Diego Kian

Construção de infinitas extensões separáveis de corpos de funções algébricas com grupos de automorfismos isomorfos

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

Santo André, 2019

Universidade Federal do ABC

Centro de Matemática, Computação e Cognição

Diego Kian

Construção de infinitas extensões separáveis de corpos de funções algébricas com grupos de automorfismos isomorfos

Orientador: Prof. Dr. Nazar Arakelian

Dissertação de mestrado apresentada ao Centro de Matemática, Computação e Cognição para obtenção do título de Mestre em Matemática

Este exemplar corresponde à versão final da dissertação
defendida pelo aluno Diego Kian,
e orientada pelo Prof. Dr. Nazar Arakelian.

Santo André, 2019

Sistema de Bibliotecas da Universidade Federal do ABC
Elaborada pelo Sistema de Geração de Ficha Catalográfica da UFABC
com os dados fornecidos pelo(a) autor(a).

Kian, Diego
Construção de infinitas extensões separáveis de corpos de funções algébricas com grupos de automorfismos isomorfos / Diego Kian. — 2019.

164 fls. : il.

Orientador: Nazar Arakelian

Dissertação (Mestrado) — Universidade Federal do ABC, Programa de Pós-Graduação em Matemática, Santo André, 2019.

1. corpos de funções algébricas. I. Arakelian, Nazar. II. Programa de Pós-Graduação em Matemática, 2019. III. Título.

Este exemplar foi revisado e alterado em relação à versão original, de acordo com as observações levantadas pela banca no dia da defesa, sob responsabilidade única do autor e com a anuência de seu orientador.

Santo André, 11 de março de 2019.

Assinatura do autor: Diego Kian

Assinatura do orientador:

MINISTÉRIO DA EDUCAÇÃO
Fundação Universidade Federal do ABC
Programa de Pós-Graduação em Matemática
Avenida dos Estados, 5001 – Bairro Santa Terezinha – Santo André – SP
CEP 09210-580 · Fone: (11) 4996-0017
ppg.matematica@ufabc.edu.br

FOLHA DE ASSINATURAS

Assinaturas dos membros da Banca Examinadora que avaliou e aprovou a Defesa de Dissertação de Mestrado do candidato Diego Kian, realizada em 1 de fevereiro de 2019:

Prof.(a) Dr.(a) **Nazar Arakelian** (Universidade Federal do ABC) – Presidente

Prof.(a) Dr.(a) **Herivelto Martins Borges Filho** (Universidade de São Paulo) – Membro Titular

Prof.(a) Dr.(a) **Luis Enrique Ramirez** (Universidade Federal do ABC) – Membro Titular

Prof.(a) Dr.(a) **Fernando Eduardo Torres Orihuela** (Universidade Estadual de Campinas) – Membro Suplente

Prof.(a) Dr.(a) **Zhanna Gennadyevna Kuznetsova** (Universidade Federal do ABC) – Membro Suplente

AGRADECIMENTOS

Agradeço ao professor Nazar Arakelian, pela orientação e pelos ensinamentos e conselhos.

Agradeço aos professores Herivelto Martins Borges Filho e Luis Enrique Ramirez, pelo aceite do convite de participação na banca e pelas sugestões de melhoria do texto da dissertação.

Pela autorização concedida para reprodução do conteúdo de um artigo, agradeço: à *Cambridge University Press* (C.U.P.), ao *Copyright Clearance Center* (C.C.C.) e ao *Journal of the Australian Mathematical Society*; a C. Álvarez-García e a G. D. Villa-Salvador (autores do artigo); e à Jessica LaFata (atendimento do C.C.C.). Atendendo aos termos e condições da licença de uso da C.U.P., fazemos menção ao referido artigo usado na dissertação:

> ÁLVAREZ-GARCÍA, Caín; VILLA-SALVADOR, Gabriel Daniel. **Finite groups as Galois groups of function fields with infinite field of constants**. Journal of the Australian Mathematical Society, Volume 88, Issue 3, 301-312, reproduced with permission.

Agradeço à CAPES, pelo apoio financeiro.

RESUMO

Sejam $E \mid k$ um corpo de funções com um corpo de constantes infinito e $E \mid k(x)$ uma extensão separável de grau maior que 1. Suponha que existe um *place* de $k(x)$ de grau 1 ramificado em $E \mid k(x)$. Seja $K \mid k$ um corpo de funções com gênero maior que 1. Neste trabalho, apresentamos uma construção de uma infinidade de extensões finitas e separáveis de corpos de funções algébricas $L \mid K$ com $\left[E : k(x)\right] = \left[L : K\right]$ e $\mathrm{Aut}\,(L \mid k) = \mathrm{Aut}\,(L \mid K) \cong \mathrm{Aut}\left(E \mid k(x)\right)$. O resultado é devido a C. Álvarez-García e G. D. Villa-Salvador, e é análogo a um teorema de H. Stichtenoth (1984).

Palavras-chave: corpo de funções algébricas, grupo de automorfismos

ABSTRACT

Let $E \mid k$ a function field over an infinite field of constants and $E \mid k(x)$ a separable extension of degree greater than 1. Suppose there is a place of $k(x)$ of degree 1 ramified in $E \mid k(x)$. Let $K \mid k$ a function field with genus greater than 1. In this work, we present a construction of a infinitely many separable finite extensions of algebraic function fields $L \mid K$ with $\left[E : k(x)\right] = \left[L : K\right]$ and $\mathrm{Aut}\,(L \mid k) = \mathrm{Aut}\,(L \mid K) \cong \mathrm{Aut}\left(E \mid k(x)\right)$. The result is due to C. Álvarez-García and G. D. Villa-Salvador, and it is analogous to an H. Stichtenoth's theorem (1984).

Keywords: algebraic function field, group of automorphisms

CONTEÚDO

1 CONVENÇÕES

O símbolo $\mathbb{N}$ (resp., $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$) denota o conjunto dos números naturais (resp., inteiros, racionais, reais e complexos).

Convencionaremos que $\mathbb{N} = \mathbb{Z}_+^*$.

1.1 NOTAÇÕES

O fim da prova de uma Afirmação será indicada com o símbolo $\diamond$, enquanto que o término da demonstração de um teorema (ou proposição, lema, etc) será denotada com o signo $\square$.

A notação $L \mid K$ indica uma extensão de corpo, e $F \mid k$ denota um corpo de funções F sobre k.

O polinômio minimal (na variável T) de um elemento $\alpha \in K$ sobre o corpo K será denotado como $m_{\alpha,K}(T)$.

Ideais serão denotados com letras góticas (tipo Fraktur): $\mathfrak{p}$, $\mathfrak{P}$, $\mathfrak{q}$, $\mathfrak{Q}$, etc.

2 | INTRODUÇÃO

Sejam $L \mid F$ uma extensão de corpo e $\alpha \in L$. Pela teoria de corpos, temos um critério para descrever a adjunção de α com o corpo base F.

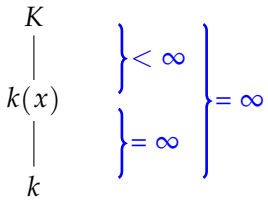
- Se α é algébrico sobre F, então $F(\alpha) \mid F$ é finitamente gerada e algébrica — e, portanto, finita (cf. Endler (2012, p. 35)).
- Se α é transcendente sobre F, então $F(\alpha)$ é de dimensão infinita sobre F, por ser isomorfo ao corpo de funções racionais em uma variável sobre F:

$$F(\alpha) \cong F(X) \tag{1}$$

  — cf. Martin (2010, p. 225).

Se $K \mid k$ é uma extensão de corpo, dizemos que $K \,/\, k$ é um corpo de funções algébricas em uma variável sobre k quando existe $x \in K$ transcendente sobre k tal que $K \mid k(x)$ é finita.

Figura 1. Ilustração para a definição de um corpo de funções algébricas.



Por comodidade, diremos que $K \,/\, k$ é um corpo de funções (sobre k), simplesmente.

Pelo isomorfismo em (1), o símbolo x pode ser visto ora como um elemento que não é raiz de nenhum polinômio em $k[X]$, ora como o polinômio $p(X) = X$ (isto é, uma variável) no corpo de frações $k(X)$ de $k[X]$.

Um elemento de K será chamado de função, e os elementos de K que são algébricos sobre k serão chamados de constantes.

Na Teoria de Corpos de Números, estudam-se extensões finitas de $\mathbb{Q}$, o corpo de números mais 'elementar'. Como todo corpo de funções K sobre k pode ser visto como uma extensão finita de um corpo de funções $k(x)$ na variável x, então podemos ver um corpo de funções racionais na Teoria de Corpos de Funções como o análogo de $\mathbb{Q}$ na Teoria de Corpos de Números, no sentido de serem os objetos mais 'simples' da teoria.

Para compreender um corpo de funções K, é interessante estudar os subanéis de K que se caracterizam por admitirem um único ideal maximal.

Um anel de valoração de um corpo de funções $K \mid k$ é um anel $\mathcal{O} \subseteq K$ tal que: (1) $k \subsetneq \mathcal{O} \subsetneq K$; e (2) ou $z \in \mathcal{O}$ ou $z^{-1} \in \mathcal{O}$, $\forall\, z \in K$.

Anéis de valoração são anéis locais: se $\mathcal{O}$ é um anel de valoração, então a coleção dos elementos *não* invertíveis em $\mathcal{O}$,

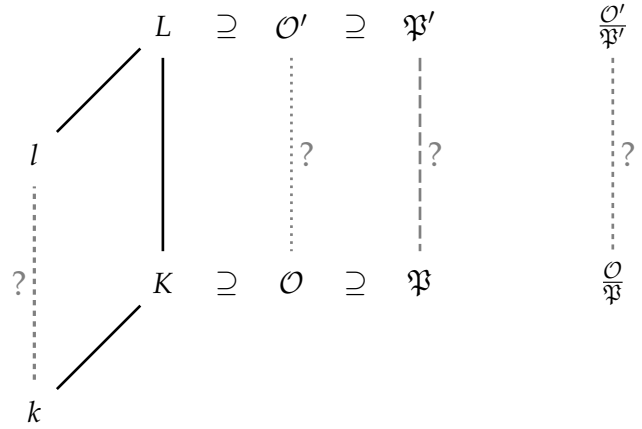
$$\mathfrak{P} := \mathcal{O} \setminus \mathcal{U}(\mathcal{O}) \,,$$

é o único ideal maximal de $\mathcal{O}$ (STICHTENOTH, 2009, p. 2).

Um *place*[1] em K é o ideal maximal de algum anel de valoração de $K \mid k$.

Considere um corpo de funções $L \mid l$ tal que L é uma extensão algébrica de K e l é uma extensão de k. O corpo de funções $L \mid l$ também tem um anel de valoração — $\mathcal{O}'$, digamos —; bem como um *place* $\mathfrak{P}'$. Um objeto de estudo de interesse na Teoria de Corpos de Funções é investigar como se relacionam os *places* ($\mathfrak{P}$ e $\mathfrak{P}'$), as constantes (em k e l) e os anéis de valoração ($\mathcal{O}$ e $\mathcal{O}'$) de K e de L (veja a Figura 2).

Figura 2. Como se relacionam as constantes e os *places* numa extensão de corpos de funções?



1 Esse termo não é usado, por exemplo, por Villa-Salvador (2006) e por Deuring (1973). Adotamos a nomenclatura de Stichtenoth (2009).

2.1 MOTIVAÇÃO: O PROBLEMA INVERSO DA TEORIA DE GALOIS

O Teorema Fundamental da Teoria de Galois (TFTG) nos fornece uma extraordinária conexão entre as teorias de corpos e de grupos. Dada uma extensão (galoisiana), o Teorema Fundamental fornece a construção de um grupo (de Galois), e estabelece uma correspondência entre subgrupos e subcorpos dos entes envolvidos.

Um problema no 'sentido contrário' seria partir de um grupo G (finito) e construir uma extensão (galoisiana) de um corpo K com grupo de Galois isomorfo a G:

Questão 2.1 (PITG: Problema Inverso da Teoria de Galois)**.** *Dados um grupo finito G e um corpo K, existe uma extensão galoisiana M de K tal que $G \cong \mathrm{Gal}(M \mid K)$?*
(JENSEN et al.*, 2002, p. 1).*

A formulação clássica do PITG refere-se ao caso em que $K = \mathbb{Q}$.

Um dos progressos parciais mais relevantes na busca da resposta ao PITG é quando G é um grupo solúvel e K é um corpo global (por definição, um corpo global é uma extensão finita de $\mathbb{Q}$ ou de $\mathbb{F}_p(t)$ (NEUKIRCH, 1999, p. 134)):

Teorema 2.2 (Šafarevič)**.** *Sejam K um corpo global e G um grupo solúvel finito.*
Então existe uma extensão galoisiana $M \mid K$ tal que $\mathrm{Gal}(M \mid K) \cong G$.
(NEUKIRCH et al.*, 2015, p. 574).*

Existem outros importantes exemplos de pares (G, K) em que se verifica a validez do Problema Inverso, já incorporados à literatura. A título de ilustração, fazemos menção a alguns casos:

- (Hilbert) Se $K = \mathbb{Q}$ e $G = \mathcal{S}_n$ é o grupo simétrico de ordem n ou $G = \mathcal{A}_n$ é o grupo alternado de ordem n (para qualquer $n \in \mathbb{N}$), então G ocorre como grupo de Galois sobre $\mathbb{Q}$ (VÖLKLEIN, 1996, p. 53). Estes dois resultados decorrem do Teorema de Irredutibilidade de Hilbert (*Theorem* 1.23 no livro de Völklein (1996, p. 18)).

- (Scholz-Reichardt) Se $K = \mathbb{Q}$ e G é um p-grupo finito (para $p \in \mathbb{Z}$ primo ímpar), o PITG tem solução positiva. Para uma prova, recomendamos o Capítulo 2 do livro de Serre (2007).

- (Kronecker-Weber) Se G é um grupo abeliano finito, sabe-se que existe uma extensão finita e galoisiana $L \mid \mathbb{Q}$ cujo grupo de Galois é isomorfo a G (MARTIN, 2010, p. 418). Nessa construção, o corpo L é um subcorpo de um corpo ciclotômico. O Teorema de Kronecker-Weber (TKW), um celebrado resultado da Teoria dos Números Algébricos, nos diz que o caso abeliano do PITG não admite outra classe de soluções:

  $$\Big[\ L \mid \mathbb{Q} \text{ é extensão abeliana } \Big] \Leftrightarrow \Big[\ \exists\, \xi_m \in \mathbb{C} \text{ raiz } m\text{-ésima da unidade: } L \subseteq \mathbb{Q}(\xi_m) \ \Big] \ .$$

  Para uma demonstração do TKW, recomendamos o livro de Janusz (1996, p. 198).

Na Teoria de Galois *Finita*, é de amplo conhecimento uma das caracterizações de extensões galoisianas: uma extensão finita $L \mid K$ é galoisiana se, e somente se, $L \mid K$ é normal e separável (DUMMIT e FOOTE, 2004, p. 574).

Alguns caminhos possíveis para a tentativa de uma construção de uma extensão galoisiana $M \mid K$ com grau preestabelecido são:

1. Se $L \mid K$ é uma extensão finita e separável, então se M é o fecho normal de $L \mid K$, temos que $M \mid K$ é uma extensão separável — cf. *Proposition* 3.3.7 no livro de Bastida (1984, p. 118) —, normal (por definição) e finita (por simples verificação). Portanto, $M \mid K$ seria finita e Galois.

2. Se $L \mid K$ é uma extensão finita e normal, então se M é o fecho separável de K em L, teríamos que $M \mid K$ seria uma extensão finita (pois M seria corpo intermediário da extensão finita L de K), normal — cf. *Proposition* 3.3.6 no livro de Bastida (1984, p. 117) — e separável (por definição de fecho separável).

3. Se G é um grupo finito arbitrário, Fried e Kollár (1978) provaram que existe uma extensão finita M de $\mathbb{Q}$ tal que o grupo dos automorfismos em M que fixa $\mathbb{Q}$ é isomorfo a G:

   $$\mathrm{Aut}\,(M \mid \mathbb{Q}) = \mathrm{Aut}\,(M) \ \cong \ G \ .$$

   Nesta construção, a extensão $M \mid \mathbb{Q}$ é separável, mas pode não ser normal.

As construções acima mencionadas são, isoladamente, simples (excetuando-se, possivelmente, a construção do item 3). A dificuldade da solução do PITG é compatibilizar

uma construção de uma extensão de corpo que seja *simultaneamente* finita, normal, separável e com grupo de automorfismos isomorfo ao grupo (arbitrário) prescrito.

Pretendemos estudar um progresso parcial do entendimento da construção de extensões *separáveis* com propriedades prescritas para o grupo de automorfismos, especificamente no contexto da Teoria de Corpos de Funções.

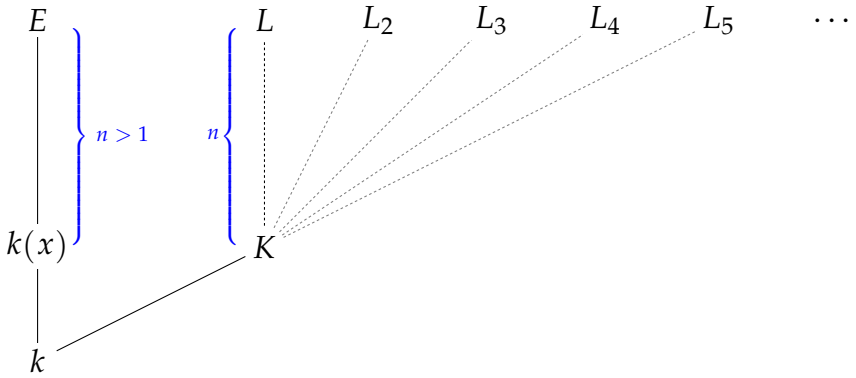
2.2 TEORIA DE GALOIS EM CORPOS DE FUNÇÕES

Alguns problemas relacionados a isomorfismos de grupos de automorfismos de extensões de corpos de funções foram solucionados com diferentes técnicas.

Em um artigo de 1984, Stichtenoth (1984) provou que: se k é algebricamente fechado e $E \mid k(x)$ é uma extensão finita separável de grau $n = \left[E : k(x)\right] > 1$, então para cada corpo de funções $K \,/\, k$, existem infinitas extensões $L \mid K$, separáveis e não isomorfas, tais que

$$\left[E : k(x)\right] = \left[L : K\right] \qquad \text{e} \qquad \operatorname{Aut}\left(E \mid k(x)\right) \cong \operatorname{Aut}\left(L \mid K\right) = \operatorname{Aut}\left(L \mid k\right). \tag{2}$$

Figura 3. Ilustração da infinidade de extensões de K dada pela construção de Stichtenoth (1984).



A construção de Stichtenoth (1984) requer que o gênero de $K \,/\, k$ seja maior que um (o gênero é um conceito relacionado a um corpo de funções que será definido no capítulo seguinte).

Em 1991, Villa-Salvador e Rzedowski-Calderón (1991) provaram que a construção de infinitas extensões separáveis de corpos de funções $L \mid K$ com as propriedades

mencionadas em (2) também pode ser feita no caso em que o corpo k é finito, se o zero de x ramifica-se em $E \mid k(x)$ e o polo de x não se ramifica em $E \mid k(x)$.

Em 1992, Madan e Rosen (1992) provaram que se K é um corpo de funções sobre um corpo algebricamente fechado k e G é um grupo finito não trivial, então existem infinitas extensões galoisianas $L \mid K$ tais que $\mathrm{Gal}(L \mid K) \cong G$.

Alguns interessantes casos resolvidos do PITG na Teoria de Corpos de Funções (com condições diferentes para as constantes) são mencionados na Seção 6.2 do Apêndice.

Neste trabalho, apresentamos o resultado análogo do histórico artigo de Stichtenoth (1984) para o caso em que o corpo de constantes k é um corpo infinito, com a hipótese adicional da existência de um *place* em $k(x)$ de grau 1 ramificado em $E \mid k(x)$. A demonstração, devida a Álvarez-García e Villa-Salvador (2010), tem técnicas essencialmente circunscritas na teoria clássica de corpos de funções.

No próximo capítulo, reproduzimos (sem demonstrações) resultados da Teoria de Corpos de Funções extraídos (em sua maioria) de duas obras que são referências-padrão na área: os livros de Stichtenoth (2009) e de Villa-Salvador (2006).

No Capítulo 4, apresentamos as ideias principais da demonstração do Teorema de Álvarez-García e Villa-Salvador (2010) — doravante, chamado de "Teorema Principal".

Finalmente, no Capítulo 5, demonstramos em detalhes o Teorema Principal.

3 REVISÃO BIBLIOGRÁFICA

3.1 BASES DE TRANSCENDÊNCIA

Para esta seção, $L \mid K$ denotará uma extensão de corpo.

Definição 3.1.

- *Um subconjunto $S \subseteq L$ é dito algebricamente dependente sobre K se existirem $n \in \mathbb{N}$, $f(x_1, x_2, \ldots, x_n) \in k[x_1, x_2, \ldots, x_n] \setminus \{0\}$ e n elementos distintos s_1, s_2, ..., $s_n \in S$ tais que $f(s_1, s_2, \ldots, s_n) = 0$.*

- *Um subconjunto de L que não é algebricamente dependente sobre K é chamado de algebricamente independente sobre K.*

(VILLA-SALVADOR, 2006, p. 1).

Definição 3.2 (base de transcendência)**.** *Uma base de transcendência de L sobre K é um subconjunto de L algebricamente independente sobre K e maximal em L.*
(VILLA-SALVADOR, 2006, p. 2).

Para uma extensão de corpo fixada, todas as suas bases de transcendência têm a mesma cardinalidade (ROMAN, 2006, p. 100). Assim, a seguinte definição faz sentido:

Definição 3.3 (grau de transcendência)**.** *O grau de transcendência de L sobre K é a cardinalidade de uma base de transcendência de L sobre K.*
(VILLA-SALVADOR, 2006, p. 3; ROMAN, 2006, p. 100).

Com a terminologia desta seção, podemos dizer que um corpo de funções algébricas (em uma variável) sobre k é uma extensão de corpo finitamente gerada sobre k com grau de transcendência 1.

3.2 VALORAÇÕES EM CORPOS DE FUNÇÕES

Definição 3.4 (valoração)**.** *Seja K um corpo. Dizemos que uma função $v : K \to \mathbb{Z} \cup \{\infty\}$ é uma valoração sobre K quando:*

1. $v(x) = \infty \Leftrightarrow x = 0$;
2. *a restrição $v \restriction_{K^*}$ for um homomorfismo sobrejetor (com relação aos grupos $(K^*, \cdot)$ e $(\mathbb{Z}, +)$); e*
3. *para quaisquer $a, b \in K^*$, valer a desigualdade*

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

A definição mais geral de valoração é dada no Apêndice.

3.2.1 Parâmetros locais

Sejam $F \,/\, k$ um corpo de funções, $\mathcal{O} \subseteq F$ um anel de valoração e $\mathfrak{P} \subseteq \mathcal{O}$ um *place*. Um parâmetro local (ou variável uniformizadora) é uma função $t \in \mathfrak{P}$ tal que $t \cdot \mathcal{O} = \mathfrak{P}$ (STICHTENOTH, 2009, p. 4).

Seja $v : F \to \mathbb{Z} \cup \{\infty\}$ uma valoração. Uma função $t \in F$ é um parâmetro local se, e somente se, $v(t) = 1$ (STICHTENOTH, 2009, p. 5).

Todo anel de valoração é um domínio de ideais principais (DIP) — cf. *Theorem* 1.1.6 no livro de Stichtenoth (2009, p. 3). Esse fato permite a seguinte construção:

Proposição 3.5 (descrição da totalidade do corpo de funções com parâmetros locais)**.** *Sejam: $K \,/\, k$ um corpo de funções; $\mathcal{O} \subseteq K$ um anel de valoração; $\mathfrak{P}$ o ideal maximal de $\mathcal{O}$; e $t \in \mathcal{O}$ um elemento gerador de $\mathfrak{P}$.*

Então para todo $z \in K \setminus \{0\}$ existe um único par $(n, u) \in \mathbb{Z} \times \mathcal{U}(\mathcal{O})$ tal que $z = t^n \cdot u$.

Recomendamos o livro de Villa-Salvador (2006, p. 26) para uma demonstração.

3.2.2 Valorações discretas

Definição 3.6 (valoração discreta)**.** *Seja $K \,/\, k$ um corpo de funções. Uma valoração discreta de $K \,/\, k$ é uma valoração $v : K \to \mathbb{Z} \cup \{\infty\}$ que satisfaz as seguintes condições:*

1. $\exists\, t \in K$ *tal que* $v(t) = 1$; *e*

2. $v \restriction_{k^*} \equiv 0$.

A existência de uma valoração discreta é dada pela seguinte construção:

Definição 3.7 (valoração discreta associada a um *place*)**.** *Sejam:* $F \,/\, k$ *um corpo de funções;* $\mathcal{O} \subseteq F$ *um anel de valoração; e* $\mathfrak{P}$ *o* place *associado a* $\mathcal{O}$*. Fixando-se um elemento gerador* $t \in \mathcal{O}$ *de* $\mathfrak{P}$*, sabe-se que, para todo* $z \in F \setminus \{0\}$ *existe um único par* $(n, u) \in \mathbb{Z} \times \mathcal{U}(\mathcal{O})$ *tal que* $z = t^n \cdot u$ *— cf. Proposição 3.5. Com isso, podemos definir uma aplicação* $v_{\mathfrak{P}} : F \to \mathbb{Z} \cup \{\infty\}$ *tal que* $v_{\mathfrak{P}}(z) = n$ *e* $v_{\mathfrak{P}}(0) = \infty$*.*

A valoração $v_{\mathfrak{P}}$ da definição acima é discreta, e o subconjunto

$$\mathcal{O}_{\mathfrak{P}} = \left\{ z \in F \;\middle|\; v_{\mathfrak{P}}(z) \geq 0 \right\} \tag{3}$$

de F é um anel de valoração com ideal maximal

$$\mathfrak{P} = \left\{ z \in F \;\middle|\; v_{\mathfrak{P}}(z) > 0 \right\} \tag{4}$$

e com

$$\mathcal{U}(\mathcal{O}_{\mathfrak{P}}) = \left\{ z \in F \;\middle|\; v_{\mathfrak{P}}(z) = 0 \right\} \tag{5}$$

como o conjunto dos invertíveis em $\mathcal{O}_{\mathfrak{P}}$.

O parâmetro local t na Definição 3.7 também é chamado de elemento primo (ou elemento uniformizador) da valoração $v_{\mathfrak{P}}$.

Nosso maior interesse são as valorações discretas, por conta do seguinte resultado:

Teorema 3.8. *Toda valoração sobre um corpo de funções é discreta.*
(VILLA-SALVADOR, 2006, p. 42).

3.2.3 Anéis de valoração em corpos de funções racionais

Quando $\left[K : k(x)\right] = 1$ — isto é, quando $K = k(x)$ é um corpo de funções racionais —, dispomos de uma descrição concreta dos anéis de valoração de K. Temos:

- para cada $p \in k[X]$ mônico e irredutível sobre k, o anel de valoração

$$\mathcal{O}_{p(X)} := \left\{ \frac{f}{g} \;\middle|\; f \in k[X]\ ,\ g \in k[X] \setminus \{0\}\ ,\ p \nmid g \text{ em } k[X] \right\}, \tag{6}$$

cujo ideal maximal é o *place*

$$\mathfrak{P}_{p(X)} := \left\{ \frac{f}{g} \;\middle|\; f \in k[X]\ ,\ g \in k[X] \setminus \{0\}\ ,\ p \nmid g \text{ em } k[X]\ ,\ p \mid f \text{ em } k[X] \right\}; \tag{7}$$

e

- o anel de valoração

$$\mathcal{O}_\infty := \left\{ \frac{f}{g} \;\middle|\; f \in k[X]\ ,\ g \in k[X] \setminus \{0\}\ ,\ \deg(f) \leq \deg(g) \right\}, \tag{8}$$

cujo ideal maximal é o *place*

$$\mathfrak{P}_\infty := \left\{ \frac{f}{g} \;\middle|\; f \in k[X]\ ,\ g \in k[X] \setminus \{0\}\ ,\ \deg(f) < \deg(g) \right\}. \tag{9}$$

Dizemos que duas valorações $v_1, v_2 : K \to \mathbb{Z} \cup \{\infty\}$ são equivalentes quando

$$\forall\, x \in K : \qquad v_1(x) > 0 \quad \Leftrightarrow \quad v_2(x) > 0\,.$$

Valorações equivalentes estão associadas a um anel de valoração comum (cf. Apêndice). Assim, é interessante conhecer um modo de discriminar classes de valorações duas a duas não equivalentes.

Teorema 3.9 (valorações em corpos de funções racionais)**.** *Seja $p \in k[X]$ irredutível. Considere: a valoração*

$$\begin{aligned} v_p : k(x) &\to \mathbb{Z} \cup \{\infty\} \\ \alpha = p^n \cdot \frac{h_\alpha}{g_\alpha} &\mapsto v_p(\alpha) = \begin{cases} n\,, & \text{se } \alpha \neq 0 \\ \infty\,, & \text{se } \alpha = 0 \end{cases}, \end{aligned} \tag{10}$$

em que, para cada $\alpha \in k(x)$, os polinômios h_α, $g_\alpha \in k[X]$ são tais que $\mathrm{mdc}\{h_\alpha, g_\alpha\} = 1$ e $p \nmid (h_\alpha \cdot g_\alpha)$; e a valoração

$$\begin{aligned} v_\infty = v_{\mathfrak{P}_\infty} : k(x) &\to \mathbb{Z} \cup \{\infty\} \\ \alpha = \frac{f}{g} &\mapsto v_\infty(\alpha) := \begin{cases} \deg(g) - \deg(f)\,, & \text{se } \alpha \neq 0 \\ \infty\,, & \text{se } \alpha = 0 \end{cases}. \end{aligned} \tag{11}$$

Toda valoração em $k(x)$ é equivalente (10) ou (11).
(VILLA-SALVADOR, 2006, p. 36).

3.2.4 Propriedades de valorações

Teorema 3.10 (Desigualdade Triangular Estrita)**.** *Sejam: $F \,/\, k$ um corpo de funções; $v : F \to \mathbb{Z} \cup \{\infty\}$ uma valoração discreta de F; e $x, y \in F$ tais que $v(x) \neq v(y)$. Então*

$$v(x+y) = \min\left\{v(x), v(y)\right\} .$$

(STICHTENOTH, 2009, p. 5).

Proposição 3.11 (propriedades operacionais)**.** *Sejam: K um corpo qualquer; v uma valoração sobre K; a, b, a_1, a_2, …, $a_n \in K$; e $n \geq 2$ inteiro. Então*

1. $v(1) = 0$.
2. $v\left(a^{-1}\right) = -v(a)$.
3. $v(a) = v(-a)$.
4. *a)* $v\left(\sum_{i=1}^{n} a_i\right) \geq \min\left\{v(a_i) \;\middle|\; 1 \leq i \leq n\right\}$.

   b) $v\left(\sum_{i=1}^{n} a_i\right) = \min\left\{v(a_i) \;\middle|\; 1 \leq i \leq n\right\}$ *se $v(a_i) \neq v\left(a_j\right)$ para todo $i \neq j$ (desigualdade triangular estrita "generalizada").*
5. *Se $\sum_{i=1}^{n} a_i = 0$, então existem j, $k \in \{1, 2, \ldots, n\}$ distintos tais que $v\left(a_j\right) = v(a_k)$.*

(VILLA-SALVADOR, 2006, p. 17).

Teorema 3.12 (Teorema de Aproximação)**.** *Sejam: $F \,/\, k$ um corpo de funções; $\mathfrak{P}_1$, …, $\mathfrak{P}_n \in \mathbb{P}(F)$* places *dois a dois distintos; x_1, …, $x_n \in F$; e r_1, …, $r_n \in \mathbb{Z}$.*

Então existe $x \in F$ tal que

$$v_{\mathfrak{P}_i}(x - x_i) = r_i \,, \qquad \forall\, i \in \{1, \ldots, n\} .$$

(STICHTENOTH, 2009, p. 12).

3.3 O CORPO DE CONSTANTES E O GRAU DE UM *place*

Por definição, o corpo de constantes de um corpo de funções $K \,/\, k$ é o conjunto dos elementos em K que são algébricos sobre k,

$$\widetilde{k} := \left\{x \in K \;\middle|\; x \text{ é algébrico sobre } k\right\} ,$$

que é um subcorpo de K.

Dizemos que k é o corpo de constantes completo de K se $\widetilde{k} = k$.

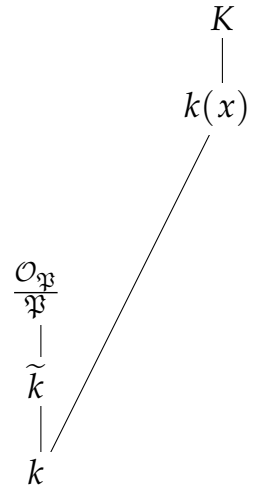
Exemplo 3.13. *O corpo de constantes completo do corpo de funções racionais $k(x) \,/\, k$ na variável x é k.*

(STICHTENOTH, 2009, p. 10).

Sejam $K \,/\, k$ um corpo de funções e $\widetilde{k}$ o corpo de constantes de K. Suponha que $\mathfrak{P}$ seja um *place* de K e que $\mathcal{O}_{\mathfrak{P}}$ seja o anel de valoração associado a $\mathfrak{P}$. O corpo residual $\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}$ pode ser visto como extensão finita de k e de $\widetilde{k}$ (STICHTENOTH, 2009, p. 7). Assim, podemos definir o grau de $\mathfrak{P}$ (sobre k) como

$$\deg_k(\mathfrak{P}) := \left[\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} : k \right] . \tag{12}$$

Figura 4. Num corpo de funções $K \,/\, k$, o corpo residual $\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}$ pode ser visto como uma extensão de k (para todo *place* $\mathfrak{P}$ em K).



3.4 DIVISORES

Seja $F \,/\, k$ um corpo de funções.

Sejam $\mathbb{P}(F)$ o conjunto dos *places* de F e $\mathrm{Div}(F) := \mathfrak{F}\big(\mathbb{P}(F)\big)$ o grupo dos divisores[1] de $F \,/\, k$.

Dado um divisor $\mathtt{D} \in \mathrm{Div}(F)$, podemos escrevê-lo como uma soma formal

$$\mathtt{D} = \sum_{\mathfrak{P} \in \mathbb{P}(F)} n_{\mathfrak{P}} \mathfrak{P} \qquad \text{com } n_{\mathfrak{P}} \in \mathbb{Z} \qquad \text{e} \qquad n_{\mathfrak{P}} = 0 \text{ para quase todo } \mathfrak{P} \in \mathbb{P}(F) \ . \tag{13}$$

O suporte de $\mathtt{D}$ é definido como

$$\mathrm{Supp}(\mathtt{D}) := \Big\{ \mathfrak{P} \in \mathbb{P}(F) \;\Big|\; n_{\mathfrak{P}} \neq 0 \Big\} \ , \tag{14}$$

e o grau de $\mathtt{D}$ (sobre k) é

$$\deg_k(\mathtt{D}) := \sum_{\mathfrak{P} \in \mathrm{Supp}(\mathtt{D})} n_{\mathfrak{P}} \cdot \deg_k(\mathfrak{P}) \ . \tag{15}$$

Para cada $\mathfrak{Q} \in \mathbb{P}(F)$, defina

$$\begin{aligned} v_{\mathfrak{Q}} : \mathrm{Div}(F) &\to \mathbb{Z} \\ \mathtt{D} = \sum_{\mathfrak{P} \in \mathbb{P}(F)} n_{\mathfrak{P}} \mathfrak{P} &\mapsto v_{\mathfrak{Q}}\left(\mathtt{D}\right) := n_{\mathfrak{Q}} \end{aligned} \tag{16}$$

(a função $v_{\mathfrak{Q}}$ definida em (16) não deve ser confundida com a valoração $v_{\mathfrak{P}}$ construída na Definição 3.7).

Uma ordem parcial em $\mathrm{Div}(F)$ pode ser definida como

$$\mathtt{D}_1 \leq \mathtt{D}_2 \qquad \Leftrightarrow \qquad v_{\mathfrak{P}}\left(\mathtt{D}_1\right) \leq v_{\mathfrak{P}}\left(\mathtt{D}_2\right) \ , \quad \forall\, \mathfrak{P} \in \mathbb{P}(F) \ .$$

Um divisor $\mathtt{D} \in \mathrm{Div}(F)$ será chamado de efetivo quando $0 \leq \mathtt{D}$.

3.4.1 Zeros e polos

Definição 3.14. *Se $z \in F$ e $\mathfrak{P} \in \mathbb{P}(F)$, dizemos que:*

1. *$\mathfrak{P}$ é um zero de z se $v_{\mathfrak{P}}(z) > 0$; e*
2. *$\mathfrak{P}$ é um polo de z se $v_{\mathfrak{P}}(z) < 0$.*

(STICHTENOTH, 2009, p. 7).

1 Se S é um conjunto não vazio, denotamos por $\mathfrak{F}(S)$ o grupo abeliano livre em S — cf. Dummit e Foote (2004, p. 355). Adotaremos a notação aditiva.

Exemplo 3.15 (o zero e o polo da variável em um corpo de funções racionais)**.** *Seja $k(x) \,/\, k$ o corpo de funções racionais na variável x.*

1. *O conjunto $\mathfrak{P}_x$ associado ao polinômio $p(x) = x$ (definido em (7)) é o único zero de x.*
2. *Analogamente, o* place *$\mathfrak{P}_\infty$ é o único polo de x.*

No Teorema de Aproximação, para

$$\begin{cases} g_1, g_2, \ldots, g_m \in \mathbb{Z}_+^* \,, \\ g_{m+1}, g_{m+2}, \ldots, g_n \in \mathbb{Z}_-^* \text{ e} \\ a_1 = \ldots = a_n = 0 \,, \end{cases}$$

podemos concluir que sempre existe uma função com zeros e polos preestabelecidos:

Corolário 3.16 (Teorema de Aproximação: escolha de função com zeros e polos prefixados)**.** *Sejam: $m \in \mathbb{N}$; $n > m$ inteiro; e $v_1, \ldots, v_n : K \to \mathbb{Z} \cup \{\infty\}$ valorações não triviais duas a duas não equivalentes em um corpo de funções $K \,/\, k$.*

Então existe $z \in K$ tal que

$$\begin{cases} v_i(z) > 0 & \text{para } i \in \{1, \ldots, m\} \\ v_j(z) < 0 & \text{para } j \in \{m+1, \ldots, n\} \end{cases} .$$

Todo ponto $z \in F \setminus k$ em um corpo de funções $F \,/\, k$ admite pelo menos um zero e um polo (STICHTENOTH, 2009, p. 8).

3.4.2 O grupo dos divisores principais

A partir dos zeros e dos polos, podemos considerar os seguintes divisores:

Definição 3.17. *Sejam: $x \in F \setminus \{0\}$; $\mathscr{Z} \subseteq \mathbb{P}(F)$ o conjunto de zeros de x; e $\mathscr{P} \subseteq \mathbb{P}(F)$ o conjunto de polos de x. Definimos:*

$$\begin{aligned} (x)_0 := (x)_0^F &:= \sum_{\mathfrak{P} \in \mathscr{Z}} v_{\mathfrak{P}}(x)\mathfrak{P} \,, \qquad \text{o } \underline{\text{divisor zero}} \text{ de } x \;; \\ (x)_\infty := (x)_\infty^F &:= \sum_{\mathfrak{P} \in \mathscr{P}} \big(-v_{\mathfrak{P}}(x)\big)\mathfrak{P} \,, \qquad \text{o } \underline{\text{divisor polo}} \text{ de } x \;; \qquad \text{e} \\ (x) := (x)^F &:= (x)_0 - (x)_\infty \,, \qquad \text{o } \underline{\text{divisor principal}} \text{ de } x \;. \end{aligned} \tag{17}$$

(STICHTENOTH, 2009, p. 16).

O divisor polo, o divisor zero e o divisor principal são divisores, pois todo ponto em um corpo de funções admite uma quantidade finita de zeros e de polos — cf. *Corollary* 1.3.4 no livro de Stichtenoth (2009, p. 15).

Teorema 3.18 (divisores principais têm grau zero)**.** *Para $x \in K \setminus k$,*

$$\deg\left((x)_0^F\right) = \deg\left((x)_\infty^F\right) = \left[K : k(x)\right] \ .$$

(VILLA-SALVADOR, 2006, p. 62; STICHTENOTH, 2009, p. 19).

Para $x, y \in F \setminus \{0\}$, temos pela definição de valoração que

$$(x \cdot y)^F = (x)^F + (y)^F \ . \tag{18}$$

Todo elemento $x \in F \setminus \{0\}$ de um corpo de funções $F \,/\, k$ que é constante satisfaz a equivalência

$$x \in k \qquad \Leftrightarrow \qquad (x)^F = 0 \tag{19}$$

(STICHTENOTH, 2009, p. 16).

O conjunto de divisores

$$\mathrm{Princ}(F) := \left\{ (x)^F \;\middle|\; x \in F \setminus \{0\} \right\} \tag{20}$$

é chamado de grupo dos divisores principais de $F \,/\, k$.

O grupo $\mathrm{Princ}(F)$ é um subgrupo de $\mathrm{Div}(F)$ (STICHTENOTH, 2009, p. 17).

O grupo quociente

$$\mathrm{Cl}(F) := \mathrm{Div}(F) \Big/ \mathrm{Princ}(F) \tag{21}$$

é chamado de grupo de classe dos divisores de $F \,/\, k$. Para um divisor $\mathtt{D} \in \mathrm{Div}(F)$, o elemento correspondente no grupo quociente $\mathrm{Cl}(F)$ é denotado por $[\mathtt{D}]$. Dizemos que $[\mathtt{D}]$ é a classe do divisor $\mathtt{D}$.

Dois divisores $\mathtt{D}, \mathtt{D}' \in \mathrm{Div}(F)$ são ditos equivalentes quando $[\mathtt{D}] = [\mathtt{D}']$; ou seja, existe $x \in F \setminus \{0\}$ tal que

$$\mathtt{D} = \mathtt{D}' + (x)^F \ . \tag{22}$$

Denotaremos $\mathtt{D} \sim \mathtt{D}'$ quando $\mathtt{D}$ for equivalente a $\mathtt{D}'$.

Esta relação é uma relação de equivalência (STICHTENOTH, 2009, p. 17).

No caso particular de igualdade $(x)^F = (y)^F$ entre dois divisores principais em $\mathrm{Div}(F)$ (para $x, y \in F$), temos pelas equações 18, 19 e 22 que

$$x = \alpha \cdot y \,, \tag{23}$$

para algum $\alpha \in k$.

3.5 O ESPAÇO DE RIEMANN-ROCH

Definição 3.19 (espaço de Riemann-Roch)**.** *Sejam: $F \,/\, k$ um corpo de funções; e $\mathtt{A} \in \mathrm{Div}(F)$ um divisor. Definimos o espaço de Riemann-Roch associado a $\mathtt{A}$ por*

$$\mathscr{L}_F(\mathtt{A}) := \left\{ x \in F \;\middle|\; (x)^F \geq -\mathtt{A} \right\} \cup \{0\} \,.$$

(STICHTENOTH, 2009, p. 17).

O espaço de Riemann-Roch é um espaço vetorial sobre k; a dimensão (sobre k) do espaço de Riemann-Roch de um divisor $\mathtt{A}$ será denotada da seguinte forma:

$$\ell(\mathtt{A}) := \ell_k(\mathtt{A}) := \dim_k\big(\mathscr{L}_F(\mathtt{A})\big) \,. \tag{24}$$

Observação 3.20. *Seja $\mathtt{A} \in \mathrm{Div}(F)$. Então $x \in \mathscr{L}_F(\mathtt{A})$ se, e somente se, $v_{\mathfrak{P}}(x) \geq -v_{\mathfrak{P}}(\mathtt{A})$ para todo $\mathfrak{P} \in \mathbb{P}(F)$.*

(STICHTENOTH, 2009, p. 17).

3.6 O GÊNERO DE UM CORPO DE FUNÇÕES

Proposição 3.21 (limitação)**.** *Existe uma constante $\gamma \in \mathbb{Z}$ tal que, para todo divisor $\mathtt{A} \in \mathrm{Div}(F)$, vale o seguinte:*

$$\deg_k(\mathtt{A}) - \ell(\mathtt{A}) \leq \gamma \,.$$

(STICHTENOTH, 2009, p. 21).

A cota mencionada na Proposição 3.21 sugere a definição de um importante invariante de um corpo de funções:

Definição 3.22 (gênero)**.** *O gênero de $F \,/\, k$ é definido por*

$$g_F := \max\left\{ \deg_k(\mathtt{A}) - \ell(\mathtt{A}) + 1 \;\middle|\; \mathtt{A} \in \mathrm{Div}(F) \right\}.$$

(STICHTENOTH, 2009, p. 22).

Observação 3.23. *O gênero de um corpo de funções é um número inteiro não negativo.*
(STICHTENOTH, 2009, p. 22).

Exemplo 3.24. *O corpo de funções racionais $k(x) \,/\, k$ tem gênero $g_{k(x)} = 0$.*
(STICHTENOTH, 2009, p. 23).

Observação 3.25. *Sejam $K_1 \,/\, k$ e $K_2 \,/\, k$ dois corpos de funções. Se $K_1 \subseteq K_2$, então*

$$g_{K_1} \leq g_{K_2}.$$

3.7 O TEOREMA DE RIEMANN-ROCH

Seja $F \,/\, k$ um corpo de funções.

Nesta seção, vamos enunciar o Teorema de Riemann-Roch, um resultado que relaciona, para um divisor arbitrário, o grau e a dimensão do espaço de Riemann-Roch com o gênero.

Para tanto, será necessário apresentar os conceitos de *adeles* e de divisores de Weil.

3.7.1 *Adeles*

Definição 3.26 (*adele*)**.** *Um* adele *de $F \,/\, k$ é uma aplicação*

$$\begin{aligned} \alpha : \; \mathbb{P}(F) &\to F \\ \mathfrak{P} &\mapsto \alpha(\mathfrak{P}) = \alpha_{\mathfrak{P}} \end{aligned}$$

tal que $\alpha(\mathfrak{P}) \in \mathcal{O}_{\mathfrak{P}}$, para quase todo $\mathfrak{P} \in \mathbb{P}(F)$.
(STICHTENOTH, 2009, p. 24).

Definição 3.27 (espaço dos *adeles*)**.** *O conjunto*

$$\mathcal{A}_F := \left\{ \alpha : \mathbb{P}(F) \to F \;\middle|\; \alpha \text{ é um adele de } F \,/\, k \right\}$$

é chamado de espaço dos adeles *de $F \,/\, k$.*
(STICHTENOTH, 2009, p. 24).

Podemos considerar um *adele* como um elemento $\alpha \in \prod_{\mathfrak{P}\in\mathbb{P}(F)} F$ no produto direto das cópias de F e, portanto, faz sentido usar uma notação análoga a de sequências: $\alpha = (\alpha_{\mathfrak{P}})_{\mathfrak{P}\in\mathbb{P}(F)}$.

O *adele* principal $\rho_x \in \prod_{\mathfrak{P}\in\mathbb{P}(F)} F$ de um elemento $x \in F$ é o *adele* cujos componentes são todos iguais a x:

$$\begin{array}{rccl} \rho_x : & \mathbb{P}(F) & \to & F \\ & \mathfrak{P} & \mapsto & \rho_x(\mathfrak{P}) = x \ . \end{array}$$

Seja $\mathcal{F}$ a coleção dos *adeles* principais de elementos de F. Temos uma imersão natural de F em $\mathcal{A}_F$, dada por

$$\begin{array}{rccl} \iota : & F & \hookrightarrow & \mathcal{F} \subseteq \mathcal{A}_F \\ & x & \mapsto & \rho_x \ . \end{array}$$

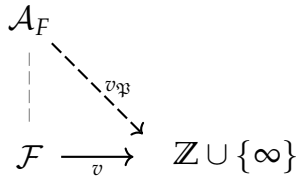
Para cada $\mathfrak{P} \in \mathbb{P}(F)$:

- existe uma função v de $\mathcal{F}$ em $\mathbb{Z} \cup \{\infty\}$ que tem essencialmente o mesmo comportamento da valoração $v_{\mathfrak{P}}$ dada na Definição 3.7; e
- a função v é naturalmente extensível a $\mathcal{A}_F$, definindo-se

$$\begin{array}{rccl} v_{\mathfrak{P}} : & \mathcal{A}_F & \to & \mathbb{Z} \cup \{\infty\} \\ & \alpha & \mapsto & v_{\mathfrak{P}}(\alpha) := v_{\mathfrak{P}}(\alpha_{\mathfrak{P}}) \end{array}$$

  (que denotaremos também por $v_{\mathfrak{P}}$, por abuso de notação).

Figura 5



Para $\mathtt{A} \in \mathrm{Div}(F)$, definimos

$$\mathcal{A}_F(\mathtt{A}) := \left\{ \alpha \in \mathcal{A}_F \;\middle|\; \forall\, \mathfrak{P} \in \mathbb{P}(F) \ : \quad v_{\mathfrak{P}}(\alpha) \geq -v_{\mathfrak{P}}(\mathtt{A}) \right\} .$$

Para cada divisor $\mathtt{A} \in \mathrm{Div}(F)$, o conjunto $\mathcal{A}_F(\mathtt{A})$ é um k-subespaço de $\mathcal{A}_F$ (STICHTENOTH, 2009, p. 24).

Observação 3.28 (corpos de funções isomorfos têm o mesmo gênero)**.** *O gênero de um corpo de funções $F \,/\, k$ pode ser calculado da seguinte forma:*

$$g_F = \dim_k \left(\frac{\mathcal{A}_F}{\mathcal{A}_F(0) + \mathcal{F}} \right) \tag{25}$$

— cf. Stichtenoth (2009, p. 25). Se $F_2 \,/\, k$ é um corpo de funções com $F_2 \cong F$, então temos os isomorfismos naturais

$$\mathcal{A}_{F_2} \cong \mathcal{A}_F\,, \qquad \mathcal{A}_{F_2}(0) \cong \mathcal{A}_F(0) \qquad e \qquad F_2 \cong \mathcal{F}\,.$$

Pela Equação 25, segue que $g_{F_2} = g_F$.

3.7.2 Diferenciais de Weil

Definição 3.29 (diferenciais de Weil)**.**

1. *Um diferencial de Weil de $F \,/\, k$ é uma aplicação k-linear*

$$\omega : \mathcal{A}_F \to k$$

que se anula em $\mathcal{A}_F(\mathtt{A}) + \mathcal{F}$, para algum divisor $\mathtt{A} \in \mathrm{Div}(F)$.

2. *Denotaremos por*

$$\Omega_F := \left\{ \omega : \mathcal{A}_F \to k \;\middle|\; \omega \text{ é um diferencial de Weil de } F \,/\, k \right\}$$

o módulo dos diferenciais de Weil de $F \,/\, k$.

3. *Para $\mathtt{A} \in \mathrm{Div}(F)$, defina*

$$\Omega_F(\mathtt{A}) := \left\{ \omega \in \Omega_F \;\middle|\; \omega \text{ anula-se em } \mathcal{A}_F(\mathtt{A}) + \mathcal{F} \right\}.$$

(STICHTENOTH, 2009, p. 27).

Seja $\omega \neq 0$ um diferencial de Weil de $F \,/\, k$. Defina

$$M(\omega) := \left\{ \mathtt{A} \in \mathrm{Div}(F) \;\middle|\; \omega \restriction_{\mathcal{A}_F(\mathtt{A})+\mathcal{F}} \equiv 0 \right\}.$$

Teorema 3.30 (existência e unicidade de divisores canônicos)**.** *Seja $\omega \in \Omega_F \setminus \{0\}$.*

Então existe um divisor unicamente determinado $\mathtt{W} \in M(\omega)$ tal que $\mathtt{A} \leq \mathtt{W}$, para todo $\mathtt{A} \in M(\omega)$.

(STICHTENOTH, 2009, p. 28).

O Teorema 3.30 sugere a seguinte definição:

Definição 3.31 (divisor canônico)**.**

1. *O divisor* $(\omega) \in \mathrm{Div}(F)$ *de um diferencial de Weil* $\omega \in \Omega_F \setminus \{0\}$ *é o divisor de* $F \,/\, k$ *unicamente determinado que satisfaz as seguintes propriedades:*
   a) ω *anula-se em* $\mathcal{A}_F\big((\omega)\big) + \mathcal{F}$*; e*
   b) *se* $\mathtt{A} \in M(\omega)$ *e* ω *anula-se em* $\mathcal{A}_F(\mathtt{A}) + \mathcal{F}$*, então* $\mathtt{A} \leq (\omega)$*.*
2. *Um divisor* $\mathtt{W} \in \mathrm{Div}(F)$ *é chamado de divisor canônico de* $F \,/\, k$ *se* $\mathtt{W} = (\omega)$*, para algum* $\omega \in \Omega_F$*.*

(STICHTENOTH, 2009, p. 29).

3.7.3 O Teorema de Riemann-Roch

Estamos em condições de enunciar o Teorema de Riemann-Roch, o teorema mais importante da Teoria de Corpos de Funções (STICHTENOTH, 2009, p. 30).

Teorema 3.32 (Teorema de Riemann-Roch)**.** *Seja* $\mathtt{W} \in \mathrm{Div}(F)$ *um divisor canônico de* $F \,/\, k$*. Então, para todo divisor* $\mathtt{A} \in \mathrm{Div}(F)$*,*

$$\ell(\mathtt{A}) = \deg_k(\mathtt{A}) + 1 - g_F + \ell(\mathtt{W} - \mathtt{A}) \,.$$

(STICHTENOTH, 2009, p. 30).

Para divisores com grau suficientemente grande, podemos calcular a dimensão do espaço de Riemann-Roch sem a necessidade de conhecermos um divisor canônico:

Teorema 3.33 (Teorema de Riemann)**.** *Seja* $F \,/\, k$ *um corpo de funções com gênero* g_F*. Então:*

1. *Para todo divisor* $\mathtt{A} \in \mathrm{Div}(F)$*,*

$$\ell(\mathtt{A}) \geq \deg_k(\mathtt{A}) + 1 - g_F \,. \tag{26}$$

2. *Existe um inteiro* $c_F = c$ *— dependendo apenas do corpo de funções* $F \,/\, k$ *— tal que*

$$\ell(\mathtt{A}) = \deg_k(\mathtt{A}) + 1 - g_F \,, \tag{27}$$

   sempre que $\deg_k(\mathtt{A}) \geq c$*.*

(STICHTENOTH, 2009, p. 23).

O teorema seguinte permite escolher a constante c no item 2 em função do gênero:

Teorema 3.34. *Se* $\mathtt{A} \in \mathrm{Div}(F)$ *é um divisor de* $F \mid k$ *de grau* $\deg_k(\mathtt{A}) \geq 2 \cdot g_F - 1$*, então*

$$\ell(\mathtt{A}) = \deg_k(\mathtt{A}) + 1 - g_F \,. \tag{28}$$

(STICHTENOTH, 2009, p. 31).

3.8 CONDIÇÕES SUFICIENTES PARA A EXISTÊNCIA DE UM ÚNICO POLO

Proposição 3.35 (elementos com um polo prefixado e único)**.** *Sejam* $\mathfrak{P} \in \mathbb{P}(F)$ *e* $n \in \mathbb{N}$ *tal que* $n \geq 2 \cdot g_F$*. Então existe um elemento* $x \in F$ *com divisor polo*

$$(x)_\infty^F = n\mathfrak{P} \,.$$

(STICHTENOTH, 2009, p. 34).

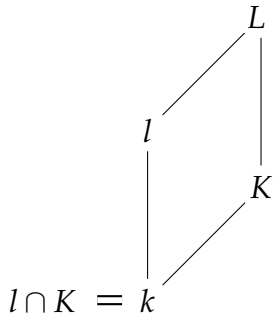
3.9 EXTENSÕES DE CORPOS DE FUNÇÕES

Definição 3.36 (extensão de corpos de funções)**.** *Sejam* $K \mid k$ *e* $L \mid l$ *dois corpos de funções. Dizemos que* $L \mid l$ *é uma extensão de* $K \mid k$ *(ou que* $L \mid K$ *é uma extensão de corpos de funções) quando:*

1. $L \supseteq K$*; e*
2. $l \cap K = k$*.*

(VILLA-SALVADOR, 2006, p. 113).

Figura 6. Uma extensão de corpos de funções.



Definição 3.37. *Sejam $F' \,/\, k'$ e $F \,/\, k$ dois corpos de funções.*

1. *Diremos que $F' \,/\, k'$ é uma extensão algébrica de $F \,/\, k$ — ou que $F' \,|\, F$ é uma extensão algébrica (de corpos de funções) — quando F' for uma extensão algébrica de F e $k' \supseteq k$.*
2. *Uma extensão algébrica $F' \,/\, k'$ de $F \,/\, k$ é chamada de extensão finita se $\left[F' : F\right] < \infty$.*

(STICHTENOTH, 2009, p. 68).

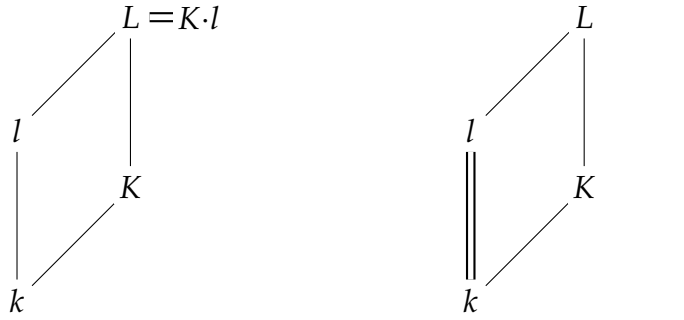
Diremos que $F' \,/\, k'$ é uma extensão separável (resp. normal) de $F \,/\, k$ quando $F' \,|\, F$ for separável (resp. normal).

Definição 3.38. *Seja $L \,/\, l$ uma extensão de $K \,/\, k$. Dizemos que*

1. *$L \,|\, K$ é uma extensão constante quando $L = K{\cdot}l$; e*
2. *$L \,|\, K$ é uma extensão geométrica quando $l = k$.*

(VILLA-SALVADOR, 2006, p. 126).

Figura 7. Ilustração de uma extensão constante e uma extensão geométrica.



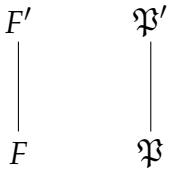
(extensão constante) (extensão geométrica)

Definição 3.39 (extensão de *places*)**.** *Sejam: $F \mid k$ um corpo de funções; $F' \mid k'$ uma extensão algébrica de $F \mid k$; $\mathfrak{P} \in \mathbb{P}(F)$; e $\mathfrak{P}' \in \mathbb{P}(F')$.*

Diremos que $\mathfrak{P}'$ é um place *sobre $\mathfrak{P}$ (ou que $\mathfrak{P}'$ está sobre $\mathfrak{P}$) quando $\mathfrak{P}' \supseteq \mathfrak{P}$. Também dizemos que $\mathfrak{P}'$ é uma extensão de $\mathfrak{P}$, e escrevemos $\mathfrak{P}' \mid \mathfrak{P}$.*

(STICHTENOTH, 2009, p. 69).

Figura 8. Ilustração para a Definição 3.39.



Os dois resultados seguintes respondem à dúvida suscitada pela Figura 2 do capítulo de Introdução.

Proposição 3.40. *Sejam: $F' \mid k'$ uma extensão algébrica de $F \mid k$; $\mathfrak{P}$ um* place *de F; e $\mathfrak{P}'$ um* place *de F'.*

1. *As seguintes afirmações são equivalentes:*
   a) $\mathfrak{P}' \mid \mathfrak{P}$;
   b) $\mathcal{O}_{\mathfrak{P}} \subseteq \mathcal{O}_{\mathfrak{P}'}$; *e*
   c) *existe um inteiro $e \geq 1$ tal que*

$$v_{\mathfrak{P}'}(x) = e \cdot v_{\mathfrak{P}}(x) \qquad \text{para todo } x \in F \ .$$

2. *Se $\mathfrak{P}' \mid \mathfrak{P}$, então:*
   a) $\mathfrak{P} = \mathfrak{P}' \cap F$; *e*
   b) $\mathcal{O}_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{P}'} \cap F$.

(STICHTENOTH, 2009, p. 69).

Por conta do item 2 da Proposição 3.40, o *place* $\mathfrak{P}$ também é chamado de restrição de $\mathfrak{P}'$ a F (STICHTENOTH, 2009, p. 69).

Proposição 3.41 (imersão de corpos residuais)**.** *Sejam: $K \mid k$ um corpo de funções; $L \mid l$ uma extensão de $K \mid k$; $\mathfrak{p}$ um* place *de K; e $\mathfrak{P}$ um* place *de L sobre $\mathfrak{p}$. Então existe uma imersão natural*

$$\iota : \frac{\mathcal{O}_{\mathfrak{p}}}{\mathfrak{p}} \hookrightarrow \frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} \ .$$

(VILLA-SALVADOR, 2006, p. 114).

Definição 3.42. *Sejam: $F \mid k$ um corpo de funções; $F' \mid k'$ uma extensão algébrica de $F \mid k$; $\mathfrak{P} \in \mathbb{P}(F)$; e $\mathfrak{P}' \in \mathbb{P}\left(F'\right)$ sobre $\mathfrak{P}$.*

1. *a) O inteiro $e\left(\mathfrak{P}' \,\middle|\, \mathfrak{P}\right) := e$ com*

$$v_{\mathfrak{P}'}(x) = e \cdot v_{\mathfrak{P}}(x) \ , \qquad \text{para todo } x \in F \ ,$$

   é chamado de índice de ramificação de $\mathfrak{P}'$ sobre $\mathfrak{P}$.

   b) A extensão $\mathfrak{P}' \mid \mathfrak{P}$ é ramificada quando $e\left(\mathfrak{P}' \,\middle|\, \mathfrak{P}\right) > 1$.

   c) A extensão $\mathfrak{P}' \mid \mathfrak{P}$ é não ramificada quando $e\left(\mathfrak{P}' \,\middle|\, \mathfrak{P}\right) = 1$.

2. *O número*

$$f\left(\mathfrak{P}' \,\middle|\, \mathfrak{P}\right) := \left[\frac{\mathcal{O}_{\mathfrak{P}'}}{\mathfrak{P}'} : \frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}\right]$$

   é chamado de grau relativo de $\mathfrak{P}'$ sobre $\mathfrak{P}$.

(STICHTENOTH, 2009, p. 71).

Definição 3.43. *Sejam $F' \,\middle|\, F$ uma extensão algébrica de corpos de funções e $\mathfrak{P} \in \mathbb{P}(F)$.*

1. *a) Dizemos que $\mathfrak{P}$ é ramificado em $F' \,\middle|\, F$ se existir pelo menos um* place *$\mathfrak{P}' \in \mathbb{P}\left(F'\right)$ sobre $\mathfrak{P}$ tal que $\mathfrak{P}' \mid \mathfrak{P}$ é ramificada.*

   b) Dizemos que $\mathfrak{P}$ é não ramificado em $F' \,\middle|\, F$ quando $\mathfrak{P}$ não for ramificado em $F' \,\middle|\, F$. Isto é,

$$\forall\, \mathfrak{P}' \in \mathbb{P}\left(F'\right) \text{ com } \mathfrak{P}' \mid \mathfrak{P} \ : \qquad e\left(\mathfrak{P}' \,\middle|\, \mathfrak{P}\right) = 1 \ .$$

2. *a) Dizemos que $F' \,\middle|\, F$ é ramificada se pelo menos um* place *$\mathfrak{P} \in \mathbb{P}(F)$ é ramificado em $F' \,\middle|\, F$.*

   b) Dizemos que $F' \,\middle|\, F$ é não ramificada quando não for ramificada. Isto é,

$$\forall\, \mathfrak{P} \in \mathbb{P}(F)\ \forall\, \mathfrak{P}' \in \mathbb{P}\left(F'\right) \text{ com } \mathfrak{P}' \mid \mathfrak{P} \ : \qquad e\left(\mathfrak{P}' \,\middle|\, \mathfrak{P}\right) = 1 \ .$$

(STICHTENOTH, 2009, p. 105).

Nas condições da Definição 3.43, diremos que $\mathfrak{P}' \in \mathbb{P}(F')$ é ramificado (resp. não ramificado) em $F' \mid F$ quando a extensão de *places* $\mathfrak{P}' \mid \mathfrak{P}' \cap F$ for ramificada (resp. não ramificada) em $F' \mid F$.

Proposição 3.44 ("equivalências de finitudes"). *Sejam $K \mid k$ um corpo de funções e $L \mid l$ uma extensão de $K \mid k$. As seguintes condições são equivalentes.*

1. $\left[l : k\right] < \infty$.
2. $\left[L : K\right] < \infty$.
3. $\left[\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} : \frac{\mathcal{O}_{\mathfrak{p}}}{\mathfrak{p}}\right] < \infty$, *para todo* place $\mathfrak{p} \in \mathbb{P}(K)$ *e para todo* place $\mathfrak{P} \in \mathbb{P}(L)$ *sobre* $\mathfrak{p}$.

(VILLA-SALVADOR, 2006, p. 114).

Proposição 3.45 ("equivalências das propriedades algébricas"). *Sejam $K \mid k$ um corpo de funções e $L \mid l$ uma extensão de $K \mid k$. As seguintes condições são equivalentes.*

1. *$l \mid k$ é algébrica.*
2. *$L \mid K$ é algébrica.*
3. $\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} \,\middle|\, \frac{\mathcal{O}_{\mathfrak{p}}}{\mathfrak{p}}$ *é algébrica, para todo* place $\mathfrak{p} \in \mathbb{P}(K)$ *e para todo* place $\mathfrak{P} \in \mathbb{P}(L)$ *sobre* $\mathfrak{p}$.

(VILLA-SALVADOR, 2006, p. 115).

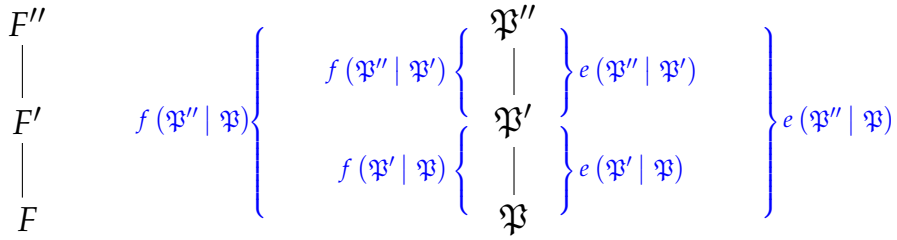
Não temos um resultado análogo às proposições 3.44 e 3.45 para as propriedades de separabilidade e de normalidade.

Proposição 3.46 (transitividade). *Sejam: $F \mid k$ um corpo de funções; $F' \mid k'$ uma extensão algébrica de $F \mid k$; $F'' \mid k''$ uma extensão algébrica de $F' \mid k'$; $\mathfrak{P} \in \mathbb{P}(F)$; $\mathfrak{P}' \in \mathbb{P}(F')$ um* place *sobre $\mathfrak{P}$; e $\mathfrak{P}'' \in \mathbb{P}(F'')$ uma extensão de $\mathfrak{P}'$. Então*

1. $e\left(\mathfrak{P}'' \mid \mathfrak{P}\right) = e\left(\mathfrak{P}'' \mid \mathfrak{P}'\right) \cdot e\left(\mathfrak{P}' \mid \mathfrak{P}\right)$
2. $f\left(\mathfrak{P}'' \mid \mathfrak{P}\right) = f\left(\mathfrak{P}'' \mid \mathfrak{P}'\right) \cdot f\left(\mathfrak{P}' \mid \mathfrak{P}\right)$

(STICHTENOTH, 2009, p. 71).

Figura 9. Ilustração da transitividade do grau relativo e do índice de ramificação.



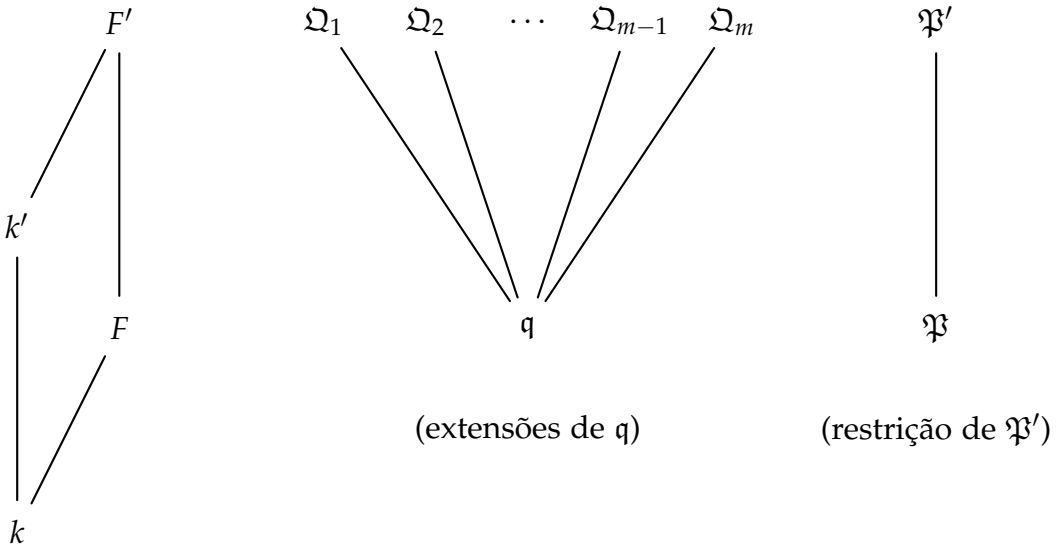
Proposição 3.47. *Sejam $F \,/\, k$ um corpo de funções e $F' \,/\, k'$ uma extensão algébrica de $F \,/\, k$.*

(restrição) Para cada place $\mathfrak{P}' \in \mathbb{P}(F')$ *existe exatamente um* place $\mathfrak{P} \in \mathbb{P}(F)$ *tal que* $\mathfrak{P}'|\mathfrak{P}$. *Especificamente,* $\mathfrak{P} = \mathfrak{P}' \cap F$.

(extensão) Reciprocamente, todo place $\mathfrak{q} \in \mathbb{P}(F)$ *tem pelo menos um, mas apenas um número finito de extensões* $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_m \in \mathbb{P}(F')$.

(STICHTENOTH, 2009, p. 71).

Figura 10. Restrição e extensões de *places*.



Teorema 3.48 (Igualdade Fundamental)**.** *Sejam: $F \,/\, k$ um corpo de funções; $F' \,/\, k'$ uma extensão finita de $F \,/\, k$; $\mathfrak{P} \in \mathbb{P}(F)$; e $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_m\} \subseteq \mathbb{P}\left(F'\right)$ a coleção de todos os* places *de F' sobre $\mathfrak{P}$. Então*

$$\sum_{i=1}^{m} e\left(\mathfrak{P}_i \mid \mathfrak{P}\right) \cdot f\left(\mathfrak{P}_i \mid \mathfrak{P}\right) = \left[F' : F\right] .$$

(STICHTENOTH, 2009, p. 74).

Corolário 3.49 (limitação pelo grau)**.** *Com as notações acima, temos o seguinte.*

1. $m \leq \left[L : K\right]$.
2. *Para $i \in \{1, 2, \ldots, m\}$, temos que*
   a) $f\left(\mathfrak{P}_i \mid \mathfrak{P}\right) \leq \left[L : K\right]$; *e*
   b) $e\left(\mathfrak{P}_i \mid \mathfrak{P}\right) \leq \left[L : K\right]$.

(VILLA-SALVADOR, 2006, p. 117).

Definição 3.50. *Sejam $F' \,/\, k'$ uma extensão finita de $F \,/\, k$ de grau $n := \left[F' : F\right]$ e $\mathfrak{P} \in \mathbb{P}(F)$.*

1. *Dizemos que $\mathfrak{P}$ <u>decompõe-se completamente</u> em $F' \,\big|\, F$ se existirem exatamente n* places *distintos $\mathfrak{P}' \in \mathbb{P}\left(F'\right)$ com $\mathfrak{P}' \mid \mathfrak{P}$.*
2. *Dizemos que $\mathfrak{P}$ é <u>totalmente ramificado</u> em $F' \,\big|\, F$ se existir um* place *$\mathfrak{P}' \in \mathbb{P}\left(F'\right)$ com*

$$\mathfrak{P}' \mid \mathfrak{P} \qquad e \qquad e\left(\mathfrak{P}' \,\middle|\, \mathfrak{P}\right) = n .$$

(STICHTENOTH, 2009, p. 75).

Observação 3.51. *Pela Igualdade Fundamental,*

- *um* place *$\mathfrak{P} \in \mathbb{P}(F)$ decompõe-se completamente em $F' \,\big|\, F$ se, e somente se, $e\left(\mathfrak{P}' \,\middle|\, \mathfrak{P}\right) = f\left(\mathfrak{P}' \,\middle|\, \mathfrak{P}\right) = 1$ para todo* place *$\mathfrak{P}' \in \mathbb{P}\left(F'\right)$ sobre $\mathfrak{P}$ (STICHTENOTH, 2009, p. 75), e*
- *se $\mathfrak{P}$ é totalmente ramificado em $F' \,\big|\, F$, então existe exatamente um* place *$\mathfrak{P}' \in \mathbb{P}\left(F'\right)$ com $\mathfrak{P}' \mid \mathfrak{P}$ (STICHTENOTH, 2009, p. 75).*

Observação 3.52. *Sejam: $F' \,\big|\, F$ uma extensão de corpos de funções; M um corpo intermediário de $F' \,\big|\, F$; e $\mathfrak{P} \in F$. Se $\mathfrak{P}$ decompõe-se completamente em $F' \,\big|\, F$, então ocorre decomposição completa de $\mathfrak{P}$ também nas extensões intermediárias $F' \,\big|\, M$ e $M \,|\, F$.*

3.10 CORPOS DE FUNÇÕES SEPARAVELMENTE GERADOS

Definição 3.53 (base separante)**.** *Seja $F \mid E$ uma extensão de corpo.*

- *Dizemos que $F \mid E$ é separavelmente gerada quando existe uma base de transcendência $\mathcal{B} := \{\alpha_i\}_{i\in I}$ de F sobre E tal que $F \mid E(\mathcal{B})$ é algébrico e separável.*
- *A base de transcendência $\mathcal{B}$ é chamada de base separante para F sobre E.*

(VILLA-SALVADOR, 2006, p. 244).

No caso em que $\mathcal{B} = \{x\}$ é uma base separante para algum $x \in K$, dizemos que x é um elemento separante para $K \,/\, k$ (STICHTENOTH, 2009, p. 30).

Teorema 3.54. *Sejam: $K \,/\, k$ um corpo de funções; $L = K{\cdot}l$ uma extensão constante; $\mathfrak{p} \in \mathbb{P}(K)$; e $\mathfrak{P} \in \mathbb{P}(L)$ um* place *sobre $\mathfrak{p}$. Suponha que l é uma extensão separavelmente gerada de k. Então*

$$\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} = \frac{\mathcal{O}_{\mathfrak{p}}}{\mathfrak{p}}{\cdot}l\,.$$

(VILLA-SALVADOR, 2006, p. 262).

3.11 SEPARABILIDADE DE *places*

Seja $E \mid F$ uma extensão de corpo.

Dizemos que

$$\mathrm{sc}_E(F) := \left\{ \alpha \in E \;\middle|\; \alpha \text{ é separável sobre } F \right\}$$

é o fecho separável de F sobre E.

Dois conceitos conhecidos são o grau de inseparabilidade e o grau de separabilidade de E sobre F:

$$[E : F]_{\mathbf{i}} := \Big[E : \mathrm{sc}_E(F)\Big] \qquad \text{e} \qquad [E : F]_{\mathbf{s}} := \Big[\mathrm{sc}_E(F) : F\Big]\,,$$

respectivamente (BASTIDA, 1984, p. 158).

Para extensões de corpos residuais, reservamos notações especiais:

Definição 3.55 (separabilidade de *places*)**.** *Sejam: $K \mid k$ um corpo de funções; $L \mid l$ uma extensão finita de $K \mid k$; $\mathfrak{p}$ um* place *de K; e $\mathfrak{P} \supseteq \mathfrak{p}$ um* place *de L.*

1. *Defina*
$$f(\mathfrak{P} \mid \mathfrak{p})_{\mathbf{i}} := \left[\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} : \frac{\mathcal{O}_{\mathfrak{p}}}{\mathfrak{p}} \right]_{\mathbf{i}} \tag{29}$$
e
$$f(\mathfrak{P} \mid \mathfrak{p})_{\mathbf{s}} := \left[\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} : \frac{\mathcal{O}_{\mathfrak{p}}}{\mathfrak{p}} \right]_{\mathbf{s}}. \tag{30}$$
2. *Se $f(\mathfrak{P} \mid \mathfrak{p})_{\mathbf{i}} = 1$, diremos que $\mathfrak{P}$ é separável — ou que $\mathfrak{P} \mid \mathfrak{p}$ é separável.*
3. *Se $f(\mathfrak{P} \mid \mathfrak{p})_{\mathbf{i}} > 1$, diremos que $\mathfrak{P}$ é inseparável — ou que $\mathfrak{P} \mid \mathfrak{p}$ é inseparável.*
4. *Se $f(\mathfrak{P} \mid \mathfrak{p})_{\mathbf{i}} = f(\mathfrak{P} \mid \mathfrak{p})$, diremos que $\mathfrak{P}$ é puramente inseparável — ou que $\mathfrak{P} \mid \mathfrak{p}$ é puramente inseparável.*

(VILLA-SALVADOR, 2006, p. 119).

Observação 3.56. *Sejam $F' \,\big|\, F$ uma extensão finita de corpos de funções e $\mathfrak{P} \in \mathbb{P}(F)$. Se $\mathfrak{P}$ é totalmente ramificado em $F' \,\big|\, F$, então existe um único* place *$\mathfrak{P}' \in \mathbb{P}(F')$ tal que $\mathfrak{P}' \mid \mathfrak{P}$ (Observação 3.51). Pela Igualdade Fundamental, este único* place *deve ter grau relativo $f(\mathfrak{P}' \,\big|\, \mathfrak{P}) = 1$. Portanto, $\mathfrak{P}' \mid \mathfrak{P}$ é separável nestas condições.*

As seguintes propriedades serão utilizadas nesta dissertação sem maiores comentários.

- Se $E \mid F$ é uma extensão finita, então as seguintes propriedades são equivalentes:
  - $E \mid F$ é separável;
  - $[E : F]_{\mathbf{i}} = 1$;
  - $E \mid F$ é separavelmente gerado; e
  - $[E : F]_{\mathbf{s}} = \Big[E : F\Big]$.

  Sugerimos os livros de Bastida (1984, p. 158) e Roman (2006, p. 80) para demonstrações.
- Se $L \mid K$ é uma extensão finita, então $\Big[L : K\Big] = [L : K]_{\mathbf{i}} \cdot [L : K]_{\mathbf{s}}$ (BASTIDA, 1984, p. 158).
- (Transitividade) se $M \mid L$ e $L \mid K$ são extensões finitas, então
$$[M : K]_{\mathbf{i}} = [M : L]_{\mathbf{i}} \cdot [L : K]_{\mathbf{i}} \qquad \text{e} \qquad [M : K]_{\mathbf{s}} = [M : L]_{\mathbf{s}} \cdot [L : K]_{\mathbf{s}}.$$
  Para uma prova, recomendamos o livro de Bastida (1984, p. 161).

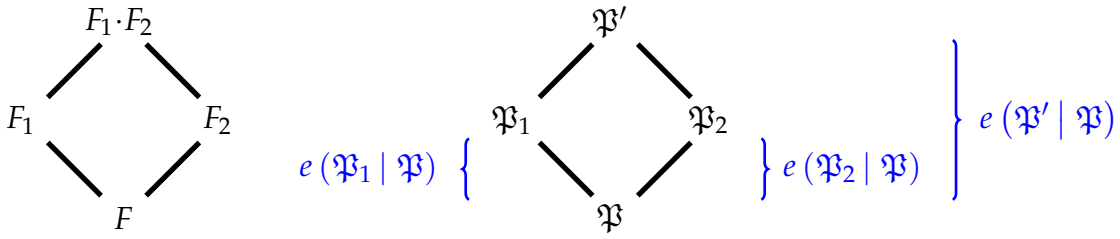
3.12 RAMIFICAÇÃO E DECOMPOSIÇÃO EM COMPÓSITO DE CORPOS DE FUNÇÕES

Nesta seção, veremos como algumas propriedades de *places* em um corpo de funções podem ser "transferidas" para *places* do compósito.

Teorema 3.57 (Lema de Abhyankar). *Sejam: $F' \mid F$ uma extensão finita separável de corpos de funções sobre k; $\mathfrak{P} \in \mathbb{P}(F)$; $\mathfrak{P}' \in \mathbb{P}(F')$ uma extensão de $\mathfrak{P}$; e $\mathfrak{P}_i := \mathfrak{P}' \cap F_i$ para $i \in \{1,2\}$.*

Suponha que $F' = F_1 \cdot F_2$ é o compósito de dois corpos intermediários de $F' \mid F$.

Figura 11. Ilustração para o Lema de Abhyankar.



Suponha que

$$e(\mathfrak{P}_i \mid \mathfrak{P}) > 1 \qquad e \qquad \operatorname{char}(k) \nmid e(\mathfrak{P}_i \mid \mathfrak{P}) ,$$

para $i = 1$ ou $i = 2$. Então

$$e(\mathfrak{P}' \mid \mathfrak{P}) = \operatorname{mmc}\{e(\mathfrak{P}_1 \mid \mathfrak{P}), e(\mathfrak{P}_2 \mid \mathfrak{P})\} .$$

(STICHTENOTH, 2009, p. 137).

Uma consequência do Lema de Abhyankar é o seguinte corolário:

Corolário 3.58 (ramificação em compósitos). *Sejam $F' \mid F$ uma extensão finita separável de corpos de funções e $\mathfrak{P} \in \mathbb{P}(F)$.*

1. *Suponha que $F' = F_1 \cdot F_2$ é o compósito de dois corpos intermediários de $F' \mid F$.*

   Se $\mathfrak{P}$ é não ramificado em $F_1 \mid F$ e em $F_2 \mid F$, então $\mathfrak{P}$ é não ramificado em $F' \mid F$.

2. *Suponha que F_0 é um corpo intermediário de $F' \mid F$ tal que $F' \mid F$ é o fecho galoisiano de $F_0 \mid F$.*

   Se $\mathfrak{P}$ é não ramificado em $F_0 \mid F$, então $\mathfrak{P}$ é não ramificado em $F' \mid F$.

(STICHTENOTH, 2009, p. 139).

Proposição 3.59 (decomposição em compósitos)**.** *Sejam:* $F' \mid F$ *uma extensão finita separável de corpos de funções;* F_1, F_2 *corpos intermediários de* $F' \mid F$ *tais que* $F' = F_1 \cdot F_2$*; e* $\mathfrak{P}$ *um* place *de* F*.*

1. *Suponha que* $\mathfrak{P}$ *decompõe-se completamente na extensão* $F_1 \mid F$*.*

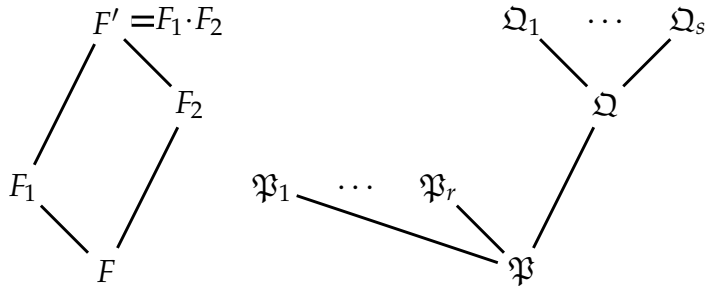
   Então todo place $\mathfrak{Q} \in \mathbb{P}(F_2)$ *sobre* $\mathfrak{P}$ *decompõe-se completamente em* $F' \mid F_2$*.*

2. *Suponha que* $\mathfrak{P} \in \mathbb{P}(F)$ *decompõe-se completamente em* $F_1 \mid F$ *e em* $F_2 \mid F$*.*

   Então $\mathfrak{P}$ *decompõe-se completamente em* $F' \mid F$*.*

(STICHTENOTH, 2006, p. 141).

Figura 12. Ilustração para o item 1 da Proposição 3.59. A decomposição completa de $\mathfrak{P}$ (em $r := \left[F_1 : F\right]$ *places* distintos) induz a decomposição completa de $\mathfrak{Q} \in \mathbb{P}(F_2)$ sobre $\mathfrak{P}$ em $s := \left[F' : F_2\right]$ *places* distintos.



3.13 DECOMPOSIÇÃO COMPLETA EM EXTENSÕES GALOISIANAS DE CORPOS DE FUNÇÕES

Lema 3.60. *Sejam:* $F_0 \mid F$ *uma extensão finita separável dos corpos de funções;* $F' \supseteq F_0$ *o fecho galoisiano de* $F_0 \mid F$*; e* $\mathfrak{P} \in \mathbb{P}(F)$ *um* place *que se decompõe completamente em* $F_0 \mid F$*.*

Então $\mathfrak{P}$ *decompõe-se completamente em* $F' \mid F$*.*

(STICHTENOTH, 2009, p. 141).

3.14 PROPRIEDADES DA CONORMA

Definição 3.61 (conorma). *Seja $F' \,/\, k'$ uma extensão algébrica de $F \,/\, k$. Para um* place *$\mathfrak{P} \in \mathbb{P}(F)$, dizemos que*

$$\mathrm{Con}_{F'|F}(\mathfrak{P}) := \sum_{\substack{\mathfrak{P}' \in \mathbb{P}(F') \\ \mathfrak{P}'|\mathfrak{P}}} e\left(\mathfrak{P}' \mid \mathfrak{P}\right)\mathfrak{P}' \tag{31}$$

é a conorma de $\mathfrak{P}$ com relação a $F' \mid F$.

(STICHTENOTH, 2009, p. 72).

A aplicação conorma é extensível a um homomorfismo de $\mathrm{Div}(F)$ em $\mathrm{Div}(F')$: para um divisor $\mathtt{D} = \sum_{\mathfrak{P} \in \mathbb{P}(F)} n_{\mathfrak{P}}\mathfrak{P} \in \mathrm{Div}(F)$, definimos

$$\mathrm{Con}_{F'|F}(\mathtt{D}) := \mathrm{Con}_{F'|F}\left(\sum n_{\mathfrak{P}}\mathfrak{P}\right) := \sum n_{\mathfrak{P}}\mathrm{Con}_{F'|F}(\mathfrak{P}) \,. \tag{32}$$

Observação 3.62 (transitividade da conorma). *Seja $F'' \supseteq F' \supseteq F$ uma torre de corpos de funções. Uma consequência imediata do item 1 da Proposição 3.46 é a fórmula*

$$\mathrm{Con}_{F''|F}(\mathtt{A}) = \mathrm{Con}_{F''|F'}\left(\mathrm{Con}_{F'|F}(\mathtt{A})\right) ,$$

válida para todo divisor $\mathtt{A} \in \mathrm{Div}(F)$.

(STICHTENOTH, 2009, p. 72).

Proposição 3.63 (conorma de divisores principais). *Sejam: $F \,/\, k$ um corpo de funções; $F' \,/\, k'$ uma extensão algébrica de $F \,/\, k$; $x \in F \setminus \{0\}$; e*

$$(x)_0^F \,, \qquad (x)_\infty^F \,, \qquad (x)^F$$

(resp. $(x)_0^{F'}$, $(x)_\infty^{F'}$, $(x)^{F'}$) o divisor zero, o divisor polo, e o divisor principal de x em $\mathrm{Div}(F)$ (resp. em $\mathrm{Div}(F')$). Então:

1. $\mathrm{Con}_{F'|F}\left((x)_0^F\right) = (x)_0^{F'}$;
2. $\mathrm{Con}_{F'|F}\left((x)_\infty^F\right) = (x)_\infty^{F'}$; *e*
3. $\mathrm{Con}_{F'|F}\left((x)^F\right) = (x)^{F'}$.

(STICHTENOTH, 2009, p. 73).

3.15 O DIFERENTE DE UMA EXTENSÃO DE CORPO

Nesta seção, apresentamos a definição do diferente, um divisor efetivo associado a uma extensão de corpo.

3.15.1 O traço de uma extensão de corpo finita

Sejam $F \,/\, k$ um corpo de funções e $F' \,/\, k'$ uma extensão de $F \,/\, k$. Suponha que $n := \left[F' : F\right] < \infty$, $F' \,\big|\, F$ é separável e o corpo de constantes de $F' \,/\, k'$ é k'.

Para cada $x \in F'$, podemos definir a aplicação

$$\begin{array}{rccc} r_x : & F' & \to & F' \\ & y & \mapsto & y \cdot x \,. \end{array}$$

Se considerarmos F' como um espaço vetorial (de dimensão finita) sobre F, então podemos ver r_x como uma transformação linear sobre F. Se $\alpha = (u_i)_{i=1}^n$ é uma base para F' sobre F, então r_x admite uma representação na forma de uma matriz de transformação $[r_x]_\alpha^\alpha = \left[a_{ij}\right] \in M_{n\times n}(F)$, em que

$$r_x(u_i) = u_i \cdot x = \sum_{j=1}^{n} a_{ij} \cdot u_j \,, \qquad \forall\, i \in \{1, \ldots, n\}$$

(JANUSZ, 1996, p. 19).

O traço de uma transformação linear é independente da escolha de base. Isso motiva a seguinte definição:

Definição 3.64. *Sejam: F um corpo; e F' uma extensão finita de F.*

O traço de F' sobre F é a aplicação

$$\begin{array}{rccc} T_{F'\big|F} : & F' & \to & F \\ & x & \mapsto & T_{F'\big|F}(x) := \mathrm{Tr}\,(r_x) = \mathrm{tr}\big([r_x]_\alpha^\alpha\big) \,, \end{array}$$

em que $\mathrm{Tr}\,(T)$ indica o traço de uma transformação linear T e $\mathrm{tr}(M)$ é o traço de uma matriz M de ordem n (na base α).

(JANUSZ, 1996, p. 20; STICHTENOTH, 2009, p. 332).

Proposição 3.65 (base dual com relação ao traço)**.** *Sejam: $M \,|\, L$ uma extensão de corpo finita e separável; e $\beta := \{z_1, \ldots, z_n\}$ uma base de M sobre L. Então:*

1. *Existem elementos unicamente determinados* $z_1^*, \ldots, z_n^* \in M$ *tais que*

$$T_{M|L}\left(z_i \cdot z_j^*\right) = \delta_{ij}\,, \qquad \forall\, i\,,\ j \in \{1, 2, \ldots, n\}\,,$$

em que δ_{ij} *indica o símbolo de Kronecker.*

2. *O conjunto* $\beta^* := \{z_1^*, \ldots, z_n^*\}$ *é uma base de* $M \mid L$.

(JANUSZ, 1996, p. 25; STICHTENOTH, 2009, p. 82).

Definição 3.66 (base dual)**.** *A base* β^* *construída na Proposição 3.65 é chamada de base dual de* $\beta := \{z_1, \ldots, z_n\}$ *(em relação ao traço).*
(JANUSZ, 1996, p. 25; STICHTENOTH, 2009, p. 82).

3.15.2 Bases inteiras

Se A, B são anéis comutativos com identidade tais que $A \subseteq B$ e a identidade 1 de B é a mesma da de A, dizemos que o conjunto

$$\overline{A}^B := \left\{ r \in B \;\middle|\; \exists\, f \in A\,[X] \text{ mônico: } f(r) = 0 \right\}$$

de B é o fecho inteiro de A em B — cf. Atiyah e MacDonald (1969, p. 60).

Teorema 3.67 (descrição do fecho inteiro com bases inteiras)**.** *Sejam:* $F \mid k$ *um corpo de funções;* $F' \mid F$ *uma extensão finita separável; e* $\mathfrak{P} \in \mathbb{P}(F)$*. Então temos os seguintes fatos.*

1. *O fecho inteiro de* $\mathcal{O}_{\mathfrak{P}}$ *em* F' *é*

$$\overline{\mathcal{O}_{\mathfrak{P}}}^{F'} = \bigcap_{\substack{\mathfrak{P}' \mid \mathfrak{P} \\ \mathfrak{P}' \in \mathbb{P}(F')}} \mathcal{O}_{\mathfrak{P}'}\,.$$

2. *Existe uma base* $\eta := \{u_1, \ldots, u_n\}$ *de* $F' \mid F$ *tal que*

$$\overline{\mathcal{O}_{\mathfrak{P}}}^{F'} = \sum_{i=1}^{n} \mathcal{O}_{\mathfrak{P}} u_i\,.$$

(STICHTENOTH, 2009, p. 85).

Uma base com a propriedade do item 2 do Teorema 3.67 é chamada de base inteira de $\overline{\mathcal{O}_{\mathfrak{P}}}^{F'}$ sobre $\mathcal{O}_{\mathfrak{P}}$ (ou uma base inteira local de $F' \mid F$ para o *place* $\mathfrak{P}$).

Teorema 3.68 (existência de infinitas bases inteiras em extensões separáveis)**.** *Sejam: $F \,/\, K$ um corpo de funções, $F' \,\big|\, F$ uma extensão finita separável de corpos de funções.*

Então toda base $\{z_1, \ldots, z_n\}$ de F' sobre F é uma base inteira para quase todo place $\mathfrak{P} \in \mathbb{P}(F)$.

(STICHTENOTH, 2009, p. 85).

3.15.3 O módulo complementar

Definição 3.69 (módulo complementar)**.** *Sejam: $\mathfrak{P} \in \mathbb{P}(F)$; $\mathcal{O}_{\mathfrak{P}}$ o anel de valoração associado a $\mathfrak{P}$; e $\overline{\mathcal{O}_{\mathfrak{P}}}^{F'}$ o fecho inteiro de $\mathcal{O}_{\mathfrak{P}}$ em F'. Então o conjunto*

$$\mathcal{C}_{\mathfrak{P}} := \left\{ z \in F' \;\middle|\; T_{F'|F}\left[z \cdot \overline{\mathcal{O}_{\mathfrak{P}}}^{F'} \right] \subseteq \mathcal{O}_{\mathfrak{P}} \right\} \tag{33}$$

é chamado de <u>módulo complementar</u> sobre $\mathcal{O}_{\mathfrak{P}}$.

(STICHTENOTH, 2009, p. 91).

Proposição 3.70 (propriedades do módulo complementar)**.**

1. *a) $\mathcal{C}_{\mathfrak{P}}$ é um $\overline{\mathcal{O}_{\mathfrak{P}}}^{F'}$-módulo e*
   b) $\overline{\mathcal{O}_{\mathfrak{P}}}^{F'} \subseteq \mathcal{C}_{\mathfrak{P}}$.
2. *Se $\{z_1, \ldots, z_n\}$ for uma base inteira de $\overline{\mathcal{O}_{\mathfrak{P}}}^{F'}$ sobre $\mathcal{O}_{\mathfrak{P}}$, então*

   $$\mathcal{C}_{\mathfrak{P}} = \sum_{i=1}^{n} = \mathcal{O}_{\mathfrak{P}} \cdot z_i^* \,,$$

   em que $\{z_1^*, \ldots, z_n^*\}$ é a base dual de $\{z_1, \ldots, z_n\}$ em relação ao traço.
3. *a) Existe um elemento $t \in F'$ (dependendo de $\mathfrak{P}$) tal que $\mathcal{C}_{\mathfrak{P}} = t \cdot \overline{\mathcal{O}_{\mathfrak{P}}}^{F'}$.*
   b) $v_{\mathfrak{P}'}(t) \leq 0$ para todo $\mathfrak{P}' \mid \mathfrak{P}$.
   c) Para cada $t' \in F'$ temos:

   $$\mathcal{C}_{\mathfrak{P}} = t' \cdot \overline{\mathcal{O}_{\mathfrak{P}}}^{F'} \qquad \Leftrightarrow \qquad v_{\mathfrak{P}'}\left(t'\right) = v_{\mathfrak{P}'}(t), \text{ para todo } \mathfrak{P}' \mid \mathfrak{P} \;.$$

4. *$\mathcal{C}_{\mathfrak{P}} = \overline{\mathcal{O}_{\mathfrak{P}}}^{F'}$ para quase todo $\mathfrak{P} \in \mathbb{P}(F)$.*

(STICHTENOTH, 2009, p. 91).

3.15.4 A definição de diferente

Definição 3.71 (expoente do diferente). *Sejam* $\mathfrak{P} \in \mathbb{P}(F)$; $\overline{\mathcal{O}_{\mathfrak{P}}}^{F'}$ *o fecho inteiro de* $\mathcal{O}_{\mathfrak{P}}$ *em* F'; $\mathcal{C}_{\mathfrak{P}} = t \cdot \overline{\mathcal{O}_{\mathfrak{P}}}^{F'}$ *o módulo complementar sobre* $\mathcal{O}_{\mathfrak{P}}$; *e* $\mathfrak{P}' \in \mathbb{P}(F')$ *um* place *sobre* $\mathfrak{P}$. *Dizemos que*

$$d\left(\mathfrak{P}' \mid \mathfrak{P}\right) := -v_{\mathfrak{P}'}(t)$$

é o expoente do diferente *de* $\mathfrak{P}'$ *sobre* $\mathfrak{P}$.

(STICHTENOTH, 2009, p. 92).

Definição 3.72 (diferente). *Dizemos que*

$$\operatorname{Diff}\left(F' \mid F\right) := \sum_{\substack{\mathfrak{P}' \mid \mathfrak{P} \\ \mathfrak{P} \in \mathbb{P}(F) \\ \mathfrak{P}' \in \mathbb{P}(F')}} d\left(\mathfrak{P}' \mid \mathfrak{P}\right)\mathfrak{P}' \tag{34}$$

é o diferente *de* $F' \mid F$.

(STICHTENOTH, 2009, p. 92).

Observação 3.73. *O diferente é um divisor efetivo, pelo item 3b da Proposição 3.70.*

Optamos por definir o diferente de uma extensão de corpos de funções seguindo a breve exposição de Stichtenoth (2009), pois nesta dissertação estamos interessados apenas em dois fatos a respeito deste divisor: o diferente é *efetivo*, e seu suporte é constituído somente de *places* ramificados ou inseparáveis.

Uma outra abordagem para definir o diferente está disponível na Seção 5.6 do livro de Villa-Salvador (2006). Deste livro, extraímos o seguinte resultado:

Teorema 3.74 (suporte do diferente). *Sejam:* $L \mid l$ *uma extensão finita separável de* $K \mid k$; $\mathfrak{p}$ *um* place *de* K; *e* $\mathfrak{P}$ *um* place *de* L *sobre* $\mathfrak{p}$. *Então*

1. $d\left(\mathfrak{P} \mid \mathfrak{p}\right) \geq e\left(\mathfrak{P} \mid \mathfrak{p}\right) - 1$.
2. *As seguintes condições são equivalentes:*
   - *a)* $d\left(\mathfrak{P} \mid \mathfrak{p}\right) > e\left(\mathfrak{P} \mid \mathfrak{p}\right) - 1$.
   - *b)* *i.* $\operatorname{char}(k)$ *divide* $e\left(\mathfrak{P} \mid \mathfrak{p}\right)$ *ou*
     ii. $\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} \,\middle|\, \frac{\mathcal{O}_{\mathfrak{p}}}{\mathfrak{p}}$ *é inseparável.*

(VILLA-SALVADOR, 2006, p. 148).

3.16 O TEOREMA DE KUMMER

Teorema 3.75 (Kummer). *Sejam $F \,/\, k$ um corpo de funções e $F' \,/\, k'$ uma extensão de $F \,/\, k$. Suponha que $F' = F(y)$, em que $y \in \overline{\mathcal{O}_{\mathfrak{P}}}^{F'}$ é inteiro sobre $\mathcal{O}_{\mathfrak{P}}$. Sejam $\varphi(T) := m_{y,F}(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0 \in \mathcal{O}_{\mathfrak{P}}[T]$ o polinômio minimal de y sobre F;*

$$\overline{\varphi}(T) = \prod_{i=1}^{r} \gamma_i(T)^{\epsilon_i} \in \left(\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}\right)[T]$$

a decomposição de $\overline{\varphi}$ em fatores irredutíveis sobre $\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}$ (ou seja, os polinômios $\gamma_1, \ldots, \gamma_r \in \left(\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}\right)[T]$ são irredutíveis sobre $\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}$, mônicos, dois a dois distintos e $\epsilon_i \geq 1$). Escolha polinômios mônicos $\varphi_i(T) \in \mathcal{O}_{\mathfrak{P}}[T]$ com

$$\overline{\varphi_i}(T) = \gamma_i(T)$$

e

$$\deg\big(\varphi_i(T)\big) = \deg\big(\gamma_i(T)\big) \,.$$

Então temos os seguintes fatos.

1. a) *Para cada $i \in \{1, 2, \ldots, r\}$, existe um* place $\mathfrak{P}_i \in \mathbb{P}\big(F'\big)$ *que satisfaz as seguintes propriedades:*
   - i. $\mathfrak{P}_i | \mathfrak{P}$;
   - ii. $\varphi_i(y) \in \mathfrak{P}_i$; *e*
   - iii. $f(\mathfrak{P}_i \mid \mathfrak{P}) \geq \deg(\gamma_i)$.

   b) $\mathfrak{P}_i \neq \mathfrak{P}_j$ *para* $i \neq j$.

2. *Sob hipóteses adicionais, pode-se provar mais.*

   Suponha que pelo menos uma das seguintes hipóteses $(*)$ ou $(**)$ é satisfeita:

   $$(*): \quad \epsilon_i = 1 \text{ para } i \in \{1, \ldots, r\}, \text{ ou}$$
   $$(**): \quad \left\{1, y, y^2, \ldots, y^{n-1}\right\} \text{ é uma base inteira para } \mathfrak{P} \,.$$

   Então

   a) *existe, para cada $i \in \{1, \ldots, r\}$, exatamente um* place $\mathfrak{P}_i \in \mathbb{P}\big(F'\big)$ *satisfazendo os itens 1(a)i e 1(a)ii:*

   $$\mathfrak{P}_i | \mathfrak{P} \qquad e \qquad \varphi_i(y) \in \mathfrak{P}_i \,.$$

b) *Os* places $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ *são todos os* places *de* F' *sobre* $\mathfrak{P}$, *e*

c) $\epsilon_i = e(\mathfrak{P}_i \mid \mathfrak{P})$. *Portanto,*

$$\mathrm{Con}_{F' \mid F}(\mathfrak{P}) = \sum_{i=1}^{r} \epsilon_i \mathfrak{P}_i \, .$$

d) $\dfrac{\mathcal{O}_{\mathfrak{P}_i}}{\mathfrak{P}_i} \cong \dfrac{\left(\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}\right)[T]}{\langle \gamma_i(T) \rangle}$.

e) $f(\mathfrak{P}_i \mid \mathfrak{P}) = \deg(\gamma_i)$.

(STICHTENOTH, 2009, p. 86).

3.17 A FÓRMULA DO GÊNERO DE RIEMANN-HURWITZ

Teorema 3.76 (Fórmula do Gênero de Riemann-Hurwitz)**.** *Sejam $K \,/\, k$ um corpo de funções com corpo de constantes k e $L \,/\, l$ uma extensão de $K \,/\, k$ com corpo de constantes l.*

Suponha que $L \mid K$ seja uma extensão separável. Então

$$g_L = 1 + \frac{\left[L : K\right]}{\left[l : k\right]} \cdot (g_K - 1) + \frac{1}{2} \cdot \deg_k\big(\mathrm{Diff}(L \mid K)\big) \, .$$

(VILLA-SALVADOR, 2006, p. 309).

3.18 EXTENSÕES CONSTANTES

Seja $L \,/\, l$ uma extensão de $K \,/\, k$. Vimos que a Fórmula do Gênero de Riemann-Hurwitz consegue relacionar os gêneros de L e de K se $L \mid K$ for separável.

Nesta seção, veremos algumas situações em que o gênero da extensão L não muda em relação a K.

Teorema 3.77. *Suponha que k seja um corpo perfeito.*

Sejam: $F \,/\, k$ um corpo de funções; e $F' \,/\, k'$ um corpo de funções tal que $F' = F \cdot k'$. Então

1. $F' \,\big|\, F$ *é não ramificada.*

2. $g_{F'} = g_F$.

(STICHTENOTH, 2009, p. 114).

Teorema 3.78. *Sejam: k um corpo; $l' \mid k$ uma extensão separavelmente gerada; $L := K \cdot l'$ um corpo de funções com corpo de constantes $l \supseteq l'$. Então*

$$g_L = g_K \cdot$$

(VILLA-SALVADOR, 2006, p. 266).

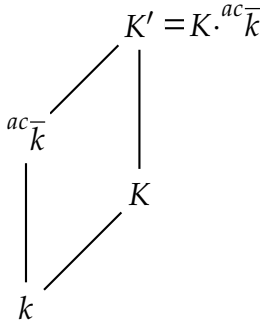
3.19 GRUPOS DE AUTOMORFISMOS DE EXTENSÕES DE CORPOS DE FUNÇÕES ALGÉBRICAS

3.19.1 Finitude do grupo de automorfismos em gêneros "grandes"

Teorema 3.79. *Sejam k um corpo algebricamente fechado e $K \mid k$ um corpo de funções.*
Suponha que $g_K \geq 2$.
Então Aut $(K \mid k)$ *é um grupo finito.*
(VILLA-SALVADOR, 2006, p. 581).

Observação 3.80 (generalização)**.** *Sejam k um corpo arbitrário e $K \mid k$ um corpo de funções com gênero $g_K \geq 2$.*
Sejam ${}^{ac}\overline{k}$ um fecho algébrico de k e $K' := K \cdot {}^{ac}\overline{k}$. Neste caso, o corpo K' é uma extensão constante de K.

Figura 13. Ilustração para a Observação 3.80.



O corpo de constantes de K' é algebricamente fechado e, portanto, perfeito; logo,

$$\begin{aligned} g_{K'} &= g_K \qquad \text{(pelo Teorema 3.77)} \\ &\geq 2 \,. \end{aligned}$$

Pelo Teorema 3.79, o grupo $\operatorname{Aut}\left(K' \,\middle|\, {}^{ac}\overline{k}\right)$ *é finito. Assim, o grupo* $\operatorname{Aut}(K \mid k)$ *também é finito, pois existe uma imersão natural*

$$\iota : \operatorname{Aut}(K \mid k) \hookrightarrow \operatorname{Aut}\left(K' \,\middle|\, {}^{ac}\overline{k}\right)$$

(a construção de ι está disponível no livro de Villa-Salvador (2006, p. 581)).

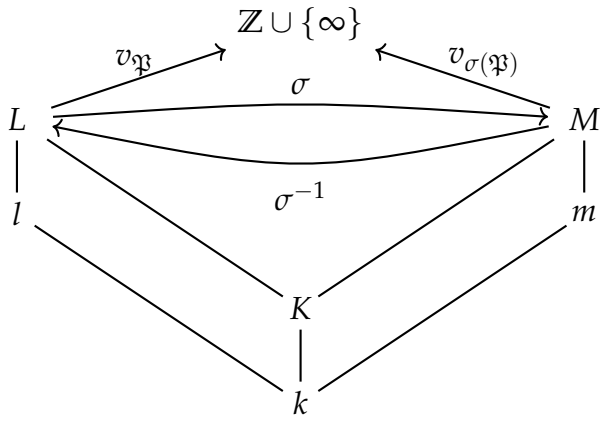
3.19.2 Ação do grupo de automorfismos em *places*

Definição 3.81. *Sejam $L \,/\, l$ e $M \,/\, m$ duas extensões de $K \,/\, k$ e $\sigma : L \to M$ um isomorfismo de corpos tal que $\sigma[l] = m$ e $\sigma\restriction_K = \mathrm{id}_K$. Então, para um* place $\mathfrak{P} \in \mathbb{P}(L)$*, definimos o* place $\sigma(\mathfrak{P})$ *de M por meio da valoração associada,*

$$\begin{aligned} v_{\sigma(\mathfrak{P})} : M &\to \mathbb{Z} \cup \{\infty\} \\ x &\mapsto v_{\sigma(\mathfrak{P})}(x) := v_{\mathfrak{P}}\left(\sigma^{-1}(x)\right) . \end{aligned}$$

(VILLA-SALVADOR, 2006, p. 119).

Figura 14. Ilustração para a Definição 3.38.



Um caso de imediato interesse é quando $M = L$ e $m = l$. Neste caso, a abordagem da ação de automorfismos em *places* no sentido de Villa-Salvador (2006) coincide com a

exposição de Stichtenoth (2009) — por exemplo, a demonstração de um lema (*Lemma* 3.5.2, p. 100) no livro do segundo autor corresponde às duas proposições abaixo, extraídas da obra do primeiro autor.

Proposição 3.82. *$\sigma(\mathfrak{P})$ é a imagem de $\mathfrak{P}$ por σ; isto é,*

$$\sigma(\mathfrak{P}) = \left\{ \sigma(\alpha) \;\middle|\; \alpha \in \mathfrak{P} \right\}.$$

(VILLA-SALVADOR, 2006, p. 119).

Proposição 3.83 (propriedades operacionais)**.**

1. *O mapa que associa $\sigma(\mathfrak{P})$ a cada* place *$\mathfrak{P}$ é uma permutação dos* places *de L.*
2. *a)* $\frac{\mathcal{O}_{\sigma(\mathfrak{P})}}{\sigma(\mathfrak{P})} \cong \frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}$
   b) $\mathcal{O}_{\mathfrak{P}} \cong \mathcal{O}_{\sigma(\mathfrak{P})}$.
3. *Se $\mathfrak{P}$ for um* place *sobre $\mathfrak{p}$, então $\sigma(\mathfrak{P})$ também será um* place *sobre $\mathfrak{p}$.*
4. *O isomorfismo $\overline{\sigma} : \frac{\mathcal{O}_{\sigma(\mathfrak{P})}}{\sigma(\mathfrak{P})} \to \frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}$ é tal que $\overline{\sigma} \restriction_{\frac{\mathcal{O}_{\mathfrak{p}}}{\mathfrak{p}}} = \mathrm{id}_{\frac{\mathcal{O}_{\mathfrak{p}}}{\mathfrak{p}}}$.*
5. *a)* $f(\mathfrak{P} \mid \mathfrak{p}) = f(\sigma(\mathfrak{P}) \mid \mathfrak{p})\, e$
   b) $e(\mathfrak{P} \mid \mathfrak{p}) = e(\sigma(\mathfrak{P}) \mid \mathfrak{p})$.

(VILLA-SALVADOR, 2006, p. 119).

3.20 EXTENSÕES NORMAIS DE CORPOS DE FUNÇÕES

Definição 3.84 (grupo de decomposição)**.** *Sejam: $L \,/\, l$ uma extensão normal finita de $K \,/\, k$; $\mathfrak{p}$ um* place *de K; e $\mathfrak{P}$ um* place *de L sobre $\mathfrak{p}$. Definimos o grupo de decomposição de $\mathfrak{P}$ por*

$$G_Z(\mathfrak{P} \mid \mathfrak{p}) := \left\{ \sigma \in \mathrm{Aut}(L \mid K) \;\middle|\; \sigma(\mathfrak{P}) = \mathfrak{P} \right\}.$$

(VILLA-SALVADOR, 2006, p. 120).

Quando $L \,/\, l$ é uma extensão normal finita de $K \,/\, k$, é possível construir um epimorfismo natural $\Psi : G_Z(\mathfrak{P} \mid \mathfrak{p}) \to \mathrm{Aut}\left(\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} \;\middle|\; \frac{\mathcal{O}_{\mathfrak{p}}}{\mathfrak{p}} \right)$ — cf. *Theorem* 5.2.10 no livro de Villa-Salvador (2006, p. 120). O núcleo de Ψ é chamado de grupo de inércia de $\mathfrak{P}$ sobre $\mathfrak{p}$, e será denotado da seguinte forma:

$$G_T(\mathfrak{P} \mid \mathfrak{p}) := \ker(\Psi). \tag{35}$$

Observação 3.85. *Seja* $\tau \in \mathrm{Aut}(L \mid K)$. *Então*

1. $G_Z\left(\tau(\mathfrak{P}') \mid \mathfrak{P}\right) = \tau G_Z\left(\mathfrak{P}' \mid \mathfrak{P}\right)\tau^{-1}$.

   (VILLA-SALVADOR, 2006, p. 120).

2. $G_T\left(\tau(\mathfrak{P}') \mid \mathfrak{P}\right) = \tau G_T\left(\mathfrak{P}' \mid \mathfrak{P}\right)\tau^{-1}$.

   (VILLA-SALVADOR, 2006, p. 122).

Teorema 3.86 (transitividade da ação de automorfismos nos *places*)**.** *Sejam:* $L \,/\, l$ *uma extensão finita normal de* $K \,/\, k$*;* $\mathfrak{p}$ *um* place *de* K*; e* $\mathfrak{P}$ *e* $\mathfrak{P}'$ *dois* places *de* L *sobre* $\mathfrak{P}$.

Então existe $\sigma \in \mathrm{Aut}(L \mid K)$ *tal que* $\sigma(\mathfrak{P}) = \mathfrak{P}'$.

(VILLA-SALVADOR, 2006, p. 120).

Teorema 3.87. *Seja* $L \,/\, l$ *uma extensão normal finita de* $K \,/\, k$. *Então*

$$\left|G_Z\left(\mathfrak{P} \mid \mathfrak{p}\right) : G_T\left(\mathfrak{P} \mid \mathfrak{p}\right)\right| = f\left(\mathfrak{P} \mid \mathfrak{p}\right)_{\mathbf{s}}.$$

(VILLA-SALVADOR, 2006, p. 122).

3.21 EXTENSÕES SEPARÁVEIS DE CORPOS DE FUNÇÕES

Proposição 3.88 (passagem da separabilidade para a extensão de constantes)**.** *Sejam* $K \,/\, k$ *um corpo de funções e* $L \,/\, l$ *uma extensão de* $K \,/\, k$.

Suponha que $L \mid K$ *seja uma extensão algébrica separável.*

Então $l \mid k$ *é uma extensão separável.*

(VILLA-SALVADOR, 2006, p. 123).

Teorema 3.89 (finitude dos *places* ramificados ou inseparáveis em extensões separáveis)**.** *Seja* $L \,/\, l$ *uma extensão algébrica separável de* $K \,/\, k$.

Existe uma quantidade finita de places *de* L *que são ramificados ou inseparáveis.*

(VILLA-SALVADOR, 2006, p. 127).

3.22 EXTENSÕES GALOISIANAS DE CORPOS DE FUNÇÕES

Sejam: $F' \mid F$ uma extensão galoisiana de corpos de funções algébricas com grupo de Galois $\mathrm{Gal}\left(F' \mid F\right)$; $\mathfrak{P} \in \mathbb{P}(F)$; e $\mathfrak{P}' \in \mathbb{P}\left(F'\right)$ uma extensão de $\mathfrak{P}$.

Definição 3.90.

1. *O corpo fixo* $Z := Z\left(\mathfrak{P}' \mid \mathfrak{P}\right)$ *de* $G_Z\left(\mathfrak{P}' \mid \mathfrak{P}\right)$ *é chamado de corpo de decomposição de* $\mathfrak{P}'$ *sobre* $\mathfrak{P}$.
2. *o corpo fixo* $T := T\left(\mathfrak{P}' \mid \mathfrak{P}\right)$ *de* $G_T\left(\mathfrak{P}' \mid \mathfrak{P}\right)$ *é chamado de corpo de inércia de* $\mathfrak{P}'$ *sobre* $\mathfrak{P}$.

(STICHTENOTH, 2009, p. 130).

Teorema 3.91. *Sejam:* $F' \mid F$ *uma extensão galoisiana de corpos de funções algébricas com grupo de Galois* $G := \mathrm{Gal}\left(F' \mid F\right)$; $\mathfrak{P} \in \mathbb{P}(F)$; *e* $\mathfrak{P}' \in \mathbb{P}\left(F'\right)$ *uma extensão de* $\mathfrak{P}$. *Então*

1. $\left|G_Z\left(\mathfrak{P}' \mid \mathfrak{P}\right)\right| = e\left(\mathfrak{P}' \mid \mathfrak{P}\right) \cdot f\left(\mathfrak{P}' \mid \mathfrak{P}\right)$
2. *a)* $G_T\left(\mathfrak{P}' \mid \mathfrak{P}\right) \trianglelefteq G_Z\left(\mathfrak{P}' \mid \mathfrak{P}\right)$
   b) $\left|G_T\left(\mathfrak{P}' \mid \mathfrak{P}\right)\right| = e\left(\mathfrak{P}' \mid \mathfrak{P}\right)$
3. *a) A extensão* $\dfrac{\mathcal{O}_{\mathfrak{P}'}}{\mathfrak{P}'} \,\Big|\, \dfrac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}$ *é uma extensão Galois.*
   b) Todo automorfismo $\sigma \in G_Z\left(\mathfrak{P}' \mid \mathfrak{P}\right)$ *induz um automorfismo*

$$\begin{aligned} \overline{\sigma} : \mathcal{O}_{\mathfrak{P}'} \Big/ \mathfrak{P}' &\to \mathcal{O}_{\mathfrak{P}'} \Big/ \mathfrak{P}' \\ z + \mathfrak{P}' &\mapsto \overline{\sigma}\left(z + \mathfrak{P}'\right) = \sigma(z) + \mathfrak{P}' \end{aligned}$$

   de $\dfrac{\mathcal{O}_{\mathfrak{P}'}}{\mathfrak{P}'}$ *sobre* $\dfrac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}$.
   c) A aplicação

$$\begin{aligned} f : G_Z\left(\mathfrak{P}' \mid \mathfrak{P}\right) &\to \mathrm{Gal}\left(\frac{\mathcal{O}_{\mathfrak{P}'}}{\mathfrak{P}'} \,\Big|\, \frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}\right) \\ \sigma &\mapsto \overline{\sigma} \end{aligned}$$

   é um homomorfismo sobrejetor cujo núcleo é o grupo de inércia:

$$\ker(f) = G_T\left(\mathfrak{P}' \mid \mathfrak{P}\right).$$

d) Em particular,

$$\mathrm{Gal}\left(\frac{\mathcal{O}_{\mathfrak{P}'}}{\mathfrak{P}'} \,\middle|\, \frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}\right) \cong \frac{G_Z\left(\mathfrak{P}' \mid \mathfrak{P}\right)}{G_T\left(\mathfrak{P}' \mid \mathfrak{P}\right)}\,.$$

4. *Seja $\mathfrak{P}_Z$ (resp. $\mathfrak{P}_T$) a restrição de $\mathfrak{P}'$ ao corpo de decomposição $Z = Z\left(\mathfrak{P}' \mid \mathfrak{P}\right)$ (resp. ao corpo de inércia $T = T\left(\mathfrak{P}' \mid \mathfrak{P}\right)$).*

   Então os índices de ramificação e os graus residuais das extensões de places

$$\mathfrak{P}'|\mathfrak{P}_T\,, \qquad \mathfrak{P}_T|\mathfrak{P}_Z \qquad e \qquad \mathfrak{P}_Z|\mathfrak{P}$$

   são

   a) (etapa "inerte")

      i. $e\left(\mathfrak{P}' \mid \mathfrak{P}_T\right) = e\left(\mathfrak{P}' \mid \mathfrak{P}\right) = \left[F' : T\right]$

      ii. $f\left(\mathfrak{P}' \mid \mathfrak{P}_T\right) = 1$

   b) (etapa da mudança do grau relativo)

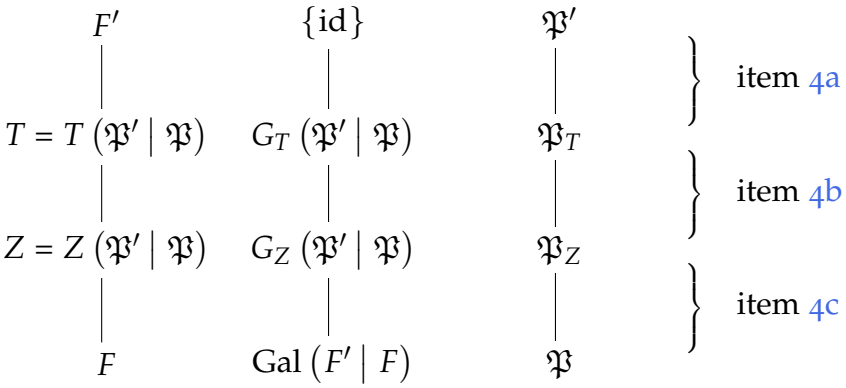
      i. $f\left(\mathfrak{P}_T \mid \mathfrak{P}_Z\right) = f\left(\mathfrak{P}' \mid \mathfrak{P}\right) = \left[T : Z\right]$

      ii. $e\left(\mathfrak{P}_T \mid \mathfrak{P}_Z\right) = 1$

   c) (etapa de decomposição completa)

      $f\left(\mathfrak{P}_Z \mid \mathfrak{P}\right) = e\left(\mathfrak{P}_Z \mid \mathfrak{P}\right) = 1$

Figura 15. Propriedades de um *place* nas restrições aos corpos de decomposição e de inércia.

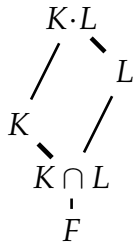


(STICHTENOTH, 2009, p. 131).

Sejam $K \mid F$ uma extensão galoisiana e $L \mid F$ uma extensão qualquer (veja a Figura 16). É conhecido que $\mathrm{Gal}\,(K{\cdot}L \mid L) \cong \mathrm{Gal}\,(K \mid K \cap L)$ e $K{\cdot}L \mid L$ é uma extensão galoisiana (DUMMIT e FOOTE, 2004, p. 591). A prova é baseada na construção do isomorfismo natural

$$\begin{aligned} \Psi : \mathrm{Gal}\,(K{\cdot}L \mid L) &\to \mathrm{Gal}\,(K \mid K \cap L) \\ \sigma &\mapsto \sigma \restriction_K . \end{aligned} \tag{36}$$

Figura 16. A propriedade galoisiana é "transferível" para o compósito.



O isomorfismo em (36) permite demonstrar o resultado seguinte, que ensina como se relacionam os grupos de inércia e de decomposição no compósito e na restrição:

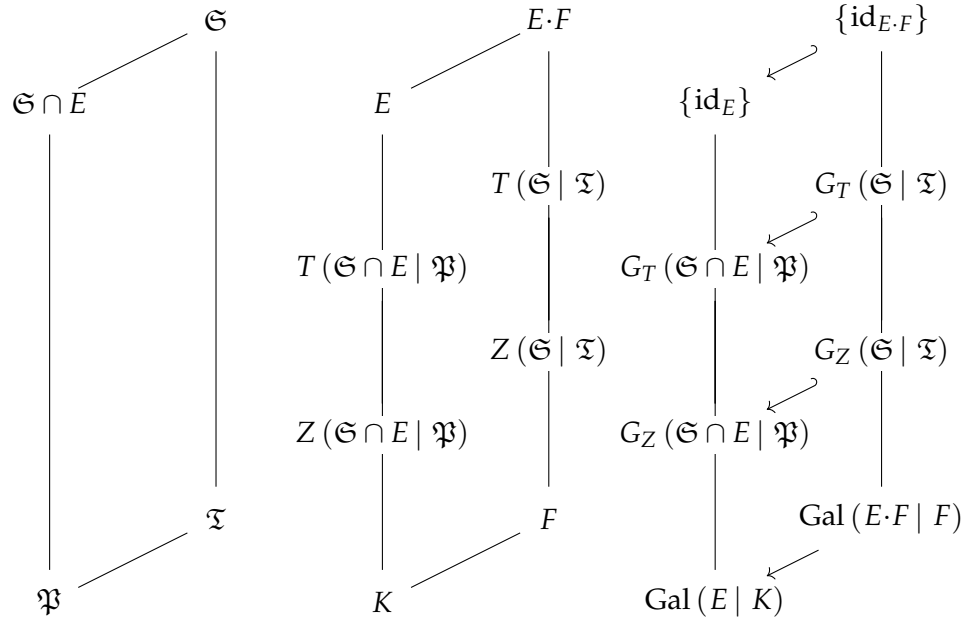
Proposição 3.92. *Sejam: $E \mid K$ uma extensão finita e galoisiana de corpos de funções; $F \mid K$ uma extensão finita; $\mathfrak{P} \in \mathbb{P}(K)$; $\mathfrak{T} \in \mathbb{P}(F)$ uma extensão de $\mathfrak{P}$; e $\mathfrak{S} \in \mathbb{P}(E{\cdot}F)$ uma extensão de $\mathfrak{T}$. Então*

1. $G_Z\,(\mathfrak{S} \mid \mathfrak{T})$ *é imersível em* $G_Z\,(\mathfrak{S} \cap E \mid \mathfrak{P})$ *e*

2. $G_T\,(\mathfrak{S} \mid \mathfrak{T})$ *é imersível em* $G_T\,(\mathfrak{S} \cap E \mid \mathfrak{P})$.

(ÁLVAREZ-GARCIA e VILLA-SALVADOR, 2008, p. 70).

Figura 17. A ilustração mostra as imersões naturais descritas na Proposição 3.92.



3.23 CORPOS SEPARAVELMENTE FECHADOS

Definição 3.93 (corpo separavelmente fechado)**.** *Um corpo k é chamado separavelmente fechado quando toda extensão algébrica de k é puramente inseparável.*

(VILLA-SALVADOR, 2006, p. 127).

Observação 3.94. *Qualquer corpo separavelmente fechado é infinito.*

(VILLA-SALVADOR, 2006, p. 127).

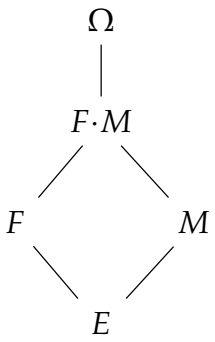
Observação 3.95. *Sejam: k um corpo arbitrário; ${}^{ac}\overline{k}$ um fecho algébrico de k; e k_s o fecho separável de k (em ${}^{ac}\overline{k}$).*

Então k_s é separavelmente fechado.

3.24 EXTENSÕES LINEARMENTE DISJUNTAS

Definição 3.96 (extensões linearmente disjuntas)**.** *Sejam F e M duas extensões de um corpo E que estejam contidas em um corpo algebricamente fechado Ω.*

Figura 18



Dizemos que F é linearmente disjunto de M sobre E quando todo conjunto finito de elementos de F que é linearmente independente sobre E também é linearmente independente sobre M.

(VILLA-SALVADOR, 2006, p. 239).

Exemplo 3.97. *Os corpos* $\mathbb{Q}\left(\sqrt{2}\right)$ *e* $\mathbb{Q}\left(\sqrt{3}\right)$ *são linearmente disjuntos sobre* $\mathbb{Q}$.

(VILLA-SALVADOR, 2006, p. 240).

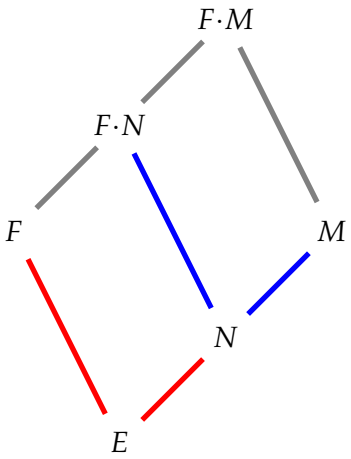
Teorema 3.98. *Sejam:* $L \mid K$ *uma extensão algébrica e separável; e* $M \mid K$ *uma extensão puramente inseparável.*

Então L e M são linearmente disjuntos sobre K.

(FRIED e JARDEN, 2008, p. 35).

Proposição 3.99. *Sejam* $F \mid E$ *e* $M \mid E$ *duas extensões de corpos e N um corpo intermediário da extensão* $M \mid E$.

Figura 19



Então as afirmações seguintes são equivalentes:

1. *F e M são linearmente disjuntos sobre E.*
2. *a) F e N são linearmente disjuntos sobre E, e*
   b) F·N e M são linearmente disjuntos sobre N.

(VILLA-SALVADOR, 2006, p. 240).

3.25 UMA CONSTANTE ASSOCIADA À CONORMA

O seguinte teorema diz que existe uma constante que relaciona o grau de um divisor com o grau de sua conorma.

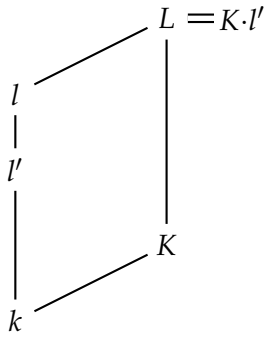
Teorema 3.100. *Seja $L \mid K$ uma extensão de corpos de funções. Então existe $\lambda_{L|K} \in \mathbb{Q}$ positivo tal que*

$$\lambda_{L|K} \cdot \deg\left(\mathrm{Con}_{L|K}(\mathtt{A})\right) = \deg(\mathtt{A}) , \qquad \forall\, \mathtt{A} \in \mathrm{Div}(K) .$$

(VILLA-SALVADOR, 2006, p. 129).

Teorema 3.101. *Sejam: $l' \mid k$ uma extensão de corpo; $K \,/\, k$ um corpo de funções; e $L \,/\, l$ um corpo de funções com corpo de constantes $l \supseteq l'$. Suponha que $L = K{\cdot}l'$.*

Figura 20



Se $g_L = g_K > 0$, então $\lambda_{L|K} = 1$.
(VILLA-SALVADOR, 2006, p. 274).

Teorema 3.102. *Sejam: $K \,/\, k$ um corpo de funções; $l \mid k$ uma extensão de corpo; e $L = K{\cdot}l$ uma extensão constante. Então*

1. *a)* $\lambda_{L|K} = 1$, *se* $\operatorname{char}(k) = 0$.

   b) $\lambda_{L|K} = p^t$ *se* $\operatorname{char}(k) = p > 0$, *para algum* $t \in \mathbb{N} \cup \{0\}$.

2. *Se l é o corpo de constantes de L, então:*

$$\lambda_{L|K} = 1 \qquad \Leftrightarrow \qquad K \text{ e } l \text{ são linearmente disjuntos sobre } k \ .$$

(VILLA-SALVADOR, 2006, p. 261).

3.26 ESTIMATIVA PARA O GÊNERO DE UM CORPO DE FUNÇÕES

Em geral, é difícil calcular o gênero de um corpo de funções (STICHTENOTH, 2009, p. 145). Mas podemos:

- conhecê-lo em contextos especiais — *e. g.*, como no Teorema 3.77 e como no Exemplo 3.24 —, ou
- estimá-lo em alguns casos específicos.

Nesta seção, indicamos algumas formas de estudar o gênero com a abordagem do último item acima.

Proposição 3.103. *Sejam: $F_1 \,/\, k$ um subcorpo de $F \,/\, k$; $n := \left[F : F_1\right]$; $\vartheta := \{z_1, \ldots, z_n\}$ uma base de $F \mid F_1$; e $\mathtt{C} \in \operatorname{Div}(F)$ um divisor tal que $\vartheta \subseteq \mathscr{L}(\mathtt{C})$. Então*

$$g_F \leq 1 + n \cdot (g_{F_1} - 1) + \deg_k(\mathtt{C}) \ .$$

(STICHTENOTH, 2009, p. 145; VILLA-SALVADOR, 2006, p. 527).

Teorema 3.104 (desigualdade de Castelnuovo-Severi)**.** *Sejam: $K \,/\, k$ um corpo de funções tal que $K \,/\, k$ seja separavelmente fechado; e $K_1 \,/\, k$ e $K_2 \,/\, k$ dois subcorpos de $K \,/\, k$ tais que $K = K_1{\cdot}K_2$. Então*

$$g_K \leq \left[K : K_1\right] \cdot g_{K_1} + \left[K : K_2\right] \cdot g_{K_2} + \left(\left[K : K_1\right] - 1\right) \cdot \left(\left[K : K_2\right] - 1\right) . \tag{37}$$

(VILLA-SALVADOR, 2006, p. 529).

3.27 EXTENSÕES PURAMENTE INSEPARÁVEIS

Teorema 3.105 (*places* em extensões puramente inseparáveis)**.** *Seja $L \mid l$ uma extensão puramente inseparável de $K \mid k$. Então:*

1. *para cada* place $\mathfrak{p} \in \mathbb{P}(K)$*, existe um único* place $\mathfrak{P} \in \mathbb{P}(L)$ *tal que* $\mathfrak{P} \mid \mathfrak{p}$*;*
2. *se* $p = \mathrm{char}(k)$*, então e* $(\mathfrak{P} \mid \mathfrak{p}) = p^t$ *para algum* $t \geq 0$ *inteiro; e*
3. $\dfrac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} \,\Big|\, \dfrac{\mathcal{O}_{\mathfrak{p}}}{\mathfrak{p}}$ *é puramente inseparável.*

(VILLA-SALVADOR, 2006, p. 124).

4 PREPARATIVOS PARA O TEOREMA PRINCIPAL

Neste capítulo, apresentamos técnicas de demonstração importantes para a prova do Teorema Principal desta dissertação.

4.1 OS *c*-*improvements*

O Teorema Principal versa sobre a construção de uma extensão de corpos de funções (sobre k) $L \mid K$ com propriedades preestabelecidas para o grupo de automorfismos $\mathrm{Aut}(L \mid K)$. Naturalmente, uma condição necessária para que todo k-automorfismo $\sigma : L \to L$ seja um elemento de $\mathrm{Aut}(L \mid K)$ é que σ fixe o corpo K enquanto conjunto; isto é,

$$\sigma[K] = K\,. \tag{38}$$

Se todo corpo M que for simultaneamente extensão própria de K e subcorpo de L tiver gênero suficientemente grande — digamos, maior que alguma expressão $C = C_{M,K} \in \mathbb{Z}_+$ dependente de M e de K, ou seja,

$$g_M > C\,, \qquad \text{para todo corpo } M \text{ com } L \supseteq M \supsetneq K \tag{39}$$

—, Madden e Valentini (1983) mostraram que todo k-automorfismo σ em $\mathrm{Aut}(L)$ satisfaz (38).

Uma tentativa de prova por redução ao absurdo seria dizer que $\widehat{\sigma}[K] \neq K$ (para algum $\widehat{\sigma} \in \mathrm{Aut}(L)$). Assim, para cairmos em uma contradição proposital, sentiríamos a necessidade de dispormos de algum método para limitar o gênero do compósito $\widehat{M} = K{\cdot}\widehat{\sigma}[K]$, o que seria uma negação de (39). A ideia descrita no artigo de Madden e Valentini (1983) foi mostrar (por absurdo) a desigualdade em (39) para

$$C = \Big[M : K\Big]^2 + 2 \cdot (g_K - 1) \cdot \Big[M : K\Big] + 1$$

usando a desigualdade de Castelnuovo-Severi (Teorema 3.104).

Com as devidas adaptações ao nosso caso de interesse, mostraremos como o método de Madden-Valentini é aplicável na demonstração do Teorema Principal.

A discussão sobre a obtenção de um resultado similar à desigualdade de Castelnuovo-Severi que concretize a ideia desenvolvida acima será postergada para o capítulo seguinte.

Por ora, vamos considerar uma forma de comparar pares de extensões de corpos de funções que têm propriedades "semelhantes" para efeito da Teoria de Galois Finita (no sentido de terem o mesmo grau e os grupos de automorfismos isomorfos) mas que diferem na coleção de possíveis valores dos gêneros dos corpos intermediários.

Definição 4.1. *Sejam:* $E_0 \mid k(x)$ *e* $E_1 \mid k(y)$ *duas extensões de corpos de funções; e* $C \in \mathbb{R}$.

Dizemos que $E_1 \mid k(y)$ *é um* C-improvement *de* $E_0 \mid k(x)$ *quando as seguintes condições forem satisfeitas:*

1. $\left[E_1 : k(y)\right] = \left[E_0 : k(x)\right]$;
2. $\mathrm{Aut}\left(E_1 \,\middle|\, k(y)\right) \cong \mathrm{Aut}\left(E_0 \,\middle|\, k(x)\right)$; *e*
3. *se* M_1 *é qualquer corpo intermediário,*

$$E_1 \supseteq M_1 \supsetneq k(y) \,,$$

então

$$g_{M_1} \geq C \,.$$

(RZEDOWSKI-CALDERÓN e VILLA-SALVADOR, 1991, p. 169).

Em virtude da discussão acima, as extensões "melhores" (para o nosso objetivo final) serão aquelas com gêneros de corpos intermediários "grandes".

4.2 A FÓRMULA DO GÊNERO

Vimos que temos interesse em construir extensões separáveis de corpos de funções com gêneros "grandes"; assim, após fabricarmos os candidatos a *C-improvements* $L \,/\, l$ de $K \,/\, k$ (para algum $C \in \mathbb{Z}_+$), é necessário certificarmos que de fato conseguimos efetuar a construção de uma extensão com a cota inferior desejada para os gêneros dos

corpos intermediários. Para fazermos essa verificação, uma ideia natural seria recorrer à Fórmula do Gênero de Riemann-Hurwitz (Teorema 3.76). Mais especificamente: por meio deste método, bastaria mostrar que $g_M \geq C$ por meio da expressão

$$g_M = 1 + \frac{\left[M : K\right]}{\left[m : k\right]} \cdot (g_K - 1) + \frac{1}{2} \cdot \deg_k\big(\mathrm{Diff}\,(M \mid K)\big)\ , \tag{40}$$

para todo corpo de funções $M \,/\, m$ com corpo de constantes m e $L \supseteq M \supsetneq K$.

Portanto, precisamos conhecer o conteúdo do suporte do diferente no caso de extensões de corpos de funções sobre corpos imperfeitos.

4.3 CORPOS DE FUNÇÕES SOBRE CORPOS IMPERFEITOS

Existe uma razoável quantidade de propriedades conhecidas acerca de corpos de funções sobre corpos perfeitos. O livro de Stichtenoth (2009), por exemplo, dedica um capítulo inteiro ao estudo dessa classe de corpos de funções.

Os teoremas principais dos artigos de Stichtenoth (1984) e de Villa-Salvador e Rzedowski-Calderón (1991) referem-se a corpos de funções $K \,/\, k$ nos casos em que k é algebricamente fechado ou k é finito, respectivamente. Em cada uma destas duas situações, k enquadra-se como um conhecido exemplo de corpo que é perfeito.

Vejamos algumas consequências da remoção da hipótese de perfeição do corpo de constantes.

4.3.1 O suporte do diferente

Seja $K \,/\, k$ um corpo de funções sobre k e $L \mid K$ uma extensão separável não trivial. A literatura registra que o suporte do diferente de $L \mid K$ coincide com a coleção $\mathscr{R} \subseteq \mathbb{P}(L)$ dos *places* ramificados em $L \mid K$ se k for perfeito — *Corollary* 3.5.5 no livro de Stichtenoth (2009, p. 106).

No caso em que k é imperfeito, o suporte do diferente é constituído adicionalmente dos *places* inseparáveis: $\mathrm{Supp}\big(\mathrm{Diff}\,(L \mid K)\big) = \mathscr{I} \cup \mathscr{R}$, em que $\mathscr{I} \subseteq \mathbb{P}(L)$ é o conjunto dos *places* inseparáveis em $L \mid K$ (Teorema 3.74). Vejamos por que isso ocorre: recordamos

que o corpo residual $\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}$ sempre pode ser visto como uma extensão finita de k, para todo *place* $\mathfrak{P} \in \mathbb{P}(K)$ (cf. Seção 3.3); assim, se k não é perfeito, não há garantia de a extensão $\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} \Big| k$ ser separável para um *place* $\mathfrak{P} \in \mathbb{P}(K)$ *arbitrário*. Ou seja, a aparição dos *places* inseparáveis é um efeito da retirada da hipótese de perfeição de k.

A seguir, veremos como os grupos de inércia estão relacionados com os *places* do suporte do diferente.

4.3.2 Ramificação ou inseparabilidade em extensões galoisianas

O cálculo da ordem de um grupo de inércia pode ser útil para identificar *places* que estejam no suporte do diferente, por conta do seguinte resultado.

Proposição 4.2 (detecção de *places* ramificados ou inseparáveis com o grupo de inércia)**.** *Seja $L \,/\, l$ uma extensão normal finita de $K \,/\, k$. Então*

$$\left|G_T\left(\mathfrak{P} \mid \mathfrak{p}\right)\right| = \frac{e\left(\mathfrak{P} \mid \mathfrak{p}\right) \cdot f\left(\mathfrak{P} \mid \mathfrak{p}\right)_{\mathfrak{i}}}{[L:K]_{\mathfrak{i}}} \,. \tag{41}$$

(VILLA-SALVADOR, 2006, p. 123).

Note que, se a extensão $L \mid K$ também for separável, então o denominador na Equação 41 é igual a um. Neste caso, se a ordem do grupo de inércia for maior que um, então o *place* $\mathfrak{P}$ será ramificado ou inseparável em $L \mid K$; e, consequentemente, o ideal $\mathfrak{P}$ estaria no suporte do diferente de $L \mid K$.

Uma forma prática de evitar este denominador seria considerar o caso em que $L \mid K$ é Galois.

4.3.3 Ramificação ou inseparabilidade em compósitos

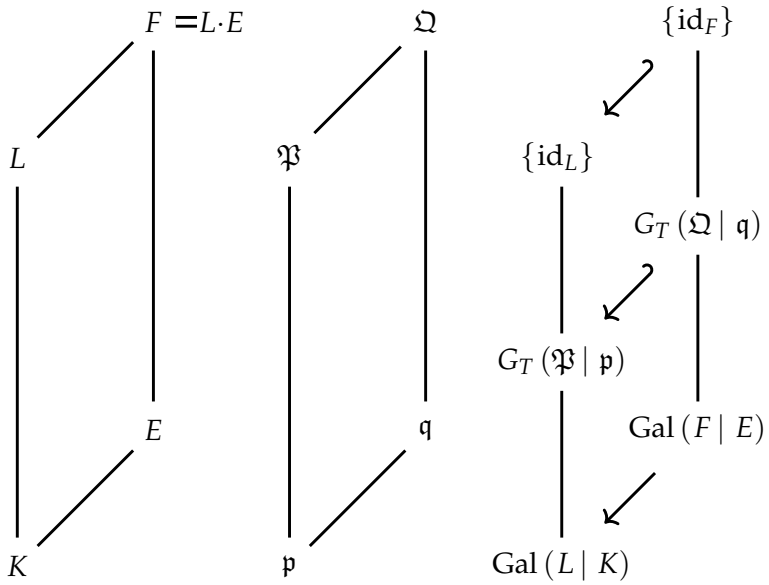
Sejam: $K \,/\, k$ um corpo de funções; $L \,/\, k$ uma extensão galoisiana e finita de $K \,/\, k$; $E \,/\, k$ uma extensão de $K \,/\, k$ tal que $L \cap E = K$; $F := L{\cdot}E$; $\mathfrak{p} \in \mathbb{P}(K)$; $\mathfrak{P} \in \mathbb{P}(L)$ um *place* sobre $\mathfrak{p}$; $\mathfrak{Q} \in \mathbb{P}(F)$ uma extensão de $\mathfrak{P}$; e $\mathfrak{q} \in \mathbb{P}(E)$ uma restrição de $\mathfrak{Q}$ a E. Suponha que $\mathfrak{p}$ seja não ramificado e separável em $L \mid K$.

Pela imersão natural entre os grupos de inércia — dada na Proposição 3.92 —, o grupo $G_T(\mathfrak{Q} \mid \mathfrak{q})$ pode ser visto como um subgrupo de $G_T(\mathfrak{P} \mid \mathfrak{p})$. Assim,

$$\begin{aligned} \left|G_T(\mathfrak{Q} \mid \mathfrak{q})\right| &\leq \left|G_T(\mathfrak{P} \mid \mathfrak{p})\right| \\ &= \frac{e(\mathfrak{P} \mid \mathfrak{p}) \cdot f(\mathfrak{P} \mid \mathfrak{p})_{\mathbf{i}}}{[L:K]_{\mathbf{i}}} \qquad \text{(pela Proposição 4.2)} \\ &= 1\,. \end{aligned}$$

Sabemos que $F \mid E$ também é extensão galoisiana — cf. discussão que precede o enunciado da Proposição 3.92. Pela Igualdade Fundamental (e novamente pela Proposição 4.2), temos que o *place* $\mathfrak{q}$ é não ramificado e separável em $F \mid E$.

Figura 21. Ilustração para a Proposição 4.3.



Para uso posterior, vamos registrar o que acabamos de provar:

Proposição 4.3 (ramificação ou inseparabilidade em compósitos)**.** *Sejam: $K \,/\, k$ um corpo de funções; $L \,/\, k$ uma extensão galoisiana e finita de $K \,/\, k$; $E \,/\, k$ uma extensão de $K \,/\, k$ tal que $L \cap E = K$; $F := L{\cdot}E$; $\mathfrak{p} \in \mathbb{P}(K)$; $\mathfrak{P} \in \mathbb{P}(L)$ um* place *sobre $\mathfrak{p}$; $\mathfrak{Q} \in \mathbb{P}(F)$ um* place *sobre $\mathfrak{P}$; e $\mathfrak{q} \in \mathbb{P}(E)$ uma restrição de $\mathfrak{Q}$ a E. Suponha que $\mathfrak{p}$ seja não ramificado e separável em $L \mid K$.*

Então $\mathfrak{q}$ é não ramificado e separável em $F \mid E$.

4.3.4 Ramificação ou inseparabilidade em extensões de corpos de funções racionais

Seja $k(x) \,/\, k$ um corpo de funções racionais sobre k e $F \,/\, k$ uma extensão separável de $k(x) \,/\, k$ com corpo de constantes k. Se k é perfeito e

$$\Big[F : k(x)\Big] > 1 \,, \tag{42}$$

então $F \mid k(x)$ é ramificada — *Corollary* 3.5.8 no livro de Stichtenoth (2009, p. 106).

No caso em que k é imperfeito, temos um resultado análogo:

Teorema 4.4. *Seja $F \mid k(x)$ uma extensão finita separável de grau $\Big[F : k(x)\Big] > 1$ tal que k é o corpo de constantes de F.*

Então $F \mid k(x)$ é ramificada ou existe um place *de $k(x)$ inseparável em $F \mid k(x)$.*

A demonstração é totalmente análoga ao caso em que o corpo de constantes é perfeito.

Repare que, por (42), exigimos que F seja uma extensão *própria* de $k(x)$. Esta hipótese não é colocada à esmo: o caso em que $\Big[F : k(x)\Big] = 1$ seria um impeditivo para a existência de *places* ramificados ou de grau relativo maior que um, por conta da Igualdade Fundamental.

4.4 RAMIFICAÇÃO EM COMPÓSITOS

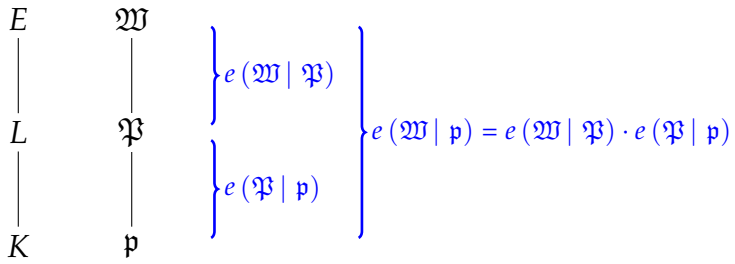
Da transitividade do índice de ramificação, o seguinte resultado é imediato.

Proposição 4.5 (ramificação em "torres")**.** *Sejam: $K \subseteq L \subseteq E$ uma torre de corpos de funções com $\Big[E : K\Big] < \infty$; $\mathfrak{W}$ um* place *de E; $\mathfrak{P} := \mathfrak{W} \cap L$; e $\mathfrak{p} := \mathfrak{P} \cap K$.*

Então $\mathfrak{P}$ é ramificado em $E \mid K$ se, e somente se, $\mathfrak{P}$ é ramificado em $E \mid L$ ou $\mathfrak{P}$ é ramificado em $L \mid K$.

(VILLA-SALVADOR, 2006, p. 126).

Figura 22. Ilustração para a Proposição 4.5.



Vamos considerar agora como a Proposição 4.5 pode ser usada para estudar a ramificação em compósitos.

Sejam $K_1 \mid F$ e $K_2 \mid F$ duas extensões de corpos de funções e $\mathfrak{p} \in \mathbb{P}(F)$. Suponha que $\mathfrak{p}$ seja ramificado em $K_1 \mid F$ mas não ramificado em $K_2 \mid F$.

Vamos ver por que a ramificação de $\mathfrak{p}$ ocorre em $K_1 \cdot K_2 \mid K_2$, passo a passo. A Figura 23 ilustra as etapas dessa demonstração.

1. Como $\mathfrak{p}$ é ramificado em $K_1 \mid F$ então existe um *place* $\mathfrak{p}_1 \in \mathbb{P}(K_1)$ tal que $e(\mathfrak{p}_1 \mid \mathfrak{p}) > 1$.

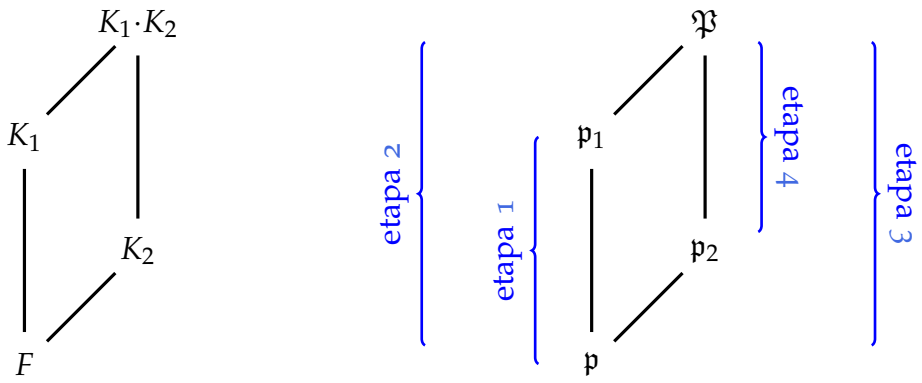
2. Seja $\mathfrak{P} \in \mathbb{P}(K_1 \cdot K_2)$ um *place* sobre $\mathfrak{p}_1$. Então a extensão de *places* $\mathfrak{P} \mid \mathfrak{p}$ também é ramificada, pois

$$\begin{aligned} e(\mathfrak{P} \mid \mathfrak{p}) &= e(\mathfrak{P} \mid \mathfrak{p}_1) \cdot e(\mathfrak{p}_1 \mid \mathfrak{p}) \qquad \text{(pela Proposição 3.46)} \\ &> 1 \,. \end{aligned}$$

3. Seja $\mathfrak{p}_2 := \mathfrak{P} \cap K_2$. A extensão $\mathfrak{P} \mid \mathfrak{p}$ pode ser vista como uma "torre" de *places* $\mathfrak{P} \supseteq \mathfrak{p}_2 \supseteq \mathfrak{p}$. Então $e(\mathfrak{P} \mid \mathfrak{p}_2) > 1$ ou $e(\mathfrak{p}_2 \mid \mathfrak{p}) > 1$ pela Proposição 4.5.

4. Como o *place* $\mathfrak{p}$ não se ramifica em $K_2 \mid F$, então a ramificação de $\mathfrak{p}$ ocorre em $K_1 \cdot K_2 \mid K_2$.

Figura 23. Ilustração para a demonstração da Proposição 4.6.



Em suma, temos o seguinte resultado.

Proposição 4.6 (ramificação em extensões intermediárias de compósitos)**.** *Sejam $K_1 \mid F$ e $K_2 \mid F$ são duas extensões de corpos de funções e $\mathfrak{p} \in \mathbb{P}(F)$. Suponha que $\mathfrak{p}$ seja ramificado em $K_1 \mid F$ mas não ramificado em $K_2 \mid F$.*

Então $\mathfrak{p}$ é ramificado em $K_1 \cdot K_2 \mid K_2$.

4.5 PRESERVAÇÃO DO GRAU EM EXTENSÕES DE CORPOS DE FUNÇÕES

Sejam K_1 e K_2 duas extensões finitas de um corpo F com graus $n := \left[K_1 : F\right]$ e $m := \left[K_2 : F\right]$. É sabido que:

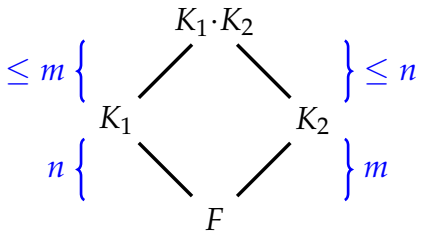
$$\left[K_1 \cdot K_2 : K_2\right] \leq n \qquad \text{e} \qquad \left[K_1 \cdot K_2 : K_1\right] \leq m \, ;$$

e, se $\mathrm{mdc}\{n, m\} = 1$, então

$$\left[K_1 \cdot K_2 : F\right] = \left[K_1 : F\right] \cdot \left[K_2 : F\right] = n \cdot m$$

— recomendamos o livro de Dummit e Foote (2004, p. 529) para as demonstrações.

Figura 24. O grau das extensões intermediárias em compósitos.



Assim, se n e m são relativamente primos, podemos "deslocar para cima" os valores dos graus das extensões inferiores; isto é,

$$\left[K_2 : F\right] = \left[K_1 \cdot K_2 : K_1\right] \qquad \text{e} \qquad \left[K_1 : F\right] = \left[K_1 \cdot K_2 : K_2\right] .$$

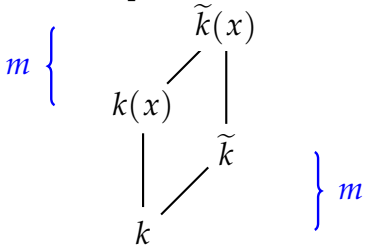
O "truque do mdc" descrito acima é um fato básico usado na teoria de extensões finitas, mas veremos que pode ser útil também na análise de extensões transcendentes; existem manipulações de extensões de corpos de funções que não alteram o grau da estrutura original.

Proposição 4.7 (preservação do grau com adjunção de elementos transcendentes)**.** *Sejam $K \,/\, k$ um corpo de funções e $\widetilde{k}$ o corpo de constantes de $K \,/\, k$. Seja $x \in K \setminus \widetilde{k}$. Então*

$$\left[\widetilde{k} : k\right] = \left[\widetilde{k}(x) : k(x)\right] . \tag{43}$$

(VILLA-SALVADOR, 2006, p. 15).

Figura 25. A ilustração da preservação do grau com adjunção de elementos transcendentes: $\left[\widetilde{k} : k\right] = \left[\widetilde{k}(x) : k(x)\right] = m$.

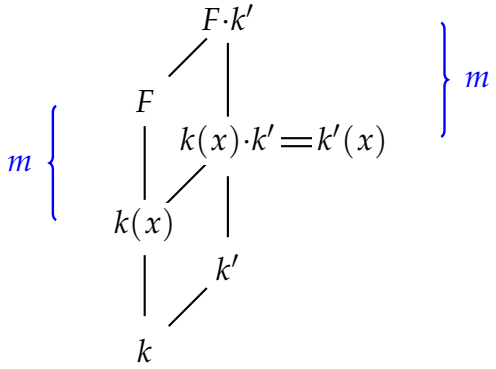


Observação 4.8 (preservação do grau em extensões constantes e separáveis)**.** *Sejam: $F \,/\, k$ um corpo de funções; k' uma extensão algébrica e separável de k; e $x \in F \setminus k$. Suponha que $m := \left[F : k(x)\right]$ seja finito. Então*

$$m = \left[F : k(x)\right] = \left[F \cdot k' : k'(x)\right] .$$

*A demonstração deste fato é totalmente análoga à prova de uma proposição (*Proposition *3.6.1) no livro de Stichtenoth (2009, p. 113). Embora a referida proposição da obra mencionada assuma como hipótese que k seja perfeito, a demonstração não usa o fato de* toda extensão *algébrica de k ser separável.*

Figura 26. A ilustração da preservação do grau em extensões constantes e separáveis.



4.6 ALGUMAS CONVENIENTES MUDANÇAS DE VARIÁVEIS EM CORPOS DE FUNÇÕES

O conteúdo desta seção é análogo a um comentário feito no livro de Villa-Salvador (2006) — cf. *Remark* 14.4.9, p. 587 —, com algumas modificações. O objetivo é expor algumas mudanças de variáveis que nos permitirão trabalhar com corpos de funções racionais em parâmetros convenientes.

Para esta seção, considere os corpos de funções racionais $k(w)$ e $k(z)$ nas variáveis w e z, respectivamente. Suponha que $K \mid k(w)$ seja uma extensão algébrica separável, e que k seja um corpo infinito.

4.6.1 Uma mudança de variáveis bastante simples

A aplicação

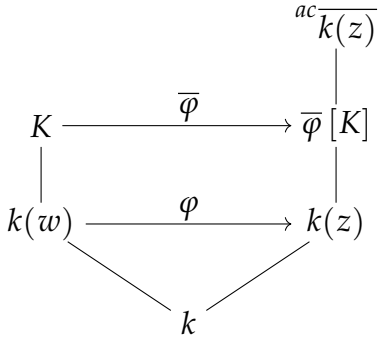
$$\begin{aligned} \varphi : k(w) &\to k(z) \\ f(w) &\mapsto \varphi\big(f(w)\big) = f(z) \end{aligned} \tag{44}$$

é um isomorfismo de corpos, claramente: o homomorfismo φ simplesmente converte uma fração $f(w) = \frac{u(w)}{v(w)}$ de polinômios $u, v \in k[w]$ (na variável w) na fração de polinômios $\frac{u(z)}{v(z)}$.

4.6.2 Mudanças de variáveis em extensões algébricas de corpos de funções racionais

Como $K \mid k(w)$ é uma extensão algébrica, então φ é extensível a um monomorfismo de corpos $\overline{\varphi} : K \to {}^{ac}\overline{k(z)}$, em que ${}^{ac}\overline{k(z)}$ é um fecho algébrico de $k(z)$ — veja (2.18) no livro de Endler (2012, p. 45) para uma demonstração deste fato. A aplicação $\overline{\varphi}$ é um isomorfismo de corpos, pois φ é homomorfismo bijetor (pela subseção anterior). Portanto, se $K_2 := \overline{\varphi}[K]$, então a extensão $K_2 \mid k(z)$ satisfaz as mesmas propriedades de $K \mid k(w)$.

Figura 27. A mudança de variáveis φ e sua extensão $\overline{\varphi}$.



4.6.3 Existência de *places* ramificados de grau um

Suponha que existe um *place* $\mathfrak{p} \in \mathbb{P}(k(w))$ de grau $\deg_k(\mathfrak{p}) = 1$ ramificado em $K \mid k(w)$.

Sendo $k(w)$ um corpo de funções racionais, temos que existe $p \in k[w]$ mônico tal que $\deg(p) = 1$ e $\mathfrak{P}_{p(w)} = \mathfrak{p}$ (cf. Equação 7). Seja $\alpha \in k$ tal que

$$p(w) = w - \alpha \ .$$

Seja $k(t) \subseteq K$ um corpo de funções racionais numa variável $t \in k(w)$.

Temos que $k(t) = k(w)$ se, e somente se, existem $a, b, c, d \in k$ tais que

$$\mathcal{D}_{a,b,c,d} := a \cdot d - b \cdot c \neq 0 \qquad \text{e} \qquad \mathcal{T}_{w;a,b,c,d} := t := \frac{a \cdot w + b}{c \cdot w + d} \tag{45}$$

— cf. (11.2) no livro de Endler (2012, p. 171). Assim, para cada quádrupla $a, b, c, d \in k$ com $\mathcal{D}_{a,b,c,d} \neq 0$ e $\mathcal{T}_{w;a,b,c,d} = t$, fica definida uma mudança de variáveis

$$\begin{aligned} \psi : k(w) &\to k(t) \\ w &\mapsto t = \mathcal{T}_{w;a,b,c,d} \ . \end{aligned} \tag{46}$$

No caso particular em que

$$a = 1 \ , \qquad b = \alpha - 1 \ , \qquad c = 0 \qquad \text{e} \qquad d = 1 \ , \tag{47}$$

o isomorfismo ψ transforma o polinômio $p(w)$ na expressão $\psi\big(p(w)\big) = \widetilde{p}(w) := w - 1$. Como $k(w)$ e $k(t)$ são o mesmo corpo, a aplicação ψ apenas altera o polinômio associado a $\mathfrak{p}$ (o "rótulo" do *place* $\mathfrak{p}$ passa a ser $\widetilde{p}(w)$), mas não modifica a propriedade de ramificação de $\mathfrak{p}$ na extensão $K \mid k(w)$.

Sejam $\mathfrak{r}, \mathfrak{s} \in \mathbb{P}\big(k(t)\big)$ o zero e o polo de t em $k(t)$, respectivamente. Afirmamos que existe um parâmetro $t_* \in k(w)$ tal que:

1. $k(t_*) = k(w)$;
2. $\mathfrak{p} = \mathfrak{P}_{t_*-1}$; e
3. o zero $\mathfrak{r}_*$ e o polo $\mathfrak{s}_*$ de t_* em $k(t_*)$ são não ramificados em $K \mid k(w)$.

Vejamos as etapas da prova deste fato:

(1^a etapa) Se as três condições acima forem satisfeitas após as escolhas de (47), tome

$$t_* := t \ , \qquad \mathfrak{r}_* := \mathfrak{r} \qquad \text{e} \qquad \mathfrak{s}_* := \mathfrak{s} \ .$$

Caso contrário, suponha (sem perda de generalidade) que $\mathfrak{r}$ seja ramificado em $K \mid k(w)$. Passemos à 2^a etapa.

(2^a etapa) Seja $p_2(w) = w - \alpha_2 \in k\,[w]$ tal que $\mathfrak{r} = \mathfrak{P}_{p_2(w)}$. Com uma construção análoga ao isomorfismo em (46) e com escolhas similares feitas em (47), obtemos uma variável $t_2 \in k(w)$ tal que $\mathfrak{p} = \mathfrak{P}_{t_2-1}$.

Se o zero $\mathfrak{r}_2$ e o polo $\mathfrak{s}_2$ de t_2 em $k(t_2)$ são não ramificados em $K \mid k(w)$, tome $t_* := t_2$, $\mathfrak{r}_* := \mathfrak{r}_2$ e $\mathfrak{s}_* := \mathfrak{s}_2$.

Caso contrário, seria necessário prosseguirmos numa 3^a etapa.

O procedimento acima termina em uma quantidade finita de passos: como a extensão $K \mid k(w)$ é separável, então pelo Teorema 3.89 existe uma quantidade finita de *places* ramificados em $K \mid k(w)$. Note que, como k é infinito, podemos efetuar uma quantidade arbitrária de etapas até obtermos t_*, $\mathfrak{r}_*$ e $\mathfrak{s}_*$.

A conclusão é que, com a existência de um *place* $\mathfrak{p} \in \mathbb{P}\big(k(w)\big)$ ramificado em $K \mid k(w)$ de grau um sobre k, temos liberdade para trabalharmos numa variável conveniente $t \in k(w)$ de modo que t tenha o zero e o polo em $k(t)$ não ramificados e o polinômio $t - 1$ seja o "rótulo" do *place* ramificado $\mathfrak{p}$:

$$\mathfrak{p} = \mathfrak{P}_{t-1} \, .$$

5 O TEOREMA PRINCIPAL

O conteúdo deste capítulo corresponde ao artigo de Álvarez-García e Villa-Salvador (2010).

5.1 CORPOS DE FUNÇÕES SOBRE UM CORPO DE CONSTANTES INFINITO

Esta seção é baseada na segunda seção do artigo de Álvarez-Garcia e Villa-Salvador (2010), e contém uma coletânea de resultados úteis para as seções subsequentes deste capítulo.

Lema 5.1. *Sejam: $k(x)$ um corpo de funções racionais; $F \mid k(x)$ uma extensão finita e galoisiana; $k(y) \supseteq k(x)$ um corpo de funções racionais tal que*

$$\operatorname{mdc}\left\{ \left[F : k(x)\right], \left[k(y) : k(x)\right] \right\} = 1 \ ; \tag{48}$$

$E \ / \ l$ um corpo intermediário de $F \mid k(x)$; e N o corpo de constantes de $E(y)$.
Suponha que a variável y seja separável sobre $k(x)$.
Então $N = l$.

Demonstração.

Afirmação 5.2. *$E(y) \mid k(x)$ e $E(y) \mid l(x)$ são extensões separáveis.*

Dem.: Como a extensão $F \mid k(x)$ é galoisiana e finita, em particular será também separável. Pela teoria de corpos, temos que a extensão intermediária $E \mid k(x)$ é separável. Como y é separável sobre $k(x)$, temos também que $E(y) \mid k(x)$ é uma extensão separável. Note que $l \supseteq k$, pois: k é o corpo de constantes de $k(x)$ (Exemplo 3.24); e E é um corpo de funções sobre l. Então $E(y) \supseteq l(x) \supseteq k(x)$ e, assim, a extensão intermediária $E(y) \mid l(x)$ de $E(y) \mid k(x)$ é separável. ◇

Da hipótese,

$$\operatorname{mdc}\left\{ \left[E : k(x)\right], \left[k(y) : k(x)\right] \right\} = 1 \,. \tag{49}$$

Pela Afirmação 5.2 e pela Proposição 3.88, temos que $N \mid l$ é separável. Assim, pela Observação 4.8, temos que

$$\left[E : l(x)\right] = \left[E{\cdot}N : N(x)\right] \,; \tag{50}$$

por argumento similar, a extensão $N \mid k$ também é separável e

$$\left[k(y) : k(x)\right] = \left[N(y) : N(x)\right] = \left[l(y) : l(x)\right] \,. \tag{51}$$

Combinando (49) e (51) e com a transitividade do grau (aplicada à torre de corpos $E \supseteq l(x) \supseteq k(x)$),

$$\operatorname{mdc}\left\{ \left[E : l(x)\right], \left[l(y) : l(x)\right] \right\} = 1 \tag{52}$$

— veja a Figura 29. Pelas equações 50, 51 e 52 segue que

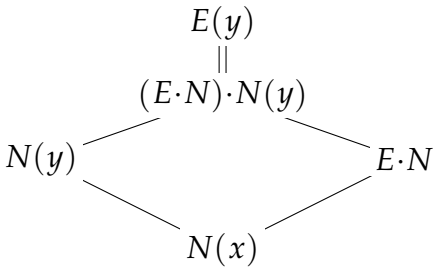
$$\operatorname{mdc}\left\{ \left[E{\cdot}N : N(x)\right], \left[N(y) : N(x)\right] \right\} = 1 \,. \tag{53}$$

Como $(E{\cdot}N){\cdot}N(y) = E(y)$, temos pela Equação 53 que

$$\left[E(y) : N(y)\right] = \left[E{\cdot}N : N(x)\right] \tag{54}$$

— veja a Figura 28.

Figura 28



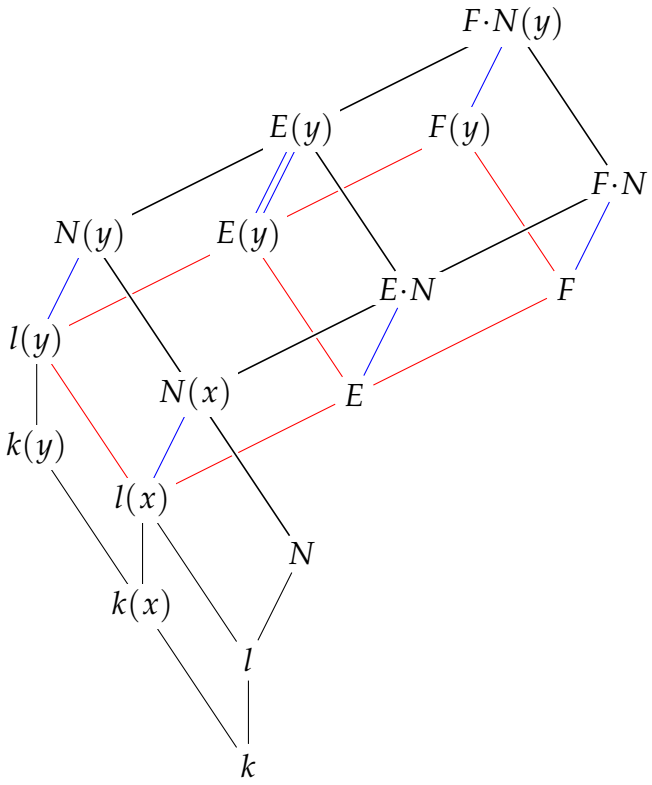
Analogamente, pela Equação 52,

$$\left[E(y) : l(y)\right] = \left[E : l(x)\right] \,. \tag{55}$$

Assim,

$$\left[E(y) : N(y)\right] \overset{\text{Eq. 54}}{=} \left[E{\cdot}N : N(x)\right] \overset{\text{Eq. 50}}{=} \left[E : l(x)\right] \overset{\text{Eq. 55}}{=} \left[E(y) : l(y)\right] \,.$$

Figura 29. Ilustração para a demonstração do Lema 5.1.



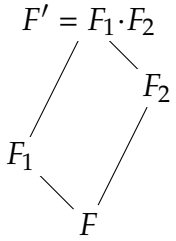
Portanto, $N(y) = l(y)$; assim,

$$\begin{aligned} 1 &= \left[N(y) : l(y)\right] \\ &= \left[N : l\right] \qquad \text{(pela Proposição 4.7)} . \end{aligned}$$

A tese segue. □

Lema 5.3. *Sejam:* $F' \mid F$ *uma extensão finita separável de corpos de funções;* F_1, F_2 *corpos intermediários de* $F' \mid F$ *tais que* $F' = F_1{\cdot}F_2$*; e* $\mathfrak{P} \in \mathbb{P}(F)$.

Figura 30. Ilustração para o Lema 5.3.



1. *Suponha que $\mathfrak{P}$ decompõe-se completamente em $F_1 \mid F$ e em $F_2 \mid F$.*

   Então $\mathfrak{P}$ decompõe-se completamente em $F' \mid F$.

2. *Suponha que $\mathfrak{P}$ é não ramificado e separável em $F_1 \mid F$ e em $F_2 \mid F$.*

   Então $\mathfrak{P}$ é não ramificado e separável em $F' \mid F$.

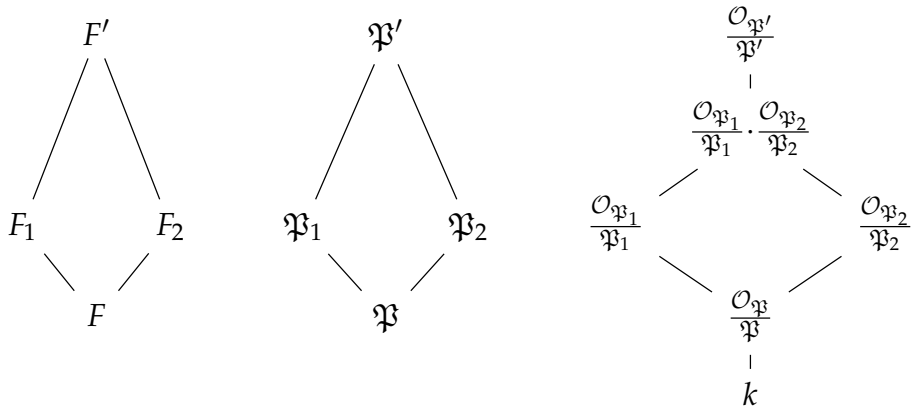
Demonstração. (Item 1): item 2 da Proposição 3.59.

(Item 2): ($\mathfrak{P}$ é não ramificado em $F' \mid F$): item 1 do Corolário 3.58.

($\mathfrak{P}$ é separável em $F' \mid F$)[1]:

Sejam: $\mathfrak{P}_1 \in \mathbb{P}(F_1)$ e $\mathfrak{P}_2 \in \mathbb{P}(F_2)$ extensões de $\mathfrak{P}$; e $\mathfrak{P}' \in \mathbb{P}(F')$ uma extensão de $\mathfrak{P}_1$ e de $\mathfrak{P}_2$.

Figura 31. Ilustração para a demonstração do item 2 do Lema 5.3.



Basta provar a seguinte afirmação.

Afirmação 5.4. $\frac{\mathcal{O}_{\mathfrak{P}'}}{\mathfrak{P}'} = \frac{\mathcal{O}_{\mathfrak{P}_1}}{\mathfrak{P}_1} \cdot \frac{\mathcal{O}_{\mathfrak{P}_2}}{\mathfrak{P}_2}$.

Dem.: ($\supseteq$): Segue da Proposição 3.41. ($\subseteq$): Seja $\alpha \in \frac{\mathcal{O}_{\mathfrak{P}'}}{\mathfrak{P}'}$. Seja $f \in \mathcal{O}_{\mathfrak{P}'}$ tal que $\alpha = f + \mathfrak{P}'$.

Se $f \in \mathfrak{P}'$, teríamos que $\alpha = 0 + \mathfrak{P}'$, e α seria elemento do compósito trivialmente. Podemos supor então que $f \in \mathcal{O}_{\mathfrak{P}'} \setminus \mathfrak{P}'$.

Como f é um elemento de $F_1 \cdot F_2$, existem

$$S_1 := \{x_1, x_2, \ldots, x_{n_1}, \widetilde{x}_1, \widetilde{x}_2, \ldots, \widetilde{x}_{n_2}\} \subseteq F_1 \setminus \{0\}$$

$$\text{e} \qquad S_2 := \{y_1, y_2, \ldots, y_{n_1}, \widetilde{y}_1, \widetilde{y}_2, \ldots, \widetilde{y}_{n_2}\} \subseteq F_2 \setminus \{0\}$$

1 A demonstração deste item foi sugerida pelo professor Nazar Arakelian (a quem agradeço).

tais que

$$f = \frac{\sum_{i=1}^{n_1} x_i \cdot y_i}{\sum_{j=1}^{n_2} \widetilde{x}_j \cdot \widetilde{y}_j} \,. \tag{56}$$

Fixe $t \in \mathfrak{P}$ um parâmetro local. O elemento t é parâmetro local também de $\mathfrak{P}'$, pois

$$\begin{aligned} v_{\mathfrak{P}'}(t) &= e\left(\mathfrak{P}' \mid \mathfrak{P}\right) \cdot v_{\mathfrak{P}}(t) \qquad \text{(da definição de índice de ramificação)} \\ &= v_{\mathfrak{P}}(t) \qquad \text{(pois } \mathfrak{P}' \mid \mathfrak{P} \text{ é não ramificada)} \\ &= 1 \qquad \text{(da propriedade de parâmetros locais)} \,. \end{aligned}$$

Como todo elemento de $S_1 \cup S_2$ é não nulo (por escolha), então pela Proposição 3.5 existem $l_i, l_j, k_i, k_j \in \mathbb{Z}$, $u_i, \widetilde{u}_j \in \mathcal{U}(\mathcal{O}_{\mathfrak{P}_1})$ e $v_i, \widetilde{v}_j \in \mathcal{U}(\mathcal{O}_{\mathfrak{P}_2})$ tais que

$$x_i = t^{l_i} \cdot u_i \,, \qquad y_i = t^{k_i} \cdot v_i \,, \qquad \widetilde{x}_j = t^{l_j} \cdot \widetilde{u}_j \qquad \text{e} \qquad \widetilde{y}_j = t^{k_j} \cdot \widetilde{v}_j \,.$$

Assim, a somatória na Equação 56 pode ser reescrita como

$$f = \frac{\sum_{i=1}^{n_1} t^{l_i+k_i} \cdot u_i \cdot v_i}{\sum_{j=1}^{n_2} t^{l_j+k_j} \cdot \widetilde{u}_j \cdot \widetilde{v}_j} \,.$$

Se definirmos

$$\eta := \min_{1 \le i \le n_1} \{l_i + k_i\} \qquad \text{e} \qquad \widetilde{\eta} := \min_{1 \le j \le n_2} \left\{l_j + k_j\right\} \,,$$

podemos reescrever f colocando as potências t^{η} e $t^{\widetilde{\eta}}$ em evidência:

$$f = \frac{t^{\eta} \cdot \left(\sum_{\eta = l_i + k_i} u_i \cdot v_i + \sum_{\eta < l_i + k_i} t^{l_i + k_i - \eta} \cdot u_i \cdot v_i \right)}{t^{\widetilde{\eta}} \cdot \left(\sum_{\widetilde{\eta} = l_j + k_j} \widetilde{u}_j \cdot \widetilde{v}_j + \sum_{\widetilde{\eta} < l_j + k_j} t^{l_j + k_j - \widetilde{\eta}} \cdot \widetilde{u}_j \cdot \widetilde{v}_j \right)} \,. \tag{57}$$

Temos que $\eta = \widetilde{\eta}$ — caso contrário, teríamos a igualdade $f + \mathfrak{P}' = 0 + \mathfrak{P}'$. Assim, podemos efetuar o cancelamento das potências de t que aparecem fora dos parênteses em (57).

Para $w \in \{1,2\}$, passando ao quociente módulo $\mathfrak{P}_w$,

$$f + \mathfrak{P}_w = \frac{\sum\limits_{\eta=l_i+k_i} (u_i + \mathfrak{P}_w) \cdot (v_i + \mathfrak{P}_w)}{\sum\limits_{\widetilde{\eta}=l_j+k_j} \left(\widetilde{u}_j + \mathfrak{P}_w\right) \cdot \left(\widetilde{v}_j + \mathfrak{P}_w\right)} .$$

Fazendo a identificação dos elementos de $\frac{\mathcal{O}_{\mathfrak{P}_w}}{\mathfrak{P}_w}$ como elementos de $\frac{\mathcal{O}_{\mathfrak{P}'}}{\mathfrak{P}'}$,

$$f + \mathfrak{P}' = \frac{\sum\limits_{\eta=l_i+k_i} \left(u_i + \mathfrak{P}'\right) \cdot \left(v_i + \mathfrak{P}'\right)}{\sum\limits_{\widetilde{\eta}=l_j+k_j} \left(\widetilde{u}_j + \mathfrak{P}'\right) \cdot \left(\widetilde{v}_j + \mathfrak{P}'\right)} .$$

Ou seja, $\alpha \in \frac{\mathcal{O}_{\mathfrak{P}_1}}{\mathfrak{P}_1} \cdot \frac{\mathcal{O}_{\mathfrak{P}_2}}{\mathfrak{P}_2}$. ◇

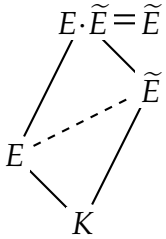
Como o compósito de extensões separáveis é separável, a tese segue da Afirmação 5.4. □

Lema 5.5. *Sejam: $K \,/\, k$ um corpo de funções; $E \mid K$ uma extensão finita e separável com fecho normal $\widetilde{E}$; e $\mathfrak{P} \in \mathbb{P}(K)$ ramificado ou inseparável em $\widetilde{E} \,\big|\, K$.*

Então $\mathfrak{P}$ é ramificado ou inseparável em $E \mid K$.

Demonstração. Segue do item 2 do Lema 5.3 — cf. Figura 32.

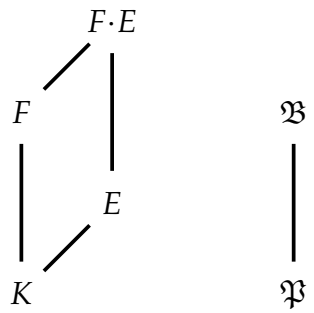
Figura 32. Ilustração do caso de uso do item 2 do Lema 5.3 (compare com a Figura 30).



□

Lema 5.6. *Sejam: $K \,/\, k$ um corpo de funções; $E \mid K$ uma extensão finita separável de corpos de funções; $\mathfrak{P} \in \mathbb{P}(K)$; $F \mid K$ uma extensão finita puramente inseparável; e $\mathfrak{B} \in \mathbb{P}(F)$ sobre $\mathfrak{P}$.*

Figura 33



Suponha que $\mathfrak{P}$ *seja um* place *de* K *ramificado ou inseparável em* $E \mid K$.
Então $\mathfrak{B}$ *é ramificado ou inseparável em* $E{\cdot}F \mid F$.

Demonstração. Seja $\mathfrak{P}_0 \in \mathbb{P}(E)$ sobre $\mathfrak{P}$ ramificado ou inseparável em $E \mid K$, e seja $\widetilde{E}$ o fecho normal de $E \mid K$.

Afirmação 5.7. *O fecho normal de* $(E{\cdot}F) \mid F$ *é* $\widetilde{E}{\cdot}F$.

Dem.: A extensão $\widetilde{E} \,\Big|\, K$ é separável, pois o fecho normal de uma extensão finita separável é separável — cf. *Proposition* 3.3.7 no livro de Bastida (1984, p. 117); então os elementos de $\widetilde{E}$ e de F que são simultaneamente separáveis e puramente inseparáveis sobre K estão no conjunto

$$\widetilde{E} \cap F = K$$

— veja o livro de Endler (1987, p. 70) para uma demonstração. A tese segue da Teoria de Galois Finita (cf. a discussão anterior à Proposição 3.92). ◇

Afirmação 5.8. $\left(\widetilde{E}{\cdot}F\right) \,\Big|\, \widetilde{E}$ *é puramente inseparável.*

Dem.: Seja $\alpha \in \widetilde{E}{\cdot}F$. Temos de mostrar que $\exists\ t \in \mathbb{N}$ tal que $\alpha^{p^t} \in \widetilde{E}$. Um elemento de $\widetilde{E}{\cdot}F$ são "combinações algébricas" de elementos de $\widetilde{E}$ e de F; então

$$\alpha = \frac{\sum_{i=1}^{r} \widetilde{e}_i \cdot f_i}{\sum_{j=1}^{s} \widetilde{e}_j \cdot f_j}\,, \qquad \text{em que} \qquad \widetilde{e}_i\,,\ \widetilde{e}_j \in \widetilde{E}\,, \qquad f_i\,,\ f_j \in F \qquad \text{e} \qquad r\,,\ s \in \mathbb{N}\,.$$

Como $F \mid K$ é puramente inseparável, então existem $t_i \in \mathbb{Z}$ e $t_j \in \mathbb{Z}$ — com $1 \leq i \leq r$ e $1 \leq j \leq s$ — tais que

$$f_i^{p^{t_i}} \in K \qquad \text{e} \qquad f_j^{p^{t_j}} \in K \,.$$

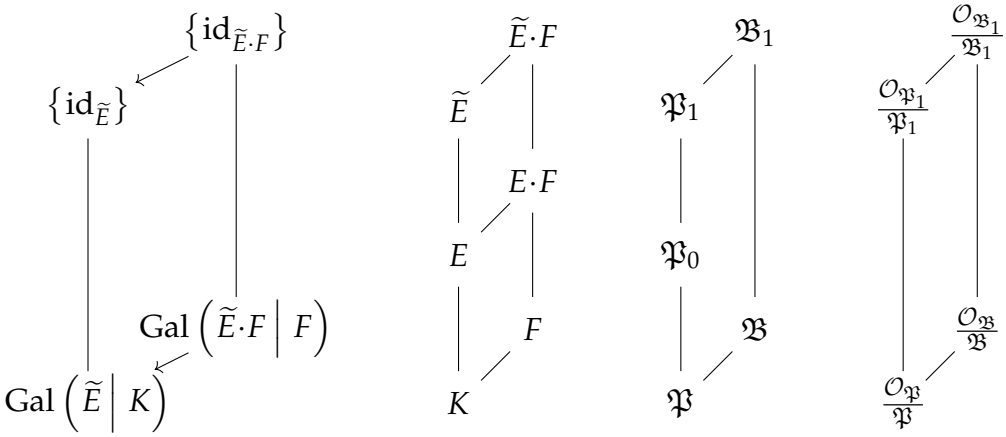
Tome $t = \max\left\{t_i, t_j \;\middle|\; 1 \leq i \leq r \,,\; 1 \leq j \leq s\right\}$. ◇

Seja $\mathfrak{P}_1 \in \mathbb{P}\left(\widetilde{E}\right)$ sobre $\mathfrak{P}_0$. Seja $\mathfrak{B}_1 \in \mathbb{P}\left(\widetilde{E}\cdot F\right)$ a única extensão de $\mathfrak{P}_1$ (a unicidade de $\mathfrak{B}_1$ segue do item 1 do Teorema 3.105). Uma vez que $\mathfrak{B}_1 \cap F \in \mathbb{P}(F)$ está sobre $\mathfrak{P}$ e $F \mid K$ é puramente inseparável, temos pelo Teorema 3.105 que $\mathfrak{B}_1$ é o único place de $E\cdot F$ sobre $\mathfrak{B}$:

$$\mathfrak{B}_1 \cap F = \mathfrak{B} \,.$$

Sejam $G_Z\left(\mathfrak{P}_1 \mid \mathfrak{P}\right)$ o grupo de decomposição de $\mathfrak{P}_1$ sobre $\mathfrak{P}$ e $G_T\left(\mathfrak{P}_1 \mid \mathfrak{P}\right)$ o grupo de inércia.

Figura 34. Ilustração para a demonstração do Lema 5.6.



Considere o isomorfismo natural (cf. Equação 36)

$$\begin{aligned} \Psi : \mathrm{Gal}\left(\widetilde{E}\cdot F \;\middle|\; F\right) &\to \mathrm{Gal}\left(\widetilde{E} \;\middle|\; K\right) \\ \sigma &\mapsto \sigma\restriction_{\widetilde{E}} \,. \end{aligned}$$

O isomorfismo Ψ induz uma imersão natural entre os grupos de decomposição (cf. Proposição 3.92):

$$\begin{array}{ccccccccc} \kappa : & G_Z\left(\mathfrak{B}_1 \mid \mathfrak{B}\right) & \subseteq & \mathrm{Gal}\left(\widetilde{E}\cdot F \;\middle|\; F\right) & \hookrightarrow & G_Z\left(\mathfrak{P}_1 \mid \mathfrak{P}\right) & \subseteq & \mathrm{Gal}\left(\widetilde{E} \;\middle|\; K\right) \\ & \sigma & & & \mapsto & \sigma\restriction_{\widetilde{E}} \,. & & \end{array}$$

Afirmação 5.9. *κ é isomorfismo.*

Dem.: Pela Afirmação 5.8 e pelo Teorema 3.105, temos que $\mathfrak{B}_1$ é a única extensão de $\mathfrak{P}_1$ em $\widetilde{E}\cdot F$. Assim, κ é uma correspondência biunívoca entre os automorfismos em $G_Z(\mathfrak{B}_1 \mid \mathfrak{B})$ que fixam $\mathfrak{B}_1$ e os automorfismos em $G_Z(\mathfrak{P}_1 \mid \mathfrak{P})$ que fixam $\mathfrak{P}_1$. A tese segue do fato de toda restrição de homomorfismo ser homomorfismo. ◇

Analogamente, o isomorfismo κ induz uma imersão entre os grupos de inércia:

$$\kappa\left[G_T(\mathfrak{B}_1 \mid \mathfrak{B})\right] \subseteq G_T(\mathfrak{P}_1 \mid \mathfrak{P}) .$$

Seja

$$\varphi := \kappa \restriction_{G_T(\mathfrak{B}_1 \mid \mathfrak{B})} : G_T(\mathfrak{B}_1 \mid \mathfrak{B}) \hookrightarrow G_T(\mathfrak{P}_1 \mid \mathfrak{P}) .$$

Afirmação 5.10. *φ é isomorfismo.*

Dem.: Como as extensões

$$\frac{\mathcal{O}_{\mathfrak{B}_1}}{\mathfrak{B}_1} \,\Big|\, \frac{\mathcal{O}_{\mathfrak{P}_1}}{\mathfrak{P}_1} \qquad \text{e} \qquad \frac{\mathcal{O}_{\mathfrak{B}}}{\mathfrak{B}} \,\Big|\, \frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}$$

são puramente inseparáveis (pelo item 3 do Teorema 3.105), temos que

$$\left[\frac{\mathcal{O}_{\mathfrak{B}_1}}{\mathfrak{B}_1} : \frac{\mathcal{O}_{\mathfrak{P}_1}}{\mathfrak{P}_1}\right]_{\mathbf{s}} = 1 \qquad \text{e} \qquad \left[\frac{\mathcal{O}_{\mathfrak{B}}}{\mathfrak{B}} : \frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}\right]_{\mathbf{s}} = 1 . \tag{58}$$

Por outro lado, da transitividade do grau,

$$\left[\frac{\mathcal{O}_{\mathfrak{B}_1}}{\mathfrak{B}_1} : \frac{\mathcal{O}_{\mathfrak{P}_1}}{\mathfrak{P}_1}\right] \cdot \left[\frac{\mathcal{O}_{\mathfrak{P}_1}}{\mathfrak{P}_1} : \frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}\right] = \left[\frac{\mathcal{O}_{\mathfrak{B}_1}}{\mathfrak{B}_1} : \frac{\mathcal{O}_{\mathfrak{B}}}{\mathfrak{B}}\right] \cdot \left[\frac{\mathcal{O}_{\mathfrak{B}}}{\mathfrak{B}} : \frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}\right] . \tag{59}$$

Então

$$\begin{aligned} &\left(f(\mathfrak{B}_1 \mid \mathfrak{P}_1)_{\mathbf{i}} \cdot f(\mathfrak{B}_1 \mid \mathfrak{P}_1)_{\mathbf{s}}\right) \cdot \left(f(\mathfrak{P}_1 \mid \mathfrak{P})_{\mathbf{i}} \cdot f(\mathfrak{P}_1 \mid \mathfrak{P})_{\mathbf{s}}\right) \\ =&\left(f(\mathfrak{B}_1 \mid \mathfrak{B})_{\mathbf{i}} \cdot f(\mathfrak{B}_1 \mid \mathfrak{B})_{\mathbf{s}}\right) \cdot \left(f(\mathfrak{B} \mid \mathfrak{P})_{\mathbf{i}} \cdot f(\mathfrak{B} \mid \mathfrak{P})_{\mathbf{s}}\right) . \end{aligned}$$

Usando (58) e a transitividade do grau de inseparabilidade, podemos efetuar cancelamentos membro a membro, para obtermos:

$$f(\mathfrak{B}_1 \mid \mathfrak{B})_{\mathbf{s}} = f(\mathfrak{P}_1 \mid \mathfrak{P})_{\mathbf{s}} . \tag{60}$$

Assim, do Teorema 3.87,

$$\left|G_Z\left(\mathfrak{B}_1 \mid \mathfrak{B}\right) : G_T\left(\mathfrak{B}_1 \mid \mathfrak{B}\right)\right| = \left|G_Z\left(\mathfrak{P}_1 \mid \mathfrak{P}\right) : G_T\left(\mathfrak{P}_1 \mid \mathfrak{P}\right)\right| .$$

Pelo Teorema de Lagrange,

$$\frac{\left|G_Z\left(\mathfrak{B}_1 \mid \mathfrak{B}\right)\right|}{\left|G_T\left(\mathfrak{B}_1 \mid \mathfrak{B}\right)\right|} = \frac{\left|G_Z\left(\mathfrak{P}_1 \mid \mathfrak{P}\right)\right|}{\left|G_T\left(\mathfrak{P}_1 \mid \mathfrak{P}\right)\right|} ;$$

e, como κ é isomorfismo, temos a igualdade das ordens dos numeradores. Portanto,

$$\kappa\left[G_T\left(\mathfrak{B}_1 \mid \mathfrak{B}\right)\right] = G_T\left(\mathfrak{P}_1 \mid \mathfrak{P}\right) ,$$

pois κ é bijeção pela Afirmação 5.9. ◇

Da hipótese e da Proposição 4.5, segue que o *place* $\mathfrak{P}$ é ramificado ou inseparável em $\widetilde{E} \mid K$. Então $\mathfrak{B}$ é ramificado ou inseparável em $\left(\widetilde{E}\cdot F\right) \mid F$, pois

$$e\left(\mathfrak{B}_1 \mid \mathfrak{B}\right) \cdot f\left(\mathfrak{B}_1 \mid \mathfrak{B}\right)_{\mathbf{i}} \overset{\text{Prop. 4.2}}{=} \left|G_T\left(\mathfrak{B}_1 \mid \mathfrak{B}\right)\right| \overset{\text{Af. 5.10}}{=} \left|G_T\left(\mathfrak{P}_1 \mid \mathfrak{P}\right)\right|$$

$$\overset{\text{Prop. 4.2}}{=} e\left(\mathfrak{P}_1 \mid \mathfrak{P}\right) \cdot f\left(\mathfrak{P}_1 \mid \mathfrak{P}\right)_{\mathbf{i}} > 1 .$$

Pelo Lema 5.5 (combinado com a Afirmação 5.7), temos que $\mathfrak{B}$ é ramificado ou inseparável em $(E\cdot F) \mid F$. □

Lema 5.11. *Seja $E \mid K$ uma extensão galoisiana de corpos de funções com corpo de constantes k. Então para todo $\sigma \in \mathrm{Gal}\left(E \mid K\right) \setminus \{\mathrm{id}_E\}$, o conjunto*

$$A_\sigma = \left\{\mathfrak{B} \in \mathbb{P}(E) \;\middle|\; \sigma(\mathfrak{B}) \neq \mathfrak{B}\right\}$$

é infinito.

Demonstração. Por absurdo, suponha que existe $\sigma \neq \mathrm{id}_E$ tal que A_σ seja finito; digamos,

$$A_\sigma = \{\mathfrak{B}_1, \ldots, \mathfrak{B}_m\} \tag{61}$$

com $m := |A_\sigma| < \infty$. Seja K_1 o corpo fixo de σ. Por definição de A_σ, temos que $\sigma(\mathfrak{B}) = \mathfrak{B}$, para todo *place* $\mathfrak{B} \in \mathbb{P}(E) \setminus A_\sigma$. Como σ não é o automorfismo identidade em E, então existe $y_1 \in E \setminus K_1$. Fixe $i \in \{1, 2, \ldots, m\}$.

Afirmação 5.12. *Existe* $y_2 \in K_1 \setminus k$ *tal que* $v_{\mathfrak{B}_i}(y_2) > 0$.

Dem.: Como $E \,/\, k$ é uma extensão geométrica de $K \,/\, k$ por hipótese, então o corpo intermediário K_1 é um corpo de funções sobre k.

Para cada $r \in \{1, 2, \ldots, m\}$, seja $\mathfrak{P}_r := K_1 \cap \mathfrak{B}_r$. Pelo Teorema de Aproximação, existe $\alpha \in K_1$ tal que $v_{\mathfrak{P}_r}(\alpha) > 0$ ($\forall\, r \in \{1, 2, \ldots, m\}$). Assim, da definição de índice de ramificação,

$$v_{\mathfrak{B}_r}(\alpha) = \underbrace{e(\mathfrak{B}_r \mid \mathfrak{P}_r)}_{\geq 1} \cdot v_{\mathfrak{P}_r}(\alpha) > 0 \,.$$

Tome $y_2 := \alpha$. ◇

Pela Afirmação 5.12, existe $j \in \mathbb{N}$ grande o suficiente tal que

$$\begin{aligned} 0 &< v_{\mathfrak{B}_i}(y_1) + j \cdot v_{\mathfrak{B}_i}(y_2) \\ &= v_{\mathfrak{B}_i}\left(y_1 \cdot y_2^j\right) . \end{aligned}$$

Afirmação 5.13. $y_1 \cdot y_2^j \notin K_1$.

Dem.: Se existisse $\alpha \in K_1$ com $y_1 \cdot y_2^j = \alpha$, então operando em E teríamos que $y_1 = \frac{\alpha}{y_2^j}$, que é um elemento de K_1: absurdo, pois $y_1 \notin K_1$. ◇

Afirmação 5.14. σ *permuta transitivamente os* places *de* A_σ.

Dem.: Basta verificar que $\sigma(\mathfrak{B}_i) \in A_\sigma$. Se fosse $\sigma(\mathfrak{B}_i) \in \mathbb{P}(E) \setminus A_\sigma$, então teríamos que $\sigma(\mathfrak{B}_i) = \mathfrak{B}_i$, uma contradição com a definição de A_σ. ◇

Sejam $c \neq 1$ uma constante em k e $y := y_1 \cdot y_2^j + c$.

Afirmação 5.15. $y \notin K_1$.

Dem.: Prova análoga à demonstração da Afirmação 5.13. ◇

Como c é uma constante, temos que $v_{\mathfrak{B}_i}(c) = 0$; então, pela Desigualdade Triangular Estrita (Teorema 3.10),

$$v_{\mathfrak{B}_i}(y) = 0 \,.$$

Afirmação 5.16.

$$\big(\sigma(y)\big)^E = (y)^E \ .$$

Dem.: Seja $\mathfrak{B} \in \mathbb{P}(E)$ arbitrário.

Se $\sigma(\mathfrak{B}) = \mathfrak{B}$, então

$$v_{\mathfrak{B}}\left(\sigma(y)\right) = v_{\sigma(\mathfrak{B})}\left(\sigma(y)\right) = v_{\mathfrak{B}}\left(\sigma^{-1}\big(\sigma(y)\big)\right) = v_{\mathfrak{B}}\left(y\right) \ .$$

Se $\sigma(\mathfrak{B}) \neq \mathfrak{B}$, então $\sigma(\mathfrak{B}) \in A_\sigma$. Pela Afirmação 5.14, existe $l \in \{1, 2, \ldots, m\}$ tal que $\mathfrak{B} = \sigma(\mathfrak{B}_l)$. O restante da prova deste caso é análogo:

$$v_{\mathfrak{B}}\left(\sigma(y)\right) = v_{\sigma(\mathfrak{B}_l)}\left(\sigma(y)\right) = v_{\mathfrak{B}_l}\left(\sigma^{-1}\big(\sigma(y)\big)\right) = v_{\mathfrak{B}_l}\left(y\right) = 0 \ .$$

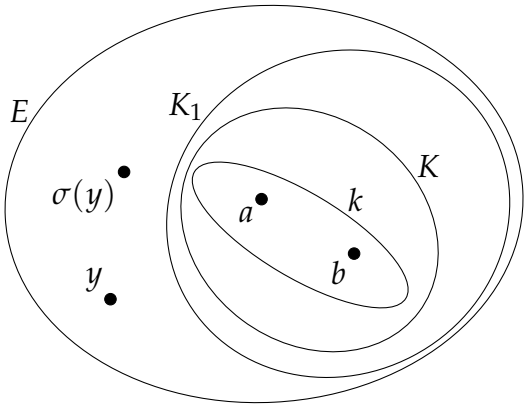
◇

Da igualdade dos divisores principais, segue que $\sigma(y)$ e y "diferem" por uma constante:

$$\sigma(y) = a \cdot y \tag{62}$$

com $a \in k$ — cf. a Equação 23.

Figura 35. Os elementos a, b, y e $\sigma(y)$ no corpo de funções $E \,/\, k$.



Como o elemento identidade $1 \in k$ também é constante, temos por argumentos totalmente análogos que

$$v_{\mathfrak{B}_i}\left(y + 1\right) = 0 \ ,$$

e que existe $b \in k$ tal que

$$\sigma(1 + y) = b \cdot (1 + y) \ . \tag{63}$$

Então

$$1 + a \cdot y \overset{\text{Eq. 62}}{=} 1 + \sigma(y) = \sigma(1) + \sigma(y) = \sigma(1 + y) \overset{\text{Eq. 63}}{=} b \cdot (1 + y) = b + b \cdot y \,. \tag{64}$$

Como $y \notin K_1$ e $K_1 \supseteq K \supseteq k$, segue que $y \notin k$.

Afirmação 5.17. $a = b$.

Dem.: Por (64), temos que $(a - b) \cdot y = b - 1$. Se fosse $a \neq b$, então

$$y = \frac{b-1}{a-b} \in k \,,$$

um absurdo. ◇

Por (64) e pela Afirmação 5.17, segue que $a = 1$ e, portanto, $\sigma(y) = y$. Assim, $y \in K_1$: contradição com a Afirmação 5.15. □

5.2 LIMITAÇÃO PARA O GÊNERO DE UM COMPÓSITO DE CORPOS DE FUNÇÕES

Esta seção corresponde à terceira seção do artigo de Álvarez-García e Villa-Salvador (2010). Os dois principais resultados são:

- o análogo da desigualdade de Castelnuovo-Severi; e
- o análogo do resultado de Madden-Valentini sobre os *C-improvements*.

5.2.1 O análogo da desigualdade de Castelnuovo-Severi

Para um corpo de funções $K \,/\, k$ com gênero g_K, seja

$$g'_K := \max\{g_K, 1\} \,. \tag{65}$$

A escolha deste número máximo evita a seleção de um valor nulo.

O resultado análogo da Desigualdade de Castelnuovo-Severi (Teorema 3.104) expressará o gênero de um compósito de corpos de funções $F = F_1 \cdot F_2$ majorado por uma expressão que contemplará, dentre outros termos:

- os números g'_{F_1} e g'_{F_2}, definidos em (65); e
- o mínimo dos graus de places no conjunto

$$\left\{ \deg_k(\mathfrak{P}) \;\middle|\; \mathfrak{P} \in \mathbb{P}(F_1) \right\} .$$

Lema 5.18. *Sejam: $F \,/\, k$ um corpo de funções com corpo de constantes separavelmente fechado; $E \mid F$ uma extensão finita geométrica separável; e*

$$d := \min \left\{ \deg_k(\mathfrak{R}) \;\middle|\; \mathfrak{R} \in \mathbb{P}(F) \right\} .$$

Então temos os seguintes fatos.

1. *Existem infinitos* places *em F que se decompõem completamente em $E \mid F$.*
2. *Podemos escolher os* places $\mathfrak{R} \in \mathbb{P}(F)$ *no item 1 de modo que*

$$\deg_k(\mathfrak{R}) \leq 2 \cdot g'_F \cdot d \, .$$

Demonstração. Seja $\mathfrak{P} \in \mathbb{P}(F)$ tal que $d = \deg_k(\mathfrak{P})$. Pela Proposição 3.35, existe $x \in F$ com divisor polo $(x)^F_\infty = (2 \cdot g'_F)\mathfrak{P}$. Assim, pelo Teorema 3.18,

$$\Big[F : k(x) \Big] = \deg_k\Big((x)^F_\infty \Big) = 2 \cdot g'_F \cdot d \, . \tag{66}$$

Em particular, $F \mid k(x)$ é finita.

Sejam:

- F_0 o fecho separável de $k(x)$ em F; e
- E_0 o fecho separável de $k(x)$ em E.

Da definição de F_0, a extensão $F \mid F_0$ é puramente inseparável. Pelo Teorema 3.98, temos que E_0 e F são linearmente disjuntos sobre F_0.

Afirmação 5.19. $E = E_0 \cdot F$.

Dem.: Por absurdo, suponha que $E \supsetneq E_0 \cdot F$. Então

$$\Big[E : E_0 \cdot F \Big] > 1 \, . \tag{67}$$

Além disso,

$$\begin{aligned}\left[F : k(x)\right]_{\mathbf{i}} &= [E : F]_{\mathbf{i}} \cdot \left[F : k(x)\right]_{\mathbf{i}} \qquad \text{(pois } E \mid F \text{ é separável)} \\ &= \left[E : k(x)\right]_{\mathbf{i}} \\ &= [E : E_0{\cdot}F]_{\mathbf{i}} \cdot [E_0{\cdot}F : F]_{\mathbf{i}} \cdot \left[F : k(x)\right]_{\mathbf{i}} \\ &\qquad \text{(da transitividade do grau de inseparabilidade)} \ .\end{aligned}$$

Então efetuando cancelamento membro a membro, podemos inferir que o primeiro fator no produto à direita da última igualdade é igual a um:

$$[E : E_0{\cdot}F]_{\mathbf{i}} = 1 \ . \tag{68}$$

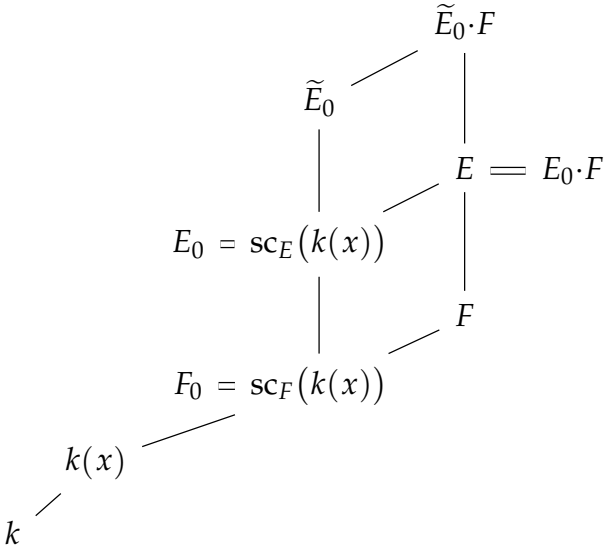
Logo,

$$[E : E_0]_{\mathbf{s}} \geq [E : E_0{\cdot}F]_{\mathbf{s}} \overset{\text{Eq. 68}}{=} [E : E_0{\cdot}F]_{\mathbf{s}} \cdot [E : E_0{\cdot}F]_{\mathbf{i}} = \left[E : E_0{\cdot}F\right] \overset{\text{Exp. 67}}{>} 1 \ .$$

Contradição com o fato de a extensão $E \mid E_0$ ser puramente inseparável. ◇

Seja $\widetilde{E}_0$ o fecho normal de $E_0 \mid F_0$.

Figura 36. Ilustração de como o fecho normal $\widetilde{E}_0$ de $E_0 \mid F_0$ está relacionado com os demais corpos de funções considerados até o momento.

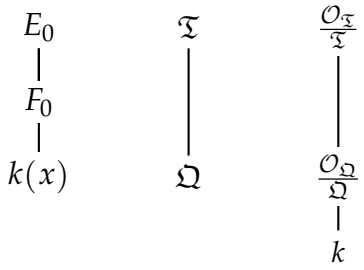


Afirmação 5.20. *Existem infinitos* places *de grau um em F_0 que se decompõem completamente em $E_0 \mid F_0$.*

Dem.: Como k é infinito (Observação 3.94), existem infinitos *places* de grau um em $\mathbb{P}\big(k(x)\big)$. Na extensão $E_0 \mid k(x)$, existe um número finito de *places* em $\mathbb{P}\big(k(x)\big)$ que são ramificados ou inseparáveis — cf. Teorema 3.89. Em particular, quase todo *place* em $\mathbb{P}\big(k(x)\big)$ de grau um é não ramificado e separável em $E_0 \mid k(x)$. Seja então $\mathfrak{Q} \in \mathbb{P}\big(k(x)\big)$ um *place* de grau $\deg_k(\mathfrak{Q}) = 1$ não ramificado e separável em $E_0 \mid k(x)$.

Seja $\mathfrak{T} \in \mathbb{P}(E_0)$ sobre $\mathfrak{Q}$.

Figura 37. Ilustração para a demonstração da Afirmação 5.20.



Como as extensões $E \mid F$ e $F \mid k(x)$ são finitas, temos que a extensão intermediária $E_0 \mid k(x)$ de $E \mid k(x)$ também é finita. Pela Proposição 3.44, a extensão $\frac{\mathcal{O}_\mathfrak{T}}{\mathfrak{T}} \,\Big|\, \frac{\mathcal{O}_\mathfrak{Q}}{\mathfrak{Q}}$ é finita (e, portanto, algébrica). Como $\mathfrak{Q}$ é de grau um sobre k, temos que $\left[\frac{\mathcal{O}_\mathfrak{Q}}{\mathfrak{Q}} : k\right] = 1$ (e $\therefore \frac{\mathcal{O}_\mathfrak{Q}}{\mathfrak{Q}} = k$); e $\frac{\mathcal{O}_\mathfrak{T}}{\mathfrak{T}}$ é uma extensão algébrica de k. Da hipótese de k ser separavelmente fechado, segue que $\frac{\mathcal{O}_\mathfrak{T}}{\mathfrak{T}} = k$ e, portanto, $f(\mathfrak{T} \mid \mathfrak{Q}) = 1$.

Então, pela Igualdade Fundamental, o *place* $\mathfrak{Q}$ decompõe-se completamente em $E_0 \mid k(x)$. A tese segue da Observação 3.52. ◇

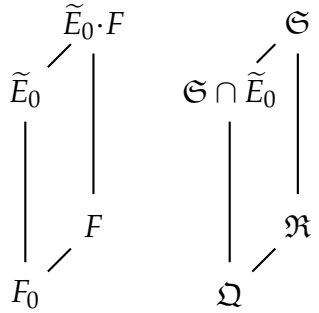
Afirmação 5.21. *Existem infinitos* places *em F que se decompõem completamente em $\widetilde{E}_0 \cdot F \,\Big|\, F$.*

Dem.: Seja $\mathfrak{Q} \in \mathbb{P}(F_0)$ um *place* de grau $\deg_k(\mathfrak{Q}) = 1$ que se decompõe completamente em $E_0 \mid F_0$ (dado pela Afirmação 5.20). Como a extensão

$F \mid F_0$ é puramente inseparável, então existe um único *place* $\mathfrak{R} \in \mathbb{P}(F)$ sobre $\mathfrak{Q}$ (item 1 do Teorema 3.105).

Seja $\mathfrak{S} \in \mathbb{P}\left(\widetilde{E}_0 \cdot F\right)$ um *place* sobre $\mathfrak{R}$. Então $\mathfrak{S} \cap \widetilde{E}_0 \in \mathbb{P}\left(\widetilde{E}_0\right)$ é um *place* sobre $\mathfrak{Q}$ (veja a Figura 38). Pelo Lema 3.60, temos que o *place* $\mathfrak{Q}$ decompõe-se completamente em $\widetilde{E}_0 \,\Big|\, F_0$; assim, pela Proposição 4.2, o grupo de inércia da extensão $\mathfrak{S} \cap \widetilde{E}_0 \mid \mathfrak{Q}$ é trivial. Como o grupo de inércia $G_T(\mathfrak{S} \mid \mathfrak{R})$ é imersível no grupo $G_T\left(\mathfrak{S} \cap \widetilde{E}_0 \,\Big|\, \mathfrak{Q}\right)$ (Proposição 3.92), temos que a extensão $\mathfrak{S} \mid \mathfrak{R}$ é não ramificada (Proposição 4.2). Do fato de k ser separavelmente fechado, $\frac{\mathcal{O}_{\mathfrak{S}}}{\mathfrak{S}} = \frac{\mathcal{O}_{\mathfrak{R}}}{\mathfrak{R}} = k$. Segue que $\mathfrak{R}$ decompõe-se completamente em $\left(\widetilde{E}_0 \cdot F\right) \,\Big|\, F$. $\diamond$

Figura 38. Extensões de $\mathfrak{Q}$ na prova da Afirmação 5.21.



Da Afirmação 5.21, temos que existem infinitos *places* $\mathfrak{R} \in \mathbb{P}(F)$ que se decompõem completamente em $\widetilde{E}_0 \cdot F \,\Big|\, F$.

(Item 1): Pela Observação 3.52, segue que a decomposição completa de $\mathfrak{R}$ ocorre também em $E_0 \cdot F \mid F$. A tese segue da Afirmação 5.19.

(Item 2): O grau de $\mathfrak{R}$ sobre k é igual a

$$\begin{aligned}
\deg_k(\mathfrak{R}) &= f(\mathfrak{R} \mid \mathfrak{Q}) \cdot \deg_k(\mathfrak{Q}) \\
&= f(\mathfrak{R} \mid \mathfrak{Q}) \\
&\leq \left[F : F_0\right] \qquad \text{(do Corolário 3.49)} \\
&\leq \left[F : F_0\right] \cdot \left[F_0 : k(x)\right] \\
&= \left[F : k(x)\right] \qquad \text{(da transitividade do grau)} \\
&= 2 \cdot d \cdot g_F' \qquad \text{(da Equação 66)} \ ,
\end{aligned}$$

como desejado. $\square$

Lema 5.22. *Sejam: k um corpo separavelmente fechado; $F \,/\, k$ um corpo de funções; $F_1 \,/\, k$ um subcorpo de F tal que $F \mid F_1$ é uma extensão separável de grau $n := \left[F : F_1\right] > 1$; $y \in F$ um elemento tal que $F = F_1(y)$; e*

$$d_1 := \min\left\{ \deg_k(\mathfrak{P}) \;\middle|\; \mathfrak{P} \in \mathbb{P}(F_1) \right\} .$$

Então existem infinitos places $\mathfrak{P} \in \mathbb{P}(F_1)$ *de grau*

$$\deg_k(\mathfrak{P}) \leq 2 \cdot g'_{F_1} \cdot d_1$$

com as seguintes propriedades.

1. $\mathfrak{P}$ *possui n extensões distintas*

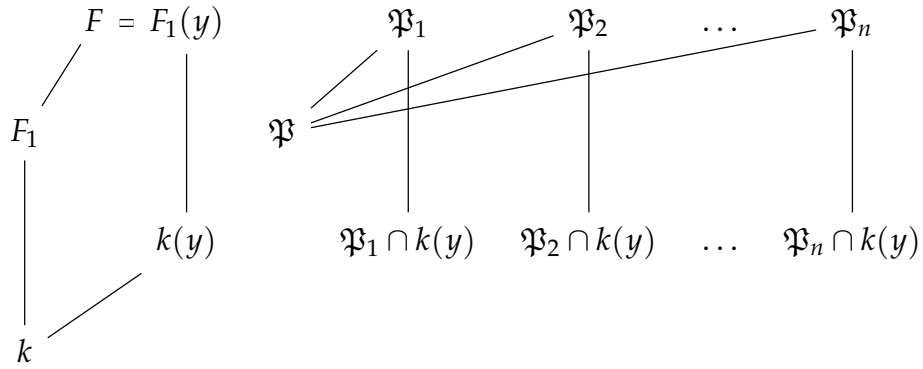
$$\mathfrak{P}_1 \,, \quad \ldots \,, \quad \mathfrak{P}_n \in \mathbb{P}(F) \,.$$

2. *As restrições*

$$\mathfrak{P}_1 \cap k(y) \,, \quad \ldots \,, \quad \mathfrak{P}_n \cap k(y) \in \mathbb{P}\big(k(y)\big)$$

são places *dois a dois distintos.*

Figura 39. Ilustração para o Lema 5.22.



Demonstração. Seja $\varphi(z) := m_{y,F_1}(z) = z^n + a_{n-1}z^{n-1} + \ldots + a_1 T + a_0 \in F_1\,[z]$ o polinômio minimal de y sobre F_1. Pelo Lema 5.18, existem infinitos *places* $\mathfrak{P} \in \mathbb{P}(F_1)$ com as seguintes propriedades:

- $\mathfrak{P}$ decompõe-se completamente em $F \mid F_1$; e

- $\deg_k(\mathfrak{P}) \leq 2 \cdot g'_{F_1} \cdot d_1$.

Pela hipótese, $F = F_1(y)$; assim, $\gamma := \left\{1, y, y^2, \ldots, y^{n-1}\right\}$ é uma base para F sobre F_1. Do Teorema 3.68, temos que γ é uma base inteira para quase todos esses *places* $\mathfrak{P}$.

Pelo Teorema de Kummer (item 2 do Teorema 3.75), existe uma correspondência entre a decomposição do polinômio $\overline{\varphi}(z) \in \left(\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}\right)[z]$ em fatores irredutíveis $\overline{\varphi_i} = \gamma_i \in \left(\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}\right)[z]$ e a decomposição de $\mathfrak{P}$ em *places* $\mathfrak{P}_i \in \mathbb{P}(F)$ sobre $\mathfrak{P}$ (com $i \in \{1, 2, \ldots, n\}$). Como a quantidade de *places* em F_1 que estendem $\mathfrak{P}$ coincide com o grau do polinômio minimal de y sobre F, devemos ter que

$$\overline{\varphi}(z) = \prod_{i=1}^{n} (z - c_i) \ ,$$

com os elementos $c_i \in \frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}$ distintos dois a dois.

Para cada $i \in \{1, 2, \ldots, n\}$, escolha $b_i \in \mathcal{O}_{\mathfrak{P}}$ de modo que

$$c_i = b_i + \mathfrak{P} \tag{69}$$

e

$$\varphi_i(z) = z - b_i \ . \tag{70}$$

Seja $p := \mathrm{char}(k)$.

Afirmação 5.23. *Existem $m \in \mathbb{N} \cup \{0\}$ e $\beta_1, \ldots, \beta_n \in \mathcal{O}_{\mathfrak{P}}$ tais que*

$$b_i^{p^m} + \mathfrak{P} = \beta_i + \mathfrak{P} \ . \tag{71}$$

Dem.: Seja $i \in \{1, 2, \ldots, n\}$.

Se $b_i \in \mathfrak{P}$, então $b_i^{p^s} \in \mathfrak{P}$ para todo $s \in \mathbb{N} \cup \{0\}$; neste caso, bastaria tomar $\beta_i = 0$.

Se $b_i \in \mathcal{O}_{\mathfrak{P}} \setminus \mathfrak{P}$, então $\overline{b_i} \neq \overline{0}$ módulo $\mathfrak{P}$. O corpo $\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}}$ pode ser visto como uma extensão finita (e, portanto, algébrica) de k. Como toda extensão algébrica de k é puramente inseparável, existem $m_i \in \mathbb{N} \cup \{0\}$ e $\alpha_i \in \mathcal{O}_{\mathfrak{P}}$ tais que $b_i^{p^{m_i}} + \mathfrak{P} = \alpha_i + \mathfrak{P} \in k$. Escolha $m := \sum_{j=1}^{n} m_j$ e $\beta_i := \alpha_i^{p^{m-m_i}}$. Tomando a p^{m-m_i}-ésima potência, teremos que

$$\begin{aligned} \beta_i + \mathfrak{P} = \alpha_i^{p^{m-m_i}} + \mathfrak{P} &= \left(b_i^{p^{m_i}}\right)^{p^{m-m_i}} + \mathfrak{P} \\ &= b_i^{p^m} + \mathfrak{P} \ , \end{aligned}$$

como desejado. ◇

Afirmação 5.24.

$$v_{\mathfrak{P}_i}(y - b_i) > 0\,, \qquad \forall\, i \in \{1, 2, \ldots, n\}\,.$$

Dem.: Seja $i \in \{1, 2, \ldots, n\}$. Pelo Teorema de Kummer (item 1(a)ii do Teorema 3.75), temos que $\varphi_i(y) \in \mathfrak{P}_i$. Ou seja, $v_{\mathfrak{P}_i}\left(\varphi_i(y)\right) > 0$. A tese segue da Equação 70. ◇

Pela Afirmação 5.23, temos que

$$b_i^{p^m} - \beta_i \in \mathfrak{P}\,, \tag{72}$$

que é equivalente a dizer que

$$v_{\mathfrak{P}}\left(b_i^{p^m} - \beta_i\right) > 0\,.$$

Por definição de índice de ramificação,

$$v_{\mathfrak{P}_i}\left(b_i^{p^m} - \beta_i\right) > 0\,. \tag{73}$$

Por outro lado, como a característica de k é positiva, temos que

$$\begin{aligned} 0 < p^m \cdot v_{\mathfrak{P}_i}(y - b_i) \quad & \text{(da Afirmação 5.24)} \\ = v_{\mathfrak{P}_i}\left((y - b_i)^{p^m}\right) \quad & \text{(da definição de valoração)}\,; \end{aligned}$$

ou seja,

$$v_{\mathfrak{P}_i}\left(y^{p^m} - b_i^{p^m}\right) > 0\,. \tag{74}$$

Portanto,

$$\begin{aligned} v_{\mathfrak{P}_i}\left(y^{p^m} - \beta_i\right) &= v_{\mathfrak{P}_i}\left(\left(y^{p^m} - b_i^{p^m}\right) + \left(b_i^{p^m} - \beta_i\right)\right) \\ &\geq \min\left\{v_{\mathfrak{P}_i}\left(y^{p^m} - b_i^{p^m}\right), v_{\mathfrak{P}_i}\left(b_i^{p^m} - \beta_i\right)\right\} \\ &> 0 \qquad \text{(pelas equações 73 e 74)}\,. \end{aligned} \tag{75}$$

Afirmação 5.25. *Vale a implicação*

$$c_i^{p^m} \neq c_j^{p^m} \;\Rightarrow\; \beta_i \neq \beta_j \ .$$

Dem.: Temos as seguintes implicações:

$$\begin{aligned}
\beta_i = \beta_j \quad &\Rightarrow \quad \beta_i + \mathfrak{P} = \beta_j + \mathfrak{P} \\
&\Rightarrow \quad b_i^{p^m} + \mathfrak{P} = b_j^{p^m} + \mathfrak{P} \qquad \text{(por (72))} \\
&\Rightarrow \quad (b_i + \mathfrak{P})^{p^m} = \left(b_j + \mathfrak{P}\right)^{p^m} \\
&\Rightarrow \quad c_i^{p^m} = c_j^{p^m} \qquad \text{(de (69))} \ .
\end{aligned}$$

Então

$$0 = c_i^{p^m} - c_j^{p^m} = \left(c_i - c_j\right)^{p^m} ,$$

o que implicaria que $c_i = c_j$. ◇

Afirmação 5.26. *As restrições $\mathfrak{P}_i \cap k\left(y^{p^m}\right)$ são duas a duas distintas.*

Dem.: Por absurdo, suponha o contrário; digamos,

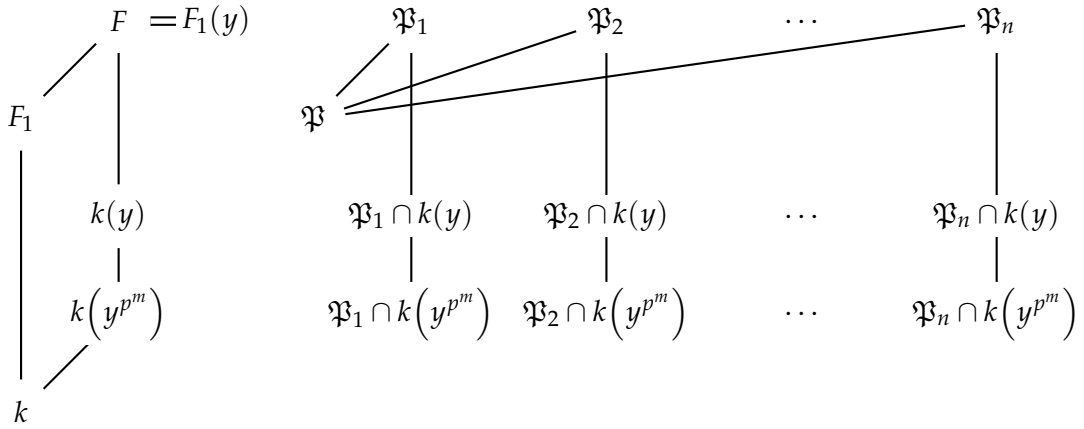
$$\mathfrak{P}_1 \cap k\left(y^{p^m}\right) = \mathfrak{P}_2 \cap k\left(y^{p^m}\right) \ . \tag{76}$$

Sejam:

$$\begin{cases} u := y^{p^m} - \beta_1 \in \mathfrak{P}_1 \cap k\left(y^{p^m}\right) \ ; \ \text{e} \\ w := y^{p^m} - \beta_2 \in \mathfrak{P}_2 \cap k\left(y^{p^m}\right) \ . \end{cases}$$

Pela igualdade dos *places* dada na Equação 76, a diferença entre w e u seria um elemento de $\mathfrak{P}_1 \cap k\left(y^{p^m}\right)$ e, portanto, pertenceria também a $\mathfrak{P}_1$: $\beta_1 - \beta_2 \in \mathfrak{P}_1$. Absurdo, pois $c_1 \neq c_2$. ◇

Figura 40. Considerar as restrições dos *places* $\mathfrak{P}_1, \ldots, \mathfrak{P}_n$ a $k\left(y^{p^m}\right)$ praticamente encerrará a demonstração.



Se existissem $i, j \in \{1, 2, \ldots, n\}$ distintos com $\mathfrak{P}_i \cap k(y) = \mathfrak{P}_j \cap k(y)$, teríamos a igualdade de *places* também nas restrições a $k\left(y^{p^m}\right)$: uma contradição com a Afirmação 5.26. Segue que os *places* $\mathfrak{P}_i \cap k(y)$ são distintos dois a dois. □

Sejam $F \,/\, k$ um corpo de funções e F_1, F_2 dois subcorpos de F tais que $F = F_1 \cdot F_2$. Os mecanismos de obtenção de cotas para o gênero do compósito F nas demonstrações do Teorema de Castelnuovo-Severi (Teorema 3.104) e do Teorema de Castelnuovo (STICHTENOTH, 2009, p. 146) são parecidos. O receituário é constituído dos seguintes passos:

(Castel.1) a escolha de um conjunto $\gamma \subseteq F$ com $\left[F : F_1\right]$ elementos, por meio de um critério específico;

(Castel.2) a prova de que γ é uma base de F sobre F_1, por meio do uso da Desigualdade Estrita;

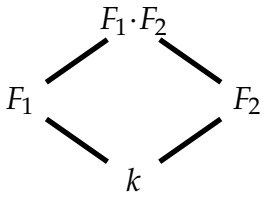
(Castel.3) a escolha de um conveniente divisor "auxiliar" $\mathtt{C} \in \mathrm{Div}(F)$, que realiza a estimativa do gênero do compósito; e

(Castel.4) a redução do problema a extensões constantes.

A seguir, vamos estimar o gênero de um compósito de corpos de funções sem impor condições acerca do corpo de constantes. O procedimento descrito acima será repetido, com ligeiras modificações.

Lema 5.27. *Sejam: $F \,/\, k$ um corpo de funções com corpo de constantes separavelmente fechado; $F_1 \,/\, k$ e $F_2 \,/\, k$ subcorpos de $F \,/\, k$ tais que $F = F_1 \cdot F_2$ e $F \mid F_1$ é separável.*

Figura 41



Então

$$g_F \leq 1 + \Big[F : F_1\Big] \cdot (g_{F_1} - 1) + 4 \cdot \Big[F : F_1\Big] \cdot \Big[F : F_2\Big] \cdot g'_{F_1} \cdot g'_{F_2} \cdot d_1 \,,$$

em que

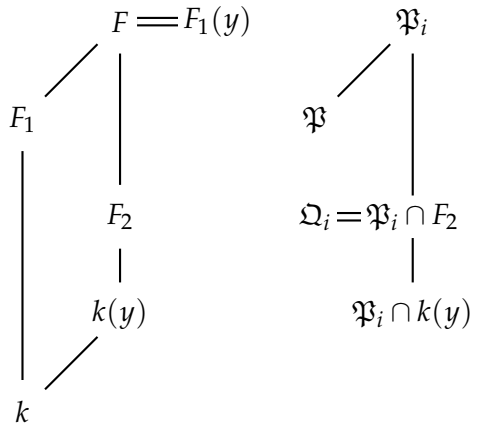
$$d_1 = \min \left\{ \deg_k(\mathfrak{P}) \;\middle|\; \mathfrak{P} \in \mathbb{P}(F_1) \right\} .$$

Demonstração. Seja $n_i := \Big[F : F_i\Big]$, para $i \in \{1, 2\}$. Podemos supor que n_1 é finito (caso contrário, a desigualdade seria trivialmente válida). Por definição de compósito, existe $S \subseteq F_2$ tal que $F = F_1 \cdot F_2 = F_1(F_2) = F_1(S)$. Como a extensão $F \mid F_1$ é finita, podemos supor que S é finito: existem $y_1, \ldots, y_s \in F_2$ com $F = F_1(y_1, \ldots, y_s)$. A extensão $F \mid F_1$ é separável, por hipótese; portanto, existem $a_1, \ldots, a_s \in F_1$ tais que $y := \sum_{j=1}^{s} a_j y_j \in F_2$ é um elemento primitivo de $F \mid F_1$. Como k é infinito (Observação 3.94), a demonstração do Teorema do Elemento Primitivo (DUMMIT e FOOTE, p. 595) permite supormos que $\{a_i\}_{i=1}^{s} \subseteq k$. Pelo Lema 5.22, existe um *place* $\mathfrak{P} \in \mathbb{P}(F_1)$ de grau limitado

$$\deg_k(\mathfrak{P}) \leq 2 \cdot g'_{F_1} \cdot d_1 \,, \tag{77}$$

com n_1 extensões distintas $\mathfrak{P}_1, \ldots, \mathfrak{P}_{n_1} \in \mathbb{P}(F)$ e tais que as restrições $\mathfrak{P}_i \cap k(y) \in \mathbb{P}\big(k(y)\big)$ são distintas duas a duas, para $i \in \{1, 2, \ldots, n_1\}$. Segue que os *places* $\mathfrak{Q}_i := \mathfrak{P}_i \cap F_2 \in \mathbb{P}(F_2)$ são distintos.

Figura 42. Caso de uso do Lema 5.22 (compare com a Figura 39).



Pela Observação 3.51, temos os seguintes fatos.

- O *place* $\mathfrak{P}$ é não ramificado em $F \mid F_1$:

$$e(\mathfrak{P}_i \mid \mathfrak{P}) = 1 , \qquad \forall\, i \in \{1, \ldots, n_1\} . \tag{78}$$

- Todas as extensões de $\mathfrak{P}$ em $F \mid F_1$ têm grau relativo igual a um:

$$f(\mathfrak{P}_i \mid \mathfrak{P}) = 1 , \qquad \forall\, i \in \{1, \ldots, n_1\} . \tag{79}$$

Afirmação 5.28. *Para* $i \in \{1, 2, \ldots, n_1\}$,

$$\deg_k(\mathfrak{O}_i) \leq 2 \cdot g'_{F_1} \cdot d_1 . \tag{80}$$

Dem.: A prova é uma simples aplicação da transitividade do grau das extensões de corpos residuais:

$$\deg_k(\mathfrak{O}_i) \leq \deg_k(\mathfrak{P}_i) = \deg_k(\mathfrak{P}) \cdot f(\mathfrak{P}_i \mid \mathfrak{P}) \overset{\text{Eq. 79}}{=} \deg_k(\mathfrak{P}) \overset{\text{Exp. 77}}{\leq} 2 \cdot g'_{F_1} \cdot d_1 .$$

◇

Pela Proposição 3.35, existe $u_i \in F_2$ com divisor polo

$$\left(2 \cdot g'_{F_2}\right) \mathfrak{O}_i = (u_i)_\infty^{F_2} = \left(-v_{\mathfrak{O}_i}(u_i)\right) \mathfrak{O}_i , \qquad \forall\, i \in \{1, 2, \ldots, n_1\} . \tag{81}$$

Esse critério de seleção das funções u_i corresponde à etapa (Castel.1) descrito previamente. O passo (Castel.2) é apresentado na afirmação seguinte.

Afirmação 5.29. *O conjunto* $\gamma := \{u_1, \ldots, u_{n_1}\}$ *é uma base de* F *sobre* F_1.

Dem.: Como $|\gamma| = \dim_{F_1}(F)$, basta verificar que γ é linearmente independente sobre F_1. Por absurdo, suponha que

$$\sum_{i=1}^{n_1} x_i \cdot u_i = 0 \qquad (\text{ com } x_i \in F_1 \ )$$

seja uma combinação linear não trivial. Seja $j \in \{1, \ldots, n_1\}$ tal que

$$v_{\mathfrak{P}}\left(x_j\right) \leq v_{\mathfrak{P}}\left(x_i\right) \tag{82}$$

para todo $i \in \{1, \ldots, n_1\}$. Vamos calcular $v_{\mathfrak{P}_j}\left(x_i \cdot u_i\right)$.

Para $j = i$,

$$\begin{aligned}
v_{\mathfrak{P}_j}\left(x_j \cdot u_j\right) &= v_{\mathfrak{P}_j}\left(x_j\right) + v_{\mathfrak{P}_j}\left(u_j\right) \qquad \text{(do item 2 da Definição 3.4)} \\
&= e\left(\mathfrak{P}_j \,\middle|\, \mathfrak{P}\right) \cdot v_{\mathfrak{P}}\left(x_j\right) + e\left(\mathfrak{P}_j \,\middle|\, \mathfrak{Q}_j\right) \cdot v_{\mathfrak{Q}_j}\left(u_j\right) \\
&\qquad \text{(da definição de índice de ramificação)} \\
&= e\left(\mathfrak{P}_j \,\middle|\, \mathfrak{P}\right) \cdot v_{\mathfrak{P}}\left(x_j\right) + \underbrace{e\left(\mathfrak{P}_j \,\middle|\, \mathfrak{Q}_j\right)}_{\geq 1} \cdot \underbrace{\left(-2 \cdot \underbrace{g'_{F_2}}_{\geq 1} \right)}_{<0} \\
&\qquad \text{(por (81))} \\
&< e\left(\mathfrak{P}_j \,\middle|\, \mathfrak{P}\right) \cdot v_{\mathfrak{P}}\left(x_j\right) \\
&= v_{\mathfrak{P}}\left(x_j\right) \qquad \text{(pela Equação 78)} \\
&\leq v_{\mathfrak{P}}\left(x_i\right) \qquad \text{(por (82))} \ .
\end{aligned}$$

Para $j \neq i$, o processo é similar:

$$\begin{aligned}
v_{\mathfrak{P}_j}\left(x_i \cdot u_i\right) &= v_{\mathfrak{P}_j}\left(x_i\right) + v_{\mathfrak{P}_j}\left(u_i\right) \qquad \text{(Definição 3.4)} \\
&= e\left(\mathfrak{P}_j \,\middle|\, \mathfrak{P}\right) \cdot v_{\mathfrak{P}}\left(x_i\right) + e\left(\mathfrak{P}_j \,\middle|\, \mathfrak{Q}_j\right) \cdot v_{\mathfrak{Q}_j}\left(u_i\right) \\
&\qquad \text{(definição de índice de ramificação)} \\
&= v_{\mathfrak{P}}\left(x_i\right) + e\left(\mathfrak{P}_j \,\middle|\, \mathfrak{Q}_j\right) \cdot v_{\mathfrak{Q}_j}\left(u_i\right) \qquad \text{(Equação 78)} \\
&\geq v_{\mathfrak{P}}\left(x_i\right) \qquad \text{(pela construção de } \gamma) \ ;
\end{aligned}$$

portanto, $v_{\mathfrak{P}_j}(x_i \cdot u_i) \neq v_{\mathfrak{P}_j}(x_j \cdot u_j)$ se $j \neq i$ e

$$\begin{aligned}\infty = v_{\mathfrak{P}_j}(0) &= v_{\mathfrak{P}_j}\left(\sum_{i=1}^{n_1} x_i \cdot u_i\right) \\ &= \min_{1\leq i\leq n_1}\left\{v_{\mathfrak{P}_j}(x_i \cdot u_i)\right\} \qquad \text{(pela Desigualdade Estrita)} \\ &< \infty\,,\end{aligned}$$

um absurdo. ◇

Seja

$$\mathtt{C} := \mathrm{Con}_{F|F_2}\left(2 \cdot g'_{F_2} \sum_{i=1}^{n_1} \mathfrak{Q}_i\right).$$

A escolha deste divisor corresponde ao passo (Castel.3); a ideia será estimar o gênero do compósito por meio do grau de $\mathtt{C}$.

Como a função $\deg_k : \mathrm{Div}(F) \to \mathbb{Z}$ é homomorfismo, temos que

$$\begin{aligned}\deg_k(\mathtt{C}) &= n_2 \cdot 2 \cdot g'_{F_2} \cdot \sum_{i=1}^{n_1} \deg_k(\mathfrak{Q}_i) \\ &\leq n_2 \cdot 2 \cdot g'_{F_2} \cdot n_1 \cdot 2 \cdot g'_{F_1} \cdot d_1 \qquad \text{(da Afirmação 5.28)} \\ &= 4 \cdot n_1 \cdot n_2 \cdot g'_{F_1} \cdot g'_{F_2} \cdot d_1\,.\end{aligned}$$

Afirmação 5.30. $\mathtt{C}$ *é efetivo.*

Dem.:

$$\begin{aligned}\mathtt{C} &= \mathrm{Con}_{F|F_2}\left(2 \cdot g'_{F_2} \sum_{i=1}^{n_1} \mathfrak{Q}_i\right) \\ &= 2 \cdot g'_{F_2} \sum_{i=1}^{n_1} \mathrm{Con}_{F|F_2}(\mathfrak{Q}_i) \qquad \text{(da Equação 32)} \\ &= \underbrace{2 \cdot g'_{F_2}}_{>0} \sum_{i=1}^{n_1} \sum_{\substack{\mathfrak{Q}' \mid \mathfrak{Q}_i \\ \mathfrak{Q}' \in \mathbb{P}(F)}} \underbrace{e\left(\mathfrak{Q}' \mid \mathfrak{Q}_i\right)}_{\geq 1} \mathfrak{Q}_i \qquad \text{(da definição de conorma)} \\ &\geq 0\,.\end{aligned}$$

◇

Afirmação 5.31. $\{u_1, u_2, \ldots, u_{n_1}\} \subseteq \mathscr{L}(\mathtt{C})$.

Dem.: Seja $i \in \{1, 2, \ldots, n_1\}$. Pela Observação 3.20, basta provarmos que

$$v_{\mathfrak{T}}(u_i) \geq -v_{\mathfrak{T}}(\mathtt{C}) , \qquad \forall\, \mathfrak{T} \in \mathbb{P}(F) . \tag{83}$$

Seja então $\mathfrak{T} \in \mathbb{P}(F)$. Pela Afirmação 5.30, temos que $v_{\mathfrak{T}}(\mathtt{C}) \geq 0$; ou, equivalentemente,

$$-v_{\mathfrak{T}}(\mathtt{C}) \leq 0 . \tag{84}$$

Se $\mathfrak{T} \neq \mathfrak{Q}_i$, então

$$v_{\mathfrak{T}}(u_i) \geq 0 , \tag{85}$$

pois u_i foi escolhido de modo a ter $\mathfrak{Q}_i$ como o único polo. Neste caso, (84) e (85) combinadas verificam (83).

Se $\mathfrak{T} = \mathfrak{Q}_i$, então

$$\begin{aligned} v_{\mathfrak{T}}(u_i) = v_{\mathfrak{Q}_i}(u_i) = -2 \cdot g'_{F_2} &\geq -2 \cdot g'_{F_2} \cdot \sum_{\substack{\mathfrak{Q}' \mid \mathfrak{Q}_i \\ \mathfrak{Q}' \in \mathbb{P}(F)}} e\left(\mathfrak{Q}' \mid \mathfrak{Q}_i\right) \\ &= -v_{\mathfrak{T}}(\mathtt{C}) . \end{aligned}$$

◇

Como os elementos $u_1, \ldots, u_{n_1}$ pertencem a $\mathscr{L}(\mathtt{C})$, temos pela Proposição 3.103 que

$$\begin{aligned} g_F &\leq 1 + n_1 \cdot (g_{F_1} - 1) + \deg_k(\mathtt{C}) \\ &\leq 1 + n_1 \cdot (g_{F_1} - 1) + 4 \cdot n_1 \cdot n_2 \cdot g'_{F_1} \cdot g'_{F_2} \cdot d_1 . \end{aligned} \tag{86}$$

É justamente em (86) que fica clara a importância do fato de g'_{F_1} e g'_{F_2} serem não nulos.

□

Proposição 5.32 (análogo da desigualdade de Castelnuovo-Severi)**.** *Sejam: F, F_1, F_2 corpos de funções com corpo de constantes k tais que $F = F_1 \cdot F_2$ e $F \mid F_1$ é separável; e*

$$d := \min\left\{ \deg_k(\mathfrak{P}) \;\middle|\; P \in \mathbb{P}(F_1) \right\} .$$

Então

$$g_F \leq 1 + \left[F : F_1\right] \cdot (g_{F_1} - 1) + 4 \cdot \left[F : F_1\right] \cdot \left[F : F_2\right] \cdot g'_{F_1} \cdot g'_{F_2} \cdot d . \tag{87}$$

Demonstração. Note que k pode não ser um corpo separavelmente fechado (fato que impede um uso direto do Lema 5.27). Para contornarmos esta dificuldade, vamos considerar o fecho separável.

Sejam: k_s um fecho separável de k;

$$\widetilde{F} := F{\cdot}k_s \ ; \tag{88}$$

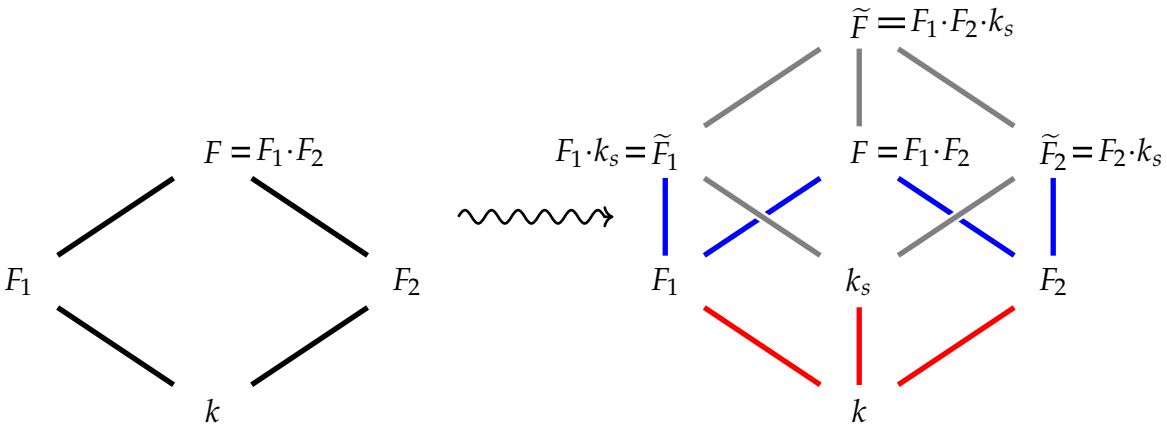
e

$$\widetilde{F}_i := F_i{\cdot}k_s \ , \qquad \text{com } i \in \{1,2\} \ . \tag{89}$$

Pela Observação 3.95, o corpo k_s é separavelmente fechado. A extensão $k_s \mid k$ é separavelmente gerada para qualquer base de transcendência, já que k_s é separável sobre k.

O processo de passagem aos compósitos reproduzido a seguir corresponde à etapa (Castel.4) descrita anteriormente (veja a Figura 43).

Figura 43. A seta indica o processo de passagem aos compósitos.



(o diagrama original, dado na hipótese)

(a passagem aos compósitos)

Uma vez que $k_s \mid k$ é separável (e portanto separavelmente gerado), temos pelo Teorema 3.78 que:

$$g_{\widetilde{F}} = g_F \ , \tag{90}$$

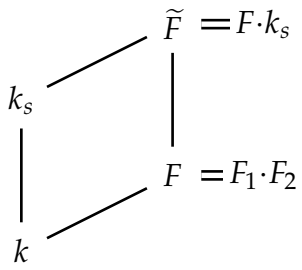
pois $\widetilde{F} \ / \ k_s$ é uma extensão constante de $F \ / \ k$; e

$$g_{\widetilde{F}_i} = g_{F_i} \ , \qquad i \in \{1,2\} \tag{91}$$

($\widetilde{F}_i \ / \ k_s$ é uma extensão constante de $F_i \ / \ k$, para $i \in \{1,2\}$). Pelo Teorema 3.101,

$$\lambda_{\widetilde{F}\,|\,F} = 1 \ .$$

Figura 44. Ilustração do caso de uso do Teorema 3.101 (compare com a Figura 20).

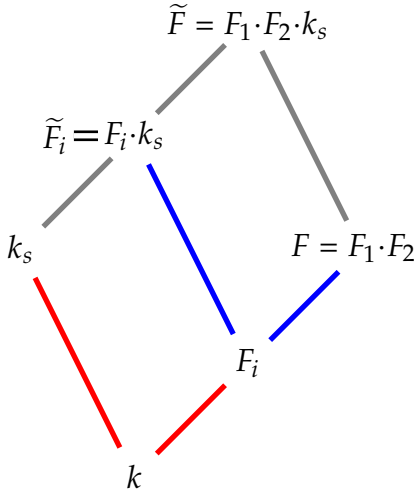


Os corpos k_s e F são linearmente disjuntos sobre k (item 2 do Teorema 3.102).

Pela implicação "1 $\Rightarrow$ 2b" da Proposição 3.99, temos que $\widetilde{F}_i$ e F são linearmente disjuntos sobre F_i, para $i \in \{1, 2\}$ (veja a Figura 45). Assim,

$$n_i = \left[\widetilde{F} : \widetilde{F}_i\right] = \left[F : F_i\right], \qquad i \in \{1, 2\}. \tag{92}$$

Figura 45. Ilustração do caso de uso da Proposição 3.99. Note que, do diagrama da Figura 43, podemos extrair um subdiagrama associado a F_i (para $i \in \{1, 2\}$).



Seja

$$d_1 := \min\left\{ \deg_{k_s}(\mathfrak{R}) \;\middle|\; \mathfrak{R} \in \mathbb{P}\left(\widetilde{F}_1\right) \right\} \tag{93}$$

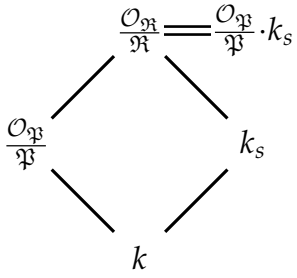
(note que o grau de cada *place* é calculado sobre k_s).

Então

$$\begin{aligned} g_F &= g_{\widetilde{F}} \qquad \text{(pela Equação 90)} \\ &\leq 1 + \left[\widetilde{F} : \widetilde{F}_1\right] \cdot \left(g_{\widetilde{F}_1} - 1\right) + 4 \cdot \left[\widetilde{F} : \widetilde{F}_1\right] \cdot \left[\widetilde{F} : \widetilde{F}_2\right] \cdot g'_{\widetilde{F}_1} \cdot g'_{\widetilde{F}_2} \cdot d_1 \\ &\qquad \text{(pelo Lema 5.27)} \\ &= 1 + \left[F : F_1\right] \cdot (g_{F_1} - 1) + 4 \cdot \left[F : F_1\right] \cdot \left[F : F_2\right] \cdot g'_{F_1} \cdot g'_{F_2} \cdot d_1 \\ &\qquad \text{(pelas equações 91 e 92)} \ . \end{aligned}$$

Resta provarmos que d_1 é majorado por d.
Escolha $\mathfrak{P} \in \mathbb{P}(F_1)$ tal que $\deg_k(\mathfrak{P}) = d$. Seja $\mathfrak{R} \in \mathbb{P}\left(\widetilde{F}_1\right)$ um *place* sobre $\mathfrak{P}$.
Pelo Teorema 3.54, temos que $\frac{\mathcal{O}_{\mathfrak{R}}}{\mathfrak{R}} = \frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} \cdot k_s$.

Figura 46



Assim,

$$d_1 \leq \left[\frac{\mathcal{O}_{\mathfrak{R}}}{\mathfrak{R}} : k_s\right] = \left[\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} \cdot k_s : k_s\right] \leq \left[\frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} : k\right] = d \ ,$$

e o resultado segue. □

5.2.2 O análogo do resultado de Madden-Valentini

Com o análogo da desigualdade de Castelnuovo-Severi à nossa disposição, concretizar as ideias desenvolvidas na Seção 4.1 passa a ser simples.

Proposição 5.33 (análogo do resultado de Madden-Valentini sobre os *C-improvements*)**.** *Sejam $L \mid K$ uma extensão finita separável de corpos de funções com corpo de constantes k e*

$$d := \min\left\{\deg_k(\mathfrak{P}) \;\middle|\; \mathfrak{P} \in \mathbb{P}(K)\right\} .$$

Suponha que, para todo corpo intermediário M, $K \subsetneq M \subseteq L$,

$$g_M > 1 + \left[M : K\right] \cdot (g_K - 1) + 4 \cdot \left[M : K\right]^2 \cdot \left(g'_K\right)^2 \cdot d \,. \tag{94}$$

Então para todo $\sigma \in \mathrm{Aut}\,(L \mid k)$, temos que $\sigma\,[K] = K$.

Demonstração. Por absurdo, suponha que existe $\sigma \in \mathrm{Aut}\,(L \mid k)$ tal que $\sigma\,[K] \neq K$. Então o corpo $\sigma\,[K] \cdot K$ é uma extensão própria de K. Em (87) do enunciado da Proposição 5.32, vamos tomar $F_1 = K$, $F_2 = \sigma\,[K]$, $M = F_1 \cdot F_2$:

$$\begin{aligned} g_M &\leq 1 + \left[M : K\right] \cdot (g_K - 1) + 4 \cdot \left[M : K\right] \cdot \left[M : \sigma\,[K]\right] \cdot g'_K \cdot g'_{\sigma[K]} \cdot d \\ &= 1 + \left[M : K\right] \cdot (g_K - 1) + 4 \cdot \left[M : K\right]^2 \cdot \left(g'_K\right)^2 \cdot d \,, \end{aligned}$$

uma contradição com a hipótese (na última igualdade, usamos a Observação 3.28). □

5.3 EXTENSÕES SEPARÁVEIS COM UM DIVISOR PRINCIPAL RAMIFICADO DE GRAU UM

Esta seção corresponde à quarta e última seção do artigo de Álvarez-Garcia e Villa-Salvador (2010).

Sejam: M um corpo; $m \geq 2$ inteiro; e $a \in M \setminus \{0\}$. É conhecido que o polinômio $X^m - a$ é irredutível em $M\,[X]$ quando as seguintes condições são simultaneamente verificadas:

- $a \notin M^q$, para todo $q \in \mathbb{Z}$ primo com $q \mid m$; e
- $a \notin -4M^4$ se $4 \mid m$.

Recomendamos o livro de Lang (2002, p. 297) para uma demonstração deste fato.

Vamos considerar uma forma prática de construir infinitos polinômios irredutíveis utilizando esse resultado. Se considerarmos apenas inteiros maiores que 4, não precisamos verificar a validade da segunda condição acima. E, se considerarmos somente *números primos* $m \in \mathbb{Z}$ (juntamente com a condição de que $m > 4$), bastaria verificar que $a \notin M^q$ apenas para o inteiro $q = m$.

A seguir, vamos ver um exemplo em que M é um corpo de funções racionais.

Exemplo 5.34. *Tomando-se $m > 4$ primo, $a = x$ e $M = k(x)$, teremos que o polinômio $f(T) := T^m - x$ é irredutível sobre M. Se um inteiro primo q divide m, então $q = m$, pois m é primo; e, claramente, a variável x não é m-ésima potência em $k(x)$ (se fosse $x^m = w$ para algum $w \in k(x)$, teríamos que x seria algébrico sobre k).*

Evidentemente, existem infinitos números primos que satisfazem a construção acima.

As ideias descritas na discussão acima permitirão a construção do corpo base dos *C-improvements* auxiliares para a prova do Teorema Principal.

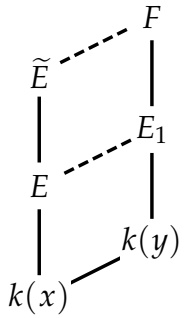
Proposição 5.35 (construção de *C-improvements* auxiliares)**.** *Sejam: k um corpo infinito; $E \mid k(x)$ uma extensão finita separável de corpos de funções sobre k; $\widetilde{E} \,/\, l$ um fecho normal de $E \mid k(x)$; e C, C_1, $C_2 \in \mathbb{R}_+$ arbitrários. Suponha que:*

- *$\mathfrak{P}_{x-1}$ seja ramificado em $E \mid k(x)$; e*
- *o zero $\mathfrak{Q}_{(0,x)}$ e o polo $\mathfrak{Q}_{(\infty,x)}$ de x em $k(x)$ sejam não ramificados e separáveis em $E \mid k(x)$.*

Então existem um corpo de funções racionais $k(y) \supseteq k(x)$ e uma extensão finita $F \,/\, l$ de $k(y) \,/\, k$ que satisfazem as seguintes propriedades.

1. *a) Existe um subcorpo $E_1 \,/\, k$ de $F \,/\, l$ tal que*
   - *i. $\left[E : k(x)\right] = \left[E_1 : k(y)\right]$,*
   - *ii. $\left[\widetilde{E} : k(x)\right] = \left[F : k(y)\right]$,*
   - *iii. $\mathrm{Aut}\left(E \,\middle|\, k(x)\right) \cong \mathrm{Aut}\left(E_1 \,\middle|\, k(y)\right)$ e*
   - *iv. F é um fecho normal de $E_1 \mid k(y)$.*

Figura 47

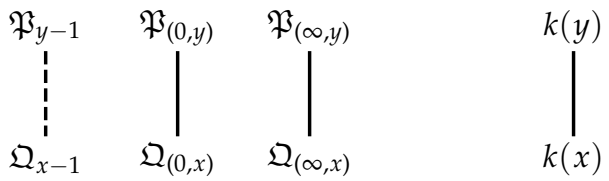


   b) i. $\mathfrak{P}_{y-1}$ é ramificado em $F \mid k(y)$, e $\mathfrak{P}_{y-1} \mid \mathfrak{P}_{x-1}$.

ii. o polo $\mathfrak{Q}_{(\infty,y)}$ de y em $k(y)$ é não ramificado e separável em $F \mid k(y)$.

iii. o zero $\mathfrak{Q}_{(0,y)}$ de y em $k(y)$ é não ramificado e separável em $F \mid k(y)$.

Figura 48



2. *Seja E_2 um corpo intermediário, $k(y) \subsetneq E_2 \subseteq E_1$. Então:*

   a) ou existe um place $\mathfrak{U} \in \mathbb{P}\big(k(y)\big)$ *ramificado ou inseparável em $E_2 \mid k(y)$ de grau*

   $$\deg_k(\mathfrak{U}) > C_2 \; ;$$

   b) ou existe um conjunto $S \subseteq \mathbb{P}\big(k(y)\big)$ de places *ramificados ou inseparáveis em $E_2 \mid k(y)$ com*

   $$|S| > C_1 \; .$$

3. *Para todo corpo intermediário k_1,*

   $$k \subseteq k_1 \subseteq l \; ,$$

   e para todo corpo M com corpo de constantes k_1 tal que

   $$k_1(y) \subsetneq M \subseteq F \; ,$$

   teremos que

   $$g_M > C \; .$$

4. *Seja $N \mid k$ uma extensão separável finita. Seja $M' \;/\; N$ um corpo intermediário,*

   $$N(y) \subsetneq M' \subseteq F{\cdot}N \; . \tag{95}$$

   Então

   $$g_{M'} > C \; .$$

Demonstração. Seja $p := \mathrm{char}(k)$.

(Itens 1 e 2): Seja $m \in \mathbb{Z}$ primo tal que

$$m > \max\{p, 4, C_1 \cdot C_2, 2 \cdot C + 3\} \tag{96}$$

e

$$\mathrm{mdc}\left\{m, \left[\widetilde{E} : k(x)\right]\right\} = 1 \ . \tag{97}$$

Seja y uma variável tal que

$$y^m = x \ . \tag{98}$$

Note que a existência de y é garantida pela teoria básica de corpos: podemos obter $y \in R$ no corpo de raízes $R \supseteq k(x)$ do polinômio

$$f(T) := T^m - x \in k(x)[T] \tag{99}$$

— veja o livro de Dummit e Foote (2004, p. 536), *Theorem* 25.

Afirmação 5.36. *$k(y) \mid k(x)$ é uma extensão separável de grau $\left[k(y) : k(x)\right] = m$.*

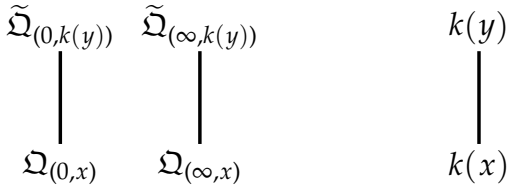
Dem.: Para provarmos que a extensão $k(y) \mid k(x)$ é separável, basta considerarmos o caso em que $p \neq 0$, já que a separabilidade é imediata em característica zero.

O polinômio $f(T)$ é irredutível (Exemplo 5.34). Como $p \nmid m$, temos que o polinômio f não tem raízes em comum com a derivada $D_T\left(f(T)\right) = mT^{m-1}$; logo, $f = m_{y,k(x)}$ e y é separável sobre $k(x)$.

Para verificar que o grau da extensão $k(y) \mid k(x)$ é igual a m, veja o livro de Dummit e Foote (2004, p. 521) — *Proposition* 11, para $\alpha = y$ e $F = k(x)$. ◇

Sejam $\widetilde{\Omega}_{(0,k(y))} \in \mathbb{P}\big(k(y)\big)$ um *place* sobre $\Omega_{(0,x)}$ e $\widetilde{\Omega}_{(\infty,k(y))} \in \mathbb{P}\big(k(y)\big)$ um *place* sobre $\Omega_{(\infty,x)}$.

Figura 49. Veremos que o *place* $\widetilde{\Omega}_{(0,k(y))}$ (resp. $\widetilde{\Omega}_{(\infty,k(y))}$) coincide com o ideal $\mathfrak{P}_{(0,y)}$ (resp. $\mathfrak{P}_{(\infty,y)}$) da Figura 48, mas ainda não sabemos disso.



Afirmação 5.37. *Os* places $\mathfrak{Q}_{(0,x)}$ *e* $\mathfrak{Q}_{(\infty,x)}$ *são totalmente ramificados em* $k(y) \mid k(x)$*:*

$$e\left(\widetilde{\mathfrak{Q}}_{(\infty,k(y))} \,\middle|\, \mathfrak{Q}_{(\infty,x)}\right) = m \qquad e \qquad e\left(\widetilde{\mathfrak{Q}}_{(0,k(y))} \,\middle|\, \mathfrak{Q}_{(0,x)}\right) = m \ .$$

Dem.: Pelo Exemplo 3.15,

$$\mathfrak{Q}_{(0,x)} - \mathfrak{Q}_{(\infty,x)} = (x)^F = v_{\mathfrak{Q}_{(0,x)}}(x)\mathfrak{Q}_{(0,x)} - v_{\mathfrak{Q}_{(\infty,x)}}(x)\mathfrak{Q}_{(\infty,x)} \ . \tag{100}$$

Então

$$v_{\mathfrak{Q}_{(0,x)}}(x) = 1 \qquad \text{e} \qquad v_{\mathfrak{Q}_{(\infty,x)}}(x) = 1 \ . \tag{101}$$

Da definição de índice de ramificação,

$$\begin{aligned} v_{\widetilde{\mathfrak{Q}}_{(0,k(y))}}(y) &= e\left(\widetilde{\mathfrak{Q}}_{(0,k(y))} \,\middle|\, \mathfrak{Q}_{(0,x)}\right) \cdot v_{\mathfrak{Q}_{(0,x)}}(y) \\ &\geq 1 \ . \end{aligned}$$

Assim,

$$\begin{aligned} m &\leq m \cdot v_{\widetilde{\mathfrak{Q}}_{(0,k(y))}}(y) \\ &= v_{\widetilde{\mathfrak{Q}}_{(0,k(y))}}(y^m) \qquad \text{(da definição de valoração)} \\ &= v_{\widetilde{\mathfrak{Q}}_{(0,k(y))}}(x) \qquad \text{(da Equação 98)} \\ &= e\left(\widetilde{\mathfrak{Q}}_{(0,k(y))} \,\middle|\, \mathfrak{Q}_{(0,x)}\right) \cdot v_{\mathfrak{Q}_{(0,x)}}(x) \\ &\qquad\qquad \text{(da definição de índice de ramificação)} \\ &= e\left(\widetilde{\mathfrak{Q}}_{(0,k(y))} \,\middle|\, \mathfrak{Q}_{(0,x)}\right) \qquad \text{(de (101))} \\ &\leq m \qquad \text{(do Corolário 3.49)} \ . \end{aligned}$$

Segue que $e\left(\widetilde{\mathfrak{Q}}_{(0,k(y))} \,\middle|\, \mathfrak{Q}_{(0,x)}\right) = m$. A demonstração da outra igualdade é totalmente análoga. ◇

Pela Observação 3.56, o ideal $\widetilde{\mathfrak{Q}}_{(0,k(y))}$ (resp. $\widetilde{\mathfrak{Q}}_{(\infty,k(y))}$) é o único *place* sobre $\mathfrak{Q}_{(0,x)}$. (resp. $\mathfrak{Q}_{(\infty,x)}$).

Afirmação 5.38. *Os únicos* places *de* $k(x)$ *que se ramificam em* $k(y) \mid k(x)$ *são* $\mathfrak{Q}_{(0,x)}$ *e* $\mathfrak{Q}_{(\infty,x)}$*, e não há* places *de* $k(x)$ *que sejam inseparáveis em* $k(y) \mid k(x)$*.*

Dem.: Seja

$$\mathtt{D} := \operatorname{Diff}\left(k(y) \,\middle|\, k(x)\right) .$$

Pelo Teorema 3.74, o conjunto dos *places* de $k(y)$ ramificados ou inseparáveis em $k(y) \mid k(x)$ coincide com o suporte de $\mathtt{D}$.

Pela Afirmação 5.36, podemos usar a Fórmula do Gênero de Riemann-Hurwitz:

$$\begin{aligned} 0 &= g_{k(y)} && \text{(Exemplo 3.24)} \\ &= 1 + \frac{\left[k(y) : k(x)\right]}{\left[k : k\right]} \cdot \left(g_{k(x)} - 1\right) + \frac{1}{2} \cdot \deg_k(\mathtt{D}) && \text{(Teorema 3.76)} \\ &= 1 + \frac{m}{1} \cdot (0 - 1) + \frac{1}{2} \cdot \deg_k(\mathtt{D}) && \text{(Afirmação 5.36 e Exemplo 3.24)} \ . \end{aligned}$$

Então

$$\deg_k(\mathtt{D}) = 2 \cdot m - 2 \ . \tag{102}$$

Os *places* $\mathfrak{Q}_{(0,x)}$ e $\mathfrak{Q}_{(\infty,x)}$ são ramificados em $k(y) \mid k(x)$ (Afirmação 5.37) — e, portanto, os *places* $\widetilde{\mathfrak{Q}}_{(0,k(y))}$ e $\widetilde{\mathfrak{Q}}_{(\infty,k(y))}$ estão no suporte do diferente de $k(y) \mid k(x)$.

Pela Equação 102 (e pelo Teorema 3.74), não há outros *places* em $\operatorname{Supp}(\mathtt{D})$. Basta então verificar que os *places* $\widetilde{\mathfrak{Q}}_{(0,k(y))}$ e $\widetilde{\mathfrak{Q}}_{(\infty,k(y))}$ são separáveis.

Como o zero e o polo de x em $k(x)$ são totalmente ramificados em $k(y) \mid k(x)$, temos pela Igualdade Fundamental (Teorema 3.48) que

$$f\left(\widetilde{\mathfrak{Q}}_{(0,k(y))} \,\middle|\, \mathfrak{Q}_{(0,x)}\right) = 1 \qquad \text{e} \qquad f\left(\widetilde{\mathfrak{Q}}_{(\infty,k(y))} \,\middle|\, \mathfrak{Q}_{(\infty,x)}\right) = 1 \ .$$

Logo, os *places* $\widetilde{\mathfrak{Q}}_{(0,k(y))}$ e $\widetilde{\mathfrak{Q}}_{(\infty,k(y))}$ não podem ser inseparáveis. ◇

Seja $F := \widetilde{E}(y)$. Vamos provar que a escolha $E_1 = E(y)$ funciona.
Note que F é o fecho normal de $E(y) \mid k(y)$, e isso prova o item 1(a)iv.
Seja E_2 um corpo intermediário,

$$k(y) \subsetneq E_2 \subseteq E_1 \ . \tag{103}$$

Considere o isomorfismo

$$\begin{aligned} \varphi : \mathrm{Gal}\left(\widetilde{E}(y) \,\middle|\, k(y)\right) &\to \mathrm{Gal}\left(\widetilde{E} \,\middle|\, k(x)\right) \\ \sigma &\mapsto \sigma \restriction_{\widetilde{E}} . \end{aligned}$$

Afirmação 5.39. $\left[E(y) : k(y)\right] = \left[E : k(x)\right]$.

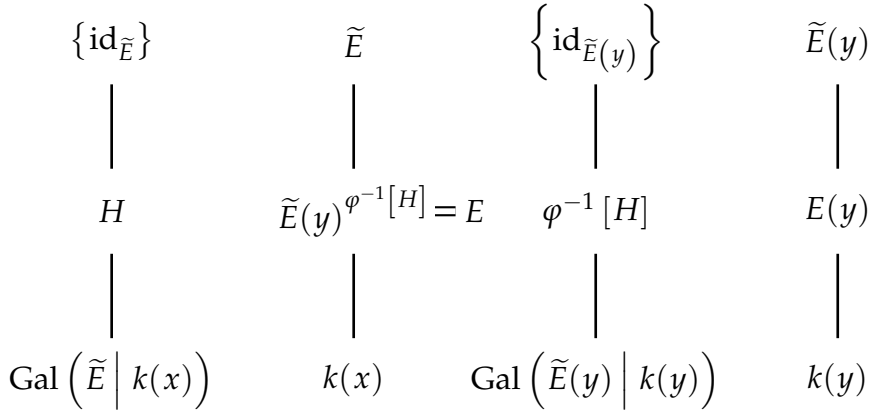
Dem.: Seja $H \leq \mathrm{Gal}\left(\widetilde{E} \,\middle|\, k(x)\right)$ tal que

$$E = \widetilde{E}^H .$$

Como y é fixado por $\varphi^{-1}[H]$, temos que

$$E(y) = \widetilde{E}(y)^{\varphi^{-1}[H]} .$$

Figura 50. Diagramas (possivelmente incompletos) das extensões $\widetilde{E} \,\middle|\, k(x)$ e $\widetilde{E}(y) \,\middle|\, k(y)$.



Assim, pelo TFTG — veja *Theorem* 14, item 2, no livro de Dummit e Foote (2004, p. 574) —,

$$\left[E(y) : k(y)\right] = \frac{\left|\mathrm{Gal}\left(\widetilde{E}(y) \,\middle|\, k(y)\right)\right|}{\left|\varphi^{-1}[H]\right|} = \frac{\left|\mathrm{Gal}\left(\widetilde{E} \,\middle|\, k(x)\right)\right|}{|H|} = \left[E : k(x)\right] .$$

◇

Afirmação 5.40. $\mathrm{Aut}\left(E(y) \,\middle|\, k(y)\right) \;\cong\; \mathrm{Aut}\left(E \,\middle|\, k(x)\right)$.

Dem.:

$$\begin{aligned}
\mathrm{Aut}\left(E \,\middle|\, k(x)\right) &\cong \left\{\tau \in \mathrm{Gal}\left(\widetilde{E} \,\middle|\, k(x)\right) \,\middle|\, \tau\left[E\right] = E\right\} \\
&= \varphi\left[\left\{\sigma \in \mathrm{Gal}\left(\widetilde{E}(y) \,\middle|\, k(y)\right) \,\middle|\, \sigma\left[E(y)\right] = E(y)\right\}\right] \\
&\cong \varphi\left[\mathrm{Aut}\left(E(y) \,\middle|\, k(y)\right)\right] \\
&\cong \mathrm{Aut}\left(E(y) \,\middle|\, k(y)\right) \qquad \text{(pois } \varphi \text{ é isomorfismo)} \;.
\end{aligned}$$

◇

Pelo Lema 5.1, temos que o corpo de constantes de E_1 é k.

Afirmação 5.41. *Existe um corpo M tal que*

$$M(y) = E_2 \qquad e \qquad k(x) \subsetneq M \subseteq \widetilde{E}\,.$$

Dem.: Seja

$$M := E_2 \cap \widetilde{E}\,.$$

Adjuntando a variável y,

$$\begin{aligned}
M(y) &= E_2(y) \cap \widetilde{E}(y) \\
&= E_2 \cap \widetilde{E}(y) \qquad \text{(pois } y \in E_2\text{)} \\
&= E_2 \qquad \text{(pois } E_2 \subseteq E(y) \subseteq \widetilde{E}(y)\text{)} \;.
\end{aligned}$$

Além disso,

$$\begin{aligned}
k(x) &\subseteq k(y) \cap \widetilde{E} \subseteq E_2 \cap \widetilde{E} \subseteq E(y) \cap \widetilde{E} \qquad \text{(por (103))} \\
&\subseteq \widetilde{E}\,.
\end{aligned}$$

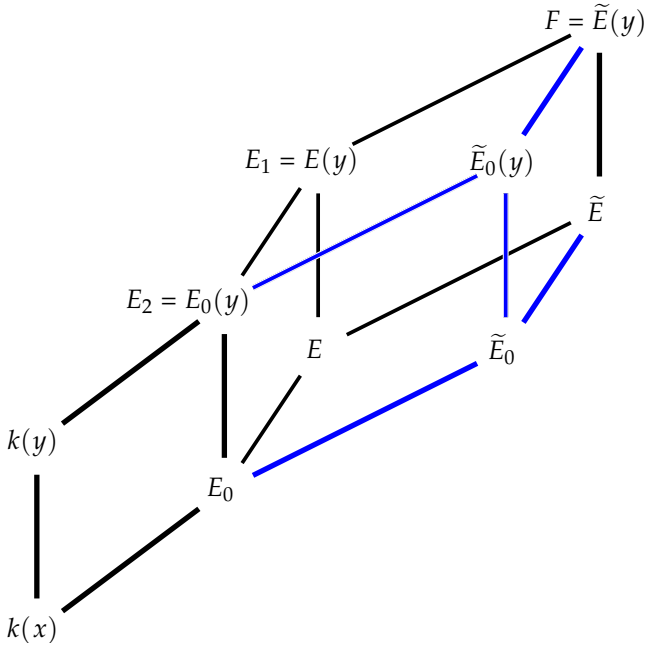
Por absurdo, suponha que $k(x) = M$. Por adjunção da variável y, teríamos que

$$k(y) = M(y) = E_2\,,$$

uma contradição com (103). ◇

Considere um corpo intermediário $E_0 \neq k(x)$ de $\widetilde{E} \,\Big|\, k(x)$ dado pela Afirmação 5.41 — isto é, E_0 é um corpo tal que $E_2 = E_0(y)$. Seja $\widetilde{E}_0 \subseteq \widetilde{E}$ o fecho normal de $E_0 \mid k(x)$.

Figura 51. O diagrama ilustra como E_0 está relacionado com os demais corpos considerados até o momento.



Pelo Teorema 4.4, existe um *place* $\mathfrak{P}_f \in \mathbb{P}\big(k(x)\big)$ ramificado ou inseparável em $E_0 \mid k(x)$, em que $f \in k[x]$ é algum polinômio mônico e irredutível. Da Proposição 4.5, o *place* $\mathfrak{P}_f$ é ramificado ou inseparável em $\widetilde{E}_0 \,\Big|\, k(x)$.

Da hipótese de o zero e o polo de x em $k(x)$ serem não ramificados e separáveis em $E \mid k(x)$, temos que $\mathfrak{Q}_{(0,x)} \neq \mathfrak{P}_f \neq \mathfrak{Q}_{(\infty,x)}$. Segue da Afirmação 5.38 que $\mathfrak{P}_f$ é não ramificado e separável em $k(y) \mid k(x)$. Suponha que o polinômio $f(x) = f(y^m)$ se decompõe (na variável y) em fatores irredutíveis distintos

$$f_1(y)\,,\ \ \ldots\,,\ f_h(y) \in k[y]$$

— veja a Figura 52.

Fixe $i \in \{1, 2, \ldots, h\}$.

Seja $\mathfrak{H}_i \in \mathbb{P}\Big(\widetilde{E}_0(y)\Big)$ uma extensão de $\mathfrak{P}_{f_i}$.

Uma vez que $\mathfrak{J}_i := \mathfrak{H}_i \cap \widetilde{E}_0$ está sobre $\mathfrak{P}_f$, então $\mathfrak{J}_i \mid \mathfrak{P}_f$ é ramificado ou inseparável em $\widetilde{E}_0 \,\Big|\, k(x)$:

$$e\left(\mathfrak{J}_i \,\middle|\, \mathfrak{P}_f\right) > 1 \qquad \text{ou} \qquad f\left(\mathfrak{J}_i \,\middle|\, \mathfrak{P}_f\right)_{\mathbf{i}} > 1\,.$$

Logo,

$$e\left(\mathfrak{J}_i \,\middle|\, \mathfrak{P}_f\right) \cdot f\left(\mathfrak{J}_i \,\middle|\, \mathfrak{P}_f\right)_{\mathbf{i}} > 1 \,.$$

Pelas transitividades do índice de ramificação e do grau de inseparabilidade (com relação à 'torre' de *places* $\mathfrak{H}_i \supseteq \mathfrak{J}_i \supseteq \mathfrak{P}_f$), temos que $\mathfrak{H}_i \mid \mathfrak{P}_f$ é ramificada ou inseparável, pois

$$\begin{aligned} e\left(\mathfrak{H}_i \,\middle|\, \mathfrak{P}_f\right) \cdot f\left(\mathfrak{H}_i \,\middle|\, \mathfrak{P}_f\right)_{\mathbf{i}} &= e\left(\mathfrak{H}_i \mid \mathfrak{J}_i\right) \cdot e\left(\mathfrak{J}_i \,\middle|\, \mathfrak{P}_f\right) \cdot f\left(\mathfrak{H}_i \mid \mathfrak{J}_i\right)_{\mathbf{i}} \cdot f\left(\mathfrak{J}_i \,\middle|\, \mathfrak{P}_f\right)_{\mathbf{i}} \\ &> 1 \,. \end{aligned}$$

Uma vez que

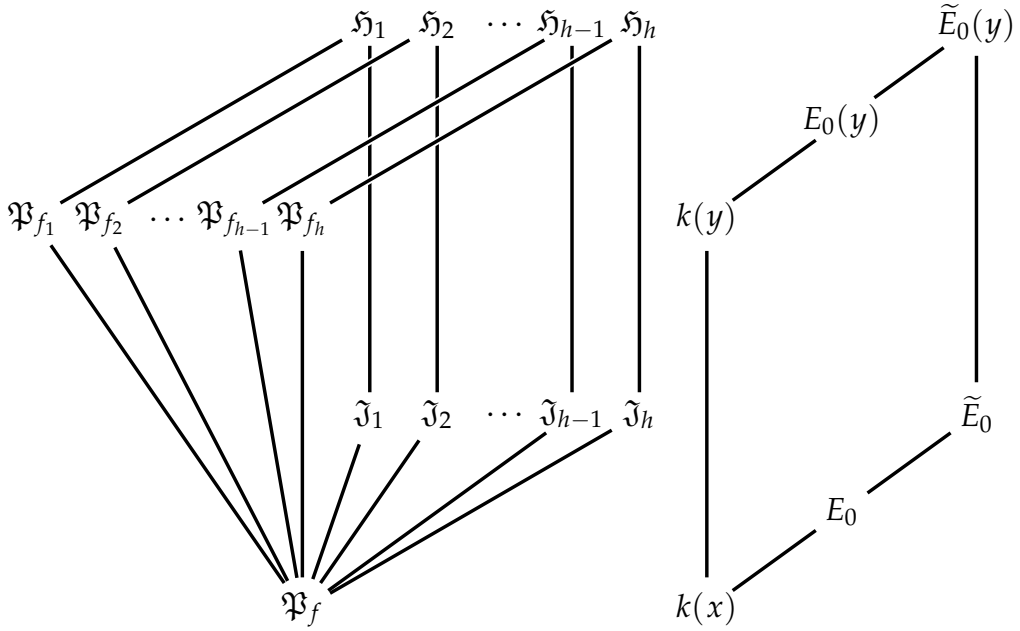
$$\mathfrak{Q}_{(0,x)} \neq \mathfrak{P}_{f_i} \cap k(x) \neq \mathfrak{Q}_{(\infty,x)}$$

(já que $\mathfrak{P}_{f_i} \cap k(x) = \mathfrak{P}_f$), temos pela Afirmação 5.38 que a extensão de *places* $\mathfrak{P}_{f_i} \mid \mathfrak{P}_f$ é não ramificada e separável em $k(y) \mid k(x)$; portanto, na torre de corpos $\widetilde{E}_0(y) \supseteq k(y) \supseteq k(x)$, a mudança do índice de ramificação ou do grau de inseparabilidade ocorre entre $\widetilde{E}_0(y)$ e $k(y)$:

$$e\left(\mathfrak{H}_i \,\middle|\, \mathfrak{P}_{f_i}\right) \cdot f\left(\mathfrak{H}_i \,\middle|\, \mathfrak{P}_{f_i}\right)_{\mathbf{i}} > 1 \,.$$

Pelo Lema 5.5, temos que $\mathfrak{P}_{f_i}$ é ramificado ou inseparável em $E_0(y) \mid k(y)$.

Figura 52. Extensões de $\mathfrak{P}_f$.



Para provar o item 2, vamos considerar duas possibilidades.

- (Caso 1, $\deg\left(f_j\right) > C_2$ para algum $j \in \{1,2,\ldots,h\}$): neste caso, tome $\mathfrak{U} := \mathfrak{P}_{f_j}$.
- (Caso 2, $\deg(f_i) \leq C_2$ para todo $i \in \{1,2,\ldots,h\}$): neste caso, o número h de fatores é mínimo quando $\deg(f_i) = C_2$, para todo $i \in \{1,2,\ldots,h\}$. Assim, se denotarmos por $\mathrm{gr}_u(r)$ o grau de um polinômio r na variável u, teremos que

$$\begin{aligned} h \cdot C_2 &= \mathrm{gr}_y(f) \\ &= m \cdot \mathrm{gr}_x(f) \qquad \text{(pela Equação 98)} \\ &\geq m \\ &> C_1 \cdot C_2 \qquad \text{(por (96))} \,. \end{aligned}$$

Segue que $h > C_1$. Tome $S := \left\{\mathfrak{P}_{f_1},\ldots,\mathfrak{P}_{f_h}\right\}$.

Afirmação 5.42. $\mathfrak{P}_{y-1} | \mathfrak{Q}_{x-1}$.

Dem.: Por definição,

$$\mathfrak{Q}_{x-1} = \left\{ \frac{t}{u} \;\middle|\; t \in k[X] \,,\quad u \in k[X] \setminus \{0\} \,,\quad (x-1) \mid t \quad \text{e} \quad (x-1) \nmid u \right\} .$$

Seja $\gamma = \frac{t}{u} \in \mathfrak{Q}_{x-1}$ com $\mathrm{mdc}\{t,u\} = 1$. Pela Equação 98, temos que

$$(y^m - 1) \mid t \qquad \text{e} \qquad (y^m - 1) \nmid u \,.$$

Pela identidade

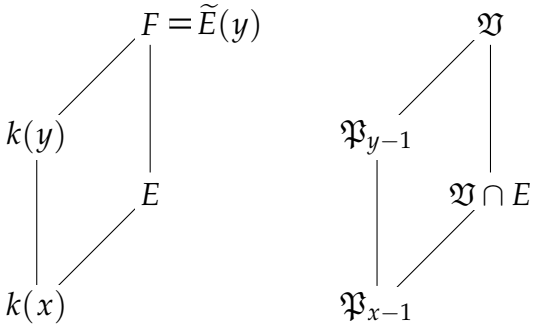
$$y^m - 1 = (y-1) \cdot \left(y^{m-1} + y^{m-2} + \ldots + y + 1\right) ,$$

segue que o polinômio $y-1$ divide $t(y)$ em $k[y]$. Se $y-1$ dividisse $u(y)$ em $k[y]$, teríamos que $\mathrm{mdc}\{t,u\} \neq 1$, um absurdo. Assim, $y-1 \nmid u(y)$ em $k[y]$ e, portanto, $\gamma \in \mathfrak{P}_{y-1}$.

Pela arbitrariedade de γ, segue que $\mathfrak{Q}_{x-1} \subseteq \mathfrak{P}_{y-1}$. ◇

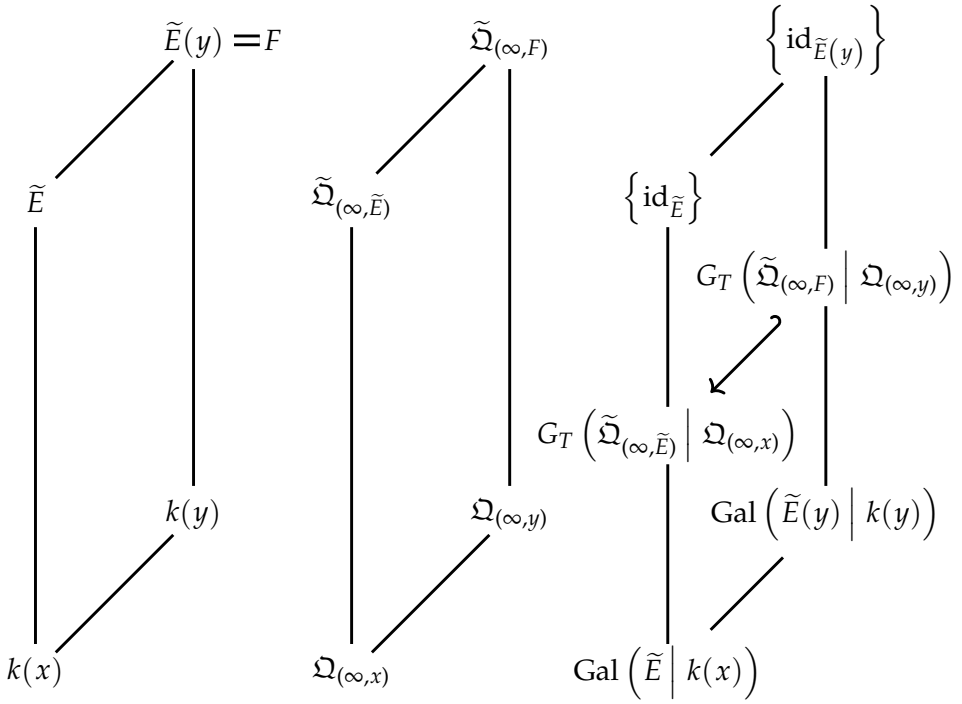
Como o *place* $\mathfrak{P}_{x-1}$ é ramificado em $E \mid k(x)$ por hipótese, então pela Proposição 4.5 existe $\mathfrak{V} \in \mathbb{P}(F)$ sobre $\mathfrak{P}_{x-1}$ tal que $e\left(\mathfrak{V} \mid \mathfrak{P}_{x-1}\right) > 1$. Pela Afirmação 5.42, o *place* $\mathfrak{V}$ é extensão de $\mathfrak{P}_{y-1}$ (veja a Figura 53). Da Afirmação 5.38, a extensão $\mathfrak{P}_{y-1} \mid \mathfrak{P}_{x-1}$ é não ramificada; e, da transitividade do índice de ramificação, segue que a extensão $\mathfrak{V} \mid \mathfrak{P}_{y-1}$ é ramificada. Isso prova o item 1(b)i.

Figura 53. Extensões de $\mathfrak{P}_{x-1}$.



Sejam $\widetilde{\mathfrak{Q}}_{(\infty,\widetilde{E})} \in \mathbb{P}\left(\widetilde{E}\right)$ um *place* sobre $\mathfrak{Q}_{(\infty,x)}$ e $\widetilde{\mathfrak{Q}}_{(\infty,F)} \in \mathbb{P}(F)$ um *place* sobre $\widetilde{\mathfrak{Q}}_{(\infty,\widetilde{E})}$ (veja a Figura 54). O *place* $\mathfrak{Q}_{(\infty,x)}$ é não ramificado e separável em $E \mid k(x)$, por hipótese; assim, pela forma contrapositiva do Lema 5.5, temos que $\widetilde{\mathfrak{Q}}_{(\infty,\widetilde{E})} \mid \mathfrak{Q}_{(\infty,x)}$ é não ramificado e separável em $\widetilde{E} \,\big|\, k(x)$. Pela Proposição 4.3, segue que o polo $\mathfrak{Q}_{(\infty,y)}$ de y é não ramificado e separável em $F \mid k(y)$. O item 1(b)ii está provado. Evidentemente, o item 1(b)iii é demonstrável com procedimento similar.

Figura 54. Ilustração do uso da Proposição 4.3 (compare com a Figura 21).



(Item 3): Sejam: k_1 um corpo intermediário de $l \mid k$; $\mathfrak{R}_1$ o zero de x em $k_1(x)$; e $\mathfrak{R}_2$ o polo de x em $k_1(x)$. Sejam $i \in \{1,2\}$ e $\mathfrak{D}_i \in \mathbb{P}\big(k_1(y)\big)$ um *place* sobre $\mathfrak{R}_i$ (veja a Figura 57).

Pelo Teorema 3.18, a extensão $k_1(x) \mid k(x)$ tem grau igual a

$$\begin{aligned}\Big[k_1(x) : k(x)\Big] &= \deg_{k_1}(\mathfrak{R}_1) = \deg_k(\mathfrak{R}_1) \\ &\qquad\qquad \text{(pois os polos de } x \text{ em } k(x) \text{ e} \\ &\qquad\qquad \text{em } k_1(x) \text{ têm o mesmo grau)} \\ &= f\left(\mathfrak{R}_1 \,\middle|\, \mathfrak{Q}_{(0,x)}\right) \cdot \deg_k\left(\mathfrak{Q}_{(0,x)}\right) \\ &= f\left(\mathfrak{R}_1 \,\middle|\, \mathfrak{Q}_{(0,x)}\right) .\end{aligned}$$

Analogamente,

$$\Big[k_1(x) : k(x)\Big] = f\left(\mathfrak{R}_2 \,\middle|\, \mathfrak{Q}_{(\infty,x)}\right) .$$

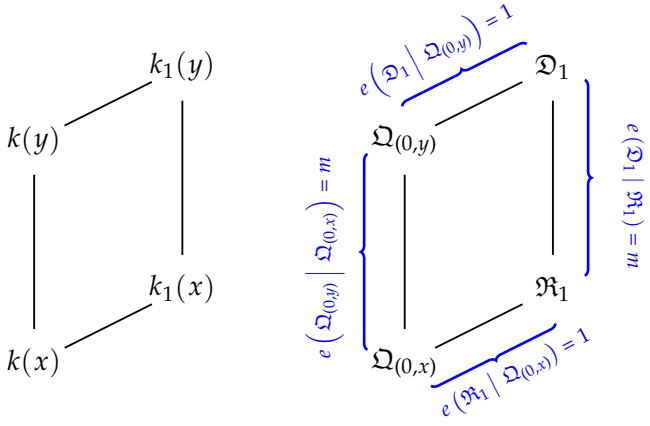
Assim, pela Igualdade Fundamental,

$$e\left(\mathfrak{R}_1 \,\middle|\, \mathfrak{Q}_{(0,x)}\right) = e\left(\mathfrak{R}_2 \,\middle|\, \mathfrak{Q}_{(\infty,x)}\right) = 1 .$$

Portanto, como o polo e o zero de y em $k(y)$ são não ramificados em $F \mid k(y)$ (itens 1(b)ii e 1(b)iii, respectivamente), e como $\mathfrak{Q}_{(0,x)}$ e $\mathfrak{Q}_{(\infty,x)}$ são totalmente ramificados em $k(y) \mid k(x)$, temos que a ramificação de $\mathfrak{Q}_{(0,x)}$ e de $\mathfrak{Q}_{(\infty,x)}$ ocorre entre $k_1(x)$ e $k_1(y)$:

$$e\left(\mathfrak{D}_i \mid \mathfrak{R}_i\right) = \Big[k_1(y) : k_1(x)\Big] = m . \tag{104}$$

Figura 55. O estudo do índice de ramificação nas extensões do zero de x em $k(x)$ nos corpos $k_1(x)$ e $k_1(y)$. O polo de x em $k(x)$ tem um comportamento análogo.



Ou seja, $\mathfrak{R}_i$ é totalmente ramificado em $k_1(y) \mid k_1(x)$.

Seja $M \;/\; k_1$ tal que

$$k_1(y) \subsetneq M \subseteq \widetilde{E}(y) \; . \tag{105}$$

Seja

$$M_0 := M \cap \widetilde{E} \; . \tag{106}$$

Pela Equação 97,

$$\Big[M : M_0\Big] = m \; . \tag{107}$$

Afirmação 5.43.

$$k_1(x) \subsetneq M_0 \subseteq \widetilde{E} \; .$$

Dem.: Pelas inclusões $k_1 \subseteq l \subseteq \widetilde{E}$ e $\{x\} \subseteq \widetilde{E}$, temos que

$$k_1(x) \subseteq l(x) \subseteq \widetilde{E} \; . \tag{108}$$

Então

$$\begin{aligned} k_1(x) &= k_1(x) \cap \widetilde{E} && \text{(por (108))} \\ &\subseteq k_1(y) \cap \widetilde{E} \subseteq M \cap \widetilde{E} \subseteq \widetilde{E}(y) \cap \widetilde{E} && \text{(por (105))} \\ &= \widetilde{E} \; . \end{aligned}$$

Se fosse $k_1(x) = M_0$, teríamos por adjunção com a variável y que

$$\begin{aligned} k_1(y) = \big(k_1(x)\big)(y) = \Big(M \cap \widetilde{E}\Big)(y) \\ &= M(y) \cap \widetilde{E}(y) \\ &= M \cap \widetilde{E}(y) && \text{(pois } y \in M\text{)} \\ &= M && \text{(pois } M \subseteq \widetilde{E}(y)\text{)} \; , \end{aligned}$$

uma contradição com (105). ◇

Seja $\mathfrak{W} \in \mathbb{P}(M)$ tal que $\mathfrak{W} | \mathfrak{D}_i$.

Afirmação 5.44.

$$e\,(\mathfrak{W} \mid \mathfrak{W} \cap M_0) = m \qquad e \qquad f\,(\mathfrak{W} \mid \mathfrak{W} \cap M_0) = 1 \; .$$

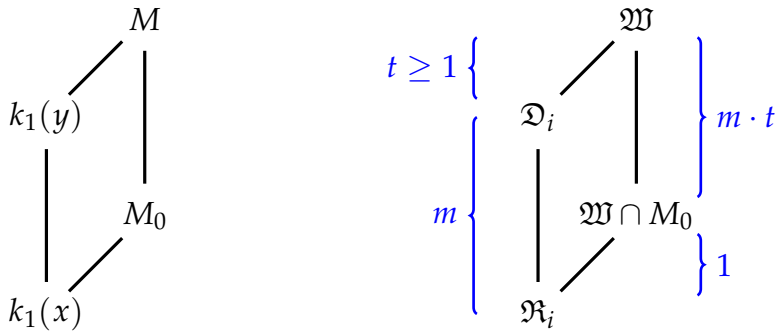
Dem.: Como $\mathfrak{W}$ é um *place* sobre $\mathfrak{D}_i \supseteq \mathfrak{R}_i$, temos que $\mathfrak{W} \cap M_0$ é uma extensão de $\mathfrak{R}_i$. Os *places* $\mathfrak{Q}_{(0,x)}$ e $\mathfrak{Q}_{(\infty,x)}$ são não ramificados em $\widetilde{E} \mid k(x)$; então o *place* $\mathfrak{R}_i$ é não ramificado na extensão intermediária $M_0 \mid k_1(x)$:

$$e\left(\mathfrak{W} \cap M_0 \mid \mathfrak{R}_i\right) = 1 \ . \tag{109}$$

O índice de ramificação $t := e\left(\mathfrak{W} \mid \mathfrak{D}_i\right)$ é algum valor inteiro que não precisaremos conhecer; bastará sabermos que $t \geq 1$. O índice da extensão $\mathfrak{D}_i \mid \mathfrak{R}_i$ é m, pela Equação 104. Assim, pela transitividade do índice, temos que

$$e\left(\mathfrak{W} \mid \mathfrak{W} \cap M_0\right) = m \cdot t \ . \tag{110}$$

Figura 56. Índices de ramificação do zero e do polo de x em $k_1(x)$ nos corpos M e M_0.



Logo,

$$m \leq m \cdot t \overset{\text{Eq. 110}}{=} e\left(\mathfrak{W} \mid \mathfrak{W} \cap M_0\right) \overset{\text{Cor. 3.49}}{\leq} \left[M : M_0\right] \overset{\text{Eq. 107}}{=} m \ .$$

Segue a primeira igualdade da tese. A segunda igualdade da tese segue da primeira, combinada com a Igualdade Fundamental (Teorema 3.48). ◇

Suponha que $\mathfrak{R}_1$ seja extensível a r *places* em M_0 — digamos,

$$\mathfrak{T}_1 \ , \ \ldots \ , \ \mathfrak{T}_r \in \mathbb{P}(M_0) \ .$$

Uma vez que $\left[M_0 : k_1(x)\right] > 1$, temos pela Igualdade Fundamental (Teorema 3.48) duas possibilidades:

- ou $r = 1$ — o que implicaria que

$$f\left(\mathfrak{T}_1 \mid \mathfrak{R}_1\right) \geq 2\,,$$

já que $\mathfrak{Q}_{(0,x)}$ é não ramificado em $\widetilde{E} \,\Big|\, k(x)$ —;

- ou $r \geq 2$.

Como $\mathfrak{W} \supseteq \mathfrak{D}_i \supseteq \mathfrak{R}_i$, temos que $\mathfrak{W} \supseteq \mathfrak{T}_j \supseteq \mathfrak{R}_1$ para $j \in \{1, 2, \ldots, r\}$.
Então:

- Ou pelo menos dois *places* são totalmente ramificados e um deles é de grau maior ou igual a dois:

$$\begin{aligned}\deg_k(\mathfrak{T}_1) &= f\left(\mathfrak{T}_1 \mid \mathfrak{R}_1\right) \cdot \deg_k(\mathfrak{R}_1) \\ &\geq 2\,.\end{aligned}$$

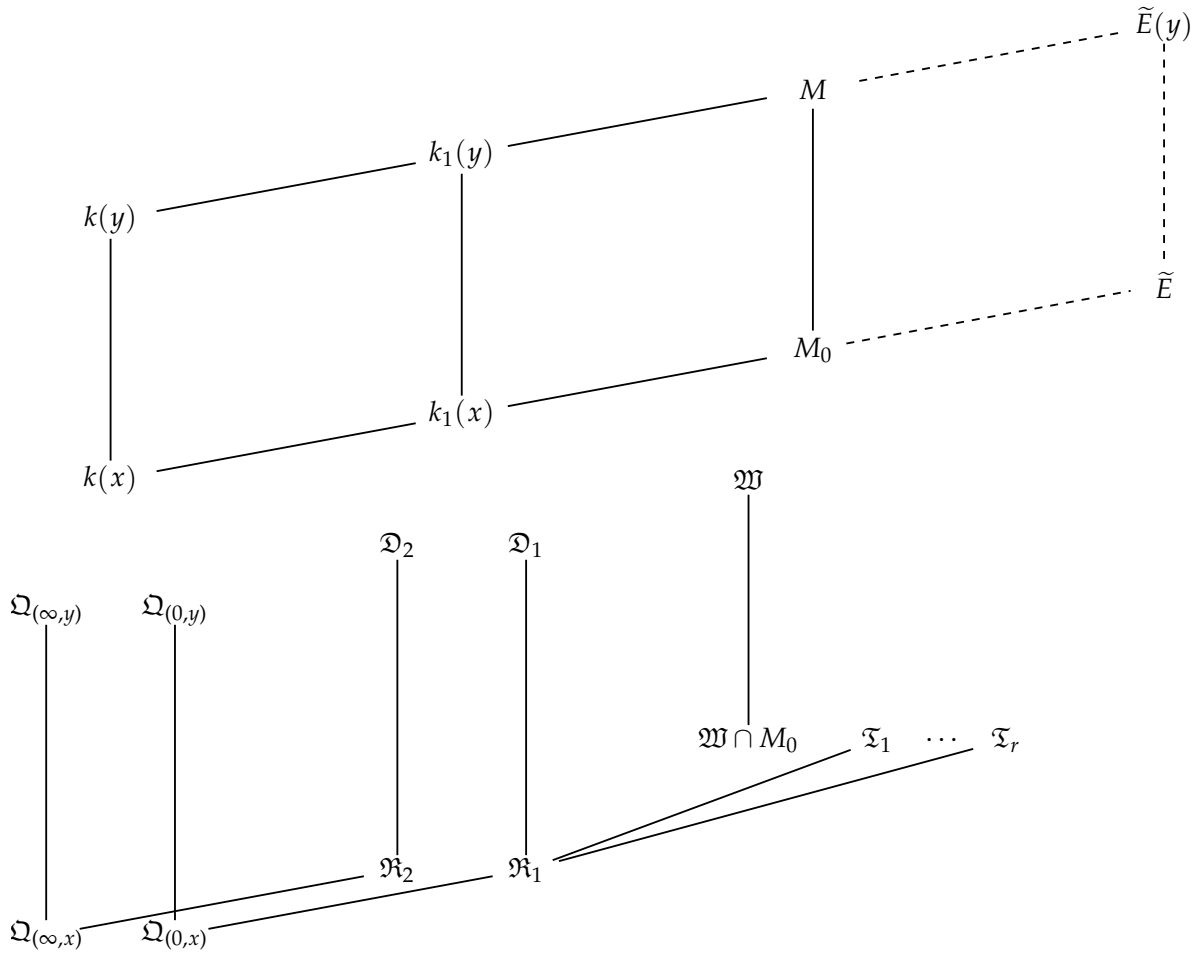
- Ou pelo menos três *places* de M são totalmente ramificados em $M \mid M_0$, já que $\mathfrak{W} \mid \mathfrak{T}_i$ para algum i.

Em qualquer caso, o suporte do diferente de $M \mid M_0$ é constituído de pelo menos três *places*.

Pela Fórmula do Gênero de Riemann-Hurwitz (Teorema 3.76), temos

$$\begin{aligned}g_M &= 1 + \frac{\left[M : M_0\right]}{\left[k_1 : k_1\right]} \cdot (g_{M_0} - 1) + \frac{1}{2} \cdot \deg_k\big(\mathrm{Diff}\left(M \mid M_0\right)\big) \\ &\geq 1 + \frac{m}{1} \cdot (0 - 1) + \frac{3}{2} \cdot (m - 1) \\ &= \frac{m-1}{2} \\ &> \frac{(2 \cdot C + 3) - 1}{2} \qquad \text{(por (96))} \\ &= C + 1 \\ &> C\,.\end{aligned}$$

Figura 57. O estudo do índice de ramificação nas extensões do zero e do polo de x em $k(x)$ nos corpos $k_1(x)$, $k_1(y)$, M e M_0.



(Item 4): Seja

$$k_1 := N \cap l\,.$$

Afirmação 5.45. $k_1(y) \subseteq N(y) \cap F$.

Dem.: Da definição de k_1, temos que $k_1(y) \subseteq N(y)$. Além disso,

$$\begin{aligned} k_1(y) = (N \cap l)(y) &\subseteq l(y) \\ &\subseteq \widetilde{E}(y) \\ &= F\,. \end{aligned}$$

A tese segue. ◇

Afirmação 5.46.

$$N(y) \cap F \subsetneq M' \cap F \subseteq F \, .$$

Dem.: As inclusões seguem da hipótese de M' ser um corpo intermediário de $(F{\cdot}N) \mid N(y)$. Resta provar que a primeira inclusão é própria.

Por absurdo, suponha que

$$N(y) \cap F = M' \cap F \, . \tag{111}$$

Vamos provar separando em dois casos.

(Caso 1 de 2, $N(y) \neq M' \cap F$): neste caso, $N(y){\cdot}\big(M' \cap F\big) \neq N(y)$; assim, teríamos que

$$N(y) = N(y){\cdot}\big(N(y) \cap F\big) \overset{\text{Eq. 111}}{\underset{\downarrow}{=}} N(y){\cdot}\big(M' \cap F\big) \supsetneq N(y) \, ,$$

um absurdo.

(Caso 2 de 2, $N(y) = M' \cap F$): neste caso,

$$N(y) = M' \cap F \overset{\text{Eq. 111}}{\underset{\downarrow}{=}} N(y) \cap F \, .$$

Então teríamos que $F \supseteq N(y) \supseteq N$ e, portanto,

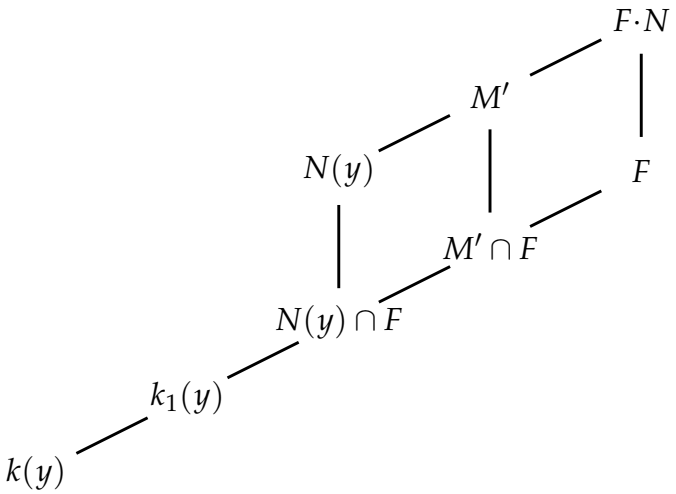
$$F{\cdot}N = F \, . \tag{112}$$

Assim,

$$M' \overset{\text{Exp. 95}}{\underset{\downarrow}{=}} M' \cap F{\cdot}N \overset{\text{Eq. 112}}{\underset{\downarrow}{=}} M' \cap F \overset{\text{Eq. 111}}{\underset{\downarrow}{=}} N(y) \cap F \overset{\text{Eq. 112}}{\underset{\downarrow}{=}} N(y) \cap F{\cdot}N \overset{\text{Exp. 95}}{\underset{\downarrow}{=}} N(y) \, ,$$

uma contradição com (95). ◇

Figura 58. Os subcorpos de $F \cdot N$.



Afirmação 5.47. $k_1(y) \subsetneq M' \cap F$.

Dem.:

$$k_1(y) \overset{\text{Af. 5.45}}{\subseteq} N(y) \cap F \overset{\text{Af. 5.46}}{\subsetneq} M' \cap F \, .$$

◇

O corpo de constantes de $M' \cap F$ é k_1 e $M' \supseteq \left(M' \cap F\right) \cdot N$. Isso implica que

$$\begin{aligned} g_{M'} &\geq g_{\left(M' \cap F\right) \cdot N} && \text{(pela Observação 3.25)} \\ &= g_{M' \cap F} && \text{(pelo Teorema 3.78)} \\ &> C && \text{(pelo item 3)} \ . \end{aligned}$$

Note que pudemos aplicar o item 3 para $M = M' \cap F$ justamente pela validez da Afirmação 5.47. □

Na próxima Proposição, vamos construir C_0-*improvements* com condições mais específicas sobre as constantes C, C_1 e C_2 da Proposição 5.35.

Proposição 5.48 (construção de C_0-*improvements* para o Teorema Principal)**.** *Sejam:* $F \mid k(y)$ *e* $E \mid k(x)$ *as extensões de corpos de funções com as propriedades indicadas na Proposição*

5.35; $m' := \left[E : k(x)\right]$; $K \,/\, k$ *uma extensão finita de* $k(y) \,/\, k$; K_0 *o fecho separável de* $k(y)$ *em* K; $C_0 \in \mathbb{R}_+$;

$$S_{K_0|\,k(y)} := \left\{ \mathfrak{P} \in \mathbb{P}\big(k(y)\big) \;\middle|\; \mathfrak{P} \text{ é ramificado ou inseparável em } K_0 \mid k(y) \right\} ; \tag{113}$$

e n_s *o número de* places *em* $S_{K_0|\,k(y)}$. *Seja* $d_s \in \mathbb{Z}$ *tal que*

$$\max \left\{ \deg_k(\mathfrak{P}) \;\middle|\; \mathfrak{P} \in S_{K_0|\,k(y)} \right\} \leq d_s \, . \tag{114}$$

Suponha que as constantes C, C_1 *e* C_1 *da Proposição 5.35 satisfaçam as condições adicionais seguintes:*

$$C > g_{K_0} \, , \qquad C_1 > n_s + 2 \cdot \big(m' + C_0\big) \, , \qquad C_2 > \max\left\{ d_s, 2 \cdot \big(m' + C_0\big) \right\} . \tag{115}$$

Então

1. *O corpo de constantes de* $E_1 \cdot K$ *é* k.
2. *a)* $\left[E_1 : k(y)\right] = \left[E_1 \cdot K : K\right]$,
   b) $\mathrm{Aut}\left(E_1 \,\middle|\, k(y)\right) \;\cong\; \mathrm{Aut}\left(E_1 \cdot K \,|\, K\right)$, *e*
   c) $F \cdot K$ *é o fecho normal de* $(E_1 \cdot K) \mid K$.
3. *Para todo corpo* H *tal que* $K \subsetneq H \subseteq E_1 \cdot K$, *temos*

$$g_H \geq C_0 \, .$$

Demonstração. O corpo de constantes de $K \cap F$ é k pelo Lema 5.1, pois $K \cap F$ é corpo intermediário da extensão $F \mid k(x)$:

$$F \supseteq F \cap K \supseteq k(y) \supseteq k(x) \, .$$

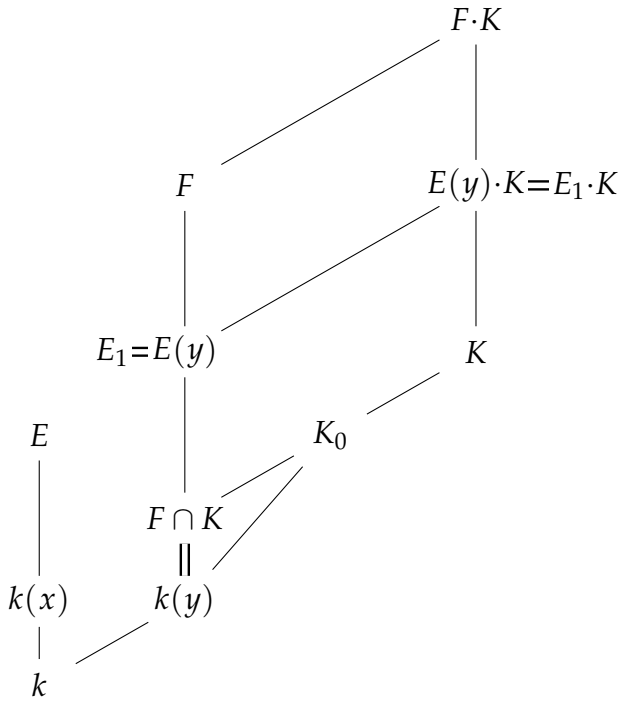
A extensão $(K \cap F) \mid k(y)$ é separável (porque $F \mid k(y)$ é Galois e, portanto, a "torre" de corpos $F \supseteq K \cap F \supseteq k(y)$ é separável). Como K_0 contém todos os elementos de K que são separáveis sobre $k(y)$, temos que $K \cap F \subseteq K_0$. Portanto,

$$\begin{aligned} g_{K \cap F} &\leq g_{K_0} && \text{(pela Observação 3.25)} \\ &< C && \text{(da hipótese)} \; . \end{aligned} \tag{116}$$

Afirmação 5.49. $K \cap F = k(y)$.

Dem.: Se fosse $K \cap F \supsetneq k(y)$, teríamos que $g_{K\cap F} > C$ pelo item 3 da Proposição 5.35: contradição com (116). ◇

Figura 59. Os corpos $k(y)$ e $F \cap K$ são iguais. A ilustração mostra como $k(y)$ está relacionada com os demais corpos de funções considerados até o momento.



(Item 2): Como F é o fecho normal de $E_1 \mid k(y)$ (item 1(a)iv da Proposição 5.35), então $F \mid k(y)$ é Galois. A demonstração do item 2 é totalmente análoga à prova das afirmações 5.39 e 5.40.

Seja $H \leq \mathrm{Gal}\left(E \mid k(y)\right)$ tal que

$$E_1 = F^H .$$

Como K é fixado por $\varphi^{-1}[H]$, temos que

$$E_1 \cdot K = (F \cdot K)^{\varphi^{-1}[H]} .$$

Assim, pelo TFTG,

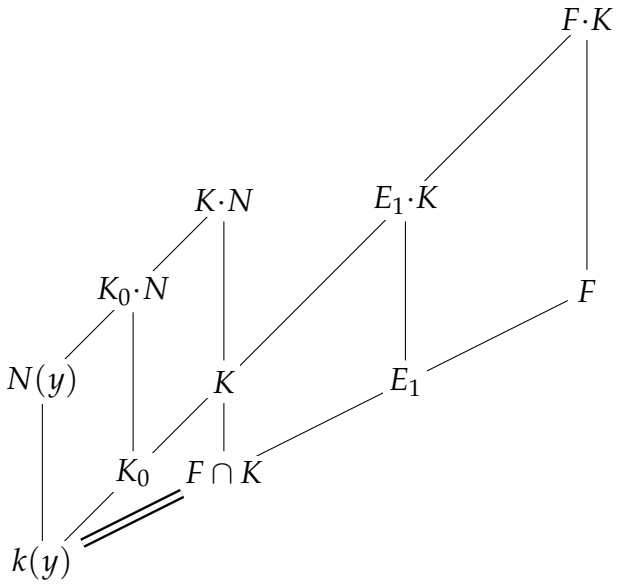
$$\left[E_1 \cdot K : K\right] = \frac{\left|\mathrm{Gal}\left(F \cdot K \mid K\right)\right|}{\left|\varphi^{-1}[H]\right|} = \frac{\left|\mathrm{Gal}\left(F \mid k(y)\right)\right|}{|H|} = \left[E_1 : k(y)\right] .$$

Além disso,

$$\begin{aligned}\operatorname{Aut}\left(E_1 \mid k(y)\right) &\cong \left\{\tau \in \operatorname{Gal}\left(F \mid k(y)\right) \;\middle|\; \tau\left[E_1\right] = E_1\right\} \\ &= \varphi\left[\left\{\sigma \in \operatorname{Gal}\left(F{\cdot}K \mid K\right) \;\middle|\; \sigma\left[E_1{\cdot}K\right] = E_1{\cdot}K\right\}\right] \\ &\cong \varphi\left[\operatorname{Aut}\left(E_1{\cdot}K \mid K\right)\right] \\ &\cong \operatorname{Aut}\left(E_1{\cdot}K \mid K\right) .\end{aligned}$$

(Item 1): Seja N o corpo de constantes de $E_1{\cdot}K$. A extensão $(E_1{\cdot}K) \mid K$ é separável, pois é extensão intermediária de $F{\cdot}K \mid K$, que é Galois pelo item 2. Pela Proposição 3.88, temos também que $N \mid k$ é separável.

Figura 60. Subcorpos de $F{\cdot}K$ e $K{\cdot}N$.



Afirmação 5.50. *O corpo de constantes de* $(F{\cdot}N) \cap (K{\cdot}N)$ *é* N.

Dem.: Veja *Lemma* 3.1.2 no livro de Stichtenoth (2009, p. 69). ◇

O fecho separável de $N(y)$ em $K{\cdot}N$ é

$$\operatorname{sc}_{K\cdot N}\left(N(y)\right) = K_0{\cdot}N \,, \tag{117}$$

pois $N \mid k$ é uma extensão separável, y é um elemento separável sobre $k(x)$ e o fecho separável de $k(y)$ em K é K_0. Portanto,

$$\begin{aligned}(F\cdot N)\cap(K\cdot N) &= N(y) && \text{(pela Afirmação 5.49)}\\ &\subseteq \mathrm{sc}_{K\cdot N}\big(N(y)\big)\\ &= K_0\cdot N && \text{(pela Equação 117)}\ ;\end{aligned}$$

Assim,

$$\begin{aligned}g_{(F\cdot N)\cap(K\cdot N)} &\leq g_{K_0\cdot N} && \text{(pela Observação 3.25)}\\ &= g_{K_0} && \text{(pelo Teorema 3.78)}\\ &< C && \text{(por hipótese)}\ .\end{aligned} \tag{118}$$

Pelo item 4 da Proposição 5.35, temos que para todo corpo intermédio M,

$$N(y) \subsetneq M \subseteq F\cdot N\ ,$$

o gênero de M é tal que

$$g_M > C\ .$$

Afirmação 5.51. $(F\cdot N)\cap(K\cdot N) = N(y)$.

Dem.: Se fosse $(F\cdot N)\cap(K\cdot N) \supsetneq N(y)$, teríamos que

$$g_{(F\cdot N)\cap(K\cdot N)} > C\ ,$$

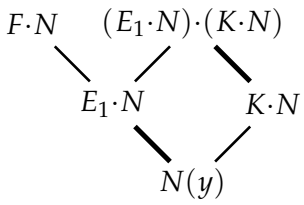
pelo item 4 da Proposição 5.35: contradição com (118). ◇

Segue que

$$\begin{aligned}\Big[E_1\cdot K : K\cdot N\Big] &= \Big[E_1\cdot N\cdot K\cdot N : K\cdot N\Big] && \text{(pela Observação 4.8)}\\ &= \Big[E_1\cdot N : N(y)\Big]\ ,\end{aligned} \tag{119}$$

pois as extensões $E_1\cdot N$ e $K\cdot N$ são disjuntas pela Afirmação 5.51 (veja a Figura 61).

Figura 61. As extensões $E_1\cdot N$ e $K\cdot N$ são disjuntas.



Afirmação 5.52.

$$K{\cdot}N = K\ .$$

Dem.: Temos que

$$\begin{aligned}
\Big[E_1{\cdot}N : N(y)\Big] \cdot \Big[K{\cdot}N : K\Big] &= \Big[E_1{\cdot}K : K{\cdot}N\Big] \cdot \Big[K{\cdot}N : K\Big] \qquad \text{(por (119))} \\
&= \Big[E_1{\cdot}K : K\Big] \qquad \text{(transitividade do grau)} \\
&= \Big[E_1 : k(y)\Big] \qquad \text{(pelo item 2)} \\
&= \Big[E_1{\cdot}N : \big(k(y)\big){\cdot}N\Big] \\
&\qquad \text{(podemos usar a Observação 4.8,} \\
&\qquad \text{pois } N \mid k \text{ é separável)} \\
&= \Big[E_1{\cdot}N : N(y)\Big] \qquad \text{(pois } k \subseteq N\text{)}\ .
\end{aligned}$$

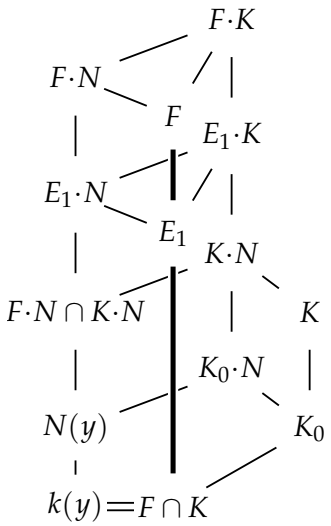
Por cancelamento,

$$\Big[K{\cdot}N : K\Big] = 1\ .$$

A tese segue. ◇

Pela Afirmação 5.52, $N \subseteq K$. Ou seja, o corpo K contém todas as constantes de $E_1{\cdot}K$. Segue que $N = k$.

Figura 62. Ilustração para a demonstração do item 1.



(Item 3): Seja E_2 um corpo tal que

$$k(y) \subsetneq E_2 \subseteq E_1 \qquad \text{e} \qquad H = E_2 \cdot K \, .$$

Pelo item 2 da Proposição 5.35, teremos que:

- ou existe um *place* $\mathfrak{U} \in \mathbb{P}\big(k(y)\big)$ ramificado ou inseparável em $E_2 \mid k(y)$ de grau

$$\deg_k(\mathfrak{U}) > C_2 \, ; \tag{120}$$

- ou existe um conjunto $S_{E_2|k(y)} \subseteq \mathbb{P}\big(k(y)\big)$ contendo r *places* ramificados ou inseparáveis em $E_2 \mid k(y)$, com $r > C_1$.

Vamos analisar cada um dos casos.

- No primeiro caso, como $\mathfrak{U}$ é ramificado ou inseparável em $E_2 \cdot K_0 \supseteq E_2 \supseteq k(y)$ e

$$\deg_k(\mathfrak{U}) > C_2 > d_s \, , \tag{121}$$

  temos a existência de um *place* de K_0 de grau maior que C_2 ramificado ou inseparável em $(E_2 \cdot K_0) \mid K_0$, pois neste caso $\mathfrak{U} \notin S_{K_0|k(y)}$ (compare (114) com (121)).

- No segundo caso,

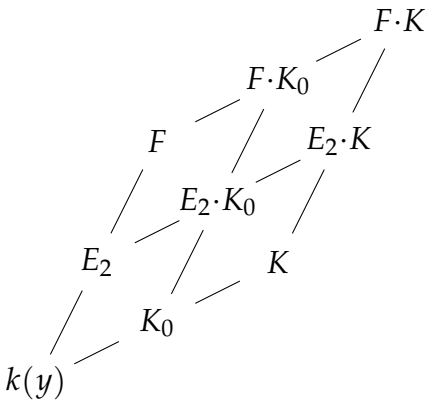
$$r > C_1 > n_s \, . \tag{122}$$

  Então existem no mínimo $r - n_s$ *places*

$$\widetilde{\mathfrak{P}} \in \mathbb{P}\big(k(y)\big) \setminus S_{K_0|k(y)} \tag{123}$$

  que são ramificados ou inseparáveis em $E_2 \mid k(y)$ (fora de $S_{K_0|k(y)}$). Tais *places* são ramificados ou inseparáveis em $E_2 \cdot K_0 \mid k(y)$; mas como $\widetilde{\mathfrak{P}} \notin S_{K_0|k(y)}$, segue que a ramificação ou a inseparabilidade de $\widetilde{\mathfrak{P}}$ ocorre entre $E_2 \cdot K_0$ e K_0. Assim, neste caso, $\mathbb{P}(K_0)$ contém mais de $C_1 - n_s$ *places* ramificados ou inseparáveis em $(E_2 \cdot K_0) \mid K_0$.

Figura 63. Subcorpos de $F \cdot K$ e $E_2 \cdot K$.



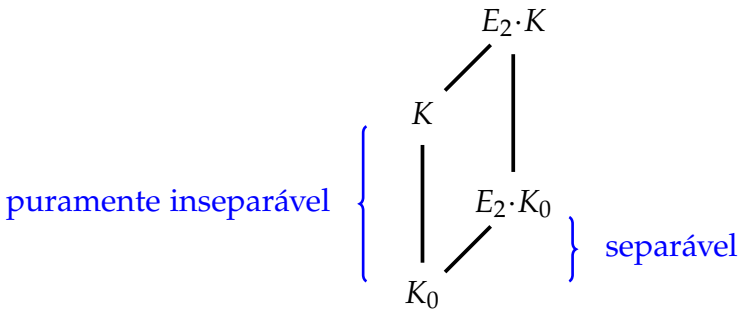
Afirmação 5.53. *A extensão* $(E_2{\cdot}K_0) \mid K_0$ *é finita e separável.*

Dem.: A extensão $E \mid k(x)$ é finita e separável, por hipótese; então $E(y) \mid k(y)$ e a extensão intermediária $E_2 \mid k(y)$ têm as mesmas propriedades.

Evidentemente, o fecho separável K_0 de K em $k(y)$ é uma extensão separável de $k(y)$. E o corpo K_0 é extensão finita de $k(y)$, pelo fato de ser extensão intermediária de $K \mid k(y)$. ◇

A validez da Afirmação 5.53 permitirá o uso do Lema 5.6 (veja a Figura 64).

Figura 64. Caso de uso do Lema 5.6 (compare com a Figura 33).



Uma vez que $K \mid K_0$ é puramente inseparável, temos pelo Lema 5.6 duas possibilidades.

- Ou existe um *place* $\widetilde{\mathfrak{U}} \in \mathbb{P}(K)$ ramificado ou inseparável em $(E_2{\cdot}K) \mid K$ de grau $\deg_k\left(\widetilde{\mathfrak{U}}\right) > C_2$.
- Ou existem mais de $C_1 - n_s$ *places* ramificados ou inseparáveis em $(E_2{\cdot}K) \mid K$.

Seja

$$\mathtt{D} := \mathrm{Diff}\,(E_2{\cdot}K \mid K)\ .$$

Afirmação 5.54. $\deg_k(\mathtt{D}) > 2 \cdot \left(m' + C_0\right)$.

Dem.: Sejam $\mathfrak{R}_1, \ldots, \mathfrak{R}_w \in \mathbb{P}(E_2{\cdot}K)$ e $a_1, \ldots, a_w \in \mathbb{N}$ tais que

$$\mathtt{D} = a_1\mathfrak{R}_1 + \ldots + a_w\mathfrak{R}_w\ .$$

Então

$$\begin{aligned}\deg_k(\mathtt{D}) = \deg_k\left(\sum_{i=1}^{w} a_i\mathfrak{R}_i\right) &= \sum_{i=1}^{w} a_i \deg_k(\mathfrak{R}_i) \\ &\geq \begin{cases} \deg_k\left(\widetilde{\mathfrak{U}}\right) & > & C_2\,, & \text{no primeiro caso; ou} \\ \sum_{i=1}^{C_1-n_s} 1 & = & C_1 - n_s\,, & \text{no segundo caso .} \end{cases}\end{aligned}$$

Em qualquer caso, a tese segue da hipótese acerca das constantes C_1 e C_2. ◇

Afirmação 5.55. $\left[E_2{\cdot}K : K\right] \leq m'$.

Dem.:

$$\begin{aligned}\left[E_2{\cdot}K : K\right] &\leq \left[E_1{\cdot}K : K\right] && \text{(pois } E_2 \subseteq E_1\text{)} \\ &= \left[E_1 : k(y)\right] && \text{(item 2a)} \\ &= \left[E : k(x)\right] && \text{(item 1(a)i da Proposição 5.35)} \\ &= m' \,.\end{aligned}$$

◇

Afirmação 5.56. *O corpo de constantes de $E_2{\cdot}K \,/\, k$ é k.*

Dem.: Pelo item 1, o corpo de constantes de $E_1{\cdot}K$ é k. O corpo $k(y)$, por sua vez, tem k como corpo de constantes (Exemplo 3.13). Então $E_1{\cdot}K \,/\, k$ é uma extensão geométrica de $k(y) \,/\, k$. A tese segue do fato de $E_2{\cdot}K$ ser corpo intermediário da extensão $E_1{\cdot}K \,|\, k(y)$. ◇

Portanto, das afirmações 5.54, 5.55 e 5.56,

$$\begin{aligned}g_H = g_{E_2\cdot K} &= 1 + \frac{\left[E_2{\cdot}K : K\right]}{\left[k : k\right]} \cdot (g_K - 1) + \frac{1}{2} \cdot \deg_k\big(\mathrm{Diff}\,(E_2{\cdot}K \mid K)\big) \\ &> -m' + \frac{1}{2} \cdot 2 \cdot \left(m' + C_0\right) \\ &= C_0 \,.\end{aligned}$$

□

Finalmente, estamos em condições de provar o Teorema Principal.

Teorema 5.57 (Álvarez-García e Villa-Salvador (2010))**.** *Sejam: $E \,/\, k$ um corpo de funções com corpo de constantes infinito; $E \mid k(x)$ uma extensão separável de grau $\left[E : k(x)\right] > 1$ que admite um* place $\mathfrak{p} \in \mathbb{P}\big(k(x)\big)$ *de grau* $\deg_k(\mathfrak{p}) = 1$ *ramificado em $E \mid k(x)$; e $K \,/\, k$ um corpo de funções de gênero $g_K > 1$.*

Então existem infinitos corpos de funções $L \supseteq K$ dois a dois não isomorfos tais que $L \mid K$ é uma extensão separável com

$$\left[L : K\right] = \left[E : k(x)\right]$$

e

$$\mathrm{Aut}\,(L \mid k) = \mathrm{Aut}\,(L \mid K) \;\cong\; \mathrm{Aut}\left(E \,\middle|\, k(x)\right) . \tag{124}$$

Demonstração. Seja $n = \big|\mathrm{Aut}\,(K \mid k)\big|$. Pela Observação 3.80, n é finito.

Vamos supor primeiro que $n > 1$. Sejam

$$\sigma_1 \,, \;\; \ldots \,, \;\; \sigma_{n-1} \in \mathrm{Aut}\,(K \mid k) \setminus \{\mathrm{id}_K\} \,. \tag{125}$$

Afirmação 5.58. *Existem $\mathfrak{B}_1, \ldots, \mathfrak{B}_{n-1} \in \mathbb{P}(K)$ distintos tais que os* places *$\sigma_1(\mathfrak{B}_1), \ldots, \sigma_{n-1}(\mathfrak{B}_{n-1})$ satisfazem*

$$\mathfrak{B}_i \neq \sigma_j\big(\mathfrak{B}_j\big) \qquad \textit{se} \quad i \,, \;\; j \in \{1, 2, \ldots, n-1\} \;\; . \tag{126}$$

Dem.: Para cada $i \in \{1, 2, \ldots, n-1\}$, existe uma coleção infinita de *places* $A_{\sigma_i} \subseteq \mathbb{P}(K)$ que não são fixados por σ_i — cf. Lema 5.11, para a extensão $K \,\Big|\, K^H$. Sejam $E_{\sigma_i} \subseteq A_{\sigma_i}$ um subconjunto infinito enumerável e

$$\mathscr{C} := \bigcup_{j=1}^{n-1} E_{\sigma_j} \,. \tag{127}$$

Fixe uma enumeração para $\mathscr{C}$:

$$(\mathfrak{Q}_\alpha)_{\alpha \in \mathbb{N}} \,. \tag{128}$$

Suponha que a sequência em (128) não tenha termos repetidos.

Vamos escolher candidatos a *places* que satisfaçam a tese, em etapas.

1^o) Seja $a \in \mathbb{N}$ tal que

$$\mathfrak{B}_1 := \mathfrak{Q}_a \in E_{\sigma_1} \ .$$

2^o) Seja $b \in \mathbb{N}$ tal que $b > a$ e

$$\mathfrak{B}_2 := \mathfrak{Q}_b \in E_{\sigma_2} \ , \qquad \mathfrak{B}_2 \neq \sigma_k(\mathfrak{B}_1) \qquad \text{e}$$
$$\mathfrak{B}_2 \neq \sigma_k(\mathfrak{B}_2) \qquad (\forall\, k \in \{1, 2, \ldots, n-1\}) \ .$$

Note que tal inteiro b existe, pois E_{σ_2} é um conjunto infinito.

3^o) Seja $c \in \mathbb{N}$ tal que $c > b$ e

$$\mathfrak{B}_3 := \mathfrak{Q}_c \in E_{\sigma_3} \ , \qquad \mathfrak{B}_3 \neq \sigma_k(\mathfrak{B}_1) \ ,$$
$$\mathfrak{B}_3 \neq \sigma_k(\mathfrak{B}_2) \qquad \text{e}$$
$$\mathfrak{B}_3 \neq \sigma_k(\mathfrak{B}_3) \qquad (\forall\, k \in \{1, 2, \ldots, n-1\}) \ .$$

Note que procuramos escolher c maior que b justamente para que sejam válidas as inequações $\mathfrak{B}_1 \neq \mathfrak{B}_3 \neq \mathfrak{B}_2$.

Prosseguindo desta forma — até o $(n-1)$-ésimo passo —, a tese segue. $\diamond$

Pelo teorema de aproximação (Corolário 3.16), existe $w \in K$ tal que

$$v_{\sigma_i(\mathfrak{B}_i)}(w) > 0 \qquad \text{e} \qquad v_{\mathfrak{B}_i}(w) = -1 \ .$$

Sejam K_0 o fecho separável de $k(w)$ em K e n_s o número de *places* no conjunto

$$S_{K_0|k(w)} := \left\{ \mathfrak{R} \in \mathbb{P}\big(k(w)\big) \;\middle|\; \mathfrak{R} \text{ é ramificado ou inseparável em } K_0 \mid k(w) \right\} . \tag{129}$$

Escolha $d_s \in \mathbb{Z}_+$ tal que

$$\max \left\{ \deg_k(\mathfrak{R}) \;\middle|\; \mathfrak{R} \in S_{K_0|k(w)} \right\} \leq d_s \ . \tag{130}$$

Pela explicação dada na Seção 4.6, podemos assumir que o *place* $\mathfrak{Q}_{x-1}$ de $k(x)$ é ramificado em $E \mid k(x)$ e que o zero e o polo de x em $k(x)$ são não ramificados e separáveis em $E \mid k(x)$.

Considere o corpo de funções $F \,/\, l$ construído na Proposição 5.35 com

$$C_0 := 1 + \Big[E : k(x)\Big] \cdot (g_K - 1) + 4 \cdot \Big[E : k(x)\Big]^2 \cdot g_K^2 \cdot d \tag{131}$$

— em que $d := \min \left\{ \deg_k(\mathfrak{B}) \;\middle|\; \mathfrak{B} \in \mathbb{P}(K) \right\}$ — e as desigualdades em (115) na Proposição 5.48.

Seja $z := \frac{1}{y-1}$. Sejam $\mathfrak{R}_\infty$ o polo de z em $k(z)$ e $\mathfrak{R}_0$ o zero de z em $k(z)$.

Afirmação 5.59. $\mathfrak{Q}_{(\infty,y)} = \mathfrak{R}_0$.

Dem.: Vamos verificar que as valorações associadas a $\mathfrak{Q}_{(\infty,y)}$ e a $\mathfrak{R}_0$ assumem o mesmo valor quando calculados em z. Temos que

$$\begin{aligned} v_{\mathfrak{Q}_{(\infty,y)}}(z) &= v_{\mathfrak{Q}_{(\infty,y)}}\left(\frac{1}{y-1}\right) \\ &= -v_{\mathfrak{Q}_{(\infty,y)}}(y-1) \\ &= -\min\left\{v_{\mathfrak{Q}_{(\infty,y)}}(y), v_{\mathfrak{Q}_{(\infty,y)}}(-1)\right\} = -\min\{-1,0\} \\ &= 1\ . \end{aligned}$$

Além disso, a valoração associada a $\mathfrak{R}_0$ também assume valor igual a 1 quando avaliada em z:

$$v_{\mathfrak{R}_0}(z) = 1\ .$$

Pela unicidade do zero de z em $k(z)$ (Exemplo 3.15), a tese segue. ◇

Afirmação 5.60. $\mathfrak{Q}_{y-1} = \mathfrak{R}_\infty$.

Dem.: A demonstração é totalmente análoga à prova da Afirmação 5.59. Verificamos primeiro que

$$v_{\mathfrak{Q}_{y-1}}(z) = v_{\mathfrak{Q}_{y-1}}\left(\frac{1}{y-1}\right) = -v_{\mathfrak{Q}_{y-1}}(y-1) = -1\ .$$

Avaliada em z, a valoração associada a $\mathfrak{R}_\infty$ também assume valor igual a -1:

$$v_{\mathfrak{R}_\infty}(z) = -1\ .$$

A tese segue também do Exemplo 3.15. ◇

Temos que

- o polo $\mathfrak{R}_\infty$ de z em $k(z)$ é ramificado em $F \mid k(z)$ (pela Afirmação 5.60 e pelo item 1(b)i da Proposição 5.35); e
- o zero $\mathfrak{R}_0$ de z em $k(z)$ é não ramificado e separável em $F \mid k(z)$ (pela Afirmação 5.59 e pelo item 1(b)ii da Proposição 5.35).

O isomorfismo

$$\begin{array}{rccc} \varphi: & k(w) & \to & k(z) \\ & f(w) & \mapsto & f(z) \end{array}$$

é extensível a um homomorfismo $\overline{\varphi}$ de K em um fecho algébrico ${}^{ac}\overline{k(z)}$ de $k(z)$ e, claramente, o homomorfismo

$$\begin{array}{ccc} K & \to & \overline{\varphi}\,[K] \subseteq {}^{ac}\overline{k(z)} \\ f & \mapsto & \overline{\varphi}(f) \end{array}$$

(que denotaremos também por $\overline{\varphi}$, por abuso) é um isomorfismo de corpos — cf. Seção 4.6. Portanto, podemos assumir que K é uma extensão de $k(z)$, que K_0 é o fecho separável de $k(z)$ em K e que n_s é o número de *places* $\mathfrak{R} \in \mathbb{P}\big(k(z)\big)$ ramificados ou inseparáveis em $K_0 \mid k(z)$ (com $\deg_k(\mathfrak{R}) \leq d_s$). Também podemos substituir $\overline{\varphi}(\mathfrak{B}_i)$ por $\mathfrak{B}_i$ e $\overline{\varphi} \circ \sigma_i \circ \overline{\varphi}^{-1}$ por σ_i de modo que

$$v_{\sigma_i(\mathfrak{B}_i)}(z) > 0 \qquad \text{e} \qquad v_{\mathfrak{B}_i}(z) = -1\,.$$

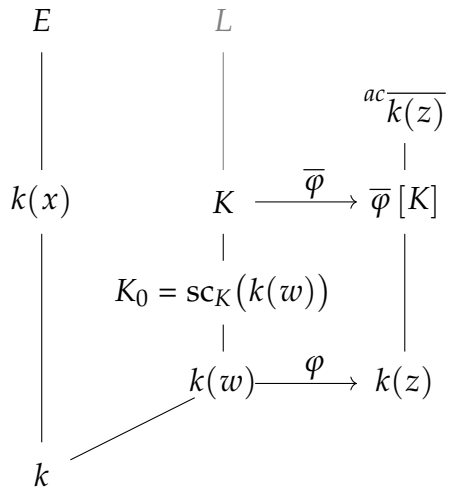
Afirmação 5.61. *Para todo $i \in \{1, 2, \ldots, n-1\}$, o* place *$\mathfrak{B}_i$ é não ramificado em $K \mid k(z)$.*

Dem.: Por absurdo, suponha que $s := e\left(\mathfrak{B}_j \,\middle|\, \mathfrak{B}_j \cap k(z)\right) > 1$, para algum $j \in \{1, 2, \ldots, n-1\}$. Então

$$-1 = v_{\mathfrak{B}_j}(z) = s \cdot v_{\mathfrak{B}_j \cap k(z)}(z)\,.$$

Assim, $v_{\mathfrak{B}_j \cap k(z)}(z) \in \mathbb{Q} \setminus \mathbb{Z}$. Pelo Teorema 3.8, isso é um absurdo. ◇

Figura 65. Não há perda de generalidade em supor que estamos trabalhando na variável z. A ilustração mostra a mudança de variáveis de w para z. A figura indica ainda onde estará situado o corpo L, a ser determinado.



Seja

$$L := E_1 \cdot K \,, \tag{132}$$

em que $E_1 = E(y)$ é o corpo de funções construído na Proposição 5.35.

Afirmação 5.62. *O corpo de constantes de L é k.*

Dem.: Item 1 da Proposição 5.48. ◇

Afirmação 5.63. $\mathrm{Aut}\left(E \,\middle|\, k(x)\right) \;\cong\; \mathrm{Aut}\,(L \mid K)$.

Dem.:

$$\begin{aligned} \mathrm{Aut}\left(E \,\middle|\, k(x)\right) &\cong \mathrm{Aut}\left(E_1 \,\middle|\, k(y)\right) \quad \text{(item 1 da Proposição 5.35)} \\ &\cong \mathrm{Aut}\,(L \mid K) \quad \text{(item 2 da Proposição 5.48)} \,. \end{aligned}$$

◇

Ainda pelo item 2 da Proposição anterior, temos também o seguinte.

Afirmação 5.64. *O grau de* $L \mid K$ *é* $\left[L : K\right] = \left[E : k(x)\right]$.

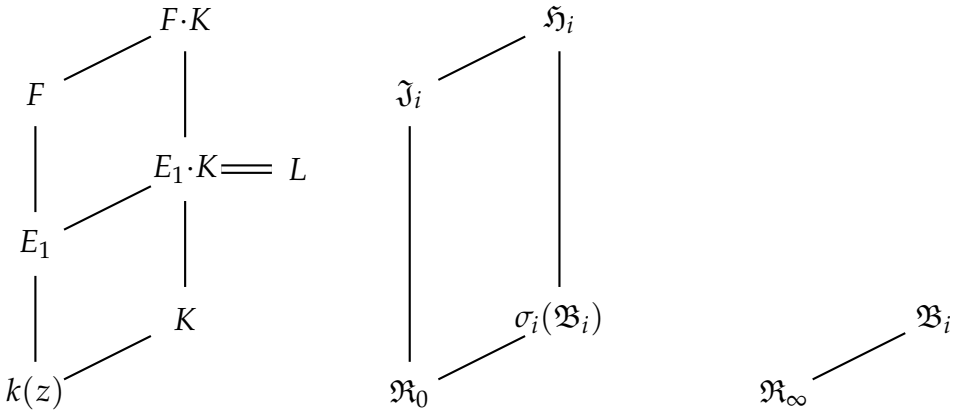
Dem.:

$$\begin{aligned}\left[L : K\right] &= \left[E_1 \cdot K : K\right] \\ &= \left[E_1 : k(y)\right] \quad \text{(item 2 da Proposição 5.48)} \\ &= \left[E : k(x)\right] \quad \text{(item 1 da Proposição 5.35)} .\end{aligned}$$

◇

Seja $\mathfrak{H}_i \in \mathbb{P}(F \cdot K)$ uma extensão de $\sigma_i(\mathfrak{B}_i)$ e $\mathfrak{J}_i := \mathfrak{H}_i \cap F$.

Figura 66. Extensões de $\mathfrak{R}_0$ e de $\mathfrak{R}_\infty$ nos subcorpos de $F \cdot K$.



Afirmação 5.65. $\mathrm{Aut}\,(L \mid k) = \mathrm{Aut}\,(L \mid K)$.

Dem.: ($\supseteq$): Seja $\sigma \in \mathrm{Aut}\,(L \mid K)$. Como σ é um automorfismo em L que fixa K, então σ também fixará o subcorpo $k \subseteq K$. ($\subseteq$): Seja $\sigma \in \mathrm{Aut}\,(L \mid k)$. Pelo item 3 da Proposição 5.48 e pela Afirmação 5.64, temos para todo corpo H com $K \subsetneq H \subseteq L$ que

$$g_H > 1 + \left[H : K\right] \cdot (g_K - 1) + 4 \cdot \left[H : K\right]^2 \cdot \left(g'_K\right)^2 \cdot d .$$

Pela Proposição 5.33, temos que $\sigma\,[K] = K$. Então $\sigma_0 := \sigma\restriction_K \in \mathrm{Aut}\,(K)$. Como σ fixa k (por escolha), então a restrição de σ a K também fixa k:

$$\sigma_0 \in \mathrm{Aut}\,(K \mid k) .$$

Basta provar que $\sigma_0 = \mathrm{id}_K$.

Como o *place* $\mathfrak{R}_\infty$ é ramificado em $F \mid k(z)$, então ele também ramifica-se em $F{\cdot}K \mid k(z)$. Pela Afirmação 5.61, a ramificação de $\mathfrak{R}_\infty$ não ocorre em $K \mid k(z)$. Portanto, a ramificação de $\mathfrak{R}_\infty$ ocorre na extensão $F{\cdot}K \mid K$. Segue que cada $\mathfrak{B}_i$ é ramificado em $(F{\cdot}K) \mid K$. Pelo Lema 5.5, cada $\mathfrak{B}_i$ é ramificado ou inseparável em $L \mid K$ (note que $F{\cdot}K$ é o fecho normal de $L \mid K$, pelo item 2 da Proposição 5.48).

Uma vez que o grupo de inércia $G_T(\mathfrak{H}_i \mid \sigma_i(\mathfrak{B}_i))$ é imersível no grupo de inércia $G_T(\mathfrak{J}_i \mid \mathfrak{R}_0)$ e $\mathfrak{R}_0$ e é não ramificado e separável em $F \mid k(z)$, os *places*

$$\sigma_1(\mathfrak{B}_1)\,, \qquad \ldots\,, \qquad \sigma_{n-1}(\mathfrak{B}_{n-1})$$

são não ramificados e separáveis em $(F{\cdot}K) \mid K$. Portanto, cada *place* $\sigma_i(\mathfrak{B}_i)$ é não ramificado e separável na extensão intermediária $L \mid K$.

A conclusão é que σ_i age nos *places* de K transformando o *place* $\mathfrak{B}_i$ (ramificado ou inseparável em $L \mid K$) no *place* $\sigma_i(\mathfrak{B}_i)$ (não ramificado e separável em $L \mid K$), para todo $i \in \{1, 2, \ldots, n-1\}$. Então $\sigma_0 \neq \sigma_i$.

Pela arbitrariedade de σ, segue por exclusão que $\mathrm{id}_K = \sigma_0$. ◇

Afirmação 5.66. *$L \mid K$ é separável.*

Dem.: A extensão $F{\cdot}K \mid K$ é Galois pela demonstração da Proposição 5.48. Então a extensão intermediária $L \mid K$ é separável. ◇

Afirmação 5.67. *Existem infinitos corpos L que satisfazem o resultado.*

Dem.: Construímos o corpo L de modo que o gênero g_H de todo corpo intermediário $H \neq K$ de $L \mid K$ tenha uma cota inferior prefixada (item 3 da Proposição 5.48). Em particular, o gênero g_L de L pode ser escolhido arbitrariamente grande. Se tivéssemos construído dois corpos L_1 e L_2 (digamos) com o mesmo procedimento da construção de L mas com gêneros distintos, teríamos necessariamente que $L_1 \not\cong L_2$ (Observação 3.28). ◇

Se $n = 1$, a extensão L é obtida como antes. Fazemos as seguintes observações para justificar o porquê de podermos escolher L como na Equação 132 também neste caso.

- As demonstrações das proposições 5.35 e 5.48 não mencionam em nenhum momento a cardinalidade do grupo $\mathrm{Aut}(K \mid k)$. Assim, as provas das afirmações 5.59, 5.60, 5.62, 5.63, 5.64, 5.66 e 5.67 podem ser replicadas *ipsis litteris*.

- No caso $n = 1$, a demonstração da Afirmação 5.65 é imediata (repare que o uso das afirmações 5.58 e 5.61 é desnecessário neste caso).

□

5.4 CONSIDERAÇÕES FINAIS

Encerramos o trabalho com dois comentários, separados em duas subseções.

5.4.1 Relação do Teorema Principal com resultados históricos

Duas motivações importantes para esta dissertação que foram mencionadas na Introdução são os teoremas demonstrados nos artigos de Villa-Salvador e Rzedowski-Calderón (1991) e de Stichtenoth (1984). Enunciamos, a seguir, tais resultados.

Teorema 5.68 (Stichtenoth (1984): análogo do Teorema Principal para corpos de funções sobre corpos algebricamente fechados)**.** *Sejam: k um corpo algebricamente fechado; $E \mid k(x)$ uma extensão de corpos de funções com $\left[E : k(x)\right] > 1$; e K um corpo de funções sobre k.*

Então existem infinitas extensões não isomorfas $L \mid K$ tais que $\left[L : K\right] = \left[E : k(x)\right]$ e

$$\mathrm{Aut}\,(L \mid k) = \mathrm{Aut}\,(L \mid K) \;\cong\; \mathrm{Aut}\left(E \;\middle|\; k(x)\right).$$

Teorema 5.69 (Villa-Salvador e Rzedowski-Calderón (1991): análogo do Teorema Principal para corpos de funções sobre corpos finitos)**.** *Sejam: k um corpo finito; $E \mid k(x)$ uma extensão de corpos de funções com $\left[E : k(x)\right] > 1$; $\mathfrak{P}_0$ o zero de x em $k(x)$; $\mathfrak{P}_\infty$ o polo de x em $k(x)$; e K um corpo de funções sobre k.*

Suponha que $\mathfrak{P}_0$ seja ramificado em $E \mid k(x)$, e que $\mathfrak{P}_\infty$ não se ramifica em $E \mid k(x)$.

Então existem infinitas extensões não isomorfas $L \mid K$ tais que $\left[L : K\right] = \left[E : k(x)\right]$ e

$$\mathrm{Aut}\,(L \mid k) = \mathrm{Aut}\,(L \mid K) \;\cong\; \mathrm{Aut}\left(E \;\middle|\; k(x)\right).$$

O Teorema de Álvarez-García e Villa-Salvador (2010) permite a construção de uma classe de corpos de funções sobre k distinta daquelas efetuadas por Stichtenoth (1984) e por Villa-Salvador e Rzedowski-Calderón (1991). Por exemplo, o corpo $k = \mathbb{R}$ não é nem algebricamente fechado nem finito.

5.4.2 Relação do Teorema Principal com o Problema Inverso da Teoria de Galois

Conforme explicado na Introdução, o Problema Inverso da Teoria de Galois (PITG) pergunta quais grupos finitos ocorrem como grupo de Galois. Mais precisamente, o Problema Inverso pode ser posto da seguinte forma: dados um grupo finito G e um corpo K, existe uma extensão galoisiana $L \mid K$ tal que

$$G \cong \operatorname{Gal}(L \mid K) \, ? \tag{133}$$

Ou seja, uma solução para o PITG consiste em construir um corpo L de modo que seja satisfeita uma condição prefixada — especificamente, dada em (133) — para o grupo de automorfismos de $L \mid K$.

Por outro lado, o Teorema Principal (Teorema 5.57) envolve a construção de uma extensão separável $L \mid K$ conforme (124). Neste caso, a condição preestabelecida é que o grupo $\operatorname{Aut}(L \mid K)$ seja isomorfo a $G := \operatorname{Aut}\left(E \,\middle|\, k(x)\right)$, em que $E \mid k(x)$ é uma extensão separável de grau $\left[E : k(x)\right] > 1$ dada na hipótese. E, como vimos na Subseção 5.4.1, o Teorema Principal admite resultados análogos nos casos em que $K \,/\, k$ é um corpo de funções sobre um corpo de constantes finito (Teorema 5.69) ou algebricamente fechado (Teorema 5.68).

O artigo de Villa-Salvador e Rzedowski-Calderón (1991) mostra uma interessante relação entre as duas classes de problemas acima descritas. O Teorema 5.69 — um resultado contido nessa publicação — permite provar um caso específico do PITG:

Teorema 5.70. *Sejam k um corpo finito com q elementos e G um grupo nilpotente finito de ordem $|G| > 1$ tal que $\operatorname{mdc}\{|G|, q-1\} = 1$. Então, para todo corpo de funções K sobre k, existem infinitas extensões galoisianas não isomorfas $L \mid K$ tais que*

$$\operatorname{Aut}(L \mid k) = \operatorname{Gal}(L \mid K) \cong G \, .$$

Pela similaridade dos enunciados (e das demonstrações) do Teorema Principal e do Teorema 5.69, é natural suspeitar que o primeiro implique na existência de um análogo do Teorema 5.70 para corpos de funções sobre corpos *infinitos*. Não temos ciência de uma publicação com esse resultado.

6 APÊNDICE A

6.1 RELAÇÕES ENTRE VALORAÇÕES, FUNÇÕES *places* E ANÉIS DE VALORAÇÃO

As noções de valorações, funções *places* e anéis de valoração são equivalentes.

A Tabela 1 ilustra o "dicionário" entre as teorias. Na coluna à esquerda, indicamos a proposição que contém o enunciado preciso da passagem de uma linguagem para outra.

Tabela 1. O "dicionário" entre as teorias de valorações, funções *places* e anéis de valoração.

	valores absolutos	valorações com $G \subseteq \mathbb{R}$	valorações	anéis de valoração	funções *places*
Proposição 6.17, p. 138	$\|\cdot\| \rightsquigarrow v_{\|\cdot\|}$				
Proposição 6.16, p. 138	$\|\cdot\|_v \leftsquigarrow v$				
Proposição 6.6, p. 135			$v_{\mathcal{O}} \leftsquigarrow \mathcal{O}$		
Proposição 6.13, p. 137				$\mathcal{O} \rightsquigarrow \varphi_{\mathcal{O}}$	
Proposição 6.5, p. 135			$v \rightsquigarrow \mathcal{O}_v$		
Proposição 6.12, p. 137				$\mathcal{O}_\varphi \leftsquigarrow \varphi$	
Proposição 6.19, p. 139	$\|\cdot\|_{v_1} \sim \|\cdot\|_{v_2} \iff v_1 \sim v_2$				
Proposição 6.8, p. 136			$v_1 \sim v_2 \iff \mathcal{O}_{v_1} = \mathcal{O}_{v_2}$		
Proposição 6.15, p. 138				$\mathcal{O}_{\varphi_1} = \mathcal{O}_{\varphi_2} \iff \varphi_1 \sim \varphi_2$	

A seguir, expomos trechos extraídos do livro de Villa-Salvador (2006). A generalidade dos resultados e das definições nesta seção é maior do que a necessária para a dissertação. A observação final (Observação 6.20) indica os casos particulares de maior interesse para esta dissertação.

Definição 6.1 (grupo ordenado). *Um grupo ordenado é um terno $(G, +, <)$ em que $(G, +)$ é um grupo abeliano e "$<$" é uma relação que satisfaz, para quaisquer α, β, $\gamma \in G$:*

1. *(tricotomia) $\alpha < \beta$ ou $\beta < \alpha$ ou $\alpha = \beta$;*
2. *(transitividade) se $\alpha < \beta$ e $\beta < \gamma$ então $\alpha < \gamma$; e*
3. *(preservação da operação do grupo) se $\alpha < \beta$ então $\alpha + \gamma < \beta + \gamma$.*

(VILLA-SALVADOR, 2006, p. 16).

Denota-se $\alpha \leq \beta$ quando $\alpha < \beta$ ou $\alpha = \beta$.

Definição 6.2 (valoração). *Sejam: K um corpo arbitrário; G um grupo ordenado; e $v : K^* \to G$ uma função.*

Dizemos que v é uma valoração sobre K quando:

1. *$v(a \cdot b) = v(a) + v(b)$, $\forall\, a, b \in K^*$;*
2. *$v(a + b) \geq \min\{v(a), v(b)\}$, para $a, b \in K^*$ tais que $a + b \neq 0$; e*
3. *v é sobrejetora.*

Dizemos também que G é grupo de valoração.
(VILLA-SALVADOR, 2006, p. 17).

Observação 6.3 (definição estendida de valoração). *Seja $v : K^* \to G$ uma valoração.*

Podemos definir $v(0) := \infty$, em que ∞ é um símbolo tal que: $\infty \notin G$;

$$\alpha < \infty\,, \qquad \forall\, \alpha \in G\,;$$

e

$$\infty + \infty := \alpha + \infty := \infty + \alpha := \infty\,, \qquad \forall\, \alpha \in G\,.$$

O propósito de considerar o símbolo ∞ é simplesmente poder definir $v(0)$ de modo que as condições 1 e 2 da Definição 6.2 permaneçam válidas.

(VILLA-SALVADOR, 2006, p. 17).

Definição 6.4 (anel de valoração)**.** *Seja A um domínio de integridade. Dizemos que A é um anel de valoração quando*

1. *A não é um corpo; e*
2. *$x \in A$ ou $x^{-1} \in A$, $\forall\, x \in \mathcal{K}(A)$.*

(VILLA-SALVADOR, 2006, p. 19).

Proposição 6.5. *Sejam K um corpo e $v : K \to \mathbb{R}$ uma valoração sobre K. Então*

1. $\mathcal{O}_v = \left\{ x \in K \,\middle|\, v(x) \geq 0 \right\}$ *é um anel de valoração.*
2. *Em particular, $\mathcal{O}_v$ é um anel local com ideal maximal*

$$\mathfrak{P}_v = \left\{ x \in K \,\middle|\, v(x) > 0 \right\} = \mathcal{O}_v \setminus \mathcal{U}(\mathcal{O}_v)\,, \qquad \mathcal{U}(\mathcal{O}_v) = \left\{ x \in K \,\middle|\, v(x) = 0 \right\}.$$

3. *$\mathcal{K}(\mathcal{O}_v) = K$ e*
4. *o grupo de valoração de v é isomorfo a $\frac{K^*}{\mathcal{U}(\mathcal{O}_v)}$*

(VILLA-SALVADOR, 2006, p. 19).

Proposição 6.6. *Sejam: $\mathcal{O}$ um anel de valoração; e $K = \mathcal{K}(\mathcal{O})$ o corpo de frações de $\mathcal{O}$. Se x, $y \in K^*$, defina*

$$x \mod \mathcal{U}(\mathcal{O}) \leq y \mod \mathcal{U}(\mathcal{O}) \qquad \textit{se} \qquad y \cdot x^{-1} \in \mathcal{O}$$

$$\left(\quad \textit{com} \quad x \mod \mathcal{U}(\mathcal{O}) < y \mod \mathcal{U}(\mathcal{O}) \quad \Leftrightarrow \quad y \cdot x^{-1} \in \mathcal{O} \setminus \mathcal{U}(\mathcal{O}) \quad \right).$$

Então:

1. $\left(\frac{K^*}{\mathcal{U}(\mathcal{O})}, \cdot, < \right)$ *é um grupo ordenado; e*
2. *a projeção natural*

$$\begin{aligned} \pi = v_{\mathcal{O}} : \quad K = \mathcal{K}(\mathcal{O}) &\to \frac{K^*}{\mathcal{U}(\mathcal{O})} \\ x &\mapsto \pi(x) = x \cdot \mathcal{U}(\mathcal{O}) \end{aligned}$$

   é uma valoração;

3. *$\mathcal{O} = \mathcal{O}_\pi$; e*

4. $\frac{K^*}{U(\mathcal{O})}$ *é um grupo de valoração.*

(VILLA-SALVADOR, 2006, p. 19).

Definição 6.7 (valorações equivalentes)**.** *Sejam* $v_1 : K^* \to (G_1, +)$ *e* $v_2 : K^* \to (G_2, +)$ *duas valorações de um corpo K. Dizemos que* v_1 *e* v_2 *são equivalentes quando para todo* $\alpha \in K^*$*:*

$$v_1(\alpha) > 0 \quad \Leftrightarrow \quad v_2(\alpha) > 0 \, .$$

(VILLA-SALVADOR, 2006, p. 20).

Denotaremos $v_1 \sim v_2$ quando v_1 e v_2 forem valorações equivalentes.

Proposição 6.8. *Sejam: K um corpo;* $v_1, v_2 : K \to \mathbb{R}$ *duas valorações sobre K. Então:*

$$v_1 \sim v_2 \quad \Leftrightarrow \quad \mathcal{O}_{v_1} = \mathcal{O}_{v_2} \, .$$

(VILLA-SALVADOR, 2006, p. 21).

Observação 6.9. *Sejam: E um corpo arbitrário; e* ∞ *um símbolo tal que* $\infty \notin E$*. Podemos estender (parcialmente) as operações de corpo de E para* $E \cup \{\infty\}$ *da seguinte maneira:*

$$x + \infty := \infty + x := \infty \, , \qquad \forall \, x \in E \, ;$$

$$x \cdot \infty := \infty \cdot x := \infty \, , \qquad \forall \, x \in E \, ;$$

e

$$\infty \cdot \infty := \infty$$

(note que

$$\infty + \infty \, , \qquad 0 \cdot \infty \qquad e \qquad \infty \cdot 0 \, .$$

não estão definidos).

(VILLA-SALVADOR, 2006, p. 21).

Definição 6.10 (função *place* — cf. Villa-Salvador (2006))**.** *Sejam: E e K dois corpos; e*

$$\varphi : \quad K \quad \to \quad E \cup \{\infty\}$$

uma aplicação. Diremos que φ *é uma função* place *em K quando:*

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$, $\forall \, a, b \in K$;
2. $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, $\forall \, a, b \in K$;

3. $\exists\, a \in K$ *tal que* $\varphi(a) = \infty$; *e*

4. $\exists\, b \in K$ *tal que* $\varphi(b) \neq \infty$ *e* $\varphi(b) \neq 0$.

(VILLA-SALVADOR, 2006, p. 22).

A expressão no axioma 1 faz sentido quando o membro direito da igualdade estiver definido — cf. Deuring (1973, p. 4). Asserção análoga vale para o axioma 2.

Observação 6.11. *O uso do termo* place *não é consistente na literatura:*

- *Stichtenoth (2009, p. 2) denomina como* place *o ideal maximal de um anel de valoração; e*
- *Villa-Salvador (2006, p. 22) e Deuring (1973, p. 4) chamam de* place *a aplicação considerada na Definição 6.10.*

Para evitar colisão de nomenclaturas, preferimos (nesta dissertação) chamar de função place *a aplicação considerada na Definição 6.10, e usar o termo* place *no sentido de Stichtenoth (2009).*

Dada uma função *place* $\varphi : K \to E \cup \{\infty\}$, definimos

$$\mathcal{O}_\varphi := \left\{ a \in K \;\middle|\; \varphi(a) \neq \infty \right\} = \varphi^{-1}\left[E\right].$$

Proposição 6.12. *Seja* $\varphi : K \to E \cup \{\infty\}$ *uma função* place. *Então:*

1. $\mathcal{O}_\varphi$ *é um domínio de integridade contido em* K;

2. $\mathcal{O}_\varphi \neq K$; *e*

3. $\mathcal{O}_\varphi \neq \{0\}$.

(VILLA-SALVADOR, 2006, p. 22).

Vimos na Proposição 6.12 como obter um anel de valoração a partir de uma função *place*. O processo reverso também é possível:

Proposição 6.13. *Sejam:* $\mathcal{O}$ *um anel de valoração;* $\mathfrak{P}$ *o ideal maximal de* $\mathcal{O}$; *e* $K = \mathcal{K}(\mathcal{O})$. *Então*

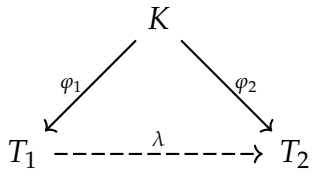
$$\begin{array}{rccl} \varphi_{\mathcal{O}} : & K = \mathcal{K}(\mathcal{O}) & \to & \frac{\mathcal{O}_{\mathfrak{P}}}{\mathfrak{P}} \cup \{\infty\} \\ & x & \mapsto & \varphi_{\mathcal{O}}(x) := \begin{cases} x + \mathfrak{P} & \text{se } x \in \mathcal{O} \\ \infty & \text{se } x \in K \setminus \mathcal{O} \end{cases} \end{array}$$

é uma função place.

(VILLA-SALVADOR, 2006, p. 23).

Definição 6.14 (funções *places* equivalentes)**.** *Diremos que duas funções* places $\varphi_1 : K \to E_1 \cup \{\infty\}$ *e* $\varphi_2 : K \to E_2 \cup \{\infty\}$ *são equivalentes se existir um isomorfismo de corpos* $\lambda : T_1 \to T_2$*, em que* $T_1 = \varphi_1\left[\mathcal{O}_{\varphi_1}\right]$*,* $T_2 = \varphi_2\left[\mathcal{O}_{\varphi_2}\right]$ *e* $\varphi_2 = \lambda \circ \varphi_1$ *— com a convenção* $\lambda(\infty) = \infty$*.*

Figura 67



(VILLA-SALVADOR, 2006, p. 23).

Denotaremos $\varphi_1 \sim \varphi_2$ quando φ_1 e φ_2 forem funções *places* equivalentes.

Proposição 6.15. *Sejam* $\varphi_1 : K \to E_1$ *e* $\varphi_2 : K \to E_2$ *duas funções* places*. Então:*

$$\varphi_1 \sim \varphi_2 \qquad \Leftrightarrow \qquad \mathcal{O}_{\varphi_1} = \mathcal{O}_{\varphi_2} \ .$$

(VILLA-SALVADOR, 2006, p. 23).

Proposição 6.16. *Seja* $v : K \to \mathbb{R}$ *uma valoração. Então a função*

$$\begin{array}{rccl} \|\cdot\|_v : & K & \to & E \cup \{\infty\} \\ & x & \mapsto & \|x\|_v := \begin{cases} e^{-v(x)} & \text{se } x \neq 0 \\ \infty & \text{se } x = 0 \end{cases} \end{array}$$

é um valor absoluto não arquimediano e não trivial sobre K.

(VILLA-SALVADOR, 2006, p. 23).

Proposição 6.17. *Seja* $\|\cdot\| : K \to \mathbb{R}$ *um valor absoluto não arquimediano sobre K. Então a função*

$$\begin{array}{rccl} v_{\|\cdot\|} : & K & \to & \mathbb{R} \cup \{\infty\} \\ & x & \mapsto & v_{\|\cdot\|}(x) := \begin{cases} -\ln|x| & \text{se } x \neq 0 \\ \infty & \text{se } x = 0 \end{cases} \end{array}$$

é uma valoração com grupo de valoração contido em $(\mathbb{R}, +)$*.*

(VILLA-SALVADOR, 2006, p. 24).

Definição 6.18 (valores absolutos equivalentes)**.** *Dois valores absolutos não triviais* $\|\cdot\|_1$ *e* $\|\cdot\|_2$ *sobre um corpo* K *são equivalentes quando para todo* $a \in K$*:*

$$\|a\|_1 < 1 \quad \Rightarrow \quad \|a\|_2 < 1 \, .$$

(VILLA-SALVADOR, 2006, p. 4).

Denotaremos $\|\cdot\|_1 \sim \|\cdot\|_2$ quando $\|\cdot\|_1$ e $\|\cdot\|_2$ forem valores absolutos equivalentes.

Proposição 6.19. *Sejam:* $\|\cdot\|_1, \|\cdot\|_2 : K \to \mathbb{R}$ *dois valores absolutos em um corpo* K*; e* $\|\cdot\|_{v_1}$, $\|\cdot\|_{v_2} : K \to \mathbb{R}$ *duas valorações associadas a* $\|\cdot\|_1$ *e* $\|\cdot\|_2$*, respectivamente. Então*

$$\|\cdot\|_1 \sim \|\cdot\|_2 \quad \Leftrightarrow \quad v_{\|\cdot\|_1} \sim v_{\|\cdot\|_2} \, .$$

(VILLA-SALVADOR, 2006, p. 24).

Observação 6.20. *Nesta dissertação, estaremos particularmente interessados nos seguintes casos.*

1. *O grupo ordenado é* $(\mathbb{Z}, +, <)$.
2. *A definição estendida de valoração é considerada no grupo ordenado* $(\mathbb{Z}, +, <)$.
3. *As valorações consideradas serão sobre corpos de funções.*

6.2 ALGUNS CASOS DO PROBLEMA INVERSO NA TEORIA DE CORPOS DE FUNÇÕES

Mencionamos (sem demonstrações) alguns casos particulares do PITG na teoria de corpos de funções.

6.2.1 O caso nilpotente do PITG para corpos de funções

No artigo de Villa-Salvador e Rzedowski-Calderón (1991), demonstra-se um resultado análogo do Teorema Principal para corpos de funções sobre corpos finitos: o Teorema 5.70, mencionado na Seção 5.3 do Capítulo 5. E, nesse artigo, mostra-se como construir infinitas extensões galoisianas cujo grupo de Galois é isomorfo a um grupo nilpotente finito não trivial dado.

Por comodidade, reproduzimos novamente o Teorema 5.70, abaixo.

Teorema 6.21. *Sejam k um corpo finito com q elementos e G um grupo nilpotente finito de ordem $|G| > 1$ tal que*

$$\mathrm{mdc}\{|G|, q-1\} = 1\,. \tag{134}$$

Então, para todo corpo de funções K sobre k, existem infinitas extensões galoisianas não isomorfas $L \mid K$ tais que

$$\mathrm{Aut}\,(L \mid k) = \mathrm{Gal}\,(L \mid K) \;\cong\; G\,.$$

A condição dada em (134) pode ser removida. Para maiores detalhes, recomendamos as seguintes fontes:

- MADAN, Manohar; RZEDOWSKI-CALDERÓN, Martha; VILLA-SALVADOR, Gabriel Daniel. **Galois Extensions with Bounded Ramification in Characteristic** p: On a Question of S. Abhyankar, Manuscripta Math. **90**, 121–135 (1996). Disponível em: <https://doi.org/10.1007/BF02568297>. Acesso em: 18 set. 2018.

- MALLE, Gunter; MATZAT, Bernd Heinrich. **Inverse Galois Theory**. Berlim: Springer-Verlag, 2018, p. 382.

6.2.2 Caso solúvel

D'Mello e Madan provaram o caso do PITG em que G é um grupo finito solúvel e $K = k(x)$ é um corpo de funções racionais sobre um corpo algebricamente fechado k.

- D'MELLO, Joseph G.; MADAN, Manohar. **Algebraic function fields with solvable automorphism group in characteristic** p, Communications in Algebra **11** (1983), 1187–1236. Disponível em: <https://doi.org/10.1080/00927878308822902>. Acesso em: 03 set. 2018.

6.2.3 O caso do grupo de Mathieu M_{23} para corpos de funções

É conhecido que a classe dos grupos esporádicos são realizáveis como grupos de Galois sobre $\mathbb{Q}$, com a possível exceção do grupo de Mathieu M_{23} (VÖLKLEIN, 1996, p. 54; JENSEN *et al.*, 2002, p. 5).

Na Teoria de Corpos de Funções, entretanto, é sabido que o PITG admite solução positiva no caso de um corpo de funções de característica 2: o grupo de Galois do polinômio

$$f(X) := X^{23} + tX^3 + 1 \in \mathbb{F}_2(t)[X] \tag{135}$$

sobre $\mathbb{F}_2(t)$ é isomorfo a M_{23}.

- ABHYANKAR, Shreeram S.; YIE, Ikkwon. **Some more Mathieu group coverings in characteristic two**, Proceedings of the American Mathematical Society **122** (1994), 1007-1014. Disponível em: <https://doi.org/10.1090/S0002-9939-1994-1239794-1>. Acesso em: 10 dez. 2018.

BIBLIOGRAFIA

[1] ÁLVAREZ-GARCÍA, Caín; VILLA-SALVADOR, Gabriel Daniel. **Groups of automorphisms of global function fields**. Int. J. Algebra, **2** (2008), 65-78. Disponível em: <http://www.m-hikari.com/ija/ija-password-2008/ija-password1-4-2008/villasalvadorIJA1-4-2008.pdf>. Acesso em: 23 out. 2017.

[2] ÁLVAREZ-GARCÍA, Caín; VILLA-SALVADOR, Gabriel Daniel. **Finite groups as Galois groups of function fields with infinite field of constants**. J. Aust. Math. Soc., **88** (2010), 301–312, reproduzido com permissão.

[3] ATIYAH, Michael Francis; MACDONALD, Ian Grant. **Introduction to Commutative Algebra**. Boston: Addison-Wesley, 1969, p. 60.

[4] BASTIDA, Julio Rafael. **Field Extensions and Galois Theory**. Cambridge: Cambridge University Press, 1984, p. 117-118.

[5] DEURING, Max. **Lectures on the theory of algebraic functions of one variable**. Berlin–Heidelberg–New York: Springer-Verlag, 1973, p. 4.

[6] DUMMIT, David S.; FOOTE, Richard. **Abstract Algebra**. Estados Unidos: John Wiley and Sons Inc., 2004.

[7] ENDLER, Otto. **Teoria dos Corpos**. Rio de Janeiro: IMPA, 2012.

[8] FRIED, Michael David; JARDEN, Moshe. **Field Arithmetic**. Berlim: Springer-Verlag, 2008, p. 35.

[9] FRIED, Ervin; KOLLÁR, János. *Authomorphism Groups of Algebraic Number Fields*. Math. Z., 163 (1978), 121–123. Disponível em: <https://eudml.org/doc/172744>. Acesso em: 07 mai. 2018.

[10] JANUSZ, Gerald J.. **Algebraic Number Fields**. Estados Unidos: AMS, 1996, p. 20, 25, 198.

[11] JENSEN, Christian U.; LEDET, Arne; YUI, Noriko. **Generic Polynomials**: Constructive Aspects of the Inverse Galois Problem. Cambridge: Cambridge University Press, 2002, p. 1, 5.

[12] MADAN, Manohar; ROSEN, Michael. **The automorphism group of a function field**, Proc. Am. Math. Soc. **115**, No.4, 923–929 (1992).

[13] MADDEN, Daniel J.; VALENTINI, Robert C.. **The Group of Automorphisms of Algebraic Function Fields**, J. Angew. Math. **343**, 162–168, (1983). Disponível em: <https://doi.org/10.1515/crll.1983.343.162>. Acesso em: 10 dez. 2018.

[14] MARTIN, Paulo Agozzini. **Grupos, corpos e Teoria de Galois**. São Paulo: Livraria da Física, 2010, p. 225, 418.

[15] NEUKIRCH, Jürgen; SCHMIDT, Alexander; WINGBERG, Kay. **Cohomology of Number Fields**, p. 574. Disponível em: <www.mathi.uni-heidelberg.de/~schmidt/NSW2e/>. Acesso em: 05 dez. 2016.

[16] NEUKIRCH, Jürgen. **Algebraic Number Theory**. Berlim: Springer-Verlag, 1999, p. 134.

[17] ROMAN, Steven. **Field Theory**. Nova Iorque: Springer, 2006.

[18] RZEDOWSKI-CALDERÓN, Martha; VILLA-SALVADOR, Gabriel Daniel. **Automorphisms of congruence function fields**. Amer. Math. Monthly, **99** (1991), 932-934.

[19] SERRE, Jean-Pierre. **Topics in Galois Theory**. Estados Unidos: AK Peters, 2007.

[20] STICHTENOTH, Henning. **Algebraic Function Fields and Codes**. Berlim: Springer-Verlag, 2009.

[21] STICHTENOTH, Henning. **Zur Realisierbarkeit endlicher Gruppen als Automorphismengruppen algebraischer Funktionenkörper**, Math. Z. **187** (1984), 221–225.

[22] VILLA-SALVADOR, Gabriel Daniel. **Topics in the Theory of Algebraic Function Fields**. Boston: Birkhäuser, 2006.

[23] VÖLKLEIN, Helmut. **Groups as Galois groups**. Cambridge: Cambridge University Press, 1996, p. 18, 53-54.

ÍNDICE