Universidade Federal de São Carlos
Centro de Ciências Exatas e de Tecnologia
Departamento de Matemática

Um estudo de valorizações transcendentes e algébricas via polinômios-chaves e pares minimais

Aluno: *Caio Henrique Silva de Souza*

Orientador: *Prof. Dr. Josnei Antonio Novacoski*

São Carlos, 24 de fevereiro de 2022.

Um estudo de valorizações transcendentes e algébricas via polinômios-chaves e pares minimais

Aluno: *Caio Henrique Silva de Souza*

Orientador: *Josnei Antonio Novacoski*

Curso: Mestrado em Matemática

Instituição: Universidade Federal de São Carlos
Centro de Ciências Exatas e de Tecnologia
Departamento de Matemática

Financiamentos: Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq)
Processo nº 132761/2020-3

Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP)
Processo nº 2020/05148-0

São Carlos, 24 de fevereiro de 2022.

Caio Henrique Silva de Souza

Josnei Antonio Novacoski

UNIVERSIDADE FEDERAL DE SÃO CARLOS

Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Matemática

Folha de Aprovação

Defesa de Dissertação de Mestrado do candidato Caio Henrique Silva de Souza, realizada em 24/02/2022.

Comissão Julgadora:

Prof. Dr. Josnei Antonio Novacoski (UFSCar)

Prof. Dr. Humberto Luiz Talpo (UFSCar)

Prof. Dr. Daniel Levcovitz (ICMC/USP)

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

O Relatório de Defesa assinado pelos membros da Comissão Julgadora encontra-se arquivado junto ao Programa de Pós-Graduação em Matemática.

Agradecimentos

Primeiramente aos meus pais Albeti e Angelo, pelo amor, dedicação, paciência e apoio que sempre me deram. Aos professores que me acompanharam por toda a minha vida escolar e universitária. Em especial, ao professor Josnei Antonio Novacoski, por me orientar neste trabalho. À FAPESP e ao CNPq, pela concessão da bolsa de mestrado que amparou a execução deste projeto. À minha irmã, Bruna, e aos meus amigos, pelas risadas e os bons momentos. Em especial, ao meu amigo Gabriel Longatto Clemente, fiel companheiro na universidade.

O que vejo, o que penso - disputam entre si o que sou.
Paul Valéry

Resumo

O objetivo geral deste trabalho será estudar as valorizações transcendentes e as valorizações algébricas. Para tal, utilizaremos alguns objetos de destaque na Teoria das Valorizações como, por exemplo, os polinômios-chaves, os truncamentos e os pares minimais. Esses objetos nos levarão aos resultados que irão compor a parte principal do texto e que serão vistos como os objetivos específicos deste trabalho. Iniciaremos estudando as valorizações de modo geral e, em seguida, focaremos nas chamadas valorizações monomiais. Exploraremos o conceito de polinômio-chave e truncamento, provando diversos resultados técnicos. Apresentaremos a ideia de par minimal de definição, relacionando-a aos polinômios-chaves e aos truncamentos. Logo em seguida, nos aprofundaremos no estudo das valorizações transcendentes e complementaremos resultados de Novacoski (2019). Veremos também parte do trabalho recente de Bengus-Lasnier (2021) sobre bolas e discoides. No último capítulo, estudaremos as valorizações algébricas. Terminaremos o trabalho apresentando a classificação proposta por Alexandru, Popescu e Zaharescu (1988, 1990a, 1990b) para todas as valorizações em $\mathbb{K}(x)$, o corpo de funções racionais sobre um corpo $\mathbb{K}$, fazendo um apanhado geral do que foi desenvolvido no texto principal.

Palavras-chaves: Valorização; Polinômios-chaves; Par minimal; Extensões de valorizações.

Abstract

The main goal of this work is to study transcendental valuations and algebraic valuations. To achieve this, we use some of the main objects in Valuation Theory, such as key polynomials, truncations and minimal pairs. These objects will lead us to the results which will build the central part of this text and will be seen as the specific goals of this work. We will begin studying valuations in a general way and then we focus on monomial valuations. We will explore the concept of key polynomials and truncations, proving many technical results. Then, we will present the idea of minimal pair of definition, relating it to key polynomials and truncations. After that, we will study transcendental valuations and complement results of Novacoski (2019). We will also study part of Bengus-Lasnier (2021) recent work on balls and diskoids. In the last chapter, we will study algebraic valuations. We will finish our work presenting a classification proposed by Alexandru, Popescu and Zaharescu (1988, 1990a, 1990b) for all valuations on $\mathbb{K}(x)$, the field of rational functions over a field $\mathbb{K}$, and with this classification we will make a general overview of the results we presented before.

Keywords: Valuation; Key polynomials; Minimal pair; Extensions of valuations.

Sumário

Introdução

Este trabalho se insere dentro da área da Matemática chamada Teoria das Valorizações. Tal teoria surge motivada pelos estudos de Hensel (1861 - 1941) sobre números p-ádicos e começa a ser formalmente desenvolvida no início do século XX, por matemáticos como Kürschák (1864 - 1933), Ostrowski (1893 - 1986) e Krull (1899 - 1971). Este último encaminha a teoria para a forma que utilizaremos neste texto. A Teoria das Valorizações foi popularizada, dentre outros motivos, devido às suas potencialidades dentro da Geometria Algébrica. Por exemplo, dois importantes problemas em aberto neste campo, o problema de resolução de singularidades e o problema da uniformização local, ambos em característica positiva, possuem programas para solução que envolvem os conhecimentos sobre valorizações (NOVACOSKI; SPIVAKOVSKY, 2016). Porém, para além de suas aplicações nesse e em outros campos da Matemática, as valorizações e os objetos ao redor destas são em si matérias interessantes para serem exploradas e melhor entendidas.

Neste trabalho, nosso objetivo geral será estudar as valorizações transcendentes e as valorizações algébricas. Estudaremos alguns objetos de destaque na Teoria das Valorizações, como por exemplo os polinômios-chaves, os truncamentos e os pares minimais. A seguir, daremos uma visão geral do trabalho e de nossos objetivos.

Na maior parte deste trabalho, estaremos interessados em estudar valorizações definidas em $\mathbb{K}[x]$, o anel dos polinômios em uma indeterminada sobre o corpo $\mathbb{K}$, ou em $\mathbb{K}(x)$, o corpo de funções racionais sobre $\mathbb{K}$. Um plano de fundo para nosso trabalho será classificar todas as valorizações em $\mathbb{K}(x)$. Dentre as possibilidades de classificação e de abordagem que a literatura nos fornece, escolheremos a série de trabalhos publicados entre 1988 e 1990 pelos matemáticos Alexandru, Popescu e Zaharescu (1988, 1990a, 1990b). A classificação se dará, principalmente, em termos de um tipo de valorização, as chamadas valorizações transcendentes.

Nos aprofundaremos no estudo das valorizações transcendentes. Para isso, lançaremos mão de conceitos como polinômios-chaves, truncamentos, pares minimais, bolas e discoides. Em torno desses conceitos surgirão os objetivos específicos deste trabalho. Tais objetivos específicos abarcam os resultados que são a parte de maior interesse deste texto. Descreveremos a seguir tais resultados.

Seja μ uma valorização em $\mathbb{K}[x]$. O truncamento de μ em um polinômio qualquer q é a aplicação que associa um polinômio f a

$$\mu_q(f) = \min_{0\leq i\leq r}\{\mu(f_i q^i)\},$$

em que $f_0, \ldots, f_r$ são os coeficientes da chamada q-expansão de f. Tal aplicação pode ou não ser uma valorização em $\mathbb{K}[x]$ (NOVACOSKI, 2018). Além disso, μ pode ou não ser definida por um truncamento, isto é, podemos ou não ter $\mu = \mu_q$ para algum polinômio q.

O *primeiro resultado principal* deste trabalho (Teorema 3.22, Teorema 3.26 e Corolário 3.27) nos diz que

μ é transcendente se, e somente se, $\mu = \mu_Q$ para algum polinômio-chave Q.

Esse resultado está conectado ao trabalho de Novacoski (2019, p. 4), onde é provado que μ é transcendente se, e somente se, $\mu = \mu_q$ para algum polinômio q (Teorema 3.24). Dessa forma, o Corolário 3.27 complementa este resultado.

Como veremos, as valorizações transcendentes se dividem em dois tipos: resíduo-transcendente e valor-transcendente. Caracterizaremos estes dois tipos em termos de pares minimais e polinômios-chaves. Consideremos uma extensão $\overline{\mu}$ de μ para $\overline{\mathbb{K}}[x]$, em que $\overline{\mathbb{K}}$ é um fecho algébrico fixado de $\mathbb{K}$. Veremos que se μ é transcendente, então $\overline{\mu}$ é igual a uma valorização monomial $\overline{\mu}_{a,\delta}$, esta dada pelo que chamaremos um par minimal de definição $(a,\delta) \in \overline{\mathbb{K}} \times \overline{\mu}(\overline{\mathbb{K}}[x])$ (Teorema 3.22 e Teorema 3.26). Se $\delta \in \overline{\mu}\overline{\mathbb{K}}$, então $\overline{\mu}_{a,\delta}$ será resíduo-transcendente. Se $\delta \in \overline{\mu}(\overline{\mathbb{K}}[x]) \setminus \overline{\mu}\overline{\mathbb{K}}$, então $\overline{\mu}_{a,\delta}$ será valor-transcendente.

Ainda no trabalho de Novacoski (2019, p. 3), é apresentada uma relação entre o conceito de par minimal e os polinômios-chaves (Teorema 3.11), que aqui complementaremos com o Teorema 3.12. Incrementaremos essa relação estudando também um resultado de Bengus-Lasnier (2021), originalmente provado por Popescu e Popescu (1989). Sejam Q um polinômio-chave para μ, $a \in \overline{\mathbb{K}}$ uma raiz otimizadora de Q e $\overline{\mu}_{x-a}$ o truncamento de $\overline{\mu}$ em $x-a$. O *segundo resultado principal* deste trabalho (Teorema 3.32 e Teorema 3.45) nos diz que

$$\overline{\mu}_{x-a}|_{\mathbb{K}[x]} = \mu_Q.$$

Apresentaremos duas provas para esse resultado. A primeira demonstração é baseada na prova de Popescu e Popescu (1989) e reescreveremos os resultados do original de acordo com a teoria que desenvolveremos aqui. A segunda demonstração é baseada no trabalho de Bengus-Lasnier (2021, p. 408) e utilizará a estrutura de anel graduado, outro importante recurso para o estudo das valorizações.

O aluno responsável por esta dissertação e seu orientador escreveram um artigo contendo o primeiro e o segundo resultados principais deste trabalho (NOVACOSKI; SILVA DE SOUZA,

2022). O artigo foi aceito para publicação e já está disponível on-line.

As valorizações resíduo-transcendentes terão um papel de destaque na classificação de todas as valorizações em $\mathbb{K}(x)$. Por isso, buscaremos outras formas de caracterizarmos valorizações desse tipo. Iniciaremos essa busca com as seguintes questões. Seja μ uma valorização em $\mathbb{K}[x]$. Existe algum conjunto $D \subset \overline{\mathbb{K}}$ tal que

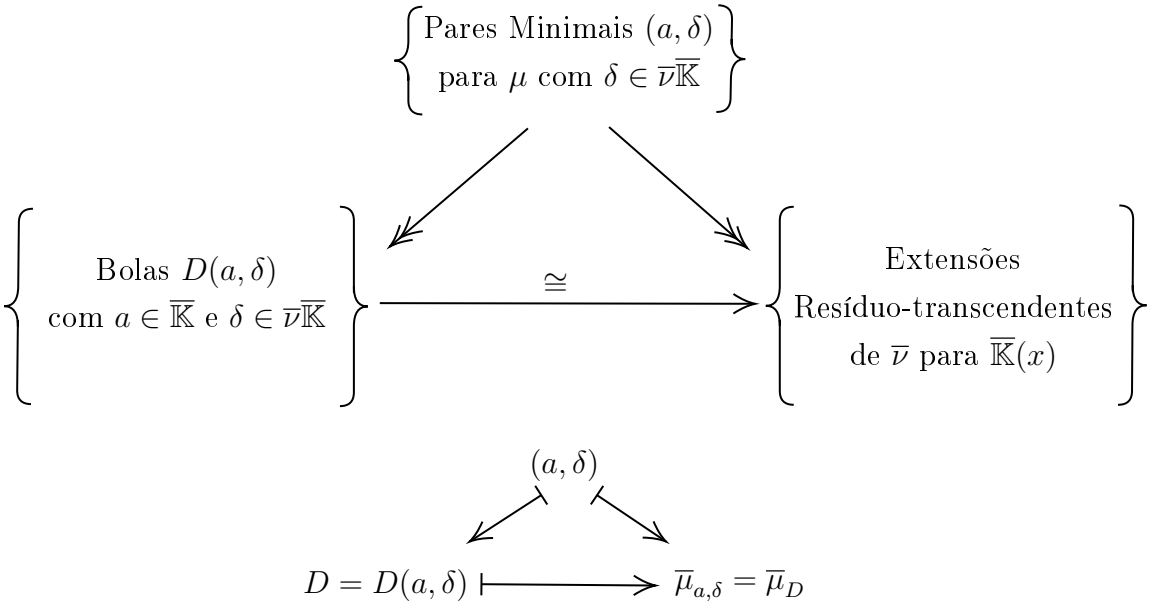
$$\mu(f) = \min_{d \in D}\{\mu(f(d))\}$$

para todo $f \in \mathbb{K}[x]$? Esse conjunto pode ser unicamente determinado, isto é, conjuntos distintos definem valorizações distintas? Inicialmente, trabalharemos com valorizações $\overline{\nu}$ em um corpo algebricamente fechado $\overline{\mathbb{K}}$. O *terceiro resultado principal* deste trabalho (Teorema 4.4) nos diz que

$$\overline{\mu}_{a,\delta}(f) = \overline{\mu}_D(f) := \min_{d \in D}\{\overline{\nu}(f(d))\},$$

em que $D = D(a,\delta) := \{d \in \overline{\mathbb{K}} \mid \overline{\nu}(d-a) \geq \delta\}$ é o subconjunto de $\overline{\mathbb{K}}$ chamado de bola fechada.

Ademais, sejam μ uma valorização em $\mathbb{K}[x]$, $\overline{\mu}$ uma valorização em $\overline{\mathbb{K}}[x]$ estendendo μ e consideremos as restrições $\nu = \mu|_{\mathbb{K}}$ e $\overline{\nu} = \overline{\mu}|_{\overline{\mathbb{K}}}$. Veremos que vale a seguinte relação entre os pares minimais, as bolas e as extensões resíduo-transcendentes de $\overline{\nu}$ para $\overline{\mathbb{K}}(x)$ (Teorema 4.5). A bijeção no diagrama abaixo nos permitirá concluir que bolas distintas definem valorizações distintas e, com isso, teremos a unicidade procurada.

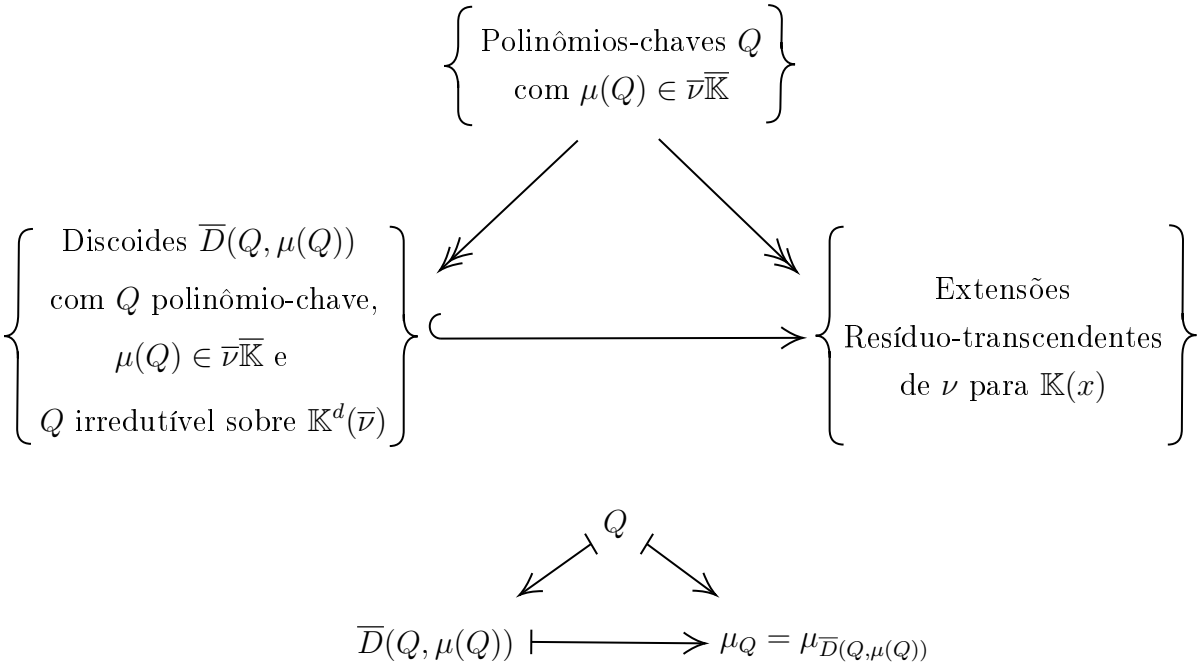


Olharemos então para uma valorização μ_Q em $\mathbb{K}[x]$, dada pelo truncamento em um polinômio-chave Q com $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$. Como $\overline{\mu}_{x-a}|_{\mathbb{K}[x]} = \overline{\mu}_{a,\delta}|_{\mathbb{K}[x]} = \mu_Q$ (Teorema 3.32 e Teorema 3.45), isso implica que também vale que μ_Q fica definida como mínimo sobre uma bola $D(a,\delta)$. Porém, nesse caso, não teremos essa bola unicamente determinada (Exemplo 4.7). Por isso, buscaremos outro subconjunto de $\overline{\mathbb{K}}$, a fim de conseguirmos tal unicidade. Veremos que os chamados discoides em $\overline{\mathbb{K}}$ serão bons candidatos para suprir essa unicidade. Antes de

Bengus-Lasnier, esses conjuntos foram estudados por Rüth (2014) em sua tese de doutorado. O *quarto resultado principal* deste trabalho (Teorema 4.18) nos diz que

$$\mu_Q(f) = \mu_{\overline{D}(Q,\mu(Q))}(f) := \min_{d\in\overline{D}(Q,\mu(Q))}\{\overline{\nu}(f(d))\},$$

em que $\overline{D}(Q,\mu(Q)) := \{d \in \overline{\mathbb{K}} \mid \overline{\nu}(Q(d)) \geq \mu(Q)\}$, $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ e Q é irredutível sobre a henselização $\mathbb{K}^d(\overline{\nu})$. Poderemos provar uma relação semelhante àquela dada pelo Teorema 4.5, desta vez entre polinômios-chaves, discoides e extensões resíduo-transcendentes de ν para $\mathbb{K}(x)$ (Teorema 4.19). A aplicação injetora no diagrama abaixo nos permitirá concluir que discoides distintos definem valorizações distintas e, com isso, teremos a unicidade procurada.



No trabalho de Bengus-Lasnier, são levantadas as seguintes conjecturas: μ_Q pode ser definido como mínimo sobre um discoide para qualquer polinômio-chave Q com $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ e a função acima, que leva um discoide em uma extensão resíduo-transcendente de ν, é na verdade uma bijeção. Estas afirmações podem ser deduzidas da seguinte conjectura: todo polinômio-chave em $\mathbb{K}[x]$ com $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ é irredutível sobre a henselização $\overline{\mathbb{K}}^d(\overline{\nu})$ (Conjectura 4.20). Discutiremos esta conjectura logo após a relação exposta acima.

Por fim, como aplicação de todo o estudo descrito acima, teremos uma classificação para todas as valorizações em $\mathbb{K}(x)$.

Faremos agora uma descrição dos cinco capítulos que formam o texto principal deste trabalho e dos apêndices.

No Capítulo 1, estudaremos de modo geral as valorizações. Na primeira seção, provaremos propriedades iniciais e apresentaremos exemplos. Na segunda seção, veremos os anéis de valorização. Introduziremos na terceira seção o conceito de equivalência entre valorizações e com

ele trataremos das valorizações no corpo dos números racionais $\mathbb{Q}$ e das valorização em $\mathbb{K}(x)$ que são triviais em $\mathbb{K}$. Por fim, na quarta seção, estudaremos as valorizações monomiais, que formam uma família de extensões de uma dada valorização de $\mathbb{K}$ para $\mathbb{K}[x]$.

Os leitores mais experientes podem começar a leitura deste trabalho a partir da Seção 1.4 do Capítulo 1.

No Capítulo 2, apresentaremos os polinômios-chaves. Na primeira seção, apresentaremos a definição desses e suas primeiras propriedades. Em seguida, na segunda seção, trataremos das valorizações definidas por truncamentos em polinômios-chaves. Por fim, na terceira seção, provaremos mais propriedade técnicas desses polinômios que serão úteis no capítulo seguinte.

No Capítulo 3, introduziremos os conceito de par de definição e de par minimal. Nas primeiras seções, definiremos o que é um par de definição e um par minimal e conectaremos estes conceitos com o que estudamos no capítulo anterior sobre polinômios-chaves e truncamentos (Teoremas 3.11 e 3.12). Em seguida, definiremos as valorizações do tipo valor-transcendente e as valorizações do tipo resíduo-transcendente. Dedicaremos uma subseção para cada um desses tipos de valorizações, caracterizando-as em termos de pares minimais e truncamentos em polinômios-chaves (Teoremas 3.20, 3.22, 3.24 e 3.26). Por fim, sendo Q um polinômio-chave para μ e $a \in \overline{\mathbb{K}}$ uma raiz otimizadora de Q, veremos que $\overline{\mu}_{x-a}$ é uma extensão de μ_Q para $\overline{\mathbb{K}}[x]$ (Teoremas 3.22 e 3.26).

No Capítulo 4, estudaremos as bolas e os discoides. Veremos na primeira seção que as valorizações monomiais $\overline{\mu}_{a,\delta}$ em $\overline{\mathbb{K}}[x]$, com $\delta \in \overline{\nu}\overline{\mathbb{K}}$, podem ser descritas a partir de um mínimo sobre uma bola definida por a e δ (Teorema 4.4). Veremos também a referida relação entre os pares minimais, as bolas e as extensões resíduo-transcendentes de $\overline{\nu}$ para $\overline{\mathbb{K}}(x)$ (Teorema 4.5). Em seguida, na segunda seção, estudaremos os discoides e veremos como esses objetos se relacionam com as bolas. Na terceira seção, utilizaremos o grupo de decomposição para descrever um truncamento μ_Q em termos de discoides (Teorema 4.18). Provaremos uma relação entre polinômios-chaves, discoides e extensões resíduo-transcendentes de ν para $\mathbb{K}(x)$ (Teorema 4.19).

No Capítulo 5, como consequência dos resultados principais deste texto, faremos a classificação de todas as valorizações em $\mathbb{K}(x)$. Na primeira seção, estudaremos mais a fundo as valorizações algébricas. Veremos como representar uma valorização desse tipo como um limite de um sistema ordenado de valorizações resíduo-transcendentes (Teorema 5.9). Na segunda seção, descreveremos as valorizações em $\mathbb{K}(x)$, fazendo um apanhado geral dos resultados provados durante os capítulos anteriores e citando outros resultados da literatura que não entraram neste trabalho.

Nosso trabalho também possui sete apêndices que complementam as discussões levantadas no corpo principal do texto. No Apêndice A, faremos um apanhado geral de Teoria de Anéis e Módulos e de Teoria de Galois. No Apêndice B, estudaremos os grupos totalmente ordenados, dando foco, na segunda seção, ao fecho divisível de um grupo abeliano. No Apêndice C,

apresentaremos as provas de alguns resultados iniciais sobre valorizações e anéis de valorização e os detalhes dos exemplos do Capítulo 1. No Apêndice D, trataremos das extensões e prolongamentos de uma valorização e mostraremos resultados clássicos, como o Teorema de Chevalley, a Desigualdade de Zariski-Abhyankar e o Teorema da Conjugação. No Apêndice E, estudaremos os pares henselianos, chegando ao conceito de henselização. Utilizaremos o grupo de decomposição para descrever as valorizações em $\overline{\mathbb{K}}[x]$ que são, ao mesmo tempo, extensão de μ em $\mathbb{K}[x]$ e $\overline{\nu}$ em $\overline{\mathbb{K}}$. Os resultados do Capítulo 4 estarão fortemente ligados aos resultados do Apêndice E. No Apêndice F, provaremos as propriedades da derivada de Hasse, ferramenta utilizada principalmente no Capítulo 2. No Apêndice G, estudaremos os polígonos de Newton e provaremos a igualdade entre $\epsilon(f)$ e $\delta(f)$ que utilizaremos no Capítulo 2. Faremos isso a partir de uma abordagem geométrica para o estudo das valorizações.

Notações e convenções: Em todo o texto, $\mathbb{N}$ é o conjunto dos números inteiros positivos, $\mathbb{Z}$ é o conjunto dos números inteiros, $\mathbb{Q}$ é o conjunto dos números racionais , $\mathbb{R}$ é o conjunto dos números reais e $\mathbb{C}$ é o conjunto dos números complexos. Denotaremos por $\mathbb{N}_0$ o conjunto $\mathbb{N} \cup \{0\}$. As letras $\mathbb{K}$, $\mathbb{L}$, $\mathbb{F}$ e $\mathbb{E}$ representam corpos. As letras $\mathcal{A}$, $\mathcal{B}$, $\mathcal{R}$, $\mathcal{O}$, $\mathcal{D}$ e $\mathcal{S}$ representam anéis comutativos com unidade 1, a menos que explicitado o contrário. Representamos por $\mathcal{A}^\times$ o conjunto das unidades de $\mathcal{A}$. As letras $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{i}$, $\mathfrak{m}$ e $\mathfrak{p}$ representam ideais. Representaremos por $\mathbb{K}[x]$ o anel de polinômios sobre $\mathbb{K}$ na indeterminada x e por $\mathbb{K}(x)$ o corpo das funções racionais. Para um polinômio $f \in \mathbb{K}[x]$, denotamos seu grau por $\deg(f)$. Convencionamos $\deg(0) = -\infty$. A notação $M \otimes N$ representa o produto tensorial de dois $\mathbb{Z}$-módulos M e N sobre $\mathbb{Z}$.

Capítulo 1

Valorizações

Neste primeiro capítulo definiremos o objeto central de estudo deste trabalho: as valorizações.

Na primeira seção, definiremos as aplicações chamadas valorizações, provaremos propriedades iniciais e apresentaremos exemplos. Na segunda seção, nos concentraremos nos anéis de valorização, mostrando a relação entre esse tipo de anel e as aplicações valorizações. Introduziremos na terceira seção o conceito de equivalência entre valorizações e com ele trataremos das valorizações no corpo dos números racionais $\mathbb{Q}$ e das valorização em corpos do tipo $\mathbb{K}(x)$ que são triviais em $\mathbb{K}$. Por fim, na quarta seção apresentaremos uma família de extensões de uma dada valorização de $\mathbb{K}$ para $\mathbb{K}[x]$, as chamadas valorizações monomiais. Os leitores mais experientes podem começar a leitura deste trabalho a partir da quarta seção.

As principais referências para a composição deste capítulo foram os trabalhos de Engler e Prestel (2005), Kuhlmann (20??a) e Novacoski (2021).

1.1 Valorizações

Seja Γ um grupo abeliano totalmente ordenado (a definição e propriedades deste objeto se encontram no Apêndice B). Estendemos esse grupo para a estrutura $\Gamma_\infty := \Gamma \cup \{\infty\}$, em que ∞ é um símbolo satisfazendo $\infty + g = g + \infty = \infty + \infty = \infty$ e $\infty > g$ para todo $g \in \Gamma$. Seja $\mathcal{R}$ um anel comutativo com unidade.

Definição 1.1. Uma **valorização** em $\mathcal{R}$ é uma aplicação $\nu : \mathcal{R} \longrightarrow \Gamma_\infty$ satisfazendo, para todo $a, b \in \mathcal{R}$, os seguintes axiomas:

$(V1)$ $\nu(ab) = \nu(a) + \nu(b)$,

$(V2)$ $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$ *e*

$(V3)$ $\nu(1) = 0$ e $\nu(0) = \infty$. ■

O subgrupo de Γ gerado por $\{\nu(a) \mid a \in \mathcal{R} \text{ e } \nu(a) \neq \infty\} \subseteq \Gamma$ é chamado ***grupo de valores*** de ν. Denotaremos este por $\nu\mathcal{R}$ ou por Γ_ν. Temos que ν é chamada trivial se $\nu\mathcal{R} = \{0\}$.

A seguir apresentaremos algumas propriedades elementares de uma valorização. Seja ν uma valorização em $\mathcal{R}$. Para todo $a, b \in \mathcal{R}$ temos as seguintes propriedades. As demonstrações dessas propriedades estão feitas no Apêndice C.

- Se a é unidade, então $\nu(a^{-1}) = -\nu(a)$. Temos também $\nu(-1) = 0$.
- Para todo a, temos $\nu(-a) = \nu(a)$.
- Se $a^m = 1$, então $\nu(a) = 0$.
- Se $\nu(a) \neq \nu(b)$, então $\nu(a+b) = \min\{\nu(a), \nu(b)\}$.
- Suponhamos $b_1, b_2, \ldots, b_n \in \mathcal{R}$. Para todo $n \geq 2$, vale

$$\nu(b_1 + b_2 + \ldots + b_n) \geq \min\{\nu(b_1), \nu(b_2), \ldots, \nu(b_n)\}.$$

- Suponhamos $a, b_1, b_2, \ldots, b_n \in \mathcal{R}$ com $\nu(a) < \nu(b_i)$ para todo i, $1 \leq i \leq n$. Então,

$$\nu(a + b_1 + b_2 + \ldots + b_n) = \nu(a).$$

Definição 1.2. *Seja $\nu : \mathcal{R} \longrightarrow \Gamma_\infty$ uma valorização. Chamamos de* ***suporte*** *de ν o conjunto* $\text{supp}(\nu) := \{a \in \mathcal{R} \mid \nu(a) = \infty\}$.

■

O lema a seguir está demonstrado no Apêndice C (Lema C.1).

Lema 1.3. *Suponhamos que $\nu : \mathcal{R} \longrightarrow \Gamma_\infty$ seja uma aplicação que satisfaz os Axiomas $(V1)$ e $(V2)$. As afirmações a seguir são equivalentes.*

1. *A aplicação ν satisfaz $(V3)$.*
2. *A aplicação ν não é constante.*
3. *O conjunto* $\text{supp}(\nu)$ *é um ideal primo de $\mathcal{R}$.*

■

Como $\text{supp}(\nu)$ é um ideal primo, o quociente $\mathcal{R}/\text{supp}(\nu)$ é um domínio de integridade. Definindo $\nu' : \mathcal{R}/\text{supp}(\nu) \longrightarrow \Gamma_\infty$ por $\nu'(a + \text{supp}(\nu)) := \nu(a)$, temos uma valorização neste domínio de integridade que possui $\text{supp}(\nu') = \{0\}$ (Exemplo C.2).

Definição 1.4. *Dizemos que uma valorização $\nu : \mathcal{R} \longrightarrow \Gamma_\infty$ é uma* ***valorização de Krull*** *se* $\mathrm{supp}(\nu) = \{0\}$.

■

Exemplo 1.5. *A valorização ν' definida anteriormente em $\mathcal{R}/\mathrm{supp}(\nu)$ é uma valorização de Krull.*

▼

Exemplo 1.6. *Se $\mathbb{K}$ é um corpo, então toda valorização ν em $\mathbb{K}$ é de Krull. De fato, os únicos ideais de um corpo são $\{0\}$ e $\mathbb{K}$. Como $\mathrm{supp}(\nu)$ é um ideal próprio, segue que $\mathrm{supp}(\nu) = \{0\}$.*

▼

Exemplo 1.7. *Um anel $\mathcal{R}$ que admite uma valorização de Krull ν deve ser um domínio. De fato, como $\mathrm{supp}(\nu) = \{0\}$ é um ideal primo, segue que $\mathcal{R} \cong \mathcal{R}/\{0\}$ é um domínio. Com isso, conseguimos estender a valorização de Krull ν para uma aplicação no corpo de frações $\mathbb{K} = \mathrm{Frac}(\mathcal{R})$, que também denotaremos por ν, definida por*

$$\nu\left(\frac{a}{b}\right) := \nu(a) - \nu(b).$$

No Apêndice C (Exemplo C.5), mostramos que ν em $\mathbb{K}$ está bem definida, satisfaz as propriedades de valorização e é a única que estende ν para $\mathbb{K}$, isto é, a única valorização em $\mathbb{K}$ tal que $\nu|_{\mathcal{R}} = \nu$.

▼

A seguir apresentaremos exemplos mais concretos de valorizações. As verificações estão todas feitas no Apêndice C.

Exemplo 1.8. *Sejam $\mathcal{D}$ um domínio de ideais principais (e.g. $\mathbb{Z}$ ou $\mathbb{F}[x]$, com $\mathbb{F}$ um corpo) e $\mathbb{K}$ seu corpo de frações (e.g. $\mathbb{Q}$ ou $\mathbb{F}(x)$). Para cada elemento irredutível $p \in \mathcal{D}$, a aplicação $\nu^p : \mathcal{D} \longrightarrow \mathbb{Z}_\infty$ dada por*

$$\nu^p(a) = \begin{cases} m & \text{se } a = p^m a' \text{ com } p \nmid a', \\ \infty & \text{se } a = 0 \end{cases}$$

é uma valorização em $\mathcal{D}$ (Exemplo C.6). Por definição, vemos que $\mathrm{supp}(\nu^p) = \{0\}$. Logo, ν^p é uma valorização de Krull e fica bem definida em $\mathbb{K}$. Chamamos a valorização ν^p em $\mathbb{K}$ de ***valorização p-ádica****.*

▼

Exemplo 1.9. *A aplicação*

$$\nu_\infty\left(\frac{f(x)}{g(x)}\right) = \begin{cases} \deg(g(x)) - \deg(f(x)) & \text{se } f(x) \text{ e } g(x) \text{ são não nulos,} \\ \infty & \text{se } f(x) \text{ é o polinômio identicamente nulo } 0 \end{cases}$$

definida em $\mathbb{F}(x)$ *é uma valorização em* $\mathbb{F}(x)$ *com grupo de valores* $\mathbb{Z}$ *(Exemplo C.8). Chamamos tal aplicação de* ***valorização grau*** *em* $\mathbb{F}(x)$.

▼

Exemplo 1.10. *Sejam* Γ *um grupo abeliano totalmente ordenado e* $\mathbb{K}$ *um corpo. Consideramos o conjunto*

$$\mathbb{K}((t^\Gamma)) := \{a : \Gamma \longrightarrow \mathbb{K} \mid \Gamma \setminus Z(a) \text{ é bem ordenado}\},$$

em que $Z(a) = \{\gamma \in \Gamma \mid a(\gamma) = 0\}$. *Munido das operações descritas no Apêndice C (Exemplo C.10),* $\mathbb{K}((t^\Gamma))$ *é um corpo, chamado* ***corpo das séries de potências formais*** *em* Γ. *A aplicação*

$$\nu_t(a) := \begin{cases} \min\{\Gamma \setminus Z(a)\} & \text{se } a \neq 0, \\ \infty & \text{se } a = 0 \end{cases}$$

é uma valorização, chamada ***valorização t-ádica****. O grupo de valores de* ν_t *é* Γ. *Em particular, quando* $\Gamma = \mathbb{Z}$, *temos que* ν_t *é uma valorização no corpo* $\mathbb{K}((t))$ *das séries de Laurent.*

▼

Exemplo 1.11. *Sejam* $\mathcal{R}$ *e* $\mathcal{D}$ *anéis e um homomorfismo* $\psi : \mathcal{R} \longrightarrow \mathcal{D}$. *Consideremos* ν' *uma valorização em* $\mathcal{D}$. *Então, a aplicação* $\nu(a) := \nu'(\psi(a))$ *é uma valorização em* $\mathcal{R}$. *Além disso, se* ν' *é de Krull, então* $\operatorname{supp}(\nu) = \ker(\psi)$ *(Exemplo C.12).*

▼

Exemplo 1.12. *Seja* $\mathbb{F}$ *um corpo finito. Qualquer valorização em* $\mathbb{F}$ *é trivial. Mais geralmente, seja* $\mathbb{E}$ *uma extensão algébrica de um corpo finito* $\mathbb{F}$. *Então, toda valorização em* $\mathbb{E}$ *é trivial (Exemplo C.14). Dessa forma, corpos dessa natureza não serão interessantes para a teoria que desenvolveremos.*

▼

1.2 Anéis de valorização

Seja ν uma valorização de Krull em um anel $\mathcal{R}$ e denotemos também por ν a valorização induzida em $\mathbb{K} = \operatorname{Frac}(\mathcal{R})$. O conjunto $\mathcal{O}_\nu := \{a \in \mathbb{K} \mid \nu(a) \geq 0\}$ é um anel e satisfaz a seguinte propriedade: para todo $a \in \mathbb{K}^\times$, devemos ter $a \in \mathcal{O}_\nu$ ou $a^{-1} \in \mathcal{O}_\nu$. De fato, suponhamos que

$a \in \mathbb{K}$ e $a \notin \mathcal{O}_\nu$. Dessa forma, $\nu(a) < 0$. Como $\nu(a^{-1}) = -\nu(a)$, segue que $\nu(a^{-1}) > 0$, logo $a^{-1} \in \mathcal{O}_\nu$.

Definição 1.13. *Um subanel $\mathcal{O}$ de um corpo $\mathbb{K}$ qualquer é chamado* ***anel de valorização*** *de $\mathbb{K}$ se, para todo $a \in \mathbb{K}^\times$, vale $a \in \mathcal{O}$ ou $a^{-1} \in \mathcal{O}$.*

■

Exemplo 1.14. *O anel $\mathcal{O}_\nu$ associado a uma valorização ν, como definido anteriormente, é um anel de valorização.*

▼

Duas propriedades dos anéis de valorização estão enunciadas na proposição abaixo e estão provadas no Apêndice C (Proposição C.4).

Proposição 1.15. *Seja $\mathcal{O} \subset \mathbb{K}$ anel de valorização. Então,* $\mathrm{Frac}(\mathcal{O}) = \mathbb{K}$. *Além disso, $\mathcal{O}$ é local.*

■

Para $\mathcal{O}_\nu$ definido a partir de uma valorização ν em um corpo $\mathbb{K}$, vejamos que o conjunto $\mathfrak{m}_\nu = \{a \in \mathbb{K} \mid \nu(a) > 0\}$ é o ideal maximal de $\mathcal{O}_\nu$. De fato, $\mathfrak{m}$ é ideal pois se $a, b \in \mathfrak{m}$, então temos

$$\nu(a+b) \geq \min\{\nu(a), \nu(b)\} > 0,$$

$$\nu(ab) = \nu(a) + \nu(b) > 0$$

e, se $c \in \mathcal{O}_\nu$, então

$$\nu(ca) = \nu(c) + \nu(a) > 0.$$

Consideremos agora o quociente $\mathcal{O}_\nu/\mathfrak{m}_\nu$. Observemos que se $a \in \mathcal{O}_\nu$ e $\nu(a) = 0$, então $\nu(a^{-1}) = -\nu(a) = 0$. Ou seja, $a^{-1} \in \mathcal{O}_\nu$ e, portanto, a é uma unidade. Logo, dado $\overline{a} \in \mathcal{O}_\nu/\mathfrak{m}_\nu$ não nulo, temos que $a \notin \mathfrak{m}_\nu$, isto é, $\nu(a) = 0$. Logo, a é inversível e $\overline{a^{-1}} = \overline{a}^{-1}$. Isso mostra que $\mathcal{O}_\nu/\mathfrak{m}_\nu$ é corpo e, portanto, $\mathfrak{m}_\nu$ é ideal maximal.

Chamamos o quociente $\mathbb{K}\nu := \mathcal{O}_\nu/\mathfrak{m}_\nu$ de ***corpo de resíduos*** de ν. Denotaremos a classe de um elemento $a \in \mathcal{O}_\nu$ módulo $\mathfrak{m}_\nu$ por $a\nu$. De modo geral, se $\mathcal{O} \subset \mathbb{K}$ é um anel de valorização e $\mathfrak{m}$ é seu ideal maximal, então $\mathcal{O}/\mathfrak{m}$ é chamado corpo de resíduos de $\mathcal{O}$.

Exemplo 1.16. *Para a valorização p-ádica ν^p temos*

$$\mathcal{O}_{\nu^p} = \left\{ \frac{a}{b} \in \mathbb{K} \,\middle|\, p \nmid b \right\} = \mathcal{D}_{\langle p \rangle}, \ \mathfrak{m}_{\nu^p} = \left\{ \frac{a}{b} \in \mathbb{K} \,\middle|\, p \mid a \ e \ p \nmid b \right\}$$

e o corpo de resíduos é $\mathbb{K}\nu^p \cong \mathrm{Frac}(\mathcal{D}/\langle p \rangle) \cong \mathcal{D}/\langle p \rangle$.

▼

Exemplo 1.17. *Para a valorização grau ν_∞, temos*

$$\mathcal{O}_{\nu_\infty} = \left\{ \frac{f(x)}{g(x)} \in \mathbb{F}(x) \;\middle|\; \deg(g(x)) \geq \deg(f(x)) \right\} \text{ e}$$

$$\mathfrak{m}_{\nu_\infty} = \left\{ \frac{f(x)}{g(x)} \in \mathbb{F}(x) \;\middle|\; \deg(g(x)) > \deg(f(x)) \right\}.$$

O corpo de resíduos é isomorfo a $\mathbb{F}$ (Exemplo C.9).

▼

Exemplo 1.18. *Considerando a valorização ν_t no corpo $\mathbb{K}((t^\Gamma))$, que possui como grupo de valores Γ, sejam $\Gamma_< = \{\gamma \in \Gamma \mid \gamma < 0\}$ e $\Gamma_\leq = \{\gamma \in \Gamma \mid \gamma \leq 0\}$. O anel de valorização associado a ν_t é o conjunto*

$$\mathcal{O}_{\nu_t} = \{a \in \mathbb{K}((t^\Gamma)) \mid \Gamma_< \subseteq Z(a)\}.$$

Ainda,

$$\mathfrak{m}_{\nu_t} = \{a \in \mathbb{K}((t^\Gamma)) \mid \Gamma_\leq \subseteq Z(a)\}.$$

O corpo de resíduos de ν_t é isomorfo a $\mathbb{K}$ (Exemplo C.11). Esse exemplo nos mostra que é sempre possível construir uma valorização com grupo de valores e corpo de resíduos pré-determinados.

▼

Para cada valorização ν em um corpo $\mathbb{K}$ associamos um anel de valorização $\mathcal{O}_\nu$. Veremos agora que anéis de valorização também definem valorizações.

Proposição 1.19. *Seja $\mathcal{O} \subseteq \mathbb{K}$ um anel de valorização de $\mathbb{K}$. Então existe uma valorização ν em $\mathbb{K}$ tal que $\mathcal{O} = \mathcal{O}_\nu$.*

Demonstração: Seja $\mathcal{O}^\times$ o grupo das unidades de $\mathcal{O}$. O quociente $\Gamma = \mathbb{K}^\times/\mathcal{O}^\times$ como grupo multiplicativo é um grupo abeliano. Reescrevendo com a notação aditiva, definimos

$$a\mathcal{O}^\times + b\mathcal{O}^\times := ab\mathcal{O}^\times.$$

Colocaremos uma ordem nesse grupo. Definimos a relação binária $\leq$ em Γ por

$$a\mathcal{O}^\times \leq b\mathcal{O}^\times \iff ba^{-1} \in \mathcal{O}.$$

Vejamos que tal ordem transforma Γ em um grupo abeliano totalmente ordenado.

- Temos $a\mathcal{O}^\times \leq a\mathcal{O}^\times$, pois $1 = aa^{-1} \in \mathcal{O}$.

- Se $a\mathcal{O}^\times \leq b\mathcal{O}^\times$ e $b\mathcal{O}^\times \leq a\mathcal{O}^\times$, então $ba^{-1} \in \mathcal{O}$ e $ab^{-1} \in \mathcal{O}$. Logo, como estes são inverso um do outro, segue que $ba^{-1}, ab^{-1} \in \mathcal{O}^\times$. Seja $c \in a\mathcal{O}^\times$ qualquer. Então, existe $c_a \in \mathcal{O}^\times$ tal que $c = ac_a$. Assim, $c = b(ab^{-1}c_a) \in b\mathcal{O}^\times$. Logo, $a\mathcal{O}^\times \subseteq b\mathcal{O}^\times$ e de modo análogo concluímos a outra inclusão.

- Se $a\mathcal{O}^\times \leq b\mathcal{O}^\times$ e $b\mathcal{O}^\times \leq c\mathcal{O}^\times$, então $ba^{-1} \in \mathcal{O}$ e $cb^{-1} \in \mathcal{O}$. Logo, $ca^{-1} = (cb^{-1})(ba^{-1}) \in \mathcal{O}$. Ou seja, $a\mathcal{O}^\times \leq c\mathcal{O}^\times$.

- Dados $a, b \in \mathbb{K}^\times$, como $\mathcal{O}$ é anel de valorização, segue que ou $ab^{-1} \in \mathcal{O}$ ou $ba^{-1} \in \mathcal{O}$. Isso significa que $a\mathcal{O}^\times \leq b\mathcal{O}^\times$ ou $b\mathcal{O}^\times \leq a\mathcal{O}^\times$.

- Suponhamos $a\mathcal{O}^\times \leq b\mathcal{O}^\times$ e seja $c\mathcal{O}^\times \in \Gamma$. Logo, $ba^{-1} \in \mathcal{O}$. Porém, $ba^{-1} = (bc)(ac)^{-1}$ pertence ao anel $\mathcal{O}$. Assim, $a\mathcal{O}^\times + c\mathcal{O}^\times \leq b\mathcal{O}^\times + c\mathcal{O}^\times$.

Definimos a aplicação $\nu : \mathbb{K} \longrightarrow \Gamma_\infty$ como $\nu(a) = a\mathcal{O}^\times$ se $a \in \mathbb{K}^\times$ e $\nu(0) = \infty$. Vejamos que tal aplicação é uma valorização.

- Temos

$$\begin{aligned} \nu(ab) &= ab\mathcal{O}^\times \\ &:= a\mathcal{O}^\times + b\mathcal{O}^\times \\ &= \nu(a) + \nu(b). \end{aligned}$$

- Se $\nu(a) \leq \nu(b)$, então $ba^{-1} \in \mathcal{O}$. Assim, também $(a+b)a^{-1} = 1 + ba^{-1} \in \mathcal{O}$. Portanto, $\nu(a+b) \geq \nu(a) = \min\{\nu(a), \nu(b)\}$.

- Por definição, $\nu(1) = 1\mathcal{O}^\times = 0$ (pois $1 \in \mathcal{O}^\times$) e $\nu(0) = \infty$.

Por fim,

$$\begin{aligned} \mathcal{O}_\nu &= \{a \in \mathbb{K} \mid \nu(a) \geq 0\} \\ &= \{a \in \mathbb{K} \mid a\mathcal{O}^\times \geq 1\mathcal{O}^\times\} \\ &= \{a \in \mathbb{K} \mid a1^{-1} = a1 = a \in \mathcal{O}\} \\ &= \mathcal{O}. \end{aligned}$$

■

1.3 Equivalência entre valorizações

Para uma valorização ν em um anel $\mathcal{R}$, consideremos a valorização de Krull ν' em $\mathcal{R}/\text{supp}(\nu)$. Dado $a \in \mathcal{R}$, denotamos por $\overline{a}$ seu resíduo módulo $\text{supp}(\nu)$. As equivalências a seguir estão demonstradas no Apêndice C (Proposição C.3).

Proposição 1.20. *Sejam ν e μ valorizações em um anel $\mathcal{R}$. As afirmações a seguir são equivalentes.*

1. *Para todo $a, b \in \mathcal{R}$, temos que $\nu(a) > \nu(b) \Leftrightarrow \mu(a) > \mu(b)$.*
2. *Existe um isomorfismo que preserva a ordem $\phi : \nu\mathcal{R} \longrightarrow \mu\mathcal{R}$ tal que $\mu = \phi \circ \nu$.*
3. $\text{supp}(\nu) = \text{supp}(\mu)$ *e para quaisquer* $\overline{a}/\overline{b} \in \text{Frac}(\mathcal{R}/\text{supp}(\nu)) = \text{Frac}(\mathcal{R}/\text{supp}(\mu))$ *temos que* $\nu'(\overline{a}/\overline{b}) \geq 0$ *se, e somente se,* $\mu'(\overline{a}/\overline{b}) \geq 0$.

■

A partir da proposição acima podemos definir uma noção de equivalência entre as valorizações em um anel $\mathcal{R}$.

Definição 1.21. *Duas valorizações ν e μ em um anel $\mathcal{R}$ são ditas equivalentes se satisfazem uma das afirmações da Proposição 1.20.*

■

No caso em que as valorizações ν e μ são Krull, a equivalência entre as valorizações pode ser verificada através de seus anéis de valorização, como veremos no corolário a seguir.

Corolário 1.22. *Duas valorizações de Krull ν e μ em um domínio $\mathcal{R}$ são equivalentes se, e somente se, estas definem o mesmo anel de valorização em* $\text{Frac}(\mathcal{R})$. *Em um corpo $\mathbb{K}$, temos uma bijeção entre os conjuntos*

$$\left\{\begin{array}{c}\textit{classes de equivalência de}\\ \textit{valorizações em } \mathbb{K}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{anéis de valorização}\\ \textit{em } \mathbb{K}\end{array}\right\}$$

Demonstração: Pelo Item 3 da Proposição 1.20, ν e μ são equivalentes se, e somente se, $\text{supp}(\nu) = \text{supp}(\mu)$, $\text{Frac}(\mathcal{R}/\text{supp}(\nu)) = \text{Frac}(\mathcal{R}/\text{supp}(\mu))$ e, para qualquer $\overline{a}/\overline{b} \in \text{Frac}(\mathcal{R}/\text{supp}(\nu))$, temos que $\nu(\overline{a}/\overline{b}) \geq 0$ se, e somente se, $\mu(\overline{a}/\overline{b}) \geq 0$. Mas, $\text{supp}(\nu) = \text{supp}(\mu) = \{0\}$ (ν e μ são valorizações de Krull) e, por isso, $\text{Frac}(\mathcal{R}/\text{supp}(\nu)) = \text{Frac}(\mathcal{R}/\text{supp}(\mu)) = \text{Frac}(\mathcal{R})$. Portanto, ν e μ são equivalentes se, e somente se, para qualquer $a/b \in \text{Frac}(\mathcal{R})$, temos que $\nu(a/b) \geq 0$ se, e somente se, $\mu(a/b) \geq 0$. Essa última condição é equivalente a dizermos que $\mathcal{O}_\nu = \mathcal{O}_\mu$.

■

1.3.1 Valorizações em $\mathbb{Q}$ e valorizações em $\mathbb{K}(x)$ triviais em $\mathbb{K}$

Com esta noção de equivalência entre valorizações mostraremos que as valorizações não triviais no corpo dos números racionais $\mathbb{Q}$ são apenas as valorizações p-ádicas e que segue um resultado similar para $\mathbb{K}(x)$.

Teorema 1.23.

1. *Toda valorização não trivial em $\mathbb{Q}$ é equivalente a uma valorização p-ádica para algum número primo p.*

2. *Toda valorização não trivial em $\mathbb{K}(x)$ que é trivial em $\mathbb{K}$ é equivalente ou a valorização ν_∞ ou a uma valorização $p(x)$-ádica para algum polinômio irredutível $p(x) \in \mathbb{K}[x]$.*

Demonstração:

1. Seja ν uma valorização não trivial em $\mathbb{Q}$. Como $1 \in \mathcal{O}_\nu$, concluímos que $\mathbb{Z} \subset \mathcal{O}_\nu$. Ao menos um primo p deve pertencer a $\mathfrak{m}_\nu$. De fato, se isso não ocorresse, então teríamos pelo Axioma $(V1)$ que $\nu(a) = 0$ para todo $a \in \mathbb{Z}$, pois todo inteiro se escreve como produto de primos. Isso nos levaria a concluir que ν é trivial em $\mathbb{Q}$, o que não é o caso. Afirmamos que existe apenas um primo em $\mathfrak{m}_\nu$. De fato, seja q um primo diferente de p tal que $q \in \mathfrak{m}_\nu$. Sabemos que existem $a, b \in \mathbb{Z}$ tais que

$$ap + bq = 1.$$

No entanto, isso implicaria que $1 \in \mathfrak{m}_\nu$, o que é uma contradição. Portanto todo primo q distinto de p é uma unidade em $\mathcal{O}_\nu$, ou seja, $\nu(q) = 0$.

Afirmamos que se $a, b \in \mathbb{Z}$ são primos entre si, então $\frac{a}{b} \in \mathcal{O}_\nu$ se, e somente se, $p \nmid b$. De fato, se $\frac{a}{b} \in \mathcal{O}$, então

$$\nu\left(\frac{a}{b}\right) = \nu(ab^{-1}) = \nu(a) - \nu(b) \geq 0.$$

Ou seja, $\nu(a) \geq \nu(b)$. Ao olharmos a e b através de suas fatorações em primos, vemos que se $p \mid b$, então seguiria que $\nu(b) > 0$ e $\nu(a) = 0$. Para atingir esta última conclusão, usamos o Axioma $(V1)$, a suposição de a e b serem coprimos e o fato de $\nu(q) = 0$ para todo primo q diferente de p. Porém, isso implicaria que $0 \geq \nu(b) > 0$, o que é uma contradição. Logo, $p \nmid b$.

Reciprocamente, se $p \nmid b$, então $\nu(b) = 0$. Logo, como $a \in \mathbb{Z} \subset \mathcal{O}_\nu$, temos $\nu\left(\frac{a}{b}\right) = \nu(a) - \nu(b) = \nu(a) \geq 0$.

Portanto, $\mathcal{O}_\nu = \mathbb{Z}_{\langle p \rangle}$. Como vimos no Exemplo 1.16, o anel de valorização de ν^p é $\mathbb{Z}_{\langle p \rangle}$. Portanto, ν é equivalente a valorização p-ádica ν^p.

2. Seja ν uma valorização não trivial em $\mathbb{K}(x)$ e tal que $\mathbb{K} \subseteq \mathcal{O}_\nu^\times$. Se $x \in \mathcal{O}_\nu$, então $\mathbb{K}[x] \subset \mathcal{O}_\nu$. Repetimos dessa forma o argumento do Item 1, substituindo $\mathbb{Z}$ por $\mathbb{K}[x]$, e concluiremos que ν é equivalente a uma valorização $p(x)$-ádica para algum polinômio irredutível $p(x)$.

   Suponhamos que $x \notin \mathcal{O}_\nu$. Dessa forma, $x^{-1} \in \mathfrak{m}_\nu$. Com isso, $\nu(x) < 0$ e $\nu(x^j) < \nu(x^i)$ se $0 \leq i < j$. Como $\nu(a) = 0$ para $a \in \mathbb{K}^\times$, se $a_n \neq 0$, então

$$\nu(a_n x^n + \ldots + a_1 + a_0) = \min_{0 \leq i \leq n} \{\nu(a_i x^i)\} = \nu(a_n x^n) = n\nu(x).$$

   Portanto, $\nu(\mathbb{K}(x))$ é igual a $\nu(x)\mathbb{Z}$. Definimos a aplicação $\rho : \nu(x)\mathbb{Z} \longrightarrow \mathbb{Z}$ por $\rho(n\nu(x)) := -n$. Temos que ρ é um isomorfismo. Além disso, este preserva a ordem. De fato, se $n\nu(x) < m\nu(x)$, então $n > m$, uma vez que $\nu(x) < 0$. Assim, temos $\rho(n\nu(x)) = -n < -m = \rho(m\nu(x))$. Agora,

$$\nu\left(f/g\right) = \nu(f) - \nu(g) = \deg(f)\nu(x) - \deg(g)\nu(x).$$

   Isso implica que

$$\rho(\nu(f/g)) = \deg(g) - \deg(f) = \nu_\infty(f/g).$$

   Fazendo a composição $\rho^{-1} \circ \nu_\infty$, obtemos ν. Portanto, ν é equivalente a valorização ν_∞.

■

Pretendemos classificar e descrever também as valorizações em $\mathbb{K}(x)$ que não são triviais em $\mathbb{K}$. Isso virá como consequência dos resultados principais deste trabalho. A seguir, na última seção deste capítulo, introduziremos uma família de valorizações que, no futuro, será essencial para atingirmos tal classificação.

1.4 Estendendo uma valorização de $\mathbb{K}$ para $\mathbb{K}[x]$ via valorizações monomiais

Veremos como construir uma valorização em $\mathbb{K}[x]$ a partir de uma valorização no corpo $\mathbb{K}$. Seja ν uma valorização em $\mathbb{K}$, com grupo de valores $\nu\mathbb{K}$. Seja Γ' um grupo totalmente ordenado que contém $\nu\mathbb{K}$ e tomemos $\gamma \in \Gamma'$. Seja $f = a_0 + a_1 x + \ldots + a_n x^n$. Definimos a seguinte aplicação:

$$\mu_\gamma(f) = \mu_\gamma(a_0 + a_1 x + \ldots + a_n x^n) := \begin{cases} \min\limits_{0 \leq i \leq n} \{\nu(a_i) + i\gamma\} & \text{se } f \neq 0, \\ \infty & \text{se } f = 0. \end{cases}$$

Nosso objetivo nesta seção será provar que μ_γ é uma valorização em $\mathbb{K}[x]$. Uma valorização

com essa forma é chamada **valorização monomial**. Utilizaremos dois resultados para provar o desejado (Lema 1.27 e Proposição 1.28). A prova destes está em termos mais gerais e teremos μ_γ como caso particular.

Para um dado $d \in \mathbb{N}$, definimos

$$\mathbb{K}[x]_d := \{f \in \mathbb{K}[x] \mid \deg(f) < d\}.$$

Como convencionamos $\deg(0) = -\infty$, temos $0 \in \mathbb{K}[x]_d$ para qualquer $d \in \mathbb{N}$.

Proposição 1.24. *Seja $q \in \mathbb{K}[x]$ um polinômio de grau $d > 0$. Para cada polinômio $f \in \mathbb{K}[x]$, $f \neq 0$, podemos escrever*

$$f = f_0 + f_1 q + \ldots + f_r q^r,$$

em que $f_i \in \mathbb{K}[x]_d$ para cada i, $0 \leq i \leq r$, sendo r o maior inteiro positivo tal que $f_r \neq 0$. O número r e os coeficientes f_i são únicos.

Demonstração: Para a existência, procederemos utilizando o Princípio de Indução Forte sobre o grau de f. Para a base de indução, suponhamos $\deg(f) < d$. Temos $f = 0q + f$. Logo, tomamos $f_0 = f \in \mathbb{K}[x]_d$. Suponhamos que, para um dado n, se $\deg(f) < n$, então o resultado é válido. Seja f um polinômio de grau n. Podemos supor $n \geq d$, devido ao que vimos na base de indução. Pelo Algoritmo da Divisão, temos $f = f_1' q + f_0$ com $f_0 \in \mathbb{K}[x]_d$. Como $\deg(f_0) < d = \deg(q) \leq \deg(f_1' q)$ e $f_1' \neq 0$, segue que

$$\deg(f) = \deg(f_1' q + f_0) = \deg(f_1' q) = \deg(f_1') + \deg(q).$$

Ou seja, $\deg(f_1') = \deg(f) - d < n$. Pela hipótese de indução, existe $r' \in \mathbb{N}$ tal que

$$f_1' = \sum_{i=0}^{r'} f_i' q^i$$

com $f_i' \in \mathbb{K}[x]_d$ para cada i, $0 \leq i \leq r'$. Escrevendo $r = r' + 1$ e $f_i' = f_{i+1}$, para $0 \leq i \leq r'$, temos

$$f = \left(\sum_{i=0}^{r'} f_i' q^i\right) q + f_0 = \left(\sum_{i=0}^{r'} f_i' q^{i+1}\right) + f_0 = \left(\sum_{i=0}^{r} f_i q^i\right).$$

Para vermos a unicidade, suponhamos que

$$f = \sum_{i=0}^{r} f_i q^i = \sum_{j=0}^{r'} g_j q^j,$$

em que $f_i, g_j \in \mathbb{K}[x]_d$ para todo i e todo j, $0 \leq i \leq r$ e $0 \leq j \leq r'$, r é o maior inteiro positivo tal que $f_r \neq 0$ e r' é o maior inteiro positivo tal que $g_{r'} \neq 0$. Sem perda de generalidade,

podemos supor que $r \leq r'$. Suponhamos, buscando uma contradição, $r < r'$. Definimos $f_j = 0$ para todo j satisfazendo $r < j \leq r'$, Assim, indexamos as duas expansões de f em j. Temos

$$0 = f - f = \sum_{j=0}^{r'} (f_j - g_j) q^j.$$

Como $q^j \neq 0$ para todo j, $0 \leq j \leq r'$, e x é transcendente sobre $\mathbb{K}$, segue que a igualdade acima é possível somente se $f_j = g_j$ para todo j. Assim, isso implica $g_{r'} = f_{r'} = 0$, o que é uma contradição. Logo, segue a unicidade de r e dos coeficientes da expansão.

■

Tiramos da proposição acima a seguinte definição.

Definição 1.25. *A expressão para f dada por*

$$f = f_0 + f_1 q + \ldots + f_r q^r,$$

em que $\deg(f_i) < \deg(q)$ para cada i, $1 \leq i \leq r$, será chamada de ***q-expansão de f***. ■

Seja $\mu : \mathbb{K}[x]_d \longrightarrow \Gamma_\infty$ uma aplicação em que Γ é um grupo totalmente ordenado, e seja $q \in \mathbb{K}[x]$ um polinômio de grau d. Tomemos um grupo Γ', também totalmente ordenado, que contém Γ e $\gamma \in \Gamma'$. Podemos definir uma aplicação $\mu' : \mathbb{K}[x] \longrightarrow \Gamma'_\infty$ a partir da q-expansão de polinômios:

$$\mu'(f) = \min_{0 \leq i \leq r} \{\mu(f_i) + i\gamma\} \tag{1.1}$$

em que $f_0, f_1, \ldots, f_r$ são os coeficientes da q-expansão de f. Convencionamos que a q-expansão de 0 é $f = f_0 = 0$. Veremos agora algumas relações entre μ e μ'.

Definição 1.26. *Seja S um subconjunto de um anel $\mathcal{R}$ e Γ um grupo abeliano totalmente ordenado. Seja $\eta : S \longrightarrow \Gamma_\infty$ uma aplicação.*

- *Dizemos que η satisfaz $(V1')$ em S se para todo $f, g \in S$, temos*

  $$\eta(fg) = \eta(f) + \eta(g)$$

  quando $fg \in S$.

- *Dizemos que η satisfaz $(V2')$ em S se para todo $f, g \in S$, temos*

  $$\eta(f + g) \geq \min\{\eta(f), \eta(g)\}$$

  quando $f + g \in S$.

■

Lema 1.27. *Se μ satisfaz $(V2')$ em $\mathbb{K}[x]_d$, então μ' satisfaz $(V2)$ em $\mathbb{K}[x]$.*

Demonstração: Sejam $f, g \in \mathbb{K}[x]$. Escrevemos a q-expansão de ambos os polinômios, que podemos tomar com mesmo índice e mesmo limite superior da soma, completando com 0 onde necessário:

$$f = \sum_{i=0}^{r} f_i q^i \text{ e } g = \sum_{i=0}^{r} g_i q^i,$$

com $f_i, g_i \in \mathbb{K}[x]_d$ para todo i, $0 \leq i \leq r$. Da unicidade da q-expansão, vemos que a q-expansão de $f+g$ é

$$f + g = \sum_{i=0}^{r} (f_i + g_i) q^i.$$

Dessa forma,

$$\begin{aligned}
\mu'(f+g) &= \min_{0\leq i\leq r} \{\mu(f_i + g_i) + i\gamma\} \\
&\geq \min_{0\leq i\leq r} \{\min\{\mu(f_i), \mu(g_i)\} + i\gamma\} \\
&= \min\left\{ \min_{0\leq i\leq r} \{\mu(f_i) + i\gamma\}, \min_{0\leq i\leq r} \{\mu(g_i) + i\gamma\} \right\} \\
&= \min\{\mu'(f), \mu'(g)\}.
\end{aligned}$$

Assim, vemos que se μ satisfaz $(V2')$, então μ' satisfaz $(V2)$ em $\mathbb{K}[x]$.

■

A proposição a seguir é um dos resultados principais de Novacoski (2021).

Proposição 1.28. *Seja S um subconjunto de $\mathbb{K}[x]$ fechado para multiplicação com $\mathbb{K}[x]_d \subseteq S$, para algum d inteiro. Sejam μ, γ e μ' como na Equação 1.1. Seja q um polinômio de grau d. Suponhamos que $\mu : S \longrightarrow \Gamma_\infty$, satisfaça $(V2')$ em S e que, para todo $\overline{f}, \overline{g} \in \mathbb{K}[x]_d$, tenhamos*

1. *$\mu(\overline{f}\overline{g}) = \mu(\overline{f}) + \mu(\overline{g})$,*

2. *se $\overline{f}\overline{g} = aq + c$ com $c \in \mathbb{K}[x]_d$ (e, por consequência, $a \in \mathbb{K}[x]_d$), então*

$$\mu(c) = \mu(\overline{f}\overline{g}) < \mu(a) + \gamma.$$

Então μ' satisfaz os Axiomas $(V1)$ e $(V2)$ em $\mathbb{K}[x]$.

Demonstração: Como μ satisfaz $(V2')$ em $S \supseteq \mathbb{K}[x]_d$, segue que μ satisfaz $(V2')$ em $\mathbb{K}[x]_d$. Pelo Lema 1.27, μ' satisfaz $(V2)$ em $\mathbb{K}[x]$.

Sejam $f, g \in \mathbb{K}[x]$ e tomemos suas q-expansões

$$f = \sum_{i=0}^{r} f_i q^i \text{ e } g = \sum_{j=0}^{s} g_j q^j.$$

Para todo i e todo j, $0 \leq i \leq r$ e $0 \leq j \leq s$, temos

$$\mu(f_i) \geq \mu'(f) - i\gamma \text{ e } \mu(g_j) \geq \mu'(g) - j\gamma.$$

Para cada i e cada j, $0 \leq i \leq r$ e $0 \leq j \leq s$, seja $f_i g_j = a_{ij} q + c_{ij}$ a q-expansão de $f_i g_j$. Se $r = 0 = s$, então, pelas hipóteses,

$$\begin{aligned} \mu'(fg) &= \min\{\mu(c_{00}), \mu(a_{00} + \gamma)\} = \mu(c_{00}) = \mu(f_0 g_0) \\ &= \mu(f_0) + \mu(g_0) = \mu'(f) + \mu'(g). \end{aligned}$$

Assim, neste caso, μ' satisfaz $(V1)$. Suponhamos então que $r > 0$ ou $s > 0$. Uma vez que μ' satisfaz $(V2)$, temos

$$\mu'(fg) \geq \min_{i,j}\{\mu'(f_i g_j q^{i+j})\} = \min_{i,j}\{\mu'(f_i q^i) + \mu'(g_j q^j)\} = \mu'(f) + \mu'(g).$$

Portanto, basta mostrarmos que $\mu'(fg) \leq \mu'(f) + \mu'(g)$. Para todo i e todo j, $0 \leq i \leq r$ e $0 \leq j \leq s$, utilizando as hipóteses, temos que

$$\mu'(f_i q^i) + \mu'(g_j q^j) = \mu(f_i g_j) + (i + j)\gamma = \mu(c_{ij}) + (i + j)\gamma = \mu'(c_{ij} q^{i+j}).$$

Sejam i_0 e j_0, $0 \leq i_0 \leq r$ e $0 \leq j_0 \leq s$, os menores inteiros não negativos tais que $\mu'(f) = \mu(f_{i_0}) + i_0\gamma$ e $\mu'(g) = \mu(g_{j_0}) + j_0\gamma$. Seja $k_0 := i_0 + j_0$. Para todo $i \leq k_0$, se $i < i_0$, então

$$\mu'(f) < \mu(f_i) + i\gamma \text{ e } \mu'(g) \leq \mu(g_{k_0 - i}) + (k_0 - i)\gamma.$$

Por outro lado, se $i > i_0$, então $k_0 - i < j$, logo temos

$$\mu'(f) \leq \mu(f_i) + i\gamma \text{ e } \mu'(g) < \mu(g_{k_0 - i}) + (k_0 - i)\gamma.$$

Dessa forma, para todo $i \neq i_0$,

$$\begin{aligned} \mu(c_{i_0 j_0}) &= \mu(f_{i_0}) + \mu(g_{j_0}) = \mu'(f) - i_0\gamma + \mu'(g) - j_0\gamma \\ &= \mu'(f) + \mu'(g) - k_0\gamma \\ &< \mu(f_i) + i\gamma + \mu(g_{k_0 - i}) + (k_0 - i)\gamma - k_0\gamma \\ &= \mu(f_i g_{k_0 - i}) = \mu(c_{i(k_0 - i)}) \end{aligned}$$

Por outro lado, para qualquer $i \leq k_0 - 1$ temos

$$\begin{aligned}
\mu(a_{i(k_0-i-1)}) &> \mu(c_{i(k_0-i-1)}) - \gamma \\
&= \mu(f_i g_{k_0-i-1}) - \gamma \\
&= \mu(f_i) + \mu(g_{k_0-i-1}) - \gamma \\
&\geq \mu'(f) + \mu'(g) - (k_0 - 1)\gamma - \gamma \\
&= \mu'(f) + \mu'(g) - k_0\gamma \\
&= \mu(c_{i_0 j_0}) + k_0\gamma - k_0\gamma \\
&= \mu(c_{i_0 j_0}).
\end{aligned}$$

Seja agora $fg = a_0 + a_1 q + \ldots + a_l q^l$ a q-expansão de fg. Como

$$\begin{aligned}
fg &= \sum_{u=0}^{r+s} \left(\sum_{t=0}^{u} f_t g_{u-t} \right) q^u = \sum_{u=0}^{r+s} \left(\sum_{t=0}^{u} a_{t(u-t)} q + c_{t(u-t)} \right) q^u \\
&= \sum_{u=0}^{r+s} \left(\sum_{t=0}^{u} a_{t(u-t)} \right) q^{u+1} + \sum_{u=0}^{r+s} \left(\sum_{t=0}^{u} c_{t(u-t)} \right) q^u,
\end{aligned}$$

pela unicidade da q-expansão temos

$$a_u = \sum_{t=0}^{u-1} a_{t(u-t-1)} + \sum_{t=0}^{u} c_{t(u-t)}$$

para todo u, $0 \leq u \leq l = r + s$. Em particular,

$$a_{k_0} = \sum_{t=0}^{k_0-1} a_{t(k_0-t)} + \sum_{t=0}^{k_0} c_{t(k_0-t)}.$$

Vimos acima que $\mu(c_{i_0 j_0}) < \mu(a_{i(k_0-i-1)})$ para $i \leq k_0 - 1$ e $\mu(c_{i_0 j_0}) < \mu(c_{i(k_0-i)})$ para $i \neq i_0$. Portanto, pela Propriedade $(V2')$ de μ, segue que

$$\mu(a_{k_0}) = \mu(c_{i_0 j_0}) = \mu(f_{i_0}) + \mu(g_{j_0}) = \mu'(f) + \mu'(g) - k_0\gamma.$$

Logo,

$$\mu'(fg) \leq \mu(a_{k_0}) + k_0\gamma = \mu'(f) + \mu'(g)$$

e concluímos que

$$\mu'(fg) = \mu'(f) + \mu'(g).$$

■

Provemos então o resultado principal desta seção.

Teorema 1.29. *A aplicação μ_γ é uma valorização em $\mathbb{K}[x]$.*

Demonstração: Tomemos, na Proposição 1.28, $\mu = \mu' = \mu_\gamma$. Verifiquemos as três propriedades que uma valorização deve satisfazer:

- $(V1)$ Como $\deg(x) = 1$ e $\mathbb{K}[x]_1 = \mathbb{K}$, segue que $\mu = \mu_\gamma$ satisfaz o Item 1 da Proposição 1.28, pois $\mathbb{K}[x]_1 = \mathbb{K}$ é fechado para a multiplicação e $\mu_\gamma|_{\mathbb{K}} = \nu$, que é uma valorização. Também, para $f, g \in \mathbb{K}$, se $fg = ax + c$, então $a = 0$ e $c = fg$ pois x é transcendente sobre $\mathbb{K}$. Portanto,

$$\mu_\gamma(fg) = \mu_\gamma(c) < \infty = \mu_\gamma(0) = \mu_\gamma(a) + \gamma.$$

  Isto é, $\mu = \mu_\gamma$ satisfaz o Item 2 da Proposição 1.28. Logo, $\mu' = \mu_\gamma$ satisfaz $(V1)$ em $\mathbb{K}[x]$.

- $(V2)$ Do Lema 1.27, como $\mu = \mu_\gamma$ satisfaz $(V2')$ em $\mathbb{K}[x]_1 = \mathbb{K}$ (pois $\mu_\gamma|_{\mathbb{K}} = \nu$ é valorização), temos que $\mu' = \mu_\gamma$ satisfaz $(V2)$ em $\mathbb{K}[x]$.

- $(V3)$ Direto da definição, $\mu_\gamma(0) = \nu(0) + 0\gamma = \infty$ e $\mu_\gamma(1) = \nu(1) + 0\gamma = 0$.

Portanto, μ_γ é uma valorização em $\mathbb{K}[x]$.

■

Como podemos ver no Apêndice F, em $\mathbb{K}[x]$ vale que todo polinômio $f(x)$ possui, para um dado $a \in \mathbb{K}$, uma representação da forma

$$f(x) = \sum_{k=0}^{r} a_k (x-a)^k,$$

em que $a_k \in \mathbb{K}$ para todo k, $0 \leq k \leq r$. Esta representação é a Expressão de Taylor de $f(x)$ em torno de a. Se ν é uma valorização em $\mathbb{K}$ e γ é um elemento nas mesmas condições que anteriormente, então a partir dessa expressão de $f(x)$ definimos

$$\mu_{a,\gamma}\left(\sum_{k=0}^{r} a_k (x-a)^k\right) := \min_{0\leq k\leq r}\{\nu(a_k) + k\gamma\}.$$

Notamos que na prova do Teorema 1.29 apenas utilizamos de $q = x$ o fato de $\deg(x) = 1$ e que x é transcendente sobre $\mathbb{K}$. Assim, repetindo a prova desse teorema com $q = x - a$ e $\mu = \mu' = \mu_{a,\gamma}$, temos que $\mu_{a,\gamma}$ é uma valorização em $\mathbb{K}[x]$. Valorizações com esse formato também são classificadas como monomiais.

Como ν é valorização de Krull em $\mathbb{K}$, temos que $\mu_{a,\gamma}$ também é valorização de Krull. De fato,

$$\mu_{a,\gamma}\left(\sum_{k=0}^{r} a_k(x-a)^k\right) := \min_{0\leq k\leq r}\{\nu(a_k)+k\gamma\} = \infty \Longleftrightarrow \nu(a_k)+k\gamma = \infty$$

para todo k, $0 \leq k \leq r$. Isso ocorre se, e somente se, $\nu(a_k) = \infty$ para todo k. Tal fato é equivalente a dizermos que $a_k = 0$ para todo k, isto é, $\mu_{a,\gamma}$ é de Krull. Dessa forma, fica bem definida a valorização $\mu_{a,\gamma}$ em $\mathbb{K}(x) = \mathrm{Frac}(\mathbb{K}[x])$ dada por

$$\mu_{a,\gamma}\left(\frac{f}{g}\right) := \mu_{a,\gamma}(f) - \mu_{a,\gamma}(g).$$

Por fim, veremos no exemplo abaixo como utilizar as valorizações monomiais e a Proposição 1.28 para construir outras valorizações em $\mathbb{K}[x]$. A valorização do exemplo a seguir será utilizada em exemplos nos próximos capítulos.

Exemplo 1.30. *Consideremos em $\mathbb{Q}$ a valorização 2-ádica ν^2 e seja $\mu = \nu^2_{0,\frac{1}{2}}$ a valorização monomial em $\mathbb{Q}[x]$ definida em um polinômio $g(x) = a_r x^r + \ldots + a_1 x + a_0$ por*

$$\mu(g) = \min_{0\leq i\leq r}\left\{\nu^2(a_i) + \frac{i}{2}\right\}.$$

Seja $Q = x^2 - 2$. Considerando $f(x) = f_0 + f_1 Q + \ldots + f_r Q^r$ a Q-expansão de f, isto é, com $f_i = 0$ ou $\deg(f_i) < \deg(Q) = 2$ (Proposição 1.24), definimos

$$\mu'(f) := \min_{0\leq i\leq r}\left\{\mu(f_i) + i\frac{3}{2}\right\}.$$

Vejamos que μ' é uma valorização em $\mathbb{Q}[x]$. De fato, usaremos a Proposição 1.28 para $\gamma = \frac{3}{2}$ e $S = \mathbb{Q}[x]$. Nela vemos que se μ em $\mathbb{Q}[x]$ é tal que

- *μ satisfaz $(V2)$,*
- *para $h_1, h_2 \in \mathbb{Q}[x]_2$, vale que $\mu(h_1h_2) = \mu(h_1) + \mu(h_2)$ e*
- *para $h_1, h_2, c \in \mathbb{Q}[x]_2$, se $h_1h_2 = aQ + c$, então $\mu(c) = \mu(h_1h_2) < \mu(a) + \gamma$,*

então segue que μ' satisfaz $(V1)$ e $(V2)$. Lembremos que

$$\mathbb{Q}[x]_2 = \{f \in \mathbb{Q}[x] \mid \deg(f) < 2\}.$$

Temos que μ satisfaz os dois primeiros itens acima, pois μ é valorização. Suponhamos que $h_1, h_2, c \in \mathbb{Q}[x]_2$ sejam tais que $h_1h_2 = aQ + c$ para algum $a \in \mathbb{Q}[x]$. De imediato vemos que

$a \in \mathbb{Q}[x]_2$. *Escrevendo* $h_1 = a_1x + b_1$ *e* $h_2 = a_2x + b_2$, *vemos que*

$$a_1a_2x^2 + (a_1b_2 + b_1a_2)x + b_1b_2 = ax^2 - 2a + c.$$

Ou seja, $a_1a_2 = a \in \mathbb{Q}$. *Se* $a_1 = 0$ *ou* $a_2 = 0$, *então segue o resultado. De fato, nesse caso teremos simplesmente* $h_1h_2 = c$ *e, portanto,* $\mu(h_1h_2) = \mu(c) < \mu(a) + \gamma$ *pois* $\mu(a) = \mu(a_1a_2) = \mu(0) = \infty$. *Suponhamos que ambos* a_1 *e* a_2 *são diferentes de zero. Sejam* $g_i = x + \frac{b_i}{a_i} = x + d_i$, *com* $i = 1, 2$. *Temos*

$$h_1h_2 = a_1a_2g_1g_2 = aQ + c = a_1a_2Q + c.$$

Logo, $g_1g_2 = Q + \frac{c}{a_1a_2} = Q + c'$. *É suficiente mostrarmos que* $\mu(g_1g_2) = \mu(c') < \gamma$ *pois, com isso,*

$$\mu(h_1h_2) = \mu(a_1a_2) + \mu(g_1g_2) = \mu(a_1a_2) + \mu(c') = \mu(a_1a_2) + \mu(c) - \mu(a_1a_2) = \mu(c)$$

e $\mu(h_1h_2) = \mu(a_1a_2) + \mu(g_1g_2) < \mu(a_1a_2) + \gamma$. *Sabemos que* $\mu(x + d_i) = \min\{\nu^2(d_i), \frac{1}{2}\} \leq \frac{1}{2}$. *Logo,*

$$\mu(g_1g_2) = \mu(x + d_1) + \mu(x + d_2) \leq \frac{1}{2} + \frac{1}{2} = 1 < \frac{3}{2} = \gamma.$$

Resta vermos que $\mu(g_1g_2) = \mu(c')$. *Separamos em dois casos. Suponhamos* $\mu(d_j) = \nu^2(d_j) < 1$ *para algum* j. *Como* $\nu^2(d_j) \in \mathbb{Z}$, *segue que* $\mu(d_j) \leq 0$. *Dessa forma,*

$$\mu(x + d_j) = \min\left\{\nu^2(d_j), \frac{1}{2}\right\} = \nu^2(d_j) < \frac{1}{2}.$$

Portanto,

$$\mu(g_1g_2) = \mu(x + d_1) + \mu(x + d_2) < \frac{1}{2} + \frac{1}{2} = 1 = \mu(Q).$$

Assim,

$$\mu(g_1g_2 - c') = \mu(Q) = 1 > \mu(g_1g_2) \geq \min\{\mu(g_1g_2), \mu(c')\},$$

o que implica $\mu(g_1g_2) = \mu(c')$. *Suponhamos agora que* $\mu(d_i) \geq 1$ *para ambos* $i = 1, 2$. *Dessa forma,*

$$\mu(x + d_i) = \frac{1}{2},\ \mu(d_1d_2) = \mu(d_1) + \mu(d_2) \geq 2,$$

$$\mu(d_1d_2 + 2) = \min\{\mu(d_1d_2), \mu(2)\} = 1$$

e

$$\mu((d_1 + d_2)x) \geq \min\{\mu(d_1x), \mu(d_2x)\} \geq \frac{3}{2}.$$

Como

$$g_1g_2 = (x + d_1)(x + d_2) = x^2 + (d_1 + d_2)x + d_1d_2 = x^2 - 2 + c',$$

vemos que $c' = (d_1 + d_2)x + d_1d_2 + 2$. *Logo,*

$$\mu(c') = \min\{\mu(d_1d_2 + 2)), \mu((d_1 + d_2)x)\} = 1 = \frac{1}{2} + \frac{1}{2} = \mu(x + d_1) + \mu(x + d_2) = \mu(g_1g_2).$$

Segue então da Proposição 1.28 que μ' *satisfaz* $(V1)$ *e* $(V2)$ *em* $\mathbb{K}[x]$. *Como* $\mu'(1) = 0$ *e* $\mu(0) = \infty$, *pois* μ *é valorização, segue que* μ' *é valorização.*

▼

Capítulo 2

Polinômios-chaves e truncamentos

Neste capítulo apresentaremos um tipo especial de polinômio que nos ajudará a construir novas valorizações no anel de polinômios $\mathbb{K}[x]$, a partir de uma valorização dada em $\mathbb{K}[x]$. Tais polinômios serão chamados polinômios-chaves. Estes serão fundamentais para caracterizar uma classe de valorizações que apresentaremos no futuro, a saber as valorizações transcendentes.

Na primeira seção, apresentaremos a definição de polinômio-chave e suas primeiras propriedades. Em seguida, na segunda seção, trataremos das valorizações definidas por truncamentos em polinômios-chaves. Por fim, na terceira seção provaremos mais propriedades desses polinômios que serão úteis no capítulo seguinte.

As principais referências para a composição deste capítulo foram os trabalhos de Novacoski e Spivakovsky (2018) e de Novacoski (2019).

2.1 Definindo $\epsilon(f)$, $\delta(f)$ e polinômios-chaves

Seja μ uma valorização em $\mathbb{K}[x]$. Para simplificar as notações que introduziremos a seguir, vamos denotar o grupo de valores de μ por Γ. Consideremos $\Gamma_{\mathbb{Q}} \cong \Gamma \otimes \mathbb{Q}$, que é o chamado fecho divisível do grupo Γ. No Apêndice B, descrevemos a forma de um elemento de $\Gamma_{\mathbb{Q}}$, que pode ser visto como uma fração $\frac{\gamma}{m}$ em que $\gamma \in \Gamma$ e $m \in \mathbb{N}$. Através do mergulho de Γ em $\Gamma_{\mathbb{Q}}$ que leva γ em $\frac{\gamma}{1}$, vamos identificar $\frac{\gamma}{1} = \gamma$. Uma vez que Γ é ordenado, também induzimos uma ordem total em $\Gamma_{\mathbb{Q}}$ que, na notação de fração, funciona como a ordem usual de $\mathbb{Q}$.

Estenderemos $\Gamma_{\mathbb{Q}}$ para a estrutura $\Gamma_{\mathbb{Q}} \cup \{-\infty, \infty\}$, em que $-\infty$ e ∞ são símbolos satisfazendo, para todo $\rho \in \Gamma_{\mathbb{Q}}$:

- $\infty + \rho = \rho + \infty = \infty$ e $\infty + \infty = \infty$;
- $-\infty + \rho = \rho + (-\infty) = -\infty$ e $-\infty + (-\infty) = -\infty$;
- $\infty > \rho$, $-\infty < \rho$ e $-\infty < \infty$.

Sejam $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{K}[x]$ e $k \in \mathbb{N}_0$. A **derivada de Hasse** de ordem k de f é o polinômio $\partial_k f$ definido como

$$(\partial_k f)(x) = \sum_{i=k}^{n} \binom{i}{k} a_i x^{i-k} \in \mathbb{K}[x],$$

se $k \leq n$, e como 0, se $k > n$. No Apêndice F, vemos que o polinômio $\partial_k f$ é o polinômio unicamente determinado tal que, para todo $a \in \mathbb{K}$, $\partial_k f(a)$ é o coeficiente do monômio de grau k na expansão de Taylor de f em torno de a. No referido apêndice também provamos algumas propriedades da derivada de Hasse que serão utilizadas neste capítulo.

A definição de $\epsilon(f)$ que veremos a seguir tem origem nos trabalhos de Decaup, Mahboub e Spivakovsky (2018) e de Novacoski e Spivakovsky (2018).

Definição 2.1. *Sejam μ uma valorização em $\mathbb{K}[x]$ e $f \in \mathbb{K}[x]$ um polinômio não nulo.*

- *Se* $\deg(f) = 0$, *então* $\epsilon(f) := -\infty$.
- *Se* $f \notin \operatorname{supp}(\mu)$ *e* $\deg(f) > 0$, *então*

$$\epsilon(f) := \max_{1 \leq k \leq \deg(f)} \left\{ \frac{\mu(f) - \mu(\partial_k f)}{k} \;\middle|\; \mu(\partial_k f) \in \Gamma \right\} \in \Gamma_{\mathbb{Q}}.$$

- *Se* $f \in \operatorname{supp}(\mu)$, *então* $\epsilon(f) := \infty$.

■

Veremos a seguir uma interpretação geométrica para $\epsilon(f)$. No Apêndice G, tal interpretação será formalizada e refinada.

Exemplo 2.2. *Consideremos em $\mathbb{Q}$ a valorização 2-ádica ν^2 e seja $\mu = \nu_{\frac{1}{2}}^2$ a valorização monomial em $\mathbb{Q}[x]$ definida como na Seção 1.4: se $g(x) = a_r x^r + \ldots + a_1 x + a_0$, então*

$$\mu(g) = \min_{0 \leq i \leq r} \left\{ \nu^2(a_i) + \frac{i}{2} \right\}.$$

Seja $f(x) = x^4 - 2x^2 + 2x + 4$. Inicialmente, calculemos $\epsilon(f)$. Temos

$$\mu(f) = \min\left\{2, 1 + \frac{1}{2}, 1 + \frac{2}{2}, 0 + \frac{4}{2}\right\} = \min\left\{2, \frac{3}{2}\right\} = \frac{3}{2}.$$

As derivadas de Hasse de f são

$$\partial_1 f(x) = 4x^3 - 4x + 2,\ \partial_2 f(x) = 6x^2 - 2,\ \partial_3 f(x) = 4x \text{ e } \partial_4 f(x) = 1.$$

Calculando $\mu(\partial_j f)$, para $1 \leq j \leq 4$, obtemos $\mu(\partial_1 f) = 1$, $\mu(\partial_2 f) = 1$, $\mu(\partial_3 f) = \frac{5}{2}$ e $\mu(\partial_4 f) = 0$. Assim,

$$\epsilon(f) = \max\left\{\frac{\frac{3}{2}-1}{1}, \frac{\frac{3}{2}-1}{2}, \frac{\frac{3}{2}-\frac{5}{2}}{3}\ \frac{\frac{3}{2}-0}{4}\right\} = \max\left\{\frac{1}{2}, \frac{1}{4}, -\frac{1}{3}, \frac{3}{8}\right\} = \frac{1}{2}.$$

Consideremos o conjunto de pontos

$$X = \left\{(0, \tfrac{3}{2}), (1,1), (2,1), (3, \tfrac{5}{2}), (4,0)\right\}$$

em $\mathbb{Q} \times \Gamma_{\mathbb{Q}}$. Este é o conjunto dos pares $(j, \mu(\partial_j f))$ com $0 \leq j \leq 4$. Construímos então a envoltória convexa de X, ilustrada na Figura 2.1, que nos fornece o polígono de Newton do conjunto X. As definições formais desses objetos serão apresentadas no Apêndice G. Olhando para as retas suportes dos lados do polígono de Newton, $y = -\frac{1}{3}x + \frac{4}{3}$ e $y = -\frac{1}{2}x + \frac{3}{2}$, vemos que a reta de menor inclinação possui inclinação igual a $-\epsilon(f)$.

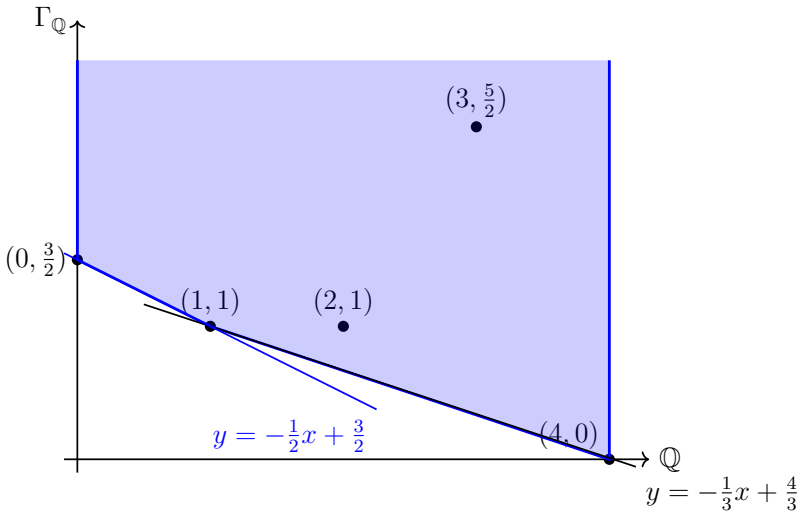


Figura 2.1: Conjunto X e sua envoltória convexa.

▼

Os polinômios-chaves, que apresentaremos a seguir, mostraram-se objetos importantes em alguns programas que pretendem provar dois problemas significativos em Geometria Algébrica. São esses o problema da uniformização local e da resolução de singularidades em característica positiva (NOVACOSKI; SPIVAKOVSKI, 2016). Em 1936, Mac Lane começou o estudo dos polinômios-chaves para entender todas as possíveis extensões de uma valorização de $\mathbb{K}$ para $\mathbb{K}[x]$ (MAC LANE, 1936). Muitos anos depois, Vaquié introduziu uma generalização dos polinômios-chaves de Mac Lane (VAQUIÉ, 2007). Em seguida, Novacoski e Spivakovsky (2018) e Decaup,

Mahboub e Spivakovsky (2018) introduzem um novo conceito de polinômio-chave. Utilizaremos neste trabalho esta última noção, que está definida abaixo.

Definição 2.3. *Um polinômio mônico $Q \in \mathbb{K}[x]$ é um* ***polinômio-chave*** *de nível $\epsilon(Q)$ se, para todo $f \in \mathbb{K}[x]$, valer*

$$\deg(f) < \deg(Q) \Rightarrow \epsilon(f) < \epsilon(Q).$$

■

Exemplo 2.4. *Todo polinômio linear $x-a$ é um polinômio-chave de nível $\epsilon(x-a) = \mu(x-a)$. De fato, suponhamos que $f \in \mathbb{K}[x]$ seja tal que $\deg(f) < \deg(x-a)$, ou seja, $\deg(f) = 0$. Assim,*

$$\epsilon(f) = -\infty < \epsilon(x-a) = \mu(x-a).$$

▼

Exemplo 2.5. *Um polinômio não nulo $g \in \mathbb{K}[x]$ que é um gerador de $\operatorname{supp}(\mu)$ também é trivialmente um polinômio-chave. De fato, $\deg(f) < \deg(g)$ implica que $f \notin \operatorname{supp}(\mu)$. Assim, $\epsilon(f) \in \Gamma_{\mathbb{Q}}$ ou $\epsilon(f) = -\infty$, ambos estritamente menores do que $\epsilon(g) = \infty$.*

▼

Exemplo 2.6. *Seja, $Q(x) = x^2 - 2$ e μ' a valorização em $\mathbb{K}[x]$ definida como no Exemplo 1.30: considerando $f(x) = f_0 + f_1 Q + \ldots + f_r Q^r$ em sua Q-expansão, definimos*

$$\mu'(f) := \min_{0 \le i \le r} \left\{ \mu(f_i) + i\frac{3}{2} \right\},$$

em que μ é a valorização monomial que utilizamos no Exemplo 2.2. Mostremos que Q é polinômio-chave para μ'. Iniciemos calculando $\epsilon(Q)$. Temos $\mu'(Q) = \frac{3}{2}$ e $\mu'(x) = \frac{1}{2}$. Calculando as derivadas de Hasse de Q, obtemos $\partial_1 Q = 2x$ e $\partial_2 Q = 1$. Logo,

$$\begin{aligned}
\epsilon(Q) &= \max\left\{ \frac{\mu'(Q) - \mu'(\partial_1 Q)}{1}, \frac{\mu'(Q) - \mu'(\partial_2 Q)}{2} \right\} \\
&= \max\left\{ \frac{\frac{3}{2} - (1 + \frac{1}{2})}{1}, \frac{\frac{3}{2} - 0}{2} \right\} \\
&= \max\left\{ 0, \frac{3}{4} \right\} \\
&= \frac{3}{4}.
\end{aligned}$$

Seja agora f tal que $\deg(f) < \deg(Q) = 2$, ou seja, $f(x) = ax + b$. Se $a = 0$, então $\epsilon(f) = \epsilon(b) = -\infty$ por definição e, com isso, $\epsilon(f) < \epsilon(Q)$. Suponhamos $a \neq 0$. Então,

$$\epsilon(f) = \epsilon(ax+b) = \frac{\mu'(ax+b) - \mu'(a)}{1} = \mu'(x+c),$$

em que $c = \frac{b}{a}$. *Como* $\mu'(c) = \nu^2(c) \in \mathbb{Z}$, *segue que* $\mu'(x) = \frac{1}{2} \neq \mu'(c)$. *Assim,*

$$\epsilon(f) = \mu'(x + c) = \min\left\{\frac{1}{2}, \mu'(c)\right\}.$$

Temos dois casos. Se $\mu'(c) > \frac{1}{2}$, *então*

$$\epsilon(f) = \frac{1}{2} < \frac{3}{4} = \epsilon(Q).$$

Se $\mu'(c) < \frac{1}{2}$, *então*

$$\epsilon(f) = \mu'(c) < \frac{1}{2} < \frac{3}{4} = \epsilon(Q).$$

Concluímos dessa forma que $Q = x^2 - 2$ *é um polinômio-chave para* μ'.

▼

Observação 2.7. *Se para um dado* $\epsilon \in \Gamma'$ *existe um polinômio* $f \in \mathbb{K}[x]$ *tal que* $\epsilon(f) \geq \epsilon$, *então existe um polinômio-chave* Q *tal que* $\epsilon(Q) \geq \epsilon$. *De fato, basta tomar* Q *um polinômio mônico de menor grau dentre os polinômios* f *com* $\epsilon(f) \geq \epsilon$. *Assim, para qualquer* $g \in \mathbb{K}[x]$ *se* $\epsilon(g) \geq \epsilon(Q)$, *então* $\epsilon(g) \geq \epsilon$ *logo, pela minimalidade do grau de* Q, $\deg(g) \geq \deg(Q)$.

▼

Observação 2.8. *Se* Q *é um polinômio-chave de nível* $\epsilon := \epsilon(Q) \in \Gamma_{\mathbb{Q}}$, *então para todo* $f \in \mathbb{K}[x]$ *com* $\deg(f) < \deg(Q)$ *e para todo* $k \in \mathbb{N}_0$ *temos*

$$\mu(\partial_k f) > \mu(f) - k\epsilon.$$

De fato, da definição de $\epsilon(f)$, *para os naturais* k *tais que* $\mu(\partial_k f) \neq \infty$ *temos*

$$\frac{\mu(f) - \mu(\partial_k f)}{k} \leq \epsilon(f) < \epsilon,$$

o que implica $\mu(\partial_k f) > \mu(f) - k\epsilon$. *Para os naturais* k *tais que* $\mu(\partial_k f) = \infty$ *e para* $k = 0$, *o resultado é imediato.*

▼

A definição de $\epsilon(f)$ não é natural em um primeiro momento. No entanto, como veremos na próxima seção, ela nos permite provar certos resultados iniciais sobre polinômios-chaves de maneira explícita. Mesmo assim, vamos atrás de uma forma mais simples de ver o valor $\epsilon(f)$ definido anteriormente.

Seja $\overline{\mathbb{K}}$ um fecho algébrico de $\mathbb{K}$ fixado. Suponhamos que exista uma valorização $\overline{\mu}$ que estenda μ para $\overline{\mathbb{K}}[x]$. Conforme podemos ver na Proposição D.11 no Apêndice D, o grupo de valores de $\overline{\mu}$, que denotaremos $\overline{\mu}(\overline{\mathbb{K}}[x])$, é isomorfo a $\Gamma_{\mathbb{Q}}$.

Definição 2.9. *Seja $f \in \mathbb{K}[x]$ um polinômio não nulo.*

- *Se* $\deg(f) > 0$, *então*

$$\delta(f) := \max\{\overline{\mu}(x-a) \mid a \in \overline{\mathbb{K}} \text{ e } f(a) = 0\}.$$

- *Se* $\deg(f) = 0$, *então* $\delta(f) := -\infty$.

Uma raiz $a \in \overline{\mathbb{K}}$ de f tal que $\delta(f) = \overline{\mu}(x-a)$ é chamada ***raiz otimizadora*** *de f.*

■

Observação 2.10. *Suponhamos* $\deg(f) > 0$. *Se $f \in \operatorname{supp}(\mu)$, então $\delta(f) = \infty$, pois ao menos uma raiz a de f é tal que $\overline{\mu}(x-a) = \infty$. Por outro lado, se $f \notin \operatorname{supp}(\mu)$, então $\delta(f) \in \overline{\mu}(\overline{\mathbb{K}}[x])$.*

▼

Quando $\deg(f) = 0$ temos que $\delta(f) = -\infty = \epsilon(f)$. A partir da Observação 2.10, vemos que $\delta(f) = \infty = \epsilon(f)$ quando $f \in \operatorname{supp}(\mu)$. No Apêndice G, que trata sobre Polígonos de Newton, apresentaremos uma demonstração de que $\delta(f) = \epsilon(f)$ também quando $\deg(f) > 0$ e $f \notin \operatorname{supp}(\mu)$, considerando $\delta(f)$ em $\Gamma_{\mathbb{Q}}$. Assumiremos essa igualdade neste e nos próximos capítulos. Vejamos abaixo um exemplo que ilustra essa igualdade.

Exemplo 2.11. *Consideremos o corpo das séries de Laurent $\mathbb{K}((t^{\mathbb{Z}})) = \mathbb{K}((t))$ do Exemplo 1.10, com $\mathbb{K}$ algebricamente fechado e de característica zero. Um fecho algébrico para tal corpo é o corpo das séries de Puiseux $\bigcup_{n\in\mathbb{N}} \mathbb{K}((t^{\frac{1}{n}})) \subset \mathbb{K}((t^{\mathbb{Q}}))$ (ROND, 2017, p. 2). Consideremos as valorizações t-ádicas ν_t em $\mathbb{K}((t^{\mathbb{Z}}))$ e μ_t em $\mathbb{K}((t^{\mathbb{Q}}))$, cujos grupos de valores são $\mathbb{Z}$ e $\mathbb{Q}$, respectivamente. No anel de polinômios $\mathbb{K}((t^{\mathbb{Z}}))[x]$, tomemos, para $\gamma = \frac{1}{2}$, a valorização monomial*

$$\nu_\gamma\left(\sum_{i=0}^{n} a_i x^i\right) := \min_{0\le i\le n}\left\{\nu_t(a_i) + i\frac{1}{2}\right\}.$$

De maneira análoga, para $\gamma = \frac{1}{2}$, tomamos a valorização monomial μ_γ em $\mathbb{K}((t^{\mathbb{Q}}))[x]$. Temos que μ_γ é uma extensão de ν_γ para $\mathbb{K}((t^{\mathbb{Q}}))[x]$, pois μ_t é uma extensão de ν_t para $\mathbb{K}((t^{\mathbb{Q}}))$.

Seja $f(x) = x^2 - t = (x - t^{\frac{1}{2}})(x + t^{\frac{1}{2}}) \in \mathbb{K}((t^{\mathbb{Z}}))$. Temos

$$\mu_\gamma(f) = \nu_\gamma(f) = \min\left\{\nu_t(t) + 0\frac{1}{2}, \nu_t(0) + 1\frac{1}{2}, \nu_t(1) + 2\frac{1}{2}\right\}$$

$$= \min\{1, \infty, 1\} = 1.$$

Vamos calcular $\epsilon(f)$. Como $\partial_1 f(x) = 2x$, $\partial_2 f(x) = 1$ e $\nu_\gamma(2x) = \frac{1}{2}, \nu_\gamma(1) = 0$, segue que

$$\begin{aligned}\epsilon(f) &= \max\left\{\frac{\nu_\gamma(f) - \nu_\gamma(\partial_1 f)}{1}, \frac{\nu_\gamma(f) - \nu_\gamma(\partial_2 f)}{2}\right\} \\ &= \max\left\{\frac{1-\frac{1}{2}}{1}, \frac{1-0}{2}\right\} \\ &= \frac{1}{2}.\end{aligned}$$

Vamos agora calcular $\delta(f)$. Como

$$\mu_\gamma(x - t^{\frac{1}{2}}) = \min\left\{\mu_t(-t^{\frac{1}{2}}), \mu_t(1) + \frac{1}{2}\right\} = \frac{1}{2} = \mu_\gamma(x + t^{\frac{1}{2}}),$$

segue que

$$\delta(f) = \max\{\mu_\gamma(x + t^{\frac{1}{2}}), \mu_\gamma(x - t^{\frac{1}{2}})\} = \frac{1}{2}.$$

Portanto, $\epsilon(f) = \delta(f)$.

▼

De imediato, tiramos da igualdade entre $\epsilon(f)$ e $\delta(f)$ que este último não depende da extensão $\overline{\mu}$ que tomamos para $\overline{\mathbb{K}}[x]$, pois $\epsilon(f)$ depende apenas de μ. Essa igualdade será muito importante neste e nos próximos capítulos. Um exemplo de seu uso está na demonstração da seguinte propriedade dos polinômios-chaves, que será apresentada após um lema.

Lema 2.12. *Para $f, g \in \mathbb{K}[x]$, temos $\delta(fg) = \max\{\delta(f), \delta(g)\}$. Como consequência, temos $\epsilon(fg) = \max\{\epsilon(f), \epsilon(g)\}$.*

Demonstração: Se $\deg(f) = 0$ ou $\deg(g) = 0$, digamos $\deg(f) = 0$, então $\delta(fg) = \delta(g) = \max\{\delta(f), \delta(g)\}$, pois $\delta(f) = -\infty$.

Suponhamos $\deg(f), \deg(g) > 0$. Se $fg \in \text{supp}(\mu)$, então $f \in \text{supp}(\mu)$ ou $g \in \text{supp}(\mu)$. Logo, $\delta(fg) = \infty = \max\{\delta(f), \delta(g)\}$.

Por fim, suponhamos $fg \notin \text{supp}(\mu)$. Seja $a \in \overline{\mathbb{K}}$ uma raiz otimizadora de fg. Então $f(a)g(a) = 0$. Logo, $f(a) = 0$ ou $g(a) = 0$. Digamos que $f(a) = 0$. Como temos que $\delta(fg) = \mu(x - a)$ é o maior dentre todos os $\mu(x - a')$ tais que a' é raiz de fg, em particular segue que $\delta(f) = \mu(x - a) = \delta(fg)$ e $\delta(f) \geq \delta(g)$, donde segue o resultado.

■

Proposição 2.13. *Todo polinômio-chave Q não constante é irredutível.*

Demonstração: Suponhamos Q redutível, ou seja, podemos escrever $Q = fg$, em que $0 < \deg(f), \deg(g) < \deg(Q)$. Pelo Lema 2.12, $\epsilon(Q) = \max\{\epsilon(f), \epsilon(g)\}$. Digamos $\epsilon(Q) = \epsilon(f) \geq \epsilon(g)$. No entanto, isso significa que temos $\deg(g) < \deg(Q)$ e $\epsilon(g) = \epsilon(Q)$, contradizendo a definição de polinômio-chave. Portanto Q deve ser irredutível.

■

Na próxima seção, veremos como construir valorizações em $\mathbb{K}[x]$ a partir de um polinômio-chave.

2.2 Polinômios-chaves e truncamentos

Sejam $f, q \in \mathbb{K}[x]$ polinômios com q mônico não constante. Consideremos a q-expansão de f como na definição 1.25, isto é, a expressão

$$f = \sum_{i=0}^{r} f_i q^i$$

em que para cada i, $0 \leq i \leq r$, temos $\deg(f_i) < \deg(q)$. Chamemos cada f_i de coeficiente da q-expansão de f.

Definição 2.14. *Seja μ uma valorização em $\mathbb{K}[x]$. Para um polinômio $q \in \mathbb{K}[x]$, o **q-truncamento** de μ é definido como*

$$\mu_q(f) := \min_{0 \leq i \leq r} \{\mu(f_i q^i)\}$$

em que f_i, $0 \leq i \leq r$, são os coeficientes da q-expansão de f.

■

Exemplo 2.15. *Usando o Axioma $(V2)$, vemos que $\mu_q(f) \leq \mu(f)$ para todo $f \in \mathbb{K}[x]$.*

▼

Exemplo 2.16. *Quando $q = x$, vemos que o q-truncamento de μ é a valorização monomial ν_γ, conforme definida na Seção 1.4 com $\gamma = \mu(x)$. Mais geralmente, para $q = x - a$, a q-expansão de um polinômio f é a sua expressão de Taylor em torno de a:*

$$f(x) = \sum_{i=0}^{r} \partial_i f(a)(x-a)^i.$$

Denotando $\mu(\partial_i f(a)) = \beta_i$ e $\mu(x-a) = \gamma$, temos

$$\mu_q(f) = \min_{0\leq i\leq r}\{\mu(\partial_i f(a)(x-a)^i)\} = \min_{0\leq i\leq r}\{\beta_i + i\gamma\}.$$

Isto é, neste caso, podemos ver μ_q como uma valorização monomial.

▼

Exemplo 2.17. *Seja μ' a valorização do Exemplo 2.6, definida como*

$$\mu'(f) := \min_{0\leq i\leq r}\left\{\mu(f_i) + i\frac{3}{2}\right\},$$

em que $f = f_0 + f_1Q + \ldots + f_rQ^r$ é a Q-expansão de f e μ é a valorização monomial definida a partir de $a = 0$, $\gamma = \frac{1}{2}$ e ν^2. Vemos que $\mu'_Q = \mu'$.

▼

Como vimos anteriormente, para $q = x - a$, com $a \in \mathbb{K}$, o q-truncamento de μ é uma valorização. No entanto, o exemplo a seguir nos mostra que, se tomarmos um polinômio q qualquer, então o truncamento μ_q pode não ser uma valorização.

Exemplo 2.18. *Consideremos uma valorização μ em $\mathbb{K}[x]$ tal que $\mu(x) = \mu(a) = 1 \in \mathbb{Z}$ para algum $a \in \mathbb{K}$ (por exemplo, tome ν^p valorização p-ádica em $\mathbb{Q}$ para algum primo p e μ a valorização monomial em $\mathbb{Q}[x]$ definida a partir de ν^p e $\gamma = 1$. Assim, $\mu(x) = 1$ e $\mu(p) = \nu^p(p) = 1$). Seja $q(x) = x^2 + 1$. Observemos que a q-expansão de $x^2 - a^2$ é*

$$x^2 - a^2 = (x^2 + 1) - (a^2 + 1).$$

Logo,

$$\mu_q(x^2 - a^2) = \min\{\mu(x^2 + 1), \mu(a^2 + 1)\} = 0,$$

pois $\mu(x^2) = 2 > 0 = \mu(1)$ e $\mu(a^2) = 2 > 0 = \mu(1)$ implicam $\mu(x^2 + 1) = 0 = \mu(a^2 + 1)$.

Por outro lado,

$$\mu_q(x + a) = \mu(x + a) \geq \min\{\mu(x), \mu(a)\} = 1$$

e o mesmo vale para $\mu_q(x - a)$. Portanto,

$$\mu_q((x - a)(x + a)) = \mu_q(x^2 - a^2) = 0 < 1 + 1 \leq \mu_q(x - a) + \mu_q(x + a),$$

o que mostra que μ_q não satisfaz $(V1)$. Logo, não é valorização.

▼

Vamos mostrar no Teorema 2.23 que se q é um polinômio-chave, então μ_q é uma valorização. Para isso, apresentaremos a seguir diversas propriedades dos polinômios-chaves e dos truncamentos.

Seja f um polinômio com $\epsilon(f) \in \Gamma_{\mathbb{Q}}$. Definimos

$$I(f) := \left\{ k \in \mathbb{N} \,\middle|\, \frac{\mu(f) - \mu(\partial_k f)}{k} = \epsilon(f) \right\} \text{ e } b(f) := \min\{k \mid k \in I(f)\}.$$

Lema 2.19. *Seja Q um polinômio-chave com $\epsilon = \epsilon(Q) \in \Gamma_{\mathbb{Q}}$. Sejam $f, g \in \mathbb{K}[x]$ tais que*

$$\deg(f) < \deg(Q) \text{ e } \deg(g) < \deg(Q).$$

Para qualquer $k \in \mathbb{N}$, as seguintes afirmações são satisfeitas.

1. *Temos $\mu(\partial_k(fg)) > \mu(fg) - k\epsilon$.*
2. *Se $\mu_Q(fQ + g) < \mu(fQ + g)$ e $k \in I(Q)$, então $\mu(\partial_k(fQ + g)) = \mu(fQ) - k\epsilon$.*

Demonstração:

1. Como $\deg(f) < \deg(Q)$ e $\deg(g) < \deg(Q)$, já vimos na Observação 2.8 que

$$\mu(\partial_j f) > \mu(f) - j\epsilon \text{ e } \mu(\partial_j g) > \mu(g) - j\epsilon$$

para todo $j \in \mathbb{N}$. Como

$$\partial_k(fg) = \sum_{j=0}^{k} (\partial_j f)(\partial_{k-j} g),$$

segue que

$$\mu(\partial_k(fg)) \geq \min_{0 \leq j \leq k} \{\mu(\partial_j f) + \mu(\partial_{k-j} g)\} > \mu(fg) - k\epsilon.$$

2. Pela definição, $\mu_Q(fQ + g) = \min\{\mu(g), \mu(fQ)\}$. Se $\mu_Q(fQ + g) < \mu(fQ + g)$, então $\mu(fQ) = \mu(g)$ (pois se $\mu(fQ) \neq \mu(g)$, então teríamos $\mu(fQ + g) = \min\{\mu(g), \mu(fQ)\}$, o que nos levaria a uma contradição). Assim,

$$\mu(\partial_k g) > \mu(g) - k\epsilon = \mu(fQ) - k\epsilon.$$

Para todo $j \in \mathbb{N}$, temos pelo Item 1 que

$$\mu((\partial_j f)(\partial_{k-j} Q)) = \mu(\partial_j f) + \mu(\partial_{k-j} Q) > \mu(f) - j\epsilon + \mu(Q) - (k - j)\epsilon = \mu(fQ) - k\epsilon.$$

Ainda, para $k \in I(Q)$ temos

$$\mu(\partial_k Q) = \mu(Q) - k\epsilon.$$

Logo,

$$\mu(f\partial_k Q) = \mu(f) + \mu(\partial_k Q) = \mu(f) + \mu(Q) - k\epsilon = \mu(fQ) - k\epsilon.$$

Portanto, para $k \in I(Q)$,

$$\mu(\partial_k(fQ+g)) = \mu\left(f\partial_k Q + \sum_{j=1}^{k}(\partial_j f)(\partial_{k-j}Q) + \partial_k g\right) = \mu(fQ) - k\epsilon.$$

■

Observação 2.20. *O Item* 1 *no lema acima nos fornece outra forma de demonstrar que polinômios-chaves são irredutíveis (independente da noção de* δ*). Suponhamos* Q *um polinômio-chave com* $\epsilon = \epsilon(Q) \in \Gamma_{\mathbb{Q}}$ *e* $Q = fg$*, em que* $0 < \deg(f), \deg(g) < \deg(Q)$*. Pelo Item* 1 *do Lema 2.19, para todo* $k \in \mathbb{N}$*,*

$$\mu(\partial_k Q) = \mu(\partial_k(fg)) > \mu(fg) - k\epsilon = \mu(Q) - k\epsilon.$$

Em particular, para $k \in I(Q)$ *temos*

$$\mu(\partial_k Q) > \mu(Q) - k\epsilon \iff \epsilon > \frac{\mu(Q) - \mu(\partial_k Q)}{k},$$

o que contradiz o fato de termos tomado k *em* $I(Q)$*. Portanto,* Q *deve ser irredutível.*

▼

Lema 2.21. *Seja* Q *um polinômio-chave com* $\epsilon = \epsilon(Q) \in \Gamma_{\mathbb{Q}}$*. Se* $f \in \mathbb{K}[x]$ *é tal que* $\epsilon(f) < \epsilon$ *e* $f = aQ + r$*, com* $\deg(r) < \deg(Q)$ *e* $r \neq 0$*, então*

$$\mu(r) = \mu(f) < \mu(aQ).$$

Demonstração: Como $\epsilon(f) < \epsilon$, certamente $f \notin \operatorname{supp}(\mu)$. Se f for constante, então o resultado segue. Suponhamos então $f \notin \operatorname{supp}(\mu)$ e não constante. Tomemos $l \in I(aQ)$ qualquer. Convencionamos

$$\frac{\mu(f) - \mu(\partial_l f)}{l} = -\infty$$

quando $\mu(\partial_l f) = \infty$. Temos

$$\epsilon > \epsilon(f) = \max_{1 \leq k \leq \deg(f)} \left\{ \frac{\mu(f) - \mu(\partial_k f)}{k} \;\middle|\; \mu(\partial_k f) \in \Gamma \right\} \geq \frac{\mu(f) - \mu(\partial_l f)}{l}.$$

Isso implica que $\mu(\partial_l f) > \mu(f) - l\epsilon$. Como $\deg(r) < \deg(Q)$, segue que da Observação 2.8 que

$\mu(\partial_l r) > \mu(r) - l\epsilon$. Pelo Lema 2.12, $\epsilon(aQ) \geq \epsilon$. Portanto,

$$\begin{aligned}\mu(aQ) - l\epsilon &\geq \mu(aQ) - l\epsilon(aQ)\\ &= \mu(\partial_l(aQ))\\ &= \mu(\partial_l(f-r))\\ &= \mu(\partial_l f - \partial_l r)\\ &\geq \min\{\mu(\partial_l f), \mu(\partial_l r)\}\\ &> \min\{\mu(f), \mu(r)\} - l\epsilon.\end{aligned}$$

Assim, $\mu(f-r) = \mu(aQ) > \min\{\mu(f), \mu(r)\}$ e, consequentemente, $\mu(r) = \mu(f) < \mu(aQ)$.

■

Lema 2.22. *Seja Q um polinômio-chave com $\epsilon(Q) \in \Gamma_{\mathbb{Q}}$. Se $h_1, \ldots, h_s$ são polinômios tais que $\deg(h_i) < \deg(Q)$ para todo i, $1 \leq i \leq s$, e*

$$\prod_{i=1}^{s} h_i = aQ + r$$

com $\deg(r) < \deg(Q)$ e $r \neq 0$, então

$$\mu(r) = \mu\left(\prod_{i=1}^{s} h_i\right) < \mu(aQ).$$

Demonstração: Como $\deg(h_i) < \deg(Q)$ para todo i, $1 \leq i \leq s$, segue que $\epsilon(h_i) < \epsilon$. Por indução, vemos pelo Lema 2.12 que

$$\epsilon(h_1 \cdots h_s) = \max_{1 \leq i \leq s}\{\epsilon(h_i)\} < \epsilon.$$

O resultado segue aplicando o Lema 2.21.

■

Mostremos agora que o truncamento em um polinômio-chave é uma valorização.

Teorema 2.23. *Se Q é um polinômio-chave com $\epsilon(Q) \in \Gamma_{\mathbb{Q}}$, então μ_Q é uma valorização.*

Demonstração: Consideremos $\gamma = \mu(Q)$ e $\mu' = \mu_Q$. Na Proposição 1.28, mostramos que μ' satisfaz os Axiomas $(V1)$ e $(V2)$ se, para $d = \deg(Q)$, a aplicação $\mu : \mathbb{K}[x] \longrightarrow \Gamma_\infty$ é tal que

- μ satisfaz $(V2)$,
- para todo $h_1, h_2 \in \mathbb{K}[x]_d$ temos $\mu(h_1 h_2) = \mu(h_2) + \mu(h_2)$ e
- sempre que $h_1 h_2 = aQ + c$ com $h_1, h_2, c \in \mathbb{K}[x]_d$ vale $\mu(c) = \mu(h_1 h_2) < \mu(a) + \gamma$.

Segue que μ satisfaz $(V1)$ e $(V2)$, pois é valorização. Uma vez que Q é irredutível, $h_1h_2 = aQ + c$, com $h_1, h_2 \in \mathbb{K}[x]_d$, implica $c \neq 0$. Logo, pelo Lema 2.22,

$$\mu(c) = \mu(h_1h_2) < \mu(aQ) = \mu(a) + \gamma.$$

Portanto, $\mu' = \mu_Q$ satisfaz $(V1)$ e $(V2)$. O Axioma $(V3)$ segue direto da definição de μ_Q, pois $\mu_Q(1) = \mu(1) = 0$ e $\mu_Q(0) = \mu(0) = \infty$.

■

Proposição 2.24. *Se Q é um polinômio-chave com $\epsilon(Q) \in \Gamma_{\mathbb{Q}}$, então a valorização μ_Q é de Krull em $\mathbb{K}[x]$. Em particular, μ_Q se estende de forma única para $\mathbb{K}(x)$.*

Demonstração: Suponhamos por contradição que exista $f \in \mathbb{K}[x]$ tal que $\mu_Q(f) = \infty$ e $f \neq 0$. Sejam $f_0, f_1, \ldots, f_s \in \mathbb{K}[x]$ os coeficientes da Q-expansão de f. Como $f \neq 0$, ao menos um coeficiente f_i é também não nulo. Como por definição

$$\mu_Q(f) = \min_{0 \leq i \leq s} \{\mu(f_i) + i\mu(Q)\}$$

e $\mu(Q) < \infty$, temos que $\mu_Q(f) = \infty$ implica $\mu(f_i) = \infty$ para todo i. Assim, por definição $\epsilon(f_i) = \infty$ para $f_i \neq 0$. Mas, $\deg(f_i) < \deg(Q)$ para cada $f_i \neq 0$, pois este é um coeficiente da Q-expansão de f. Logo, deveríamos ter para $f_i \neq 0$ que $\epsilon(f_i) < \epsilon(Q) \in \Gamma_{\mathbb{Q}}$, pois Q é polinômio-chave, o que é uma contradição. Assim, $\text{supp}(\mu_Q) = \{0\}$.

■

Para terminarmos a seção, veremos que não vale a recíproca do Teorema 2.23, isto é, não é verdade que μ_q é valorização somente quando q é polinômio-chave. Para isso, provaremos o lema abaixo.

Lema 2.25. *Seja μ uma valorização em $\mathbb{K}[x]$. Seja q um polinômio tal que μ_q é valorização e $\mu_q = \mu$. Então $\mu_{q^2} = \mu$.*

Demonstração: Seja $f \in \mathbb{K}[x]$ um polinômio e escrevemos sua q-expansão

$$f = f_0 + f_1q + \ldots + f_rq^r.$$

Se r for par, então acrescentaremos $f_{r+1}q^{r+1}$ à expansão com $f_{r+1} = 0$. Desse modo, podemos supor que r é ímpar. Vemos que a q^2-expansão de f é

$$f = (f_0 + f_1q) + (f_2 + f_3q)q^2 + \ldots + (f_{r-1} + f_rq)(q^2)^{\frac{r-1}{2}}.$$

Por hipótese, $\mu = \mu_q$. Logo,

$$\mu((f_{2i} + f_{2i+1}q)q^{2i}) = \min\{\mu(f_{2i}q^{2i}), \mu(f_{2i+1}q^{2i+1})\}$$

e, com isso,

$$\begin{aligned}\mu_{q^2}(f) &= \min_{0\leq i\leq \frac{r-1}{2}}\{\mu((f_{2i} + f_{2i+1}q)q^{2i})\} \\ &= \min_{0\leq i\leq \frac{n-1}{2}}\{\min\{\mu(f_{2i}q^{2i}), \mu(f_{2i+1}q^{2i+1})\}\} \\ &= \mu_q(f) = \mu(f).\end{aligned}$$

■

Corolário 2.26. *Existem uma valorização μ em $\mathbb{K}[x]$ e um polinômio $q \in \mathbb{K}[x]$ tais que μ_q é valorização em $\mathbb{K}[x]$ mas q não é polinômio-chave.*

Demonstração: Seja ν uma valorização não trivial em $\mathbb{K}$ e consideremos $\mu = \nu_\gamma$ uma valorização monomial em $\mathbb{K}[x]$. Assim, para $f = f_0 + f_1x + \ldots + f_rx^r$, temos

$$\mu_x(f) = \min_{0\leq i\leq r}\{\mu(f_ix^i)\} = \min_{0\leq i\leq r}\{\nu_\gamma(f_ix^i)\} = \min_{0\leq i\leq r}\{\nu(f_i) + i\gamma\} = \nu_\gamma(f) = \mu(f).$$

Pelo lema anterior, temos $\mu = \mu_{x^2}$. Como polinômios-chaves são irredutíveis, temos que $q = x^2$ não é polinômio-chave e μ_q é valorização, como queríamos.

■

2.3 Propriedades dos polinômios-chaves

Dedicaremos esta seção a provar resultados técnicos sobre polinômios-chaves que serão úteis mais adiante. Algumas notações também serão introduzidas ao longo dos resultados.

Iniciamos dando uma forma geral para os elementos de $I(Q)$. Antes, vejamos dois lemas técnicos. Seja ν uma valorização em $\mathbb{K}$. Seja $n \in \mathbb{N}$ e tomemos em $\mathbb{K}$ o elemento $n := n \cdot 1$, em que 1 representa a unidade de $\mathbb{K}$. Como $\nu(n) = \nu(1 + \ldots + 1) \geq \min\{\nu(1), \ldots, \nu(1)\} = 0$, temos que $n \in \mathcal{O}_\nu$. Consideremos a projeção $\overline{n}$ de n no corpo de resíduos $\mathbb{K}\nu$.

Lema 2.27. *Se $\mathrm{char}(\mathbb{K}\nu) = 0$, então $\nu(n) = 0$. Se $\mathrm{char}(\mathbb{K}\nu) = p > 0$, então $\overline{n} = \overline{0}$ se, e somente se, $p \mid n$. Consequentemente, $\nu(n) = 0$ se, e somente se, $p \nmid n$.*

Demonstração: Se $\mathrm{char}(\mathbb{K}\nu) = 0$, então $\overline{n} = n\overline{1} \neq \overline{0}$ em $\mathbb{K}\nu$, ou seja, $n \notin \mathfrak{m}_\nu$, o que implica $\nu(n) = 0$. Se $\mathrm{char}(\mathbb{K}\nu) = p > 0$, então veremos que $\overline{n} = \overline{0}$ se, e somente se, $p \mid n$.

($\Leftarrow$) Temos que $p \mid n$ implica que existe $m \in \mathbb{N}$ tal que $n = pm$. Com isso, $\overline{n} = \overline{pm} = \overline{p}\,\overline{m} = \overline{0}\overline{m} = \overline{0}$.

($\Rightarrow$) Se $\overline{n} = \overline{0}$, então suponhamos, buscando por uma contradição, que $p \nmid n$. Logo, $n = pq + r$ com $0 < r < p$. Assim,

$$\overline{n} = \overline{pq + r} = \overline{p}\,\overline{q} + \overline{r} = \overline{r}.$$

Isso implica que $r\overline{1} = \overline{r} = \overline{n} = \overline{0}$, contradizendo $\mathrm{char}(\mathbb{K}\nu) = \mathrm{p} > \mathrm{r}$. Portanto, $\overline{n} = \overline{0}$ se, e somente se, $p \mid n$. Consequentemente,

$$\nu(n) = 0 \Longleftrightarrow n \notin \mathfrak{m}_\nu \Longleftrightarrow \overline{n} \neq \overline{0} \Longleftrightarrow p \nmid n.$$

■

Lema 2.28. *Sejam p^n uma potência de um número primo p e r um natural tal que* $\mathrm{mdc}(p^n, r) = 1$. *Então, para todo $t \in \mathbb{N} \cup \{0\}$,*

$$p^n \nmid \binom{p^{nt}r}{p^{nt}}.$$

Demonstração: Temos

$$\begin{aligned}\binom{p^{nt}r}{p^{nt}} &= \frac{(p^{nt}r)!}{(p^{nt}r - p^{nt})!p^{nt}!} \\ &= \frac{p^{tn}r(p^{tn}r - 1)\cdots(p^{tn}r - p^{tn} + 1)}{p^{tn}(p^{tn} - 1)\cdots 1} \\ &= r\frac{(p^{tn}r - 1)\cdots(p^{tn}r - p^{tn} + 1)}{(p^{tn} - 1)\cdots 1}.\end{aligned}$$

Consideremos a fração

$$\frac{(p^{tn}r - 1)\cdots(p^{tn}r - p^{tn} + 1)}{(p^{tn} - 1)\cdots 1}. \tag{2.1}$$

Seja $J = \{m \in \mathbb{N} \mid p^n \mid m \text{ e } 1 \leq m < p^{tn}\}$. Os fatores no numerador de (2.1) que são divisíveis por p^n são os fatores da forma $p^{tn}r - m$ com $m \in J$. Por outro lado, os fatores no denominador de (2.1) que são divisíveis por p são da forma $p^{tn} - m$ com $m \in J$. Para um dado $m \in J$, escrevemos $m = p^l s$ com $p^n \nmid s$. Então,

$$p^{tn}r - m = p^l(p^{tn-l}r - s) \quad \text{e} \quad p^{tn} - m = p^l(p^{tn-l} - s).$$

Como $p^n \nmid s$, concluímos que $p^n \nmid p^{tn-l}r - s$ e $p^n \nmid p^{tn-l} - s$. Assim, todas as potências de p^n que aparecem no numerador de (2.1) também aparecem em seu denominador, e por isso elas se cancelam. Como $\mathrm{mdc}(p^n, r) = 1$, concluímos que p^n não divide o binomial.

■

Chamaremos de **característica de expoente** o número p definido por

$$p = \begin{cases} 1 & \text{se } \operatorname{char}(\mathbb{K}\nu) = 0, \\ \operatorname{char}(\mathbb{K}\nu) & \text{se } \operatorname{char}(\mathbb{K}\nu) > 0. \end{cases}$$

Para uma valorização μ em $\mathbb{K}[x]$, a característica de expoente de μ é definida como a característica de expoente de $\mu|_{\mathbb{K}}$. Para simplificar a notação, escreveremos $\mathbb{K}\mu$ para representar o corpo de resíduos de $\mu|_{\mathbb{K}}$. Veremos na proposição abaixo que os elementos de $I(Q)$ são potências da característica de expoente de μ.

Proposição 2.29. *Seja μ uma valorização em $\mathbb{K}[x]$. Seja Q um polinômio-chave para μ com $\epsilon = \epsilon(Q) \in \Gamma_{\mathbb{Q}}$. Todos os elementos de $I(Q)$ são potências da característica de expoente p de μ.*

Demonstração: Seja $k \in I(Q)$ e suponhamos, por contradição, que $k = p^t r$ com $r > 1$ e $\operatorname{mdc}(p, r) = 1$. Se $p = 1$, então $\operatorname{char}(\mathbb{K}\mu) = 0$. Logo, pelo Lema 2.27 segue que

$$\mu\left(\binom{k}{p^t}\right) = \mu(r) = 0.$$

Por outro lado, se $p > 1$, então o Lema 2.28 nos diz que $p \nmid \binom{k}{p^t}$. Pelo Lema 2.27, temos

$$\mu\left(\binom{k}{p^t}\right) = 0.$$

Sabemos que

$$\binom{k}{p^t}\partial_k f = \partial_{p^t}\partial_{k'} f$$

para todo $f \in \mathbb{K}[x]$ (ver Apêndice F), em que $k' = k - p^t$. Logo, temos

$$\mu(\partial_{k'}Q) - \mu(\partial_k Q) = \mu(\partial_{k'}Q) - \mu\left(\binom{k}{p^t}\partial_k Q\right) = \mu(\partial_{k'}Q) - \mu(\partial_{p^t}(\partial_{k'}Q)) \leq p^t\epsilon(\partial_{k'}Q) < p^t\epsilon,$$

pois, sendo Q um polinômio-chave, vale que $\deg(\partial_{k'}Q) < \deg(Q)$ implica $\epsilon(\partial_{k'}Q) < \epsilon$. Portanto,

$$k\epsilon = \mu(Q) - \mu(\partial_k Q) = \mu(Q) - \mu(\partial_{k'}Q) + \mu(\partial_{k'}Q) - \mu(\partial_k Q) < k'\epsilon + p^t\epsilon = k\epsilon,$$

o que é uma contradição. Dessa forma, k deve ser uma potência de p.

■

Seja Q um polinômio-chave fixado e tomemos $h \in \mathbb{K}[x]$ com $\deg(h) < \deg(Q)$. Para cada $k, n \in \mathbb{N}$, aplicando as regras da derivada de Hasse obtemos

$$\partial_k(hQ^n) = \sum_{k_0+\ldots+k_r=k} T_k(k_0, \ldots, k_r)$$

com $k_0 \geq 0$, $k_i > 0$ se $i > 0$ e

$$T_k(k_0, \ldots, k_r) = \partial_{k_0} h \left(\prod_{i=1}^{r} \partial_{k_i} Q \right) Q^{n-r}. \tag{2.2}$$

Lema 2.30. *Sejam Q um polinômio-chave, $h \in \mathbb{K}[x]$ com $\deg(h) < \deg(Q)$ e $\epsilon := \epsilon(Q) \in \Gamma_{\mathbb{Q}}$. Para cada $k, n \in \mathbb{N}$ temos*

$$\mu_Q(T_k(k_0, \ldots, k_r)) \geq \mu(hQ^n) - k\epsilon.$$

Além disso, se $k_0 > 0$ ou $k_i \notin I(Q)$ para algum i, $1 \leq i \leq r$, então

$$\mu_Q(T_k(k_0, \ldots, k_r)) > \mu(hQ^n) - k\epsilon.$$

Demonstração: Como Q é polinômio-chave e $\deg(h) < \deg(Q)$, temos $\epsilon(h) < \epsilon$. Portanto, se $k_0 > 0$, então temos pelo Lema 2.19, Item 1,

$$\mu(\partial_{k_0} h) \geq \mu(h) - k_0 \epsilon(h) > \mu(h) - k_0 \epsilon.$$

Pela definição de ϵ, sabemos que $\mu(\partial_{k_i} Q) \geq \mu(Q) - k_i \epsilon$ para todo i, $1 \leq i \leq r$. Se $k_i \notin I(Q)$, então

$$\mu(\partial_{k_i} Q) > \mu(Q) - k_i \epsilon.$$

Temos também $\mu_Q(\partial_{k_0} h) = \mu(\partial_{k_0} h)$ e $\mu_Q(\partial_{k_i} Q) = \mu(\partial_{k_i} Q)$, pois o grau de $\partial_{k_0} h$ e o grau de $\partial_{k_i} Q$ são estritamente menores do que o grau de Q. Assim,

$$\begin{aligned}
\mu_Q(T_k(k_0, \ldots, k_r)) &= \mu_Q \left((\partial_{k_0} h) \left(\prod_{i=1}^{r} \partial_{k_i} Q \right) Q^{n-r} \right) \\
&= \mu_Q(\partial_{k_0} h) + \sum_{i=1}^{r} \mu_Q(\partial_{k_i} Q) + (n-r)\mu_Q(Q) \\
&\geq \mu(h) - k_0 \epsilon + \sum_{i=1}^{r} (\mu(Q) - k_i \epsilon) + (n-r)\mu(Q) \\
&\geq \mu(hQ^n) - k\epsilon.
\end{aligned}$$

Além disso, se $k_0 > 0$ ou $k_i \notin I(Q)$ para algum i, então a desigualdade acima é estrita.

■

Corolário 2.31. *Sejam Q um polinômio-chave, $h \in \mathbb{K}[x]$ com $\deg(h) < \deg(Q)$ e $\epsilon := \epsilon(Q) \in \Gamma_{\mathbb{Q}}$. Então, para todo $k, n \in \mathbb{N}$, temos*

$$\mu_Q(\partial_k(hQ^n)) \geq \mu(hQ^n) - k\epsilon.$$

Demonstração: Pelo Axioma $(V2)$ e pelo lema acima, temos

$$\begin{aligned}\mu_Q(\partial_k(hQ^n)) &= \mu_Q\left(\sum_{k_0+\ldots+k_r=k} T_k(k_0,\ldots,k_r)\right)\\ &\geq \min\{\mu_Q(T_k(k_0,\ldots,k_r))\}\\ &\geq \mu(hQ^n) - k\epsilon.\end{aligned}$$

■

Para $f, q \in \mathbb{K}[x]$ polinômios com q não constante, seja $f = f_0 + f_1 q + \ldots + f_r q^r$ a q-expansão de f. Definimos

$$S_q(f) := \{i \in \{0,\ldots,r\} \mid \mu(f_i q^i) = \mu_q(f)\}.$$

Proposição 2.32. *Seja Q um polinômio-chave e denotemos $\epsilon := \epsilon(Q) \in \Gamma_{\mathbb{Q}}$. Para todo $f \in \mathbb{K}[x]$, as seguintes afirmações são satisfeitas.*

1. *Para cada $k \in \mathbb{N}$ temos*
$$\frac{\mu_Q(f) - \mu_Q(\partial_k f)}{k} \leq \epsilon. \tag{2.3}$$
2. *Se $S_Q(f) \neq \{0\}$, então vale a igualdade em (2.3) para algum $k \in \mathbb{N}$.*
3. *Se para algum $k \in \mathbb{N}$ vale a igualdade em (2.3) e $\mu_Q(\partial_k f) = \mu(\partial_k f)$, então $\epsilon(f) \geq \epsilon$. Se, além disso, $\mu(f) > \mu_Q(f)$, então $\epsilon(f) > \epsilon$.*

Demonstração:

1. Dado $f \in \mathbb{K}[x]$, consideremos sua Q-expansão
$$f = f_0 + f_1 Q \ldots + f_n Q^n.$$
Para cada i, $0 \leq i \leq n$, o Corolário 2.31 nos diz que
$$\mu_Q(\partial_k(f_i Q^i)) \geq \mu(f_i Q^i) - k\epsilon.$$
Portanto,
$$\mu_Q(\partial_k(f)) \geq \min_{0\leq i\leq n}\{\mu_Q(\partial_k(f_i Q^i))\} \geq \min_{0\leq i\leq n}\{\mu(f_i Q^i) - k\epsilon\} = \mu_Q(f) - k\epsilon.$$
Ou seja,
$$\frac{\mu_Q(f) - \mu_Q(\partial_k f)}{k} \leq \epsilon.$$
2. Suponhamos $S_Q(f) \neq \{0\}$ e tomemos $j_0 = \min(S_Q(f) \setminus \{0\})$. Sendo p a característica de expoente de μ, temos $j_0 = p^e l$ para algum $e \in \mathbb{N} \cup \{0\}$ e algum $l \in \mathbb{N}$ com $\mathrm{mdc}(l, p) = 1$. Definimos $k := p^e b(Q)$. Mostraremos que $\mu_Q(\partial_k(f)) = \mu_Q(f) - k\epsilon$.

Pelo Algorítimo da Divisão para polinômios, podemos escrever

$$f_{j_0}(\partial_{b(Q)}Q)^{p^e} = h_1Q + h_2$$

para certos $h_1, h_2 \in \mathbb{K}[x]$ com $h_2 \neq 0$ (pois Q é irredutível, $Q \nmid f_{j_0}$ e $Q \nmid \partial_{b(Q)}$) e $\deg(h_2) < \deg(Q)$. Pelo Lema 2.22,

$$\mu(h_2) = \mu(f_{j_0}(\partial_{b(Q)}Q)^{p^e}).$$

Vejamos que isso implica

$$\mu(h_2Q^{j_0-p^e}) = \mu_Q(f) - k\epsilon.$$

De fato,

$$\begin{aligned}
\mu(h_2Q^{j_0-p^e}) &= \mu(h_2) + \mu(Q^{j_0-p^e}) = \mu(f_{j_0}(\partial_{b(Q)}Q)^{p^e}) + \mu(Q^{j_0-p^e}) \\
&= \mu(f_{j_0}) + p^e\mu(\partial_{b(Q)}Q) + (j_0 - e)\mu(Q) \\
&= \mu(f_{j_0}) + p^e(\mu(Q) - b(Q)\epsilon) + (j_0 - p^e)\mu(Q) \\
&= \mu(f_{j_0}) + j_0\mu(Q) - p^eb(Q)\epsilon \\
&= \mu(f_{j_0}Q^{j_0}) - p^eb(Q)\epsilon = \mu_Q(f) - k\epsilon.
\end{aligned}$$

Sabemos que $\partial_k(f) = \partial_k(f_0) + \partial_k(f_1Q) + \ldots + \partial_k(f_nQ^n)$, devido à linearidade da derivada de Hasse. Para cada $j \notin S_Q(f)$, $0 \leq j \leq n$, temos

$$\mu_Q(\partial_k(f_jQ^j)) \geq \mu(f_jQ^j) - k\epsilon > \mu_Q(f) - k\epsilon.$$

Logo, colocando

$$h_3 = \sum_{j \notin S_Q(f)} \partial_k(f_jQ^j),$$

vemos que $\mu_Q(h_3) > \mu_Q(f) - k\epsilon$.

Podemos escrever cada $\partial_k(f_jQ^j)$ como uma soma de termos da forma $T_k(k_0, \ldots, k_r)$, definidos pela Equação 2.2. Considerando $j \in S_Q(f)$, $0 \leq j \leq n$, separamos os elementos $T_k(k_0, \ldots, k_r)$ da seguintes forma:

- No primeiro caso, $k_0 > 0$ ou $k_i \notin I(Q)$ para algum i. Então teremos $\mu_Q(T_k(k_0, \ldots, k_r)) > \mu_Q(f) - k\epsilon$. Em particular, sendo h_4 a soma de todos os termos $T_k(k_0, \ldots, k_r)$ nessa situação, temos $\mu_Q(h_4) > \mu_Q(f) - k\epsilon$.
- No segundo caso, $k_0 = 0$ e $k_i \in I(Q)$ para todo i, mas $k_{i_0} \neq b(Q)$ para algum i_0. Como $j \in S_Q(f)$, temos $j \geq j_0$. Como $k := p^eb(Q)$, segue que nessa situação temos $r < p^e$. Caso contrário, como $k_i \in I(Q)$, se $r \geq p^e$, então concluiríamos que a soma

$k_0 + \ldots + k_r$ teria como limitante inferior

$$(r-1)b(Q) + k_{i_0} \geq p^e b(Q) - b(Q) + k_{i_0} > p^e b(Q) = k,$$

o que não pode ocorrer. Portanto, podemos escrever

$$T_k(k_0, \ldots, k_r) = (\partial_{k_0} f_j) \left(\prod_{i=1}^{r} \partial_{k_i} Q \right) Q^{j-r} = s Q^{j_0 - p^e + 1}$$

para algum $s \in \mathbb{K}[x]$. Pelo Lema 2.30,

$$\mu_Q(T_k(k_0, \ldots, k_r)) \geq \mu(f_j Q^j) - k\epsilon \geq \mu_Q(f) - k\epsilon.$$

- No terceiro caso, $k_0 = 0$, $k_i = b(Q) \in I(Q)$ para todo i e $j > j_0$. Nessa situação necessariamente $r = p^e$. Assim,

$$T_k(k_0, \ldots, k_r) = f_j \left(\partial_{b(Q)} Q \right)^{p^e} Q^{j-p^e} = s' Q^{j_0 - p^e + 1}$$

para algum $s' \in \mathbb{K}[x]$. Também, $\mu_Q(T_k(k_0, \ldots, k_r)) \geq \mu(f_j Q^j) - k\epsilon \geq \mu_Q(f) - k\epsilon$.

- No quarto e último caso, $k_0 = 0$, $k_i = b(Q) \in I(Q)$ para todo i e $j = j_0$. Temos aqui também $r = p^e$ e, portanto,

$$\begin{aligned} T_k(k_0, \ldots, k_r) &= f_{j_0} (\partial_{b(Q)} Q)^{p^e} Q^{j_0 - p^e} \\ &= (h_1 Q + h_2) Q^{j_0 - p^e} \\ &= h_2 Q^{j_0 - p^e} + h_1 Q^{j_0 - p^e + 1} \end{aligned}$$

Lembramos que o número de vezes que o termo $T_k(k_0, \ldots, k_r)$ aparece em $\partial_k(f_j Q^j)$, neste caso em que $r = p^e$, é igual a $\binom{j_0}{p^e}$.

Assim, podemos escrever

$$\begin{aligned} \partial_k(f) &= \partial_k(f_0) + \partial_k(f_1 Q) + \ldots + \partial_k(f_n Q^n) \\ &= h_3 + h_4 + s Q^{j_0 - p^e + 1} + s' Q^{j_0 - p^e + 1} + \binom{j}{p^e} \left(h_2 Q^{j_0 - p^e} + h_1 Q^{j_0 - p^e + 1} \right) \\ &= \binom{j_0}{p^e} h_2 Q^{j_0 - p^e} + \left(s + s' + \binom{j_0}{p^e} h_1 \right) Q^{j_0 - p^e + 1} + h_3 + h_4. \end{aligned}$$

Se a característica de expoente p for um número primo, então $p \nmid \binom{j_0}{p^e} = \binom{p^e l}{p^e}$ (Lema 2.28). Ou seja, pelo Lema 2.27, seja a característica de expoente igual a 1 ou igual a um número

primo, temos $\mu\left(\binom{j_0}{p^e}\right) = 0$. Logo,

$$\mu\left(\binom{j_0}{p^e} h_2 Q^{j_0-p^e}\right) = \mu_Q(f) - k\epsilon.$$

Assim, como em

$$\binom{j_0}{p^e} h_2 Q^{j_0-p^e} + \left(s + s' + \binom{j_0}{p^e} h_1\right) Q^{j_0-p^e+1}$$

a parcela $\binom{j_0}{p^e} h_2 Q^{j_0-p^e}$ é a única que possui a potência $j_0 - p^e$ de Q e $\deg(h_2) < \deg(Q)$, esta parcela é um dos termos da Q-expansão da soma em destaque acima. Portanto, uma vez que μ_Q é definido como o mínimo dentre o valor das parcelas da Q-expansão, temos

$$\begin{aligned}\mu_Q\left(\binom{j_0}{p^e} h_2 Q^{j_0-p^e} + \left(s + s' + \binom{j_0}{p^e} h_1\right) Q^{j_0-p^e+1}\right) &\leq \mu_Q\left(\binom{j_0}{p^e} h_2 Q^{j_0-p^e}\right) \\ &= \mu_Q(f) - k\epsilon.\end{aligned}$$

Lembrando que $\mu_Q(h_3 + h_4) > \mu_Q(f) - k\epsilon$, temos

$$\begin{aligned}\mu_Q(\partial_k f) &= \mu_Q\left(\binom{j_0}{p^e} h_2 Q^{j_0-p^e} + \left(s + s' + \binom{j_0}{p^e} h_1\right) Q^{j_0-p^e+1}\right) \\ &\leq \mu_Q(f) - k\epsilon.\end{aligned}$$

3. Suponhamos que k seja tal que

$$\frac{\mu_Q(f) - \mu_Q(\partial_k f)}{k} = \epsilon$$

e $\mu_Q(\partial_k f) = \mu(\partial_k f)$. Então,

$$\epsilon(f) \geq \frac{\mu(f) - \mu(\partial_k f)}{k} \geq \frac{\mu_Q(f) - \mu_Q(\partial_k f)}{k} = \epsilon$$

e a desigualdade é estrita se $\mu(f) > \mu_Q(f)$.

■

Proposição 2.33. *Sejam $Q, Q' \in \mathbb{K}[x]$ polinômios-chaves para μ, com $\epsilon(Q), \epsilon(Q') \in \Gamma_{\mathbb{Q}}$.*

1. *Se $\deg(Q) < \deg(Q')$, então $\epsilon(Q) < \epsilon(Q')$.*
2. *Se $\epsilon(Q) < \epsilon(Q')$, então $\mu_Q(Q') < \mu(Q')$.*
3. *Se $\deg(Q) = \deg(Q')$, então*

$$\mu(Q) < \mu(Q') \iff \mu_Q(Q') < \mu(Q') \iff \epsilon(Q) < \epsilon(Q').$$

Demonstração:

1. Segue direto da definição de polinômio-chave.

2. Sejam $\epsilon := \epsilon(Q)$ e $b' := b(Q')$. Pela Proposição 2.32, Item 1, sabemos que

$$\mu_Q(Q') \leq \mu_Q(\partial_{b'}Q') + b'\epsilon.$$

   Como por hipótese $\epsilon(Q) < \epsilon(Q')$, temos

$$\mu(\partial_{b'}Q') + b'\epsilon < \mu(\partial_{b'}Q') + b'\epsilon(Q') = \mu(Q').$$

   Assim, como $\mu_Q(\partial_{b'}Q') \leq \mu(\partial_{b'}Q')$, segue que $\mu_Q(Q') < \mu(Q')$.

3. Suponhamos $\deg(Q) = \deg(Q')$. Como ambos Q e Q' são polinômios mônicos, concluímos que a Q-expansão de Q' é dada por $Q' = (Q' - Q) + Q$. Portanto,

$$\mu_Q(Q') = \min\{\mu(Q), \mu(Q' - Q)\}.$$

   Com isso, concluímos que

$$\mu(Q) < \mu(Q') \iff \mu_Q(Q') < \mu(Q').$$

   Do Item 2, já temos que $\epsilon(Q) < \epsilon(Q')$ implica $\mu_Q(Q') < \mu(Q')$. Para mostrar a outra implicação, suponhamos agora que $\mu_Q(Q') < \mu(Q')$. Vejamos que $S_Q(Q') \neq \{0\}$. De fato, se $S_Q(Q') = \{0\}$, então $\mu(Q' - Q) < \mu(Q)$ e

$$\mu(Q') = \mu(Q' - Q + Q) = \mu(Q' - Q) = \mu_Q(Q'),$$

   o que é uma contradição. Pela Proposição 2.32, Item 2,

$$\frac{\mu_Q(Q') - \mu_Q(\partial_k Q')}{k} = \epsilon(Q)$$

   para algum $k \in \mathbb{N}$. Mas, $\deg(Q) = \deg(Q')$ implica $\deg(\partial_k Q') < \deg(Q)$ e, por isso, $\mu_Q(\partial_k Q') = \mu(\partial_k Q')$. Portanto, pela Proposição 2.32, Item 3, temos $\epsilon(Q) < \epsilon(Q')$.

■

Dado um polinômio-chave Q, definimos

$$\alpha(Q) := \min\{\deg(f) \mid \mu_Q(f) < \mu(f)\}$$

e

$$\Psi(Q) := \{f \in \mathbb{K}[x] \mid f \text{ é mônico, } \mu_Q(f) < \mu(f) \text{ e } \deg(f) = \alpha(Q)\}.$$

Se $\mu_Q = \mu$, então definimos $\alpha(Q) = \infty$ e, por isso, $\Psi(Q) = \emptyset$.

Proposição 2.34. *Se Q é um polinômio-chave, então todo elemento $Q' \in \Psi(Q)$ também é polinômio-chave. Além disso, $\epsilon(Q) < \epsilon(Q')$.*

Demonstração: Seja $Q' \in \Psi(Q)$. Pela definição de $\Psi(Q)$, temos $\mu_Q(Q') < \mu(Q)$. Veremos que isso implica $S_Q(Q') \neq \{0\}$. De fato, escrevendo $Q' = a_0 + a_1Q + \ldots + a_nQ^n$ a Q-expansão de Q', se $S_Q(Q') = \{0\}$, então $\mu(a_0) < \mu(a_iQ^i)$ para todo i, $1 \leq i \leq n$, e

$$\mu(Q') = \mu(a_0 + a_1Q + \ldots + a_nQ^n) = \mu(a_0) = \min_{0\leq i\leq n}\{\mu(a_iQ^i)\} = \mu_Q(Q'),$$

o que é uma contradição. Logo, $S_Q(Q') \neq \{0\}$. Pela Proposição 2.32, Item 2, existe $k \in \mathbb{N}$ tal que $\mu_Q(Q') - \mu_Q(\partial_k Q') = k\epsilon(Q)$. Como $\deg(\partial_k Q') < \deg(Q') = \alpha(Q)$, temos $\mu_Q(\partial_k Q') = \mu(\partial_k Q')$. Assim, pela Proposição 2.32, Item 3, segue que $\epsilon(Q) < \epsilon(Q')$.

Seja agora $f \in \mathbb{K}[x]$ um polinômio com $\deg(f) < \deg(Q') = \alpha(Q)$. Então $\mu_Q(f) = \mu(f)$. Além disso, para cada $k \in \mathbb{N}$, temos $\deg(\partial_k f) < \deg(Q') = \alpha(Q)$. Logo, $\mu_Q(\partial_k f) = \mu(\partial_k f)$. Portanto, para todo $k \in \mathbb{N}$,

$$\frac{\mu(f) - \mu(\partial_k f)}{k} = \frac{\mu_Q(f) - \mu_Q(\partial_k f)}{k} \leq \epsilon(Q) < \epsilon(Q').$$

Ou seja, $\epsilon(f) < \epsilon(Q')$, mostrando que Q' é polinômio-chave.

■

No próximo capítulo, utilizaremos os resultados técnicos desta seção para provar, por exemplo, que um par da forma $(a, \delta(Q))$, em que a é uma raiz otimizadora de um polinômio-chave Q, possui uma certa minimalidade. Esses pares minimais nos permitirão descrever uma classe de valorizações em $\mathbb{K}[x]$.

Capítulo 3

Pares minimais e valorizações transcendentes

Neste capítulo introduziremos os conceito de par de definição e de par minimal. Estes pares, juntamente com os polinômios-chaves, nos ajudarão a descrever um tipo especial de valorização no anel $\mathbb{K}[x]$, que são as valorizações transcendentes. Dentre estas valorizações, as que se identificarão como resíduo-transcendente terão um papel importante na descrição futura de todas as valorizações no corpo $\mathbb{K}(x)$ que estendem uma dada valorização ν em $\mathbb{K}$.

Nas primeiras seções, definiremos o que é um par de definição e um par minimal e conectaremos estes conceitos com o que estudamos no capítulo anterior sobre polinômios-chaves e truncamentos. Em seguida, definiremos as valorizações do tipo valor-transcendente e as valorizações do tipo resíduo-transcendente. Dedicaremos uma subseção para cada um desses tipos de valorizações, caracterizando-os em termos de pares minimais e truncamentos em polinômios-chaves. Por fim, estabeleceremos uma relação de extensão entre truncamentos definidos em ambiente distintos.

As principais referências para a composição deste capítulo foram os trabalhos de Alexandru, Popescu e Zaharescu (1988), Bengus-Lasnier (2021), Novacoski (2019) e Popescu e Popescu (1989).

3.1 Pares de definição

Sejam $\mathbb{K}$ um corpo, $\overline{\mathbb{K}}$ um fecho algébrico fixado para $\mathbb{K}$ e $\overline{\nu}$ uma valorização em $\overline{\mathbb{K}}$. Como vimos no Capítulo 1, Seção 1.4, podemos construir uma família de valorizações para $\overline{\mathbb{K}}[x]$ da seguinte forma: para $a \in \overline{\mathbb{K}}$ e $\delta \in \Phi$, em que $\Phi \supseteq \overline{\nu}\overline{\mathbb{K}}$, definimos

$$\overline{\mu}_{a,\delta}\left(\sum_{i=0}^{r} a_i(x-a)^i\right) := \min_{0\leq i\leq r}\{\overline{\nu}(a_i) + i\delta\},$$

em que $a_i \in \overline{\mathbb{K}}$. Essas valorizações são chamadas monomiais.

As valorizações monomiais são definidas a partir de um par (a, δ). Como muitos pares podem eventualmente definir a mesma valorização $\overline{\mu}_{a,\delta}$, veremos uma forma de caracterizar pares que definem a mesma valorização.

Lema 3.1. *Dois pares (a, δ) e (a', δ') definem a mesma valorização monomial se, e somente se, $\delta = \delta'$ e $\overline{\nu}(a - a') \geq \delta$.*

Demonstração:

($\Rightarrow$) Suponhamos que (a, δ) e (a', δ') definem a mesma valorização. Então,

$$\delta' = \overline{\mu}_{a',\delta'}(x - a') = \overline{\mu}_{a,\delta}(x - a') = \min\{\delta, \overline{\nu}(a - a')\}.$$

Por um argumento simétrico, concluímos que $\delta = \min\{\delta', \overline{\nu}(a-a')\}$. Assim $\delta = \delta'$ e $\overline{\mu}(a-a') \geq \delta$.

($\Leftarrow$) Mostremos que $\overline{\mu}_{a',\delta'} = \overline{\mu}_{a,\delta}$ se $\delta' = \delta$ e $\overline{\nu}(a - a') \geq \delta$. É suficiente mostrar que estas coincidem nos polinômios de grau zero e de grau um, pois $\overline{\mathbb{K}}$ é algebricamente fechado e todo polinômio em $\overline{\mathbb{K}}[x]$ se fatora como uma constante que multiplica um produto de polinômios de grau um.

Para $b \in \overline{\mathbb{K}}$, temos $\overline{\mu}_{a',\delta'}(b) = \overline{\nu}(b) = \overline{\mu}_{a,\delta}(b)$. Agora, para $x - b \in \overline{\mathbb{K}}[x]$ temos

$$\overline{\mu}_{a,\delta}(x - b) = \min\{\delta, \overline{\nu}(a - b)\}$$

e

$$\overline{\mu}_{a',\delta}(x - b) = \min\{\delta, \overline{\nu}(a' - b)\}$$

- Se $\overline{\nu}(a - b) \geq \delta$, então $\overline{\mu}_{a,\delta}(x - b) = \delta$ e

$$\overline{\nu}(a' - b) = \overline{\nu}(a' - a + a - b) \geq \min\{\overline{\nu}(a' - a), \overline{\nu}(a - b)\} \geq \delta.$$

  Assim

$$\overline{\mu}_{a,\delta}(x - b) = \delta = \overline{\mu}_{a',\delta}(x - b).$$

- Se $\overline{\nu}(a - b) < \delta$, então

$$\overline{\nu}(a' - b) = \overline{\nu}(a' - a + a - b) = \overline{\nu}(a - b).$$

  Assim

$$\overline{\mu}_{a,\delta}(x - b) = \overline{\nu}(a - b) = \overline{\nu}(a' - b) = \overline{\mu}_{a',\delta}(x - b).$$

■

Seja $\overline{\mu}$ uma valorização em $\overline{\mathbb{K}}[x]$ tal que $\overline{\mu}|_{\overline{\mathbb{K}}} = \overline{\nu}$.

Definição 3.2. *Um par $(a, \delta) \in \overline{\mathbb{K}} \times \Phi$ tal que $\overline{\mu} = \overline{\mu}_{a,\delta}$ é chamado um* ***par de definição*** *para $\overline{\mu}$.*

■

Observação 3.3. *De imediato, vemos que se $\overline{\mu} = \overline{\mu}_{a,\delta}$, então $\overline{\mu}(x-a) = \overline{\mu}_{a,\delta}(x-a) = \delta$. Portanto, nesse caso $\overline{\mu}_{a,\delta} = \overline{\mu}_{x-a}$ pois*

$$\overline{\mu}_{a,\delta}\left(\sum_{i=0}^{r} a_i(x-a)^i\right) = \min_{0\leq i\leq r}\{\overline{\nu}(a_i) + i\delta\} = \min_{0\leq i\leq r}\{\overline{\mu}(a_i) + i\overline{\mu}(x-a)\} = \overline{\mu}_{x-a}\left(\sum_{i=0}^{r} a_i(x-a)^i\right).$$

Por outro lado, se $\overline{\mu} = \overline{\mu}_{x-a}$, então $(a, \overline{\mu}(x-a))$ é um par de definição para $\overline{\mu}$. Portanto, $\overline{\mu}$ admite um par de definição se, e somente se, $\overline{\mu}$ é um truncamento em um polinômio da forma $x-a$.

▼

A seguir, veremos dois lemas que nos ajudarão a caracterizar pares de definição.

Lema 3.4. *Sejam $a, c \in \overline{\mathbb{K}}$. Se $\overline{\mu}(x-a) \geq \overline{\mu}(x-c)$, então*

$$\overline{\mu}(a-c) \geq \overline{\mu}(x-c) \text{ e } \overline{\mu}_{x-a}(x-c) = \overline{\mu}(x-c).$$

Mais ainda, se $\overline{\mu}(x-a) > \overline{\mu}(x-c)$, então

$$\overline{\mu}_{x-a}(x-c) = \overline{\mu}(x-c) = \overline{\mu}(a-c).$$

Demonstração: Como $x-c = (x-a)+(a-c)$ e $\overline{\mu}(x-a) \geq \overline{\mu}(x-c)$, temos que

$$\overline{\mu}_{x-a}(x-c) = \min\{\overline{\mu}(x-a), \overline{\mu}(a-c)\}$$

e

$$\overline{\mu}(a-c) \geq \min\{\overline{\mu}(x-a), \overline{\mu}(x-c)\} = \overline{\mu}(x-c).$$

Temos dois casos para analisar:

- Se $\overline{\mu}(x-a) = \overline{\mu}(x-c)$, então $\overline{\mu}(a-c) \geq \overline{\mu}(x-a)$ e $\overline{\mu}_{x-a}(x-c) = \overline{\mu}(x-a) = \overline{\mu}(x-c)$.
- Se $\overline{\mu}(x-a) > \overline{\mu}(x-c)$, então $\overline{\mu}(a-c) = \overline{\mu}(x-c)$ e $\overline{\mu}_{x-a}(x-c) = \overline{\mu}(a-c) = \overline{\mu}(x-c)$.

■

Lema 3.5. *Um par (a,δ) é um par de definição para $\overline{\mu}$ se, e somente se, $\delta = \overline{\mu}(x-a) \geq \overline{\mu}(x-c)$ para todo $c \in \overline{\mathbb{K}}$.*

Demonstração:

($\Rightarrow$) Suponhamos que (a,δ) é um par de definição. Pela Observação 3.3, sabemos que $\delta = \overline{\mu}(x-a)$ e $\overline{\mu} = \overline{\mu}_{x-a}$. Logo, para todo $c \in \overline{\mathbb{K}}$, temos

$$\overline{\mu}(x-c) = \overline{\mu}_{x-a}(x-c) = \min\{\overline{\mu}(x-a), \overline{\nu}(a-c)\} \leq \overline{\mu}(x-a) = \delta.$$

($\Leftarrow$) Suponhamos $\delta = \overline{\mu}(x-a) \geq \overline{\mu}(x-c)$ para todo $c \in \overline{\mathbb{K}}$. Uma vez que todo polinômio em $\overline{\mathbb{K}}[x]$ pode ser escrito como produto de fatores de grau um, basta provarmos que $\overline{\mu}(x-c) = \overline{\mu}_{x-a}(x-c)$ para todo $c \in \overline{\mathbb{K}}$. Logo, o resultado segue do Lema 3.4.

■

Observação 3.6. *Se $a \in \overline{\mathbb{K}}$ é tal que (a,δ) é um par de definição para $\overline{\mu}$, então pelo Lema 3.5 vemos que a é uma raiz otimizadora de seu polinômio minimal sobre $\mathbb{K}$.*

▼

3.2 Pares minimais e polinômios-chaves

Sejam $\mathbb{K}$ um corpo, $\overline{\mathbb{K}}$ um fecho algébrico fixado de $\mathbb{K}$ e $\overline{\nu}$ uma valorização em $\overline{\mathbb{K}}$. Consideremos um grupo $\Phi \supseteq \overline{\nu}\overline{\mathbb{K}}$.

Definição 3.7. *Um **par minimal** para $\overline{\nu}$ (com relação à extensão $\overline{\mathbb{K}} \mid \mathbb{K}$) é um par da forma $(a,\gamma) \in \overline{\mathbb{K}} \times \Phi$ tal que, para todo $b \in \overline{\mathbb{K}}$,*

$$\overline{\nu}(b-a) \geq \gamma \Rightarrow [\mathbb{K}(b):\mathbb{K}] \geq [\mathbb{K}(a):\mathbb{K}].$$

■

Exemplo 3.8. *Para quaisquer $a \in \mathbb{K}$ e $\gamma \in \Phi$, o par (a,γ) é trivialmente um par minimal para $\overline{\nu}$ pois $[\mathbb{K}(b):\mathbb{K}] \geq [\mathbb{K}(a):\mathbb{K}] = 1$ para qualquer que seja $b \in \overline{\mathbb{K}}$.*

▼

Seja $\overline{\mu}$ uma valorização em $\overline{\mathbb{K}}[x]$ tal que $\overline{\mu}|_{\overline{\mathbb{K}}} = \overline{\nu}$. Nesta situação, um par (a,γ) é dito um par minimal para $\overline{\mu}$ se é um par minimal para $\overline{\nu}$ (com relação à extensão $\overline{\mathbb{K}} \mid \mathbb{K}$).

Definição 3.9. *Um par (a,γ) é **par minimal de definição** para $\overline{\mu}$ se é um par minimal e um par de definição para $\overline{\mu}$.*

■

Consideremos o conjunto

$$S := \{a \in \overline{\mathbb{K}} \mid \overline{\mu} = \overline{\mu}_{x-a}\}.$$

Lema 3.10. *Suponhamos $S \neq \emptyset$. Se $a \in S$ tem o menor grau sobre $\mathbb{K}$ dentre os elementos de S, então $(a, \overline{\mu}(x-a))$ é um par minimal de definição para $\overline{\mu}$.*

Demonstração: Seja $\delta = \overline{\mu}(x-a)$. Sabemos que (a, δ) é, por hipótese, um par de definição para $\overline{\mu}$. Tomemos $b \in \overline{\mathbb{K}}$ tal que $\overline{\mu}(b-a) \geq \delta$. Então, pelo Lema 3.1, $\overline{\mu}_{x-a} = \overline{\mu}_{a,\delta} = \overline{\mu}_{b,\delta} = \overline{\mu}_{x-b}$. Assim, $b \in S$. Pela minimalidade do grau de a, segue que

$$[\mathbb{K}(b) : \mathbb{K}] \geq [\mathbb{K}(a) : \mathbb{K}]$$

e por isso $(a, \overline{\mu}(x-a))$ é um par minimal para $\overline{\mu}$. Ou seja, $(a, \overline{\mu}(x-a))$ é um par minimal de definição para $\overline{\mu}$.

■

Seja μ uma valorização em $\mathbb{K}[x]$ e consideremos uma extensão $\overline{\mu}$ de μ para $\overline{\mathbb{K}}[x]$. Denotemos $\overline{\mu}|_{\mathbb{K}} = \overline{\nu}$. O seguinte teorema é um dos resultado principais do artigo de Novacoski (2019).

Teorema 3.11. *Seja $Q \in \mathbb{K}[x]$ um polinômio mônico irredutível e seja $a \in \overline{\mathbb{K}}$ uma raiz de Q tal que $\overline{\mu}(x-a) = \delta(Q)$.*

1. *Temos que Q é um polinômio-chave para μ se, e somente se, $(a, \delta(Q))$ é um par minimal para $\overline{\mu}$.*

2. *Temos que Q é um polinômio-chave para μ e $\mu = \mu_Q$ se, e somente se, $(a, \delta(Q))$ é um par minimal de definição para $\overline{\mu}$.*

Demonstração:

1. ($\Rightarrow$) Suponhamos que Q seja um polinômio-chave para μ. Tomemos $b \in \overline{\mathbb{K}}$ tal que $\overline{\mu}(b-a) \geq \delta(Q)$. Como $\overline{\mu}(x-a) = \delta(Q)$, temos que $\overline{\mu}(x-b) \geq \delta(Q)$, pois $\delta(Q) = \overline{\mu}(x-a) = \overline{\mu}(x-a+b-b) \geq \min\{\overline{\mu}(x-b), \overline{\mu}(b-a)\}$ e

   - se $\overline{\mu}(x-b) > \overline{\mu}(b-a)$, então $\overline{\mu}(x-b) > \overline{\mu}(b-a) = \delta(Q)$;
   - se $\overline{\mu}(x-b) = \overline{\mu}(b-a)$, então $\delta(Q) \geq \overline{\mu}(x-b) = \overline{\mu}(b-a) \geq \delta(Q)$, logo $\delta(Q) = \overline{\mu}(x-b)$;
   - se $\overline{\mu}(x-b) < \overline{\mu}(b-a)$, então $\delta(Q) = \min\{\overline{\mu}(x-b), \overline{\mu}(b-a)\} = \overline{\mu}(x-b)$.

   Sendo p_b o polinômio minimal de b sobre $\mathbb{K}$, temos que $\delta(p_b) \geq \overline{\mu}(x-b) \geq \delta(Q)$. Então $\epsilon(p_b) \geq \epsilon(Q)$ e, por Q ser um polinômio-chave, segue que $\deg(p_b) \geq \deg(Q)$. Portanto,

$$[\mathbb{K}(a) : \mathbb{K}] = \deg(Q) \leq \deg(p_b) = [\mathbb{K}(b) : \mathbb{K}].$$

($\Leftarrow$) Assumimos que, para todo $b \in \overline{\mathbb{K}}$, se $\overline{\mu}(b-a) \geq \delta(Q)$, então $[\mathbb{K}(a):\mathbb{K}] \leq [\mathbb{K}(b):\mathbb{K}]$. Mostremos que, para todo polinômio $f \in \mathbb{K}[x]$, se $\deg(f) < \deg(Q)$, então $\epsilon(f) < \epsilon(Q)$. Seja $f \in \mathbb{K}[x]$ tal que $\deg(f) < \deg(Q)$. Assim, para cada raiz b de f em $\overline{\mathbb{K}}$, temos que

$$[\mathbb{K}(b):\mathbb{K}] \leq \deg(f) < \deg(Q) = [\mathbb{K}(a):\mathbb{K}].$$

Isso implica $\overline{\mu}(b-a) < \delta(Q)$. Portanto,

$$\overline{\mu}(x-b) = \min\{\overline{\mu}(x-a), \overline{\mu}(b-a)\} = \overline{\mu}(b-a) < \delta(Q).$$

Então, $\epsilon(f) = \delta(f) < \delta(Q) = \epsilon(Q)$ e concluímos que Q é um polinômio-chave.

2. ($\Rightarrow$) Suponhamos que Q é um polinômio-chave e $\mu = \mu_Q$. Por Q ser polinômio-chave, segue do item anterior que $(a, \delta(Q))$ é par minimal para $\overline{\mu}$. Como por hipótese temos que $\overline{\mu}(x-a) = \delta(Q)$, basta mostrarmos que $\overline{\mu}(x-a) \geq \overline{\mu}(x-b)$ para todo $b \in \overline{\mathbb{K}}$.

   Assumimos, buscando por uma contradição, que existe $b \in \overline{\mathbb{K}}$ tal que vale $\delta(Q) = \overline{\mu}(x-a) < \overline{\mu}(x-b)$. Temos $\epsilon(Q) < \epsilon(p_b)$, em que p_b é o polinômio minimal de b sobre $\mathbb{K}$. Consideremos o conjunto

$$\{q \in \mathbb{K}[x] \mid \epsilon(p_b) \leq \epsilon(q)\}.$$

   Seja Q' um elemento deste conjunto com grau mínimo. Se f é tal que $\deg(f) < \deg(Q')$, então f não está no conjunto anterior e assim $\epsilon(f) < \epsilon(p_b) \leq \epsilon(Q')$. Temos com isso que Q' é polinômio-chave, pela definição, e $\epsilon(p_b) \leq \epsilon(Q')$. Assim, $\epsilon(Q) < \epsilon(Q')$ e , pela Proposição 2.33 Item 2, isso significa que $\mu_Q(Q') < \mu(Q')$. Porém, isso contradiz $\mu = \mu_Q$. Portanto, $\overline{\mu}(x-a) \geq \overline{\mu}(x-b)$ para todo $b \in \overline{\mathbb{K}}$ e assim $(a, \delta(Q))$ é um par minimal de definição para $\overline{\mu}$.

   ($\Leftarrow$) Suponhamos que $(a, \delta(Q))$ é um par minimal de definição para $\overline{\mu}$. Por $(a, \delta(Q))$ ser um par minimal para μ, segue do item anterior que Q é polinômio-chave. Mostremos que $\mu_Q = \mu$. Por contradição, suponhamos que exista $f \in \mathbb{K}[x]$ tal que $\mu_Q(f) < \mu(f)$. Então, $\Psi(Q) \neq \emptyset$. Logo, pela Proposição 2.34, existe um polinômio-chave Q' tal que $\epsilon(Q) < \epsilon(Q')$. Seja $b \in \overline{\mathbb{K}}$ uma raiz de Q' tal que $\overline{\mu}(x-b) = \delta(Q')$. Temos

$$\overline{\mu}(x-b) = \delta(Q') = \epsilon(Q') > \epsilon(Q) = \delta(Q) = \overline{\mu}(x-a),$$

   contradizendo o fato de $(a, \delta(Q))$ ser par minimal de definição para $\overline{\mu}$ (Lema 3.5). Portanto, $\mu_Q = \mu$.

■

O resultado abaixo complementará o teorema anterior. O ponto principal do teorema a seguir é que basta $\overline{\mu}$ ser um truncamento em algum $x-a$ (isto é, admitir um par de definição) para que μ seja o truncamento em um polinômio-chave.

Teorema 3.12. *Temos $\overline{\mu} = \overline{\mu}_{x-a}$ para algum $a \in \overline{\mathbb{K}}$ se, e somente se, $\mu = \mu_Q$ para algum polinômio-chave $Q \in \mathbb{K}[x]$.*

Demonstração:

($\Rightarrow$) Se $\overline{\mu} = \overline{\mu}_{x-a}$ para algum $a \in \overline{\mathbb{K}}$, então $S \neq \emptyset$. Tomemos $a \in S$ com menor grau sobre $\mathbb{K}$ dentre os elementos de S. Pelo Lema 3.10, $(a, \overline{\mu}(x-a))$ é um par minimal de definição para $\overline{\mu}$. Seja $Q \in \mathbb{K}[x]$ polinômio minimal de a sobre $\mathbb{K}$. Pela Observação 3.6, a é uma raiz otimizadora de Q, isto é, $\delta(Q) = \overline{\mu}(x-a)$. Pelo Teorema 3.11, Q é um polinômio-chave e $\mu = \mu_Q$.

($\Leftarrow$) Suponhamos que $\mu = \mu_Q$ para algum polinômio-chave $Q \in \mathbb{K}[x]$. Seja $a \in \overline{\mathbb{K}}$ uma raiz otimizadora de Q. Pelo Item 2 do Teorema 3.11, $(a, \delta(Q))$ é um par minimal de definição para $\overline{\mu}$. Pela Observação 3.3, concluímos que $\overline{\mu} = \overline{\mu}_{x-a}$.

■

Exemplo 3.13. *Seja μ' a valorização definida no Exemplo 2.6 e tomemos $\overline{\mu'}$ uma extensão qualquer de μ' para $\overline{\mathbb{Q}}[x]$. Vimos no exemplo citado que $Q = x^2 - 2$ é um polinômio-chave para μ' e $\epsilon(Q) = \frac{3}{4}$. As raízes de Q são $\sqrt{2}$ e $-\sqrt{2}$. Temos*

$$\frac{3}{2} = \overline{\mu'}(x^2-2) = \overline{\mu'}(x-\sqrt{2}) + \overline{\mu'}(x+\sqrt{2})$$

e

$$\epsilon(Q) = \delta(Q) = \max\{\overline{\mu'}(x-\sqrt{2}), \overline{\mu'}(x+\sqrt{2})\} = \frac{3}{4}.$$

Portanto, $\overline{\mu'}(x-\sqrt{2}) = \overline{\mu'}(x+\sqrt{2}) = \frac{3}{4}$. Pelo Teorema 3.11, $(\sqrt{2}, \frac{3}{4})$ e $(-\sqrt{2}, \frac{3}{4})$ são pares minimais para $\overline{\mu'}$. Mais do que isso, como $\mu' = \mu'_Q$, concluímos também que ambos são pares minimais de definição para $\overline{\mu'}$.

▼

3.3 Valorizações transcendentes

Seja μ valorização em $\mathbb{K}[x]$ e $\nu = \mu|_{\mathbb{K}}$. Apresentaremos a seguir classes de valorizações em $\mathbb{K}[x]$.

Definição 3.14. *Uma valorização μ em $\mathbb{K}[x]$ é chamada **valor-transcendente** se existe $f \in \mathbb{K}[x]$, $f \neq 0$, tal que a imagem de $\mu(f)$ no grupo quociente $\mu(\mathbb{K}[x])/\nu\mathbb{K}$ é livre de torção.* ■

Exemplo 3.15. *Se μ não é trivial em $\mathbb{K}[x]$ mas é trivial em $\mathbb{K}$, isto é, $\nu(a) = 0$ para todo $a \in \mathbb{K}$, então μ é valor-transcendente. De fato, neste caso $\nu\mathbb{K} = \{0\}$ e por isso $\mu(\mathbb{K}[x])/\nu\mathbb{K} \cong \mu(\mathbb{K}[x])$. Como este é totalmente ordenado, segue que tal grupo é livre de torção (Proposição B.8). Logo, qualquer elemento $f \in \mathbb{K}[x]$ tal que $\mu(f) \neq 0$ terá sua imagem livre de torção em $\mu(\mathbb{K}[x])/\nu\mathbb{K}$.*

▼

O porquê do nome "valor-transcendente" ficará mais claro na Seção 3.3.2. Consideramos que ∞ é livre de torção sobre $\nu\mathbb{K}$ pois $n \cdot \infty = \infty \notin \nu\mathbb{K}$ para qualquer $n \in \mathbb{N}$. Assim, se μ não é valor-transcendente, então $\mu(f) \neq \infty$ para todo $f \in \mathbb{K}[x]$ não nulo, ou seja, $\operatorname{supp}(\mu) = \{0\}$. Nesta situação, vimos que podemos estender μ para $\mathbb{K}(x)$ da maneira usual e considerar o resíduo de cada elemento de $\mathbb{K}(x)$.

Definição 3.16. *Uma valorização de Krull μ em $\mathbb{K}[x]$ é chamada* ***resíduo-transcendente*** *se existe $f \in \mathcal{O}_\mu$ tal que o resíduo de f em $\mathbb{K}(x)\mu$ é transcendente sobre $\mathbb{K}\nu$.*

■

Definição 3.17. *Uma valorização μ em $\mathbb{K}[x]$ é* ***transcendente*** *se é valor-transcendente ou resíduo-transcendente. Caso contrário, μ é dita* ***algébrica****.*

■

Observação 3.18. *Uma valorização não pode ser simultaneamente valor-transcendente e resíduo-transcendente. Usaremos a Desigualdade de Zariski-Abhyankar para provar tal afirmação. Como mostramos no Teorema D.18, sendo $\mathbb{L} \mid \mathbb{K}$ uma extensão de corpos, $\nu : \mathbb{K} \to \nu\mathbb{K} \cup \{\infty\}$ uma valorização e $\mu : \mathbb{L} \to \mu\mathbb{L} \cup \{\infty\}$ um prolongamento de ν para $\mathbb{L}$, vale*

$$\operatorname{tr.deg}(\mathbb{L}\mu \mid \mathbb{K}\nu) + \operatorname{rat.rk}(\mu\mathbb{L}/\nu\mathbb{K}) \leq \operatorname{tr.deg}(\mathbb{L} \mid \mathbb{K}).$$

No nosso caso específico, temos $\operatorname{tr.deg}(\mathbb{K}(x) \mid \mathbb{K}) = 1$ e, consequentemente,

$$\operatorname{tr.deg}(\mathbb{K}(x)\mu \mid \mathbb{K}\nu) + \operatorname{rat.rk}(\mu\mathbb{K}(x)/\nu\mathbb{K}) \leq 1.$$

Se μ é valor-transcendente, então existe f tal que $\mu(f)$ é $\mathbb{Z}$-independente em $\mu\mathbb{K}(x)/\nu\mathbb{K}$, logo $1 \leq \operatorname{rat.rk}(\mu\mathbb{K}(x)/\nu\mathbb{K})$ e, com isso, $\operatorname{tr.deg}(\mathbb{K}(x)\mu \mid \mathbb{K}\nu) = 0$. Ou seja, $\mathbb{K}(x)\mu \mid \mathbb{K}\nu$ é uma extensão algébrica e, portanto, μ não é resíduo-transcendente. Analogamente, se μ é resíduo-transcendente, então $1 \leq \operatorname{tr.deg}(\mathbb{K}(x)\mu \mid \mathbb{K}\nu)$, o que nos leva a $\operatorname{rat.rk}(\mu\mathbb{K}(x)/\nu\mathbb{K}) = 0$. Mas, isso significa que o grupo quociente $\mu\mathbb{K}(x)/\nu\mathbb{K}$ é de torção (Apêndice B, Seção B.2). Portanto, μ não é valor-transcendente.

▼

Estudaremos nas duas subseções a seguir as relações entre as valorizações transcendentes em $\mathbb{K}[x]$, os truncamentos em polinômios-chaves, os pares minimais e os pares de definição, buscando resultados nos moldes do Teorema 3.11 da seção anterior.

Mais especificamente, gostaríamos de complementar o seguinte resultado de Novacoski (2019, p. 4): μ em $\mathbb{K}[x]$ é transcendente se, e somente se, $\mu = \mu_q$ para algum polinômio $q \in \mathbb{K}[x]$. Veremos que μ em $\mathbb{K}[x]$ é transcendente se, e somente se, $\mu = \mu_Q$ para algum polinômio-chave $Q \in \mathbb{K}[x]$. Este será o primeiro resultado principal deste trabalho.

3.3.1 Valorizações resíduo-transcendentes

Seja ν uma valorização em $\mathbb{K}$ e μ uma extensão de ν para $\mathbb{K}(x)$. Pelo Teorema D.25 no Apêndice D, fixada uma extensão $\overline{\nu}$ de ν para $\overline{\mathbb{K}}$, podemos sempre tomar $\overline{\mu}$ em $\overline{\mathbb{K}}(x)$ de modo que esta seja uma extensão de μ, ν e $\overline{\nu}$ simultaneamente. A Figura 3.1 esquematiza essas valorizações.

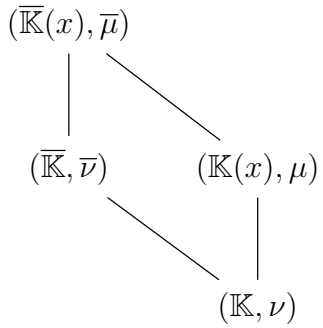


Figura 3.1: Diagrama das extensões

Tomemos $\overline{\mu}_{a,\delta}$ uma valorização monomial em $\overline{\mathbb{K}}[x]$. Como $\overline{\mu}_{a,\delta}$ é uma valorização de Krull, podemos estendê-la de forma única para $\overline{\mathbb{K}}(x)$, denotando a extensão também por $\overline{\mu}_{a,\delta}$. Veremos no Corolário 3.21 uma forma de verificar quando $\overline{\mu}_{a,\delta}$ é uma extensão resíduo-transcendente de $\overline{\nu}$, isto é, veremos um critério para decidir quando a extensão de corpos $\overline{\mathbb{K}}(x)\overline{\mu}_{a,\delta} \mid \overline{\mathbb{K}}\overline{\nu}$ é transcendente.

Em geral, se ν é uma valorização em um corpo $\mathbb{K}$ e μ é uma valorização em $\mathbb{K}(x)$ que estende ν, então diremos que $\mu \mid \nu$ é uma **extensão resíduo-transcendente** se $\mathbb{K}(x)\mu \mid \mathbb{K}\nu$ é transcendente. Ou seja, $\mu|_{\mathbb{K}[x]}$ é uma valorização resíduo-transcendente no sentido da Definição 3.16.

Lema 3.19. *Sejam $q \in \mathbb{K}[x]$, $c \in \mathbb{K}^\times$ e $n \in \mathbb{N}$ tais que $\mu = \mu_q$ e $n\mu(q) = \nu(c)$. Então $(q^n/c)\mu \in \mathbb{K}(x)\mu$ é transcendente sobre $\mathbb{K}\nu$. Em particular, $\mu \mid \nu$ é uma extensão resíduo-transcendente.*

Demonstração: Suponhamos que existam $b_0, \ldots, b_r \in \mathcal{O}_\nu$ tais que

$$\sum_{i=0}^{r} (b_i\mu) \left(\frac{q^n}{c}\mu\right)^i = 0 \text{ em } \mathbb{K}\mu,$$

isto é,

$$\mu\left(\sum_{i=0}^{r} b_i \left(\frac{q^n}{c}\right)^i\right) > 0.$$

Como $\mu = \mu_q$, para todo j, $0 \leq j \leq r$, temos que vale

$$\mu\left(b_j \left(\frac{q^n}{c}\right)^j\right) \geq \min_{0\leq i\leq r}\left\{\mu\left(b_i \left(\frac{q^n}{c}\right)^i\right)\right\} = \mu\left(\sum_{i=0}^{r} b_i \left(\frac{q^n}{c}\right)^i\right) > 0.$$

Assim, $(b_j\mu)((q^n/c)\mu)^j = (b_j(q^n/c)^j)\mu = 0$. Uma vez que $(q^n/c)\mu \neq 0$, temos $b_j\mu = 0$ para todo j. Concluímos que $(q^n/a)\mu$ é transcendente sobre $\mathbb{K}\nu$. Dessa forma, $\mu \mid \nu$ é uma extensão resíduo-transcendente.

■

As valorizações da forma $\overline{\mu}_{a,\delta}$ nos ajudam a estudar as extensões resíduo-transcendentes de ν e de $\overline{\nu}$. Por exemplo, temos o seguinte teorema.

Teorema 3.20. *Sejam ν, $\overline{\nu}$, μ e $\overline{\mu}$ como na Figura 3.1. As afirmações a seguir são equivalentes.*

1. *$\mu \mid \nu$ é extensão resíduo-transcendente.*
2. *$\overline{\mu} \mid \overline{\nu}$ é extensão resíduo-transcendente.*
3. *Existem $a \in \overline{\mathbb{K}}$ e $\delta = \overline{\mu}(x-a) \in \overline{\nu}\overline{\mathbb{K}}$ tais que $\overline{\mu} = \overline{\mu}_{a,\delta}$.*
4. *Vale $\overline{\mu}\overline{\mathbb{K}}(x) = \overline{\nu}\overline{\mathbb{K}}$ e o conjunto $\{\overline{\mu}(x-b) \mid b \in \overline{\mathbb{K}}\}$ possui máximo.*

Demonstração:

(1. $\Rightarrow$ 2.) Se $\mu \mid \nu$ é resíduo-transcendente, então existe $r \in \mathbb{K}(x)$ tal que $r\mu$ é transcendente sobre $\mathbb{K}\nu$. Porém, $r\mu = r\overline{\mu} \in \overline{\mathbb{K}}(x)\overline{\mu}$. Assim, $r\overline{\mu}$ é transcendente sobre $\mathbb{K}\nu$. Então, como a propriedade de ser algébrico é transitiva, temos que $r\mu$ é também transcendente sobre qualquer extensão algébrica de $\mathbb{K}\nu$ contida em $\overline{\mathbb{K}}(x)\overline{\mu}$. Portanto, $r\overline{\mu}$ é transcendente sobre $\overline{\mathbb{K}}\overline{\nu}$, mostrando que $\overline{\mu} \mid \overline{\nu}$ é resíduo-transcendente.

(2. $\Rightarrow$ 1.) Se $\overline{\mu} \mid \overline{\nu}$ é resíduo-transcendente, então existe $r \in \overline{\mathbb{K}}(x)$ tal que $r\overline{\mu}$ é transcendente sobre $\overline{\mathbb{K}}\overline{\nu}$. Pela Proposição D.10, como $\overline{\mathbb{K}}(x) \mid \mathbb{K}(x)$ é algébrica, segue que $\overline{\mathbb{K}}(x)\overline{\mu} \mid \mathbb{K}(x)\mu$ é algébrica. Se $\mathbb{K}(x)\mu \mid \mathbb{K}\nu$ fosse algébrica, então $r\overline{\mu}$ seria, por transitividade, algébrico sobre $\mathbb{K}\nu$, o que é uma contradição. Então $\mathbb{K}(x)\mu$ possui ao menos um elemento transcendente sobre $\mathbb{K}\nu$, mostrando que $\mu \mid \nu$ é resíduo-transcendente.

(2. $\Rightarrow$ 3.) Primeiramente, veremos que a extensão $\overline{\mu} \mid \overline{\nu}$ ser resíduo-transcendente implica $\overline{\mu}\overline{\mathbb{K}}(x) = \overline{\nu}\overline{\mathbb{K}}$. De fato, pela Desigualdade de Zariski-Abhyankar, temos $\mathrm{rat.rk}(\overline{\mu}\overline{\mathbb{K}}(x)/\overline{\nu}\overline{\mathbb{K}}) = 0$, ou seja, $\overline{\mu}\overline{\mathbb{K}}(x)/\overline{\nu}\overline{\mathbb{K}}$ é de torção (Apêndice B). Assim, para todo $\gamma \in \overline{\mu}\overline{\mathbb{K}}(x)$ existe $m \in \mathbb{N}$ tal que $m\gamma \in \overline{\nu}\overline{\mathbb{K}}$. Mas, $\overline{\nu}\overline{\mathbb{K}}$ é um grupo divisível (Proposição D.11). Portanto, para $\omega = m\gamma \in \overline{\nu}\overline{\mathbb{K}}$

e $m \in \mathbb{N}$ existe $\gamma' \in \overline{\nu}\overline{\mathbb{K}}$ tal que $m\gamma = m\gamma'$. Como $\overline{\nu}\overline{\mathbb{K}}$ é livre de torção, essa igualdade implica $\gamma = \gamma' \in \overline{\nu}\overline{\mathbb{K}}$. Ou seja, $\overline{\mu}\overline{\mathbb{K}}(x) \subseteq \overline{\nu}\overline{\mathbb{K}}$. A outra inclusão segue de $\overline{\mu} \mid \overline{\nu}$ ser uma extensão. Logo, $\overline{\mu}\overline{\mathbb{K}}(x) = \overline{\nu}\overline{\mathbb{K}}$.

Seja $f/g \in \overline{\mathbb{K}}(x)$ tal que $(f/g)\overline{\mu} \in \overline{\mathbb{K}}(x)\overline{\mu}$ é transcendente sobre $\overline{\mathbb{K}}\overline{\nu}$. Escrevemos

$$f = \alpha \prod_{i=1}^{r}(x - a_i) \text{ e } g = \beta \prod_{j=1}^{s}(x - b_j).$$

Como $\overline{\mu}\overline{\mathbb{K}}(x) = \overline{\nu}\overline{\mathbb{K}}$, existem $c_i, d_j \in \overline{\mathbb{K}}$, $1 \leq i \leq r$, $1 \leq j \leq s$ tais que $\overline{\nu}(c_i) = \overline{\mu}(x - a_i)$ e $\overline{\nu}(d_j) = \overline{\mu}(x - b_j)$. Seja

$$h = \frac{\prod_{i=1}^{r}(x - a_i)/c_i}{\prod_{j=1}^{s}(x - b_j)/d_j}.$$

O resíduo de h em $\overline{\mathbb{K}}(x)\overline{\mu}$ é transcendente sobre $\overline{\mathbb{K}}\overline{\nu}$. Como todos os fatores $(x - a_i)/c_i$ e $(x - b_j)/d_j$ tem valor 0, temos que, quando levamos h para $\overline{\mathbb{K}}(x)\overline{\mu}$, pelo menos um de seus fatores é transcendente sobre $\overline{\mathbb{K}}\overline{\nu}$. Digamos que um destes seja $(x - a)/c$. Chamemos de $\delta = \overline{\mu}(x - a) = \overline{\nu}(c)$.

Seja $p \in \overline{\mathbb{K}}[x]$ um polinômio qualquer. Escrevemos

$$p = \sum_{i=1}^{t} p_i(x - a)^i,$$

em que $p_i \in \overline{\mathbb{K}}$. Seja $d \in \overline{\mathbb{K}}$ tal que $\overline{\nu}(d) = \min_{1 \leq i \leq t}\{\overline{\nu}(p_i c^i)\}$. Para todo i, $1 \leq i \leq t$, temos $\overline{\nu}(p_i c^i/d) \geq 0$ e, para algum i, $\overline{\nu}(p_i c^i/d) = 0$. Assim, o resíduo do polinômio

$$\frac{p}{d} = \sum_{i=1}^{t} \frac{p_i c^i}{d} \left(\frac{x - a}{c}\right)^i$$

em $\overline{\mathbb{K}}(x)\overline{\mu}$ é uma expressão polinomial não nula em $\frac{x-a}{c}\overline{\mu}$. Com isso, $\overline{\mu}(p/d) = 0$ pois, caso contrário, o resíduo de $(x - a)/c$ seria algébrico sobre $\overline{\mathbb{K}}\overline{\nu}$. Portanto,

$$\overline{\mu}(p) = \overline{\nu}(d) = \min_{1 \leq i \leq t}\{\overline{\nu}(p_i c^i)\} = \min_{1 \leq i \leq t}\{\overline{\nu}(p_i) + i\delta\} = \overline{\mu}_{a,\delta}(p)$$

e, consequentemente, $\overline{\mu} = \overline{\mu}_{a,\delta}$.

(3. $\Rightarrow$ 2.) Já sabemos que $\overline{\mu}\overline{\mathbb{K}}(x) \supseteq \overline{\nu}\overline{\mathbb{K}}$, por se tratar de uma extensão. Mas, como por hipótese $\delta = \overline{\mu}(x - a) \in \overline{\nu}\overline{\mathbb{K}}$, temos que $\overline{\mu}_{a,\delta}(f) = \min_{0 \leq i \leq r}\{\overline{\nu}(a_i) + i\delta\} \in \overline{\nu}\overline{\mathbb{K}}$ para todo $f \in \overline{\mathbb{K}}[x]$. Logo $\overline{\mu}\overline{\mathbb{K}}(x) = \overline{\nu}\overline{\mathbb{K}}$. Tomamos $c \in \overline{\mathbb{K}}$ tal que $\overline{\nu}(c) = \delta$. Pelo Lema 3.19, aplicado para $\overline{\mu}$, $x - a$ e c, o representante de $\frac{x-a}{c}$ em $\overline{\mathbb{K}}(x)\overline{\mu}$ é transcendente sobre $\overline{\mathbb{K}}\overline{\nu}$.

(3. $\Rightarrow$ 4.) Se $\overline{\mu} = \overline{\mu}_{a,\delta}$, então já vimos que $\overline{\mu}\overline{\mathbb{K}}(x) = \overline{\nu}\overline{\mathbb{K}}$. Além disso, pelo Lema 3.5, temos $\delta = \overline{\mu}(x-a) \geq \overline{\mu}(x-b)$ para todo $b \in \overline{\mathbb{K}}$.

(4. $\Rightarrow$ 3.) Suponhamos $\overline{\mu}\overline{\mathbb{K}}(x) = \overline{\nu}\overline{\mathbb{K}}$ e $\delta = \overline{\mu}(x-a) = \max\{\overline{\mu}(x-b) \mid b \in \overline{\mathbb{K}}\}$. Pela hipótese, $\overline{\mu}(x-a) \in \overline{\nu}\overline{\mathbb{K}}$ pois existe $c \in \overline{\mathbb{K}}$ tal que $\overline{\mu}(x-a) = \overline{\nu}(c)$. Além disso, pelo Lema 3.5, segue que $\overline{\mu}_{a,\delta} = \overline{\mu}$.

■

Logo, uma extensão resíduo-transcendente $\overline{\mu} \mid \overline{\nu}$ fica determinada por um par de definição $(a,\delta) \in \overline{\mathbb{K}} \times \overline{\nu}\overline{\mathbb{K}}$. Como vimos, $\delta = \overline{\mu}(x-a)$ e $\overline{\mu}(x-a) \geq \overline{\mu}(x-b)$ para todo $b \in \overline{\mathbb{K}}$. Se tomarmos a de modo que $[\mathbb{K}(a) : \mathbb{K}]$ seja mínimo, então temos que o par de definição de $\overline{\mu}$ é um par minimal de definição, conforme a Definição 3.7.

Corolário 3.21. *Seja $\overline{\nu}$ uma valorização em $\overline{\mathbb{K}}$ e Φ um grupo que contém $\overline{\nu}\overline{\mathbb{K}}$. Tomemos $a \in \overline{\mathbb{K}}$, $\delta \in \Phi$ e consideremos a valorização $\overline{\mu}_{a,\delta}$ em $\overline{\mathbb{K}}(x)$. Temos que $\overline{\mu}_{a,\delta} \mid \overline{\nu}$ é uma extensão resíduo-transcendente se, e somente se, $\delta \in \overline{\nu}\overline{\mathbb{K}}$.*

Demonstração:

($\Rightarrow$) Se $\overline{\mu}_{a,\delta}$ é extensão resíduo-transcendente de $\overline{\nu}$, então encontramos δ' e a' tais que $\overline{\mu}_{a,\delta} = \overline{\mu}_{a',\delta'}$ com $\delta' = \overline{\mu}_{a,\delta}(x-a') \in \overline{\nu}\overline{\mathbb{K}}$. Mas, pelo Lema 3.1, se (a,δ) e (a',δ') definem a mesma valorização monomial, então $\delta = \delta'$. Logo, $\delta \in \overline{\nu}\overline{\mathbb{K}}$.

($\Leftarrow$) Se $\delta \in \overline{\nu}\overline{\mathbb{K}}$, então segue do Lema 3.19, para $\overline{\mu} = \overline{\mu}_{a,\delta}$, que a extensão $\overline{\mu}_{a,\delta} \mid \overline{\nu}$ resíduo-transcendente.

■

A seguir, temos uma parte do primeiro resultado principal deste trabalho.

Teorema 3.22. *Sejam μ uma valorização em $\mathbb{K}[x]$. Se μ é resíduo-transcendente, então $\mu = \mu_Q$ para algum polinômio-chave Q. Além disso, tomando $\overline{\mu}$ uma extensão de μ para $\overline{\mathbb{K}}[x]$, vemos que $\overline{\mu}$ admite par minimal de definição.*

Demonstração: Como μ em $\mathbb{K}[x]$ é resíduo-transcendente, ela se estende para $\mathbb{K}(x)$. Seja $\nu = \mu|_{\mathbb{K}}$. Tomamos $\overline{\mu}$ e $\overline{\nu}$ como na Figura 3.1. Se μ em $\mathbb{K}[x]$ é resíduo-transcendente, então, olhando para μ em $\mathbb{K}(x)$, vemos que $\mu \mid \nu$ é uma extensão resíduo-transcendente. Pelo Teorema 3.20 isso é equivalente a dizer que existe $a' \in \overline{\mathbb{K}}$ tal que $\overline{\mu}|_{\overline{\mathbb{K}}[x]} = \overline{\mu}_{a',\delta}$ em que $\delta = \overline{\mu}(x-a')$.

Tomemos $a \in \overline{\mathbb{K}}$ de modo que este tenha grau mínimo dentre os elementos de $\{c \in \overline{\mathbb{K}} \mid \overline{\mu}(c-a') \geq \delta\}$. Dessa forma, $\overline{\mu}_{a,\delta}|_{\mathbb{K}[x]} = \overline{\mu}_{a',\delta}|_{\mathbb{K}[x]} = \overline{\mu}|_{\mathbb{K}[x]} = \mu$ e o par (a,δ) é um par minimal de definição para $\overline{\mu}$. Pelo Teorema 3.12, tomando Q o polinômio minimal de a sobre $\mathbb{K}$, este é um polinômio-chave para μ e $\mu = \mu_Q$.

■

3.3.2 Valorizações valor-transcendentes

Iniciamos vendo que uma valorização transcendente é o mesmo que um truncamento.

Lema 3.23. *Suponhamos que $q \in \mathbb{K}[x]$ seja um polinômio tal que $\mu(q)$ é livre de torção sobre $\nu\mathbb{K}$ e que para todo $f \in \mathbb{K}[x]$ com $\deg(f) < \deg(q)$ tenhamos que $\mu(f)$ é de torção sobre $\nu\mathbb{K}$. Então $\mu = \mu_q$.*

Demonstração: Para qualquer $f \in \mathbb{K}[x]$ não nulo, seja $f = f_0 + \ldots + f_s q^s$ sua q-expansão. Para todo i, temos $\deg(f_i) < \deg(q)$. Tomemos dois coeficientes f_i e f_j de f com $i > j$. Afirmamos que se $f_i, f_j \notin \text{supp}(\mu)$, então $\mu(f_i q^i) \neq \mu(f_j q^j)$. De fato, se valesse a igualdade, então

$$\mu(f_i) + i\mu(q) = \mu(f_j) + j\mu(q),$$

o que implica

$$(i-j)\mu(q) = \mu(f_j) - \mu(f_i).$$

Mas, como $\deg(f_i), \deg(f_j) < \deg(q)$, temos por hipótese que os valores de f_i e f_j são de torção sobre $\nu\mathbb{K}$. Então, $\mu(f_i) - \mu(f_j)$ é de torção e, consequentemente, também $\mu(q)$ o seria. Isso contradiz nossa hipótese. Portanto $\mu(f_i q^i) \neq \mu(f_j q^j)$ se $i \neq j$ e $f_i, f_j \notin \text{supp}(\mu)$.

Logo,

$$\mu(f) = \mu(f_0 + \ldots + f_s q^s) = \min_{0 \leq i \leq s} \{\mu(f_i q^i)\} = \mu_q(f).$$

■

Teorema 3.24. *Uma valorização μ em $\mathbb{K}[x]$ é transcendente se, e somente se, existe um polinômio $q \in \mathbb{K}[x]$ tal que $\mu = \mu_q$.*

Demonstração:

($\Rightarrow$) Se μ é resíduo-transcendente, então o Teorema 3.22 nos diz que $\mu = \mu_Q$ para algum polinômio(-chave) em $\mathbb{K}[x]$.

Se μ é valor-transcendente, então existe $q \in \mathbb{K}[x]$ tal que $\mu(q)$ é livre de torção sobre $\nu\mathbb{K}$. Escolhemos q com o menor grau possível. Assim, para qualquer $f \in \mathbb{K}[x]$ com $\deg(f) < \deg(q)$ temos que $\mu(f)$ é de torção sobre $\nu\mathbb{K}$. Pelo Lema 3.23, segue que $\mu = \mu_q$.

($\Leftarrow$) Suponhamos que $\mu = \mu_q$ para algum polinômio $q \in \mathbb{K}[x]$. Se $\mu(q)$ é livre de torção sobre $\nu\mathbb{K}$, então μ é valor-transcendente, logo μ é transcendente.

Suponhamos então que $\mu(q)$ não é livre de torção sobre $\nu\mathbb{K}$, isto é, existem $a \in \mathbb{K}^\times$ e $n \in \mathbb{N}$ tais que $n \cdot \mu(q) = \nu(a)$ ou, equivalentemente, $\mu(q^n/a) = 0$. Assim, em $\mathbb{K}\mu$, temos $q^n\mu \neq 0$. Pelo Lema 3.19, $(q^n/c)\mu$ é transcendente sobre $\mathbb{K}\nu$. Assim, μ é resíduo-transcendente, logo é transcendente.

■

Sejam μ uma valorização em $\mathbb{K}[x]$ e $\overline{\mu}$ uma extensão de μ para $\overline{\mathbb{K}}[x]$. Podemos afirmar que se $\mu = \mu_Q$ para algum polinômio-chave (ou equivalentemente, $\overline{\mu}$ admite um par minimal de definição), então μ é transcendente. Isso segue direto do Teorema 3.24 acima. A recíproca dessa afirmação é garantida no caso em que μ é resíduo-transcendente, como visto no Teorema 3.22. Mas, no caso em que μ é valor-transcendente, não podemos afirmar a recíproca de imediato. Já vimos que uma valorização valor-transcendente μ pode ser vista como um truncamento μ_q para algum polinômio em $\mathbb{K}[x]$. O que mostraremos a seguir é que uma valorização valor-transcendente em $\mathbb{K}[x]$ também é um truncamento em um polinômio-chave, concluindo assim o primeiro resultado principal deste trabalho.

Iniciaremos trabalhando com um caso particular.

Lema 3.25. *Sejam $\overline{\nu}$ uma valorização em $\overline{\mathbb{K}}$ e $\overline{\mu}$ uma extensão de $\overline{\nu}$ para $\overline{\mathbb{K}}[x]$. Suponhamos que $\overline{\mu}$ é valor-transcendente em $\overline{\mathbb{K}}[x]$. Então existem $a \in \overline{\mathbb{K}}$ e $\delta \in \overline{\mu}(\overline{\mathbb{K}}[x])$ tais que $\overline{\mu}(x-a) = \delta$ e $\overline{\mu} = \overline{\mu}_{a,\delta}$.*

Demonstração: Como $\overline{\mu}$ é valor-transcendente o grupo quociente $\overline{\mu}(\overline{\mathbb{K}}[x])/\overline{\nu}\overline{\mathbb{K}}$ possui um elemento livre de torção. Portanto, existe $\gamma \in \overline{\mu}(\overline{\mathbb{K}}[x])$ tal que $\gamma\mathbb{Z} \cap \overline{\nu}\overline{\mathbb{K}} = \{0\}$. Seja $g \in \overline{\mathbb{K}}[x]$ tal que $\gamma = \overline{\mu}(g)$. Como $\overline{\mathbb{K}}$ é algebricamente fechado, temos

$$\gamma = \overline{\mu}(g) = \overline{\mu}\left(c\prod_{i=1}^{s}(x-a_i)\right) = \overline{\mu}(c) + \sum_{i=1}^{s}\overline{\mu}(x-a_i).$$

Se $\mu(x-b)$ fosse de torção sobre $\overline{\nu}\overline{\mathbb{K}}$ para todo $b \in \overline{\mathbb{K}}$, então $\overline{\mu}(g)$ também o seria, contradizendo a escolha de γ. Logo, deve existir ao menos um $a \in \overline{\mathbb{K}}$ tal que $\delta = \overline{\mu}(x-a)$ é livre de torção sobre $\overline{\nu}\overline{\mathbb{K}}$. Assim, aplicando o Lema 3.23 para $\overline{\mu}$, $\overline{\nu}$ e $x-a$, concluímos que $\overline{\mu} = \overline{\mu}_{x-a} = \overline{\mu}_{a,\delta}$.

■

Ou seja, as valorizações valor-transcendentes em $\overline{\mathbb{K}}[x]$ se parecem com as valorizações resíduo-transcendentes, pois ambas podem ser definidas por um par de definição (a,δ). Como apontam Alexandru, Popescu e Zaharescu (1990a, p. 289), a principal diferença entre o par de definição de uma valorização valor-transcendente e o par de definição de uma valorização resíduo-transcendente é o local em que se encontra δ. No caso da valorização resíduo-transcendente, temos que $\delta \in \overline{\nu}\overline{\mathbb{K}}$ e, no caso da valorização valor-transcendente, temos que $\delta \in \overline{\mu}(\overline{\mathbb{K}}[x]) \setminus \overline{\nu}\overline{\mathbb{K}}$.

Teorema 3.26. *Seja μ uma valorização em $\mathbb{K}[x]$. Se μ é valor-transcendente, então $\mu = \mu_Q$ para algum polinômio-chave $Q \in \mathbb{K}[x]$. Além disso, tomando $\overline{\mu}$ uma extensão de μ para $\overline{\mathbb{K}}[x]$, vemos que $\overline{\mu}$ admite par minimal de definição.*

Demonstração: Se $\text{supp}(\mu) = \langle Q \rangle$, com Q não nulo, então por definição $\epsilon(Q) = \infty$ e assim Q é polinômio-chave. Agora, dado $f \in \mathbb{K}[x]$, sendo $f = f_0 + \ldots + f_s Q^s$ sua Q-expansão, como $\deg(f_0) < \deg(Q)$, temos que $\mu(f_0) \neq \infty$ e

$$\mu(f) = \mu(f_0 + \ldots + f_s Q^s) = \mu(f_0) = \mu_Q(f).$$

Suponhamos agora que μ é valorização de Krull em $\mathbb{K}[x]$. Podemos estendê-la para $\mathbb{K}(x)$ naturalmente. Seja $\nu = \mu|_{\mathbb{K}}$. Tomemos uma extensão $\overline{\nu}$ de ν para $\overline{\mathbb{K}}$ e uma valorização $\overline{\mu}$ em $\overline{\mathbb{K}}(x)$ que estenda ambas $\overline{\nu}$ e μ. Temos que $\overline{\mu}$ também será valor-transcendente em $\overline{\mathbb{K}}[x]$. De fato, suponhamos por contradição que $\overline{\mu}(\overline{\mathbb{K}}[x])/\overline{\nu}\overline{\mathbb{K}}$ é de torção. Por hipótese, $\mu(\mathbb{K}[x])/\nu\mathbb{K}$ possui um elemento livre de torção, isto é, existe $\gamma \in \mu(\mathbb{K}[x])$ tal que $\gamma\mathbb{Z} \cap \nu\mathbb{K} = \{0\}$. Como $\mu(\mathbb{K}[x]) \subset \overline{\mu}(\overline{\mathbb{K}}[x])$ temos que $\gamma \in \overline{\mu}(\overline{\mathbb{K}}[x])$. Como estamos supondo $\overline{\mu}(\overline{\mathbb{K}}[x])/\overline{\nu}\overline{\mathbb{K}}$ de torção existe $s \in \mathbb{N}$ tal que $s\gamma \in \overline{\nu}\overline{\mathbb{K}}$. Mas, $\overline{\nu}\overline{\mathbb{K}} = \nu\mathbb{K} \otimes \mathbb{Q}$ (Proposição D.11), isto é, $s\gamma = \gamma' \otimes \frac{1}{m}$. Isso é o mesmo que dizer $ms\gamma = \gamma' \in \nu\mathbb{K}$ o que implicaria que γ é de torção sobre $\nu\mathbb{K}$ contradizendo a escolha que fizemos de γ. Logo, $\overline{\mu}(\overline{\mathbb{K}}[x])/\overline{\nu}\overline{\mathbb{K}}$ deve possuir um elemento livre de torção.

Pelo lema anterior, existem $a \in \overline{\mathbb{K}}$ e $\delta = \overline{\mu}(x-a) \in \overline{\mu}(\overline{\mathbb{K}}[x])$ tais que $\overline{\mu} = \overline{\mu}_{a,\delta}$. Podemos tomar a com grau minimal. Seja Q o polinômio minimal de a sobre $\mathbb{K}$. Assim, pelo Lema 3.10 e pelo Teorema 3.12, temos que (a, δ) é um par minimal de definição para $\overline{\mu}$ e Q é um polinômio-chave tal que $\mu = \mu_Q$.

■

Portanto, concluímos o seguinte.

Corolário 3.27. *Seja μ uma valorização em $\mathbb{K}[x]$. Temos que μ é transcendente se, e somente se, $\mu = \mu_Q$ para algum polinômio-chave $Q \in \mathbb{K}[x]$*

Demonstração: Basta juntarmos o Teorema 3.22, o Teorema 3.24 e o Teorema 3.26.

■

3.4 Uma relação entre os truncamentos $\overline{\mu}_{x-a}$ e μ_Q

Seja μ uma valorização em $\mathbb{K}(x)$ que é uma extensão resíduo-transcendente de uma valorização ν em $\mathbb{K}$. Estendemos μ para $\overline{\mathbb{K}}(x)$ e ν para $\overline{\mathbb{K}}$ como na Figura 3.2 a seguir, obtendo $\overline{\mu}$ e $\overline{\nu}$, respectivamente.

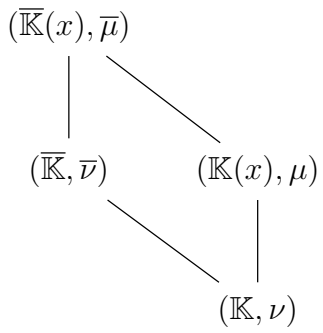


Figura 3.2: Diagrama das extensões

Pelo Teorema 3.22, existe um polinômio-chave $Q \in \mathbb{K}[x]$ tal que para alguma de suas raízes $a \in \overline{\mathbb{K}}$ temos $\delta = \delta(Q) = \overline{\mu}(x-a)$, $\overline{\mu} = \overline{\mu}_{a,\delta}$ em $\overline{\mathbb{K}}(x)$ e

$$\overline{\mu}|_{\mathbb{K}[x]} = \overline{\mu}_{a,\delta}|_{\mathbb{K}[x]} = \mu = \mu_Q.$$

Como, para esse valor de δ, temos $\overline{\mu}_{a,\delta} = \overline{\mu}_{x-a}$, terminamos concluindo como corolário que $\overline{\mu}_{x-a}$ coincide com μ_Q em $\mathbb{K}[x]$.

Seja agora $Q \in \mathbb{K}[x]$ um polinômio-chave previamente escolhido para μ. Considerando $a \in \overline{\mathbb{K}}$ uma raiz otimizadora de Q (isto é, uma raiz tal que $\delta(Q) = \overline{\mu}(x-a)$), nos perguntamos se é possível estabelecer uma relação de igualdade, como a anterior, entre os truncamentos $\overline{\mu}_{x-a}$ e μ_Q.

Consideremos $\nu, \mu, \overline{\nu}$ e $\overline{\mu}$ como anteriormente, porém agora a extensão $\mu \mid \nu$ não precisa ser necessariamente resíduo-transcendente. Seja $Q \in \mathbb{K}[x]$ um polinômio-chave qualquer para μ. Considerando $a \in \overline{\mathbb{K}}$ uma raiz otimizadora de Q, mostraremos nesta seção o segundo resultado principal deste trabalho: $\overline{\mu}_{x-a}|_{\mathbb{K}[x]} = \mu_Q$. Além disso, como μ_Q é de Krull, concluiremos também que $\overline{\mu}_{x-a} = \mu_Q$ em $\mathbb{K}(x)$.

A prova compreende dois casos principais: o caso em que $\mu(Q) \notin \overline{\nu}\overline{\mathbb{K}}$ e o caso em que $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$. O segundo caso requer argumentos mais elaborados do que o primeiro. Daremos duas provas para o caso $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$. A primeira prova segue a estrutura da demonstração originalmente apresentada nos trabalhos de Popescu e Popescu (1989) e de Alexandru, Popescu e Zaharescu (1988). Porém, daremos versões próprias de muitos dos resultados intermediários. A segunda prova segue a estrutura da demonstração apresentada por Bengus-Lasnier (2021), que é mais sintética que a anterior e se utiliza da estrutura do anel graduado associado a uma valorização.

3.4.1 O caso $\mu(Q) \notin \overline{\nu}\overline{\mathbb{K}}$

Para ambos os casos da demonstração principal, o seguinte lema se faz crucial.

Lema 3.28. *Sejam $f \in \overline{\mathbb{K}}[x]$ e $a \in \overline{\mathbb{K}}$ uma raiz otimizadora de f. Se $g \in \overline{\mathbb{K}}[x]$ é tal que $\delta(g) < \delta(f)$, então*

$$\overline{\mu}_{x-a}(g) = \overline{\mu}(g) = \overline{\nu}(g(a)) \text{ e } \left(\frac{g}{g(a)}\right)\overline{\mu}_{x-a} = 1.$$

Ainda, se $f = Q \in \mathbb{K}[x]$ é um polinômio-chave para μ, então

$$\overline{\mu}_{x-a}(Q) = \overline{\mu}(Q).$$

Demonstração: Uma vez que $\overline{\mathbb{K}}$ é algebricamente fechado, é suficiente mostrar a primeira parte do resultado para $g = x - c$, com $c \in \overline{\mathbb{K}}$. Sabemos que

$$\overline{\mu}(x-c) = \delta(g) < \delta(f) = \overline{\mu}(x-a).$$

Pelo Lema 3.4, segue que

$$\overline{\mu}_{x-a}(x-c) = \overline{\mu}(x-c) = \overline{\mu}(a-c).$$

Além disso,

$$\overline{\mu}(g-g(a)) = \overline{\mu}(x-a) > \overline{\mu}(x-c) = \overline{\mu}(a-c) = \overline{\mu}(g(a)).$$

Assim, temos

$$\overline{\mu}_{x-a}\left(\frac{g-g(a)}{g(a)}\right) > 0,$$

o que implica,

$$\left(\frac{g-g(a)}{g(a)}\right)\overline{\mu}_{x-a} = 0.$$

Portanto,

$$\left(\frac{g}{g(a)}\right)\overline{\mu}_{x-a} = \left(\frac{g(a)}{g(a)}\right)\overline{\mu}_{x-a} = 1.$$

Sejam Q um polinômio-chave e $a \in \overline{\mathbb{K}}$ uma raiz otimizadora de Q. Para cada raiz $c_i \in \overline{\mathbb{K}}$ de Q, sabemos que $\overline{\mu}(x-c_i) \leq \overline{\mu}(x-a)$. Pelo Lema 3.4, segue que $\overline{\mu}_{x-a}(x-c_i) = \overline{\mu}(x-c_i)$ para cada raiz c_i de Q. Usando o Axioma $(V1)$ concluímos que $\overline{\mu}_{x-a}(Q) = \overline{\mu}(Q)$.

■

Lema 3.29. *Seja (a,γ) um par minimal para μ, com $\gamma = \overline{\mu}(x-a)$. Para todo $f \in \mathbb{K}[x]$ com $\deg(f) < [\mathbb{K}(a):\mathbb{K}]$ vale $\delta(f) < \gamma$.*

Demonstração: Para qualquer raiz $b \in \overline{\mathbb{K}}$ de f, sabemos que

$$[\mathbb{K}(b):\mathbb{K}] \leq \deg(f) < [\mathbb{K}(a):\mathbb{K}].$$

Logo, pela definição de par minimal, $\overline{\mu}(b-a) < \gamma = \overline{\mu}(x-a)$. Suponhamos agora que b seja tal que $\delta(f) = \overline{\mu}(x-b)$. Assim,

$$\delta(f) = \overline{\mu}(x-b) = \overline{\mu}(x-a+(a-b)) = \overline{\mu}(a-b) < \gamma.$$

■

Observação 3.30. *Seja $g \in \mathbb{K}[x]$ tal que $\deg(g) < \deg(Q)$, com Q polinômio-chave. Sendo $a \in \overline{\mathbb{K}}$ uma raiz otimizadora de Q, sabemos que $(a, \delta(Q))$ é um par minimal (Teorema 3.11) e $\deg(Q) = [\mathbb{K}(a):\mathbb{K}]$. Logo, pelo Lema 3.29, $\delta(g) < \delta(Q)$ e, pelo Lema 3.28,*

$$\overline{\mu}_{x-a}(g) = \overline{\mu}(g) = \mu(g) = \mu_Q(g) = \overline{\nu}(g(a)) \text{ e } \overline{\mu}_{x-a}(g-g(a)) > \overline{\mu}_{x-a}(g(a)).$$

▼

Lema 3.31. *Para todo $f \in \mathbb{K}[x]$ não constante, temos que $\mu(f) \in \overline{\nu}\overline{\mathbb{K}}$ se, e somente se, $\delta(f) \in \overline{\nu}\overline{\mathbb{K}}$.*

Demonstração: Seja $a \in \overline{\mathbb{K}}$ uma raiz otimizadora de f. Escrevemos

$$f(x) = \prod_{i=1}^{k}(x-a_i)\prod_{j=k+1}^{n}(x-a_j)$$

em que $a = a_1$ e

$$\delta(f) = \overline{\mu}(x-a_1) = \ldots = \overline{\mu}(x-a_k) > \overline{\mu}(x-a_j)$$

para todo j, $k+1 \leq j \leq n$. Assim, $\delta(f) > \delta(x-a_j)$ e, pelo Lema 3.28, $\overline{\mu}(x-a_j) = \overline{\nu}(a-a_j) \in \overline{\nu}\overline{\mathbb{K}}$ para todo j, $k+1 \leq j \leq n$. Portanto, como

$$\mu(f) = \overline{\mu}(f) = k\delta(f) + \sum_{j=k+1}^{n}\overline{\mu}(x-a_j)$$

vemos que se $\delta(f) \in \overline{\nu}\overline{\mathbb{K}}$, então $\mu(f) \in \overline{\nu}\overline{\mathbb{K}}$.

Por outro lado, se $\mu(f) \in \overline{\nu}\overline{\mathbb{K}}$, então $k\delta(f) \in \overline{\nu}\overline{\mathbb{K}}$, isto é, $\delta(f) \in \overline{\nu}\overline{\mathbb{K}} \otimes \mathbb{Q} \cong \overline{\nu}\overline{\mathbb{K}}$.

■

Com o auxílio dos lemas anteriores, podemos demonstrar o resultado principal desta seção no caso em que $\mu(Q) \notin \overline{\nu\mathbb{K}}$.

Teorema 3.32. *Seja $Q \in \mathbb{K}[x]$ um polinômio-chave para μ. Seja $a \in \overline{\mathbb{K}}$ uma raiz de Q tal que $\delta(Q) = \overline{\mu}(x-a)$. Se $\mu(Q) \notin \overline{\nu\mathbb{K}}$, então $\overline{\mu}_{x-a} = \mu_Q$ em $\mathbb{K}(x)$.*

Demonstração: Para solucionarmos este caso, basta mostrarmos que $\mu = \mu_Q$ em $\mathbb{K}[x]$ e que $\overline{\mu}_{x-a} = \overline{\mu}$ em $\mathbb{K}(x)$, pois assim concluiremos que $\overline{\mu}_{x-a}|_{\mathbb{K}[x]} = \overline{\mu}|_{\mathbb{K}[x]} = \mu = \mu_Q$.

Mostremos inicialmente que $\mu(Q) \in \overline{\mu\mathbb{K}}(x) \setminus \overline{\nu\mathbb{K}}$ é livre de torção sobre $\overline{\nu\mathbb{K}}$. Se supormos por contradição que $\mu(Q)$ é de torção, então existe $b \in \mathbb{N}$ menor natural tal que $g = b\mu(Q) \in \overline{\nu\mathbb{K}}$. Mas $\overline{\nu\mathbb{K}}$ é divisível, logo para esse g e esse $b \in \mathbb{N}$ existe um elemento $h \in \overline{\nu\mathbb{K}}$ tal que $g = b\mu(Q) = bh$, o que implica, $b(\mu(Q) - h) = 0$. Porém, $\overline{\nu\mathbb{K}}$ é livre de torção, logo a última igualdade só é possível se $\mu(Q) = h \in \overline{\nu\mathbb{K}}$, o que contradiz $\mu(Q) \in \overline{\mu\mathbb{K}}(x) \setminus \overline{\nu\mathbb{K}}$. Logo $\mu(Q)$ é livre de torção sobre $\overline{\nu\mathbb{K}}$ e, em particular, é livre de torção sobre $\nu\mathbb{K}$.

Agora, vejamos que $\mu = \mu_Q$ em $\mathbb{K}[x]$. Para qualquer $f \in \mathbb{K}[x]$ com $\deg(f) < \deg(Q)$, sabemos pelo Lema 3.28 que $\mu(f) = \mu(f(a)) \in \overline{\nu\mathbb{K}}$. Ou seja, $\mu(f)$ é de torção sobre $\nu\mathbb{K}$ para todo f com $\deg(f) < \deg(Q)$. Portanto, aplicando o Lema 3.23 para μ e Q, temos que $\mu = \mu_Q$.

Para mostrar que $\overline{\mu}_{x-a} = \overline{\mu}$ em $\mathbb{K}(x)$ basta lembrarmos que $\mu(Q) \in \overline{\nu\mathbb{K}}$ se, e somente se, $\delta(Q) \in \overline{\nu\mathbb{K}}$ (Lema 3.31). Assim, como estamos supondo que $\mu(Q) \notin \overline{\nu\mathbb{K}}$, temos que $\delta(Q) \notin \overline{\nu\mathbb{K}}$. Mas, usando que $\overline{\nu\mathbb{K}}$ é divisível concluímos que $\delta(Q) = \overline{\mu}(x-a)$ é livre de torção sobre $\overline{\nu\mathbb{K}}$. Pelo Lema 3.23, aplicado para $\overline{\mu}$ e $x-a$, segue que $\overline{\mu}_{x-a} = \overline{\mu}$.

■

3.4.2 O caso $\mu(Q) \in \overline{\nu\mathbb{K}}$: primeira prova

A primeira prova que apresentaremos para o caso em que $\mu(Q) \in \overline{\nu\mathbb{K}}$ utiliza apenas os conhecimentos sobre valorizações que desenvolvemos até o momento e os argumentos envolvem, principalmente, os corpos de resíduo das valorizações em questão. Essa prova foi apresentada originalmente nos trabalhos de Popescu e Popescu (1989) e de Alexandru, Popescu e Zaharescu (1988).

Iniciaremos o caminho até essa primeira prova com uma sequência de resultados auxiliares. Começamos exibindo um elemento transcendente para a extensão de corpos $\mathbb{K}(x)\mu_Q \mid \mathbb{K}\nu$, construído a partir de Q. Para isso, usaremos dois lemas. O primeiro é um derivado do Lema 2.22 aplicado para μ_Q.

Lema 3.33. *Seja μ uma valorização em $\mathbb{K}[x]$, Q um polinômio-chave para μ e considere a valorização μ_Q em $\mathbb{K}[x]$. As seguintes afirmações são satisfeitas.*

1. *O polinômio Q é um polinômio-chave para μ_Q.*
2. *Tomemos $h_1, \ldots, h_s \in \mathbb{K}[x]$ com $\deg(h_i) < \deg(Q)$ para todo i, $1 \leq i \leq s$. Se*

$$\prod_{i=1}^{s} h_i = lQ + p$$

com $\deg(p) < \deg(Q)$, então

$$\mu_Q\left(\prod_{i=1}^{s} h_i\right) = \mu_Q(p) < \mu_Q(lQ).$$

Demonstração:

1. Notamos que se $\deg(f) < \deg(Q)$, então $\deg(\partial_b f) \leq \deg(f) < \deg(Q)$ para todo b, $1 \leq b \leq \deg(f)$. Denotemos por $\epsilon_Q(f)$ o valor ϵ associado a f com relação à valorização μ_Q. Portanto,

$$\epsilon_Q(f) := \max_{1 \leq b \leq \deg(f)} \left\{ \frac{\mu_Q(f) - \mu_Q(\partial_b f)}{b} \right\} = \max_{1 \leq b \leq \deg(f)} \left\{ \frac{\mu(f) - \mu(\partial_b f)}{b} \right\} =: \epsilon(f).$$

   Usando a mesma argumentação acima e a definição de μ_Q, concluímos que $\epsilon_Q(Q) = \epsilon(Q)$. Dessa forma, como Q é polinômio-chave para μ, temos $\epsilon(f) < \epsilon(Q)$, o que é o mesmo que $\epsilon_Q(f) < \epsilon_Q(Q)$. Portanto, Q é um polinômio-chave para μ_Q.

2. Segue do Lema 2.22, aplicado para μ_Q.

■

Lema 3.34. *Seja Q um polinômio-chave para μ e tomemos*

$$f = f_0 + f_1 Q + \ldots + f_s Q^s$$

em que cada f_i é o produto de polinômios de grau menor do que $n = \deg(Q)$. Então

$$\mu_Q(f) = \min_{0 \leq i \leq s} \{\mu(f_i Q^i)\}.$$

Demonstração: Para cada i, $0 \leq i \leq s$, escrevemos $f_i = q_i Q + r_i$ com $\deg(r_i) < n$. Pelo Lema 3.33, temos

$$\mu_Q(f_i) = \mu(f_i) = \mu_Q(r_i) < \mu_Q(q_i Q).$$

Seja $g = r_0 + r_1Q + \ldots + r_sQ^s$ e tomemos $m \in \mathbb{N}$ tal que $\mu_Q(g) = \mu(r_mQ^m)$. Então, para todo i, concluímos que

$$\mu_Q(q_iQ^{i+1}) > \mu(r_iQ^i) \geq \mu(r_mQ^m).$$

Como

$$f - g = \sum_{i=0}^{s} q_iQ^{i+1},$$

obtemos que

$$\mu_Q(f - g) > \mu(r_mQ^m) = \mu_Q(g).$$

Dessa forma, $\mu_Q(f) = \mu_Q(g)$. Consequentemente

$$\mu_Q(f) \geq \min_{0\leq i\leq s}\{\mu(f_iQ^i)\} = \min_{0\leq i\leq s}\{\mu(r_iQ^i)\} = \mu_Q(g) = \mu_Q(f).$$

■

Observação 3.35. *O Lema 3.34 continua verdadeiro se algum dos coeficientes f_i é nulo. Nesse caso, colocamos $q_i = r_i = 0$ onde for preciso.*

▼

Proposição 3.36. *Seja Q um polinômio-chave para μ e suponhamos que existe $e \in \mathbb{N}$ tal que $\mu(Q^e) = \mu(h)$, em que $h \in \mathbb{K}[x]$ satisfaz $\deg(h) < \deg(Q)$. Definimos $\zeta = \frac{Q^e}{h}$. Então o resíduo de ζ em $\mathbb{K}(x)\mu_Q$ é transcendente sobre $\mathbb{K}\nu$. Em particular, o resíduo de ζ em $\mathbb{K}(x)\mu_Q$ é transcendente sobre qualquer extensão algébrica de $\mathbb{K}\nu$ contida em $\mathbb{K}(x)\mu_Q$.*

Demonstração: De imediato vemos que $\mu_Q(\zeta) = 0$. Suponhamos que existam $b_0, \ldots, b_s \in \mathbb{K}$ tais que $\nu(b_i) \geq 0$ para todo i, $0 \leq i \leq s$, e

$$\sum_{i=0}^{s}(b_i\mu_Q)(\zeta\mu_Q)^i = \sum_{i=0}^{s}\left(b_i\frac{Q^{ei}}{h^i}\right)\mu_Q = 0.$$

Então,

$$0 = \sum_{i=0}^{s}\left(b_i\frac{Q^{ei}}{h^i}\right)\mu_Q = \left(\frac{h^sb_0 + h^{s-1}b_1Q^e + \ldots + b_sQ^{es}}{h^s}\right)\mu_Q.$$

Dessa forma,

$$\mu_Q(h^sb_0 + h^{s-1}b_1Q^e + \ldots + b_sQ^{es}) > \mu_Q(h^s).$$

Pela definição de h, temos

$$\mu_Q(h^s) = se\mu(Q).$$

Também vemos que

$$\begin{aligned}\mu_Q(h^{s-i}b_iQ^{ei}) &= (s-i)\mu_Q(h) + \mu_Q(b_i) + ei\mu_Q(Q)\\ &= (s-i)e\mu(Q) + \mu_Q(b_i) + ei\mu(Q)\\ &= \mu_Q(b_i) + se\mu(Q) \geq se\mu(Q).\end{aligned}$$

Suponhamos, buscando uma contradição, que existe j, $0 \leq j \leq s$, tal que $b_j\mu_Q \neq 0$. Então $\nu(b_j) = 0$ e teríamos que

$$\mu_Q(h^s) = \min_{0\leq i\leq s}\{\mu_Q(h^{s-i}b_iQ^{ei})\} = \min_{0\leq i\leq s}\{\mu(h^{s-i}b_iQ^{ei})\}.$$

Logo,

$$\mu_Q(h^sb_0 + h^{s-1}b_1Q^e + \ldots + b_sQ^{es}) > \min_{0\leq i\leq s}\{\mu(h^{s-i}b_iQ^{ei})\}.$$

Porém, isso contradiz o Lema 3.34. Portanto, devemos ter $b_i\mu_Q = 0$ para todo i, $0 \leq i \leq s$. Isso significa que $\zeta\mu_Q \in \mathbb{K}(x)\mu_Q$ é transcendente sobre $\mathbb{K}\nu$.

■

Em seguida, provaremos que o resíduo de $\zeta = \frac{Q^e}{h}$ em $\mathbb{K}(x)\overline{\mu}_{x-a}$ também é transcendente sobre $\mathbb{K}\nu$ (Proposição 3.39). Usaremos os seguintes lemas.

Lema 3.37. *Seja $a \in \overline{\mathbb{K}}$ uma raiz otimizadora do polinômio-chave Q. Suponhamos $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$. Seja $d_a \in \overline{\mathbb{K}}$ tal que $\overline{\mu}(x-a) = \delta(Q) = \overline{\nu}(d_a) \in \overline{\nu}\overline{\mathbb{K}}$. Para $b \in \overline{\mathbb{K}}$, suponhamos que exista $d_b \in \overline{\mathbb{K}}$ tal que $\overline{\mu}(x-b) = \overline{\nu}(d_b)$. Temos o seguinte:*

1. *O elemento $y = \dfrac{x-a}{d_a}\overline{\mu}_{x-a} \in \overline{\mathbb{K}}(x)\overline{\mu}_{x-a}$ é transcendente sobre $\overline{\mathbb{K}}\overline{\nu}$.*
2. *Se $\overline{\mu}(x-b) \leq \overline{\mu}(x-a)$, então $\overline{\mu}\left(\dfrac{x-b}{d_b}\right) = 0$ e $\dfrac{x-b}{d_b}\overline{\mu}_{x-a} \in \overline{\mathbb{K}}\overline{\nu}[y]$.*

Demonstração:

1. Segue do Lema 3.36 aplicado para $\overline{\mu}$ e seu polinômio-chave $x-a$.
2. Suponhamos $\overline{\mu}(x-b) \leq \overline{\mu}(x-a)$. Pelo Lema 3.4, segue que

$$\overline{\mu}(a-b) \geq \overline{\mu}(x-b) \text{ e } \overline{\mu}_{x-a}(x-b) = \overline{\mu}(x-b).$$

Dessa forma,

$$\overline{\mu}_{x-a}\left(\frac{x-b}{d_b}\right) \geq 0,\ \overline{\mu}_{x-a}\left(\frac{a-b}{d_b}\right) \geq 0 \text{ e } \overline{\mu}_{x-a}\left(\frac{x-a}{d_b}\right) \geq 0.$$

Portanto,

$$\begin{aligned}\frac{x-b}{d_b}\overline{\mu}_{x-a} &= \frac{x-a+a-b}{d_b}\overline{\mu}_{x-a}\\ &= \frac{x-a}{d_b}\overline{\mu}_{x-a}+\frac{a-b}{d_b}\overline{\mu}_{x-a}\\ &= y\frac{d_a}{d_b}\overline{\mu}_{x-a}+\frac{a-b}{d_b}\overline{\mu}_{x-a}\in\overline{\mathbb{K}}\overline{\nu}[y].\end{aligned}$$

■

Observação 3.38. *Se existe $e \in \mathbb{N}$ tal que $\mu(Q^e) = \mu(h)$, para algum $h \in \mathbb{K}[x]$ com $\deg(h) < \deg(Q)$, então $\mu(Q) \in \nu\overline{\mathbb{K}}$. De fato, pela Observação 3.30 temos que*

$$e\mu(Q) = \mu(h) = \nu(h(a)) \in \nu\overline{\mathbb{K}}.$$

Como $\nu\overline{\mathbb{K}}$ é um grupo divisível, segue que existe $c \in \overline{\mathbb{K}}$ tal que $\nu(h(a)) = e\nu(c)$. Logo, $e(\mu(Q) - \nu(c)) = 0$. Como $\nu\overline{\mathbb{K}}$ é livre de torção, concluímos que $\mu(Q) = \nu(c) \in \nu\overline{\mathbb{K}}$.

Por outro lado, se assumirmos que $\mu(Q) \in \nu\overline{\mathbb{K}}$, como $\nu\overline{\mathbb{K}}$ é o fecho divisível de $\nu\mathbb{K}$, então existe $e \in \mathbb{N}$ tal que $e\nu(Q) \in \nu\mathbb{K}$. Portanto, essas duas condições são equivalentes.

▼

Proposição 3.39. *Seja Q um polinômio-chave para μ e suponhamos que existe $e \in \mathbb{N}$ tal que $\mu(Q^e) = \mu(h)$, em que $h \in \mathbb{K}[x]$ satisfaz $\deg(h) < \deg(Q)$. Definimos $\zeta = \frac{Q^e}{h}$. Então o resíduo de ζ em $\overline{\mathbb{K}}(x)\overline{\mu}_{x-a}$ é transcendente sobre $\overline{\mathbb{K}}\overline{\nu}$.*

Demonstração: Pela Observação 3.30, vemos que $\overline{\mu}_{x-a}(\zeta) = 0$. Sejam $a = a_1, \ldots, a_n \in \overline{\mathbb{K}}$ todas as raízes de Q. Escrevemos

$$Q = \prod_{i=1}^{k}(x - a_i)\prod_{j=k+1}^{n}(x - a_j) \in \overline{\mathbb{K}}(x),$$

com $a_1 = a$,

$$\delta(Q) = \overline{\mu}(x - a_1) = \ldots = \overline{\mu}(x - a_k) > \overline{\mu}(x - a_j)$$

para todo j, $k + 1 \leq j \leq n$. Então, pela Observação 3.30,

$$\overline{\mu}_{x-a}(x - a_j) = \overline{\nu}(a - a_j) = \overline{\nu}(d_j),$$

em que $d_j = a - a_j$. Pela Observação 3.38, temos que $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$. Logo, $\delta(Q) = \overline{\mu}(x-a) \in \overline{\nu}\overline{\mathbb{K}}$ pelo Lema 3.31. Dessa forma, existe $d_1 \in \overline{\mathbb{K}}$ tal que $\overline{\mu}(x - a) = \overline{\nu}(d_1)$. Logo, para todo i, $2 \leq i \leq k$,

$$\overline{\mu}_{x-a}(x - a_i) = \min\{\overline{\nu}(a - a_i), \overline{\mu}(x - a)\} = \min\{\overline{\nu}(a - a_i), \overline{\nu}(d_1)\} := \overline{\nu}(d_i),$$

em que $d_i \in \{a - a_i, d_1\}$. Então, $\overline{\mu}_{x-a}((x-a_i)/d_i) = 0$ e $\overline{\mu}_{x-a}((x-a_j)/d_j) = 0$.

Seja $d = d_1 \cdots d_n$ e $y = \dfrac{x-a}{d_1}\overline{\mu}_{x-a} \in \overline{\mathbb{K}}(x)\overline{\mu}_{x-a}$ Temos, pelo Lema 3.37,

$$\begin{aligned}\left(\frac{Q^e}{h}\right)\overline{\mu}_{x-a} &= \left(\frac{d^e}{h}\frac{Q^e}{d^e}\right)\overline{\mu}_{x-a} = \left(\frac{d^e}{h}\right)\overline{\mu}_{x-a}\left(\frac{Q^e}{d^e}\right)\overline{\mu}_{x-a} \\ &= \left(\frac{d^e}{h}\right)\overline{\mu}_{x-a}\left(\prod_{i=1}^{n}\frac{(x-a_i)^e}{d_i^e}\right)\overline{\mu}_{x-a} \\ &= y^e\left(\frac{d^e}{h(a)}\right)\overline{\nu}\left(\prod_{i=2}^{k}p_i(y)\right)\overline{\mu}_{x-a} \\ &= yp(y) \in \overline{\mathbb{K}}\overline{\nu}[y] \setminus \overline{\mathbb{K}}\overline{\nu}.\end{aligned}$$

Como y é transcendente sobre $\overline{\nu}\overline{\mathbb{K}}$, concluímos que $yp(y) = \zeta\overline{\mu}_{x-a}$ é também transcendente sobre $\overline{\nu}\overline{\mathbb{K}}$.

■

A seguir trabalharemos com o corpo $\mathbb{K}(a)\overline{\nu}$, em que a é uma raiz otimizadora de um polinômio-chave Q. Consideremos a restrição $\overline{\nu}|_{\mathbb{K}(a)}$. Como $\mathbb{K}(a)$ é a extensão simples de $\mathbb{K}$ obtida a partir de a, todos os elementos dessa extensão são da forma $g(a)$, em que $g \in \mathbb{K}[x]$ e $\deg(g) < \deg(Q) = [\mathbb{K}(a) : \mathbb{K}]$. Assim, pela Observação 3.30 temos

$$\mu_Q(g) = \mu(g) = \overline{\nu}(g(a)).$$

Vejamos que a aplicação Φ, dada por

$$\Phi : \mathbb{K}(a)\overline{\nu} \longrightarrow \mathbb{K}[x]\mu_Q$$

$$g(a)\overline{\nu} \longmapsto g(x)\mu_Q,$$

é um homomorfismo de anéis bem definido e que, além disso, tal aplicação é injetora. De fato, dados $f, g \in \mathbb{K}[x]$ com $\deg(f), \deg(g) < \deg(Q)$ e tais que $\overline{\nu}(f(a)) = \overline{\nu}(g(a)) = 0$, temos que

$$\begin{aligned}f(a)\overline{\nu} = g(a)\overline{\nu} &\iff \overline{\nu}(f(a) - g(a)) > 0 \\ &\iff \mu_Q((f-g) > 0 \\ &\iff f\mu_Q = g\mu_Q.\end{aligned}$$

Segue que a aplicação está bem definida e é injetora. Além disso,

$$\mu_Q(f+g) = \overline{\nu}(f(a) + g(a)) \geq 0.$$

Logo,

$$\begin{aligned}\Phi(f(a)\overline{\nu}+g(a)\overline{\nu}) &= \Phi((f(a)+g(a))\overline{\nu})\\ &= (f+g)\mu_Q\\ &= f\mu_Q+g\mu_Q\\ &= \Phi(f(a)\overline{\nu})+\Phi(g(a)\overline{\nu}).\end{aligned}$$

Agora, escrevendo $fg = qQ + r$, usamos o Lema 3.33 para concluirmos que

$$\mu_Q(fg-r) > \mu_Q(r) = \overline{\nu}(r(a)) = \overline{\nu}(f(a)) + \overline{\nu}(g(a)) = 0.$$

Dessa forma,

$$(f(a)g(a))\overline{\nu} = r(a)\overline{\nu} \text{ e } (fg)\mu_Q = r(a)\mu_Q.$$

Logo,

$$\begin{aligned}\Phi(f(a)\overline{\nu}g(a)\overline{\nu}) &= \Phi(r(a)\overline{\nu})\\ &= r\mu_Q\\ &= (fg)\mu_Q\\ &= \Phi(f(a)\overline{\nu})\Phi(g(a)\overline{\nu}).\end{aligned}$$

Por isso, podemos dizer que há um mergulho $\mathbb{K}(a)\overline{\nu} \hookrightarrow \mathbb{K}(x)\mu_Q$. Como a extensão $\overline{\mathbb{K}} \mid \mathbb{K}(a)$ é algébrica, pela Proposição D.10 sabemos que o grupo quociente $\overline{\nu}\overline{\mathbb{K}}/\overline{\nu}\mathbb{K}(a)$ é de torção.

Como vimos na Observação 3.38, se supormos que $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$, então existe $e \in \mathbb{N}$ tal que $e\mu(Q) \in \nu'\mathbb{K}(a)$. Podemos tomar esse inteiro positivo como o menor com essa propriedade. Tal minimalidade será útil no que se segue.

Corolário 3.40. *Suponhamos $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ e tomemos $e \in \mathbb{N}$ o menor inteiro positivo tal que $e\mu(Q) \in \overline{\nu}\mathbb{K}(a)$. Escolhemos $h \in \mathbb{K}[x]$ com $\deg(h) < \deg(Q)$ e tal que $e\mu(Q) = \overline{\nu}(h(a))$. Definimos $\zeta = \frac{Q^e}{h}$. Então os elementos*

$$\zeta\mu_Q \in \mathbb{K}(x)\mu_Q \text{ e } \zeta\overline{\mu}_{x-a} \in \overline{\mathbb{K}}(x)\overline{\mu}_{x-a}$$

são transcendentes sobre $\mathbb{K}(a)\overline{\nu}$.

Demonstração: A prova segue direto da Proposição 3.36 e da Proposição 3.39.

■

Usando esse elemento ζ e o inteiro positivo e acima podemos provar, quando $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$, que a igualdade desejada vale no corpo intermediário $\mathbb{K}(\zeta)$ e, inicialmente, para todos os polinômios com grau menor do que ne, em que $n = \deg(Q)$. Estes resultados interme-

diários nos ajudarão com o caso geral.

Lema 3.41. *Suponhamos $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$. Sejam $e \in \mathbb{N}$ o menor inteiro positivo tal que $e\mu(Q) \in \mathbb{K}(a)\overline{\nu}$ e $n = \deg(Q)$. Se $g \in \mathbb{K}[x]$ é tal que $\deg(g) < ne$, então $\overline{\mu}_{x-a}(g) = \mu_Q(g)$.*

Demonstração: Seja $g \in \mathbb{K}[x]$ com $\deg(g) < ne$. Ao escrever a Q-expansão de g obtemos

$$g = \sum_{i=0}^{e-1} g_i Q^i,$$

em que $\deg(g_i) < n$. Afirmamos que $\overline{\mu}_{x-a}(g) = \min_{0\leq i\leq e-1}\{\overline{\mu}_{x-a}(g_i) + i\overline{\mu}_{x-a}(Q)\}$. De fato, caso contrário, deveriam existir i_0 e i_1, $0 \leq i_0 < i_1 \leq e-1$, tais que

$$\overline{\mu}_{x-a}(g_{i_0}) + i_0\overline{\mu}_{x-a}(Q) = \overline{\mu}_{x-a}(g_{i_1}) + i_1\overline{\mu}_{x-a}(Q).$$

Logo,

$$\overline{\mu}_{x-a}(g_{i_0}) - \overline{\mu}_{x-a}(g_{i_1}) = (i_1 - i_0)\overline{\mu}_{x-a}(Q) = (i_1 - i_0)\mu(Q).$$

Como pela Observação 3.30 temos que $\overline{\mu}_{x-a}(g_i) = \overline{\nu}(g_i(a)) \in \overline{\nu}\mathbb{K}(a)$ para todo i, segue que $(i_1-i_0)\mu(Q) \in \overline{\nu}\mathbb{K}(a)$. Como $i_1 - i_0 < e$, estamos contradizendo a minimalidade de e. Portanto,

$$\overline{\mu}_{x-a}(g) = \min_{0\leq i\leq e-1}\{\overline{\mu}_{x-a}(g_i) + i\overline{\mu}_{x-a}(Q)\} = \min_{0\leq i\leq e-1}\{\mu(g_i) + i\mu(Q)\} = \mu_Q(g).$$

■

Lema 3.42. *Suponhamos $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$. Sejam $e \in \mathbb{N}$ o menor inteiro positivo tal que $e\mu(Q) \in \mathbb{K}(a)\overline{\nu}$ e $n = \deg(Q)$. Tomemos $f, g \in \mathbb{K}[x]$ tais que $\deg(f), \deg(g) < ne$ e seja $u = f/g$. Se $\overline{\mu}_{x-a}(u) = 0$, então $u\overline{\mu}_{x-a}$ é algébrico sobre $\mathbb{K}\nu$.*

Demonstração: Como $\deg(f), \deg(g) < ne$, as Q-expansões desses polinômios são da forma

$$f = \sum_{i=0}^{e-1} f_i Q^i \text{ and } g = \sum_{i=0}^{e-1} g_i Q^i,$$

com $\deg(f_i)\deg(g_i) < n$. Estamos supondo $\overline{\mu}_{x-a}(u) = 0$. Então, pelo Lema 3.41,

$$\overline{\mu}_{x-a}(u) = \overline{\mu}_{x-a}(f) - \overline{\mu}_{x-a}(g) = \min_{0\leq i\leq e-1}\{\overline{\mu}_{x-a}(f_i r^i)\} - \min_{0\leq i\leq e-1}\{\overline{\mu}_{x-a}(g_i r^i)\} = 0$$

Dessa forma, existem i e j tais que $\overline{\mu}_{x-a}(f_i r^i) = \overline{\mu}_{x-a}(g_j r^j)$. Pela minimalidade de e concluímos que $i = j = i_0$ e i_0 é único. Escrevendo

$$u = \frac{f_{i_0}}{g_{i_0}} \frac{\frac{f_0}{f_{i_0} r^{i_0}} + \ldots + 1 + \ldots + \frac{f_{e-1} r^{e-1}}{f_{i_0} r^{i_0}}}{\frac{g_0}{g_{i_0} r^{i_0}} + \ldots + 1 + \ldots + \frac{g_{e-1} r^{e-1}}{g_{i_0} r^{i_0}}},$$

vemos que

$$u\overline{\mu}_{x-a} = \frac{f_{i_0}}{g_{i_0}}\overline{\mu}_{x-a}.$$

Agora escrevemos

$$f_{i_0} = b\prod_{j=1}^{s}(x-b_i) \text{ and } g_{i_0} = c\prod_{k=1}^{l}(x-c_i),$$

com $b_i, c_i \in \overline{\mathbb{K}}$. Como $\deg(f_{i_0}), \deg(g_{i_0}) < n$, concluímos pela Observação 3.30 e pelo Lema 3.37 que existem $d_j, m_k \in \overline{\mathbb{K}}$ tais que

$$\frac{x-b_i}{d_i}\overline{\mu}_{x-a} \text{ e } \frac{x-c_i}{m_i}\overline{\mu}_{x-a}$$

são algébricos sobre $\mathbb{K}\nu$. Denotamos $d = d_1 \cdots d_s$ e $m = m_1 \cdots m_l$. Portanto,

$$u\overline{\mu}_{x-a} = \frac{f_{i_0}}{g_{i_0}}\overline{\mu}_{x-a} = \left(\frac{d}{m}\frac{f_{i_0}}{d}\frac{m}{g_{i_0}}\right)\overline{\mu}_{x-a}$$

é algébrico sobre $\mathbb{K}\nu$.

■

Lema 3.43. *Suponhamos $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ e seja $\zeta = \frac{Q^e}{h}$ como no Corolário 3.40. Seja $g = t_0 + t_1\zeta + \ldots + t_s\zeta^s$, em que $t_i \in \mathbb{K}[x]$ e $\deg(t_i) < ne$. Então*

$$\overline{\mu}_{x-a}(g) = \min_{0\leq i\leq s}\{\overline{\mu}_{x-a}(t_i)\}.$$

Demonstração: Sabemos que

$$\overline{\mu}_{x-a}(g) \geq \min_{0\leq i\leq s}\{\overline{\mu}_{x-a}(t_i\zeta^i)\} = \min_{0\leq i\leq s}\{\overline{\mu}_{x-a}(t_i) + i\overline{\mu}_{x-a}(\zeta)\} = \min_{0\leq i\leq s}\{\overline{\mu}_{x-a}(t_i)\},$$

pois $\overline{\mu}_{x-a}(\zeta) = 0$. Se caso $\overline{\mu}_{x-a}(g) > \min_{0\leq i\leq s}\{\overline{\mu}_{x-a}(t_i)\}$, então existiriam i_0 e i_1, com $0 \leq i_0 < i_1 \leq s$, tais que

$$\overline{\mu}_{x-a}(t_{i_0}) = \overline{\mu}_{x-a}(t_{i_1}) = \min_{0\leq i\leq s}\{\overline{\mu}_{x-a}(t_i)\}.$$

Consequentemente, $\overline{\mu}_{x-a}(t_{i_0}) \neq \infty$ e $t_{i_0} \neq 0$. Tomemos $gt_{i_0}^{-1}$. Temos $\overline{\mu}_{x-a}(gt_{i_0}^{-1}) > 0$ pois, caso contrário, $\overline{\mu}_{x-a}(gt_{i_0}^{-1}) = 0$ implicaria $\overline{\mu}_{x-a}(g) = \overline{\mu}_{x-a}(t_{i_0})$, contradizendo o que assumimos. Logo,

$$(gt_{i_0}^{-1})\overline{\mu}_{x-a} = \left(\sum_{i=0}^{s}\frac{t_i}{t_{i_0}}\zeta^i\right)\overline{\mu}_{x-a} = \zeta^{i_0}\overline{\mu}_{x-a} + \sum_{\substack{i=0\\ i\neq i_0}}^{s}\left(\frac{t_i}{t_{i_0}}\zeta^i\right)\overline{\mu}_{x-a} = 0$$

em $\mathbb{K}(x)\overline{\mu}_{x-a}$. Vimos no Lema 3.42 que todos os elementos $(t_i/t_{i_0})\overline{\mu}_{x-a}$ que são não nulos (isto é, aqueles com $\overline{\mu}_{x-a}(t_i/t_{i_0}) = 0$) são algébricos sobre $\nu\mathbb{K}$. Como existe ao menos um desses que

é não nulo, a saber $(t_{i_1}/t_{i_0})\overline{\mu}_{x-a}$, concluiríamos que o resíduo de ζ é algébrico sobre $\mathbb{K}\nu$, o que é uma contradição. Portanto, tais i_0 e i_1 não existem e $\overline{\mu}_{x-a}(g) = \min_{0\leq i\leq s}\{\overline{\mu}_{x-a}(t_i)\}$.

■

Lema 3.44. *Suponhamos $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ e seja $\zeta = \frac{Q^e}{h}$ como no Corolário 3.40. Seja $g = t_0 + t_1\zeta + \ldots + t_s\zeta^s$, em que $t_i \in \mathbb{K}[x]$ e $\deg(t_i) < ne$. Então*

$$\overline{\mu}_{x-a}(g) = \mu_Q(g).$$

Em particular, $\overline{\mu}_{x-a} = \mu_Q$ em $\mathbb{K}(\zeta)$.

Demonstração: Pelo Lema 3.43, $\overline{\mu}_{x-a}(g) = \min_{0\leq i\leq s}\{\overline{\mu}_{x-a}(t_i)\}$. Aplicando o Lema 3.42 e o Lema 3.43 para μ e Q concluímos que $\mu_Q(g) = \min_{0\leq i\leq s}\{\mu_Q(t_i)\}$. Pelo Lema 3.41, como $\deg(t_i) < ne$, temos $\overline{\mu}_{x-a}(t_i) = \mu_Q(t_i)$. Portanto, segue a igualdade.

■

Agora temos o que é necessário para a primeira demonstração to resultado principal desta seção no caso em que $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$.

Teorema 3.45. *Seja $Q \in \mathbb{K}[x]$ um polinômio-chave para μ. Seja $a \in \overline{\mathbb{K}}$ uma raiz de Q tal que $\delta(Q) = \overline{\mu}(x-a)$. Se $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$, então $\overline{\mu}_{x-a} = \mu_Q$ em $\mathbb{K}(x)$.*

Demonstração: Consideremos o corpo $\mathbb{K}(r)$, com ζ como no Corolário 3.40. A extensão $\mathbb{K}(x) \mid \mathbb{K}(\zeta)$ é algébrica e possui grau ne. Além disso, podemos ver $\mathbb{K}(x)$ como $\mathbb{K}(\zeta)(x)$. Cada elemento $f(x) \in \mathbb{K}(x)$ pode ser escrito na forma

$$f(x) = \sum_{i=0}^{ne-1} f_i(\zeta)x^i$$

em que $f_i(\zeta) \in \mathbb{K}(\zeta)$. Seja, para cada i,

$$f_i(\zeta) = \frac{g_i(\zeta)}{l(\zeta)},$$

$g_i, l \in \mathbb{K}[\zeta]$. Assim,

$$f = \frac{g_0(\zeta) + g_1(\zeta)x + \ldots + g_{ne-1}x^{ne-1}}{l(\zeta)}.$$

Reescrevendo o numerador de f como um polinômio em ζ obtemos

$$f = \frac{t_0(x) + t_1(x)\zeta + \ldots + t_s(x)\zeta^s}{l(\zeta)},$$

em que $t_i(x) \in \mathbb{K}[x]$, $\deg(t_i(x)) < ne$ para todo i, $0 \leq i \leq s$. Temos

$$\overline{\mu}_{x-a}(f) = \overline{\mu}_{x-a}(t_0 + t_1\zeta + \ldots + t_s\zeta^s) - \overline{\mu}_{x-a}(l(\zeta)).$$

Sabemos, pelo Lema 3.44 que $\overline{\mu}_{x-a}(l(\zeta)) = \mu_Q(l(\zeta))$ e

$$\overline{\mu}_{x-a}(t_0 + t_1\zeta + \ldots + t_s\zeta^s) = \mu_Q(t_0 + t_1\zeta + \ldots + t_s\zeta^s).$$

Portanto $\overline{\mu}_{x-a}(f) = \mu_Q(f)$.

■

3.4.3 O caso $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$: segunda prova

A segunda prova para o Teorema 3.45 fará uso de uma estrutura de anel graduado que associaremos às valorizações em questão. Esse ferramental teórico nos levará a uma prova que sintetizará os extensos argumentos da demonstração apresentada na seção anterior. Essa prova foi elaborada por Bengus-Lasnier (2021).

Iniciaremos apresentando a estrutura de anel graduado associado a uma valorização que pode ser descrita como um truncamento. Seja μ uma valorização em $\mathbb{K}[x]$ e suponhamos que $q \in \mathbb{K}[x]$ seja tal que μ_q é uma valorização. Para cada $\gamma \in \mu_q(\mathbb{K}[x])$, consideremos os grupos abelianos

$$\mathcal{P}_\gamma = \{f \in \mathbb{K}[x] \mid \mu_q(f) \geq \gamma\} \text{ e } \mathcal{P}^+_\gamma = \{f \in \mathbb{K}[x] \mid \mu_q(f) > \gamma\}.$$

Definição 3.46. *O anel graduado associado à μ_q é definido por*

$$\mathcal{G}_q = \mathrm{gr}_{\mu_q}(\mathbb{K}[x]) := \bigoplus_{\gamma \in \mu_q(\mathbb{K}[x])} \mathcal{P}_\gamma/\mathcal{P}^+_\gamma.$$

■

A soma em $\mathcal{G}_q$ é feita coordenada a coordenada e o produto é dado estendendo o produto de elementos homogêneos, que por sua vez é descrito por

$$\left(f + \mathcal{P}^+_\beta\right) \cdot \left(g + \mathcal{P}^+_\gamma\right) := \left(fg + \mathcal{P}^+_{\beta+\gamma}\right).$$

Para $f \notin \mathrm{supp}(\mu_q)$, denotaremos por $\mathrm{in}_q(f)$ a imagem de f em $\mathcal{P}_{\mu_q(f)}/\mathcal{P}^+_{\mu_q(f)}$. Se $f \in \mathrm{supp}(\mu_q)$, então definimos $\mathrm{in}_q(f) = 0$.

Lema 3.47. *Sejam $f, g \in \mathbb{K}[x]$. As seguintes afirmações são verdadeiras.*

1. *$\mathcal{G}_q$ é um domínio de integridade.*
2. *$\mathrm{in}_q(f) \cdot \mathrm{in}_q(g) = \mathrm{in}_q(fg)$.*
3. *$\mathrm{in}_q(f) = \mathrm{in}_q(g)$ se, e somente se, $\mu_q(f) = \mu_q(g)$ e $\mu_q(f-g) > \mu_q(f)$.*

Demonstração:

1. É suficiente provar a propriedade de integridade para elementos homogêneos. Se $f+\mathcal{P}_\beta^+$ e $g+\mathcal{P}_\gamma^+$ são diferentes de zero, então $\mu_q(f)=\beta$ e $\mu_q(g)=\gamma$. Portanto, $\mu_q(fg)=\beta+\gamma\in\mathcal{G}_q$ e, assim, a classe $fg+\mathcal{P}_{\beta+\gamma}^+$ é diferente de zero.

2. Segue direto da definição do produto, pois

$$\mathrm{in}_q(fg)=\left(fg+\mathcal{P}^+_{\mu_q(f)+\mu_q(g)}\right)=\left(f+\mathcal{P}^+_{\mu_q(f)}\right)\cdot\left(g+\mathcal{P}^+_{\mu_q(g)}\right)=\mathrm{in}_q(f)\cdot\mathrm{in}_q(g).$$

3. ($\Rightarrow$) Observemos que $\mu_q(g)\neq\mu_q(g)$ implica $\mathrm{in}_q(f)\neq\mathrm{in}_q(g)$ pois esses elementos homogêneos estarão em componentes distintas. Logo, se supormos $\mathrm{in}_q(f)=\mathrm{in}_q(g)$, então $\mu_q(g)\neq\mu_q(g)$. Mais que isso, nesse caso $(f-g)\in\mathcal{P}^+_{\mu_q(f)}=\mathcal{P}^+_{\mu_q(g)}$, ou seja, $\mu_q(f-g)>\nu(f)$.

   ($\Leftarrow$) Se $\mu_q(f)=\mu_q(g)$, então as componentes $\mathcal{P}_{\mu_q(f)}/\mathcal{P}^+_{\mu_q(f)}$ e $\mathcal{P}_{\mu_q(g)}/\mathcal{P}^+_{\mu_q(g)}$ são iguais. Logo, se $\mu_q(f-g)>\mu_q(f)$, então $(f-g)\in\mathcal{P}^+_{\mu_q(f)}$ e por isso $\mathrm{in}_q(f)=\mathrm{in}_q(g)$.

■

Seja R_q o subgrupo aditivo de $\mathcal{G}_q$ gerado por

$$\{\mathrm{in}_q(f)\mid f\in\mathbb{K}[x]_d\},$$

em que $d=\deg(q)$ e $\mathbb{K}[x]_d=\{f\in\mathbb{K}[x]\mid\deg(f)<d\}$. Fixemos $y:=\mathrm{in}_q(q)$. O lema a seguir nos diz que y pode ser entendido como um elemento transcendente sobre R_q.

Lema 3.48. *Suponhamos $q\notin\mathrm{supp}(\nu)$. Se*

$$a_0+a_iy+\ldots+a_sy^s=0$$

para certos $a_0,\ldots,a_s\in R_q$, então $a_i=0$ para todo i, $0\leq i\leq s$.

Demonstração: Suponhamos que existem $a_0,\ldots,a_s\in R_q$ tais que

$$a_0+a_1y+\ldots+a_sy^s=0. \tag{3.1}$$

Queremos mostrar que $a_i=0$ para todo i, $0\leq i\leq s$. Observamos que todo elemento em R_q é da forma $\sum_{i=1}^{l}\mathrm{in}_Q(f_i)$ para certos $f_1,\ldots,f_l\in\mathbb{K}[x]_d$. Assim, a Equação (3.1) pode ser reescrita como

$$0=\sum_{j=1}^{m}F_j\text{ com }F_j=\sum_{i=0}^{s}\mathrm{in}_Q(f_{i,j})y^i\text{ para certos }f_{i,j}\in\mathbb{K}[x]_d$$

tais que cada F_j pertence a componentes homogêneas distintas de $\mathcal{G}_Q$. Como um elemento em $\mathcal{G}_Q$ é zero se, e somente se, cada uma de suas componentes homogêneas é zero, podemos assumir que $a_i = \text{in}_q(f_i)$ com $f_i \in \mathbb{K}[x]_d$ para todo i, $0 \leq i \leq s$.

Se $a_j \neq 0$ para algum j, $0 \leq j \leq s$, então $f_j \notin \text{supp}(\mu_q)$. Escrevemos a q-expansão de f como

$$f = \sum_{i=1}^{s} f_i q^i.$$

Seja $S_q(f) = \{i \mid \mu_q(f) = \mu(f_i q^i)\}$. Pela hipótese e pela definição de μ_q temos que

$$0 = \sum_{i \in S_q(f)} a_i y^i = \text{in}_q \left(\sum_{i \in S_q(f)} f_i q^i \right) = \text{in}_q(f).$$

Porém, isso contradiz $f \notin \text{supp}(\mu_q)$. Logo, segue o resultado.

■

Lema 3.49. *Temos*

$$\mathcal{G}_q = R_q[y].$$

Demonstração: Seja $f \in \mathbb{K}[x]$ qualquer. Escrevemos sua q-expansão $f = f_0 + f_1 q + \ldots + f_r q^s$, com $f_i \in \mathbb{K}[x]_d \cup \{0\}$ para todo i, $0 \leq i \leq s$. Então

$$\mu_q \left(f - \sum_{i \in S_q(f)} f_i q^i \right) = \mu_q \left(\sum_{i \notin S_q(f)} f_i q^i \right) = \min_{i \notin S_q(f)} \{\mu(f_i q^i)\} > \mu_q(f).$$

Dessa forma,

$$\text{in}_q(f) = \text{in}_q \left(\sum_{i \in S_q(f)} f_i q^i \right) = \sum_{i \in S_q(f)} \text{in}_q(f_i) y^i \in R_q[y].$$

Portanto, $\mathcal{G}_q = R_q[y]$. ■

Observação 3.50. *Se q é um polinômio de grau um, digamos $q = x - a$, então temos $R_{x-a} = \text{gr}_\mu(\mathbb{K})$. Assim, pelo Lema 3.49 temos $\mathcal{G}_{x-a} = \text{gr}_\mu(\mathbb{K})[z]$, em que $z = \text{in}_{x-a}(x-a)$.*

▼

Estabelecemos acima os conceitos de anel graduado que utilizaremos na prova alternativa do Teorema 3.45. A seguir demonstraremos outros dois lemas gerais que serão necessários.

Lema 3.51. *Seja $Q \in \mathbb{K}[x]$ um polinômio-chave. Temos, para todo $f \in \mathbb{K}[x]$,*

$$\overline{\mu}_{x-a}(f) \geq \mu_Q(f).$$

Demonstração: Dado $f \in \mathbb{K}[x]$, escrevemos sua Q-expansão. Seja $f = f_0 + f_1 Q + \ldots + f_r Q^s$, com $f_i \in \mathbb{K}[x]_d$ para todo i, $0 \leq i \leq s$. Logo, pelo Axioma $(V2)$ temos

$$\overline{\mu}_{x-a}(f) \geq \min_{0 \leq i \leq s} \{\overline{\mu}_{x-a}(f_i Q^i)\}.$$

Pelo Lema 3.28 e pela Observação 3.30, $\overline{\mu}_{x-a}(f_i) = \mu(f_i)$ e $\overline{\mu}_{x-a}(Q) = \mu(Q)$. Logo,

$$\overline{\mu}_{x-a}(f) \geq \min_{0 \leq i \leq s} \{\overline{\mu}_{x-a}(f_i Q^i)\} = \min_{0 \leq i \leq s} \{\mu(f_i Q^i)\} = \mu_Q(f).$$

■

Lema 3.52. *Seja $\phi : R \longrightarrow S$ um homomorfismo entre domínios e uma extensão $\tilde{\phi} : R[x] \longrightarrow S[y]$ tal que $\tilde{\phi}(x) = p(y) \in S[y] \setminus S$. Se ϕ é injetor, então $\tilde{\phi}$ é também injetor.*

Demonstração: Seja $f \in R[x]$ um polinômio não nulo. Se $f \in R$, então $\tilde{\phi}(f) = \phi(f) \neq 0$, pois ϕ é injetor. Se $\deg(f) \geq 1$, então $\deg(\tilde{\phi}(f)) = \deg(f)\deg(p) \geq 1$, pois R e S são domínios. Logo, $\tilde{\phi}(f) \neq 0$, mostrando que o núcleo de $\tilde{\phi}$ contém apenas o polinômio nulo. Portanto, $\tilde{\phi}$ é injetor.

■

Vejamos portanto uma prova alternativa para o Teorema 3.45.

Demonstração: [Segunda prova do Teorema 3.45] Sejam $\mathcal{G}_Q$ e $\mathcal{G}_{x-a}$ os anéis graduados associados às valorizações μ_Q e $\overline{\mu}_{x-a}$, respectivamente. Pelo Lema 3.51, temos as inclusões

$$\mathcal{P}_\gamma(\mathbb{K}[x], \mu_Q) \subseteq \mathcal{P}_\gamma(\overline{\mathbb{K}}[x], \overline{\mu}_{x-a})$$

e

$$\mathcal{P}^+_\gamma(\mathbb{K}[x], \mu_Q) \subseteq \mathcal{P}^+_\gamma(\overline{\mathbb{K}}[x], \overline{\mu}_{x-a})$$

para qualquer $\gamma \in \mu_Q \mathbb{K}[x] \subseteq \overline{\mu}_{x-a}\overline{\mathbb{K}}[x]$. Consideremos a seguinte aplicação bem definida:

$$\Phi : \mathcal{G}_Q \longrightarrow \mathcal{G}_{x-a}$$

dada por

$$\Phi(\mathrm{in}_Q(f)) = \begin{cases} \mathrm{in}_{x-a}(f) & \text{se } \mu_Q(f) = \mu_{x-a}(f) \\ 0 & \text{se } \mu_Q(f) < \mu_{x-a}(f) \end{cases}$$

e estendida naturalmente para um elemento qualquer. Tal aplicação é, por construção, um homomorfismo homogêneo de anéis graduados. Consideremos $\ker(\Phi)$. Vemos que $\ker(\Phi) = \langle I \rangle$ em que

$$I = \{\mathrm{in}_Q(f) \mid \overline{\mu}_{x-a}(f) > \mu_Q(f)\}.$$

Logo, mostrar que $\overline{\mu}_{x-a} = \mu_Q$ é equivalente a mostrar que $\ker(\Phi) = \{0\}$, isto é, o mesmo que mostrar que Φ é injetor.

Sabemos que $\mathcal{G}_Q = R_Q[y]$ e $\mathcal{G}_{x-a} = \mathrm{gr}_{\overline{\nu}}(\overline{\mathbb{K}})[z]$, em que $y = \mathrm{in}_Q(Q)$ e $z = \mathrm{in}_{x-a}(x-a)$. Consideremos a restrição de Φ ao conjunto $R_Q \subseteq \mathcal{G}_Q$. Afirmamos que $\Phi(R_Q) \subseteq \mathrm{gr}_{\overline{\nu}}(\overline{\mathbb{K}})$ e que a restrição $\Phi|_{R_Q}$ é injetora. De fato, basta olharmos que a imagem dos geradores de R_Q estão em $\mathrm{gr}_{\overline{\nu}}(\overline{\mathbb{K}})$. Dado $f \in \mathbb{K}[x]$ com $\deg(f) < \deg(Q)$, como $\mu_Q(f) = \overline{\mu}_{x-a}(f)$ (Observação 3.30), segue que $\Phi(\mathrm{in}_Q(f)) = \mathrm{in}_{x-a}(f)$. Mas, pela Observação 3.30,

$$\overline{\mu}_{x-a}(f) = \overline{\nu}(f(a)) \text{ e } \overline{\mu}_{x-a}(f - f(a)) > \overline{\mu}_{x-a}(f(a)).$$

Logo,

$$\Phi(\mathrm{in}_Q(f)) = \mathrm{in}_{x-a}(f) = \mathrm{in}_{x-a}(f(a)) \in \mathrm{gr}_{\overline{\nu}}(\overline{\mathbb{K}}).$$

Para vermos a injetividade, sejam $f, g \in \mathbb{K}[x]$ com $\deg(f), \deg(g) < \deg(Q)$ e suponhamos $\Phi(\mathrm{in}_Q(f)) = \Phi(\mathrm{in}_Q(g))$. Então,

$$\mathrm{in}_{x-a}(f) = \Phi(\mathrm{in}_Q(f)) = \Phi(\mathrm{in}_Q(g)) = \mathrm{in}_{x-a}(g).$$

Pelo Lema 3.47, isso implica que $\overline{\mu}_{x-a}(f) = \overline{\mu}_{x-a}(g)$ e $\overline{\mu}_{x-a}(f-g) > \overline{\mu}_{x-a}(f)$. Mas, $\overline{\mu}_{x-a}(f) = \mu_Q(f)$ e $\overline{\mu}_{x-a}(g) = \mu_Q(g)$. Logo, pelo Lema 3.47 temos $\mathrm{in}_Q(f) = \mathrm{in}_Q(g)$.

Por fim, como pelo Lema 3.28 temos $\overline{\mu}_{x-a}(Q) = \mu(Q)$, vemos que $\Phi(\mathrm{in}_Q(Q)) = \mathrm{in}_{x-a}(Q) \neq 0$. Como in_{x-a} é multiplicativo e $x-a$ divide Q em $\overline{\mathbb{K}}[x]$, segue que $z = \mathrm{in}_{x-a}(x-a)$ divide $\mathrm{in}_{x-a}(Q)$. Ou seja, $\Phi(y) = \Phi(\mathrm{in}_Q(Q)) \in \mathrm{gr}_{\overline{\nu}}(\overline{\mathbb{K}})[z] \setminus \mathrm{gr}_{\overline{\nu}}(\overline{\mathbb{K}})$. Portanto, como temos que $\Phi|_{R_Q}$ é injetor, o Lema 3.52 nos diz que $\Phi : R_Q[y] \longrightarrow \mathrm{gr}_{\overline{\nu}}(\overline{\mathbb{K}})[z]$ é também injetor, como queríamos.

■

Capítulo 4

Bolas e Discoides

Terminamos o capítulo anterior estabelecendo relações entre valorizações dadas por truncamentos em diferentes ambientes. Tomando ν uma valorização em $\mathbb{K}$, μ uma extensão de ν para $\mathbb{K}[x]$, $\overline{\nu}$ uma extensão de ν para $\overline{\mathbb{K}}$ e $\overline{\mu}$ uma extensão comum de $\overline{\nu}$ e μ para $\overline{\mathbb{K}}[x]$, obtemos que

$$\overline{\mu}_{a,\delta}|_{\mathbb{K}[x]} = \overline{\mu}_{x-a}|_{\mathbb{K}[x]} = \mu_Q,$$

sendo como Q um polinômio-chave para μ e (a,δ) um par minimal definido a partir de Q. Neste capítulo caracterizaremos essas valorizações monomiais e esses truncamentos em polinômios-chaves por meio de subconjuntos especiais de $\overline{\mathbb{K}}$. Buscaremos responder as seguintes questões. Seja μ uma valorização em $\mathbb{K}[x]$. Existe algum conjunto $D \subset \overline{\mathbb{K}}$ tal que

$$\mu(f) = \min_{d\in D}\{\mu(f(d))\}$$

para todo $f \in \mathbb{K}[x]$? Esse conjunto pode ser unicamente determinado, isto é, conjuntos distintos definem valorizações distintas? Veremos na primeira seção que as valorizações monomiais $\overline{\mu}_{a,\delta}$ em $\overline{\mathbb{K}}[x]$, com $\delta \in \overline{\nu}\overline{\mathbb{K}}$, podem ser descritas a partir das chamadas bolas, subconjuntos de $\overline{\mathbb{K}}$ que se comparam às bolas já conhecidas da teoria de Espaços Métricos. Mais especificamente, mostraremos que

$$\overline{\mu}_{a,\delta}(f) = \min_{d\in D}\{\overline{\nu}(f(d))\}$$

em que $D = D(a,\delta)$ será a bola definida por a e δ. Mostraremos que existe uma bijeção entre as bolas e as extensões resíduo-transcendentes de $\overline{\nu}$ para $\overline{\mathbb{K}}(x)$. Como consequência, bolas distintas descreverão valorizações monomiais distintas, que é o que entenderemos como unicidade. Em seguida, na segunda seção, buscaremos caracterizar μ_Q em $\mathbb{K}[x]$ por meio de um subconjunto de $\overline{\mathbb{K}}$, chamado discoide, de modo que μ_Q poderá também ser descrita como um mínimo sobre esse conjunto, quando Q satisfizer certas propriedades. Veremos que as bolas não serão suficientes para termos a unicidade nesse caso, uma vez que bolas distintas podem induzir o mesmo truncamento μ_Q em $\mathbb{K}[x]$. Descreveremos discoides utilizando bolas, conectando assim

os dois objetos. Com os discoides, conseguiremos vislumbrar, na terceira seção, uma relação entre esses e as extensões resíduo-transcendentes de ν para $\mathbb{K}(x)$. Tal relação será uma bijeção se assumirmos uma conjectura.

A principal referência para a composição deste capítulo foi o trabalho de Bengus-Lasnier (2021).

4.1 Bolas

Seja $(\mathbb{K}, \nu) \subseteq (\overline{\mathbb{K}}, \overline{\nu})$ uma extensão, em que $\overline{\mathbb{K}}$ é um fecho algébrico de $\mathbb{K}$ fixado.

Definição 4.1. *Fixemos $a \in \overline{\mathbb{K}}$ e $\delta \in \overline{\nu}\overline{\mathbb{K}}$. A **bola fechada** em torno de a e de raio δ é o subconjunto*

$$D(a, \delta) := \{d \in \overline{\mathbb{K}} \mid \overline{\nu}(d - a) \geq \delta\}.$$

■

Vejamos o porquê desse nome.

Observação 4.2. *Seja $\nu : \overline{\mathbb{K}} \longrightarrow \mathbb{R} \cup \{\infty\}$ uma valorização. Seja $|\cdot|$ a aplicação*

$$|\cdot| : \overline{\mathbb{K}} \longrightarrow \mathbb{R}$$

$$x \longmapsto \mathrm{e}^{-\nu(x)},$$

em que e *designa o número de Euler. Tal aplicação define um valor absoluto não arquimediano em $\overline{\mathbb{K}}$. Dessa forma, dados $a \in \overline{\mathbb{K}}$ e $\delta > 0$, temos que o conjunto $B(a, \delta) = \{d \in \overline{\mathbb{K}} \mid |d-a| \leq \delta\}$ é o que chamamos, no sentido usual dentro da teoria de espaços métricos, de bola fechada. Pela definição do valor absoluto,*

$$|d - a| \leq \delta \iff \mathrm{e}^{-\nu(d-a)} \leq \delta \iff \nu(d - a) \geq \ln(\delta)$$

isto é, $d \in D(a, \ln(\delta))$. Dessa forma, temos uma ligação direta entre as bolas fechadas dadas pelo valor absoluto derivado da valorização e os conjuntos que chamamos bolas na definição acima, justificando assim a escolha do nome.

▼

Devido ao Axioma $(V2)$, as bolas que definimos (e também as definidas através do valor absoluto, como no exemplo acima) possuem uma propriedade que as afastam da interpretação geométrica usual do conceito de bola na métrica euclidiana. Veremos no lema abaixo que todo ponto em $D(a, \delta)$ é centro para essa bola.

Lema 4.3. *Sejam $a \in \overline{\mathbb{K}}$ e $\delta \in \overline{\nu}\overline{\mathbb{K}}$. Tomemos $b \in D(a,\delta)$. Então $D(b,\delta) = D(a,\delta)$.*

Demonstração: Seja $d \in D(a,\delta)$. Temos

$$\overline{\nu}(d-b) = \overline{\nu}(d-a+a-b) \geq \min\{\overline{\nu}(d-a), \overline{\nu}(a-b)\} \geq \delta$$

pois $b \in D(a,\delta)$. Logo $d \in D(b,\delta)$ e portanto $D(a,\delta) \subseteq D(b,\delta)$. Pelo mesmo argumento mostra-se a outra inclusão.

■

Utilizaremos as bolas para apresentar uma segunda maneira de vermos as valorizações monomiais $\overline{\mu}_{a,\delta}$ em $\overline{\mathbb{K}}[x]$ com $\delta \in \overline{\nu}\overline{\mathbb{K}}$. No teorema abaixo, que é o terceiro dos resultados principais deste trabalho, veremos que $\overline{\mu}_{a,\delta}$ fica definida como o mínimo sobre uma bola.

Teorema 4.4. *Seja $D = D(a,\delta)$ uma bola fechada não vazia. Seja $f \in \overline{\mathbb{K}}[x]$ um polinômio qualquer. Então $\min\limits_{d\in D}\{\overline{\nu}(f(d))\}$ está bem definido e*

$$\min_{d\in D}\{\overline{\nu}(f(d))\} = \min_{i\in\mathbb{N}}\{\overline{\nu}(\partial_i f(a)) + i\delta\}.$$

Portanto, a aplicação

$$\begin{aligned} \overline{\mu}_D : \overline{\mathbb{K}}[x] &\longrightarrow \overline{\nu}\overline{\mathbb{K}} \\ f &\longmapsto \min_{d\in D}\{\overline{\nu}(f(d))\} \end{aligned}$$

é uma valorização e $\overline{\mu}_D = \overline{\mu}_{a,\delta}$. Ademais, $\overline{\mu}_D$ quando estendida da maneira usual para $\overline{\mathbb{K}}(x)$ é uma extensão resíduo-transcendente de $\overline{\nu}$.

Demonstração: Seja $f \in \overline{\mathbb{K}}[x]$. Escrevemos

$$f(x) = \sum_{i=0}^{n} a_i b^i \left(\frac{x-a}{b}\right)^i,$$

em que $a_i \in \overline{\mathbb{K}}$ e $b \in \overline{\mathbb{K}}$ é tal que $\overline{\nu}(b) = \delta$. Como $d \in D$ se, e somente se, $\overline{\nu}\left(\frac{d-a}{b}\right) \geq 0$, pelo Axioma $(V2)$ das valorizações

$$\overline{\nu}(f(d)) \geq \min_{0\leq i\leq n}\left\{\overline{\nu}(a_i b^i) + i\overline{\nu}\left(\frac{d-a}{b}\right)\right\} \geq \min_{0\leq i\leq n}\{\overline{\nu}(a_i b^i)\}.$$

Assim, $\{\overline{\nu}(f(d)) \mid d \in D\}$ possui uma cota inferior. Mostremos que vale a igualdade para algum $d \in D$. Seja $g = f/(a_j b^j)$, em que a_j é tal que $\overline{\nu}(a_j b^j) = \min\limits_{0\leq i\leq n}\{\overline{\nu}(a_i b^i)\}$. Escrevemos

$$g(x) = \sum_{i=0}^{n} a_i' b^i \left(\frac{x-a}{b}\right)^i,$$

em que $a_i^{'} = a_i/(a_j b^j)$, $0 \leq i \leq n$. Assim, temos $\min\limits_{0\leq i\leq n}\{\overline{\nu}(a_i^{'}b^i)\} = 0$ e $\overline{\nu}(a_i^{'}b^i) \geq 0$ para todo i, $0 \leq i \leq n$. Logo, $a_i^{'}b^i \in \mathcal{O}_{\overline{\nu}}$ para todo i, $0 \leq i \leq n$. Reduzindo os coeficientes $a_i^{'}b^i$ de g para $\overline{\mathbb{K}}\overline{\nu}$, obtemos um polinômio não nulo

$$\overline{g}(y) = \sum_{i=0}^{n}(a_i^{'}b^i)\overline{\nu}y^i \in \overline{\mathbb{K}}\overline{\nu}[y].$$

Como $\overline{\mathbb{K}}$ é algebricamente fechado, também $\overline{\mathbb{K}}\overline{\nu}$ é algebricamente fechado (Proposição D.12 do Apêndice D). Logo, $\overline{\mathbb{K}}\overline{\nu}$ é infinito e, portanto, deve haver algum elemento $d_0 \in \mathcal{O}_{\overline{\nu}}$ tal que seu resíduo em $\overline{\mathbb{K}}\overline{\nu}$ é diferente de zero e não é raiz de $\overline{g}(y)$, isto é, $\overline{g}(d_0\overline{\nu}) \neq 0$ e $\overline{\nu}(d_0) = 0$.

Escolhendo $d = d_0 b + a \in \overline{\mathbb{K}}$ para algum $d_0 \in \mathcal{O}_{\overline{\nu}}$ tal que $\overline{g}(d_0\overline{\nu}) \neq 0$, mostremos que

$$\left(\frac{d-a}{b}\right)\overline{\nu} = d_0\overline{\nu}$$

e $d \in D$. De fato, caso contrário, teríamos $\overline{\nu}\left(\frac{d-a}{b}\right) < 0$. Isso implica que

$$\overline{\nu}\left(d-a\right) = \overline{\nu}(d_0 b + a - a) < \overline{\nu}(b).$$

Porém, disso resulta que $\overline{\nu}(d_0) + \overline{\nu}(b) < \overline{\nu}(b)$, o que implica $\overline{\nu}(d_0) < 0$, contradizendo o fato de $d_0 \in \mathcal{O}_{\overline{\nu}}$. Logo, $d \in D$. Além disso, $\overline{\nu}(g(d)) = 0$. De fato,

$$\overline{\nu}(g(d)) \geq \min_{0\leq i\leq n}\left\{\overline{\nu}(a_i^{'}b^i) + i\overline{\nu}\left(\frac{d-a}{b}\right)\right\} \geq \min_{0\leq i\leq n}\{\overline{\nu}(a_i^{'}b^i)\} = 0.$$

Se valesse $\overline{\nu}(g(d)) > 0$, então teríamos

$$\sum_{i=0}^{n}(a_i^{'}b^i)\overline{\nu}\left(\frac{d_0 b + a - a}{b}\right)^i\overline{\nu} = 0.$$

Isso implica que

$$\overline{g}(d_0\overline{\nu}) = \sum_{i=0}^{n}(a_i^{'}b^i)\overline{\nu}(d_0\overline{\nu})^i = 0,$$

o que é uma contradição. Dessa forma,

$$\begin{aligned}\overline{\nu}(f(d)) &= \overline{\nu}(a_j b^j g(d)) \\ &= \overline{\nu}(a_j b^j) + \overline{\nu}(g(d)) \\ &= \overline{\nu}(a_j b^j) \\ &= \min_{0\leq i\leq n}\{\overline{\nu}(a_i b^i)\}.\end{aligned}$$

Portanto,

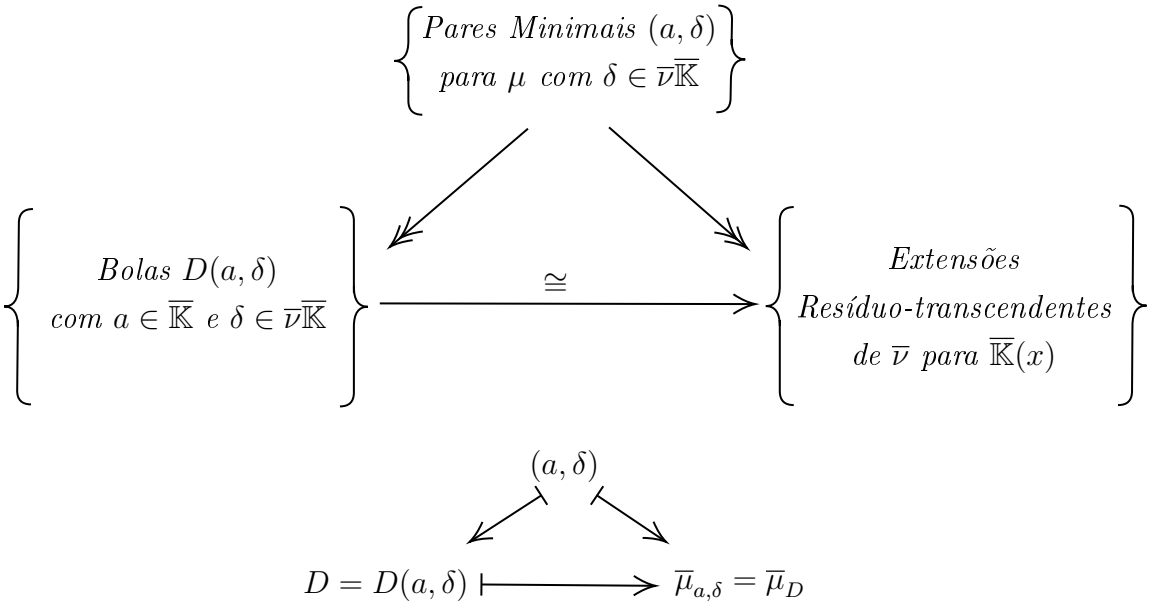
$$\begin{aligned}
\overline{\nu}(f(d)) &= \min_{0\leq i\leq n}\left\{\overline{\nu}(a_i b^i) + i\overline{\nu}\left(\frac{d-a}{b}\right)\right\} \\
&= \min_{0\leq i\leq n}\left\{\overline{\nu}\left(\partial_i f(a)\right) + \overline{\nu}(b^i) + i\overline{\nu}\left(d-a\right) - \overline{\nu}(b^i)\right\} \\
&= \min_{0\leq i\leq n}\left\{\overline{\nu}\left(\partial_i f(a)\right) + i\overline{\nu}\left(d_0 b + a - a\right)\right\} \\
&= \min_{0\leq i\leq n}\left\{\overline{\nu}\left(\partial_i f(a)\right) + i\overline{\nu}\left(d_0\right) + i\overline{\nu}\left(b\right)\right\} \\
&= \min_{0\leq i\leq n}\left\{\overline{\nu}\left(\partial_i f(a)\right) + i\delta\right\} \\
&= \overline{\mu}_{a,\delta}(f).
\end{aligned}$$

As últimas afirmações do teorema seguem da igualdade $\overline{\mu}_D = \overline{\mu}_{a,\delta}$ e do fato de $\delta \in \overline{\nu}\overline{\mathbb{K}}$ (Corolário 3.21).

■

Assim, vemos que as valorizações monomiais podem ser descritas em termos de bolas. Como as valorizações monomiais têm forte relação com as extensões resíduo-transcendentes, poderemos estabelecer também uma relação entre as bolas e esse tipo de extensão, apresentada no teorema abaixo. Essa relação nos dirá que, dadas duas bolas D e D', temos que $\overline{\mu}_D = \overline{\mu}_{D'}$ implica $D = D'$. Assim, teremos a unicidade sobre a qual nos questionamos na introdução do capítulo.

Teorema 4.5. *Sejam μ uma valorização em $\mathbb{K}[x]$, $\overline{\mu}$ uma valorização em $\overline{\mathbb{K}}[x]$ estendendo μ e consideremos as restrições $\nu = \mu|_{\mathbb{K}}$ e $\overline{\nu} = \overline{\mu}|_{\overline{\mathbb{K}}}$. Temos as seguintes relações entre os conjuntos abaixo:*



Demonstração: Olhemos inicialmente para a aplicação que toma um par minimal $(a,\delta) \in \overline{\mathbb{K}} \times \overline{\nu}\overline{\mathbb{K}}$ e o leva na valorização $\overline{\mu}_{a,\delta}$. Pelo Corolário 3.21 sabemos que $\overline{\mu}_{a,\delta} \mid \overline{\nu}$ é de fato resíduo-transcendente. Além disso, dada uma extensão resíduo-transcendente de $\overline{\nu}$ para $\overline{\mathbb{K}}(x)$ qualquer, o Teorema 3.20 garante a existência de $(a,\delta) \in \overline{\mathbb{K}} \times \overline{\nu}\overline{\mathbb{K}}$ tal que essa terá a forma $\overline{\mu}_{a,\delta}$. Tomando a com grau minimal dentre os elementos que definem a mesma valorização monomial que $\overline{\mu}_{a,\delta}$, temos que (a,δ) é par minimal para μ. De fato, para todo $b \in \overline{\mathbb{K}}$, se $\overline{\mu}(b-a) = \overline{\nu}(b-a) \geq \delta$, então $\overline{\mu}_{a,\delta} = \overline{\mu}_{b,\delta}$ (Lema 3.1) e, pela minimalidade de a, segue que $[\mathbb{K}(b) : \mathbb{K}] \geq [\mathbb{K}(a) : \mathbb{K}]$.

Vejamos agora que a aplicação que toma um par minimal $(a,\delta) \in \overline{\mathbb{K}} \times \overline{\nu}\overline{\mathbb{K}}$ e o leva na bola $D(a,\delta)$ é sobrejetora. Dada uma bola $D(a',\delta)$, sabemos que $D(a',\delta) = D(b,\delta)$ para todo $b \in D(a',\delta)$. Tomando $a \in D(a',\delta)$ com grau minimal, teremos que (a,δ) é um par minimal para μ. De fato, se $\overline{\mu}(b-a) = \overline{\nu}(b-a) \geq \delta$, então $b \in D(a,\delta)$. Portanto, $[\mathbb{K}(b) : \mathbb{K}] \geq [\mathbb{K}(a) : \mathbb{K}]$. Logo, a aplicação é sobrejetora.

Olhemos por fim a aplicação que toma a bola $D(a,\delta)$ e leva na extensão resíduo-transcendente de $\overline{\nu}$ dada por $\overline{\mu}_D = \overline{\mu}_{a,\delta}$. Tal aplicação é sobrejetora pois, dada $\overline{\mu}_{a,\delta}$, basta tomar no domínio $D(a,\delta)$. Vejamos que a aplicação é injetora. Sejam $D = D(a,\delta)$ e $D' = D(a',\delta')$ duas bolas e suponhamos $\overline{\mu}_D = \overline{\mu}_{D'}$. Então $\overline{\mu}_{a,\delta} = \overline{\mu}_{a',\delta'}$ e, pelo Lema 3.1, devemos ter $\delta = \delta'$ e $\overline{\nu}(a-a') \geq \delta$. Assim, $D = D'$, mostrando que a aplicação é injetora.

■

4.2 Discoides

Gostaríamos de obter teoremas semelhantes ao Teorema 4.4 e ao Teorema 4.5 para μ_Q, com Q polinômio-chave, e para as extensões resíduo-transcendentes de ν para $\mathbb{K}(x)$. Isto é, gostaríamos de encontrar uma coleção de conjuntos em $\overline{\mathbb{K}}$ tais que o truncamento μ_Q seja definido como um mínimo sobre um único conjunto dessa coleção. Uma ideia inicial é tentarmos utilizar as mesmas bolas da seção anterior. Como $\mu_Q = \overline{\mu}_{a,\delta}|_{\mathbb{K}[x]}$ (Seção 3.4), temos pelo Teorema 4.5 que μ_Q é definida como um mínimo sobre uma bola. Porém, veremos no Exemplo 4.7 que não é garantida uma bijeção entre truncamentos e bolas, pois bolas distintas podem induzir a mesma valorização μ_Q.

Lema 4.6. *Considere $a \in \overline{\mathbb{K}}$ e $\delta \in \overline{\nu}\overline{\mathbb{K}}$. Se $\sigma \in G^d(\overline{\nu}) := \{\sigma \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K}) \mid \overline{\nu} \circ \sigma = \overline{\nu}\}$, então*

$$\sigma(D(a,\delta)) = D(\sigma(a),\delta).$$

Demonstração: Como $\sigma \in G^d(\overline{\nu})$, temos, para qualquer $d \in \overline{\mathbb{K}}$,

$$\overline{\nu}(\sigma(d) - \sigma(a)) = \overline{\nu}(\sigma(d-a)) = \overline{\nu}(d-a).$$

Assim, sendo $d' \in \overline{\mathbb{K}}$ tal que $\sigma(d') = d$, temos

$$\begin{aligned} d \in D(\sigma(a), \delta) &\iff \overline{\nu}(d - \sigma(a)) \geq \delta \\ &\iff \overline{\nu}(\sigma(d') - \sigma(a)) \geq \delta \\ &\iff \overline{\nu}(\sigma(d' - a)) \geq \delta \\ &\iff \overline{\nu}(d' - a) \geq \delta \\ &\iff d' \in D(a, \delta). \end{aligned}$$

Portanto, $d \in D(\sigma(a), \delta)$ se, e somente se, $\sigma(d') = d$ para algum $d' \in D(a, \delta)$. Ou seja, $\sigma(D(a, \delta)) = D(\sigma(a), \delta)$.

■

Exemplo 4.7. *Suponhamos $\mu_Q = \overline{\mu}_{D(a,\delta)}|_{\mathbb{K}[x]}$. Tomemos $\sigma \in G^d(\overline{\nu})$ qualquer. Então, para todo $f \in \mathbb{K}[x]$ segue que*

$$\begin{aligned} \overline{\mu}_{D(\sigma(a),\delta)}(f) &= \min_{d \in D(\sigma(a),\delta)} \overline{\nu}(f(d)) \\ &= \min_{\sigma(d) \in \sigma(D(a,\delta))} \overline{\nu}(f(\sigma(d))) \\ &= \min_{d \in D(a,\delta)} \overline{\nu}(\sigma(f(d))) \\ &= \min_{d \in D(a,\delta)} \overline{\nu}(f(d)) \\ &= \overline{\mu}_{D(a,\delta)}(f) = \mu_Q(f). \end{aligned}$$

Portanto, vemos que bolas distintas podem definir o mesmo truncamento em $\mathbb{K}[x]$.

▼

Apresentaremos um subconjunto que promete ultrapassar tal problema que encontramos com as bolas. Esses serão os chamados discoides, que como veremos se relacionarão bem com as já conhecidas bolas. Antes de Bengus-Lasnier (2021), esses conjuntos foram estudados por Rüth (2014) em sua tese de doutorado.

Definição 4.8. *Fixemos $f \in \overline{\mathbb{K}}[x]$ e $\rho \in \overline{\nu}\overline{\mathbb{K}}$. O **discoide** centrado f e de raio ρ é o subconjunto*

$$\overline{D}(f, \rho) := \{d \in \overline{\mathbb{K}} \mid \overline{\nu}(f(d)) \geq \rho\}.$$

■

Vamos iniciar investigando a estrutura dos discoides a fim de conseguirmos um resultado semelhante ao Teorema 4.4.

Lema 4.9. *Fixemos $f \in \overline{\mathbb{K}}[x]$, $a \in \overline{\mathbb{K}}$ uma raiz de f e $\rho \in \overline{\nu}\overline{\mathbb{K}}$. Está bem-definido o elemento*

$$\epsilon(a; f, \rho) := \min\{\lambda \in \overline{\nu}\overline{\mathbb{K}} \mid D(a, \lambda) \subseteq \overline{D}(f, \rho)\},$$

que pode ser descrito como

$$\epsilon(a; f, \rho) = \max_{1 \leq i \leq \deg(f)} \left\{ \frac{\rho - \overline{\nu}(\partial_i f(a))}{i} \right\} \in \overline{\nu}\overline{\mathbb{K}} \otimes \mathbb{Q}.$$

Demonstração: Escrevemos

$$f(x) = \sum_{i=0}^{r} a_i (x-a)^i,$$

em que $a_i = \partial_i f(a)$. Então,

$$\begin{aligned} D(a,\lambda) \subseteq \overline{D}(f,\rho) &\iff \text{para todo } d \in D(a,\lambda) \text{ vale } \overline{\nu}(f(d)) \geq \rho \\ &\iff \min_{d \in D(a,\lambda)} \{\overline{\nu}(f(d))\} \geq \rho \\ &\iff \min_{1 \leq i \leq r} \{\overline{\nu}(a_i) + i\lambda\} \geq \rho \\ &\iff \lambda \geq \max_{1 \leq i \leq r} \left\{ \frac{\rho - \overline{\nu}(\partial_i f(a))}{i} \right\} =: \lambda_m \end{aligned}$$

A existência e a equivalência entre os mínimos acima são garantidas pelo Teorema 4.4. Assim, tomando λ_m como o máximo indicado na última equivalência, obtemos que $D(a, \lambda_m)$ é a menor bola contida em $\overline{D}(f, \rho)$. De fato, se λ satisfaz $D(a, \lambda) \subseteq \overline{D}(f, \rho)$, então vimos pelas equivalências que $\lambda \geq \lambda_m$. Logo, $\lambda_m = \epsilon(a; f, \rho)$.

■

Quando Q é um polinômio-chave com $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$, se tomarmos a uma raiz otimizadora de Q, então $\epsilon(a; Q, \mu(Q))$ coincide com a quantidade $\epsilon(Q) = \delta(Q)$ já por nós conhecida. O lema a seguir demonstra tal fato.

Lema 4.10. *Seja Q um polinômio-chave em $\mathbb{K}[x]$ com relação a μ. Seja $(a, \delta(Q))$ um par tal que $a \in \overline{\mathbb{K}}$ é uma raiz de Q e $\delta(Q) = \overline{\mu}(x-a)$. Suponhamos $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$. Então*

$$\epsilon(a; Q, \mu(Q)) = \epsilon(Q) = \delta(Q).$$

Demonstração: Por definição,

$$\epsilon(a; Q, \mu(Q)) := \max_{1 \leq i \leq \deg(Q)} \left\{ \frac{\mu(Q) - \overline{\nu}(\partial_i Q(a))}{i} \right\} \in \overline{\nu}\overline{\mathbb{K}} \otimes \mathbb{Q}$$

e

$$\epsilon(Q) := \max_{1 \leq i \leq \deg(Q)} \left\{ \frac{\mu(Q) - \mu(\partial_i Q)}{i} \right\} \in \mu(\mathbb{K}[x]) \otimes \mathbb{Q}.$$

Como $\deg(\partial_i Q) < \deg(Q)$ para cada i, $1 \leq i \leq \deg(Q)$, segue da Observação 3.30 que

$$\mu(\partial_i Q) = \overline{\mu}(\partial_i Q) = \overline{\nu}(\partial_i Q(a)).$$

Portanto,

$$\epsilon(a; Q, \mu(Q)) = \epsilon(Q) = \delta(Q).$$

Em particular, $\delta(Q) \in \overline{\nu}\overline{\mathbb{K}}$.

■

Os discoides podem ser descritos em termos de bolas. Essa forma de ver um discoide permitirá que definamos uma aplicação semelhante à valorização dada pelo mínimo sobre uma bola. Essa será a aplicação que associa um polinômio g ao mínimo de $\overline{\nu}(g(d))$ quando d varia no discoide.

Lema 4.11. *Para cada $f \in \overline{\mathbb{K}}[x]$ e $\rho \in \overline{\nu}\overline{\mathbb{K}}$, temos que $\overline{D}(f, \rho)$ é uma união finita de bolas centradas em torno das raízes de f, isto é,*

$$\overline{D}(f, \rho) = \bigcup_{\substack{a \in \overline{\mathbb{K}} \\ f(a)=0}} D(a, \epsilon(a; f, \rho)).$$

Demonstração: Sejam $a_1, \ldots, a_n$ as raízes distintas de f em $\overline{\mathbb{K}}$ com multiplicidades $c_1, \ldots, c_n$, respectivamente. Para cada a_i, temos definido $\epsilon_i = \epsilon(a_i; f, \rho)$ tal que $D(a_i, \epsilon_i) \subseteq \overline{D}(f, \rho)$ e este é a bola centrada em a_i com menor raio. É imediato que

$$\overline{D}(f, \rho) \supseteq \bigcup_{\substack{a \in \overline{\mathbb{K}} \\ f(a)=0}} D(a, \epsilon(a; f, \rho)).$$

Mostremos a outra inclusão. Seja $d \in \overline{D}(f, \rho)$, ou seja, $d \in \overline{\mathbb{K}}$ satisfazendo

$$\rho \leq \overline{\nu}(f(d)) = \sum_{i=1}^{n} c_i \overline{\nu}(d - a_i)$$

Seja $i_d \in \{1, \ldots, n\}$ tal que

$$\overline{\nu}(d - a_{i_d}) \geq \overline{\nu}(d - a_i)$$

para todo i, $1 \leq i \leq n$. Vejamos que $D(a_{i_d}, \overline{\nu}(d - a_{i_d})) \subseteq \overline{D}(f, \rho)$. Seja $p \in D(a_{i_d}, \overline{\nu}(d - a_{i_d}))$. Temos

$$\overline{\nu}(f(p)) = \sum_{i=1}^{n} c_i \overline{\nu}(p - a_i) = \overline{\nu}(p - a_{i_d}) + \sum_{\substack{i=1 \\ i \neq i_d}}^{n} c_i \overline{\nu}(p - a_i)$$

Reescrevemos $\overline{\nu}(p - a_i) = \overline{\nu}(p - a_{i_d} + a_{i_d} - d + d - a_i)$. Como $\overline{\nu}(d - a_{i_d}) \geq \overline{\nu}(d - a_i)$ e

$\overline{\nu}(p-a_{i_d}) \geq \overline{\nu}(d-a_{i_d})$, temos

$$\overline{\nu}(p-a_{i_d}+a_{i_d}-d+d-a_i) \geq \max\{\overline{\nu}(p-a_{i_d}),\overline{\nu}(a_{i_d}-d),\overline{\nu}(d-a_i)\} = \overline{\nu}(d-a_i).$$

Dessa forma,

$$\begin{aligned}\overline{\nu}(f(p)) &= \overline{\nu}(p-a_{i_d}) + \sum_{\substack{i=1\\ i\neq i_d}}^{n} c_i\overline{\nu}(p-a_i)\\ &\geq \overline{\nu}(d-a_{i_d}) + \sum_{\substack{i=1\\ i\neq i_d}}^{n} c_i\overline{\nu}(d-a_i)\\ &\geq \rho\end{aligned}$$

Logo, $p \in \overline{D}(f,\rho)$. Assim, $D(a_{i_d},\overline{\nu}(d-a_{i_d})) \subseteq \overline{D}(f,\rho)$. Como, $D(a_{i_d},\epsilon_{i_d})$ é a bola centrada em a_{i_d} contido em $\overline{D}(f,\rho)$ com menor raio, segue que $\epsilon_{i_d} \leq \overline{\nu}(d-a_{i_d})$. Portanto $d \in D(a_{i_d},\epsilon_{i_d})$, provando a outra inclusão procurada. Dessa forma,

$$\overline{D}(f,\rho) = \bigcup_{\substack{a\in\overline{\mathbb{K}}\\ f(a)=0}} D(a,\epsilon(a;f,\rho)).$$

■

Proposição 4.12. *Seja $f \in \overline{\mathbb{K}}[x]$ e $\rho \in \overline{\nu}\overline{\mathbb{K}}$. Consideremos o discoide $\overline{D}(f,\rho)$. Seja $g \in \overline{\mathbb{K}}[x]$ um polinômio qualquer. Está bem definido*

$$\min_{d\in\overline{D}(f,\rho)}\{\overline{\nu}(g(d))\}.$$

Demonstração: Segundo o Lema 4.11, o discoide $\overline{D}(f,\rho)$ pode ser escrito como a união das bolas $D(a_i,\epsilon(a_i;f,\rho))$, $1 \leq i \leq n$, em que $a_1,\ldots,a_n$ são as raízes distintas de f em $\overline{\mathbb{K}}$. Portanto, para cada i, está bem definido

$$m_i = \min_{d\in D(a_i,\epsilon(a_i;f,\rho))}\{\overline{\nu}(g(d))\} = \overline{\mu}_{D(a_i,\epsilon(a_i;f,\rho))}(g).$$

Assim, dado um d qualquer em $\overline{D}(f,\rho)$, este deve pertencer a $D(a_i,\epsilon(a_i;f,\rho))$ para algum i. Com isso, $m_i \leq \overline{\nu}(g(d))$. Logo, tomando $m = \min\{m_1,\ldots,m_n\}$, temos que $m \leq \overline{\nu}(g(d))$ para todo $d \in \overline{D}(f,\rho)$, isto é,

$$m = \min_{d\in\overline{D}(f,\rho)}\{\overline{\nu}(g(d))\}.$$

■

Com a proposição acima, fica bem definida a aplicação

$$\begin{aligned}\overline{\mu}_{\overline{D}(f,\rho)} : \overline{\mathbb{K}}[x] &\longrightarrow \overline{\nu}\overline{\mathbb{K}} \cup \{\infty\} \\ g &\longmapsto \min_{d\in\overline{D}(f,\rho)} \{\overline{\nu}(g(d))\} \text{ se } g \neq 0, \\ 0 &\longmapsto \infty.\end{aligned}$$

Vejamos que $\overline{\mu}_{\overline{D}(f,\rho)}$ satisfaz o Axioma $(V2)$. Sejam $g, h \in \overline{\mathbb{K}}[x]$ e consideremos $\overline{\mu}_{\overline{D}(f,\rho)}(g+h)$. Seja $x \in \overline{D}(f,\rho)$ tal que $\overline{\mu}_{\overline{D}(f,\rho)}(g+h) = \overline{\mu}(g(x)+h(x))$. Temos

$$\begin{aligned}\overline{\mu}_{\overline{D}(f,\rho)}(g+h) &= \overline{\mu}(g(x)+h(x)) \\ &\geq \min\{\overline{\mu}(g(x)), \overline{\mu}(h(x))\} \\ &\geq \min\{\overline{\mu}_{\overline{D}(f,\rho)}(g), \overline{\mu}_{\overline{D}(f,\rho)}(h)\},\end{aligned}$$

como queríamos. Pelo mesmo argumento,

$$\overline{\mu}_{\overline{D}(f,\rho)}(gh) \geq \overline{\mu}_{\overline{D}(f,\rho)}(g) + \overline{\mu}_{\overline{D}(f,\rho)}(h).$$

Porém, $\overline{\mu}_{\overline{D}(f,\rho)}$ pode não ser uma valorização, uma vez que não é sempre que o Axioma $(V1)$ é satisfeito. O exemplo a seguir ilustra isso.

Exemplo 4.13. *Seja $a \in \mathbb{K}$ tal que $\nu(a) < 0$. Consideremos as bolas $D_a = D(a,0)$, $D_0 = D(0,0)$ e a união $D = D_a \cup D_0$. Tomando $f(x) = x(x-a)$, como $\partial_1(x(x-a)) = 2x - a$ e $\partial_2(x(x-a)) = 1$, segue que*

$$\begin{aligned}\epsilon(0; f, \nu(a)) &= \epsilon(a; f, \nu(a)) \\ &= \max\left\{\frac{\nu(a) - \overline{\nu}(\partial_1 f(a))}{1}, \frac{\nu(a) - \overline{\nu}(\partial_2 f(a))}{2}\right\} \\ &= \max\left\{\nu(a) - \nu(a), \frac{\nu(a)}{2}\right\} = 0.\end{aligned}$$

Logo,

$$\overline{D}(f, \nu(a)) = D(a,0) \cup D(0,0) = D.$$

Também temos que

$$\overline{\mu}_{D_0}(x) = 0,\ \overline{\mu}_{D_a}(x-a) = 0,\ \overline{\mu}_{D_a}(x) = \nu(a) \text{ e } \overline{\mu}_{D_0}(x-a) = \nu(a).$$

Então,

$$\overline{\mu}_{\overline{D}(f,\overline{\nu}(a))}(x) = \overline{\mu}_{\overline{D}(f,\overline{\nu}(a))}(x-a) = \nu(a).$$

Por outro lado, $\overline{\mu}_{\overline{D}(f,\overline{\nu}(a))}(x(x-a)) = \nu(a)$. *No entanto,*

$$\overline{\mu}_{\overline{D}(f,\overline{\nu}(a))}(x) + \overline{\mu}_{\overline{D}(f,\overline{\nu}(a))}(x-a) = 2\nu(a) < \nu(a) = \overline{\mu}_{\overline{D}(f,\overline{\nu}(a))}(x(x-a)).$$

Ou seja, $\overline{\mu}_{\overline{D}(f,\overline{\nu}(a))}$ *não satisfaz* $(V1)$.

▼

Na próxima seção, veremos que $\mu_{\overline{D}(f,\rho)} := \overline{\mu}_{\overline{D}(f,\rho)}|_{\mathbb{K}[x]}$ será uma valorização se as raízes do polinômio f se relacionarem com o grupo de decomposição de $\overline{\nu}$ por meio de uma ação de grupo transitiva.

4.3 Bolas, discoides e o grupo de decomposição

Sejam $(\mathbb{K},\nu)$, $(\overline{\mathbb{K}},\overline{\nu})$, $(\mathbb{K}(x),\mu)$ e $(\overline{\mathbb{K}}(x),\overline{\mu})$ de modo que temos o diagrama de extensões abaixo.

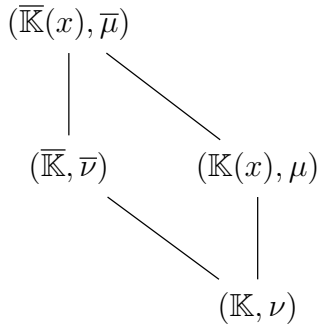


Figura 4.1: Diagrama das extensões

Iniciaremos esta seção vendo como $G^d(\overline{\nu}) := \{\sigma \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K}) \mid \overline{\nu}\circ\sigma = \overline{\nu}\}$, o grupo de decomposição (estudado no Apêndice E, Seção E.2), se relaciona com as valorizações monomiais e com as bolas. Em seguida, uma ação do grupo de decomposição no conjunto de raízes de um dado polinômio f permitirá concluir, sob certas hipóteses, que a aplicação $\mu_{\overline{D}(f,\overline{\mu}(f))}$ é uma valorização em $\mathbb{K}[x]$. Se o polinômio em questão for um polinômio-chave $Q \in \mathbb{K}[x]$ irredutível sobre a henselização $\mathbb{K}^d(\overline{\nu})$ (ver Seção E.2), então teremos μ_Q definida como um mínimo sobre um discoide, junto com a unicidade deste. Estabeleceremos então um diagrama, análogo ao do Teorema 4.5, relacionando as valorizações resíduo-transcendentes de $\mathbb{K}[x]$, os polinômios-chaves e os discoides.

Vejamos antes alguns lemas técnicos.

Lema 4.14. *Seja $\overline{\mu}_{a,\delta}$ a valorização monomial definida por um dado $a \in \overline{\mathbb{K}}$ e um dado $\delta \in \overline{\mu}\overline{\mathbb{K}}(x)$. Se $\sigma \in \mathrm{Aut}(\overline{\mathbb{K}}(x) \mid \mathbb{K}(x))$ é tal que $\sigma|_{\overline{\mathbb{K}}} \in G^d(\overline{\nu})$, então*

$$\overline{\mu}_{a,\delta} \circ \sigma^{-1} = \overline{\mu}_{\sigma(a),\delta}.$$

Demonstração: Temos um isomorfismo $\mathrm{Aut}(\overline{\mathbb{K}}(x) \mid \mathbb{K}(x)) \cong \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K})$ dado através da restrição, isto é, $\sigma|_{\overline{\mathbb{K}}} \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K})$. Assim, $a \in \overline{\mathbb{K}}$ implica $\sigma(a) \in \overline{\mathbb{K}}$. Seja $f \in \overline{\mathbb{K}}[x]$ qualquer. Podemos escrever f como

$$f(x) = \sum_{i=1}^{r} a_i (x - \sigma(a))^i,$$

para certos $a_i \in \overline{\mathbb{K}}$. Temos que $\sigma|_{\overline{\mathbb{K}}} \in G^d(\overline{\nu})$ implica $\sigma^{-1}|_{\overline{\mathbb{K}}} \in G^d(\overline{\nu})$. Logo, segue que

$$\begin{aligned}
(\overline{\mu}_{a,\delta} \circ \sigma^{-1})(f) &= \overline{\mu}_{a,\delta}\left(\sum_{i=1}^{r} \sigma^{-1}(a_i)(x-a)^i\right) \\
&= \min_{0\le i\le r}\{\overline{\nu}(\sigma^{-1}(a_i)) + i\delta\} \\
&= \min_{0\le i\le r}\{\overline{\nu}(a_i) + i\delta\} \\
&= \overline{\mu}_{\sigma(a),\delta}\left(\sum_{i=1}^{r} a_i (x-\sigma(a))^i\right) \\
&= \overline{\mu}_{\sigma(a),\delta}(f).
\end{aligned}$$

■

No capítulo anterior, vimos que dado um polinômio-chave Q para μ, se considerarmos um par minimal (a, δ) que é definido por Q (isto é, com a raiz otimizadora de Q e $\delta = \overline{\mu}(x-a)$), então a valorização $\overline{\mu}_{a,\delta}$ é tal que

$$\overline{\mu}_{a,\delta}|_{\mathbb{K}[x]} = \mu_Q \text{ e } \overline{\mu}_{a,\delta}|_{\overline{\mathbb{K}}} = \overline{\nu}.$$

Sejam $\mathcal{E}(\overline{\nu}, \overline{\mathbb{K}}, \overline{\mathbb{K}}[x])$ o conjunto das extensões de $\overline{\nu}$ de $\overline{\mathbb{K}}$ para $\overline{\mathbb{K}}[x]$ e $\mathcal{E}(\mu_Q, \mathbb{K}[x], \overline{\mathbb{K}}[x])$ o conjunto das extensões de μ_Q de $\mathbb{K}[x]$ para $\overline{\mathbb{K}}[x]$. Podemos descrever, usando os elementos de $G^d(\overline{\nu})$, quem são as valorizações em $\overline{\mathbb{K}}[x]$ que estendem simultaneamente $\overline{\nu}$ e μ_Q.

Corolário 4.15. *Nas condições do parágrafo acima, temos*

$$\mathcal{E}(\overline{\nu}, \overline{\mathbb{K}}, \overline{\mathbb{K}}[x]) \cap \mathcal{E}(\mu_Q, \mathbb{K}[x], \overline{\mathbb{K}}[x]) = \{\overline{\mu}_{\sigma(a),\delta} \mid \sigma \in G^d(\overline{\nu})\}.$$

Demonstração: Basta juntarmos o lema anterior com a Proposição E.12 da Seção E.3.

■

Seja $\mathbb{K}^d(\overline{\nu}) = \mathrm{Fix}(G^d(\overline{\nu}))$ a henselização de $\mathbb{K}$ com relação a valorização ν (Apêndice E, Seção E.2).

Lema 4.16. *Seja $f \in \mathbb{K}^d(\overline{\nu})[x]$ um polinômio. Suponhamos $\overline{\mu}(f) \in \overline{\nu}\overline{\mathbb{K}}$ e seja $a \in \overline{\mathbb{K}}$. Para cada $\sigma \in G^d(\overline{\nu})$ temos*

$$\epsilon(\sigma(a); f, \overline{\mu}(f)) = \epsilon(a; f, \overline{\mu}(f)).$$

Demonstração: Temos $\overline{\nu}(\sigma(g(a)) = \overline{\nu}(g(a))$ e $h(\sigma(a)) = \sigma(h(a))$ para todo $g, h \in \mathbb{K}^d(\overline{\nu})[x]$, pois $\sigma \in G^d(\overline{\nu})$. Logo,

$$\begin{aligned}
\epsilon(\sigma(a); f, \overline{\mu}(f)) &:= \max_{1 \le i \le \deg(f)} \left\{ \frac{\overline{\mu}(f) - \overline{\nu}(\partial_i f(\sigma(a)))}{i} \right\} \\
&= \max_{1 \le i \le \deg(f)} \left\{ \frac{\overline{\mu}(f) - \overline{\nu}(\sigma(\partial_i f(a)))}{i} \right\} \\
&= \max_{1 \le i \le \deg(f)} \left\{ \frac{\overline{\mu}(f) - \overline{\nu}(\partial_i f(a))}{i} \right\} \\
&= \epsilon(a; f, \overline{\mu}(f)).
\end{aligned}$$

■

Dado um $f \in \mathbb{K}^d(\overline{\nu})[x]$, se $a \in \overline{\mathbb{K}}$ é uma raiz de f, então $\sigma(a)$ também é uma raiz de f para qualquer $\sigma \in G^d(\overline{\nu})$. Diremos que $G^d(\overline{\nu})$ **age transitivamente nas raízes** de f se, dadas raízes $a_i, a_j \in \overline{\mathbb{K}}$ de $f(x)$, existe $\sigma \in G^d(\overline{\nu})$ tal que $\sigma(a_i) = a_j$. Isto é, se a ação do grupo $G^d(\overline{\nu})$ no conjunto das raízes de f, dada por $(\sigma, a_i) \mapsto \sigma(a_i)$, for uma ação transitiva. Nessa situação, fixada uma raiz a de f, podemos descrever o conjunto das raízes de f como $\{\sigma(a) \mid \sigma \in G^d(\overline{\nu})\}$.

No teorema a seguir, veremos que $\mu_{\overline{D}(f,\overline{\mu}(f))}$ é uma valorização em $\mathbb{K}[x]$ (mais ainda, em $\mathbb{K}^d(\overline{\nu})[x]$) quando $f \in \mathbb{K}^d(\overline{\nu})[x]$ é um polinômio com $\overline{\mu}(f) \in \overline{\nu}\overline{\mathbb{K}}$ e tal que $G^d(\overline{\nu})$ age transitivamente em suas raízes.

Teorema 4.17. *Seja $f \in \mathbb{K}^d(\overline{\nu})[x]$ tal que $G^d(\overline{\nu})$ age transitivamente em suas raízes. Suponhamos que $\overline{\mu}(f) \in \overline{\nu}\overline{\mathbb{K}}$ e que $(a, \delta(f)) \in \overline{\mathbb{K}} \times \overline{\nu}\overline{\mathbb{K}}$ seja tal que a é raiz de f e $\overline{\mu}(x - a) = \delta(f)$. Para simplificar a notação, vamos escrever $\epsilon(b; f, \overline{\mu}(f)) =: \epsilon(b, f)$. Então,*

$$\overline{D}(f, \overline{\mu}(f)) = \bigcup_{\substack{a_i \in \overline{\mathbb{K}} \\ f(a_i)=0}} D(a_i, \epsilon(a_i, \overline{\mu}(f))) = \bigcup_{\sigma \in G^d(\overline{\nu})} D(\sigma(a), \epsilon(a, f)).$$

Também, $\mu_{\overline{D}(f,\overline{\mu}(f))}$ é uma valorização em $\mathbb{K}[x]$ (mais ainda, $\overline{\mu}_{\overline{D}(f,\overline{\mu}(f))}$ é uma valorização em $\mathbb{K}^d(\overline{\nu})[x]$) e as valorizações da forma $\overline{\mu}_{D(\sigma(a),\epsilon(a,f))}$, com $\sigma \in G^d(\overline{\nu})$, estendem $\mu_{\overline{D}(f,\overline{\mu}(f))}$ para $\overline{\mathbb{K}}[x]$.

Demonstração: Como vimos acima, o conjunto das raízes de f pode ser descrito como $\{\sigma(a) \mid \sigma \in G^d(\overline{\nu})\}$. Assim, o Lema 4.11 nos diz que a união no enunciado acima está bem indexada. Pelo Lema 4.16, $\epsilon(\sigma(a), \overline{\mu}(f)) = \epsilon(a, \overline{\mu}(f))$. Já vimos que cada $\overline{\mu}_{D(\sigma(a),\epsilon(a,f))}$ é uma valorização bem definida e que coincide com $\overline{\mu}_{\sigma(a),\epsilon(a,f)} = \overline{\mu}_{a,\epsilon(a,f)} \circ \sigma^{-1}$.

Seja $g \in \mathbb{K}^d(\overline{\nu})[x]$ qualquer. Mostremos que $\overline{\mu}_{D(\sigma(a),\epsilon(a,f))}(g) = \overline{\mu}_{D(a,\epsilon(a,f))}(g)$ para todo $\sigma \in G^d(\overline{\nu})$. De fato, como σ fixa os coeficientes de g e é a restrição de um automorfismo em $\mathrm{Aut}(\overline{\mathbb{K}}(x) \mid \mathbb{K}(x))$, vemos que $\sigma(g) = g$ (e o mesmo vale para σ^{-1}). Logo,

$$\begin{aligned}\overline{\mu}_{D(\sigma(a),\epsilon(a,f))}(g) &= \overline{\mu}_{\sigma(a),\epsilon(a,f)}(g) \\ &= (\overline{\mu}_{a,\epsilon(a,f)} \circ \sigma^{-1})(g) \\ &= \overline{\mu}_{a,\epsilon(a,f)}(g) \\ &= \overline{\mu}_{D(a,\epsilon(a,f))}(g).\end{aligned}$$

Assim, como temos pela Proposição 4.12

$$\overline{\mu}_{\overline{D}(f,\overline{\mu}(f))}(g) = \min_{d \in \overline{D}(f,\overline{\mu}(f))} \{\overline{\nu}(g(d))\} = \min_{\sigma \in G^d(\overline{\nu})} \{\overline{\mu}_{D(\sigma(a),\epsilon(a,f))}(g)\}$$

e $\overline{\mu}_{D(\sigma(a),\epsilon(a,f))}(g) = \overline{\mu}_{D(a,\epsilon(a,f))}(g)$, concluímos que $\overline{\mu}_{\overline{D}(f,\overline{\mu}(f))} = \overline{\mu}_{D(a,\epsilon(a,f))}$ em $\mathbb{K}^d(\overline{\nu})[x]$, ou seja, $\overline{\mu}_{\overline{D}(f,\overline{\mu}(f))}$ é uma valorização em $\mathbb{K}^d(\overline{\nu})[x]$. Em particular, $\mu_{\overline{D}(f,\overline{\mu}(f))}$ é uma valorização em $\mathbb{K}[x]$.

Como $\overline{\mu}_{D(a,\epsilon(a,f))}$ é uma valorização em $\overline{\mathbb{K}}[x]$ que estende simultaneamente $\mu_{\overline{D}(f,\overline{\mu}(f))}$ e $\overline{\nu}$, temos pela Proposição E.12 que as valorizações da forma

$$\overline{\mu}_{D(a,\epsilon(a,f))} \circ \sigma^{-1} = \overline{\mu}_{D(\sigma(a),\epsilon(a,f))},$$

com $\sigma \in G^d(\overline{\nu})$, são todas as extensões simultâneas de $\mu_{\overline{D}(f,\overline{\mu}(f))}$ e $\overline{\nu}$ para $\overline{\mathbb{K}}[x]$.

■

Uma classe de polinômios que verifica a transitividade da ação do grupo de decomposição sobre suas as raízes são os polinômios irredutíveis em $\mathbb{K}^d(\overline{\nu})[x]$. De fato, se $f \in \mathbb{K}^d(\overline{\nu})[x]$ é irredutível, então dadas duas raízes a_i e a_j de f, existe um isomorfismo $\sigma_0 : \mathbb{K}^d(\overline{\nu})(a_i) \to \mathbb{K}^d(\overline{\nu})(a_j)$ com $\sigma_0(a_i) = a_j$ e $\sigma_0|_{\mathbb{K}^d(\overline{\nu})} = \mathrm{id}$ (Apêndice B, Lema A.43). Tal σ_0 se estende para um isomorfismo $\sigma : \overline{\mathbb{K}} \to \overline{\mathbb{K}}$ (Apêndice B, Lema A.44). Logo, como $\sigma \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K}^d(\overline{\nu})) = G^d(\overline{\nu})$, segue que $G^d(\overline{\nu})$ age transitivamente nas raízes de um polinômio irredutível $f \in \mathbb{K}^d(\overline{\nu})[x]$.

Juntando o teorema acima, o Lema 4.10 e os resultados da Seção 3.4, temos o quarto resultado principal deste trabalho.

Teorema 4.18. *Seja Q um polinômio-chave com $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$. Suponhamos que Q seja irredutível sobre $\mathbb{K}^d(\overline{\nu})$. Seja $(a,\delta) = (a,\delta(Q))$ um par minimal associado a Q. Então*

$$\overline{D}(Q,\mu(Q)) = \bigcup_{\sigma \in G^d(\overline{\nu})} D(\sigma(a),\delta(Q)),$$

$\mu_{\overline{D}(Q,\mu(Q))}$ é uma valorização em $\mathbb{K}[x]$ e

$$\mu_Q = \mu_{\overline{D}(Q,\mu(Q))}.$$

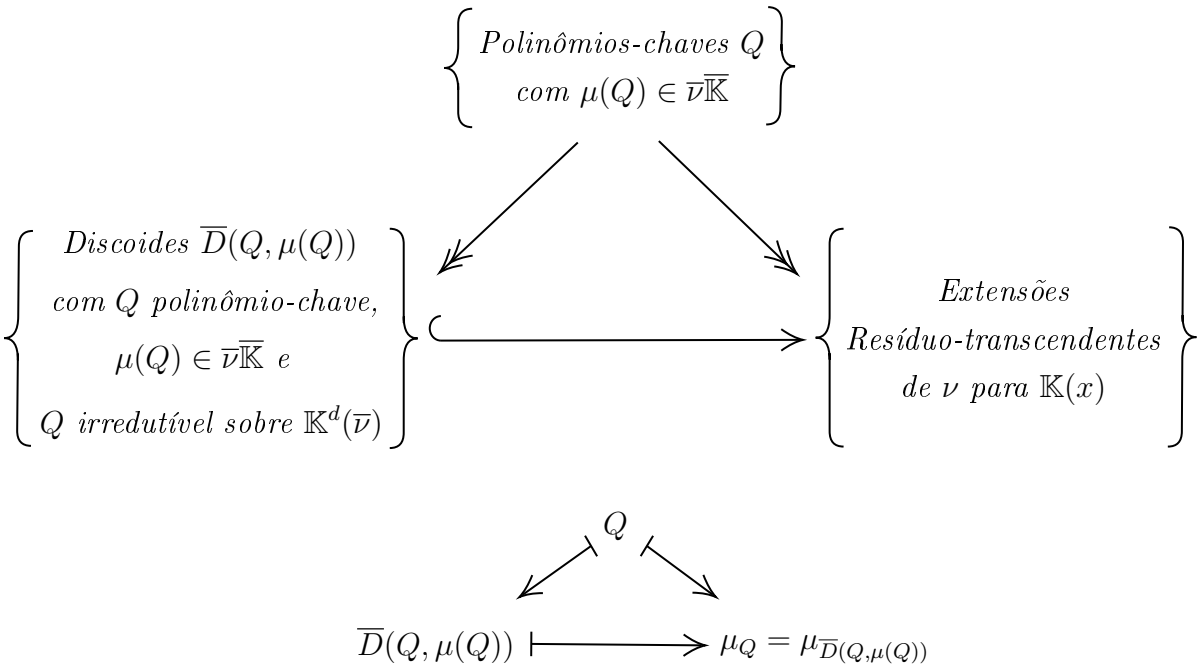
Demonstração: A descrição do discoide e o fato de $\overline{\mu}_{\overline{D}(Q,\mu(Q))}$ ser valorização seguem do Teorema 4.17. Sendo (a,δ) um par minimal associado ao polinômio-chave Q temos

$$\mu_Q = \overline{\mu}_{a,\delta}|_{\mathbb{K}[x]} = \overline{\mu}_{D(a,\delta)}|_{\mathbb{K}[x]} = \mu_{\overline{D}(Q,\mu(Q))}.$$

■

Podemos agora demonstrar um análogo do Teorema 4.5, em que veremos que os discoides nos fornecem a unicidade que buscamos, no sentido de que $\mu_{\overline{D}(Q,\mu(Q))} = \mu_{\overline{D}(Q',\mu(Q'))}$ implicará $\overline{D}(Q,\mu(Q)) = \overline{D}(Q',\mu(Q'))$.

Teorema 4.19. *Seja ν valorização em $\mathbb{K}$. Sejam μ uma valorização em $\mathbb{K}[x]$ e $\overline{\nu}$ uma valorização em $\overline{\mathbb{K}}$, ambas extensões de ν. Temos as seguintes relações entre os conjuntos abaixo:*



Demonstração: A aplicação que toma um polinômio-chave Q com $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ e leva no discoide $\overline{D}(Q,\mu(Q))$ é sobrejetora se restringimos a coleção dos discoides aos discoides centrados em polinômios chaves com valor em $\overline{\nu}\overline{\mathbb{K}}$.

Olhemos agora para a aplicação que toma um polinômio-chave Q com $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ e leva na valorização μ_Q. Como vimos no Corolário 3.40, μ_Q é de fato uma extensão resíduo-transcendente de ν. Agora, dada uma extensão resíduo-transcendente μ qualquer de ν para $\mathbb{K}(x)$, temos que essa é resíduo-transcendente em $\mathbb{K}[x]$. Logo, $\mu = \mu_Q$ para algum polinômio chave Q e $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ (Teorema 3.20 e Teorema 3.22), mostrando a sobrejetividade da aplicação em questão.

Consideremos por último a aplicação que leva um discoide $\overline{D}(Q, \mu(Q))$, com Q polinômio-chave, $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ e Q irredutível sobre $\mathbb{K}^d(\overline{\nu})$, na valorização $\mu_Q = \mu_{\overline{D}(Q,\mu(Q))}$. Pelo Corolário 3.40, μ_Q é de fato uma extensão resíduo-transcendente de ν. Mostraremos a injetividade. Sejam $\overline{D}(Q, \mu(Q))$ e $\overline{D}(Q', \mu(Q'))$ dois discoides com Q e Q' polinômios-chaves irredutíveis sobre $\mathbb{K}^d(\overline{\nu})$ tais que $\mu(Q), \mu(Q') \in \overline{\nu}\overline{\mathbb{K}}$. Sejam $a, a' \in \overline{\mathbb{K}}$ raízes, respectivamente, de Q e Q' satisfazendo $\delta(Q) = \overline{\mu}(x - a)$ e $\delta(Q') = \overline{\mu}(x - a')$. Pelo Teorema 4.18, temos

$$\overline{D}(Q, \mu(Q)) = \bigcup_{\sigma \in G^d(\overline{\nu})} D(\sigma(a), \delta(Q))$$

e

$$\overline{D}(Q', \mu(Q')) = \bigcup_{\sigma \in G^d(\overline{\nu})} D(\sigma(a'), \delta(Q')).$$

Suponhamos $\mu_{\overline{D}(Q,\mu(Q))} = \mu_{\overline{D}(Q',\mu(Q'))}$. Pelo Teorema 4.18,

$$\mu_{\overline{D}(Q,\mu(Q))} = \mu_Q = \overline{\mu}_{a,\delta(Q)}|_{\mathbb{K}[x]} \text{ e } \mu_{\overline{D}(Q',\mu(Q'))} = \mu_{Q'} = \overline{\mu}_{a',\delta(Q')}|_{\mathbb{K}[x]}.$$

Dessa forma, ambas $\overline{\mu}_{a,\delta(Q)}$ e $\overline{\mu}_{a',\delta(Q')}$ são extensões de μ_Q e $\overline{\nu}$ para $\overline{\mathbb{K}}[x]$. Logo, deve existir $\tau \in G^d(\overline{\nu})$ tal que

$$\overline{\mu}_{a',\delta(Q')} = \overline{\mu}_{\tau(a),\delta(Q)}.$$

Porém essas duas valorizações monomiais serão iguais se, e somente se, $\delta = \delta(Q) = \delta(Q')$ e $\overline{\nu}(a' - \tau(a)) \geq \delta$. Dessa forma, dado $\sigma \in G^d(\overline{\nu})$ qualquer, temos que

$$D(\sigma(a'), \delta) = D(\sigma(\tau(a)), \delta),$$

pois

$$\overline{\nu}(\sigma(a') - \sigma(\tau(a))) = \overline{\nu}(\sigma(a' - \tau(a))) = \overline{\nu}(a' - \tau(a)) \geq \delta,$$

e

$$D(\sigma(a), \delta) = D(\sigma(\tau^{-1}(a')), \delta),$$

uma vez que

$$\begin{aligned}\overline{\nu}(\sigma(a)-\sigma(\tau^{-1}(a'))) &= \overline{\nu}(\sigma(a-\tau^{-1}(a'))) \\ &= \overline{\nu}(a-\tau^{-1}(a')) \\ &= \overline{\nu}(\tau^{-1}(\tau(a)-a'))) \\ &= \overline{\nu}(\tau(a)-a') \\ &\geq \delta.\end{aligned}$$

Isto é,

$$\overline{D}(Q,\mu(Q)) = \bigcup_{\sigma\in G^d(\overline{\nu})} D(\sigma(a),\delta(Q)) = \bigcup_{\sigma\in G^d(\overline{\nu})} D(\sigma(a'),\delta(Q')) = \overline{D}(Q',\mu(Q')),$$

mostrando a injetividade da aplicação.

■

No trabalho de Bengus-Lasnier (2021), são levantadas as seguintes conjecturas: μ_Q pode ser definido como mínimo sobre um discoide para qualquer polinômio-chave Q com $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ e a função acima, que leva um discoide $\overline{D}(Q,\mu(Q))$ com $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ em uma extensão resíduo-transcendente de ν, é na verdade uma bijeção. Estas afirmações podem ser deduzidas da seguinte conjectura.

Conjectura 4.20. *Todo polinômio-chave $Q \in \mathbb{K}[x]$ com $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ é irredutível sobre $\mathbb{K}^d(\overline{\nu})$.*

A condição $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$ implica que μ_Q será uma extensão resíduo-transcendente de ν. Assim, assumindo a conjectura, a sobrejetividade da função mencionada anteriormente segue do fato que uma extensão resíduo-transcendente $\mu \mid \nu$ é igual a um truncamento em um polinômio-chave Q com valor em $\overline{\nu}\overline{\mathbb{K}}$ (Teorema 3.22).

Tal conjectura é um resultado imediato se o corpo $\mathbb{K}$ for henseliano, pois nessa situação $\mathbb{K}^d(\overline{\nu}) = \mathbb{K}$ e sabemos que Q um polinômio-chave sempre é irredutível em $\mathbb{K}[x]$. No trabalho de Bengus-Lasnier (2021, p. 425), outro caso particular, porém não trivial, é demonstrado. O autor demonstra que a conjectura é verdadeira quando a valorização ν em $\mathbb{K}$ é de posto um, isto é, quando podemos mergulhar o grupo de valores $\nu\mathbb{K}$ no grupo aditivo $(\mathbb{R},+,0)$. Segundo Bengus-Lasnier (2021, p. 428), Kuhlmann é pessimista quanto a validade da Conjectura 4.20 em geral, isto é, para valorizações cujo posto de seu grupo de valores é maior do que um (veja a definição de posto no Apêndice B).

Capítulo 5

Todas as valorizações em $\mathbb{K}(x)$

Neste último capítulo descreveremos todas as valorizações no corpo de funções racionais $\mathbb{K}(x)$. Ao longo do texto, foram definidas classes de valorizações em $\mathbb{K}(x)$. São estas: as valorizações transcendentes, que se subdividem em dois tipos, e as valorizações algébricas. Tratamos das valorizações transcendentes no Capítulo 3. Resta então discutirmos sobre as valorizações algébricas.

Na primeira seção, apresentaremos e discutiremos o conceito de sistema ordenado de valorizações resíduo-transcendentes. Abriremos então uma subseção, em que descreveremos uma valorização algébrica como um limite de um sistema ordenado de valorizações resíduo-transcendentes. Em seguida, na segunda seção, faremos a descrição das valorizações em $\mathbb{K}(x)$ com base na teoria que desenvolvemos ao longo deste trabalho.

As principais referências para a composição deste capítulo foram os trabalhos de Alexandru, Popescu e Zaharescu (1990a, 1990b).

5.1 Sistemas ordenados de valorizações

Nesta seção vamos estudar o conceito de sistemas ordenados de valorizações resíduo-transcendentes. Usaremos essa ferramenta para mostrar, na seção a seguir, que uma valorização algébrica pode ser vista como um limite de um sistema dessa natureza.

Definição 5.1. *Seja ν uma valorização em $\mathbb{K}$ e consideremos μ_1 e μ_2 duas extensões resíduo-transcendentes de ν para $\mathbb{K}(x)$. Diremos que $\boldsymbol{\mu_1 \leq \mu_2}$ se $\mu_1(f) \leq \mu_2(f)$ para todo $f \in \mathbb{K}[x]$. Se $\mu_1 \leq \mu_2$ e existe $f \in \mathbb{K}[x]$ tal que $\mu_1(f) < \mu_2(f)$, então escreveremos $\boldsymbol{\mu_1 < \mu_2}$.*

■

A desigualdade $\mu_1(f) \leq \mu_2(f)$ acontece em $\nu\mathbb{K} \otimes \mathbb{Q}$, isto é, em $\overline{\nu}\overline{\mathbb{K}}$, uma vez fixados $\overline{\mathbb{K}}$ e $\overline{\nu}$. Isto porque vimos no Teorema 3.20 que para qualquer extensão $\overline{\mu}_1$ de μ_1 e $\overline{\mu}_2$ de μ_2 para $\overline{\mathbb{K}}(x)$, estas serão também resíduo-transcendentes e $\mu_i\mathbb{K}(x) \subset \overline{\mu}_i\overline{\mathbb{K}}(x) = \overline{\nu}\overline{\mathbb{K}}$, $i = 1, 2$.

Proposição 5.2. *Seja $\overline{\nu}$ valorização em $\overline{\mathbb{K}}$ e consideremos $\overline{\mu}_1$ e $\overline{\mu}_2$ extensões resíduo-transcendentes de $\overline{\nu}$ para $\overline{\mathbb{K}}(x)$. Seja (a_i, δ_i) um par de definição de $\overline{\mu}_i$, $i = 1, 2$. As afirmações a seguir são equivalentes.*

1. $\overline{\mu}_1 \leq \overline{\mu}_2$.

2. $\delta_1 \leq \delta_2$ *e* $\overline{\nu}(a_1 - a_2) \geq \delta_1$.

Além disso, $\overline{\mu}_1 < \overline{\mu}_2$ se, e somente se, $\delta_1 < \delta_2$ e $\overline{\nu}(a_1 - a_2) \geq \delta_1$.

Demonstração:

(1. $\Rightarrow$ 2.) Do Teorema 3.20 sabemos que $\overline{\mu}_i(x - a_i) = \delta_i$. Se $\overline{\mu}_1 \leq \overline{\mu}_2$, então

$$\delta_1 = \overline{\mu}_1(x - a_1) \leq \overline{\mu}_2(x - a_1) = \min\{\delta_2, \overline{\nu}(a_1 - a_2)\}.$$

Ou seja, $\delta_1 \leq \delta_2$ e $\overline{\nu}(a_1 - a_2) \geq \delta_1$.

(2. $\Rightarrow$ 1.) Se $\overline{\nu}(a_1 - a_2) \geq \delta_1$, então, segundo o Lema 3.1, (a_2, δ_1) é também um par de definição para $\overline{\mu}_1$. Seja $f \in \mathbb{K}[x]$ qualquer e o escrevamos como

$$f(x) = \sum_{j=0}^{s} b_j(x - a_2)^j.$$

Temos

$$\overline{\mu}_1(f) = \min_{0 \leq j \leq s}\{\overline{\nu}(b_j) + j\delta_1\} \text{ e } \overline{\mu}_2(f) = \min_{0 \leq j \leq s}\{\overline{\nu}(b_j) + j\delta_2\}.$$

Como $\delta_1 \leq \delta_2$ segue que $\overline{\nu}(b_j) + j\delta_1 \leq \overline{\nu}(b_j) + j\delta_2$ para todo j, $0 \leq j \leq s$. Logo, $\overline{\mu}_1(f) \leq \overline{\mu}_2(f)$.

Por fim, suponhamos $\overline{\mu}_1 < \overline{\mu}_2$. Logo existe $a \in \overline{\mathbb{K}}$ tal que

$$\overline{\mu}_1(x - a) = \min\{\delta_1, \overline{\nu}(a_1 - a)\} < \overline{\mu}_2(x - a) = \min\{\delta_2, \overline{\nu}(a_2 - a)\}.$$

Da equivalência acima já sabemos que $\delta_1 \leq \delta_2$. Se $\delta_1 = \delta_2$, então teríamos duas opções. Na primeira opção,

$$\delta_1 = \min\{\delta_1, \overline{\nu}(a_1 - a)\} < \min\{\delta_2, \overline{\nu}(a_2 - a)\} \leq \delta_2,$$

o que seria uma contradição. Na segunda opção,

$$\overline{\nu}(a_1 - a) = \min\{\delta_1, \overline{\nu}(a_1 - a)\} < \min\{\delta_2, \overline{\nu}(a_2 - a)\}.$$

Isso implicaria que

$$\delta_1 \leq \overline{\nu}(a_1 - a_2) = \min\{\overline{\nu}(a_1 - a), \overline{\nu}(a_2 - a)\} = \overline{\nu}(a_1 - a) < \delta_2,$$

o que também é uma contradição. Assim, devemos ter $\delta_1 < \delta_2$.

Por outro lado, se $\delta_1 < \delta_2$ e $\overline{\nu}(a_1 - a_2) \geq \delta_1$, então pela equivalência anterior termos $\overline{\mu}_1 \leq \overline{\mu}_2$. Mas,

$$\overline{\mu}_1(x - a_2) = \delta_1 < \delta_2 = \overline{\mu}_2(x - a_2).$$

Ou seja, $\overline{\mu}_1 < \overline{\mu}_2$.

■

Definição 5.3. *Seja ν uma valorização em $\mathbb{K}$. Um* ***sistema ordenado de extensões resíduo-transcendentes*** *de ν para $\mathbb{K}(x)$ é uma família $(\mu_i)_{i\in I}$ de extensões resíduo-transcendentes de ν para $\mathbb{K}(x)$ tal que $\mu_i \leq \mu_j$ se $i < j$, sendo I um conjunto bem-ordenado sem maior elemento.*

■

Seja $(\mu_i)_{i\in I}$ um sistema ordenado de extensões resíduo-transcendentes de ν para $\mathbb{K}(x)$. Lembrando que $\mu_i\mathbb{K}(x) \subseteq \overline{\nu}\overline{\mathbb{K}}$, para cada $f \in \mathbb{K}[x]$ podemos considerar o subconjunto $\{\mu_i(f) \mid i \in I\} \subset \overline{\nu}\overline{\mathbb{K}}$. Olharemos para $\sup_{i\in I}\{\mu_i(f)\}$, que pode ou não existir. Diremos que o sistema ordenado $(\mu_i)_{i\in I}$ possui **limite** se para todo $f \in \mathbb{K}[x]$ tivermos que $\sup_{i\in I}\{\mu_i(f)\}$ existe em $\overline{\nu}\overline{\mathbb{K}}$. Nessa situação, vejamos que a aplicação

$$\begin{aligned} \mu : \mathbb{K}[x] &\longrightarrow \overline{\nu}\overline{\mathbb{K}} \cup \{\infty\} \\ f &\longmapsto \sup_{i\in I}\{\mu_i(f)\},\ f \neq 0 \\ 0 &\longmapsto \infty \end{aligned}$$

define uma valorização em $\mathbb{K}[x]$, que será estendida para $\mathbb{K}(x)$ da maneira canônica.

- $(V1)$ Sejam $f, g \in \mathbb{K}[x]$. Por hipótese $\mu(f) = \sup_{i\in I}\{\mu_i(f)\}$ e $\mu(g) = \sup_{i\in I}\{\mu_i(g)\}$. Portanto,

  $$\mu(f) + \mu(g) \geq \mu_i(f) + \mu_i(g) = \mu_i(fg)$$

  para todo $i \in I$. Logo, $\mu(f) + \mu(g)$ é um limitante superior para $\{\mu_i(fg)\}_{i\in I}$. Mas, por hipótese, existe $\mu(fg) = \sup_{i\in I}\{\mu_i(fg)\}$. Dessa forma,

  $$\mu(f) + \mu(g) \geq \mu(fg).$$

Suponhamos, por contradição, que $\mu(f)+\mu(g) > \mu(fg)$. Seja $\gamma = \mu(f)+\mu(g)-\mu(fg) > 0$. Como $\overline{\nu}\overline{\mathbb{K}}$ é divisível e livre de torção, existe um único $\gamma' \in \overline{\nu}\overline{\mathbb{K}}$ tal que $2\gamma' = \gamma$. Mais que isso, como $\gamma > 0$ segue que também teremos $\gamma' > 0$.

Uma vez que $\mu(f) > \mu(f) - \gamma'$ e $\mu(g) > \mu(g) - \gamma'$, existem $j, k \in I$ tais que

$$\mu_j(f) > \mu(f) - \gamma' \text{ e } \mu_k(g) > \mu(g) - \gamma'.$$

Seja $m = \max\{j, k\}$. Assim,

$$\begin{aligned}\mu_m(fg) = \mu_m(f) + \mu_m(g) &> \mu(f) - \gamma' + \mu(g) - \gamma' \\ &= \mu(f) + \mu(g) - \gamma \\ &= \mu(f) + \mu(g) - \mu(f) - \mu(g) + \mu(fg) \\ &= \mu(fg),\end{aligned}$$

contradizendo o fato de $\mu(fg)$ ser supremo de $\{\mu_i(fg)\}_{i\in I}$. Logo, $\mu(fg) = \mu(f) + \mu(g)$.

- $(V2)$ Sejam $f, g \in \mathbb{K}[x]$ e suponhamos, sem perda de generalidade, que $\mu(f) \geq \mu(g)$. Suponhamos por contradição que $\mu(f) \geq \mu(g) > \mu(f+g)$. Então $\mu(f+g)$ não é limitante superior para os conjuntos $\{\mu_i(f)\}_{i\in I}$ e $\{\mu_i(g)\}_{i\in I}$. Assim, existem $j, k \in I$ tais que

$$\mu_j(f) > \mu(f+g) \text{ e } \mu_k(g) > \mu(f+g).$$

Seja $m = \max\{j, k\}$. Então

$$\mu(f+g) = \sup_{i\in I}\{\mu_i(f+g)\} \geq \mu_m(f+g) \geq \min\{\mu_m(f), \mu_m(g)\} > \mu(f+g),$$

o que é uma contradição. Logo, $\mu(f+g) \geq \min\{\mu(f), \mu(g)\}$.

- $(V3)$ Temos $\mu(1) = \sup_{i\in I}\{\mu_i(1)\} = \sup_{i\in I}\{0\} = 0$. Por definição, $\mu(0) = \infty$.

Essa valorização é uma extensão de ν para $\mathbb{K}(x)$ e será chamada de **limite** do sistema $(\mu_i)_{i\in I}$. Denotaremos $\mu = \sup_{i\in I} \mu_i$.

Consideremos $\overline{\mathbb{K}}$ um corpo algebricamente fechado e $(\overline{\mu}_i)_{i\in I}$ um sistema ordenado de extensões resíduo-transcendentes de $\overline{\nu}$ em $\overline{\mathbb{K}}$ para $\overline{\mathbb{K}}(x)$. Para cada $i \in I$, fixamos um par de definição (a_i, δ_i) para $\overline{\mu}_i$. Pela Proposição 5.2, $\{\delta_i\}_{i\in I}$ é um subconjunto bem ordenado de $\overline{\nu}\overline{\mathbb{K}}$. A seguir veremos uma condição para a existência de limite para o sistema $(\overline{\mu}_i)_{i\in I}$ com base nos pares de definição. É interessante notar que o limite de um sistema ordenado pode não ser uma valorização resíduo-transcendente. Antes, mostraremos um lema.

Lema 5.4. *Seja $(\overline{\mu}_i)_{i\in I}$ um sistema ordenado de extensões resíduo-transcendentes de $\overline{\nu}$ em $\overline{\mathbb{K}}$ para $\overline{\mathbb{K}}(x)$. Seja*

$$f(x) = c\prod_{l=1}^{n}(x-b_l) \in \overline{\mathbb{K}}[x]$$

tal que, para cada b_l, existe $j_l \in I$ tal que $\sup\limits_{i\in I}\{\overline{\mu}_i(x-b_l)\} = \overline{\mu}_{j_l}(x-b_l)$. Então, $\sup\limits_{i\in I}\{\overline{\mu}_i(f)\}$ está bem definido em $\overline{\nu}\overline{\mathbb{K}}$.

Demonstração: Como $\sup\limits_{i\in I}\{\overline{\mu}_i(x-b_l)\} = \overline{\mu}_{j_l}(x-b_l)$, segue que para todo $i \in I$

$$S = \overline{\nu}(c) + \sum_{l=1}^{n}\overline{\mu}_{j_l}(x-b_l) \geq \overline{\mu}_i(c) + \sum_{l=1}^{n}\overline{\mu}_i(x-b_l) = \overline{\mu}_i(f(x)).$$

Isso mostra que S é um limitante superior para $\{\overline{\mu}_i(f(x))\}_{i\in I}$. Vejamos que S pertence a $\{\overline{\mu}_i(f(x))\}_{i\in I}$, o que mostra que S é supremo do conjunto. Seja $k \in I$ tal que $k \geq \max\limits_{1\leq l\leq n}\{j_l\}$. Tal k existe pois I não possui maior elemento. Então, como $(\overline{\mu}_i)_{i\in I}$ é um sistema ordenado, para todo l vale $\overline{\mu}_k \geq \overline{\mu}_{j_l}$. Isso implica que $\overline{\mu}_k(x-b_l) \geq \overline{\mu}_{j_l}(x-b_l)$. Mas, $\overline{\mu}_{j_l}(x-b_l) \geq \overline{\mu}_k(x-b_l)$ pois $\overline{\mu}_{j_l}(x-b_l)$ é o supremo. Logo, $\overline{\mu}_{j_l}(x-b_l) = \overline{\mu}_k(x-b_l)$. Assim,

$$S = \overline{\nu}(c) + \sum_{l=1}^{n}\overline{\mu}_{j_l}(x-b_l) = \overline{\mu}_k(c) + \sum_{l=1}^{n}\overline{\mu}_k(x-b_l) = \overline{\mu}_k(f(x)).$$

Portanto, $\sup\limits_{i\in I}\{\overline{\mu}_i(f)\}$ está bem definido em $\overline{\nu}\overline{\mathbb{K}}$.

■

Proposição 5.5. *Sejam $\overline{\mathbb{K}}$ um corpo algebricamente fechado e $(\overline{\mu}_i)_{i\in I}$ um sistema ordenado de extensões resíduo-transcendentes de $\overline{\nu}$ em $\overline{\mathbb{K}}$ para $\overline{\mathbb{K}}(x)$. Para cada $i \in I$, seja (a_i, δ_i) um par minimal de definição para $\overline{\mu}_i$ fixado. As afirmações a seguir são equivalentes.*

1. *O sistema ordenado $(\overline{\mu}_i)_{i\in I}$ possui limite $\overline{\mu}$ que não é uma extensão resíduo-transcendente de $\overline{\nu}$ para $\overline{\mathbb{K}}(x)$.*
2. *Para todo $a \in \overline{\mathbb{K}}$ existe $j \in I$ tal que $\overline{\mu}_j(x-a) < \delta_j$.*

Demonstração:

(1. $\Rightarrow$ 2.) Seja $\overline{\mu} = \sup\limits_{i\in I}\overline{\mu}_i$. Por hipótese, $\overline{\mu}$ não é uma extensão resíduo-transcendente de $\overline{\nu}$. Pelo Teorema 3.20, isso significa que o conjunto

$$M_{\overline{\mu}} := \{\overline{\mu}(x-b) \mid b \in \overline{\mathbb{K}}\} \subseteq \overline{\mu}\overline{\mathbb{K}}(x)$$

ou não é limitado em $\overline{\mu}\overline{\mathbb{K}}(x)$ ou é limitado mas não contém seu limitante superior. Seja $a \in \overline{\mathbb{K}}$. Em ambos os casos, deve existir $b \in \overline{\mathbb{K}}$ tal que $\overline{\mu}(x-a) < \overline{\mu}(x-b)$. Mas, $\overline{\mu}(x-b) = \sup\limits_{i\in I}\{\overline{\mu}_i(x-b)\}$.

Pela definição de supremo, existe $j \in I$ tal que $\overline{\mu}(x-a) < \overline{\mu}_j(x-b)$. Ainda, pelo Lema 3.5, temos $\overline{\mu}_j(x-b) \leq \overline{\mu}_j(x-a_j) = \delta_j$. Como $\overline{\mu}(x-a) = \sup_{i\in I}\{\overline{\mu}_i(x-a)\}$, temos

$$\overline{\mu}_j(x-a) \leq \overline{\mu}(x-a) < \overline{\mu}_j(x-b) \leq \overline{\mu}_j(x-a_j) = \delta_j.$$

(2. $\Rightarrow$ 1.) Seja $a \in \overline{\mathbb{K}}$. Por hipótese, existe $j \in J$ tal que $\overline{\mu}_j(x-a) < \delta_j$. Mostremos que isso implica $\sup_{i\in I}\{\overline{\mu}_i(x-a)\} = \overline{\mu}_j(x-a)$.

Como $\overline{\mu}_j(x-a) \in \{\overline{\mu}_i(x-a)\}_{i\in I}$, basta mostrar que $\overline{\mu}_j(x-a)$ é um limitante superior. De fato, suponhamos por contradição que existe $i \in I$ tal que

$$\overline{\mu}_i(x-a) = \min\{\delta_i, \overline{\nu}(a_i-a)\} > \overline{\mu}_j(x-a) = \min\{\delta_j, \overline{\nu}(a_j-a)\} = \overline{\nu}(a_j-a).$$

A desigualdade acima nos diz que $\overline{\nu}(a_i-a) > \overline{\nu}(a_j-a)$. Como $(\overline{\mu}_i)_{i\in I}$ é um sistema ordenado, com certeza $i > j$. Assim, pela Proposição 5.2,

$$\overline{\mu}_i \geq \overline{\mu}_j \iff \delta_j \leq \delta_i \text{ e } \overline{\nu}(a_j-a_i) \geq \delta_j.$$

Porém,

$$\overline{\nu}(a_j-a_i) = \min\{\overline{\nu}(a_j-a), \overline{\nu}(a-a_i)\} = \overline{\nu}(a_j-a).$$

Isso que implica $\overline{\mu}_j(x-a) = \overline{\nu}(a_j-a) \geq \delta_j$, contradizendo nossa hipótese. Portanto, $\overline{\mu}_j(x-a)$ é limitante superior e o supremo do conjunto.

Pelo Lema 5.4, $\sup_{i\in I}\{\overline{\mu}_i(x-a)\} = \overline{\mu}_j(x-a)$ para todo $a \in \overline{\mathbb{K}}$ implica que $\sup_{i\in I}\{\overline{\mu}_i(f)\}$ está bem-definido para todo $f \in \overline{\mathbb{K}}[x]$. Portanto, $\overline{\mu} = \sup_{i\in I}\overline{\mu}_i$ está definido.

Por fim, mostremos que $\overline{\mu}$ não é uma extensão resíduo-transcendente de $\overline{\nu}$. Suponhamos, por contradição, que $\overline{\mu}$ é uma extensão resíduo-transcendente de $\overline{\nu}$, logo é definida por um par (a,δ). Por hipótese, existe $j \in I$ tal que $\overline{\mu}_j(x-a) < \delta_j$. Assim, $\overline{\mu}(x-a) < \delta_j$ pois $\overline{\mu}(x-a) = \sup_{i\in I}\{\overline{\mu}_i(x-a)\} = \overline{\mu}_j(x-a)$. Temos também que $\overline{\mu} \geq \overline{\mu}_i$ para todo $i \in I$. Dessa forma,

$$\overline{\mu}_j(x-a_j) = \delta_j \leq \overline{\mu}(x-a_j) = \min\{\overline{\mu}(x-a), \overline{\nu}(a-a_j)\} \leq \overline{\mu}(x-a),$$

o que é uma contradição. Portanto, $\overline{\mu}$ não é resíduo-transcendente.

■

Uma condição necessária e suficiente para que o sistema ordenado $(\overline{\mu}_i)_{i\in I}$ possua um limite que é uma valorização resíduo-transcendente é existir um elemento $a \in \overline{\mathbb{K}}$ tal que $\overline{\nu}(a-a_i) \geq \delta_i$, para todo $i \in I$, e $\sup_{i\in I}\{\delta_i\}$ existir e pertencer a $\overline{\nu}\overline{\mathbb{K}}$ (ALEXANDRU; POPESCU; ZAHARESCU, 1990a, p. 283).

No teorema abaixo veremos que um sistema ordenado em $\overline{\mathbb{K}}(x)$ induz um sistema ordenado em $\mathbb{K}(x)$.

Teorema 5.6. *Sejam $\mathbb{K}$ um corpo e $(\overline{\mu}_i)_{i\in I}$ um sistema ordenado de extensões resíduo-transcendentes de $\overline{\nu}$ de $\overline{\mathbb{K}}$ para $\overline{\mathbb{K}}(x)$. Denotemos por μ_i a restrição de $\overline{\mu}_i$ a $\mathbb{K}(x)$. As afirmações a seguir são satisfeitas.*

1. *Temos que $(\mu_i)_{i\in I}$ é um sistema ordenado de extensões resíduo-transcendentes de ν para $\mathbb{K}(x)$.*

2. *Suponhamos que esteja bem-definido $\overline{\mu} = \sup_{i\in I} \overline{\mu}_i$. Seja μ a restrição de $\overline{\mu}$ para $\mathbb{K}(x)$. Então $\mu = \sup_{i\in I} \mu_i$.*

Demonstração:

- Devido às equivalências do Teorema 3.20, sabemos que $\overline{\mu}_i$ é extensão resíduo-transcendente de $\overline{\nu}$ se, e somente se, μ_i é extensão resíduo-transcendente de ν. Seja $f \in \mathbb{K}[x]$. O fato de $(\overline{\mu}_i)_{i\in I}$ ser um sistema ordenado implica que, para $i, j \in I$ com $i < j$, temos
$$\mu_i(f) = \overline{\mu}_i(f) \leq \overline{\mu}_j(f) = \mu_j(f).$$
Portanto, $(\mu_i)_{i\in I}$ é um sistema ordenado de extensões resíduo-transcendentes de ν para $\mathbb{K}(x)$.

- Suponhamos $\overline{\mu} = \sup_{i\in I} \overline{\mu}_i$. Então $\mu = \sup_{i\in I} \mu_i$ pois, para todo $f \in \mathbb{K}[x]$, temos
$$\sup_{i\in I}\{\mu_i(f)\} = \sup_{i\in I}\{\overline{\mu}_i(f)\} = \overline{\mu}(f) = \mu(f) \in \overline{\nu}\overline{\mathbb{K}}.$$

■

5.1.1 Valorizações algébricas

Lembramos que uma valorização é dita algébrica se não é transcendente. Ou seja, μ é algébrica se, e somente se, $\mathrm{supp}(\mu) = \{0\}$, o valor de todo polinômio não nulo de $\mathbb{K}[x]$ é de torção sobre $\nu\mathbb{K}$ (isto é, $\mu\mathbb{K}(x)/\nu\mathbb{K}$ é grupo de torção) e o resíduo de todo elemento de $\mathcal{O}_\mu$ é algébrico sobre $\mathbb{K}\nu$ (isto é, $\mathbb{K}(x)\mu \mid \mathbb{K}\nu$ é uma extensão algébrica).

Lema 5.7. *Se μ é algébrica, então $\mu\mathbb{K}(x) \subseteq \overline{\nu}\overline{\mathbb{K}}$.*

Demonstração: Se μ é algébrica, então $\mu\mathbb{K}(x)/\nu\mathbb{K}$ é de torção, por isso para todo $\gamma \in \mu\mathbb{K}(x)$ existe $m \in \mathbb{N}$ tal que $m\gamma \in \overline{\nu}\overline{\mathbb{K}}$. Mas, $\overline{\nu}\overline{\mathbb{K}}$ é divisível. Logo, para o mesmo número natural m existe $\gamma' \in \overline{\nu}\overline{\mathbb{K}}$ tal que $m\gamma = m\gamma'$. Porém, o grupo $\overline{\nu}\overline{\mathbb{K}}$ é livre de torção, logo a igualdade anterior implica $\gamma = \gamma' \in \overline{\nu}\overline{\mathbb{K}}$, mostrando a inclusão desejada.

■

Veremos que as valorização algébricas podem ser descritas como limite de um sistema ordenado de extensões resíduo-transcendentes de $\nu = \mu|_{\mathbb{K}}$. Ou seja, as valorizações algébricas podem ser vistas em termos de valorizações transcendentes, mais especificamente em termos de valorizações resíduo-transcendentes.

Teorema 5.8. *Seja $\overline{\mu}$ uma extensão de $\overline{\nu}$ em $\overline{\mathbb{K}}$ para $\overline{\mathbb{K}}(x)$ tal que $\overline{\mu}$ é valorização algébrica. Então existe $(\overline{\mu}_i)_{i\in I}$ um sistema ordenado de extensões resíduo-transcendentes de $\overline{\nu}$ para $\overline{\mathbb{K}}(x)$ tal que $\overline{\mu} = \sup_{i\in I} \overline{\mu}_i$.*

Demonstração: Como $\overline{\mu}$ é valorização algébrica, o quociente $\overline{\mu}\overline{\mathbb{K}}(x)/\overline{\nu}\overline{\mathbb{K}}$ é um grupo de torção. Mostremos inicialmente que $\overline{\mu}\overline{\mathbb{K}}(x) = \overline{\nu}\overline{\mathbb{K}}$. Já sabemos que $\overline{\nu}\overline{\mathbb{K}} \subseteq \overline{\mu}\overline{\mathbb{K}}(x)$. A outra inclusão segue do Lema 5.7.

Consideremos $M_{\overline{\mu}} = \{\overline{\mu}(x-b) \mid b \in \overline{\mathbb{K}}\}$. Como $\overline{\mu}$ não é resíduo-transcendente segue do Teorema 3.20 que ou $M_{\overline{\mu}}$ não possui limitante superior ou esse conjunto não contém seu limitante superior. Sabemos que $M_{\overline{\mu}} \subset \overline{\nu}\overline{\mathbb{K}}$ é totalmente ordenado. Então $M_{\overline{\mu}}$ deve conter um subconjunto $\{\delta_i\}_{i\in I}$ bem ordenado e cofinal (HOWARD; RUBIN, 1998). Isto é, a ordem de $M_{\overline{\mu}}$ torna $\{\delta_i\}_{i\in I}$ bem-ordenado e, para todo $\gamma \in M_{\overline{\mu}}$, existe $\delta_j \in \{\delta_i\}_{i\in I}$ tal que $\gamma \leq \delta_j$. Ordenamos I com a relação $i < j$ se, e somente se, $\delta_i < \delta_j$ para todo $i, j \in I$. Como $M_{\overline{\mu}}$ não contém um limitante superior, concluímos que I é bem-ordenado e não possui maior elemento.

Para cada $i \in I$, escolhemos $a_i \in \overline{\mathbb{K}}$ tal que

$$\overline{\mu}(x - a_i) = \delta_i.$$

Consideramos $\overline{\mu}_i := \overline{\mu}_{a_i,\delta_i}$. Como $\delta_i \in \overline{\nu}\overline{\mathbb{K}}$, o Corolário 3.21 nos diz que $\overline{\mu}_i$ é uma extensão resíduo-transcendente de $\overline{\nu}$ para $\overline{\mathbb{K}}(x)$. Mostremos que $(\overline{\mu}_i)_{i\in I}$ é um sistema ordenado de extensões resíduo-transcendentes de $\overline{\nu}$ para $\overline{\mathbb{K}}(x)$. Sejam $i, j \in I$, com $i < j$. Como $\overline{\mathbb{K}}$ é algebricamente fechado, é suficiente mostrar que para todo $b \in \overline{\mathbb{K}}$ temos

$$\overline{\mu}_i(x - b) \leq \overline{\mu}_j(x - b).$$

Como $i < j$ se, e somente se, $\delta_i = \overline{\mu}(x - a_i) < \delta_j = \overline{\mu}(x - a_j)$, temos que

$$\overline{\nu}(a_i - a_j) = \overline{\mu}(a_i - a_j) = \overline{\mu}(a_i - x + x - a_j) = \overline{\mu}(a_i - x) = \delta_i.$$

Para todo $b \in \overline{\mathbb{K}}$ sabemos que

$$\overline{\mu}_i(x-b) = \min\{\delta_i, \overline{\nu}(a_i - b)\} \text{ e } \overline{\mu}_j(x-b) = \min\{\delta_j, \overline{\nu}(a_j - b)\}.$$

Portanto,

$$\overline{\nu}(a_j - b) = \overline{\nu}(a_j - a_i + a_i - b) \geq \min\{\delta_i, \overline{\nu}(a_i - b)\} = \overline{\mu}_i(x-b)$$

e

$$\overline{\mu}_j(x-b) = \min\{\delta_j, \overline{\nu}(a_j - b)\} \geq \min\{\delta_i, \overline{\nu}(a_i - b)\} = \overline{\mu}_i(x-b).$$

Dessa forma, vemos que $(\overline{\mu}_i)_{i\in I}$ é um sistema ordenado de extensões resíduo-transcendentes de $\overline{\nu}$ para $\overline{\mathbb{K}}(x)$.

Vejamos que $\overline{\mu} = \sup_{i\in I} \overline{\mu}_i$. Seja $b \in \overline{\mathbb{K}}$. Mostremos primeiro que existe $j \in I$ tal que

$$\overline{\mu}(x-b) = \overline{\mu}_j(x-b) = \sup_{i\in I}\{\overline{\mu}_i(x-b)\}.$$

De fato, temos que $\overline{\mu}(x-b)$ é um limitante superior desse conjunto pois

$$\overline{\mu}(x-b) \geq \min\{\overline{\mu}(x-a_i), \overline{\nu}(a_i - b)\} = \min\{\delta_i, \overline{\nu}(a_i - b)\} = \overline{\mu}_i(x-b)$$

para todo $i \in I$. Agora, como $\overline{\mu}(x-b) \in M_{\overline{\mu}}$ e $\{\delta_i\}_{i\in I}$ é cofinal, deve existir $j \in I$ tal que $\overline{\mu}(x-b) < \delta_j$. Assim,

$$\overline{\mu}(x-b) \geq \min\{\delta_i, \overline{\nu}(a_j - b)\}$$

ou seja, $\overline{\mu}(x-b) = \overline{\nu}(a_j - b) < \delta_i$. Logo, $\overline{\mu}_j(x-b) = \overline{\nu}(a_j - b)$. Portanto $\overline{\mu}(x-b) = \overline{\mu}_j(x-b) \in \{\overline{\mu}_i(x-b)\}_{i\in I}$, o que mostra que $\overline{\mu}(x-b) = \overline{\mu}_j(x-b) = \sup_{i\in I}\{\overline{\mu}_i(x-b)\}$.

Pelo Lema 5.4, segue que $\sup_{i\in I}\{\overline{\mu}_i(f)\}$ está bem definido em $\overline{\nu}\overline{\mathbb{K}}$ e, por consequência, está bem definido $\sup_{i\in I} \overline{\mu}_i$. Como $\overline{\mu}(f) = \sup_{i\in I}\{\overline{\mu}_i(f)\}$, conclui-se que $\overline{\mu} = \sup_{i\in I} \overline{\mu}_i$.

■

Teorema 5.9. *Seja μ uma extensão de ν em $\mathbb{K}$ para $\mathbb{K}(x)$ tal que μ é valorização algébrica em $\mathbb{K}[x]$. Então existe $(\mu_i)_{i\in I}$ um sistema ordenado de extensões resíduo-transcendentes de ν para $\mathbb{K}(x)$ tal que $\mu = \sup_{i\in I} \mu_i$.*

Demonstração: Tomamos $\overline{\mu}$ em $\overline{\mathbb{K}}(x)$ e $\overline{\nu}$ em $\overline{\mathbb{K}}$ de modo já tradicional. Vejamos que $\overline{\mu}$ também é valorização algébrica em $\overline{\mathbb{K}}[x]$. De fato, como μ não é resíduo-transcendente temos que $\overline{\mu}$ também não o é (Teorema 3.20). Falta verificarmos que $\overline{\mu}$ não é valor-transcendente. Como vimos anteriormente, μ valorização algébrica implica $\mu\mathbb{K}(x) \subseteq \overline{\nu}\overline{\mathbb{K}}$. Se supormos por contradição que $\overline{\mu}$ é valor-transcendente, então existe $\gamma \in \overline{\mu}\overline{\mathbb{K}}(x)$ tal que $m\gamma \notin \overline{\nu}\overline{\mathbb{K}}$ para todo $m \in \mathbb{N}$. Mas, o grupo $\overline{\mu}\overline{\mathbb{K}}(x)/\mu\mathbb{K}(x)$ é de torção pois $\overline{\mathbb{K}}(x) \mid \mathbb{K}(x)$ é uma extensão algébrica.

Então deveria existir $m \in \mathbb{N}$ tal que $m\gamma \in \mu\mathbb{K}(x) \subseteq \overline{\nu}\overline{\mathbb{K}}$, contradição. Logo, $\overline{\mu}$ não é valor-transcendente nem resíduo-transcendente e concluímos que esta é valorização algébrica.

Pelo Teorema acima, existe $(\overline{\mu}_i)_{i\in I}$ um sistema ordenado de extensões resíduo-transcendentes de $\overline{\nu}$ para $\overline{\mathbb{K}}(x)$ tal que $\overline{\mu} = \sup_{i\in I} \overline{\mu}_i$. Denotando por $\mu_i := \overline{\mu}_i|_{\mathbb{K}(x)}$, o Teorema 5.6 nos garante que $\mu = \sup_{i\in I} \mu_i$.

■

5.2 Caracterização das valorizações em $\mathbb{K}(x)$

Nesta última seção descreveremos as valorizações em $\mathbb{K}(x)$ com base no que foi desenvolvido ao longo deste trabalho.

Seja μ uma valorização em $\mathbb{K}(x)$. Denotamos por $\nu = \mu|_{\mathbb{K}}$. Seja $\overline{\nu}$ uma extensão de ν para $\overline{\mathbb{K}}$. Seja $\overline{\mu}$ uma extensão de ambas μ e $\overline{\nu}$ para $\overline{\mathbb{K}}(x)$. Um fato interessante demonstrado no trabalho de Alexandru, Popescu e Zaharescu (1990b) é que existe apenas um número finito de valorizações em $\overline{\mathbb{K}}(x)$ que estendem mutualmente $\overline{\nu}$ e μ. Com base em tudo o que discutimos nesse texto e em outras referências a serem citadas, podemos dizer que a valorização μ se encaixa em alguma das classes disjuntas a seguir:

1. **As valorizações valor-transcendentes**: são aquelas tais que o grupo quociente $\mu\mathbb{K}(x)/\nu\mathbb{K}$ possui um elemento livre de torção. Vimos que μ valor-transcendente implica $\overline{\mu}$ valor-transcendente. No Lema 3.25 prova-se que $\overline{\mu} = \overline{\mu}_{a,\delta}$, em que $\delta = \overline{\mu}(x-a) \in \overline{\mu}\overline{\mathbb{K}}(x) \setminus \overline{\nu}\overline{\mathbb{K}}$ é um elemento livre de torção em $\overline{\mu}\overline{\mathbb{K}}(x)/\overline{\nu}\overline{\mathbb{K}}$.

   O Teorema 3.26 nos diz que $\mu = \mu_Q$ para algum polinômio-chave $Q \in \mathbb{K}[x]$. Este polinômio-chave é o polinômio minimal de a sobre $\mathbb{K}$ e o par (a, δ) é um par minimal de definição para $\overline{\mu}$. Além disso,

   $$\overline{\mu}_{a,\delta}|_{\mathbb{K}(x)} = \overline{\mu}_{x-a}|_{\mathbb{K}(x)} = \mu = \mu_Q.$$

   No artigo de Alexandru, Popescu e Zaharescu (1990a, p. 291) encontra-se ainda uma caracterização do grupo de valores e do corpo de resíduos de μ. Sendo ν' a restrição de $\overline{\nu}$ para $\mathbb{K}(a)$ e $\gamma = \mu(Q)$, temos que

   $$\mathbb{K}(x)\mu = \mathbb{K}(a)\nu' \text{ e } \mu\mathbb{K}(x) = \nu'\mathbb{K}(a) \oplus \gamma\mathbb{Z}.$$

   No caso particular em que μ é trivial em $\mathbb{K}$, vimos no Teorema 1.23 que existem duas possibilidades:

(a) $\boldsymbol{\mu(x) \geq 0}$: temos que μ é equivalente a uma valorização p-ádica para algum polinômio irredutível $p \in \mathbb{K}[x]$. Isto é, $\mu \sim \mu^p$, em que

$$\mu^p(f) = \begin{cases} m \text{ se } f = p^m g \text{ com } p \nmid g \\ \infty \text{ se } f = 0. \end{cases}$$

(b) $\boldsymbol{\mu(x) < 0}$: temos que μ é equivalente a valorização μ_∞. Isto é, $\mu \sim \mu_\infty$, em que

$$\mu_\infty\left(\frac{f}{g}\right) = \begin{cases} \deg(g) - \deg(f) \text{ se } f \text{ e } g \text{ são não nulos,} \\ \infty \qquad\qquad\qquad\quad \text{se } f = 0. \end{cases}$$

2. **As valorizações resíduo-transcendentes**: são aquelas tais que a extensão $\mathbb{K}(x)\mu \mid \mathbb{K}\nu$ é transcendente. Vimos que μ resíduo-transcendente implica $\overline{\mu}$ resíduo-transcendente. No Teorema 3.20, prova-se que $\overline{\mu} = \overline{\mu}_{a,\delta}$ em que $\delta = \overline{\mu}(x-a) \in \overline{\nu}\overline{\mathbb{K}}$ é máximo do conjunto $\{\overline{\mu}(x-b) \mid b \in \overline{\mathbb{K}}\}$.

   Podemos também descrever $\overline{\mu} = \overline{\mu}_{a,\delta}$ utilizando bolas:

$$\overline{\mu}_{a,\delta}(f) = \min_{d \in D(a,\delta)} \{\overline{\nu}(f(d))\}$$

   em que $D(a,\delta) := \{d \in \overline{\mathbb{K}} \mid \overline{\nu}(d-a) \geq \delta\}$. Pelo Teorema 3.22, $\mu = \mu_Q$ para algum polinômio-chave $Q \in \mathbb{K}[x]$. Este polinômio é polinômio minimal de a sobre $\mathbb{K}$ e o par (a,δ) é um par minimal de definição para $\overline{\mu}$. Ainda,

$$\overline{\mu}_{a,\delta}|_{\mathbb{K}(x)} = \overline{\mu}_{x-a}|_{\mathbb{K}(x)} = \mu_Q = \mu.$$

   Se $Q \in \mathbb{K}[x]$ for irredutível sobre a henselização $\mathbb{K}^d(\overline{\nu})$ e $\mu(Q) \in \overline{\nu}\overline{\mathbb{K}}$, então podemos também descrever $\mu = \mu_Q$ utilizando discoides:

$$\mu_Q(g) = \mu_{\overline{D}(Q,\mu(Q))}(g) = \min_{d \in \overline{D}(Q,\mu(Q))} \{\overline{\nu}(g(d))\}.$$

   em que $\overline{D}(Q,\mu(Q)) := \{d \in \overline{\mathbb{K}} \mid \overline{\nu}(Q(d)) \geq \mu(Q)\}$. Sobre os grupos de valores de $\overline{\mu}$ e de μ e o corpo de resíduos de μ, o Teorema 3.20 e a Desigualdade de Zariski-Abhyankar nos dizem que $\overline{\mu}\overline{\mathbb{K}}(x) = \overline{\nu}\overline{\mathbb{K}}$, $\mu\mathbb{K}(x)/\nu\mathbb{K}$ é grupo de torção e $\text{tr.deg}(\mathbb{K}(x)\mu \mid \mathbb{K}\nu) = 1$.

3. **As valorizações algébricas**: essas valorizações são aquelas que não são do tipo transcendente. Isto é, $\mu\mathbb{K}(x)/\nu\mathbb{K}$ é grupo de torção e $\mathbb{K}(x)\mu \mid \mathbb{K}\nu$ é uma extensão algébrica.

Pelo Teorema 5.9, μ é o limite de $(\mu_i)_{i \in I}$ um sistema ordenado de extensões resíduo-

transcendentes de ν para $\mathbb{K}(x)$. Cada μ_i é a restrição de uma valorização da forma $\overline{\mu}_{a_i,\delta_i}$ em $\overline{\mathbb{K}}(x)$, em que $\delta_i = \overline{\mu}(x - a_i)$ e $\{\delta_i\}_{i\in I}$ é um subconjunto de $\{\overline{\mu}(x-b) \mid b \in \overline{\mathbb{K}}\}$ cofinal e bem-ordenado.

Sobre o grupo de valores, o Lema 5.7 nos garante que $\mu\mathbb{K}(x) \subseteq \overline{\nu}\overline{\mathbb{K}}$. Segundo Alexandru, Popescu e Zaharescu (1990a, p. 291), se tomarmos cada a_i com grau minimal sobre $\mathbb{K}$ obtemos

$$\mathbb{K}(x)\mu = \bigcup_{i\in I} \mathbb{K}(a_i)\nu_i \text{ e } \mu\mathbb{K}(x) = \bigcup_{i\in I} \nu_i\mathbb{K}(a_i)$$

em que $\nu_i = \overline{\nu}|_{\mathbb{K}(a_i)}$.

Decidimos terminar desta maneira nossa classificação das valorizações em $\mathbb{K}(x)$. Porém, é possível aprofundar mais os resultados acima, seja seguindo a abordagem de Alexandru, Popescu e Zaharescu (1989, 1990a, 1990b), seja indo atrás de outras abordagens. Por exemplo, os três autores citados continuam os estudos sobre valorizações resíduo-transcendentes buscando caracterizar de forma mais precisa os pares minimais que definem esse tipo de valorização. Eles mostram que para toda extensão resíduo-transcendente μ de ν para $\mathbb{K}(x)$, com $(\mathbb{K}, \nu)$ henseliano, existe um par minimal de definição (a, δ) para μ com a separável sobre $\mathbb{K}$ (1990b, p. 218). Além disso, os autores provam a existência de extensões resíduo-transcendentes com corpo de resíduos e grupo de valores predefinidos (1990b, p. 223). Resultados semelhantes a este último são alcançados também para extensões valor-transcendentes e algébricas (1990a, p. 295)

Por outro lado, Kuhlmann (2004) trata o problema de classificação das valorizações em $\mathbb{K}(x)$ com outras ferramentas. Separando as valorizações nas mesmas classes que apresentamos (valor-transcendente, resíduo-transcendente e algébrica), o autor faz uso, por exemplo, de sequências pseudo Cauchy para provar seus resultados (2004, p. 4579). Nesse trabalho Kuhlmann também trata da existência de extensões com grupo de valores e corpo de resíduos predefinidos (2004, p. 4569).

É possível ir além e buscar formas de caracterizar as extensões de uma valorização ν de $\mathbb{K}$ para $\mathbb{K}(x_1, \ldots, x_n)$. Nos trabalhos de Öke (2010, 2013), os resultados de Alexandru, Popescu e Zaharescu (1990a) são pensados de forma generalizada para o corpo $\mathbb{K}(x_1, \ldots, x_n)$. Por exemplo, Öke prova que uma extensão resíduo-transcendente de ν para $\mathbb{K}(x_1, \ldots, x_n)$, sob determinadas hipóteses, é na verdade uma extensão comum de valorizações $\mu_1, \ldots, \mu_n$ para $\mathbb{K}(x_1, \ldots, x_n)$, em que μ_j é uma extensão resíduo transcendente de ν para $\mathbb{K}(x_j)$, para $j = 1, \ldots, n$ (ÖKE, 2010, p. 250). Outro resultado interessante é que uma valorização algébrica em $\mathbb{K}(x_1, \ldots, x_n)$ é, como no Teorema 5.9, o limite de um sistema ordenado de extensões resíduo-transcendentes de ν para $\mathbb{K}(x_1, \ldots, x_n)$, sendo estas extensões resíduo-transcendentes definidas como extensões comuns de valorizações em $\mathbb{K}(x_j)$, $j = 1, \ldots, n$, como descrito anteriormente (ÖKE, 2013, p. 5).

Considerações finais

Neste, trabalho estudamos alguns objetos de destaque na Teoria das Valorizações, como por exemplo os polinômios-chaves, os truncamentos, os pares minimais e as valorizações transcendentes. Desenvolvemos desde tópicos iniciais e clássicos envolvendo tais objetos, até questões recentes de pesquisa sobre os mesmos.

Como fruto deste trabalho, o aluno responsável por esta dissertação e seu orientador escreveram um artigo (NOVACOSKI; SILVA DE SOUZA, 2022), que foi aceito para publicação no Journal of Pure and Applied Algebra e já está disponível on-line.

O aluno pretende continuar seus estudos sobre valorizações no doutorado. Uma direção possível para seus estudos será entender com profundidade os anéis graduados associados às valorizações definidas por polinômios-chaves limites.

Em suma, foi um trabalho que acrescentou muito à formação do aluno, tanto através do conhecimento específico da área em que ele pretende se aprofundar nos estudos futuros de pós-graduação, quanto através da solidificação de conceitos gerais importantes que serão ferramentas úteis também em outros contextos matemáticos.

Referências Bibliográficas

1 ALBERICH-CARRAMIÑANA, M.; GUÀRDIA, J.; NART, E.; ROÉ, J.; *Valuative trees over valued fields*, 2021. Disponível em: https://arxiv.org/abs/2107.09813. Acesso em: 29 nov. 2021.

2 ALEXANDRU V.; POPESCU N.; ZAHARESCU, A. A theorem of characterization of residual transcendental extensions of a valuation. **J. Math. Kyoto Univ.** v. 28, n. 4, pp. 579-592, 1988.

3 ALEXANDRU V.; POPESCU N.; ZAHARESCU, A. All valuations on K(x). **J. Math. Kyoto Univ.** v. 30, n. 2, pp. 281-296, 1990.

4 ALEXANDRU V.; POPESCU N.; ZAHARESCU, A. Minimal pairs of definition of a residual transcendental extension of a valuation. **J. Math. Kyoto Univ.** v. 30, n. 2, pp. 207-225, 1990.

5 BENGUS-LASNIER, A., Minimal Pairs, Truncation and Diskoids. **J. Algebra**, v. 579, pp. 388-427, 2021.

6 BORGES, H.; TENGAN, E. **Álgebra Comutativa em quatro movimentos.** Rio de Janeiro: IMPA, 2015. 490 p.

7 DEITMAR, A.; ECHTERHOFF, S. **Principles of Harmonic Analysis**, 2ª Edição. Springer International Publishing, 2014. 332 p.

8 DECAUP J.; SPIVAKOVSKY, M.; MAHBOUB, W. Abstract key polynomials and comparison theorems with the key polynomials of MacLane – Vaquie. **Illinois J. Math.**, v. 62, n. 1-4, pp. 253-270, 2018.

9 ENDLER, O. **Valuation Theory**. Nova York-Berlin: Springer-Verlag, 1972. 243 p.

10 ENGLER, A.; PRESTEL, A. **Valued Fields**. Nova York: Springer-Verlag, 2005. 205 p.

11 FRALEIGH, J. B. **A First Course in Abstract Algebra**, 7ª edição. Pearson, 2002. 590 p.

12 HÖFT, H.; HOWARD, P. Well Ordered Subsets of Linearly Ordered Sets. **Notre Dame J. Form. Log.**, v. 35, n. 3, pp. 413-425, 1994.

13 HOWARD, P.; RUBIN, J. **Consequences of the Axiom of Choice**. American Mathematical Society, 1998.

14 HUNGERFORD, T. W. **Algebra**. Nova York: Springer-Verlag, 1974. 502 p. (Graduate Texts in Mathematics 73)

15 ISAACS, I. M. **Algebra, a graduate course**, 1ª Edição. Brooks/Cole Publishing Company, 1993. 516 p.

16 KOBLITZ, N. **p-adic numbers, p-adic analysis and zeta-functions**. Nova Iorque: Springer-Verlag, 1977. 122 p.

17 KUHLMANN, F. V. Valued fields. *In*: **Valuation Theory**. Livro em preparação, 20??. Disponível em: https://math.usask.ca/∼fvk/bookch4.pdf. Acesso em: 01 dez. 2020.

18 KUHLMANN, F. V. Valued fields extensions. *In*: **Valuation Theory**. Livro em preparação, 20??. Disponível em: https://math.usask.ca/∼fvk/bookch6.pdf. Acesso em: 01 dez. 2020.

19 KUHLMANN, F. V. Ramification Theory. *In*: **Valuation Theory**. Livro em preparação, 20??. Disponível em: https://math.usask.ca/∼fvk/bookch7.pdf. Acesso em: 01 dez. 2020.

20 KUHLMANN, F. V. Preliminaries from algebra. *In*: **Valuation Theory**. Livro em preparação, 20??. Disponível em: https://math.usask.ca/∼fvk/bookch24.pdf. Acesso em: 01 dez. 2020.

21 KUHLMANN, F. V. Value groups, residue fields, and bad places of rational function fields. **Trans. Amer. Math. Soc.**, v. 356, pp. 4559-4600, 2004.

22 LEE, G. T. **Abstract Algebra**: An Introductory Course. Springer, 2018. 301 p.

23 MAC LANE, S., A construction for absolute values in polynomial rings. **Trans. Amer. Math. Soc.** v. 40, pp. 363–395, 1936

24 NOVACOSKI, J. Key polynomials and minimal pairs. **J. Algebra**, v. 523, pp. 1-14, 2019.

25 NOVACOSKI, J. A. *On the extensions of a valuation from K to K[x].* Notas de Aula. 2020.

26 NOVACOSKI, J. On MacLane-Vaquié key polynomials. **J. Pure Appl. Algebra**, v. 225, pp. 1-20, 2021.

27 NOVACOSKI, J.; BARNABÉ, M. Valuations on K[x] approaching a fixed irreducible polynomial. **J. Algebra**, v. 592, pp. 100-117, 2022

28 NOVACOSKI, J.; SILVA DE SOUZA, C. H. On truncations of valuations. **J. Pure Appl. Algebra**, v. 226, 2022. Disponível em: https://doi.org/10.1016/j.jpaa.2021.106965. Acesso em: 26 nov. 2021.

29 NOVACOSKI, J.; SPIVAKOVSKY, M. On the local uniformization problem. **Algebra, Logic and Number Theory, Banach Center Publ.** v. 108, pp. 231–238, 2016

30 NOVACOSKI, J.; SPIVAKOVSKY, M. Key polynomials and pseudo-convergent sequences. **J. Algebra**, v. 495, pp. 199-219, 2018.

31 ÖKE, F. On Residual Transcendental Extensions of a Valuation on K to K(x1,...,xn). **International Journal of ALgebra**, v. 4, n. 5, pp. 247-252, 2010.

32 ÖKE, F. On residual algebraic torsion extensions of a valuation of a field K to K(x1,...,xn). **J. Fixed Point Theory Appl.**, n. 46, pp. 1-7, 2013.

33 POPESCU, L.; POPESCU, N. Sur la definition des prolongements résiduels transcendents d'une valuation sur un corps K à K(x). **Bulletin mathématique de la Société des Sciences Mathématiques de la République Socialiste de Roumanie**, Nouvelle Série, v. 33 (81), n. 3, pp. 257-264, 1989.

34 ROND, G. About the algebraic closure of the field of power series in several variables in characteristic zero. **J. Singul.**, v. 16 pp. 1-51, 2017.

35 RÜTH, J. P. **Models of Curves and Valuations**, 2014. 117 f. Tese (Doutorado em Matemática), Ulm University, 2014.

36 **The Stacks project**. Disponível em: https://stacks.math.columbia.edu/. Acesso em: 06 mar. 2021

37 VAQUIÉ, M. Extension d'une valuation. **Trans. Amer. Math. Soc.** v. 359, n. 7, pp. 3439–3481, 2007.

38 WEINTRAUB, S. H. **Galois Theory**. Nova York: Springer, 2006. 185 p.

39 ZARISKI, O.; SAMUEL, P. **Commutative Algebra II**. Berlin: Springer-Verlag, 1960. 416 p.

Apêndice A

Apanhado geral de Teoria de Anéis e Módulos e Teoria de Galois

Neste apêndice listamos definições, resultados e exemplos envolvendo a Teoria de Anéis comutativos e Módulos, Teoria de Corpos e Teoria de Galois que foram utilizados ao longo deste texto. Não daremos provas para os resultados apresentados.

As principais referências para a composição deste apêndice foram os livros de Borges e Tengan (2015), Fraleigh (2002), Hungerford (1974), Isaacs (1993) e Weintraub (2006).

A.1 Anéis e ideais

A menos que seja especificado o contrário, trabalharemos sempre ao longo deste apêndice com **anéis comutativos com unidade**. O elemento neutro do produto será representado por 1. Se $\mathcal{A} = \{0\}$ é o anel nulo, então $1 = 0$. Caso contrário, sempre teremos $1 \neq 0$ e a unicidade de 1 em $\mathcal{A}$. Um elemento $a \in \mathcal{A}$ é dito uma **unidade** se existe $a^{-1} \in \mathcal{A}$ satisfazendo $aa^{-1} = 1$. Chamamos de $\mathcal{A}^\times$ o conjunto das unidades de $\mathcal{A}$. Um subconjunto $\mathcal{S}$ de $\mathcal{A}$ é chamado **subanel** se é um anel com a operação restrita e contém a unidade de $\mathcal{A}$.

Um **homomorfismo de anéis** é uma aplicação $\psi : \mathcal{A} \to \mathcal{B}$ do anel $\mathcal{A}$ no anel $\mathcal{B}$ satisfazendo

$$\psi(a+b) = \psi(a) + \psi(b) \text{ e } \psi(ab) = \psi(a)\psi(b)$$

para $a, b \in A$. Para nós, exigiremos que $\psi(1_\mathcal{A}) = 1_\mathcal{B}$, sendo $1_\mathcal{A}$ e $1_\mathcal{B}$ unidades de $\mathcal{A}$ e $\mathcal{B}$, respectivamente. Se o homomorfismo for injetor, então o chamamos de **monomorfismo** (ou também imersão/mergulho/inclusão). Caso o homomorfismo seja injetor e sobrejetor, então estamos lidando com um **isomorfismo** de anéis. Dizemos nesse caso que os anéis $\mathcal{A}$

e $\mathcal{B}$ são isomorfos e denotamos $\mathcal{A} \cong \mathcal{B}$. Todo homomorfismo ψ nos fornece os conjuntos

$$\ker(\psi) = \{a \in \mathcal{A} \mid \psi(a) = 0\}$$

e

$$\mathrm{im}(\psi) = \{\psi(a) \mid a \in \mathcal{A}\},$$

chamados **núcleo** e **imagem** de ψ, respectivamente. Para $\mathcal{B}'$ subanel de $\mathcal{B}$, o conjunto

$$\psi^{-1}[\mathcal{B}'] = \{a \in \mathcal{A} \mid \psi(a) \in \mathcal{B}'\}$$

é chamado **imagem inversa**. O núcleo e a imagem inversa de um subanel são subanéis de $\mathcal{A}$. A imagem é um subanel de $\mathcal{B}$. Temos que ψ é um monomorfismo se, e somente se, $\ker(\psi) = \{0\}$.

Um **ideal** $\mathfrak{a}$ de é um subconjunto de $\mathcal{A}$ que é fechado por combinações $\mathcal{A}$-lineares:

$$ax + by \in \mathfrak{a} \text{ para } a, b \in \mathcal{A} \text{ e } x, y \in \mathfrak{a}.$$

O núcleo de um homomorfismo de anéis é um ideal de domínio. Um ideal $\mathfrak{a} \subset \mathcal{A}$ é dito **próprio** quando $\mathfrak{a}$ é um subconjunto próprio de $\mathcal{A}$. Prova-se que $\mathfrak{a}$ é próprio se, e somente se, $1 \notin \mathfrak{a}$, o que é equivalente a dizermos que $\mathcal{A}^\times \cap \mathfrak{a} = \emptyset$.

Tomando um conjunto de elementos $X = \{b_\lambda\}_{\lambda \in \Lambda}$ de um anel $\mathcal{A}$, o conjunto $\{a_1 b_{\lambda_1} + \cdots + a_k b_{\lambda_k} \mid k \in \mathbb{N} \text{ e } a_i \in \mathcal{A}\}$ das combinações lineares (somas finitas) dos elementos de X é um ideal de $\mathcal{A}$, chamado **ideal gerado** por X. Tal ideal é o menor ideal que contém X. Quando X é finito, denotaremos o ideal $\mathfrak{b}$ gerado por tal conjunto por $\langle b_1, \ldots, b_n \rangle$. Caso contrário, podemos utilizar a notação $\mathfrak{b} = \langle X \rangle$. Um ideal é dito **principal** se é gerado por um único elemento.

Seja $\mathfrak{i}$ ideal de um anel $\mathcal{A}$. Definiremos a seguinte relação de equivalência:

$$a \equiv b \,(\mathrm{mod}\, \mathfrak{i}) \iff a - b \in \mathfrak{i}.$$

Denotaremos a classe de equivalência de um elemento $a \in \mathcal{A}$ por essa relação como $a + \mathfrak{i}$ ou $\bar{a}$. O conjunto das classes de equivalência será denotado $\mathcal{A}/\mathfrak{i}$. Com as operações

$$\overline{a} + \overline{b} := \overline{a + b} \text{ e } \overline{a} \cdot \overline{b} := \overline{ab},$$

temos que $\mathcal{A}/\mathfrak{i}$ é um anel, chamado **anel quociente**. Um homomorfismo associado ao anel quociente é a aplicação

$$\begin{aligned} \pi : \mathcal{A} &\longrightarrow \mathcal{A}/\mathfrak{i} \\ a &\longmapsto \overline{a}, \end{aligned}$$

um homomorfismo de anéis sobrejetor denominado **projeção**.

Sejam $\mathcal{A}$ e $\mathcal{B}$ anéis, $\mathfrak{i}$ ideal de $\mathcal{A}$ e o homomorfismo projeção $\pi : \mathcal{A} \to \mathcal{A}/\mathfrak{i}$ associado. Denotamos por $\mathrm{Hom}(\mathcal{A}, \mathcal{B})$ o conjunto de todos os homomorfismos de anéis de $\mathcal{A}$ em $\mathcal{B}$. Seja $\mathrm{Hom}_{\mathfrak{i}}(\mathcal{A}, \mathcal{B}) = \{\psi \in \mathrm{Hom}(\mathcal{A}, \mathcal{B}); \psi(\mathfrak{i}) = \{0\}\}$ o conjunto dos homomorfismos ψ tais que $\mathfrak{i} \subseteq \ker(\psi)$. A seguir, enunciamos três importantes resultados sobre homomorfismos, que podem consultados no livro de Borges e Tengan (2015, pp. 13-15).

Teorema A.1. ***(Propriedade Universal do Quociente)*** *Existe uma bijeção natural entre* $\mathrm{Hom}(\mathcal{A}/\mathfrak{i}, \mathcal{B})$ *e* $\mathrm{Hom}_{\mathfrak{i}}(\mathcal{A}, \mathcal{B})$ *dada por*

$$\begin{aligned} \mathrm{Hom}(\mathcal{A}/\mathfrak{i}, \mathcal{B}) &\xrightarrow{\approx} \mathrm{Hom}_{\mathfrak{i}}(\mathcal{A}, \mathcal{B}) \\ \psi &\longmapsto \psi \circ \pi \\ \overline{\varphi} &\longmapsfrom \varphi \end{aligned}$$

com $\overline{\varphi} : \mathcal{A}/\mathfrak{i} \longrightarrow \mathcal{B}$ *definida por* $\overline{\varphi}(\overline{a}) = \varphi(a)$.

■

Teorema A.2. ***(Teorema do Isomorfismo)*** *Sendo* $\psi : \mathcal{A} \longrightarrow \mathcal{B}$ *um homomorfismo de anéis, este induz um isomorfismo*

$$\begin{aligned} \overline{\psi} : \frac{\mathcal{A}}{\ker(\psi)} &\xrightarrow{\approx} \mathrm{im}(\psi) \\ \overline{a} &\longmapsto \psi(a) \end{aligned}$$

■

Teorema A.3. ***(Teorema da Correspondência)*** *Sendo* $\mathcal{A}$ *um anel e* $\mathfrak{i}$ *ideal, temos a seguinte correspondência:*

$$\begin{aligned} \{ \textit{ ideais } \mathfrak{j} \subseteq \mathcal{A} \textit{ tais que } \mathfrak{i} \subseteq \mathfrak{j}\} &\xrightarrow{\approx} \{ \textit{ ideais } \mathfrak{h} \subseteq \mathcal{A}/\mathfrak{i}\} \\ \mathfrak{j} &\longmapsto \pi(\mathfrak{j}) \\ \pi^{-1}[\mathfrak{h}] &\longmapsfrom \mathfrak{h} \end{aligned}$$

■

Um ideal $\mathfrak{p}$ próprio do anel $\mathcal{A}$ é dito **ideal primo** se satisfaz uma das duas condições equivalentes a seguir.

1. Dados $a, b \in \mathcal{A}$, se $ab \in \mathfrak{p}$, então $a \in \mathfrak{p}$ ou $b \in \mathfrak{p}$.
2. Dados $\mathfrak{a}$ e $\mathfrak{b}$ ideais de $\mathcal{A}$, se $\mathfrak{ab} \subseteq \mathfrak{p}$, então $\mathfrak{a} \subseteq \mathfrak{p}$ ou $\mathfrak{b} \subseteq \mathfrak{p}$.

Um elemento $p \in \mathcal{A} \setminus (\mathcal{A}^{\times} \cup \{0\})$ é dito **primo** se o ideal principal (p) é primo.

Seja $\mathcal{A}$ um anel e $\mathfrak{a}$ um ideal próprio de $\mathcal{A}$. O ideal $\mathfrak{a}$ é dito **ideal maximal** se, dado um ideal $\mathfrak{b}$, temos que $\mathfrak{a} \subset \mathfrak{b}$ implica $\mathfrak{a} = \mathfrak{b}$ ou $\mathfrak{b} = \mathcal{A}$.

Se a e b são dois elementos não nulos do anel tais que $ab = 0$, então ambos são denominados **divisores de zero**. Um anel não nulo $\mathcal{D}$ é dito um **domínio de integridade** (ou simplesmente um domínio) se não possui divisores de zero. Ou seja, para todo $a, b \in \mathcal{D}$ vale que $ab = 0$ implica $a = 0$ ou $b = 0$. Em um domínio $\mathcal{D}$, dizemos que a **divide** b, denotado $a \mid b$, se existe $c \in \mathcal{D}$ tal que $b = ca$. Um elemento $p \in \mathcal{D} \setminus (\mathcal{D}^\times \cup \{0\})$ é dito **irredutível** se $p = ab$ implica $a \in \mathcal{D}^\times$ ou $b \in \mathcal{D}^\times$. Em um domínio, p primo implica p irredutível. Dizemos que $\mathcal{D}$ é um **domínio de fatoração única** se, para qualquer $d \neq 0$, este pode ser escrito como um produto de irredutíveis de forma única, a menos de ordem dos fatores e produto por unidades. Em um domínio de fatoração única, os conceitos de elemento primo e irredutível são equivalentes.

Um anel $\mathbb{K}$ é dito **corpo** se todo elemento não nulo é uma unidade. Ou seja, $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$. As afirmações a seguir estão demonstradas no livro de Borges e Tengan (2015, p. 16 e p. 97).

Proposição A.4. *Sejam $\mathcal{A}$ um anel e $\mathfrak{p}, \mathfrak{m} \subset \mathcal{A}$ ideais. Temos as seguintes propriedades.*

1. *$\mathfrak{p}$ é próprio se, e somente se, $\mathfrak{p}$ está contido em algum ideal maximal $\mathfrak{m}$.*

2. *$u \in \mathcal{A}$ é uma unidade se, e somente se, u não pertence a nenhum ideal maximal.*

3. *$\mathcal{A}$ é corpo se, e somente se, possui apenas (0) como ideal próprio.*

4. *$\mathfrak{m} \subset \mathcal{A}$ é maximal se, e somente se, $\mathcal{A}/\mathfrak{m}$ é um corpo.*

5. *$\mathfrak{p} \subset \mathcal{A}$ é primo se, e somente se, $\mathcal{A}/\mathfrak{p}$ é um domínio.*

■

Dados $\mathfrak{a}$ e $\mathfrak{b}$ ideais de $\mathcal{A}$, definimos a soma $\mathfrak{a} + \mathfrak{b}$ como sendo

$$\mathfrak{a} + \mathfrak{b} := \{a + b \mid a \in \mathfrak{a} \text{ e } b \in \mathfrak{b}\}.$$

O produto $\mathfrak{a} \cdot \mathfrak{b}$ é definido como sendo

$$\mathfrak{a} \cdot \mathfrak{b} := \{a_1 b_1 + \ldots + a_r b_r \mid r \in \mathbb{N}, a_1, \ldots, a_r \in \mathfrak{a} \text{ e } b_1, \ldots, b_r \in \mathfrak{b}\}.$$

Dois ideais $\mathfrak{a}$ e $\mathfrak{b}$ são ditos **coprimos** se $\mathfrak{a} + \mathfrak{b} = \mathcal{A}$. O teorema a seguir está demonstrado no livro de Borges e Tengan (2015, p. 19).

Teorema A.5. ***(Teorema Chinês dos Restos)*** *Sejam $\mathcal{A}$ um anel e $\mathfrak{i}_k$, $1 \leq k \leq n$, ideais dois a dois coprimos. Então*

1. $\mathfrak{i}_1 \cap \mathfrak{i}_2 \cap \cdots \cap \mathfrak{i}_n = \mathfrak{i}_1 \cdot \mathfrak{i}_2 \cdot \ldots \cdot \mathfrak{i}_n$
2. *A aplicação*

$$\begin{aligned} \frac{\mathcal{A}}{\mathfrak{i}_1 \cdot \ldots \cdot \mathfrak{i}_n} = \frac{\mathcal{A}}{\mathfrak{i}_1 \cap \cdots \cap \mathfrak{i}_n} &\xrightarrow{\approx} \frac{\mathcal{A}}{\mathfrak{i}_1} \times \cdots \times \frac{\mathcal{A}}{\mathfrak{i}_n} \\ a \mod (\mathfrak{i}_1 \cap \cdots \cap \mathfrak{i}_n) &\longmapsto (a \mod \mathfrak{i}_1, \ldots, a \mod \mathfrak{i}_n) \end{aligned}$$

é um isomorfismo. ■

A.2 Módulos

Definição A.6. *Seja $\mathcal{A}$ um anel qualquer (não necessariamente comutativo). Um* ***$\mathcal{A}$-módulo*** *M à esquerda é um grupo abeliano $\langle M, + \rangle$ junto com uma função $\alpha : \mathcal{A} \times M \to M$, chamada uma $\mathcal{A}$-ação em M e denotada $\alpha(a, m) = am$, satisfazendo, para $a, b \in \mathcal{A}$ e $m, n \in M$,*

- $(a + b)m = am + bm$;
- $a(m + n) = am + an$;
- $a(bm) = (ab)m$;
- *Se $\mathcal{A}$ possui unidade, $1m = m$. Nesse caso, o $\mathcal{A}$-módulo M é dito unitário.*

■

De forma análoga definimos um $\mathcal{A}$-módulo M à direita. Quando $\mathcal{A}$ é comutativo, definindo $\alpha_d : M \times \mathcal{A} \to M$ por $\alpha_d(m, a) := \alpha_e(a, m)$ (a $\mathcal{A}$-ação em M do módulo à esquerda), vemos que

- $\alpha_d(m, a + b) := \alpha_e(a + b, m) = \alpha_e(a, m) + \alpha_e(b, m) := \alpha_d(m, a) + \alpha_d(m, b)$;
- $\alpha_d(m + n, a) := \alpha_e(a, m + n) = \alpha_e(a, m) + \alpha_e(a, n) := \alpha_d(m, a) + \alpha_e(n, a)$;
- $\alpha_d(\alpha_d(m, b), a) := \alpha_e(a, \alpha_e(b, m)) = \alpha_e(ab, m) = \alpha_e(ba, m) := \alpha_d(m, ba)$.

Logo, para $\mathcal{A}$ comutativo, um $\mathcal{A}$-módulo M é tanto módulo à esquerda quanto à direita e podemos dizer que $am = ma$.

Muitas das definições e resultados da Teoria de Grupos e Anéis ganham análogos quando tratamos sobre módulos. Por exemplo, definimos um **$\mathcal{A}$-submódulo** de M como sendo um

subgrupo N de M tal que se $n \in N$ e $a \in \mathcal{A}$, então $an \in N$. Se M e N são $\mathcal{A}$-módulos, um **homomorfismo de $\mathcal{A}$-módulos** é uma aplicação ψ que, para todo $a_1, a_2 \in \mathcal{A}$ e $m_1, m_2 \in M$, satisfaz

$$\psi(a_1 m1 + a_2 m_2) = a_1\psi(m_1) + a_2\psi(m_2).$$

Aqui também ψ é injetor se, e somente se, $\ker(\psi) := \psi^{-1}(0) = \langle 0 \rangle$.

Para N um $\mathcal{A}$-submódulo de M, com a relação de equivalência

$$a \equiv b \, (mod\, N) \iff a - b \in N$$

definimos o **$\mathcal{A}$-módulo quociente** M/N, sendo a $\mathcal{A}$-ação dada por $a\overline{m} := \overline{am}$, $a \in \mathcal{A}$, $m \in M$. É importante notar que tal quociente é bem definido pois, visto como grupo quociente, N é normal uma vez que M é abeliano. Temos então o **homomorfismo projeção** $\pi : M \to M/N, \pi(a) = \overline{a}$, homomorfismo de $\mathcal{A}$-módulos sobrejetor com $\ker(\pi) = N$. O Teorema do Isomorfismo e o Teorema da correspondência valem nesse contexto e as demonstrações seguem o mesmo raciocínio.

Exemplo A.7. *Quando trabalhamos com um corpo $\mathbb{K}$, um $\mathbb{K}$-módulo unitário M é chamado um **espaço vetorial** sobre $\mathbb{K}$.*

▼

Exemplo A.8. *Todo grupo abeliano $\langle G, + \rangle$ é um $\mathbb{Z}$-módulo, com $ng = \overbrace{g + \ldots + g}^{n \text{ vezes}}$ para $n \neq 0$ e $0g = 0$ Um homomorfismo de grupos é, neste contexto, um homomorfismo de $\mathbb{Z}$-módulos.*

▼

Exemplo A.9. *Todo anel $\mathcal{A}$ é um $\mathcal{A}$-módulo sobre si mesmo. Para um ideal $\mathfrak{i} \subseteq \mathcal{A}$, o anel quociente $\mathcal{A}/\mathfrak{i}$ é um $\mathcal{A}$-módulo, em que $\alpha(a, \overline{m}) = \pi(a)\overline{m}$. A projeção $\pi : \mathcal{A} \to \mathcal{A}/\mathfrak{i}$ é um homomorfismo de $\mathcal{A}$-módulos.*

▼

Exemplo A.10. *Dada uma família de $\mathcal{A}$-módulos $\{M_i\}_{i \in I}$, consideramos o conjunto*

$$\prod_{i \in I} M_i = \left\{ f : I \to \bigcup_{i \in I} M_i \mid f(i) \in M_i \text{ para todo } i \in I \right\}.$$

Identificamos $f := (m_i)_{i \in I}$, em que $m_i = f(i)$ para todo $i \in I$, e definimos a soma

$$(m_i)_{i \in I} + (n_i)_{i \in I} := (m_i + n_i)$$

e o produto por escalar

$$\alpha(a, (m_i)_{i \in I}) = (am_i)_{i \in I} \text{ para todo } a \in \mathcal{A}.$$

Então $\prod_{i\in I} M_i$ é um $\mathcal{A}$-módulo, chamado ***produto direto****. Consideramos agora o subconjunto do produto direto*

$$\bigoplus_{i\in I} M_i = \left\{ (m_i)_{i\in I} \in \prod_{i\in I} M_i \mid m_i \neq 0 \text{ apenas para uma quantidade finita de índices } i \right\}.$$

Com as operações restritas de $\prod_{i\in I}$, temos que $\bigoplus_{i\in I}$ é um $\mathcal{A}$-submódulo de $\prod_{i\in I}$, chamado ***soma direta****.*

▼

Seja M um $\mathcal{A}$-módulo. Se existe um conjunto $\{\omega_\lambda\}_{\lambda\in\Lambda}$ tal que todo elemento de M se escreve como combinação $\mathcal{A}$-linear finita dos elementos ω_λ, então $\{\omega_\lambda\}_{\lambda\in\Lambda}$ é um conjunto de geradores de M. Caso o conjunto de geradores seja finito, M é então dito **finitamente gerado**. Generalizando o conceito de independência linear da Álgebra Linear, uma quantidade finita de elementos $\omega_1, \ldots, \omega_n \in M$ são **linearmente independentes** sobre A se a equação $a_1\omega_1 + \ldots + a_n\omega_n = 0$, com $a_i \in \mathcal{A}$, tem $a_1 = a_2 = \ldots = a_n = 0$ como única solução. Seja agora $\{\omega_i\}_{i\in I} \subset M$ uma coleção qualquer de elementos, com I um conjunto de índices qualquer. A coleção $\{\omega_i\}_{i\in I}$ é dita **linearmente independente** sobre A se, para qualquer subconjunto finito $I' \subseteq I$ e qualquer subconjunto $\{\omega_i\}_{i\in I'} \subset \{\omega_i\}_{i\in I}$,temos que $\{\omega_i\}_{i\in I'}$ é linearmente independente. Se M admite um conjunto de geradores linearmente independentes, este é uma **base** para M e, nessa situação, dizemos que M é um **módulo livre**.

Exemplo A.11. *Nem todo módulo é livre. Se tomarmos $\mathcal{A} = \mathbb{Z}$ e $M = \mathbb{Z}/\langle n\rangle \cong \mathbb{Z}_n$ o conjunto $\{\overline{1}\}$ é um conjunto de geradores. Porém, na equação $a\overline{1} = \overline{0}$ podemos tomar qualquer $a \equiv 0\,(mod\, n)$ como solução e, portanto, há soluções não triviais.*

▼

Como nos espaços vetoriais, os módulos livres possuem como invariante a cardinalidade de suas bases, conforme a proposição a seguir enuncia (ver o livro de Borges e Tengan (2015, p. 28) para uma prova deste fato).

Proposição A.12. *Sejam $\mathcal{A}$ anel não nulo e um M um $\mathcal{A}$-módulo livre finitamente gerado. Então as bases de M possuem a mesma cardinalidade.*

■

A.3 Produto tensorial

Sejam M e N dois $\mathcal{A}$-módulos. Consideremos o $\mathcal{A}$-módulo livre

$$\bigoplus_{(m,n)\in M\times N} \mathcal{A}e_{m,n}$$

gerado pela base $\{e_{m,n} \mid (m,n) \in M \times N\}$. Seja R o submódulo gerado pelos elementos da forma

$$e_{am,n} - ae_{m,n}, \quad e_{m,an} - ae_{m,n},$$

$$e_{m_1+m_2,n} - e_{m_1,n} - e_{m_2,n},$$

$$e_{m,n_1+n_2} - e_{m,n_1} - e_{m,n_2},$$

com $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ e $a \in \mathcal{A}$.

Definição A.13. *O módulo quociente*

$$M \otimes_{\mathcal{A}} N := \frac{\bigoplus_{(m,n)\in M\times N} \mathcal{A}e_{m,n}}{R},$$

é chamado ***produto tensorial*** *de M e N sobre $\mathcal{A}$.* ■

A imagem de cada $e_{m,n}$ em $M \otimes_{\mathcal{A}} N$ será denotada por $m \otimes n$ e denominaremos **tensor elementar**. Os tensores elementares geram $M \otimes_{\mathcal{A}} N$ e satisfazem

$$(am) \otimes n = a(m \otimes n) = m \otimes (an),$$

$$(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n \text{ e}$$

$$m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2.$$

Dessa forma, a aplicação

$$\otimes : M \times N \to M \otimes_{\mathcal{A}} N$$

$$(m,n) \longmapsto m \otimes n$$

é bilinear. Uma observação importante é que para definir um homomorfismo saindo de $M \otimes_{\mathcal{A}} N$ basta defini-lo nos tensores elementares, pois todo elemento do produto tensorial é uma soma finita desses tensores elementares.

O produto tensorial $M \otimes_{\mathcal{A}} N$ possui a seguinte propriedade, que motiva sua construção: para qualquer $\mathcal{A}$-módulo T, se ϕ é uma aplicação bilinear de $M \times N$ em T, então existe um único homomorfismo de $\mathcal{A}$-módulos $f : M \otimes_{\mathcal{A}} N \to T$ que faz o diagrama abaixo comutar:

$$\begin{array}{ccc} M \times N & \xrightarrow{\phi} & T \\ \downarrow{\scriptstyle \otimes} & \nearrow_{f} & \\ M \otimes_{\mathcal{A}} N & & \end{array} .$$

De fato, ϕ induz a seguinte função

$$f' : \bigoplus_{(m,n)\in M\times N} \mathcal{A}e_{m,n} \longrightarrow T$$
$$\sum_i a_i e_{m_i,n_i} \longmapsto \sum_i a_i\phi(m_i,n_i).$$

Por ϕ ser bilinear, $R \subseteq \ker(f')$. Pela Propriedade Universal do Quociente, f' nos dá uma aplicação

$$f : M \otimes_{\mathcal{A}} N \longrightarrow T$$
$$\sum_i a_i m_i \otimes n_i \longmapsto \sum_i a_i\phi(m_i,n_i)$$

que satisfaz $f \circ \otimes = \phi$. Se g é outro homomorfismo de $M \otimes_{\mathcal{A}} N$ em T satisfazendo $g \circ \otimes = \phi$, então, nos tensores elementares, $g(m \otimes n) = \phi(m,n) = f(m \otimes n)$. Logo, $g = f$.

Observação A.14. *Quando $\mathcal{A} = \mathbb{Z}$, escreveremos apenas $M \otimes N$.*

▼

A.4 Anéis e Álgebras graduadas

Definição A.15. *Seja $(G,+)$ um monoide comutativo. Um anel $\mathcal{A}$ é dito G-**graduado** se seu grupo aditivo $(\mathcal{A},+)$ admite uma decomposição como soma direta de subgrupos abelianos A_g de modo que*

$$\mathcal{A} = \bigoplus_{g\in G} A_g$$

e, para todo $g,h \in G$ vale: se $a_g \in A_g$ e $a_h \in A_h$, então $a_g a_h \in A_{g+h}$.

■

Os elementos $a_g \in \mathcal{A}_g \subseteq \mathcal{A}$ são ditos **homogêneos de grau** g. Todo elemento em $\mathcal{A}$ pode ser unicamente escrito como uma soma de elementos homogêneos a_g, com $g \in G$. Um homomorfismo $\phi : \mathcal{A} \to \mathcal{B}$ entre dois anéis G-graduados é um **homomorfismo homogêneo** se $\phi(A_g) \subseteq B_g$ para todo $g \in G$.

Definição A.16. *Seja $\mathcal{A}$ um anel. Uma $\mathcal{A}$-**álgebra** $\mathcal{R}$ (ou uma álgebra sobre $\mathcal{A}$) é um anel $\mathcal{R}$ tal que $(\mathcal{R},+)$ é um $\mathcal{A}$-módulo unitário e $a(rs) = (ar)s = r(as)$ para todo $a \in \mathcal{A}$ e $r,s \in \mathcal{R}$.*

■

Uma subálgebra de uma $\mathcal{A}$-álgebra $\mathcal{R}$ é um subanel de $\mathcal{R}$ que é também um $\mathcal{A}$-submódulo de $\mathcal{R}$. Um homomorfismo de $\mathcal{A}$-álgebras $\psi : \mathcal{R} \to \mathcal{S}$ é um homomorfismo de anéis que é também um homomorfismo de $\mathcal{A}$-módulos.

Exemplo A.17. *O anel de polinômios $\mathcal{A}[x_1, \ldots, x_n]$ é uma $\mathcal{A}$-álgebra.*

▼

Exemplo A.18. *Sejam $\mathcal{A}$ e $\mathcal{B}$ dois anéis e $\phi : \mathcal{A} \to \mathcal{B}$ um homomorfismo de anéis. Temos que $\mathcal{B}$ é uma $\mathcal{A}$-álgebra pois $(\mathcal{B}, +)$ é um $\mathcal{A}$-módulo com $\mathcal{A}$-ação $\alpha : \mathcal{A} \times \mathcal{B} \to \mathcal{B}$ dada por $\alpha(a, b) = \phi(a)b$ e o produto em $\mathcal{B}$ é associativo.*

▼

Definição A.19. *Seja $(G, +)$ um monóide comutativo. Um anel $\mathcal{R}$ é dito uma* ***$\mathcal{A}$-álgebra G-graduada*** *se $\mathcal{R}$ é uma $\mathcal{A}$-álgebra e seu grupo aditivo $(\mathcal{R}, +)$ admite uma decomposição como soma direta de subgrupos abelianos $\mathcal{R}_g$ de modo que*

$$\mathcal{R} = \bigoplus_{g \in G} \mathcal{R}_g$$

como $\mathcal{A}$-módulos e, para todo $g, h \in G$ vale: se $r_g \in \mathcal{R}_g$ e $r_h \in \mathcal{R}_h$, então $r_g r_h \in \mathcal{R}_{g+h}$.

■

Exemplo A.20. *O anel de polinômios $\mathcal{A}[x_1, \ldots, x_n]$ é uma $\mathcal{A}$-álgebra G-graduada, em que $(G, +) = (\mathbb{N}_0, +)$, pois*

$$\mathcal{A}[x_1, \ldots, x_n] = \bigoplus_{d \geq 0} \mathcal{A}[x_1, \ldots, x_n]_d,$$

sendo $\mathcal{A}[x_1, \ldots, x_n]_d$ o $\mathcal{A}$-módulo livre cuja base é composta pelos monômios $x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n}$ de grau $d = e_1 + e_2 + \ldots + e_n$.

▼

A.5 Localização

Definição A.21. *Seja $\mathcal{A}$ um anel. Um* ***conjunto multiplicativo*** *$S \subset \mathcal{A}$ é um subconjunto tal que $1 \in S$ e, para todos $s, t \in S$, vale $st \in S$.*

■

Definição A.22. *Seja $S \subset \mathcal{A}$ um conjunto multiplicativo. Consideremos o conjunto*

$$S^{-1}\mathcal{A} = (\mathcal{A} \times S)/\sim,$$

em que $\sim$ é a relação de equivalência dada por $(a_1, s_1) \sim (a_2, s_2)$ se, e somente se, existe $t \in S$ tal que $t(a_1 s_2 - a_2 s_1) = 0$ em $\mathcal{A}$. Sendo $\frac{a}{s} := \overline{(a, s)}$, a classe de (a, s), munimos $S^{-1}\mathcal{A}$ das operações

$$\frac{a_1}{s_1} + \frac{a_2}{s_2} := \frac{a_1 s_2 + a_2 s_1}{s_1 s_2} \quad e \quad \frac{a_1}{s_1} \cdot \frac{a_2}{s_2} := \frac{a_1 a_2}{s_1 s_2}.$$

Com estas operações $S^{-1}\mathcal{A}$ é um anel, chamado ***localização*** *do anel $\mathcal{A}$ com relação a S.*

■

A localização $S^{-1}\mathcal{A}$ nos fornece uma aplicação $\rho : \mathcal{A} \to S^{-1}\mathcal{A}$ dado por $\rho(a) = a/1$, chamada **localização**. Uma forma de interpretarmos $S^{-1}\mathcal{A}$ é como o maior anel em que todos os elementos de S se tornam unidades (BORGES; TENGAN, 2015).

De forma análoga, podemos localizar um $\mathcal{A}$-módulo M com relação a um conjunto multiplicativo S de $\mathcal{A}$, que será o $S^{-1}\mathcal{A}$-módulo $S^{-1}M = (M \times S)/\sim$, em que $\sim$ e as operações são definidas como acima.

Exemplo A.23. *Seja $\mathfrak{p}$ um ideal primo de $\mathcal{A}$. Considerando $S = A \setminus \mathfrak{p}$, por $\mathfrak{p}$ ser primo, S é um conjunto multiplicativo de $\mathcal{A}$. Denotamos por $\mathcal{A}_\mathfrak{p}$ a localização $S^{-1}\mathcal{A}$.*

▼

Exemplo A.24. *Se $\phi : M \to N$ é um homomorfismo de $\mathcal{A}$-módulos, temos um homomorfismo induzido de $S^{-1}\mathcal{A}$-módulos*

$$\begin{aligned} S^{-1}\phi : S^{-1}M &\longrightarrow S^{-1}N \\ \frac{m}{s} &\longmapsto \frac{\phi(m)}{s}. \end{aligned}$$

▼

Teorema A.25. *Seja S um conjunto multiplicativo de $\mathcal{A}$, S e $M \xrightarrow{\phi} N \xrightarrow{\psi} P$ uma sequência exata de $\mathcal{A}$-módulos, isto é,* $\mathrm{im}(\phi) = \ker(\psi)$. *Então*

$$S^{-1}M \xrightarrow{S^{-1}\phi} S^{-1}N \xrightarrow{S^{-1}\psi} S^{-1}P$$

é uma sequência exata de $S^{-1}\mathcal{A}$-módulos. ■

A demonstração do teorema acima e do corolário abaixo podem ser encontradas no livro de Borges e Tengan (2015, p. 123).

Corolário A.26. *Sejam $\mathcal{A}$ um anel, S um conjunto multiplicativo e um homomorfismo de $\mathcal{A}$-módulos $\phi : M \to N$. Temos as seguintes propriedades.*

1. $\ker(S^{-1}\phi) \cong S^{-1}\ker(\phi)$ *e* $\mathrm{im}(S^{-1}\phi) \cong S^{-1}\mathrm{im}(\phi)$.

2. *Se ϕ é injetor (respectivamente sobrejetor, bijetor), então o mesmo vale para $S^{-1}\phi$.*

3. *Se M é um submódulo de N, então $S^{-1}(N/M) \cong S^{-1}N/S^{-1}M$.*

■

Exemplo A.27. *Seja $\mathcal{A}_\mathfrak{p}$ a localização de $\mathcal{A}$ com relação ao conjunto multiplicativo $S = \mathcal{A} \setminus \mathfrak{p}$, para um ideal primo $\mathfrak{p}$ de $\mathcal{A}$. Qualquer outro ideal próprio de $\mathcal{A}$ que não está contido em $\mathfrak{p}$ deixa de ser próprio em $\mathcal{A}_\mathfrak{p}$ pois seus elementos se tornam unidades em $\mathcal{A}_\mathfrak{p}$. Dessa forma $\mathcal{A}_\mathfrak{p}$ possui um único ideal maximal $S^{-1}\mathfrak{p}$, denotado também por $\mathfrak{p}\mathcal{A}_\mathfrak{p}$. Temos*

$$\begin{aligned}\frac{\mathcal{A}_\mathfrak{p}}{\mathfrak{p}\mathcal{A}_\mathfrak{p}} = \frac{S^{-1}\mathcal{A}}{S^{-1}\mathfrak{p}} &\cong S^{-1}\left(\frac{\mathcal{A}}{\mathfrak{p}}\right) \\ &= \left\{\frac{\overline{a}}{\overline{b}} \mid \overline{a}, \overline{b} \in \frac{\mathcal{A}}{\mathfrak{p}} \text{ e } \overline{b} \notin \pi(\mathfrak{p})\right\} \\ &= \left\{\frac{\overline{a}}{\overline{b}} \mid \overline{a}, \overline{b} \in \frac{\mathcal{A}}{\mathfrak{p}} \text{ e } \overline{b} \neq \overline{0}\right\} \\ &= \operatorname{Frac}\left(\frac{\mathcal{A}}{\mathfrak{p}}\right).\end{aligned}$$

▼

A.6 Extensões de Corpos

Para um anel $\mathcal{A}$, denotaremos por $\mathcal{A}[x]$ o **anel de polinômios** na indeterminada x (veja o livro de Hungerford (1974, p. 149) para uma apresentação formal desse anel). Um elemento genérico de $\mathcal{A}[x]$ será denotado por

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

em que $a_i \in \mathcal{A}$ para cada i, $1 \leq i \leq n$. Os elementos a_i são chamados coeficientes de $p(x)$. Para um polinômio não nulo ($a_i \neq 0$ para algum i, $0 \leq i \leq n$), o menor n tal que $a_n \neq 0$ e $a_j = 0$ para todo $j \geq n$ é chamado **grau** do polinômio $p(x)$ e o denotaremos por $\deg(p(x))$. Convencionamos que $\deg(0) = -\infty$. O polinômio $p(x)$ será dito **mônico** quando $a_n = 1$.

Teorema A.28. *Sejam $p(x)$ e $t(x)$ polinômios de $\mathbb{K}[x]$, ambos não nulos e com $\deg(t(x)) > 0$. Então existem únicos $q(x), r(x) \in \mathbb{K}[x]$ tais que $p(x) = t(x)q(x) + r(x)$, com $r(x) = 0$ ou $\deg(r(x)) < \deg(t(x))$.* ■

Teorema A.29. *O anel $\mathbb{K}[x]$ é domínio de ideais principais (isto é, todos os seus ideais são principais).*

■

Tomando um elemento $\alpha \in \mathcal{A}$, temos um homomorfismo $\psi_\alpha : \mathcal{A}[x] \to \mathcal{A}$ sobrejetor definido por $\psi_\alpha(p(x)) = p(\alpha) := a_n\alpha^n + \ldots + a_1\alpha + a_0$ se $\alpha \in \mathcal{A}$. Tal homomorfismo será chamado **homomorfismo avaliação**.

Se $\alpha \in \mathcal{A}$ é tal que $p(\alpha) = a_n\alpha^n + \ldots + a_1\alpha + a_0 = 0$, então chamaremos α de **raiz** ou **zero** de $p(x)$. Uma aplicação imediata do algoritmo da divisão e do conceito de raiz é que α é um

zero de $p(x) \in \mathbb{K}[x]$ se, e somente se, $p(x) = (x - \alpha)q(x)$, com $q(x) \in \mathbb{K}[x]$.

Definição A.30. *O corpo $\mathbb{L}$ é uma **extensão** de um corpo $\mathbb{K}$ se $\mathbb{K}$ é subcorpo de $\mathbb{L}$, isto é, $\mathbb{K} \subseteq \mathbb{L}$ é um subanel de $\mathbb{L}$ que é também um corpo. Denotaremos por $\mathbb{L} \mid \mathbb{K}$.*

■

Sendo $X \subset \mathbb{L}$ um subconjunto e $\mathbb{K} \subset \mathbb{L}$ um subcorpo, podemos tomar a interseção de todos os subcorpos de $\mathbb{L}$ que contém $X \cup \mathbb{K}$ e isso resultará em um corpo (HUNGERFORD, 1974, p. 232). Se $X = \{\alpha_1, \ldots, \alpha_n\}$, então escrevemos $\mathbb{K}(\alpha_1, \ldots, \alpha_n)$. O processo de criar extensões como $\mathbb{K}(\alpha_1, \ldots, \alpha_n)$ é chamado de **adjunção de elementos**. A extensão $\mathbb{K}(\alpha)$ criada pela adjunção de um elemento é dita **extensão simples**. Intuitivamente, $\mathbb{K}(\alpha_1, \alpha_2)$ pode ser visto como o menor corpo que contém $\mathbb{K}, \alpha_1$ e α_2. Dessa forma, tal corpo é também identificado como $(\mathbb{K}(\alpha_1))(\alpha_2)$, isto é, a extensão simples de $\mathbb{K}(\alpha_1)$ por α_2. Indutivamente, $\mathbb{K}(\alpha_1, \ldots, \alpha_n) = (\mathbb{K}(\alpha_1, \ldots, \alpha_{n-1}))(\alpha_n)$.

Definição A.31. *Sejam $\mathbb{L}$ extensão do corpo $\mathbb{K}$ e $\alpha \in \mathbb{L}$. Se existir $f(x) \in \mathbb{K}[x]$ tal que $f(\alpha) = 0$, então α é **algébrico** sobre $\mathbb{K}$. Caso contrário, α é dito **transcendente** sobre $\mathbb{K}$. o corpo $\mathbb{L}$ é uma **extensão algébrica** de $\mathbb{K}$ se todos os elementos de $\mathbb{L}$ são algébricos sobre $\mathbb{K}$.*

■

Os resultados e definições a seguir podem ser consultados no livro de Fraleigh (2003, pp. 269-285).

Proposição A.32. *Seja $\alpha \in \mathbb{L}$ elemento algébrico em $\mathbb{K}$. Existe um único polinômio mônico irredutível $m_\alpha(x) \in \mathbb{K}[x]$ com α como raiz. Tal polinômio satisfaz: se $f(x) \in \mathbb{K}[x]$ se anula também em α, então $m_\alpha(x)$ divide $f(x)$.*

■

Definição A.33. *Chamamos o polinômio $m_\alpha(x)$ de **polinômio minimal** de α sobre $\mathbb{K}$. Dizemos que o grau de $m_\alpha(x)$ é o grau de α sobre $\mathbb{K}$.*

■

Teorema A.34. *Sejam $m_\alpha(x) \in \mathbb{K}[x]$ o polinômio minimal de α de grau n e $\mathbb{K}(\alpha) = \text{im}(\psi_\alpha)$ a extensão simples de $\mathbb{K}$. Então o conjunto $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ forma uma base para $\mathbb{K}(\alpha)$ como espaço vetorial sobre $\mathbb{K}$ e*

$$\mathbb{K}(\alpha) = \{a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 \mid a_i \in \mathbb{K}\}.$$

■

Proposição A.35. *Sejam $\alpha \in \mathbb{L}$ algébrico em $\mathbb{K}$, $\mathbb{K}(\alpha)$ a extensão simples de $\mathbb{K}$ por α e $m_\alpha(x) \in \mathbb{K}[x]$ polinômio minimal de α. Temos*

$$\frac{\mathbb{K}[x]}{\langle m_\alpha(x)\rangle} \cong \mathbb{K}(\alpha).$$

■

Definição A.36. *O grau da extensão $\mathbb{L}$ do corpo $\mathbb{K}$ é a dimensão de $\mathbb{L}$ como espaço vetorial sobre $\mathbb{K}$, denotada por $[\mathbb{L} : \mathbb{K}]$. A extensão é dita finita quando $[\mathbb{L} : \mathbb{K}] < \infty$.*

■

Corolário A.37. *Temos as seguintes propriedades.*

- *Seja $\mathbb{L} \mid \mathbb{K}$ uma extensão de corpos. Um elemento $\alpha \in \mathbb{L}$ é algébrico sobre $\mathbb{K}$ se, e somente se, $\mathbb{K}(\alpha)$ é uma extensão finita de $\mathbb{K}$. Nesse caso, $[\mathbb{K}(\alpha) : \mathbb{K}] = \deg(m_\alpha(x))$.*
- *Toda extensão finita é algébrica.*
- *Se $\mathbb{E} \mid \mathbb{L}$ e $\mathbb{L} \mid \mathbb{K}$ são extensões algébricas, então $\mathbb{E} \mid \mathbb{K}$ é também algébrica.*

■

Teorema A.38. ***(Teorema da Torre)*** *Sejam $\mathbb{L} \mid \mathbb{K}$ e $\mathbb{F} \mid \mathbb{L}$ extensões finitas de corpos. Então $\mathbb{F}$ é extensão finita de $\mathbb{K}$ e $[\mathbb{F} : \mathbb{L}][\mathbb{L} : \mathbb{K}] = [\mathbb{F} : \mathbb{K}]$.*

■

A.7 Extensões transcendentes

Seja $\mathbb{K}[x_1, \ldots, x_n]$ o anel de polinômios em n indeterminadas (veja o livro de Hungerford (1974, p. 151) para uma apresentação formal desse anel).

Definição A.39. *Seja $\mathbb{L} \mid \mathbb{K}$ uma extensão de corpos. Dados $s_1, \ldots, s_n \in \mathbb{L}$, diremos que esses são **algebricamente independentes** sobre $\mathbb{K}$ se para qualquer $f(x_1, \ldots, x_n) \in \mathbb{K}[x_1, \ldots, x_n]$ vale*

$$f(s_1, \ldots, s_n) = 0 \Rightarrow f(x_1, \ldots, x_n) \equiv 0.$$

*Um subconjunto $S \subseteq \mathbb{L}$ será dito **algebricamente independente** sobre $\mathbb{K}$ se para quaisquer $s_1, \ldots, s_n \in S$ esses são algebricamente independentes sobre $\mathbb{K}$.*

■

Uma **base de transcendência** de $\mathbb{L}$ sobre $\mathbb{K}$ é um subconjunto Ω de $\mathbb{L}$ algebricamente independente sobre $\mathbb{K}$ que é maximal, com relação à ordem dada pela inclusão, dentre todos os subconjuntos algebricamente independentes sobre $\mathbb{K}$. Prova-se que quaisquer duas bases de transcendência de $\mathbb{L}$ sobre $\mathbb{K}$ possuem a mesma cardinalidade (BORGES; TENGAN, 2015, p. 479).

Definição A.40. *Sejam $\mathbb{L} \mid \mathbb{K}$ uma extensão de corpos e Ω uma base de transcendência de $\mathbb{L}$ sobre $\mathbb{K}$. Chamamos a cardinalidade de Ω de **grau de transcendência** de $\mathbb{L}$ sobre $\mathbb{K}$ e denotaremos por* $\text{tr.deg}(\mathbb{L} \mid \mathbb{K})$. ■

A.8 Corpo de raízes e fecho algébrico

Definição A.41. *Seja $f(x) \in \mathbb{K}[x]$ um polinômio não constante. Se $\mathbb{L} \supseteq \mathbb{K}$ é tal que $\mathbb{L}$ contém todas as raízes de $f(x)$, então dizemos que $f(x)$ **se fatora** em $\mathbb{L}[x]$. Caso $f(x)$ se fatore em $\mathbb{L}[x]$, mas não em $\mathbb{F}[x]$, para qualquer subcorpo de $\mathbb{F}$ de $\mathbb{L}$, então $\mathbb{L}$ é o **corpo de raízes** de $f(x)$.*

■

Equivalentemente, $\mathbb{L}$ é o corpo de raízes de $f(x)$ se $\mathbb{L}$ contém todas as raízes de $f(x)$ e nenhum subcorpo próprio de $\mathbb{L}$ contém todas as raízes de $f(x)$. Dessa forma, considerando $\mathbb{E}$ um corpo que contém todas as raízes $\alpha_1, \ldots, \alpha_n$ de $f(x)$, temos $\mathbb{L} = \mathbb{K}(\alpha_1, \ldots, \alpha_n) \subseteq \mathbb{E}$.

Os próximos quatro resultados podem ser consultados no livro de Weintraub (2006, p. 22 e p. 24) ou no livro de Lee (2018, pp. 223-224).

Proposição A.42. *Seja $f(x) \in \mathbb{K}[x]$ polinômio não constante. Então $f(x)$ possui um corpo de raízes.*

■

Para $\sigma : \mathcal{A} \longrightarrow \mathcal{B}$ um homomorfismo de anéis e $f(x) = a_n x^n + \ldots + a_0 \in \mathcal{A}[x]$, definimos $\sigma(f(x)) := \sigma(a_n)x^n + \ldots + \sigma(a_0) \in \mathcal{B}[x]$.

Lema A.43. *Seja $\sigma_0 : \mathbb{F}_1 \to \mathbb{F}_2$ um isomorfismo de corpos. Sejam $f_1(x) \in \mathbb{F}_1[x]$ um polinômio irredutível e $\mathbb{E}_1 = \mathbb{F}_1(\beta_1)$, em que β_1 é tal que $f_1(\beta_1) = 0$. Seja $f_2 = \sigma_0(f_1(x))$ em $\mathbb{F}_2[x]$ e consideremos $\mathbb{E}_2 = \mathbb{F}_2(\beta_2)$, em que β_2 é tal que $f_2(\beta_2) = 0$. Então σ_0 se estende unicamente a um isomorfismo $\sigma : \mathbb{E}_1 \to \mathbb{E}_2$ com $\sigma(\beta_1) = \beta_2$.*

■

Lema A.44. *Seja $\sigma_0 : \mathbb{F}_1 \to \mathbb{F}_2$ um isomorfismo de corpos. Sejam $f_1 \in \mathbb{F}_1[x]$ e $f_2(x) = \sigma_0(f_1(x)) \in \mathbb{F}_2[x]$. Seja $\mathbb{E}_1$ o corpo de raízes de $f_1(x)$ e seja $\mathbb{E}_2$ o corpo de raízes de $f_2(x)$. Então σ_0 se estende a um isomorfismo $\sigma : \mathbb{E}_1 \to \mathbb{E}_2$.*

■

Teorema A.45. *Quaisquer dois corpos de raízes de $f(x) \in \mathbb{F}[X]$ são isomorfos.*

■

Definição A.46. *Um corpo $\mathbb{K}$ é dito* ***algebricamente fechado*** *se a única extensão algébrica de $\mathbb{K}$ é o próprio $\mathbb{K}$.*

■

O resultado a seguir está demonstrado no livro de Borges e Tengan (2015, p. 449).

Proposição A.47. *Seja $\mathbb{K}$ um corpo. As afirmações a seguir são equivalentes.*

1. *$\mathbb{K}$ é algebricamente fechado.*
2. *Todo polinômio não constante $f(x) \in \mathbb{K}[x]$ é um produto de fatores lineares em $\mathbb{K}[x]$.*
3. *Todo polinômio não constante $f(x) \in \mathbb{K}[x]$ possui uma raiz em $\mathbb{K}$.*
4. *Um polinômio $f(x) \in \mathbb{K}[x]$ é irredutível se, e somente se, $\deg(f(x)) = 1$.*

■

Exemplo A.48. *Se $\mathbb{K}$ é algebricamente fechado, então $\mathbb{K}$ é infinito. De fato, suponhamos que $\mathbb{F}$ seja um corpo finito com n elementos e consideremos o polinômio*

$$f(x) = x^n - x + 1.$$

Os coeficientes de $f(x)$ pertencem todos a $\mathbb{F}$ e $\deg(f(x)) > 0$. Portanto $f(x) \in \mathbb{F}[x]$. Como consequência do Pequeno Teorema de Fermat, temos que em $\mathbb{F}$ vale $a^n = a$ para todo $a \in \mathbb{F}$ (WEINTRAUB, 2006, p. 10) . Logo, $f(a) = 1 \neq 0$ para todo $a \in \mathbb{F}$, isto é, $f(x)$ não possui raiz em $\mathbb{F}$. Dessa forma, um corpo finito não é algebricamente fechado. Pela contrapositiva, se $\mathbb{K}$ é algebricamente fechado, então $\mathbb{K}$ é infinito.

▼

Definição A.49. *Seja $\mathbb{K}$ um corpo. Um* ***fecho algébrico*** *$\overline{\mathbb{K}}$ de $\mathbb{K}$ é uma extensão algébrica de $\mathbb{K}$ que é algebricamente fechada.*

■

A prova do teorema abaixo pode ser consultada no livro de Weintraub (2006, p. 152) ou no livro de Borges e Tengan (2015, p. 450).

Teorema A.50. *Seja $\mathbb{K}$ um corpo qualquer. Então $\mathbb{K}$ possui um fecho algébrico $\overline{\mathbb{K}}$ e este é único a menos de isomorfismo.*

■

Exemplo A.51. *O fecho algébrico do corpo dos números racionais é o corpo dos números algébricos* $\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid f(\alpha) = 0 \text{ para algum } f(x) \in \mathbb{Q}[x]\}$ *(WEINTRAUB, 2006, p. 154).*

▼

Exemplo A.52. *O corpo dos números complexos* $\mathbb{C}$ *é algebricamente fechado. Este é o conhecido Teorema Fundamental da Álgebra (WEINTRAUB, 2006, p. 155).*

▼

Todo homomorfismo $\varphi : \mathbb{L} \to \mathbb{F}$ entre corpos é injetor, isto é, todo homomorfismo entre corpos é um mergulho. Quando $\mathbb{L} \mid \mathbb{K}$ é uma extensão de corpos, $\mathbb{F} \mid \mathbb{K}$ e $\varphi|_{\mathbb{K}} = \mathrm{id}$, chamaremos φ de um **$\mathbb{K}$-mergulho.** Quando é uma extensão de corpos $\mathbb{L} \mid \mathbb{K}$ e $\varphi : \mathbb{L} \to \mathbb{L}$ é um isomorfismo que é um $\mathbb{K}$-mergulho, chamaremos φ de um **$\mathbb{K}$-automorfismo** de $\mathbb{L}$.

A proposição a seguir está demonstrado no livro de Fraleigh (2002, p. 428).

Proposição A.53. *Seja* $\mathbb{L} \mid \mathbb{K}$ *uma extensão algébrica. Seja* $\mathbb{K}'$ *um corpo tal que exista* $\sigma : \mathbb{K} \to \mathbb{K}'$ *um isomorfismo. Então* σ *pode ser estendido a um isomorfismo* $\tau : \mathbb{L} \to \mathbb{F}$*, tal que* $\mathbb{F} \subseteq \overline{\mathbb{K}'}$ *e* $\tau|_{\mathbb{K}} = \sigma$*.*

■

Corolário A.54. *Sejam* $\mathbb{L} \mid \mathbb{K}$ *uma extensão algébrica e* $\overline{\mathbb{K}}$ *um fecho algébrico de* $\mathbb{K}$*. Então existe um* $\mathbb{K}$*-mergulho* $\varphi : \mathbb{L} \hookrightarrow \overline{\mathbb{K}}$*.*

■

Exemplo A.55. *O corolário anterior diz que, dada uma extensão algébrica* $\mathbb{L} \mid \mathbb{K}$*, podemos considerar* $\mathbb{L}$ *contido em um fecho algébrico fixado* $\overline{\mathbb{K}}$ *de* $\mathbb{K}$*. Dessa forma, como teríamos então* $\overline{\mathbb{K}} \mid \mathbb{L}$*, temos um* $\mathbb{L}$*-mergulho (em particular um* $\mathbb{K}$*-mergulho) que nos permite olhar* $\overline{\mathbb{K}} \subseteq \overline{\mathbb{L}}$*. Ainda, isto nos permite olhar para a extensão* $\overline{\mathbb{L}} \mid \mathbb{K}$ *e, aplicando novamente o corolário, podemos, quando conveniente, tomar* $\overline{\mathbb{L}} = \overline{\mathbb{K}}$*.*

▼

Exemplo A.56. *Seja* $\mathbb{K}$ *algebricamente fechado e suponhamos que* $\sigma : \mathbb{K} \longrightarrow \mathbb{F}$*, com* $\mathbb{F} \subseteq \mathbb{K}$*, é um isomorfismo tal que* $\mathbb{K}$ *é algébrico sobre* $\sigma(\mathbb{K}) \subset \mathbb{F}$*. Então* σ *é um automorfismo de* $\mathbb{K}$*. De fato, consideremos o isomorfismo* $\sigma^{-1} : \sigma(\mathbb{K}) \longrightarrow \mathbb{K}$*. Como* $\mathbb{K}$ *é algebricamente fechado e* $\mathbb{K} \mid \sigma(\mathbb{K})$ *é uma extensão algébrica, pela Proposição A.53 segue que* σ^{-1} *pode ser estendido a um isomorfismo* $\tau : \mathbb{K} \longrightarrow \mathbb{L}$ *tal que* $\mathbb{L} \subseteq \mathbb{K}$ *e* $\tau|_{\sigma(\mathbb{K})} = \sigma^{-1}$*. Assim,* $\mathbb{K} = \tau(\sigma(\mathbb{K})) \subseteq \tau(\mathbb{K})$*. Como* $\tau(\mathbb{K}) \subseteq \mathbb{K}$*, segue que* $\tau(\mathbb{K}) = \mathbb{K}$ *e, portanto,* τ *é um automorfismo de* $\mathbb{K}$*.*

▼

Exemplo A.57. *Seja* $\mathbb{L} \mid \mathbb{K}$ *uma extensão algébrica. Então todo isomorfismo de* $\mathbb{L}$ *em um subcorpo de* $\overline{\mathbb{K}}$ *que deixa* $\mathbb{K}$ *fixado pode ser estendido a um automorfismo de* $\overline{\mathbb{K}}$*. De fato, seja*

$\sigma : \mathbb{L} \to \mathbb{F} \subset \overline{\mathbb{K}}$ um isomorfismo que fixa $\mathbb{K}$. Vimos que podemos tomar $\mathbb{K}^{alg} = \overline{\mathbb{L}}$, $\overline{\mathbb{F}} \subseteq \overline{\mathbb{K}}$ e, além disso, a extensão $\overline{\mathbb{K}} \mid \mathbb{L}$ é algébrica. Pelo Teorema A.53, σ pode ser estendido a um isomorfismo τ de $\overline{\mathbb{K}}$ em um subcorpo de $\overline{\mathbb{F}} \subseteq \overline{\mathbb{K}}$. Assim, pelo exemplo anterior, τ é um $\mathbb{K}$-automorfismo de $\overline{\mathbb{K}}$ que estende σ.

▼

Corolário A.58. *Seja $\overline{\mathbb{K}}$ um fecho algébrico de $\mathbb{K}$. Então todo automorfismo de $\mathbb{K}$ pode ser estendido a um $\mathbb{K}$-automorfismo de $\overline{\mathbb{K}}$.*

■

A.9 Extensões separáveis e puramente inseparáveis

Definição A.59. *Seja $\mathbb{K}$ um corpo e $\overline{\mathbb{K}}$ um fecho algébrico de $\mathbb{K}$.*

- *Se $f(x)$ não possui raízes repetidas em $\overline{\mathbb{K}}$, então $f(x)$ é dito um **polinômio separável**. Caso contrário, $f(x)$ é dito um **polinômio inseparável**.*
- *Seja $\mathbb{L}$ um extensão algébrica de $\mathbb{K}$. Um elemento $\alpha \in \mathbb{L}$ é dito **separável** se seu polinômio minimal $m_\alpha(x) \in \mathbb{K}[x]$ é separável em $\mathbb{K}[x]$. Caso contrário, o elemento é dito **inseparável**.*
- *Uma extensão algébrica $\mathbb{L}$ de $\mathbb{K}$ é dita **separável** se todos os elementos de $\mathbb{L}$ são separáveis. Caso contrário, a extensão é dita **inseparável**.*

■

Definição A.60. *Dizemos que um corpo possui **característica** $p \in \mathbb{N}$ se vale*

$$p1 = \overbrace{1 + \ldots + 1}^{p \text{ vezes}} = 0$$

e p é o menor inteiro positivo tal que isso ocorre. Caso tal p não exista, dizemos que o corpo possui característica 0. Denotamos por $\mathrm{char}(\mathbb{K})$ a característica do corpo $\mathbb{K}$.

■

Definição A.61. *Uma extensão $\mathbb{L} \mid \mathbb{K}$ de corpos com característica $p > 0$ é dita **puramente inseparável** se satisfaz uma das seguintes condições equivalentes.*

1. *Para todo $\alpha \in \mathbb{L}$ existe $n = n(\alpha)$ tal que $\alpha^{p^n} \in \mathbb{K}$.*
2. *Nenhum elemento de $\mathbb{L} \setminus \mathbb{K}$ é separável.*

3. *O polinômio minimal de um elemento* $\alpha \in \mathbb{L}$ *tem a forma* $m_\alpha(x) = x^{p^n} - a$ *para algum inteiro* $n \geq 0$ *e algum elemento* $a \in \mathbb{K}$.

■

As equivalências acima estão demonstradas no livro de Isaacs (1993, p. 298). Já o resultado a seguir está demonstrado no livro de Borges e Tengan (2015, p. 458).

Proposição A.62. *Um polinômio não nulo* $f(x) \in \mathbb{K}[x]$ *é separável se, e somente se,* $f(x)$ *e* $f'(x)$ *(a derivada formal de* $f(x)$*) são primos entre si. Além disso, se* $f(x)$ *é irredutível em* $\mathbb{K}[x]$*, então* $f(x)$ *é separável se, e somente se,* $f'(x) \neq 0$.

■

Um corolário imediato da proposição acima está enunciado a seguir.

Corolário A.63. *Se* $\mathbb{L} \mid \mathbb{K}$ *é uma extensão algébrica de corpos com* $\mathrm{char}(\mathbb{K}) = 0$*, então* $\mathbb{L} \mid \mathbb{K}$ *é separável.*

■

Definimos o **fecho separável relativo** de $\mathbb{K}$ em $\mathbb{L}$ como sendo

$$\mathbb{L} \cap \mathbb{K}^s := \{x \in \mathbb{L} \mid x \text{ é separável sobre } \mathbb{K}\}.$$

Definimos também o chamado **fecho separável** $\mathbb{K}^s$ de $\mathbb{K}$ como sendo o fecho separável relativo de $\mathbb{K}$ em $\overline{\mathbb{K}}$. Temos que $\mathbb{L} \cap \mathbb{K}^s$ é um corpo e é uma extensão intermediária de $\mathbb{K}$ e $\mathbb{L}$, sendo uma extensão separável de $\mathbb{K}$.

Chamamos de **grau de separabilidade** $[\mathbb{L} : \mathbb{K}]_s$ de $\mathbb{L}$ sobre $\mathbb{K}$ o número de $\mathbb{K}$-imersões de $\mathbb{L}$ em $\overline{\mathbb{K}}$. Se a extensão $\mathbb{L} \mid \mathbb{K}$ for finita, então $[\mathbb{L} : \mathbb{K}]_s \leq [\mathbb{L} : \mathbb{K}]$, valendo a igualdade se, e somente se, $\mathbb{L} \mid \mathbb{K}$ é separável (BORGES; TENGAN, 2015, p. 460). Temos ainda o seguinte resultado, que pode ser consultado em Borges e Tengan (2015, pp. 460-462).

Proposição A.64. *Sejam* $\mathbb{L} \supseteq \mathbb{F} \supseteq \mathbb{K}$ *extensões algébricas de corpos. As seguintes afirmações são satisfeitas.*

1. $\mathbb{L} \mid \mathbb{K}$ *é separável se, e somente se,* $\mathbb{L} \mid \mathbb{F}$ *e* $\mathbb{F} \mid \mathbb{K}$ *são separáveis.*

2. *Se* $\mathbb{L} \supseteq \mathbb{F} \supseteq \mathbb{K}$ *são extensões finitas, então* $[\mathbb{L} : \mathbb{K}]_s = [\mathbb{L} : \mathbb{F}]_s [\mathbb{F} : \mathbb{K}]_s$.

3. *Se* $\mathbb{L} \mid \mathbb{K}$ *é puramente inseparável, então* $[\mathbb{L} : \mathbb{K}]_s = 1$*. Se* $\mathbb{L} \mid \mathbb{K}$ *é finita, então vale a recíproca.*

4. $\mathbb{L} \cap \mathbb{K}^s$ *é um subcorpo de* $\mathbb{L}$ *e* $\mathbb{L} \mid \mathbb{L} \cap \mathbb{K}^s$ *é puramente inseparável. Se* $\mathbb{L} \mid \mathbb{K}$ *é finita, então* $[\mathbb{L} : \mathbb{K}]_s = [\mathbb{L} \cap \mathbb{K}^s : \mathbb{K}]$.

■

Exemplo A.65. *Sejam* $\mathbb{K}$ *e* $\mathbb{K}^s$ *como anteriormente e suponhamos que* $\mathbb{F}$ *seja um corpo tal que* $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{K}^s$. *Considerando* $\overline{\mathbb{F}} = \overline{\mathbb{K}}$, *vejamos que* $\mathbb{F}^s = \mathbb{K}^s$. *Pela forma como* $\mathbb{K}^s$ *é definido, sabemos que* $\mathbb{K}^s \mid \mathbb{K}$ *é uma extensão separável. Pelo Item 1 da proposição anterior, temos que* $\mathbb{K}^s \mid \mathbb{F}$ *é separável. Logo, todos os elementos de* $\mathbb{K}^s$ *são separáveis com relação a* $\mathbb{F}$, *portanto* $\mathbb{K}^s \subseteq \mathbb{F}^s$. *Novamente,* $\mathbb{F}^s \mid \mathbb{F}$ *é separável por definição. Assim,* $\mathbb{F}^s \mid \mathbb{K}^s$ *é separável pelo Item 1. Portanto, temos* $\mathbb{F}^s \supseteq \mathbb{K}^s \supseteq \mathbb{K}$, *com ambas extensões* $\mathbb{F}^s \mid \mathbb{K}^s$ *e* $\mathbb{K}^s \mid \mathbb{K}$ *separáveis. Pelo Item 1,* $\mathbb{F}^s \mid \mathbb{K}$ *é separável, isto é, todos os elementos de* $\mathbb{F}^s$ *são separáveis sobre* $\mathbb{K}$. *Logo, pela definição de* $\mathbb{K}^s$, *devemos ter que* $\mathbb{F}^s \subseteq \mathbb{K}^s$, *donde concluímos que* $\mathbb{F}^s = \mathbb{K}^s$. ▼

A.10 Extensões normais e galoisianas

Definição A.66. *Uma extensão algébrica* $\mathbb{L} \mid \mathbb{K}$ *é dita* ***normal*** *se, para todo polinômio irredutível* $f(x) \in \mathbb{K}[x]$, $f(\alpha) = 0$ *para algum* $\alpha \in \mathbb{L}$ *implica que* $f(x)$ *se fatora em* $\mathbb{L}[x]$.

■

Exemplo A.67. *Se* $\mathbb{K}^s$ *é o fecho separável de* $\mathbb{K}$ *(dentro de* $\mathbb{K}^{alg}$*), então* $\mathbb{K}^s \mid \mathbb{K}$ *é normal. De fato, se* $f(x) \in \mathbb{K}[x]$ *é irredutível e* $f(\alpha) = 0$ *para algum* $\alpha \in \mathbb{K}^s$, *então, sem perda de generalidade, podemos tomar* $f(x) = m_\alpha(x)$. *Como* α *é separável,* $m_\alpha(x)$ *se fatora como produto de fatores lineares em* $\mathbb{K}^s[x]$, *ou seja, as outras raízes de* $m_\alpha(x)$ *também são separáveis. Logo, se* $f(x) \in \mathbb{K}[x]$ *possui uma raiz em* $\mathbb{K}^s$, *então todas as outras raízes de* $f(x)$ *também estão em* $\mathbb{K}^s$ *e concluímos que* $\mathbb{K}^s \mid \mathbb{K}$ *é normal.*

▼

Se $\mathbb{L} \supseteq \mathbb{F} \supseteq \mathbb{K}$ com $\mathbb{L} \mid \mathbb{K}$ normal, então $\mathbb{L} \mid \mathbb{F}$ é também normal (BORGES; TENGAN, 2015, p. 454). A próxima proposição nos dá uma caracterização de extensões normais e a demonstração pode ser vista no livro de Borges e Tengan (2015, p. 455).

Proposição A.68. *Seja* $\mathbb{L} \mid \mathbb{K}$ *uma extensão algébrica. As afirmações a seguir são equivalentes.*

1. *A extensão* $\mathbb{L} \mid \mathbb{K}$ *é normal.*
2. $\mathbb{L}$ *é o corpo de raízes de um família de polinômios* $S \subseteq \mathbb{K}[x]$.
3. *Todo* $\mathbb{K}$*-mergulho* $\sigma : \mathbb{L} \hookrightarrow \mathbb{L}^{alg}$ *se restringe a um* $\mathbb{K}$*-automorfismo de* $\mathbb{L}$.

■

Definição A.69. *Seja* $\mathbb{L}$ *uma extensão algébrica de* $\mathbb{K}$. *O* ***grupo de automorfismos*** $\mathrm{Aut}(\mathbb{L} \mid \mathbb{K})$ *é o conjunto de todos os* $\mathbb{K}$*-automorfismos de* $\mathbb{L}$*, isto é,*

$$\mathrm{Aut}(\mathbb{L} \mid \mathbb{K}) = \{\sigma : \mathbb{L} \longrightarrow \mathbb{L} \mid \sigma \text{ é automorfismo e } \sigma|_{\mathbb{K}} = \mathrm{id}\},$$

munido da operação de composição. ■

Os seguintes resultados estão demonstrados no livro de Borges e Tengan (2015, p. 456 e p. 463).

Proposição A.70. *Seja* $\mathbb{L} \mid \mathbb{K}$ *uma extensão normal finita. Seja* $\mathbb{F}$ *tal que* $\mathbb{L} \supseteq \mathbb{F} \supseteq \mathbb{K}$ *e* $\mathbb{F} \mid \mathbb{K}$ *é normal. Então todo* $\mathbb{K}$*-automorfismo de* $\mathbb{L}$ *se restringe a um* $\mathbb{K}$*-automorfismo de* $\mathbb{F}$ *e temos um homomorfismo sobrejetor de grupo*

$$\mathrm{Aut}(\mathbb{L} \mid \mathbb{K}) \longrightarrow \mathrm{Aut}(\mathbb{F} \mid \mathbb{K})$$

$$\sigma \longmapsto \sigma|_{\mathbb{F}}.$$

■

Proposição A.71. *Seja* $\mathbb{L} \mid \mathbb{K}$ *uma extensão algébrica e seja* $\mathbb{L} \cap \mathbb{K}^s$ *o fecho separável de* $\mathbb{K}$ *em* $\mathbb{L}$. *Todo* $\mathbb{K}$*-automorfismo de* $\mathbb{L}$ *se restringe a um* $\mathbb{K}$*-automorfismo de* $\mathbb{L} \cap \mathbb{K}^s$ *e temos um homomorfismo injetor de grupo*

$$\mathrm{Aut}(\mathbb{L} \mid \mathbb{K}) \hookrightarrow \mathrm{Aut}(\mathbb{L} \cap \mathbb{K}^s \mid \mathbb{K})$$

$$\sigma \mapsto \sigma|_{\mathbb{L}\cap\mathbb{K}^s}.$$

Se $\mathbb{L} \mid \mathbb{K}$ *é normal, então* $\mathbb{L}\cap\mathbb{K}^s \mid \mathbb{K}$ *é normal. Se* $\mathbb{L} \mid \mathbb{K}$ *é normal e finita, então a aplicação acima é um isomorfismo.*

■

Exemplo A.72. *Se na proposição acima* $\mathbb{L} = \overline{\mathbb{K}}$*, então é possível mostrar que a aplicação vista é um isomorfismo e assim* $\mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K}) \cong \mathrm{Aut}(\mathbb{K}^s \mid \mathbb{K})$. *De fato, vimos no Exemplo A.57 que todo isomorfismo de* $\mathbb{K}^s$ *em um subcorpo de* $\overline{\mathbb{K}}$ *que deixa* $\mathbb{K}$ *fixado pode ser estendido a um* $\mathbb{K}$*-automorfismo de* $\overline{\mathbb{K}}$. *Assim, dado* $\sigma \in \mathrm{Aut}(\mathbb{K}^s \mid \mathbb{K})$, *existe* $\tilde{\sigma} \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K})$ *tal que* $\tilde{\sigma}|_{\mathbb{K}^s} = \sigma$. *Portanto, a aplicação é sobrejetora e assim temos o isomorfismo de grupos.*

▼

Definição A.73. *Seja* G *um subgrupo do grupo de automorfismos de um corpo* $\mathbb{L}$. *O* ***corpo fixado*** *por* G *é definido como* $\mathrm{Fix}(G, \mathbb{L}) = \{\alpha \in \mathbb{L} \mid \sigma(\alpha) = \alpha \text{ para todo } \sigma \in G\}$.

■

O corpo $\mathrm{Fix}(G, \mathbb{L})$ é um subcorpo de $\mathbb{L}$. Ainda, temos $\mathbb{K} \subseteq \mathrm{Fix}(\mathrm{Aut}(\mathbb{L} \mid \mathbb{K}), \mathbb{L})$ (WEINTRAUB, 2006, p. 27).

Definição A.74. *Seja $\mathbb{L}$ uma extensão algébrica de $\mathbb{K}$. Dizemos que $\mathbb{L}$ é uma **extensão galoisiana** de $\mathbb{K}$ se $\mathrm{Fix}(\mathrm{Aut}(\mathbb{L} \mid \mathbb{K}), \mathbb{L}) = \mathbb{K}$. Nesta situação, o grupo $\mathrm{Aut}(\mathbb{L} \mid \mathbb{K})$ passa a ser chamado **grupo de Galois** da extensão e será denotado $\mathrm{Gal}(\mathbb{L} \mid \mathbb{K})$.*

■

A seguir veremos uma forma de caracterizar extensões galoisianas. Para a prova da proposição, consultar o livro de Hungerford (1974, p. 262)

Proposição A.75. *Seja $\mathbb{L} \mid \mathbb{K}$ uma algébrica. As afirmações a seguir são equivalentes.*

1. *$\mathbb{L} \mid \mathbb{K}$ é galoisiana.*

2. *$\mathbb{L} \mid \mathbb{K}$ é normal e separável.*

3. *$\mathbb{L}$ é o corpo de raízes de um conjunto de polinômios separáveis em $\mathbb{K}[x]$.*

■

Assim, se $\mathbb{L} \supseteq \mathbb{F} \supseteq \mathbb{K}$ com $\mathbb{L} \mid \mathbb{K}$ galoisiana, então $\mathbb{L} \mid \mathbb{F}$ é também galoisiana (BORGES; TENGAN, 2015, p. 465).

Exemplo A.76. *O fecho separável $\mathbb{K}^s$ de um corpo $\mathbb{K}$ é uma extensão galoisiana pois é normal e separável. Em particular, se $\overline{\mathbb{K}} \mid \mathbb{K}$ for separável (por exemplo, quando $\mathrm{char}(\mathbb{K}) = 0$), então $\mathbb{K}^s = \overline{\mathbb{K}}$ e concluímos que, neste caso, $\overline{\mathbb{K}} \mid \mathbb{K}$ é uma extensão galoisiana.*

▼

A.11 Teorema Fundamental da Teoria de Galois

Os resultados desta seção podem ser consultados no livro de Borges e Tengan (2015, pp. 467-472).

Dada uma extensão $\mathbb{L} \mid \mathbb{K}$ diremos que $\mathbb{F}$ é um subcorpo ou extensão intermediária se $\mathbb{L} \supseteq \mathbb{F} \supseteq \mathbb{K}$.

Teorema A.77. *(Teorema Fundamental da Teoria de Galois) Seja* $\mathbb{L} \mid \mathbb{K}$ *uma extensão Galois finita. Temos:*

- $|\mathrm{Gal}(\mathbb{L} \mid \mathbb{K})| = [\mathbb{L} : \mathbb{K}]$.
- *Existe uma bijeção*

$$\begin{aligned} \{ \textit{ subgrupos } H \textit{ de } \mathrm{Gal}(\mathbb{L} \mid \mathbb{K})\} &\longleftrightarrow \{ \textit{ subcorpos intermediários } \mathbb{F} \textit{ de } \mathbb{L} \mid \mathbb{K}\} \\ H &\longmapsto \mathrm{Fix}(H, \mathbb{L}) \\ \mathrm{Gal}(\mathbb{L} \mid \mathbb{F}) &\longmapsfrom \mathbb{F}. \end{aligned}$$

- *Seja* $\mathbb{F}$ *um subcorpo intermediário de* $\mathbb{L} \mid \mathbb{K}$. *Temos que* $\mathbb{F} \mid \mathbb{K}$ *é galoisiana se, e somente se,* $\mathrm{Gal}(\mathbb{L} \mid \mathbb{F})$ *é subgrupo normal de* $\mathrm{Gal}(\mathbb{L} \mid \mathbb{K})$.

■

Como $\mathbb{K}^s$ é uma extensão galoisiana de $\mathbb{K}$, chamamos de **grupo de Galois absoluto** $\mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K})$.

Proposição A.78. *Se* $\mathbb{F}$ *é um corpo intermediário de* $\mathbb{K}^s \mid \mathbb{K}$ *e* $\mathbb{F} \mid \mathbb{K}$ *é galoisiana, então todo elemento de* $\mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K})$ *se restringe a um* $\mathbb{K}$*-automorfismo de* $\mathbb{F}$ *e a aplicação*

$$\begin{aligned} \mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K}) &\longrightarrow \mathrm{Gal}(\mathbb{F} \mid \mathbb{K}) \\ \sigma &\longmapsto \sigma|_{\mathbb{F}} \end{aligned}$$

é sobrejetora com núcleo igual a $\mathrm{Gal}(\mathbb{K}^s \mid \mathbb{F})$.

■

Quando a extensão galoisiana $\mathbb{L} \mid \mathbb{K}$ não é finita, não temos a correspondência descrita no Teorema Fundamental da Teoria de Galois. Segundo Borges e Tengan (2015, p. 470), em geral há mais subgrupos do que subcorpos intermediários. No entanto, é possível elaborar uma correspondência parecida com a do Teorema A.77 se considerarmos $\mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K})$ como um grupo topológico.

Lema A.79. *Seja* $G_{\mathbb{K}} = \mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K})$ *o grupo de Galois absoluto. Consideremos o seguinte conjunto*

$$\mathcal{B}' = \{G_{\mathbb{F}} := \mathrm{Gal}(\mathbb{K}^s \mid \mathbb{F}) \mid \textit{ a extensão intermediária } \mathbb{F} \mid \mathbb{K} \textit{ é galoisiana e finita } \}.$$

O conjunto $\mathcal{B} = \{\sigma G_{\mathbb{F}} \mid \sigma \in G_{\mathbb{K}} \textit{ e } G_{\mathbb{F}} \in \mathcal{B}'\}$ *é uma base para uma topologia em* $G_{\mathbb{K}}$, *a chamada* ***Topologia de Krull****.*

■

Teorema A.80. *(Teorema Fundamental da Teoria de Galois Infinita) Seja $\mathbb{K}$ um corpo e $G_{\mathbb{K}}$ o seu grupo de Galois absoluto, equipado com a topologia de Krull.*

- *Para todo subcorpo intermediário $\mathbb{F}$, $G_{\mathbb{F}} = \mathrm{Gal}(\mathbb{K}^s \mid \mathbb{F})$ é um subgrupo fechado de $G_{\mathbb{K}}$.*
- *Temos uma bijeção*

$$\begin{aligned} \{ \text{ subgrupos fechados } H \text{ de } \mathrm{G}_{\mathbb{K}}\} &\longleftrightarrow \{ \text{ subcorpos intermediários } \mathbb{F} \text{ de } \mathbb{K}^s \mid \mathbb{K}\} \\ H &\longmapsto \mathrm{Fix}(\mathrm{H}, \mathbb{K}^{\mathrm{s}}) \\ G_{\mathbb{F}} = \mathrm{Gal}(\mathbb{K}^{sep} \mid \mathbb{F}) &\longmapsfrom \mathbb{F}. \end{aligned}$$

- *Seja $\mathbb{F}$ um subcorpo intermediário de $\mathbb{K}^s \mid \mathbb{K}$. Temos que $\mathbb{F} \mid \mathbb{K}$ é galoisiana (respectivamente finita) se, e somente se, $G_{\mathbb{F}}$ é subgrupo normal de $G_{\mathbb{K}}$ (respectivamente $G_{\mathbb{F}}$ tem índice finito em $G_{\mathbb{K}}$).*

■

Apêndice B

Grupos totalmente ordenados e fecho divisível

Neste apêndice, trazemos algumas definições e resultados sobre grupos totalmente ordenados que melhoram a compreensão do texto principal. Faremos também uma apresentação detalhada do fecho divisível de um grupo abeliano.

As principais referências para a composição deste apêndice foram os livros de Deitmar e Echterhoff (2009), Endler (1972) e Engler e Prestel (2005).

B.1 Grupos totalmente ordenados

Definição B.1. *Um grupo abeliano* $(\Gamma, +, 0)$ *será chamado um* ***grupo totalmente ordenado*** *se existir uma relação binária* $\leq$ *em* Γ *satisfazendo, para todo* $\gamma, \delta, \lambda \in \Gamma$*:*

(OT1) $\gamma \leq \gamma$;

(OT2) $\gamma \leq \delta$ *e* $\delta \leq \gamma \Rightarrow \gamma = \delta$;

(OT3) $\gamma \leq \delta$ *e* $\delta \leq \lambda \Rightarrow \gamma \leq \lambda$;

(OT4) $\gamma \leq \delta$ *ou* $\delta \leq \gamma$;

(OT5) $\gamma \leq \delta \Rightarrow \gamma + \lambda \leq \delta + \lambda$.

■

Lemos $\gamma \leq \delta$ como "γ é menor do que ou igual a δ". Escreveremos em alguns momentos $\delta \geq \gamma$ (lê-se "δ é maior do que ou igual a γ") para dizer $\gamma \leq \delta$. Se sabemos que $\gamma \leq \delta$ e $\gamma \neq \delta$, então escreveremos $\gamma < \delta$ (lê-se "γ é menor do que δ").

As propriedades a seguir consequências diretas da definição.

- Se $\alpha \leq \beta$ e $\gamma \leq \delta$, então $\alpha + \gamma \leq \beta + \delta$. De fato, pela Propriedade $(OT5)$

$$\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma.$$

  Também,

$$\gamma \leq \delta \Rightarrow \gamma + \beta \leq \delta + \beta.$$

  Como Γ é abeliano, então $\gamma + \beta = \beta + \gamma$. Assim, pela Propriedade $(OT3)$,

$$\alpha + \gamma \leq \beta + \gamma \text{ e } \beta + \gamma = \gamma + \beta \leq \delta + \beta$$

  o que implica $\alpha + \gamma \leq \delta + \beta$.

- Em particular, para qualquer $n \in \mathbb{N}$, por indução obtemos que $\gamma \leq \delta$ implica $n\gamma \leq n\delta$.

- Se $0 \leq \gamma$, então $-\gamma \leq 0$. De fato, pela Propriedade (OT5),

$$0 \leq \gamma \Rightarrow 0 + (-\gamma) \leq \gamma + (-\gamma) = 0 \Rightarrow -\gamma \leq 0.$$

  Vale também a recíproca, isto é, se $-\gamma \leq 0$, então $0 \leq \gamma$.

Exemplo B.2. *Sejam Γ e Δ grupos totalmente ordenados e consideremos o grupo dado pela soma direta $\Gamma \oplus \Delta$. A* ***ordem lexicográfica*** *em $\Gamma \oplus \Delta$ é dada pela seguinte relação: para $\gamma, \gamma' \in \Gamma$ e $\delta, \delta' \in \Delta$, temos*

$$(\gamma, \delta) \leq \gamma', \delta' \Leftrightarrow (\gamma < \gamma') \text{ ou } (\gamma = \gamma' \text{ e } \delta \leq \delta').$$

A verificação de que a relação acima torna $\Gamma \oplus \Delta$ um grupo totalmente ordenado requer apenas cálculos diretos. Denotamos por $\Gamma \oplus_{lex} \Delta$ o grupo $\Gamma \oplus \Delta$ munido da ordem lexicográfica.

▼

Um subgrupo Δ de um grupo ordenado Γ é dito **convexo** em Γ se, dado $\delta \in \Delta$, todo $\gamma \in \Gamma$ satisfazendo $0 \leq \gamma \leq \delta$ é tal que $\gamma \in \Delta$. A coleção de todos os subgrupos convexos próprios de Γ satisfaz as condições (OT1), (OT2), (OT3) e (OT4) da Definição B.1 quando considerada a relação dada pela inclusão.

Definição B.3. *Chamamos de* ***posto*** *de Γ o tipo de ordem da coleção de todos os subgrupos convexos próprios de Γ.*

■

Denotamos o posto de Γ por $\mathrm{rk}(\Gamma)$. Se o número de subgrupos convexos for finito, digamos n, então Γ possui posto n.

Definição B.4. *Uma ordem $\leq$ em um grupo abeliano Γ é chamada* ***arquimediana*** *se, para todo $\gamma, \epsilon \in \Gamma$ com $\epsilon > 0$, existe $n \in \mathbb{N}$ tal que $\gamma \leq n\epsilon$.*

■

Exemplo B.5. *Todo subgrupo Δ do grupo aditivo $(\mathbb{R}, +, 0)$ é arquimediano com respeito a ordem canônica induzida de $\mathbb{R}$.*

▼

Um grupo totalmente ordenado com uma ordem arquimediana será chamado de grupo ordenado arquimediano. Um grupo totalmente ordenado arquimediano não possui subgrupos convexos diferentes do trivial, tendo então posto 1 (ENGLER; PRESTEL, 2005, p. 26). A proposição a seguir, cuja demonstração pode ser encontrada no livro de Engler e Prestel (2005, p. 26), complementa o exemplo acima.

Proposição B.6. *Um grupo abeliano totalmente ordenado Γ é de posto um se, e somente se, existe um isomorfismo entre Γ e um subgrupo não trivial de $(\mathbb{R}, +, 0)$, com a ordem canônica induzida de $\mathbb{R}$, e tal isomorfismo preserva a ordem.*

■

A seguinte noção de elemento de torção será amplamente utilizada no texto principal.

Definição B.7. *Seja G um grupo qualquer com elemento neutro e. Um elemento $g \in G$ é dito um* ***elemento de torção*** *se $g^n = e$ para algum $n \in \mathbb{N}$, isto é, g possui ordem finita. Um grupo G é dito de* ***torção*** *se todos os seus elementos são de torção. Um grupo G qualquer é dito* ***livre de torção*** *se não possui elementos de torção.*

■

No caso abeliano, com a notação aditiva, G é livre de torção se, para $n \in \mathbb{N}$ e $g \in G$, vale que $ng = 0$ implica $g = 0$.

Proposição B.8. *Se Γ é um grupo abeliano totalmente ordenado, então Γ é livre de torção.*

Demonstração: Suponhamos, por contradição, que para algum $\gamma \in \Gamma$, $\gamma \neq 0$ e algum $n \in \mathbb{N}$ vale $n\gamma = 0$. Então, também $n(-\gamma) = 0$. Dessa forma, sem perda de generalidade, suponhamos $0 \leq \gamma$. Assim, pelas Propriedades (OT3) e (OT5) da Definição B.1, obtemos

$$0 \leq \gamma \leq 2\gamma \leq \ldots \leq n\gamma = 0.$$

A Propriedade (OT2) então nos diz que deveríamos ter $\gamma = 0$, o que é uma contradição. Logo, Γ ordenado não pode conter elementos de torção.

■

Em particular, vemos que grupos finitos não são totalmente ordenados, pois um grupo livre de torção deve ser infinito.

B.2 Fecho divisível

Definição B.9. *Seja G um grupo abeliano. Dizemos que G é **divisível** se para qualquer $g \in G$ e todo $n \in \mathbb{N}$ existe $h \in G$ tal que $g = nh$.*

■

Exemplo B.10. *O grupo aditivo $(\mathbb{Q}, +, 0)$ é divisível pois, para qualquer $a/b \in \mathbb{Q}$ e $n \in \mathbb{N}$ temos*

$$\frac{a}{b} = n\frac{a}{nb}.$$

▼

Exemplo B.11. *O grupo $(\mathbb{Z}, +, 0)$ não é divisível. Por exemplo, para $g = 3$ e $n = 2$, uma vez que $2 \nmid 3$, não existe $h \in \mathbb{Z}$ tal que $3 = 2h$.*

▼

Lema B.12. *Seja G um grupo abeliano divisível e livre de torção. Então existe uma única aplicação $\cdot : G \times \mathbb{Q} \to G$ que torna G um $\mathbb{Q}$-espaço vetorial.*

Demonstração: Começamos mostrando que, por G ser divisível e livre de torção, então para cada $g \in G$ e $n \in \mathbb{N}$ existe um único $h \in G$ tal que $g = nh$. De fato, como G é divisível, existe pelo menos um h com essa propriedade. Suponhamos que h' é outro elemento de G tal que $g = nh'$. Então

$$n(h - h') = nh - nh' = g - g = 0.$$

Como G é livre de torção, a equação anterior implica que $h - h' = 0$, logo $h = h'$. Denotaremos o único h tal que $g = nh$ por $\frac{1}{n}g$.

Definimos a aplicação

$$\begin{aligned} \cdot \ : G \times \mathbb{Q} &\longrightarrow G \\ \left(g, \frac{a}{n}\right) &\longmapsto \cdot \left(g, \frac{a}{n}\right) := a\left(\frac{1}{n}g\right), \end{aligned}$$

em que $\frac{a}{n}$ é tomado como fração irredutível, $a \in \mathbb{Z}$ e $n \in \mathbb{N}$. Tal ação é bem definida pois tomamos o representante irredutível de $\frac{a}{n}$ e $\frac{1}{n}g$ está unicamente determinado. Como G já é grupo, basta verificarmos os axiomas de espaço vetorial que envolvem o produto por escalar que será dado por "$\cdot$".

- Temos $\dfrac{a}{n}(g_1 + g_2) := a\left(\dfrac{1}{n}(g_1 + g_2)\right)$.

  No entanto,

$$n\left(\frac{1}{n}(g_1 + g_2)\right) = g_1 + g_2 = n\left(\frac{1}{n}g_1\right) + n\left(\frac{1}{n}g_2\right) = n\left(\frac{1}{n}g_1 + \frac{1}{n}g_2\right).$$

Pela unicidade, $\frac{1}{n}(g_1+g_2)=\frac{1}{n}g_1+\frac{1}{n}g_2$. Portanto,

$$\frac{a}{n}(g_1+g_2)=a\left(\frac{1}{n}(g_1+g_2)\right)=a\left(\frac{1}{n}g_1+\frac{1}{n}g_2\right)=a\left(\frac{1}{n}g_1\right)+a\left(\frac{1}{n}g_2\right)=\frac{a}{n}g_1+\frac{a}{n}g_2.$$

- Temos $\left(\frac{a}{n}+\frac{b}{m}\right)g=\left(\frac{am+bn}{nm}\right)g:=(am+bn)\left(\frac{1}{nm}g\right)=am\left(\frac{1}{nm}g\right)+bn\left(\frac{1}{nm}g\right)$.

  No entanto, $am\left(\frac{1}{nm}g\right)=a\left(m\frac{1}{nm}g\right)$. Como

  $$n\left(m\frac{1}{nm}g\right)=nm\left(\frac{1}{nm}g\right)=g,$$

  pela unicidade devemos ter $m\frac{1}{nm}g=\frac{1}{n}g$. Analogamente, temos $n\frac{1}{nm}g=\frac{1}{m}g$. Portanto,

  $$\left(\frac{a}{n}+\frac{b}{m}\right)g=am\left(\frac{1}{nm}g\right)+bn\left(\frac{1}{nm}g\right)=a\left(\frac{1}{n}g\right)+b\left(\frac{1}{m}g\right)=\frac{a}{n}g+\frac{b}{m}g.$$

- Temos $\frac{a}{n}\left(\frac{b}{m}g\right):=a\left(\frac{1}{n}\left(\frac{b}{m}g\right)\right)=a\left(\frac{1}{n}\left(b\frac{1}{m}g\right)\right)$.

  No entanto,

  $$n\left(b\frac{1}{nm}g\right)=b\left(n\frac{1}{nm}g\right)=b\frac{1}{m}g.$$

  Pela unicidade, $\frac{1}{n}\left(b\frac{1}{m}g\right)=b\frac{1}{nm}g$. Portanto,

  $$\frac{a}{n}\left(\frac{b}{m}g\right)=a\left(\frac{1}{n}\left(b\frac{1}{m}g\right)\right)=a\left(b\frac{1}{nm}g\right)=ab\left(\frac{1}{nm}g\right)=\left(\frac{ab}{nm}\right)g.$$

- Temos $\frac{1}{1}g:=1\left(\frac{1}{1}g\right)=1g=g$.

Vejamos que o produto por escalar definido é único. Suponhamos que $*$ seja outro produto por escalar tornando G um $\mathbb{Q}$-espaço vetorial. Para $k\in\mathbb{N}$ temos

$$k*g=\left(\sum_{i=1}^{k}1\right)*g=\sum_{i=1}^{k}g=kg=k(\frac{1}{1}g)=\cdot(g,k)$$

Para $k=-1$ temos

$$g+(-1*g)=1*g+(-1)*g=(1-1)*g=0*g=0,$$

logo $(-1) * g = -g = \cdot(g, -1)$, de modo que concluímos que $k * g = \cdot(g, k)$ para todo $k \in \mathbb{Z}$ e para todo $g \in G$. Para $q = \frac{a}{n} \in \mathbb{Q}$ temos

$$n(q * g) = \cdot(q * g, n) = n * (q * g) = (nq) * g = a * g = \cdot(g, a) = \cdot(g, nq) = n(\cdot(g, q)).$$

Cancelando n obtemos que $q * g = \cdot(g, q)$ para todo $(g, q) \in G \times \mathbb{Q}$, donde segue a unicidade.

■

Dessa forma, em um grupo livre de torção e divisível fica bem definida a divisão de um elemento do grupo por um número natural não nulo. Gostaríamos de levar essa noção de divisão para grupos abelianos livre de torção (não necessariamente divisíveis), como por exemplo os grupos totalmente ordenados. Faremos isso encontrando um grupo livre de torção que contenha nosso grupo inicial e que seja divisível. Construiremos tal grupo com base no raciocínio desenvolvido no livro de Deitmar e Echterhoff (2009, p. 91).

Proposição B.13. *Seja G um grupo abeliano livre de torção. Existe um $\mathbb{Q}$-espaço vetorial $G_{\mathbb{Q}}$, divisível e livre de torção, e um monomorfismo de grupos $\phi : G \hookrightarrow G_{\mathbb{Q}}$ tais que se V é um $\mathbb{Q}$-espaço vetorial e $\psi : G \to V$ é um homomorfismo, então existe um único homomorfismo $\mathbb{Q}$-linear $\psi_{\mathbb{Q}} : G_{\mathbb{Q}} \to V$ tal que $\psi = \psi_{\mathbb{Q}} \circ \phi$. Mais que isso, o espaço vetorial $G_{\mathbb{Q}}$ é gerado por $\phi(G)$.*

Demonstração: Consideremos no cartesiano $G \times \mathbb{N}$ a seguinte relação de equivalência:

$$(g_1, m_1) \sim (g_2, m_2) \iff m_2 g_1 = m_1 g_2.$$

De maneira simples verifica-se que $\sim$ é uma relação de equivalência. Definimos

$$G_{\mathbb{Q}} := \frac{G \times \mathbb{N}}{\sim}.$$

Vamos denotar a classe de equivalência de (g, m) por $\frac{g}{m}$. Definimos em $G_{\mathbb{Q}}$ a seguinte operação:

$$\frac{g_1}{m_1} + \frac{g_2}{m_2} := \frac{m_2 g_1 + m_1 g_2}{m_1 m_2}.$$

Tal operação torna $G_{\mathbb{Q}}$ um grupo abeliano, com elemento neutro $\frac{0}{1}$. A verificação é feita sem complicações. Também vemos que a aplicação ϕ dada por $g \mapsto \frac{g}{1}$ é um homomorfismo injetor e portanto temos um mergulho de G em $G_{\mathbb{Q}}$.

Vejamos que $G_{\mathbb{Q}}$ é livre de torção e divisível. De fato, se $n\frac{g}{m} = \frac{0}{1}$, então

$$\frac{0}{1} = m\frac{0}{1} = mn\frac{g}{m} = n\frac{g}{1}.$$

Logo, olhando a equação em G através do homomorfismo, temos $0 = ng$, o que implica, $g = 0$.

Isto é, $\frac{g}{m} = \frac{0}{m} = \frac{0}{1}$. Assim, $G_{\mathbb{Q}}$ é livre de torção. Sabemos que

$$n\frac{g}{mn} = \frac{g}{m}.$$

Portanto, dados $n \in \mathbb{N}$ e $\frac{g}{m} \in G_{\mathbb{Q}}$, tomamos $h = \frac{g}{mn}$ e vemos que $G_{\mathbb{Q}}$ é divisível.

Pelo lema anterior, $G_{\mathbb{Q}}$ é um $\mathbb{Q}$-espaço vetorial. Dessa forma, como

$$\frac{g}{m} = \cdot \left(\frac{g}{1}, \frac{1}{m}\right) := \frac{1}{m} \cdot \frac{g}{1},$$

segue que $G_{\mathbb{Q}}$ é gerado pela imagem de G em $G_{\mathbb{Q}}$ via combinações $\mathbb{Q}$-lineares. Mais do que isso, $G_{\mathbb{Q}}/\phi(G)$ é um grupo de torção.

Por fim, seja $\psi : G \to V$ um homomorfismo de grupos chegando em um $\mathbb{Q}$-espaço vetorial V. Definimos

$$\begin{aligned} \psi_{\mathbb{Q}} : G_{\mathbb{Q}} &\longrightarrow V \\ \frac{g}{m} &\longmapsto \frac{1}{m}\psi(g). \end{aligned}$$

Assim, $\psi = \psi_{\mathbb{Q}} \circ \phi$ e, se $f : G_{\mathbb{Q}} \to V$ é outro homomorfismo $\mathbb{Q}$-linear tal que $\psi = f \circ \phi$ e

$$f\left(\frac{g}{m}\right) = f\left(\frac{1}{m} \cdot \frac{g}{1}\right) = \frac{1}{m} f\left(\frac{g}{1}\right) = \frac{1}{m}(f \circ \phi)(g) = \frac{1}{m}\psi(g) = \psi_{\mathbb{Q}}\left(\frac{g}{m}\right).$$

Portanto, $f = \psi_{\mathbb{Q}}$.

■

O $\mathbb{Q}$-espaço vetorial $G_{\mathbb{Q}}$ é chamado **fecho divisível** (ou **envoltória divisível**) de G. A dimensão do $\mathbb{Q}$-espaço vetorial $G_{\mathbb{Q}}$ é chamada **posto racional** de G, denotado por $\mathrm{rat.rk}(G)$. Não é difícil verificar que se G é divisível e livre de torção, então $G_{\mathbb{Q}} \cong G$, definido a inversa de ϕ como a função que leva a classe de (g, m) no único elemento h tal que $mh = g$.

Notemos que, na proposição acima, a hipótese de G ser livre de torção só foi necessária para estabelecer que $G_{\mathbb{Q}}$ é também livre de torção e que o produto por escalar é unicamente determinado (Lema B.12). Ou seja, podemos definir $G_{\mathbb{Q}}$, fecho divisível de G, para qualquer grupo abeliano. Esse será também um $\mathbb{Q}$-espaço vetorial, se definirmos o produto por escalar por

$$\begin{aligned} G_{\mathbb{Q}} \times \mathbb{Q} &\longrightarrow G_{\mathbb{Q}} \\ \left(\frac{g}{m}, \frac{a}{n}\right) &\longmapsto a\left(\frac{g}{nm}\right), \end{aligned}$$

com $\frac{a}{n}$ tomado como fração irredutível de denominador positivo. A definição de posto racional também se aplica. Temos a seguinte propriedade do posto racional.

Proposição B.14. *Dado um grupo abeliano G, temos que* $\text{rat.rk}(G) = 0$ *se, e somente se, G é de torção.*

Demonstração:

($\Rightarrow$) Pela contrapositiva, se G não é de torção, então existe $g \in G$ tal que $ng \neq 0$ para todo $n \in \mathbb{N}$. Assim, $\frac{g}{1} \in G_{\mathbb{Q}}$ satisfaz, para todo racional não nulo $a/m \in \mathbb{Q}$, com $m \in \mathbb{N}$,

$$\frac{a}{m} \cdot \frac{g}{1} = \frac{ag}{m} \neq \frac{0}{1}.$$

Logo, $\frac{g}{1}$ é $\mathbb{Q}$-independente, isto é, $\text{rat.rk}(G) \geq 1$.

($\Leftarrow$) Se G é de torção, então para todo $g \in G$ existe $n_g \in \mathbb{N}$ tal que $ng = 0$. Seja $\frac{g}{m}$ um elemento qualquer de $G_{\mathbb{Q}}$. Então

$$\frac{n_g}{1} \cdot \frac{g}{m} = \frac{n_g g}{m} = \frac{0}{1}$$

pois $n_g g = 0m = 0$. Logo, todo elemento não nulo é linearmente dependente sobre $\mathbb{Q}$. Portanto, $\text{rat.rk}(G) = 0$.

■

O nome fecho divisível se justifica por meio da proposição a seguir. A proposição nos dirá que existe uma cópia de $G_{\mathbb{Q}}$ em todo grupo divisível que contenha uma cópia de G e que $G_{\mathbb{Q}}$ é, a menos de isomorfismo, o único grupo divisível que contém uma cópia G tal que $G_{\mathbb{Q}}/\phi(G)$ é de torção.

Proposição B.15. *Seja G um grupo abeliano e seja V um $\mathbb{Q}$-espaço vetorial tal que existe um homomorfismo $\psi : G \to V$. Se ψ é injetor, então existe uma cópia de $G_{\mathbb{Q}}$ contida em V. Se além disso o grupo quociente $V/\psi(G)$ é de torção, então $V \cong G_{\mathbb{Q}}$.*

Demonstração: Consideremos a aplicação $\psi_{\mathbb{Q}} : G_{\mathbb{Q}} \to V$ definida anteriormente por $\psi_{\mathbb{Q}}(g/m) = (1/m)\psi(g)$. Mostremos que $\psi_{\mathbb{Q}}$ é injetora se ψ é injetora.

Sejam $g_1/m_1, g_2/m_2 \in G_{\mathbb{Q}}$. Temos

$$\begin{aligned}
\psi_{\mathbb{Q}}\left(\frac{g_1}{m_1}\right) = \psi_{\mathbb{Q}}\left(\frac{g_2}{m_2}\right) &\iff \frac{1}{m_1}\psi(g_1) = \frac{1}{m_2}\psi(g_2) \\
&\iff m_1 m_2 \frac{1}{m_1}\psi(g_1) = m_1 m_2 \frac{1}{m_2}\psi(g_2) \\
&\iff m_2\psi(g_1) = m_1\psi(g_2) \\
&\iff \psi(m_2 g_1) = \psi(m_1 g_2).
\end{aligned}$$

Pela injetividade de ψ, a última igualdade implica $m_2 g_1 = m_1 g_2$, que é o mesmo que dizer $\frac{g_1}{m_1} = \frac{g_2}{m_2}$. Assim, $\psi_{\mathbb{Q}}$ é injetora e $\psi_{\mathbb{Q}}(G_{\mathbb{Q}}) \subseteq V$ é uma cópia de $G_{\mathbb{Q}}$ em V. Suponhamos agora

que ψ é injetora e $V/\psi(G)$ é um grupo de torção. Mostremos que $\psi_{\mathbb{Q}}$ é sobrejetora. De fato, dado $h \in V$, existe $m \in \mathbb{N}$ tal que $mh = \psi(g) \in \psi(G)$, pois $V/\psi(G)$ é de torção. Assim,

$$\psi_{\mathbb{Q}}\left(\frac{g}{m}\right) = \frac{1}{m}\psi(g) = \frac{1}{m}mh = h.$$

Portanto, $V \cong G_{\mathbb{Q}}$. ■

Veremos a seguir que $G_{\mathbb{Q}} \cong G \otimes \mathbb{Q}$. Na literatura, é comum definir o fecho divisível de G simplesmente como $G \otimes \mathbb{Q}$. Por exemplo, nos trabalhos de Bengus-Lasnier (2021) e no livro de Engler e Prestel (2005), a definição via produto tensorial é a escolhida. Aqui preferimos trazer as duas apresentações. Definir $G_{\mathbb{Q}}$ como fecho divisível torna este objeto independente da noção de produto tensorial e traz, a princípio, uma melhor visualização de como são os elementos do fecho divisível. No entanto, o produto tensorial é uma estrutura muito rica, sendo então interessante vincular o fecho divisível às suas propriedades.

Proposição B.16. *Seja G um grupo abeliano. Temos*

$$G_{\mathbb{Q}} \cong G \otimes \mathbb{Q}.$$

Demonstração: Para simplificar a notação, escreveremos apenas $G \otimes \mathbb{Q}$. Iniciamos vendo que todo elemento de $G \otimes \mathbb{Q}$ é da forma $g \otimes q$. Seja

$$t = \sum_{j=1}^{s} g_j \otimes q_j \in G \otimes \mathbb{Q}$$

um elemento qualquer. Temos $q_j = a_j/b_j$ para cada j, $1 \leq j \leq s$. Seja

$$n = \prod_{i=1}^{s} b_i.$$

Assim,

$$q_j = \frac{a_j}{b_j} = \frac{a_j}{b_j}\frac{n/b_j}{n/b_j} = \frac{m_j}{n},$$

com $m_j = a_j(n/b_j)$. Portanto,

$$\begin{aligned} t &= \sum_{j=1}^{s} g_j \otimes q_j = \sum_{j=1}^{s} g_j \otimes \frac{m_j}{n} \\ &= \sum_{j=1}^{s} m_j g_j \otimes \frac{1}{n} = \left(\sum_{j=1}^{s} m_j g_j\right) \otimes \frac{1}{n} \\ &= g \otimes q. \end{aligned}$$

Definimos

$$\psi : G \otimes \mathbb{Q} \longrightarrow G_{\mathbb{Q}}$$
$$g \otimes \frac{a}{b} \longmapsto \frac{ag}{b}$$

e

$$\varphi : G_{\mathbb{Q}} \longrightarrow G \otimes \mathbb{Q}$$
$$\frac{g}{b} \longmapsto g \otimes \frac{1}{b}.$$

Vejamos que ψ e ϕ são homomorfismos. Para quaisquer $g_1 \otimes \frac{a_1}{b_1}, g_2 \otimes \frac{a_2}{b_2} \in G \otimes \mathbb{Q}$, definindo $n = b_1 b_2$ e $m_j = a_j(n/b_j)$ verifica-se diretamente que $\frac{a_j}{b_j} = \frac{m_j}{n}$ para $j = 1, 2$. Assim,

$$\begin{aligned}
\psi\left(g_1 \otimes \frac{a_1}{b_1} + g_2 \otimes \frac{a_2}{b_2}\right) &= \psi\left((m_1 g_1 + m_2 g_2) \otimes \frac{1}{n}\right) \\
&= \frac{m_1 g_1 + m_2 g_2}{n} = \frac{m_1 g_1}{n} + \frac{m_2 g_2}{n} \\
&= \psi\left(g_1 \otimes \frac{m_1}{n}\right) + \psi\left(g_2 \otimes \frac{m_2}{n}\right) \\
&= \psi\left(g_1 \otimes \frac{a_1}{b_1}\right) + \psi\left(g_2 \otimes \frac{a_2}{b_2}\right).
\end{aligned}$$

Para quaisquer $\frac{g_1}{b_1}, \frac{g_2}{b_2} \in G_{\mathbb{Q}}$ temos

$$\begin{aligned}
\varphi\left(\frac{g_1}{b_1} + \frac{g_2}{b_2}\right) &= \varphi\left(\frac{b_2 g_1 + b_1 g_2}{b_1 b_2}\right) \\
&= (b_2 g_1 + b_1 g_2) \otimes \frac{1}{b_1 b_2} \\
&= b_2 g_1 \otimes \frac{1}{b_1 b_2} + b_1 g_2 \otimes \frac{1}{b_1 b_2} \\
&= g_1 \otimes \frac{b_2}{b_1 b_2} + g_2 \otimes \frac{b_1}{b_1 b_2} \\
&= g_1 \otimes \frac{1}{b_1} + g_2 \otimes \frac{1}{b_2} \\
&= \varphi\left(\frac{g_1}{b_1}\right) + \varphi\left(\frac{g_2}{b_2}\right).
\end{aligned}$$

Para concluir, vejamos que ψ e φ são inversas uma da outra. Para quaisquer $\frac{g}{b} \in G_{\mathbb{Q}}$ e $g \otimes \frac{a}{b} \in G \otimes \mathbb{Q}$ temos

$$(\psi \circ \varphi)\left(\frac{g}{b}\right) = \psi\left(g \otimes \frac{1}{b}\right) = \frac{g}{b}$$

e

$$(\varphi \circ \psi)\left(g \otimes \frac{a}{b}\right) = \varphi\left(\frac{ag}{b}\right) = ag \otimes \frac{1}{b} = g \otimes \frac{a}{b}.$$

Portanto, $G_{\mathbb{Q}} \cong G \otimes \mathbb{Q}$. ■

Proposição B.17. *Sejam Γ um grupo totalmente ordenado e $\Gamma_{\mathbb{Q}} \cong \Gamma \otimes \mathbb{Q}$. Então, o fecho divisível de Γ pode ser totalmente ordenado.*

Demonstração: Sejam $\frac{\gamma_1}{b_1}, \frac{\gamma_2}{b_2} \in \Gamma_{\mathbb{Q}}$. Definimos a seguinte relação

$$\frac{\gamma_1}{b_1} \leq \frac{\gamma_2}{b_2} \Longleftrightarrow b_2\gamma_1 \leq b_1\gamma_2 \text{ em } \Gamma.$$

Vejamos que tal relação satisfaz as cinco propriedades da Definição B.1. Vamos nos referir às propriedades de ordem de Γ por $(\text{OT1})_\Gamma, \ldots, (\text{OT5})_\Gamma$. Sejam $\frac{\gamma_1}{b_1}, \frac{\gamma_2}{b_2}, \frac{\gamma_3}{b_3} \in \Gamma_{\mathbb{Q}}$.

(OT1) $\frac{\gamma_1}{b_1} \leq \frac{\gamma_1}{b_1}$ pois, em Γ, $b_1\gamma_1 \leq b_1\gamma_1$.

(OT2) Se $\frac{\gamma_1}{b_1} \leq \frac{\gamma_2}{b_2}$ e $\frac{\gamma_2}{b_2} \leq \frac{\gamma_1}{b_1}$, então, em Γ, $b_2\gamma_1 \leq b_1\gamma_2$ e $b_1\gamma_2 \leq b_2\gamma_1$. Por $(\text{OT2})_\Gamma$, segue que $b_2\gamma_1 = b_1\gamma_2$. Logo $\frac{\gamma_1}{b_1} = \frac{\gamma_2}{b_2}$

(OT3) Suponhamos

$$\frac{\gamma_1}{b_1} \leq \frac{\gamma_2}{b_2} \text{ e } \frac{\gamma_2}{b_2} \leq \frac{\gamma_3}{b_3}.$$

Assim, em Γ,

$$b_2\gamma_1 \leq b_1\gamma_2 \text{ e } b_3\gamma_2 \leq b_2\gamma_3.$$

Usando também $(\text{OT3})_\Gamma$ para os naturais b_3 e b_1, temos

$$b_3b_2\gamma_1 \leq b_3b_1\gamma_2 \text{ e } b_1b_3\gamma_2 \leq b_1b_2\gamma_3 \Rightarrow b_3b_2\gamma_1 \leq b_1b_2\gamma_3.$$

Portanto, pela definição da nossa relação,

$$b_3b_2\gamma_1 \leq b_1b_2\gamma_3 \Longleftrightarrow \frac{\gamma_1}{b_1} = \frac{b_2\gamma_1}{b_2b_1} \leq \frac{\gamma_3}{b_3}.$$

(OT4) Suponhamos que $\frac{\gamma_1}{b_1}$ não está relacionado com $\frac{\gamma_2}{b_2}$ por meio de $\leq$, o que denotaremos por $\frac{\gamma_1}{b_1} \not\leq \frac{\gamma_2}{b_2}$. Assim, em Γ, $b_2\gamma_1 \not\leq b_1\gamma_2$. Por $(\text{OT4})_\Gamma$, temos $b_1\gamma_2 \leq b_2\gamma_1$, isto é, $\frac{\gamma_2}{b_2} \leq \frac{\gamma_1}{b_1}$.

(OT5) Suponhamos $\frac{\gamma_1}{b_1} \leq \frac{\gamma_2}{b_2}$, isto é, $b_2\gamma_1 \leq b_1\gamma_2$. Então,

$$b_3^2b_2\gamma_1 \leq b_3^2b_1\gamma_2.$$

Pela Propriedade $(\text{OT5})_\Gamma$, podemos somar $b_1b_2b_3\gamma_3$ de modo que

$$b_3^2b_2\gamma_1 + b_1b_2b_3\gamma_3 \leq b_3^2b_1\gamma_2 + b_1b_2b_3\gamma_3 \Longleftrightarrow b_2b_3(b_3\gamma_1 + b_1\gamma_3) \leq b_1b_3(b_3\gamma_2 + b_2\gamma_3).$$

Aplicando a definição da relação $\leq$ em $\Gamma_{\mathbb{Q}}$, obtemos

$$\frac{b_3\gamma_1 + b_1\gamma_3}{b_1b_2} \leq \frac{b_3\gamma_2 + b_2\gamma_3}{b_2b_3} \iff \frac{\gamma_1}{b_1} + \frac{\gamma_3}{b_3} \leq \frac{\gamma_2}{b_2} + \frac{\gamma_3}{b_3}.$$

De maneira análoga definimos em $\Gamma \otimes \mathbb{Q}$ e seguinte relação

$$\gamma_1 \otimes \frac{1}{b_1} \leq \gamma_2 \otimes \frac{1}{b_2} \iff b_2\gamma_1 \leq b_1\gamma_2 \text{ em } \Gamma.$$

Lembremos que todos os elementos de $\Gamma \otimes \mathbb{Q}$ tem a forma $\gamma \otimes \frac{a}{b} = a\gamma \otimes \frac{1}{b}$. Tal relação faz com que $\Gamma \otimes \mathbb{Q}$ se torne um grupo ordenado.

Além disso, o isomorfismo $\varphi : \Gamma_{\mathbb{Q}} \to \Gamma \otimes \mathbb{Q}$ preserva as ordens, isto é,

$$\begin{aligned} \frac{\gamma_1}{b_1} \leq \frac{\gamma_2}{b_2} &\iff b_2\gamma_1 \leq b_1\gamma_2 \\ &\iff \gamma_1 \otimes \frac{1}{b_1} \leq \gamma_2 \otimes \frac{1}{b_2} \\ &\iff \varphi\left(\frac{\gamma_1}{b_1}\right) \leq \varphi\left(\frac{\gamma_2}{b_2}\right). \end{aligned}$$

■

Apêndice C

Propriedades iniciais das valorizações e exemplos

Neste apêndice, provaremos as propriedades iniciais de uma valorização e exibiremos os cálculos envolvidos nos exemplos apresentados no Capítulo 1.

As principais referências para a composição deste apêndice foram os trabalhos de Engler e Prestel (2005), Kuhlmann (20??a) e Novacoski (2021).

C.1 Propriedades iniciais das valorizações e dos anéis de valorização

Seja ν uma valorização em $\mathcal{R}$. Para todo $a, b \in \mathcal{R}$ temos as seguintes propriedades.

- Se a é unidade, então

$$0 = \nu(1) = \nu(aa^{-1}) = \nu(a) + \nu(a^{-1}).$$

  Logo, $\nu(a^{-1}) = -\nu(a)$.

- Temos, pelo item anterior, que $\nu(-1) = -\nu(-1)$, isto é, $\nu(-1) + \nu(-1) = 0$. Como Γ é totalmente ordenado, todos os seus elementos não nulos são livre de torção (ver Apêndice B). Assim, $\nu(-1) = 0$.

- Como consequência do item anterior, segue que $\nu(-a) = \nu(-1) + \nu(a) = \nu(a)$.

- Pelo Axioma $(V1)$, se $a \in \mathcal{R}$, então $\nu(a^m) = m\nu(a)$. Em particular, se $a^m = 1$, então $\nu(a^m) = m\nu(a) = 0$, isto é, $\nu(a) = 0$.

- Suponhamos que $\nu(a) \neq \nu(b)$. Pela ordem total de Γ, podemos supor, sem perda de generalidade, que $\nu(b) > \nu(a)$. Assim,

$$\begin{aligned}\nu(a) &= \nu(a+b-b)\\ &\geq \min\{\nu(a+b), \nu(-b)\}\\ &= \min\{\nu(a+b), \nu(b)\}\end{aligned}$$

Se $\nu(a+b) > \nu(b)$, então

$$\nu(a) \geq \min\{\nu(a+b), \nu(b)\} = \nu(b) > \nu(a),$$

o que é uma contradição. Dessa forma, devemos ter $\nu(a+b) \leq \nu(b)$. Portanto,

$$\nu(a) \geq \min\{\nu(a+b), \nu(b)\} = \nu(a+b) \geq \min\{\nu(a), \nu(b)\} = \nu(a).$$

Logo, se $\nu(a) \neq \nu(b)$, então $\nu(a+b) = \min\{\nu(a), \nu(b)\}$.

- Suponhamos $b_1, b_2 \ldots, b_n \in \mathcal{R}$. Mostremos por indução que, para todo $n \geq 2$,

$$\nu(b_1 + b_2 + \ldots + b_n) \geq \min\{\nu(b_1), \nu(b_2), \ldots, \nu(b_n)\}.$$

Para $n = 2$ o resultado se resume ao Axioma $(V2)$, que vale pois ν é uma valorização. Suponhamos que o resultado seja verdadeiro para $n-1$. Temos

$$\nu(b_1 + b_2 + \ldots + b_n) \geq \min\{\nu(b_1 + b_2 + \ldots + b_{n-1}), \nu(b_n)\}.$$

Como

$$\min\{\min\{\nu(b_1), \nu(b_2), \ldots, \nu(b_{n-1})\}, \nu(b_n)\} = \min\{\nu(b_1), \nu(b_2), \ldots, \nu(b_n)\},$$

segue que

$$\begin{aligned}\nu(b_1 + b_2 + \ldots + b_n) &\geq \min\{\nu(b_1 + b_2 + \ldots + b_{n-1}), \nu(b_n)\}\\ &\geq \min\{\min\{\nu(b_1), \nu(b_2), \ldots, \nu(b_{n-1})\}, \nu(b_n)\}\\ &= \min\{\nu(b_1), \nu(b_2), \ldots, \nu(b_{n-1}), \nu(b_n)\}.\end{aligned}$$

- Suponhamos $a, b_1, b_2 \ldots, b_n \in \mathcal{R}$ com $\nu(a) < \nu(b_i)$ para todo i, $1 \leq i \leq n$. Assim,

$$\nu(b_1 + b_2 + \ldots + b_n) \geq \min\{\nu(b_1), \nu(b_2), \ldots, \nu(b_n)\} > \nu(a).$$

Logo, $\nu(b_1 + b_2 + \ldots + b_n) > \nu(a)$ e portanto

$$\nu(a + (b_1 + b_2 + \ldots + b_n)) = \nu(a).$$

O lema abaixo mostra que o suporte de uma valorização é um ideal primo de $\mathcal{R}$.

Lema C.1. *Suponhamos que $\nu : \mathcal{R} \longrightarrow \Gamma_\infty$ seja uma aplicação que satisfaz os Axiomas $(V1)$ e $(V2)$. As afirmações a seguir são equivalentes.*

1. *A aplicação ν satisfaz $(V3)$.*
2. *A aplicação ν não é constante.*
3. *O conjunto $\mathrm{supp}(\nu)$ é um ideal primo de $\mathcal{R}$.*

Demonstração:

(1. $\Leftrightarrow$ 2.) Se $\nu(1) = 0$ e $\nu(0) = \infty$, então ν não é constante. Para a recíproca, suponhamos que ν não é constante. Dessa forma, existe $a \in \mathcal{R}$ tal que $\nu(a) = \gamma \neq \infty$. Assim,

$$\gamma = \nu(a) = \nu(a \cdot 1) = \nu(a) + \nu(1) = \gamma + \nu(1),$$

o que implica $\nu(1) = 0$. Como ν não é constante, existe $b \in \mathcal{R}$ tal que $\nu(b) = \delta \neq 0$. Dessa forma, temos

$$\nu(0) = \nu(b \cdot 0) = \nu(b) + \nu(0) = \delta + \nu(0).$$

Essa igualdade só é possível se $\nu(0) = \infty$.

(2. $\Leftrightarrow$ 3.) Suponhamos que ν não é constante. Mostremos inicialmente que $\mathrm{supp}(\nu)$ é um ideal próprio de $\mathcal{R}$. Sejam $a, a' \in \mathrm{supp}(\nu)$ e $b \in \mathcal{R}$. Temos

$$\nu(a + a') \geq \min\{\nu(a), \nu(a')\} = \infty$$

e

$$\nu(ab) = \nu(a) + \nu(b) = \infty.$$

Assim, $a + a'$ e ab são elementos de $\mathrm{supp}(\nu)$, mostrando que este é um ideal de $\mathcal{R}$. Como ν não é constante, existe $b \in \mathcal{R}$ tal que $\nu(b) \neq \infty$, logo $\mathrm{supp}(\nu)$ é ideal próprio. Vejamos que tal ideal é primo. Sejam $a, b \in \mathcal{R}$ tais que $ab \in \mathrm{supp}(\nu)$. Dessa forma,

$$\infty = \nu(ab) = \nu(a) + \nu(b).$$

Logo, $\nu(a) = \infty$ ou $\nu(b) = \infty$, mostrando que $\mathrm{supp}(\nu)$ é um ideal primo.

Para a recíproca, se $\mathrm{supp}(\nu)$ é um ideal primo de $\mathcal{R}$, então $1 \notin \mathrm{supp}(\nu)$ e $0 \in \mathrm{supp}(\nu)$. Logo, $\nu(1) \neq \infty$ e $\nu(0) = \infty$, mostrando que ν não é constante. ■

Exemplo C.2. *Seja ν uma valorização. Como* $\mathrm{supp}(\nu)$ *é um ideal primo, o quociente* $\mathcal{R}/\mathrm{supp}(\nu)$ *é um domínio de integridade. Definindo* $\nu' : \mathcal{R}/\mathrm{supp}(\nu) \longrightarrow \Gamma_\infty$ *por* $\nu'(a + \mathrm{supp}(\nu)) := \nu(a)$, *temos uma valorização neste domínio de integridade que possui* $\mathrm{supp}(\nu') = \{0\}$. *De fato, vejamos que ν' está bem definida e satisfaz os axiomas de valorização. De fato, se* $a + \mathrm{supp}(\nu) = b + \mathrm{supp}(\nu)$, *então* $a - b \in \mathrm{supp}(\nu)$. *Logo,* $\infty = \nu(a - b) \geq \min\{\nu(a), \nu(b)\}$. *Assim,* $\nu(a) = \nu(b)$. *Os Axiomas* $(V1)$, $(V2)$ *e* $(V3)$ *seguem direto do fato de ν ser valorização. Ademais,* $\nu'(a + \mathrm{supp}(\nu)) := \nu(a) = \infty$ *implica que* $a \in \mathrm{supp}(\nu)$. *Isto é,* $a + \mathrm{supp}(\nu) = 0$, *donde concluímos que* $\mathrm{supp}(\nu') = \{0\}$.

▼

A proposição a seguir é a responsável pelo conceito de equivalência entre valorizações que utilizamos ao longo deste trabalho.

Proposição C.3. *Sejam ν e μ valorizações em um anel $\mathcal{R}$. As afirmações a seguir são equivalentes.*

1. *Para todo* $a, b \in \mathcal{R}$, *temos que* $\nu(a) > \nu(b) \Leftrightarrow \mu(a) > \mu(b)$.

2. *Existe um isomorfismo que preserva a ordem* $\phi : \nu\mathcal{R} \longrightarrow \mu\mathcal{R}$ *tal que* $\mu = \phi \circ \nu$.

3. *Temos* $\mathrm{supp}(\nu) = \mathrm{supp}(\mu)$ *e para quaisquer* $\overline{a}/\overline{b} \in \mathrm{Frac}(\mathcal{R}/\mathrm{supp}(\nu)) = \mathrm{Frac}(\mathcal{R}/\mathrm{supp}(\mu))$ *temos que* $\nu'(\overline{a}/\overline{b}) \geq 0$ *se, e somente se,* $\mu'(\overline{a}/\overline{b}) \geq 0$.

Demonstração:

$(1 \Rightarrow 2)$ Suponhamos que $\nu(a) > \nu(b) \Leftrightarrow \mu(a) > \mu(b)$ para quaisquer $a, b \in \mathcal{R}$. Definimos $\phi : \nu\mathcal{R} \longrightarrow \mu\mathcal{R}$ por $\phi(\nu(a)) := \mu(a)$ para $a \in \mathcal{R}$ e estendemos para $\nu\mathcal{R}$ canonicamente. Como $\mu = \phi \circ \nu$, basta vermos que ϕ é um isomorfismo de grupos que preserva a ordem. É suficiente mostrar isso para os geradores $\{\nu(a) \mid a \in \mathcal{R}, \nu(a) \neq \infty\}$. Sejam $a, b \in \mathcal{R}$. Pelo Axioma $(V1)$ temos

$$\begin{aligned}\phi(\nu(a) + \nu(b)) &= \phi(\nu(ab)) \\ &= \mu(ab) \\ &= \mu(a) + \mu(b) \\ &= \phi(\nu(a)) + \phi(\nu(b)).\end{aligned}$$

Por hipótese, $\nu(a) > \nu(b)$ se, e somente se, $\mu(a) > \mu(b)$. Logo, ϕ preserva a ordem. Ainda, isso implica que ϕ é injetora. Para $\mu(a) \in \mu\mathcal{R}$, temos pela definição de ϕ que, para este a, $\phi(\nu(a)) = \mu(a)$. Logo, ϕ é sobrejetora. Assim, temos que ϕ é um isomorfismo de grupos que preserva a ordem e $\mu = \phi \circ \nu$.

$(2 \Rightarrow 3)$ Suponhamos que exista $\phi : \nu\mathcal{R} \longrightarrow \mu\mathcal{R}$ um isomorfismo que preserva a ordem tal que $\mu = \phi \circ \nu$. Para cada $a \in \mathcal{R}$ temos

$$\begin{aligned} a \notin \text{supp}(\nu) &\iff \nu(a) \in \nu\mathcal{R} \\ &\iff \mu(a) = (\phi \circ \nu)(a) \in \mu\mathcal{R} \\ &\iff a \notin \text{supp}(\mu). \end{aligned}$$

Portanto, $\text{supp}(\nu) = \text{supp}(\mu)$. Agora, para $\overline{a}/\overline{b} \in \text{Frac}(\mathcal{R}/\text{supp}(\nu))$, temos

$$\begin{aligned} \nu'(\overline{a}/\overline{b}) \geq 0 &\iff \nu(a) \geq \nu(b) \\ &\iff \mu(a) \geq \mu(b) \\ &\iff \mu'(\overline{a}/\overline{b}) \geq 0. \end{aligned}$$

$(3 \Rightarrow 1)$ Suponhamos que vale a Afirmação 3 e sejam $a, b \in \mathcal{R}$. Se $b \in \text{supp}(\nu) = \text{supp}(\mu)$, então ambos $\nu(a) > \nu(b)$ e $\mu(a) > \mu(b)$ não acontecem. Dessa forma, suponhamos $b \notin \text{supp}(\nu)$. Se $a \in \text{supp}(\nu) = \text{supp}(\mu)$, então segue o resultado. Caso contrário,

$$\begin{aligned} \nu(a) > \nu(b) &\iff \nu'(\overline{a}/\overline{b}) < 0 \\ &\iff \mu'(\overline{a}/\overline{b}) < 0 \\ &\iff \mu(a) > \mu(b). \end{aligned}$$

■

Sobre os anéis de valorização, dentre as diversas propriedades destes, evidenciamos duas que são básicas.

Proposição C.4. *Seja $\mathcal{O} \subset \mathbb{K}$ anel de valorização. Então,* $\text{Frac}(\mathcal{O}) = \mathbb{K}$. *Além disso, $\mathcal{O}$ é local.*

Demonstração: Seja $a \in \mathbb{K}$ não nulo. Dessa forma, $a \in \mathcal{O}$ ou $a^{-1} \in \mathcal{O}$. Se $a \in \mathcal{O}$, então identificamos $a = a/1$. Se $a^{-1} \in \mathcal{O}$, então identificamos $a = 1/a^{-1}$. Logo, $\text{Frac}(\mathcal{O}) = \mathbb{K}$

Vejamos agora que $\mathcal{O}$ é local. Se $\mathcal{O}$ é um corpo, então segue o resultado. Caso contrário, $\mathcal{O}$ possui um ideal não nulo e maximal $\mathfrak{m}$. Se $\mathfrak{m}'$ é outro ideal maximal de $\mathcal{O}$ distinto de $\mathfrak{m}$, então sejam $a, b \in \mathcal{O}$ tais que $a \in \mathfrak{m}, b \notin \mathfrak{m}$ e $a \notin \mathfrak{m}', b \in \mathfrak{m}'$. Consideremos ab^{-1} e $(ab^{-1})^{-1} = ba^{-1}$ elementos de $\mathbb{K}$. Se $ba^{-1} \in \mathcal{O}$, então $b = ba^{-1}a \in \mathfrak{m}$, o que não é verdade. Logo ba^{-1} não pode pertencer a $\mathcal{O}$. Analogamente, ab^{-1} não pode pertencer a $\mathcal{O}$. Porém, isso contradiz $\mathcal{O}$ ser anel de valorização. Portanto, $\mathfrak{m}$ é o único ideal maximal de $\mathcal{O}$.

■

Ademais, pode-se provar também que $\mathcal{O}$ ser anel de valorização de $\mathbb{K}$ é equivalente as afirmações abaixo.

- O conjunto dos ideais principais de $\mathcal{O}$ é totalmente ordenado pela inclusão.
- O conjunto dos ideais de $\mathcal{O}$ é totalmente ordenado pela inclusão.
- $\mathcal{O}$ é um anel local e todo ideal finitamente gerado de $\mathcal{O}$ é principal.

Além disso, $\mathcal{O} = \{a \in \mathbb{K} \mid f(a) = 0 \text{ para algum } f \in \mathcal{O}[x]\}$, isto é, $\mathcal{O}$ é integralmente fechado em $\mathbb{K}$.

C.2 Exemplos de valorizações e de anéis de valorização

Exemplo C.5. *Um anel $\mathcal{R}$ que admite uma valorização de Krull ν deve ser um domínio. De fato, como $\text{supp}(\nu) = \{0\}$ é um ideal primo, segue que $\mathcal{R} \cong \mathcal{R}/\{0\}$ é um domínio. Com isso, conseguimos estender a valorização de Krull ν para uma aplicação no corpo de frações $\mathbb{K} = \text{Frac}(\mathcal{R})$, que também denotaremos por ν, definida por*

$$\nu\left(\frac{a}{b}\right) := \nu(a) - \nu(b).$$

Vejamos que ν em $\mathbb{K}$ está bem definida, satisfaz as propriedades de valorização e é a única que estende ν para $\mathbb{K}$, isto é, a única valorização em $\mathbb{K}$ tal que $\nu|_{\mathcal{R}} = \nu$.

De fato, se $\frac{a_1}{b_1} = \frac{a_2}{b_2}$, então $a_1b_2 = a_2b_1$. Logo, $\nu(a_1) + \nu(b_2) = \nu(a_2) + \nu(b_1)$, o que implica $\nu(a_1) - \nu(b_1) = \nu(a_2) - \nu(b_2)$. Portanto, ν está bem definida em $\mathbb{K}$. Vejamos que ν é uma valorização.

- $(V1)$ *Para $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathbb{K}$, temos que*

$$\begin{aligned}\nu\left(\frac{a_1}{b_1}\frac{a_2}{b_2}\right) = \nu\left(\frac{a_1a_2}{b_1b_2}\right) &:= \nu(a_1a_2) - \nu(b_1b_2)\\ &= \nu(a_1) + \nu(a_2) - \nu(b_1) - \nu(b_2)\\ &= \nu\left(\frac{a_1}{b_1}\right) + \nu\left(\frac{a_2}{b_2}\right)\end{aligned}$$

- $(V2)$ *Para $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathbb{K}$, temos*

$$\begin{aligned}\nu\left(\frac{a_1}{b_1} + \frac{a_2}{b_2}\right) = \nu\left(\frac{a_1b_2 + a_2b_1}{b_1b_2}\right) &:= \nu(a_1b_2 + a_2b_1) - \nu(b_1b_2)\\ &= \nu(a_1b_2 + a_2b_1) - \nu(b_1) - \nu(b_2)\\ &\geq \min\{\nu(a_1b_2), \nu(a_2b_1)\} - \nu(b_1) - \nu(b_2).\end{aligned}$$

Sejam $i, j \in \{1,2\}$, $i \neq j$, tais que $\min\{\nu(a_1b_2), \nu(a_2b_1)\} = \nu(a_ib_j)$. Assim,

$$\begin{aligned}
\nu\left(\frac{a_1}{b_1} + \frac{a_2}{b_2}\right) &\geq \min\{\nu(a_1b_2), \nu(a_2b_1)\} - \nu(b_1) - \nu(b_2) \\
&= \nu(a_ib_j) - \nu(b_1) - \nu(b_2) \\
&= \nu(a_i) + \nu(b_j) - \nu(b_1) - \nu(b_2) \\
&= \nu(a_i) - \nu(b_i) \\
&= \min\{\nu(a_1) - \nu(b_1), \nu(a_2) - \nu(b_2)\} \\
&= \min\left\{\nu\left(\frac{a_1}{b_1}\right), \nu\left(\frac{a_2}{b_2}\right)\right\},
\end{aligned}$$

pois

$$\nu(a_ib_j) \leq \nu(a_jb_i) \Rightarrow \nu(a_i) + \nu(b_j) \leq \nu(a_j) + \nu(b_i) \Rightarrow \nu(a_i) - \nu(b_i) \leq \nu(a_j) + \nu(b_j).$$

- *$(V3)$ Temos, para $b \neq 0$,*

$$\nu\left(\frac{1}{1}\right) := \nu(1) - \nu(1) = 0 \text{ e } \nu\left(\frac{0}{b}\right) := \nu(0) - \nu(b) = \infty - \nu(b) = \infty.$$

Por fim, tomemos ν' uma valorização em $\mathbb{K} = \mathrm{Frac}(\mathcal{R})$, tal que $\nu'|_{\mathcal{R}} = \nu$. Então

$$\begin{aligned}
\nu'\left(\frac{a}{b}\right) &= \nu'\left(a \cdot \frac{1}{b}\right) \\
&= \nu'(a) + \nu'\left(\frac{1}{b}\right) \\
&= \nu'(a) - \nu'(b) \\
&= \nu(a) - \nu(b) \\
&= \nu\left(\frac{a}{b}\right),
\end{aligned}$$

donde segue a unicidade.

▼

Exemplo C.6. *Sejam $\mathcal{D}$ um domínio de ideais principais (e.g. $\mathbb{Z}$ ou $\mathbb{F}[x]$, com $\mathbb{F}$ um corpo) e $\mathbb{K}$ seu corpo de frações (e.g. $\mathbb{Q}$ ou $\mathbb{F}(x)$). Para cada elemento irredutível $p \in \mathcal{D}$, a aplicação $\nu^p : \mathcal{D} \longrightarrow \mathbb{Z}_\infty$ dada por*

$$\nu^p(a) = \begin{cases} m & \text{se } a = p^m a' \text{ com } p \nmid a', \\ \infty & \text{se } a = 0 \end{cases}$$

é uma valorização em $\mathcal{D}$. De fato:

- $(V1)$ *Se* $a = p^{m_a}a'$ *e* $b = p^{m_b}b'$, *com* $p \nmid a'$ *e* $p \nmid b'$, *então*

$$\nu^p(ab) = \nu^p(p^{m_a+m_b}a'b') = m_a + m_b = \nu^p(a) + \nu^p(b).$$

  Isso porque $\mathcal{D}$ *é domínio de ideais principais (logo, domínio de fatoração única). Assim* p *irredutível é também primo. Portanto, se* $p \nmid a'$ *e* $p \nmid b'$, *então* $p \nmid a'b'$.

- $(V2)$ *Se* $a = p^{m_a}a'$ *e* $b = p^{m_b}b'$ *com* $p \nmid a'$ *e* $p \nmid b'$, *então suponhamos que* $m_a \leq m_b$. *Assim,* $a + b = p^{m_a}(a' + p^{m_b-m_a}b')$, *isto é,* $p^{m_a} \mid a + b$. *Como* $\nu^p(a + b)$ *é o maior expoente* m *tal que* $a + b = p^m c$, *com* $p \nmid c$, *e* $p^{m_a} \mid a + b$, *pela unicidade da fatoração em irredutíveis temos que* $m \geq m_a$. *Logo,*

$$\nu^p(a + b) = m \geq m_a = \min\{m_a, m_b\} = \min\{\nu^p(a), \nu^p(b)\}.$$

- $(V3)$ *Por definição,* $\nu^p(0) = \infty$ *e, como* $1 = p^0 1$, *segue que* $\nu^p(1) = 0$.

Ainda, vemos que $\operatorname{supp}(\nu^p) = \{0\}$. *Logo,* ν^p *é uma valorização de Krull e fica bem definida em* $\mathbb{K}$. *Chamamos a valorização* ν^p *em* $\mathbb{K}$ *de* ***valorização p-ádica***.

▼

Exemplo C.7. *Para a valorização p-ádica* ν^p *temos*

$$\mathcal{O}_{\nu^p} = \left\{ \frac{a}{b} \in \mathbb{K} \,\middle|\, p \nmid b \right\} = \mathcal{D}_{\langle p \rangle}, \ \mathfrak{m}_{\nu^p} = \left\{ \frac{a}{b} \in \mathbb{K} \,\middle|\, p \mid a \text{ e } p \nmid b \right\}$$

e o corpo de resíduos é $\mathbb{K}\nu^p = \mathcal{O}_{\nu^p}/\mathfrak{m}_{\nu^p} \cong \operatorname{Frac}(\mathcal{D}/\langle p \rangle) \cong \mathcal{D}/\langle p \rangle$ *(Exemplo A.27).*

▼

Exemplo C.8. *Consideremos a aplicação*

$$\nu_\infty\left(\frac{f(x)}{g(x)}\right) = \begin{cases} \deg(g(x)) - \deg(f(x)) & \text{se } f(x) \text{ e } g(x) \text{ são não nulos,} \\ \infty & \text{se } f(x) \text{ é o polinômio identicamente nulo } 0 \end{cases}$$

definida em $\mathbb{F}(x)$. *Vamos mostrar que* ν_∞ *é uma valorização em* $\mathbb{F}(x)$ *com grupo de valores* $\mathbb{Z}$. *Chamamos tal aplicação de* ***valorização grau*** *em* $\mathbb{F}(x)$. *Ocultaremos a indeterminada* x *para simplificar a notação.*

- $(V1)$ *Sejam* $\frac{a}{b}, \frac{c}{d} \in \mathbb{F}(x)^\times$. *Dessa forma,*

$$\begin{aligned} \nu_\infty\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \nu_\infty\left(\frac{ac}{bd}\right) &:= \deg(bd) - \deg(ac) \\ &= \deg(b) + \deg(d) - \deg(a) - \deg(c) \\ &= \nu_\infty\left(\frac{a}{b}\right) + \nu_\infty\left(\frac{c}{d}\right). \end{aligned}$$

Se $\frac{a}{b} = 0$ *ou* $\frac{c}{d} = 0$*, digamos o primeiro destes, então*

$$\begin{aligned}\nu_\infty\left(0 \cdot \frac{c}{d}\right) &= \nu_\infty(0) \\ &= \infty \\ &= \infty + \nu_\infty\left(\frac{c}{d}\right) \\ &= \nu_\infty(0) + \nu_\infty\left(\frac{c}{d}\right).\end{aligned}$$

- $(V2)$ *Basta vermos que, para* $f, g \in \mathbb{F}[x]$*, temos*

$$\deg(f+g) \leq \max\{\deg(f), \deg(g)\}.$$

Assim, tomando os elementos $\frac{a}{b}, \frac{c}{d} \in \mathbb{F}(x)^\times$ *e supondo, sem perda de generalidade, que* $\nu_\infty\left(\frac{a}{b}\right) \geq \nu_\infty\left(\frac{c}{d}\right)$*, temos*

$$\begin{aligned}\nu_\infty\left(\frac{a}{b} + \frac{c}{d}\right) = \nu_\infty\left(\frac{ad+cb}{bd}\right) &:= \deg(bd) - \deg(ad+cb) \\ &= \deg(b) + \deg(d) - \deg(ad+cb) \\ &\geq \deg(b) + \deg(d) - \max\{\deg(ad), \deg(cb)\}\end{aligned}$$

Se $\max\{\deg(ad), \deg(cb)\} = \deg(ad)$*, então*

$$\deg(b) + \deg(d) - \max\{\deg(ad), \deg(cb)\} = \deg(b) - \deg(a) = \nu_\infty\left(\frac{a}{b}\right).$$

Se $\max\{\deg(ad), \deg(cb)\} = \deg(cb)$*, então*

$$\deg(b) + \deg(d) - \max\{\deg(ad), \deg(cb)\} = \deg(d) - \deg(c) = \nu_\infty\left(\frac{c}{d}\right).$$

Em qualquer um dos casos, temos

$$\begin{aligned}\nu_\infty\left(\frac{a}{b} + \frac{c}{d}\right) &\geq \deg(b) + \deg(d) - \max\{\deg(ad), \deg(cb)\} \\ &\geq \nu_\infty\left(\frac{c}{d}\right) \\ &= \min\left\{\nu_\infty\left(\frac{a}{b}\right), \nu_\infty\left(\frac{c}{d}\right)\right\}.\end{aligned}$$

Se $\frac{a}{b} = 0$ *ou* $\frac{c}{d} = 0$, *digamos o primeiro destes, então*

$$\begin{aligned}\nu_\infty\left(0 + \frac{c}{d}\right) &= \nu_\infty\left(\frac{c}{d}\right) \\ &\geq \min\left\{\nu_\infty(0), \nu_\infty\left(\frac{c}{d}\right)\right\} \\ &= \nu_\infty\left(\frac{c}{d}\right).\end{aligned}$$

- $(V3)$ *Pela definição,* $\nu_\infty(0) = \infty$ *e* $\nu_\infty\left(\frac{1}{1}\right) = \deg(1) - \deg(1) = 0$.

▼

Exemplo C.9. *Para a valorização grau* ν_∞, *temos*

$$\mathcal{O}_{\nu_\infty} = \left\{ \frac{f(x)}{g(x)} \in \mathbb{F}(x) \;\middle|\; \deg(g(x)) \geq \deg(f(x)) \right\} \text{ e}$$

$$\mathfrak{m}_{\nu_\infty} = \left\{ \frac{f(x)}{g(x)} \in \mathbb{F}(x) \;\middle|\; \deg(g(x)) > \deg(f(x)) \right\}.$$

O corpo de resíduos é isomorfo a $\mathbb{F}$. *De fato, basta vermos que*

$$\mathcal{O}_{\nu_\infty} = \left\{ \frac{p(x^{-1})}{q(x^{-1})} \in \mathbb{F}(x) \;\middle|\; p, q \in \mathbb{F}[x] \text{ e } q(0) \neq 0 \right\}.$$

De fato, vejamos que um conjunto contém o outro. Se $\frac{f}{g} \in \mathcal{O}_{\nu_\infty}$, *com*

$$f(x) = a_n x^n + \ldots + a_0,\ g(x) = b_m x^m + \ldots + b_0,\ m \geq n \text{ e } a_n, b_m \neq 0,$$

então tomamos

$$p(x) = a_n x^{m-n} + \ldots + a_1 x^{m+1} + a_0 x^m \text{ e } q(x) = b_m + \ldots + b_1 x^{m-1} + b_0 x^m$$

e vemos, por cálculos diretos, que $q(0) \neq 0$ *e* $\frac{f(x)}{g(x)} = \frac{p(x^{-1})}{q(x^{-1})}$. *Agora, sejam*

$$p(x) = a_n x^n + \ldots + a_0 \text{ e } q(x) = b_m x^m + \ldots + b_0,$$

com $q(0) \neq 0$. *Se* $n \geq m$, *então tomamos* $f(x) = x^n p(x^{-1})$ *e* $g(x) = x^n q(x^{-1})$ *e vemos que* $\frac{p(x^{-1})}{q(x^{-1})} = \frac{f(x)}{g(x)}$ *e* $\deg(f(x)) \leq \deg(g(x))$. *Se* $m \geq n$ *então tomamos* $f(x) = x^m p(x^{-1})$ *e* $g(x) = x^m q(x^{-1})$ *e segue a mesma conclusão.*

Ademais, vemos que

$$\mathfrak{m}_{\nu_\infty} = \left\{ \frac{p(x^{-1})}{q(x^{-1})} \in \mathbb{F}(x) \;\middle|\; p, q \in \mathbb{F}[x], q(0) \neq 0 \text{ e } p(0) = 0 \right\}.$$

Consideremos a aplicação

$$\begin{aligned}\phi : \mathcal{O}_{\nu_\infty} &\longrightarrow \mathbb{F}\\ \frac{p(x^{-1})}{q(x^{-1})} &\longmapsto \frac{p(0)}{q(0)}.\end{aligned}$$

Por cálculos diretos vemos que ϕ é um homomorfismo de anéis. Além disso, ϕ é sobrejetor. De fato, dado $c \in \mathbb{F}$, tomamos $\frac{p(x^{-1})}{q(x^{-1})} = \frac{c}{1}$ e obtermos $\phi\left(\frac{c}{1}\right) = c$. Temos ainda que $\ker(\phi) = \mathfrak{m}_{\nu_\infty}$. Logo, pelo Teorema do Isomorfismo,

$$\frac{\mathcal{O}_{\nu_\infty}}{\ker(\phi)} = \frac{\mathcal{O}_{\nu_\infty}}{\mathfrak{m}_{\nu_\infty}} \cong \mathbb{F}.$$

▼

Exemplo C.10. *Sejam Γ um grupo abeliano totalmente ordenado e $\mathbb{K}$ um corpo. Consideramos o conjunto*

$$\mathbb{K}((t^\Gamma)) := \{a : \Gamma \longrightarrow \mathbb{K} \mid \Gamma \setminus Z(a) \text{ é bem ordenado } \},$$

em que $Z(a) = \{\gamma \in \Gamma \mid a(\gamma) = 0\}$. Denotaremos $a \in \mathbb{K}((t^\Gamma))$ por

$$a = \sum_{\gamma\in\Gamma} a_\gamma t^\gamma, \qquad \text{com } a_\gamma := a(\gamma) \in \mathbb{K}.$$

Definimos duas operações em $\mathbb{K}((t^\Gamma))$:

$$\sum_{\gamma\in\Gamma} a_\gamma t^\gamma + \sum_{\gamma\in\Gamma} b_\gamma t^\gamma := \sum_{\gamma\in\Gamma} (a_\gamma + b_\gamma) t^\gamma$$

e

$$\left(\sum_{\gamma\in\Gamma} a_\gamma t^\gamma\right) \cdot \left(\sum_{\gamma\in\Gamma} b_\gamma t^\gamma\right) := \sum_{\gamma\in\Gamma} \left(\sum_{\sigma+\tau=\gamma} a_\sigma b_\tau\right) t^\gamma.$$

O termo $\displaystyle\sum_{\sigma+\tau=\gamma} a_\sigma b_\tau$ são está bem definido pois, para $\sigma_1 + \tau_1 = \gamma = \sigma_2 + \tau_2$ e $\sigma_1 < \sigma_2$, temos $\tau_1 < \tau_2$ e, como conjuntos bem-ordenados não permitem sequências descendentes infinitas, segue que são finitos os σ's e τ's tais que $\sigma + \tau = \gamma$.

A identidade em $\mathbb{K}((t^\Gamma))$ é aplicação $1 : \Gamma \longrightarrow \mathbb{K}$ dada por $1(0) = 1$ e $1(\gamma) = 0$ para todo $\gamma \neq 0$. Com tais operações $\mathbb{K}((t^\Gamma))$ é um corpo, chamado ***corpo das séries de potências formais*** *em Γ.*

A aplicação

$$\nu_t(a) := \begin{cases} \min\{\Gamma \setminus Z(a)\} & \text{se } a \neq 0,\\ \infty & \text{se } a = 0 \end{cases}$$

é uma valorização, chamada ***valorização t-ádica****. De fato:*

- $(V1)$ *Para* $a, b \in \mathbb{K}((t^\Gamma))$, *ambos não nulos, sejam* $\gamma_a = \min\{\Gamma \setminus Z(a)\}$ *e* $\gamma_b = \min\{\Gamma \setminus Z(b)\}$. *Dessa forma, para todo* $\sigma < \gamma_a$ *e* $\tau < \gamma_b$, *temos* $a_\sigma = b_\tau = 0$. *Suponhamos, sem perda de generalidade, que* $\gamma_a \leq \gamma_b$. *Assim,*

$$\nu_t(ab) = \nu_t\left(\sum_{\gamma \geq \gamma_a + \gamma_b}\left(\sum_{\sigma+\tau=\gamma} a_\sigma b_\tau\right) t^\gamma\right) = \gamma_a + \gamma_b,$$

pois, $a_{\gamma_a} b_{\gamma_b} \neq 0$. *Portanto,* $\nu_t(ab) = \nu_t(a) + \nu_t(b)$. *Se* $a = 0$ *ou* $b = 0$, *digamos* $a = 0$, *então* $\nu_t(ab) = \nu_t(0) = \infty = \infty + \nu_t(b) = \nu_t(a) + \nu_t(b)$.

- $(V2)$ *Para* $a, b \in \mathbb{K}((t^\Gamma))$, *ambos não nulos, sejam* $\gamma_a = \min\{\Gamma \setminus Z(a)\}$ *e* $\gamma_b = \min\{\Gamma \setminus Z(b)\}$, *com* $\gamma_a \leq \gamma_b$. *Dessa forma,*

$$\nu_t(a+b) = \nu_t\left(\sum_{\gamma \geq \gamma_a}(a_\gamma + b_\gamma)t^\gamma\right).$$

Se $a_{\gamma_a} + b_{\gamma_a} = 0$, *então* $\nu_t(a+b) > \gamma_a$. *Agora, se* $a_{\gamma_a} + b_{\gamma_a} \neq 0$ *então* $\nu_t(a+b) = \gamma_a$. *Assim,*

$$\nu_t(a+b) \geq \gamma_a = \min\{\nu_t(a), \nu_t(b)\}.$$

Se $a = 0$ *ou* $b = 0$, *digamos* $a = 0$, *então segue que* $\nu_t(a+b) = \nu_t(b) \geq \nu_t(b) = \min\{\infty, \nu_t(b)\} = \min\{\nu_t(a), \nu_t(b)\}$.

- $(V3)$ *Temos* $\nu_t(1) = 0$ *e, por definição,* $\nu_t(0) = \infty$.

O grupo de valores de ν_t *é* Γ. *Em particular, quando* $\Gamma = \mathbb{Z}$, *temos que* ν_t *é uma valorização no corpo* $\mathbb{K}((x))$ *das séries de Laurent.*

▼

Exemplo C.11. *Considerando a valorização* ν_t *no corpo* $\mathbb{K}((t^\Gamma))$, *que possui como grupo de valores* Γ, *sejam* $\Gamma_< = \{\gamma \in \Gamma \mid \gamma < 0\}$ *e* $\Gamma_\leq = \{\gamma \in \Gamma \mid \gamma \leq 0\}$. *O anel de valorização associado a* ν_t *é o conjunto*

$$\mathcal{O}_{\nu_t} = \{a \in \mathbb{K}((t^\Gamma)) \mid \Gamma_< \subseteq Z(a)\}.$$

Ainda,

$$\mathfrak{m}_{\nu_t} = \{a \in \mathbb{K}((t^\Gamma)) \mid \Gamma_\leq \subseteq Z(a)\}.$$

O corpo de resíduos de ν_t *é isomorfo a* $\mathbb{K}$. *De fato, todo elemento* $a \in \mathcal{O}_{\nu_t}$ *pode ser escrito como* $a_0 t^0 + b$, *com* $b \in \mathfrak{m}_{\nu_t}$. *A aplicação* $a \longmapsto a_0$ *é um homomorfismo sobrejetor de* $\mathcal{O}_{\nu_t}$ *em* $\mathbb{K}$ *com núcleo igual a* $\mathfrak{m}_{\nu_t}$. *Pelo Teorema do Isomorfismo,*

$$\frac{\mathcal{O}_{\nu_t}}{\mathfrak{m}_{\nu_t}} \cong \mathbb{K}.$$

Esse exemplo nos mostra que é sempre possível construir uma valorização com grupo de valores e corpo de resíduos pré-determinados.

▼

Exemplo C.12. *Sejam $\mathcal{R}$ e $\mathcal{D}$ anéis e um homomorfismo $\psi : \mathcal{R} \longrightarrow \mathcal{D}$. Consideremos ν' uma valorização em $\mathcal{D}$. Então, a aplicação $\nu(a) := \nu'(\psi(a))$ é uma valorização em $\mathcal{R}$. Além disso, se ν' é de Krull, então* $\mathrm{supp}(\nu) = \ker(\psi)$. *De fato:*

- $(V1)$ *Para $a, b \in \mathcal{R}$,*

$$\begin{aligned}\nu(ab) &= \nu'(\psi(ab)) \\ &= \nu'(\psi(a)\psi(b)) \\ &= \nu'(\psi(a)) + \nu'(\psi(b)) \\ &= \nu(a) + \nu(b).\end{aligned}$$

- $(V2)$ *Para $a, b \in \mathcal{R}$,*

$$\begin{aligned}\nu(a+b) &= \nu'(\psi(a+b)) \\ &= \nu'(\psi(a) + \psi(b)) \\ &\geq \min\{\nu'(\psi(a)), \nu'(\psi(b))\} \\ &= \min\{\nu(a), \nu(b)\}.\end{aligned}$$

- $(V3)$ *Temos $\nu(1) = \nu'(\psi(1)) = \nu'(1) = 0$ e $\nu(0) = \nu'(\psi(0)) = \nu'(0) = \infty$.*
- *Suponhamos que ν' é de Krull. Vejamos que* $\mathrm{supp}(\nu) = \ker(\psi)$. *Se $a \in \mathrm{supp}(\nu)$, então*

$$\begin{aligned}\nu(a) = \infty &\iff \nu'(\psi(a)) = \infty \\ &\iff \psi(a) \in \mathrm{supp}(\nu') = \{0\} \\ &\iff \psi(a) = 0.\end{aligned}$$

Logo, $a \in \mathrm{supp}(\nu)$ se, e somente e, $a \in \ker(\psi)$, mostrando a igualdade entre os conjuntos.

▼

Exemplo C.13. *Seja $\mathbb{K}$ um corpo de característica positiva p. Seja $\mathbb{L} = \mathbb{K}(t)^{\frac{1}{p^\infty}}$ o seguinte subcorpo de $\mathbb{K}((t^{\mathbb{Q}}))$:*

$$\mathbb{K}(t)^{\frac{1}{p^\infty}} := \{b \in \mathbb{K}((t^{\mathbb{Q}})) \mid b^{p^n} \in \mathbb{K}(t) \text{ para algum } n \in \mathbb{N}_0\}.$$

Este corpo é chamado ***envoltória perfeita*** *de $\mathbb{K}(t)$ em $\mathbb{K}((t^{\mathbb{Q}}))$. Consideremos o anel $\mathcal{R} = \mathbb{L}[x]$ e um homomorfismo $\psi : \mathcal{R} \longrightarrow \mathbb{K}((t^{\mathbb{Q}}))$ que leva x em um elemento fixado*

$a \in \mathbb{K}((t^{\mathbb{Q}})) \setminus \mathbb{L}$. Pelo que vimos no exemplo anterior, ψ e a valorização t-ádica de $\mathbb{K}((t^{\mathbb{Q}}))$ induzem uma valorização ν em $\mathbb{L}[x]$.

Por exemplo, seja

$$a = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{\infty} t^{i-\frac{1}{p^j}} \right) = t^{-1} + t^{-\frac{1}{p}} + t^{-\frac{1}{p^2}} + \ldots + 1 + t^{1-\frac{1}{p}} + t^{1-\frac{1}{p^2}} + \ldots \in \mathbb{K}((t^{\mathbb{Q}})) \setminus \mathbb{L}.$$

Dessa forma,

$$\begin{aligned} \nu\left(x - \sum_{i=0}^{n-1} t^{-\frac{1}{p^i}} \right) &= \nu_t \left(a - \sum_{i=0}^{n-1} t^{-\frac{1}{p^i}} \right) \\ &= \nu_t(a - t^{-1} - t^{-\frac{1}{p}} - \ldots - t^{-\frac{1}{p^{n-1}}}) \\ &= \nu_t(t^{-\frac{1}{p^n}} + t^{-\frac{1}{p^{n+1}}} + \ldots + 1 + t^{1-\frac{1}{p}} + t^{1-\frac{1}{p^2}} + \ldots) \\ &= -\frac{1}{p^n}. \end{aligned}$$

▼

Exemplo C.14. *Seja $\mathbb{F}$ um corpo finito com m elementos. Olhando para o grupo multiplicativo $\mathbb{F}^\times$, este possui ordem $m-1$. Pelo Teorema de Lagrange, a ordem de qualquer elemento $a \in \mathbb{F}^\times$ divide $m-1$. Logo $a^{m-1} = 1$ para todo $a \in \mathbb{F}^\times$ (esta é a versão do Pequeno Teorema de Fermat para corpos finitos). Dessa forma, qualquer valorização em um corpo finito $\mathbb{F}$ é trivial. De fato, para qualquer que seja ν valorização em $\mathbb{F}$ e para todo $a \in \mathbb{F}^\times$, temos $a^{m-1} = 1$ e, portanto, $\nu(a) = 0$.*

Mais geralmente, seja $\mathbb{E}$ uma extensão algébrica de um corpo finito $\mathbb{F}$ e ν uma valorização em $\mathbb{E}$. Para todo $a \in \mathbb{E}$, temos que $\mathbb{F}(a)$ é um corpo finito. Logo, $\nu(a) = 0$. Assim, concluímos que toda valorização em $\mathbb{E}$ é trivial.

▼

Apêndice D

Extensões e prolongamentos de valorizações

Neste apêndice estudaremos as propriedades das extensões e dos prolongamentos de valorizações/anéis de valorização.

Na primeira seção, veremos, através do Teorema de Chevalley, que sempre é possível prolongar um anel de valorização de um corpo para uma extensão qualquer deste, bem como algumas propriedades desses prolongamentos. Na segunda seção provaremos que toda valorização admite uma extensão. Na terceira seção, estudaremos alguns invariantes associados a esses prolongamentos. Veremos na quarta seção certos comportamentos desses prolongamentos quando as extensões de corpos são algébricas e, na quinta seção, conheceremos uma desigualdade muito importante no estudo das valorização transcendentes. Por fim, na sexta seção daremos caracterizações dos prolongamentos de uma valorização em termos de composições com certos automorfismos.

As principais referências para a composição deste apêndice foram os trabalhos de Engler e Prestel (2005) e Kuhlmann (20??a, 20??b).

D.1 Teorema de Chevalley

Seja $\mathbb{K}_2$ extensão de $\mathbb{K}_1$ e $\mathcal{O}_i \subseteq \mathbb{K}_i$ anéis de valorização, com $i = 1, 2$. Diremos que $\mathcal{O}_2$ é um **prolongamento** de $\mathcal{O}_1$ se $\mathcal{O}_2 \cap \mathbb{K}_1 = \mathcal{O}_1$. Podemos dizer também que $\mathcal{O}_2$ **prolonga** $\mathcal{O}_1$. A notação $(\mathbb{K}_1, \mathcal{O}_1) \subseteq (\mathbb{K}_2, \mathcal{O}_2)$ indica que $\mathbb{K}_1 \subseteq \mathbb{K}_2$ e $\mathcal{O}_2$ prolonga $\mathcal{O}_1$. Se $\mathfrak{m}_i$ é o ideal maximal de $\mathcal{O}_i$ e $\mathcal{O}_2$ prolonga $\mathcal{O}_1$, então $\mathfrak{m}_2 \cap \mathbb{K}_1 = \mathfrak{m}_2 \cap \mathcal{O}_1 = \mathfrak{m}_1$ e $\mathcal{O}_2^\times \cap \mathbb{K}_1 = \mathcal{O}_2^\times \cap \mathcal{O}_1 = \mathcal{O}_1^\times$.

Em termos de aplicações, tomando uma valorização ν_1 em $\mathbb{K}_1$ e uma valorização ν_2 em $\mathbb{K}_2$, temos que $(\mathbb{K}_1, \nu_1) \subseteq (\mathbb{K}_2, \nu_2)$ indica que $\mathbb{K}_1 \subseteq \mathbb{K}_2$ e $\nu_2|_{\mathbb{K}_1} \sim \nu_1$. Isto é, existe um isomorfismo ϕ entre os grupos $\Gamma_{\nu_2|_{\mathbb{K}_1}}$ e Γ_{ν_1}, que preserva a ordem, tal que $\nu_2|_{\mathbb{K}_1} = \phi \circ \nu_1$. Nesta situação, diremos que ν_2 é um **prolongamento** de ν_1, ou ainda que ν_2 **prolonga** ν_1. Quando $\nu_2|_{\mathbb{K}_1} = \nu_1$, diremos que ν_2 é uma **extensão** de ν_1, ou ainda que ν_2 **estende** ν_1.

O primeiro teorema desta seção, o Teorema de Chevalley, nos permitirá concluir que prolongamentos de anéis de valorização sempre existem, independente da natureza da extensão de corpos.

Lema D.1. *Seja $\mathcal{S}$ um subanel de um corpo $\mathbb{K}$ e seja $\mathfrak{i}$ um ideal próprio de $\mathcal{S}$. Para cada $c \in \mathbb{K}$, temos que $\mathcal{S}[c]\mathfrak{i}$ é um ideal próprio do anel $\mathcal{S}[c]$ ou $\mathcal{S}[c^{-1}]\mathfrak{i}$ é um ideal próprio do anel $\mathcal{S}[c^{-1}]$.*

Demonstração: Suponhamos

$$\mathcal{S}[c]\mathfrak{i} = \mathcal{S}[c] \text{ e } \mathcal{S}[c^{-1}]\mathfrak{i} = \mathcal{S}[c^{-1}].$$

Existem $a_0, \ldots, a_n, b_0, \ldots, b_m \in \mathfrak{i}$ tais que

$$1 = \sum_{i=0}^{n} a_i c^i \text{ e } 1 = \sum_{i=0}^{m} b_i c^{-i}.$$

com n e m minimais, isto é, $a_n \neq 0$, $a_j = 0$ para $j > n$ e n é o menor número natural com estas propriedades (análogo para b_m). Suponhamos que $m \leq n$. Multiplicando a equação à esquerda por $1 - b_0$ e a equação à direita por $a_n c^n$, obtemos

$$1 - b_0 = \sum_{i=0}^{n} (1 - b_0) a_i c^i \text{ e}$$

$$(1 - b_0) a_n c^n = \sum_{i=1}^{m} a_n b_i c^{n-i}.$$

Dessa forma,

$$1 = b_0 + \sum_{i=0}^{n-1} (1 - b_0) a_i c^i + \sum_{i=1}^{m} a_n b_i c^{n-i} = \sum_{i=0}^{n-1} c_i c^i.$$

Os coeficientes no lado direito da equação são todos elementos de $\mathfrak{i}$. Assim, encontramos uma forma de escrever 1 em $\mathcal{S}[c]\mathfrak{i}$ de modo que a maior potência de c na expressão é no máximo $n - 1$, contradizendo a minimalidade de n. Portanto, no caso em que $m \leq n$, devemos ter $\mathcal{S}[c]\mathfrak{i} \neq \mathcal{S}[c]$ ou $\mathcal{S}[c^{-1}]\mathfrak{i} \neq \mathcal{S}[c^{-1}]$. A prova é análoga quando $n < m$.

■

Proposição D.2. *Seja $\mathcal{S}$ um subanel do corpo $\mathbb{K}$ e seja $\mathfrak{i}$ um ideal próprio de $\mathcal{S}$. Então existe um anel de valorização $\mathcal{O}$ de $\mathbb{K}$ tal que $\mathcal{S} \subset \mathcal{O}$ e o ideal maximal $\mathfrak{m}$ contém $\mathfrak{i}$.*

Demonstração: Consideremos o conjunto

$$\Omega = \{\mathcal{S}' \subseteq \mathbb{K} \mid \mathcal{S}' \text{ é subanel de } \mathbb{K}, \mathcal{S} \subseteq \mathcal{S}' \text{ e } \mathcal{S}'\mathfrak{i} \neq \mathcal{S}'\}.$$

Temos $\Omega \neq \emptyset$, uma vez que $\mathcal{S} \in \Omega$. Ainda, Ω pode ser parcialmente ordenado. De fato, para cada $\mathcal{S}'_j \in \Omega$ $(j = 1, 2)$ diremos que

$$\mathcal{S}'_1 \leq \mathcal{S}'_2 \iff \mathcal{S}'_1 \subseteq \mathcal{S}'_2$$

Dada uma cadeia qualquer $\{\mathcal{S}'_j \mid j \in J\} \subset \Omega$, isto é, um subconjunto totalmente ordenado, temos que

$$\mathcal{S}'_0 = \bigcup_{j \in J} \mathcal{S}'_j$$

é um anel. Temos $\mathcal{S} \subset \mathcal{S}'_0$. Agora suponhamos $\mathcal{S}'_0\mathfrak{i} = \mathcal{S}'_0$. Existem elementos $s_1, \ldots, s_n \in \mathcal{S}'_0$ e $a_1, \ldots a_n \in \mathfrak{i}$ tais que

$$\sum_{i=1}^{n} s_i a_i = 1.$$

Mas, uma vez que $\mathcal{S}'_0$ é uma união de conjuntos totalmente ordenados, existe um anel $\mathcal{S}' \in \{\mathcal{S}'_j \mid j \in J\}$ que contém todos os s_i, donde concluímos que $\mathcal{S}'\mathfrak{i} = \mathcal{S}'$. Isso contradiz $\mathcal{S}' \in \Omega$. Dessa forma, $\mathcal{S}'_0\mathfrak{i} \neq \mathcal{S}'_0$ e $\mathcal{S}'_0 \in \Omega$.

Como qualquer cadeia possui limitante superior, pelo Lema de Zorn temos que Ω possui um elemento maximal, que chamaremos de $\mathcal{O}$. Temos $\mathcal{S} \subset \mathcal{O}$ e $\mathcal{O}\mathfrak{i} \neq \mathcal{O}$. Mostremos que $\mathcal{O}$ é um anel de valorização. Seja $c \in \mathbb{K}$ e suponhamos $c, c^{-1} \notin \mathcal{O}$. Assim, $\mathcal{O} \subsetneq \mathcal{O}[c]$ e $\mathcal{O} \subsetneq \mathcal{O}[c^{-1}]$. Pelo Lema D.1, segue que $\mathcal{O}[c]\mathfrak{i}$ é um ideal próprio do anel $\mathcal{O}[c]$ ou $\mathcal{O}[c^{-1}]\mathfrak{i}$ é um ideal próprio do anel $\mathcal{O}[c^{-1}]$. Portanto, $\mathcal{O}[c] \in \Omega$ ou $\mathcal{O}[c^{-1}] \in \Omega$, contradizendo a maximalidade de $\mathcal{O}$. Dessa forma, $\mathcal{O}$ é um anel de valorização. Como $\mathfrak{m}$ é o único ideal maximal de $\mathcal{O}$, ele deve conter o ideal próprio $\mathcal{O}\mathfrak{i}$ e, em particular, $\mathfrak{i} \subset \mathfrak{m}$.

■

Teorema D.3. *(Teorema de Chevalley) Para um corpo $\mathbb{K}$, seja $\mathcal{S} \subseteq \mathbb{K}$ um subanel e seja $\mathfrak{p}$ um ideal primo de $\mathcal{S}$. Então existe um anel de valorização $\mathcal{O}$ de $\mathbb{K}$ tal que*

$$\mathcal{S} \subseteq \mathcal{O} \text{ e } \mathfrak{m} \cap \mathcal{S} = \mathfrak{p},$$

em que $\mathfrak{m}$ é o ideal maximal de $\mathcal{O}$.

Demonstração: Seja $\mathcal{S}_\mathfrak{p}$ a localização de $\mathcal{S}$ em $\mathfrak{p}$ com único ideal maximal

$$\mathfrak{p}\mathcal{S}_\mathfrak{p} = \left\{ \frac{a}{s} \mid a \in \mathfrak{p}, s \notin \mathfrak{p} \right\}.$$

Temos $\mathfrak{p}\mathcal{S}_\mathfrak{p} \cap \mathcal{S} = \mathfrak{p}$. De fato, a inclusão $\mathfrak{p}\mathcal{S}_\mathfrak{p} \cap \mathcal{S} \supseteq \mathfrak{p}$ segue de $\mathcal{S} \subseteq \mathcal{S}_\mathfrak{p}$. Suponhamos, buscando uma contradição, $\mathfrak{p}\mathcal{S}_\mathfrak{p} \cap \mathcal{S} \not\subset \mathfrak{p}$. Com isso, $\mathfrak{p}\mathcal{S}_\mathfrak{p}$ conteria um elemento de $\mathcal{S} \setminus \mathfrak{p}$. Porém, este elemento é invertível em $\mathcal{S}_\mathfrak{p}$, o que contradiz $\mathfrak{p}\mathcal{S}_\mathfrak{p}$ ser ideal maximal. Logo, segue a igualdade $\mathfrak{p}\mathcal{S}_\mathfrak{p} \cap \mathcal{S} = \mathfrak{p}$.

Pela Proposição D.2, existe um anel de valorização $\mathcal{O} \supset \mathcal{S}_\mathfrak{p} \supset \mathcal{S}$ tal que o ideal maximal $\mathfrak{m} \subset \mathcal{O}$ contém $\mathfrak{p}\mathcal{S}_\mathfrak{p}$. Como $\mathcal{S}_\mathfrak{p} \setminus \mathfrak{p}\mathcal{S}_\mathfrak{p}$ somente contém unidades e $\mathfrak{m}$ é maximal, segue que $\mathfrak{m} \cap \mathcal{S}_\mathfrak{p} = \mathfrak{p}\mathcal{S}_\mathfrak{p}$. Logo, $\mathfrak{m} \cap \mathcal{S} = \mathfrak{m} \cap (\mathcal{S}_\mathfrak{p} \cap \mathcal{S}) = \mathfrak{p}\mathcal{S}_\mathfrak{p} \cap \mathcal{S} = \mathfrak{p}$.

■

Teorema D.4. *Seja $\mathbb{K}_2$ uma extensão do corpo $\mathbb{K}_1$ e seja $\mathcal{O}_1 \subseteq \mathbb{K}_1$ um anel de valorização. Então existe um prolongamento $\mathcal{O}_2$ de $\mathcal{O}_1$ em $\mathbb{K}_2$.*

Demonstração: Como $\mathcal{O}_1$ é um subanel de $\mathbb{K}_2$, pelo Teorema de Chevalley existe um anel de valorização $\mathcal{O}_2$ em $\mathbb{K}_2$ com $\mathcal{O}_1 \subseteq \mathcal{O}_2$ e tal que os ideais maximais satisfazem $\mathfrak{m}_2 \cap \mathcal{O}_1 = \mathfrak{m}_1$. Como $\mathcal{O}_2 \cap \mathbb{K}_1$ e $\mathcal{O}_1$ são anéis de valorização com o mesmo ideal maximal, estes devem coincidir. De fato, se fossem distintos, então existiria uma unidade $a \in \mathcal{O}_2 \cap \mathbb{K}_1 \setminus \mathfrak{m}_2 \cap \mathcal{O}_1$ tal que $a \notin \mathcal{O}_1$. Mas, com isso teríamos $a^{-1} \in \mathcal{O}_1$ e concluiríamos que $a^{-1} \in \mathfrak{m}_1 = \mathfrak{m}_2 \cap \mathcal{O}_1$, contradizendo o fato de a ser uma unidade.

■

De maneira imediata, temos o seguinte corolário.

Corolário D.5. *Seja $\mathbb{K}_2$ uma extensão do corpo $\mathbb{K}_1$ e seja ν_1 uma valorização em $\mathbb{K}_1$. Então existe uma valorização ν_2 em $\mathbb{K}_2$ tal que $\nu_2|_{\mathbb{K}_1} \sim \nu_1$.*

Demonstração: Seja $\mathcal{O}_1 = \mathcal{O}_{\nu_1}$ o anel de valorização associado a ν_1. Pelo Teorema D.4, existe $\mathcal{O}_2 \subseteq \mathbb{K}_2$ anel de valorização que prolonga $\mathcal{O}_{\nu_1}$. Seja ν_2 a valorização definida por $\mathcal{O}_2$, cujo anel de valorização é $\mathcal{O}_{\nu_2} = \mathcal{O}_2$. Então, $\nu_2|_{\mathbb{K}}$ possui como anel de valorização $\mathcal{O}_{\nu_2} \cap \mathbb{K} = \mathcal{O}_{\nu_1}$. Ou seja, $\nu_2|_{\mathbb{K}_1} \sim \nu_1$.

■

Fecharemos esta seção trazendo propriedades dos prolongamentos de um dado anel de valorização que serão úteis nas próximas seções.

Lema D.6. *Suponhamos $\mathcal{O}_1, \ldots, \mathcal{O}_r$ anéis de valorização de um corpo $\mathbb{K}$ com ideias maximais $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$, respectivamente. Sejam*

$$\mathcal{R} := \bigcap_{i=1}^{r} \mathcal{O}_i \text{ e } \mathfrak{p}_i := \mathcal{R} \cap \mathfrak{m}_i.$$

Então, para cada i, $1 \leq i \leq r$, temos $\mathcal{O}_i = \mathcal{R}_{\mathfrak{p}_i}$

Demonstração: Mostremos as duas inclusões. Inicialmente, temos

$$\mathcal{R}_{\mathfrak{p}_i} = \left\{ \frac{a}{b} \mid a \in \mathcal{R} \text{ e } b \in \mathcal{R} \setminus \mathfrak{p}_i \right\} = \left\{ \frac{a}{b} \mid a, b \in \bigcap_{i=1}^{r} \mathcal{O}_i \text{ e } b \notin \mathfrak{m}_i \right\} \subseteq$$

$$\subseteq \left\{ \frac{a}{b} \mid a, b \in \mathcal{O}_i \text{ e } b \notin \mathfrak{m}_i \right\} = \left\{ \frac{a}{b} \mid a \in \mathcal{O}_i \text{ e } b \in \mathcal{O}_i^{\times} \right\} = \mathcal{O}_i.$$

Para a outra inclusão, sejam $a \in \mathcal{O}_i$ e $I_a = \{j \mid a \in \mathcal{O}_j\}$. Escrevemos $\alpha_j = a + \mathfrak{m}_j \in \overline{\mathbb{K}}_j$ para cada $j \in I_a$. Escolhemos $p \in \mathbb{N}$ primo tal que, para cada $j \in I_a$, temos $p > \text{char}(\overline{\mathbb{K}}_j)$ e α_j não seja uma raiz primitiva p-ésima de 1. Definimos $b = 1 + a + \ldots + a^{p-1}$. Observamos que

$$\alpha_j = 1 \Rightarrow \overline{b} = \overline{1} + \overline{1} + \ldots + \overline{1} = \overline{p} \neq \overline{0} \text{ em } \overline{\mathbb{K}}_j \text{ e}$$

$$\alpha_j \neq 1 \Rightarrow \overline{b} = \overline{(1 - \alpha_j^p)(1 - \alpha_j)^{-1}} \neq \overline{0} \text{ em } \overline{\mathbb{K}}_j.$$

Portanto, $b \in \mathcal{O}_j^{\times}$ para todo $j \in I_a$. Assim, para $j \in \{1, \ldots, r\} \setminus I_a$, temos $a \notin \mathcal{O}_j$, ou seja, $a^{-1} \in \mathfrak{m}_j$. Vejamos que

$$1 + a^{-1} + \ldots + a^{-(p-1)} \in \mathcal{O}_j^{\times}.$$

De fato, suponhamos, buscando uma contradição, $1 + a^{-1} + \ldots + a^{-(p-1)} \in \mathfrak{m}_j$. Logo, teríamos $(1 - a^{-p})(1 - a^{-1})^{-1} \in \mathfrak{m}_j$. Com isso, $1 - a^{-p} \in \mathfrak{m}_j$ ou $(1 - a^{-1})^{-1} \in \mathfrak{m}_j$. Sabemos que $a^{-1} \in \mathfrak{m}_j$ implica $a^{-p} \in \mathfrak{m}_j$. Assim, se $1 - a^{-p} \in \mathfrak{m}_j$, então $1 - a^{-p} + a^{-p} \in \mathfrak{m}_j$, o que é uma contradição. Agora, se $(1 - a^{-1})^{-1} \in \mathfrak{m}_j$, então $1 - a^{-1} \notin \mathcal{O}_j$. Porém, $1 \in \mathcal{O}_j$ e $a^{-1} \in \mathcal{O}_j$, logo $1 - a^{-1} \notin \mathcal{O}_j$ é uma contradição. Portanto, devemos ter $1 + a^{-1} + \ldots + a^{-(p-1)} \in \mathcal{O}_j^{\times}$. Com cálculos diretos, vemos que

$$b^{-1} = a^{-(p-1)}(1 + a^{-1} + \ldots + a^{-(p-1)})^{-1} = a^{-(p-1)} \left(\frac{1 - a^{-p}}{1 - a^{-1}} \right)^{-1} \in \mathcal{O}_j.$$

Assim,

$$ab^{-1} = a^{-(p-2)}(1 + a^{-1} + \ldots + a^{-(p-1)})^{-1} \in \mathcal{O}_j.$$

Portanto, para todo j, com $1 \leq j \leq r$, temos ambos $b^{-1}, ab^{-1} \in \mathcal{O}_j$. Ou seja, $b^{-1}, ab^{-1} \in \mathcal{R}$ e $b^{-1} \notin \mathfrak{m}_i \cap \mathcal{R} = \mathfrak{p}_i$, pois $b \in \mathcal{O}_i^{\times}$. Logo, $a = ab^{-1}/b^{-1} \in \mathcal{R}_{\mathfrak{p}_i}$.

■

Teorema D.7. *Suponhamos $\mathcal{O}_1, \ldots, \mathcal{O}_r$ anéis de valorização de um corpo $\mathbb{K}$ com ideais maximais $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$. Seja*

$$\mathcal{R} := \bigcap_{i=1}^{r} \mathcal{O}_i \text{ e } \mathfrak{p}_i := \mathcal{R} \cap \mathfrak{m}_i.$$

Suponhamos $\mathcal{O}_i \not\subseteq \mathcal{O}_j$ para $i \neq j$. As seguintes afirmações são satisfeitas.

1. *Vale $\mathfrak{p}_1 \not\subset \mathfrak{p}_j$ para $i \neq j$,*
2. *Temos que $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ é o conjunto de todos os ideais maximais de $\mathcal{R}$.*
3. *Para cada r-upla $(a_1, \ldots, a_r) \in \mathcal{O}_1 \times \cdots \times \mathcal{O}_r$, existe $a \in \mathcal{R}$ tal que $a - a_i \in \mathfrak{m}_i$.*

Demonstração:

1. Pelo Lema D.6, se $\mathfrak{p}_i \subseteq \mathfrak{p}_j$, então $\mathcal{O}_j = \mathcal{R}_{\mathfrak{p}_j} \subseteq \mathcal{R}_{\mathfrak{p}_i} = \mathcal{O}_i$. Logo, se $i \neq j$, então $\mathfrak{p}_i \not\subset \mathfrak{p}_j$.

2. Mostremos que todo ideal $\mathfrak{a} \neq \mathcal{R}$ está contido em algum $\mathfrak{p}_i$. Suponhamos, buscando uma contradição, que existe um ideal $\mathfrak{a} \neq \mathcal{R}$ tal que para todo i, $1 \leq i \leq r$, existe $a_i \in \mathfrak{a} \setminus \mathfrak{p}_i$. Para cada $j \neq i$, existe $b_{ij} \in \mathfrak{p}_i \setminus \mathfrak{p}_j$. Então o elemento

$$c_j := \prod_{j \neq i} b_{ij}$$

é tal que $c_j \in \mathfrak{p}_i \setminus \mathfrak{p}_j$ para todo $i \neq j$. Assim, $a_j c_j \in \mathfrak{p}_i$ para todo $i \neq j$ e $a_j c_j \notin \mathfrak{p}_j$ para todo j, $1 \leq j \leq n$. Portanto,

$$d = \sum_{j=1}^{r} a_j c_j \notin \mathfrak{p}_i \text{ para todo } i,\ 1 \leq i \leq r.$$

Para visualizarmos isso, peguemos por exemplo $\mathfrak{p}_1$. Como $a_j c_j \in \mathfrak{p}_1$ para todo j, $2 \leq j \leq n$, segue que $a_2 c_2 + \ldots + a_r c_r \in \mathfrak{p}_1$. Se $d \in \mathfrak{p}_1$, então $d - a_2 c_2 + \ldots + a_r c_r \in \mathfrak{p}_1$. Ou seja, $a_1 c_1 \in \mathfrak{p}_1$, o que é uma contradição.

Dessa forma, $d \notin \mathfrak{p}_i = \mathcal{R} \cap \mathfrak{m}_i$. Como $d \in \mathcal{R}$ (pois $a_j \in \mathfrak{a} \subset \mathcal{R}$ e $c_j \in \mathfrak{p}_i \subset \mathcal{R}$), segue que $d \notin \mathfrak{m}_i$. Assim, $d^{-1} \in \mathcal{O}_i$ para cada i, $1 \leq i \leq r$. Por conseguinte, $d^{-1} \in \mathcal{R}$. Como $d \in \mathfrak{a}$, teremos $1 = dd^{-1} \in \mathfrak{a}$, contradizendo $\mathfrak{a} \neq \mathcal{R}$. Portanto, cada ideal próprio de $\mathcal{R}$ está contido em algum $\mathfrak{p}_i$. Dessa forma, se $\mathfrak{p}_j \subseteq \mathfrak{a} \neq \mathcal{R}$, então $\mathfrak{p}_j \subseteq \mathfrak{a} \subseteq \mathfrak{p}_i$. Isso implica $\mathfrak{a} = \mathfrak{p}_i = \mathfrak{p}_j$.

3. Se $i \neq j$, então, pelos itens anteriores, $\mathfrak{p}_i + \mathfrak{p}_j = \mathcal{R}$. Pelo Teorema Chinês dos Restos, temos um isomorfismo

$$\mathcal{R} \longrightarrow \mathcal{R}/\mathfrak{p}_1 \times \ldots \times \mathcal{R}/\mathfrak{p}_r.$$

$$\frac{\mathcal{R}}{\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r} \xrightarrow{\approx} \frac{\mathcal{R}}{\mathfrak{p}_1} \times \cdots \times \frac{\mathcal{R}}{\mathfrak{p}_r}$$
$$a \mod (\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r) \longmapsto (a \mod \mathfrak{p}_1, \ldots, a \mod \mathfrak{p}_r).$$

Para cada i, $1 \leq i \leq r$, vale $\mathcal{R}/\mathfrak{p}_i \cong \mathcal{R}_{\mathfrak{p}_i}/\mathfrak{p}_i\mathcal{R}_{\mathfrak{p}_i}$, em que $\mathfrak{p}_i\mathcal{R}_{\mathfrak{p}_i}$ é o ideal maximal de $\mathcal{R}_{\mathfrak{p}_i}$. Além disso, pelo Lema D.6 temos $\mathcal{R}_{\mathfrak{p}_i} = \mathcal{O}_i$. Ou seja,

$$\frac{\mathcal{R}}{\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r} \xrightarrow{\approx} \frac{\mathcal{O}_1}{\mathfrak{m}_1} \times \cdots \times \frac{\mathcal{O}_r}{\mathfrak{m}_r}$$
$$a \mod (\mathfrak{p}_1 \cap \cdots \cap \mathfrak{p}_r) \longmapsto (a \mod \mathfrak{m}_1, \ldots, a \mod \mathfrak{m}_r).$$

Logo, para cada r-upla $(a_1, \ldots, a_r) \in \mathcal{O}_1 \times \ldots \times \mathcal{O}_r$, existe $a \in \mathcal{R}$ tal que $a_i \mod \mathfrak{m}_i = a \mod \mathfrak{m}_i$ para cada i, $1 \leq i \leq r$.

■

D.2 Índice de ramificação e grau de resíduo

Seja $(\mathbb{K}_1, \mathcal{O}_1) \subseteq (\mathbb{K}_2, \mathcal{O}_2)$ um prolongamento. Para cada $\mathcal{O}_i$ temos uma valorização correspondente $\nu_i : \mathbb{K}_i \to \nu_i\mathbb{K}_i \cup \{\infty\}$, com $i = 1, 2$. A aplicação $\nu_i|_{\mathbb{K}_i^\times} : \mathbb{K}_i^\times \twoheadrightarrow \nu_i\mathbb{K}_i$ é um homomorfismo de grupos com núcleo $\mathcal{O}_i^\times$. Pelo Teorema do Isomorfismo, temos $\mathbb{K}_i^\times/\mathcal{O}_i^\times \cong \nu_i\mathbb{K}_i$.

A composição $\mathbb{K}_1^\times \hookrightarrow \mathbb{K}_2^\times \twoheadrightarrow \nu_2\mathbb{K}_2 \cong \mathbb{K}_2^\times/\mathcal{O}_2^\times$ possui núcleo $\mathcal{O}_2^\times \cap \mathbb{K}_1^\times = \mathcal{O}_1^\times$. Então

$$\nu_1\mathbb{K}_1 \cong \mathbb{K}_1^\times/\mathcal{O}_1^\times \hookrightarrow \mathbb{K}_2^\times/\mathcal{O}_2^\times \cong \nu_2\mathbb{K}_2,$$

donde podemos ver $\nu_1\mathbb{K}_1$ como subgrupo de $\nu_2\mathbb{K}_2$. Chamaremos

$$e = e(\mathcal{O}_2 \mid \mathcal{O}_1) := [\nu_2\mathbb{K}_2 : \nu_1\mathbb{K}_1]$$

de **índice de ramificação** da extensão (denotamos a imagem isomorfa de Γ_1 dentro de Γ_2 também por Γ_1). Seja $\mathfrak{m}_i$ ideal maximal de $\mathcal{O}_i$. A composição $\mathcal{O}_1 \hookrightarrow \mathcal{O}_2 \twoheadrightarrow \mathcal{O}_2/\mathfrak{m}_2 = \mathbb{K}_2\nu_2$ possui núcleo $\mathfrak{m}_2 \cap \mathcal{O}_1 = \mathfrak{m}_1$. Portanto,

$$\mathbb{K}_1\nu_1 = \mathcal{O}_1/\mathfrak{m}_1 \hookrightarrow \mathcal{O}_2/\mathfrak{m}_2 = \mathbb{K}_2\nu_2$$

e assim temos a extensão de corpos $\mathbb{K}_2\nu_2 \mid \mathbb{K}_1\nu_1$. Definimos

$$f = f(\mathcal{O}_2 \mid \mathcal{O}_1) := [\mathbb{K}_2\nu_2 : \mathbb{K}_1\nu_1],$$

que é chamado **grau de resíduo** ou **índice de inércia** da extensão.

Veremos que o índice de inércia e o grau de resíduo sempre são finitos se o grau da extensão de corpos é finito. Antes, provaremos um lema.

Lema D.8. *Suponhamos* $(\mathbb{K}_1, \mathcal{O}_1) \subseteq (\mathbb{K}_2, \mathcal{O}_2)$ *e* $\nu_i : \mathbb{K}_i \to \nu_i\mathbb{K}_i \cup \{\infty\}$ *uma valorização correspondente a* $\mathcal{O}_i$*. Tomemos as coleções* $\{\omega_i\}_{i\in I} \subset \mathcal{O}_2^\times$ *e* $\{\pi_j\}_{j\in J} \subset \mathbb{K}_2^\times$ *tais que*

1. *para qualquer quantidade finita de elementos* $\omega_{i_1}, \ldots, \omega_{i_s} \in \{\omega_i\}_{i\in I}$*,* $s \in \mathbb{N}$*, os resíduos* $\omega_{i_1}\nu_2, \ldots, \omega_{i_s}\nu_2 \in \mathbb{K}_2\nu_2$ *são linearmente independentes sobre* $\mathbb{K}_1\nu_1$ *e*
2. *para qualquer quantidade finita de elementos* $\pi_{j_1}, \ldots, \pi_{j_t} \in \{\pi_j\}_{j\in J}$*,* $t \in \mathbb{N}$*, os valores* $\nu_2(\pi_{j_1}), \ldots, \nu_2(\pi_{j_t})$ *são representantes de classes laterais de* $\nu_2\mathbb{K}_2/\nu_1\mathbb{K}_1$ *de modo que valores com índices distintos representam classes distintas.*

Então $\{\omega_i\pi_j \mid i \in I,\ j \in J\}$ *é um conjunto linearmente independente sobre* $\mathbb{K}_1$*.*

Demonstração: Sejam $s, t \in \mathbb{N}$ e tomemos $\omega_{i_1}, \ldots, \omega_{i_s} \in \{\omega_i\}_{i\in I}$ e $\pi_{j_1}, \ldots, \pi_{j_t} \in \{\pi_j\}_{j\in J}$ quaisquer. Seja $\{a_{ij} \mid 1 \le i \le s,\ 1 \le j \le t\} \subset \mathbb{K}_1$. Suponhamos que nem todos os a_{ij} são nulos. Sejam $K \in \{1, \ldots, s\}$ e $L \in \{1, \ldots, t\}$ tais que

$$\nu_2(a_{KL}\pi_{j_L}) = \min_{\substack{1\le k\le s\\ 1\le l\le t}} \{\nu_2(a_{kl}\pi_{j_l})\}.$$

Vejamos que $\nu_2(a_{KL}\pi_{j_L}) < \nu_2(a_{kl}\pi_{j_l})$ para todo $l \neq L$. De fato, como $\nu_2(a_{KL}\pi_{j_L})$ é o mínimo, com certeza $\nu_2(a_{KL}\pi_{j_L}) \le \nu_2(a_{kl}\pi_{j_l})$. Agora, como $\nu_2(a_{KL}\pi_{j_L}) = \nu_2(a_{KL}) + \nu_2(\pi_{j_L})$, se $\nu_2(a_{KL}\pi_{j_L}) = \nu_2(a_{kl}\pi_{j_l})$ para algum $l \neq L$, então teríamos

$$\nu_2(\pi_{j_L}) - \nu_2(\pi_{j_l}) = \nu_2(a_{kl}) - \nu_2(a_{KL}) \in \nu_1\mathbb{K}_1,$$

contradizendo a segunda hipótese.

Escrevemos

$$z = \sum_{k=1}^{s}\sum_{l=1}^{t} a_{kl}\omega_{i_k}\pi_{j_l}.$$

Temos

$$\nu_2(z) \ge m = \min_{\substack{1\le k\le s\\ 1\le l\le t}} \{\nu_2(a_{kl}\omega_{i_k}\pi_{j_l})\}.$$

Suponhamos, por contradição, que $\nu_2(z) > m$. Dessa forma,

$$\nu_2(z(a_{KL}\pi_{j_L})^{-1}) = \nu_2(z) - \nu_2(a_{KL}\pi_{j_L}) > m - \nu_2(a_{KL}\pi_{j_L}) \ge 0,$$

o que implica $z(a_{KL}\pi_{j_L})^{-1} \in \mathfrak{m}_2$. Ainda, $a_{kl}\pi_{j_L}(a_{KL}\pi_{j_L})^{-1} \in \mathfrak{m}_2$ para todo $l \neq L$, pois $\nu_2(a_{kl}\pi_{j_l}(a_{KL}\pi_{j_L})^{-1}) = \nu_2(a_{kl}\pi_{j_l}) - \nu_2(a_{KL}\pi_{j_L}) > 0$.

Portanto,

$$\sum_{k=1}^{s} a_{kL}a_{KL}^{-1}\omega_{i_k} = z(a_{KL}\pi_{j_L})^{-1} - \sum_{k=1}^{s}\sum_{\substack{l=1\\ l\neq L}}^{t} a_{kl}\omega_{i_k}\pi_{j_l}(a_{KL}\pi_{j_L})^{-1} \in \mathfrak{m}_2,$$

o que implica

$$\sum_{k=1}^{s}(a_{kL}a_{KL}^{-1}\omega_{i_k})\nu_2 = 0 \text{ em } \mathbb{K}_2\nu_2,$$

contradizendo a primeira hipótese. Logo $\nu_2(z) = \min\limits_{\substack{1\leq k\leq s\\ 1\leq l\leq t}}\{\nu_2(a_{kl}\omega_{i_k}\pi_{j_l})\}$.

Assim, se

$$z = \sum_{k=1}^{s}\sum_{l=1}^{t} a_{kl}\omega_{i_k}\pi_{j_l} = 0,$$

então $\infty = \nu_2(z) = \min\limits_{\substack{1\leq k\leq s\\ 1\leq l\leq t}}\{\nu_2(a_{kl}\omega_{i_k}\pi_{j_l})\}$, o que implica

$$\nu_2(a_{kl}\omega_{i_k}\pi_{j_l}) = \nu_2(a_{kl}) + \nu_2(\omega_{i_k}) + \nu_2(\pi_{j_l}) = \infty$$

para todo $k \in \{1,\ldots,s\}$ e $l \in \{1,\ldots,t\}$. Porém, sabemos pelas hipóteses que $\{\omega_i\}_{i\in I} \subset \mathcal{O}_2^{\times}$. Logo, $\nu_2(\omega_{i_k}) = 0$ para todo k. Também pelas hipóteses sabemos que os valores $\nu_2(\pi_{j_1}),\ldots,\nu_2(\pi_{j_t})$ são representantes de classes laterais de $\nu_2\mathbb{K}_2/\nu_1\mathbb{K}_1$. Logo, estes pertencem a $\nu_2\mathbb{K}_2$. Com isso, a única forma de termos $\nu_2(a_{kl}) + \nu_2(\omega_{i_k}) + \nu_2(\pi_{j_l}) = \infty$ é se $\nu_2(a_{kl}) = \infty$ para todo a_{kl}. Como a valorização em um corpo é Krull, isso implicaria que todos os elementos a_{kl} são nulos, o que é uma contradição. Portanto, $\{\omega_i\pi_j \mid i \in I,\ j \in J\}$ é um conjunto linearmente independente sobre $\mathbb{K}_1$.

■

Teorema D.9. *Suponhamos* $(\mathbb{K}_1,\mathcal{O}_1) \subseteq (\mathbb{K}_2,\mathcal{O}_2)$ *e seja* $n = [\mathbb{K}_2 : \mathbb{K}_1]$, $e = e(\mathcal{O}_2 \mid \mathcal{O}_1)$, $f = f(\mathcal{O}_2 \mid \mathcal{O}_1)$. *Se* n *é finito, então ambos o índice de ramificação e o grau de resíduo são finitos e*

$$ef \leq n.$$

Demonstração: Sejam I, J conjuntos de índices tais que $|I| = f$ e $|J| = e$. Pelo Lema D.8, o conjunto $\{\omega_i\pi_j \mid i \in I, j \in J\}$ (com ω_i e π_j são tomados satisfazendo as hipóteses do lema) é linearmente independente sobre $\mathbb{K}_1$. Como n é a dimensão de $\mathbb{K}_2$ sobre $\mathbb{K}_1$, seque que $|\{\omega_i\pi_j \mid i \in I\, j \in J\}| \leq n$. Assim, e e f devem ser finitos. Mais ainda, $|\{\omega_i\pi_j \mid i \in I\, j \in J\}| = ef$ e segue que $ef \leq n$.

■

D.3 Valorizações em extensões algébricas de corpos

Nesta seção focaremos no caso em que $\mathbb{L} \mid \mathbb{K}$ é uma extensão algébrica. Veremos uma condição para se ter unicidade no prolongamento de um anel de valorização e veremos alguns dos resultados deste apêndice em ação em um exemplo.

Proposição D.10. *Seja $(\mathbb{K}, \mathcal{O}_\mathbb{K}) \subseteq (\mathbb{L}, \mathcal{O}_\mathbb{L})$ um prolongamento com $\mathbb{L}$ algébrico sobre $\mathbb{K}$. Sejam ν e μ valorizações associadas a $\mathcal{O}_\mathbb{K}$ e a $\mathcal{O}_\mathbb{L}$ com grupos de valores $\nu\mathbb{K}$ e $\mu\mathbb{L}$ e corpos de resíduos $\mathbb{K}\nu$ e $\mathbb{L}\mu$, respectivamente. Denotamos a imagem isomorfa de $\nu\mathbb{K}$ em $\mu\mathbb{L}$ também por $\nu\mathbb{K}$.*

1. *Para todo $\gamma \in \mu\mathbb{L}$ existe $m \in \mathbb{N}$ tal que $m\gamma \in \nu\mathbb{K}$, isto é, $\mu\mathbb{L}/\nu\mathbb{K}$ é um grupo de torção.*
2. *O corpo de resíduos $\mathbb{L}\mu$ é uma extensão algébrica de $\mathbb{K}\nu$.*

Demonstração:

1. Sejam $\gamma \in \mu\mathbb{L}$ qualquer e $a \in \mathbb{L}$ tal que $\mu(a) = \gamma \in \mu\mathbb{L}$. Consideremos $\mathbb{K}(a) \supseteq \mathbb{K}$, $\mathcal{O} = \mathcal{O}_\mathbb{L} \cap \mathbb{K}(a)$ e $\mu' = \mu|_{\mathbb{K}(a)}$. Seja $\Gamma \subseteq \mu\mathbb{L}$ o grupo gerado por $\mu'(\mathbb{K}(a))$. Então $\nu\mathbb{K} \subseteq \Gamma$. Como a é algébrico sobre $\mathbb{K}$, segue que $[\mathbb{K}(a) : \mathbb{K}] < \infty$. Pelo Teorema D.9, $\Gamma/\nu\mathbb{K}$ é um grupo finito com ordem $e = e(\mathcal{O} \mid \mathcal{O}_\mathbb{K})$. Assim, para $\gamma = \mu(a) = \mu'(a) \in \Gamma$, temos $e\gamma \in \nu\mathbb{K}$.
2. Seja $a \in \mathcal{O}_\mathbb{L}^\times$ qualquer e sejam $\mathbb{K}(a)$, $\mathcal{O}$ e μ' como no Item 1. Pelo Teorema D.9, o corpo de resíduos $\mathbb{K}(a)\mu'$ é uma extensão finita de $\mathbb{K}\nu$, logo algébrica. Como $a\mu' \in \mathbb{K}(a)\mu' \subseteq \mathbb{L}\mu$, temos que $a\mu' \in \mathbb{L}\mu$ é algébrico sobre $\mathbb{K}\nu$.

■

Proposição D.11. *Seja ν uma valorização em $\mathbb{K}$ e consideremos uma extensão $\overline{\nu}$ de ν para um fecho algébrico $\overline{\mathbb{K}}$ de $\mathbb{K}$ fixado. Então o grupo $\overline{\nu}\overline{\mathbb{K}}$ é divisível. Além disso, $\overline{\nu}\overline{\mathbb{K}} \cong \nu\mathbb{K} \otimes \mathbb{Q}$.*

Demonstração: Sejam $\gamma \in \overline{\nu}\overline{\mathbb{K}}$ e $m \in \mathbb{N}$. Tomemos $b \in \overline{\mathbb{K}}$ tal que $\overline{\nu}(b) = \gamma$. Como $\overline{\mathbb{K}}$ é algebricamente fechado, existe $a \in \overline{\mathbb{K}}$ tal que $a^m = b$. Então $\gamma = m\overline{\nu}(a)$, mostrando que $\overline{\nu}\overline{\mathbb{K}}$ é divisível. Como $\overline{\nu}\overline{\mathbb{K}}/\nu\mathbb{K}$ é de torção pela Proposição D.10, temos que $\overline{\nu}\overline{\mathbb{K}} \cong \nu\mathbb{K} \otimes \mathbb{Q}$ (Proposição B.15 e Proposição B.16).

■

A proposição a seguir pode ser consultada no livro em construção de Kuhlmann (20??b, p. 160) ou no livro de Engler e Prestel (2005, p. 66). Não apresentaremos sua demonstração devido a certas tecnicidades.

Proposição D.12. *Consideremos $(\mathbb{K}, \nu) \subseteq (\overline{\mathbb{K}}, \overline{\nu})$, em que $\overline{\mathbb{K}}$ é um fecho algébrico para $\mathbb{K}$. Temos que $\overline{\mathbb{K}}\overline{\nu}$ é um fecho algébrico para $\mathbb{K}\nu$.* ■

Proposição D.13. *Suponhamos $\mathbb{L} \mid \mathbb{K}$ uma extensão algébrica de corpos, $\mathcal{O}$ anel de valorização de $\mathbb{K}$ e sejam $\mathcal{O}_1$ e $\mathcal{O}_2$ anéis de valorização de $\mathbb{L}$ que prolongam $\mathcal{O}$. Se $\mathcal{O}_1 \subseteq \mathcal{O}_2$, então $\mathcal{O}_1 = \mathcal{O}_2$.*

Demonstração: Como $\mathcal{O}_1 \subseteq \mathcal{O}_2$ implica $\mathfrak{m}_2 \subseteq \mathfrak{m}_1$, temos que $\mathcal{O}_1$ é mapeado em um anel de valorização $\mathcal{O}' = \mathcal{O}_1/\mathfrak{m}_2$ dentro do corpo de resíduo $\mathcal{O}_2/\mathfrak{m}_2$. Como $\mathcal{O}_1$ estende $\mathcal{O}$, temos $\mathcal{O}/\mathfrak{m} \hookrightarrow \mathcal{O}'$. Pela Proposição D.10, $\mathcal{O}_2/\mathfrak{m}_2$ é uma extensão algébrica de $\mathcal{O}/\mathfrak{m}$.

Vejamos que $\mathcal{O}'$ é anel de valorização de $\mathcal{O}_2/\mathfrak{m}_2$. Seja $\overline{x} \in \mathcal{O}_2/\mathfrak{m}_2^{\times}$. Então $x \notin \mathfrak{m}_2$. Suponhamos $\overline{x} \notin \mathcal{O}'$. Logo, devemos ter $x \notin \mathcal{O}_1$, o que implica $x^{-1} \in \mathcal{O}_1$. Assim, $\overline{x^{-1}} = \overline{x}^{-1} \in \mathcal{O}_1/\mathfrak{m}_2 = \mathcal{O}'$. Além disso, vejamos que $\mathcal{O}'$ é um corpo. Seja $\overline{x} \in \mathcal{O}'^{\times}$. Dessa forma, $x \in \mathcal{O}_1$ e $x \notin \mathfrak{m}_2$. Como $\mathfrak{m}_2 \subseteq \mathfrak{m}_1$, segue que $x \in \mathcal{O}_1$ e $x \notin \mathfrak{m}_1$. Isso implica que $x^{-1} \in \mathcal{O}_1$, ou seja, $\overline{x^{-1}} = \overline{x}^{-1} \in \mathcal{O}'$.

Portanto, sendo $\mathcal{O}'$ um corpo e um anel de valorização de $\mathcal{O}_2/\mathfrak{m}_2$, concluímos que $\mathcal{O}' = \mathcal{O}_2/\mathfrak{m}_2$. Por hipótese, já sabemos que $\mathcal{O}_1 \subseteq \mathcal{O}_2$. Mostremos que $\mathcal{O}' = \mathcal{O}_2/\mathfrak{m}_2$ implica $\mathcal{O}_2 \subseteq \mathcal{O}_1$. Seja $x \in \mathcal{O}_2$. Logo, $\overline{x} \in \mathcal{O}_2/\mathfrak{m}_2 = \mathcal{O}_1/\mathfrak{m}_2$. Ou seja, $\overline{x} \in \mathcal{O}_1/\mathfrak{m}_2$. Isso significa que existe $a \in \mathcal{O}_1$ tal que $\overline{a} = \overline{x}$, ou seja, $a - x \in \mathfrak{m}_2 \subseteq \mathfrak{m}_1$. Suponhamos, buscando por uma contradição, que $x \notin \mathcal{O}_1$. Com isso, $x^{-1} \in \mathcal{O}_1$ e, além disso, $x^{-1} \in \mathfrak{m}_1$. Portanto, como $a - x \in \mathfrak{m}_1$ e $x^{-1} \in \mathfrak{m}_1$, concluímos que $(a - x)x^{-1} = ax^{-1} - 1 \in \mathfrak{m}_1$. Porém, $-ax^{-1} \in \mathfrak{m}_1$, implicando que $-1 \in \mathfrak{m}_1$, o que é uma contradição. Dessa forma $x \in \mathcal{O}_1$ e concluímos que $\mathcal{O}_1 = \mathcal{O}_2$.

■

Sejam $\mathbb{L} \cap \mathbb{K}^s$ o fecho separável relativo de $\mathbb{K}$ em $\mathbb{L}$ e $[\mathbb{L} : \mathbb{K}]_s := [\mathbb{L} \cap \mathbb{K}^s : \mathbb{K}]$ o grau de separabilidade de $\mathbb{L}$ sobre $\mathbb{K}$ (ver Apêndice A, Seção A.9). Veremos no teorema a seguir que o grau de separabilidade (quando finito) é um limitante superior para o número de prolongamentos de um anel de valorização.

Teorema D.14. *Seja $\mathbb{L}$ extensão algébrica de $\mathbb{K}$ com $[\mathbb{L} : \mathbb{K}]_s$ finito. Seja $\mathcal{O}$ um anel de valorização de $\mathbb{K}$. Então o número r de todos os prolongamentos de $\mathcal{O}$ para $\mathbb{L}$ é finito e*

$$r \leq [\mathbb{L} : \mathbb{K}]_s.$$

Demonstração: Sejam $\mathcal{O}_1, \ldots, \mathcal{O}_r$ uma coleção de r prolongamentos distintos de $\mathcal{O}$ para $\mathbb{L}$ com ideais maximais $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$, respectivamente. Pela Proposição D.13, estes prolongamentos são dois a dois incomparáveis segundo a ordem dada pela inclusão. Portanto, aplicando o Teorema D.7, existe $(c_1, \ldots, c_r) \in \mathcal{O}_1 \times \cdots \times \mathcal{O}_r$ tais que para quaisquer $i, j \in \{1, \ldots, r\}$ vale

$$c_j - 1 \in \mathfrak{m}_j \text{ e } c_i \in \mathfrak{m}_j \text{ para } i \neq j.$$

Se $\mathrm{char}(\mathbb{K}) = p > 0$, como $\mathbb{L} \mid \mathbb{L} \cap \mathbb{K}^s$ é puramente inseparável (ver Apêndice B), então

tomamos $k \in \mathbb{N}$ grande o suficiente para garantir que

$$c_1^{p^k}, \ldots, c_r^{p^k} \in \mathbb{L} \cap \mathbb{K}^s.$$

Se $\mathrm{char}(\mathbb{K}) = 0$, então tomamos $p^k = 1$. Os r elementos listados são $\mathbb{K}$-independentes. De fato, suponhamos que existam $a_1, \ldots, a_r \in \mathbb{K}$, nem todos nulos, tais que

$$\sum_{i=1}^{r} a_i c_i^{p^k} = 0.$$

Seja j tal que $\nu(a_j) = \min\{\nu(a_1), \ldots, \nu(a_r)\}$, sendo ν a valorização associada a $\mathcal{O}$. Então, $\nu(a_j) \neq \infty$, o que implica $a_j \neq 0$. Logo,

$$c_j^{p^k} = -\sum_{i \neq j} a_j^{-1} a_i c_i^{p^k} \in \mathfrak{m}_j,$$

o que implica $c_j \in \mathfrak{m}_j$. Mas, como $c_j - 1 \in \mathfrak{m}_j$, isso significaria que $-1 \in \mathfrak{m}_j$, o que é uma contradição. Logo, $c_1^{p^k}, \ldots, c_r^{p^k}$ são $\mathbb{K}$-independentes. Consequentemente, $r \leq [\mathbb{L} : \mathbb{K}]_s$.

Assim, se $[\mathbb{L} : \mathbb{K}]_s$ é finito, não é possível termos infinitos prolongamentos distintos de $\mathcal{O}$ para $\mathbb{L}$ pois qualquer quantidade finita de prolongamentos é menor que o grau de separabilidade.

■

Passando o teorema acima em termos de valorizações, se ν é uma valorização em $\mathbb{K}$ e $\mathbb{L} \mid \mathbb{K}$ é uma extensão algébrica com grau de separabilidade finito, então existem no máximo $[\mathbb{L} : \mathbb{K}]_s$ prolongamentos não equivalentes de ν para $\mathbb{L}$.

Corolário D.15. *Seja $\mathbb{L}$ uma extensão puramente inseparável de $\mathbb{K}$. Então todo anel de valorização $\mathcal{O}$ de $\mathbb{K}$ possui exatamente um prolongamento para $\mathbb{L}$.*

Demonstração: Se a extensão $\mathbb{L} \mid \mathbb{K}$ é puramente inseparável, então temos $[\mathbb{L} : \mathbb{K}]_s = 1$ (Proposição A.64). Logo, sendo r o número de prologamentos de $\mathcal{O}$, vemos que $r \leq [\mathbb{L} : \mathbb{K}]_s = 1$, implicando que $r = 1$.

■

Em termos de valorizações, se ν é uma valorização em $\mathbb{K}$ e $\mathbb{L} \mid \mathbb{K}$ é puramente inseparável, então existe um único prolongamento de ν para $\mathbb{L}$. Neste caso, o único prolongamento é de fato uma extensão.

Exemplo D.16. *Seja ν^2 a valorização 2-ádica em $\mathbb{Q}$. Consideremos a extensão $\mathbb{Q}(i) \mid \mathbb{Q}$. Como $\mathrm{char}(\mathbb{Q}) = 0$, temos que esta extensão é separável, logo $[\mathbb{Q}(i) : \mathbb{Q}]_s = [\mathbb{Q}(i) : \mathbb{Q}] = 2$. Portanto, temos no máximo dois prolongamentos de ν^2 para $\mathbb{Q}(i)$. Vamos exibir nesse exemplo um deles.*

O anel de inteiros $\mathbb{Z}[i] \subset \mathbb{Q}(i)$ é domínio de fatoração única. Consideremos o ideal primo $\langle 1-i\rangle \subset \mathbb{Z}[i]$. Temos $\langle 2\rangle = \langle 1-i\rangle^2$, pois $2 = (1-i)^2 i$ e $(1-i)^2 = 2(-i)$. Seja ν^{1-i} a valorização $(1-i)$-ádica em $\mathbb{Q}(i)$, isto é, para $x \in \mathbb{Z}[i]$ temos $\nu^{1-i}(x) = n$ com $n = \max\{m \in \mathbb{Z} \mid x \in \langle 1-i\rangle^m\}$ e, para $\alpha = x/y \in \mathbb{Q}(i) = \mathrm{Frac}(\mathbb{Z}[i])$, definimos

$$\nu^{1-i}(\alpha) = \begin{cases} \nu^{1-i}(x) - \nu^{1-i}(y) & \text{se } \alpha \neq 0, \\ \infty & \text{se } \alpha = 0. \end{cases}$$

O grupo de valores de ν^{1-i} é $\mathbb{Z}$. Seja $\nu = \frac{1}{2}\nu^{1-i}$, que é equivalente a valorização $(1-i)$-ádica. O grupo de valores de ν é $\frac{1}{2}\mathbb{Z}$ subgrupo aditivo de $\mathbb{Q}$. Olhando para o anel de valorização associado $\mathcal{O}_\nu = \{\alpha \in \mathbb{Q}(i) \mid \nu(\alpha) \geq 0\}$, mostremos que $\mathcal{O}_\nu \cap \mathbb{Q} = \mathcal{O}_{\nu^2}$. Observamos que $\mathcal{O}_\nu \cap \mathbb{Q} = \{\frac{x}{y} \in \mathbb{Q} \mid \nu(x) - \nu(y) \geq 0\}$. Assim, basta verificarmos que $\nu(x) = \nu^2(x)$ para todo $x \in \mathbb{Z}$. Com isso, concluiremos também que ν é extensão de ν^2.

Mostremos inicialmente que se $x \in \mathbb{Z}$ e $x = (1-i)^k(a+bi)$, com $k > 0$ e $a+bi \in \mathbb{Z}[i]$, então x é par. Provaremos por indução em k.

- *Para $k = 1$, se $x = (1-i)(a+bi) = a+b+bi-ai$, então $a+b = x$ e $a-b = 0$ donde vemos que $x = 2a$. Analogamente, para $k = 2$, se $x = (1-i)^2(a+bi) = -2i(a+bi) = -2ai+2b$, então $a = 0$ e $x = 2b$.*
- *Suponhamos que para j, $2 \leq j \leq k-1$, vale que $x = (1-i)^j(a+bi)$ implica x par. Então,*

$$\begin{aligned} x = (1-i)^k(a+bi) &= a(1-i)^k + bi(1-i)^k \\ &= a(1-i)^2(1-i)^{k-2} + bi(1-i)^2(1-i)^{k-2} \\ &= -2ai(1-i)^{k-2} + 2b(1-i)^{k-2} \\ &= 2(1-i)^{k-2}(b-ai) \in \mathbb{Z}. \end{aligned}$$

  Assim, $x' = (1-i)^{k-2}(b-ai) \in \mathbb{Z}$. Pela hipótese de indução, x' é par. Logo, $x = 2x'$ é par.

Como $\mathbb{Z}[i]$ é domínio de fatoração única e $1-i$ é um irredutível, todo $x \in \mathbb{Z}$ se escreve como $x = (1-i)^k(a+bi)$ para algum $k \in \mathbb{N} \cup \{0\}$ e $a+bi$ não divisível por $1-i$. Logo, se x é ímpar, então $k = 0$ e $\nu(x) = 0 = \nu^2(x)$.

Suponhamos então x par. Escrevemos $x = (1-i)^k(a+bi)$ para algum $k \in \mathbb{N} \cup \{0\}$ e $a+bi$ não divisível por $1-i$. Se $\nu(x) = k/2$, com $k = \nu^{1-i}(x)$, então temos duas possibilidades: k é par ou k é ímpar.

Se $\nu(x) = k/2$ com k ímpar, então

$$x = (1-i)^k(a+bi) = \ldots = 2^{\frac{k-1}{2}}(-i)^{\frac{k-1}{2}}(a+bi)(1-i)$$

$$= 2^{\frac{k-1}{2}}(-i)^{\frac{k-1}{2}}(a+b+bi-ai) \in \mathbb{Z}.$$

Se $(k-1)/2$ é par, então $b-a=0$ e portanto $a+bi=a(1+i)=ai(1-i)$. Se $(k-1)/2$ é ímpar, então $a+b=0$ e portanto $a+bi=a(1-i)$. Ambos os casos contradizem o fato de tomarmos $a+bi$ não divisível por $1-i$. Portanto, k deve ser par.

Se $\nu(x)=k/2$ com k par, então

$$x=(1-i)^k(a+bi)=2(1-i)^{k-2}(b-ai)=$$

$$=2^2(1-i)^{k-4}(a+bi)=\ldots=2^{k/2}(-i)^{k/2}(a+bi)\in\mathbb{Z}.$$

Se $k/2$ é par, então $b=0$ e, como $a+bi=a$ não é divisível por $1-i$, também a não é divisível por 2 (pois $\langle 2\rangle=\langle 1-i\rangle^2\subset\langle 1-i\rangle$). Analogamente para $k/2$ ímpar. Assim, $\nu^2(x)=k/2=\nu(x)$.

Portanto, ν é um prolongamento da valorização 2-ádica ν^2. Como ν é equivalente a ν^{1-i}, temos que

$$\mathcal{O}_{\nu^{1-i}}\cap\mathbb{Q}=\mathbb{Z}[i]_{\langle 1-i\rangle}\cap\mathbb{Q}=\mathcal{O}_\nu\cap\mathbb{Q}=\ \mathcal{O}_{\nu^2}=\mathbb{Z}_{\langle 2\rangle}.$$

Além disso, se $x/y\in\mathbb{Q}$, então

$$\nu(x/y)=\nu(x)-\nu(y)=\nu^2(x)-\nu^2(y)=\nu^2(x/y).$$

Ou seja, $\nu|_{\mathbb{Q}}=\nu^2$. Por fim, como $\frac{1}{2}\mathbb{Z}/\mathbb{Z}\cong\mathbb{Z}/2\mathbb{Z}$, temos que $e(\mathcal{O}_\nu\mid\mathcal{O}_{\nu^2})=2$. Assim, uma vez que $ef\leq n=2$, segue que $f(\mathcal{O}_\nu\mid\mathcal{O}_{\nu^2})=[\mathbb{Q}(i)\nu:\mathbb{Q}\nu^2]=1$.

▼

D.4 Desigualdade de Zariski-Abhyankar

Nesta seção, apresentaremos uma desigualdade muito importante no Capítulo 3, quando tratamos das valorizações transcendentes. A definição de elementos algebricamente independentes, usada a seguir, encontra-se no Apêndice A, Seção A.7.

Lema D.17. *Seja $\mathbb{L}\mid\mathbb{K}$ uma extensão de corpos. Seja $\nu:\mathbb{K}\to\nu\mathbb{K}\cup\{\infty\}$ uma valorização e consideremos $\mu:\mathbb{L}\to\mu\mathbb{L}\cup\{\infty\}$ um prolongamento de ν para $\mathbb{L}$. Seja $\mathcal{O}\subseteq\mathbb{L}$ anel de valorização de μ. Tomemos $\{x_i\}_{i\in I}\subset\mathcal{O}$ e $\{y_j\}_{j\in J}\subset\mathbb{L}^\times$, com $|I|=r\in\mathbb{N}\cup\{0\}$ e $|J|=s\in\mathbb{N}\cup\{0\}$ tais que:*

1. *os resíduos $x_1\mu,\ldots,x_r\mu\in\mathbb{L}\mu$ são algebricamente independentes sobre $\mathbb{K}\nu$.*
2. *$\overline{\mu(y_1)},\ldots,\overline{\mu(y_s)}\in\mu\mathbb{L}/\nu\mathbb{K}$ são $\mathbb{Z}$-independentes.*

Então $x_1\ldots x_r,y_1\ldots,y_s$ são algebricamente independente sobre $\mathbb{K}$.

Demonstração: A prova será feita por indução sobre $r+s$. Para a base de indução, vejamos que o resultado é válido quando $r+s=1$.

- Se $r=1$ e $s=0$, então precisamos mostrar que x_1 é transcendente sobre $\mathbb{K}$. Por contradição, se x_1 fosse algébrico sobre $\mathbb{K}$, então a extensão $\mathbb{K}(x_1) \mid \mathbb{K}$ é algébrica. Logo, $\mathbb{K}(x_1)\mu \mid \mathbb{K}\nu$ é algébrica pela Proposição D.10. Mas, com isso $x_1\mu$ seria algébrico sobre $\mathbb{K}\nu$, contradizendo a Hipótese 1.

- Se $r=0$ e $s=1$, então precisamos mostrar que y_1 é transcendente sobre $\mathbb{K}$. Por contradição, se y_1 fosse algébrico sobre $\mathbb{K}$, então $[\mathbb{K}(y_1):\mathbb{K}]<\infty$. Pelo Teorema D.9, temos $[\Gamma':\Gamma]<\infty$, sendo $\Gamma' \subset \mu\mathbb{L}$ o contradomínio de $\mu|_{\mathbb{K}(y_1)}$. Mas, pela Hipótese 2, $\overline{\mu(y_1)}$ é $\mathbb{Z}$-independente em $\mu\mathbb{L}/\nu\mathbb{K}$, isto é, $l\mu(y_1) \notin \nu\mathbb{K}$ para todo $l \in \mathbb{Z}\setminus\{0\}$. Assim, vemos que $\overline{\mu(y_1)}$ é também $\mathbb{Z}$-independente em $\Gamma'/\nu\mathbb{K}$, donde concluímos que $\Gamma'/\nu\mathbb{K}$ é infinito, uma contradição com o que vimos antes.

Suponhamos que o resultado é válido para todo par $m,l \in \mathbb{N}\cup\{0\}$ tal que $m+l<k$, $k\geq 1$. Sejam $r,s \in \mathbb{N}\cup\{0\}$ com $r+s=k$. Temos dois casos: $s\neq 0$ ou $r\neq 0$. Se $s\neq 0$, como $r+(s-1)<k$, então pela hipótese de indução

$$x_1,\ldots,x_r,y_1,\ldots,y_{s-1} \in \mathbb{L}' = \mathbb{K}(x_1,\ldots,x_r,y_1,\ldots,y_{s-1})$$

são algebricamente independentes sobre $\mathbb{K}$. Aplicando o que foi feito na segunda parte da base de indução para y_s e os corpos $\mathbb{L}'$ e $\mathbb{L}$, vemos que y_s é transcendente sobre $\mathbb{L}'$. Portanto, $x_1,\ldots,x_r,y_1,\ldots,y_s$ são algebricamente independentes sobre $\mathbb{K}$. Para o caso $r\neq 0$ basta fazer um raciocínio análogo, aplicando o que foi feito na primeira parte da base de indução para x_r.

■

Dado um prolongamento $(\mathbb{K},\nu) \subseteq (\mathbb{L},\mu)$, a Desigualdade de Zariski-Abhyankar relaciona o grau de transcendência da extensão $\mathbb{L}\mu \mid \mathbb{K}\nu$ e o posto racional do quociente $\mu\mathbb{L}/\nu\mathbb{K}$ com o grau de transcendência da extensão $\mathbb{L} \mid \mathbb{K}$. A definição de grau de transcendência encontra-se no Apêndice A, Seção A.7. A definição de posto racional encontra-se no Apêndice B, Seção B.2

Teorema D.18. *(Desigualdade de Zariski-Abhyankar) Seja $\mathbb{L} \mid \mathbb{K}$ uma extensão de corpos. Seja $\nu:\mathbb{K}\to\nu\mathbb{K}\cup\{\infty\}$ uma valorização e consideremos $\mu:\mathbb{L}\to\mu\mathbb{L}\cup\{\infty\}$ um prolongamento de ν para $\mathbb{L}$. Então vale*

$$\text{tr.deg}(\mathbb{L}\mu \mid \mathbb{K}\nu) + \text{rat.rk}(\mu\mathbb{L}/\nu\mathbb{K}) \leq \text{tr.deg}(\mathbb{L} \mid \mathbb{K}).$$

Demonstração: Tomemos $\{x_i\mu\}_{i\in I} \subset \mathbb{L}\mu$ uma base de transcendência para $\mathbb{L}\mu$ sobre $\mathbb{K}\nu$ e $\{\overline{\mu(y_j)} \otimes \frac{1}{m_j}\}_{j\in J} \subset (\mu\mathbb{L}/\nu\mathbb{K})\otimes\mathbb{Q}$ uma base para o $\mathbb{Q}$-espaço vetorial $(\mu\mathbb{L}/\nu\mathbb{K})\otimes\mathbb{Q}$ (pela Proposição B.16, todos os tensores em $(\mu\mathbb{L}/\nu\mathbb{K})\otimes\mathbb{Q}$ se resumem a tensores elementares).

Como $\{x_i\mu\}_{i\in I} \subset \mathbb{L}\mu$ é uma base de transcendência para $\mathbb{L}\mu$ sobre $\mathbb{K}\nu$, vemos que $\{x_i\mu\}_{i\in I}$ é um conjunto algebricamente independente sobre $\mathbb{K}$. Logo, para qualquer $r \in \mathbb{N}$, os elementos $x_1\mu, \ldots, x_r\mu$ são algebricamente independentes.

Como $\{\overline{\mu(y_j)} \otimes \frac{1}{m_j}\}_{j\in J} \subset (\mu\mathbb{L}/\nu\mathbb{K}) \otimes \mathbb{Q}$ é uma base para o $\mathbb{Q}$-espaço vetorial $(\mu\mathbb{L}/\nu\mathbb{K}) \otimes \mathbb{Q}$, tomando o conjunto $\{\overline{\mu(y_j)}\}_{j\in J}$, este é $\mathbb{Z}$-independente em $\mu\mathbb{L}/\nu\mathbb{K}$. Isto é, para qualquer $s \in \mathbb{N}$, os elementos $y_1\mu, \ldots, y_s\mu$ são $\mathbb{Z}$-independentes.

Consideremos o conjunto $\{x_i\}_{i\in I} \cup \{y_j\}_{j\in J} \subset \mathbb{L}$, pensando essa união com possíveis repetições. Este conjunto é algebricamente independente sobre $\mathbb{K}$ pois, para qualquer quantidade finita de elementos que tomarmos, podemos aplicar o Lema D.17 e concluir que esses são algebricamente independentes. Portanto,

$$\text{tr.deg}(\mathbb{L}\mu) + \text{rat.rk}(\mu\mathbb{L}/\nu\mathbb{K}) = |\{x_i\}_{i\in I} \cup \{y_j\}_{j\in J}| \leq \text{tr.deg}(\mathbb{L} \mid \mathbb{K}).$$

■

D.5 Teorema da Conjugação e os prolongamentos de uma valorização

Nesta seção, veremos como o grupo de automorfismos de uma extensão se relaciona com os prolongamentos de um anel de valorização. O Teorema da Conjugação (Teorema D.20) nos permitirá alcançar todos os prolongamentos de um dado anel de valorização a partir de um prolongamento fixado. O mesmo será possível para as valorizações.

Teorema D.19. *Sejam $\mathbb{L} \mid \mathbb{K}$ uma extensão normal e finita com $G = Aut(\mathbb{L} \mid \mathbb{K})$ e $\mathcal{O}$ anel de valorização de $\mathbb{K}$. Sejam $\mathcal{O}'$ e $\mathcal{O}''$ prolongamentos de $\mathcal{O}$ para $\mathbb{L}$. Então existe $\sigma \in G$ tal que $\sigma(\mathcal{O}') = \mathcal{O}''$.*

Demonstração: Separamos a extensão $\mathbb{L} \mid \mathbb{K}$ em $\mathbb{L} \mid \mathbb{L}\cap\mathbb{K}^s$ e $\mathbb{L}\cap\mathbb{K}^s \mid \mathbb{K}$. Pelo Corolário D.15, todo prolongamento de $\mathcal{O}$ para $\mathbb{L} \cap \mathbb{K}^s$ possui apenas um prolongamento para $\mathbb{L}$. Além disso $\text{Aut}(\mathbb{L} \cap \mathbb{K}^s \mid \mathbb{K})$ e G podem ser identificados, pois são isomorfos (Proposição A.71). Assim, podemos considerar somente o caso em que $\mathbb{L}$ é extensão separável de $\mathbb{K}$.

Sejam $H' = \{\sigma \in G \mid \sigma(\mathcal{O}') = \mathcal{O}'\}$ e $H'' = \{\tau \in G \mid \tau(\mathcal{O}'') = \mathcal{O}''\}$. Ambos H' e H'' são subgrupos de G e para todo $\sigma \in H'$ temos $\sigma(\mathfrak{m}') = \mathfrak{m}'$, em que $\mathfrak{m}'$ é o ideal maximal de $\mathcal{O}'$. O mesmo vale para o ideal maximal $\mathfrak{m}''$ de $\mathcal{O}''$.

Escrevemos G como união das classes laterais de H' e H'':

$$G = \bigcup_{i=1}^{s} H'\sigma_i^{-1} \text{ e } G = \bigcup_{j=1}^{m} H''\tau_j^{-1},$$

em que $\sigma_1, \ldots, \sigma_s$ e $\tau_1, \ldots, \tau_m$ são os representantes das classes laterais.

Suponhamos $\sigma_i(\mathcal{O}') \not\subseteq \tau_j(\mathcal{O}'')$ e $\tau_j(\mathcal{O}'') \not\subseteq \sigma_i(\mathcal{O}')$ para quaisquer i e j, $1 \leq i \leq s$ e $1 \leq j \leq m$. Como $\sigma_1^{-1}, \ldots, \sigma_s^{-1}$ é um sistema completo de representantes para as classes laterais de H', vemos que para $k \neq t$ temos $\sigma_k(\mathcal{O}') \not\subseteq \sigma_t(\mathcal{O}')$. De fato, se tivéssemos $\sigma_k(\mathcal{O}') \subseteq \sigma_t(\mathcal{O}')$, então, pela Proposição D.13, seguiria que $\sigma_k(\mathcal{O}') = \sigma_t(\mathcal{O}')$. Assim, $\sigma_t^{-1}\sigma_k \in H'$, o que implica $k = t$. Analogamente, $\tau_k(\mathcal{O}') \not\subseteq \tau_t(\mathcal{O}')$ se $k \neq t$.

Tomamos

$$\mathcal{R} = \left(\bigcap_{i=1}^{s} \sigma_i(\mathcal{O}')\right) \bigcap \left(\bigcap_{j=1}^{m} \tau_j(\mathcal{O}'')\right).$$

Pelo Teorema D.7, existe $a \in \mathcal{R}$ tal que $a - 1 \in \sigma(\mathfrak{m}')$ para todo i, $1 \leq i \leq s$, e $a \in \tau_j(\mathfrak{m}'')$ para todo j, $1 \leq j \leq m$. Dessa forma, tomando $\sigma \in G$ e escrevendo $\sigma = \rho\sigma_i^{-1}$ para algum i e $\rho \in H'$, segue que $\sigma(a-1) \in \rho\sigma_i^{-1}(\sigma_i(\mathfrak{m}')) = \rho(\mathfrak{m}') = \mathfrak{m}'$. Analogamente, escrevendo $\sigma = \rho\tau_j$ obtemos $\sigma(a) \in \mathfrak{m}''$ para todo $\sigma \in G$.

Tomando normas, vemos que

$$N_{\mathbb{L}|\mathbb{K}}(a) = \prod_{\sigma \in G} \sigma(a) \in (\mathfrak{m}' + 1) \cap \mathbb{K} = \mathfrak{m} + 1 \text{ e}$$

$$N_{\mathbb{L}|\mathbb{K}}(a) = \prod_{\sigma \in G} \sigma(a) \in \mathfrak{m}'' \cap \mathbb{K} = \mathfrak{m},$$

em que $\mathfrak{m} + 1 = \{b + 1 \mid b \in \mathfrak{m}\}$ (análogo para $\mathfrak{m}' + 1$). Ou seja, $N_{\mathbb{L}|\mathbb{K}}(a) = b + 1$, com $b \in \mathfrak{m}$ e $u \in \mathcal{O}^\times$, e $N_{\mathbb{L}|\mathbb{K}}(a) = c$, com $c \in \mathfrak{m}$. Porém, isso implica que $b + 1 = c$. Logo, teríamos $1 = c - b \in \mathfrak{m}$, o que é falso.

Portanto, $\sigma_i(\mathcal{O}') \not\subseteq \tau_j(\mathcal{O}'')$ ou $\tau_j(\mathcal{O}'') \not\subseteq \sigma_i(\mathcal{O}')$ para algum i, $1 \leq i \leq s$, e algum j, $1 \leq j \leq m$. Pela Proposição D.13, $\sigma_i(\mathcal{O}') = \tau_j(\mathcal{O}'')$ e, por isso, $\tau_j^{-1}\sigma_i(\mathcal{O}') = \mathcal{O}''$.

■

Quando dois prolongamentos $\mathcal{O}'$ e $\mathcal{O}''$ de $\mathcal{O} \subset \mathbb{K}$ para $\mathbb{L}$ estão conectados por meio de um automorfismo, isto é, existe σ tal que $\sigma(\mathcal{O}') = \mathcal{O}''$, dizemos que este prolongamentos são **conjugados** sobre $\mathbb{K}$. Essa nomenclatura explica o porquê do nome do teorema a seguir.

Teorema D.20. *(Teorema da Conjugação) Sejam $\mathbb{L}$ é uma extensão normal de $\mathbb{K}$ e $\mathcal{O}$ um anel de valorização de $\mathbb{K}$. Sejam $\mathcal{O}'$ e $\mathcal{O}''$ anéis de valorização de $\mathbb{L}$ prolongando $\mathcal{O}$. Então existe $\sigma \in Aut(\mathbb{L} \mid \mathbb{K})$ tal que $\sigma(\mathcal{O}') = \mathcal{O}''$.*

Demonstração: Seja S o conjunto dos pares ordenados $(\mathbb{K}_i, \sigma_i)$, em que $\mathbb{K} \subseteq \mathbb{K}_i \subseteq \mathbb{L}$ é uma extensão normal e $\sigma_i \in \mathrm{Aut}(\mathbb{K}_i \mid \mathbb{K})$ satisfaz, para $\mathcal{O}_i' = \mathcal{O}' \cap \mathbb{K}_i$ e $\mathcal{O}_i'' = \mathcal{O}'' \cap \mathbb{K}_i$, a igualdade $\sigma_i(\mathcal{O}_i') = \mathcal{O}_i''$. O conjunto dos pares ordenados com estas propriedades é não vazio, pois $(\mathbb{K}, \mathrm{id})$

satisfaz os requisitos anteriores. Colocaremos a seguinte ordem parcial em S:

$$(\mathbb{K}_i, \sigma_i) \leq (\mathbb{K}_j, \sigma_j) \Longleftrightarrow \mathbb{K}_i \subseteq \mathbb{K}_j \text{ e } \sigma_i = \sigma_j|_{\mathbb{K}_i}.$$

Seja $C \subset S$ uma cadeia em S. Consideremos

$$\mathbb{K}_M = \bigcup_{(\mathbb{K}_i, \sigma_i) \in C} \mathbb{K}_i$$

e

$$\begin{aligned} \sigma_M : \mathbb{K}_M &\longrightarrow \mathbb{K}_M \\ a &\longmapsto \sigma_i(a), \end{aligned}$$

em que o índice i é tal que $a \in \mathbb{K}_i \subset \mathbb{K}_M$. Verifica-se diretamente que $\mathbb{K}_M$ é um corpo, que $\sigma_M \in \mathrm{Aut}(\mathbb{K}_M \mid \mathbb{K})$ e que o par $(\mathbb{K}_M, \sigma_M) \in S$ é um limitante superior para a cadeia C. Pelo Lema de Zorn, existe um par maximal $(\mathbb{K}_m, \sigma_m)$ com $\mathbb{K} \subseteq \mathbb{K}_m \subseteq \mathbb{L}$ extensão normal e $\sigma_m \in \mathrm{Aut}(\mathbb{K}_m \mid \mathbb{K})$ satisfazendo, para $\mathcal{O}'_m = \mathcal{O}' \cap \mathbb{K}_m$ e $\mathcal{O}''_m = \mathcal{O}'' \cap \mathbb{K}_m$, a igualdade $\sigma_m(\mathcal{O}'_m) = \mathcal{O}''_m$.

Mostremos que $\mathbb{K}_m = \mathbb{L}$. Por contradição, suponhamos que exista $\alpha \in \mathbb{L} \setminus \mathbb{K}_m$. Seja $m_\alpha(x) \in \mathbb{K}[x]$ o polinômio minimal de α com relação a $\mathbb{K}$. Como $\mathbb{K} \subset \mathbb{K}_m$, podemos olhar para m_α em $\mathbb{K}_m[x]$. Seja $\mathbb{F}$ o corpo de raízes de $m_\alpha \in \mathbb{K}_m[x]$ dentro de $\mathbb{L}$.

Sendo $\overline{\mathbb{K}}$ fecho algébrico de $\mathbb{K}$ (e lembrando que podemos tomar $\overline{\mathbb{K}}$ igual ao fecho algébrico de $\mathbb{K}_m$ e igual ao fecho algébrico de $\mathbb{L}$), estendemos σ_m para um automorfismo de $\overline{\mathbb{K}}$ que fixa $\mathbb{K}$, que será denotado também por σ_m. Como $\mathbb{L} \mid \mathbb{K}$ é normal, temos $\sigma_m(\mathbb{L}) = \mathbb{L}$. Ainda, temos que $\mathbb{F}$ pode ser visto como a menor extensão de $\mathbb{K}$ que contém a união de $\mathbb{K}_m$ com o corpo de raízes de m_α sobre $\mathbb{K}$ dentro de $\mathbb{L}$ (isto é, o compósito sobre $\mathbb{K}$ de $\mathbb{K}_m$ com o corpo de raízes de m_α sobre $\mathbb{K}$ dentro de $\mathbb{L}$). Como $\mathbb{K}_m \mid \mathbb{K}$ é normal e o corpo de raízes de m_α é uma extensão normal de $\mathbb{K}$, segue que o compósito $\mathbb{F}$ é uma extensão normal de $\mathbb{K}$. Assim, $\sigma_m(\mathbb{F}) = \mathbb{F}$.

Sejam $\mathcal{O}^* := \mathcal{O}' \cap \mathbb{F}$ e $\mathcal{O}^{**} := \sigma_m^{-1}(\mathcal{O}'' \cap \mathbb{F})$. Temos

$$\mathcal{O}^* \cap \mathbb{K}_m = \mathcal{O}' \cap \mathbb{F} \cap \mathbb{K}_m = \mathcal{O}' \cap \mathbb{K}_m = \mathcal{O}'_m \text{ e}$$

$$\mathcal{O}^{**} \cap \mathbb{K}_m = \mathcal{O}' \cap \mathbb{F} \cap \mathbb{K}_m = \mathcal{O}' \cap \mathbb{K}_m = \mathcal{O}'_m.$$

Logo, $\mathcal{O}^*$ e $\mathcal{O}^{**}$ são prolongamentos de $\mathcal{O}'_m$ para de $\mathbb{K}_m$ para $\mathbb{F}$. Como $\mathbb{F}$ é corpo de raízes, temos que $\mathbb{F} \mid \mathbb{K}_m$ é uma extensão normal finita (WEINTRAUB, 2006, p. 23). Pelo Teorema D.19, existe $\sigma \in \mathrm{Aut}(\mathbb{F} \mid \mathbb{K}_m)$ tal que $\mathcal{O}^{**} = \sigma(\mathcal{O}^*)$. Então,

$$(\sigma_m \circ \sigma)(\mathcal{O}' \cap \mathbb{F}) = (\sigma_m \circ \sigma)(\mathcal{O}^*) = \sigma_m(\mathcal{O}^{**}) = \mathcal{O}'' \cap \mathbb{F}.$$

Assim, $(\mathbb{F}, \sigma_m \circ \sigma) \in S$, pois $\mathbb{K} \subseteq \mathbb{F} \subseteq \mathbb{L}$ é uma extensão normal e $\sigma_m \circ \sigma \in \mathrm{Aut}(\mathbb{F} \mid \mathbb{K})$ satisfaz, para $\mathcal{O}' \cap \mathbb{F}$ e $\mathcal{O}'' \cap \mathbb{F}$, a igualdade $(\sigma_m \circ \sigma)(\mathcal{O}' \cap \mathbb{F}) = \mathcal{O}'' \cap \mathbb{F}$. Além disso, temos $\mathbb{K}_m \subsetneq \mathbb{F}$ e $\sigma_m = \sigma_m \circ \sigma|_{\mathbb{K}_m}$, ou seja, $(\mathbb{K}_m, \sigma_m) \leq (\mathbb{F}, \sigma_m \circ \sigma)$, contradizendo a maximalidade de $(\mathbb{K}_m, \sigma_m)$. Dessa forma, segue o resultado.

■

Como consequência do Teorema da Conjugação, traremos agora algumas formas de alcançar os prolongamentos de uma dada valorização a partir de um prolongamento dado.

Teorema D.21. *Sejam $\mathbb{L} \mid \mathbb{K}$ uma extensão algébrica e ν uma valorização em $\mathbb{K}$. Então quaisquer dois prolongamentos de ν para $\mathbb{L}$ são conjugados. Isto é, se μ e μ' são prolongamentos de ν para $\mathbb{L}$, então existe um $\mathbb{K}$-automorfismo $\sigma \in \mathrm{Aut}(\overline{\mathbb{L}} \mid \mathbb{K})$ tal que $\mu' \sim (\tilde{\mu} \circ \sigma)|_{\mathbb{L}}$, em que $\tilde{\mu}$ é um prolongamento de μ para o fecho algébrico $\overline{\mathbb{L}}$. Ademais, dado um prolongamento qualquer $\tilde{\nu}$ de ν para , o conjunto de todos os prolongamentos de ν para $\mathbb{L}$ é*

$$\{(\tilde{\nu} \circ \sigma)|_{\mathbb{L}} \mid \sigma \in \mathrm{Aut}(\overline{\mathbb{L}} \mid \mathbb{K})\}.$$

Demonstração: Tomemos $\overline{\mathbb{L}} = \overline{\mathbb{K}}$. A extensão $\overline{\mathbb{L}} \mid \mathbb{K}$ é normal e $\overline{\mathbb{L}} \supseteq \mathbb{L} \supseteq \mathbb{K}$. Sejam μ e μ' dois prolongamentos de ν para $\mathbb{L}$. Sejam $\tilde{\mu}$ e $\tilde{\mu}'$ prolongamentos de μ e μ' para $\overline{\mathbb{L}}$, respectivamente. Consideremos $\mathcal{O}_{\tilde{\mu}}$ e $\mathcal{O}_{\tilde{\mu}'}$ os respectivos anéis de valorização. Como $\mathcal{O}_{\tilde{\mu}} \cap \mathbb{K} = \mathcal{O}_{\tilde{\mu}'} \cap \mathbb{K} = \mathcal{O}_\nu$, segue do Teorema da Conjugação que existe $\sigma^{-1} \in \mathrm{Aut}(\overline{\mathbb{L}} \mid \mathbb{K})$ tal que $\sigma^{-1}(\mathcal{O}_{\tilde{\mu}}) = \mathcal{O}_{\tilde{\mu}'}$. Por cálculos diretos, vemos que $\tilde{\mu} \circ \sigma$ é uma valorização em $\overline{\mathbb{L}}$ com anel de valorização igual a $\sigma(\mathcal{O}_{\tilde{\mu}})$. Isto é, $\tilde{\mu} \circ \sigma \sim \tilde{\mu}'$. Sejam

$$\phi_{\tilde{\mu}'} : \Gamma_{\mu'} \longrightarrow \Gamma_{\tilde{\mu}'|_{\mathbb{L}}} \text{ e } \phi_{\tilde{\mu}\circ\sigma} : \Gamma_{\tilde{\mu}'} \longrightarrow \Gamma_{\tilde{\mu}\circ\sigma}$$

isomorfismos que preservam as ordens e tais que $\tilde{\mu}'(b) = \phi_{\tilde{\mu}'}(\mu'(b))$ e $(\tilde{\mu} \circ \sigma)(c) = \phi_{\tilde{\mu}\circ\sigma}(\tilde{\mu}'(c))$, para todo $b \in \mathbb{L}$ e $c \in \overline{\mathbb{L}}$. Assim, para todo $b \in \mathbb{L}$, temos

$$\phi_{\tilde{\mu}\circ\sigma}(\phi_{\tilde{\mu}'}(\mu'(b))) = \phi_{\tilde{\mu}\circ\sigma}(\tilde{\mu}'(b)) = (\tilde{\mu} \circ \sigma)(b).$$

Logo, $\mu' \sim (\tilde{\mu} \circ \sigma)|_{\mathbb{L}}$.

Por fim, fixamos $\tilde{\nu}$ um prolongamento de ν para $\overline{\mathbb{L}}$. Tomemos $\mu = \tilde{\nu}|_{\mathbb{L}}$ e $\tilde{\mu} = \tilde{\nu}$. Assim, qualquer prolongamento μ' de ν para $\mathbb{L}$ é da forma $(\tilde{\nu} \circ \sigma)|_{\mathbb{L}}$, sendo σ um $\mathbb{K}$-automorfismo de $\overline{\mathbb{L}}$.

■

Nos dois corolários a seguir temos casos particulares do Teorema D.21. Em seguida, revisitaremos o Exemplo D.16, aplicando os conhecimentos adquiridos nesta seção.

Corolário D.22. *Seja ν uma valorização em $\mathbb{K}$. Fixamos $\tilde{\nu}$ um prolongamento de ν para $\overline{\mathbb{K}}$, fecho algébrico de $\mathbb{K}$. O conjunto de todos os prolongamentos de ν para $\overline{\mathbb{K}}$ é*

$$\{\tilde{\nu} \circ \sigma \mid \sigma \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K})\}.$$

■

Corolário D.23. *Seja ν uma valorização em $\mathbb{K}$. Seja $\mathbb{L} \mid \mathbb{K}$ uma extensão normal e fixemos $\tilde{\nu}$ um prolongamento de ν para $\mathbb{L}$. O conjunto de todos os prolongamentos de ν para $\mathbb{L}$ é*

$$\{\tilde{\nu} \circ \sigma \mid \iota \in \mathrm{Aut}(\mathbb{L} \mid \mathbb{K})\}.$$

■

Exemplo D.24. *No Exemplo D.16, estendemos a valorização 2-ádica ν^2 de $\mathbb{Q}$ para $\mathbb{Q}(i)$, encontrando a valorização $\nu = \frac{1}{2}\nu^{1-i}$, sendo ν^{1-i} a valorização $(1-i)$-ádica em $\mathbb{Q}(i)$. Como $[\mathbb{Q}(i) : \mathbb{Q}]_s = 2$, vimos que existem no máximo dois prolongamentos de ν^2 para $\mathbb{Q}(i)$. Como $\mathbb{Q}(i)$ é o corpo de decomposição de uma família de polinômios em $\mathbb{Q}[x]$, então $\mathbb{Q}(i) \mid \mathbb{Q}$ é uma extensão normal. Temos Gal$(\mathbb{Q}(i) \mid \mathbb{Q}) = \{\mathrm{id}, \mathrm{conj}\}$, em que* $\mathrm{conj} : \mathbb{Q}(\mathrm{i}) \to \mathbb{Q}(\mathrm{i})$ *é a aplicação definida por* $\mathrm{conj}(\mathrm{a} + \mathrm{bi}) := \mathrm{a} - \mathrm{bi}$. *Pelo Corolário D.23, o outro prolongamento de ν^2 para $\mathbb{Q}(i)$ deve ser $\nu \circ \mathrm{conj}$. Esta composição coincide com a valorização $\nu' = \frac{1}{2}\nu^{1+i}$, em que ν^{1+i} é a valorização $(1+i)$-ádica em $\mathbb{Q}(i)$. Como $1 + i = i(1-i)$, isto é, estes são associados, a quantidade de vezes que $1+i$ está presente na fatoração de $x \in \mathbb{Z}[i]$ coincide com a quantidade de vezes que $1-i$ está na fatoração de x. Logo, $\mathcal{O}_{\nu^{1+i}} = \mathcal{O}_{\nu^{1-i}}$ e portanto ν^{1+i} e ν^{1-i} são equivalentes (e, por conseguinte, ν é equivalente a ν'). Concluímos que ν^2 possui um único prolongamento (a menos de equivalência) para $\mathbb{Q}(i)$.*

▼

Outra aplicação para esses corolários é a demonstração do seguinte teorema, que trata da possibilidade de tomar uma valorização em $\overline{\mathbb{K}}(x)$ que seja, simultaneamente, um prolongamento de valorizações pré-determinadas em $\mathbb{K}$, $\mathbb{K}(x)$ e $\overline{\mathbb{K}}$.

Teorema D.25. *Seja ν uma valorização no corpo $\mathbb{K}$. Seja μ um prolongamento de ν para o corpo $\mathbb{K}(x)$. Seja $\overline{\mathbb{K}}$ um fecho algébrico fixado de $\mathbb{K}$ e tomemos uma valorização $\overline{\nu}$ em $\overline{\mathbb{K}}$ que prolonga ν. Então existe uma valorização $\overline{\mu}$ em $\overline{\mathbb{K}}(x)$ que prolonga ν e tal que $\overline{\mu}|_{\mathbb{K}(x)} \sim \mu$ e $\overline{\mu}|_{\overline{\mathbb{K}}} \sim \overline{\nu}$.*

Demonstração: Temos um isomorfismo entre $\mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K})$ e $\mathrm{Aut}(\overline{\mathbb{K}}(x) \mid \mathbb{K}(x))$ definido da seguinte forma: dado $\sigma \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K})$, levaremos este em $\overline{\sigma} \in \mathrm{Aut}(\overline{\mathbb{K}}(x) \mid \mathbb{K}(x))$ tal que, para $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, temos $\overline{\sigma}(f(x)) = \sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_n)x^x$ e $\overline{\sigma}(f(x)/g(x)) = \overline{\sigma}(f(x))/\overline{\sigma}(g(x))$.

Seja $\overline{\mu}'$ um prolongamento de μ para $\overline{\mathbb{K}}(x)$ e seja $\overline{\nu}' = \overline{\mu}'|_{\overline{\mathbb{K}}}$. Sejam

$$\phi_\mu : \Gamma_\nu \longrightarrow \Gamma_{\mu|_{\mathbb{K}}} \text{ e } \phi_{\overline{\mu}'} : \Gamma_\mu \longrightarrow \Gamma_{\overline{\mu}'|_{\mathbb{K}}}$$

isomorfismos que preservam as respectivas ordens tais que $\mu(a) = \phi_\mu(\nu(a))$ e $\overline{\mu}'(c) = \phi_{\overline{\mu}'}(\mu(c))$, para todo $a \in \mathbb{K}$ e $c \in \mathbb{K}(x)$. Temos, para todo $a \in \mathbb{K}$,

$$\overline{\nu}'(a) = \overline{\mu}'(a) = \phi_{\overline{\mu}'}(\phi_\mu(\nu(a))).$$

Logo, $\overline{\nu}'$ é um prolongamento de ν para $\overline{\mathbb{K}}$. Pelo Corolário D.22, existe $\sigma \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K})$ tal que $\overline{\nu} \sim \overline{\nu}' \circ \sigma$. Definimos $\overline{\mu} := \overline{\mu}' \circ \overline{\sigma}$. Assim, pelo Corolário D.23, $\overline{\mu}$ é um prolongamento de μ para $\overline{\mathbb{K}}(x)$. Sejam

$$\phi_{\overline{\nu}'\circ\sigma} : \Gamma_{\overline{\nu}} \longrightarrow \Gamma_{\overline{\nu}'\circ\sigma} \text{ e } \phi_{\overline{\mu}} : \Gamma_\mu \longrightarrow \Gamma_{\overline{\mu}|_{\mathbb{K}(x)}}$$

isomorfismos que preservam as respectivas ordens tais que $(\overline{\nu}' \circ \sigma)(b) = \phi_{\overline{\nu}'\circ\sigma}(\overline{\nu}(b))$ e $\overline{\mu}(c) = \phi_{\overline{\mu}}(\mu(c))$, para todo $b \in \overline{\mathbb{K}}$ e $c \in \mathbb{K}(x)$. Assim, para todo $a \in \mathbb{K}$ e $b \in \overline{\mathbb{K}}$, temos

$$\overline{\mu}(a) = \phi_{\overline{\mu}}(\mu(a)) = \phi_{\overline{\mu}}(\phi_\mu(\nu(a))) \text{ e}$$

$$\overline{\mu}(b) = \overline{\mu}'(\overline{\sigma}(b)) = \overline{\nu}'(\sigma(b)) = \phi_{\overline{\nu}'\circ\sigma}(\overline{\nu}(b)).$$

Ou seja, $\overline{\mu}$ é também um prolongamento de ν e de $\overline{\nu}$ para $\overline{\mathbb{K}}(x)$.

■

No diagrama abaixo ilustramos a situação descrita no enunciado do Teorema D.25. Essa configuração foi largamente utilizada no Capítulo 3.

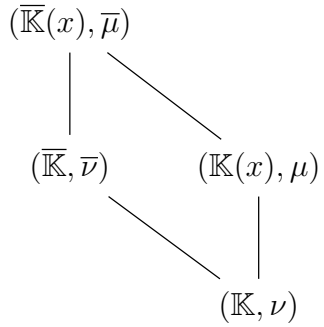


Figura D.1: Diagrama dos prolongamentos

Observação D.26. *Na literatura, é comum não se fazer distinção entre os termos prolongamento e extensão, como fizemos neste apêndice. Se $(\mathbb{L}, \mu) \subseteq (\mathbb{K}, \nu)$ é um prolongamento, então existe um isomorfismo ϕ_μ entre $\Gamma_{\mu|_{\mathbb{K}}}$ e Γ_ν que preserva a ordem e tal que $\mu|_{\mathbb{K}} = \phi_\mu \circ \nu$. Portanto, podemos trabalhar com $\phi_\mu \circ \nu$ no lugar de ν (ambas possuem o mesmo anel de valorização, mesmo ideal maximal associado e mesmo corpo de resíduos). Assim, abusamos da notação e*

dizemos que $\mu|_{\mathbb{K}} = \nu$. *Neste apêndice, escolhemos deixar explícita a diferença entre os dois conceitos. No texto principal deste trabalho e no apêndice a seguir, não faremos distinção entre extensão e prolongamento, deixando implícitos os mergulhos entre grupos e tratando-os como inclusões.*

▼

Apêndice E

Henselização

Neste apêndice continuamos a discussão sobre extensões e prolongamentos de valorizações. Estudaremos os pares henselianos, que são pares da forma $(\mathbb{K}, \nu)$ tais que ν possui um único prolongamento para qualquer extensão algébrica de $\mathbb{K}$.

Na primeira seção veremos algumas propriedades desses pares e apresentaremos exemplos. Em seguida, na segunda seção, estudaremos o grupo e o corpo de decomposição associados a uma dada valorização. Chegaremos ao conceito de henselização, que será intuitivamente o menor par henseliano que contém um dado par $(\mathbb{K}, \nu)$ não necessariamente henseliano. Por fim, na terceira seção utilizaremos o grupo de decomposição para descrever as valorizações em $\overline{\mathbb{K}}[x]$ que são ao mesmo tempo extensão de μ em $\mathbb{K}[x]$ e $\overline{\nu}$ em $\overline{\mathbb{K}}$. Os resultados deste apêndice foram utilizados unicamente no desenvolvimento do Capítulo 4.

As principais referências para a composição deste apêndice foram os trabalhos de Engler e Prestel (2005), Kuhlmann (20??c) e Bengus-Lasnier (2021).

E.1 Pares henselianos

Começamos apresentando a definição de um par henseliano.

Definição E.1. *Sejam $\mathbb{K}$ um corpo e ν uma valorização em $\mathbb{K}$. O par $(\mathbb{K}, \nu)$ é dito* ***henseliano*** *se ν admite um único prolongamento para qualquer extensão algébrica de $\mathbb{K}$.*

■

A propriedade de ser henseliano é tal que, dada uma extensão algébrica $(\mathbb{K}_1, \nu_1) \subseteq (\mathbb{K}_2, \nu_2)$, se $(\mathbb{K}_1, \nu_1)$ é henseliano, então $(\mathbb{K}_2, \nu_2)$ é também henseliano.

Consideremos o fecho separável de $\mathbb{K}$, descrito como

$$\mathbb{K}^s := \{\alpha \in \overline{\mathbb{K}} \,|\, \alpha \text{ é separável sobre } \mathbb{K}\},$$

para $\overline{\mathbb{K}}$ um fecho algébrico de $\mathbb{K}$ fixado. Para simplificar a notação, não diferenciaremos prolongamento de extensão e, por abuso de notação, escreveremos $\mu = \mu'$ quando $\mu \sim \mu'$.

Proposição E.2. *O par $(\mathbb{K}, \nu)$ é henseliano se, e somente se, ν se prolonga de maneira única para $\mathbb{K}^s$.*

Demonstração:

($\Rightarrow$) Se $(\mathbb{K}, \nu)$ é henseliano, então por definição ν se prolonga de maneira única para $\mathbb{K}^s$, uma vez que a extensão $\mathbb{K}^s \mid \mathbb{K}$ é algébrica.

($\Leftarrow$) Seja $\mathbb{L}$ uma extensão algébrica de $\mathbb{K}$. Todo prolongamento de ν para $\mathbb{L} \cap \mathbb{K}^s$ possui um prolongamento ν' para $\mathbb{K}^s$ tal que $\nu'|_{\mathbb{K}} = \nu$. Por hipótese, temos que ν possui um único prolongamento para $\mathbb{K}^s$. Afirmamos que ν possui um único prolongamento para $\mathbb{L} \cap \mathbb{K}^s$. De fato, se ν_1 e ν_2 são prolongamentos distintos (isto é, não equivalentes) de ν para $\mathbb{L} \cap \mathbb{K}^s$, então existem prolongamentos ν_1' e ν_2' para $\mathbb{K}^s$ tais que $\nu_i'|_{\mathbb{K}^s} = \nu_i$, $(i = 1, 2)$. Portanto, ν_1' e ν_2' são distintos. Como $\nu_i'|_{\mathbb{K}} = \nu_i|_{\mathbb{K}} = \nu$, então teríamos prolongamentos distintos de ν para $\mathbb{K}^s$, o que não ocorre por hipótese.

Pelo Corolário D.15, toda valorização de $\mathbb{L} \cap \mathbb{K}^s$ possui um único prolongamento para $\mathbb{L}$. Portanto, ν possui um único prolongamento para $\mathbb{L}$. De fato, se ν_1 e ν_2 são prolongamentos de ν para $\mathbb{L}$, então $\nu_1|_{\mathbb{L}\cap\mathbb{K}^s}$ e $\nu_2|_{\mathbb{L}\cap\mathbb{K}^s}$ são prolongamentos de ν para $\mathbb{L} \cap \mathbb{K}^s$, que vimos que devem ser equivalentes. Logo, $\nu_1|_{\mathbb{L}\cap\mathbb{K}^s} = \nu_2|_{\mathbb{L}\cap\mathbb{K}^s} = \nu'$. Então, ν_1 e ν_2 são prolongamentos de ν' de $\mathbb{L} \cap \mathbb{K}^s$ para $\mathbb{L}$ e, pelo Corolário D.15, $\nu_1 = \nu_2$.

■

Utilizando os mesmos argumentos acima, obtemos outra forma de caracterizar pares $(\mathbb{K}, \nu)$ henselianos.

Proposição E.3. *$(\mathbb{K}, \nu)$ é henseliano se, e somente se, ν se prolonga de maneira única para $\overline{\mathbb{K}}$.*

■

Na proposição a seguir, veremos que a propriedade de ser henseliano pode ser transferida de um par a outro quando os corpos envolvidos são isomorfos e as valorizações se relacionam a partir do isomorfismo.

Proposição E.4. *Sejam $(\mathbb{K}, \nu)$ e $(\mathbb{L}, \mu)$ corpos com valorizações. Seja $\sigma : \mathbb{K} \longrightarrow \mathbb{L}$ um isomorfismo tal que $\mu \circ \sigma = \nu$. Se $(\mathbb{K}, \nu)$ é henseliano, então $(\mathbb{L}, \mu)$ é henseliano.*

Demonstração: Iniciamos estendendo σ para um isomorfismo $\overline{\sigma} : \overline{\mathbb{K}} \longrightarrow \overline{\mathbb{L}}$. Suponhamos que μ_1 e μ_2 são dois prolongamentos distintos de μ para $\overline{\mathbb{L}}$. Seja ϕ_i um isomorfismo entre os grupos de valores de μ e $\mu_i|_{\mathbb{L}}$ que preserva a ordem e tal que $\phi \circ \mu = \mu_i|_{\mathbb{L}}$ $(i = 1, 2)$. Então,

$$(\mu_i \circ \overline{\sigma})|_{\mathbb{K}} = \mu_i|_{\mathbb{K}} \circ \overline{\sigma}|_{\mathbb{L}} = \phi_i \circ \mu \circ \sigma = \phi_i \circ \nu.$$

Portanto, $\mu_1 \circ \overline{\sigma}$ e $\mu_2 \circ \overline{\sigma}$ são prolongamentos distintos de ν para $\overline{\mathbb{K}}$, contradizendo $(\mathbb{K}, \nu)$ ser henseliano. Assim, $(\mathbb{L}, \mu)$ deve ser henseliano.

■

O nome "henseliano" se deve ao fato de que o corpo $\mathbb{K}$ e o anel de valorização $\mathcal{O}_\nu$ satisfazem o que é conhecido na literatura como **Lema de Hensel**: para cada $f \in \mathcal{O}_\nu[x]$ e $a_0 \in \mathcal{O}_\nu$ com $\nu(f(a_0)) > 2\nu(f'(a_0))$, existe um $a \in \mathcal{O}_\nu$ tal que $f(a) = 0$ e $\nu(a - a_0) > \nu(f'(a_0))$. De fato, o par $(\mathbb{K}, \nu)$ é henseliano se, e somente se, $\mathcal{O}_\nu$ satisfaz o Lema de Hensel (ENGLER; PRESTEL, 2005, pp. 87-88). O Lema de Hensel não ganhará foco em nosso trabalho, por isso não o discutiremos mais a fundo. No entanto, os dois exemplos abaixo mostram onde podemos encontrar este resultado na literatura e servirão para exibir um par henseliano.

Exemplo E.5. *Consideremos $\mathbb{K}$ um corpo com uma valorização ν tal que $\nu\mathbb{K}$ é subgrupo de $(\mathbb{R}, +)$. Podemos definir um valor absoluto $|\cdot|$ em $\mathbb{K}$ através da expressão $|a| := e^{-\nu(a)}$, em que e representa o número de Euler. Um corpo $\mathbb{K}$ com um valor absoluto $|\cdot|$ é dito* ***completo*** *se toda sequência de Cauchy em $\mathbb{K}$ converge para algum elemento de $\mathbb{K}$. Em corpos completos vale o Lema de Hensel (ENGLER; PRESTEL, 2005, p. 20). Assim, o par $(\mathbb{K}, \nu)$, nesse caso, é henseliano.*

Suponhamos agora que $\mathbb{K}$ não é completo com relação ao valor absoluto $|\cdot|$. Podemos seguir a construção de $\mathbb{R}$ por meio de sequências de Cauchy de números racionais e obtemos, a partir de $(\mathbb{K}, |\cdot|)$, um corpo que é o chamado ***completamento*** *de $\mathbb{K}$ com respeito ao valor absoluto $|\cdot|$. O completamento de $\mathbb{K}$ com respeito a $|\cdot|$ é completo, estende $\mathbb{K}$ e possui um valor absoluto que estende $|\cdot|$ (ENGLER; PRESTEL, 2005, p. 9).*

▼

Exemplo E.6. *Dado um primo $p \in \mathbb{N}$, consideramos em $\mathbb{Q}$ a valorização p-ádica ν^p. Como $\nu\mathbb{Q} \subset \mathbb{R}$, podemos definir um valor absoluto $|\cdot|_p$ em $\mathbb{Q}$ como no exemplo acima. O corpo $\mathbb{Q}$ não é completo com relação a $|\cdot|_p$. O completamento dos racionais com relação a $|\cdot|_p$ é o conhecido* ***corpo dos números p-ádicos****, que será denotado por $\mathbb{Q}_p$. Outra forma de vermos esse corpo é a seguinte:*

$$\mathbb{Q}_p \cong \left\{ \sum_{i=m}^{\infty} a_i p^i \mid a_i \in \{0, \ldots, p-1\}, m \in \mathbb{Z} \right\}.$$

Estendemos ν^p para $\mathbb{Q}^p$ fazendo

$$\nu^p \left(\sum_{i=m}^{\infty} a_i p^i \right) = \min\{i \mid a_i \neq 0\}.$$

O exemplo anterior nos diz que o par $(\mathbb{Q}_p, \nu^p)$ satisfaz o Lema de Hensel, portanto é henseliano.

▼

E.2 Grupo de decomposição e henselização

Sejam $\mathbb{K}$ um corpo e ν uma valorização em $\mathbb{K}$. Seja ν^s uma extensão de ν para o fecho separável $\mathbb{K}^s$ de $\mathbb{K}$ (em relação a um fecho algébrico $\overline{\mathbb{K}}$ de $\mathbb{K}$ fixado).

Definimos

$$G^d(\nu^s) := \{\sigma \in \mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K}) \mid \nu^s \circ \sigma = \nu^s\}.$$

Temos que $G^d(\nu^s)$ é um subgrupo de $\mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K})$, chamado **grupo de decomposição** de ν^s sobre $\mathbb{K}$. Tal subgrupo é um fechado quando consideramos a topologia de Krull em $\mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K})$ (KUHLMANN, 2021, p. 171).

Se tivermos uma valorização $\overline{\nu}$ em $\overline{\mathbb{K}} \supseteq \mathbb{K}^s$, então tomando $\nu^s = \overline{\nu}|_{\mathbb{K}^s}$ veremos que $G^d(\nu^s) \cong G^d(\overline{\nu}) := \{\sigma \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K}) \mid \overline{\nu} \circ \sigma = \overline{\nu}\}$. De fato, temos o isomorfismo $\mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K}) \cong \mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K})$, dado pela restrição. Logo, se $\sigma \in G^d(\overline{\nu})$, então $\nu^s \circ \sigma|_{\mathbb{K}^s} = \nu^s$. Ou seja, podemos dizer, por abuso de notação, que $\sigma \in G^d(\nu^s)$. Agora, se $\sigma = \tau|_{\mathbb{K}^s} \in G^d(\nu^s)$ (com $\tau \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K})$), então não podemos ter $\overline{\nu} \circ \tau \neq \overline{\nu}$. De fato, se isso ocorresse, então $\overline{\nu} \circ \tau$ seria uma segunda extensão de ν^s para $\overline{\mathbb{K}}$, o que não pode acontecer, uma vez que $\overline{\mathbb{K}} \mid \mathbb{K}^s$ é puramente inseparável. Assim, todos os resultados que veremos a seguir para $G^d(\nu^s)$ possuem os seus correspondentes se considerarmos $G^d(\overline{\nu})$ (que será utilizado na próxima seção e no Capítulo 4).

O corpo fixado de $G^d(\nu^s)$ é chamado **corpo de decomposição** de ν^s sobre $\mathbb{K}$, denotado $\mathbb{K}^d(\nu^s)$ ou simplesmente $\mathbb{K}^d$, quando não houver confusão sobre qual é a valorização em questão. Explicitamente,

$$\mathbb{K}^d(\nu^s) = \{a \in \mathbb{K}^s \mid \sigma(a) = a \text{ para todo } \sigma \in G^d(\nu^s)\} \subseteq \mathbb{K}^s.$$

Associamos ao corpo de decomposição $\mathbb{K}^d$ a valorização $\nu^d := \nu^s|_{\mathbb{K}^d}$, que é uma extensão de ν para $\mathbb{K}^d$. A seguir, veremos uma série de resultados que nos permitirão entender melhor o par $(\mathbb{K}^d, \nu^d)$.

Proposição E.7.

1. *O par $(\mathbb{K}^d, \nu^d)$ é henseliano.*
2. *Seja μ^s outra extensão de ν para $\mathbb{K}^s$. Seja $\mathbb{K}^d(\mu^s)$ o corpo de decomposição de μ^s e seja $\mu^d := \mu^s|_{\mathbb{K}^d(\mu^s)}$. Existe um único $\iota \in \mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K})$ tal que $\iota^{-1}|_{\mathbb{K}^d(\nu^s)} : \mathbb{K}^d(\nu^s) \longrightarrow \mathbb{K}^d(\mu^s)$ é um isomorfismo satisfazendo $\mu^d = \nu^d \circ \iota|_{\mathbb{K}^d(\mu^s)}$.*

Demonstração:

1. Tomemos $\overline{\mathbb{K}^d} = \overline{\mathbb{K}}$. Seja $\nu^d = \nu^s|_{\mathbb{K}^d}$ valorização em $\mathbb{K}^d \subseteq \mathbb{K}^s$. Seja μ um prolongamento de ν^s de $\mathbb{K}^s$ para $\overline{\mathbb{K}}$. Como $\overline{\mathbb{K}} \mid \mathbb{K}^s$ é puramente inseparável, temos que μ é único. Como

$\mu|_{\mathbb{K}^s} = \nu^s$, segue que $\mu|_{\mathbb{K}^d} = \nu^d$, ou seja, μ é um prolongamento de ν^d para $\overline{\mathbb{K}}$. Pelo Corolário D.22, fixando μ, temos que o conjunto de todos os prolongamentos de ν^d para $\overline{\mathbb{K}}$ é

$$\{\mu \circ \iota \mid \iota \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K}^d)\}.$$

Porém,

$$\mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K}^d) \cong \mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K}^d) = G^d,$$

uma vez que G^d é um subgrupo fechado de $\mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K})$ com relação a topologia de Krull (ver Exemplo A.65, Exemplo A.72 e Teorema A.80 no Apêndice A). Tal isomorfismo é dado tomando $\iota \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K}^d)$ e associando $\iota|_{\mathbb{K}^s}$ em G^d. Vejamos que, para qualquer $\iota \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K}^d)$, temos que $\mu \circ \iota = \mu$. Chamado $\sigma = \iota|_{\mathbb{K}^s} \in G^d$, temos

$$(\mu \circ \iota)|_{\mathbb{K}^s} = \mu|_{\mathbb{K}^s} \circ \sigma = \nu^s \circ \sigma = \nu^s.$$

Logo, $\mu \circ \iota$ é um prolongamento de ν^s de $\mathbb{K}^s$ para $\overline{\mathbb{K}}$. Como só há um prolongamento de ν^s para $\overline{\mathbb{K}}$, concluímos que $\mu \circ \iota = \mu$. Portanto, $(\mathbb{K}^d, \nu^d)$ é henseliano.

2. Seja μ^s outra extensão de ν para $\mathbb{K}^s$. Pelo Corolário D.23, existe $\iota \in \mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K})$ tal que $\mu^s = \nu^s \circ \iota$. Logo, $G^d(\mu^s) = G^d(\nu^s \circ \iota)$. Vejamos que $G^d(\nu^s \circ \iota) = \iota^{-1} G^d(\nu^s)\iota$. De fato, se $\iota^{-1}\sigma\iota \in \iota^{-1}G^d(\nu^s)\iota$, então $\sigma \in G^d(\nu^s)$ e

$$\nu^s \circ \iota \circ \iota^{-1}\sigma\iota = \nu^s \circ \sigma \circ \iota = \nu^s \circ \iota.$$

Assim, $\iota^{-1}\sigma\iota \in G^d(\nu^s \circ \iota)$. Por outro lado, se $\tau \in G^d(\nu^s \circ \iota)$, então $\nu^s \circ \iota \circ \tau = \nu^s \circ \iota$. Aplicando ι^{-1} em ambos os lados da equação, temos $\nu^s \circ (\iota \circ \tau \circ \iota^{-1}) = \nu^s$. Logo, $\sigma = \iota \circ \tau \circ \iota^{-1} \in G^d(\nu^s)$, o que implica $\tau = \iota^{-1} \circ \sigma \circ \iota \in \iota^{-1}G^d(\nu^s)\iota$. Portanto, $\mathrm{G^d}(\mu^s) = \iota^{-1}\mathrm{G^d}(\nu^s)\iota$. Olhando agora para os corpos fixados $\mathbb{K}^d(\mu^s)$ e $\mathbb{K}^d(\nu^s)$, vemos que

$$\begin{aligned} a \in \mathbb{K}^d(\mu^s) &\iff \sigma(a) = a \text{ para todo } \sigma \in G^d(\mu^s) \\ &\iff (\iota^{-1}\tau\iota)(a) = a \text{ para todo } \tau \in G^d(\nu^s) \\ &\iff \tau(\iota(a) = \iota(a) \text{ para todo } \tau \in G^d(\nu^s) \\ &\iff \iota(a) \in \mathbb{K}^d(\nu^s) \\ &\iff a \in \iota^{-1}(\mathbb{K}^d(\nu^s)). \end{aligned}$$

Isto é, $\mathbb{K}^d(\mu^s) = \iota^{-1}(\mathbb{K}^d(\nu^s))$. Ou seja, $\iota^{-1}|_{\mathbb{K}^d(\nu^s)} : \mathbb{K}^d(\nu^s) \hookrightarrow \mathbb{K}^d(\mu^s)$ é sobrejetora, logo um isomorfismo. Concluímos que $\mathbb{K}^d(\nu^s) \cong \mathbb{K}^d(\mu^s)$ através do isomorfismo $\iota^{-1}|_{\mathbb{K}^d(\nu^s)}$. Ainda,

$$\mu^d = \mu^s|_{\mathbb{K}^d(\mu^s)} = (\nu^s \circ \iota)|_{\mathbb{K}^d(\mu^s)} = \nu^s|_{\mathbb{K}^d(\nu^s)} \circ \iota|_{\mathbb{K}^d(\mu^s)} = \nu^d \circ \iota|_{\mathbb{K}^d(\mu^s)}.$$

Suponhamos agora que $\sigma \in \mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K})$ é outro automorfismo tal que $\sigma^{-1}|_{\mathbb{K}^d(\nu^s)}$ é um

isomorfismo entre $\mathbb{K}^d(\nu^s)$ e $\mathbb{K}^d(\mu^s)$ e $\mu^d = \nu^d \circ \sigma|_{\mathbb{K}^d(\mu^s)}$. Logo, em $\mathbb{K}^d(\mu^s) = \iota^{-1}(\mathbb{K}^d(\nu^s))$ temos

$$\nu^s \circ \sigma = \nu^d \circ \sigma = \mu^d = \nu^s \circ \iota,$$

o que implica $\nu^s \circ (\sigma \circ \iota^{-1}) = \nu^s$. Assim, ν^s e $\nu^s \circ (\sigma \circ \iota^{-1})$ são duas extensões de ν^d para $\mathbb{K}^s$. Como $(\mathbb{K}^d(\nu^s), \nu^d)$ é henseliano, segue que $\nu^s = \nu^s \circ (\sigma \circ \iota^{-1})$ em $\mathbb{K}^s$. Porém, isso ocorre se, e somente se, $\sigma \circ \iota^{-1} \in G^d(\nu^s)$, pela forma como foi definido este grupo. Pela definição de $\mathbb{K}^d(\nu^s)$, como $\sigma \circ \iota^{-1} \in G^d(\nu^s)$, segue que $(\sigma \circ \iota^{-1})(b) = b$ para todo $b \in \mathbb{K}^d(\nu^s)$. Ou seja, $\sigma^{-1} = \iota^{-1}$, mostrando que ι^{-1} é o único isomorfismo entre $\mathbb{K}^d(\nu^s)$ e $\mathbb{K}^d(\mu^s)$ tal que $\mu^d = \nu^d \circ \iota|_{\mathbb{K}^d(\mu^s)}$.

■

Proposição E.8. *Seja $(\mathbb{L}, \mu)$ uma extensão de $(\mathbb{K}, \nu)$ tal que $\mathbb{L} \mid \mathbb{K}$ é uma extensão algébrica separável e $(\mathbb{L}, \mu)$ é henseliano. Então existe um único $\mathbb{K}$-mergulho $\tau : \mathbb{K}^d(\nu^s) \hookrightarrow \mathbb{L}$ tal que $\mu \circ \tau = \nu^d$. Além disso, $\mathbb{K}^d(\mu^s) \subseteq \mathbb{L}$.*

Demonstração: Uma vez que $\mathbb{L} \mid \mathbb{K}$ é algébrica e separável, podemos considerar $\mathbb{L} \subseteq \mathbb{K}^s$, tomando um fecho algébrico comum para $\mathbb{K}$ e $\mathbb{L}$. Como $(\mathbb{L}, \mu)$ é henseliano por hipótese, seja μ^s a única extensão de μ para $\mathbb{K}^s$. Então, $\mathrm{Gal}(\mathbb{K}^s \mid \mathbb{L}) \subseteq G^d(\mu^s)$ pois, para qualquer $\sigma \in \mathrm{Gal}(\mathbb{K}^s \mid \mathbb{L})$, como $\sigma(a) = a$ para todo $a \in \mathbb{L}$, temos que

$$(\mu^s \circ \sigma)(a) = \mu^s(\sigma(a)) = \mu^s(a).$$

Porém, $\mathrm{Gal}(\mathbb{K}^s \mid \mathbb{L}) \subseteq G^d(\mu^s)$ se, e somente se, $\mathbb{K}^d(\mu^s) \subseteq \mathbb{L}$. Como μ^s também é uma extensão de ν para $\mathbb{K}^s$, vimos que existe um único $\iota \in \mathrm{Gal}(\mathbb{K}^s \mid \mathbb{K})$ tal que $\mu^s = \nu^s \circ \iota$ e $\mathbb{K}^d(\mu^s) = \iota^{-1}|_{\mathbb{K}^d(\nu^s)}(\mathbb{K}^d(\nu^s))$. Como $\mathbb{K}^d(\mu^s) \subseteq \mathbb{L}$, vemos que $\tau = \iota^{-1}|_{\mathbb{K}^d(\nu^s)}$ é um $\mathbb{K}$-mergulho de $\mathbb{K}^s(\nu^s)$ em $\mathbb{L}$.

Agora, como $\mu^s|_{\mathbb{L}} = \mu$ e $\mu^s = \nu^s \circ \iota$, isto é, $\mu^s \circ \iota^{-1} = \nu^s$, temos

$$\nu^d = \nu^s|_{\mathbb{K}^d(\nu^s)} = (\mu^s \circ \iota^{-1})|_{\mathbb{K}^d(\nu^s)} = \mu^s|_{\mathbb{L}} \circ \iota^{-1}|_{\mathbb{K}^d(\nu^s)} = \mu \circ \tau.$$

Vejamos agora a unicidade de τ. Seja $\kappa : \mathbb{K}^d \longrightarrow \mathbb{L}$ outro $\mathbb{K}$-mergulho tal que $\mu \circ \kappa = \nu^d$. Como vimos na seção anterior, o par $(\kappa(\mathbb{K}^d), \mu')$ é henseliano, com $\mu' = \mu|_{\kappa(\mathbb{K}^d)}$. Pelo que foi provado acima, $\mathbb{K}^d(\mu^s) \subseteq \kappa(\mathbb{K}^d)$. Por outro lado, $(\kappa^{-1}(\mathbb{K}^d(\mu^s)), \nu')$ é henseliano, com $\nu' = \nu^s|_{\kappa^{-1}(\mathbb{K}^d(\mu^s))}$. Logo, $\mathbb{K}^d(\nu^s) \subseteq \kappa^{-1}(\mathbb{K}^d(\mu^s))$ e concluímos que $\mathbb{K}^d(\nu^s) = \kappa^{-1}(\mathbb{K}^d(\mu^s))$. Dessa forma, τ e κ são dois isomorfismos entre $\mathbb{K}^d(\nu^s)$ e $\mathbb{K}^d(\mu^s)$ tais que $\mu^d = \nu^d \circ \tau^{-1}$ e $\mu^d = \nu^d \circ \kappa^{-1}$. Pela unicidade vista no Item 2 da Proposição E.7, devemos ter $\kappa = \tau$.

■

Corolário E.9. *Temos que $(\mathbb{K},\nu)$ é henseliano se, e somente se, $(\mathbb{K},\nu)=(\mathbb{K}^d(\nu^s),\nu^d)$.*

Demonstração:

($\Rightarrow$) Se $(\mathbb{K},\nu)$ é henseliano, então seja ν^s a única extensão de ν para $\mathbb{K}^s$. Pelo resultado anterior, $\mathbb{K}^d(\nu^s)\subseteq\mathbb{K}$. Logo, como sempre $\mathbb{K}\subseteq\mathbb{K}^d(\nu^s)$, segue que $\mathbb{K}=\mathbb{K}^d(\nu^s)=\mathbb{K}^d$. Ainda pelo resultado anterior, existe um único $\mathbb{K}$-mergulho $\tau:\mathbb{K}^d\hookrightarrow\mathbb{K}$ tal que $\nu\circ\tau=\nu^d$. Como a identidade é um $\mathbb{K}$-mergulho de $\mathbb{K}^d$ em $\mathbb{K}$, devemos ter, pela unicidade, que τ é a identidade e portanto $\nu=\nu\circ\tau=\nu^d$.

($\Leftarrow$) Imediato, pois $(\mathbb{K}^d,\nu^d)$ é henseliano.

■

Lema E.10. *Seja $(\mathbb{L},\mu)$ uma extensão de $(\mathbb{K},\nu)$ tal que $\mathbb{L}\mid\mathbb{K}$ é uma extensão qualquer e $(\mathbb{L},\mu)$ é henseliano. Tomemos $\overline{\mathbb{L}}=\overline{\mathbb{K}}$ e seja $\mathbb{K}^s\cap\mathbb{L}$ o fecho separável relativo de $\mathbb{K}$ em $\mathbb{L}$. Então $(\mathbb{K}^s\cap\mathbb{L},\mu')$ é henseliano, com $\mu'=\mu|_{\mathbb{K}^s\cap\mathbb{L}}$.*

Demonstração: Começamos observando que $\mathbb{K}^s\subseteq\mathbb{L}^s$. De fato, se $\alpha\in\mathbb{K}^s$, então seu polinômio minimal $m_\alpha(x)\in\mathbb{K}[x]$ é separável, ou seja, não possui raízes repetidas em $\overline{\mathbb{K}}=\overline{\mathbb{L}}$. Assim, sendo $m'_\alpha(x)\in\mathbb{L}[x]$ o polinômio minimal de α sobre $\mathbb{L}$, devemos ter que $m'_\alpha(x)\mid m_\alpha(x)$. Assim, $m'_\alpha(x)$ é separável, logo $\alpha\in\mathbb{L}^s$.

Também observamos que $(\mathbb{K}^s\cap\mathbb{L})^s=\mathbb{K}^s$. De fato, como $\mathbb{K}\subseteq\mathbb{K}^s$ e $\mathbb{K}\subseteq\mathbb{L}$, segue que $\mathbb{K}\subseteq\mathbb{K}^s\cap\mathbb{L}\subseteq\mathbb{K}^s$. Como $\mathbb{K}^s\mid\mathbb{K}$ é separável, temos que $\mathbb{K}^s\mid\mathbb{K}^s\cap\mathbb{L}$ e $\mathbb{K}^s\cap\mathbb{L}\mid\mathbb{K}$ são separáveis. Logo, $\mathbb{K}^s\subseteq(\mathbb{K}^s\cap\mathbb{L})^s$. Por outro lado, $\mathbb{K}\subseteq\mathbb{K}^s\cap\mathbb{L}\subseteq(\mathbb{K}^s\cap\mathbb{L})^s$. Como $(\mathbb{K}^s\cap\mathbb{L})^s\mid\mathbb{K}^s\cap\mathbb{L}$ e $\mathbb{K}^s\cap\mathbb{L}\mid\mathbb{K}$ são separáveis, segue que $(\mathbb{K}^s\cap\mathbb{L})^s\mid\mathbb{K}$ é separável. Logo, $\mathbb{K}^s\supseteq(\mathbb{K}^s\cap\mathbb{L})^s$, donde segue a igualdade.

Seja μ'^s uma extensão de μ' para $(\mathbb{K}^s\cap\mathbb{L})^s=\mathbb{K}^s$. Seja μ^s a única extensão de μ em $\mathbb{L}$ para $\mathbb{L}^s$ (única pois $(\mathbb{L},\mu)$ é henseliano). Mostremos que $(\mathbb{K}^s\cap\mathbb{L})^d(\mu'^s)\subseteq\mathbb{K}^s\cap\mathbb{L}^d(\mu^s)$. De fato, como por definição

$$(\mathbb{K}^s\cap\mathbb{L})^d(\mu'^s)\subset(\mathbb{K}^s\cap\mathbb{L})^s=\mathbb{K}^s,$$

basta vermos que $(\mathbb{K}^s\cap\mathbb{L})^d(\mu'^s)\subset\mathbb{L}^d(\mu^s)$. Seja $a\in(\mathbb{K}^s\cap\mathbb{L})^d(\mu'^s)\subset\mathbb{K}^s\subset\mathbb{L}^s$. Seja $\sigma\in G^d(\mu^s)\subset\mathrm{Gal}(\mathbb{L}^s\mid\mathbb{L})$ qualquer. Pela Proposição A.71 (Apêndice A), temos $\sigma|_{\mathbb{K}^s}\in\mathrm{Gal}(\mathbb{K}^s\mid\mathbb{K}^s\cap\mathbb{L})$. Como $\mu^s\circ\sigma=\mu^s$, segue que $\mu'^s\circ\sigma|_{\mathbb{K}^s}=\mu'^s$, ou seja, $\sigma|_{\mathbb{K}^s}\in G^d(\mu'^s)$. Mas, pela definição de $(\mathbb{K}^s\cap\mathbb{L})^d(\mu'^s)$, devemos ter $\sigma(a)=\sigma|_{\mathbb{K}^s}(a)=a$. Logo, para qualquer $\sigma\in G^d(\mu^s)$ e qualquer $a\in(\mathbb{K}^s\cap\mathbb{L})^d(\mu'^s)$, temos $\sigma(a)=a$. Portanto, $(\mathbb{K}^s\cap\mathbb{L})^d(\mu'^s)\subset\mathbb{L}^d(\mu^s)$.

Dessa forma, $(\mathbb{K}^s\cap\mathbb{L})^d(\mu'^s)\subset\mathbb{K}^s\cap\mathbb{L}^d(\mu^s)$. Porém, como $(\mathbb{L},\mu)$ é henseliano, então $\mathbb{L}^d(\mu^s)=\mathbb{L}$. Assim, $(\mathbb{K}^s\cap\mathbb{L})^d(\mu'^s)\subset\mathbb{K}^s\cap\mathbb{L}$. Mas, sempre temos $\mathbb{K}^s\cap\mathbb{L}\subseteq(\mathbb{K}^s\cap\mathbb{L})^d(\mu'^s)$. Portanto, $(\mathbb{K}^s\cap\mathbb{L})^d(\mu'^s)=\mathbb{K}^s\cap\mathbb{L}$. Vemos então que $(\mathbb{K}^s\cap\mathbb{L},\mu')$ é henseliano pelo Corolário E.9

■

Podemos agora estender o resultado da Proposição E.8 para uma extensão $\mathbb{L}\mid\mathbb{K}$ qualquer.

Corolário E.11. *Seja* $(\mathbb{L}, \mu)$ *uma extensão de* $(\mathbb{K}, \nu)$ *tal que* $\mathbb{L} \mid \mathbb{K}$ *é uma extensão qualquer e* $(\mathbb{L}, \mu)$ *é henseliano. Então existe um único* $\mathbb{K}$*-mergulho* $\tau : \mathbb{K}^d(\nu^s) \hookrightarrow \mathbb{L}$ *tal que* $\mu \circ \tau = \nu^d$.

Demonstração: Seja $(\mathbb{K}^s \cap \mathbb{L}, \mu')$ com $\mu' = \mu|_{\mathbb{K}^s \cap \mathbb{L}}$. Pelo que acabamos de ver, temos que $(\mathbb{K}^s \cap \mathbb{L}, \mu')$ é henseliano. Como $\mathbb{K}^s \cap \mathbb{L} \mid \mathbb{K}$ é uma extensão algébrica e separável, aplicamos a Proposição E.8 e garantimos dessa forma a existência de um único $\mathbb{K}$-mergulho $\mathbb{K}^d(\nu^s) \hookrightarrow \mathbb{K}^s \cap \mathbb{L} \subseteq \mathbb{L}$ tal que $\mu \circ \tau = \mu|_{\mathbb{K}^s \cap \mathbb{L}} \circ \tau = \nu^d$.

■

Devido à propriedade descrita no corolário acima, o par $(\mathbb{K}^d, \nu^d)$ será chamado de **henselização** de $(\mathbb{K}, \nu)$. Na literatura, é comum definir a henselização de um par $(\mathbb{K}, \nu)$ como sendo um par $(\mathbb{K}^h, \nu^h)$ henseliano tal que, para qualquer extensão $(\mathbb{L}, \mu)$ de $(\mathbb{K}, \nu)$ com $(\mathbb{L}, \mu)$ henseliano, existe um $\mathbb{K}$-mergulho $\iota : \mathbb{K}^h \hookrightarrow \mathbb{L}$ tal que $\mu \circ \iota = \nu^h$ (BENGUS-LASNIER, 2021, p. 23). Nessa forma de apresentação do conceito, o par $(\mathbb{K}^d, \nu^d)$ é um exemplo de henselização. Porém, quaisquer duas henselizações são isomorfas (ENGLER; PRESTEL, 2005, p. 121). Logo, não perdemos em generalidade ao definirmos a henselização de $(\mathbb{K}, \nu)$ como sendo o corpo de decomposição $\mathbb{K}^d$ e sua valorização ν^d.

Conforme vimos nos resultados acima, a henselização $(\mathbb{K}^d, \nu^d)$ está mergulhada em todo par henseliano que contém $(\mathbb{K}, \nu)$. Dessa forma, podemos enxergar a henselização como o menor par henseliano que contém $(\mathbb{K}, \nu)$.

E.3 Extensões de valorizações de $\overline{\mathbb{K}}$ e $\mathbb{K}[x]$ para $\overline{\mathbb{K}}[x]$

Sejam ν uma valorização em $\mathbb{K}$, $\overline{\nu}$ uma extensão de ν para $\overline{\mathbb{K}}$ e μ uma extensão de ν para $\mathbb{K}[x]$. Suponhamos que μ seja uma valorização de Krull. Queremos estudar as valorizações que estendem ambas $\overline{\nu}$ e μ para $\overline{\mathbb{K}}[x]$. Usaremos como base o trabalho de Bengus-Lasnier (2021, p. 24).

Denotando também por μ a única extensão de μ em $\mathbb{K}[x]$ para $\mathbb{K}(x)$, seja $\mathcal{E}(\mu, \mathbb{K}(x), \overline{\mathbb{K}}(x))$ o conjunto de todas as extensões de μ de $\mathbb{K}(x)$ para $\overline{\mathbb{K}}(x)$. Analogamente, definimos $\mathcal{E}(\mu, \mathbb{K}[x], \overline{\mathbb{K}}[x])$ e $\mathcal{E}(\overline{\nu}, \overline{\mathbb{K}}, \overline{\mathbb{K}}[x])$. Suponhamos que $\overline{\mu}$ seja uma extensão de ambas μ e $\overline{\nu}$ para $\overline{\mathbb{K}}[x]$. Denotemos a única extensão de $\overline{\mu}$ de $\overline{\mathbb{K}}[x]$ para $\overline{\mathbb{K}}(x)$ também por $\overline{\mu}$. Ou seja, $\overline{\mu}$ pertence a $\mathcal{E}(\mu, \mathbb{K}(x), \overline{\mathbb{K}}(x))$. Uma vez que a extensão $\overline{\mathbb{K}}(x) \mid \mathbb{K}(x)$ é normal, vimos no Corolário D.23 que se $\iota \in \mathrm{Aut}(\overline{\mathbb{K}}(x) \mid \mathbb{K}(x))$, então $\overline{\mu} \circ \iota$ em $\overline{\mathbb{K}}(x)$ é um prolongamento de μ em $\mathbb{K}(x)$. Para além disso, como $\iota|_{\mathbb{K}[x]} = \mathrm{id}_{\mathbb{K}[x]}$ para qualquer $\iota \in \mathrm{Aut}(\overline{\mathbb{K}}(x) \mid \mathbb{K}(x))$, temos

$$(\overline{\mu} \circ \iota)|_{\mathbb{K}[x]} = \overline{\mu}|_{\mathbb{K}[x]} \circ \iota|_{\mathbb{K}[x]} = \mu \circ \mathrm{id}_{\mathbb{K}[x]} = \mu.$$

Observamos que $\iota(\overline{\mathbb{K}}) = \overline{\mathbb{K}}$ e, como x é fixado por ι, também $\iota(\overline{\mathbb{K}}[x]) = \overline{\mathbb{K}}[x]$. Concluímos que $(\overline{\mu} \circ \iota)|_{\overline{\mathbb{K}}[x]}$ é uma valorização em $\overline{\mathbb{K}}[x]$ que estende μ.

Suponhamos agora que μ' seja outra extensão de μ para $\overline{\mathbb{K}}[x]$. Levando μ' para $\overline{\mathbb{K}}(x)$, esta se torna uma extensão de μ em $\mathbb{K}(x)$ para $\overline{\mathbb{K}}(x)$. Assim, existe $\iota \in \mathrm{Aut}(\overline{\mathbb{K}}(x) \mid \mathbb{K}(x))$ tal que $\mu' = \overline{\mu} \circ \iota$. Dessa forma, μ' em $\overline{\mathbb{K}}[x]$ é igual a $\overline{\mu} \circ \iota|_{\overline{\mathbb{K}}[x]}$, donde concluímos que

$$\mathcal{E}(\mu, \mathbb{K}[x], \overline{\mathbb{K}}[x]) = \{\overline{\mu} \circ \iota|_{\overline{\mathbb{K}}[x]} \mid \iota \in \mathrm{Aut}(\overline{\mathbb{K}}(x) \mid \mathbb{K}(x))\}.$$

Lembrando que $\overline{\mu}$ é também, por hipótese, uma extensão de $\overline{\nu}$ para $\overline{\mathbb{K}}[x]$, vejamos o que é necessário para que uma valorização da forma $\overline{\mu} \circ \iota|_{\overline{\mathbb{K}}[x]}$ seja uma extensão de $\overline{\nu}$ para $\overline{\mathbb{K}}[x]$. Temos:

$$\begin{aligned}
\overline{\mu} \circ \iota|_{\overline{\mathbb{K}}[x]} \in \mathcal{E}(\overline{\nu}, \overline{\mathbb{K}}, \overline{\mathbb{K}}[x]) &\iff (\overline{\mu} \circ \iota|_{\overline{\mathbb{K}}[x]})|_{\overline{\mathbb{K}}} = \overline{\nu} \\
&\iff \overline{\mu}|_{\overline{\mathbb{K}}} \circ \iota|_{\overline{\mathbb{K}}} = \overline{\nu} \\
&\iff \overline{\nu} \circ \iota|_{\overline{\mathbb{K}}} = \overline{\nu} \\
&\iff \iota|_{\overline{\mathbb{K}}} \in G^d(\overline{\nu}) := \{\sigma \in \mathrm{Aut}(\overline{\mathbb{K}} \mid \mathbb{K}) \mid \overline{\nu} \circ \sigma = \overline{\nu}\}.
\end{aligned}$$

A conclusão dessa argumentação está sintetizada na Proposição E.12.

Proposição E.12. *Fixada $\overline{\mu}$ uma extensão de μ e de $\overline{\nu}$ para $\overline{\mathbb{K}}[x]$ temos:*

$$\mathcal{E}(\overline{\nu}, \overline{\mathbb{K}}, \overline{\mathbb{K}}[x]) \cap \mathcal{E}(\mu, \mathbb{K}[x], \overline{\mathbb{K}}[x]) = \{\overline{\mu} \circ \iota|_{\overline{\mathbb{K}}[x]} \mid \iota \in \mathrm{Aut}(\overline{\mathbb{K}}(x) \mid \mathbb{K}(x)) \text{ e } \iota|_{\overline{\mathbb{K}}} \in \mathrm{G}^d(\overline{\nu})\}.$$

■

No Capítulo 4, utilizamos essa proposição e outros resultados para descrever essas extensões comuns quando a valorização $\overline{\mu}$ for trocada por uma valorização monomial (apresentada no fim do Capítulo 1, na Seção 1.4) e a valorização μ for trocada por um tipo especial de valorização, a saber as que são definidas por meio do processo de truncamento em um polinômio-chave. Estas últimas noções (truncamento e polinômio-chave) foram apresentadas no Capítulo 2.

Apêndice F

Derivada de Hasse

Neste apêndice, provaremos propriedades da derivada de Hasse, ferramenta utilizada no estudo dos polinômios-chaves no Capítulo 2.

A principal referência para a composição deste apêndice foram as notas de aula de Novacoski (2020).

F.1 A Derivada de Hasse

Definição F.1. *Sejam $f(x) = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{K}[x]$ e $k \in \mathbb{N}_0$. A **derivada de Hasse** de ordem k de f é o polinômio $\partial_k f$ definido como*

$$(\partial_k f)(x) = \sum_{i=k}^{n} \binom{i}{k} a_i x^{i-k} \in \mathbb{K}[x].$$

■

Quando $k = 0$, temos $\partial_0 f = f$. Quando $k > n$, temos $\partial_k f$ o polinômio identicamente nulo. Quando $k = 1$, temos

$$(\partial_1 f)(x) = \sum_{i=1}^{n} \binom{i}{1} a_i x^{i-1} = \sum_{i=1}^{n} i a_i x^{i-1} = f'(x),$$

que é a derivada formal de f.

Provaremos algumas propriedades da derivada de Hasse que são importantes para o desenvolvimento do texto principal. Como caso particular, teremos provado as principais propriedades da derivada formal de um polinômio.

Proposição F.2. *Sejam $f, g \in \mathbb{K}[x]$ polinômios quaisquer, $a \in \mathbb{K}$ e $k, l \in \mathbb{N}_0$.*

(i) $k!\partial_k f = \dfrac{d^k}{dx^k} f$, *em que* $\dfrac{d^k}{dx^k}$ *indica a aplicação da derivada formal k vezes.*

(ii) $\partial_k \partial_l f = \binom{k+l}{l} \partial_{k+l} f$.

(iii) (Expansão de Taylor) $f(x) = f(a) + \sum_{k=1}^{m} \partial_k f(a)(x-a)^k$, *para algum $m \in \mathbb{N}_0$. Se f é não nulo, então $m = \deg(f)$. Além disso, os coeficientes $\partial_k f(a)$, $0 \leq k \leq m$, são os únicos que fazem valer tal igualdade.*

(iv) (Regra de Leibniz) $\partial_k(fg) = \sum_{j=0}^{k} (\partial_j f)(\partial_{k-j} g)$.

Demonstração:

(i) Vejamos inicialmente que a derivada de Hasse é linear, isto é, dados $c, b \in \mathbb{K}$ e $f, g \in \mathbb{K}[x]$ vale $\partial_k(cf + bg) = c\partial_k f + b\partial_k g$. De fato, sejam

$$f(x) = \sum_{i=0}^{n} c_i x^i \text{ e } g(x) = \sum_{i=0}^{m} b_i x^i$$

com $n \geq m$. Colocando $b_i = 0$ para $i > m$, temos

$$\begin{aligned}
\partial_k (cf + bg) &= \partial_k \left(\sum_{i=0}^{n} (cc_i + bb_i) x^i \right) = \sum_{i=k}^{n} \binom{i}{k} (cc_i + bb_i) x^{i-k} \\
&= \sum_{i=k}^{n} \binom{i}{k} (cc_i x^{i-k} + bb_i x^{i-k}) = \sum_{i=k}^{n} \binom{i}{k} cc_i x^{i-k} + \sum_{i=k}^{n} \binom{i}{k} bb_i x^{i-k} \\
&= a \sum_{i=k}^{n} \binom{i}{k} c_i x^{i-k} + b \sum_{i=k}^{m} \binom{i}{k} b_i x^{i-k} \\
&= c\partial_k f + b\partial_k g.
\end{aligned}$$

Logo, é suficiente verificar a afirmação para $f(x) = x^n$, $n \in \mathbb{N}_0$. Como ainda $\partial_k x^n = 0$ se $k > n$, podemos nos restringir a $k \leq n$. Temos

$$\begin{aligned}
k!\partial_k f = k! \binom{n}{k} x^{n-k} &= k! \frac{n!}{k!(n-k)!} x^{n-k} \\
&= n(n-1)\cdots(n-k+1)x^{n-k} = \frac{d^k}{dx^k} x^n.
\end{aligned}$$

(ii) Pela linearidade, é suficiente mostrar o resultado para $f(x) = x^n$ com $k + l \leq n$. Temos

$$\begin{aligned}
\partial_k \partial_l f &= \partial_k \left(\binom{n}{l} x^{n-l} \right) = \binom{n-l}{k} \binom{n}{l} x^{n-l-k} \\
&= \frac{(n-l)!}{k!(n-l-k)!} \cdot \frac{n!}{l!(n-l)!} x^{n-l-k} \\
&= \frac{n!}{k!\, l!\, (n-l-k)!} x^{n-l-k} \\
&= \frac{(k+l)!}{k!\, l!} \cdot \frac{n!}{(k+l)!\, (n-l-k)!} x^{n-l-k} \\
&= \binom{k+l}{k} \binom{n}{k+l} x^{n-l-k} \\
&= \binom{k+l}{k} \partial_{k+l} f.
\end{aligned}$$

(iii) Para f nulo o resultado é imediato, para qualquer que seja m. Se f é não nulo, novamente mostraremos apenas para $f(x) = x^n$ e o resultado se estende por linearidade. Para $x \neq a$ temos, utilizando o Teorema Binomial,

$$\begin{aligned}
\sum_{i=0}^{\deg(f)} \partial_i f(a)(x-a)^i &= \sum_{i=0}^{n} \left(\binom{n}{i} x^{n-i} \right) (a)(x-a)^i \\
&= \sum_{i=0}^{n} \binom{n}{i} a^{n-i} (x-a)^i \\
&= (a + (x-a))^n = x^n = f(x).
\end{aligned}$$

Além disso, vemos que a expansão de Taylor de f é a $(x-a)$-expansão de f. Segue que os coeficientes $\partial_k f(a)$ são únicos, pois a $(x-a)$-expansão é única.

(iv) Para qualquer $a \in \mathbb{K}$, se $x \neq a$, temos pelo Item (iii) que

$$\begin{aligned}
(fg)(x) &= f(x)g(x) \\
&= \left(\sum_{i=0}^{\deg(f)} \partial_i f(a)(x-a)^i \right) \left(\sum_{i=0}^{\deg(g)} \partial_i g(a)(x-a)^i \right) \\
&= \sum_{k=0}^{\deg(f)+\deg(g)} \left(\sum_{j=0}^{k} (\partial_j f)(\partial_{k-j} g) \right) (a)(x-a)^k.
\end{aligned}$$

Esta última expressão é justamente a $(x-a)$-expansão de fg, que como vimos coincide com a expansão de Taylor. Logo, segue da unicidade dos coeficientes da expansão que

$$\partial_k (fg)(a) = \left(\sum_{j=0}^{k} (\partial_j f)(\partial_{k-j} g) \right) (a)$$

para todo $a \in \mathbb{K}$. Portanto, temos o resultado.

■

Corolário F.3. *Se, para algum $a \in \mathbb{K}$, $(\partial_k f)(a) = 0$ para todo $k \in \mathbb{N}_0$, então f é o polinômio identicamente nulo.*

Demonstração: Pela expansão de Taylor, para algum $m \in \mathbb{N}_0$, temos

$$f(x) = f(a) + \sum_{k=1}^{m} (\partial_k f)(a)(x-a)^k.$$

Mas, por hipótese, $(\partial_k f)(a) = 0$ para todo $k \in \mathbb{N}_0$. Ou seja, a expressão acima representa o polinômio nulo.

■

Corolário F.4. *Para todo $f \in \mathbb{K}[x]$ e todo $a, b \in \mathbb{K}$ temos*

$$f(b) - f(a) = \sum_{i=1}^{m} (\partial_i f)(a)(b-a)^i.$$

Demonstração: Basta colocar $x = b$ na expansão de Taylor de f para a.

■

A seguir, denotaremos por $N_r = \{1, 2, \ldots, r\}$, para $r \in \mathbb{N}$, e $N_0 = \emptyset$. Denotaremos por $|I|$ o cardinal de um conjunto I.

Proposição F.5. *Suponhamos*

$$f(x) = \prod_{i=1}^{n} (x - c_i) \text{ com } c_i \in \mathbb{K}.$$

Para todo k, $1 \leq k \leq n$, temos

$$\partial_k f = \sum_{\substack{I \subset N_n \\ |I|=k}} \left(\prod_{i \in N_n \setminus I} (x - c_i) \right).$$

Demonstração: Provaremos por indução em n e em k. Porém, antes observemos que se $k = n$, então o resultado segue. Escrevendo

$$f(x) = \prod_{i=1}^{n} (x - c_i) = \sum_{i=0}^{n} a_i x^i, \text{ com } a_i \in \mathbb{K},$$

temos

$$\partial_n f = \sum_{i=n}^{n} \binom{i}{n} a_i x^{i-n} = a_n = 1$$

e, por convenção,

$$\sum_{\substack{I \subset N_n \\ |I|=n}} \left(\prod_{i \in N_n \setminus I} (x - c_i) \right) = \prod_{i \in N_n \setminus N_n} (x - c_i) = 1.$$

Suponhamos então $n \neq k$. Para a base de indução, vejamos que o resultado vale para $n = 2$ e $k = 1$. De fato,

$$\begin{aligned} \partial_1((x - c_1)(x - c_2)) &= \partial_1(x^2 + (-c_1 - c_2)x + c_1 c_2) \\ &= \partial_1(x^2 + a_1 x + a_0) = \sum_{i=1}^{2} \binom{i}{1} a_i x^{i-1} \\ &= a_1 + 2a_2 x = 2x + (-c_1 - c_2) \end{aligned}$$

e

$$\begin{aligned} \sum_{\substack{I \subset N_2 \\ |I|=1}} \left(\prod_{i \in N_2 \setminus I} (x - c_i) \right) &= \prod_{i \in N_2 \setminus \{1\}} (x - c_i) + \prod_{i \in N_2 \setminus \{2\}} (x - c_i) \\ &= x - c_1 + x - c_2 = 2x + (-c_1 - c_2). \end{aligned}$$

Suponhamos que, para algum $n \in \mathbb{N}$ e para algum k, $1 \leq k < n$, o resultado seja válido para todo i, $1 \leq i \leq n - 1$, e para $k - 1$. Lembrando que $\partial_l h = 0$ se $l > \deg(h)$, temos, pela Regra de Leibniz,

$$\begin{aligned} \partial_k \left(\prod_{i=1}^{n} (x - c_i) \right) &= \partial_k \left((x - c_n) \prod_{i=1}^{n-1} (x - c_i) \right) = \sum_{j=0}^{k} \partial_j (x - c_n) \partial_{k-j} \left(\prod_{i=1}^{n-1} (x - c_i) \right) \\ &= (x - c_n) \partial_k \left(\prod_{i=1}^{n-1} (x - c_i) \right) + \overbrace{\partial_{k-1} \left(\prod_{i=1}^{n-1} (x - c_i) \right)}^{P_{k-1,n-1}} \\ &= (x - c_n) \left[\partial_k \left((x - c_{n-1}) \prod_{i=1}^{n-2} (x - c_i) \right) \right] + P_{k-1,n-1}. \end{aligned}$$

Aplicamos novamente a Regra de Leibniz, obtendo

$$\begin{aligned}\partial_k\left(\prod_{i=1}^{n}(x-c_i)\right) &= (x-c_n)\left[\partial_k\left((x-c_{n-1})\prod_{i=1}^{n-2}(x-c_i)\right)\right] + P_{k-1,n-1}\\ &= (x-c_n)\left[(x-c_{n-1})\partial_k\left(\prod_{i=1}^{n-2}(x-c_i)\right) + \overbrace{\partial_{k-1}\left(\prod_{i=1}^{n-2}(x-c_i)\right)}^{P_{k-1,n-2}}\right] + P_{k-1,n-1}\\ &= \prod_{i=n-1}^{n}(x-c_i)\partial_k\left(\prod_{i=1}^{n-2}(x-c_i)\right) + \prod_{i=n-1}^{n-1}(x-c_i)P_{k-1,n-2} + P_{k-1,n-1}.\end{aligned}$$

Aplicando sucessivamente a Regra de Leibniz em $\partial_k\left(\prod_{i=1}^{r}(x-c_i)\right)$ com $1 \leq r \leq n-2$, chegamos a

$$\partial_k\left(\prod_{i=1}^{n}(x-c_i)\right) = \prod_{i=k+1}^{n}(x-c_i)\partial_k\left(\prod_{i=1}^{k}(x-c_i)\right) + \sum_{j=k+2}^{n}\left[\prod_{i=j}^{n}(x-c_i)P_{k-1,j-2}\right] + P_{k-1,n-1}.$$

Porém, vimos que

$$\partial_k\left(\prod_{i=1}^{k}(x-c_i)\right) = 1$$

Logo,

$$\partial_k f = \partial_k\left(\prod_{i=1}^{n}(x-c_i)\right) = \prod_{i=k+1}^{n}(x-c_i) + \sum_{j=k+2}^{n}\left[\prod_{i=j}^{n}(x-c_i)P_{k-1,j-2}\right] + P_{k-1,n-1}. \tag{F.1}$$

Aplicando a hipótese de indução, obtemos da Equação F.1 que

$$\partial_k f = \overbrace{\prod_{i=k+1}^{n}(x-c_i)}^{(1)} + \sum_{j=k+2}^{n}\left[\overbrace{\prod_{i=j}^{n}(x-c_i)\sum_{\substack{I\subset N_{j-2}\\|I|=k-1}}\left(\prod_{i\in N_{j-2}\setminus I}(x-c_i)\right)}^{(2)}\right] + \overbrace{\sum_{\substack{I\subset N_{n-1}\\|I|=k-1}}\left(\prod_{i\in N_{n-1}\setminus I}(x-c_i)\right)}^{(3)}.$$

Em (3) os produtos possuem exatamente $n-1-(k-1) = n-k$ fatores. Cada um destes

não possui o fator $x - c_n$. Assim, em (3) obtemos todos os produtos de $n - k$ fatores que não envolvem $x - c_n$.

Olhemos agora os produtos que possuem o fator $x - c_n$. Vamos particionar o conjunto N_n como $N_n = N_k \cup (N_n \setminus N_k)$. Em (1), temos um produto com $n - k$ fatores envolvendo todos os $x - c_i$ com $i \in N_n \setminus N_k$. Em (2), para cada j, $k + 2 \leq j \leq n$, os produtos de

$$\sum_{\substack{I \subset N_{j-2} \\ |I| = k-1}} \left(\prod_{i \in N_{j-2} \setminus I} (x - c_i) \right)$$

possuem $j - 2 - (k - 1) = j - k - 1$ fatores. Assim, cada produto

$$\prod_{i=j}^{n} (x - c_i) \prod_{i \in N_{j-2} \setminus I} (x - c_i)$$

possui $n - j + 1 + j - k - 1 = n - k$ fatores e envolve $x - c_n$. Além disso, os produto em (2) varrem todas as possibilidades de produtos com $n - k$ fatores em que está presente $x - c_n$ porém apenas alguns $x - c_i$ com $i \in N_n \setminus N_k$ estão presentes (não todos, eventualmente apenas o $x - c_n$).

Dessa forma, passamos por todas as possibilidades de produtos de $n - k$ fatores. Ou seja,

$$\partial_k f = \sum_{\substack{I \subset N_n \\ |I| = k}} \left(\prod_{i \in N_n \setminus I} (x - c_i) \right).$$

■

Apêndice G

Polígonos de Newton

Neste apêndice, apresentaremos a noção de polígono de Newton. Tal objeto nos ajudará a visualizar o valor $\epsilon(f)$ definido no Capítulo 2. Também usaremos os polígonos de Newton para provar a igualdade $\epsilon(f) = \delta(f)$, conforme prometido no Capítulo 2.

As principais referências para a composição deste apêndice foram o trabalho de Bengus-Lasnier (2021) e o livro de Koblitz (1977).

G.1 Definições e construção do polígono de Newton de um conjunto finito

Seja Φ um grupo totalmente ordenado. Consideremos $\Phi_{\mathbb{Q}} \cong \Phi \otimes \mathbb{Q}$. Para $\phi \in \Phi$ e $q \in \mathbb{Q}$, denotamos $\phi \otimes q$ por $q\phi = \phi q$.

Definição G.1. *Sejam $q \in \mathbb{Q}$ e $\alpha, \beta \in \Phi_{\mathbb{Q}}$ fixados. Uma **reta** $L \subseteq \mathbb{Q} \times \Phi_{\mathbb{Q}}$ é um subconjunto da forma*

$$L = L_{q,\alpha,\beta} := \{(x, \phi) \in \mathbb{Q} \times \Phi_{\mathbb{Q}} \mid q\phi + \alpha x + \beta = 0\}.$$

*Quando $q \neq 0$, chamaremos $s(L) = -\alpha/q := \left(-\frac{1}{q}\right)\alpha \in \Phi_{\mathbb{Q}}$ de **inclinação** de L.*

■

Sempre existe uma linha passando por dois pontos distintos de $\mathbb{Q} \times \Phi_{\mathbb{Q}}$, isto é, uma reta L que contém ambos os pontos. De fato, para $P_1 = (x_1, \phi_1), P_2 = (x_2, \phi_2) \in \mathbb{Q} \times \Phi_{\mathbb{Q}}$, tomando $q = x_2 - x_1$, $\alpha = \phi_1 - \phi_2$ e $\beta = x_1\phi_2 - x_2\phi_1$ temos que a reta $L_{q,\alpha,\beta}$ contém o ponto P_1 pois

$$q\phi_1 + \alpha x_1 + \beta = (x_2 - x_1)\phi_1 + (\phi_1 - \phi_2)x_1 + x_1\phi_2 - x_2\phi_1 = 0$$

e, por uma conta análoga, $L_{q,\alpha,\beta}$ também contém P_2. Neste caso, denotamos a reta $L_{q,\alpha,\beta}$ por $L_{P_1P_2}$ e podemos ver que $s(L_{P_1P_2}) = -\alpha/q = (\phi_2 - \phi_1)/(x_2 - x_1)$.

Considerando $m_x = \min\{x_1, x_2\}$, $M_x = \max\{x_1, x_2\}$, $m_\phi = \min\{\phi_1, \phi_2\}$ e $M_\phi = \max\{\phi_1, \phi_2\}$, o **segmento** definido por P_1 e P_2 é o conjunto

$$\overline{P_1P_2} := \{(x', \phi') \in L_{P_1P_2} \mid m_x \leq x' \leq M_x \text{ e } m_\phi \leq \phi' \leq M_\phi\}.$$

Para cada reta $L = L_{q,\alpha,\beta}$ em $\mathbb{Q} \times \Phi_\mathbb{Q}$ ficam definidos os **semiplanos**

$$H^L_{\geq} := \{(x, \phi) \in \mathbb{Q} \times \Phi_\mathbb{Q} \mid q\phi + \alpha x + \beta \geq 0\} \text{ e}$$

$$H^L_{\leq} := \{(x, \phi) \in \mathbb{Q} \times \Phi_\mathbb{Q} \mid q\phi + \alpha x + \beta \leq 0\}.$$

Definição G.2. *Dado um subconjunto $A \subseteq \mathbb{Q} \times \Phi_\mathbb{Q}$, a **envoltória convexa** de A é a interseção de todos os semiplanos que contém A, ou seja,*

$$\text{Conv}(A) := \bigcap_{\substack{H \text{ semiplano} \\ A \subseteq H}} H.$$

■

Uma **face** de A é um subconjunto $F = \text{Conv}(A) \cap L$, em que $L \subset \mathbb{Q} \times \Phi_\mathbb{Q}$ é uma reta satisfazendo

$$\text{Conv}(A) \subset H^L_{\geq} \text{ ou } \text{Conv}(A) \subset H^L_{\leq}$$

e F contém no mínimo dois pontos.

Definição G.3. *Para $X \subseteq \mathbb{Q} \times \Phi_\mathbb{Q}$, o **polígono de Newton** associado ao conjunto X é dado por*

$$\text{PN}(X) := \text{Conv}(\{(x, \phi + \delta) \mid (x, \phi) \in X,\ \delta \in \Phi_\mathbb{Q} \text{ e } \delta \geq 0\}).$$

■

Utilizaremos os polígonos de Newton em um contexto particular, quando X é um subconjunto finito específico de $\mathbb{N}_0 \times \Phi \subset \mathbb{Q} \times \Phi$. Suponhamos

$$X = \{P_i = (i, \gamma_i) \mid 0 \leq i \leq m\}$$

e tomemos $PN(X)$ o polígono de Newton associado ao conjunto X. Neste caso, é possível interpretar geometricamente a construção da envoltória convexa que dá origem ao polígono de Newton.

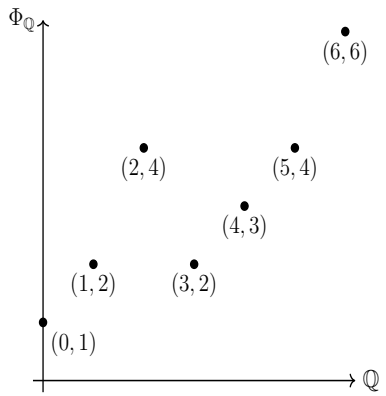


Figura G.1: Exemplo de conjunto X, para $\Phi = \mathbb{Z}$.

- Iniciamos tomando o par $P_0 = (0, \gamma_0)$ e definimos $i_1 = 0$. Consideremos

$$S_{i_1} = \{L_{P_0P_i} \mid 1 \leq i \leq m\}.$$

Seja P_{i_2} tal que $L_{P_0P_{i_2}}$ possui a menor inclinação dentre as retas do conjunto S_0 e i_2 é o maior índice tal que isto ocorre. Tomemos o segmento $\overline{P_{i_1}P_{i_2}}$. Este primeiro passo está representado na Figura G.2.

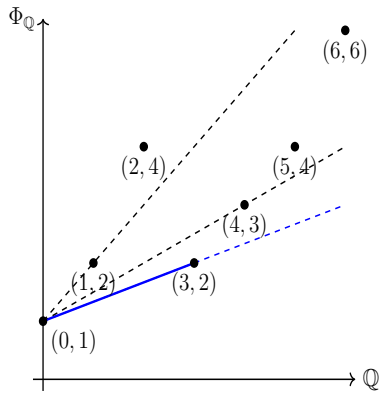


Figura G.2: Passo da construção do Polígono de Newton de X.

- Consideramos então

$$S_{i_2} = \{L_{P_{i_2}P_i} \mid i_2 + 1 \leq i \leq m\}.$$

Definimos P_{i_3} tal que $L_{P_{i_2}P_{i_3}}$ possui a menor inclinação dentre as retas do conjunto S_{i_2} e i_3 é o maior índice tal que isto ocorre. Tomemos o segmento $\overline{P_{i_2}P_{i_3}}$. Este segundo passo está representado na Figura G.3.

- Repetimos este processo sucessivamente até que cheguemos em P_m. Sejam $i_1, i_2, i_3, \ldots, i_{k+1}$ os índices destacados no processo anterior, em que $i_1 = 0$ e $i_{k+1} = m$.

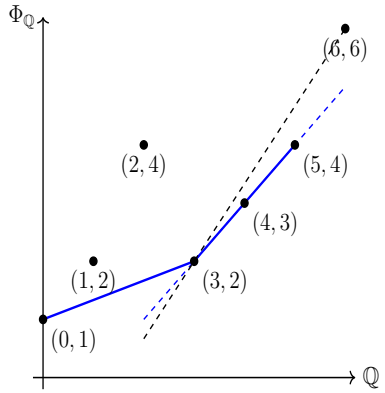


Figura G.3: Passo da construção do Polígono de Newton de X.

- Tomemos os segmentos $\overline{P_{i_l}P_{i_{l+1}}}$, com $1 \leq l \leq k$, e os conjuntos $\{(i, \gamma_i + \delta) \mid \delta \geq 0\}$ para $i = 0$ e $i = m$. Temos a seguinte região P delimitada no cartesiano determinada pela interseção

$$P = \left(\bigcap_{l=1}^{k} H_{\geq}^{L_{P_{i_l}P_{i_{l+1}}}} \right) \cap H^{\gamma_0} \cap H^{\gamma_m},$$

em que $H^{\gamma_0} = \{(x, \phi) \mid x \geq 0\}$ e $H^{\gamma_m} = \{(x, \phi) \mid x \leq m\}$. Uma ilustração da região P está na Figura G.4.

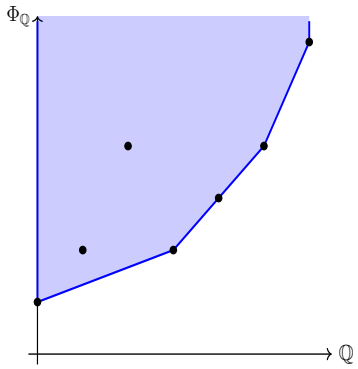


Figura G.4: Resultado dos passos da construção do Polígono de Newton de X

Mostremos que $P = PN(X)$. Seja $Y = \{(x, \phi + \delta) \mid (x, \phi) \in X, \delta \in \Phi_{\mathbb{Q}} \text{ e } \delta \geq 0\}$, de modo que $PN(X) = \text{Conv}(Y)$. Vejamos inicialmente que $Y \subset P$. De fato, seja $(x, \phi) \in Y$. Temos duas opções para este elemento: para algum i, $0 \leq i \leq m$, $(x, \phi) = (i, \gamma_i)$ ou $(x, \phi) = (i, \gamma_i + \delta)$ para algum $\delta \geq 0$. Suponhamos o primeiro caso, $(x, \phi) = (i, \gamma_i)$.

Consideremos os índices $i_1, \ldots, i_{k+1}$ da construção acima. Para simplificar a notação, chamemos $L_{P_{i_l}P_{i_{l+1}}} = L_{l,l+1}$. Mostremos que $(i, \gamma_i) \in H_{\geq}^{L_{l,l+1}}$ para todo l, $1 \leq l \leq k$. Pela propriedade que define i_l e i_{l+1}, o coeficiente angular da reta que passa por P_{i_l} e (i, γ_i) é maior

do que ou igual ao coeficiente angular da reta que passa por P_{i_l} e $P_{i_{l+1}}$. Isto é,

$$\frac{\gamma_i - \gamma_{i_l}}{i - i_l} \geq \frac{\gamma_{i_{l+1}} - \gamma_{i_l}}{i_{l+1} - i_l}.$$

Manipulando esta desigualdade conseguimos:

$$(i_{l+1} - i_l)(\gamma_i - \gamma_{i_l}) \geq (i - i_l)(\gamma_{i_{l+1}} - \gamma_{i_l})$$

se, e somente se,

$$(i_{l+1} - i_l)(\gamma_i - \gamma_{i_l}) \geq i(\gamma_{i_{l+1}} - \gamma_{i_l}) - i_l(\gamma_{i_{l+1}} - \gamma_{i_l})$$

se, e somente se,

$$(i_{l+1} - i_l)(\gamma_i - \gamma_{i_l}) + i_l(\gamma_{i_{l+1}} - \gamma_{i_l}) \geq i(\gamma_{i_{l+1}} - \gamma_{i_l})$$

se, e somente se,

$$-(i_{l+1} - i_l)(\gamma_i - \gamma_{i_l}) - i_l(\gamma_{i_{l+1}} - \gamma_{i_l}) \leq i(\gamma_{i_l} - \gamma_{i_{l+1}}).$$

Assim, como $\alpha = \gamma_l - \gamma_{l+1}$, $q = i_{l+1} - i_l$ e $\beta = i_l\gamma_{i_{l+1}} - \gamma_{i_l}i_{l+1}$, temos

$$\begin{aligned}(i_{l+1} - i_l)\gamma_i + i(\gamma_l - \gamma_{l+1}) + \beta &\geq (i_{l+1} - i_l)\gamma_i - (i_{l+1} - i_l)(\gamma_i - \gamma_{i_l}) - i_l(\gamma_{i_{l+1}} - \gamma_{i_l}) + \beta \\ &= \gamma_{i_l}(i_{l+1} - i_l) - i_l(\gamma_{i_{l+1}} - \gamma_{i_l}) + \beta \\ &= \gamma_{i_l}i_{l+1} - i_l\gamma_{i_{l+1}} + \beta = 0.\end{aligned}$$

Ou seja, $(i, \gamma_i) \in H_{\geq}^{L_{l,l+1}}$.

Agora, se $(x, \phi) = (i, \gamma_i + \delta)$ com $\delta \geq 0$, então

$$(i_{l+1} - i_l)(\gamma_i + \delta) + i(\gamma_l - \gamma_{l+1}) + \beta = (i_{l+1} - i_l)\delta + (i_{l+1} - i_l)\gamma_i + i(\gamma_l - \gamma_{l+1}) + \beta \geq 0,$$

pois $(i_{l+1} - i_l)\delta \geq 0$ e $(i_{l+1} - i_l)\gamma_i + i(\gamma_l - \gamma_{l+1}) + \beta \geq 0$. Dessa forma, $(i, \gamma_i + \delta) \in H_{\geq}^{L_{l,l+1}}$.

Além disso, para todo i, (i, γ_i) e $(i, \gamma_i + \delta)$ pertencem a H^{γ_0} e H^{γ_m}. Assim, vemos que $Y \subset H_{\geq}^{L_{l,l+1}}$ para qualquer l e $Y \subset H^{\gamma_0} \cap H^{\gamma_m}$. Logo,

$$Y \subset P = \left(\bigcap_{l=1}^{k} H_{\geq}^{L_{l,l+1}}\right) \cap H^{\gamma_0} \cap H^{\gamma_m}.$$

Vejamos que $PN(X) = P$.

- $PN(X) \subseteq P$: pela definição de $PN(X)$, temos que $PN(X) \subset H$ para todo semiplano H que contém Y. Logo, consideremos os semiplanos $H_{\geq}^{L_{l,l+1}}$ para todo l, $1 \leq l \leq k$, e os semiplanos H^{γ_0} e H^{γ_m}. Pelo que vimos acima, $Y \subset H_{\geq}^{L_{l,l+1}}$ para todo l, $1 \leq l \leq k$, e $Y \subset H^{\gamma_0} \cap H^{\gamma_m}$. Portanto, $PN(X) \subset H_{\geq}^{L_{l,l+1}}$ para todo l e $PN(X) \subset H^{\gamma_0} \cap H^{\gamma_m}$. Com

isso, $PN(X) \subseteq P$.

- $P \subseteq PN(X)$: Seja $H = H^L_{\geq}$ um semiplano determinado por $L = L_{\alpha,q,\beta}$ tal que $Y \subset H$. Mostremos que $P \subset H$. Seja $(x, \phi) \in P$. Se $(x, \phi) \in Y$, então segue que $(x, \phi) \in H$.

  Suponhamos que (x, ϕ) está contido em algum segmento $\overline{P_{i_l} P_{i_{l+1}}}$. Então, $m_x \leq x \leq M_x$ e $m_\phi \leq \phi \leq M_\phi$, em que $m_x = \min\{i_l, i_{l+1}\}$, $M_x = \max\{i_l, i_{l+1}\}$, $m_\phi = \min\{\gamma_{i_l}, \gamma_{i_{l+1}}\}$ e $M_\phi = \max\{\gamma_{i_l}, \gamma_{i_{l+1}}\}$. Então,

$$q\phi + \alpha x + \beta \geq q m_\phi + \alpha m_x + \beta \geq 0,$$

  logo $(x, \phi) \in H$.

  Suponhamos por fim que $(x, \phi) \in P$ não corresponde aos dois casos anteriores. Considerando os índices $i_1, i_2, \ldots, i_{k+1}$, como estes são distintos, $i_1 = 0$ e $i_{k+1} = m$, temos que estes formam uma partição do intervalo $[0, m]$. Logo, existe l, $1 \leq l \leq k$, tal que $i_l \leq x \leq i_{l+1}$. Tomemos no segmento $\overline{P_{i_l} P_{i_{l+1}}}$ um ponto (x, ϕ'), $m_\phi \leq \phi' \leq M_\phi$. Como (x, ϕ) não está contido em segmento algum, então $\phi > \phi'$. Logo,

$$q\phi + \alpha x + \beta > q\phi' + \alpha x + \beta \geq 0,$$

  pois (x, ϕ') pertence a um segmento, logo pelo caso anterior está em H. Assim, $P \subset H$. Como H é um semiplano qualquer que contém Y, então $P \subseteq PN(X)$.

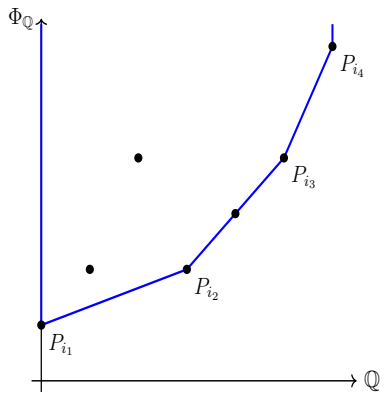


Figura G.5: Vértices e faces do Polígono de Newton.

Portanto $P = PN(X)$. Os pontos P_{i_l}, $1 \leq l \leq k+1$, são os **vértices** do polígono. Os segmentos $\overline{P_{i_l} P_{i_{l+1}}}$ são as faces de $PN(X)$. A inclinação da face/segmento $\overline{P_{i_l} P_{i_{l+1}}}$ é a inclinação da reta $L_{l,l+1}$, que será denotada daqui em diante por

$$\delta_l = \frac{\alpha_l}{q_l} = \frac{\gamma_{i_{l+1}} - \gamma_{i_l}}{i_{l+1} - i_l}.$$

Chamamos $q_l = i_{l+1} - i_l$ de **comprimento** da inclinação δ_l.

G.2 Polígonos de Newton e valorizações

Seja $\mathbb{K}$ um corpo e ν uma valorização em $\mathbb{K}$. Seja $\overline{\mathbb{K}}$ um fecho algébrico de $\mathbb{K}$ fixado. Seja μ uma valorização que estende ν para $\overline{\mathbb{K}}$, sendo $\Gamma = \Gamma_\nu \subset \Gamma_\mu$ os grupos de valores de ν e de μ, respectivamente.

Consideremos

$$g(x) = \sum_{j=0}^{n} a_j x^j = \prod_{j=1}^{n} \left(1 - \frac{x}{c_j}\right) \in \mathbb{K}[x]$$

tal que $a_0 = 1$ e $c_1, \ldots, c_n \in \overline{\mathbb{K}}$ são as raízes de g, listadas com possíveis repetições. Temos $c_i \neq 0$ para todo j, $1 \leq j \leq n$. Sejam $\lambda_j = \mu(1/c_j)$, $1 \leq j \leq n$. Reorganizamos os índices das raízes $c_1, \ldots, c_n$ de modo que $\lambda_1 \leq \lambda_2 \leq \ldots \leq \lambda_n$.

Seja

$$X = \{(j, \nu(a_j)) \mid 0 \leq j \leq n \text{ e } a_j \neq 0\} \subset \mathbb{Q} \times \Gamma_\mu.$$

Consideremos o polígono de Newton $PN(X)$, com os bem definidos δ_l e q_l, $1 \leq l \leq k$.

Proposição G.4. *Para cada inclinação δ_l de $PN(X)$, temos*

$$|\{j \mid \lambda_j = \delta_l\}| = q_l.$$

Mais precisamente, tomemos $r_1, r_2, \ldots, r_t \in \{1, 2, \ldots, n\}$ tais que $r_1 + r_2 + \ldots + r_t = n$ e

$$\begin{aligned} \lambda_1 = \lambda_2 = \ldots = \lambda_{r_1} &< \lambda_{r_1+1} = \lambda_{r_1+2} = \ldots = \lambda_{r_1+r_2} \\ &< \lambda_{r_1+r_2+1} = \lambda_{r_1+r_2+2} = \ldots = \lambda_{r_1+r_2+r_3} \\ &\vdots \\ &< \lambda_{r_1+r_2+\ldots+r_{t-1}+1} = \ldots = \lambda_{r_1+r_2+\ldots+r_t} = \lambda_n. \end{aligned}$$

Então, $t = k$, $\delta_l = \lambda_{r_1+\ldots+r_l}$ e $q_l = r_l$ para todo l, $1 \leq l \leq k$. Além disso,

$$\delta_1 < \delta_2 < \ldots < \delta_k.$$

Demonstração: Digamos que $\lambda_1 = \lambda_2 = \ldots = \lambda_{r_1} < \lambda_{r_1+1}$. Vamos mostrar inicialmente que o primeiro segmento em $PN(X)$, $\overline{P_{i_1}P_{i_2}}$, é o segmento $\overline{P_0P_{r_1}}$, em que $P_0 = (0,0)$ e $P_{r_1} = (r_1, r_1\lambda_1)$.

Para cada j, $0 \leq j < n$, escrevendo $j = n - p_j$ temos, pelas Fórmulas de Viète,

$$a_j = a_{n-p_j} = a_n(-1)^{-p_j} \left[\sum_{1 \leq j_1 < j_2 < \ldots < j_{p_j} \leq n} \left(\prod_{t=1}^{p_j} c_{j_t}\right)\right] \text{ e } a_n = \frac{(-1)^n}{c_1 c_2 \cdots c_n}.$$

Ou seja, sendo $N_n = \{1, 2 \ldots, n\}$,

$$a_j = (-1)^j \left[\sum_{1 \leq j_1 < j_2 < \ldots < j_{p_j} \leq n} \left(\prod_{j_t \in N_n \setminus \{j_1, j_2, \ldots, j_{p_j}\}} \frac{1}{c_{j_t}} \right) \right].$$

Calculando o valor de a_j, vemos que

$$\nu(a_j) = \mu(a_j) = j\mu(-1) + \mu \left(\sum_{1 \leq j_1 < j_2 < \ldots < j_p \leq n} \left(\prod_{j_t \in N_n \setminus \{j_1, j_2, \ldots, j_{p_j}\}} \frac{1}{c_{j_t}} \right) \right)$$

$$\geq \min_{1 \leq j_1 < j_2 < \ldots < j_{p_j} \leq n} \left\{ \mu \left(\prod_{j_t \in N_n \setminus \{j_1, j_2, \ldots, j_{p_j}\}} \frac{1}{c_{j_t}} \right) \right\}.$$

Porém,

$$\mu \left(\prod_{j_t \in N_n \setminus \{j_1, j_2, \ldots j_{p_j}\}} \frac{1}{c_{j_t}} \right) = \sum_{j_t \in N_n \setminus \{j_1, j_2, \ldots, j_{p_j}\}} \mu \left(\frac{1}{c_{j_t}} \right) = \sum_{j_t \in N_n \setminus \{j_1, j_2, \ldots, j_{p_j}\}} \lambda_{j_t} \geq j\lambda_1.$$

para qualquer escolha de $1 \leq j_1 < j_2 < \ldots < j_{p_j} \leq n$. Assim, $\nu(a_j) \geq j\lambda_1$. Portanto,

$$\frac{\nu(a_j) - \nu(a_0)}{j - 0} = \frac{\nu(a_j)}{j} \geq \frac{j\lambda_1}{j} = \lambda_1 \text{ para todo } j,\ 1 \leq j \leq n.$$

Isto é, o coeficiente angular de qualquer reta do conjunto $S_{i_1} = \{L_{P_0 P_j} \mid 1 \leq j \leq n\}$ é maior ou igual a λ_1, ou ainda, $\delta_1 \geq \lambda_1$.

Olhemos agora para a_{r_1}. Na expressão

$$a_{r_1} = (-1)^{r_1} \left[\sum_{1 \leq j_1 < j_2 < \ldots < j_{n-r_1} \leq n} \left(\prod_{j_t \in N_n \setminus \{j_1, \ldots, j_{n-r_1}\}} \frac{1}{c_{j_t}} \right) \right], \tag{G.1}$$

temos que

$$\mu \left(\frac{1}{c_1 \cdots c_{r_1}} \right) = \sum_{j=1}^{r_1} \mu \left(\frac{1}{c_j} \right) = \sum_{j=1}^{r_1} \lambda_1 = r_1 \lambda_1.$$

Além disso, esta é a única parcela da soma presente na Equação G.1 que possui valor $r_1\lambda_1$, pois qualquer outro produto que é parcela em G.1 envolve pelo menos um dentre os índices $r_1 + 1, \ldots, n$. Portanto, quando tomamos o valor deste produto, teremos uma soma que envolve

pelo menos um dentre $\lambda_{r_1+1}, \ldots, \lambda_n$, que são todos maiores do que λ_1. Por exemplo,

$$\mu\left(\frac{1}{c_1 \cdots c_{r_1-1} c_{r_1+1}}\right) = \sum_{j=1}^{r_1-1} \mu\left(\frac{1}{c_j}\right) + \mu\left(\frac{1}{c_{r_1+1}}\right) = \sum_{j=1}^{r_1-1} \lambda_1 + \lambda_{r_1+1} > r_1\lambda_1.$$

Logo, qualquer outro produto, parcela em G.1, possui valor estritamente maior do que $r_1\lambda_1$, isto é,

$$\mu\left(\sum_{\substack{1\le j_1<j_2<\ldots<j_{n-r_1}\le n \\ \exists j_t \le r_1}} \left(\prod_{j_t \in N_n \setminus \{j_1,\ldots,j_{n-r_1}\}} \frac{1}{c_{j_t}}\right)\right) > r_1\lambda_1 = \mu\left(\frac{1}{c_1 \cdots c_{r_1}}\right).$$

Portanto, como

$$a_{r_1} = (-1)^{r_1}\left[\frac{1}{c_1 \cdots c_{r_1}} + \sum_{\substack{1\le j_1<j_2<\ldots<j_{n-r_1}\le n \\ \exists j_t \le r_1}} \left(\prod_{j_t \in N_n \setminus \{j_1,\ldots,j_{n-r_1}\}} \frac{1}{c_{j_t}}\right)\right],$$

temos que

$$\nu(a_{r_1}) = \mu(a_{r_1}) = \mu\left(\frac{1}{c_1 \cdots c_{r_1}}\right) = r_1\lambda_1.$$

Olhando para a inclinação de $L_{P_0P_{r_1}}$ obtemos

$$\frac{\nu(a_{r_1})}{r_1} = \frac{r_1\lambda_1}{r_1} = \lambda_1.$$

Tomemos agora $j > r_1$. Na expressão de a_j, cada produto é composto por j fatores $\frac{1}{c_{j_t}}$. Logo, como $j > r_1$, cada produto possui pelo menos um dentre $\frac{1}{c_{r_1+1}}, \ldots \frac{1}{c_n}$. Portanto, todos os produtos na soma que define a_j possuem valor estritamente maior do que $j\lambda_1$. Assim, a inclinação de $L_{P_0P_i}$ é

$$\frac{\nu(a_j)}{j} > \frac{j\lambda_1}{j} = \lambda_1.$$

Dessa forma, vimos que todos as inclinações das retas em S_{i_1} são maiores do que ou iguais a λ_1, que $L_{P_0P_{r_1}}$ possui inclinação exatamente λ_1 e r_1 é o maior índice com tal inclinação, pois para $i > r_1$ tem-se inclinação estritamente maior do que λ_1. Assim, o segmento $\overline{P_0P_{r_1}}$ é a primeira face de $PN(X)$, com inclinação $\delta_1 = \lambda_1$ e $q_1 = r_1$. Segue também que

$$|\{j \mid \lambda_j = \delta_1\}| = |\{1, 2, \ldots, r_1\}| = r_1 = q_1.$$

Digamos então que $\lambda_{r_1} < \lambda_{r_1+1} = \lambda_{r_1+2} = \ldots = \lambda_{r_1+r_2} < \lambda_{r_1+r_2+1}$. Repetiremos o raciocínio acima para provar que $\overline{P_{i_2}P_{i_3}} = \overline{P_{r_1}P_{r_1+r_2}}$, em que $P_{r_1} = (r_1, r_1\lambda_1)$ e

$P_{r_1+r_2} = (r_1 + r_2, r_1\lambda_1 + r_2\lambda_{r_1+1})$.

Tomamos agora $j > r_1$. Com $p_j = n - j$, temos

$$\mu\left(\prod_{j_t \in N_n \setminus \{j_1, j_2, \ldots, j_{p_j}\}} \frac{1}{c_{j_t}}\right) = \sum_{j_t \in N_n \setminus \{j_1, j_2, \ldots, j_{p_j}\}} \mu\left(\frac{1}{c_{j_t}}\right)$$
$$= \sum_{j_t \in N_n \setminus \{j_1, j_2, \ldots, j_{p_j}\}} \lambda_{j_t} \geq r_1\lambda_1 + (j - r_1)\lambda_{r_1+1},$$

para qualquer escolha de $1 \leq j_1 < j_2 < \ldots < j_{p_j} \leq n$. Logo,

$$\frac{\nu(a_j) - \nu(a_{r_1})}{j - r_1} = \frac{\nu(a_j) - r_1\lambda_1}{j - r_1} \geq \frac{r_1\lambda_1 + (j - r_1)\lambda_{r_1+1} - r_1\lambda_1}{j - r_1} = \lambda_{r_1+1}.$$

Ou seja, $\delta_2 \geq \lambda_{r_1+1}$.

Para $r_1 + r_2$, temos

$$\mu\left(\frac{1}{c_1 \cdots c_{r_1+r_2}}\right) = \sum_{j=1}^{r_1+r_2} \mu\left(\frac{1}{c_j}\right) = \sum_{j=1}^{r_1} \lambda_1 + \sum_{j=r_1+1}^{r_1+r_2} \lambda_{r_1+1} = r_1\lambda_1 + r_2\lambda_{r_1+1}$$

e esta é a única parcela na expressão de $a_{r_1+r_2}$ com tal valor. Além disso, todas as demais tem valor estritamente maior do que $r_1\lambda_1 + r_2\lambda_{r_1+1}$. Assim, $\nu(a_{r_1+r_2}) = r_1\lambda_1 + r_2\lambda_{r_1+1}$ e com isso vemos que

$$\frac{\nu(a_{r_1+r_2}) - \nu(a_{r_1})}{r_1 + r_2 - r_1} = \frac{r_1\lambda_1 + r_2\lambda_{r_1+1} - r_1\lambda_1}{r_2} = \lambda_{r_1+1}.$$

Por fim, para $j > r_1 + r_2$, pelo mesmo argumento acima vemos que $\nu(a_j) > r_1\lambda_1 + r_2\lambda_{r_1+1}$, donde segue que a inclinação de $L_{P_{r_1}P_j}$ é estritamente maior do que λ_{r_1+1}.

Portanto, o segundo segmento de $PN(X)$ é $\overline{P_{r_1}P_{r_1+r_2}}$, com inclinação $\delta_2 = \lambda_{r_1+1}$ e $q_2 = r_2$. Mais uma vez,

$$|\{j \mid \lambda_j = \delta_2\}| = |\{r_1 + 1, r_1 + 2, \ldots, r_1 + r_2\}| = r_2 = q_2.$$

O próximo segmento de $PN(X)$ é o segmento que liga $(r_1 + r_2, r_1\lambda_1 + r_2\lambda_{r_1+1})$ a $(r_1 + r_2 + r_3, r_1\lambda_1 + r_2\lambda_{r_1+1} + r_3\lambda_{r_1+r_2+1})$, em que r_3 é tal que

$$\lambda_{r_1+r_2} < \lambda_{r_1+r_2+1} = \lambda_{r_1+r_2+2} = \ldots = \lambda_{r_1+r_2+r_3} < \lambda_{r_1+r_2+r_3+1}.$$

De modo geral, se $\lambda_s < \lambda_{s+1} = \ldots = \lambda_{s+u} < \lambda_{s+u+1}$, então o segmento que liga $(s, \lambda_1 + \lambda_2 + \ldots + \lambda_s)$ a $(s + u, \lambda_1 + \lambda_2 + \ldots + \lambda_s + u\lambda_{s+1})$ será um segmento do polígono de Newton, com inclinação $\delta_l = \lambda_{s+1}$ de comprimento $q_l = u$ para um certo l, de modo que

$$|\{j \mid \lambda_j = \delta_l\}| = u = q_l.$$

Como em algum momento $s+u=n$, passaremos por todas as faces de $PN(X)$ e obteremos assim o resultado.

■

Seja agora

$$g(x)=\sum_{j=0}^{n} a_j x^j \in \mathbb{K}[x]$$

com $a_0 \neq 0$. Tomamos novamente o polígono de Newton associado ao conjunto

$$X=\{(j,\nu(a_j)) \mid 0 \leq j \leq n \text{ e } a_j \neq 0\} \subset \mathbb{Q}\times\Gamma_\mu.$$

Corolário G.5. *Para cada l, $1 \leq l \leq k$, o polinômio g possui uma raiz com valor $-\delta_l$ e multiplicidade no máximo q_l. Mais do que isso, cada raiz c de g está associada a um determinado δ_l a partir da relação $\nu(c)=-\delta_l$.*

Demonstração: Como $a_0 \neq 0$ e ao dividir g por a_0 não se alteram as raízes, basta aplicarmos a proposição anterior para $g'=\frac{1}{a_0}g$. Sejam $c_1,\ldots,c_n$ as raízes de g (que são as mesmas de g'). Definimos

$$\lambda_j=\mu\left(\frac{1}{c_j}\right)$$

para cada j, $1 \leq j \leq n$. Então, para cada l, $1 \leq l \leq k$, existem q_l índices j tais que $\lambda_j=\delta_l$. Isto é, existe pelo menos uma raiz $c=c_i$, $1 \leq i \leq n$, tal que

$$\mu\left(\frac{1}{c}\right)=\delta_l.$$

Isso implica $\mu(c)=-\delta_l$.

Agora, seja $c=c_i$, $1 \leq i \leq n$, uma raiz qualquer de g. Pela Proposição G.4, $\lambda_i=\lambda_{r_1+r_2+\ldots+r_l}$ para algum l, $1 \leq l \leq k$. Assim, pela mesma proposição citada, $\lambda_i=\delta_l$. Também segue que $\mu(c)=-\delta_l$.

■

Seja $\mathbb{K}$ um corpo algebricamente fechado e ν uma valorização em $\mathbb{K}(x)$. Seja $f \in \mathbb{K}[x]$ polinômio não nulo de grau n e consideremos

$$X=\{(j,\nu(\partial_j f(x)) \mid 1 \leq j \leq n\}.$$

Seja $PN(X)$ o polígono de Newton associado ao conjunto X, com k, δ_l e q_l bem-definidos e $1 \leq l \leq k$.

Teorema G.6. *Para cada l, $1 \leq l \leq k$, o polinômio f possui uma raiz c de multiplicidade no máximo q_l e tal que $\nu(x-c)=-\delta_l$. Mais do que isso, cada raiz c de f está associada a um determinado δ_l a partir da relação $\nu(x-c)=-\delta_l$.*

Demonstração: Consideremos o polinômio

$$g(z) := \sum_{j=0}^{n} (\partial_j f)(x) z^j = \sum_{j=0}^{n} a_j z^j \in \mathbb{K}(x)[z].$$

Vejamos inicialmente que c é raiz de $f(x)$ se, e somente se, $c - x$ é raiz de $g(z)$. De fato, temos

$$\sum_{j=0}^{n} \partial_j x^n (c-x)^j = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} (c-x)^j = (x + (c-x))^n = c^n.$$

Logo, usando a linearidade da derivada de Hasse, vemos que para qualquer $c \in \mathbb{K}$ temos

$$f(c) = \sum_{j=0}^{n} (\partial_j f)(x)(c-x)^j = g(c-x)$$

Assim, $f(c) = 0$ se, e somente se, $g(c-x) = 0$.

Como $a_0 = f \neq 0$, podemos aplicar o Corolário G.5 para o polinômio $g(z)$ e o polígono de Newton associado ao conjunto

$$X' = \{(j, \nu(a_j)) \mid 0 \leq i \leq n\} = X.$$

Então, para cada l, $1 \leq l \leq k$, g possui uma raiz $c - x$ com multiplicidade no máximo q_l e tal que $\nu(c-x) = \nu(x-c) = -\delta_l$. Como vimos, isso é o mesmo que dizer que para cada l, $1 \leq l \leq k$, f possui uma raiz c com multiplicidade no máximo q_l e tal que $\nu(x-c) = -\delta_l$. Pelo Corolário G.5 e usando o mesmo raciocínio com as raízes de g, concluímos que cada raiz c de f está associada a uma inclinação δ_l tal que $\nu(x-c) = -\delta_l$.

■

G.3 Igualdade entre $\epsilon(f)$ e $\delta(f)$

Seja $\mathbb{K}$ um corpo e ν uma valorização em $\mathbb{K}[x]$. Seja $\overline{\mathbb{K}}$ um fecho algébrico de $\mathbb{K}$ fixado. Suponhamos que exista uma valorização μ que estende ν para $\overline{\mathbb{K}}(x)$. Sejam Γ_ν e Γ_μ os grupos de valores de ν e de μ, respectivamente. Lembremos que $\Gamma_\mu \cong \Gamma_\mu \otimes \mathbb{Q}$.

Relembramos que, para $f \in \mathbb{K}[x]$, $\deg(f) = n > 0$, se $f \notin \operatorname{supp}(\nu)$, então definimos

$$\epsilon(f) := \max_{1 \leq j \leq n} \left\{ \frac{\nu(f) - \nu(\partial_j f)}{j} \;\middle|\; \nu(\partial_j f) \in \Gamma \right\} \in \Gamma \otimes \mathbb{Q}.$$

e

$$\delta(f) := \max\{\mu(x-c) \mid c \in \overline{\mathbb{K}} \text{ e } f(c) = 0\} \in \Gamma_\mu.$$

Teorema G.7. *Temos $\epsilon(f) = \delta(f)$. Além disso, $\delta(f)$ não depende da escolha da extensão μ e do fecho algébrico $\overline{\mathbb{K}}$.*

Demonstração: Consideremos o polígono de Newton de

$$X = \{(j, \nu(\partial_j f)) \mid 1 \leq j \leq n \text{ e } \nu(\partial_j f) \neq \infty\}.$$

Como vimos, cada raiz c de f está associada a uma inclinação δ_l de modo que $\mu(x - c) = -\delta_l$ e cada inclinação está associada a uma raiz. Então, existe uma raiz c tal que $\mu(x - c) = -\delta_1$. Temos $-\delta_1 > -\delta_l$ para todo l, $2 \leq l \leq k$. Portanto,

$$\delta(f) = \max\{\mu(x - c) \mid c \in \overline{\mathbb{K}}, f(c) = 0\} = -\delta_1.$$

Agora, pela definição do polígono de Newton de X, vemos que

$$\begin{aligned}
\delta_1 = & \min_{1 \leq j \leq n} \left\{ \frac{\nu(\partial_j f) - \nu(f)}{j} \,\middle|\, \nu(\partial_j f) \in \Gamma \right\} \\
= & -\max_{1 \leq j \leq n} \left\{ \frac{\nu(f) - \nu(\partial_j f)}{j} \,\middle|\, \nu(\partial_j f) \in \Gamma \right\} \\
= & -\epsilon(f).
\end{aligned}$$

Portanto, $\epsilon(f) = -\delta_1 = \delta(f)$. Concluímos também que $\delta(f)$ não depende da escolha da extensão μ e do fecho algébrico $\overline{\mathbb{K}}$, pois $\epsilon(f)$ depende apenas de ν em $\mathbb{K}$.

■

Índice Remissivo