $deg\,A_1$ - $dim\,A_1 \leq deg\,A_2$ - $dim\,A_2$, pelo Teorema 1.2.4. Fixemos $x \in F \setminus \tilde{K}$ e consideremos o divisor $B:= (x)_\infty= \sum_{i=1}^{r} -v_{P_i}(x)P_i$, onde $P_1, P_2, ..., P_r$ são os pólos de x. Então $deg\,B= \sum_{i=1}^{r} v_{P_i}(x^{-1}).deg\,P_i \leq [F : K(x)] =: n$ (pelo Lema 1.1.16). Escolhemos $u_1, u_2, ..., u_n$ uma base de $F/K(x)$ e um divisor $C \geq 0$ tal que $(u_i) \geq -C$ para $i = 1, ..., n$. Logo,

$$dim\,(lB + C) \geq n(l + 1) \qquad (1)$$

pois $x^i u_j \in \mathcal{L}(lB + C)$ para todo $l \geq 0$, $0 \leq i \leq l$ e $1 \leq j \leq n$ e são linearmente independentes sobre K. Por outro lado,

$$dim(lB + C) \leq dim, (lB) + deg\,C \quad (2)$$

pelo Teorema 1.2.4. Combinando (1) e (2), obtemos: $(l + 1)deg\,B \leq dim\,(lB + C) \leq dim\,(lB) + deg\,C$, implicando em $dim\,(lB) \geq deg\,(lB) + deg\,(B)$ - $deg\,(C)=$

$= deg\,(lB) + [F : K(x)]$ - $deg\,(C)$ (de fato, pela Proposição 1.2.5, $deg\,(B) = [F : K(x)]$). Fazendo-se $\lambda := deg\,(C) - [F : K(x)]$, obtemos o resultado para o divisor lB. Agora provemos isso para $A \in D_F$ qualquer.

Escolha um divisor $A_1 \geq A$ tal que $A_1 \geq 0$. Então $dim\,(lB - A_1) \geq dim\,(lB)$ - $deg\,(A_1)$ $\geq deg\,(lB)$ - λ - $deg\,(A_1)$ > 0 para l suficientemente grande. Como $dim(lB - A_1) > 0$, $\mathcal{L}(lB - A_1) \neq \{0\}$. Portanto, existe $0 \neq z \in \mathcal{L}(lB - A_1)$. Assim, -(z) $\leq lB - A_1$. Defindo $D := A_1 - (z)$, obtemos que $A_1 \sim D$ e $D \leq lB$. Pelos Teoremas 1.2.4 e 1.2.6, temos que $deg\,(A)$ - $dim\,(A) \leq deg\,(A_1)$ - $dim\,(A_1) = deg\,(D)$ - $dim\,(D) \leq deg\,(lB)$ - $dim\,(lB) \leq \lambda$. ∎

Definição 1.2.8. O gênero g de F/K é $g := \text{máx}\{deg\,(A) - dim(A) + 1\,;\ A \in \mathcal{D}_F\}$, o qual está bem definido pela Proposição 1.2.7. Além disso, escolhendo $A = 0$, vê-se que $g \geq 0$.

Teorema 1.2.9. *Se A é um divisor de F/K de grau $\geq 2g$ - 1, então $dim\,(A) = deg\,(A)$ + 1 - g.* ∎

Teorema 1.2.10. *Se F/K é um corpo de funções racionais, então F/K tem gênero zero.*

Demonstração. Seja $F = K(x)$ para algum $x \in F$ transcendente sobre K. O único pólo de x é P_∞ e $deg(P_\infty) = 1$. Além disso x^{-1} é um elemento primitivo desse lugar. Logo,

$$(x)_\infty = \sum_{P \in N} -v_P(x).P = -v_\infty(x)P_\infty = P_\infty.$$

Considere o espaço vetorial $\mathcal{L}(rP_\infty)$, onde $r \geq 0$. Para todo $0 \leq \lambda \leq r$, temos $\lambda P_\infty \leq rP_\infty$ e, portanto, $\mathcal{L}(\lambda P_\infty) \subset \mathcal{L}(rP_\infty)$. Obviamente, $1 \in \mathcal{L}(P_\infty) \subset \mathcal{L}(rP_\infty)$. Como $(x^\lambda) = \lambda(x) = \lambda[(x)_0 - (x)_\infty] = \lambda[(x)_0 - P_\infty] \geq -\lambda P_\infty$, temos que $x^\lambda \in \mathcal{L}(\lambda P_\infty)$para todo $0 \leq \lambda \leq r$. Assim: 1, x, x^2, ..., $x^r \in \mathcal{L}(rP_\infty)$ e pelo Teorema 1.2.9, $(r+1) \leq dim\,(rP_\infty) = deg\,(rP_\infty)$ $+ 1 - g = r + 1$ - g para r suficientemente grande. Logo, $(r+1) \leq r + 1 - g$, o que implica que $g \leq 0$. Como $g \geq 0$ sempre, temos $g = 0$. ∎

Teorema 1.2.11. *(Teorema da Aproximação) Sejam $S \subsetneq \mathbb{P}_F$ e $P_1, ..., P_r \in S$. Suponha que $x_1, ..., x_r \in F$ e $n_1, ..., n_r \in \mathbb{Z}$. Então existe $x \in F$ tal que $v_{P_i}(x - x_i) = n_i$, i= 1, ..., r, e $v_P(x) \geq 0$ para todo $P \in S \backslash \{P_1, ..., P_r\}$.* ∎

Como conseqüência do Teorema da Aproximação, temos que F/K possui uma infinidade de lugares.

Corolário 1.2.12. *F/K possui uma infinidade de lugares.*

Demonstração. Suponha que haja apenas um número finito de lugares $P_1, P_2, ..., P_n$ em F/K e considere os conjuntos $S_1 = \{P_1, ..., P_{n-1}\}$ e $S_2 = \{P_2, ..., P_n\}$ (note que $n \leq 2$ pois todo elemento de F transcendente sobre K possui pelo menos um zero e um pólo). Pelo Teorema da Aproximação, existe $0 \neq x \in F$ satisfazendo $v_{P_i}(x) = -2$ para $i = 1, 2, ..., n-1$. Assim, $v_{P_n}(x) > 0$, pois do contrário x não teria zeros e, portanto, seria algébrico. Analogamente, existe $0 \neq y \in F$ satisfazendo $v_{P_i}(y) = -1$ para $i = 2, 3, ..., n$ e $v_{P_1}(x) > 0$. Assim, temos: $v_{P_i}(x+y) = -2$ para $i = 2, 3, ..., n-1$, $v_{P_1}(x+y) = -2$ e $v_{P_n}(x+y) = -1$. Logo, $x+y$ não possui zeros e é algébrico. Conseqüentemente, $v_{P_i}(x+y) = 0$ para todo $i \in \{1, 2, ..., n\}$, o que é uma contradição. ∎

Corolário 1.2.13. *O corpo de constantes $\tilde{K}$ de um corpo de funções algébricas F/K é uma extensão finita de K.*

Demonstração. Seja $P \in \mathbb{P}_F$. Como $\tilde{K} \subset O_P$ pode ser imerso naturalmente em F_P via $O_P \longrightarrow F_P$ e $deg\ (P) < \infty$ (Proposição 1.1.5), segue que $[\tilde{K} : K] \leq [F_P : K] = deg\ (P) < \infty$. ∎

1.3 Extensões de Kummer

Nessa seção provaremos os dois principais teoremas desse capítulo: o Teorema de Kummer (Teorema 1.3.12) e o Teorema 1.3.24 (para extensões de Kummer).

Definição 1.3.1. Um corpo de funções algébricas F'/K' é uma extensão algébrica de F/K se $F' \supset F$ é uma extensão algébrica e $K' \supset K$. Também dizemos que F'/K' é uma extensão finita de F/K se $[F' : F] < \infty$.

Dada uma extensão F'/K' de F/K, dizemos que um lugar $P' \in \mathbb{P}_{F'}$ está acima de $P \in \mathbb{P}_F$ (ou é uma extensão de P em F') se $P \subseteq P'$. Expressamos essa inclusão através da notação $P'|P$.

O número natural $f(P'|P) = [F'_{P'} : F_P]$ é o grau relativo de P' sobre P.

Ao longo dessa seção, dados um corpo de funções F/K e uma extensão F'/K' dele, K será sempre considerado um corpo perfeito.

Proposição 1.3.2. *Seja F'/K' uma extensão finita de um corpo de funções algébricas F/K. Então $[K' : K] < \infty$.*

Demonstração. Com efeito, como F'/F é finita, F'/K pode ser considerado um corpo de funções algébricas com corpo de constantes $\tilde{K}'$. Pelo Corolário 1.2.13, segue que $[\tilde{K}' : K] < \infty$. Como $K' \subset \tilde{K}'$, temos o resultado. ∎

Proposição 1.3.3. *Seja F'/K' uma extensão algébrica de F/K. Suponha que P (resp. P') seja um lugar de F/K (resp. F'/K'), que $O_P \subset F$ (resp. $O_{P'} \subset F$') seja o anel de valoração correspondente e v_P (resp. $v_{P'}$)a valoração correspondente. São equivalentes:*

(i) $P'|P$;

(ii) $O_P \subset O_{P'}$;

(iii) Existe um inteiro $e \geq 1$ tal que $v_{P'}(x) = e.v_P(x)$ para todo $x \in F$. Além disso, se $P'|P$, então $P = P' \cap F$ e $O_P = O_{P'} \cap F$

Demonstração. $(i) \Longrightarrow (ii)$: Suponha que $P'|P$ mas que $O_P \not\subset O_{P'}$. Então, existe $u \in F$ com $v_P(u) \geq 0$ e $v_{P'}(u) < 0$. Como $P \subset P'$, temos que $v_P(u)= 0$. Considere $t \in F$ tal que $v_P(t) = 1$. Desse modo, $t \in P'$ e $r := v_{P'}(t) > 0$. Conseqüentemente, $v_P(u^r t)= r.v_P(u) + v_P(t)= r.0+1= 1$ e $v_{P'}(u^r t)= r.v_{P'}(u) + v_{P'}(t) \leq$ -r+r= 0. Logo, $u^r t \in P$ mas $u^r t \notin P'$. Um absurdo.

$(ii) \Longrightarrow (iii)$: Suponhamos que $O_P \subset O_{P'}$. Note que se $y \in F$ satisfaz $v_P(y) = 0$, temos $y, y^{-1} \in O_{P'}$ e, conseqüentemente, $v_{P'}(y) = 0$. Afirmamos que $O_P = O_{P'} \cap F$. De fato, $O_P \subset F \cap O_{P'}$ e $F \cap O_{P'}$ é um subanel de F. Pelo Teorema 1.1.11(iii), segue que $O_P = O_{P'} \cap F$. Seja $t \in F$ tal que $v_P(t) = 1$; logo, $t^{-1} \notin O_P$ e pela Afirmação anterior, $t^{-1} \notin O_{P'}$. Conseqüentemente, $e := v_{P'}(t) \geq 1$. Tomando-se $x \in F\backslash\{0\}$, temos $v_P(x) =: r$ e $v_P(xt^{-r})= 0$. Assim, $v_{P'}(x) = v_{P'}(xt^{-r}) + v_{P'}(t^r)= r.v_{P'}(t)= v_P(x).e$. Para $x = 0$, a igualdade acima é imediata.

$(iii) \Longrightarrow (i)$: Se existe um inteiro $e \geq 1$ tal que $v_{P'}(x) = e.v_P(x)$ para todo $x \in F$, então dado $y \in P$, temos: $v_{P'}(y) = e.v_P(y) \geq 1.v_P(y) \geq 1.1= 1$ e, portanto, $y \in P'$. ∎

Definição 1.3.4. Seja F'/K' uma extensão algébrica de F/K, e seja $P' \in \mathbb{P}_{F'}$ com $P'|P$, $P \in \mathbb{P}_F$. O inteiro $e =: e(P'|P)$ satisfazendo $v_{P'}(x) = e.v_P(x)$ para todo $x \in F$ é chamado *índice de ramificação de P' sobre P.*

Dizemos que $P'|P$ é *ramificado* se $e(P'|P) > 1$ e que $P'|P$ é *não ramificado*, caso contrário.

P é ramificado em F'/F se existir ao menos um lugar P' de F'/K' tal que $P'|P$ seja ramificado; P é não-ramificado, caso contrário. Finalmente, dizemos que P é totalmente ramificado em F'/F se existir um único lugar P' em F'/K' que esteja acima de P e $e(P'|P)$=$[F' : F]$.

Proposição 1.3.5. *Seja F'/K' uma extensão algébrica de F/K e P' um lugar de F'/K' acima de $P \in \mathbb{P}_F$. Se F"/K"é uma extensão algébrica de F'/K' e P"$\in \mathbb{P}_{F''}$ está acima de P', então e(P"|P)= e(P"|P')e(P'|P).*

Demonstração. Da hipótese, resulta que F"/K" é uma extensão algébrica de F/K. Portanto, dado $x \in F$, temos $v_{P''}(x) = e(P''|P)v_P(x)$.

Por outro lado, como $P''|P'$, temos também que $v_{P''}(x) = e(P''|P')v_{P'}(x)$. Logo, $e(P''|P)v_P(x) = e(P''|P')v_{P'}(x) = e(P''|P')e(P'|P)v_P(x)$. Como $e(P'|P)$ independe da escolha de $x \in F$, dependendo apenas de P' e de P, podemos tomar $x \in F$ tal que $v_P(x) = 1$ e a Proposição está demonstrada. ∎

É natural perguntarmo-nos se, caso F'/K' seja uma extensão algébrica de F/K e $P \in \mathbb{P}_F$, existe uma extensão de P em F'/F. Reciprocamente, também gostaríamos de saber se dado $P' \in \mathbb{P}_{F'}$, existe $P \in \mathbb{P}_F$ tal que $P'|P$. A resposta para ambas as perguntas é dada na próxima Proposição.

Proposição 1.3.6. *Seja F'/K' uma extensão algébrica de F/K.*

(i) Para qualquer lugar $P' \in \mathbb{P}_{F'}$ existe exatamente um lugar $P \in \mathbb{P}_F$ tal que $P'|P$ e $P = P' \cap F$;

(ii) Reciprocamente, todo $P \in \mathbb{P}_F$ tem pelo menos uma, e no máximo um número finito, de extensões $P' \in \mathbb{P}_{F'}$.

Demonstração. (i) Começamos provando a seguinte **Afirmação**: existe $z \in F \setminus \{0\}$ com $v_{P'}(z) \neq 0$. Suponhamos que seja falsa. Seja $t \in F'$ um elemento primitivo de

P'. Como F'/F é algébrica, t é raiz de $f(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in F[x]$ com $c_n x^n \neq 0 \neq c_0$. Como $c_0 \in F$, temos $v_{P'}(c_0) = 0$. Conseqüentemente, $v_{P'}(f(t)) = v_{P'}(\sum_{i=0}^{n} c_i t^i) = \min\{v_{P'}(c_i) + iv_{P'}(t);\, i = 1, ..., n\} = \min\{v_{P'}(c_i) + i;\, i = 0, ..., n\} = 0$, o que contradiz o fato de que $f(t) = 0$.

Defina $O := O_{P'} \cap F$. Temos $O \subsetneq F$, já que existe $z \in F$ com $v_{p'}(z) < 0$. Além disso, $K \subsetneq O$. De fato, $K \subset F \cap O_{P'}$ e pela Afirmação anterior, existe $z \in F$ tal que $v_{P'}(z) \neq 0$ e, portanto, ou z ou z^{-1} pertence a $O_{P'}$ mas não pertence a K. E da definição de O é imediato que se $z \in F$, então $z \in O$ ou $z^{-1} \in O$. Portanto, O é um anel de valoração de F/K. Finalmente, pela Proposição 1.3.3, temos que P é o ideal maximal de $O =: O_P \subset O_{P'}$, donde $P'|P$ e $P = P' \cap F$.

(ii) Seja $P \in \mathbb{P}_F$. Como $\mathbb{P}_F$ é infinito, $S = \mathbb{P}_F \setminus \{P\}$ satisfaz $\varnothing \neq S \subsetneq \mathbb{P}_F$. Pelo Teorema da Aproximação (Teorema 1.2.11), existem $z \in F$ e $Q \in S$ tal que $v_Q(z) > 0$ e $v_{\tilde{Q}}(z) \geq 0$ para todo $\tilde{Q} \in S \setminus Q$. Como z é transcendente sobre K (pois Q é zero de z), temos necessariamente que P é pólo (e único) de z. Conseqüentemente, $x := z^{-1}$ tem P como seu único zero em F/K.

Afirmação: $P'|P \iff v_{P'}(x) > 0$
Demonstração: Com efeito, se $P'|P$, então $v_{P'}(x) = e(P'|P)v_P(x) > 0$. Reciprocamente, se $v_{P'}(x) > 0$ e P' está acima de $Q \in \mathbb{P}_F$ (existe Q, pelo item (a)), então $v_Q(x) > 0$ e, portanto, $Q = P$, já que P é o único zero de x. □

Como x possui um número finito de zeros em F'/K', a Afirmação anterior garante que há um número finito de lugares P' em $\mathbb{P}_{F'}$ acima de P. ∎

Ao final deste capítulo, definiremos extensões F'/F de Kummer. Veremos que para tais extensões é fácil decidir quais os lugares de F que não se ramificam em F'.

Lema 1.3.7. *Seja F/K um corpo de funcões algébricas e F'/K' uma extensão desse corpo. Se K'/K é uma extensão finita e $x \in F'$ é transcendente sobre K, então [K'(x):K(x)]=[K':K].*

Demonstração. Já que K'/K é finita e separável (pois K é perfeito), o Teorema do Elemento Primitivo garante que existe $\alpha \in K'$ tal que $K' = K(\alpha)$. Como $K'(x) = K(x)(\alpha)$, temos $[K'(x) : K(x)] \leq [K' : K]$. Basta-nos então provar a desigualdade inversa.

Para isso precisamos mostrar que o polinônio mínimo de α sobre K continua irredutível em $K(x)$. Seja $\phi(T) \in K[T]$ o polinômio mínimo de α sobre K. Suponhamos que $\phi(T)$ seja redutível sobre $K(x)$, isto é, existem $g(T), h(T) \in K(x)[T]$ mônicos com $1 \leq deg(h), deg(g) < deg(\phi) =: n$ tais que $\phi(T) = h(T).g(T)$. Como $\phi(\alpha) = 0$ temos $g(\alpha) = 0$ ou $h(\alpha) = 0$. Podemos supor, sem perda de generalidade, que $g(\alpha) = 0$. Escrevendo

$$g(T) = a_0(x) + a_1(x)T + ... + a_{r-1}(x)T^{r-1} + T^r$$

com $a_i \in K(x)$ e $1 \leq r < n$, temos

$$a_0(x) + a_1(x)\alpha + ... + a_{r-1}(x)\alpha^{r-1} + \alpha^r = 0.$$

Multiplicando $g(\alpha)$ pelo mínimo múltiplo comum dos denominadores, obtemos

$$g_0(x) + g_1(x)\alpha + ... + g_{r-1}(x)\alpha^{r-1} + g_r(x)\alpha^r = 0$$

para certos $g_i(x) \in K[x]$. Podemos assumir, sem perda de generalidade, que $x \nmid g_i$ para algum $i \in \{1, 2, ..., r\}$. Obtemos assim que α é raiz de $f(T) = \sum_{i=1}^{r} g_i(0)T^i \in K[T]$, contrariando a minimalidade do grau de $\phi(T)$. ∎

Teorema 1.3.8. *(Igualdade Fundamental) Sejam K um corpo perfeito, F'/K' uma extensão finita de F/K, P um lugar de F/K e $P_1, P_2, ..., P_m$ todos os lugares de F'/K' acima de P. Sejam $e_i = e(P_i|P)$ e $f_i = f(P_i|P)$ o índice de ramificação e o grau relativo de P_i sobre P, respectivamente. Então*

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

Demonstração. Seja $x \in F \backslash \{0\}$ tal que P é o único zero de x em F/K e seja $v_P(x) = r > 0$. Os lugares $P_1, ..., P_m$ são exatamente os zeros de x em F'/K'. De fato, se $Q = P' \cap F \in F/K$ para algum zero P' de x em $\mathbb{P}_{F'}$, então $v_Q(x) > 0$, implicando em $Q = P$. Agora analisaremos o grau $[F' : K(x)]$ de duas maneiras:

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

que é igual, pela Proposição 1.2.5 e pelo Lema 1.3.7 a:

$$(\sum_{i=1}^{m} v_{P_i}(x).deg(P_i))[K' : K] = \sum_{i=1}^{m} (e_i v_P(x)).([F'_{P_i} : K'].[K' : K])$$

$$= r.\sum_{i=1}^{m} e_i.[F'_{P_i} : F_P].[F_P : K] = r.deg(P).\sum_{i=1}^{m} e_i f_i.$$

Por outro lado, pela Proposição 1.2.5, temos que

$$[F' : K(x)] = [F' : F].[F : K(x)] = [F' : F].r.deg(P)\ ,$$

e o Teorema está demonstrado. ∎

Exemplo 5. Seja $\mathcal{H}/\mathbb{F}_{q^2}$ o corpo de funções Hermitiano (Exemplo 2). Calculemos o número de lugares de $\mathcal{H}$ acima de $P_\infty \in \mathbb{F}_{q^2}(y)$, onde $x^{q+1} = y^q + y$ (x, y transcendentes sobre $\mathbb{F}_{q^2}$). Tomemos P acima de P_∞ em $\mathcal{H}/\mathbb{F}_{q^2}$. Temos:

$$(q+1).v_P(x) = v_P(x^{q+1}) = e(P|P_\infty).v_{P_\infty}(y^q + y) = -q.e(P|P_\infty). \quad (1)$$

Como $e(P|P_\infty) \leq [\mathcal{H} : \mathbb{F}_{q^2}(y)] = q+1$ e $mdc\ (q, q+1) = 1$, segue que $v_P(x) = -q$ e $e(P|P_\infty) = q+1$. Logo, $P_\infty \in \mathbb{F}_{q^2}(y)$ se ramifica totalmente em $\mathcal{H}/\mathbb{F}_{q^2}(y)$ e temos, pela Igualdade Fundamental (Teorema 1.3.8), que o único lugar $P'_\infty \in \mathcal{H}$ acima de P_∞ satisfaz $f(P'_\infty|P_\infty) = 1$ e $deg\,(P'_\infty) = 1$. Os demais lugares de $\mathbb{F}_{q^2}(y)$ que se ramificam em $\mathcal{H}$ serão analisados no Exemplo 7.

Definição 1.3.9. Sejam F'/K' uma extensão algébrica de F/K e $P \in \mathbb{P}_F$. Definimos sua *conorma* com respeito a F'/F como

$$Con_{F'/F}(P) := \sum_{P'|P} e(P'|P).P'\ ,\ P' \in \mathbb{P}_{F'}.$$

Estendemos essa definição a $\mathcal{D}_F$ linearmente, ou seja, $Con_{F'/F}(\sum_{P\in\mathbb{P}_F} n_P.P\ ) = \sum n_P.Con_{F'/F}(P)$ (note que isso implica que $Con_{F'/F}(\mathcal{D}_F) \subset \mathcal{D}_{F'}$).

Corolário 1.3.10. *Seja F'/K' uma extensão finita de F/K. Então para todo $A \in \mathcal{D}_F$,*

$$deg\,Con_{F'/F}(A) = \tfrac{[F':F]}{[K':K]}.deg\,A.$$

Demonstração. Da Definição da conorma e da aditividade do grau, é suficiente provarmos o Teorema para o caso em que $A = P \in \mathbb{P}_F$. Temos:

$$deg\,Con_{F'/F}(P) = deg\,(\sum_{P'|P} e(P'|P).P') = \sum_{P'|P} e(P'|P).[F'_{P'} : K'] =$$
$$= \sum_{P'|P} e(P'|P).\tfrac{[F'_{P'}:K]}{[K':K]} = \tfrac{1}{[K':K]} \sum_{P'|P} e(P'|P).[F'_{P'} : F_P][F_P : K] =$$
$$= \tfrac{1}{[K':K]}(\sum_{P'|P} e(P'|P).f(P'|P))deg\,P = \tfrac{[F':F]}{[K':K]}deg\,P.$$

∎

Muitas vezes, é fácil saber se os lugares de um corpo de funções F/K se ramificam em F'/K'. O próximo Teorema é uma ferramenta útil nos casos em que $F' = F(y)$ para algum y algébrico sobre F.

Lema 1.3.11. *Sejam A,B e C anéis e $\rho : A \longrightarrow B$ e $\pi : A \longrightarrow C$ homomorfismos tais que ρ e π são sobrejetores e $Ker\,\rho \subseteq Ker\,\pi$. Então existe um único homomorfismo sobrejetor $\sigma : B \longrightarrow C$ satisfazendo $\pi = \sigma \circ \rho$.*

Demonstração. Sejam $c \in C$ e $b \in B$ tais que $\pi(a) = c$ e $\rho(a) = b$. Defina

$$\sigma : \begin{cases} B \longrightarrow C \\ b \longmapsto \pi \circ \rho^{-1}(b) \end{cases} .$$

Afirmação 1: σ está bem definida.
Demonstração: Como ρ é sobrejetiva, para todo $b \in B$ existe $a \in A$ tal que $\rho(a) = b$. Seja $\tilde{a} \in A$ satisfazendo $\rho(a) = b = \rho(\tilde{a})$.

Como $0 = \rho(a) - \rho(\tilde{a}) = \rho(a - \tilde{a})$ e $Ker\ \rho \subset Ker\ \pi$, temos que $a - \tilde{a} \in Ker\ \pi$. Logo, $\pi(a) = \pi(\tilde{a})$ e, portanto, $\sigma(b) = \pi \circ \rho^{-1}(b)$ independe da pré-imagem de b por ρ. Isso conclui nossa Afirmação. □

Pela definição de σ, é imediato que $\pi = \sigma \circ \rho$.
Afirmação 2: σ é um homomorfismo sobrejetor.
Demonstração: Sejam $b, \tilde{b} \in B$ tais que $b = \rho(a)$ e $\tilde{b} = \rho(\tilde{a})$, onde $a, \tilde{a} \in A$. Temos:

$$\sigma(b + \tilde{b}) = \pi \circ \rho^{-1}(b + \tilde{b}) = \pi \circ \rho^{-1}(\rho(a + \tilde{a})) = \pi(a + \tilde{a}) = \pi(a) + \pi(\tilde{a}) =$$

$$= \pi \circ \rho^{-1}(b) + \pi \circ \rho^{-1}(\tilde{b}) = \sigma(b) + \sigma(\tilde{b}).$$

$$\sigma(b\tilde{b}) = \pi \circ \rho^{-1}(b\tilde{b}) = \pi \circ \rho^{-1}(\rho(a\tilde{a})) = \pi(a\tilde{a}) = \pi(a)\pi(\tilde{a}) =$$

$$= \pi \circ \rho^{-1}(b)\pi \circ \rho^{-1}(\tilde{b}) = \sigma(b)\sigma(\tilde{b}).$$

Logo, σ é um homomorfismo. Para mostrar que é sobrejetor, tome $c \in C$. Como π é sobrejetora, existe $a \in A$ tal que $c = \pi(a) = \sigma \circ \rho(a)$. Como $\rho(a) \in B$, temos provada nossa Afirmação. □

Finalmente, temos que σ é o único homomorfismo sobrejetor de B em C que satisfaz $\pi = \sigma \circ \rho$. De fato, sejam $\phi : B \longrightarrow C$ um homomorfismo sobrejetor tal que $\pi = \phi \circ \rho$ e $b \in B$ um elemento qualquer. Temos que $b = \rho(a)$ para algum $a \in A$ e $\sigma(b) = \pi \circ \rho^{-1}(b) = \pi(a) = \phi \circ \rho(a) = \phi(b)$. ∎

Teorema 1.3.12. *(Kummer) Sejam F/K um corpo de funções e P um lugar de F/K. Suponha que F'= F(y) seja uma extensão algébrica de F e que o polinômio mínimo φ de y sobre F tenha coeficientes em O_P.*

Considere $\varphi(T)\,(mod\,P) = \bar{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\varepsilon_i}$ a fatoração de $\bar{\varphi}(T)$, onde $\varepsilon_i \geq 1$, $\gamma_i(T)$ é mônico e irredutível sobre $F_P := F\,(mod\,P)$ para todo $i \in \{1, \cdots, r\}$ e $\gamma_i \neq \gamma_j$ sempre que $i \neq j$, $j = 1, \cdots, r$.

Escolha $\varphi_i(T) \in O_P[T]$ com $\bar{\varphi}_i(T) = \gamma_i(T)$ e $deg\,\varphi_i(T) = deg\,\gamma_i(T)$.

Então, para $1 \leq i \leq r$, existem lugares $P_i \in \mathbb{P}_{F'}$ satisfazendo

$$P_i|P, \quad \varphi_i(y) \in P_i \text{ e } f(P_i|P) \geq deg\,\gamma_i(T)$$

Além disso, $P_i \neq P_j$ sempre que $i \neq j$ e se para todo $i \in \{1, \cdots, r\}$ tivermos $\varepsilon_i = 1$, então:

- *existe um único lugar $P_i \in \mathbb{P}_{F'}$ com $P_i|P$ e $\varphi_i(y) \in P_i$;*
- *os lugares $P_1, \cdots, P_r$ são todos os lugares de F' acima de P;*
- *$e(P_i|P) = \varepsilon_i$ e $f(P_i|P) = deg\,\gamma_i(T)$.*

Demonstração. Seja $F_{P,i} = F_P[T]/\langle \gamma_i(T) \rangle$. Como $\gamma_i(T)$ é irredutível sobre F_P, $\langle \gamma_i(T) \rangle$ é um ideal maximal de $F_P[T]$. Portanto, $F_{P,i}$ é uma extensão de F_P e $[F_{P,i}:F_P] = deg\,\gamma_i(T)$.

Considere o anel $O_P[y] = \sum_{j=0}^{n-1} O_P y^j$ onde $n = deg\varphi(T) = [F' : F]$ e os homomorfismos

$$\rho : \begin{cases} O_P[T] \longrightarrow O_P[y] \\ \sum c_j T^j \longmapsto \sum c_j y^j \end{cases} \quad \text{e} \quad \pi_i : \begin{cases} O_P[T] \longrightarrow F_{P,i} \\ \sum c_j T^j \longmapsto \sum \bar{c}_j T^j \; mod\; \gamma_i(T) \end{cases}$$

Temos que $Ker\,\rho = \{f(T) = \sum c_j T^j \in O_P[T]; \sum c_j y^j = 0\} = \{f(T) \in O_P[T]; f(y) = 0\} = \langle \varphi(T) \rangle$.

Além disso, $\pi_i(\varphi(T)) = \bar{\varphi}(T)\, mod\, \gamma_i(T) = 0$ e, portanto, $Ker\,\rho \subseteq Ker\,\pi_i$.

Como ρ e π_i são, por definição, sobrejetivas, o Lema 1.3.11 garante que existe um único homomorfismo sobrejetor $\sigma_i : O_P[y] \longrightarrow \mathbb{F}_{P,i}$ tal que $\pi_i = \sigma_i \circ \rho$.

σ_i é explicitamente dada por $\sigma_i : \begin{cases} O_P[y] \longrightarrow F_{P,i} \\ \sum_{j=0}^{n-1} c_j y^j \longmapsto \sum_{j=0}^{n-1} \bar{c}_j T^j \, mod\, \gamma_i(T) \end{cases}$.

Afirmação. $Ker\, \sigma_i = P.O_P[y] + \varphi_i(y).O_P[y]$.

Demonstração: Se $z \in P.O_P[y] + \varphi_i(y).O_P[y]$, $z = a\sum_{j=0}^{n-1} c_j y^j + \varphi_i(y)\sum_{j=0}^{n-1} d_j y^j$, $a \in P$ e $c_j, d_j \in O_P$. Temos:

$$\sigma_i(z) = \sigma_i(a\sum_{j=0}^{n-1} c_j y^j) + \sigma_i(\varphi_i(y)\sum_{j=0}^{n-1} d_j y^j) =$$

$$= \sum_{j=0}^{n-1} \bar{a}\bar{c}_j T^j \, mod\, \gamma_i(T) + \sum_{j=0}^{n-1} \bar{\varphi}_i(T)\bar{d}_j T^j \, mod\, \gamma_i(T) = \bar{0} + \bar{0} = \bar{0}.$$

Logo, $z \in Ker\, \sigma_i$.

Por outro lado, se $\sum_{j=0}^{n-1} c_j y^j \in Ker\, \sigma_i$, então $\sum_{j=0}^{n-1} \bar{c}_j T^j \, mod\, \gamma_i(T) = \bar{0}$. Logo, existe $\psi(T) \in F_P[T]$ tal que

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

Portanto, $\sum_{j=0}^{n-1} c_j T^j - \psi(T)\varphi_i(T) \in P.O_P[T]$ e temos $\sum_{j=0}^{n-1} c_j y^j - \psi(y)\varphi_i(y) \in P.O_P[y]$. Conseqüentemente, $\sum_{j=0}^{n-1} c_j y^j \in P.O_P[y] + \psi(y)\varphi_i(y)$, o que conclui nossa Afirmação. □

Pelo Teorema 1.1.14, existe $i \in \{1, 2, \cdots, r\}$ tal que $Ker\ \sigma_i \subseteq P_i$ (de fato, $Ker\ \sigma_i$ é um ideal próprio não nulo do subanel $O_P[y] \subset F'$) e $O_P[y] \subseteq O_{P_i}$. Portanto, $O_P \subset O_{P_i}$ e, pela Proposição 1.3.3, $P_i|P$. Além disso, como $\varphi_i(y) \in Ker\, \sigma_i$, temos que $\varphi_i(y) \in P_i$. Temos também que $O_{P_i}/P_i \supset O_P[y]/Ker\, \sigma_i \simeq F_{P,i}$. Portanto,

$$f(P_i|P) \geq [F_{P,i} : F_P] = deg\, \gamma_i(T).$$

Como os polinômios $\gamma_i(T) = \bar{\varphi}_i(T)$ e $\gamma_j(T) = \bar{\varphi}_j(T)$ são irredutíveis sobre F_P, temos para $i \neq j$

$$1 = \bar{\varphi}_i(T).\bar{\lambda}_i(T) + \bar{\varphi}_j(T).\bar{\lambda}_j(T) \text{ para certos } \bar{\lambda}_i(T), \bar{\lambda}_j(T) \in F_P[T].$$

Logo, $\varphi_i(T)\lambda_i(T) + \varphi_j(T)\lambda_j(T) - 1 \in P.O_P[T]$. Em particular, para $T = y$, temos que $\varphi_i(y)\lambda_i(y) + \varphi_j(y)\lambda_j(y) - 1 \in P.O_P[y]$ e, pela Afirmação anterior, segue que $1 \in Ker\, \sigma_i + Ker\, \sigma_j$. Logo, $P_i \neq P_j$ sempre que $i \neq j$ (pois se $P_i = P_j$, temos $1 \in Ker\, \sigma_i + Ker\, \sigma_j \subset P_i + P_j = P_i$, o que é absurdo).

Finalmente, se $\varepsilon_i = 1$ para todo $i = 1, \cdots, r$, então:

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

Disso resultam:

- $e(P_i|P) = 1$ já que $\sum_{i=1}^{r} f(P_i|P) = \sum_{i=1}^{r} e(P_i|P)f(P_i|P)$.
- Para cada $i = 1, \cdots, r$ existe um único $P_i \in \mathbb{P}_{F'}$ acima de P já que $\sum_{i=1}^{r} e(P_i|P)f(P_i|P) = \sum_{P'|P} e(P'|P)f(P'|P)$.

∎

Definição 1.3.13. Sejam F/K e F'/K' extensões algébricas de corpos com F'/F finita e separável. Para $P \in \mathbb{P}_F$, definimos o módulo complementar sobre O_P como o conjunto $\mathcal{C}_P := \{z \in F';\, Tr_{F'/F}(z.O'_P) \subseteq O_P\}$, onde $O'_P = \bigcap_{P'|P} O_{P'}$ é o fecho integral de O_P em F'.

A fim de não alongarmos muito o texto, alguns Teoremas e Proposições serão apenas enunciados.

Proposição 1.3.14. *Com a notação da Definição anterior, valem as seguintes afirmações:*

(i) $\mathcal{C}_P$ é um O'_P- módulo e $O'_P \subseteq \mathcal{C}_P$;

(ii) Existe uma função $t \in F'$ (que depende do lugar P) tal que $\mathcal{C}_P = t.O'_P$. Além disso,

$$v_{P'}(t) \leq 0 \text{ para todo } P'|P;$$

(iii) $\mathcal{C}_P = O'_P$ para quase todo $P \in \mathbb{P}_F$. ∎

Definição 1.3.15. Considere $P \in \mathbb{P}_F$ e o fecho integral O'_P de O_P em F'. Seja $\mathcal{C}_P = t.O'_P$ o módulo complementar sobre O_P. Para cada $P'|P$, definimos o expoente da diferente de P' sobre P por

$$d(P'|P) := -v_{P'}(t).$$

Teorema 1.3.16. *(Dedekind) Seja F'/F uma extensão finita e separável, onde F/K e F'/K' são corpos de funções algébricas com corpos de constantes K e K', respectivamente. Então para todo $P' \in \mathbb{P}_{F'}$, $P \in \mathbb{P}_F$ tais que $P'|P$, temos:*

(i) $d(P'|P) \geq e(P'|P) - 1$*;*
(ii) $d(P'|P) = e(P'|P) - 1$ *se, e somente se, char* K *não divide* $e(P'|P)$*.* ∎

Proposição 1.3.17. *Sejam F/K e F'/K' corpos de funções algébricas com corpos de constantes K e K', respectivamente. Suponha que* $F' = F(y)$ *seja uma extensão finita e separável de F de grau [F': F]= n. Seja* $P \in \mathbb{P}_F$ *tal que o polinômio mínimo* $\varphi(T)$ *de y sobre F tenha coeficientes em* O_P *e sejam* $P_1, \ldots, P_r \in \mathbb{P}_{F'}$ *todos os lugares de F' acima de P. Então* $d(P_i|P) \leq v_{P_i}(\varphi'(y))$ *para* $1 \leq i \leq r$*.* ∎

Pela Proposição 1.3.14 e pela Definição 1.3.15, para cada $P'|P$ temos $d(P'|P) \geq 0$. Além disso, como $\mathcal{C}_P = 1.O'_P$ para quase todo $P \in \mathbb{P}_F$, concluímos que $d(P'|P) = 0$ para quase todo $P \in \mathbb{P}_F$ e $P'|P$. Desse modo é possível definir o divisor

$$Diff(F'/F) := \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P).P',$$

o qual é chamado a diferente de F'/F.

Teorema 1.3.18. *(Fórmula do gênero de Hurwitz) Sejam F/K e F'/K' corpos de funções algébricas de gêneros g e g', respectivamente. Suponha também que K e K' sejam seus respectivos corpos de constantes. Se a extensão F'/F for finita e separável, então*

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

∎

Proposição 1.3.19. *Sejam F/K e F'/K' corpos de funções algébricas com corpos de constantes K e K', respectivamente. Suponha que F'/F seja uma extensão algébrica de corpos de funções,* $P \in \mathbb{P}_F$ *e* $P' \in \mathbb{P}_{F'}$ *com* $P'|P$*. Considere um automorfismo* σ *de* F'/F*.*
Então $\sigma(P') := \{\sigma(z); z \in P'\}$ *é um lugar de* F' *e temos:*
(i) $v_{\sigma(P')}(y) = v_{P'}(\sigma^{-1}(y))$ *para todo* $y \in F'$*;*
(ii) $\sigma(P')|P$*;*
(iii) $e(\sigma(P')|P) = e(P'|P)$ *e* $f(\sigma(P')|P) = f(P'|P)$*.*

Demonstração. Em primeiro lugar, provemos que $\sigma(O_{P'})$ é um anel de valoração de F', isto é, são válidas as seguintes afirmações:

(a) $\sigma(O_{P'}) \subsetneq F'$.

Com efeito, $\sigma(O_{P'}) \subset F'$ e como $O_{P'} \subsetneq F'$ e σ é bijetiva, não podemos ter $\sigma(O_{P'}) = F'$.

(b) $K' \subsetneq \sigma(O_{P'})$.

De fato, $K' \subset O_{P'}$ e como σ é um automorfismo, temos $\sigma(O_{P'}) \supsetneq \sigma(K') = K'$.

(c) Dado $x \in F'\backslash\{0\}$, $x \in \sigma(O_{P'})$ ou $x^{-1} \in \sigma(O_{P'})$.

Com efeito, temos $\sigma^{-1}(x) = y$ para algum $y \in F'$. Se $y \in O_{P'}$, a Afirmação está provada. Se não, $y^{-1} \in O_{P'}$ e temos $\sigma^{-1}(x^{-1}) = y^{-1}$ (note que a injetividade de σ implica que $y \neq 0$), resultando em $x^{-1} \in \sigma(O_{P'})$.

Para provarmos que $\sigma(P')$ é um lugar de F', resta-nos mostrar que $\sigma(P')$ é um ideal maximal de $\sigma(O_{P'})$. De fato,

- $\sigma(P') \subsetneq \sigma(O_{P'})$ é um ideal próprio de $\sigma(O_{P'})$, pois σ é um automorfismo e P' é um ideal próprio de $O_{P'}$;

- Se J é um ideal próprio de $\sigma(O_{P'})$ com $\sigma(P') \subset J \subsetneq \sigma(O_{P'})$, então $J = \sigma(P')$. Com efeito, $P' \subset \sigma^{-1}(J)$ e dados $a = \sigma^{-1}(x)$,$b = \sigma^{-1}(y) \in \sigma^{-1}(J)$ e $z \in O_{P'}$, temos $a.b \in \sigma^{-1}(J)$ e $a.z = \sigma^{-1}(x).z \in \sigma^{-1}(J)$. Conseqüentemente, $\sigma^{-1}(J)$ é um ideal próprio de $O_{P'}$ satisfazendo $P' \subset \sigma^{-1}(J) \subsetneq O_{P'}$ e como P' é o único ideal maximal de $O_{P'}$, temos o resultado.

Logo, $\sigma(P')$ é um lugar de F' e seu anel de valoração correspondente é $O_{\sigma(P')} = \sigma(O_{P'})$.

Seja $t' \in F'$ um elemento primitivo de P'. Então $\sigma(P') = \sigma(t').\sigma(O_{P'})$ e temos que $\sigma(t')$ é um elemento primitivo de $\sigma(P')$.

(i) Seja $0 \neq y = \sigma(z)$, $z \in P'$. Pelo Teorema 1.1.9(ii), $z = t'^r.u$, onde $r = v_{P'}(z)$ e $u \in O_{P'}\backslash P'$. Obtemos: $y = \sigma(t')^r.\sigma(u)$, com $\sigma(u) \in \sigma(O_{P'})\backslash\sigma(P')$. Conseqüentemente,

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

(ii) Como $\sigma(P') \supset \sigma(P) = P$, temos que $\sigma(P')$ está acima de P.

(iii) Seja $x \in F$ um elemento primitivo de P. Temos:

$$e(\sigma(P')|P) = v_{\sigma(P')}(x) = v_{P'}(\sigma^{-1}(x)) = v_{P'}(x) = e(P'|P).$$

Finalmente, o automorfismo σ de F'/F induz um isomorfismo $\bar{\sigma}$ do corpo $F'_{P'}$ em $F'_{\sigma(P')}$ dado por $\bar{\sigma}(z + P') = \sigma(z) + \sigma(P')$, o qual é a identidade restrito a F_P. Logo,

$$f(P'|P) = [F'_{P'} : F_P] = [F'_{\sigma(P')} : F_P] = f(\sigma(P')|P).$$

∎

Definição 1.3.20. Uma extensão F'/K' de um corpo de funções F/K é dita de Galois (ou galoisiana) se o grupo $Aut_F(F') = \{\sigma : F' \to F'; \sigma \text{ é um isomorfismo e } \sigma(x) = x \text{ para todo } x \in F\}$ tem ordem $[F' : F] < \infty$.

Teorema 1.3.21. *Seja F'/K' uma extensão de Galois de F/K e $P_1, P_2 \in \mathbb{P}_{F'}$ extensões de $P \in \mathbb{P}_F$. Então $P_2 = \sigma(P_1)$ para algum $\sigma \in Aut_F(F')$.*

Demonstração. Suponha, por absurdo, que $\sigma(P_1) \neq P_2$ para todo $\sigma \in G := Aut_F(F')$. Pela Proposição 1.3.6($ii$) e pelo Teorema 1.2.11, existe $z \in F'$ tal que $v_{P_2}(z) > 0$ e $v_Q(z) = 0$ para todo $Q \in \mathbb{P}_{F'} \backslash \{P_2\}$ com $Q|P$. Considere $N_{F'/F} : F' \to F$ a aplicação norma. Temos:

$$v_{P_1}(N_{F'/F}(z)) = v_{P_1}(\prod_{\sigma \in G} \sigma(z)) = \sum_{\sigma \in G} v_{P_1}(\sigma(z)) = \sum_{\sigma \in G} v_{\sigma^{-1}(P_1)}(z) = \sum_{\sigma \in G} v_{\sigma(P_1)}(z) = 0$$

e

$$v_{P_2}(N_{F'/F}(z)) = v_{P_2}(\prod_{\sigma \in G} \sigma(z)) = \sum_{\sigma \in G} v_{\sigma^{-1}(P_2)}(z) = \sum_{\sigma \in G} v_{\sigma(P_2)}(z) > 0,$$

pois a identidade pertence a G.

Como P_1 está acima de P, temos que $v_P(N_{F'/F}(z)) = 0$. Analogamente, P_2 está acima de P e temos que $v_P(N_{F'/F}(z)) > 0$, o que é uma contradição. ∎

Corolário 1.3.22. *Seja F'/K' uma extensão de Galois de F/K, onde K' e K são seus respectivos corpos de constantes. Mantendo as notações do Teorema anterior, considere $P_1, P_2, ..., P_r \in \mathbb{P}_{F'}$ todos os lugares de F' acima de P. Então:*

(i) $e(P_i|P) = e(P_j|P) =: e(P)$ *e* $f(P_i|P) = f(P_j|P) =: f(P)$ *para todo* $i, j \in \{1, \ldots, r\}$;

(ii) $e(P).f(P).r = [F' : F]$;

(iii) $d(P_i|P) = d(P_j|P)$ *para todo* $i, j \in \{1, \ldots, r\}$.

Demonstração. (i) Segue diretamente da Proposição 1.3.19(iii) e do Teorema 1.3.21.

(ii) É imediato do item (i) e do Teorema 1.3.8.

(*iii*) Seja $\sigma \in G$. Temos

$$Tr_{F'/F}(\sigma(u)) = \sum_{\tilde{\sigma}\in G}(\tilde{\sigma}\sigma)(u) = \sum_{\tau\in G}\tau(u) = Tr_{F'/F}(u). \qquad (*)$$

Note que $O_{P_i} = P_i \cup K'$ implica que

$$\sigma(O_{P_i}) = \sigma(P_i) \cup \sigma(K') = P_j \cup K' = O_{P_j} \qquad (**)$$

e que $\sigma(O_{P_i}) \neq \sigma(O_{P_j})$ sempre que $i \neq j$, já que σ é injetiva.

Logo, $\sigma(O'_P) = \bigcap_{i=1}^{r} \sigma(O_{P_i}) = \bigcap_{i=1}^{r} O_{P_j} = O'_P$ e

$$Tr_{F'/F}(z.O'_P) = Tr_{F'/F}(\sigma(z.O'_P)) = Tr_{F'/F}(\sigma(z)\sigma(O'_P)) = Tr_{F'/F}(\sigma(z).O'_P). \qquad (***)$$

Além disso, $(* \ * \ *)$ implica diretamente que $\sigma(C_P) = C_P$, já que $C_P = \{z \in F'; Tr_{F'/F}(z.O'_P) \subset O_P\}$.

Seja $t \in F'$ tal que $C_P = t.O'_P$. Logo, $t.O'_P = C_P = \sigma(C_P) = \sigma(t).\sigma(O'_P) = \sigma(t).O'_P$ e $v_{P_i}(t) = -d(P_i|P) = v_{P_i}(\sigma(t))$ para $1 \leq i \leq r$. Finalmente, escolha $\sigma \in G$ tal que $\sigma(P_j) = P_i$ (tal σ existe pelo Teorema 1.3.21). Então $-d(P_i|P) = v_{P_i}(\sigma(t)) = v_{\sigma^{-1}(P_i)}(t) = v_{P_j}(t) = -d(P_j|P)$. ∎

Definição 1.3.23. (**EXTENSÕES DE KUMMER**) Seja F/K um corpo de funções algébricas com corpo de constantes K tal que K contém uma $n-ésima$ raiz primitiva da unidade, sendo $n > 1$ e $mdc(n, char(K)) = 1$. Suponha que exista uma função $u \in F$ satisfazendo

$$u \neq w^d \text{ para todo } d \mid n,\ d > 1.$$

A extensão F'/F, onde $F' = F(y)$ com $y^n = u$, é dita uma extensão de Kummer de F.

Exemplo 6. Se $F' \supset F \supset \mathbb{F}_{q^2}$, q ímpar, satisfaz $[F' : F] = 2$, então $F'|F$ é uma extensão de Kummer. De fato, se $[F' : F] = 2$, existe $\gamma \in F' \setminus F$ tal que $a\gamma^2 + b\gamma + c = 0$, com $a, b, c \in F$ e $a \neq 0$. Logo, $\gamma^2 + a^{-1}b\gamma + \left(\frac{a^{-1}b}{2}\right)^2 = -a^{-1}c + \left(\frac{a^{-1}b}{2}\right)^2$ e temos que $\left(\gamma + \frac{b}{2a}\right)^2 = \frac{b^2-4ac}{4a^2} \in F$.

Como $F' = F[\gamma] = F\left[\gamma + \frac{b}{2a}\right]$, temos que F'/F é uma extensão de Kummer com gerador $\gamma + \frac{b}{2a}$ (note que $\mathbb{F}_{q^2}$ contém raiz quadrada primitva da unidade e $b^2 - 4ac \neq z^2$ para todo $z \in F$ já que o polinômio mínimo $p_{\gamma+\frac{b}{2a},F}$ de $\gamma + \frac{b}{2a}$ sobre F tem grau 2).

Teorema 1.3.24. *(Para Extensões de Kummer) Sejam F/K e F'/K' corpos de funções algébricas com corpos de constantes K e K', respectivamente. Suponha que $F' = F(y)$ seja uma extensão de Kummer do corpo F com $y^n = u$, para algum $u \in F$. Então:*

(i) O polinômio $\phi(T) = T^n - u$ é o polinômio mínimo de y sobre F e a extensão F'/F é de Galois de grau n;

(ii) Sejam $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ tais que $P'|P$. Então:

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

onde $r_P = mdc(n, v_P(u))$;

(iii) Se g é o gênero de F/K e g', o de F'/K', então:

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

Demonstração. (i) O polinômio mínimo $p_{y,F}(T)$ de y sobre F satisfaz $1 \leq deg\, p_{y,F}(T) \leq n$. Além disso, sabemos que $\phi(T) = T^n - u = 0$ se, e somente se, $T = y.\xi_n^j$, $j \in \{0, 1, 2, \cdots, n-1\}$, onde ξ_n é uma n-ésima raiz primitiva da unidade. Suponhamos, por absurdo, que $\phi(T) = p_{y,F}(T).f(T)$, com $f(T) \in F(T)$ mônico de grau maior que 1. Logo,

$$p_{y,F}(T) = \prod_{j \in A \subsetneq \{0,1,\cdots,n-1\}} (T - \xi_n^j.y). \qquad (*)$$

Seja $c \in F$ o termo independente de $p_{y,F}(T)$. Por $(*)$, $c = y^r.\beta$, onde $r = deg\, p_{y,F}(T)$ e $\beta = \prod_{j \in A \subsetneq \{1,2,\cdots,n-1\}} \xi_n^j$. Tendo em vista que F contém uma n-ésima raiz primitiva da unidade (e, portanto, contém todas), $\beta \in F$ e, então, $y^r \in F$. Seja $d = mdc(r, n)$. Como d é uma combinação linear de r e n, temos também que $w := y^d \in F$. Conseqüentemente, $u = w^{\frac{n}{d}} \in F$, o que é uma contradição.

A extensão F'/F é claramente de Galois. Com efeito, F'/F é separável (pois $p_{y,F}(T)$ se fatora completamente em $F'[T]$ como produto de fatores lineares) e como $\xi_n^j \in F$ para todo $j \in \{0, \cdots, n-1\}$, temos $F' = F(y) = F(\xi_n^j.y)_{j \in \{1,\cdots,n-1\}}$. Logo, F'/F é uma extensão normal.

(ii) Caso 1: $r_P = 1$. Como $y^n = u$, temos que $n.v_{P'}(y) = v_{P'}(u) = e(P'|P).v_P(u) \leq n.v_P(u)$. Logo, $v_{P'}(y) \leq v_P(u)$. Se valer a igualdade, temos que $e(P'|P) = n$. Por outro lado, se $v_{P'}(y) < v_P(u)$, temos que $v_{P'}(y) \neq 0 \neq v_P(u)$ e, portanto, $v_{P'}(y) = \frac{e(P'|P).v_P(u)}{n}$

e como $mdc(n, v_P(u)) = 1$, n deve dividir $e(P'|P)$, o que implica em $e(P'|P) = n$. Como $mdc(charK, n) = 1$ (veja Definição 1.3.23) o Teorema 1.3.16(ii) garante que $d(P'|P) = n - 1$.

Caso 2: $r_P = n$. Suponhamos que $v_P(u) = l.n$ para algum $l \in \mathbb{Z}$. Sejam $\tilde{t}$ um elemento primitivo de P e $t = \tilde{t}^l$. Considere $y_1 := t^{-1}y$ e $u_1 = t^{-n}u$. Temos:

$$y_1^n = u_1 \text{ e } n.v_{P'}(y_1) = e(P'|P)v_P(u_1) = e(P'|P)(-n.v_P(t) + v_P(u)) = 0. \qquad (**)$$

Como $F' = F(y) = F(t^{-1}y) = F(y_1)$, temos que $[F(y_1) : F] = n$ e, portanto, $\psi(T) = T^n - u_1 \in O_P[T]$ é o polinômio mínimo de y_1 sobre F. Da Proposição 1.3.17 e de $(**)$, obtemos

$$0 \leq d(P'|P) \leq v_{P'}(\psi'(y_1)) = v_{P'}(n.y_1^{n-1}) = (n-1).v_{P'}(y_1) = 0.$$

Finalmente, o Teorema 1.3.16(i) garante que $e(P'|P) = 1$.

Caso 3: $1 < r_P < n$. Considere o corpo intermediário $F_0 := F(y_0)$ com $y_0 := y^{n/r_P}$. Então $[F' : F_0] = n/r_P$ e $[F_0 : F] = r_P$ com $y_0^{r_P} = u$. Seja $P_0 = P' \cap F_0$. O caso 2 aplicado à extensão F_0/F garante que $e(P_0|P) = 1$. Como $v_{P_0}(y_0) = \frac{e(P_0|P).v_P(u)}{n} = \frac{v_P(u)}{n}$ é relativamente primo com n/r_P (de fato, se existisse $d \neq 1$ divisor de ambos, $d.r_P$ dividiria $v_{P_0}(u)$ e n, o que contrariaria a maximalidade de r_P), o caso 1 se aplica à extensão F'/F (note que $F' = F_0(y)$). Conseqüentemente, $e(P'|P_0) = n/r_P$ e $e(P'|P) = e(P'|P_0).e(P_0|P) = n/r_P$. Finalmente, o Teorema 1.3.16(ii) garante que $d(P'|P) = e(P'|P) - 1 = n/r_P - 1$.

(iii) O grau do diferente $Diff\,(F'|F)$ é

$$deg\, Diff(F'/F) = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P).deg\,(P') = \sum_{P \in \mathbb{P}_F} \left(\frac{n}{r_P} - 1 \right) . \sum_{P'|P} deg\,(P'). \qquad (***)$$

Como F'/F é de Galois, fixado $P \in \mathbb{P}_F$, temos que $e(P) = e(P'|P)$ independe da escolha do P' acima de P. Portanto, pelo Corolário 1.3.10:

$$\sum_{P'|P} deg\,(P') = \frac{1}{e(P)}.\, deg \left(\sum_{P'|P} e(P'|P).P' \right) = \frac{1}{e(P)}.\, deg\, Con_{F'/F}(P) =$$

$$= \frac{r_P}{n}.\, \frac{n}{[K' : K]}\, .deg\,(P) = \frac{r_P}{[K' : K]}.\, deg\,(P)\,,$$

que substituído em $(***)$ fornece:

$$deg\, Diff(F'/F) = \sum_{P \in \mathbb{P}_F} \frac{n - r_P}{r_P}.\, \frac{r_P}{[K' : K]}.\, deg\,(P) = \frac{n}{[K' : K]} \sum_{P \in \mathbb{P}_F} \left(1 - \frac{r_P}{n} \right) . deg\,(P).$$

Finalmente, substituindo-se a última igualdade na *Fórmula do gênero de Hurwitz* (Teorema 1.3.18), obtemos o resultado. ∎

Lema 1.3.25. *Sejam F/K um corpo de funções algébricas, K algebricamente fechado em F, e $\alpha \in \bar{F}$, onde $\bar{F}$ é o fecho algébrico de F. Então $[K(\alpha) : K] = [F(\alpha) : F]$.*

Demonstração. Obviamente, $[F(\alpha) : F] \leq [K(\alpha) : K]$. Para provar o Lema, basta mostrarmos que o polinômio mínimo $p_{\alpha,K}(T)$ de α sobre K continua irredutível sobre F.

Suponha, por absurdo, que se tenha $[F(\alpha) : F] < [K(\alpha) : K]$, isto é, que $p_{\alpha,K}(T) = g(T).f(T)$ com $g(T), f(T) \in F(T)$ mônicos de grau maior que 1. Qualquer raiz de $f(T)$ e de $g(T)$ é também raiz de $p_{\alpha,K}(T)$, portanto algébrica sobre K. Conseqüentemente, os coeficientes de $f(T)$ e de $g(T)$ são também algébricos sobre K. Como K é algébricamente fechado em F, tais coeficientes também pertencem a K, o que contradiz a irredutibilidade de $p_{\alpha,K}(T)$ sobre K. ∎

Lema 1.3.26. *Sejam F/K um corpo de funções algébricas, onde K é um corpo perfeito algebricamente fechado em F, e $K' \supseteq K$ o corpo de constantes de $F' = FK'$. Se a extensão F'/F é finita, então $e(P'|P) = 1$ para todo $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ acima de P.*

Demonstração. Como K é perfeito e a extensão K'/K é finita (isso decorre diretamente da Proposição 1.3.2) K'/K é separável. Logo, existe $\alpha \in K'$ tal que $K' = K(\alpha)$. Conseqüentemente, $F' = F(\alpha)$ e pelo Lema 1.3.25 , o polinômio mínimo $\varphi(T)$ de α sobre K permanece irredutível sobre F.

Sejam $P \in \mathbb{P}_F$ e $P' \in \mathbb{P}_{F'}$ com $P'|P$. Pela Proposição 1.3.17, temos

$$0 \leq d(P'|P) \leq v_{P'}(\varphi'(\alpha)) = 0$$

(de fato, a separabilidade de α garante que $\varphi'(\alpha) \in K'\backslash\{0\}$). Finalmente o Teorema 1.3.16(i) garante que $e(P'|P) = 1$. ∎

Teorema 1.3.27. *Sejam F/K e F'/K' corpos de funções algébricas de corpos de constantes K (K perfeito) e K', respectivamente. Suponha que $F' = F(y)$ com $y^n = u \in F$, onde $n \neq 0$ (mod char K) e K contém uma n-ésima raiz primitiva da unidade. Se existe um lugar $Q \in \mathbb{P}_F$ tal que $mdc(v_Q(u), n) = 1$, então a extensão F'/F é de Kummer, $K' = K$ e*

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

onde g' (resp. g) é o gênero do corpo de funções F'/K' (resp. F/K).

Demonstração. A existência de um lugar $Q \in \mathbb{P}_F$ satisfazendo $mdc(v_Q(u), n) = 1$ implica necessariamente que $u \neq w^d$ para todo d divisor de n maior que 1 e $w \in F$. Portanto, F'/F é uma extensão de Kummer de grau n e pelo Teorema 1.3.24(iii), segue que

$$g' = 1 + n(g-1) + \frac{1}{2}\sum_{P \in \mathbb{P}_F}\left(1 - \frac{r_P}{n}\right).$$

Tome $Q' \in \mathbb{P}_{F'}$ acima de Q. Pelo Teorema 1.3.24(ii), temos que $e(Q'|Q) = [F' : F] = n$.

Suponhamos, por absurdo, que $[K' : K] > 1$, e consideremos o corpo intermediário $F_1 := FK'$. Temos $F_1 \neq F$, pois K'/K sendo finita, é algébrica e como K é algebricamente fechado em F e $K' \neq K$, $K' \not\subset F$. Finalmente, considere $Q_1 := Q' \cap F_1$ um lugar acima de Q. Pelo Lema 1.3.26, temos que $e(Q_1|Q) = 1$. Por outro lado, $e(Q_1|Q)$ divide $e(Q'|Q) = n = [F' : F]$ e, portanto, $e(Q_1|Q) = [F_1 : F] > 1$. Um absurdo.

∎

Definição 1.3.28. (**CURVA MAXIMAL**) Sejam $f(x, y) = 0$ um modelo afim de uma curva algébrica projetiva, não-singular e irredutível sobre $\mathbb{F}_{q^2}$ e $\mathbb{F}_{q^2}(x, y)/\mathbb{F}_{q^2}$ seu corpo de funções algébricas correspondente. A curva $f(x, y) = 0$ é chamada maximal (sobre $\mathbb{F}_{q^2}$) se o número de lugares racionais de $\mathbb{F}_{q^2}(x, y)/\mathbb{F}_{q^2}$ é igual a $q^2 + 1 + 2.g.q$, onde g é o gênero desse corpo de funções. Nesse caso, dizemos também que $\mathbb{F}_{q^2}(x, y)/\mathbb{F}_{q^2}$ é um corpo de funções maximal ou que $\mathbb{F}_{q^2}(x, y)$ é maximal sobre $\mathbb{F}_{q^2}$.

Gilles Lachaud provou (Proposição 6, [L]) que se $f(x, y) = 0$ é um modelo afim de uma curva maximal sobre um corpo finito $\mathbb{F}_{q^2}$ e $L \subset \mathbb{F}_{q^2}(x, y)$ é um corpo, então L é também maximal sobre $\mathbb{F}_{q^2}$.

Exemplo 7. Seja $q = p^n$, onde p é um número primo. Considere o corpo de funções Hermitiano $\mathcal{H}/\mathbb{F}_{q^2}$, onde $\mathcal{H} = \mathbb{F}_{q^2}(x, y)$ é definido pela curva Hermitiana $x^{q+1} = y^q + y$. Como y é transcendente sobre $\mathbb{F}_{q^2}$, temos $\tilde{\mathbb{F}}_{q^2} = \{z \in \mathbb{F}_{q^2}(y); z \text{ é algébrico sobre } \mathbb{F}_{q^2}\} = \mathbb{F}_{q^2}$. Portanto, $\mathbb{F}_{q^2}$ é o corpo de constantes do corpo de funções racionais $\mathbb{F}_{q^2}(y)/\mathbb{F}_{q^2}$.

A extensão $\mathcal{H}/\mathbb{F}_{q^2}(y)$ é de Kummer de grau $q + 1$ e o corpo de constantes do corpo de funções Hermitiano é $\mathbb{F}_{q^2}$. De fato, $\mathbb{F}_{q^2}$ contém uma $(q+1)$-ésima raiz primitiva da unidade

e $mdc(q+1,\, char.\, \mathbb{F}_{q^2}) = \ mdc(q+1,p) = 1$. Além disso, temos $mdc\ (v_{P_\infty}(y^q+y), q+1) = mdc\ (-q, q+1) = 1$, onde $P_\infty \in \mathbb{P}_{\mathbb{F}_{q^2}(y)}$ é o pólo de $y^q + y$. Logo, pelo Teorema 1.3.27, a extensão $\mathcal{H}/\mathbb{F}_{q^2}(y)$ é uma extensão de Kummer de grau $q+1$ e o corpo de constantes de $\mathcal{H}/\mathbb{F}_{q^2}$ é $\mathbb{F}_{q^2}$.

Mostraremos agora que o corpo Hermitiano é maximal, ou seja, que o gênero g' de $\mathcal{H}/\mathbb{F}_{q^2}$ satisfaz a igualdade

$$\#\mathcal{N}_{\mathbb{F}_{q^2}}(\mathcal{H}) = \ q^2 + 1 - 2.g'.q\ ,$$

onde $\#\mathbb{N}_{\mathbb{F}_{q^2}}(\mathcal{H})$ é o conjunto dos lugares racionais de $\mathcal{H}/\mathbb{F}_{q^2}$. Novamente faremos uso do Teorema 1.3.27 para obtermos o valor de g'.

Primeiramente, observemos que o polinômio $f(y) = y^q + y$ é separável, pois $f'(y) = 1$. Além disso, se α é uma raiz de $f(y)$, temos $\alpha^{q^2} = (-\alpha)^q = -\alpha^q = \alpha$ e, portanto, $\alpha \in \mathbb{F}_{q^2}$. Logo,

$$x^{q+1} = \prod_{i=1}^{q}(y - \alpha_i). \qquad (*)$$

Sejam $P \in \mathbb{P}_{\mathbb{F}_{q^2}(y)}$ e $r_P = mdc(q+1, v_P(f(y)))$. Temos:

1. Se $P = P_\infty$, onde P_∞ é o pólo de $f(y)$ em $F_{q^2}(y)$, temos $r_P = mdc(q+1, -q) = 1$ e $deg\ (P) = 1$;

2. Se $P = P_{\alpha_i}$, $i = 1, 2, \cdots, q$, onde P_{α_i} é o zero de $y - \alpha_i$ em $\mathbb{F}_{q^2}(y)$, temos $r_P = mdc(q+1, 1) = 1$ e $deg\,(P) = 1$;

3. Se P não corresponde a nenhum dos itens 1. e 2. anteriores, temos $r_P = mdc(q+1, 0) = q+1$.

Conseqüentemente, pelo Teorema 1.3.27,

$$g' = 1 + (q+1)(-1) + \frac{1}{2}\sum_{P\in\mathbb{P}_{\mathbb{F}_{q^2}(y)}} [(q+1) - r_P].\ deg\ (P) =$$

$$= -q + \frac{1}{2}[(q+1) - r_{P\infty}].deg\ (P_\infty)] + \frac{1}{2}\sum_{i=1}^{q}[(q+1) - r_{P_{\alpha_i}}].deg\ (P_{\alpha_i}) +$$

$$+ \frac{1}{2} \sum_{\substack{P\in\mathbb{P}_{\mathbb{F}_{q^2}(y)} \\ P\neq P_\infty \ e\ P\neq P_{\alpha_i},\ i=1,\cdots,q}} [(q+1) - r_P].deg\ (P) =$$

$$= -q + \frac{1}{2}[q+1-1].1 + \frac{1}{2}.q[q+1-1].1 + 0 = \frac{q(q-1)}{2} \ . \qquad (**)$$

Resta-nos agora determinar o número de lugares racionais do corpo Hermitiano. Antes de mais nada, observemos que:

Nota 1.3.29. Se $P' \in \mathbb{P}_{\mathcal{H}}$ é um lugar de grau 1 e se $P \in \mathbb{P}_{\mathbb{F}_{q^2}(x)}$ está abaixo de P, então P é um lugar racional de $\mathbb{P}_{\mathbb{F}_{q^2}(x)}$. Com efeito, ambos os corpos de funções têm o mesmo corpo de constantes. Conseqüentemente, $1 = deg\,(P') = [F'_{P'} : \mathbb{F}_{q^2}] = f(P'|P).[F_P : \mathbb{F}_{q^2}] = f(P'|P).deg\,(P)$ e temos $deg\ (P) = 1$. É natural perguntarmo-nos se vale a recíproca, ou seja, dado $P \in \mathbb{P}_{\mathbb{F}_{q^2}(x)}$ de grau 1 e $P' \in \mathbb{P}_{\mathcal{H}}$ acima de P, será que P' também tem grau 1? Obviamente, isso depende do valor do grau relativo $f(P'|P)$ e a recíproca valerá se ele for igual a 1.

Consideremos $\psi(T) = T^q + T - x^{q+1}$ o polinômio mínimo de y sobre $\mathbb{F}_{q^2}(x)$. Ele é separável, já que $\psi'(T) = 1$. Fixe $\beta \in \mathbb{F}_{q^2}$.

1. Se $\beta^{q+1} = 0$ e $\psi(\alpha) = 0$, então, $\alpha^q = -\alpha$. Conseqüentemente, $\alpha^{q^2} = (-\alpha)^q = \alpha$ e temos que as raízes de $\psi(T) = T^q + T$ pertencem a $\mathbb{F}_{q^2}$.

2. Se $\beta^{q+1} \neq 0$ e $\psi(\alpha) = 0$, então $\alpha^q + \alpha = \beta^{q+1} = (\beta^{q+1})^q = (\alpha^q + \alpha)^q = \alpha^{q^2} + \alpha^q$ e temos que $\alpha \in \mathbb{F}_{q^2}$.

Pelos Ítens 1. e 2. e pelo Teorema de Kummer (Teorema 1.3.12), fixado $\alpha \in \mathbb{F}_{q^2}$, há exatamente q lugares de $\mathcal{H}$ acima de $P_\alpha \in \mathbb{P}_{\mathbb{F}_{q^2}(x)}$ e seus índices de ramificação e graus relativos sobre P_α são iguais a 1. Concluímos que $\mathcal{H}$ tem pelo menos $q^2.q = q^3$ lugares racionais.

Para $P_\infty \in \mathbb{F}_{q^2}(x)$ e $P' \in \mathcal{H}$ acima de P_∞, temos:

$$-(q+1)e(P'|P_\infty) = v_{P'}(y^q + y) = v_{P'}(y^q) = q.v_{P'}(y)$$

e como $mdc\,(q, q+1) = 1$, $v_{P'}(y) = -(q+1)e(P'|P_\infty)/q \in \mathbb{Z}$ se, e somente se, q divide $e(P'|P_\infty) \leq q$. Conseqüentemente, $e(P'|P_\infty) = q$ e, pelo Teorema da Igualdade Fundamental, segue que $f(P'|P_\infty) = 1$. Logo, há um único lugar em $\mathcal{H}$ acima de P_∞ e tal lugar tem grau 1.

Pela Nota 1.3.29, temos que esses $q^3 + 1$ lugares são todos os lugares racionais de $\mathcal{H}$ (também é interessante notar que o número deles coincide com o número de pontos racionais da curva Hermitiana).

Finalmente,

$$q^3 + 1 = q^2 + 1 + q^3 - q^2 = q^2 + 1 + q.[q(q-1)] = q^2 + 1 + 2.g'.q$$

e temos que o corpo Hermitiano é, de fato, maximal sobre $\mathbb{F}_{q^2}$.

Capítulo 2

Os Polinômios de Chebyshev

Neste capítulo definiremos os polinômios de Chebyshev e algumas de suas propriedades. Eles aparecerão nas equações que definem as curvas maximais correspondentes a certos subcorpos do corpo Hermitiano $\mathcal{H}/\mathbb{F}_{q^2}$, assunto que abordaremos no próximo capítulo.

Ao longo deste e do próximo capítulos, $\mathbb{F}_{q^2}$ denotará um corpo finito com $q = p^n$ elementos, onde p é um número primo diferente de 2.

2.1 Definição e propriedades

Para cada $n \in \mathbb{N}$, considere a função $T_n : [-1, 1] \longrightarrow [-1, 1]$ tal que

$$T_n(cos\theta) = cos\, n\theta\,,\ 0 \leq \theta \leq \pi.$$

Fazendo-se $x = cos\theta$, temos que para $x \in$ I=[-1,1], existe um único $\theta = arccos(x)$ tal que $0 \leq \theta \leq \pi$ e, portanto, $T_n(x) = cos\,(n.arccos(x))$.

Como $e^{i\theta} = \cos\,\theta + \text{i sen}\,\theta$, temos:

$$e^{in\theta} = cos\, n\theta + isen\, n\theta. \qquad (1)$$

Por outro lado,

$$e^{in\theta} = (e^{i\theta})^n = (cos\,\theta + isen\,\theta)^n = \sum_{j=0}^{n} \binom{n}{j} cos^{n-j}\,\theta.(isen\,\theta)^j. \qquad (2)$$

Igualando as partes reais de (1) e (2), obtemos:

$$cos\, n\theta = \sum_{q=0}^{\lfloor n/2 \rfloor} \binom{n}{2q} cos^{n-2q}\, \theta.(-1)^q sen^{2q}.\, \theta. \qquad (3)$$

E, como $(sen^2\, \theta)^q$=$(1 - cos^2\, \theta)^q$, temos:

$$cos\, n\theta = \sum_{q=0}^{\lfloor n/2 \rfloor} \binom{n}{2q} cos^{n-2q}\, \theta.(-1)^q (1 - cos^2\, \theta)^q =$$

$$= \sum_{q=0}^{\lfloor n/2 \rfloor} \binom{n}{2q} cos^{n-2q}\, \theta.(-1)^q (\sum_{k=0}^{q} (-1)^k \binom{q}{k} cos^{2k}\, \theta). \qquad (4)$$

Portanto,

$$T_n(x) = \sum_{q=0}^{\lfloor n/2 \rfloor} \binom{n}{2q} x^{n-2q}.(-1)^q (\sum_{k=0}^{q} (-1)^k \binom{q}{k} x^{2k})$$

$$= \sum_{q=0}^{\lfloor n/2 \rfloor} \sum_{k=0}^{q} (-1)^{(q-k)+2k} \binom{n}{2q} \binom{q}{k} x^{n-2(q-k)}. \qquad (5)$$

Fazendo-se $r = q - k$, temos $r \leq \lfloor n/2 \rfloor$ e $q = r + k$ para $0 \leq k \leq \lfloor n/2 \rfloor - r$.

Assim, (5) pode ser reescrito da seguinte maneira:

$$T_n(x) = \sum_{r=0}^{\lfloor n/2 \rfloor} \sum_{q=r}^{\lfloor n/2 \rfloor} (-1)^r \binom{n}{2q} \binom{q}{q-r} x^{n-2r} =$$

$$= \sum_{r=0}^{\lfloor n/2 \rfloor} \left((-1)^r \sum_{q=r}^{\lfloor n/2 \rfloor} \binom{n}{2q} \binom{q}{r} \right) x^{n-2r}. \qquad (6)$$

Dessa última igualdade, concluímos que:

(a) O polinômio $T_n(x)$ tem grau n;

(b) Se n é ímpar, $n - 2r$ é ímpar e, portanto, só os coeficientes de potências ímpares de x são não nulos. Analogamente, se n é par, os únicos coeficientes de x diferentes de zero são os das potências pares de x. Em outras palavras, $T_n(-x) = (-1)^n T_n(x)$;

(c) O coeficiente líder de $T_n(x)$ é $\sum_{q=0}^{\lfloor n/2 \rfloor} \binom{n}{2q}\binom{q}{0} = \sum_{q=0}^{\lfloor n/2 \rfloor} \binom{n}{2q} = [(1+1)^n + (1-1)^n]/2 = 2^{n-1}$.

Definição 2.1.1. Definimos $\phi_n(x) = 2.T_n(x/2)$, $n \geq 1$, como o ***n-ésimo polinômio de Chebyshev***.

Proposição 2.1.2. *Seja ϕ_n o n-ésimo polinômio de Chebyshev. Então:*

(i) ϕ_n é um polinômio mônico de grau n;

(ii) $\phi_n(T) \in \mathbb{Z}[T]$ e $\phi_{n+1}(T) = T\phi_n(T) - \phi_{n-1}(T)$ para todo $n \geq 1$ e $T \in \mathbb{C}$;

(iii) Para todo $y \in \mathbb{C} \setminus \{0\}$ e $n \in \mathbb{N}$, $\phi_n(y + y^{-1}) = y^n + y^{-n}$.

Demonstração. (i) De fato, $T_n(x/2)$ tem grau n e seu coeficiente líder é $2^{n-1}/2^n = 1/2$.

(ii) Com efeito,

$$\phi_1(x) = 2.T_1(x/2) = 2.(x/2) = x.$$

Suponhamos que $\phi_n(T) \in \mathbb{Z}[T]$ para todo natural menor ou igual a n.

Como $cos\,(n+1)\theta = cos\,n\theta.cos\,\theta - sen\,n\theta.sen\,\theta$ e $cos\,(n-1)\theta = cos\,n\theta.cos\,\theta + sen\,n\theta.sen\,\theta$, temos que $cos\,(n+1)\theta + cos\,(n-1)\theta = 2cos\,n\theta cos\,\theta$, donde

$$2cos\,(n+1)\theta + 2cos\,(n-1)\theta = 2cos\,n\theta.2cos\,\theta.$$

Isto é,

$$2T_{n+1}(x) + 2T_{n-1}(x) = 2T_n(x)2T_1(x) \Longrightarrow 2T_{n+1}(2x/2) + 2T_{n-1}(2x/2) = 2T_n(2x/2)2x \Longrightarrow$$
$$\phi_{n+1}(2x) + \phi_{n-1}(2x) = \phi_n(2x)2x.$$

Fazendo-se $T := 2x$, obtemos:

$$\phi_{n+1}(T) = T\phi_n(T) - \phi_{n-1}(T),\ n \geq 1\,. \qquad (7)$$

Temos também que (7) vale para todo $T \in \mathbb{C}$, pois o polinômio $\phi_{n+1}(T) - T\phi_n(T) + \phi_{n-1}(T)$ se anula em [-2,+2] e, portanto, anula-se em um número infinito de pontos. Desse modo, pelo Teorema Fundamental da Álgebra, ele é identicamente nulo.

Concluímos, por indução, que $\phi_n(T) \in \mathbb{Z}[T]$.

(iii) É suficiente demonstrar que a identidade $\phi_n(y + y^{-1}) = y^n + y^{-n}$ vale em $S^1 = \{z \in \mathbb{C}; |z| = 1\}$, já que tal conjunto é infinito.

Seja $y \in S^1$, então $y = e^{i\theta}$ para algum $\theta \in [0, 2\pi)$ e $y^n + y^{-n} = e^{in\theta} + e^{-in\theta} = 2cos\,n\theta = 2T_n(x) = 2T_n(cos\,\theta) = 2T_n(2cos\,\theta/2) = \phi_n(2cos\,\theta) = \phi_n(e^{i\theta} + e^{-i\theta}) = \phi_n(y + y^{-1})$. Logo,

$$\phi_n(y + y^{-1}) = y^n + y^{-n} \text{ para todo } n \text{ natural.} \qquad (8)$$

∎

Corolário 2.1.3. *Sejam ϕ_n e ϕ_m o n-ésimo e o m-ésimo polinômios de Chebyshev, respectivamente. Então $\phi_n(\phi_m(T)) = \phi_{mn}(T) = \phi_m(\phi_n(T))$ para todo $T \in \mathbb{C}$.*

Demonstração. A prova é imediata do item (*iii*) do Teorema anterior. ∎

Proposição 2.1.4. *Seja $\phi_n(T)$ o n-ésimo polinômio de Chebyshev. Então:*

(i) Se n é ímpar, temos $\phi_n(T) - 2 = (T-2)(P_{(n-1)/2}(T))^2$, onde $P_{(n-1)/2}(T) = (1 + \sum_{j=1}^{(n-1)/2} \phi_j(T))$;

(ii) Se n é ímpar, temos $\phi_n(T) + 2 = (T+2)(Q_{(n-1)/2}(T))^2$, onde $Q_{(n-1)/2}(T) = (1 + \sum_{j=1}^{(n-1)/2} \phi_j(-T))$;

(iii) Se n é par, temos $\phi_n(T) - 2 = (T^2-4)(F_{(n-2)/2}(T))^2$, onde

$$F_{(n-2)/2}(T) = \left(\sum_{j=1}^{r} \phi_{2j-1}(T)\right), \text{ se } n = 2(2r) \text{ para algum } r \in \mathbb{N}$$

e

$$F_{(n-2)/2}(T) = \left(1 + \sum_{j=1}^{r} \phi_{2j}(T)\right), \text{ se } n = 2(2r+1) \text{ para algum } r \in \mathbb{N};$$

(iv) Se n é par, $\phi_n(T) + 2 = (\phi_{n/2}(T))^2$.

Demonstração. Seja $T = y + y^{-1}$. (*i*) Se n é ímpar, temos:

$$\phi_n(T) - 2 = y^n + y^{-n} - 2 = (y^{n/2} - y^{-n/2})^2 = (y^{1/2} - y^{-1/2})^2 \left(\frac{y^{n/2} - y^{-n/2}}{y^{1/2} - y^{-1/2}}\right)^2 =$$

$$= (y + y^{-1} - 2)\left(y^{\frac{1-n}{2}}\left(\frac{y^n - 1}{y - 1}\right)\right)^2 = (y + y^{-1} - 2)(y^{\frac{1-n}{2}}(1 + y + y^2 + \cdots + y^{n-1}))^2 =$$

$$= (T-2)[(y^{\frac{n-1}{2}} + y^{\frac{1-n}{2}}) + (y^{\frac{n-3}{2}} + y^{\frac{3-n}{2}}) + \cdots + (y + y^{-1}) + 1]^2 =$$

$$= (T-2)(1 + \sum_{j=1}^{(n-1)/2} \phi_j(T))^2 = (T-2)(P_{\frac{n-1}{2}}(T))^2.$$

(*ii*) Se n é ímpar, temos:

$$\phi_n(T) + 2 = -\phi_n(-T) + 2 = -(\phi_n(-T) - 2) = -(-T-2)(P_{\frac{n-1}{2}}(-T))^2 =$$

$$= (T+2)(P_{\frac{n-1}{2}}(-T))^2 = (T+2)(Q_{\frac{n-1}{2}}(T))^2.$$

(*iii*) Seja $n \in \mathbb{N}$ par. Logo:

$$\phi_n(T) - 2 = y^n + y^{-n} - 2 = (y^{n/2} - y^{-n/2})^2 =$$

$$= (y - y^{-1})^2 \left(\frac{y^{n/2} - y^{-n/2}}{y - y^{-1}}\right)^2 = (y^2 + y^{-2} - 2)\left(y^{1-n/2}\left(\frac{y^n - 1}{y^2 - 1}\right)\right)^2 =$$

$$= ((y + y^{-1})^2 - 4)(y^{1-n/2}(1 + y^2 + y^4 + \cdots + y^{n-2}))^2. \qquad (*)$$

Há dois casos a considerar:

- Se $n = 2(2r) = 4r$, para algum $r \in \mathbb{N}$. Nesse caso, obtemos de $(*)$ que:

$$\phi_n(T) - 2 = ((y + y^{-1})^2 - 4)(y^{1-2r}(1 + y^2 + y^4 + \cdots + y^{2(2r-1)}))^2 =$$

$$= ((y + y^{-1})^2 - 4)((y^{2r-1} + y^{1-2r}) + (y^{2r-3} + y^{3-2r}) + \cdots + (y + y^{-1}))^2 =$$

$$= (T^2 - 4)(\sum_{j=1}^{r} \phi_{2j-1}(T))^2 = (T^2 - 4)(F_{(n-2)/2}(T))^2.$$

- Se $n = 2(2r+1) = 4r + 2$, para algum $r \in \mathbb{N}$. Analogamente ao item anterior, obtemos de $(*)$:

$$\phi_n(T) - 2 = ((y + y^{-1})^2 - 4)(y^{-2r}(1 + y^2 + \cdots + y^{4r}))^2 =$$

$$= (T^2 - 4)((y^{2r} + y^{-2r}) + (y^{2r-2} + y^{2-2r}) + \cdots + (y^2 + y^{-2}) + 1)^2 =$$

$$= (T^2 - 4)(1 + \sum_{j=1}^{r} \phi_{2j}(T))^2 = (T^2 - 4)(F_{(n-2)/2}(T))^2.$$

(*iv*) Finalmente, se n é par: $\phi_n(T) + 2 = y^n + y^{-n} + 2 = (y^{n/2} + y^{-n/2})^2 = (\phi_{n/2}(T))^2$.

∎

Lema 2.1.5. *Sejam p a característica de $\mathbb{F}_{q^2}$ e $\varphi_n(T) := \phi_n(T) \ (mod\ p) \in \mathbb{F}_{q^2}[T]$, onde ϕ_n é o n-ésimo polinômio de Chebyshev. Se $mdc\,(n, p) = 1$, então $\varphi_n(T)$ é separável (além disso, se n divide $\frac{q-1}{2}$, as raízes de $\varphi_n(T)$ pertencem a $\mathbb{F}_{q^2}$).*

Demonstração. Seja $T = y + y^{-1}$ para algum $y \in \overline{\mathbb{F}}_{q^2}$. Temos $\varphi_n(T) = y^n + y^{-n} = 0$ se, e somente se, $y^{2n} = -1$. Como $mdc\,(n, p) = 1$, a equação $\xi^{2n} = -1$ possui exatamente $2n$ raízes distintas.

Para mostrar que $\varphi_n(T)$ é separável, basta observar que se $x_1, x_2 \in \mathbb{F}_{q^2}$ e $z_1 = x_1 + {x_1}^{-1}$ e $z_2 = x_2 + {x_2}^{-1}$ são raízes de $\varphi_n(T)$, então $z_1 = z_2$ se, e somente se, $x_1 = x_2$ ou $x_1 = {x_2}^{-1}$. Logo, toda raiz de $\xi^{2n} = -1$, bem como sua inversa, correspondem a uma mesma raiz de $\varphi_n(T)$. Como 1 e -1 não são raízes de $\xi^{2n} = -1$, qualquer raiz de $\xi^{2n} = -1$ é diferente de sua inversa. Desse modo, $\varphi_n(T)$ possui exatamente $n = 2n/2$ raízes distintas e, portanto, é separável.

Finalmente, seja $z = x + x^{-1} \in \overline{\mathbb{F}}_{q^2}$ tal que $\varphi_n(z) = 0$. Logo, $x^{2n} = -1$. Se n divide $\frac{q-1}{2}$, então $4n$ divide $q^2 - 1$ e temos que $x \in \mathbb{F}_{q^2}$, o que resulta em $z \in \mathbb{F}_{q^2}$. ∎

Corolário 2.1.6. *Seja $\varphi_n(T)$ como no Lema 2.1.5. Considere $p_k(T) := P_k(T)\ (mod\, p)$, $q_k(T) = Q_k(T)\ (mod\ p)$, $f_{\tilde{k}}(T) = F_{\tilde{k}}(T)\ (mod\ p)$, onde $k = (n-1)/2$ e $\tilde{k} = (n-2)/2$, e $P_k(T)$, $Q_k(T)$ e $F_{\tilde{k}}(T)$ são os polinômios dados na Proposição 2.1.4. Então:*

(i) Valem as afirmativas $(i) - (iv)$ da Proposição 2.1.4, trocando: P_k por p_k, Q_k por q_k, $F_{\tilde{k}}$ por $f_{\tilde{k}}$ e ϕ_n por φ_n;

(ii) $\varphi_n(T) - 2$ e $\varphi_n(T) + 2$ têm raízes em $\mathbb{F}_{q^2}$ sempre que n divide $q - 1$;

(iii) Os polinômios p_k, q_k, $f_{\tilde{k}}$ e $\varphi_{n/2}$ em cada uma das afirmativas em (i) (deste Corolário) são separáveis.

Demonstração. (i) Imediato.

(ii) Seja $z = x + x^{-1}, x \in \overline{\mathbb{F}}_{q^2}$, uma raiz de $\varphi_n(T) - 2$. Como $\varphi_n(z) = \varphi_n(x + x^{-1}) = x^n + x^{-n}$, temos $x^n + x^{-n} - 2 = 0$, isto é, $(x^n - 1)^2/x^n = 0$. Logo, z é raiz de $\varphi_n(T) - 2$ se, e somente se, $x^n = 1$. Assim, $x^{q-1} = (x^n)^{\frac{q-1}{n}} = 1$ e temos $x \in \mathbb{F}_{q^2}$. Portanto, $z \in \mathbb{F}_{q^2}$.

Analogamente, prova-se que se $z \in \overline{\mathbb{F}}_{q^2}$ é raiz de $\varphi_n(T) + 2$, então $z \in \mathbb{F}_{q^2}$. A única diferença é que se $z = x + x^{-1}$ é raiz de $\varphi_n(T) + 2$, então $(x^n + 1)^2/x^n = 0$. Portanto, z é raiz de $\varphi_n(T) + 2$ se, e somente se, $x^n = -1$, donde $x^{q^2-1} = ((x^n)^{q+1})^{(q-1)/n} = 1$.

(iii) Sejam $x_1, x_2 \in \mathbb{F}_{q^2}$ e $z_1 = x_1 + {x_1}^{-1}$ e $z_2 = x_2 + {x_2}^{-1}$.

- Caso $\varphi_n(T) - 2$: se z_1 é uma raiz de $\varphi_n(T) - 2$, então ${x_1}^n = 1$. Temos $z_1 = z_2$ se, e somente se, $x_1 = {x_2}^{-1}$ ou $x_1 = x_2$. Logo:

  Se n é ímpar, a única raiz de $x^n = 1$ que é igual à sua inversa é 1. Logo, $\varphi_n(T) - 2$ possui exatamente $\frac{n-1}{2} + 1$ raízes distintas. Como $\varphi_n(T) - 2 = (T - 2){p_k}^2(T)$ e

$deg\, p_k(T) = \frac{n-1}{2}$, $p_k(T)$ tem no máximo $\frac{n-1}{2}$ raízes. Em particular, 2 não é raiz de $p_k(T)$, pois caso contrário $\varphi_n(T) - 2 = (T-2){p_k}^2(T)$ teria no máximo $\frac{n-1}{2}$ raízes, absurdo. Concluímos também que $p_k(T)$ tem exatamente $\frac{n-1}{2}$ raízes distintas e, portanto, é separável.

Por outro lado, se $n = 2l$ é par, as únicas raizes de $x^n = 1$ que são iguais às suas inversas são 1 e -1 (isso independe de l ser par ou ímpar). Logo, $\varphi_n(T) - 2 = (T^2-4){f_{\tilde{k}}}^2(T)$ possui exatamente $\frac{n-2}{2} + 2$ raízes distintas. Um argumento análogo ao que fizemos para n ímpar mostra que $f_{\tilde{k}}$ é separável e que nem 2 e nem -2 são suas raízes.

- Caso $\varphi_n(T) + 2$: se n é par, pelo Lema 2.1.5 segue que $\varphi_{n/2}(T)$ é separável já que $mdc\,(n/2, q) = 1$.

  Por outro lado, se n é ímpar, temos $\varphi_n(T)+2 = (-1)^n\varphi_n(-T)+2 = -\varphi_n(-T)+2 = -(\varphi_n(-T) - 2)$ e pelo caso anterior, $q_k(T)$ é separável e não se anula em -2.

∎

Definição 2.1.7. Para um polinômio $\varphi(z) \in \mathbb{F}_{q^2}[z]$, definimos

$$N(\varphi) = \{\alpha \in \mathbb{F}_{q^2};\ \varphi(\alpha) \in \mathbb{F}_q\}.$$

A Proposição seguinte generaliza o Teorema 6.2 de [G-S].

Proposição 2.1.8. *Considerando-se a Definição* 2.1.7*, se n divide $q-1$, então:*
(i) $N(\varphi_n) = (q(n+1) - n + 1)/2$ se n é ímpar;
(ii) $N(\varphi_n) = (q(n+2) - n)/2$ se n é par.
Em particular, $N(\varphi_{q-1}) = (q^2+1)/2$.

Demonstração. Seja $\alpha = x + x^{-1} \in \mathbb{F}_{q^2}$, para algum $x \in \overline{\mathbb{F}}_{q^2}$. Temos:

$$(x + x^{-1})^{q^2} = x + x^{-1} \Longleftrightarrow x^{q^2} + x^{-q^2} = x + x^{-1} \Longleftrightarrow$$

$$\Longleftrightarrow x^{q^2} = x \text{ ou } x^{q^2} = x^{-1} \Longleftrightarrow x \in \mathbb{F}_{q^2} \text{ ou } x^{q^2+1} = 1. \qquad (*)$$

Logo,

$$\varphi_n(\alpha) = \varphi_n(x + x^{-1}) = x^n + x^{-n} \in \mathbb{F}_q \Longleftrightarrow (x^n + x^{-n})^q = x^n + x^{-n} \Longleftrightarrow$$

$$\iff x^{nq}+x^{-nq}=x^n+x^{-n} \iff x^{nq}=x^n \ \ ou \ \ x^{nq}=x^{-n} \iff x^n \in \mathbb{F}_q \ \ ou \ \ x^{n(q+1)}=1 \qquad (**)$$

De $(*)$ e $(**)$, é imediato que

$$N(\varphi_n)=(\#A+2)/2, \qquad (***)$$

onde

$$A=\{x \in \mathbb{F}_{q^2};\ x^n \in \mathbb{F}_q \ \ ou \ \ x^{n(q+1)}=1\} \cup \{x \in \overline{\mathbb{F}}_{q^2};\ x^{q^2+1}=1 \text{ e } (x^n \in \mathbb{F}_q \ \ ou \ \ x^{n(q+1)}=1)\} =$$

$$= \{x;\ x^{q^2-1}=1 \ \ e \ \ x^{n(q-1)}=1\} \cup \{x;\ x^{q^2-1}=1 \ \ e \ \ x^{n(q+1)}=1\} \cup$$

$$\cup \{x;\ x^{q^2+1}=1 \ \ e \ \ x^{n(q-1)}=1\} \cup \{x;\ x^{q^2+1}=1 \ \ e \ \ x^{n(q+1)}=1\} \qquad (****)$$

e o acréscimo de 2 à cardinalidade de A corresponde aos valores de $\alpha = x + x^{-1}$ para os quais $x = x^{-1}$ (que são exatamente 1 e -1).

Notemos que x satisfaz $x^a = 1$ e $x^b = 1$ se, e somente se, $x^{mdc\,(a,b)} = 1$. Logo:

(i) Se n é ímpar:

1. $x^{q^2-1}=1$ e $x^{n(q-1)}=1 \iff 1=x^{mdc(q^2-1,\,n(q-1))}=x^{q-1}$;
2. $x^{q^2-1}=1$ e $x^{n(q+1)}=1 \iff 1=x^{mdc(q^2-1,\,n(q+1))}=x^{n(q+1)}$;
3. $x^{q^2+1}=1$ e $x^{n(q-1)}=1 \iff 1=x^{mdc(q^2+1,\,n(q-1))}=x^2$;
4. $x^{q^2+1}=1$ e $x^{n(q+1)}=1 \iff 1=x^{mdc(q^2+1,\,n(q+1))}=x^2$.

Como as raízes de x^2-1 são também raízes de $x^{q-1}-1$, temos de $(****)$, que:

$$A=\{x;\ x^{q-1}=1\} \cup \{x;\ x^{n(q+1)}=1\}.$$

Além disso,

$$\{x;\ x^{q-1}=1\} \cap \{x;\ x^{n(q+1)}=1\} = \{x;\ 1=x^{mdc(q-1,n(q+1))}=x^{2n}\}.$$

Portanto,

$$\#A=(q-1)+n(q+1)-2n \ \ e \ \ N(\varphi_n)=((q-1)+n(q+1)-2n+2)/2=(q(n-1)-n+1)/2.$$

(*ii*) Se n é par: a única diferença para o item (i) é que $mdc(q^2-1, n(q-1)) = 2(q-1)$. Logo, para A (definido por $(****)$) , temos

$$A = \{x;\ x^{2(q-1)} = 1\} \cup \{x;\ x^{n(q+1)} = 1\}$$

e $\{x;\ x^{2(q-1)} = 1\} \cap \{x;\ x^{n(q+1)} = 1\} = \{x;\ x^{2n} = 1\}$.

Portanto,

$$\#A = 2(q-1)+n(q+1)-2n \ \ e \ \ N(\varphi_n) = (2(q-1)+n(q+1)-2n+2)/2 = (q(n+2)-n)/2.$$

Em particular, para $n = q-1$, temos $N(\varphi_{q-1}) = (q(q+1)-q+1)/2 = (q^2+1)/2$. ∎

Para a demonstração do próximo Teorema, faremos uso da Proposição 3.3.1 e do Corolário 3.3.3, demonstrados ao final do próximo capítulo.

Teorema 2.1.9. *Sejam p um número primo diferente de 2 e $q = p^r$ para algum $r \in \mathbb{N}\backslash\{0\}$. Considere o polinômio $\varphi_{q-1} = \phi_{q-1}\,(mod\ p)$, onde ϕ_{q-1} é o $(q-1)$-ésimo polinômio de Chebyshev. Então $\phi_{q-1}(T-2) \in \mathbb{Z}[T]$ é tal que os coeficientes de T^j, $1 \leq j\ < (q+1)/2$, são múltiplos de p.*

Demonstração. Da Proposição 3.3.1 e do Corolário 3.3.3 (veja-os no capítulo 3), obtemos que:

$\varphi_{\frac{q-1}{2}}(T-2)(T)^{\frac{q+1}{2}} = T + T^q + \varphi_{q-1}(T-2) - 2$, onde $T = y + y^{-1} + 2$.

Logo, $\varphi_{q-1}(T-2) = 2 - T + \varphi_{\frac{q-1}{2}}(T-2).T^{\frac{q+1}{2}} - T^q$.

Como os coeficientes de $\varphi_{\frac{q-1}{2}}(T-2)T^{\frac{q+1}{2}}$ de grau menor que $\frac{q+1}{2}$ são nulos, o resultado é imediato. ∎

Capítulo 3

Curvas Maximais e Polinômios de Chebyshev

Um dos objetivos desse capítulo é obter equações explícitas para algumas curvas maximais. Para isso, usaremos o fato de que qualquer subcorpo do corpo Hermitiano é o corpo de funções de alguma curva maximal e daremos exemplos de subcorpos de $\mathcal{H}$ cuja equação para a curva maximal envolve polinômios de Chebyshev.

Relembramos que ao longo deste capítulo, $\mathbb{F}_{q^2}$ denotará um corpo finito com $q = p^n$ elementos, onde p é um primo ímpar.

3.1 Subgrupos de automorfismos de $\mathcal{H}/\mathbb{F}_{q^2}$

Seja $\mathcal{H}/\mathbb{F}_{q^2}$ o corpo de funções Hermitiano, onde $\mathcal{H} = \mathbb{F}_{q^2}(x, y)$, definido pela equação $x^{q+1} = y^q + y$. Considere $\mathcal{A} := \{\sigma : \mathcal{H} \longrightarrow \mathcal{H};\ \sigma \text{ é um automorfismo de } \mathcal{H}/\mathbb{F}_{q^2}\}$ o grupo de automorfismos da extensão $\mathcal{H}/\mathbb{F}_{q^2}$. Sejam $a \in \mathbb{F}_{q^2} \setminus \{0\}$ uma (q^2-1)-ésima raiz primitiva da unidade e ε dado por $\varepsilon(x) = ax$ e $\varepsilon(y) = a^{q+1}y$; $\varepsilon \in \mathcal{A}$ e $\varepsilon|_{\mathbb{F}_{q^2}} = id$ pois:

$$[\varepsilon(y)]^q + \varepsilon(y) = (a^{q+1}y)^q + a^{q+1}y = a^{(q+1)q}y^q + a^{q+1}y = a^{q^2+q+1-1}y^q + a^{q+1}y =$$

$$= a^{q^2-1}a^{q+1}y^q + a^{q+1}y = a^{q+1}y^q + a^{q+1}y = a^{q+1}x^{q+1} = [\varepsilon(x)]^{q+1}.$$

Seja ω definido por $\omega(x) = x/y$ e $\omega(y) = y^{-1}$; $\omega \in \mathcal{A}$ e $\omega|_{\mathbb{F}_{q^2}} = id$ pois:

$$[\omega(y)]^q + \omega(y) - \omega(x)^{q+1} = \frac{1}{y^q} + \frac{1}{y} - \frac{x^{q+1}}{y^{q+1}} = 0.$$

A prova do próximo resultado pode ser encontrada, por exemplo, em [G-L].

Proposição 3.1.1. *Sejam $s \geq 1$ um inteiro, G um grupo finito e $a,b \in G$ satisfazendo $bab^{-1} = a^s$. Sejam também m e n naturais positivos tais que $a^n = e$, $b^m \in \langle a \rangle$.* $(*)$

Se os inteiros m, n são escolhidos minimalmente satisfazendo $(*)$, então o grupo $\langle a, b \rangle$ tem ordem igual a mn. ∎

Finalmente, considere o subgrupo $\mathcal{C} = \langle \varepsilon, \omega \rangle$ de $\mathcal{A}$ gerado por ε e ω. $\mathcal{C}$ tem ordem $2(q^2-1)$. De fato, $ord\,(\omega) = 2$, $ord\,(\varepsilon) = q^2-1$, $\omega^{-1}.\varepsilon.\omega = \varepsilon^{-q} = \varepsilon^{q^2-1-q}$ e pela Proposição 3.1.1 segue que $|\langle \varepsilon, \omega \rangle| = 2(q^2-1)$.

Para um divisor m de q^2-1, considere o subgrupo $\mathcal{G} = \langle \lambda, \omega \rangle$ de $\mathcal{C}$ gerado por λ e ω, onde $\lambda = \varepsilon^{\frac{q^2-1}{m}}$. Pela Proposição 3.1.1, $|\mathcal{G}| = 2m$ já que $ord\,(\omega) = 2$, $ord\,\lambda = m$ e $\omega^{-1}.\lambda.\omega = \lambda^{-q} = \lambda^{\delta.\omega - q}$, onde $\delta =$ mín $\{a \in \mathbb{N} \setminus \{0\}\ ; a.m > q\}$.

Vamos estudar o subcorpo $\mathcal{H}^{\mathcal{G}}$ de $\mathcal{H}$, corpo fixo pelo grupo $\mathcal{G}$, nos seguintes casos:

(1) m é um divisor de $(q-1)$

(2) m é um divisor de $(q+1)$

3.2 O caso em que m divide $q-1$

Começamos a seção com o seguinte Lema (cuja demonstração pode ser encontrada em, por exemplo, [E]):

Lema 3.2.1. *Sejam K um corpo e $L = K(\mathcal{R}_{x^n-a})$ o corpo de decomposição de $x^n - a$ sobre K, para algum $a \in K^*$. Suponhamos que $\mathcal{P}_n(K) := \{y \in K^*; ord\,(y) = n\} \neq \varnothing$. Então:*

(a) $Aut_K(L)$ é um grupo cíclico e $|Aut_K(L)| = [L:K] = n$ se, e somente se, $x^n - a$ for irredutível em $K[x]$. ∎

Ao longo deste capítulo, vamos considerar $\mathcal{H} = \mathbb{F}_{q^2}(x, y)$, onde $x^{q+1} = y^q + y$, e $F := \mathbb{F}_{q^2}(x^{q-1}, y^{q-1})$.

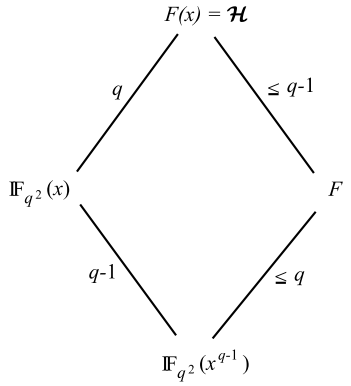
Teorema 3.2.2. *$\mathcal{H}/F$ é uma extensão cíclica de grau $(q-1)$.*

Demonstração. Primeiro analisemos a extensão $\mathcal{H}/F(x)$. Temos que:

$$y^q + y = x^{q+1} \Rightarrow y(y^{q-1}+1) = x^{q+1} \Rightarrow y = \frac{x^{q+1}}{y^{q-1}+1} \in \mathbb{F}_{q^2}(x, y^{q-1}) = F(x)$$

Logo, $F(x) = \mathcal{H}$.

Temos também que, $y^{q-1}(y^{q-1}+1)^{q-1} = (x^{q-1})^{q+1}$ e, portanto, y^{q-1} é raiz de $p(u) = u(u+1)^{q-1} - (x^{q-1})^{q+1} \in \mathbb{F}_{q^2}(x^{q-1})[u]$ e temos $[F : \mathbb{F}_{q^2}(x^{q-1})] \leq \deg p(u) = q$. Também sabemos que x é raiz de $h(u) = u^{q-1} - x^{q-1} \in F[u]$, logo $[\mathcal{H} : F] = [F(x) : F] \leq q-1$.



Por outro lado, $[\mathbb{F}_{q^2}(x) : \mathbb{F}_{q^2}(x^{q-1})] = q-1$ e $[\mathcal{H}/\mathbb{F}_{q^2}(x)] = q$. Logo, $[F : \mathbb{F}_{q^2}(x^{q-1})] = q$ e $[\mathcal{H} : F] = q-1$, ou seja, $h(u)$ é irredutível em $F[u]$.

$F = \mathbb{F}_{q^2}(x^{q-1}, y^{q-1})$ contém uma $(q-1)$-ésima raiz primitiva da unidade e $\mathcal{H} = F(x) = F(\mathcal{R}_{u^{q-1}-x^{q-1}})$, então pelo Lema 3.2.1 temos que $Aut_F(\mathcal{H})$ é cíclico, ou seja, $\mathcal{H}/F$ é uma extensão cíclica. ∎

Para um divisor m de $(q-1)$ denotamos por E_1 o único corpo intermediário de $\mathcal{H}/F$ satisfazendo $[\mathcal{H} : E_1] = m$ (tal corpo existe e é único, pois $\mathcal{H}/F$ é cíclica).

Considere $E_1^\omega := E_1^{\langle\omega\rangle}$ o subcorpo de E_1 fixo pelo subgrupo de $\mathcal{A}$ gerado por ω. Temos $E_1^\omega = \mathcal{H}^\mathcal{G}$ (de fato, $\mathcal{H}^{\langle\lambda\rangle} = E_1$ já que $ord\,(\lambda) = m$ e E_1 é o único subcorpo de $\mathcal{H}$ de ordem m. Assim, $E_1^{\langle\omega\rangle} = \mathcal{H}^{\langle\lambda\rangle\langle\omega\rangle} = \mathcal{H}^{\langle\lambda,\omega\rangle} = \mathcal{H}^\mathcal{G}$).

Lema 3.2.3. *Sejam $F = \mathbb{F}_{q^2}(x^{q-1}, y^{q-1})$, onde $x^{q+1} = y^q + y$, e F^ω seu corpo fixo pelo automorfismo ω dado por $\omega(x) = x/y$ e $w(y) = y^{-1}$. Então $F^\omega = \mathbb{F}_{q^2}(x^2/y)$ é um corpo de funções racionais.*

Demonstração. Temos que $\frac{x^2}{y} = \frac{y^{q-1}+1}{x^{q-1}} \in \mathbb{F}_{q^2}(x^{q-1}, y^{q-1}) = F$.

Além disso,

$$\omega\left(\frac{x^2}{y}\right) = \frac{[\omega(x)]^2}{\omega(y)} = \frac{x^2}{y}.$$

Logo, $\mathbb{F}_{q^2}(\frac{x^2}{y}) \subset F^\omega \subset \mathcal{H}$. Como $(y^{q-1} - y^{-(q-1)}) \in F \setminus F^\omega$ e $(y^{q-1} - y^{-(q-1)})^2 = (y^{q-1} + y^{-(q-1)}) - 4 \in F^\omega$, temos que $[F : F^\omega] = 2$. Portanto, $[\mathcal{H} : F^\omega] = 2(q-1)$ e basta provarmos que $\left[\mathcal{H} : \mathbb{F}_{q^2}\left(\frac{x^2}{y}\right)\right] = 2(q-1)$. Para isso, determinaremos o divisor de pólos da função $\frac{x^2}{y}$ em $\mathcal{H}/\mathbb{F}_{q^2}$ e usaremos a Proposição 1.2.5, que diz que $deg\left(\frac{x^2}{y}\right)_\infty = \left[\mathcal{H} : \mathbb{F}_{q^2}\left(\frac{x^2}{y}\right)\right]$.

Seja $P' \in \mathbb{P}_\mathcal{H}$. Como $y^q + y = x^{q+1}$, temos:

- Se $v_{P'}(y) > 0$, $v_{P'}(y) = v_{P'}(y^q + y) = (q+1)v_{P'}(x)$. Portanto, $v_{P'}(x) > 0$ e $v_{P'}(x^2/y) = 2v_{P'}(x) - v_{P'}(y) = -(q-1)v_{P'}(x)$ e temos que P' é um pólo de x^2/y na extensão $\mathcal{H}/\mathbb{F}_{q^2}$.

- Se $v_{P'}(y) < 0$, $qv_{P'}(y) = v_{P'}(y^q + y) = (q+1)v_{P'}(x)$. Portanto, $v_{P'}(x) = -q.a$ para algum $a \in \mathbb{N}^*$ e $v_{P'}(x^2/y) = 2v_{P'}(x) - v_{P'}(y) = -2qa + (q+1)a = -a(q-1) < 0$ e temos que P' é um pólo de x^2/y em $\mathcal{H}/\mathbb{F}_{q^2}$.

- Se $v_{P'}(y) = 0$, $(q+1)v_{P'}(x) = v_{P'}(y^q + y) \geq \text{mín}\ \{\ v_{P'}(y^q), v_{P'}(y)\ \} \geq 0$. Portanto, $v_{P'}(x^2/y) = 2v_{P'}(x) - v_{P'}(y) = 2v_{P'}(x)$ e temos que P' não é pólo de x^2/y em $\mathcal{H}/\mathbb{F}_{q^2}$.

Mostramos acima que se P' é pólo de x ou zero de y em $\mathcal{H}$, então P' é pólo de $\frac{x^2}{y}$ em $\mathcal{H}$. Por outro lado, os pólos de $\frac{x^2}{y}$ em $\mathcal{H}$ são os pólos de x ou zeros de y em $\mathcal{H}$. Deste modo, os únicos pólos de x^2/y em $\mathcal{H}$ são os zeros de y em $\mathcal{H}$ e os pólos de x em $\mathcal{H}$.

Seja $P'_0 \in \mathbb{P}_\mathcal{H}$ tal que $P'_0|P_0$, onde $P_0 \in \mathbb{P}_{\mathbb{F}_{q^2}(y)}$ é o zero de y em $\mathbb{F}_{q^2}(y)/\mathbb{F}_{q^2}$, então:

$$0 < e(P'_0|P_0) = e(P'_0|P_0)v_{P_0}(y) = v_{P'_0}(y) = v_{P'_0}(y) + v_{P'_0}(y^{q-1} + 1) = (q+1)v_{P'_0}(x).$$

E como $e(P'_0|P_0) \leq q+1$, segue que $e(P'_0|P_0) = q+1$. Portanto, P_0 ramifica-se totalmente em $\mathcal{H}/\mathbb{F}_{q^2}(y)$, $v_{P'_0}(y) = q+1$ e $v_{P'_0}(x) = 1$.

Por outro lado, se $P'|P_\infty$, onde $P' \in \mathbb{P}_\mathcal{H}$ e $P_\infty \in \mathbb{P}_{\mathbb{F}_{q^2}(x)}$ é o pólo de x em $\mathbb{F}_{q^2}(x)/\mathbb{F}_{q^2}$, temos:

$$v_{P'}(x) = e(P'|P_\infty)v_{P_\infty}(x) = -e(P'|P_\infty) \text{ e } q{\cdot}v_{P'}(y) = v_{P'}(y^q{+}y) = (q{+}1)v_{P'}(x) = -(q{+}1)e(P'|P_\infty).$$

E como $mdc\,(q+1,q) = 1$ e $e(P'_\infty|P_\infty) \leq q$, temos que $e(P'|P_\infty) = q$, ou seja, P_∞ ramifica-se totalmente em $\mathcal{H}/\mathbb{F}_{q^2}(x)$, $v_{P'}(x) = -q$ e $v_{P'}(y) = -(q+1)$.

Finalmente,

$$\begin{aligned}(x^2/y)_\infty &= -v_{P'}(x^2/y)P' - v_{P'_0}(x^2/y)P'_0 = \\ &= [-v_{P'}(x^2) + v_{P'}(y)]P' + [-v_{P'_0}(x^2) + v_{P'_0}(y)]P'_0 = \\ &= [2q-(q+1)]P' + [-2+q+1]P'_0 = (q-1)P' + (q-1)P'_0.\end{aligned}$$

Dado que $x^2/y \in F^\omega$, $2(q-1) = deg\,(x^2/y)_\infty = [\mathcal{H} : \mathbb{F}_{q^2}(x^2/y)]$ e $[\mathcal{H} : F^\omega] = 2(q-1)$, concluímos que:

$$[F^\omega : \mathbb{F}_{q^2}(x^2/y)] = [\mathcal{H} : \mathbb{F}_{q^2}(x^2/y)]/[\mathcal{H} : F^\omega] = \frac{2(q-1)}{2(q-1)} = 1, \text{ como queríamos demonstrar.}$$

∎

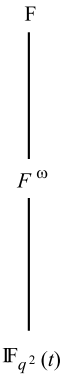
Lema 3.2.4. *Existem exatamente $(q+1)$ lugares de F^ω que se ramificam na extensão $F|F^\omega$ e eles são os zeros (cada um deles simples) de $y^{q-1} + y^{-(q-1)} - 2$.*

Demonstração. Seja $t = y^{q-1} + y^{-(q-1)} \in F^\omega$. Temos que:

$$\left(\frac{x^2}{y}\right)^{q+1} = \frac{(x^{q+1})^2}{y^{q+1}} = \frac{(y^q+y)^2}{y^{q+1}} = \frac{y^{2q}+2y^{q+1}+y^2}{y^{q+1}} = y^{q-1} + y^{-(q-1)} + 2 = t+2.$$

Afirmação: $z^{q+1} - (t+2)$ é o polinômio mínimo de $\frac{x^2}{y}$ sobre $\mathbb{F}_{q^2}(t)$. Em particular, $t+2 \neq u^d$, para todo $d > 1$ divisor de $q+1$ e para todo $u \in \mathbb{F}_{q^2}(t)$.
Demonstração: De fato, $F/\mathbb{F}_{q^2}(y^{q-1})$ tem grau $q+1$ pois o polinômio mínimo de x^{q-1} sobre $\mathbb{F}_{q^2}(y^{q-1})$ é $p_{x^{q-1},\mathbb{F}_{q^2}(y^{q-1})}(z) = z^{q+1} - y^{q-1}(1+y^{q-1})^{q-1}$ e como $[\mathbb{F}_{q^2}(y^{q-1}) : \mathbb{F}_{q^2}(t)] = 2$, temos que $[F : \mathbb{F}_{q^2}(t)] = [F : \mathbb{F}_{q^2}(y^{q-1})][\mathbb{F}_{q^2}(y^{q-1}) : \mathbb{F}_{q^2}(t)] = 2(q+1)$. Conseqüentemente, $[F^\omega : \mathbb{F}_{q^2}(t)] = [F : \mathbb{F}_{q^2}(t)]/[F : F^\omega] = (2(q+1))/2 = q+1$. □

Além disso, $\mathbb{F}_{q^2}$ contém uma $(q+1)$-ésima raiz primitiva da unidade e $mdc\,(q+1,p) = 1$. Logo, $\mathbb{F}_{q^2}(t)(x^2/y) = F^\omega(t) = F^\omega$ é uma extensão de Kummer de $\mathbb{F}_{q^2}(t)$ de grau $q+1$ (veja a Definição 1.3.23).



Pelo Teorema 1.3.24(ii), os únicos lugares que podem se ramificar em $F^{\omega}/\mathbb{F}_{q^2}(t)$ são o zero e o pólo de $t+2$ em $F_{q^2}(t)$.

Sejam P_{-2} e P_2 os zeros de $t+2$ e de $t-2$ em $\mathbb{F}_{q^2}(t)$, respectivamente. Sejam também $P_2^* \in \mathbb{P}_{F^{\omega}}$ e $P_{-2}^* \in \mathbb{P}_{F^{\omega}}$ zeros de $t-2$ e de $t+2$, respectivamente, em F^{ω} e P_{∞}^* um pólo de t em F^{ω}. Temos:

$$v_{P_{-2}^*}(t^2-4) = e(P_{-2}^*|P_{-2})v_{P_{-2}}(t^2-4) = q+1,$$

já que $e(P_{-2}^*|P_{-2}) = \frac{q+1}{mdc(q+1, v_{P_{-2}}(t+2))} = q+1$. Analogamente,

$$v_{P_{\infty}^*}(t^2-4) = e(P_{\infty}^*|P_{\infty})v_{\infty}(t^2-4) = \frac{q+1}{mdc\,(q+1, v_{P_{\infty}}(t+2))}.(-2) = -2(q+1) \text{ e}$$

$$v_{P_2^*}(t^2-4) = e(P_2^*|P_2)v_{P_2}(t^2-4) = 1, \text{ já que } e(P_2^*|P_2) = \frac{q+1}{mdc\,(q+1, v_{P_2}(t+2))} = 1.$$

Uma vez que $y^{q-1} - y^{-(q-1)} \in F \setminus F^{\omega}$ e $[F : F^{\omega}] = 2$, temos que $F = F^{\omega}(y^{q-1} - y^{-(q-1)})$ é uma extensão de Kummer de F^{ω} (veja o Exemplo 6 na Seção 1.3) e $(y^{q-1} - y^{-(q-1)})^2 = t^2 - 4 \in F^{\omega}$. Portanto, os únicos lugares que podem se ramificar em F/F^{ω} são os zeros e os pólos em F^{ω}, de $t+2$ e de $t-2$.

Sejam P_2^{**}, $P_{-2}^{**} \in \mathbb{P}_F$ tais que $P_2^{**}|P_2^*$ e $P_{-2}^{**}|P_{-2}^*$. Considere também $P_{\infty}^{**} \in \mathbb{P}_F$ acima de P_{∞}^*. Temos:

$$e(P_2^{**}|P_2^*) = \frac{2}{mdc\,(2, v_{P_2^*}(t^2-4))} = \frac{2}{mdc\,(2,1)} = \frac{2}{1} = 2. \qquad (1)$$

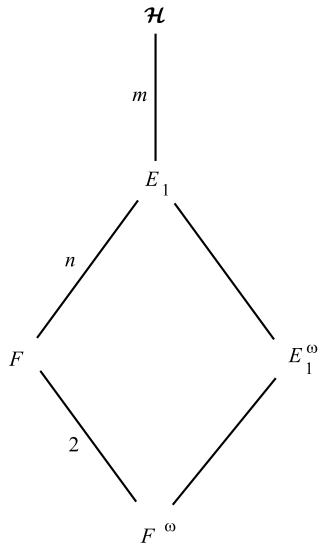
$$e(P_{\infty}^{**}|P_{\infty}^*) = \frac{2}{mdc\,(2, v_{P_{\infty}^*}(t^2-4))} = \frac{2}{mdc\,(2, -2(q+1))} = 1. \qquad (2)$$

$$e(P_{-2}^{**}|P_{-2}^{*}) = \frac{2}{mdc\,(2, v_{P_{-2}^{*}}(t^2-4))} = \frac{2}{mdc\,(2,\, q+1)} = 1. \qquad (3)$$

De (1), (2) e (3), concluímos que os únicos lugares que se ramificam em F/F^{ω} são os zeros de $t-2$ em F^{ω}. Fazendo-se $t=2$ em $\left(\frac{x^2}{y}\right)^{q+1} = t+2$ e considerando que $z^{q+1}=4$ possui $q+1$ raízes distintas , temos que há exatamente $q+1$ zeros de $t-2$ em $F^{\omega}/\mathbb{F}_{q^2}(t)$ (Teorema de Kummer) e o índice de ramificação de cada um deles nessa extensão é 1. Conseqüentemente, há exatamente $q+1$ zeros de $t-2$ em F^{ω} que se ramificam na extensão F/F^{ω}. ∎

Teorema 3.2.5. *Sejam m um divisor de $q-1$, E_1 o único corpo intermediário de $\mathcal{H}/F$ tal que $[\mathcal{H} : E_1] = m$ e ω um automorfismo de $\mathcal{H}/\mathbb{F}_{q^2}$ que satisfaz $\omega(x) = x/y$ e $\omega(y) = y^{-1}$. Existem exatamente $(q+1)$ lugares de E_1^{ω} que se ramificam na extensão E_1/E_1^{ω}. Eles são os zeros em E_1^{ω} (cada um deles simples) da função $y^m + y^{-m} - 2$.*

Demonstração. Considere o diagrama:



Vamos começar tratando o caso:

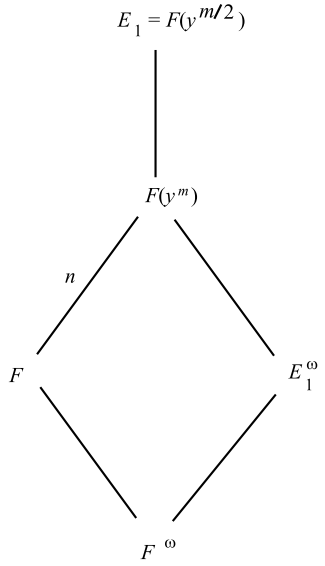
1) $\mathbf{n} := [\mathbf{E_1} : \mathbf{F}] = \frac{\mathbf{q-1}}{\mathbf{m}}$ é ímpar

Seja $u := y^m + y^{-m}$.

Afirmação 1: $E_1^{\omega} = F^{\omega}(u)$.

Demonstração: Como $\mathcal{H}/F$ é cíclica de grau $(q-1)$ e $\mathcal{H} = F(x)$, temos que $E_1 = F(x^m)$.

Além disso, $(x^m)^2 = y^m \cdot \alpha^m$, onde $\alpha = \frac{y^{q-1}+1}{x^{q-1}} \in F$, implica que $x^m = y^{m/2} \cdot \alpha^{m/2}$ ($m/2 \in \mathbb{N}$ pois n ímpar implica m par). Conseqüentemente, $E_1 = F(x^m) = F(y^{m/2})$ e, portanto, $y^m \in E_1$. Conseqüentemente $u \in E_1$ e como $\omega(u) = u$, temos que $u \in E_1^\omega$.



Resta-nos ainda mostrar que u gera E_1^ω na extensão $E_1^\omega | F^\omega$. Com efeito, $[E_1 : F(y^m)] \leq 2$ e divide $[E_1 : F] = n$; como n é ímpar, temos

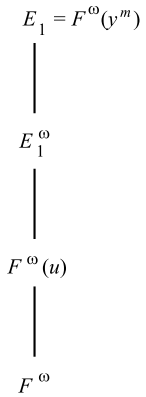
$$F(y^m) = F(y^{m/2}) = E_1.$$

Além disso, $y^{q-1} \in F^\omega(y^m)$ e $x^{q-1} = \frac{y^{q-1}+1}{x^2/y} \in \mathbb{F}_{q^2}(\frac{x^2}{y})(y^m) = F^\omega(y^m)$. Logo, $F \subset F^\omega(y^m)$. Conseqüentemente, $E_1 = F(y^m) \subset F^\omega(y^m)$ e concluímos que $E_1 = F^\omega(y^m)$.

Finalmente,

$$[E_1 : F^\omega(u)] = [F^\omega(y^m) : F^\omega(u)] = 2,$$

pois y^m é raiz de $p(T) = T^2 - T.u + 1$ e $y^m \notin F^\omega$.



Logo,

$$[E_1^{\omega} : F^{\omega}(u)] = \frac{[E_1 : F^{\omega}(u)]}{[E_1 : E_1^{\omega}]} = \frac{2}{2} = 1.$$

□

Assim, $\varphi_n(u) = y^{q-1} + y^{-(q-1)}$ é o polinômio mínimo de u sobre F^{ω}. Pelo Corolário 2.1.6(i),

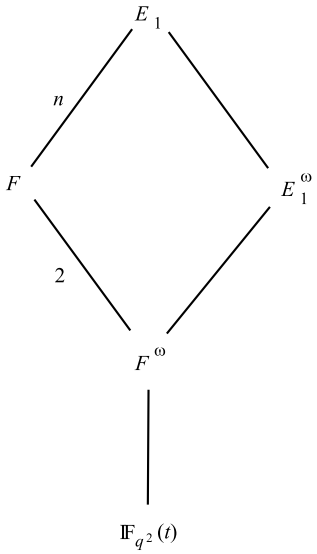
$$\varphi_n(u) - 2 = (u-2)[p_k(u)]^2, \quad k = \frac{n-1}{2}.$$

Logo,

$$y^{q-1} + y^{-(q-1)} - 2 = (u-2)[p_k(u)]^2 \qquad (*)$$

Por outro lado, o Corolário 2.1.6(iii) garante que $p_k(u)$ é separável em F^{ω} e que suas raízes pertencem a $\mathbb{F}_{q^2}$ e são diferentes de 2. Denotemos por $\beta_i \in \mathbb{F}_{q^2}$, $i = 1, 2, ..., \frac{n-1}{2}$, cada uma das $\frac{n-1}{2}$ raízes (distintas) de $p_k(u)$. Desse modo, fazendo-se $t = y^{q-1} + y^{-(q-1)}$, $(*)$ escreve-se como:

$$t - 2 = y^{q-1} + y^{-(q-1)} - 2 = (u-2)\prod_{i=1}^{\frac{n-1}{2}}(u-\beta_i)^2 \cdot \qquad (**)$$



Antes de determinarmos os lugares que se ramificam em E_1/E_1^{ω}, determinaremos quais os lugares que se ramificam em E_1/F^{ω}.

Note que como $[E_1 : F] = (q-1)/m = n$, $\theta^n - y^{q-1} \in \mathbb{F}_{q^2}[\theta]$ é o polinômio mínimo de y^m sobre F. Conseqüentemente, $y^{q-1} \neq r^d$ para todo $r \in F$ e $d > 1$ divisor de n.

Além disso, $mdc\,(n,p)=1$ e, portanto, a extensão de grau n E_1/F é de Kummer. Dessa forma, dado $P\in\mathbb{P}_F$ as possíveis ramificações de P em E_1/F ocorrem se P é um pólo ou um zero de y^{q-1} em F, ou seja, se P é um pólo de t. Por outro lado, o Lema 3.2.4 garante que somente os zeros de $t-2$ em F^ω ramificam-se em F/F^ω. Concluímos que os únicos lugares que podem se ramificar em E_1/F^ω são os zeros de $t-2$ e os pólos de t em F^ω.

Afirmação 2: Se $P\in\mathbb{P}_{F^\omega}$ é um zero de $t-2$ e se $P''\in\mathbb{P}_{E_1}$ está acima de P, então $e(P''|P)=2$.
Demonstração: Pelo Lema 3.2.4, há exatamente $(q+1)$ zeros de $t-2$ em F^ω que se ramificam (totalmente) em F/F^ω. Por outro lado, como tais zeros não se ramificam em E_1/F (pois só os pólos de t ramificam-se nesta extensão), seus índices de ramificação em E_1/F^ω são iguais a 2 (pela Proposição 1.3.5). □

Denotaremos por $P_1,P_2,\ldots,P_{q+1}$ os zeros de $t-2$ em F^ω. Se $P\in\mathbb{P}_{E_1^\omega}$ é um zero de $t-2$, obtemos que

$$0\ <v_P(t-2)=v_P((u-2)\prod_{i=0}^{\frac{n-1}{2}}(u-\beta_i)^2)$$

e, portanto, devemos ter $v_P(u-2)\ >0$ ou $v_P(\prod_{i=0}^{\frac{n-1}{2}}(u-\beta_i))\ >0$, ou seja, as extensões de P_j $(j=1,2,...,q+1)$ em E_1^ω, são exatamente os zeros de $u-2$ e de $u-\beta_i$ $(i=1,2,...,\frac{n-1}{2})$ em E_1^ω.

Por outro lado, se $P=P_{\beta_i}\in\mathbb{P}_{E_1^\omega}$ para algum $i\in\{1,2,\cdots,\frac{n-1}{2}\}$, temos que $v_{P_{\beta_i}}(u-\beta_j)=0$ se $j\neq i$ e $v_{P_{\beta_i}}(u-2)=0$. Conseqüentemente, $v_{P_{\beta_i}}(t-2)=2v_{P_{\beta_i}}(u-\beta_i)\ >0$ e temos que P_{β_i} é um zero de $t-2$ em E_1^ω. Analogamente, obtemos que P_{u-2} é um zero de $t-2$ em E_1^ω. Concluímos que $P\in\mathbb{P}_{E_1^\omega}$ é um zero de $t-2$ se, e somente se, $P=P_{u-2}$ ou $P=P_{\beta_i}$ para algum $i\in\{1,2,\cdots,\frac{n-1}{2}\}$.

Afirmação 3: Os zeros de $u-\beta_i$ não se ramificam em E_1/E_1^ω, $i=1,2,...,\frac{n-1}{2}$.
Demonstração: Seja $P_{\beta_i}\in\mathbb{P}_{E_1^\omega}$ um zero de $u-\beta_i$. Para $P_\lambda=P_{\beta_i}\cap F^\omega$, $\lambda\in\{1,\cdots,q+1\}$, temos:

$$e(P_{\beta_i}|P_\lambda)=e(P_{\beta_i}|P_\lambda)v_{P_\lambda}(t-2)=v_{P_{\beta_i}}(t-2)=2v_{P_{\beta_i}}(p_k(u))+v_{P_{\beta_i}}(u-2)=2v_{P_{\beta_i}}(u-\beta_i)\geq 2$$

Como o índice de ramificação de P_λ em E_1/F^ω é 2 (pela Afirmação **2**), concluímos que

$e(P_{\beta_i}|P_\lambda) = 2$. Conseqüentemente, P_{β_i} não se ramifica em E_1/E_1^ω. □

Sejam $P_{\beta_i} \in \mathbb{P}_{E_1^\omega}$, $i = 1, \cdots, \frac{n-1}{2}$, um zero de $u-\beta_i$ e $P_{u-2} \in \mathbb{P}_{E_1^\omega}$ um zero de $u-2$. Para cada P_j ($j = 1, 2, \cdots, q+1$), temos $(\varphi_n(u)-2-(t-2))(P_j) = (u-2)(P_j)\prod_{i=1}^{n-1}(u-\beta_i)^2(P_j)$. Logo, pelo Teorema de Kummer, há acima de P_j, em E_1^ω, pelo menos um zero de $u-\beta_i$, $i = 1, \cdots, \frac{n-1}{2}$ e um zero de $u-2$.

Fixe $P_j \in \mathbb{P}_{F^\omega}$, $j = 1, 2, \cdots, q+1$; podemos aplicar a Afirmação 3 e a Igualdade Fundamental à extensão E_1^ω/F^ω, obtendo:

$$n = \sum_{\substack{P|P_j \\ P\in E_1^\omega}} e(P|P_j)f(P|P_j) \geq \tfrac{n-1}{2}.2 + e(P_{u-2}|P_j)f(P_{u-2}|P_j) \qquad (***)$$

o que se verifica se, e somente se, $e(P_{u-2}|P_j) = f(P_{u-2}|P_j) = 1$. Conseqüentemente, $P_(u-2)$ deve ramificar-se totalmente em E_1/E_1^ω (Afirmação 2). Note que $(***)$ também implica que para cada $j \in \{1, 2, \cdots, q+1\}$ há apenas um zero de $u-2$ em E_1^ω acima de P_j. Portanto, há exatamente $q+1$ zeros de $u-2$ em E_1^ω os quais se ramificam em E_1/E_1^ω.

Como vimos no parágrafo anterior à Afirmação 2, somente os zeros de $t-2$ e os pólos de t podem se ramificar em E_1/F^ω e, conseqüentemente, em E_1/E_1^ω. Portanto, para finalizar a demonstração para o caso em que n é ímpar, resta-nos mostrar que os pólos de t não se ramificam em E_1/E_1^ω. Mas isso é imediato já que a extensão E_1/E_1^ω é galoisiana de grau 2 e, portanto, se os pólos de t se ramificassem em E_1/E_1^ω, ramificar-se-iam também em E_1/F (pela Proposição 1.3.5 e pelo Lema 3.2.4) e pela Igualdade Fundamental aplicada à extensão E_1/F, 2 teria que dividir n, o que seria uma contradição.

Concluímos que somente os $q+1$ zeros de $u-2$ em E_1^ω ramificam-se em E_1/E_1^ω.

2) $\mathbf{n = \frac{q-1}{m}}$ par

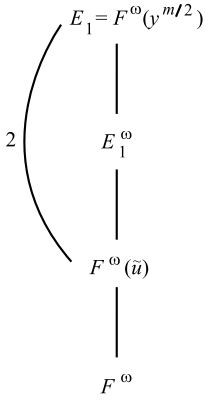
Há duas possibilidades há serem consideradas:

a) m é par

Nesse caso, temos ainda $E_1 = F(y^{m/2})$. Como $y^{q-1} \in F^\omega(y^{m/2})$ (já que $\frac{m}{2}$ divide $q-1$) e $x^{q-1} = \frac{y^{q-1}+1}{x^2/y} \in F^\omega(y^{m/2})$, temos que $F \subset F^\omega(y^{m/2})$. Conseqüentemente, $E_1 = F(y^{m/2}) \subset F^\omega(y^{m/2})$ e temos que $E_1 = F^\omega(y^{m/2})$.

Seja $\tilde{u} = y^{m/2} + y^{-m/2}$.

Note que $[E_1 : F^\omega(\tilde{u})] = [F^\omega(y^{m/2}) : F^\omega(\tilde{u})] = 2$ pois $y^{m/2}$ é raiz de $p(T) = T^2 - T.\tilde{u} + 1$ e $y^{m/2} \notin F^\omega$.



Portanto: $[E_1^\omega : F^\omega(\tilde{u})] = \frac{[E_1:F^\omega(\tilde{u})]}{[E_1:E_1^\omega]} = \frac{2}{2} = 1,$ ou seja, $E_1^\omega = F^\omega(\tilde{u})$.

Como $[E_1^\omega : F^\omega] = n$ e $y^{\frac{q-1}{2}} = x^{q-1}.\left(\frac{x^{q-1}}{y^{q-1}+1}\right)^{\frac{q-1}{2}} \in F^\omega$, temos que

$$\varphi_n(\tilde{u}) = \varphi_n(y^{m/2} + y^{-m/2}) = y^{(q-1)/2} + y^{-(q-1)/2} \in F^\omega$$

é o polinômio mínimo de $\tilde{u}$ sobre F^ω. Além disso, pelos ítens (i) e (ii) do Corolário 2.1.6

$$\varphi_n(\tilde{u}) - 2 = y^{(q-1)/2} + y^{-(q-1)/2} - 2 = (\tilde{u}^2 - 4)[f_k(\tilde{u})]^2\ , \quad k = \frac{n-2}{2},$$

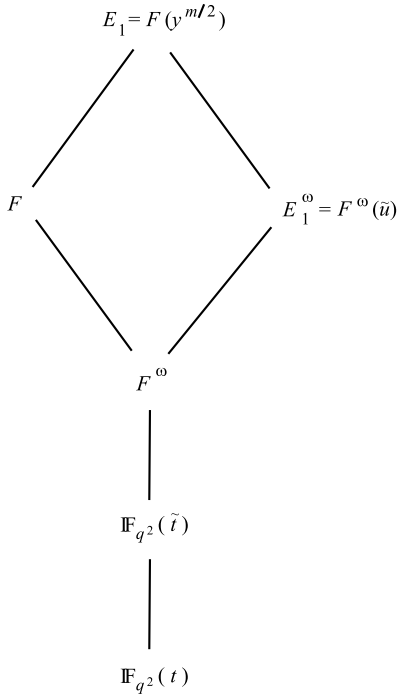
e 2 e -2 não são raízes do polinômio (separável e com raízes em $\mathbb{F}_{q^2}$) $f_k(\tilde{u})$. Logo, fazendo-se $\tilde{t} = \varphi_n(\tilde{u})$, obtemos:

$$\tilde{t} - 2 = (\tilde{u}^2 - 4)\prod_{i=1}^{\frac{n-2}{2}}(\tilde{u} - \beta_i)^2,\ \beta_i \in \mathbb{F}_{q^2} \text{ distintas.} \qquad (****)$$

Note que

$$\tilde{t}^2 = [\varphi_n(\tilde{u})]^2 = y^{q-1} + y^{-(q-1)} + 2 = t + 2.$$

Conseqüentemente, $t - 2 = \tilde{t}^2 - 4 = (\tilde{t} + 2)(\tilde{t} - 2)$. Pelo Teorema de Kummer (Teorema 1.3.12), há exatamente dois lugares em $\mathbb{F}_{q^2}(\tilde{t})$ acima do zero de $t-2$ (que não se ramificam em $\mathbb{F}_{q^2}(\tilde{t})/\mathbb{F}_{q^2}(t)$) em $\mathbb{F}_{q^2}(\tilde{t})$: o zero de $\tilde{t} + 2$ e o zero de $\tilde{t} - 2$. Vamos denotar por P_2' o zero de $\tilde{t} - 2$ e por P_{-2}', o zero de $\tilde{t} + 2$, ambos em $\mathbb{P}_{\mathbb{F}_{q^2}(\tilde{t})}$.



Nota 1: Como $E_1 = F(y^{m/2})$, temos, de modo análogo ao que foi visto no caso n ímpar, que os únicos lugares de F^{ω} que podem se ramificar em E_1/F^{ω} são os zeros de $t-2$ e os pólos de t. Além disso, como antes, os índices de ramificação em E_1/F^{ω} dos zeros de $t-2$ em F^{ω} são exatamente 2. Novamente, denotaremos por P_j, $j = 1, 2, \cdots, q+1$, os zeros de $t-2$ em F^{ω}.

Os zeros de $t-2$ em F^{ω} são extensões dos zeros de $\tilde{t}-2$ e de $\tilde{t}+2$ em $F^{\omega}/\mathbb{F}_{q^2}(\tilde{t})$. Basta-nos, portanto, analisar as extensões destes em E_1/F^{ω}.

Primeiramente, analisemos as extensões de P_2' em E_1/F^{ω}.

Como

$$\tilde{t}-2 = (\tilde{u}^2-4)[f_k(\tilde{u})]^2 = (\tilde{u}^2-4)\prod_{i=1}^{(n-2)/2}(\tilde{u}-\beta_i)^2\,,$$

temos, analogamente ao caso n ímpar, que as extensões de P_2' em E_1^{ω}/F^{ω} são exatamente os zeros, em E_1^{ω}, de $\tilde{u}-2$, de $\tilde{u}+2$ e de $\tilde{u}-\beta_i$ $(i = 1, 2, \cdots, \frac{n-2}{2})$. Logo, se Q_2 é um zero de $\tilde{t}-2$ em F^{ω}, há, em E_1^{ω}, pelo menos: $\frac{n-2}{2}$ zeros de $f_k(\tilde{u})$ acima de Q_2, um zero de $\tilde{u}-2$ acima de Q_2 e um zero de $\tilde{u}+2$ acima de Q_2.

Afirmação 4: Seja P_{β_i} um zero de $\tilde{u} - \beta_i$ em E_1^ω, $i \in \{1, \cdots, \frac{n-2}{2}\}$. Para cada i, P_{β_i} ramifica-se totalmente em E_1^ω/F^ω.
Demonstração: De fato, dado $i \in \{1, 2, \cdots, \frac{n-2}{2}\}$, temos:

$$e(P_{\beta_i}|P_2') = e(P_{\beta_i}|P_2')v_{P_2'}(\tilde{t}-2) = v_{P_{\beta_i}}(\tilde{t}-2) = 2v_{P_{\beta_i}}(\tilde{u}-\beta_i) \geq 2.$$

Conseqüentemente, para $P_\lambda := P_{\beta_i} \cap F^\omega$, temos que $2 \leq e(P_{\beta_i}|P_2') = e(P_{\beta_i}|P_\lambda).e(P_\lambda|P_2') = e(P_{\beta_i}|P_\lambda) \leq 2$. Logo, P_λ ramifica-se totalmente em E_1^ω/F^ω e, portanto, P_{β_i} não se ramifica em E_1/E_1^ω. □

Nota 2: Sejam $P_{\tilde{u}+2}$ e $P_{\tilde{u}-2}$ zeros, em E_1^ω, de $\tilde{u}+2$ e de $\tilde{u}-2$, respectivamente, e seja $Q_2 \in \mathbb{P}_{F^\omega}$ um zero de $\tilde{t}-2$ abaixo deles. Pela Igualdade Fundamental aplicada à extensão E_1^ω/F^ω, temos:

$$n = \sum_{\substack{P|Q_2 \\ P \in E_1^\omega}} e(P|Q_2)f(P|Q_2) \geq \frac{n-2}{2}.2 + e(P_{\tilde{u}-2}|Q_2)f(P_{\tilde{u}-2}|Q_2) + e(P_{\tilde{u}+2}|Q_2)f(P_{\tilde{u}+2}|Q_2),$$

o que implica que $e(P_{\tilde{u}-2}|Q_2) = f(P_{\tilde{u}-2}|Q_2) = e(P_{\tilde{u}+2}|Q_2) = f(P_{\tilde{u}+2}|Q_2) = 1$. Em particular, para cada zero de $\tilde{t}-2$ em F^ω, há em E_1^ω um único zero de $\tilde{u}-2$ e um único zero de $\tilde{u}+2$ acima dele. Como os zeros de $\tilde{t}-2$ em F^ω são zeros de $t-2$ em F^ω, temos que os zeros de $\tilde{u}+2$ e de $\tilde{u}-2$ em E_1^ω ramificam-se totalmente em E_1/E_1^ω.

Afirmação 5: Há $q+1$ zeros de $\tilde{u}^2-4$ em E_1^ω.
Demonstração: De fato, o Lema 3.2.4 garante que há exatamente $q+1$ zeros de $t-2$ em F^ω. Destes, $\frac{q+1}{2}$ estão acima de P_{-2}' e $\frac{q+1}{2}$, de P_2'. De fato, $F^\omega/\mathbb{F}_{q^2}(\tilde{t})$ é de Kummer de grau $\frac{q+1}{2}$; em particular, galoisiana, e portanto, há $(q+1)/2$ automorfismos de $F^\omega/\mathbb{F}_{q^2}(\tilde{t})$. Portanto, se $\tilde{P} \in \mathbb{P}_{F^\omega}$ e $\tilde{P}|P_2'$, para cada $\sigma \in Aut_{\mathbb{F}_{q^2}(\tilde{t})}F^\omega$ temos $\sigma(\tilde{P})|P_2'$ e estes são todos os lugares de F^ω acima de P_2'. Analogamente, para P_{-2}'. Como a soma dos lugares acima de P_2' e de P_{-2}' em F^ω é $q+1$ (pois $\tilde{t}^2-4 = t-2$), temos que exatamente $\frac{q+1}{2}$ estão acima de P_2' e exatamente $\frac{q+1}{2}$, de P_{-2}'. Fixe um dos $(q+1)/2$ lugares acima de P_2'. Como acima dele há, em E_1^ω, um único zero de $\tilde{u}-2$ e um único zero de $\tilde{u}+2$ (Nota 2), temos concluída nossa Afirmação. □

Agora vamos analisar as extensões de $\tilde{t}+2$ em E_1/F^ω.

Como n é par, temos que $\tilde{t}+2=[\varphi_{n/2}(\tilde{u})]^2=\prod_{i=1}^{n/2}(\tilde{u}-\alpha_i)^2$, $\alpha_i\in\mathbb{F}_{q^2}$ distintas (veja Corolário 2.1.6(i)). Seja P_{α_i} um zero de $\tilde{u}-\alpha_i$ em E_1^{ω}, $i=1,2,\cdots,\frac{n}{2}$. Para cada i, temos:

$$2\geq e(P_{\alpha_i}|P'_{-2})=e(P_{\alpha_i}|P'_{-2})v_{P'_{-2}}(\tilde{t}+2)=v_{P_{\alpha_i}}(\tilde{t}+2)=2v_{P_{\alpha_i}}(\varphi_{n/2}(\tilde{u}))\geq 2.$$

Portanto, P'_{-2} ramifica-se totalmente em E_1^{ω}/F^{ω} e, conseqüentemente, não se ramifica em E_1/E_1^{ω}.

Logo, dos zeros de $t-2$ em E_1^{ω}, somente os zeros de $\tilde{t}-2$ em E_1^{ω} ramificam-se em E_1/E_1^{ω}, a saber: os $\frac{q+1}{2}$ zeros de $\tilde{u}-2$ e os $\frac{q+1}{2}$ zeros de $\tilde{u}+2$, ou seja, os $q+1$ zeros (em E_1^{ω}) de $\tilde{u}^2-4=\left(y^{m/2}+y^{-m/2}\right)^2-4=y^m+y^{-m}-2$.

Para terminar a demonstração desse caso, resta-nos mostrar que:

Afirmação 6: Se P um pólo de t em E_1^{ω}, então P não se ramifica em E_1/E_1^{ω}.
Demonstração: Como $[E_1:E_1^{\omega}]=2$, E_1/E_1^{ω} é de Kummer. Em particular, tal extensão é galoisiana. Assim, para provarmos a Afirmação acima, é suficiente mostrarmos que há dois lugares em E_1 acima de P. Seja $\tilde{P}\in\mathbb{P}_{E_1}$ acima de P, então $\omega(\tilde{P})\in\mathbb{P}_{E_1}$ também está acima de P. Suponhamos, por absurdo, que $\omega(\tilde{P})=\tilde{P}$. Temos:

$$v_{\tilde{P}}(y^m)=v_{\omega(\tilde{P})}(y^m)=v_{\tilde{P}}(\omega^{-1}(y^m))=v_{\tilde{P}}(\tfrac{1}{y^m})$$

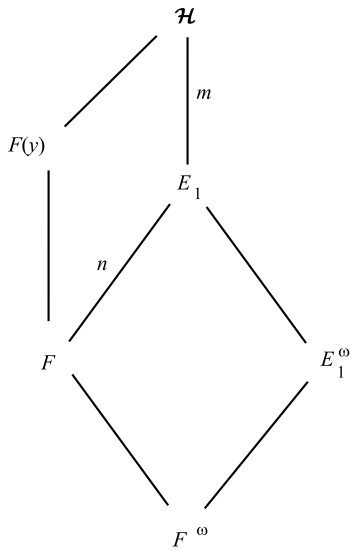
donde se conclui que $v_{\tilde{P}}(y^m)=0$. Conseqüentemente, $0=nv_{\tilde{P}}(y^m)=v_{\tilde{P}}(y^{q-1})$, o que é absurdo, já que $\tilde{P}$ é um pólo de $t=y^{q-1}+y^{-q-1}$. □

Finalmente, analisaremos o caso:

b) m é ímpar

Para resolver esse caso, usaremos o resultado anterior para $\tilde{m}=2m$, como veremos a seguir.

Como m é ímpar, $E_1\not\subset F(y)$, pois $[\mathcal{H}:F(y)]=2$ e 2 não divide m. Logo, $E_1\neq F(y^j)$ para todo $j\in\mathbb{N}$. No entanto, é sempre verdade que $E_1=F(x^m)$.

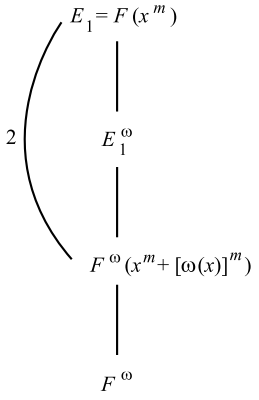


Afirmação 7: $E_1^{\omega} = F^{\omega}(x^m + [\omega(x)]^m)$.

Demonstração: Como $[\omega(x)]^m = (\frac{x}{y})^m = \frac{(y^{q-1}+1)^m}{(x^m)^q} \in F(x^m) = E_1$, temos que $x^m + [\omega(x)]^m \in E_1$. Além disso, $o(\omega) = 2$ e, portanto, $\omega(x^m + [\omega(x)]^m) = [\omega(x)]^m + x^m$ e temos que $x^m + [\omega(x)]^m \in E_1^{\omega}$.

Como x^m é raiz do polinômio $f(T) = T^2 - (x^m + [\omega(x)]^m)T + (\frac{x^2}{y})^m \in F^{\omega}(x^m + [\omega(x)]^m)[T]$ e não é fixo por ω, temos que $x^m \notin F^{\omega}(x^m + [\omega(x)]^m)$. Logo, $[F(x^m) : F^{\omega}(x^m + [\omega(x)]^m)] = 2$ e

$$[E_1^{\omega} : F^{\omega}(x^m + [\omega(x)]^m)] = \frac{[F(x^m):F^{\omega}(x^m+[\omega(x)]^m)]}{[E_1:E_1^{\omega}]} = \frac{2}{2} = 1.$$



□

Seja $\alpha \in Aut_{\mathbb{F}_{q^2}}\mathcal{H}$ o automorfismo de ordem 2 tal que $\alpha(x) = -x$ e $\alpha(y) = y$. Como $\mathcal{H}/F$ é cíclica, tal extensão contém um único corpo intermediario L tal que $[\mathcal{H} : L] = 2$. Logo, $L = \mathcal{H}^\alpha$. Desse modo, como $[\mathcal{H} : F(y)] = 2$, temos que $\mathcal{H}^\alpha = F(y)$.

Antes de examinarmos os lugares que se ramificam em E_1/E_1^ω, analisaremos as extensões $E_1^\alpha/E_1^{\alpha,\omega}$ e $E_1^\omega/E_1^{\alpha,\omega}$. A esta última extensão aplicaremos o resultado já obtido no item (a) do caso 2.

Afirmação 8: $E_1^\alpha = F(y^m)$.

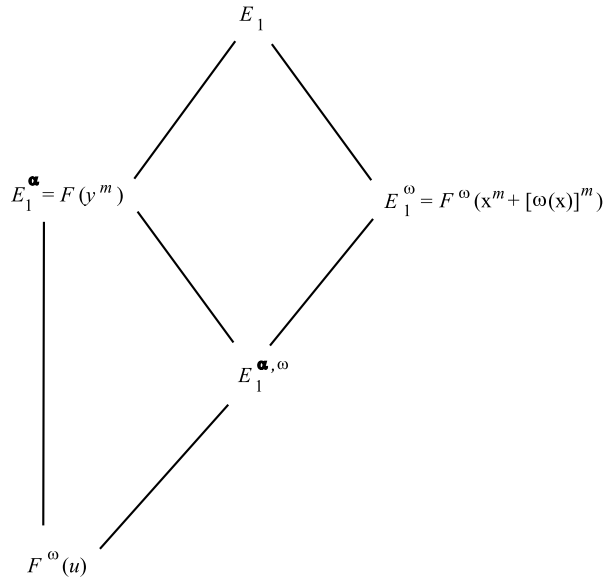
Demonstração: De fato, $[E_1 : E_1^\alpha] = 2$ e $y^m \in E_1^\alpha$ implicam que $F(y^m) \subset E_1^\alpha$. Além disso,

$$(x^m)^2 = y^m\left[\frac{y^{q-1}+1}{x^{q-1}}\right]^m \in F(y^m) \text{ e, portanto , } [E_1 : F(y^m)] \leq 2.$$

Como $x^m \notin E_1^\alpha$ (pois m é ímpar), temos que $x^m \notin F(y^m)$ e $[E_1 : F(y^m)] = 2$. Logo, $[E_1^\alpha : F(y^m)] = \frac{[E_1:F(y^m)]}{[E_1:E_1^\alpha]} = 1$. □

Afirmação 9: $E_1^{\alpha,\omega} = F^\omega(u)$, onde $u = y^m + y^{-m}$.

Demonstração: $F^\omega(u) = F^\omega(y^m + y^{-m}) \subset F^\omega(y^m) \subset F(y^m) = E_1^\alpha$ e como $\omega(u) = u$, temos que $F^\omega(u) \subset E_1^{\alpha,\omega}$.



Por outro lado, $\{x^m + [\omega(x)]^m\}^2 = (\frac{x^2}{y})^m(u+2) \in F^\omega(u)$ e temos $[F^\omega(x^m + [\omega(x)]^m) : F^\omega(u)] = [E_1^\omega : F^\omega(u)] \leq 2$. Conseqüentemente,

$$1 \leq [E_1^{\alpha,\omega} : F^\omega(u)] = \frac{[E_1^\omega : F^\omega(u)]}{[E_1^\omega : E_1^{\alpha,\omega}]} \leq \frac{2}{2} = 1.$$

□

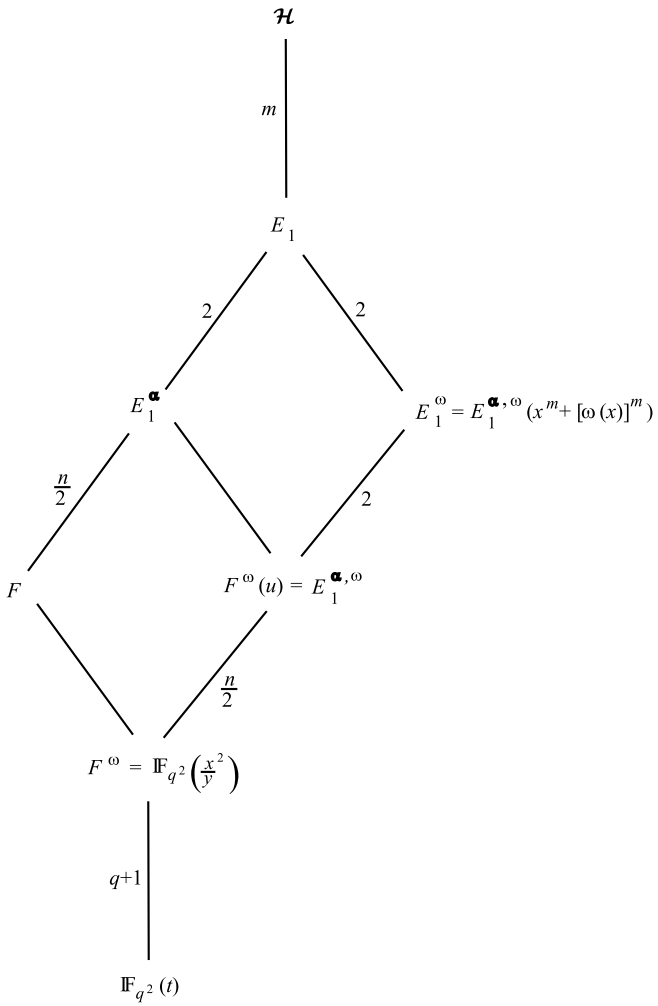
Analisaremos os lugares que se ramificam em E_1/E_1^ω da seguinte forma:

1. Determinaremos os lugares de $E_1^{\alpha,\omega}$ que se ramificam em $E_1^\omega/E_1^{\alpha,\omega}$;
2. Determinaremos os lugares de $E_1^{\alpha,\omega}$ que se ramificam em $E_1^\alpha/E_1^{\alpha,\omega}$;
3. Determinaremos os lugares de $E_1^{\alpha,\omega}$ que se ramificam em $E_1/E_1^{\alpha,\omega}$;
4. Compararemos os índices de ramificação dos lugares obtidos no item 3 nas extensões $E_1/E_1^{\alpha,\omega}$, $E_1^\alpha/E_1^{\alpha,\omega}$ e $E_1^\omega/E_1^{\alpha,\omega}$.

As afirmações 7 e 9 implicam que

$$E_1^\omega \supset E_1^{\alpha,\omega}(x^m + [\omega(x)]^m) \supset F^\omega(x^m + [\omega(x)]^m) = E_1^\omega$$

Desse modo, $E_1^\omega = E_1^{\alpha,\omega}(x^m + [\omega(x)]^m)$ e como $\alpha(x^m + [\omega(x)]^m) = -(x^m + [\omega(x)]^m)$, temos que $x^m + [\omega(x)]^m \notin E_1^{\alpha,\omega}$. Além disso, temos que $\{x^m + [\omega(x)]^m\}^2 = (\frac{x^2}{y})^m(u+2) \in E_1^{\alpha,\omega}$ e, portanto, a extensão $E_1^\omega/E_1^{\alpha,\omega}$ tem grau 2 e a equação anterior é o polinômio mínimo de $(x^m + [\omega(x)]^m)$ sobre $E_1^{\alpha,\omega}$. Conseqüentemente, tal extensão é uma extensão de Kummer.



Deste modo, os únicos lugares de $E_1^{\alpha,\omega}$ que podem se ramificar em $E_1^{\omega}/E_1^{\alpha,\omega}$ são os zeros ou pólos de $(\frac{x^2}{y})$ e os zeros ou pólos de $(u+2)$. Como $(\frac{x^2}{y})^{q+1} = t+2$, onde $t = y^{q-1} + y^{-(q-1)}$, os zeros de $(\frac{x^2}{y})$ nos corpos intermediários de E_1/F^{ω} são os zeros de $t+2$ nesses mesmos corpos. Analogamente, os pólos de x^2/y em tais corpos são os pólos de t neles. Notemos também que se $\tilde{P}$ é um pólo de $u+2$ em $E_1^{\alpha,\omega}$, então $\tilde{P}$ é pólo de t nesse corpo.

Afirmação 10: Os zeros de $\frac{x^2}{y}$ em $E_1^{\alpha,\omega}$ ramificam-se (em particular, ramificam-se totalmente) em $E_1^{\omega}/E_1^{\alpha,\omega}$.

Demonstração: Seja P um zero de $\frac{x^2}{y}$ em $E_1^{\alpha,\omega}$. Como P é também um zero de $t+2$ em $E_1^{\alpha,\omega}$, denotá-lo-emos por $P_{-2}^{**} \in \mathbb{P}_{E_1^{\alpha,\omega}}$. Consideremos também um lugar $P_{-2}^{***} \in E_1^{\omega}$ tal

que $P_{-2}^{**} = P_{-2}^{***} \cap E_1^{\alpha,\omega}$, $P_{-2}^{*} = P_{-2}^{**} \cap F^{\omega}$ um zero de $t+2$ em F^{ω} e P_{-2} o zero de $t+2$ em $F_{q^2}(t)$. Temos:

$$(q+1)v_{P_{-2}^*}(\tfrac{x^2}{y}) = v_{P_{-2}^*}(t+2) = e(P_{-2}^*|P_{-2})v_{P_{-2}}(t+2) = q+1$$

(pois $e(P_{-2}^*|P_{-2}) = \frac{q+1}{mdc\,(q+1, v_{P_{-2}}(t+2))} = q+1$) e, conseqüentemente, $v_{P_{-2}^*}(\frac{x^2}{y}) = 1$.

Além disso, $\left(\frac{x^2}{y}\right)^{\frac{q+1}{2}} = \frac{x^{q+1}}{y^{\frac{q+1}{2}}} = y^{\frac{q-1}{2}} + y^{\frac{-(q-1)}{2}} = \varphi_{\frac{n}{2}}(u) \iff x^{q+1} = y^q + y$. Como $\varphi_{\frac{n}{2}}(u)$ é separável e suas raízes pertencem a $\mathbb{F}_{q^2}(t)$, o Teorema de Kummer garante que existem exatamente $\frac{n}{2}$ zeros de $\frac{x^2}{y}$ em $E_1^{\alpha,\omega} = F^{\omega}(u)$ acima de $P_{-2}^* \in F^{\omega}$ e seus índices de ramificação em $E_1^{\alpha,\omega}/F^{\omega}$ são iguais a 1. Conseqüentemente, temos $e(P_{-2}^{**}|P_{-2}^*) = 1$.

Finalmente, temos:

$$2v_{P_{-2}^{***}}(x^m + [w(x)]^m) = me(P_{-2}^{***}|P_{-2}^{**})v_{P_{-2}^{**}}(\frac{x^2}{y}) + v_{P_{-2}^{***}}(u+2) =$$

$$= me(P_{-2}^{***}|P_{-2}^{**})e(P_{-2}^{**}|P_{-2}^{*})v_{P_{-2}^*}(\frac{x^2}{y}) = me(P_{-2}^{***}|P_{-2}^{**})$$

e como m é ímpar, devemos ter $e(P_{-2}^{***}|P_{-2}^{**}) = 2$ (note que $v_{P_{-2}^{***}}(u+2) = 0$, já que $u+2$ divide $\varphi_n(u) - 2 = t - 2$ (Corolário 2.1.6(i)). □

Para os zeros de $u+2$ em $E_1^{\alpha,\omega}$ vale o seguinte:

Afirmação 11: Os zeros de $u+2$ ramificam-se (em particular, ramificam-se totalmente) em $E_1^{\omega}/E_1^{\alpha,\omega}$.

Demonstração: Sabemos que $t-2 = \varphi_n(u) - 2 = (u^2-4)\prod_{i=1}^{\frac{n-2}{2}}(u-\beta_i)^2$, $\beta_i \in \mathbb{F}_{q^2}$. De modo análogo ao item (a), temos:

- As extensões de P_j (zeros de $t-2$ em F^{ω}), $j \in \{1, \cdots, q+1\}$, em $E_1^{\alpha,\omega}$ são os zeros de $u-\beta_i$ em $E_1^{\alpha,\omega}$ ($i = 1, \cdots, \frac{n-2}{2}$), os zeros de $u-2$ em $E_1^{\alpha,\omega}$ e os zeros de $u+2$ em $E_1^{\alpha,\omega}$.

- Para cada P_j, há acima dele, em $E_1^{\alpha,\omega}$, pelo menos: um zero de $u-\beta_i$ ($i = 1, \cdots, \frac{n-2}{2}$), um zero de $u+2$ e um zero de $u-2$.

- Fixado j, considere P_{β_i} um zero de $u-\beta_i$ em $E_1^{\alpha,\omega}$, $i \in \{1, \cdots, \frac{n-2}{2}\}$, P_{u+2} um zero de $u+2$ em $E_1^{\alpha,\omega}$ e P_{u-2} um zero de $u-2$ em $E_1^{\alpha,\omega}$ lugares acima de P_j.

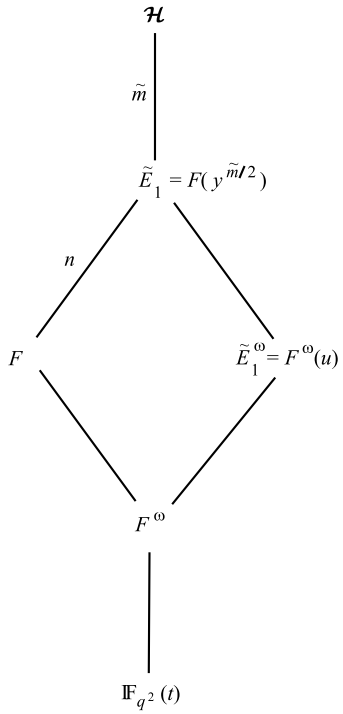
Temos $e(P_{\beta_i}|P_j) = 2$ e $f(P_{u-2}|P_j) = e(P_{u-2}|P_j) = e(P_{u+2}|P_j) = f(P_{u+2}|P_j) = 1$.

Conseqüentemente, $1 = e(P_{u+2}|P_j) = e(P_{u+2}|P_j)v_{P_j}(t-2) = v_{P_{u+2}}(u+2)$. Logo, para $P'_{u+2} \in \mathbb{P}_{E_1^\omega}$ zero de $u+2$ em E_1^ω, temos: $e(P'_{u+2}|P_{u+2}) = \frac{2}{mdc(2, v_{P_{u+2}}(u+2))} = 2$.

Nota 3: Para terminar o estudo dos lugares que se ramificam em $E_1^\omega/E_1^{\alpha,\omega}$ a fim de determinarmos os lugares de E_1^ω que se ramificam em E_1/E_1^ω, falta verificar se os pólos de t em $E_1^{\alpha,\omega}$ se ramificam nesta extensão. No entanto, isso será omitido — mostraremos diretamente, ao final dessa demonstração, que os pólos de t em E_1^ω não se ramificam em E_1/E_1^ω, sem analisar as extensões $E_1^\omega/E_1^{\alpha,\omega}$ e $E_1^\alpha/E_1^{\alpha,\omega}$.

Agora analisemos a extensão $E_1^\alpha/E_1^{\alpha,\omega}$.

Afirmação 12: Há, em $E_1^{\alpha,\omega}$, exatamente $\frac{q+1}{2}$ zeros de $u+2$ e exatamente $\frac{q+1}{2}$ zeros de $u-2$ que se ramificam na extensão $E_1^\alpha/E_1^{\alpha,\omega}$.
Demonstração: Fazendo-se $\tilde{m} = 2m$ e $\tilde{E}_1 = E_1^\alpha$, temos $u = y^{\frac{\tilde{m}}{2}} + y^{-\frac{\tilde{m}}{2}}$.



Pelo item (a), há exatamente $\frac{q+1}{2}$ zeros de $u+2$ e exatamente $\frac{q+1}{2}$ zeros de $u-2$,

ambos em $\tilde{E}_1^{\omega}$, que se ramificam na extensão $\tilde{E}_1/\tilde{E}_1^{\omega}$. Como os $\frac{q+1}{2}$ zeros de $u-2$ em $\tilde{E}_1^{\omega}$ não se ramificam em $E_1^{\omega}/\tilde{E}_1^{\omega}$ e seus graus relativos nessa extensão são iguais a 1 (veja Nota abaixo), temos que há $2.\frac{q+1}{2}$ zeros de $u-2$ em E_1^{ω} que se ramificam em E_1/E_1^{ω}. □

Nota 4: Em primeiro lugar, como $(\frac{x^2}{y})^{q+1}-4 = t-2 = (u^2-4)\prod_{i=1}^{\frac{n-2}{2}}(u-\beta_i)^2$, temos que qualquer zero Q de $u-2$ em $\tilde{E}_1^{\omega}$ está acima do zero de $(\frac{x^2}{y})^{q+1}-4$ em F^{ω} e, conseqüentemente, de $\frac{x^2}{y}-\beta$, para algum $\beta \in \mathbb{F}_{q^2}$ satisfazendo $\beta^{q+1}=4$. Logo, $(x^m+[\omega(x)]^m)^2 = 4\beta^m \ (modQ)$ e como $z^2 = 4\beta^m$ tem duas raízes distintas em $\mathbb{F}_{q^2}$, o Teorema de Kummer garante que há exatamente dois lugares em E_1^{ω} acima de Q (lembre-se de que $E_1^{\omega} = \tilde{E}_1^{\omega}(x^m+[\omega(x)]^m)$ e, portanto, podemos aplicar o Teorema de Kummer a essa extensão).

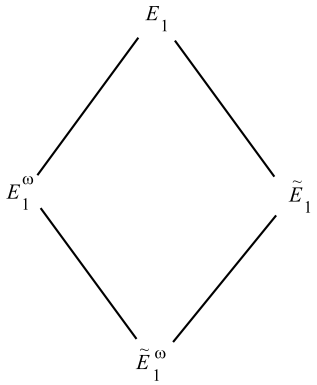
Finalmente, analisemos a extensão $E_1/E_1^{\alpha,\omega}$, ou seja, a extensão $E_1/\tilde{E}_1^{\omega}$.

Afirmação 13: Os únicos lugares de $\tilde{E}_1$ que podem se ramificar em $E_1/\tilde{E}_1$ são os zeros de $\frac{x^2}{y}$ e os pólos de t.
Demonstração: De fato, $E_1 = F(x^m)$, $\tilde{E}_1 = F(y^m)$ e como

$$(x^m)^2 = y^m\left(\frac{x^2}{y}\right)^m,$$

os únicos lugares de $\tilde{E}_1$ que podem se ramificar na extensão de Kummer $E_1/\tilde{E}_1$ são os zeros de $\frac{x^2}{y}$ e de y^m ou os pólos dessas funções. Como os zeros e os pólos de y^m são pólos de t e o mesmo vale para os pólos de $\frac{x^2}{y}$, a afirmativa está provada. □

Logo, pelas Afirmações 12 e 13, os únicos lugares de $\tilde{E}_1^{\omega}$ que podem se ramificar em $E_1/\tilde{E}_1^{\omega}$ são os zeros de $u-2$, de $u+2$, de $\frac{x^2}{y}$ e os pólos de t.



Para finalizarmos a demonstração de nosso Teorema, basta mostrarmos que:

- Os $\frac{q+1}{2}$ zeros de $u+2$ em $\tilde{E}_1$ não se ramificam em $E_1/\tilde{E}_1$ (com efeito, mostrando-se isso, as Afirmações 11 e 12 implicarão que os zeros de $u+2$ não se ramificam em E_1/E_1^{ω});
- Os zeros de $\frac{x^2}{y}$ em $\tilde{E}_1^{\omega}$ não se ramificam na extensão E_1/E_1^{ω};
- Os pólos de t em E_1^{ω} não se ramificam em E_1/E_1^{ω}.

Com efeito, se provarmos os três ítens anteriores, provaremos nosso Teorema para o caso em que m é ímpar, já que há $(q+1)$ zeros de $u-2$ em E_1^{ω} que se ramificam na extensão E_1/E_1^{ω} (conforme o final da demonstração da Afirmação 12).

Afirmação 14: Com as notações anteriores, temos:

(i) Os $\frac{q+1}{2}$ zeros de $u+2$ em $\tilde{E}_1$ não se ramificam em $E_1/\tilde{E}_1$;

(ii) Os zeros de $\frac{x^2}{y}$ em $\tilde{E}_1^{\omega}$ não se ramificam na extensão E_1/E_1^{ω};

(iii) Os pólos de t em E_1^{ω} não se ramificam em E_1/E_1^{ω}.

Demonstração: (i) Como os zeros de $u+2$ em $\tilde{E}_1$ estão acima do zero de $t-2$ em $\mathbb{F}_{q^2}(t)$, eles não podem estar acima de pólos de t e nem mesmo dos zeros de $\frac{x^2}{y}$ em F^{ω}, já que esses últimos são extensões do zero de $t+2$ em $\mathbb{F}_{q^2}(t)$. Portanto, de acordo com a Afirmação 13, os zeros de $u+2$ em $\tilde{E}_1$ não podem se ramificar na extensão $E_1/\tilde{E}_1^{\omega}$.

(ii) Decorre imediatamente das Afirmações 10 e 12.

(iii) Sabemos que $E_1 = F(x^m)$ e que se P é um pólo de t em E_1^{ω} e $P' \in \mathbb{P}_{E_1}$ está acima

de P, então $\omega(P')$ também está acima de P e

$$v_{\omega(P')}(x^m) = v_{P'}(\omega^{-1}(x^m)) = v_{P'}\left(\frac{x^m}{y^m}\right).$$

Logo, se $\omega(P') = P'$, temos que $v_{P'}(x^m) = v_{\omega(P')}(x^m) = v_{P'}(x^m) - v_{P'}(y^m)$ e conseqüentemente, $v_{P'}(y^m) = 0$. Um absurdo. Concluímos que $\omega(P') \neq P'$. Como $[E_1 : E_1^\omega] = 2$, temos que $e(P'|P) = e(\omega(P')|P) = 1$. □

Provamos então que há exatamente $(q+1)$ lugares que se ramificam em E_1/E_1^ω e são justamente os zeros, em E_1^ω, da função $u - 2 = y^m + y^{-m} - 2$.

∎

Visto que o gênero $g(E_1)$ de $E_1/\mathbb{F}_{q^2}$ depende dos lugares que se ramificam na extensão E_1/E_1^ω e do gênero de $E_1^\omega/\mathbb{F}_{q^2}$, concluímos que o Teorema 3.2.5 é útil para a determinação de $g(E_1)$.

O Corolário seguinte generaliza a Nota 4.4 de [G-S].

Corolário 3.2.6. *Com as notações do Teorema anterior, temos:*

(i) se n é ímpar, então $E_1^\omega = \mathbb{F}_{q^2}(u, v)$ onde

$$v^{q+1} = \varphi_n(u) + 2$$

é uma equação irredutível.

(ii) se n e m são pares, então $E_1^\omega = \mathbb{F}_{q^2}(\tilde{u}, v)$ onde

$$v^{\frac{q+1}{2}} = \varphi_n(\tilde{u})$$

é uma equação irredutível.

(iii) Se n é par e m é ímpar, $E_1^\omega = \mathbb{F}_{q^2}(\tilde{l}, v)$ onde

$$v^{\frac{q+1}{2}} = \varphi_{\frac{n}{2}}(v\tilde{l}^2 - 2)$$

é uma equação irredutível.

Demonstração. Considere $v = \frac{x^2}{y}$ e $u = y^m + y^{-m}$.

(i) A demonstração segue imediatamente da prova do Teorema 3.2.5.

(*ii*) Seja $\tilde{u} = y^{\frac{m}{2}} + y^{-\frac{m}{2}}$. Pelo Teorema 3.2.5, temos que $E_1^\omega = F^\omega(\tilde{u})$ e $v^{\frac{q+1}{2}} = \frac{x^{q+1}}{y^{\frac{q+1}{2}}} = y^{\frac{q-1}{2}} + y^{-\frac{q-1}{2}} = \varphi_n(\tilde{u})$.

(*iii*) Seja $\tilde{l} = \frac{l}{v^{\frac{m+1}{2}}}$, onde $l = x^m + [\omega(x)]^m$. Pelo Teorema 3.2.5, temos que $E_1^\omega = F^\omega(l) = \mathbb{F}_{q^2}(v)(l) = \mathbb{F}_{q^2}(\tilde{l}, v)$ e $v\tilde{l}^2 = \frac{l^2}{v^m} = u + 2$. Conseqüentemente, $v^{q+1} = \left[\varphi_{\frac{n}{2}}(u)\right]^2 = \left[\varphi_{\frac{n}{2}}(v\tilde{l}^2 - 2)\right]^2$. ∎

Exemplo 8. Considere a curva afim $v^3 = \varphi_2(y^{\frac{2}{2}} + y^{\frac{2}{2}}) = y^2 + y^{-2}$ sobre $\mathbb{F}_{25}$. Pelo Corolário 3.2.6, tal equação é irredutível e $E_1^\omega = \mathbb{F}_{25}(v, \tilde{u})$ (onde $\tilde{u} = y^{2/2} + y^{-2/2}$), subcorpo do corpo Hermitiano $\mathcal{H}$ sobre $\mathbb{F}_{25}$. Tal curva é, portanto, um exemplo de uma curva maximal sobre $\mathbb{F}_{25}$.

3.3 O caso em que m divide $q+1$

Seja E_2 o único corpo intermediário da extensão $\mathcal{H}/\mathbb{F}_{q^2}(y)$ tal que $[\mathcal{H} : E_2] = m$, onde m é um divisor de $q+1$ (tal corpo existe pois a extensão $\mathcal{H}/\mathbb{F}_{q^2}(y)$ sendo de Kummer, em particular, é cíclica).

Considere E_2^ω o corpo fixo pelo automorfismo $\omega \in Aut_{\mathbb{F}_{q^2}}\mathcal{H}$ tal que $\omega(y) = y^{-1}$ e $\omega(x) = xy^{-1}$. Temos $E_2^\omega = \mathcal{H}^{\mathcal{G}}$ onde $\mathcal{G} = \langle \lambda, \omega \rangle$ é dado na primeira Seção deste Capítulo), já que $E_2 = \mathcal{H}^\lambda$, pela unicidade de E_2.

Proposição 3.3.1. *Seja $z = y^1 + y^{-1}$. A extensão $\mathcal{H}^\omega/\mathbb{F}_{q^2}(z)$ é de Kummer de grau (q+ 1) e $[x + \omega(x)]$ é um gerador dessa extensão.*

Demonstração. De fato, $\mathbb{F}_{q^2}$ contém uma $(q+1)$-ésima raiz primitiva da unidade e $mdc\,(q+1, char\,\mathbb{F}_{q^2}) = mdc\,(q+1, p) = 1$. Além disso, $x + \omega(x) \in \mathcal{H}^\omega$, pois $\omega\,(x + \omega(x)) = \omega(x) + \omega^2(x) = x + \omega(x)$. Temos também que

$$x + \omega(x) = \frac{xy + x}{y} = \frac{x}{y^{1/2}} . \frac{y+1}{y^{1/2}}$$

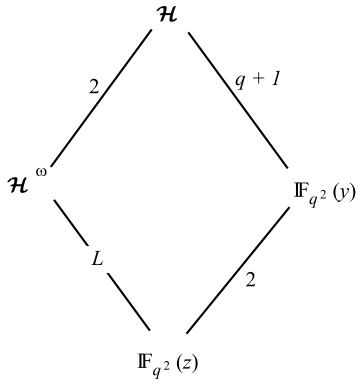
$$[x + \omega(x)]^{q+1} = \frac{x^{q+1}}{y^{\frac{q+1}{2}}} . \frac{(y+1)^{q+1}}{y^{\frac{q+1}{2}}} = \frac{x^{q+1}}{y^{\frac{q+1}{2}}} . \left[\frac{(y+1)^2}{y}\right]^{\frac{q+1}{2}} =$$

$$= (y^q + y).y^{-\frac{(q-1)}{2}} . \left[\frac{y^2 + 2y + 1}{y}\right]^{\frac{q+1}{2}} = \left(y^{\frac{q-1}{2}} + y^{-\frac{q-1}{2}}\right)(z+2)^{\frac{q+1}{2}} =$$

$$= \varphi_{\frac{q-1}{2}}(z)(z+2)^{\frac{q+1}{2}} \in \mathbb{F}_{q^2}(z) \qquad (1)$$

Como $[\mathcal{H} : \mathbb{F}_{q^2}(z)] = q+1$, $p(u) = u^{q+1} - \varphi_{\frac{q-1}{2}}(z)(z+2)^{\frac{q+1}{2}} \in \mathbb{F}_{q^2}(z)[u]$ é o polinômio mínimo de $[x+\omega(x)]$ sobre $\mathbb{F}_{q^2}(z)$. Logo, $\beta := \varphi_{\frac{q-1}{2}}(z)(z+2)^{\frac{q+1}{2}}$ satisfaz $\beta \neq w^d$ para todo $w \in \mathbb{F}_{q^2}(z)$ e para todo $d > 1$, d divisor de $(q+1)$.

Seja $L := \mathbb{F}_{q^2}(z)(x+\omega(x))$.



Sabemos que o grau do polinômio $p_{y,\mathbb{F}_{q^2}(z)}$, polinômio mínimo de y sobre $\mathbb{F}_{q^2}(z)$, é 2 e como $L \supset \mathbb{F}_{q^2}(z)$, temos que $\partial\, p_{y,L} \leq 2$. Como $\mathcal{H} = L(y)$ (de fato, $x+\omega(x) = x(1+y^{-1})$), temos $[\mathcal{H} : L] = \partial\, p_{y,L} \leq 2$. Logo, $[\mathcal{H}^{\omega} : L] = \frac{[\mathcal{H}:L]}{[\mathcal{H}:\mathcal{H}^{\omega}]} = \frac{[\mathcal{H}:L]}{2} \leq 1$. ∎

Proposição 3.3.2. *$E_2^{\omega}/\mathbb{F}_{q^2}(z)$ é uma extensão de Kummer de grau $\frac{q+1}{m}$ e $[x+\omega(x)]^m$ é um gerador dessa extensão.*

Demonstração. Primeiramente, mostremos que $[x+\omega(x)]^m \in E_2^{\omega} = \mathcal{H}^{\mathcal{G}}$. De fato,

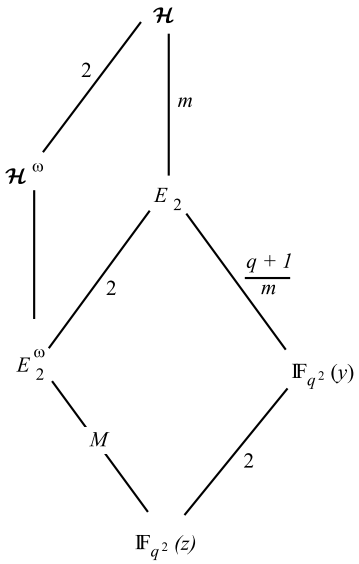
$$\lambda([x+\omega(x)]^m) = (\lambda(\,[x+\omega(x)]\,))^m = [\varepsilon^{\frac{q^2-1}{m}}(\,[x+\omega(x)]\,)]^m =$$

$$= [\varepsilon^{\frac{q^2-1}{m}}(x) + \varepsilon^{\frac{q^2-1}{m}}(\omega(x))]^m = [\varepsilon^{\frac{q^2-1}{m}}(x) + \varepsilon^{\frac{q^2-1}{m}}\left(\frac{x}{y}\right)]^m =$$

$$= \left[a^{\frac{q^2-1}{m}}x + \frac{a^{\frac{q^2-1}{m}}x}{a^{\frac{q^2-1}{m}(q+1)}y}\right]^m = \left[a^{\frac{q^2-1}{m}}(x) + \frac{a^{\frac{q^2-1}{m}}x}{y}\right]^m =$$

$$= [a^{\frac{q^2-1}{m}}(x+x/y)]^m = a^{q^2-1}(x+x/y)^m = [x+\omega(x)]^m.$$

Logo, $[x+\omega(x)]^m \in \mathcal{H}^{\lambda}$. Como $[x+\omega(x)]^m \in \mathcal{H}^{\omega}$ (Proposição 3.3.1), temos que $[x+\omega(x)]^m \in \mathcal{H}^{\langle\lambda,\omega\rangle} = \mathcal{H}^{\mathcal{G}} = E_2^{\omega}$. Seja $M = \mathbb{F}_{q^2}(z)((x+\omega(x)^m)$.



Como $[\mathcal{H}^{\omega} : \mathbb{F}_{q^2}(z)] = q+1$, se $[M : \mathbb{F}_{q^2}(z)] < \frac{q+1}{m}$, então $[\mathcal{H}^{\omega} : M] > m$, o que seria absurdo, já que $x + \omega(x)$ é raiz de $u^m - [x + \omega(x)]^m \in M[u]$. Logo, $[M : \mathbb{F}_{q^2}(z)] = \frac{q+1}{m}$ e $[\mathcal{H}^{\omega} : M] = m$.

Logo,

$$m = [E_2^{\omega} : M] = \frac{[\mathcal{H}^{\omega} : M]}{[\mathcal{H}^{\omega} : E_2^{\omega}]} = 1.$$

Portanto, $E_2^{\omega} = M = \mathbb{F}_{q^2}(z)([x + \omega(x)]^m)$ e pela equação (1), temos que

$$\{[x + \omega(x)]^m\}^{\frac{q+1}{m}} = \varphi_{\frac{q-1}{2}}(z)(z+2)^{\frac{q+1}{2}} \in \mathbb{F}_{q^2}(z) \qquad (4)$$

é o polinômio mínimo de $[x + \omega(x)]^m$ sobre $\mathbb{F}_{q^2}(z)$. Como $\mathbb{F}_{q^2}$ contém uma $\frac{q+1}{m}$-ésima raiz primitiva da unidade (pois $(a^{m(q-1)})^{\frac{q+1}{m}} = 1$ para todo $a \in \mathbb{F}_{q^2}$) e $mdc\,(q+1/m,\, p) = 1$, a extensão $E_2^{\omega}/\mathbb{F}_{q^2}(z)$ é uma extensão de Kummer de grau $\frac{q+1}{m}$ e $[x + \omega(x)]^m$ é um gerador dela. ∎

Corolário 3.3.3. *Com as notações anteriores, temos que $E_2^{\omega} = \mathbb{F}_{q^2}(u, v)$, onde u e v satisfazem a equação irredutível*

$$v^{\frac{q+1}{m}} = u + u^q + \varphi_{q-1}(u-2) - 2.$$

Demonstração. Em primeiro lugar, observamos que

$$[x+\omega(x)]^{q+1} = \left[x\left(1+\tfrac{1}{y}\right)\right]^{q+1} = (y^q+y)\left(1+\tfrac{1}{y}\right)(1+y^{-1})^q =$$
$$= (y^q+y)\left(1+\tfrac{1}{y}\right)(1+y^{-q}) = (y^q+y)(1+y^{-q}+y^{-1}+y^{-(q+1)}) =$$
$$= (y^{-1}+y+2)+(y^q+y^{-q}+2)+(y^{q-1}+y^{-(q-1)}-2)$$
$$= (z+2)+(z+2)^q+(y^{q-1}+y^{-(q-1)}-2)$$

Definindo-se $v := [x+\omega(x)]^m$ e $u = z+2$, temos pela Proposição 3.3.2 e pela igualdade acima que $E_2^\omega = \mathbb{F}_{q^2}(z)(v) = \mathbb{F}_{q^2}(z+2)(v) = \mathbb{F}_{q^2}(u,v)$ e

$$v^{\frac{q+1}{m}} = u + u^q + \varphi_{q-1}(u-2) - 2$$

é o polinômio mínimo de v sobre $F_{q^2}(u)$. ∎

Corolário 3.3.4. *Seja E_2 o único corpo intermediário da extensão $\mathcal{H}/\mathbb{F}_{q^2}(y)$ tal que $[\mathcal{H} : E_2] = m$, onde m é um divisor de $q+1$. Considere E_2^ω o corpo fixo pelo automorfismo $\omega \in Aut_{\mathbb{F}_{q^2}}\mathcal{H}$ tal que $\omega(y) = y^{-1}$ e $\omega(x) = xy^{-1}$. Temos:*

$$g(E_2^\omega) = \begin{cases} \frac{(q-3)(q+1-m)}{4m}, \textit{ se } m \textit{ é par} \\ \frac{(q-3)(q+1-m)+(q+1)}{4m}, \textit{ se } m \textit{ é ímpar} \end{cases}$$

onde $g(E_2^\omega)$ é o gênero de E_2^ω.

Demonstração. Pela Proposição 3.3.2, a extensão de grau $\frac{q+1}{m}$ $E_2^\omega/\mathbb{F}_{q^2}(z)$ é de Kummer, com $E_2^\omega = \mathbb{F}_{q^2}(z)([x+\omega(x)]^m)$ e

$$\{[x+\omega(x)]^m\}^{\frac{q+1}{m}} = \varphi_{\frac{q-1}{2}}(z)(z+2)^{\frac{q+1}{2}}. \qquad (*)$$

Deste modo, os únicos lugares de $\mathbb{F}_{q^2}(z)$ que podem se ramificar em $E_2^\omega/\mathbb{F}_{q^2}(z)$ são os zeros ou pólos de $\varphi_{\frac{q-1}{2}}(z)(z+2)^{\frac{q+1}{2}}$. Por outro lado, pelo Lema 2.1.6, o polinômio $\varphi_{\frac{q-1}{2}}(z)$ é separável e possui todas as suas raízes em $\mathbb{F}_{q^2}$. Logo, $(*)$ pode ser reescrita como

$$\{[x+\omega(x)]^m\}^{\frac{q+1}{m}} = (z+2)^{\frac{q+1}{2}}.\prod_{i=1}^{\frac{q-1}{2}}(z-\beta_i) \ \ , \textit{onde} \ \ \varphi_{\frac{q-1}{2}}(\beta_i) = 0$$

e os únicos lugares de $\mathbb{F}_{q^2}(z)$ que podem se ramificar em $E_2^\omega/\mathbb{F}_{q^2}(z)$ são os zeros de $z-\beta_i$ ($i \in \{1,\cdots,\frac{q-1}{2}\}$), o zero P_{-2} de $z+2$ e o pólo P_∞ de $\varphi_{\frac{q-1}{2}}(z)(z+2)^{\frac{q+1}{2}}$. Seja P_{β_i} um zero de $u-\beta_i$. Há quatro possibilidades a serem consideradas:

- $P \in \mathbb{P}_{\mathbb{F}_{q^2}}$ e $P \notin \{P_{\beta_i}, P_{-2}, P_\infty; i = 1, \cdots, \frac{q-1}{2}\}$. Nesse caso, $v_P(\varphi_{\frac{q-1}{2}}(z)(z+2)^{\frac{q+1}{2}}) = 0$ e para todo $P' \in \mathbb{P}_{E_2^\omega}$ acima de P, temos $e(P'|P) = \frac{(q+1)/m}{mdc((q+1)/m,0)} = 1$.

- se $P = P_{-2}$, temos $v_P(\varphi_{\frac{q-1}{2}}(z)(z+2)^{\frac{q+1}{2}}) = \frac{q+1}{2}$ e para todo $P'_{-2} \in \mathbb{P}_{E_2^\omega}$ acima de P_{-2}, temos $e(P'_{-2}|P_{-2}) = \frac{(q+1)/m}{d}$, onde

$$d = mdc\left(\frac{q+1}{m}, \frac{q+1}{2}\right) = \frac{mdc(\frac{2(q+1)}{m}, q+1)}{2}. \qquad (**)$$

  De $(**)$, temos que d é múltiplo de $\frac{q+1}{2m}$ e é divisor de $\frac{q+1}{m}$. Logo, $d \in \left\{\frac{q+1}{2m}, \frac{q+1}{m}\right\}$. Se m for par, temos $d = \frac{q+1}{m}$ e, nesse caso, $e(P'_{-2}|P_{-2}) = 1$. Se m for ímpar, temos $d = \frac{q+1}{2m}$ e, nesse caso, $e(P'_{-2}|P_{-2}) = 2$.

- Se $P = P_\infty$, temos $v_\infty(\varphi_{\frac{q-1}{2}}(z)(z+2)^{\frac{q+1}{2}}) = -q$ e para todo $P'_\infty \in \mathbb{P}_{E_2^\omega}$ acima de P_∞, temos $e(P'_\infty|P_\infty) = \frac{(q+1)/m}{mdc((q+1)/m,-q)} = (q+1)/m$.

- Finalmente, se $\beta_i \in \mathbb{F}_{q^2}$ satisfaz $\varphi_{\frac{q-1}{2}}(\beta_i) = 0$, temos para $P = P_{\beta_i}$ que $v_{\beta_i}(\varphi_{\frac{q-1}{2}}(z)(z+2)^{\frac{q+1}{2}}) = 1$ e para todo $P'_{\beta_i} \in \mathbb{P}_{E_2^\omega}$ acima de P_{β_i}, temos $e(P'_{\beta_i}|P_{\beta_i}) = \frac{(q+1)/m}{mdc((q+1)/m,1)} = (q+1)/m$. Portanto, há exatamente $\frac{q-1}{2}$ zeros de $\varphi_{\frac{q-1}{2}}(z)$ em $\mathbb{F}_{q^2}(z)$, os quais ramificam-se totalmente na extensão $E_2^\omega/\mathbb{F}_{q^2}(z)$.

Afirmação: Seja K' o corpo de constantes de E_2^ω. Se $K := \mathbb{F}_q^2$, então $K' = \mathbb{F}_{q^2}$.
Demonstração: Seja K'' o corpo de constantes de $\mathcal{H}$. Como $E_2^\omega \subset \mathcal{H}$, temos que $K' \subset K''$. Além disso, $\mathcal{H}/\mathbb{F}_{q^2}(y)$ é uma extensão de Kummer e para $P'_0 \in \mathbb{P}_{\mathcal{H}}$ acima de P_0, zero de y em $\mathbb{F}_{q^2}(y)$, temos $v_{P'_0}(y(y^{q-1}+1)) = 1$ e pelo Teorema 1.3.27, segue que $K'' = \mathbb{F}_{q^2}$. Logo, $\mathbb{F}_{q^2} = K \subset K' \subset K'' = \mathbb{F}_{q^2}$. □

Finalmente, podemos aplicar o Teorema 1.3.27 à extensão $E_2^\omega/\mathbb{F}_{q^2}(z)$ para calcular o gênero de E_2^ω:

$$g(E_2^\omega) = 1 + \frac{q+1}{m}(g-1) + \frac{1}{2}\sum_{P \in \mathbb{P}_{\mathbb{F}_{q^2}(z)}} \left(\frac{q+1}{m} - r_P\right) deg\, P\,,$$

onde g é o gênero de $\mathbb{F}_{q^2}(z)$ e $r_P = mdc\left(\frac{q+1}{m}, v_P(\varphi_{\frac{q-1}{2}}(z)(z+2)^{\frac{q+1}{2}})\right)$.

Caso 1: m é par

Nesse caso, temos:

- Se $P = P_{-2}$, $e(P'_{-2}|P_{-2}) = 1$ e $r_{P_{-2}} = (q+1)/m$.
- Se $P = P_{\beta_i}$, onde $\varphi_{\frac{q-1}{2}}(\beta_i) = 0$, temos $e(P'_{\beta_i}|P_{\beta_i}) = (q+1)/m$ e $r_{P_{\beta_i}} = 1$.
- Se $P = P_\infty$, temos $e(P'_\infty|P_\infty) = (q+1)/m$ e $r_{P_\infty} = 1$.

Portanto,

$$g(E_2^\omega) = 1 - \frac{q+1}{m} + \frac{1}{2}\left[\frac{q+1}{2}\left(\frac{q+1}{m} - 1\right) + \left(\frac{q+1}{m} - \frac{q+1}{m}\right)\right] =$$
$$= 1 - \frac{q+1}{m} + \frac{(q+1)(q+1-m)}{4m} = \frac{-4(q+1-m) + (q+1)(q+1-m)}{4m} =$$
$$= \frac{(q-3)(q+1-m)}{4m}.$$

Caso 2: m é ímpar

Nesse caso, a única diferença é que $e(P'_{-2}|P_{-2}) = 2$ e $r_{P_{-2}} = (q+1)/2m$.

Logo,

$$g(E_2^\omega) = 1 - \frac{q+1}{m} + \frac{1}{2}\left[\frac{q+1}{2}\left(\frac{q+1}{m} - 1\right) + \left(\frac{q+1}{m} - \frac{q+1}{2m}\right)\right] =$$
$$= 1 - \frac{q+1}{m} + \frac{1}{2}\left[(q+2-m)\frac{(q+1)}{2m}\right] = \frac{4m - 4(q+1) + (q+1)(q+2-m)}{4m} =$$
$$= \frac{-m(q-3) + q^2 - q - 2}{4m} = \frac{-m(q-3) + (q-2)(q+1)}{4m} =$$
$$= \frac{-m(q-3) + (q-3)(q+1) + (q+1)}{4m} = \frac{(q-3)(q+1-m) + (q+1)}{4m}.$$

∎

Exemplo 9. Seja $v^4 = u^7 + u + \varphi_6(u-2) - 2$ sobre $\mathbb{F}_{49}$. Pelo Corolário 3.3.3, tal curva é maximal sobre $\mathbb{F}_{49}$ e seu gênero é 3 (Corolário 3.3.4).

Referências Bibliográficas

[E] Otto Endler : Teoria dos Corpos, Monografias de Matemática (44), IMPA (1987).

[G-L] A. Garcia, Y. Lequain: Elementos de Álgebra, IMPA (2003).

[G-S] A. Garcia, H. Stichtenoth: On Chebyshev Polinomials and Maximal Curves, Acta Arithmetica, XC.4 (1999).

[L] Gilles Lachaud: Sommes d'Eisenstein et nombre de points de certaines courbes algébriques sur les corps finis, C. R. Acad. Sci. Paris: t. 305, I, p. 729-732 (1987).

[N] H. Niederreiter, R. Lidl: Introduction to Finite Fields and their Applications, Cambridge University Press (1986).

[R] Theodore J. Rivlin: Chebyshev Polynomials: From Approximation Theory to Algebra and Number Theory, Wiley-Interscience (1990).

[S] Henning Stichtenoth: Algebraic Function Fields and Codes, Springer-Verlag (1993).