Universidade Federal de São Carlos
Centro de Ciências Exatas e de Tecnologia
Programa de Pós-Graduação em Matemática

Matheus dos Santos Barnabé

A álgebra graduada associada a uma valorização

São Carlos - SP

2021

Matheus dos Santos Barnabé

A álgebra graduada associada a uma valorização

Tese apresentada ao programa de Pós-Graduação em Matemática da UFSCar como parte dos requisitos para obtenção do título de Doutor em Matemática.

Orientador: Dr. Josnei Antonio Novacoski.

São Carlos - SP

2021

U N I V E R S I D A D E F E D E R A L D E S Ã O C A R L O S

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

Folha de Aprovação

Defesa de Tese de Doutorado do candidato Matheus dos Santos Barnabé, realizada em 30/11/2021.

Comissão Julgadora:

Prof. Dr. Josnei Antonio Novacoski (UFSCar)

Prof. Dr. Humberto Luiz Talpo (UFSCar)

Prof. Dr. Daniel Levcovitz (ICMC/USP)

Prof. Dr. Mark Spivakovsky (UPS)

Prof. Dr. Enric Nart (UAB)

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

Agradeço ao Dr. Josnei Antonio Novacoski por ter me aceitado como seu orientando, sempre me incentivar e por ter se tornado um grande amigo. Obrigado pelos ensinamentos, conselhos e pela confiança depositada em mim.

Agradeço ao Dr. Mark Spivakovsky pela colaboração nos resultados obtidos sobre a estrutura da álgebra graduada que se tornaram um artigo e um capítulo desta tese.

Agradeço ao Dr. Enric Nart pelas sugestões de trabalhos futuros e ao Dr. Humberto Luiz Talpo e ao Dr. Daniel Levcovitz pela leitura cuidadosa desta tese que fizeram desta versão final um texto de leitura agradável.

Agradeço aos professores e funcionários da Universidade Federal de São Carlos. Em especial ao Dr. Edivaldo Lopes dos Santos pela excelente condução, administração e coordenação do Programa de Pós-Graduação em Matemática da UFSCar e à Priscila Helen Carvalho pela admirável capacidade e competência de orientar os alunos em relação aos regimentos e normas da pós-graduação.

Por fim, agradeço a Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) pela bolsa de estudos de doutorado.

"Quod erat demonstrandum."

(Euclides, Os elementos)

Lista de Figuras

Resumo

Iniciamos este trabalho com um estudo da álgebra graduada associada a uma valorização $\nu : K \longrightarrow \Gamma_\infty$. Mostramos que nos casos em que o grupo de valores é livre ou o corpo do resíduos é fechado por radicais, então a álgebra graduada é isomorfa à $K\nu\left[t^{\nu(R)}\right]$. Em seguida, apresentamos diferentes definições que aparecem na literatura para sequências geradoras, e verificamos que, em certas situações, elas são equivalentes. Após isso, introduzimos os polígonos de Newton e relacionamos estes objetos geométricos com determinadas propriedades das valorizações. Por fim, aplicamos alguns dos resultados obtidos em extensões de Artin-Schreier.

Palavras–chave: valorizações, álgebra graduada associada, sequências geradoras, polinômios chave, polígonos de Newton.

Abstract

We begin this work with a study of the graded algebra associated to a valuation $\nu : K \longrightarrow \Gamma_\infty$. We verify that in the cases where the value group is free or the residue field is closed by radicals, the graded algebra is isomorphic to $K\nu\left[t^{\nu(R)}\right]$. Then we present the different definitions of generating sequences that appear in the literature and we verify that under certain situations they are equivalent. After that, we introduce Newton polygons and relate this object with certain properties of valuations. Finally, we apply some of the results obtained for Artin-Schreier extensions.

Keywords: valuations, associated graded algebra, generating sequences, key polynomials, Newton polygons.

Sumário

Introdução

O conceito de valorizações apresenta-se na matemática desde a antiguidade, quando Euclides provou a unicidade da decomposição de um número natural em números primos. Desde então, esse resultado permitiu codificar os números naturais pelos expoentes com os quais os vários primos p ocorrem nesses números. Esses expoentes representam as valorizações p-ádicas usadas na teoria dos números. No entanto, a teoria das valorizações como um sistema separado e sistemático, com base em um conjunto de axiomas, foi iniciada apenas no século XX com o matemático húngaro Josef Kürschák (1864-1933). Deve-se à Kürschák o primeiro teorema da estrutura abstrata em corpos valorizados, anunciado em 1912 no Cambridge International Congress of Mathematicians.

A principal motivação de Kürschák era fornecer uma base sólida para a teoria dos corpos p-ádicos, conforme definido por Kurt Hensel. Nas décadas seguintes, podemos observar um rápido desenvolvimento da teoria das valorizações. Isso foi desencadeado principalmente pela descoberta de que muito da teoria algébrica dos números poderia ser melhor compreendido através de noções e métodos da teoria das valorizações. Uma notável figura nesse desenvolvimento foi Helmut Hasse, mas houve também contribuições dadas por Alexander Ostrowski. Ao mesmo tempo, Wolfgang Krull apresentou uma definição mais geral e universal de valorização, o que acabou sendo aplicável em muitas disciplinas, como geometria algébrica e análise funcional.

No decorrer dos anos 1940 e meados dos anos 1950, a teoria das valorizações foi desenvolvida de forma intensa e sistemática por Zariski, Samuel e Abhyankar (ver [1] e [42]). Os destaques são as soluções de Zariski e Abhyankar para o problema de resolução de singularidades no caso de variedades algébricas de dimensão três. Zariski apresenta sua prova sobre um corpo de característica zero (ver [40] e [41]) enquanto que Abhyankar aborda características maiores do que seis (ver [2]). Cutkosky simplifica a prova de Abhyankar em [8], enquanto Cossart e Piltant completam o problema para todas as características positivas em [6] e [7].

A resolução de singularidades é conhecida para variedades algébricas sobre um corpo de característica zero. A primeira prova completa disso foi apresentada em [18] por Hironaka (por este trabalho ele recebeu uma medalha Fields em 1970). Todavia, tanto a resolução de singularidades quanto a uniformização local (forma local da resolução de singularidades) são problemas em aberto para variedades algébricas de dimensão maior do que três no caso de característica positiva.

Nos casos em que a uniformização local é conhecida, a prova geralmente procede por indução no posto da valorização. Em [28], Novacoski e Spivakovsky mostram que para valorizações centradas em domínios de integridade é suficiente provar para o caso de posto um. Já em [29], os autores estendem esse resultado para valorizações centradas em qualquer tipo de anéis locais Noetherianos (por exemplo, tais anéis podem ter elementos nilpotentes diferente de zero).

Em [35], Teissier apresenta uma prova combinatória de uniformização local, quando a extensão de semigrupos é finitamente gerada. Isso motiva o estudo do semigrupo $\nu(R)$ de uma valorização ν em um anel local R dominado por um anel de valorização $\mathcal{O}_\nu$.

Em [34], Spivakovsky dá uma caracterização dos semigrupos de valorizações dominando anéis locais regulares algébricos bidimensionais com corpos de resíduos algebricamente fechados. Ele obtém esse resultado construindo uma sequência geradora especial para tal valorização e aplica isso para classificar singularidades. Isso permite a dessingularização de superfícies sobre $\mathbb{C}$ pela transformação de Nash normalizada (ver [33]). O método de Spivakovsky só funciona para corpos de resíduos algebricamente fechados e sua prova é complexa. A versão simplificada de sua construção é fornecida por Favre e Jonsson em [13].

Outro objeto de alta relevância na teoria das valorizações são os polinômios chave. O conceito de polinômio chave foi introduzido por Mac Lane em [22] e [23] a fim de compreender extensões de uma valorização ν_0 em um corpo K para o corpo $K(x)$. A ideia é que para uma dada valorização ν em $K(x)$, um polinômio chave $Q \in K[x]$ para ν nos permita aumentar ν, ou seja, construir uma nova valorização ν' com $\nu \leq \nu'$ (i.e., $\nu(f) \leq \nu'(f)$ para todo $f \in K[x]$)

e $\nu(Q) < \nu'(Q)$.

No Capítulo 4 de sua tese ([31]), San Saturnino reduziu o problema da uniformização local no caso de característica positiva para o problema da monomialização do primeiro polinômio chave limite de uma certa extensão de corpos simples explicitamente definida $K \hookrightarrow K(x)$ assumindo uniformização local em dimensões inferiores (ver [32], Teorema 6.5). No Capítulo 5, sob algumas hipóteses adicionais, ele provou uma redução semelhante para uniformização local no caso de característica mista.

Álgebras graduadas também desempenham um papel importante na teoria das valorizações, sendo usadas para entender extensões de valorizações (veja por exemplo, [16], [17], [37] e [38]). Álgebras graduadas são os objetos centrais na abordagem de Teissier para uniformização local (ver [35] e [36]). Seu conceito está intimamente relacionado à sequências geradoras. Estudamos a estrutura da álgebra graduada associada a uma valorização no Capítulo 2, tendo como referência [5], que é um dos resultados desta tese de doutorado.

Intuitivamente, uma sequência geradora é um conjunto cujas imagens geram a álgebra graduada. A ideia é que dada uma valorização ν em um anel R, uma sequência geradora seja um subconjunto $\mathbf{Q}$ de R que determina completamente a valorização ν. A formalização dessa ideia aparece em diferentes trabalhos de maneiras ligeiramente distintas. Um dos objetivos desta tese é estabelecer a relação entre essas definições que ocorrem na literatura. Fazemos isso em [3], e no Capítulo 3 sintetizamos a comparação dessas maneiras de se entender a noção de sequência geradora.

O Capítulo 4 é dedicado a apresentar a definição de polígonos de Newton. O objetivo principal é relacionar esses objetos geométricos com as extensões de uma dada valorização ν_0 em um corpo K, para uma valorização ν em $K[x]/(f)$, onde $f \in K[x]$ é irredutível. Nesse capítulo provamos que cada valorização ν em $K[x]/(f)$, que estende a valorização dada ν_0 em K, está relacionada com uma raiz $a \in \overline{K}$ de f. Aplicamos esses resultados em extensões de Artin-Schreier, simplificando as provas que Kuhlmann apresenta em [20]. O Capítulo 4 contém resultados obtidos em [4].

Capítulo 1

Pré-Requisitos

Temos como objetivo para este capítulo apresentar alguns conceitos e resultados que utilizaremos neste trabalho, buscando facilitar a compreensão do tema que abordaremos.

1.1 Valorizações

Nesta seção apresentamos a definição de valorização. Para mais detalhes sugerimos [11] e [12].

Definição 1.1.1. Seja R um anel comutativo com unidade. Uma **valorização** em R é uma aplicação $\nu : R \longrightarrow \Gamma_\infty := \Gamma \cup \{\infty\}$, onde Γ é um grupo abeliano ordenado e a extensão da adição e da ordem de Γ para Γ_∞ é a usual, satisfazendo para todos $f, g \in R$ os seguintes axiomas.

(V1) $\nu(fg) = \nu(f) + \nu(g)$.

(V2) $\nu(f+g) \geq \min\{\nu(f), \nu(g)\}$.

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

Por grupo abeliano ordenado entendemos um grupo abeliano $(\Gamma, +, 0)$ com uma ordem total $\leq$ em Γ, tal que a seguinte propriedade

$$\gamma \leq \alpha \Longrightarrow \gamma + \beta \leq \alpha + \beta$$

é satisfeita para todos $\alpha, \beta, \gamma \in \Gamma$. Note que, sob essas condições, Γ é livre de torção. Isto é, dado $\gamma \in \Gamma$, se $n\gamma = 0$ para algum inteiro $n \neq 0$, então $\gamma = 0$.

Observação 1.1.2. Supondo que as condições **(V1)** e **(V2)** são satisfeitas, temos a propriedade **(V3)** equivalente a

(V3') ν não é constante.

De fato, se ν não é constante, então existe $f \in R$ tal que $\nu(f) = \alpha \neq \infty$. Logo,

$$\alpha = \nu(f) = \nu(f \cdot 1) = \nu(f) + \nu(1) = \alpha + \nu(1).$$

O que implica em $\nu(1) = 0$. Ainda, como estamos assumindo que ν não é constante, existe $g \in R$ tal que $\nu(g) = \beta \neq 0$. Então,

$$\nu(0) = \nu(g \cdot 0) = \nu(g) + \nu(0) = \beta + \nu(0),$$

o que só é possível se $\nu(0) = \infty$. A outra implicação segue trivialmente.

Proposição 1.1.3. *Seja $\nu : R \longrightarrow \Gamma_\infty$ uma valorização. Então temos o seguinte.*

a) $\nu(f) = \nu(-f)$, *para todo* $f \in R$.

b) $\nu(f^{-1}) = -\nu(f)$, *para todo* $f \in R^\times$.

c) Para todos $f, g \in R$, *se* $\nu(f) \neq \nu(g)$, *então* $\nu(f+g) = \min\{\nu(f), \nu(g)\}$.

Demonstração. a) Note primeiro que

$$0 = \nu(1) = \nu(-1) + \nu(-1) = 2\nu(-1).$$

Logo, como Γ é livre de torção, temos

$$\nu(-1) = 0.$$

Então, para todo $f \in R$, temos

$$\nu(-f) = \nu(-1) + \nu(f) = \nu(f).$$

b) Dado $f \in R^\times$, temos

$$0 = \nu(1) = \nu(f \cdot f^{-1}) = \nu(f) + \nu(f^{-1}),$$

o que implica o desejado.

c) Para o último item assuma, sem perda de generalidade, $\nu(f) < \nu(g)$. Por absurdo, suponha que $\nu(f+g) > \min\{\nu(f), \nu(g)\} = \nu(f)$. Portanto,

$$\nu(f) = \nu(f+g-g) \geq \min\{\nu(f+g), \nu(g)\} > \nu(f).$$

De onde obtemos uma contradição. Consequentemente, $\nu(f+g) = \min\{\nu(f), \nu(g)\}$. $\square$

Seja $\nu : R \longrightarrow \Gamma_\infty$ uma valorização. O subgrupo de Γ gerado por

$$\{\nu(f) \mid f \in R \text{ e } \nu(f) \neq \infty\}$$

é chamado de **grupo de valores de** ν e é denotado por Γ_ν. Uma valorização ν é chamada **trivial** se $\Gamma_\nu = \{0\}$.

Proposição 1.1.4. *Seja* $\nu : R \longrightarrow \Gamma_\infty$ *uma valorização. O conjunto* $\operatorname{supp}(\nu) := \nu^{-1}(\infty)$ *é um ideal primo de* R*.*

Demonstração. Note primeiro que $\operatorname{supp}(\nu)$ é um ideal de R. De fato, se $f, g \in \operatorname{supp}(\nu)$, então

$$\nu(f+g) \geq \min\{\nu(f), \nu(g)\} = \infty.$$

Logo, $f + g \in \operatorname{supp}(\nu)$. Considere agora $f \in R$ e $g \in \operatorname{supp}(\nu)$. Nesse caso, temos que

$$\nu(fg) = \nu(f) + \nu(g) = \infty.$$

Portanto, $fg \in R$. Assim, $\operatorname{supp}(\nu)$ é um ideal de R.

Para concluir a demonstração falta ver que $\operatorname{supp}(\nu)$ é um ideal primo. Para isso considere $fg \in \operatorname{supp}(\nu)$. Então,

$$\nu(f) + \nu(g) = \nu(fg) = \infty$$

implica que $\nu(f) = \infty$ ou $\nu(g) = \infty$. Portanto, $f \in \operatorname{supp}(\nu)$ ou $g \in \operatorname{supp}(\nu)$. De onde concluímos que $\operatorname{supp}(\nu)$ é um ideal primo de R. $\square$

Definição 1.1.5. Seja $\nu : R \longrightarrow \Gamma_\infty$ uma valorização. O conjunto $\operatorname{supp}(\nu)$ é chamado **suporte de** ν. Se $\operatorname{supp}(\nu) = \{0\}$, então dizemos que ν é uma **valorização de Krull**.

Como os únicos ideias de um corpo K são o ideal trivial e o corpo todo, obtemos que toda valorização ν definida em um corpo é uma valorização de Krull.

Observação 1.1.6. Se o anel R admite uma valorização de Krull ν, então R é um domínio. De fato, assuma que ν é uma valorização de Krull no anel R. Pela Proposição 1.1.4, sabemos que $\{0\} = \operatorname{supp}(\nu)$ é um ideal primo de R. Então, lembrando que R é um domínio se, e somente se, $\{0\}$ é um ideal primo, obtemos que R é um domínio. Nessa situação, podemos estender ν para o corpo $K := \operatorname{Quot}(R)$ definindo

$$\nu\left(\frac{f}{g}\right) = \nu(f) - \nu(g).$$

1.2 Valorizações em corpos

Valorizações definidas em corpos são o objeto inicial de estudo em diversos trabalhos, onde o propósito é obter uma valorização em $K[x]$ que estende a valorização dada (veja, por exemplo, [23] e [38]). Introduzimos nesta seção os conceitos de anel de valorização, corpo de resíduos e equivalência entre duas valorizações definidas no mesmo corpo.

Definição 1.2.1. Um **anel de valorização** de um corpo K é um subanel $\mathcal{O} \subseteq K$ tal que para todo $f \in K^{\times}$, temos

$$f \in \mathcal{O} \text{ ou } f^{-1} \in \mathcal{O}.$$

Seja $\nu : K \longrightarrow \Gamma_\infty$ uma valorização. Então o conjunto

$$\mathcal{O}_\nu := \{f \in K \mid \nu(f) \geq 0\}$$

é um anel de valorização de K, chamado de **anel de valorização de** ν. As unidades de $\mathcal{O}_\nu$ compõem o conjunto

$$\mathcal{O}_\nu^\times = \{f \in K \mid \nu(f) = 0\},$$

e os elementos que não são unidades formam o ideal maximal

$$\mathfrak{m}_\nu = \{f \in K \mid \nu(f) > 0\}.$$

Esse é o único ideal maximal de $\mathcal{O}_\nu$. O quociente

$$K\nu := \mathcal{O}_\nu / \mathfrak{m}_\nu$$

é chamado **corpo de resíduos de** ν.

Proposição 1.2.2. *Dado um anel de valorização* $\mathcal{O}$ *de* K*, existe uma valorização* ν *em* K *tal que* $\mathcal{O}_\nu = \mathcal{O}$.

Demonstração. Considere $\Gamma := K^\times/\mathcal{O}^\times$ com a operação definida por

$$(f\mathcal{O}^\times) + (g\mathcal{O}^\times) := fg\mathcal{O}^\times.$$

Em Γ consideramos a ordem dada por

$$(f\mathcal{O}^\times) \geq (g\mathcal{O}^\times) \Longleftrightarrow fg^{-1} \in \mathcal{O}.$$

Seja agora $\nu : K \longrightarrow \Gamma_\infty$ a aplicação definida por

$$\nu(0) = \infty \text{ e } \nu(f) = f\mathcal{O}^\times, \text{ se } f \neq 0.$$

A única propriedade não trivial para que ν seja uma valorização é

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

Para verificar essa propriedade, considere $f, g \in K \setminus \{0\}$. Assumimos, sem perda de generalidade, que $\nu(f) \geq \nu(g)$, isto é, $fg^{-1} \in \mathcal{O}^\times$. Como $fg^{-1} + 1 \in \mathcal{O}$, temos que

$$(f+g)g^{-1} = fg^{-1} + 1 \in \mathcal{O},$$

ou seja,

$$(f+g)\mathcal{O}^\times \geq g\mathcal{O}^\times.$$

Assim,

$$\nu(f+g) = (f+g)\mathcal{O}^\times \geq g\mathcal{O}^\times = \min\{\nu(f), \nu(g)\}.$$

Portanto, ν é uma valorização em K com

$$\mathcal{O}_\nu = \{f \in K \mid \nu(f) \geq \nu(1)\} = \{f \in K \mid f \in \mathcal{O}\} = \mathcal{O},$$

o que finaliza a demonstração. □

Definição 1.2.3. Duas valorizações ν, μ em um corpo K são **equivalentes** se possuem o mesmo anel de valorização.

Observação 1.2.4. Em geral, duas valorizações ν, μ em um anel R são equivalentes quando existe um isomorfismo $\varphi : \Gamma_\nu \longrightarrow \Gamma_\mu$ preservando a ordem tal que $\mu = \varphi \circ \nu$.

Os exemplos que seguem finalizam esta seção.

Exemplo 1.2.5. Considere $K = \mathbb{Q}$ e fixe p um número primo. Para cada $f \in \mathbb{Q} \setminus \{0\}$ podemos escrever

$$f = p^l \frac{a}{b},$$

para algum $l \in \mathbb{Z}$ e com $(p, a) = (p, b) = 1$. Pode-se verificar facilmente que a aplicação $\nu_p : \mathbb{Q} \longrightarrow \mathbb{Z}_\infty$ definida por $\nu_p(f) = l$ e $\nu_p(0) = \infty$ é uma valorização em $\mathbb{Q}$. Essa valorização é chamada valorização **p-ádica** em $\mathbb{Q}$. Ainda, dada qualquer constante positiva $c \in \mathbb{R}$, $\mu := c \cdot \nu : K \longrightarrow c\mathbb{Z}_\infty$ é uma valorização equivalente a ν.

Exemplo 1.2.6. De modo similar ao exemplo anterior, podemos definir uma valorização p-ádica ν_p em $K(x)$, onde K é um corpo. Explicitamente, fixado um polinômio irredutível $p \in K[x]$ e dado $f \in K(x)^\times$ escrevemos

$$f = p^l \frac{g}{h},$$

com $l \in \mathbb{Z}$, $g, h \in K[x]$ e $(p, g) = (p, h) = 1$. Então, definimos a aplicação $\nu_p : K[x] \longrightarrow \mathbb{Z}_\infty$ por $\nu_p(f) = l$ e $\nu_p(0) = \infty$.

Exemplo 1.2.7. Sejam K um corpo e Γ um subgrupo de Γ'. Suponha que $\mu_0 : K \longrightarrow \Gamma_\infty$ é uma valorização. Para cada $\gamma \in \Gamma'$, definimos a aplicação $\mu : K[x] \longrightarrow \Gamma'$ por

$$\mu\,(f) := \min_{0 \le i \le n} \{\mu_0(a_i) + \gamma\},$$

onde $f = a_0 + \ldots + a_n x^n$. Pode-se provar que μ é uma valorização em $K[x]$ (Teorema 2.2.1 de [12]). Essa valorização é chamada de **valorização monomial** em $K[x]$.

1.3 Álgebra graduada

Sejam ν uma valorização de Krull definida no anel R e $\nu(R)$ a imagem de $R \setminus \{0\}$ em Γ_ν. O **anel graduado de R associado à ν** é

$$\mathrm{gr}_\nu(R) := \bigoplus_{\gamma \in \nu(R)} \mathcal{P}_\gamma / \mathcal{P}_\gamma^+,$$

onde

$$\mathcal{P}_\gamma = \{f \in R \,|\, \nu(f) \geq \gamma\} \text{ e } \mathcal{P}_\gamma^+ = \{f \in R \,|\, \nu(f) > \gamma\}.$$

Considere agora $\mathcal{O}_\nu$ o anel de valorização de uma valorização ν definida em um corpo K. Sejam $K\nu = \mathcal{O}_\nu/\mathfrak{m}_\nu$ o corpo de resíduos e $R \subseteq \mathcal{O}_\nu$ um subanel. Nesse caso, temos que $\mathcal{P}_\gamma$ e $\mathcal{P}_\gamma^+$ são ideais de R. Além disso, se definirmos

$$\mathfrak{m} := \mathcal{P}_0^+ = \{f \in R \mid \nu(f) > 0\} = R \cap \mathfrak{m}_\nu,$$

então $\mathfrak{m}$ é um ideal primo e para cada $\gamma \in \nu(R)$ temos que $\mathcal{P}_\gamma/\mathcal{P}_\gamma^+$ é um $R/\mathfrak{m}$-módulo. Nesse caso, $\mathrm{gr}_\nu(R)$ é uma $R/\mathfrak{m}$-álgebra, chamada de **álgebra graduada de R associada à ν**.

A adição em $\mathrm{gr}_\nu(R)$ é dada pela estrutura de grupo abeliano e a multiplicação é dada pela extensão da multiplicação

$$\left(f + \mathcal{P}^+_{\nu(f)}\right) \cdot \left(g + \mathcal{P}^+_{\nu(g)}\right) := \left(fg + \mathcal{P}^+_{\nu(f)+\nu(g)}\right)$$

para $\mathrm{gr}_\nu(R)$ da maneira óbvia.

Para $f \in R \setminus \{0\}$ denotamos por $\mathrm{in}_\nu(f)$ a imagem de f em

$$\mathcal{P}_{\nu(f)}/\mathcal{P}^+_{\nu(f)} \subseteq \mathrm{gr}_\nu(R).$$

Lema 1.3.1. *Para $f, g \in R \setminus \{0\}$ temos as seguintes propriedades.*

a) $\mathrm{in}_\nu(f) \cdot \mathrm{in}_\nu(g) = \mathrm{in}_\nu(fg)$.

b) $\mathrm{in}_\nu(f) = \mathrm{in}_\nu(g)$ *se, e somente se,* $\nu(f - g) > \nu(f)$.

c) Se $\nu(f) < \nu(g)$, *então* $\mathrm{in}_\nu(f) = \mathrm{in}_\nu(f + g)$.

d) $\mathrm{in}_\nu(f + g) = \mathrm{in}_\nu(f) + \mathrm{in}_\nu(g)$ *se, e somente se,* $\nu(f) = \nu(g) = \nu(f + g)$.

Demonstração. O item *a)* segue diretamente da definição. Para *b)* observamos que $\mathrm{in}_\nu(f) = \mathrm{in}_\nu(g)$ se, e somente se, $(f-g) \in \mathcal{P}^+_{\nu(f)}$. Logo, $\mathrm{in}_\nu(f) = \mathrm{in}_\nu(g)$ se, e somente se, $\nu(f-g) > \nu(f)$.

Assuma que $\nu(f) < \nu(g)$. Então $\nu(f + g) = \nu(f) < \nu(g) = \nu(-g)$. Logo, pelo item *b)*, temos $\mathrm{in}_\nu(f) = \mathrm{in}_\nu(f + g)$. Para provar *d)*, observamos que se $\nu(f) = \nu(g) = \nu(f + g)$, então

$$\begin{aligned} \mathrm{in}_\nu(f+g) &= (f+g) + \mathcal{P}^+_{\nu(f)} = \left(f + \mathcal{P}^+_{\nu(f)}\right) + \left(g + \mathcal{P}^+_{\nu(g)}\right) \\ &= \mathrm{in}_\nu(f) + \mathrm{in}_\nu(g). \end{aligned}$$

A recíproca segue diretamente de *c)*. □

Lema 1.3.2. *Assuma que*

$$\operatorname{in}_\nu(f) = \operatorname{in}_\nu\left(\sum_{i=1}^{r} f_i\right), \text{ para alguns } f_1, \ldots, f_r \in R,$$

com $\nu(f) = \nu(f_i)$ *para cada* i, $1 \leq i \leq r$. *Então existe* $I \subseteq \{1, \ldots, r\}$ *tal que*

$$\operatorname{in}_\nu(f) = \sum_{i \in I} \operatorname{in}_\nu(f_i).$$

Demonstração. Vamos provar por indução em r. Se $r = 1$, não há nada a provar. Assuma $r > 1$ e que o resultado vale para $r - 1$. Se $\nu(f_1) < \nu\left(\sum_{i=2}^{r} f_i\right)$, então pelo Lema 1.3.1 *c)* temos

$$\operatorname{in}_\nu(f_1) = \operatorname{in}_\nu\left(f_1 + \sum_{i=2}^{r} f_i\right) = \operatorname{in}_\nu(f).$$

Por outro lado, se $\nu(f_1) = \nu\left(\sum_{i=2}^{r} f_i\right)$, então pelo Lema 1.3.1 *d)* temos

$$\operatorname{in}_\nu(f) = \operatorname{in}_\nu\left(f_1 + \sum_{i=2}^{r} f_i\right) = \operatorname{in}_\nu(f_1) + \operatorname{in}_\nu\left(\sum_{i=2}^{r} f_i\right)$$

e o resultado segue pela hipótese de indução. □

1.4 Polinômios Chave

Dada uma valorização ν em um corpo K, é importante entender as possíveis extensões de ν para $K[x]$. Esse problema foi extensivamente estudado e muitos objetos foram introduzidos para descrever tais extensões. Por exemplo, Mac Lane introduziu em [23] o conceito de polinômios chave e provou que no caso discreto, toda extensão de ν para $K[x]$ é determinada por uma (possivelmente infinita) sequência de polinômios chave. Em [38], Vaquié generalizou esse resultado, provando que toda valorização é definida por uma sequência de polinômios chave, desde que admitamos um tipo especial de polinômios chave sem predecessor imediato, que são chamados de polinômios chave limite. A definição de polinômios chave dada por Mac Lane e Vaquié é recursiva, no sentido de que servem para aumentar uma dada valorização (ou uma sequência de valorizações no caso de polinômios chave limite).

Uma definição alternativa de polinômio chave foi introduzida em [30], a qual apresentamos nesta seção. Tal definição difere da apresentada por Mac Lane e Vaquié de uma forma muito essencial: ela dá uma maneira de truncar uma valorização ao invés de aumentá-la. Essa propriedade oferece muitas vantagens ao lidar com valorizações. Por exemplo, permite determinar se um polinômio é um polinômio chave, sem ter que definir recursivamente uma sequência de valorizações. Também oferece uma maneira mais natural de lidar com o problema de uniformização local, pois fornece um meio para provar os resultados para um dado truncamento da valorização (para mais detalhes consulte [27]). Uma comparação entre os polinômios chave de Mac Lane e Vaquié e os apresentados aqui pode ser encontrada em [10].

Observação 1.4.1. Para este texto, por simplicidade de exposição, consideramos que o polinômio $1 \in K[x]$ não é mônico. Isso evita termos que excluir esse caso nas definições de polinômio chave, q-expansão e q-truncamento que veremos adiante. O conjunto dos inteiros positivos será sempre denotado por $\mathbb{N}$. Assim, estamos assumindo $\mathbb{N} = \{1, 2, 3, \ldots\}$. Ao usarmos a notação $\mathbb{N}_0$, estaremos nos referindo aos inteiros não-negativos, isto é, $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$.

Antes de introduzirmos o conceito de polinômio chave precisamos da noção de derivada de Hasse, apresentada abaixo.

Definição 1.4.2. Dado um polinômio $f = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$ e $b \in \mathbb{N}_0$, a **derivada de Hasse de ordem b de f** é o polinômio $\partial_b f$ definido por

$$\partial_b f = \sum_{i=b}^{n} \binom{i}{b} a_i x^{i-b} \in K[x].$$

As principais propriedades da derivada de Hasse estão listadas no lema que segue. Para mais detalhes veja [15].

Lema 1.4.3. *Sejam $f, g \in K[x]$ dois polinômios, $c \in K$ e $b, l \in \mathbb{N}_0$. Então:*

a) $b! \cdot \partial_b f = \dfrac{d^b}{dx^b}(f)$.

b) $\partial_b \partial_l f = \dbinom{b+l}{l} \partial_{b+l} f$.

c) (Fórmula de Taylor) $f(x) = \sum_{b=0}^{\deg(f)} \partial_b f(a)(x-a)^b$.

d) (Regra de Leibniz) $\partial_b(fg) = \sum_{i=0}^{b} \partial_i f \partial_{b-i} g$.

Observação 1.4.4. Tendo em mente o item *a)* do Lema 1.4.3, escrevemos

$$\partial_b f = \frac{1}{b!}\frac{d^b}{dx^b}(f),$$

mesmo que $\frac{1}{b!}$ não esteja bem definido (por exemplo, em características positivas).

Fixado um polinômio $f \in K[x]$ e $\nu : K \to \Gamma$ uma valorização, fazemos

$$\epsilon(f) := \max_{k\in\mathbb{N}}\left\{\frac{\nu(f)-\nu(\partial_k f)}{k}\right\} \in \Gamma_{\mathbb{Q}},$$

onde $\Gamma_{\mathbb{Q}} = \Gamma \otimes \mathbb{Q}$ é o fecho divisível de Γ.

Definição 1.4.5. Um polinômio mônico $Q \in K[x]$ é um **polinômio chave** (de nível $\epsilon(Q)$) se a seguinte propriedade é satisfeita para todo $f \in K[x]$.

(PC) Se $\epsilon(f) \geq \epsilon(Q)$, então $\deg(f) \geq \deg(Q)$.

Exemplo 1.4.6. Todo polinômio linear $x-a$ é um polinômio chave de nível $\nu(x-a)$.

O próximo resultado é uma caracterização para $\epsilon(f)$. Considere uma extensão μ de ν para $\overline{K}[x]$ (aqui $\overline{K}$ denota um fecho algébrico de K). Para um polinômio $f \in K[x]$, definimos

$$\delta(f) = \max\{\mu(x-a) \mid a \in \overline{K} \text{ é uma raiz de } f\}.$$

A princípio o valor $\delta(f)$ parece depender da extensão μ escolhida, mas em [27] é provado que isso não ocorre.

Proposição 1.4.7 (Proposição 3.1 de [26])**.** *Se $f \in K[x]$ é um polinômio mônico, então $\epsilon(f) = \delta(f)$.*

Observação 1.4.8. A condição de ser mônico pode ser abandonada na proposição acima. Isso decorre do fato de que para cada $c \in K^\times$ temos que

$$\epsilon(f) = \max_{k\in\mathbb{N}}\left\{\frac{\nu(f)-\nu(\partial_k f)}{k}\right\} = \max_{k\in\mathbb{N}}\left\{\frac{\nu(cf)-\nu(\partial_k (cf))}{k}\right\} = \epsilon(cf)$$

e como f e cf possuem as mesmas raízes, temos $\delta(f) = \delta(cf)$.

Corolário 1.4.9. *Para* $f, g \in K[x]$ *temos* $\epsilon(fg) = \max\{\epsilon(f), \epsilon(g)\}$.

Demonstração. Temos que a é uma raiz de fg se, e somente se, a é uma raiz de f ou g. Logo,

$$\begin{aligned} \epsilon(fg) &= \delta(fg) = \max\{\mu(x-a) \mid a \text{ é uma raiz de } fg\} \\ &= \max\{\mu(x-a) \mid a \text{ é uma raiz de } f \text{ ou de } g\} = \max\{\delta(f), \delta(g)\} \\ &= \max\{\epsilon(f), \epsilon(g)\}. \end{aligned}$$

□

Corolário 1.4.10. *Todo polinômio chave é irredutível.*

Demonstração. Assuma que Q seja um polinômio chave redutível. Escreva $Q = fg$ onde $\deg(f) < \deg(Q)$ e $\deg(g) < \deg(Q)$. Então $\epsilon(Q) = \max\{\epsilon(f), \epsilon(g)\}$. O que implica que $\epsilon(f) = \epsilon(Q)$ ou $\epsilon(g) = \epsilon(Q)$. Como $\deg(f) < \deg(Q)$ e $\deg(g) < \deg(Q)$, temos uma contradição com o fato de Q ser um polinômio chave. Portanto, todo polinômio chave é irredutível. □

Observação 1.4.11. O Corolário 1.4.10 foi provado em [30] (Proposição 2.4 **(ii)**), no entanto a prova acima é mais simples.

1.5 Polinômios chave e truncamentos

Dados $f, q \in K[x]$, com q mônico, definimos a **q-expansão de f** como a seguinte expressão

$$f = f_0 + f_1 q + \ldots + f_n q^n,$$

onde, para cada i, $0 \leq i \leq n$, $f_i = 0$ ou $\deg(f_i) < \deg(q)$. Note que, sob essas condições, a escrita apresentada é única. Tendo a q-expansão de f, definimos o **q-truncamento de ν** como

$$\nu_q(f) := \min_{0 \leq i \leq n} \{\nu(f_i q^i)\}.$$

Observação 1.5.1. Se $q = x - a$, então a q-expansão de um dado polinômio $f \in K[x]$ é a Fórmula de Taylor de f em torno do ponto a

$$f(x) = f(a) + f(a)(x-a) + \ldots + \partial_n f(a)(x-a)^n,$$

onde $n = \deg(f)$. Se colocarmos $\beta_i = \nu(\partial_i f(a))$ e $\nu(x-a) = \gamma$, então

$$\nu_q(f) = \min_{0\leq i\leq n}\{\beta_i + i\gamma\}.$$

Em particular, $\nu_q(f) \leq \nu(f(a))$.

O próximo exemplo mostra que ν_q nem sempre é uma valorização em $K[x]$.

Exemplo 1.5.2. Considere uma valorização ν em $\mathbb{R}[x]$ tal que $\nu(x) = \nu(a) = 1$ para algum $a \in \mathbb{R}$. Tome $f(x) = x^2 - a^2$ e $q(x) = x^2 + 1$, então

$$\nu_q(x^2 - a^2) = \min\{\nu(x^2+1), \nu(a^2+1)\} = 0.$$

Por outro lado, se ν_q fosse uma valorização,

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

Portanto, ν_q não pode ser uma valorização.

Dado um polinômio não constante $f \in K[x]$, seja

$$\mathcal{I}(f) := \left\{ b \in \mathbb{N} \;\middle|\; \frac{\nu(f) - \nu(\partial_b f)}{b} = \epsilon(f) \right\}.$$

Lema 1.5.1. *Seja Q um polinômio chave.*

i) Se h é um polinômio tal que $\epsilon(h) < \epsilon(Q)$ e $h = qQ + r$ com $r \neq 0$ e $\deg(r) < \deg(Q)$, então

$$\nu(r) = \nu(h) < \nu(qQ).$$

ii) Se $h_1, \ldots, h_s$ são polinômios tais que $1 \leq \deg(h_i) < \deg(Q)$, para todo $i = 1, \ldots, s$, e $\prod_{i=1}^{s} h_i = qQ + r$ com $r \neq 0$ e $\deg(r) < \deg(Q)$, então

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

Demonstração. i) Suponha, por contradição, que $\nu(qQ) \leq \nu(r)$. Logo,

$$\nu(h) \geq \min\{\nu(r), \nu(qQ)\} \geq \nu(qQ).$$

Ainda, como $\epsilon(h) < \epsilon(Q)$, temos também

$$\nu(\partial_b h) \geq \nu(h) - b\epsilon(h) > \nu(h) - b\epsilon(Q) \geq \nu(qQ) - b\epsilon(Q), \forall b \in \mathbb{N}.$$

Similarmente,

$$\nu(\partial_b r) \geq \nu(r) - b\epsilon(r) > \nu(r) - b\epsilon(Q) \geq \nu(qQ) - b\epsilon(Q), \forall b \in \mathbb{N},$$

pois $\deg(r) < \deg(Q)$, com Q polinômio chave, implica que $\epsilon(r) < \epsilon(Q)$.

Seja agora $b \in \mathcal{I}(qQ)$, então

$$\nu(qQ) - b\epsilon(qQ) = \nu(\partial_b qQ) = \nu(\partial_b h - \partial_b r) > \nu(qQ) - b\epsilon(Q).$$

Portanto, $\epsilon(Q) > \epsilon(qQ) = \max\{\epsilon(q), \epsilon(Q)\}$, o que nos dá uma contradição. Logo,

$$\nu(qQ) > \nu(r) \text{ e } \nu(r) = \nu(h).$$

ii) Coloque

$$h := \prod_{i=1}^{s} h_i.$$

Visto que

$$\deg(h_i) < \deg(Q) \Longrightarrow \epsilon(h_i) < \epsilon(Q),$$

temos que $\epsilon(h) = \max\limits_{1 \leq i \leq s}\{\epsilon(h_i)\} < \epsilon(Q)$. Portanto, podemos usar o item anterior e, com isso, finalizamos esta proposição. $\square$

Observação 1.5.3. Em [21], Leloup apresenta o item *ii)* do Lema 1.5.1 para $s = 2$ como a definição de polinômio chave. Na Seção 3 desse artigo, ele prova que essas duas definições são equivalentes.

O Lema 1.5.1 faz parte de uma sequência de resultados apresentados em [30]. Essa abordagem visa levar até a demonstração que se Q é um polinômio chave, então ν_Q é uma valorização.

Proposição 1.5.4 (Proposição 2.6 de [30])**.** *Se Q é um polinômio chave, então ν_Q é uma valorização de $K[x]$.*

Proposição 1.5.5 (Proposição 2.10 de [30]). *Para dois polinômios chave $Q, Q' \in K[x]$ temos as seguintes propriedades.*

(i) *Se* $\deg(Q) < \deg(Q')$, *então* $\epsilon(Q) < \epsilon(Q')$.

(ii) *Se* $\epsilon(Q) < \epsilon(Q')$, *então* $\nu_Q(Q') < \nu(Q')$.

(iii) *Se* $\deg(Q) = \deg(Q')$, *então*

$$\nu(Q) < \nu(Q') \Longleftrightarrow \nu_Q(Q') < \nu(Q') \Longleftrightarrow \epsilon(Q) < \epsilon(Q'). \tag{1.1}$$

Corolário 1.5.6. *Se Q e Q' são polinômios chave tais que $\epsilon(Q) \leq \epsilon(Q')$, então $\nu_{Q'}(Q) = \nu(Q)$.*

Demonstração. Como $\epsilon(Q) \leq \epsilon(Q')$, temos que $\deg(Q) \leq \deg(Q')$. Se $\deg(Q) < \deg(Q')$, nós temos que $\nu_{Q'}(Q) = \nu(Q)$ pela definição de $\nu_{Q'}$. Se $\deg(Q') = \deg(Q)$, então, usando que $\epsilon(Q') < \epsilon(Q)$ não ocorre, o resultado segue pelo item *iii)* da Proposição 1.5.5. □

Corolário 1.5.7. *Sejam Q e Q' polinômios chave tais que $\epsilon(Q) \leq \epsilon(Q')$. Para cada $f \in K[x]$, se $\nu_Q(f) = \nu(f)$, então $\nu_{Q'}(f) = \nu(f)$.*

Demonstração. Segue do Corolário 1.5.6 que $\nu_{Q'}(Q) = \nu(Q)$. Como $\deg(Q) \leq \deg(Q')$, para cada $f_i \in K[x]$ com $\deg(f_i) < \deg(Q)$ temos $\nu_{Q'}(f_i) = \nu(f_i)$. Portanto, $\nu_{Q'}(f_iQ^i) = \nu(f_iQ^i)$.

Seja $f \in K[x]$ tal que $\nu_Q(f) = \nu(f)$ e considere

$$f = f_0 + f_1Q + \ldots + f_nQ^n$$

a Q-expansão de f. Então

$$\nu_{Q'}(f) \geq \min_{0 \leq i \leq n}\{\nu_{Q'}(f_iQ^i)\} = \min_{0 \leq i \leq n}\{\nu(f_iQ^i)\} = \nu_Q(f) = \nu(f).$$

Como $\nu_{Q'}(f) \leq \nu(f)$ para cada $f \in K[x]$, temos o resultado. □

Denotamos por p a **característica expoente** de $K\nu$, isto é,

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

Proposição 1.5.8. *Seja $Q \in K[x]$ um polinômio chave, então todo elemento em $\mathcal{I}(Q)$ é uma potência de p.*

Demonstração. Seja $b \in \mathcal{I}(Q)$ e assuma, por contradição, que b não é uma potência de p. Escreva $b = p^t r$, onde $r > 1$ é primo com p. Então $\binom{b}{p^t}$ é primo com p, portanto $\nu\left(\binom{b}{p^t}\right) = 0$.

Note que

$$p^t!(b-p^t)!\binom{b}{p^t}\partial_b Q = \frac{d^b}{dx^b}(Q)$$

e que

$$p^t!(b-p^t)!\partial_{p^t}\partial_{b-p^t}Q = \frac{d^{b+p^t-p^t}}{dx^{b+p^t-p^t}}(Q).$$

Assim,

$$\binom{b}{p^t}\partial_b Q = \partial_{p^t}\partial_{b-p^t}Q.$$

Portanto,

$$\begin{aligned} \nu(\partial_{b-p^t}Q) - \nu(\partial_b Q) &= \nu(\partial_{b-p^t}Q) - \nu(\partial_{p^t}\partial_{b-p^t}Q) \\ &\leq p^t\delta(\partial_{b-p^t}Q). \end{aligned}$$

Por fim, $\delta(\partial_{b-p^t}Q) < \delta(Q)$, pois Q é um polinômio chave e $\deg(\partial_{b-p^t}Q) < \deg(Q)$, implica que

$$\begin{aligned} b\delta(Q) &= \nu(Q) - \nu(\partial_b Q) \\ &= \nu(Q) - \nu(\partial_{b-p^t}Q) + \nu(\partial_{b-p^t}Q) - \nu(\partial_b Q) \\ &< (b-p^t)\delta(Q) + p^t\delta(Q) \\ &= b\delta(Q). \end{aligned}$$

O que nos dá uma contradição. Assim concluímos que todo elemento em $\mathcal{I}(Q)$ é uma potência de p. □

Com o corolário abaixo finalizamos este capítulo.

Corolário 1.5.9. *Seja $f \in K[x]$. Se existe $b \in \mathcal{I}(f)$ tal que b não é potência de p, então f não é um polinômio chave.*

Capítulo 2

Estrutura da álgebra graduada

O objetivo deste capítulo é estudar a estrutura da álgebra graduada associada à uma valorização. Provamos aqui que a álgebra graduada $\mathrm{gr}_\nu(R)$ de um subanel $(R, \mathfrak{m})$ de um anel de valorização $\mathcal{O}_\nu$ é isomorfa à $K\nu\left[t^{\nu(R)}\right]$, quando $K\nu = \mathcal{O}_\nu/\mathfrak{m}_\nu = R/\mathfrak{m}$ e a multiplicação é dada por um *twisting*. Mostramos que essa multiplicação pode ser escolhida para ser a usual nos casos em que o grupo de valores é livre ou o corpo do resíduos é fechado por radicais. Apresentamos também um exemplo que mostra que o isomorfismo com um *twisting* trivial não precisa existir.

2.1 Preliminares

Seja $\nu : R \longrightarrow \Gamma_\infty$ uma valorização. O **anel de semigrupo** $K\nu\left[t^{\nu(R)}\right]$ é o conjunto de somas formais finitas

$$\sum_{i=1}^{n} a_i \cdot t^{\gamma_i}, \text{ com } a_i \in K\nu \text{ e } \gamma_i \in \nu(R), 1 \leq i \leq n,$$

onde

$$\sum_{i=1}^{n} a_i \cdot t^{\gamma_i} + \sum_{i=1}^{n} b_i \cdot t^{\gamma_i} = \sum_{i=1}^{n} (a_i + b_i) \cdot t^{\gamma_i}$$

e

$$\left(\sum_{i=1}^{n} a_i \cdot t^{\gamma_i}\right) \times \left(\sum_{j=1}^{m} b_j \cdot t^{\gamma_j}\right) := \sum_{i,j} a_i b_j \cdot t^{\gamma_i + \gamma_j}.$$

Chamamos de **função escolha** qualquer inversa à direita de ν, ou seja, uma aplicação $\tau : \nu(R) \longrightarrow R$ tal que $\nu(\tau(\gamma)) = \gamma$ para cada $\gamma \in \nu(R)$. Sempre consideramos funções escolha para as quais $\tau(0) = 1$. Para cada função escolha, podemos definir a aplicação **twisting**

$$\overline{\tau} : \nu(R) \times \nu(R) \longrightarrow K\nu, \text{ por } \overline{\tau}(\gamma, \gamma') := \left(\frac{\tau(\gamma)\tau(\gamma')}{\tau(\gamma+\gamma')}\right)\nu.$$

Podemos definir também

$$\times_\tau : K\nu\left[t^{\nu(R)}\right] \times K\nu\left[t^{\nu(R)}\right] \longrightarrow K\nu\left[t^{\nu(R)}\right], (a, b) \mapsto a \times_\tau b,$$

colocando $t^\gamma \times_\tau t^{\gamma'} := \overline{\tau}(\gamma, \gamma') \cdot t^{\gamma+\gamma'}$ e estendendo para $K\nu\left[t^{\nu(R)}\right]$ de maneira óbvia. Na Proposição 2.2.2 demonstramos que o anel $K\nu\left[t^{\nu(R)}\right]_\tau := (K\nu\left[t^{\nu(R)}\right], +, \times_\tau)$ é um anel comutativo.

Nosso teorema principal é o seguinte.

Teorema 2.1.1. *Se $K\nu = R/\mathfrak{m}$, então para cada função escolha τ temos*

$$\mathrm{gr}_\nu(R) \simeq K\nu\left[t^{\nu(R)}\right]_\tau.$$

Em seguida, estudamos se existe uma função escolha τ para a qual a multiplicação dada pelo *twisting* é a usual, ou seja, tal que $t^\gamma \times_\tau t^{\gamma'} = t^{\gamma+\gamma'}$ para todos $\gamma, \gamma' \in \nu(R)$. Observe que isso é o mesmo que dizer que $\overline{\tau} \equiv 1\nu$. Mostramos o seguinte.

Teorema 2.1.2. *Se Γ_ν é um grupo livre ou $K\nu$ é fechado por radicais, então existe uma função escolha τ para a qual $\overline{\tau} \equiv 1\nu$.*

Lembramos que um corpo K é fechado por radicais se para todo $a \in K$ e $n \in \mathbb{N}$ existe $b \in K$ tal que $b^n = a$.

A condição de Γ_ν ser um grupo livre é satisfeita para uma grande classe de valorizações. Por exemplo, é satisfeito quando ν é Abhyankar, ou seja, quando vale a igualdade na desigualdade

$$\dim_{\mathbb{Q}}(\Gamma_\nu \otimes_{\mathbb{Z}} \mathbb{Q}) + \mathrm{tr.deg}(K\nu \mid R/\mathfrak{m}) \leq \dim R$$

(veja a Desigualdade de Abhyankar[42, Apêndice 5] para mais detalhes).

2.2 O isomorfismo entre a álgebra graduada e o anel de semigrupo

Começamos apresentando algumas observações sobre uma dada função escolha τ.

Observação 2.2.1. **(i)** A aplicação $\overline{\tau}$ é simétrica e $\overline{\tau}(0,\alpha) = 1\nu$, para todo $\alpha \in \nu(R)$.

(ii) Dados três elementos $\alpha, \beta, \gamma \in \nu(R)$, temos

$$\begin{aligned}
\overline{\tau}(\alpha,\beta)\cdot\overline{\tau}(\alpha+\beta,\gamma) &= \left(\frac{\tau(\alpha)\tau(\beta)}{\tau(\alpha+\beta)}\right)\nu\cdot\left(\frac{\tau(\alpha+\beta)\tau(\gamma)}{\tau(\alpha+\beta+\gamma)}\right)\nu \\
&= \left(\frac{\tau(\alpha)\tau(\beta)\tau(\gamma)}{\tau(\alpha+\beta+\gamma)}\right)\nu \\
&= \left(\frac{\tau(\alpha)\tau(\beta+\gamma)}{\tau(\alpha+\beta+\gamma)}\right)\nu\cdot\left(\frac{\tau(\beta)\tau(\gamma)}{\tau(\beta+\gamma)}\right)\nu \\
&= \overline{\tau}(\alpha,\beta+\gamma)\cdot\overline{\tau}(\beta,\gamma).
\end{aligned} \tag{2.1}$$

Mostramos agora que a aplicação $\times_\tau$ induz uma estrutura de anel comutativo em $K\nu\left[t^{\nu(R)}\right]$.

Proposição 2.2.2. *Para cada função escolha τ, o conjunto $K\nu\left[t^{\nu(R)}\right]$ com a soma usual e a multiplicação dada por $\times_\tau$ é um anel comutativo.*

Demonstração. Para a soma, temos que $K\nu\left[t^{\nu(R)}\right]$ é um grupo abeliano aditivo por definição. Para a multiplicação, da forma como está definida, basta verificar as propriedades apenas para os elementos da forma $f = f_\alpha t^\alpha$. Tome $f = f_\alpha \cdot t^\alpha, g = g_\beta \cdot t^\beta \in K\nu\left[t^{\nu(R)}\right]$. Então

$$f \times_\tau g = (f_\alpha g_\beta)\cdot t^\alpha \times_\tau t^\beta = (g_\beta f_\alpha)\cdot t^\beta \times_\tau t^\alpha = g \times_\tau f.$$

Consequentemente $\times_\tau$ é comutativa. Além disso, para $1 := (1\nu)\cdot t^0 \in K\nu\left[t^{\nu(R)}\right]$ temos

$$1 \times_\tau f = f_\alpha \overline{\tau}(0,\alpha)\cdot t^{0+\alpha} = f_\alpha \cdot t^\alpha = f,$$

então $K\nu\left[t^{\nu(R)}\right]$ tem uma unidade.

Para provar que $\times_\tau$ é distributivo, tome $h = h_\beta \cdot t^\beta$ e observe que

$$\begin{aligned}
f \times_\tau (g+h) &= f_\alpha \cdot t^\alpha \times_\tau (g_\beta + h_\beta)\cdot t^\beta = f_\alpha(g_\beta+h_\beta)\cdot t^\alpha \times_\tau t^\beta \\
&= (f_\alpha g_\beta)\cdot t^\alpha \times_\tau t^\beta + (f_\alpha h_\beta)\cdot t^\alpha \times_\tau t^\beta \\
&= f \times_\tau g + f \times_\tau h.
\end{aligned}$$

Por último, para provar que $\times_\tau$ é associativo basta provar para elementos da forma $f = t^\alpha, g = t^\beta$ e $h = t^\gamma$. Nesse caso, temos

$$\begin{aligned}(f \times_\tau g) \times_\tau h &= \left(\overline{\tau}(\alpha,\beta)\cdot t^{\alpha+\beta}\right) \times_\tau t^\gamma = \overline{\tau}(\alpha,\beta)\overline{\tau}(\alpha+\beta,\gamma)\cdot t^{\alpha+\beta+\gamma}\\ &\overset{(2.1)}{=} \overline{\tau}(\alpha,\beta+\gamma)\overline{\tau}(\beta,\gamma)\cdot t^{\alpha+\beta+\gamma} = \overline{\tau}(\beta,\gamma)\cdot t^\alpha \times_\tau t^{\beta+\gamma}\\ &= f \times_\tau (g \times_\tau h).\end{aligned}$$

O que conclui a demonstração. □

Para $f \in R \setminus \{0\}$ definimos

$$\psi(\mathrm{in}_\nu(f)) = \left(\frac{f}{D(f)}\right)\nu \cdot t^{\nu(f)},$$

onde $D = \tau \circ \nu$. Estenda ψ para $\mathrm{gr}_\nu(R)$ definindo

$$\psi\left(\sum_{\alpha\in\Delta}\mathrm{in}_\nu(f_\alpha)\right) = \sum_{\alpha\in\Delta}\psi(\mathrm{in}_\nu(f_\alpha)) \text{ and } \psi(0) = 0,$$

onde Δ é um subconjunto finito de $\nu(R)$ e $\nu(f_\alpha) = \alpha$. Verificaremos adiante que ψ está bem definida.

Observação 2.2.3. Note que

$$t^{\nu(f)} \times_\tau t^{\nu(g)} = \left(\frac{D(f)D(g)}{D(fg)}\right)\nu \cdot t^{\nu(fg)}$$

para todos $f, g \in K$.

O Teorema 2.1.1 segue da seguinte proposição.

Proposição 2.2.4. *A aplicação ψ é um homomorfismo injetivo de $\mathrm{gr}_\nu(R)$ para $K\nu\left[t^{\nu(R)}\right]_\tau$. Além disso, se $(R, \mathfrak{m})$ é um anel local dominado por $\mathcal{O}_\nu$ tal que $R/\mathfrak{m} = K\nu$, então esta aplicação é um isomorfismo.*

Demonstração. Provamos primeiro que ψ é injetiva e está bem definida, ou seja, que

$$\mathrm{in}_\nu(f) = \mathrm{in}_\nu(g) \Leftrightarrow \psi(\mathrm{in}_\nu(f)) = \psi(\mathrm{in}_\nu(g)), \tag{2.2}$$

para todos $f, g \in R$. Para $f, g \in R$ temos $\mathrm{in}_\nu(f) = \mathrm{in}_\nu(g)$ se, e somente se,

$$\nu(f) = \nu(g) \text{ e } \nu(f - g) > \nu(f).$$

Como $\nu(f) = \nu(D(f))$, isso é equivalente a

$$\nu(f) = \nu(g) \text{ e } \nu\left(\frac{f-g}{D(f)}\right) > 0,$$

o que é equivalente a

$$\nu(f) = \nu(g) \text{ e } \left(\frac{f-g}{D(f)}\right)\nu = 0.$$

Isso acontece se, e somente se, $\psi(\mathrm{in}_\nu(f)) = \psi(\mathrm{in}_\nu(g))$.

Para provar que ψ é um homomorfismo aditivo entre grupos basta mostrar que se $\nu(f) = \nu(g)$, então

$$\psi(\mathrm{in}_\nu(f) + \mathrm{in}_\nu(g)) = \psi(\mathrm{in}_\nu(f)) + \psi(\mathrm{in}_\nu(g)).$$

Para verificar esta propriedade, temos que considerar duas possibilidades: $\nu(f+g) > \nu(f)$ ou $\nu(f+g) = \nu(f) = \nu(g)$. No primeiro caso temos

$$\psi(\mathrm{in}_\nu(f) + \mathrm{in}_\nu(g)) = 0 = \left(\frac{f+g}{D(f)}\right)\nu = \psi(\mathrm{in}_\nu(f)) + \psi(\mathrm{in}_\nu(g)).$$

No segundo caso,

$$\begin{aligned}
\psi(\mathrm{in}_\nu(f) + \mathrm{in}_\nu(g)) &= \psi(\mathrm{in}_\nu(f+g)) = \left(\frac{f+g}{D(f+g)}\right)\nu \cdot t^{\nu(f+g)} \\
&= \left(\frac{f}{D(f)}\right)\nu \cdot t^{\nu(f)} + \left(\frac{g}{D(g)}\right)\nu \cdot t^{\nu(g)} \\
&= \psi(\mathrm{in}_\nu(f)) + \psi(\mathrm{in}_\nu(g)).
\end{aligned}$$

Para mostrar que ψ é multiplicativo, basta mostrar que para $f, g \in R$ temos

$$\psi(\mathrm{in}_\nu(f)\mathrm{in}_\nu(g)) = \psi(\mathrm{in}_\nu(f)) \times_\tau \psi(\mathrm{in}_\nu(g)).$$

Visto que

$$t^{\nu(fg)} = t^{\nu(f)+\nu(g)} = \left(\frac{D(fg)}{D(f)D(g)}\right)\nu \cdot t^{\nu(f)} \times_\tau t^{\nu(g)}$$

temos

$$\begin{aligned}
\psi(\mathrm{in}_\nu(f)\mathrm{in}_\nu(g)) &= \psi(\mathrm{in}_\nu(fg)) = \left(\frac{fg}{D(fg)}\right)\nu \cdot t^{\nu(fg)} \\
&= \left(\frac{fg}{D(fg)}\frac{D(fg)}{D(f)D(g)}\right)\nu \cdot t^{\nu(f)} \times_\tau t^{\nu(g)} \\
&= \left(\frac{f}{D(f)}\right)\nu \cdot t^{\nu(f)} \times_\tau \left(\frac{g}{D(g)}\right)\nu \cdot t^{\nu(g)} \\
&= \psi(\mathrm{in}_\nu(f)) \times_\tau \psi(\mathrm{in}_\nu(g)).
\end{aligned}$$

Isso prova que ψ é um homomorfismo injetor entre anéis.

Suponha agora que $R/\mathfrak{m} = K\nu$ e tome qualquer elemento $x \cdot t^{\alpha} \in K\nu\left[t^{\nu(R)}\right]$. Fixe $f' \in R$ tal que $f'\nu = x$. É fácil verificar que para $f = \tau(\alpha)f'$ temos

$$\psi\left(\mathrm{in}_{\nu} f\right) = x \cdot t^{\alpha}.$$

Portanto ψ é sobrejetora. □

Observação 2.2.5. Observamos que a aplicação ψ é um homomorfismo *graduado* entre anéis, ou seja, para cada $f \in R$ temos $\deg(\mathrm{in}_{\nu}(f)) = \deg(\psi(\mathrm{in}_{\nu}(f)))$. Aqui, deg é a aplicação que associa cada elemento homogêneo $\mathrm{in}_{\nu}(f)$ ao elemento $\gamma = \nu(f)$ no semigrupo graduado.

Agora vamos estudar quando podemos escolher τ de forma que a multiplicação $\times_{\tau}$ seja a usual, ou seja, quando a aplicação $\overline{\tau}$ é constante e igual a 1. Começamos com a seguinte observação.

Observação 2.2.6. A aplicação $\overline{\tau}$ é constante e igual a 1 se, e somente se, $\mathrm{in}_{\nu} \circ \tau$ é um homomorfismo de semigrupo entre $\nu(R)$ e o semigrupo multiplicativo de $\mathrm{gr}_{\nu}(R)$. De fato, para $\alpha, \beta \in \nu(R)$ temos

$$\begin{aligned}
\overline{\tau}(\alpha,\beta) = 1\nu \iff & \left(\frac{\tau(\alpha)\tau(\beta)}{\tau(\alpha+\beta)}\right)\nu = 1\nu \iff \nu\left(\frac{\tau(\alpha)\tau(\beta)}{\tau(\alpha+\beta)} - 1\right) > 0 \\
\iff & \nu\left(\tau(\alpha)\tau(\beta) - \tau(\alpha+\beta)\right) > \nu(\tau(\alpha+\beta)) \\
\iff & \mathrm{in}_{\nu} \circ \tau(\alpha+\beta) = (\mathrm{in}_{\nu} \circ \tau(\alpha)) \cdot (\mathrm{in}_{\nu} \circ \tau(\beta))
\end{aligned}$$

Provamos o Teorema 2.1.2 como dois teoremas separados. O Teorema 2.2.7 para quando Γ_{ν} for um grupo livre e o Teorema 2.2.8 para quando $K\nu$ for fechado por radicais.

Teorema 2.2.7. *Assuma que Γ_{ν} é um grupo livre. Então existe uma função escolha $\tau : \Gamma_{\nu} \longrightarrow K$ tal que $\overline{\tau} \equiv 1\nu$.*

Demonstração. Escreva $\Gamma_{\nu} = \bigoplus_{i \in I} \gamma_i \mathbb{Z}$ para alguns $\gamma_i \in \Gamma_{\nu}$. Para cada γ_i escolhemos $z_i \in K$ tal que $\nu(z_i) = \gamma_i$ e para cada $\alpha \in \Gamma_{\nu}$, escrevemos

$$\alpha = n_1\gamma_{i_1} + \cdots + n_r\gamma_{i_r} \in \Gamma_{\nu}, \text{ para alguns } n_i \in \mathbb{Z}. \tag{2.3}$$

Defina

$$\tau(\alpha) := z_{i_1}^{n_1} \cdots z_{i_r}^{n_r}.$$

Uma vez que a expressão em (2.3) é única, esta aplicação está bem definida. Além disso, τ é uma função escolha porque $\nu(\tau(\alpha)) = \alpha$, para todos $\alpha \in \nu(R)$.

Sejam $\alpha, \beta \in \Gamma_\nu$ e escreva (adicionando n_i's ou m_j's iguais a zero, se necessário)

$$\alpha = n_1\gamma_{i_1} + \cdots + n_r\gamma_{i_r} \text{ e } \beta = m_1\gamma_{i_1} + \cdots + m_r\gamma_{i_r}.$$

Então

$$\tau(\alpha)\tau(\beta) = z_{i_1}^{n_1} \cdots z_{i_r}^{n_r} \cdot z_{i_1}^{m_1} \cdots z_{i_r}^{m_r} = z_{i_1}^{n_1+m_1} \cdots z_{i_r}^{n_r+m_r} = \tau(\alpha+\beta).$$

Portanto,

$$\overline{\tau}(\alpha, \beta) = \left(\frac{\tau(\alpha)\tau(\beta)}{\tau(\alpha+\beta)}\right)\nu = 1\nu,$$

que é o que queríamos provar. $\square$

Teorema 2.2.8. *Se $K\nu$ é fechado por radicais, então existe uma função escolha $\tau : \Gamma_\nu \longrightarrow K$ tal que $\overline{\tau} \equiv 1\nu$.*

Demonstração. Considere o conjunto

$$\mathcal{P} := \left\{(\Phi, \tau_\Phi) \mid \Phi \subseteq \Gamma_\nu \text{ é um subgrupo e } \tau_\Phi : \Phi \longrightarrow K \text{ é uma função escolha com } \overline{\tau}_\Phi \equiv 1\nu\right\}.$$

Definimos uma ordem parcial em $\mathcal{P}$ por

$$(\Phi_1, \tau_{\Phi_1}) \prec (\Phi_2, \tau_{\Phi_2}) \Longleftrightarrow \Phi_1 \subseteq \Phi_2 \text{ e } \tau_{\Phi_2} \text{ estende } \tau_{\Phi_1}.$$

Para qualquer elemento não nulo fixado $\alpha \in \Gamma_\nu$ seja

$$\langle\alpha\rangle := \{n\alpha \mid n \in \mathbb{Z}\}$$

o subgrupo de Γ_ν gerado por α. Escolhemos $z \in K$ tal que $\nu(z) = \alpha$ e definimos

$$\tau_{\langle\alpha\rangle} : \langle\alpha\rangle \longrightarrow K \text{ por } \tau_{\langle\alpha\rangle}(n\alpha) = z^n.$$

Visto que $\left(\langle\alpha\rangle, \tau_{\langle\alpha\rangle}\right) \in \mathcal{P}$, temos $\mathcal{P} \neq \emptyset$.

Seja $Q = \{(\Phi_i, \tau_{\Phi_i})\}_{i\in I}$ um subconjunto totalmente ordenado de $\mathcal{P}$. Definimos $\Phi_Q := \bigcup_{i\in I} \Phi_i$. Para cada $\alpha \in \Phi$ escolhemos $i \in I$ tal que $\alpha \in \Phi_i$ e definimos $\tau_{\Phi_Q}(\alpha) = \tau_{\Phi_i}(\alpha)$.

Como Q é totalmente ordenado, essa aplicação está bem definida. É simples verificar que $(\Phi_Q, \tau_{\Phi_Q}) \in \mathcal{P}$ e que (Φ_Q, τ_{Φ_Q}) é uma cota superior para Q. Portanto, podemos aplicar o Lema de Zorn para obter um elemento maximal (Φ, τ_Φ) de $\mathcal{P}$.

Mostraremos que $\Phi = \Gamma_\nu$ e isso concluirá nossa prova. Suponha, por contradição, que $\Phi \neq \Gamma_\nu$ e tome $\gamma \in \Gamma_\nu \setminus \Phi$. Temos duas possibilidades:

$$\langle\gamma\rangle \cap \Phi = \emptyset \text{ ou } \langle\gamma\rangle \cap \Phi \neq \emptyset.$$

No primeiro caso, pegamos $x_\gamma \in K$ com $\nu(x_\gamma) = \gamma$ e definimos $\Psi := \Phi + \langle\gamma\rangle$ e $\tau_\Psi : \Psi \longrightarrow K$ por

$$\tau_\Psi(\alpha + n\gamma) := \tau_\Phi(\alpha) \cdot x_\gamma^n, \text{ para } \alpha \in \Phi \text{ e } n \in \mathbb{Z}.$$

Como $n\gamma \notin \Phi$ para todos $n \in \mathbb{Z}$, temos que para $\alpha, \beta \in \Phi$ e $n, m \in \mathbb{Z}$

$$\alpha + n\gamma = \beta + m\gamma \Longrightarrow \alpha = \beta \text{ e } n = m.$$

Portanto, τ_Ψ está bem definido e pode-se verificar que $(\Psi, \tau_\Psi) \in \mathcal{P}$.

Agora, se $\langle\gamma\rangle \cap \Phi \neq \emptyset$, definimos

$$n_0 = \min\{n \geq 2 \mid n\gamma \in \Phi\}.$$

Seja $x_0 = \tau_\Phi(n_0\gamma) \in K$ e $x_\gamma \in K$ tal que $\nu(x_\gamma) = \gamma$. Como $K\nu$ é fechado por radicais, existe $a \in K$ tal que

$$\left(\frac{x_0}{x_\gamma^{n_0}}\right)\nu = (a^{n_0})\nu. \tag{2.4}$$

Cada elemento em $\Psi := \Phi + \langle\gamma\rangle$ tem a forma $\alpha + n\gamma$, para um determinado $\alpha \in \Phi$ e n, $0 \leq n < n_0$. De fato, se $\alpha + n\gamma = \alpha' + m\gamma$, $0 \leq m \leq n < n_0$, então $(n-m)\gamma = \alpha' - \alpha \in \Phi$. Logo, $n = m$ e $\alpha = \alpha'$e isso nos dá a unicidade. Para a existência, cada elemento em Ψ é da forma $\alpha' + r\gamma$ para algum $r \in \mathbb{Z}$. Usando a divisão euclidiana, escrevemos $r = n_0 l + n$ com $0 \leq n < n_0$ e $l \in \mathbb{Z}$. Portanto, $\alpha := \alpha' + n_0\gamma \in \Phi$ que é o que precisávamos.

Definimos $\tau_\Psi : \Psi \longrightarrow K$ por

$$\tau_\Psi(\alpha + n\gamma) = \tau_\Phi(\alpha) \cdot (a x_\gamma)^n,$$

onde $\alpha + n\gamma \in \Psi$, com $\alpha \in \Phi$ e $0 \leq n \leq n_0$. Portanto τ_Ψ está bem definida.

Mostraremos que $(\Psi, \tau_\Psi) \in \mathcal{P}$, e como $(\Phi, \tau_\Phi) \prec (\Psi, \tau_\Psi)$ obtemos uma contradição com a maximalidade de (Φ, τ_Φ) em $\mathcal{P}$. Seja $\alpha + n_1\gamma$ e $\beta + n_2\gamma$ dois elementos em Ψ, onde $0 \leq n_1, n_2 < n_0$. Vamos considerar dois casos.

Caso 1: Se $n_1 + n_2 < n_0$, então

$$\begin{aligned}
\overline{\tau}_\Psi(\alpha + n_1\gamma, \beta + n_2\gamma) &= \left(\frac{\tau_\Psi(\alpha + n_1\gamma)\ \tau_\Psi(\beta + n_2\gamma)}{\tau_\Psi(\alpha + \beta + (n_1 + n_2)\gamma)} \right) \nu \\
&= \left(\frac{\tau_\Phi(\alpha)\ (ax_\gamma)^{n_1}\ \tau_\Phi(\beta)\ (ax_\gamma)^{n_2}}{\tau_\Phi(\alpha + \beta)\ (ax_\gamma)^{n_1 + n_2}} \right) \nu \\
&= \left(\frac{\tau_\Phi(\alpha)\ \tau_\Phi(\beta)}{\tau_\Phi(\alpha + \beta)} \right) \nu \cdot \left(\frac{(ax_\gamma)^{n_1}\ (ax_\gamma)^{n_2}}{(ax_\gamma)^{n_1 + n_2}} \right) \nu \\
&= \overline{\tau}_\Phi(\alpha, \beta) \cdot 1\nu = 1\nu
\end{aligned}$$

Caso 2: Se $n_1 + n_2 \geq n_0$, então $n_0 \leq n_1 + n_2 < 2n_0$ e

$$(\alpha + n_1\gamma) + (\beta + n_2\gamma) = (\alpha + \beta + n_0\gamma) + (n_1 + n_2 - n_0)\gamma.$$

Como $0 \leq n_1 + n_2 - n_0 < n_0$, temos

$$\tau_\Psi((\alpha + n_1\gamma) + (\beta + n_2\gamma)) = \tau_\Phi(\alpha + \beta + n_0\gamma) \cdot (ax_\gamma)^{n_1 + n_2 - n_0}.$$

Portanto,

$$\begin{aligned}
\overline{\tau}_\Psi(\alpha + n_1\gamma, \beta + n_2\gamma) &= \left(\frac{\tau_\Psi(\alpha + n_1\gamma)\ \tau_\Psi(\beta + n_2\gamma)}{\tau_\Psi((\alpha + n_1\gamma) + (\beta + n_2\gamma))} \right) \nu \\
&= \left(\frac{\tau_\Phi(\alpha)\ (ax_\gamma)^{n_1}\ \tau_\Phi(\beta)\ (ax_\gamma)^{n_2}}{\tau_\Phi(\alpha + \beta + n_0\gamma)\ (ax_\gamma)^{n_1 + n_2 - n_0}} \right) \nu \\
&= \left(\frac{\tau_\Phi(\alpha)\ \tau_\Phi(\beta)\ (ax_\gamma)^{n_0}}{\tau_\Phi(\alpha + \beta + n_0\gamma)} \right) \nu
\end{aligned}$$

Visto que $\left(\dfrac{\tau_\Phi(n_0\gamma)}{(ax_\gamma)^{n_0}} \right) \nu = 1\nu$, multiplicamos o lado direito da equação acima para obter

$$\begin{aligned}
\overline{\tau}_\Psi(\alpha + n_1\gamma, \beta + n_2\gamma) &= \left(\frac{\tau_\Phi(\alpha)\tau_\Phi(\beta)(ax_\gamma)^{n_0}}{\tau_\Phi(\alpha + \beta + n_0\gamma)} \right) \nu \cdot \left(\frac{\tau_\Phi(n_0\gamma)}{(ax_\gamma)^{n_0}} \right) \nu \\
&= \left(\frac{\tau_\Phi(\alpha)\tau_\Phi(\beta)\tau_\Phi(n_0\gamma)}{\tau_\Phi(\alpha + \beta + n_0\gamma)} \right) \nu = 1\nu.
\end{aligned}$$

Isso completa a prova. $\square$

2.3 Exemplo

Apresentamos aqui um exemplo onde temos que usar um *twisting* não trivial para obter o isomorfismo do Teorema 2.1.1.

Considere $\mathbf{P} \subseteq \mathbb{N}$ o conjunto de todos os números primos e $\mathbf{X} = \{x_p \mid p \in \mathbf{P}\}$ um conjunto de variáveis independentes. Faça

$$K := \mathbb{Q}(x_p \mid x_p \in \mathbf{X}) \text{ e } \Gamma := \sum_{p \in \mathbf{P}} \frac{1}{p}\mathbb{Z} \subset \mathbb{Q}.$$

Vamos construir uma valorização $\nu : K^\times \longrightarrow \Gamma$. Comece definindo $\nu(x_p) := 1/p$ para cada $p \in \mathbf{P}$, $\nu(a) = 0$ para cada $a \in \mathbb{Q}^\times$ e $\nu(0) = \infty$. Considere agora funções

$$\lambda : \mathbf{P} \longrightarrow \mathbb{N}_0,$$

tais que $\lambda(p) \neq 0$ somente para finitos $p \in \mathbf{P}$ e

$$\mathbf{X}^\lambda := \prod_{\lambda(x_p) \neq 0} x_p^{\lambda(p)} \in K.$$

Assim podemos definir ν em cada monômio $a\mathbf{X}^\lambda \in K$ como segue

$$\nu\left(a\mathbf{X}^\lambda\right) = \nu\left(a \prod_{\lambda(p)\neq 0} x_p^{\lambda(p)}\right) := \sum_{\lambda(p)\neq 0} \frac{\lambda(p)}{p} = \sum_{\lambda(p)\neq 0} \left(\nu(a) + \lambda(p)\nu(x_p)\right).$$

Estendemos ν para K monomialmente, ou seja, definindo

$$\nu\left(\sum_{i=1}^{n} a_i \mathbf{X}^{\lambda_i}\right) = \min_{a_i \neq 0}\left\{\nu\left(a_i \mathbf{X}^{\lambda_i}\right)\right\},$$

em $\mathbb{Q}[x_p \,|\, x_p \in \mathbf{X}]$ e $\nu(P/Q) = \nu(P) - \nu(Q)$ em K.

Assuma que exista uma função escolha $\tau : \Gamma \longrightarrow K$ tal que $\overline{\tau}$ é constante e igual a 1. Vamos obter uma contradição com o fato de τ ser uma inversa à direita de ν. Isso provará que não pode existir um *twisting* trivial.

Definição 2.3.1. Para qualquer polinômio

$$P = \sum_{i=1}^{n} a_i \mathbf{X}^{\lambda_i} \in \mathbb{Q}[x_p \,|\, x_p \in \mathbf{X}]$$

definimos a **parte inicial de** P **com respeito a** ν por

$$\mathrm{ip}_\nu(P) := \sum_{\nu(a_i \mathbf{X}^{\lambda_i}) = \nu(P)} a_i \mathbf{X}^{\lambda_i}.$$

Um polinômio P é dito **inicial** se $\mathrm{ip}_\nu(P) = P$.

Observação 2.3.2. É fácil verificar que para $P, Q \in \mathbb{Q}[x_p \mid x_p \in \mathbf{X}]$, temos

(i) $\mathrm{in}_\nu\left(\mathrm{ip}_\nu(P)\right) = \mathrm{in}_\nu\left(P\right)$.

(ii) $\mathrm{in}_\nu(P) = \mathrm{in}_\nu(Q) \Longleftrightarrow \mathrm{ip}_\nu(P) = \mathrm{ip}_\nu(Q)$. Em particular, se P e Q são polinômios iniciais, então

$$\mathrm{in}_\nu(P) = \mathrm{in}_\nu(Q) \Longleftrightarrow P = Q.$$

Definição 2.3.3. Diremos que a função escolha $\tau : \Gamma \longrightarrow K$ é **inicial**, se para cada $\alpha \in \Gamma$, tivermos $\tau(\alpha) = \frac{P}{Q}$ com P e Q iniciais.

Afirmação 2.3.4. *Se τ é uma função escolha tal que $\overline{\tau} \equiv 1\nu$, então existe uma função escolha inicial τ' tal que $\overline{\tau'} \equiv 1\nu$.*

Demonstração. Para cada $\alpha \in \Gamma$ escrevemos $\tau(\alpha) = \frac{P_\alpha}{Q_\alpha} \in K$. Coloque $\tau'(\alpha) := \frac{\mathrm{ip}_\nu(P_\alpha)}{\mathrm{ip}_\nu(Q_\alpha)}$. Então

$$\alpha = \nu(\tau(\alpha)) = \nu\left(\frac{P_\alpha}{Q_\alpha}\right) = \nu(P_\alpha) - \nu(Q_\alpha) = \nu(\mathrm{ip}_\nu(P_\alpha)) - \nu(\mathrm{ip}_\nu(Q_\alpha)) = \nu(\tau'(\alpha)),$$

assim τ' é uma inversa à direita para ν. Além disso, pela Observação 2.2.6,

$$\begin{aligned}
\overline{\tau}(\alpha,\beta) = 1\nu \quad &\Longleftrightarrow \quad \mathrm{in}_\nu\left(\tau(\alpha)\right) \cdot \mathrm{in}_\nu\left(\tau(\beta)\right) = \mathrm{in}_\nu\left(\tau(\alpha+\beta)\right) \\
&\Longleftrightarrow \quad \mathrm{in}_\nu\left(\frac{P_\alpha}{Q_\alpha}\right) \cdot \mathrm{in}_\nu\left(\frac{P_\beta}{Q_\beta}\right) = \mathrm{in}_\nu\left(\frac{P_{\alpha+\beta}}{Q_{\alpha+\beta}}\right) \\
&\Longleftrightarrow \quad \mathrm{in}_\nu\left(\frac{\mathrm{ip}_\nu(P_\alpha)}{\mathrm{ip}_\nu(Q_\alpha)}\right) \cdot \mathrm{in}_\nu\left(\frac{\mathrm{ip}_\nu(P_\beta)}{\mathrm{ip}_\nu(Q_\beta)}\right) = \mathrm{in}_\nu\left(\frac{\mathrm{ip}_\nu(P_{\alpha+\beta})}{\mathrm{ip}_\nu(Q_{\alpha+\beta})}\right) \\
&\Longleftrightarrow \quad \overline{\tau'}(\alpha,\beta) = 1\nu.
\end{aligned}$$

□

Tendo a Afirmação 2.3.4, podemos assumir que τ é uma função escolha inicial.

Afirmação 2.3.5. *Para uma função escolha inicial $\tau : \Gamma \longrightarrow K$, se $\overline{\tau} \equiv 1\nu$, então $\tau(n\alpha) = \tau(\alpha)^n$ para cada $n \in \mathbb{N}$ e $\alpha \in \Gamma$.*

Demonstração. Fixe arbitrariamente $\alpha \in \Gamma$ e $n \in \mathbb{N}$. Coloque

$$\tau(\alpha) = \frac{P}{Q} \quad \text{e} \quad \tau(n\alpha) = \frac{P'}{Q'}.$$

Nossa hipótese garante que $\left(\dfrac{\tau(\alpha)^n}{\tau(n\alpha)}\right)\nu = 1\nu$. Isso nos dá

$$0 < \nu\left(\frac{\tau(\alpha)^n}{\tau(n\alpha)} - 1\right) = \nu\left(\frac{P^nQ'}{Q^nP'} - 1\right) = \nu\left(\frac{P^nQ' - Q^nP'}{Q^nP'}\right).$$

Portanto,

$$\nu\left(P^nQ' - Q^nP'\right) > \nu\left(Q^nP'\right).$$

Pela observação 2.3.2 **(ii)**, temos $P^nQ' = Q^nP'$ e consequentemente

$$\tau(\alpha)^n = \frac{P^n}{Q^n} = \frac{P'}{Q'} = \tau(n\alpha).$$

$\square$

Como consequência da Afirmação 2.3.5, obtemos

$$\tau(1) = \tau\left(p\,\frac{1}{p}\right) = \tau\left(\frac{1}{p}\right)^p, \text{ para cada } p \in \mathbf{P}. \tag{2.5}$$

Para um elemento $R = P/Q \in K$ definimos $\deg(R) := \max\{\deg_{\mathbf{X}}(P), \deg_{\mathbf{X}}(Q)\}$. Então, $\deg(R^n) = n\deg(R)$ para cada $R \in K$ e $n \in \mathbb{N}$. Por (2.5), temos

$$p \mid \deg(\tau(1)), \text{ para cada } p \in \mathbf{P}.$$

Isso implica que $\deg(\tau(1)) = 0$, logo $\tau(1) \in \mathbb{Q}$. Assim, $\nu(\tau(1)) = 0$, o que é uma contradição a suposição de que τ é uma inversa à direita de ν.

Observação 2.3.6. Antes de finalizarmos o presente capítulo, ressaltamos que a recíproca do Teorema 2.1.2 não é válida. De fato, considere Γ o grupo abeliano ordenado $\sum_{p\in\mathbf{P}} \frac{1}{p}\mathbb{Z}$, como no exemplo acima, e $K = \mathbb{Q}((\Gamma))$ o corpo das séries formais de Laurent. Isto é, os elementos $b \in K$ são séries formais

$$b = \sum_{\gamma\in\Gamma} b_\gamma t^\gamma,$$

tais que

$$\operatorname{supp}(b) = \{\gamma \in \Gamma \mid b_\gamma \neq 0\}$$

é um subconjunto bem ordenado de Γ. Nessa situação, consideramos $\nu : K \longrightarrow \Gamma$ a valorização definida por

$$\nu(b) := \min\{\operatorname{supp}(b)\}, \text{ para cada } b \in K,$$

e a função escolha $\tau : \Gamma \longrightarrow K$ dada por

$$\tau(\gamma) := t^\gamma, \text{ para cada } \gamma \in \Gamma.$$

Visto que

$$\tau(\alpha)\tau(\beta) = t^\alpha t^\beta = t^{\alpha+\beta} = \tau(\alpha + \beta),$$

obtemos $\overline{\tau} \equiv 1\nu$. Todavia, $K\nu$ não é fechado por radicais, pois $-1\nu \in K\nu$ não possui raiz quadrada, e Γ não é um grupo livre. Portanto, a recíproca do Teorema 2.1.2 não é válida.

Capítulo 3

Sequência geradora

A finalidade deste capítulo é estudar as diferentes definições de sequências geradoras que aparecem na literatura. Apresentamos essas definições e mostramos que, em certas situações, elas são equivalentes. Todavia, em geral, elas não são equivalentes, conforme nosso Exemplo 3.2.1 garante. Também apresentamos a relação entre sequências geradoras e polinômios chave.

3.1 Preliminares

Seja R um anel e ν uma valorização em R. Para $\mathbf{Q} \subseteq R$ denotamos

$$\mathbb{N}_0^{\mathbf{Q}} := \{\lambda : \mathbf{Q} \longrightarrow \mathbb{N}_0 \mid \lambda(Q) \neq 0 \text{ somente para finitos } Q \in \mathbf{Q}\}$$

e

$$\mathbf{Q}^\lambda := \prod_{\lambda(Q) \neq 0} Q^{\lambda(Q)} \in R.$$

Em [17], a definição da sequência geradora é uma ligeira variação do seguinte. Um conjunto $\mathbf{Q} \subseteq R$ satisfaz **(GS1)** se para cada $\gamma \in \nu(R)$ o grupo abeliano $\mathcal{P}_\gamma$ é gerado por

$$\left\{ a\mathbf{Q}^\lambda \mid \nu(a\mathbf{Q}^\lambda) \geq \gamma \text{ onde } \lambda \in \mathbb{N}_0^{\mathbf{Q}} \text{ e } a \in R^\times \right\}.$$

A definição da sequência geradora em [14] e [34] é a seguinte. Se ν é centrada em R (i.e, $\nu(f) \geq 0$ para todo $f \in R$), então $\mathbf{Q} \subseteq R$ satisfaz **(GS2)** se para cada $\gamma \in \nu(R)$ o ideal

$\mathcal{P}_\gamma$ é gerado por

$$\left\{\mathbf{Q}^\lambda \mid \nu(\mathbf{Q}^\lambda) \geq \gamma \text{ onde } \lambda \in \mathbb{N}_0^{\mathbf{Q}}\right\}.$$

Observamos que se ν é centrada, então **(GS1)** implica **(GS2)** e que **(GS2)** só faz sentido para valorizações centradas. Além disso, ao lidar com polinômios chave para uma valorização ν em $K[x]$, o caso em que ν é centrada não é interessante (ver Lema 3.3.4).

A definição de uma sequência geradora em [9], [25] e [39] é a seguinte. Se ν é centrada em R, então $\mathbf{Q} \subseteq R$ satisfaz **(GS3)** se o conjunto

$$\mathrm{in}_\nu(\mathbf{Q}) := \{\mathrm{in}_\nu(Q) \mid Q \in \mathbf{Q}\}$$

gera $\mathrm{gr}_\nu(R)$ como $R/\mathfrak{m}$-álgebra.

Um dos principais objetivos deste capítulo é estabelecer a relação entre essas diferentes definições. Mais especificamente, provamos o seguinte.

Teorema 3.1.1. *Seja R um anel, ν uma valorização em R e $\boldsymbol{Q}$ um subconjunto de R.*

*(i) Se ν é centrada e $\boldsymbol{Q}$ satisfaz **(GS2)**, então para cada $\gamma \in \nu(R)$ o grupo $\mathcal{P}_\gamma/\mathcal{P}_\gamma^+$ é gerado por*

$$\left\{a\boldsymbol{Q}^\lambda + \mathcal{P}_\gamma^+ \mid \lambda \in \mathbb{N}_0^{\boldsymbol{Q}}, \nu(Q^\lambda) = \gamma \text{ e } \nu(a) = 0\right\}.$$

*Em particular, $\boldsymbol{Q}$ satisfaz **(GS3)**.*

*(ii) Se $\boldsymbol{Q}$ satisfaz **(GS3)**, então o semigrupo $\nu(R)$ é gerado por*

$$\nu(\boldsymbol{Q}) := \{\nu(Q) \mid Q \in \boldsymbol{Q}\}.$$

*Reciprocamente, se R é um domínio com $K = \mathrm{Quot}(R)$, $K\nu = R/\mathfrak{m}$ e $\nu(\boldsymbol{Q})$ gera $\nu(R)$, então **(GS3)** é satisfeito.*

Na Seção 3.2 apresentamos um exemplo que mostra que a recíproca do item *(i)* do Teorema 3.1.1 não é válida em geral.

Na Seção 3.3 estudamos a relação entre sequências geradoras e polinômios chave. O caso de estudo interessante é para valorizações ν em $K[x]$ que não são triviais em K. Portanto, queremos comparar as sequências de polinômios chave que são completas e as sequências satisfazendo **(GS1)**. Fazemos uma mudança sutil em **(GS1)** quando $R = K[x]$. Diremos que $\mathbf{Q}$ satisfaz **(GS1*)** se para cada $f \in K[x]$ existem $a_1, \ldots, a_r \in K$ e $\lambda_1, \ldots, \lambda_r \in \mathbb{N}_0^{\mathbf{Q}}$, tais que

$$f = \sum_{i=1}^{r} a_i \mathbf{Q}^{\lambda_i} \text{ com } \nu\left(a_i \mathbf{Q}^{\lambda_i}\right) \geq \nu(f), \text{ para cada } i, 1 \leq i \leq r,$$

e para cada i, $1 \leq i \leq r$, se $\lambda_i(Q) \neq 0$, então $\deg(Q) \leq \deg(f)$. Como $K[x]^\times = K^\times$, a única diferença entre **(GS1)** e **(GS1*)** é a condição nos graus.

Outro importante resultado deste capítulo é o seguinte.

Teorema 3.1.2. *Seja $\boldsymbol{Q}$ um conjunto de polinômios chave para $K[x]$. Então $\boldsymbol{Q}$ é completo se, e somente se, $\boldsymbol{Q}$ satisfaz **(GS1*)**.*

3.2 Demonstração do Teorema 3.1.1

Demonstração do Teorema 3.1.1. A fim de provar *(i)*, assuma que $\mathbf{Q}$ satisfaz **(GS2)**. Fixe $\gamma \in \nu(R)$ e escolha $f \in R$ tal que $\nu(f) = \gamma$. Como $\mathcal{P}_\gamma$ é gerado como um ideal por

$$\left\{\mathbf{Q}^\lambda \mid \lambda \in \mathbb{N}_0^{\mathbf{Q}} \text{ e } \nu\left(\mathbf{Q}^\lambda\right) \geq \gamma\right\},$$

existem $a_1, \ldots, a_r \in R$ e $\lambda_1, \ldots, \lambda_r \in \mathbb{N}_0^{\mathbf{Q}}$ tais que

$$f = \sum_{i=1}^{r} a_i \mathbf{Q}^{\lambda_i} \text{ e } \nu\left(\mathbf{Q}^{\lambda_i}\right) \geq \gamma = \nu(f) \text{ para cada } i, 1 \leq i \leq r. \tag{3.1}$$

Seja

$$I = \{i \in \{1, \ldots, r\} \mid \nu(a_i) = 0 \text{ e } \nu\left(\mathbf{Q}^{\lambda_i}\right) = \gamma\}.$$

Segue de (3.1) que $I \neq \emptyset$. Então,

$$\nu\left(f - \sum_{i \in I} a_i \mathbf{Q}^{\lambda_i}\right) = \nu\left(\sum_{i \notin I} a_i \mathbf{Q}^{\lambda_i}\right) > \gamma.$$

Portanto, $f - \sum_{i \in I} a_i \mathbf{Q}^{\lambda_i} \in \mathcal{P}_\gamma^+$. Além disso, usando o Lema 1.3.2, temos

$$\operatorname{in}_\nu(f) = \operatorname{in}_\nu\left(\sum_{i \in I} a_i \mathbf{Q}^{\lambda_i}\right) = \sum_{i \in I'} \operatorname{in}_\nu\left(a_i \mathbf{Q}^{\lambda_i}\right) = \sum_{i \in I'} \overline{a_i}\left(\operatorname{in}_\nu\left(\mathbf{Q}\right)\right)^{\lambda_i}$$

para algum $I' \subseteq I$. Portanto, $\mathbf{Q}$ satisfaz **(GS3)**.

Para provar *(ii)* assuma que $\mathbf{Q} \subseteq R$ satisfaz **(GS3)**. Tome $\gamma \in \nu(R)$ e $f \in R$ tal que $\nu(f) = \gamma$. Pela nossa hipótese, existem $a_1, \dots, a_r \in R \setminus \mathfrak{m}$ e $\lambda_1, \dots, \lambda_r \in \mathbb{N}_0^{\mathbf{Q}}$ tais que

$$\mathrm{in}_\nu(f) = \sum_{i=1}^{r} \overline{a_i}\mathrm{in}_\nu\left(\mathbf{Q}^{\lambda_i}\right). \tag{3.2}$$

Como $\mathrm{in}_\nu(f)$ é homogêneo, podemos assumir que os elementos à direita de (3.2) são homogêneos e estão na mesma componente homogênea de $\mathrm{in}_\nu(f)$. Isso significa que para cada um desses índices i temos

$$\gamma = \nu(f) = \nu\left(\mathbf{Q}^{\lambda_i}\right) = \sum_{\lambda_i(Q)\neq 0} \lambda_i(Q)\nu(Q),$$

que é o que queríamos provar.

Agora assuma que $K\nu = R/\mathfrak{m}$ e que $\nu(R)$ é gerado por $\nu(\mathbf{Q})$. Para $f \in R$ existem $n_1, \dots, n_r \in \mathbb{N}$ e $Q_1, \dots, Q_r \in \mathbf{Q}$ tais que

$$\nu(f) = \sum_{i=1}^{r} n_i\nu(Q_i) = \nu\left(\prod_{i=1}^{r} Q_i^{n_i}\right)$$

Como $K\nu = R/\mathfrak{m}$, existe $z \in R \setminus \mathfrak{m}$ tal que

$$z\nu = \frac{f}{\prod_{i=1}^{r} Q_i^{n_i}}\nu.$$

Isso significa que $\nu\left(f - z\prod_{i=1}^{r} Q_i^{n_i}\right) > \nu(f)$ e consequentemente

$$\mathrm{in}_\nu(f) = \mathrm{in}_\nu\left(z\prod_{i=1}^{r} Q_i^{n_i}\right) = \overline{z}\prod_{i=1}^{r}\left(\mathrm{in}_\nu(Q_i)\right)^{n_i}.$$

□

Exemplo 3.2.1. Este exemplo mostra que a recíproca do Teorema 3.1.1 *(i)* não vale em geral. Considere um corpo k e uma valorização em $k[x, y]$ induzida pela imersão de $k[x, y]$ em $K = k((t^{\mathbb{Q}}))$ definida por

$$x \longmapsto t \text{ e } y \longmapsto \sum_{i=1}^{\infty} t^{i^2} = t + t^4 + t^9 + t^{16} + \dots,$$

onde $\nu(k^\times) = 0$ e $\nu(t) = 1$. Para cada $p(x,y) \in k[x,y]$ existe $n_0 \in \mathbb{N}$ e $a_{n_0} \in k$ tal que

$$\nu(p(x,y) - a_{n_0}x^{n_0}) > n_0.$$

De fato, podemos escrever

$$p\left(t, \sum_{i=1}^{\infty} t^{i^2}\right) = \sum_{k=n_0}^{\infty} a_k t^k.$$

Logo,

$$\nu\left(p(x,y) - a_{n_0}x^{n_0}\right) = \nu_t\left(p\left(t, \sum_{i=1}^{\infty} t^{i^2}\right) - a_{n_0}t^{n_0}\right) > n_0.$$

Como $\nu\left(a_{n_0}x^{n_0}\right) = n_0$ temos que

$$\mathrm{in}_\nu(p) = \mathrm{in}_\nu(a_{n_0}x^{n_0}) = \overline{a_{n_0}}\mathrm{in}_\nu(x)^{n_0}.$$

Portanto, $\mathbf{Q} = \{x\}$ satisfaz **(GS3)**. Contudo, $y \in \mathcal{P}_1$ e como x e y são algebricamente independentes sobre k, para cada $p_1, \ldots, p_r \in k[x,y]$ temos

$$y \neq \sum_{i=1}^{r} p_i x^i.$$

Portanto, $\mathbf{Q} = \{x\}$ não satisfaz **(GS2)**.

3.3 Sequências geradoras vs polinômios chave

Nesta seção, discutimos a relação entre polinômios chave e sequências geradoras.

Definição 3.3.1. Um conjunto $\mathbf{Q} \subseteq K[x]$ é chamado de **conjunto completo para** ν se para cada $f \in K[x]$ existe $Q \in \mathbf{Q}$ com $\deg(Q) \leq \deg(f)$ tal que $\nu_Q(f) = \nu(f)$. Se o conjunto $\mathbf{Q}$ admite uma ordem sob a qual é bem ordenado, então é chamado de **sequência completa**.

Teorema 3.3.2 (Teorema 1.1 de [30]). *Toda valorização ν em $K[x]$ admite um conjunto completo $\mathbf{Q}$ de polinômios chave. Além disso, $\mathbf{Q}$ pode ser escolhido como bem ordenado em relação à ordem dada por $Q < Q'$ se $\epsilon(Q) < \epsilon(Q')$.*

Observação 3.3.3. Em [30], a definição de sequência completa não requer que $\deg(Q) \leq \deg(f)$ como na Definição 3.3.1. Essa propriedade é importante e a prova do Teorema 1.1 em [30] garante que a sequência obtida satisfaz essa propriedade adicional.

Lema 3.3.4. *Uma valorização ν em $K[x]$ é centrada se, e somente se, $\nu(a) = 0$ para cada $a \in K \setminus \{0\}$ e $\nu(x) \geq 0$.*

Demonstração. Assuma que ν é centrada. Em particular, $\nu(x) \geq 0$. Além disso, como ν é centrada, $\nu(a) \geq 0$ para cada $a \in K \setminus \{0\}$. Se $\nu(a) > 0$, então

$$\nu(a^{-1}) = -\nu(a) < 0,$$

o que é uma contradição. Consequentemente, $\nu(a) = 0$.

Assuma agora que $\nu(x) \geq 0$ e $\nu(a) = 0$ para cada $a \in K \setminus \{0\}$. Dado $f = a_0 + \ldots + a_n x^n \in K[x]$ temos

$$\nu(f) \geq \min\{\nu(a_i x^i)\} \geq 0.$$

Portanto, ν é centrada. □

Para provar o Teorema 3.1.2, precisamos de alguns resultados. Nosso primeiro resultado mostra que qualquer conjunto completo (independentemente de ser formado por polinômios chave) satisfaz **(GS1*)**.

Proposição 3.3.5. *Se $\mathbf{Q} \subseteq K[x]$ é um conjunto completo para ν, então $\mathbf{Q}$ satisfaz **(GS1*)**.*

Demonstração. Provaremos por indução no grau de f. Se $\deg(f) = 1$, então $f = x - a$ para algum $a \in K$. Pela nossa hipótese, existe $x - b \in \mathbf{Q}$ tal que

$$\beta := \nu(x - a) = \nu_{x-b}(x - a) = \min\{\nu(x - b), \nu(b - a)\}.$$

Isso implica que $\nu(x-b) \geq \beta$, $\nu(b-a) \geq \beta$ e que $f = (x-b)+(b-a)$, que é o que queríamos provar.

Assuma agora que para cada $k \in \mathbb{N}$ e para cada $f \in K[x]$ de $\deg(f) < k$ nosso resultado é satisfeito. Seja f um polinômio de grau k. Como $\mathbf{Q}$ é um conjunto completo para ν, existe $q \in \mathbf{Q}$ tal que $\deg(q) \leq \deg(f)$ e $\nu_q(f) = \nu(f)$. Seja

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

a q-expansão de f. Como $\deg(q) \leq \deg(f)$, temos $\deg(f_i) < \deg(f) = k$ para cada i, $1 \leq i \leq s$. Pela hipótese de indução, existem

$$a_{11}, \ldots, a_{1r_1}, \ldots, a_{s1}, \ldots, a_{sr_s} \in K \text{ e } \lambda_{11}, \ldots, \lambda_{1r_1}, \ldots, \lambda_{s1}, \ldots, \lambda_{sr_s} \in \mathbb{N}_0^{\mathbf{Q}},$$

tais que para cada i, $0 \leq i \leq s$,

$$f_i = \sum_{j=1}^{r_i} a_{ij}\mathbf{Q}^{\lambda_{ij}} \text{ com } \nu\left(a_{ij}\mathbf{Q}^{\lambda_{ij}}\right) \geq \nu(f_i) \text{ para cada } j, 1 \leq j \leq r_i,$$

e $\deg(Q) \leq \deg(f_i) \leq \deg(f)$ para cada polinômio Q tal que $\lambda_{ij}(Q) \neq 0$ para alguns i, j. Isso implica que

$$f = \sum_{i=0}^{s}\left(\sum_{j=1}^{r_i} a_{ij}\mathbf{Q}^{\lambda_{ij}}\right) q^i = \sum_{0 \leq i \leq s, 1 \leq j \leq r_i} a_{ij}\mathbf{Q}^{\lambda'_{ij}},$$

onde

$$\lambda'_{ij}(q') = \begin{cases} \lambda_{ij}(q') + i & \text{if } q' = q \\ \lambda_{ij}(q') & \text{if } q' \neq q \end{cases}.$$

Além disso, como $\nu_q(f) = \min\limits_{0 \leq i \leq s}\{\nu(f_i q^i)\} = \nu(f)$ e

$$\nu\left(a_{ij}\mathbf{Q}^{\lambda_{ij}}\right) \geq \nu(f_i), \text{ para cada } i, 0 \leq i \leq n \text{ e } j, 1 \leq j \leq r_i,$$

temos

$$\nu(f) \leq \nu(f_i) + i\nu(q) \leq \nu\left(a_{ij}\mathbf{Q}^{\lambda_{ij}}\right) + i\nu(q) = \nu\left(a_{ij}\mathbf{Q}^{\lambda'_{ij}}\right),$$

para cada i, $0 \leq i \leq s$ e j, $1 \leq j \leq r_i$, que é o que queríamos provar. $\square$

O próximo resultado fornece a recíproca da Proposição 3.3.5.

Proposição 3.3.6. *Assuma que* $\boldsymbol{Q}$ *é um subconjunto de* $K[x]$ *com as seguintes propriedades.*

- ν_Q *é uma valorização para cada* $Q \in \boldsymbol{Q}$*.*
- *Para cada subconjunto finito* $\mathcal{F} \subseteq \boldsymbol{Q}$*, existe* $Q' \in \mathcal{F}$ *tal que* $\nu_{Q'}(Q) = \nu(Q)$ *para cada* $Q \in \mathcal{F}$*.*
- ***(GS1*)*** *é satisfeito.*

Então $\boldsymbol{Q}$ *é um conjunto completo para* ν*.*

Demonstração. Fixe arbitrariamente um polinômio $f \in K[x]$ e coloque $\beta := \nu(f)$. Então, existem $a_1, \ldots, a_r \in K$ e $\lambda_1, \ldots, \lambda_r \in \mathbb{N}_0^{\mathbf{Q}}$ tais que

$$f = \sum_{i=1}^{r} a_i\mathbf{Q}^{\lambda_i} \text{ com } \nu\left(a_i\mathbf{Q}^{\lambda_i}\right) \geq \beta, \text{ para cada } i, 1 \leq i \leq r,$$

e $\deg(Q) \leq \deg(f)$ para cada $Q \in \mathbf{Q}$ tal que $\lambda_i(Q) \neq 0$ para algum i, $1 \leq i \leq r$. Seja

$$\mathcal{F} := \{Q \in \mathbf{Q} \mid \lambda_i(Q) \neq 0 \text{ para algum } i, 1 \leq i \leq n\}.$$

Como $\mathcal{F}$ é finito, existe $Q' \in \mathcal{F}$ tal que $\nu_{Q'}(Q) = \nu(Q)$ para cada $Q \in \mathcal{F}$. Em particular, $\nu\left(a_i \mathbf{Q}^{\lambda_i}\right) = \nu_{Q'}\left(a_i \mathbf{Q}^{\lambda_i}\right)$ para cada i, $1 \leq i \leq r$. Então

$$\beta \leq \min_{1 \leq i \leq n} \left\{\nu\left(a_i \mathbf{Q}^{\lambda_i}\right)\right\} = \min_{1 \leq i \leq n} \left\{\nu_{Q'}\left(a_i \mathbf{Q}^{\lambda_i}\right)\right\} \leq \nu_{Q'}(f) \leq \nu(f) = \beta.$$

Portanto, $\nu_Q(f) = \nu(f)$ e isso conclui a prova. □

Demonstração do Teorema 3.1.2. Se $\mathbf{Q}$ é um conjunto completo para ν, então, pela Proposição, 3.3.5 $\mathbf{Q}$ satisfaz **(GS1*)**.

Para provar a recíproca, observamos que como cada elemento Q em $\mathbf{Q}$ é um polinômio chave, pela Proposição 1.5.4, temos que ν_Q é uma valorização. Além disso, como $\mathbf{Q}$ é ordenado por $Q < Q'$ se, e somente se, $\epsilon(Q) < \epsilon(Q')$, para cada conjunto finito $\mathcal{F}$ podemos escolher $Q' \in \mathcal{F}$ tal que $\epsilon(Q) \leq \epsilon(Q')$ para cada $Q \in \mathcal{F}$. Aplicando o Corolário 1.5.7 obtemos

$$\nu_{Q'}(Q) = \nu(Q) \text{ para cada } Q \in \mathcal{F}.$$

O resultado agora segue da Proposição 3.3.6. □

Uma consequência interessante do Teorema 3.1.2 é a seguinte.

Corolário 3.3.7. *Para cada valorização ν em $K[x]$, existe um conjunto de polinômios chave $\mathbf{Q} \subseteq K[x]$ tal que $\mathbf{Q}$ satisfaz **(GS1*)**. Além disso, este conjunto pode ser escolhido para ser bem ordenado em relação à ordem $Q < Q'$ se $\epsilon(Q) < \epsilon(Q')$.*

Demonstração. Segue diretamente dos Teoremas 3.3.2 e 3.1.2. □

Capítulo 4

Polígono de Newton

Neste capítulo introduzimos a noção de polígono de Newton em relação a um dado polinômio q. Uma vez calculada as inclinações das arestas do polígono de Newton, verificamos quando $-\nu(q)$ é um desses valores. Mostramos, em seguida, que o cálculo do q-truncamento de uma valorização ν pode ser simplificado. Também obtemos alguns resultados para a álgebra graduada de $K[x]$ associada à ν_q. Por último, apresentamos o Lema 4 de [19], no contexto de uma valorização ν_0 definida em um corpo K, e aplicamos esses resultados para extensões de Artin-Schreier.

4.1 Preliminares

Sejam K um corpo, $f, q \in K[x]$, com q mônico, $\nu : K[x] \longrightarrow \Gamma_\infty$ uma valorização e considere

$$f = a_0 + a_1 q + \ldots + a_n q^n$$

a q-expansão de f. Denotamos por $\Delta_{q,\nu}(f)$ o fecho convexo de

$$X := \{(i, \nu(a_i) + \gamma) \,|\, 0 \leq i \leq n, \nu(a_i) \neq \infty \text{ e } \gamma \in \Gamma_{\mathbb{Q}} \text{ com } \gamma \geq 0\} \tag{4.1}$$

em $\mathbb{Q} \times \Gamma_{\mathbb{Q}}$. O conjunto $\Delta_{q,\nu}(f)$ é chamado de **polígono de Newton de f com respeito a q e ν**. Observe que precisamos apenas que ν esteja definida em polinômios de grau estritamente menor do que o grau de q.

Outra maneira de se obter o conjunto $\Delta_{q,\nu}(f)$ é tomando a interseção de todos os semiplanos que contém X, ou seja,

$$\Delta_{q,\nu}(f) = \mathrm{Conv}(X) = \bigcap_{\substack{H \text{ semiplano} \\ X \subseteq H}} H.$$

Considere uma reta não vertical L em $\mathbb{Q} \times \Gamma_{\mathbb{Q}}$ tal que $\Delta_{q,\nu}(f)$ está contido em apenas um dos dois semiplanos definidos por L e $\Delta_{q,\nu}(f) \cap L$ contém pelo menos dois pontos. Nessas condições, uma **aresta** do polígono de Newton de f com respeito a q e ν é o conjunto $I = \Delta_{q,\nu}(f) \cap L$. A reta L é chamada de **reta suporte da aresta** F. A **inclinação** da aresta I é a inclinação da reta L, que é denotada por $s(L)$ ou, simplesmente, por $s(I)$.

Um **vértice** V é um ponto inicial ou final de uma aresta. Por exemplo, pontos que pertencem simultaneamente a duas arestas distintas de $\Delta_{Q,\nu}(f)$ são vértices. Denotamos o conjunto de todos os vértices de $\Delta_{q,\nu}(f)$ por $\{(a_{i_0}, \nu(a_{i_0})), \ldots, (a_{i_m}, \nu(a_{i_m}))\}$, onde $i_0 = 0$ e $i_m = n$.

Note que, fixados dois vértices $(a_{i_l}, \nu(a_{i_l}))$ e $(a_{i_k}, \nu(a_{i_k}))$ de $\Delta_{Q,\nu}(f)$, eles pertencem a mesma aresta se, e somente se, são consecutivos. Deste modo, para obter resultados relacionados as arestas de $\Delta_q(f)$, vamos considerar i_l e i_k em $\{i_0, \ldots, i_m\}$ tais que $k = l + 1$. Isto é, vamos considerar l, $0 \leq l < m$, e $k = l + 1$.

Para cada l, $0 \leq l < m$, e $k = l + 1$, denotamos por I_{i_k} o segmento em $\mathbb{Q} \times \Gamma_{\mathbb{Q}}$ que une os vértices $(a_{i_l}, \nu(a_{i_l}))$ e $(a_{i_k}, \nu(a_{i_k}))$.

Exemplo 4.1.1. A inclinação da primeira aresta de $\Delta_{q,\nu}(f)$ é

$$s(I_{i_1}) = \frac{\nu(a_{i_1}) - \nu(a_0)}{i_1 - 0}.$$

Ainda, assumindo

$$\nu_q(f) < \nu(f),$$

temos que $-\nu(q)$ é um limitante superior para a primeira inclinação de $\Delta_{q,\nu}(f)$. De fato, note que

$$\nu(a_0) < \min_{0 < j \leq n} \{\nu(a_j q^j)\},$$

implica que

$$\nu(f) = \min\{\nu(a_0), \nu(a_1 q + \ldots + a_n q^n)\} = \nu(a_0) = \min_{0 \leq j \leq n} \{\nu(a_j q^j)\} = \nu_q(f).$$

O que não é nosso caso. Logo, existe j, $0 < j \leq n$, tal que

$$\nu(a_j q^j) \leq \nu(a_0).$$

Assim,

$$\frac{\nu(a_{i_1}) - \nu(a_0)}{i_1 - 0} = \min_{0<i\leq n}\left\{\frac{\nu(a_i) - \nu(a_0)}{i - 0}\right\} \leq \frac{\nu(a_j) - \nu(a_0)}{j - 0} \leq -\nu(q).$$

Notação 4.1.2. Por simplicidade, quando não houver risco de confusão, escrevemos $\Delta_q(f)$ em vez de $\Delta_{q,\nu}(f)$.

O seguinte exemplo mostra o polígono de Newton de f com respeito a q e ν, onde $\nu : K[x] \longrightarrow \Gamma_\infty$ é uma valorização fixada, $q = x$, e $f = a_0 + a_1 x + a_2 x^2 + a_4 x^4 + a_5 x^5$ é um polinômio tal que $\nu(a_0) = 1$, $\nu(a_1) = 2$, $\nu(a_2) = 2$, $\nu(a_4) = 4$ e $\nu(a_5) = 5$.

Exemplo 4.1.3. O primeiro vértice é o par $(0, \nu(a_0)) = (0, 1)$. Para determinar o segundo vértice tomamos i_1, $0 < i_1 \leq 5$, o maior valor tal que

$$\frac{\nu(a_{i_1}) - \nu(a_0)}{i_1 - 0} \leq \min_{0<i\leq 5}\left\{\frac{\nu(a_i) - \nu(a_0)}{i - 0}\right\} = \min\left\{\frac{2-1}{1}, \frac{2-1}{2}, \frac{4-1}{4}, \frac{5-1}{5}\right\} = \frac{1}{2}.$$

Nesse caso, $i_1 = 2$ e o segundo vértice é o par $(i_1, \nu(a_{i_1})) = (2, 2)$. O terceiro vértice é o par $(i_2, \nu(a_{i_2}))$, onde i_2, $2 < i_2 \leq 5$, é o maior valor tal que

$$\frac{\nu(a_{i_2}) - \nu(a_{i_1})}{i_2 - i_1} \leq \min_{2<i\leq 5}\left\{\frac{\nu(a_i) - \nu(a_{i_1})}{i - i_1}\right\} = \min\left\{\frac{4-2}{4-2}, \frac{5-2}{5-2}\right\} = 1.$$

Visto que $i_2 = 5$, obtemos que $(i_2, \nu(a_{i_2})) = (5, 5)$ é o último vértice que precisamos determinar. Os segmentos $\overline{(0,1)(2,2)}$ e $\overline{(2,2)(5,5)}$ são as arestas do polígono de Newton.

Note que na Figura 4.1 destacamos os vértices do polígono de Newton em questão e suas arestas.

Para os próximos resultados estamos considerando K um corpo, $f, q \in K[x]$, com q mônico, $\nu : K[x] \longrightarrow \Gamma_\infty$ uma valorização e

$$f = a_0 + a_1 q + \ldots + a_n q^n$$

a q-expansão de f.

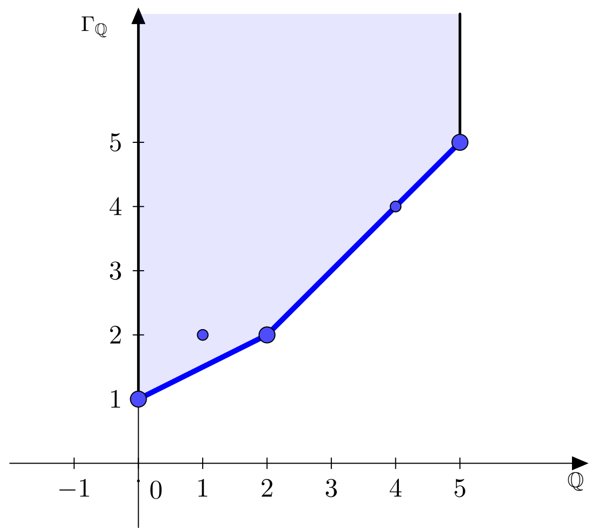


Figura 4.1: Polígono de Newton de f com respeito a q e ν.

Lema 4.1.4. *A equação da reta suporte da aresta de $\Delta_q(f)$ de vértices $(i_l, \nu(a_{i_l}))$ e $(i_k, \nu(a_{i_k}))$, $k = l + 1$, é*

$$y = s(I_{i_k})x + \nu(a_{i_l}) - s(I_{i_k})i_l. \tag{4.2}$$

Demonstração. Basta notar que

$$s(I_{i_k}) = \frac{\nu(a_{i_k}) - \nu(a_{i_l})}{i_k - i_l}$$

é a inclinação correspondente a aresta cujos vértices são $(i_l, \nu(a_{i_l}))$ e $(i_k, \nu(a_{i_k}))$ e a reta (4.2) passa pelo ponto $(i_l, \nu(a_{i_l}))$ de $\mathbb{Q} \times \Gamma_{\mathbb{Q}}$. $\square$

Corolário 4.1.5. *A equação da reta suporte da aresta de $\Delta_q(f)$ de vértices $(i_l, \nu(a_{i_l}))$ e $(i_k, \nu(a_{i_k}))$, $k = l + 1$, intersecta a reta $\{0\} \times \Gamma_{\mathbb{Q}}$ no ponto*

$$(0, \nu(a_{i_l}) - s(I_{i_k})i_l)\,.$$

Observação 4.1.6. Se no Corolário 4.1.5 $s(I_{i_k}) = -\nu(q)$, então

$$(0, \nu(a_{i_l}) - s(I_{i_k})i_l) = \left(0, \nu(a_{i_l}q^{i_l})\right),$$

ou seja, a reta suporte cruza o "eixo y" na altura $\nu(a_{i_l}q^{i_l})$.

Para os próximos resultados fixamos $f \in K[x]$ irredutível. Note que dada uma classe $\overline{g} = g + (f)$ em $K[x]/(f)$, podemos assumir $\deg(g) < \deg(f)$, pois considerando

$$g = g_0 + g_1 f + \ldots + g_n f^n$$

a f-expansão de g, temos a seguinte igualdade de classes em $K[x]/(f)$

$$\overline{g_0} = \overline{g},$$

com $\deg(g_0) < \deg(f)$.

Lema 4.1.7. *Uma valorização ν definida em $K[x]$ com* $\operatorname{supp}(\nu) = (f)$ *define uma valorização de Krull $\overline{\nu}$ em $K[x]/(f)$ e vice-versa.*

Demonstração. Suponha que ν seja uma valorização em $K[x]$ com $\nu(f) = \infty$ para algum $f \in K[x]$. Para cada $\overline{g} = g + (f) \in K[x]/(f)$, com $\deg(g) < \deg(f)$, defina

$$\overline{\nu}(\overline{g}) := \nu(g).$$

Veja que $\overline{\nu}$ está bem definida, pois se $g_1 + (f) = g_2 + (f)$ em $K[x]/(f)$ com $\deg(g_1), \deg(g_2) < \deg(f)$, então

$$\nu(g_1 - g_2) = \nu(\lambda f) = \infty$$

implica que $\nu(g_1) = \nu(g_2)$. Logo,

$$\overline{\nu}(\overline{g_1}) = \nu(g_1) = \nu(g_2) = \overline{\nu}(\overline{g_2}).$$

Ainda, $\overline{\nu}$ herda as propriedades de valorização de ν, sendo $\overline{f}$ a classe do elemento nulo em $K[x]/(f)$.

Por outro lado, se tivermos uma valorização $\overline{\nu}$ definida em $K[x]/(f)$, podemos colocar

$$\nu(g) = \overline{\nu}(\overline{g})$$

para todo $g \in K[x]$. Assim, ν é uma valorização em $K[x]$ com

$$\nu(f) = \overline{\nu}(\overline{f}) = \infty.$$

Como queríamos demonstrar. $\square$

Note que o Lema 4.1.7 nos permite trabalhar com valorizações ν em $K[x]$ com $\operatorname{supp}(\nu) = (f)$ em vez de trabalhar com valorizações $\overline{\nu}$ em $K[x]/(f)$. Esse lema será usado de forma implícita na Seção 4.3 e na Seção 4.4.

Lema 4.1.8. *Suponha que* $\operatorname{supp}(\nu) = (f)$*. Então,*

$$\nu_q(f) < \nu(f),$$

para cada $q \in K[x]$ *com* $\deg(q) < \deg(f)$*.*

Demonstração. Seja

$$f = a_0 + a_1 q + \ldots + a_n q^n$$

a q-expansão de f. Dado que $\operatorname{supp}(\nu)$ é um ideal primo e $\deg(a_i), \deg(q) < \deg(f)$, $0 \leq i \leq n$, implica que $a_i, q \notin \operatorname{supp}(\nu)$, $0 \leq i \leq n$. Concluímos que $a_i q^i \notin \operatorname{supp}(\nu)$, $0 \leq i \leq n$. Portanto,

$$\nu_q(f) = \min_{0 \leq i \leq n} \{\nu(a_i q^i)\} < \infty = \nu(f).$$

□

4.2 Polígono de Newton e truncamento

Buscamos com esta seção obter resultados que relacionem as inclinações das arestas do polígono de Newton de f com respeito a q e ν e relacioná-los com o q- truncamento de ν.

A menos que seja dito o contrário, supomos K um corpo, $f, q \in K[x]$, com q mônico, $\nu : K[x] \longrightarrow \Gamma_\infty$ uma valorização,

$$f = a_0 + a_1 q + \ldots + a_n q^n$$

a q-expansão de f e $\{(a_{i_0}, \nu(a_{i_0})), \ldots, (a_{i_m}, \nu(a_{i_m}))\}$ o conjunto de todos os vértices de $\Delta_q(f)$.

O Lema abaixo nos dá uma equivalência que permite saber quando $-\nu(q)$ é de uma das inclinações das arestas de $\Delta_q(f)$.

Lema 4.2.1. *Temos que* $-\nu(q)$ *é uma inclinação de uma das arestas de* $\Delta_q(f)$ *se, e somente se, para* l*,* $0 \leq l < m$*, e* $k = l + 1$*, vale* $\nu(a_{i_l} q^{i_l}) = \nu(a_{i_k} q^{i_k})$*.*

Demonstração. Note que

$$\begin{aligned} \nu(a_{i_k} q^{i_k}) = \nu(a_{i_l} q^{i_l}) \quad &\Longleftrightarrow \quad \nu(a_{i_k}) - \nu(a_{i_l}) = -(i_k - i_l)\nu(q) \\ &\Longleftrightarrow \quad -\nu(q) = s(I_{i_k}). \end{aligned} \tag{4.3}$$

Visto que a expressão do lado direito da última igualdade em (4.3) corresponde a inclinação do segmento $\overline{(i_l, \nu(a_{i_l}))(k, \nu(a_{i_k}))}$, o resultado segue. □

Lema 4.2.2. *Se $\nu_q(f) < \nu(f)$, então $-\nu(q)$ é a inclinação de uma das arestas de $\Delta_q(f)$.*

Demonstração. Observe que não podemos ter apenas um índice i tal que

$$\nu(a_i q^i) = \min_{0 \le i \le n} \{\nu(a_i q^i)\},$$

pois isso implicaria em

$$\nu(f) = \min_{0 \le i \le n} \{\nu(a_i q^i)\} = \nu_q(f).$$

Portanto, devem existir índices i e j, $0 \le i < j \le n$, tais que

$$\nu(a_i q^i) = \nu(a_j q^j) = \min_{0 \le i \le n} \{\nu(a_i q^i)\}. \tag{4.4}$$

Além disso, podemos tomar i o menor índice e j o maior índice tais que a igualdade em (4.4) ocorre.

Suponha, por redução ao absurdo, que exista $k \in \{0, 1, \ldots, n\}$ tal que $i < k < j$ e o ponto $(k, (\nu(a_k))$ está abaixo da reta que une os pontos $(i, \nu(a_i))$ e $(j, \nu(a_j))$ (veja a Figura 4.2).

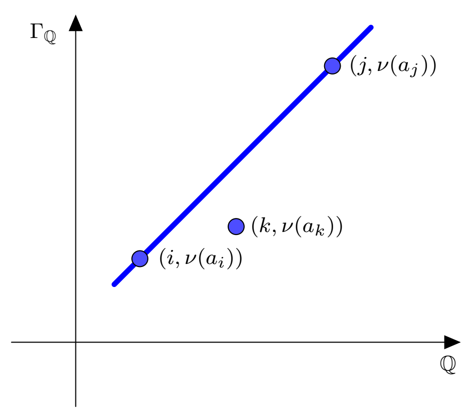


Figura 4.2: O ponto $(k, (\nu(a_k))$ está abaixo da reta que passa por $(i, \nu(a_i))$ e $(j, \nu(a_j))$.

Nessa situação,

$$\nu(a_k) < \frac{\nu(a_j) - \nu(a_i)}{j - i} k + \nu(a_i) - \frac{\nu(a_j) - \nu(a_i)}{j - i} i.$$

Obtemos então que

$$\nu(a_k) < -\nu(q)k + \nu(a_i) + \nu(q)i,$$

e a contradição segue da seguinte desigualdade estrita

$$\nu(a_k q^k) < \nu(a_i q^i) = \min_{0 \le i \le n}\{\nu(a_i q^i)\}.$$

Portanto não existe um índice $k \in \{0, 1, \ldots, n\}$ com a propriedade descrita.

A argumentação anterior nos permite concluir que $(i, \nu(a_i))$ e $(j, \nu(a_j))$ pertencem a alguma aresta de $\Delta_q(f)$. Portanto, existem i_l e i_k, $k = l + 1$, em $\{i_0, \ldots, i_m\}$ tais que a inclinação do segmento $\overline{(i_l, \nu(a_{i_l}))(i_k, \nu(a_{i_k}))}$ é a mesma do segmento $\overline{(i, \nu(a_i))(j, \nu(a_j))}$, ou seja, $-\nu(q)$. □

Corolário 4.2.3. *Sejam $f, q \in K[x]$ com $\nu_q(f) < \nu(f)$, então*

$$\min_{0 \le k \le m}\{\nu(a_{i_k} q^{i_k})\} = \nu_q(f).$$

Demonstração. Usamos aqui a mesma notação da demonstração do Lema 4.2.2. Note que $(i_l, \nu(a_{i_l}))$, $(i, \nu(a_i))$, $(j, \nu(a_j))$ e $(i_k, \nu(a_{i_k}))$ estão na mesma aresta de $\Delta_q(f)$ (veja a Figura 4.3). Ainda, $-\nu(q)$ é a inclinação do segmento $\overline{(i_l, \nu(a_{i_l}))(i_k, \nu(a_{i_k}))}$. Logo, $-\nu(q)$ corresponde ao valor da inclinação do segmento $\overline{(i_l, \nu(a_{i_l}))(j, \nu(a_j))}$. Portanto, temos que

$$\nu(a_{i_l} q^{i_l}) = \nu(a_j q^j) = \min_{0 \le i \le n}\{\nu(a_i q^i)\} = \nu_Q(f).$$

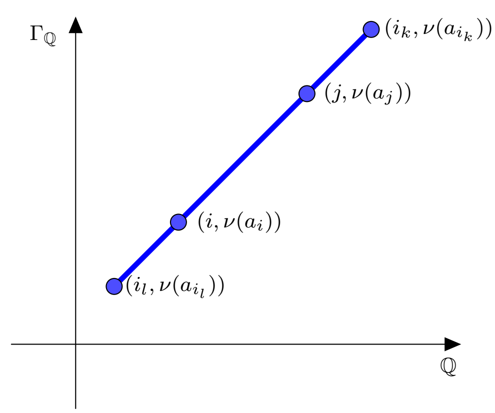


Figura 4.3: Aresta I_{i_k} de $\Delta_q(f)$.

□

Definição 4.2.4. Para cada $q \in K[x]$ consideremos os conjuntos

$$\overline{\Psi}(q) := \{f \in K[x] \mid \nu_q(f) < \nu(f)\}$$

e

$$\Psi(q) := \{f \in \overline{\Psi}(q) \mid f \text{ é mônico e } \deg(f) \leq \deg(g) \text{ para todo polinômio } g \in \overline{\Psi}(q)\}.$$

Lema 4.2.5. *Sejam $q \in K[x]$, com q mônico, e $f \in K[x]$ um polinômio de menor grau tal que $f \in \overline{\Psi}(q)$. Então*

$$s(I_n) = -\nu(q).$$

Demonstração. Mantemos a notação da demonstração do Lema 4.2.2. Suponha que $-\nu(q)$ não é o valor da última inclinação das arestas de $\Delta_q(f)$, então $i_k < n$. Defina agora

$$g := \sum_{i=0}^{i_k} a_i q^i.$$

Nesse caso,

$$\nu_q(g) = \min_{0 \leq i \leq i_k} \{\nu(a_i q^i)\} = \nu(a_{i_k} q^{i_k}) = \min_{0 \leq i \leq n} \{\nu(a_i q^i)\} = \nu_q(f).$$

Portanto, g é um polinômio de grau estritamente menor do que o grau de f com

$$\nu_q(g) < \nu(g). \tag{4.5}$$

De fato, conforme definido em (4.4), temos que j, $j \leq i_k < n$, é o maior índice tal que

$$\nu(a_j q^j) = \min_{0 \leq i \leq n} \{\nu(a_i q^i)\}.$$

Em outras palavras, as parcelas da soma que definem g contemplam todos os valores para os quais o mínimo

$$\min_{0 \leq i \leq n} \{\nu(a_i q^i)\}$$

é atingido. Logo, a igualdade em (4.5) implicaria em

$$\nu(f) = \min\{\nu(g), \nu(a_{i_{k+1}} q^{i_{k+1}} + \ldots + a_n q^n)\} = \nu_q(g) = \nu_q(f).$$

Ou seja, uma contradição com $f \in \overline{\Psi}(q)$. Portanto temos a desigualdade estrita (4.5). □

Lema 4.2.6. *Seja q um polinômio mônico e $f \in \Psi(q)$. Então o polígono de Newton $\Delta_q(f)$ possui apenas uma aresta.*

Demonstração. Como $f \in \Psi(q)$, temos que $\nu_q(f) < \nu(f)$. Logo, sabemos que $-\nu(q)$ corresponde ao valor da última inclinação das arestas de $\Delta_q(f)$. Agora suponha, por absurdo, que exista mais de uma aresta. Nesse caso, para todos i_l e i_k, $k = l+1$, em $\{i_0, \ldots, i_m\}$ temos

$$\frac{\nu(a_{i_k}) - \nu(a_{i_l})}{i_k - i_l} < -\nu(q).$$

Logo,

$$\nu(a_{i_k} q^{i_k}) < \nu(a_{i_l} q^{i_l}).$$

Assim,

$$\nu(a_n q^n) < \ldots < \nu(a_{i_k} q^{i_k}) < \nu(a_{i_l} q^{i_l}) < \ldots < \nu(a_0).$$

Portando, para

$$g := \sum_{i=1}^{n} a_i q^i = f - a_0 = q(a_1 + \ldots + a_n q^{n-1}),$$

temos

$$\nu_q(g) = \min_{1 \le i \le n} \{\nu(a_i q^i)\} = \min_{0 \le i \le n} \{\nu(a_i q^i)\} = \nu_q(f).$$

Ainda,

$$\nu_q(g) < \nu(g),$$

pois a igualdade implicaria em

$$\nu(f) = \min\{\nu(a_0), \nu(g)\} = \min\{\nu(a_0), \nu_q(g)\} = \nu_q(g) = \nu_q(f).$$

Assim, para $\overline{f} := \sum_{i=1}^{n} a_i q^{i-1}$, temos

$$\nu_q(q) + \nu_q(\overline{f}) = \nu_q(g) < \nu(g) = \nu(q) + \nu(\overline{f}),$$

ou seja,

$$\nu_q(\overline{f}) < \nu(\overline{f}).$$

Um absurdo, pois $\deg(\overline{f}) < \deg(f)$ e f é um polinômio de menor grau que satisfaz

$$\nu_q(f) < \nu(f).$$

Portanto, o polígono de Newton $\Delta_q(f)$ possui apenas uma aresta. $\square$

4.3 Polígonos de Newton e extensões de valorizações

O seguinte lema é um resultado conhecido da literatura, apresentado em [19] na página 90. Neste texto optamos por enunciá-lo em termos de valorizações.

Lema 4.3.1. *Seja ν_0 uma valorização em um corpo K. Dado um polinômio $f = \prod_{i=1}^{r}(x-a_i) \in K[x]$ com $a_i \neq 0$, $1 \leq i \leq r$, considere $\Delta_x(f)$ o polígono de Newton de f com respeito a ν_0 e a x. Então, o conjunto de todas das inclinações das arestas de $\Delta_x(f)$ é $\{-\nu_0(a_i) \,|\, 1 \leq i \leq r\}$.*

Observação 4.3.2. Na demonstração do Lema 4.3.1 em [19], também fica mostrado que o comprimento da projeção no eixo $\mathbb{Q}$ de uma aresta fixada de $\Delta_x(f)$ com inclinação α é igual a quantidade de raízes a_i de f tais que $\nu_0(a_i) = -\alpha$.

Corolário 4.3.3. *Sejam ν_0 uma valorização em um corpo K e $f = \prod_{i=1}^{r}(x-a_i), g = \prod_{i=1}^{r}(x-b_i) \in K[x]$ com $a_i, b_i \neq 0$, $1 \leq i \leq r$. Suponha que $\Delta_x(f) = \Delta_x(g)$. Então, a menos de uma reordenação, temos $\nu_0(a_i) = \nu_0(b_i)$ para todo i, $1 \leq i \leq r$.*

Proposição 4.3.4. *Sejam K um corpo, ν_0 uma valorização em K e $f \in K[x]$ um polinômio irredutível. Para cada aresta de $\Delta_x(f)$ com inclinação α existe pelo menos uma extensão da valorização ν_0 para uma valorização ν em $K[x]/(f)$ com $\nu(x) = -\alpha$.*

Demonstração. Fixe uma extensão μ_0 de ν_0 para $\overline{K}$. Tome uma raiz $a \in \overline{K}$ de f com $\mu_0(a) = -\alpha$ e defina a aplicação

$$\nu(g) := \mu_0(g(a)), \text{ para toda } g \in K[x]. \tag{4.6}$$

Do fato de μ_0 ser uma valorização, concluímos que ν também é uma valorização que estende ν_0 com $\nu(x) = \mu_0(a) = -\alpha$. Ainda,

$$\nu(f) = \mu_0(f(a)) = \mu_0(0) = \infty,$$

e, portanto, $\operatorname{supp}(\nu) = (f)$, pois f é irredutível. $\square$

Note que não garantimos que as valorizações, como introduzidas em (4.6), em $K[x]/(f)$ são distintas. Por exemplo, é suficiente que uma raiz $a \in \overline{K}$ de f tenha grau de multiplicidade maior do que 1 para que duas extensões coincidam.

Corolário 4.3.5. *Sejam K um corpo, ν_0 uma valorização em K e $f \in K[x]$ um polinômio irredutível. Se existe somente uma valorização ν em $K[x]/(f)$ estendendo ν_0, então $\Delta_x(f)$ tem somente uma aresta. Mais ainda, a inclinação dessa única aresta é igual à $-\nu(x)$.*

4.4 Aplicações em extensões de Artin-Schreier

Sejam K um corpo e ν_0 uma valorização em K. Assumimos nesta seção que $\mathrm{char}(K) = p > 0$, ν_0 é uma valorização de posto um e fixamos $F = x^p - x - a \in K[x]$ um polinômio de Artin-Schreier. Estudamos aqui as possíveis extensões de ν_0 a $K(\eta) = K[x]/(F)$.

Note que para cada $b \in K$, se escrevermos $y = x - b$, temos então

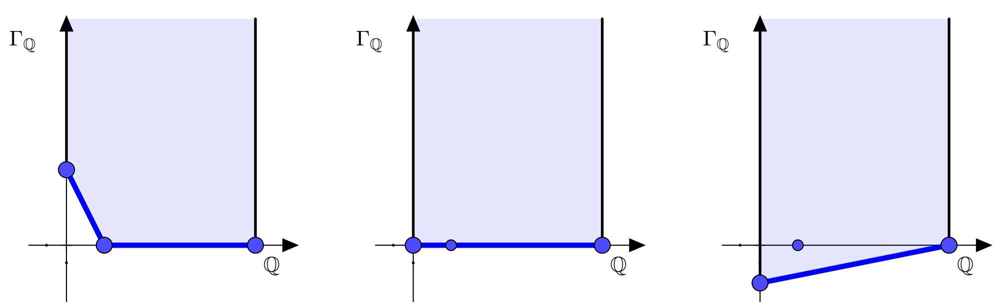
$$F(x) = x^p - x - a = y^p - y + (b^p - b - a) = y^p - y + F(b) =: G(y).$$

e

$$K(\eta) = K[x]/(F(x)) = K[y]/(G(y)).$$

Queremos estudar as extensões de ν_0 a $K(\eta)$ em termos de polígonos de Newton. Portanto, podemos analisar os polígonos de Newton dos polinômios $G(y) = y^p - y + F(b)$ para $b \in K$.

Na Figura 4.4 apresentamos os possíveis polígonos de Newton de G com respeito a ν_0 e $y = x - b$.



(a) $\nu_0(F(b)) > 0$ (b) $\nu_0(F(b)) = 0$ (c) $\nu_0(F(b)) < 0$

Figura 4.4: Polígonos de Newton $\Delta_{x-b}(G)$ para $b \in K$.

Se $\nu_1, \ldots, \nu_g$ são todas as extensões de ν_0 a $K(\eta)$, então a desigualdade fundamental

(Teorema 3.3.4 de [12]) nos dá

$$p = [K(\eta) : K] \geq \sum_{i=1}^{g} e_i f_i,$$

onde $e_i := (\Gamma_{\nu_i} : \Gamma_\nu)$ é o **índice de ramificação** e $f_i := [K(\eta)\nu_i : K\nu]$ o **índice de inércia** da extensão $(K(\eta)|K, \nu_i)$. Em particular, o número máximo de extensões de ν_0 a $K(\eta)$ é p.

Se houver uma única extensão ν de ν_0 para $K(\eta)$, então definimos o **defeito** como

$$d = \frac{[K(\eta) : K]}{ef}, \tag{4.7}$$

onde e e f são os índices de ramificação e inércia de $(K(\eta)|K, \nu)$, respectivamente. Então

$$p = [K(\eta) : K] = def.$$

Em particular, um desses números é p e os outros são 1.

Teorema 4.4.1. *Na notação descrita acima, temos o seguinte.*

(i) *Existe $b \in K$ tal que $\nu_0(F(b)) > 0$ se, e somente se, existem p extensões distintas de ν_0 a $K(\eta)$.*

(ii) *Suponha que $\nu_0(F(b)) \leq 0$ para todo $b \in K$. Seja ν a única extensão de ν_0 para $K[x]/(F)$ e seja*

$$S := \left\{ \frac{\nu_0(F(b))}{p} \mid b \in K \right\} \subseteq \frac{1}{p}\Gamma_0.$$

Então, para o índice de ramificação e e de inércia f e o defeito d de $(K[x]/(F)|K, \nu)$, vale o seguinte.

- *Se $S \not\subseteq \Gamma_0$, então $e = p$.*
- *Se $S \subseteq \Gamma_0$ e S tem um máximo, então $f = p$.*
- *Se $S \subseteq \Gamma_0$ e S não tem um máximo, então $d = p$.*

Demonstração. Suponha que exista $b \in K$ tal que $\nu_0(F(b)) > 0$. Isso significa que, para cada i, $0 \leq i \leq p-1$, o polígono de Newton $\Delta_{x-b+i}(F)$ tem um lado com inclinação $\alpha < 0$. Nesse caso, temos

$$\alpha = \frac{0 - \nu_0(F(b))}{p - 0} = \frac{\nu_0(F(b))}{p}.$$

Pela Proposição 4.3.4 existem valorizações ν_i tais que $\nu_i(x-b+i) = -\alpha > 0$. Então, para $i \neq j$, temos

$$\nu_i(x-b+j) = \min\{\nu_i(x-b+i), \nu_i(j-i)\} = 0 \neq -\alpha = \nu_j(x-b+j).$$

Portanto, essas valorizações são distintas. O recíproca seguirá de **(ii)** e (4.7).

Para provar **(ii)** assuma que $\nu_0(F(b)) \leq 0$ para todo $b \in K$. Portanto, $\Delta_{x-b}(F)$ tem apenas um lado, este de inclinação $-\frac{\nu_0(F(b))}{p}$. Para qualquer extensão ν de ν_0 a $K(\eta)$, pelo Lema 4.3.1, temos $\nu(x-b) = \frac{\nu_0(F(b))}{p}$. Em particular, se $\frac{\nu(F(b))}{p} \notin \Gamma_0$ para algum $b \in K$, então $e = p$.

Suponha que $S \subseteq \Gamma_0$. Afirmamos que S tem um máximo se, e somente se, $f \neq 1$. Se $\nu_0(F(b)) = 0$, então

$$x^p - x - F(b)\nu \in K\nu_0[x]$$

é irredutível (porque é um polinômio Artin-Schreier sem raiz em $K\nu_0$). Portanto, $f = p$. Suponha que $\nu_0(F(b)) < 0$. Fixe $c \in K$ tal que $\nu_0(c) = \dfrac{\nu_0(F(b))}{p}$ e defina $\eta' = \eta + b$. Então

$$\left(\frac{\eta'}{c}\right)^p - \frac{\eta'}{c^p} + \frac{F(b)}{c^p} = \frac{\eta'^p - \eta' + F(b)}{c^p} = \frac{F(\eta)}{c^p} = 0.$$

Logo,

$$\left(\frac{\eta'}{c}\nu\right)^p = \frac{F(b)}{c^p}\nu_0.$$

Visto que $K(\eta)\nu = K\nu_0\left(\dfrac{\eta'}{c}\nu\right)$, temos $f = 1$ se, e somente se, $\dfrac{\eta'}{c}\nu = c'\nu_0$ para algum $c' \in K$. Isso é equivalente a $\nu(\eta' - cc') > \nu_0(c)$. Assuma que $f = 1$ e tome $b \in K$. Então existe $c' \in K$ tal que

$$\frac{\nu_0(F(cc'-b))}{p} = \nu\left(\eta' - cc'\right) > \nu_0(c) = \frac{\nu_0(F(b))}{p}.$$

Portanto, S não tem um máximo. Por outro lado, suponha que $f \neq 1$. Então, para cada $c' \in K$, devemos ter

$$\frac{\nu_0(F(cc'-b))}{p} \leq \frac{\nu_0(F(b))}{p}.$$

Em particular, para cada $r \in K$ se definirmos $c' = \dfrac{r-b}{c}$ temos

$$\frac{\nu_0(F(r))}{p} = \frac{\nu_0(F(cc'-b))}{p} \leq \frac{\nu_0(F(b))}{p}.$$

Consequentemente, S tem um máximo.

Suponha que S não tenha um máximo (em particular, $f = 1$) e tome outra valorização μ estendendo ν_0. Então, para cada $b \in K$ e $g \in K[x]$ escrevemos $g = a_r(x-b)^r + \ldots + a_0$ $(x-b)$-expansão de g. Então

$$\nu_{x-b}(g) = \min_{0 \leq i \leq r}\{\nu_0(a_i) + i\nu(x-b)\} = \min_{0 \leq i \leq r}\left\{\nu_0(a_i) + i\frac{\nu_0(F(b))}{p}\right\} = \mu_{x-b}(g).$$

Além disso, para cada polinômio $g(x)$ de grau menor que p temos, pelo Teorema 1.1 de [24] (onde usamos que ν_0 tem posto um), que existe $b \in K$ tal que

$$\nu(g(\eta)) = \nu(g(x)) = \nu_{x-b}(g) = \mu_{x-b}(g) = \mu(g(x)) = \mu(g(\eta)). \tag{4.8}$$

Portanto, ν é a única valorização em $K(\eta)$ estendendo ν_0. Ainda, segue de (4.8) que $e = 1$. Consequentemente, $d = p$. $\square$

Observação 4.4.2. Fixe um polinômio $F = x^p - x - a \in K[x]$ com $\nu(a) = 0$. Então $\nu(F(b)) > 0$ para algum $b \in K$ se, e somente se, $b\nu_0$ é uma raiz de $\overline{F} = x^p - x - a\nu_0$. Portanto, $\overline{F}$ tem uma raiz em $K\nu_0$ se, e somente se, existem p valorizações distintas estendendo ν_0 para $K(\eta)$.

Referências

[1] S. Abhyankar, *Ramification Theoretic Methods in Algebraic Geometry*, Princeton University Press, 1959.

[2] S. Abhyankar, *Resolution of Singularities of Embedded Algebraic Surfaces*, Academic Press, 1966.

[3] M. S. Barnabé and J. Novacoski, *Generating sequences and key polynomial*, arXiv:2007.12293, 2021.

[4] M. S. Barnabé and J. Novacoski, *Valuations on K[x] approaching a fixed irreducible polynomial.*, J. Algebra, 592, 110-117, 2021.

[5] M. S. Barnabé, J. Novacoski and M. Spivakovsky *On the structure of the graded algebra associated to a valuation*, J. Algebra, 560, 667-679, 2020.

[6] V. Cossart and O. Piltant, *Resolution of Singularities of Threefolds in Positive Characteristic I. Reduction to Local Uniformization on Artin-Schreier and purely inseparable coverings*, J. Algebra, 320, 1051-1082, 2008.

[7] V. Cossart and O. Piltant, *Resolution of Singularities of Threefolds in Positive Characteristic II*, J. Algebra, 321, 1836-1976, 2009.

[8] S. D. Cutkosky, *A skeleton key to Abhyankar's proof of Embedded Resolution of Characteristic p Surfaces*, Asian J. Math. 15, 369-416, 2011.

[9] S. D. Cutkosky, H. Mourtada and B. Teissier, *On the construction of valuations and generating sequences on hypersurface singularities*, arXiv:1904.10702, 2019.

[10] J. Decaup, M. Spivakovsky and W. Mahboub, *Abstract key polynomials and comparison theorems with the key polynomials of Mac Lane-Vaquié*, Illinois J. Math., 62, 253-270, 2018.

[11] O. Endler, *Valuation Theory*, Springer, 1972.

[12] A. J. Engler and A. Prestel, *Valued Fields*, Springer, 2005.

[13] C. Favre and M. Jonsson, *The Valuative Tree*, Springer, 2004.

[14] L. Ghezzi and O. Kashcheyeva, *Toroidalization of generating sequences in dimension two function fields*, J. Algebra, 209, 631-649, 2079.

[15] David M. Goldschmidt, *Algebraic functions and projective curves*, Springer-Verlag, 2003.

[16] F. J. Herrera Govantes, M. A. Olalla Acosta and M. Spivakovsky, *Valuations in algebraic field extensions*, J. Algebra, 312, 1033-1074, 2007.

[17] F. J. Herrera Govantes, W. Mahboub, M. A. Olalla Acosta and M. Spivakovsky, *Key polynomials for simple extensions of valued fields*, hal-01887698, 2018.

[18] H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero*, Ann. of Math. 79, 109-203, 1964.

[19] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer, 1984.

[20] F.-V. Kuhlmann, *A classification of Artin-Schreier defect extensions and characterizations of defectless fields*, Illinois J. Math., 54, 397-448, 2010.

[21] G. Leloup, *Key polynomials, separate and immediate valuations, and simple extensions of valued fields*, arXiv:1809.07092, 2019.

[22] S. Mac Lane, *A construction for prime ideals as absolute values of an algebraic field*, Duke Math. Journ., 2, 492-510, 1936.

[23] S. Mac Lane, *A construction for absolute values in polynomial rings*, Transactions of the AMS, 40, 363-395, 1936.

[24] M. Moraes and J. Novacoski, *Limit key polynomials as p-polynomials*, J. Algebra, 579, 152-173, 2021.

[25] H. Mourtada, *Jet schemes and generating sequences of divisorial valuations in dimension two*, Michigan Math. J., 66, 155-174, 2017.

[26] J. Novacoski, *Key polynomials and minimal pairs*, J. Algebra, 523, 1-14, 2019.

[27] J. Novacoski, *The structure of spaces of valuations and the local uniformization problem*, PhD thesis, College of University of Saskatchewan, 2013.

[28] J. Novacoski and M. Spivakovsky, *Reduction of local uniformization to the rank one case*, Valuation Theory in Interaction, 149, 404-431, 2014.

[29] J. Novacoski and M. Spivakovsky, *On the local uniformization problem*, Banach Center Publications, 108, 231-238, 2016.

[30] J. Novacoski and M. Spivakovsky, *Key polynomials and pseudo-convergent sequences*, J. Algebra, 495, 199-219, 2018.

[31] J. C. San Saturnino, *Théorème de Kaplansky effectif et uniformisation locale des schémas quasi-excellents*, PhD thesis, Institut de Mathé-matiques de Toulouse, 2013.

[32] J. C. San Saturnino, *Defect of an extension, key polynomials and local uniformization*, J. Algebra, 481, 1-14, 2017.

[33] M. Spivakovsky, *Sandwiched Singularities and Desingularization of Surfaces by Normalized Nash Transformations*, Ann. of Math., 131, 411-491, 1990.

[34] M. Spivakovsky, *Valuations in function fields of surfaces*, Amer. J. Math, 112, 107-156, 1990.

[35] B. Teissier, *Overweight deformations of affine toric varieties and local uniformization*, Valuation Theory in Interaction, EMS Series of Congress Reports, 474-565, 2014.

[36] B. Teissier, *Valuations, deformations, and toric geometry.* Valuation theory and its applications, 33, 361-459, 2003.

[37] M. Vaquié, *Famille admissible de valuations et defaut d'une extension*, J. Algebra, 311, 859-876, 2007.

[38] M. Vaquié, *Extension d'une valuation*, Trans. Amer. Math. Soc., 359, 3439-3481, 2007.

[39] P. A. Vinh, *Generating sequences of valuations and applications*, PhD thesis, University of Missouri, 2014.

[40] O. Zariski, *The Reduction of the Singularities of an Algebraic Surface*, Ann. of Math. 40, 639-689, 1939.

[41] O. Zariski, *Reduction of the Singularities of Algebraic Three Dimensional Varieties*, Ann. of Math., 45, 472-542, 1944.

[42] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. II, Springer, 1960.