UNIVERSIDADE FEDERAL FLUMINENSE

Domínios de Dedekind como interseção de anéis de valorização

Cristiane de Mello

Rio de Janeiro, Agosto de 2006

Cristiane de Mello

DISSERTAÇÃO DE MESTRADO

Orientadora: Maria Lúcia Villela

Rio de Janeiro, Agosto de 2006

Agradecimentos

Sumário

Introdução

Domínios de Dedekind são domínios noetherianos, integralmente fechados, tais que todo ideal primo não-nulo é maximal. O objetivo deste trabalho é apresentar, no Capítulo 5, domínios de Dedekind como interseção de um conjunto de anéis de valorizaçòes discretas de seu corpo de frações, que tem a propriedade da aproximação forte, mostrar a equivalência das duas definições e que a propriedade de ser domínio de Dedekind se preserva em extensões separáveis de corpos.

O trabalho foi organizado levando em conta os seguintes fatos:

- Anéis de valorização discreta são anéis de valorização de posto 1, cujo grupo de valores é isomorfo a $\mathbb{Z}$.

- Os anéis de valorização de posto 1 estão em bijeção com as classes de equivalência de valores absolutos não-arquimedianos de seu corpo de frações K e dão a K uma estrutura de espaço métrico.

- Para o melhor entendimento do comportamento de uma extensão a um corpo L de uma valorização de K de posto 1 a análise dos diversos completamentos é muito útil.

- A extensão de uma valorização é tratada, mais facilmente, considerando-se o conceito mais geral de valorização de Krull.

No Capítulo 1 são apresentadas as propriedades dos valores absolutos arquimedianos e não-arquimedianos, o completamento e a caracterização dos valores absolutos de $\mathbb{Q}$.

No Capítulo 2 é introduzido o conceito de valorização de um corpo K, conforme será concluido no capítulo 4, uma valorização de Krull de posto 1.

No Capítulo 3 é tratado o completamento de Q com respeito ao valor absoluto p-ádico, ou equivalentemente, correspondente à valorização p-ádica. Além disso, é descrito o completamento de um corpo K com respeito a uma valorização discreta, essencial para tratar uma extensão a um corpo L de uma valorização discreta de K.

No Capítulo 4 são tratados os anéis de valorização e as valorizações de Krull , obtendo-se a equivalência entre as valorizações de Krull de posto 1 e as valorizações do Capítulo 2.

No Capítulo 6-Apêndice estão os resultados elementares de grupo abeliano ordenado, necessários para a compreensão das valorizações de Krull e a equivalência entre as valorizações de Krull de posto 1 e as valorizações do Capítulo 2.

A construção deste material é baseada, essencialmente em [Cohn]; o Capítulo 2, em [Endler]; o Capítulo 3, seção 1, em [Koblitz] e o Capítulo 4, seção 1, em [Endler]. No Capítulo 1 incorporamos algumas idéias de [Endler] e [Lang].

Os resultados relevantes de Álgebra Comutativa podem ser encontrados em [Atiyah-MacDonald].

Capítulo 1

Valores absolutos

Neste primeiro capítulo, estudaremos os valores absolutos em um corpo K e suas principais propriedades, veremos que os mesmos definem uma métrica em K tornando-o um espaço topológico e, então, finalmente, discutiremos o completamento de K.

1.1 Valor absoluto

Nesta primeira seção, apresentaremos basicamente as principais propriedades de um valor absoluto em um domínio D, o caracterizaremos em corpos finitos e o estenderemos ao corpo de frações de D.

Seja D um domínio.

Definição 1.1 *Um valor absoluto $|\ |$ em D é uma função $|\ | : D \to \mathbb{R}$ tal que:*

$(A.1)$ $|x| \geqslant 0$, $\forall\ x \in D$, *e* $|x|=0$ *se, e somente se,* $x=0$;

$(A.2)$ $|x+y| \leq |x| + |y|$, $\forall\ x, y \in D$ *(Desigualdade triangular);*

$(A.3)$ $|xy| = |x||y|$, $\forall\ x, y \in D$.

Proposição 1.2 *Qualquer valor absoluto $|\ |$ em D tem as seguintes propriedades:*

(i) $|\ |$ *não é identicamente nulo.*

(ii) $|1| = 1 = |-1|$.

(iii) $|-x| = |x|, \forall\ x \in D$.

(iv) $|x-y| \leq |x| + |y|$, $\forall\ x, y \in D$.

(v) $|\ |x| - |y|\ | \leq |x+y|, \forall\ x, y \in D$.

(vi) $|x_1 + \cdots + x_n| \leq |x_1| + \cdots + |x_n|$, $\forall\ x_1, \ldots, x_n \in D$.

Demonstração. (i): Segue do fato de que $1 \neq 0$ em um domínio e de $(A.1)$.

(ii): A primeira igualdade segue de $1 = 1\,.\,1$, de $(A.3)$ e de $|1| \neq 0$, visto que $1 \neq 0$ em um domínio; a segunda igualdade segue de $(A.3)$ e da primeira igualdade.

(iii): Segue do fato de que $-x = (-1)\,x$, para todo $x \in D$, de $(A.3)$ e de (ii).

(iv): Segue de $(A.2)$ e de (iii).

(v): Como $|x| = |(x+y)-y|$ e $|y| = |(x+y)-x|$, para quaisquer $x, y \in D$, segue de (iv) que $|x| \leq |x+y| + |y|$ e $|y| \leq |x+y| + |x|$. Daí,

$$-|x+y| \leq |x| - |y| \leq |x+y|.$$

Portanto, $| \, |x| - |y| \, | \leq |x+y|$.

(vi): Segue de ($A.2$), por indução sobre n. ∎

Observação 1.3 *Seja $x \in D$, $x \neq 0$. Se $x^{-1} \in D$, então $|x^{-1}| = |x|^{-1}$. Em particular, se D é um corpo, então $|x^{-1}| = |x|^{-1}$, para todo $x \in D$, $x \neq 0$.*

Com efeito, se $x \in D$ é invertível em D, então $1 = xx^{-1}$. Daí,

$$1 = |1| = |xx^{-1}| = |x||x^{-1}| \Rightarrow |x^{-1}| = |x|^{-1}.$$

Exemplo 1.4 *A função $| \, | : D \to \mathbb{R}$ dada por*

$$|x| = \begin{cases} 1, & se \quad x \neq 0 \\ 0, & se \quad x = 0 \end{cases}$$

é o valor absoluto em D chamado valor absoluto trivial.

Exemplo 1.5 *Exemplos conhecidos de valores absolutos em corpos são os valores absolutos usuais em $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$.*

Exemplo 1.6 *Fixemos um número natural primo p. Então, dado $c \in \mathbb{Q}$, $c \neq 0$, podemos escrever*

$$c = p^{\gamma} \frac{m}{n}, \text{ onde } \gamma, m \in \mathbb{Z}, \ n \in \mathbb{N}, \ n \neq 0, \ e \ p \nmid mn.$$

A função $| \, |_p : \mathbb{Q} \to \mathbb{R}$ definida por

$$|c|_p = \begin{cases} p^{-\gamma}, & se \quad c \neq 0 \\ 0 \ , & se \quad c = 0 \end{cases}$$

é o valor absoluto p-ádico em $\mathbb{Q}$, que foi introduzido por Hensel em 1904.

Observação 1.7 *O valor absoluto p-ádico em $\mathbb{Q}$, pelo teorema fundamental da aritmética, é claramente determinado por $|p|_p = p^{-1}$ e $|q|_p = 1$, para qualquer número natural primo $q \neq p$.*

Exemplo 1.8 *Seja K um corpo e seja $p(x) \in K[x]$ um polinômio mônico irredutível sobre K. Então, dada $\phi(x) \in K(x)$, $\phi(x) \neq 0$, podemos escrever*

$$\phi(x) = p(x)^{\gamma} \frac{f(x)}{g(x)}, \text{ onde } \gamma \in \mathbb{Z}, \ f(x), g(x) \in K[x], \ g(x) \neq 0, \ e \ p(x) \nmid f(x)g(x).$$

A função $| \, |_{p(x)} : K(x) \to \mathbb{R}$ definida por

$$|\phi(x)|_{p(x)} = \begin{cases} 2^{-\gamma}, & se \quad \phi(x) \neq 0 \\ 0 \ , & se \quad \phi(x) = 0 \end{cases}$$

é o valor absoluto em $K(x)$ chamado valor absoluto $p(x)$-ádico. Em particular, se K é algebricamente fechado, então $p(x) = x - a$, onde $a \in K$.

Exemplo 1.9 *Seja K um corpo. A função $| \, |_{\infty} : K(x) \to \mathbb{R}$ definida por*

$$\left| \frac{f(x)}{g(x)} \right|_{\infty} = \begin{cases} 2^{\,grau\, f(x) - grau\, g(x)}, & se \quad \dfrac{f(x)}{g(x)} \neq 0 \\ \\ 0 \qquad\quad , & se \quad \dfrac{f(x)}{g(x)} = 0 \end{cases}$$

é um valor absoluto em $K(x)$.

Os exemplos 1.6, 1.8, 1.9 e 1.4 satisfazem uma propriedade mais forte do que a propriedade $(A.2)$, a saber:

$(A.2')$ $|x+y| \leq \max\{|x|, |y|\}$, $\forall\, x, y \in D$ (Desigualdade ultramétrica).

Definição 1.10 *Um valor absoluto $|\ |$ em um domínio D é chamado valor absoluto não-arquimediano se, e somente se, $|\ |$ satisfaz a propriedade $(A.2')$; caso contrário, $|\ |$ é chamado valor absoluto arquimediano.*

Exemplo 1.11 *Os exemplos 1.6, 1.8, 1.9 e 1.4 são exemplos de valores absolutos não-arquimedianos.*

Exemplo 1.12 *Os valores absolutos usuais em $\mathbb{Q}, \mathbb{R}$ ou $\mathbb{C}$ são valores absolutos arquimedianos.*

Proposição 1.13 *Seja $|\ |$ um valor absoluto não-arquimediano em um domínio D. Então, para quaisquer $x, y \in D$, temos que*

$$|x| \neq |y| \Rightarrow |x-y| = \max\{|x|, |y|\}.$$

Demonstração. Sejam $x, y \in D$ tais que $|x| \neq |y|$, digamos $|x| < |y|$. De $(A.2')$ segue que $|x-y| \leq \max\{|x|, |y|\}$. Suponhamos, por contradição, que $|x-y| < \max\{|x|, |y|\} = |y|$. Então, $|y| > \max\{|x|, |x-y|\}$. Tomando $y = x-(x-y)$ obtemos uma contradição com $(A.2')$. Portanto, $|x-y| = \max\{|x|, |y|\}$. ∎

Veremos, agora, a caracterização dos valores absolutos em corpos finitos e, em seguida, a caracterização dos valores absolutos não-arquimedianos em um domínio.

Proposição 1.14 *Se K é um corpo finito, então K não tem valor absoluto não-trivial.*

Demonstração. Seja K um corpo finito, digamos com q elementos, e seja $|\ |$ um valor absoluto em K. Então, $x^{q-1} = 1$, para todo $x \in K$, $x \neq 0$. Daí, $1 = |1| = |x^{q-1}| = |x|^{q-1}$. Logo, $|x| = 1$, para todo $x \in K$, $x \neq 0$. Portanto, $|\ |$ é o valor absoluto trivial em K. ∎

Proposição 1.15 *Para qualquer valor absoluto $|\ |$ em um domínio, as seguintes afirmações são equivalentes:*

(i) $|\ |$ *é não-arquimediano.*

(ii) $|n1| \leq 1$, $\forall\, n \in \mathbb{N}$.

(iii) $|n1| \leq 1$, *para algum* $n \in \mathbb{N}$, $n > 1$.

(iv) O conjunto $\{|n1|; n \in \mathbb{N}\}$ *é limitado.*

Demonstração. $(i) \Rightarrow (ii)$: Suponhamos que $|\ |$ é não-arquimediano. É claro que $|0| = 0 \leq 1$. Seja, então, $n > 0$. Temos que

$$|n1| = |\underbrace{1 + \cdots + 1}_{n \text{ parcelas}}| \leq \max\{\underbrace{|1|, \ldots, |1|}_{n \text{ parcelas}}\} = |1| = 1.$$

$(ii) \Rightarrow (iii)$: É imediato.

$(iii) \Rightarrow (iv)$: Seja $m \in \mathbb{N}$, $m > 1$, tal que $|m1| \leq 1$. Dado $n \in \mathbb{N}$, escrevemos n na base m da seguinte maneira:

$$n = a_0 + a_1 m + a_2 m^2 + \cdots + a_r m^r, \text{ onde } 0 \leq a_i < m,\ i = 0, \ldots, r, \text{ e } a_r \neq 0.$$

Segue que $m^r \leq n$, daí $r \leq \log n$, onde o logaritmo é tomado na base m. Como

$$|a_i 1| = |\underbrace{1+\cdots+1}_{a_i \text{ parcelas}}| \leq \underbrace{|1|+\cdots+|1|}_{a_i \text{ parcelas}} = \underbrace{1+\cdots+1}_{a_i \text{ parcelas}} = a_i < m, \text{ para todo } i = 0, \ldots, r,$$

temos que

$$\begin{aligned} |n1| &\leq |a_0 1| + |a_1 1||m1| + |a_2 1||m1|^2 + \cdots + |a_r 1||m1|^r \\ &\leq a_0 + a_1|m1| + a_2|m1|^2 + \cdots + a_r|m1|^r \\ &< m + m|m1| + m|m1|^2 + \cdots + m|m1|^r \\ &\leq m(1+r) \\ &\leq m(1+\log n) \end{aligned}$$

Substituindo, então, n por n^s, obtemos $|n1|^s \leq m(1+s\log n)$. Tomando a raiz s-ésima e fazendo $s \to \infty$, obtemos

$$|n1| \leq \lim_{s\to\infty} (m(1+s\log n))^{\frac{1}{s}} = 1.$$

Portanto, o conjunto $\{|n1|; n \in \mathbb{N}\}$ é limitado.

$(iv) \Rightarrow (i)$: Suponhamos que existe uma constante M tal que $|n1| \leq M$, para todo $n \in \mathbb{N}$. Então,

$$|x+y|^n = |(x+y)^n| = \left|\sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}\right| \leq \sum_{i=0}^{n} \left|\binom{n}{i}\right| |x|^i |y|^{n-i} \leq M \sum_{i=0}^{n} |x|^i |y|^{n-i}.$$

Se $|x| \leq |y|$, então $|x|^i \leq |y|^i$, para todo $i = 0, \ldots, n$. Daí,

$$|x|^i |y|^{n-i} \leq |y|^n, \text{ para todo } i = 0, \ldots, n.$$

Assim,

$$|x+y|^n \leq M(n+1)\max\{|x|^n, |y|^n\}.$$

Tomando, então, a raiz n-ésima e fazendo $n \to \infty$, obtemos

$$\begin{aligned} |x+y| &\leq \lim_{n\to\infty} \left(M(n+1)\max\{|x|^n, |y|^n\}\right)^{\frac{1}{n}} \\ &= \lim_{n\to\infty} (M(n+1))^{\frac{1}{n}} \ \max\{|x|, |y|\} \\ &= \max\{|x|, |y|\}. \end{aligned}$$

Portanto, o valor absoluto $|\ |$ é não-arquimediano. ∎

Corolário 1.16 *Seja $|\ |$ um valor absoluto arquimediano em um corpo K. Então, K tem característica zero.*

Demonstração. Suponhamos que o corpo K tem característica $p \neq 0$. Então, o conjunto $\{|n1|; n \in \mathbb{N}\}$ é finito e, portanto, limitado. Segue do teorema anterior que $|\ |$ é um valor absoluto não-arquimediano. ∎

Mostraremos, agora, que todo valor absoluto em um domínio D pode ser estendido de maneira única a um valor absoluto no corpo de frações de D.

Proposição 1.17 *Seja $|\ |$ um valor absoluto em D. Então, $|\ |$ pode ser estendido de maneira única a um valor absoluto no corpo de frações de D.*

Demonstração. Seja K o corpo de frações de D. Dado $u \in K$, temos que $u = \dfrac{a}{b}$, onde $a, b \in D$, $b \neq 0$. Assim, se $|\ |$ pode ser estendido a K, então, como $a = u\,b$, temos $|a| = |u||b|$. Daí,

$$|u| = \left|\frac{a}{b}\right| = \frac{|a|}{|b|}. \quad (*)$$

Segue que existe, no máximo, uma extensão.

Primeiramente, mostremos que a extensão do valor absoluto $|\ |$ dada em $(*)$ está bem definida: sejam $a_1, b_1 \in D, b_1 \neq 0$, tais que $u = \dfrac{a_1}{b_1}$; então,

$$\frac{a}{b} = \frac{a_1}{b_1} \Rightarrow a\,b_1 = b\,a_1 \Rightarrow |a||b_1| = |b||a_1| \Rightarrow \frac{|a|}{|b|} = \frac{|a_1|}{|b_1|} \Rightarrow \left|\frac{a}{b}\right| = \left|\frac{a_1}{b_1}\right|.$$

Mostremos, agora, que a extensão do valor absoluto $|\ |$ dada em $(*)$ é, de fato, um valor absoluto: dado $u \in K$, temos que $u = \dfrac{a}{b}$, onde $a, b \in D$, $b \neq 0$; daí,

$$|u| = \left|\frac{a}{b}\right| = \frac{|a|}{|b|} \geq 0 \quad \text{e} \quad |u| = \left|\frac{a}{b}\right| = \frac{|a|}{|b|} = 0 \Leftrightarrow |a| = 0 \Leftrightarrow a = 0 \Leftrightarrow u = 0.$$

Logo, $|u| \geq 0$, para todo $u \in K$, e $|u| = 0$ se, e somente se, $u = 0$.

Dados $u_1, u_2 \in K$, com $u_1 = \dfrac{a_1}{b_1}$ e $u_2 = \dfrac{a_2}{b_2}$, onde $a_1, a_2, b_1, b_2 \in D$, $b_1 \neq 0$ e $b_2 \neq 0$, temos que

$$\begin{aligned} |u_1 + u_2| &= \left|\frac{a_1}{b_1} + \frac{a_2}{b_2}\right| = \left|\frac{a_1b_2 + a_2b_1}{b_1b_2}\right| = \frac{|a_1b_2 + a_2b_1|}{|b_1b_2|} \leq \frac{|a_1b_2| + |a_2b_1|}{|b_1b_2|} \\ &= \frac{|a_1||b_2| + |a_2||b_1|}{|b_1||b_2|} = \frac{|a_1|}{|b_1|} + \frac{|a_2|}{|b_2|} = \left|\frac{a_1}{b_1}\right| + \left|\frac{a_2}{b_2}\right| = |u_1| + |u_2| \end{aligned}$$

e

$$\begin{aligned} |u_1u_2| &= \left|\frac{a_1}{b_1}\,\frac{a_2}{b_2}\right| = \left|\frac{a_1a_2}{b_1b_2}\right| = \frac{|a_1a_2|}{|b_1b_2|} = \frac{|a_1||a_2|}{|b_1||b_2|} \\ &= \frac{|a_1|}{|b_1|}\,\frac{|a_2|}{|b_2|} = \left|\frac{a_1}{b_1}\right|\left|\frac{a_2}{b_2}\right| = |u_1||u_2|. \end{aligned}$$

Daí, $|u_1 + u_2| \leq |u_1| + |u_2|$ e $|u_1u_2| = |u_1||u_2|$, para quaisquer $u_1, u_2 \in K$.

Portanto, a extensão do valor absoluto $|\ |$ dada em $(*)$ é um valor absoluto em K. ∎

Para concluirmos nossa primeira seção, apresentaremos a definição de um valor absoluto em uma extensão de corpos, seguida de um exemplo e de uma observação.

Definição 1.18 *Seja $|\ |$ um valor absoluto no corpo K e seja k um subcorpo de K. Dizemos que $|\ |$ é um valor absoluto da extensão de corpos $K|k$ se, e somente se, a restrição de $|\ |$ a k é trivial.*

Denotaremos por $|\ |_{|k}$ a restrição de $|\ |$ a k.

Exemplo 1.19 *Se $p(x)$ é um polinômio mônico irredutível em $K[x]$ e $|\ |_{p(x)}$ é o valor absoluto $p(x)$-ádico em $K(x)$, então $|a|_{p(x)} = 1$, para todo $a \in K$, $a \neq 0$. Logo, $|\ |_{p(x)}$ é um valor absoluto da extensão $K(x)|K$.*

Observação 1.20 *Seja $|\ |$ um valor absoluto no corpo K. Então, as seguintes afirmações são triviais:*

(1) *$|\ |$ é arquimediano se, e somente se, sua restrição ao corpo primo de K é arquimediano.*

(2) *Se $|\ |_{|k}$ é trivial para algum subcorpo k de K, então $|\ |$ é não-arquimediano. Em particular, se $|\ |$ é um valor absoluto da extensão de corpos $K|k$, então $|\ |$ é não-arquimediano.*

1.2 A topologia definida por um valor absoluto

Nesta seção, utilizaremos um valor absoluto em um corpo K para definir uma métrica em K. Assim, poderemos considerar K um espaço topológico e, então, utilizar os conceitos topológicos para estudá-lo.

Sejam K um corpo e $|\ |$ um valor absoluto em K. A função $d : K \times K \to \mathbb{R}$ definida por $d(x, y) = |x-y|$, para todo $x, y \in K$, tem as seguintes propriedades, para quaisquer $x, y, z, a \in K$:

$(M.1)$ $d(x, y) \geq 0$ e $d(x, y) = 0$ se, e somente se, $x = y$.

$(M.2)$ $d(x, y) = d(y, x)$ (Simetria).

$(M.3)$ $d(x, z) \leq d(x, y) + d(y, z)$ (Desigualdade triangular).

$(M.4)$ $d(x + a, y + a) = d(x, y)$ (Invariante por translação).

$(M.5)$ $d(ax, ay) = |a|d(x, y)$.

Assim, d pode ser interpretada como uma função distância sobre K e, deste modo, K torna-se um espaço métrico no qual as operações são contínuas. Diremos que a topologia definida por d em K é a *topologia de K definida por* $|\ |$ e a mesma será denotada por $T_{|\ |}$.

Proposição 1.21 *Seja $|\ |$ um valor absoluto no corpo K. $|\ |$ é o valor absoluto trivial se, e somente se, $T_{|\ |}$ é discreta em K.*

Demonstração. ($\Rightarrow$:) Se $|\ |$ é o valor absoluto trivial em K, então todo ponto de K é aberto. Logo, $T_{|\ |}$ é discreta em K.

($\Leftarrow$:) Suponhamos que $|\ |$ é um valor absoluto não-trivial em K. Então, existe $a \in K$, $a \neq 0$, tal que $0 < |a| < 1$. Logo, $a^n \to 0$. Segue que $T_{|\ |}$ não é discreta em K. ∎

Definição 1.22 *Sejam $|\ |_1$ e $|\ |_2$ dois valores absolutos no corpo K. Dizemos que $|\ |_1$ e $|\ |_2$ são equivalentes se, e somente se, existe algum número real positivo γ tal que $|x|_1 = |x|_2^{\gamma}$, para todo $x \in K$; caso contrário, dizemos que $|\ |_1$ e $|\ |_2$ são não-equivalentes.*

Exemplo 1.23 *Se p e q são números naturais primos distintos e $|\ |_p$ e $|\ |_q$ são, respectivamente, os valores absolutos p-ádico e q-ádico em $\mathbb{Q}$, então $|\ |_p$ e $|\ |_q$ são não-equivalentes em virtude de*

$$|p|_p = p^{-1} \neq 1 = |p|_q.$$

Exemplo 1.24 *Se $p(x)$ e $q(x)$ são polinômios mônicos irredutíveis distintos em $K[x]$, então os valores absolutos $p(x)$-ádico e $q(x)$-ádico em $K(x)$ são não-equivalentes, visto que*

$$|p(x)|_{p(x)} = 2^{-1} \neq 1 = |p(x)|_{q(x)}, \text{ assim como } |\ |_\infty \text{ e } |\ |_{p(x)}.$$

Definição 1.25 *Sejam $|\ |_K$ e $|\ |_L$ valores absolutos nos corpos K e L, res-pectivamente. Uma função $f : K \to L$ é dita analítica se, e somente se, preserva o valor absoluto, isto é, se*

$$|f(x)|_L = |x|_K, \text{ para todo } x \in K.$$

Observação 1.26 *Sejam $|\ |_1$ e $|\ |_2$ dois valores absolutos equivalentes no corpo K. Se estes valores absolutos são não-triviais em um subcorpo F de K e coincidem em F, então eles coincidem em K, isto é, a função identidade é um isomorfismo analítico.*

O seguinte teorema caracteriza topologicamente os valores absolutos não-triviais equivalentes em um corpo K.

Teorema 1.27 *Para quaisquer valores absolutos não-triviais $|\ |_1$ e $|\ |_2$ no corpo K, as seguintes afirmações são equivalentes:*

(i) $|\ |_1$ *e* $|\ |_2$ *são equivalentes.*

(ii) $T_{|\ |_1} = T_{|\ |_2}$.

(iii) $T_{|\ |_1}$ *é mais forte que* $T_{|\ |_2}$.

(iv) $|x|_1 < 1 \Rightarrow |x|_2 < 1$, *para todo* $x \in K$.

(v) $|x|_1 \leq 1 \Leftrightarrow |x|_2 \leq 1$, *para todo* $x \in K$.

Demonstração. $(i) \Rightarrow (ii)$ e $(ii) \Rightarrow (iii)$ são triviais.

$(iii) \Rightarrow (iv)$: Como $T_{|\ |_1}$ é mais forte que $T_{|\ |_2}$, temos que

$$\{x \in K;\, |x|_1 < \epsilon\} \subseteq \{x \in K;\, |x|_2 < 1\}, \text{ para algum } \epsilon > 0.$$

Seja $x \in K$ tal que $|x|_1 < 1$. Então, $|x^n|_1 < \epsilon$, para algum $n \in \mathbb{N}$. Daí, $|x^n|_2 < 1$. Logo, $|x|_2 < 1$.

$(iv) \Rightarrow (v)$: Suponhamos, primeiramente, que $|x|_2 \leq 1$. Então, $|x^{-1}|_2 \geq 1$ e, por (iv), $|x^{-1}|_1 \geq 1$. Logo, $|x|_1 \leq 1$.

Seja, agora, $x \in K$ tal que $|x|_1 \leq 1$. Então, para todo $n \in \mathbb{N}$, $|x|_1^n \leq 1$. Como $|\ |_1$ é não-trivial, existe $y \in K$ tal que $0 < |y|_1 < 1$. Daí, $|x^n y|_1 < 1$ e, por (iv), $|x^n y|_2 < 1$. Logo, $|x|_2^n < |y|_2^{-1}$ para todo $n \in \mathbb{N}$. Segue da afirmação abaixo que $|x|_2 \leq 1$.

Afirmação: Sejam γ e α números reais tais que $\gamma^n \leq \alpha$ para todo $n \in \mathbb{N}$. Então, $\gamma \leq 1$.

De fato, tomando $f(x) = x^n$ temos, para $x > 1$, que

$$f(x) \geq f(1) + f'(1)(x-1).$$

Daí, $x^n \geq 1 + n(x-1)$, para $x > 1$, para todo $n \in \mathbb{N}$.

Suponhamos, por absurdo, que $\gamma > 1$. Então, existe $n_0 \in \mathbb{N}$ tal que $n_0(\gamma - 1) > \alpha$. Logo,

$$\gamma^{n_0} \geq 1 + n_0(\gamma - 1) > 1 + \alpha > \alpha, \text{ o que contradiz a hipótese.}$$

Portanto, $\gamma \leq 1$.

$(v) \Rightarrow (i)$: Como $|\ |_1$ é não-trivial, existe $y \in K$ tal que $|y|_1 > 1$. Daí, $|y|_2 > 1$.

Afirmamos que, para qualquer $x \in K$, $x \neq 0$, a seguinte igualdade é verdadeira:

$$\frac{\log |x|_1}{\log |y|_1} = \frac{\log |x|_2}{\log |y|_2}.$$

Com efeito, para quaisquer $m, n \in \mathbb{Z}$, $n > 0$, temos

$$\begin{aligned}
\frac{\log |x|_1}{\log |y|_1} \leq \frac{m}{n} &\Leftrightarrow \log |x|_1^n \leq \log |y|_1^m \Leftrightarrow |x|_1^n \leq |y|_1^m \Leftrightarrow |x|_1^n\, |y|_1^{-m} \leq 1 \\
&\Leftrightarrow |x^n|_1\, |y^{-m}|_1 \leq 1 \Leftrightarrow |x^n y^{-m}|_1 \leq 1 \Leftrightarrow |x^n y^{-m}|_2 \leq 1 \\
&\Leftrightarrow |x^n|_2\, |y^{-m}|_2 \leq 1 \Leftrightarrow |x|_2^n\, |y|_2^{-m} \leq 1 \Leftrightarrow |x|_2^n \leq |y|_2^m \\
&\Leftrightarrow \log |x|_2^n \leq \log |y|_2^m \\
&\Leftrightarrow \frac{\log |x|_2}{\log |y|_2} \leq \frac{m}{n}.
\end{aligned}$$

Assim, tomando $\gamma = \dfrac{\log |y|_1}{\log |y|_2} > 0$, obtemos

$$\log|x|_1 = \gamma \log|x|_2 \Rightarrow \log|x|_1 = \log|x|_2^{\gamma}.$$

Portanto,

$$|x|_1 = |x|_2^{\gamma}, \text{ onde } \gamma = \frac{\log|y|_1}{\log|y|_2} > 0.$$

■

Veremos, agora, que valores absolutos não-triviais em um corpo K, dois a dois não-equivalentes, satisfazem uma propriedade muito interessante.

Teorema 1.28 ***(Teorema da aproximação)*** *Sejam $|\ |_1, \ldots, |\ |_r$ valores absolutos não-triviais no corpo K dois a dois não-equivalentes. Então, qualquer r-upla em K pode ser simultaneamente aproximada, isto é, para quaisquer $\alpha_1, \ldots, \alpha_r \in K$ e $\epsilon > 0$, existe $\alpha \in K$ tal que*

$$|\alpha - \alpha_i|_i < \epsilon,\ i = 1, \ldots, r$$

Demonstração. Primeiramente, observamos que, para qualquer valor absoluto $|\ |$ em K, se $|a| < 1$, para algum $a \in K$, então $a^n \to 0$, daí

$$\lim_{n\to\infty} a^n(1+a^n)^{-1} = \begin{cases} 1, & \text{se} \quad |a| > 1 \\ 0, & \text{se} \quad |a| < 1. \end{cases}$$

Afirmamos, inicialmente, que existe $c \in K$ tal que

$$|c|_1 > 1, |c|_i < 1, i = 2, \ldots, r$$

Com efeito, façamos indução sobre r. Se $r = 2$, temos, pelo teorema 1.27, que existem $a, b \in K$ tais que $|a|_1 > 1 \geq |a|_2$ e $|b|_2 > 1 \geq |b|_1$. Tomando, então, $c = ab^{-1} \in K$, obtemos $|c|_1 = |a|_1|b^{-1}|_1 = |a|_1\dfrac{1}{|b|_1} > 1$ e, analogamente, $|c|_2 < 1$. Portanto, para $r = 2$ a afirmação é verdadeira.

Suponhamos, agora, que a afirmação é verdadeira para $r - 1 \geq 2$ e mostremos, então, que vale para r. Por hipótese de indução, temos que existe $a \in K$ tal que $|a|_1 > 1$ e $|a|_i < 1$, $i = 2, \ldots, r-1$. Como $|\ |_1$ e $|\ |_r$ são não-equivalentes, segue do teorema 1.27 que existe $b \in K$ tal que $|b|_1 > 1 > |b|_r$. Temos, então, dois casos a considerar:

(1) Se $|a|_r \leq 1$, tomamos $c_n = a^n b \in K,\ n \in \mathbb{N}$, e obtemos

$$|c_n|_1 = |a|_1^n|b|_1 > 1,\ |c_n|_r = |a|_r^n|b|_r < 1 \text{ e } |c_n|_i = |a|_i^n|b|_i \to 0 < 1,\ i = 2, ..., r-1.$$

Portanto, neste caso, para $n \in \mathbb{N}$ suficientemente grande, a afirmação é verdadeira para r.

(2) Se $|a|_r > 1$, tomamos $c_n = a^n b\,(1+a^n)^{-1} \in K$, $n \in \mathbb{N}$, e obtemos

$|c_n|_1 = |b|_1|a^n(1+a^n)^{-1}|_1 \to |b|_1 > 1$ (pois, como $|a|_1 > 1$, temos que $|a^n(1+a^n)^{-1}|_1 \to 1$),
$|c_n|_r = |b|_r|a^n(1+a^n)^{-1}|_r \to |b|_r < 1$ (pois, como $|a|_r > 1$, temos que $|a^n(1+a^n)^{-1}|_r \to 1$) e
$|c_n|_i = |b|_i|a^n(1+a^n)^{-1}|_i \to 0 < 1$ (pois, como $|a|_i < 1$, temos que $|a^n(1+a^n)^{-1}|_i \to 0$),

para todo $i = 1, \ldots, r-1$. Portanto, neste caso, para $n \in \mathbb{N}$ suficientemente grande, a afirmação é verdadeira para r.

Concluímos, assim, a prova da afirmação.

Seja, então, $c \in K$ tal que $|c|_1 > 1$ e $|c|_i < 1$, $i = 2, ..., r$. Daí,

$$c^n(1+c^n)^{-1} \to 1 \text{ no } |\ |_1 \text{ e } c^n(1+c^n)^{-1} \to 0 \text{ no } |\ |_i,\ i = 2, \ldots, r.$$

Assim, para qualquer $\delta > 0$, existem $n_1, n_2 \in \mathbb{N}$ tais que

$$|c^n(1+c^n)^{-1}-1|_1 < \delta,\ \forall\, n > n_1,\ \text{e}\ |c^n(1+c^n)^{-1}|_i < \delta,\ \forall\, n > n_2,\ i = 2, ..., r.$$

Tomando, então, $n_0 = \max\{n_1, n_2\}$, temos que

$$|c^n(1+c^n)^{-1}-1|_1 < \delta \text{ e } |c^n(1+c^n)^{-1}|_i < \delta,\ \forall\, n > n_0,\ i = 2, \ldots, r.$$

Fixando $n \in \mathbb{N}, n > n_0$, e escrevendo $u_1 = c^n(1+c^n)^{-1}$ obtemos $u_1 \in K$ tal que, para qualquer $\delta > 0$, $|u_1 - 1|_1 < \delta$ e $|u_1|_i < \delta,\ i = 2, \ldots, r$.

Para cada $i = 2, \ldots, r$, uma prova análoga à anterior nos garante a existência de um elemento $c \in K$ tal que $|c|_i > 1$ e $|c|_j < 1,\ 1 \le j \le r$ e $j \neq i$. Assim, para qualquer $\delta > 0$, existem $u_i \in K, i = 1, \ldots, r$, tais que $|u_i - 1|_i < \delta$ e $|u_i|_j < \delta, 1 \le j \le r$ e $j \neq i$.

Tomando, então, $M = \max_i \Big\{ \sum_{j=1}^{r} |\alpha_j|_i \Big\}$, $\delta < \dfrac{\epsilon}{M}$ e escrevendo $\alpha = \sum_{j=1}^{r} \alpha_j u_j$, obtemos

$$\begin{aligned}
|\alpha - \alpha_i|_i &= \Big| \sum_{j=1}^{r} \alpha_j u_j - \alpha_i \Big|_i = \Big| \alpha_i(u_i - 1) + \sum_{j \neq i} \alpha_j u_j \Big|_i \\
&\le \Big| \alpha_i(u_i - 1) \Big|_i + \Big| \sum_{j \neq i} \alpha_j u_j \Big|_i \\
&\le |\alpha_i(u_i - 1)|_i + \sum_{j \neq i} |\alpha_j u_j|_i \\
&= |\alpha_i|_i |u_i - 1|_i + \sum_{j \neq i} |\alpha_j|_i |u_j|_i \\
&\le \delta \Big(\sum_{j=1}^{r} |\alpha_j|_i \Big) \\
&< \delta M < \epsilon, \text{ para cada } i = 1, \ldots, r.
\end{aligned}$$

■

O teorema da aproximação pode também ser formulado de modo puramente topológico: se denotarmos por K_i o corpo K com a topologia induzida por $|\ |_i$, então a imagem de K pela função diagonal $d : K \to K_1 \times \cdots \times K_r$ é densa em $K_1 \times \cdots \times K_r$.

Observação 1.29 *Seja $|\ |$ um valor absoluto no corpo K. Então, a seguinte afirmação é trivial: se $|\ |$ é arquimediano, então qualquer valor absoluto em K equivalente a $|\ |$ também é arquimediano.*

Os teoremas que seguem caracterizam os valores absolutos não-triviais em $\mathbb{Q}$.

Teorema 1.30 ***(Primeiro teorema de Ostrowski)*** *Qualquer valor absoluto arquimediano em $\mathbb{Q}$ é equivalente ao valor absoluto usual.*

Demonstração. Seja $|\ |$ um valor absoluto arquimediano em $\mathbb{Q}$ e denotemos por $|\ |_\infty$ o valor absoluto usual em $\mathbb{Q}$. Queremos mostrar que, dado $x \in \mathbb{Q}$, $|x| = |x|_\infty^\gamma$, para algum número real positivo γ. Sejam, então, $r, s \in \mathbb{Z}$, $r, s > 1$. Expressando s na base r, obtemos:

$$s = a_0 + a_1 r + a_2 r^2 + \cdots + a_v r^v, \quad (*)$$

onde $0 \le a_i < r$, $i = 0, \ldots, v$ e $a_v \neq 0$. Segue que $s \ge r^v$ e, daí,

$$v \leq \frac{\log s}{\log r}. \qquad (**)$$

Como $|a_i| \leq a_i < r$, para $i = 0, \ldots, v$, segue de $(*)$ que

$$\begin{aligned} |s| &\leq |a_0| + |a_1||r| + |a_2||r|^2 + \cdots + |a_v||r|^v \\ &< r[1 + |r| + |r|^2 + \cdots + |r|^v]. \end{aligned}$$

Se $|r| \leq 1$, então cada parcela do colchete acima é ≤ 1; se $|r| > 1$, então cada parcela do colchete acima é $\leq |r|^v$. Assim, $|s| \leq r(1+v)\max\{1, |r|^v\}$.

De $(**)$, segue, então, que

$$|s| \leq r\Big(1 + \frac{\log s}{\log r}\Big) \max\{1, |r|^{\frac{\log s}{\log r}}\}.$$

Substituindo s por s^n e extraindo a raiz n-ésima, obtemos

$$|s| \leq r^{\frac{1}{n}}\Big(1 + n\frac{\log s}{\log r}\Big)^{\frac{1}{n}} \max\{1, |r|^{\frac{\log s}{\log r}}\}.$$

Fazendo $n \to \infty$, obtemos $|s| \leq \max\{1, |r|^{\frac{\log s}{\log r}}\}$. Como $|\ |$ é arquime-diano, temos, pela proposição 1.15, que $|n| > 1$, para todo $n > 1$. Logo, $|s| \leq |r|^{\frac{\log s}{\log r}}$. Daí,

$$\log|s| \leq \frac{\log s}{\log r} \log|r| \Rightarrow \frac{\log|s|}{\log s} \leq \frac{\log|r|}{\log r}.$$

Analogamente, mostramos que $\dfrac{\log|s|}{\log s} \geq \dfrac{\log|r|}{\log r}$. Portanto,

$$\frac{\log|s|}{\log s} = \frac{\log|r|}{\log r} = \gamma.$$

Segue que $\log|r| = \gamma \log r$, para todo $r \in \mathbb{Z}$, $r > 1$. Daí, $|r| = r^\gamma$. Logo,

$$|-r| = |r| = r^\gamma \text{ e } \Big|\frac{r}{s}\Big| = \Big(\frac{r}{s}\Big)^\gamma.$$

Portanto, $|x| = |x|_\infty^\gamma$, para todo $x \in \mathbb{Q}$. ∎

Teorema 1.31 *Qualquer valor absoluto $|\ |$ não-trivial em $\mathbb{Q}$ é equivalente ou ao valor absoluto p-ádico $|\ |_p$ em $\mathbb{Q}$, para algum número natural primo p, ou ao valor absoluto usual $|\ |_\infty$ em $\mathbb{Q}$. Mais ainda, para todo $x \in \mathbb{Q}$, $x \neq 0$, o conjunto $\{p \in \mathbb{N},\ p \text{ primo};\ |x|_p \neq 1\}$ é finito e*

$$\prod_{p \in \mathcal{P}} |x|_p = 1, \text{ onde } \mathcal{P} = \{p \in \mathbb{N},\ p \text{ primo}\} \bigcup \{\infty\}.$$

Demonstração. Já vimos que, se p e q são números naturais primos distintos, $|\ |_p$ e $|\ |_q$ são valores absolutos não-equivalentes em $\mathbb{Q}$. É claro que $|\ |_\infty$ e $|\ |_p$ são valores abolutos não-equivalentes em $\mathbb{Q}$, para qualquer número natural primo p.

Seja $|\ |$ um valor absoluto não-trivial em $\mathbb{Q}$. Se $|\ |$ é arquimediano então, pelo teorema anterior, temos que $|\ |$ e $|\ |_\infty$ são equivalentes em $\mathbb{Q}$. Suponhamos, então, que $|\ |$ é um valor absoluto não-arquimediano.

Afirmamos que $\beta = \{a \in \mathbb{Z}; |a| < 1\}$ é um ideal primo não-nulo de $\mathbb{Z}$.

Com efeito, dados $a, b \in \beta$ e $n \in \mathbb{Z}$, temos que:

(1) $|a+b| \leq \max\{|a|, |b|\} < 1 \Rightarrow a + b \in \beta$.

(2) $|na| = |n||a| < |n| = |n1| \leq 1 \Rightarrow na \in \beta$, para todo $n \geq 0$.

(3) $|na| = |n||a| = |-n||a| < |-n| = |(-n)1| \leq 1 \Rightarrow na \in \beta$, para todo $n < 0$.

Segue que β é um ideal de $\mathbb{Z}$.

Sejam $m, n \in \mathbb{Z}$ tais que $mn \in \beta$. Suponhamos que $n \notin \beta$. Pela proposição 1.15, temos que $|n| = 1$. Daí,

$$1 > |mn| = |m||n| = |m| \Rightarrow m \in \beta.$$

Logo, β é um ideal primo de $\mathbb{Z}$.

Suponhamos, por absurdo, que β é o ideal nulo de $\mathbb{Z}$. Então, $|n| = 1$, para todo $n \in \mathbb{Z}$, $n \neq 0$. Logo, $|\ |$ é trivial em $\mathbb{Z}$. Como $\mathbb{Q}$ é o corpo de frações de $\mathbb{Z}$, segue que $|\ |$ é trivial em $\mathbb{Q}$, o que é um absurdo por hipótese. Portanto, β é um ideal não-nulo de $\mathbb{Z}$, ou seja, $\beta = p\mathbb{Z}$, para algum natural primo p. Em particular, $p \in \beta$, ou seja, $|p| < 1$. Daí, existe algum $\gamma > 0$ tal que $|p| = p^{-\gamma} = (p^{-1})^{\gamma} = |p|_p^{\gamma}$. Mais ainda, $|\ |$ e $|\ |_p$ coincidem em $\mathbb{Z}\backslash\beta = \{a \in \mathbb{Z}; |a| = 1\}$. Assim, dado $x \in \mathbb{Q}$, $x \neq 0$, temos

$$x = p^m \frac{a}{b}, \text{ onde } m \in \mathbb{Z} \text{ e } a, b \in \mathbb{Z}\backslash\beta.$$

Logo,

$$|x| = |p|^m \frac{|a|}{|b|} = (|p|_p^{\gamma})^m = (|p|_p^m)^{\gamma} = |x|_p^{\gamma}.$$

Portanto, $|\ |$ e $|\ |_p$ são equivalentes em $\mathbb{Q}$.

Resta mostrarmos, ainda, as duas últimas afirmações do teorema: dado qualquer $x \in \mathbb{Q}$, $x \neq 0$, podemos escrever

$$x = \pm \prod_{p\ primo} p^{n_p}, \quad (*)$$

com $n_p \in \mathbb{Z}$, para todo número natural primo p, e $n_p = 0$ para quase todo número natural primo p. Daí, $|x|_p = 1$, para quase todo número natural primo p, isto é, o conjunto $\{p \in \mathbb{N},\ p\ primo;\ |x|_p \neq 1\}$ é finito.

Para qualquer número natural primo q, temos

$$\prod_{p\ primo} |q|_p = |q|_q = |q|_{\infty}^{-1}.$$

Tomando, então, $\mathcal{P} = \{p \in \mathbb{N},\ p\ primo\} \bigcup \{\infty\}$, obtemos

$$\prod_{p \in \mathcal{P}} |q|_p = 1 \quad (**)$$

De $(*)$ e $(**)$, segue que

$$\prod_{p \in \mathcal{P}} |x|_p = 1.$$

■

1.3 Corpos completos

Nesta seção, discutiremos o completamento de um corpo com um valor absoluto, veremos que este completamento terá novamente a estrutura de um corpo e que, no caso de corpos completos com um valor absoluto arquimediano, o mesmo será determinado explicitamente.

Sejam D um domínio e $|\ |$ um valor absoluto em D.

Definição 1.32

(*i*) *Uma sequência* (c_v) *de elementos de* D *é dita uma* <u>*sequência convergente*</u> *se, e somente se, existe* $c \in D$ *tal que* $|c_v - c| \to 0$ *quando* $v \to \infty$.

Notação: $c_v \to c$.

(*ii*) *Uma sequência* (c_v) *de elementos de* D *é dita uma* <u>*sequência de Cauchy*</u> *se, e somente se,* $|c_u - c_v| \to 0$ *quando* $u, v \to \infty$.

Observação 1.33 (1) *Seja* (c_v), $c_v \in D$, *uma sequência convergente. Então,* (c_v) *é uma sequência de Cauchy.*

Com efeito, seja $c \in D$ *tal que* $c_v \to c$. *Como* $|c_u - c_v| \leq |c_u - c| + |c_v - c|$, *segue que, quando* $u, v \to \infty$, $|c_u - c_v| \to 0$ *quando. Logo,* (c_v) *é uma sequência de Cauchy.*

(2) *Seja* (c_v), $c_v \in D$, *uma sequência de Cauchy. Então,* (c_v) *é limitada.*

Com efeito, dado $\epsilon = 1 > 0$, *temos que existe* $v_0 \in \mathbb{N}$ *tal que* $|c_u - c_v| < 1$ *sempre que* $u, v \geq v_0$. *Em particular,*

$$v \geq v_0 \Rightarrow |c_v - c_{v_0}| < 1 \Rightarrow |c_v| < 1 + |c_{v_0}|.$$

Tomando $M_1 = 1 + |c_{v_0}|$ *e* $M_2 = \max\{|c_v|;\, 1 \leq v \leq v_0 - 1\}$, *seja* $M = \max\{M_1, M_2\} > 0$. *Então,* $|c_v| \leq M$, *para todo* v. *Logo,* (c_v) *é limitada.*

Definição 1.34 *Dizemos que* D *é um domínio* <u>*completo*</u> *se, e somente se, toda sequência de Cauchy de elementos de* D *é convergente.*

O próximo teorema afirma que, quando D não é completo, existe um único domínio $\widehat{D}$ tal que D é um subanel de $\widehat{D}$ e o valor absoluto de $\widehat{D}$ estende o valor absoluto de D, de modo que $\widehat{D}$ seja completo e D seja denso em $\widehat{D}$.

Teorema 1.35 *Sejam* D *um domínio e* $|\ |$ *um valor absoluto em* D. *Então, existem um domínio completo* $\widehat{D}$ *com um valor absoluto e um homomorfismo injetor analítico* $\lambda : D \to \widehat{D}$ *tal que* $\lambda(D)$ *é denso em* $\widehat{D}$ *e* $\widehat{D}$ *é único, a menos de isomorfismos analíticos. Se* D *é um corpo, então* $\widehat{D}$ *também o é.*

Demonstração. Seja $D^{\mathbb{N}} = \{(c_v);\, c_v \in D, \forall\, v \in \mathbb{N}\}$. Temos que $D^{\mathbb{N}}$ é um anel comutativo com unidade, com as operações

$$(c_v) + (c'_v) := (c_v + c'_v) \text{ e } (c_v)(c'_v) := (c_v c'_v),\ \forall\, v \in \mathbb{N}.$$

Observamos que $0_{D^{\mathbb{N}}} = (c_v)$, onde $c_v = 0_D$, $\forall\, v \in \mathbb{N}$ e $1_{D^{\mathbb{N}}} = (c_v)$, onde $c_v = 1_D$, $\forall\, v \in \mathbb{N}$.

Consideremos o subconjunto C de $D^{\mathbb{N}}$ constituído de todas as sequências de Cauchy em D, isto é,

$$C = \{(c_v);\, c_v \in D \text{ e } (c_v) \text{ é de Cauchy}\}.$$

Afirmamos que C é um subanel de $D^{\mathbb{N}}$.

Com efeito, dadas $(c_v), (b_v) \in C$, temos que, quando $u, v \to \infty$,

$$|(c_u + b_u) - (c_v + b_v)| \leq |c_u - c_v| + |b_u - b_v| \to 0 \text{ e}$$
$$|(c_u\, b_u) - (c_v\, b_v)| \leq |c_u|\, |b_u - b_v| + |c_u - c_v|\, |b_v| \to 0.$$

Logo, $(c_v) + (b_v) = (c_v + b_v) \in C$ e $(c_v)\,(b_v) = (c_v\, b_v) \in C$. Em particular, $0_{D^{\mathbb{N}}} \in C$ e $1_{D^{\mathbb{N}}} \in C$. Portanto, C é um subanel de D.

Consideremos, agora, o subconjunto η de C constituido pelas sequências de D que convergem para zero, isto é,

$$\eta=\{(c_v);\ c_v \in D \text{ e } |c_v| \to 0 \text{ quando } v \to \infty\}.$$

Afirmamos que η é um ideal de C.

Com efeito, dadas $(a_v), (b_v) \in \eta$ e $(c_v) \in C$, temos que, quando $v \to \infty$,

$$|a_v + b_v| \leq |a_v| + |b_v| \to 0 \quad \text{e} \quad |c_v\, a_v| = |c_v|\,|a_v| \leq M\,|a_v| \to 0,$$

onde a sequência de Cauchy é limitada por M, conforme (2) na observação 1.33. Logo,

$$(a_v) + (b_v) = (a_v + b_v) \in \eta \quad \text{e} \quad (c_v)\,(a_v) = (c_v\, a_v) \in \eta.$$

Portanto, η é um ideal de C.

Consideremos, então, o anel quociente C/η. Escrevendo $\widehat{D} = C/\eta$, temos que

$$\widehat{D} = \{\alpha = (c_v)\,(\text{mod } \eta);\ (c_v) \in C\}, \text{ onde}$$

$$(c_v) \equiv (d_v) \Leftrightarrow (c_v) - (d_v) = (c_v - d_v) \in \eta, \text{ para quaisquer } (c_v), (d_v) \in C.$$

Afirmamos que $\widehat{D}$ é um domínio.

Com efeito, dados $\alpha, \beta \in \widehat{D}$, onde $\alpha = (c_v)\,(\text{mod}\,\eta)$, $\beta = (c'_v)\,(\text{mod}\,\eta)$, tais que $\alpha\beta \equiv \eta$, temos que $\eta \equiv \alpha\beta = (c_v)\,(\text{mod}\,\eta)(c'_v)\,(\text{mod}\,\eta) = (c_v c'_v)(\text{mod}\,\eta)$. Daí, $(c_v c'_v) \in \eta$, ou seja $(c_v)(c'_v) \in \eta$. Logo, $(c_v) \in \eta$ ou $(c'_v) \in \eta$. Portanto, $\alpha \equiv \eta$ ou $\beta \equiv \eta$.

Para estendermos o valor absoluto de D para $\widehat{D}$, observamos que, para qualquer sequência $(c_v) \in C$, temos $|\,|c_u| - |c_v|\,| \leq |c_u - c_v|$, para todo $u, v \in \mathbb{N}$. Segue que $(|c_v|)$ é uma sequência de Cauchy em $\mathbb{R}$ e, como $\mathbb{R}$ é completo, existe $L = \lim\limits_{v\to\infty} |c_v| \in \mathbb{R}$. Assim, o valor absoluto em $\widehat{D}$ estendido do valor absoluto de D é definido por $|(c_v)| = \lim\limits_{v\to\infty} |c_v|$, para todo $(c_v) \in \widehat{D}$.

Com efeito, dados $(c_v), (d_v) \in \widehat{D}$, temos que

$$(c_v) \equiv (d_v) \Leftrightarrow (c_v) - (d_v) = (c_v - d_v) \in\ \eta.$$

Daí,

$$\lim_{v\to\infty} (c_v - d_v) = 0 \Rightarrow \lim_{v\to\infty} |c_v - d_v| = 0 \Rightarrow \lim_{v\to\infty} |\,|c_v| - |d_v|\,| = 0 \Rightarrow \lim_{v\to\infty} |c_v| = \lim_{v\to\infty} |d_v|.$$

Logo, $|(c_v)| = |(d_v)|$. Portanto, o valor absoluto estendido está bem definido.

Mostremos, agora, que o valor absoluto estendido é, de fato, um valor absoluto sobre $\widehat{D}$:

$(A.1)$: Dado $(c_v) \in \widehat{D}$, $(c_v) \notin \eta$, temos que $|(c_v)| = \lim\limits_{v\to\infty} |c_v| > 0$. Daí,

$$|(c_v)| \geq 0 \text{ e } |(c_v)| = 0 \text{ se, e somente se, } (c_v) \in \eta.$$

$(A.2)$: Dados $(c_v), (d_v) \in \widehat{D}$, temos que

$$\begin{aligned} |(c_v) + (d_v)| &= |(c_v + d_v)| = \lim_{v\to\infty} |c_v + d_v| \leq \lim_{v\to\infty} (|c_v| + |d_v|) \\ &= \lim_{v\to\infty} |c_v| + \lim_{v\to\infty} |d_v| = |(c_v)| + |(d_v)|. \end{aligned}$$

Logo, $|(c_v) + (d_v)| \leq |(c_v)| + |(d_v)|$.

$(A.3)$: Dados $(c_v), (d_v) \in \widehat{D}$, temos que

$$|(c_v)(d_v)| = |(c_v\, d_v)| = \lim_{v\to\infty} |c_v\, d_v| = \lim_{v\to\infty} |c_v| \lim_{v\to\infty} |d_v| = |(c_v)|\,|(d_v)|.$$

Daí, $|(c_v)\,(d_v)| = |(c_v)|\,|(d_v)|$.

Segue de $(A.1), (A.2)$ e de $(A.3)$ que o valor absoluto estendido é, de fato, um valor absoluto em $\widehat{D}$.

Se identificarmos D com o subanel de $\widehat{D}$ constituído das sequências constantes, então D torna-se um subanel de C tal que $D \cap \eta = 0_{D^{\mathbb{N}}}$. Definamos, então, a função $\lambda : D \to \widehat{D}$ por $\lambda(c) = (c)$, para todo $c \in D$, onde $(c) = (c, c, \ldots) \in \widehat{D}$.

Afirmamos que λ é um homomorfismo injetor analítico de anéis.

Com efeito, dados $a, b \in D$, temos que

$$\lambda(a+b) = (a+b, a+b, \ldots) = (a, a, \ldots) + (b, b, \ldots) = \lambda(a) + \lambda(b) \text{ e}$$
$$\lambda(a \cdot b) = (a \cdot b, a \cdot b, \ldots) = (a, a, \ldots) \cdot (b, b, \ldots) = \lambda(a) \cdot \lambda(b).$$

Além disso, $\lambda(1_D) = (1_D, 1_D, \ldots) = 1_{D^{\mathbb{N}}}$. Segue que λ é um homomorfismo de anéis.
Mostremos, agora, que λ é injetor: sejam $a, b \in D$ tais que $\lambda(a) = \lambda(b)$, então

$$(a) \equiv (b) \Rightarrow (a) - (b) = (a-b) = (a-b, a-b \ldots) \in \eta.$$

Daí, $a = b$.
Resta mostrar que λ é analítico: dado $c \in D$, temos que

$$|\lambda(c)| = |(c)| = \lim_{v \to \infty} |c| = |c|.$$

Portanto, λ é um homomorfismo injetor analítico de anéis.
Tomando $D' = \lambda(D)$, temos que D e D' são isomorfos.

Afirmamos que D' é denso em $\widehat{D}$.
Com efeito, dada $(c_v) \in \widehat{D}$, onde $(c_v) = (c_1, c_2, \ldots, c_v, \ldots)$, seja $(c_v{}') \subset D'$ uma sequência , com $c_v{}' = (c_v, c_v, c_v, \ldots)$. Temos que $(c_v) - c_v{}' = (c_1 - c_v, c_2 - c_v, \ldots)$. Logo,

$$|(c_v) - c_v{}'| = \lim_{u \to \infty} |c_u - c_v|.$$

Como (c_v) é uma sequência de Cauchy, segue que $|c_u - c_v| \to 0$ quando $u, v \to \infty$. Daí,

$$|(c_v) - c_v{}'| \to 0 \text{ quando } v \to \infty.$$

Portanto, $c_v{}' \to (c_v)$.

Afirmamos, agora, que $\widehat{D}$ é completo.
De fato, seja $(\alpha_v) \subset \widehat{D}$ uma sequência de Cauchy. Como D' é denso em $\widehat{D}$, para cada v existe $c_v{}' \in D'$ tal que $|c_v{}' - \alpha_v| < \dfrac{1}{v}$. Segue que a sequência $(c_v{}' - \alpha_v) \in \eta$. Daí, quando $u, v \to \infty$,

$$|c_u{}' - c_v{}'| \leq |c_u{}' - \alpha_u| + |\alpha_u - \alpha_v| + |\alpha_v - c_v{}'| \to 0,$$

Portanto, a sequência $(c_v{}') \subset D'$ é um sequência de Cauchy. Assim, como

$$\begin{aligned} |c_u{}' - c_v{}'| &= |(c_u, c_u, \ldots) - (c_v, c_v, \ldots)| = |(c_u - c_v, c_u - c_v, \ldots)| \\ &= |\lambda(c_u - c_v)| = |c_u - c_v|, \end{aligned}$$

temos que a sequência (c_v), com $c_v \in D$, é de Cauchy, ou seja, $(c_v) \in C$. Seja, então, $(c_v) \in \widehat{D}$. Temos que

$$c_v{}' - (c_v) = (c_v, c_v \ldots) - (c_1, c_2, \ldots) = (c_v - c_1, c_v - c_2, \ldots).$$

Daí, $|c_v{}' - (c_v)| = \lim_{u \to \infty} |c_v - c_u|$. Logo, $|c_v{}' - (c_v)| \to 0$ quando $v \to \infty$. Segue que, quando $v \to \infty$,

$$|\alpha_v - (c_v)| \leq |\alpha_v - c_v{}'| + |c_v{}' - (c_v)| \to 0.$$

Daí, $\alpha_v \to (c_v)$ quando $v \to \infty$. Portanto, $\widehat{D}$ é completo.

Para provarmos a unicidade de $\widehat{D}$, mostraremos que a propriedade que segue é satisfeita: dado qualquer homomorfismo injetor analítico $f : D \to D_1$ de D em qualquer outro domínio D_1 completo com um valor absoluto, existe um único homomorfismo injetor analítico $f_1 : \widehat{D} \to D_1$ que estende f.

Seja $\alpha \in \widehat{D}$, digamos $\alpha = \lim_{v \to \infty} a_v$, onde (a_v), com $a_v \in D$, é uma sequência de Cauchy em D. Então, $(f(a_v))$ é uma sequência de Cauchy em D_1 e, como D_1 é completo, existe $\lim_{v \to \infty} (f(a_v))$.

Se $(a_v{}')$, com $a_v{}' \in D$, é outra sequência de Cauchy em D tal que $\lim_{v\to\infty} a_v{}' = \alpha$, então

$$\begin{aligned}\lim_{v\to\infty} a_v = \lim_{v\to\infty} a_v{}' &\Rightarrow \lim_{v\to\infty}(a_v - a_v{}') = 0 \Rightarrow \lim_{v\to\infty} f(a_v - a_v{}') = 0 \\ &\Rightarrow \lim_{v\to\infty}(f(a_v) - f(a_v{}')) = 0 \Rightarrow \lim_{v\to\infty} f(a_v) = \lim_{v\to\infty} f(a_v{}').\end{aligned}$$

Segue que o $\lim_{v\to\infty} f(a_v)$ independe da sequência considerada. Definamos, então,

$$f_1(\alpha) = \lim_{v\to\infty} f(a_v),$$

onde (a_v), com $a_v \in D$, é uma sequência de Caychy em D tal que $\lim_{v\to\infty} a_v = \alpha$.

Afirmamos que f_1 é um homomorfismo injetor analítico.

De fato, dados $\alpha, \beta \in \widehat{D}$, sejam $(a_v), (b_v)$, com $a_v, b_v \in D$, sequências de Cauchy em D tais que $\lim_{v\to\infty} a_v = \alpha$ e $\lim_{v\to\infty} b_v = \beta$. Então,

$$\begin{aligned}f_1(\alpha) + f_1(\beta) &= \lim_{v\to\infty} f(a_v) + \lim_{v\to\infty} f(b_v) = \lim_{v\to\infty}(f(a_v) + f(b_v)) \\ &= \lim_{v\to\infty} f(a_v + b_v) = f_1(\alpha + \beta)\end{aligned}$$

e

$$\begin{aligned}f_1(\alpha) \cdot f_1(\beta) &= \lim_{v\to\infty} f(a_v) \cdot \lim_{v\to\infty} f(b_v) = \lim_{v\to\infty}(f(a_v) \cdot f(b_v)) \\ &= \lim_{v\to\infty} f(a_v \cdot b_v) = f_1(\alpha \cdot \beta).\end{aligned}$$

Além disso, $f_1(a) \cdot f_1(1_{\widehat{D}}) = f_1(a \cdot 1_{\widehat{D}}) = f_1(a)$, para todo $a \in \widehat{D}$. Daí, $f_1(1_{\widehat{D}}) = 1_{D_1}$. Segue que f_1 é um homomorfismo de anéis.

Mostremos, agora, que f_1 é um homomorfismo de anéis injetor: dados $\alpha, \beta \in \widehat{D}$, sejam $(a_v), (b_v)$, com $a_v, b_v \in D$, sequências de Cauchy em D tais que $\lim_{v\to\infty} a_v = \alpha$ e $\lim_{v\to\infty} b_v = \beta$. Então,

$$\begin{aligned}f_1(\alpha) = f_1(\beta) &\Rightarrow \lim_{v\to\infty} f(a_v) = \lim_{v\to\infty} f(b_v) \Rightarrow \lim_{v\to\infty}(f(a_v) - f(b_v)) = 0 \\ &\Rightarrow \lim_{v\to\infty} f(a_v - b_v) = 0 \Rightarrow \lim_{v\to\infty}(a_v - b_v) = 0 \\ &\Rightarrow (a_v - b_v) \in \eta \Rightarrow \lim_{v\to\infty} a_v = \lim_{v\to\infty} b_v \\ &\Rightarrow \alpha = \beta.\end{aligned}$$

Logo, f_1 é um homomorfismo injetor de anéis.

Resta mostrarmos que f_1 é analítico: dado $\alpha \in \widehat{D}$, seja (a_v), com $a_v \in D$, uma sequência de Cauchy em D tal que $\lim_{v\to\infty} a_v = \alpha$. Então,

$$|f_1(\alpha)| = |\lim_{v\to\infty} f(a_v)| = \lim_{v\to\infty} |f(a_v)| = \lim_{v\to\infty} |a_v| = |\alpha|.$$

Portanto, f_1 é um homomorfismo injetor analítico de anéis.

Mostremos, agora, que f_1 é uma extensão de f: dado $a \in D$, temos que

$$f_1(a) = \lim_{v\to\infty} f(a) = f(a).$$

Logo, f_1 é uma extensão de f.

Afirmamos que a extensão f_1 é única.

Com efeito, temos que D é denso em $\widehat{D}$ e o valor absoluto sobre D está determinado. Assim, se f_2 é outro homomorfismo injetor analítico que estende f, temos que $f_2(a) = f(a) = f_1(a)$,

para todo $a \in D$, e, como f_1 e f_2 são contínuas, $f_1(\alpha) = f_2(\alpha)$, para todo $\alpha \in \widehat{D}$. Daí, $f_2 = f_1$. Em particular, f_1 é um isomorfismo analítico de $\widehat{D}$ sobre $f_1(\widehat{D}) \subset D_1$. Assim, como $\widehat{D}$ é completo e D é denso em $\widehat{D}$, temos que $f_1(\widehat{D})$ é completo e D é denso em $f_1(\widehat{D})$. Portanto, se D é denso em D_1, então, como D_1 é completo, $f_1(\widehat{D}) = D_1$. Segue que f_1 é um isomorfismo analítico de $\widehat{D}$ sobre D_1.

Para concluirmos nossa demonstração, resta mostrarmos que se D é um corpo, então $\widehat{D}$ também o é: suponhamos que D é um corpo. Dado $\alpha \in \widehat{D}$, $\alpha \neq 0$, seja (c_v), onde $c_v \in D$, uma sequência de Cauchy em D tal que $\lim_{v\to\infty} c_v = \alpha$. Dado $p = \dfrac{2}{|\alpha|} > 0$, existe $v_0 \in \mathbb{N}$, tal que

$$\begin{aligned} v > v_0 \quad &\Rightarrow \quad |c_v - \alpha| < \frac{1}{p} \Rightarrow -\frac{1}{p} < |c_v| - |\alpha| \\ &\Rightarrow \quad |\alpha| - \frac{1}{p} < |c_v| \Rightarrow \frac{2}{p} - \frac{1}{p} < |c_v| \\ &\Rightarrow \quad \frac{1}{p} < |c_v| \Rightarrow |c_v| > 0 \text{ e } |c_v|^{-1} < p. \end{aligned}$$

Assim, se $v > v_0$, então $c_v \neq 0$ e, como D é um corpo, existe c_v^{-1}. Logo, para $u, v > v_0$, temos

$$|c_u^{-1} - c_v^{-1}| = |c_u^{-1}(c_v - c_u)c_v^{-1}| = |c_v|^{-1}|c_v - c_u||c_v|^{-1} < p^2|c_v - c_u|.$$

Fazendo $u, v \to \infty$, obtemos $|c_u^{-1} - c_v^{-1}| \to 0$. Portanto, (c_v^{-1}) é uma sequência de Cauchy em D para $v > v_0$.

Seja, então, $\alpha' \in \widehat{D}$ tal que $\lim_{v\to\infty} c_v^{-1} = \alpha'$. Como $c_v\, c_v^{-1} = 1$, para $v > v_0$, segue que

$$1 = \lim_{v\to\infty} (c_v\, c_v^{-1}) = \lim_{v\to\infty} (c_v) \lim_{v\to\infty} (c_v^{-1}) = \alpha\, \alpha'.$$

Daí, $\alpha' = \alpha^{-1} \in \widehat{D}$. Portanto, $\widehat{D}$ é um corpo. ∎

Definição 1.36 *Sejam D um domínio e $|\ |$ um valor absoluto em D. Então, com as notações do teorema anterior, $\widehat{D}$ é o chamado <u>completamento</u> de D.*

Definição 1.37 *Sejam K um corpo e $|\ |$ um valor absoluto em K. Um espaço vetorial <u>normado sobre K</u> é um K-espaço vetorial V com uma função real $\|\ \| : V \to \mathbb{R}$ tal que:*

$(N.1)$ $\|x\| \geq 0$, $\forall\, x \in V$, *e* $\|x\| = 0$ *se, e somente se,* $x = 0$.

$(N.2)$ $\|x + y\| \leq \|x\| + \|y\|$, $\forall\, x, y \in V$.

$(N.3)$ $\|\alpha x\| = |\alpha|\|x\|$, $\forall\, x \in V$ *e* $\alpha \in K$.

A função $\|\ \|$ é chamada <u>norma de V</u>.

Exemplo 1.38 *Qualquer extensão de corpos $E|K$ com o valor absoluto estendido de K é um espaço vetorial normado sobre K.*

Definição 1.39 *Sejam K um corpo e $|\ |$ um valor absoluto em K. Qualquer K-espaço vetorial V de dimensão finita n tem pelo menos uma norma, a <u>norma cúbica</u>, definida como segue: tome qualquer base $\{e_1, \ldots, e_n\}$ de V e defina a função $\|\ \| : V \to \mathbb{R}$ por*

$$\|x\| = \max_i\{|\alpha_i|\},\ \textit{onde}\ x = \sum_{i=1}^{n} \alpha_i e_i,\ \alpha_i \in K,\ i = 1, \ldots, n.$$

No próximo teorema, veremos que qualquer extensão algébrica E de um corpo completo com um valor absoluto $|\ |$ tem, no máximo, uma extensão de $|\ |$ e E é completo na topologia induzida por esta. Para a demonstração de tal teorema necessitaremos, no entanto, do lema que segue.

Lema 1.40 *Sejam K um corpo completo e $|\ |$ um valor absoluto em K. Se V é um espaço vetorial de dimensão finita n sobre K, então V é completo na topologia induzida pela norma cúbica e qualquer outra norma induz a mesma topologia. Em particular, se K é discreto, então V também o é.*

Demonstração. Primeiramente, vamos mostrar que V é completo na topologia induzida pela norma cúbica.

Seja $\{e_1, \ldots, e_n\}$ uma base de V sobre K e seja (x_v), $x_v \in V$, uma sequência de Cauchy, com

$$x_v = \sum_{i=1}^{n} \xi_{iv} e_i, \text{ onde } \xi_{iv} \in K,\ i = 1, \ldots, n.$$

Então, $\|x_u - x_v\| \to 0$ quando $u, v \to \infty$, ou seja, $\max_i\{|\xi_{iu} - \xi_{iv}|\} \to 0$, quando $u, v \to \infty$. Daí, para cada $i = 1, \ldots, n$, $|\xi_{iu} - \xi_{iv}| \to 0$, quando $u, v \to \infty$. Logo, (ξ_{iv}) é uma sequência de Cauchy e, como K é completo, $\xi_{iv} \to \xi_i \in K$, para cada $i = 1, \ldots, n$. Escrevendo, então,

$$x = \sum_{i=1}^{n} \xi_i e_i \in V,$$

obtemos

$$\|x - x_v\| = \max_i\{|\xi_i - \xi_{iv}|\} \to 0, \text{ quando } v \to \infty, \text{ ou seja, } x_v \to x.$$

Portanto, V é completo na topologia induzida pela norma cúbica.

Seja N uma outra norma qualquer em V. Para mostrarmos a segunda afirmação, façamos indução sobre n.

Se $n = 1$, então, dado $x \in V$, $x = \xi_1 e_1$, temos que

$$N(x) = |\xi_1| N(e_1) = \|x\| M, \text{ onde } M \text{ independe de } x.$$

Logo, $\|x_v\| \to 0$ se, e somente se, $N(x_v) \to 0$.

Suponhamos, então, que a afirmação é verdadeira para K-espaços vetoriais de dimensão $n-1$ e mostremos que a mesma vale para K-espaços vetoriais de dimensão n.

Dado $x \in V$, onde $x = \sum_{i=1}^{n} \xi_i e_i$, temos que

$$\begin{aligned} N(x) = N\Big(\sum_{i=1}^{n} \xi_i e_i\Big) &\leq |\xi_1| N(e_1) + \cdots + |\xi_n| N(e_n) \\ &\leq \max_i\{|\xi_i|\} \sum_{i=1}^{n} N(e_i) \\ &= \|x\| M, \end{aligned}$$

onde M independe de x.

Portanto, quando $\|x_v\| \to 0$, teremos $N(x_v) \to 0$.

Suponhamos que (x_v) é uma sequência de V tal que $N(x_v) \to 0$, mas de modo que $\|x_v\| \nrightarrow 0$. Escrevendo $x_v = \sum_{i=1}^{n} \xi_{iv} e_i$; se $|\xi_{iv}| \to 0$ para todo $i = 1, \ldots, n$ quando $v \to \infty$, então

$$\|x_v\| = \max_i\{|\xi_{iv}|\} \to 0 \text{ quando } v \to \infty,$$

o que é um absurdo.

Portanto, existe algum i, digamos $i = 1$, tal que $|\xi_{1v}| \nrightarrow 0$. Passando a uma subsequência podemos então supor que existe $\epsilon > 0$ tal que $|\xi_{1v}| \geq \epsilon$, para todo v. Tomando

$$y_v = \xi_{1v}^{-1} x_v = \sum_{i=1}^{n} \eta_{iv} e_i,$$

obtemos

$$N(y_v) = N(\xi_{1v}^{-1} x_v) = |\xi_{1v}^{-1}| N(x_v) \leq \epsilon^{-1} N(x_v).$$

Como $N(x_v) \to 0$, segue que $N(y_v) \to 0$ e, portanto, $y_v \to 0$. Logo,

$$\sum_{i=2}^{n} \eta_{iv} e_i \to -e_1$$

na topologia definida pela norma N.

Seja W o subespaço de V gerado por $\{e_2, \ldots, e_n\}$. Temos que W tem dimensão $n-1$. Como W é um espaço vetorial de dimensão finita também sobre o corpo completo K com valor absoluto, temos que W é completo na topologia induzida pela norma cúbica e, como sua dimensão é $n-1$, temos, por hipótese de indução, que a norma N induz em W a mesma topologia induzida pela norma cúbica. Logo, W é completo na topologica induzida pela norma N. Assim, como

$$\sum_{i=2}^{n} \eta_{iv} e_i \in W \text{ para todo } v \text{ e } \sum_{i=2}^{n} \eta_{iv} e_i \to -e_1$$

na topologia induzida pela norma N, segue que $-e_1 \in W$, o que é uma contradição. Portanto, quando $N(x_v) \to 0$, teremos $\|x_v\| \to 0$.

Suponhamos, finalmente, que K é discreto. Então, o valor absoluto $|\ |$ em K é trivial. Seja $x \in V$, $x = \sum_{i=1}^{n} \alpha_i e_i$. Temos que

$$\|x\| = \max_i\{|\alpha_i|\} = \begin{cases} 0, & \text{se} \quad \alpha_i = 0, \text{ para todo } i, \text{ ou seja, se } x = 0 \\ 1, & \text{se} \quad \alpha_i \neq 0, \text{ para algum } i, \text{ ou seja, se } x \neq 0 \end{cases}$$

Portanto, V é discreto na topologia induzida pela norma cúbica.

Como qualquer outra norma em V induz a mesma topologia induzida pela norma cúbica, segue que V é discreto. ∎

Teorema 1.41 *Sejam K um corpo completo e $|\ |$ um valor absoluto em K. Então, qualquer extensão algébrica E de K tem, no máximo, uma extensão do valor absoluto $|\ |$ e E é completo na topologia induzida por esta.*

Demonstração. Sejam $|\ |_1$ e $|\ |_2$ duas extensões a E do valor absoluto $|\ |$. Temos que mostrar que $|\alpha|_1 = |\alpha|_2$, para todo $\alpha \in E$.

Para cada $\alpha \in E$, consideremos a extensão algébrica $K(\alpha)$ de K. Temos que

$$[K(\alpha) : K] = \text{grau } p_{\alpha,K} < \infty$$

Logo, $K(\alpha)$ é um espaço vetorial de dimensão finita sobre K.

Pelo lema 1.40, temos que $|\ |_1$ e $|\ |_2$ induzem a mesma topologia em $K(\alpha)$ e este é completo nessa topologia. Em particular, $|\ |_1$ e $|\ |_2$ são equivalentes em $K(\alpha)$. Se $|\ |_1$ ou $|\ |_2$ é trivial, então K é discreto e, pelo lema 1.40, $K(\alpha)$ é discreto e, daí, ambos são valores absolutos triviais;

se $|\ |_1$ e $|\ |_2$ são não-triviais, então, pela observação 1.26, eles coincidem em $K(\alpha)$. Portanto, $|\alpha|_1 = |\alpha|_2$, para todo $\alpha \in E$. ∎

Como último resultado deste capítulo, temos que qualquer extensão de $\mathbb{R}$ com um valor absoluto estendido do valor absoluto usual de $\mathbb{R}$ ou é o próprio $\mathbb{R}$ ou é $\mathbb{C}$. Este resultado é uma consequência do teorema a seguir.

Teorema 1.42 ***(Gelfand-Mazur)*** *Seja A uma álgebra comutativa sobre os números reais tal que A contém um elemento i, com $i^2 = -1$, e seja $\mathbb{C} = \mathbb{R} + \mathbb{R}i$. Suponha que A é normado (como espaço vetorial sobre $\mathbb{R}$) e que $|xy| \leq |x||y|$ para todo $x, y \in A$. Então, dado $x_0 \in A$, $x_0 \neq 0$, existe um elemento $c \in \mathbb{C}$ tal que $x_0 - c$ não é invertível em A.*

Demonstração. Escreveremos $|\ | = |\ |_\infty$ em $\mathbb{C}$. Suponhamos, primeiramente, que $x_0 \in \mathbb{C}$. Então, tomando $c = x_0 \in \mathbb{C}$, temos que $x_0 - c = 0$ e, portanto, $x_0 - c$ não é invertível em A. Suponhamos, agora, que $x_0 \notin \mathbb{C}$ e, por absurdo, que $x_0 - z$ é invertível em A para todo $z \in \mathbb{C}$. Definimos, então, a função $f : \mathbb{C} \to A$ por $f(z) = (x_0 - z)^{-1}$, para todo $z \in \mathbb{C}$. Temos que $f(z) \neq 0$, para todo $z \in \mathbb{C}$ e, como a operação inversa é contínua, a função f é contínua. Assim, para todo $z \in \mathbb{C}$, $z \neq 0$, temos

$$f(z) = \frac{1}{z}\left(\frac{1}{\frac{x_0}{z} - 1}\right)$$

Daí, $f(z) \to 0$ quando $z \to \infty$ em $\mathbb{C}$. Em particular, $|f(z)| \to 0$ quando $z \to \infty$ em $\mathbb{C}$.

Consideremos, então, a aplicação $|f| : \mathbb{C} \to [0, +\infty)$ definida por $|f|(z) = |f(z)|$, para todo $z \in \mathbb{C}$. Temos que a aplicação $|f|$ é contínua, visto que a mesma é uma composição de funções contínuas.

Afirmamos que $|f|$ é limitada.

Com efeito, fixado $R_0 \in \mathbb{R}$, $R_0 > 0$, consideremos a bola fechada de centro na origem e raio R_0, denotada por $B_{R_0}[0]$. Como $|f|$ é contínua e $B_{R_0}[0]$ é compacta, segue que existe $z_0 \in B_{R_0}[0]$ tal que $|f(z)| \leq |f(z_0)|$, para todo $z \in B_{R_0}[0]$. Daí, $|f(z_0)| > 0$, pois, caso contrário, $f(z) = 0$, para todo $z \in B_{R_0}[0]$, o que seria um absurdo.

Escrevendo $M_0 = |f(z_0)| > 0$, obtemos $|f(z)| \leq M_0$, para todo $z \in B_{R_0}[0]$. Como $f(z) \to 0$ quando $z \to \infty$ em $\mathbb{C}$, segue que existe $B > 0$ tal que

$$|f(z)| < \frac{M_0}{2}, \text{ sempre que } |z| > B,\ z \in \mathbb{C}. \qquad (*)$$

Seja $R = \max\{R_0, B\}$ e consideremos a bola fechada de centro na origem e de raio R denotada por $B_R[0]$. Como $|f|$ é contínua e $B_R[0]$ é compacta, segue que existe $z' \in B_R[0]$ tal que $|f(z)| \leq |f(z')|$, para todo $z \in B_R[0]$. Daí, $|f(z')| > 0$ pois, caso contrário, $f(z) = 0$ para todo $z \in B_R[0]$, o que seria, novamente, um absurdo.

Escrevendo, então, $M = |f(z')| > 0$, obtemos $|f(z)| \leq M$, para todo $z \in B_R[0]$. Em particular, $M_0 \leq M$.

Suponhamos que $z \notin B_R[0]$, isto é, que $|z| > R$, então, $|z| > B$ e de $(*)$ segue que $|f(z)| < M_0$. Logo, $|f(z)| \leq M$, para todo $z \in \mathbb{C}$. Portanto, f é limitada.

Seja $D = \{z \in \mathbb{C};\ |f(z)| = M\}$. temos que:

(i) $D \neq \varnothing$, visto que $z' \in D$;

(ii) D é fechado, visto que $D = |f|^{-1}(\{M\})$;

(iii) D é limitado, visto que $D \subset B_R[0]$.

Afirmamos que D é aberto.

Com efeito, seja $c_0 \in D$. Depois de uma translação, podemos supor $c_0 = 0$. Daí,

$$|f(0)| = \left|\frac{1}{x_0}\right| = M.$$

Afirmamos que, se $r \in \mathbb{R}$, $r > 0$ suficientemente pequeno, então todos os pontos sobre o círculo de raio r encontram-se em D.

Com efeito, consideremos a soma

$$S(n) = \frac{1}{n}\sum_{k=1}^{n}\frac{1}{x_0 - w^k r},$$

onde w é uma raiz primitiva n-ésima da unidade.

Temos que $x^n - r^n = \prod_{k=1}^{n}(x - w^k r)$. Logo,

$$\log(x^n - r^n) = \log\Big(\prod_{k=1}^{n}(x - w^k r)\Big) = \sum_{k=1}^{n}\log(x - w^k r).$$

Derivando, obtemos

$$\frac{nx^{n-1}}{x^n - r^n} = \sum_{k=1}^{n}\frac{1}{x - w^k r}.$$

Dividindo primeiramente por n, depois por x^{n-1} e, finalmente substituindo x por x_0, obtemos

$$S(n) = \frac{1}{n}\sum_{k=1}^{n}\frac{1}{x_0 - w^k r} = \frac{x_0^{n-1}}{x_0^n - r^n} = \frac{1}{x_0 - r\left(\frac{r}{x_0}\right)^{n-1}}.$$

Logo,

$$S(n) = \frac{1}{x_0 - r\left(\frac{r}{x_0}\right)^{n-1}}.$$

Tomando r suficientemente pequeno de modo que $\left|\frac{r}{x_0}\right| < 1$, temos que

$$|S(n)| \to \left|\frac{1}{x_0}\right| = M \text{ quando } n \to \infty.$$

Suponhamos, por absurdo, que existe um número $\lambda \in \mathbb{C}$, com $|\lambda| = 1$ e tal que

$$\left|\frac{1}{x_0 - \lambda r}\right| < M.$$

Então, λr está sobre o círculo de raio r e, no entanto, $\lambda r \notin D$.

Consideremos a função

$$g(x) = \left|\frac{1}{x_0 - xr}\right|, \text{ para todo } x \in \mathbb{C},\ |x| = 1.$$

Temos que g é contínua e $g(\lambda) < M$. Logo, existem um intervalo I sobre o círculo unitário e $\epsilon > 0$, tais que para toda ξ raiz da unidade em I, temos $g(\xi) < M - \epsilon < M$, isto é,

$$\left|\frac{1}{x_0 - \xi r}\right| < M - \epsilon < M.$$

Assim, para toda ξ raiz da unidade pertencente ao intervalo I, temos que ξr está sobre o círculo de raio r e, no entanto, $\xi r \notin D$.

Seja n suficientemente grande e seja b_n o número de raízes n-ésimas da unidade pertencentes ao intervalo I. Então, o comprimento $l(I)$ do intervalo I é aproximadamente $\frac{2\pi}{n}\, b_n$. Expressamos a soma $S(n)$ como

$$S(n) = \frac{1}{n}\left[\sum_{I}\frac{1}{x_0 - w^k r} + \sum_{II}\frac{1}{x_0 - w^k r}\right],$$

onde $\sum_I$ é a soma referente às raízes w^k da unidade sobre o intervalo I e $\sum_{II}$ é a soma referente às raízes w^k da unidade restantes. Daí,

$$|S(n)| \leq \frac{1}{n}\left[\Big|\sum_{I}\Big| + \Big|\sum_{II}\Big|\right] \leq \frac{1}{n}\left[b_n(M-\epsilon) + (n-b_n)M\right] = M - \frac{b_n}{n}\,\epsilon. \qquad (**)$$

Temos que $\lim\limits_{n\to\infty}\dfrac{2\pi}{n}\,b_n = l(I)$. Logo, $\lim\limits_{n\to\infty}\dfrac{b_n}{n} = \dfrac{l(I)}{2\pi} > 0$. Assim, de $(**)$, segue que

$$\lim_{n\to\infty}|S(n)| \leq M - \frac{l(I)}{2\Pi}\,\epsilon < M,$$

o que é um absurdo. Portanto, D é aberto.

Temos, então, que $D \subseteq \mathbb{C}$ é aberto e fechado. Como $\mathbb{C}$ é conexo, segue que $D = \mathbb{C}$. Daí, f é constante, o que é um absurdo. ∎

Corolário 1.43 *Seja K um corpo, o qual é uma extensão de $\mathbb{R}$, e seja $|\ |$ um valor absoluto em K estendido do valor absoluto usual de $\mathbb{R}$. Então, $K = \mathbb{R}$ ou $K = \mathbb{C}$.*

Demonstração. Suponhamos, primeiramente, que $\mathbb{C} \subseteq K$. Mostremos que $K \subseteq \mathbb{C}$.

Seja $x_0 \in K$, $x_0 \neq 0$. Então, pelo teorema anterior, existe $c \in \mathbb{C}$ tal que $x_0 - c$ não é invertível em K. Como K é um corpo, segue que $x_0 - c = 0$. Daí, $x_0 = c \in \mathbb{C}$. Logo, $K \subseteq \mathbb{C}$. Portanto, $K = \mathbb{C}$.

Suponhamos, agora, que $\mathbb{C} \nsubseteq K$, isto é, o polinômio $x^2 + 1 = 0$ é irredutível sobre K. Então, adicionamos a raiz i desta equação a K e obtemos o corpo $K(i)$.

Afirmamos que a aplicação $\|\ \| : K(i) \to \mathbb{R}$ definida por

$$\|x+iy\| = \begin{cases} 0 \quad , & \text{se} \quad x+iy = 0, \text{ ou seja, se } x = y = 0 \\ |x| + |y|, & \text{se} \quad x+iy \neq 0, \text{ ou seja, se } x \neq 0 \text{ ou } y \neq 0 \end{cases}$$

é uma norma em $K(i)$.

Com efeito,

$(N.1)$: Dado $x+iy \in K(i)$, $x+iy \neq 0$, temos que $\|x+iy\| = |x|+|y| > 0$. Logo, $\|x+iy\| \geq 0$ para todo $x+iy \in K(i)$ e $\|x+iy\| = 0$ se, e somente se, $x+iy = 0$.

$(N.2)$: Dados $x_1+iy_1, x_2+iy_2 \in K(i)$, temos que

$$\begin{aligned} \|(x_1+iy_1)+(x_2+iy_2)\| &= \|(x_1+x_2)+(y_1+y_2)i\| \\ &= |x_1+x_2|+|y_1+y_2| \\ &\leq (|x_1|+|x_2|)+(|y_1|+|y_2|) \\ &= (|x_1|+|y_1|)+(|x_2|+|y_2|) \\ &= \|x_1+iy_1\|+\|x_2+iy_2\|. \end{aligned}$$

$(N.3)$: Dados $x+iy \in K(i)$ e $\lambda \in \mathbb{R}$, temos que

$$\begin{aligned} \|\lambda(x+iy)\| &= \|\lambda x + i\lambda y\| = |\lambda x| + |\lambda y| \\ &= |\lambda||x| + |\lambda||y| = |\lambda|(|x|+|y|) \\ &= |\lambda|\|x+iy\|. \end{aligned}$$

Segue de $(N.1)$, $(N.2)$ e de $(N.3)$, que a aplicação $\| \ \|$ é, de fato, uma norma em $K(i)$. Dados $x_1 + iy_1, x_2 + iy_2 \in K(i)$, temos também que

$$\begin{aligned}
\|(x_1 + iy_1)(x_2 + iy_2)\| &= \|(x_1x_2 - y_1y_2) + (x_1y_2 + x_2y_1)i\| \\
&= |x_1x_2 - y_1y_2| + |x_1y_2 + x_2y_1| \\
&\leq |x_1x_2| + |y_1y_2| + |x_1y_2| + |x_2y_1| \\
&= |x_1||x_2| + |y_1||y_2| + |x_1||y_2| + |x_2||y_1| \\
&= (|x_1| + |y_1|)(|x_2| + |y_2|) \\
&= \|x_1 + iy_1\| \, \|x_2 + iy_2\|
\end{aligned}$$

Assim, $\mathbb{C} \subseteq K(i)$ e $K(i)$ é um corpo que satisfaz às condições do teorema anterior.

Mostremos, agora, que $K(i) \subseteq \mathbb{C}$.

Seja $x_0 \in K(i)$. Então, pelo teorema anterior, existe $c \in \mathbb{C}$ tal que $x_0 - c$ não é invertível em $K(i)$. Como $K(i)$ é um corpo, segue que $x_0 - c = 0$. Daí, $x_0 = c \in \mathbb{C}$. Logo, $K(i) \subseteq \mathbb{C}$. Portanto, $K(i) = \mathbb{C}$ e, como $\mathbb{R} \subseteq K \nsubseteq K(i) = \mathbb{C}$, obtemos $K = \mathbb{R}$. ■

Capítulo 2

Valorizações

No capítulo anterior, apresentamos um esboço razoavelmente completo de corpos com um valor absoluto arquimediano. Como Krull (1931) observou, um valor absoluto não-arquimediano utiliza somente a multiplicatividade e a ordem dos números reais. Nesta capítulo, estudaremos o conceito de valorizações de um corpo K, que nos ajudará na compreensão da apresentação de corpos com um valor absoluto não-arquimediano.

2.1 Valorização

Nesta seção, estudaremos as valorizações de um corpo K e suas principais propriedades, estabeleceremos uma bijeção entre os valores absolutos não-arquimedianos em K e as valorizações de K e caracterizaremos as valorizações de $\mathbb{Q}$.

Sejam K um corpo e $K^* = K\backslash\{0\}$.

Definição 2.1 *Uma valorização v de K é uma aplicação $v : K \to \mathbb{R} \cup \{\infty\}$ que satisfaz as seguintes condições:*

$(V.1)$ $v(x) = \infty \Leftrightarrow x = 0$;

$(V.2)$ $v(x+y) \geq \min\{v(x), v(y)\}$, $\forall\, x, y \in K$;

$(V.3)$ $v(xy) = v(x) + v(y)$, $\forall\, x, y \in K$;

onde convencionamos $a + \infty = \infty$ e $a < \infty$, para todo $a \in \mathbb{R}$.

Proposição 2.2 *Qualquer valorização v de K possui as seguintes propriedades:*

(i) $v(1) = 0$;

(ii) $v(x^{-1}) = -v(x)$, $\forall\, x \in K$, $x \neq 0$;

(iii) $v(-x) = v(x)$, $\forall\, x \in K$;

(iv) $v(x_1 + \cdots + x_n) \geq \min\{v(x_1), \ldots, v(x_n)\}$, $\forall\, x_1, \ldots, x_n \in K$.

Demonstração. (i): Segue do fato de que $1 \neq 0$ e $1 = 1 \,.\, 1$ em K e de $(V.3)$.

(ii): Segue do fato de que $x \,.\, x^{-1} = 1$, para todo $x \in K^*$, de $(V.3)$ e de (i).

(iii): Segue do fato de que $-x = (-1)\, x$, para todo $x \in K$, de $(V.3)$ e de (ii).

(iv): Segue de $(V.2)$, por indução sobre n. ∎

Exemplo 2.3 *A aplicação* $v : K \to \mathbb{R} \cup \{\infty\}$ *definida por*

$$v(x) = \begin{cases} 0, & se \quad x \neq 0 \\ \infty, & se \quad x = 0 \end{cases}$$

é a valorização trivial de K.

Exemplo 2.4 *Fixemos um número natural primo* p. *Então, dado* $x \in \mathbb{Q}$, $x \neq 0$, *podemos escrever*

$$x = p^{\gamma} \frac{m}{n}, \text{ onde } \gamma, m, n \in \mathbb{Z},\ n > 0 \text{ e } p \nmid mn.$$

A aplicação $v_p : \mathbb{Q} \to \mathbb{R} \cup \{\infty\}$ *definida por*

$$v_p(x) = \begin{cases} \gamma\ , & se \quad x \neq 0 \\ \infty, & se \quad x = 0 \end{cases}$$

é a valorização p-ádica de $\mathbb{Q}$.

Observação 2.5 *A valorização p-ádica de* $\mathbb{Q}$, *pelo teorema fundamental da aritmética, é claramente determinada por* $v_p(p) = 1$ *e* $v_p(q) = 0$, *para qualquer número natural primo* $q \neq p$.

Exemplo 2.6 *Seja* $p(x) \in K[x]$ *um polinômio mônico irredutível sobre* K. *Então, dada* $\phi(x) \in K(x)$, $\phi(x) \neq 0$, *podemos escrever*

$$\phi(x) = p(x)^{\gamma} \frac{f(x)}{g(x)}, \text{ onde } \gamma \in \mathbb{Z},\ f(x), g(x) \in K[x],\ g(x) \neq 0,\ e\ p(x) \nmid f(x)g(x).$$

A aplicação $v_{p(x)} : K(x) \to \mathbb{R} \cup \{\infty\}$ *definida por*

$$v_{p(x)}(\phi(x)) = \begin{cases} \gamma, & se \quad \phi(x) \neq 0 \\ \infty, & se \quad \phi(x) = 0 \end{cases}$$

é a valorização p(x)-ádica de $K(x)$.

Exemplo 2.7 *A aplicação* $v_\infty : K(x) \to \mathbb{R} \cup \{\infty\}$ *definida por*

$$v_\infty\left(\frac{f(x)}{g(x)}\right) = \begin{cases} grau\, g(x) - grau\, f(x), & se \quad \dfrac{f(x)}{g(x)} \neq 0 \\ \\ \infty \qquad\qquad\quad , & se \quad \dfrac{f(x)}{g(x)} = 0 \end{cases}$$

é uma valorização de $K(x)$.

Proposição 2.8 *Existe uma correspondência bijetora entre as valorizações* v *de* K *e os valores absolutos não-arquimedianos* $|\ |$ *em* K.

Demonstração. Primeiramente, convencionamos $e^{-\infty} = 0$ e $-\ln\ 0 = \infty$.

Seja v uma valorização de K. Consideremos, então, a função $|\ | : K \to \mathbb{R}$ definida por $|x| = e^{-v(x)}$, para todo $x \in K$.

Afirmamos que $|\ |$ é um valor absoluto não-arquimediano em K.

De fato, para quaisquer $x, y \in K$, temos que:

$(A.1)$ $|x| = 0 \Leftrightarrow e^{-v(x)} = 0 \Leftrightarrow v(x) = \infty \Leftrightarrow x = 0$;

$(A.2)$

$$\begin{aligned} |x+y| = e^{-v(x+y)} &\leq e^{-\min\{v(x),v(y)\}} = e^{\max\{-v(x),-v(y)\}} \\ &= \max\{e^{-v(x)}, e^{-v(y)}\} = \max\{|x|,|y|\}; \end{aligned}$$

$(A.3)$ $|xy| = e^{-v(xy)} = e^{-(v(x)+v(y))} = e^{-v(x)-v(y)} = e^{-v(x)}e^{-v(y)} = |x||y|$;

Logo, $|\ |$ é um valor absoluto não-arquimediano em K.

Reciprocamente, seja $|\ |$ um valor absoluto não-arquimediano em K. Consideremos, então, a aplicação $v : K \to \mathbb{R} \cup \{\infty\}$ definida por

$$v(x) = \begin{cases} -\ln|x|, & \text{se} \quad x \neq 0 \\ \infty \quad , & \text{se} \quad x = 0 \end{cases}$$

Afirmamos que v é uma valorização de K.

De fato,

$(V.1)$ $v(x) = \infty \Leftrightarrow -\ln|x| = \infty \Leftrightarrow x = 0$, $\forall\, x \in K$.

$(V.2)$ Sejam $x, y \in K^*$ tais que $x + y \neq 0$. Então,

$$\begin{aligned} v(x+y) &= -\ln|x+y| = \ln|x+y|^{-1} \geq \ln(\max\{|x|,|y|\})^{-1} \\ &= \ln(\min\{|x|^{-1}, |y|^{-1}\}) = \min\{\ln|x|^{-1}, \ln|y|^{-1}\} \\ &= \min\{-\ln|x|, -\ln|y|\} = \min\{v(x), v(y)\}. \end{aligned}$$

É claro que, para os demais casos, a desigualdade acima é verdadeira.

$(V.3)$ Sejam $x, y \in K$ tais que $xy \neq 0$. Então,

$$v(xy) = -\ln|xy| = -\ln(|x||y|) = -\ln|x| - \ln|y| = v(x) + v(y).$$

É claro que, para o caso $xy = 0$, a igualdade acima é verdadeira.

Portanto, v é uma valorização de K. ■

Exemplo 2.9 *A valorização trivial de K corresponde ao valor absoluto trivial em K.*

Exemplo 2.10 *Com as notações do exemplo* 1.6*, a valorização de $\mathbb{Q}$ correspondente ao valor absoluto p-ádico em $\mathbb{Q}$ é dada por*

$$v(x) = \begin{cases} \gamma\, \ln p, & se \quad x \neq 0 \\ \infty \quad , & se \quad x = 0 \end{cases}$$

Exemplo 2.11 *A valorização de $K(x)$ correspondente ao valor absoluto não-arquimediano em $K(x)$, definido no exemplo* 1.9*, é dada por*

$$v\left(\frac{f(x)}{g(x)}\right) = \begin{cases} (grau\, g(x) - grau\, f(x))\, \ln 2, & se \quad \dfrac{f(x)}{g(x)} \neq 0 \\ \\ \infty \qquad\qquad\qquad , & se \quad \dfrac{f(x)}{g(x)} = 0 \end{cases}$$

Proposição 2.12 *Seja v uma valorização de K e sejam $x, y \in K$. Então,*

$$v(x) \neq v(y) \Rightarrow v(x+y) = \min\{v(x), v(y)\}.$$

Demonstração. Seja $|\ |$ o valor absoluto não-arquimediano em K correspondente a v e sejam $x, y \in K$ tais que $v(x) \neq v(y)$. Se $x = 0$ ou $y = 0$, então a igualdade segue imediatamente. Suponhamos, então, que $x \neq 0$ e $y \neq 0$. Daí, $x + y \neq 0$ (pois, caso contrário, $v(x) = v(-y) = v(y)$, contradizendo a hipótese). Logo, $v(x + y) = -\ln|x + y| \neq \infty$. Como $v(x) \neq v(y)$, temos que $-\ln|x| \neq -\ln|y|$ e, daí, $|x| \neq |y|$. Assim, como $|\ |$ é não-arquimediano, segue que $|x + y| = \max\{|x|, |y|\}$. Daí,

$$\begin{aligned} v(x+y) &= -\ln|x+y| = \ln|x+y|^{-1} = \ln(\max\{|x|,|y|\})^{-1} \\ &= \ln(\min\{|x|^{-1}, |y|^{-1}\}) = \min\{\ln|x|^{-1}, \ln|y|^{-1}\} \\ &= \min\{-\ln|x|, -\ln|y|\} = \min\{v(x), v(y)\}. \end{aligned}$$

■

Observação 2.13 (1) *Segue da proposição anterior que, se v é uma valorização de K e $x_1, \ldots, x_n \in K$ são tais que $v(x_i) \neq v(x_j)$, para todo $i, j = 1, \ldots, n$, $i \neq j$, então*

$$v(x_1 + \cdots + x_n) = \min\{v(x_1), \ldots, v(x_n)\}.$$

(2) *Seja v uma valorização de K e sejam $x, y \in K$ tais que $v(x - y) > 0$ e $v(x) = 0$. Então, $v(y) = 0$.*

De fato, suponhamos, por absurdo, que $v(y) \neq 0$. Então,

$$v(x - y) = \min\{v(x), v(y)\} = \min\{0, v(y)\}.$$

Se $v(y) > 0$, então $v(x - y) = 0$; se $v(y) < 0$, então $v(x - y) = v(y) < 0$. Em ambos os casos, chegamos a um absurdo. Portanto, $v(y) = 0$.

Proposição 2.14 ***(Princípio da dominação)*** *Seja v uma valorização de K e sejam $x_1, \ldots, x_n \in K$. Se $x_1 + \cdots + x_n = 0$, então pelo menos dois dos valores $v(x_i)$ são iguais.*

Demonstração. Suponhamos, por contradição, que os valores $v(x_i)$ são todos distintos. Reenumeramos os x_i's de modo que $v(x_1) < v(x_2) < \cdots < v(x_n)$. Então,

$$v(x_1) < \min\{v(x_2), \ldots, v(x_n)\} = v(x_2).$$

Por outro lado, como $v(x_1) = v(-x_1)$, temos que

$$v(x_1) = v(-x_1) = v(x_2 + \cdots + x_n) \geq \min\{v(x_2), \ldots, v(x_n)\} = v(x_2),$$

o que é uma contradição. ■

Definição 2.15 *Seja v uma valorização de K. A imagem $v(K^*)$ é um subgrupo de $\mathbb{R}$ chamado grupo de valores e é denotado por Γ_v. O corpo K com valorização $v : K^* \to \Gamma_v$, onde Γ_v é um subgrupo de $\mathbb{R}$, é chamado corpo valorizado.*

Sejam $|\ |_1$ e $|\ |_2$ dois valores absolutos não-arquimedianos equivalentes em K. Então, existe um número real positivo γ tal que $|x|_2 = |x|_1^{\gamma}$, para todo $x \in K$. Sejam $v : K^* \to \Gamma_v$ e $w : K^* \to \Gamma_w$ as valorizações correspondentes a $|\ |_2$ e $|\ |_1$, respectivamente. Então,

$$v(x) = -\ln|x|_2 = -\gamma \ln|x|_1 = \gamma\, w(x), \text{ para todo } x \in K^*.$$

As considerações acima motivam a seguinte definição.

Definição 2.16 *Sejam v e w duas valorizações de K. Dizemos que v e w são equivalentes se, e somente se, $v = \gamma w$, para algum número real positivo γ. Caso contrário, v e w são ditas não-equivalentes.*

Observação 2.17 *Segue da proposição* 2.8 *que duas valorizações de K são equivalentes se, e somente se, os correspondentes valores absolutos não-arquimedianos em K são equivalentes.*

A proposição que segue caracteriza as valorizações equivalentes de K.

Proposição 2.18 *Duas valorizações v e w de K são equivalentes se, e somente se, existe um isomorfismo que preserva a ordem $\phi : \Gamma_v \to \Gamma_w$ tal que $w = \phi \circ v$.*

Demonstração. ($:\Rightarrow$) Sejam v e w duas valorizações equivalentes de K. Então, existe um número real positivo γ tal que $v(x) = \gamma w(x)$, para todo $x \in K^*$. Daí, $w(x) = \dfrac{1}{\gamma}\, v(x)$, para todo $x \in K^*$.

Consideremos a aplicação $\phi : \Gamma_v \to \Gamma_w$ definida por $\phi(a) = \dfrac{1}{\gamma}\, a$, para todo $a \in \Gamma_v$. É claro que ϕ é um isomorfismo que preserva a ordem. Ainda,

$$(\phi \circ v)(x) = \phi(v(x)) = \frac{1}{\gamma}\, v(x) = w(x), \text{ para todo } x \in K^*.$$

($\Leftarrow:$) Seja $\phi : \Gamma_v \to \Gamma_w$ um isomorfismo que preserva a ordem e tal que $w = \phi \circ v$.

Como Γ_v e Γ_w são subgrupos aditivos de $\mathbb{R}$, então ambos são triviais, ou discretos ou são densos em $\mathbb{R}$. No primeiro caso, v e w são triviais; no segundo, $\Gamma_v = \lambda_1\mathbb{Z}$ e $\Gamma_w = \lambda_2\mathbb{Z}$, para λ_1, λ_2 números reais positivos e, no terceiro caso, ϕ se estende a um isomorfismo $\phi : \mathbb{R} \to \mathbb{R}$. Então, em qualquer dos casos, $\phi(a) = \gamma a$, para algum número real positivo γ. Daí,

$$w(x) = (\phi \circ v)(x) = \phi(v(x)) = \gamma\, v(x) \Rightarrow v(x) = \frac{1}{\gamma} w(x), \text{ para todo } x \in K^*.$$

Portanto, v e w são duas valorizações equivalentes de K. ∎

Exemplo 2.19 *A valorização p-ádica e a valorização v dada no exemplo* 2.10 *são valorizações equivalentes de $\mathbb{Q}$ e $\Gamma_{v_p} = \mathbb{Z} \cong (\ln p)\mathbb{Z} = \Gamma_v$.*

Exemplo 2.20 *A valorização v_∞ de dada no exemplo* 2.7 *e a valorização v do exemplo* 2.11 *são valorizações equivalentes de $K(x)$ com $\Gamma_{v_\infty} = \mathbb{Z} \cong (\ln 2)\mathbb{Z} = \Gamma_v$.*

Teorema 2.21 ***(Teorema da aproximação para valorizações)*** *Sejam $v_1, \ldots, v_r$ valorizações não-triviais de K duas a duas não-equivalentes. Então, para quaisquer $\alpha_1, \ldots, \alpha_r \in K$ e $N > 0$, existe $\alpha \in K$ tal que*

$$v_i(\alpha - \alpha_i) > N,\ i = 1, \ldots, r.$$

Demonstração. Pela proposição 2.8, existem valores absolutos não-arquime-dianos não-triviais $|\ |_1, \ldots, |\ |_r$ em K correspondentes às valorizações $v_1, \ldots, v_r$ de K, respectivamente. Como $v_1, \ldots, v_r$ são duas a duas não-equivalentes, segue, da observação 2.17, que $|\ |_1, \ldots, |\ |_r$ são dois a dois não-equivalentes. Logo, pelo teorema 1.28, dados $\alpha_1, \ldots, \alpha_r \in K$ e $e^{-N} > 0$, existe $\alpha \in K$ tal que

$$|\alpha - \alpha_i|_i < e^{-N},\ i = 1, \ldots, r.$$

Segue da demonstração da proposição 2.8 que

$$v_i(\alpha - \alpha_i) > N,\ i = 1, \ldots, r.$$

∎

Proposição 2.22 *Qualquer valorização de $\mathbb{Q}$ é trivial ou é equivalente a uma valorização p-ádica de $\mathbb{Q}$, para algum número natural primo p.*

Demonstração. Seja v uma valorização não-trivial de $\mathbb{Q}$ e seja $|\ |$ o valor absoluto não-arquimediano não-trivial em $\mathbb{Q}$ correspondente a v. Pelo teorema 1.31, temos que $|\ |$ é equivalente a um valor absoluto p-ádico em $\mathbb{Q}$, para algum número natural primo p. Segue da observação 2.17, que v é equivalente à valorização p-ádica de $\mathbb{Q}$. ∎

Antes de apresentarmos mais algumas propriedades de valorizações de K, recordaremos alguns resultados importantes de Álgebra Comutativa [Atyah, Mac. Donald].

Teorema 2.23 *Todo anel V, comutativo com unidade, tem pelo menos um ideal maximal.*

Demonstração. Seja $\sum$ o conjunto de todos os ideais $J \subseteq V$, $J \neq V$. Temos que $\sum$ é parcialmente ordenado pela inclusão e $\sum \neq \varnothing$, visto que $0 \in \sum$. Seja (I_α) um subconjunto de $\sum$ totalmente ordenado pela inclusão. Consideremos a união $I = \bigcup_\alpha I_\alpha$.

Afirmamos que I é um ideal de V e $I \neq V$.

Com efeito, sejam $x, y \in I$. Então, $x \in I_\alpha$ para algum α e $y \in I_\beta$ para algum β. Suponhamos que $I_\beta \subseteq I_\alpha$. Então, $x, y \in I_\alpha$ e como I_α é um ideal, temos $x + y \in I_\alpha$. Daí, $x + y \in I$. Dado $a \in V$, temos que $ax \in I_\alpha$, visto que $x \in I_\alpha$ e I_α é um ideal. Logo, $ax \in I$. Portanto, I é um ideal de V.

Como $1 \notin I_\alpha$, para todo α (pois $I_\alpha \neq V$, para todo α), segue que $1 \notin I$.
Assim, I é um ideal de V, $I \neq V$, e $I_\alpha \subset I$, para todo α. Logo, I é o elemento maximal de (I_α). Segue do lema de Zorn que o conjunto $\sum$ tem elemento maximal. ∎

Corolário 2.24 *Se $I \neq V$ é um ideal do anel V, comutativo com unidade, então existe um ideal maximal de V contendo I.*

Demonstração. Como I é um ideal de V e $I \neq V$, temos que o anel quociente $V/I \neq 0$. Logo, pelo teorema anterior, V/I tem pelo menos um ideal maximal. Portanto, V possui um ideal maximal contendo I. ∎

Corolário 2.25 *Todo elemento não-invertível do anel V, comutativo com unidade, está contido em um ideal maximal de V.*

Demonstração. Seja $x \in V$ um elemento não-invertível, então $(x) \neq V$. Assim, pelo corolário anterior, existe um ideal maximal M de V contendo (x). Em particular, $x \in M$. ∎

Definição 2.26 *Um anel V, comutativo com unidade, que possui exatamente um ideal maximal M é chamado anel local. O corpo V/M é chamado corpo residual de V.*

Proposição 2.27 *Seja V um anel comutativo com unidade e seja $M \neq V$ um ideal de V tal que todo elemento $x \in V \backslash M$ é invertível em V. Então, V é um anel local e M é seu ideal maximal.*

Demonstração. Todo ideal I de V com $I \neq V$ consiste de elementos não-invertíveis de V. Logo, todo ideal I de V com $I \neq V$ está contido no ideal M. Portanto, M é o único ideal maximal de V. ∎

Agora, retornaremos ao estudo das valorizações de K, apresentando a definição de um anel de valorização de K e algumas de suas propriedades.

Definição 2.28 *Um subanel V de K é chamado anel de valorização de K se, e somente se, para qualquer $x \in K^*$, $x \in V$ ou $x^{-1} \in V$.*

Proposição 2.29 *Se V é um anel de valorização de K, então K é o corpo de frações de V.*

Demonstração. Seja F o corpo de frações de V. É claro que $F \subseteq K$. Dado $x \in K, x \notin V$, temos que

$$x^{-1} \in V \Rightarrow x^{-1} = a \in V,\ a \neq 0 \Rightarrow \frac{1}{x} = a \Rightarrow x = \frac{1}{a} \in F.$$

■

Proposição 2.30 *Se V é um anel de valorização de K, então V é um anel local.*

Demonstração. Seja M o conjunto de todos os elementos não-invertíveis de V. Então,

$$x \in M \Rightarrow x = 0 \text{ ou } x^{-1} \notin V.$$

Mostremos, primeramente, que M é um ideal de V.

Sejam $a \in V$ e $x, y \in M$. Se $a = 0$ ou $x = 0$, então $ax = 0 \in M$. No caso $a \neq 0$ e $x \neq 0$, suponhamos que $ax \notin M$. Então, $(ax)^{-1} \in V$. Daí, $x^{-1} = (ax)^{-1}a \in V$, o que é um absurdo. Portanto, $ax \in M$. Por outro lado, se $x = 0$ ou $y = 0$, é claro que $x + y \in M$. Suponhamos que $x \neq 0$ e $y \neq 0$. Temos que $xy^{-1} \in V$ ou $x^{-1}y \in V$. Se $xy^{-1} \in V$, então $x + y = (1 + xy^{-1})y \in VM \subseteq M$; se $x^{-1}y \in V$, então analogamente obtemos $x + y \in M$. Segue da proposicão 2.27, que V é um anel local e M é o seu ideal maximal. ■

Proposição 2.31 *Seja v uma valorização de K. Então,*

(i) $O_v = \{x \in K \mid v(x) \geq 0\}$ *é um anel de valorização de K.*

(ii) $M_v = \{x \in K \mid v(x) > 0\}$ *é o único ideal maximal de O_v.*

(iii) $U_v = O_v \backslash M_v$ *é o grupo multiplicativo de todos os elementos invertíveis de O_v.*

(iv) *v é trivial* $\Leftrightarrow O_v = K \Leftrightarrow M_v = \{0\} \Leftrightarrow U_v = K^*$.

Demonstração. (i): Sejam $x, y \in O_v$. Então, $v(x) \geq 0$ e $v(y) \geq 0$. Daí,

$$v(x + y) \geq \min\{v(x), v(y)\} \geq 0 \text{ e } v(xy) = v(x) + v(y) \geq 0.$$

Logo, $x + y \in O_v$ e $xy \in O_v$. Como $v(0) = \infty > 0$, $v(1) = 0$ e $v(-x) = v(x) \geq 0$, temos que $0, 1, -x \in O_v$. Portanto, O_v é um subanel de K.

Dado $x \in K^*$, temos que ou $v(x) \geq 0$ ou $v(x) < 0$. Se $v(x) \geq 0$, então $x \in O_v$; se $v(x) < 0$, então $v(x^{-1}) = -v(x) > 0$ e, daí, $x^{-1} \in O_v$.

(ii): Dado $x \in O_v$, $x \neq 0$, temos que x é invertível em O_v se, e somente se, $v(x) = 0$ (pois $v(x^{-1}) = -v(x)$, para todo $x \in K^*$). Daí, M_v é constituído por todos os elementos não-invertíveis de O_v. Pela demonstração da proposição anterior, segue que M_v é o único ideal maximal de O_v.

(iii) e (iv) São imediatas. ■

Denotaremos por K_v o corpo residual de O_v, isto é, $K_v = O_v/M_v$, e por $\kappa_v : O_v \to K_v$ o homomorfismo canônico de O_v em K_v.

Observação 2.32 *As seguintes afirmações são imediatas:*

(1) *Sejam v e w duas valorizações de K. Então, v e w são equivalentes se, e somente se, $O_v = O_w$. Neste caso, $K_v = K_w$ e $\kappa_v = \kappa_w$.*

(2) *Para quaisquer $x, y \in O_v$, temos*

$$v(x-y) > 0 \Leftrightarrow x - y \in M_v \Leftrightarrow \kappa_v(x-y) = 0 \Leftrightarrow \kappa_v(x) = \kappa_v(y).$$

(3) *Seja K_0 um subcorpo de K. Então,*

$$v|_{K_0} \text{ é trivial} \Leftrightarrow K_0 \subseteq O_v \Leftrightarrow K_0 \cap M_v = \{0\}.$$

Neste caso, a restrição de κ_v a K_0 é um homomorfismo injetor.

Proposição 2.33 *Seja v uma valorização de K. As seguintes afirmações são equivalentes:*

(*i*) $car\, K_v \neq car\, K$.

(*ii*) *A restrição de v ao corpo primo de K é não-trivial.*

(*iii*) *Para algum número natural primo p e para algum número real positivo γ, existe uma inclusão $(\mathbb{Q}, \gamma\, v_p) \to (K, v)$.*

Neste caso, $car\, K = 0$ e $car\, K_v = p$.

Demonstração. (*i*) $\Rightarrow$ (*ii*): Segue de (3) na observação anterior.

(*ii*) $\Rightarrow$ (*iii*): Pela proposição 1.14, o corpo primo de K não é finito, logo existe um isomorfismo ϕ de $\mathbb{Q}$ no corpo primo de K e, pela proposição 2.22, $v \circ \phi = \gamma\, v_p$, para algum número natural primo p e para algum número real positivo γ. Logo, $(\mathbb{Q}, \gamma\, v_p) \to (K, v)$ é uma inclusão.

(*iii*) $\Rightarrow$ (*i*) Temos que $car\, K = car\, \mathbb{Q} = 0$. Como

$$v(p.1) = v(\phi(p)) = \gamma\, v_p(p) > 0,$$

segue que $p\, \kappa_v(1) = \kappa_v(p.1) = 0$. Logo, $car\, K_v = p$.

■

Antes de apresentarmos exemplos de anéis de valorizações, introduziremos o conceito de valorização discreta, visto que a maioria das valorizações aqui já apresentadas se constituem exemplos de valorizações discretas.

2.2 Valorização discreta

Definição 2.34 *Uma valorização v de um corpo K é dita valorização discreta se, e somente se, v é não-trivial e seu grupo de valores Γ_v é um subespaço discreto de $\mathbb{R}$ (de acordo com a topologia usual).*

A seguinte proposição caracteriza as valorizações discretas de um corpo K.

Proposição 2.35 *Seja Γ um subgrupo não-trivial de $\mathbb{R}$. As seguintes afirmações são equivalentes:*

(*i*) Γ *é um subespaço discreto de $\mathbb{R}$.*

(*ii*) Γ *não é denso em $\mathbb{R}$.*

(*iii*) *O conjunto $\{\gamma \in \Gamma\,;\, \gamma > 0\}$ tem um elemento mínimo.*

(*iv*) $\Gamma = \rho\mathbb{Z}$, *para algum número real positivo ρ.*

Demonstração. $(i) \Rightarrow (ii)$: É imediato.

$(ii) \Rightarrow (iii)$: Suponhamos que o conjunto $\{\gamma \in \Gamma\,;\, \gamma > 0\}$ não possui um elemento mínimo. Então, dado $\epsilon > 0$, existe $\gamma \in \Gamma$ tal que $0 < \gamma \leq \epsilon$ e, para todo $\rho \in \mathbb{R}$, existe $n \in \mathbb{Z}$ tal que $n\gamma \leq \rho < (n+1)\gamma$. Daí,

$$0 \leq \rho - n\gamma < \gamma \leq \epsilon \Rightarrow \rho < \gamma + n\gamma < \epsilon + n\gamma,$$

onde $\gamma + n\gamma \in \Gamma$. Portanto, Γ é denso em $\mathbb{R}$.

$(iii) \Rightarrow (iv)$: Suponhamos que o conjunto $\{\gamma \in \Gamma\,;\, \gamma > 0\}$ tem um elemento mínimo, digamos γ_0. Como Γ é um subgrupo (aditivo) de $\mathbb{R}$ e $\gamma_0 \in \Gamma$, segue que todo múltiplo inteiro de γ_0 pertence a Γ. Logo, $\gamma_0\mathbb{Z} \subseteq \Gamma$. Por outro lado, dado $\gamma \in \Gamma$, existe $n \in \mathbb{Z}$ tal que $n\gamma_0 \leq \gamma < (n+1)\gamma_0$. Daí, $0 \leq \gamma - n\gamma_0 < \gamma_0$. Como $\gamma, n\gamma_0 \in \Gamma$, segue que $\gamma - n\gamma_0 \in \Gamma$. Mas γ_0 é o elemento mínimo positivo de Γ. Logo, $\gamma - n\gamma_0 = 0$, ou seja, $\gamma = n\gamma_0$. Portanto, $\Gamma \subseteq \gamma_0\mathbb{Z}$. Tomando $\rho = \gamma_0$, obtemos $\Gamma = \rho\mathbb{Z}$.

$(iv) \Rightarrow (i)$: Suponhamos que $\Gamma = \rho\mathbb{Z}$, para algum número real positivo ρ. Dado qualquer $\gamma \in \Gamma$, temos que $(\gamma - \rho, \gamma + \rho) \cap \Gamma = \{\gamma\}$. Portanto, Γ é um subespaço discreto de $\mathbb{R}$. ∎

Exemplo 2.36 *A valorização p-ádica e a valorização dada no exemplo* 2.10 *são valorizações discretas equivalentes de* $\mathbb{Q}$.

Exemplo 2.37 *A valorização* v_∞ *e a valorização dada no exemplo* 2.11 *são valorizações discretas equivalentes de* $K(x)$.

Definição 2.38 *Seja* K *um corpo e seja* v *uma valorização discreta de* K *com* $\Gamma_v = \rho\mathbb{Z}$, *para algum* $\rho > 0$. *Então,* $\pi \in K$ *é uma* uniformizante local *de* v *se, e somente se,* $v(\pi) = \rho$.

Exemplo 2.39 *Seja* $v_{p(x)}$ *a valorização* $p(x)$*-ádica de* $K(x)$. *Então,* $p(x)$ *é uma uniformizante local de* $v_{p(x)}$ *e, para qualquer* $a \in K$, $a \neq 0$, $ap(x)$ *é uma uniformizante local de* $v_{p(x)}$.

Observação 2.40 *Se* v *é uma valorização discreta do corpo* K *com* $\Gamma_v = \rho\mathbb{Z}$ *e* π *é uma uniformizante local de* v, *então, para qualquer* $u \in U_v$, $u\pi$ *é uma uniformizante de* v.

Com efeito, dado $u \in U_v$, *temos que* $v(u) = 0$. *Logo,* $v(u\pi) = v(u) + v(\pi) = v(\pi) = \rho$.

Definição 2.41 *Uma valorização discreta* v *de um corpo* K *é dita* valorização normalizada *de* K *se, e somente se,* $\Gamma_v = \mathbb{Z}$.

Exemplo 2.42 *A valorização p-ádica de* $\mathbb{Q}$ *e a valorização* v_∞ *de* $K(x)$ *são valorizações normalizadas.*

Observação 2.43 *Segue da proposição* 2.35, *que toda valorização discreta é equivalente a exatamente uma valorização normalizada.*

Proposição 2.44 *Sejam* K *um corpo e* $K^* = K\backslash\{0\}$ *e seja* $v : K^* \to \Gamma_v = \mathbb{Z}$ *uma valorização discreta de* K. *Então,*

(i) O_v *é um anel de valorização principal, onde o ideal maximal é* $M_v = (\pi)$, *com* π *uma uniformizante local de* v, *os ideais não-nulos são da forma* $M_v^n = (\pi^n)$, *para* $n \geq 0$, *e* $\cap M_v^n = \{0\}$.

(ii) *Cada* $x \in K^*$ *se escreve de modo único como* $x = \pi^r u$, *onde* $r \in \mathbb{Z}$ *e* $u \in U_v$.

Demonstração. (i): Segue da proposição 2.31 que $M_v = \{x \in K;\, v(x) \geq 1\}$ e $M_v = (\pi)$, onde π é uma uniformizante local de v.

Seja I um ideal não-nulo de O_v e consideremos $S = \{v(x);\, x \in I, x \neq 0\} \subseteq \mathbb{N}$. Como $S \neq \varnothing$, S tem um menor elemento, digamos $n = v(x_0)$, onde $x_0 \in I\backslash\{0\}$.

Afirmamos que $I = (x_0)$.

De fato, é claro que $(x_0) \subseteq I$. Seja $x \in I$. Pela escolha de x_0, $v(x) \geq v(x_0)$. Então, $v\Big(\dfrac{x}{x_0}\Big) \geq 0$, isto é, $\dfrac{x}{x_0} \in O_v$. Logo, $x \in (x_0)$. Logo, $I = (x_0)$. Além disso, como $v(x_0) = v(\pi^n)$, temos que $x_0 = u\pi^n$, para algum $u \in U_v$. Portanto, $I = (\pi^n)$.

É claro que $\cap M_v^n = \{0\}$:

$$x \in \cap M_v^n \Leftrightarrow x \in M_v^n, \forall\, n \Leftrightarrow v(x) \geq n, \forall\, n \Leftrightarrow v(x) = \infty \Leftrightarrow x = 0.$$

(ii): Dado $x \in K^*$, seja $r = v(x)$. Então, $v(x) = v(\pi^r)$ e, daí, $\dfrac{x}{\pi^r} \in U_v$. Logo, $x = \pi^r u$, onde u é invertível em O_v. ∎

Como valorizações equivalentes são essencialmente iguais, segue da observação anterior que o estudo das valorizações discretas de um corpo K pode ser reduzido ao estudo das valorizações discretas normalizadas de K.

A proposição 2.22 nos diz que qualquer valorização não-trivial de $\mathbb{Q}$ é equivalente a uma valorização p-ádica de $\mathbb{Q}$, para algum número natural primo p. O próximo teorema generaliza esta afirmação para qualquer corpo K que é corpo de frações de algum domínio principal. Mais geralmente, provaremos para qualquer corpo K que é corpo de frações de algum domínio de fatoração única.

Teorema 2.45 *Seja D um domínio de fatoração única com corpo de frações K e seja $\mathcal{P}$ um conjunto de representantes dos elementos irredutíveis de D (isto é, qualquer elemento irredutível de D é associado a exatamente um elemento de $\mathcal{P}$). Então,*

(i) Para qualquer $p \in \mathcal{P}$, a função $v_p : K \to \mathbb{R} \cup \{\infty\}$ definida por

$$v_p(0) = \infty \text{ e } v_p\Big(u \prod_{q \in \mathcal{P}} q^{n_q}\Big) = n_p, \text{ onde } n_q \in \mathbb{Z} \text{ e } u \text{ é invertível em } D,$$

é uma valorização normalizada de K, com

$$O_{v_p} = D_{pD} \supseteq D,\ M_{v_p} = pD_{pD},\ pD = M_{v_p} \cap D \text{ e } D/pD \cong \kappa_{v_p}(D) \subseteq K_{v_p},$$

onde $\kappa_{v_p} : O_{v_p} \to K_{v_p} = O_{v_p}/M_{v_p}$ é o homomorfismo canônico.

(ii) $D = \bigcap_{p \in \mathcal{P}} O_{v_p}$.

(iii) Para qualquer $x \in K$, $x \neq 0$, o conjunto $\{p \in \mathcal{P};\, v_p(x) \neq 0\}$ é finito.

(iv) Se D é um domínio principal, então $\kappa_{v_p}(D) = K_{v_p}$, para todo $p \in \mathcal{P}$, e qualquer valorização não-trivial v de K, tal que $O_v \supseteq D$, é equivalente a v_p para exatamente um elemento $p \in \mathcal{P}$ e é, portanto, discreta.

Demonstração. (ii) e (iii) seguem da fatoração única em D.

(i): A igualdade $O_{v_p} = D_{pD}$ segue da fatoração única em D e o anel local $D_{pD} \supseteq D$ tem ideal maximal pD_{pD}, com $pD = pD_{pD} \cap D$. Logo, $M_{v_p} = pD_{pD}$ e $M_{v_p} \cap D = pD$. Além disso, a inclusão $i : D \hookrightarrow D_{pD} = O_{v_p}$ induz o homomorfismo injetor $D/pD \to K_v = O_{v_p}/M_{v_p}$, pois $M_{v_p} \cap D = pD$, de modo que o diagrama abaixo é comutativo.

$$\begin{array}{ccc} D & \hookrightarrow & D_{pD} = O_{v_p} \\ \downarrow & & \downarrow \\ D/pD & \to & O_{v_p}/M_{v_p} = K_{v_p} \end{array}$$

Portanto, $D_{pD} \cong \kappa_p(D) \subseteq K_{v_p}$.

(iv): Suponhamos que D é um domínio principal. Dado $y \in K_{v_p}$, temos que $y = \kappa_{v_p}(x)$, para algum $x \in O_{v_p}$. Como $O_{v_p} = D_{pD}$, por (i), segue que $x = ab^{-1}$, onde $a, b \in D$ e $b \notin pD$. Sejam, então, $c, d \in D$ tais que $cp + db = 1$. Temos que $cp = 1 - db$, donde $(ab^{-1})cp = ab^{-1} - ad$. Como $M_{v_p} = pD_{pD}$, por (i), segue que $(ab^{-1})cp = (acp)b^{-1} \in M_{v_p}$, isto é, $ab^{-1} - ad \in M_{v_p}$. Daí, $\kappa_{v_p}(ab^{-1}) = \kappa_{v_p}(ad) \in \kappa_{v_p}(D)$. Logo,

$$y = \kappa_{v_p}(x) = \kappa_{v_p}(ab^{-1}) \in \kappa_{v_p}(D).$$

Portanto, $K_{v_p} \subseteq \kappa_{v_p}(D)$. Como, por (i), $\kappa_{v_p}(D) \subseteq K_{v_p}$, segue que $\kappa_{v_p}(D) = K_{v_p}$.

Seja v uma valorização não-trivial de K tal que $O_v \supseteq D$. Então, $M_v \cap D$ é um ideal primo não-nulo de D, ou seja, $M_v \cap D = pD$, para algum $p \in \mathcal{P}$. Daí, $v(p) = \rho = \rho\, v_p(p)$, para algum número real positivo ρ. Por outro lado, dado $a \in D \backslash pD$, temos que $v(a) = 0 = \rho\, v_p(a)$.

Seja, então, $x \in K$, $x \neq 0$. Temos que $x = p^m ab^{-1}$, onde $m \in \mathbb{Z}$ e $a, b \in D \backslash pD$. Logo,

$$\begin{aligned} v(x) &= v(p^m ab^{-1}) = v(p^m) + v(ab^{-1}) = mv(p) + v(a) - v(b) \\ &= m(\rho v_p(p)) + \rho v_p(a) - \rho v_p(b) = \rho(m v_p(p)) + \rho v_p(ab^{-1}) \\ &= \rho(v_p(p^m) + v_p(ab^{-1})) = \rho(v_p(p^m ab^{-1})) = \rho v_p(x). \end{aligned}$$

Assim, temos que v é equivalente a v_p e, portanto, v é discreta. A unicidade de p segue do fato de que, para quaisquer $p, q \in \mathcal{P}$, $p \neq q$, as valorizações v_p e v_q são não-equivalentes. ∎

Uma primeira aplicação do teorema anterior é no caso em que $D = \mathbb{Z}$, $K = \mathbb{Q}$ e $\mathcal{P}$ é o conjunto dos números naturais primos. Assim, se p é um número natural primo qualquer, então a valorização p-ádica v_p de $\mathbb{Q}$ tem o anel de valorização $O_{v_p} = \mathbb{Z}_{p\mathbb{Z}}$, o ideal maximal $M_{v_p} = p\mathbb{Z}_{p\mathbb{Z}}$ e o corpo de classes residuais $K_{v_p} \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, isto é, K_{v_p} é isomorfo ao corpo primo de característica p.

Uma outra aplicação do teorema anterior é no caso em que $D = K_0[x]$, onde x é transcendente sobre o corpo K_0, $K = K_0(x)$ e $\mathcal{P}$ é o conjunto dos polinômios mônicos irredutíveis de $K_0[x]$. Como $D = K_0[x]$ é um domínio principal, segue que, para qualquer $p \in \mathcal{P}$, a função $v_p : K \to \mathbb{R} \cup \{\infty\}$ definida por

$$v_p(0) = \infty \text{ e } v_p\Big(u \prod_{q \in \mathcal{P}} q(x)^{n_q}\Big) = n_p, \text{ onde } n_q \in \mathbb{Z} \text{ e } u \in K_0,\ u \neq 0,$$

é uma valorização normalizada de $K|K_0$ tal que $O_{v_p} \supseteq D$ e qualquer valorização v de $K|K_0$ tal que $O_v \supseteq D$ é equivalente a v_p para algum $p \in \mathcal{P}$. Além dessas valorizações normalizadas de $K|K_0$, conhecemos também a valorização normalizada v_∞, apresentada no Exemplo 2.7. Considerando esta última, obtemos o resultado que segue.

Corolário 2.46 *Seja $K = K_0(x)$ uma extensão transcendente do corpo K_0. Então,*

(i) Qualquer valorização não-trivial de $K|K_0$ é equivalente a v_p para exatamente um $p \in \mathcal{P} \cup \{\infty\}$ e é, portanto, discreta. Em particular, $p \mapsto v_p$ é uma bijeção do conjunto $\mathcal{P} \cup \{\infty\}$ no conjunto das valorizações normalizadas de $K|K_0$.

(ii) $\displaystyle\bigcap_{p \in \mathcal{P} \cup \{\infty\}} O_{v_p} = K_0.$

(iii) Para qualquer $p \in \mathcal{P} \cup \{\infty\}$, o corpo residual $K_{v_p} = O_{v_p}/M_{v_p}$ é uma extensão simples da imagem isomorfa $\kappa_{v_p}(K_0)$ de K_0,

$$[K_{v_p} : k_{v_p}(K_0)] = grau\, p,\ p \in \mathcal{P},\ e\ [K_{v_\infty} : \kappa_{v_\infty}(K_0)] = grau\, \infty = 1.$$

(*iv*) *Para qualquer* $\varphi \in K$, *o conjunto* $\{p \in \mathcal{P} \cup \{\infty\};\ v_p(\varphi) \neq 0\}$ *é finito e*

$$\sum_{p \in \mathcal{P} \cup \{\infty\}} v_p(\varphi)\, grau\, p = 0.$$

Demonstração. (*i*): Seja v uma valorização não-trivial de $K|K_0$. Então, ou $O_v \supseteq K_0[x]$ ou $O_v \not\supseteq K_0[x]$. Se $O_v \supseteq K_0[x]$, então, pelo teorema anterior, v é equivalente a v_p para exatamente um $p \in \mathcal{P}$ e é, portanto, discreta. Se $O_v \not\supseteq K_0[x]$, afirmamos que v é equivalente a v_∞ e, portanto, discreta. Com efeito, se $O_v \not\supseteq K_0[x]$, então $x \notin O_v$. Daí, $v(x) = -\rho$, para algum número real positivo ρ. Dado $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K_0[x]$, $a_n \neq 0$, temos que $v(a_i x^i) \neq v(a_j x^j)$, para quaisquer $i, j = 0, 1, \ldots, n$, $i \neq j$, e, ainda,

$$\min_i \{v(a_i x^i)\} = v(a_n x^n) = -n\rho.$$

Segue que $v(p(x)) = -n\rho = \rho\, v_\infty(p(x))$. Assim, para qualquer $\dfrac{f(x)}{g(x)} \in K$, $\dfrac{f(x)}{g(x)} \neq 0$, obtemos

$$\begin{aligned} v\left(\frac{f(x)}{g(x)}\right) &= v(f(x)g(x)^{-1}) = v(f(x)) - v(g(x)) \\ &= \rho\, v_\infty(f(x)) - \rho\, v_\infty(g(x)) \\ &= \rho(v_\infty(f(x)g(x)^{-1})) \\ &= \rho\left(v_\infty\left(\frac{f(x)}{g(x)}\right)\right). \end{aligned}$$

(*ii*): Pelo teorema anterior, temos que $K_0[x] = \bigcap_{p \in \mathcal{P}} O_{v_p}$. Logo, $\bigcap_{p \in \mathcal{P} \cup \{\infty\}} O_{v_p} = K_0[x] \cap O_{v_\infty}$. Portanto, $\bigcap_{p \in \mathcal{P} \cup \{\infty\}} O_{v_p} = K_0$.

(*iii*): Dado $p \in \mathcal{P}$, temos que v_p restrita a K_0 é a valorização trivial, logo $K_0 \subseteq O_{v_p} \backslash M_{v_p} = U_v$ e κ_p restrita a K_0 é um homomorfismo de corpos e, portanto, injetor. Logo, $K_0 \cong \kappa_{v_p}(K_0)$ e, pelo teorema anterior, que $K_{v_p} = \kappa_{v_p}(K_0[x])$. Logo, $K_{v_p} = \kappa_{v_p}(K_0)[\zeta]$, onde $\zeta = \kappa_{v_p}(x)$. Além disso, como $\kappa_{v_p}(p)$ é o polinômio mínimo de ζ sobre $\kappa_{v_p}(K_0)$, obtemos

$$[K_{v_p} : \kappa_{v_p}(K_0)] = [\kappa_{v_p}(K_0)[\zeta] : \kappa_{v_p}(K_0)] = \text{grau}\, \kappa_{v_p}(p) = \text{grau}\, p.$$

Nesse caso, $K_{v_p} \cong K_0[x]/(p(x))$.

Se $p = \infty$, então afirmamos que $v_\infty = v_q$, onde $q(y) = y$, com $y = x^{-1}$.

Com efeito, dado $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in K_0[x]$, $a_n \neq 0$, escrevemos $f(y) = a_n y^{-n} + a_{n-1}y^{-(n-1)} + \cdots + a_1 y^{-1} + a_0 \in K_0[y]$. Como $v_q(a_i y^{-i}) \neq v_q(a_j y^{-j})$, para quaisquer $i, j = 0, 1, \ldots, n$, $i \neq j$, e

$$\min_i \{v_q(a_i y^{-i})\} = v_q(a_n y^{-n}) = -n,$$

segue que $v_q(f(y)) = -n = v_\infty(f(x))$. Assim, para qualquer $\dfrac{f(x)}{g(x)} \in K$, $\dfrac{f(x)}{g(x)} \neq 0$, obtemos

$$\begin{aligned} v_q\left(\frac{f(y)}{g(y)}\right) &= v_q(f(y)g(y)^{-1}) = v_q(f(y)) - v_q(g(y)) \\ &= v_\infty(f(x)) - v_\infty(g(x)) = v_\infty(f(x)g(x)^{-1}) \\ &= v_\infty\left(\frac{f(x)}{g(x)}\right). \end{aligned}$$

Logo, $\operatorname{grau} q = 1$ e, daí, $[K_{v_\infty} : \kappa_{v_\infty}(K_0)] = 1$ e $K_{v_\infty} = \kappa_{v_\infty}(K_0)$.

(iv) A primeira afirmação segue imediatamente do teorema anterior. Por outro lado, dado $q \in \mathcal{P}$, temos que $v_\infty(q) = -\operatorname{grau} q$ e

$$v_p(q) = \begin{cases} 1 \ , & \text{se} \quad p = q \\ 0 \ , & \text{se} \quad p \neq q \end{cases}$$

Portanto, se $\varphi(x) = \prod_{p \in \mathcal{P}} p(x)^{n_p} \in K_0[x]$, então

$$\sum_{p \in \mathcal{P}} v_p(\varphi) \operatorname{grau} p = \sum_{p \in \mathcal{P}} n_p \operatorname{grau} p = \operatorname{grau} \varphi(x) \text{ e } v_\infty(\varphi) = -\operatorname{grau} \varphi(x).$$

Assim, a igualdade vale em $K_0[x]$ e, portanto, vale em $K_0(x)$. ■

Capítulo 3

Completamento de corpos com valorizações discretas

Neste capítulo estudaremos basicamente o completamento de um corpo K com relação a uma valorização discreta de K e caracterizaremos seus elementos como séries de potências.

3.1 O corpo dos números p-ádicos ($\widehat{\mathbb{Q}}_p$)

Nesta seção, estudaremos primeiramente o completamento de $\mathbb{Q}$ com relação ao valor absoluto p-ádico, para um número natural primo p fixado, e mostraremos que os elementos deste podem ser representados por séries de potências.

Fixemos um número natural primo p.

Definição 3.1 *O corpo dos números p-ádicos é o completamento de $\mathbb{Q}$ com relação ao valor absoluto p-ádico $|\ |_p$ em $\mathbb{Q}$ e é denotado por $\widehat{\mathbb{Q}}_p$.*

Observação 3.2 *É importante observarmos que no processo de completamento de $\mathbb{Q}$ para $\mathbb{R}$ os valores possíveis do valor absoluto usual são ampliados para incluir todos os números reais não-negativos, enquanto que no processo de completamento de $\mathbb{Q}$ para $\widehat{\mathbb{Q}}_p$, os valores possíveis de $|\ |_p$ permanecem os mesmos, a saber $\{p^n\}_{n\in\mathbb{Z}} \cup \{0\}$.*

O teorema seguinte nos ajudará a determinar a expansão p-ádica de um número p-ádico qualquer não-nulo, a qual poderá ser tomada no sentido de uma série infinita. Para a demonstração de tal teorema, necessitaremos do lema a seguir.

Lema 3.3 *Se $x \in \mathbb{Q}$ e $|x|_p \leq 1$, então para qualquer $i \in \mathbb{N}$, $i \neq 0$, existe um inteiro α tal que $|\alpha - x|_p \leq p^{-i}$. O inteiro α pode ser escolhido no conjunto $\{0, 1, \ldots, p^i - 1\}$.*

Demonstração. Seja $x = \dfrac{a}{b}$, onde $a, b \in \mathbb{Z}$, $b \neq 0$, e $\text{mdc}(a, b) = 1$. Como $|x|_p \leq 1$, temos que $p \nmid b$ pois, caso contrário, $b = cp^j$, para algum $j \in \mathbb{N}$, $j \neq 0$, com $p \nmid c$ e, daí, $x = \dfrac{a}{cp^j}$, donde $|x|_p = p^j > 1$, o que é um absurdo. Logo, b e p^i são relativamente primos, para todo $i \in \mathbb{N}$. Podemos, então, encontrar $m, n \in \mathbb{Z}$ de modo que $mb + np^i = 1$.

Seja $\alpha = am$. A idéia é que mb difere de 1 por uma quantidade p-adicamente pequena, assim m é uma boa aproximação para $\dfrac{1}{b}$ e, portanto, α é uma boa aproximação para x. Mais precisamente, temos

$$|\alpha - x|_p = \left|am - \frac{a}{b}\right|_p = \left|\frac{a}{b}\right|_p |mb-1|_p \leq |mb-1|_p = |np^i|_p = |n|_p\, p^{-i} \leq p^{-i}.$$

Finalmente, escrevendo $\alpha = qp^i + r$, onde $0 \leq r < p^i$ e $q, r \in \mathbb{Z}$, temos

$$\begin{aligned} |r - x|_p &= |\alpha - qp^i - x|_p = |\alpha - x - qp^i|_p \\ &\leq \max\{|\alpha - x|_p, |qp^i|_p\} \\ &\leq p^{-i}. \end{aligned}$$

Portanto, adicionando um múltiplo inteiro conveniente de p^i ao inteiro α, podemos obter um inteiro entre 0 e $p^i - 1$. ∎

Teorema 3.4 *Cada classe de equivalência $a \in \widehat{\mathbb{Q}}_p$, com $|a|_p \leq 1$, é representada por uma única sequência de Cauchy $\{a_i\}$ tal que:*

(i) $a_i \in \mathbb{Z}$, *para todo* $i \in \mathbb{N}$, $i \neq 0$;

(ii) $0 \leq a_i < p^i$, *para todo* $i \in \mathbb{N}$, $i \neq 0$;

(iii) $a_i \equiv a_{i+1}\,(mod\, p^i)$, *para todo* $i \in \mathbb{N}$, $i \neq 0$.

Demonstração. Provemos, primeiramente, a unicidade: seja $\{a'_i\} \neq \{a_i\}$ uma outra sequência de Cauchy satisfazendo (i), (ii) e (iii), e seja $a_{i_0} \neq a'_{i_0}$. Como a_{i_0} e a'_{i_0} estão ambos entre 0 e $p^{i_0} - 1$, segue que $a_{i_0} \not\equiv a'_{i_0}\,(mod\, p^{i_0})$. Daí, para todo $i \geq i_0$, temos $a_i \equiv a_{i_0} \not\equiv a'_{i_0} \equiv a'_i\,(mod\, p^{i_0})$, ou seja, $a_i \not\equiv a'_i\,(mod\, p^{i_0})$. Logo, $|a_i - a'_i|_p > \dfrac{1}{p^{i_0}}$. Portanto, $\{a'_i\} \not\sim \{a_i\}$.

Seja, então, $\{b_i\}$ uma sequência de Cauchy representante da classe de equivalência $a \in \widehat{\mathbb{Q}}_p$. Nosso objetivo é encontrar uma sequência $\{a_i\}$ equivalente a $\{b_i\}$ satisfazendo (i), (ii) e (iii). Como $\{b_i\}$ é uma sequência de Cauchy, temos que, para cada $j \in \mathbb{N}$, $j \neq 0$, existe $N(j) \in \mathbb{N}$ tal que

$$|b_i - b_{i'}|_p \leq p^{-j} \quad \text{se} \quad i, i' \geq N(j).$$

Podemos tomar a sequência $N(j)$ estritamente crescente. Em particular, $N(j) \geq j$. Notemos que $|b_i|_p \leq 1$ se $i \geq N(1)$ pois, para todo $i' \geq N(1)$, temos

$$|b_i|_p \leq \max\{|b_{i'}|_p, |b_i - b_{i'}|_p\} \leq \max\left\{|b_{i'}|_p, \frac{1}{p}\right\},$$

com $|b_{i'}|_p \to |a|_p \leq 1$ quando $i' \to \infty$. Em particular, $|b_i|_p \leq 1$ se $i \geq 1$. Pelo lema anterior, temos uma sequência de inteiros a_j, com $0 \leq a_j < p^j$, tais que $|a_j - b_{N(j)}|_p \leq \dfrac{1}{p^j}$.

Afirmamos que a sequência $\{a_j\}$ assim construída é a sequência desejada.
Com efeito, basta mostrarmos que $a_{j+1} \equiv a_j\,(mod\, p^j)$ e que $\{b_i\} \sim \{a_j\}$. Como

$$\begin{aligned} |a_{j+1} - a_j|_p &= |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})|_p \\ &\leq \max\{|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |a_j - b_{N(j)}|_p\} \\ &\leq \max\left\{\frac{1}{p^{j+1}}, \frac{1}{p^j}, \frac{1}{p^j}\right\} = \frac{1}{p^j}, \end{aligned}$$

temos que $a_{j+1} \equiv a_j\,(mod\, p^j)$. Por outro lado, dado qualquer j, para $i \geq N(j) \geq j$, temos

$$\begin{aligned} |a_i - b_i|_p &= |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p \\ &\leq \max\{|a_i - a_j|_p, |a_j - b_{N(j)}|_p, |b_i - b_{N(j)}|_p\} \\ &\leq \max\{\frac{1}{p^j}, \frac{1}{p^j}, \frac{1}{p^j}\} = \frac{1}{p^j}. \end{aligned}$$

Daí, $|a_i - b_i|_p \to 0$ quando $i \to \infty$. Logo, $\{b_i\} \sim \{a_j\}$. ∎

Seja, então, $a \in \widehat{\mathbb{Q}}_p$, com $|a| \leq 1$. Pelo teorema anterior, temos que o número p-ádico a pode ser representado por uma sequência de Cauchy $\{a_i\}$ de números inteiros não-negativos. Será conveniente escrevermos todos os elementos a_i desta sequência na base p, isto é,

$$a_i = b_0 + b_1 p + b_2 p^2 + \cdots + b_{i-1} p^{i-1},$$

onde os $b_j{}'s \in \{0, 1, \ldots, p-1\}$. A condição (iii) do mesmo teorema nos dá

$$a_{i+1} = b_0 + b_1 p + b_2 p^2 + \cdots + b_{i-1} p^{i-1} + b_i p^i,$$

onde $b_0, b_1, b_2, \ldots, b_{i-1}$ são os mesmo de a_i. Assim, a pode ser visto intuitivamente como um número, escrito na base p, que estende-se infinitamente para a direita, isto é, adicionamos a cada passo um novo termo a a_i para chegar a a_{i+1}. Obtemos, então, a seguinte igualdade:

$$a = b_0 + b_1 p + b_2 p^2 + \cdots + b_{i-1} p^{i-1} + b_i p^i + \cdots$$

A igualdade acima é chamada *expansão p-ádica de a*.

Quando $|a|_p > 1$, podemos multiplicar a por uma potência conveniente p^m de p, a saber $m \geq 1$ tal que $|a|_p = p^m$, para obtermos um número p-ádico $a' = ap^m$ que satisfaça $|a'|_p \leq 1$. Daí, $a = a'p^{-m}$ é representado por uma sequência $\{a_i\}$ na qual $a_i = a_i' p^{-m}$. Agora, a passa a ser visto intuitivamente como um número, escrito na base p, que possui finitos termos com potências negativas de p e infinitos termos com potências positivas de p. A expansão p-ádica de a é, então, dada por

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \cdots + \frac{b_{m-1}}{p} + b_m + b_{m+1} p + b_{m+2} p^2 + \cdots$$

Veremos, agora, que a expansão p-ádica de um número p-ádico qualquer não-nulo pode ser tomada no sentido de um série infinita.

Seja $\{c_i\}$ uma sequência de números p-ádicos tal que $|c_i|_p \to 0$ quando $i \to \infty$. Então, a sequência de somas parciais $S_N = c_1 + \cdots + c_N$ converge para um limite em $\widehat{\mathbb{Q}}_p$, o qual denotamos por $\displaystyle\sum_{i=1}^{\infty} c_i$.

Com efeito, se $M > N$, então, quando $n \to \infty$

$$|S_M - S_N|_p = |c_{N+1} + \cdots + c_M| \leq \max\{|c_{N+1}|_p, \ldots, |c_M|_p\} \to 0.$$

Em particular, uma série converge em $\widehat{\mathbb{Q}}_p$ se, e somente se, seus termos aproximam-se de zero.

Consideremos, então, $a \in \widehat{\mathbb{Q}}_p$, $a \neq 0$, com expansão p-ádica

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \cdots + \frac{b_{m-1}}{p} + b_m + b_{m+1} p + b_{m+2} p^2 + \cdots,$$

onde $b_i{}'s \in \{0, 1, \ldots, p-1\}$. Temos que os termos da série infinita

$$\frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \cdots + \frac{b_{m-1}}{p} + b_m + b_{m+1} p + b_{m+2} p^2 + \cdots,$$

aproximam-se de zero. Logo, esta série converge para a e, daí, a igualdade pode ser tomada no sentido de uma série infinita.

Concluímos, então, que cada elemento $a \in \widehat{\mathbb{Q}}_p$, $a \neq 0$, pode ser representado por

$$a = \sum_{i=r}^{\infty} b_i p^i,$$

onde b_i'$s \in \{0, 1, \ldots, p-1\}$ e $b_r \neq 0$, para algum $r \in \mathbb{Z}$.

Antes de apresentarmos a valorização p-ádica em $\widehat{\mathbb{Q}}_p$, definiremos o anel dos inteiros p-ádicos:

Definição 3.5 *O conjunto de todos os elementos $a \in \widehat{\mathbb{Q}}_p$, com $|a|_p \leq 1$, é o subanel de $\widehat{\mathbb{Q}}_p$ chamado anel dos inteiros p-ádicos e será denotado por $\widehat{\mathbb{Z}}_p$.*

O conjunto dos inteiros p-ádicos invertíveis em será denotado por $\widehat{\mathbb{Z}}_p^*$, isto é,

$$\widehat{\mathbb{Z}}_p^* = \{a \in \widehat{\mathbb{Z}}_p;\ |a|_p = 1\}.$$

Em particular, $\widehat{\mathbb{Z}}_p$ é o conjunto de todos os elementos de $\widehat{\mathbb{Q}}_p$ que são expansões p-ádicas envolvendo somente potências não-negativas de p e $\widehat{\mathbb{Z}}_p^*$ é o conjunto de todos inteiros p-ádicos que possuem o primeiro termo não-nulo, isto é, dado $a \in \widehat{\mathbb{Z}}_p$, temos que

$$a \in \widehat{\mathbb{Z}}_p^* \Leftrightarrow a = b_0 + b_1 p + b_2 p^2 + \cdots,$$

onde b_i'$s \in \{0, 1, \ldots, p-1\}$ e $b_0 \neq 0$.

A valorização p-ádica $v_p : \widehat{\mathbb{Q}}_p \to \mathbb{R} \cup \{\infty\}$ é, portanto, dada por $v_p(0) = \infty$ e $v_p(a) = r$, com $a = \sum_{i=r}^{\infty} b_i p^i$, onde $b_i \in \{0, 1, \ldots, p-1\}$ e $b_r \neq 0$, para algum $r \in \mathbb{Z}$. O anel de valorização O_{v_p} é o anel dos inteiros p-ádicos $\widehat{\mathbb{Z}}_p$ e seu ideal maximal M_{v_p} é o conjunto $\widehat{\mathbb{Z}}_p \backslash \widehat{\mathbb{Z}}_p^*$, isto é, dado $a \in \widehat{\mathbb{Q}}_p$, temos que

$$a \in O_{v_p} \Leftrightarrow a = \sum_{i \geq 0} b_i p^i \quad \text{e} \quad a \in M_{v_p} \Leftrightarrow a = \sum_{i \geq 1} b_i p^i.$$

As operações de adição, subtração, multiplicação e divisão em $\widehat{\mathbb{Q}}_p$ são semelhantes às operações correspondentes de números decimais. A única diferença é que em $\widehat{\mathbb{Q}}_p$ efetuamos as operações da esquerda para a direita, como veremos nos exemplos que seguem.

Exemplo 3.6 *Consideremos o corpo $\widehat{\mathbb{Q}}_5$. Então,*

$$\begin{array}{rccccccc}
 & 4 & + & 3\times 5 & + & 2\times 5^2 & + & \cdots \\
\times & 2 & + & 4\times 5 & + & 1\times 5^2 & + & \cdots \\
\hline
 & 3 & + & 2\times 5 & + & 0\times 5^2 & + & \cdots \\
 & & & 6\times 5 & + & 4\times 5^2 & + & \cdots \\
 & & & & & 4\times 5^2 & + & \cdots \\
\hline
 & 3 & + & 3\times 5 & + & 4\times 5^2 & + & \cdots
\end{array}$$

Exemplo 3.7 *Consideremos o corpo $\widehat{\mathbb{Q}}_7$. Então,*

$$\begin{array}{rccccccc}
 & 2\times 7^{-1} & + & 0\times 7^0 & + & 3\times 7^1 & + & \cdots \\
- & 4\times 7^{-1} & + & 6\times 7^0 & + & 5\times 7^1 & + & \cdots \\
\hline
 & 5\times 7^{-1} & + & 0\times 7^0 & + & 4\times 7^1 & + & \cdots
\end{array}$$

Agora, apresentamos alguns exemplos de números p-ádicos.

Exemplo 3.8

$$-1 = \sum_{i=0}^{\infty}(p-1)p^i.$$

Exemplo 3.9

$$\frac{1}{1-p^k} = \sum_{i=0}^{\infty} p^{ki}, \text{ para todo } k \geq 1.$$

A seguinte proposição caracteriza o conjunto dos números racionais em $\widehat{\mathbb{Q}}_p$ como o conjunto de todas as séries infinitas periódicas.

Proposição 3.10 *O elemento $a \in \widehat{\mathbb{Q}}_p$, $a \neq 0$, representado por $\sum_{i=r}^{\infty} b_i p^i$, onde $b_r \neq 0$ e $b_i \in \{0, 1, \ldots, p-1\}$, é um número racional se, e somente se, a sequência $\{b_i\}$ é periódica.*

Demonstração. Suponhamos que $r = 0$.

($\Rightarrow$:) Seja $a \in \widehat{\mathbb{Q}}$, $a \neq 0$, tal que $a \in \mathbb{Q}$.

Afirmamos que existem $m, n \in \mathbb{N}$, $n \geq 1$, e $t, u \in \mathbb{Z}$ tais que $0 \leq t < p^m$, $0 \leq u < p^n$ e $a = t + up^m(1-p^n)^{-1}$.

Com efeito, temos que $a = \dfrac{b}{c}$, onde $b, c \in \mathbb{Z}$, $c > 0$ e $\operatorname{mdc}(p, c) = 1$. Daí, existe $n \in \mathbb{N}$, $n \geq 1$, tal que $p^n \equiv 1 \pmod{c}$. Logo, $p^n - 1 = rc$, para algum $r \in \mathbb{Z}$, $r \neq 0$, ou seja, $c = r^{-1}(p^n - 1)$. Portanto, $a = \dfrac{b}{r^{-1}(p^n-1)}$, ou seja, $a = d\,(p^n-1)^{-1}$, onde $d = br \in \mathbb{Z}$.

Tomemos, então, $m \in \mathbb{N}$ de modo que $-p^m \leq d < p^m$. Como $\operatorname{mdc}(p^m, p^n - 1) = 1$, segue que existem $t, u \in \mathbb{Z}$ tais que $d = t\,(p^n-1) - up^m$. Se $a > 0$, então podemos tomar u de modo que $0 \leq u < p^n$; se $a < 0$, então tomamos u de modo que $1 \leq u < p^n$. Assim,

$$a = d\,(p^n-1)^{-1} \Rightarrow a = (t\,(p^n-1) - up^m)(p^n-1)^{-1} \Rightarrow a = t + up^m(1-p^n)^{-1}.$$

Escrevendo t e u na base p, temos que existem $b_0, \ldots, b_{m+n-1} \in \{0, 1, \ldots, p-1\}$ tais que

$$t = \sum_{i=0}^{m-1} b_i p^i \text{ e } u = \sum_{i=0}^{n-1} b_{m+i}\, p^i.$$

Como $(1-p^n)^{-1} = \sum_{i=0}^{\infty} p^{in}$, temos que $a = \sum_{i=0}^{\infty} b_i p^i$, onde $b_{i+n} = b_i$ para todo $i \geq m$. Portanto, a sequência $\{b_i\}$ é periódica.

($\Leftarrow$:) Suponhamos que a sequência $\{b_i\}$ é periódica. Então, existem $m, n \in \mathbb{N}$, $n \geq 1$, tais que $b_{i+n} = b_i$ para todo $i \geq m$. Sejam

$$s = \sum_{i=0}^{m-1} b_i p^i \quad \text{e} \quad s' = \sum_{i=m}^{m+n-1} b_i p^i.$$

Então,

$$\begin{aligned} a - s &= \sum_{i=0}^{\infty} b_i p^i - \sum_{i=0}^{m-1} b_i p^i = \sum_{i=m}^{\infty} b_i p^i = \sum_{i=m}^{m+n-1} b_i p^i + \sum_{i=m+}^{\infty} b_i p^i \\ &= s' + \sum_{i=m+n}^{\infty} b_i p^i = s' + p^n \sum_{i=m}^{\infty} b_i p^i = s' + p^n\,(a-s). \end{aligned}$$

Daí,

$$\begin{aligned} s' = (a-s) - p^n(a-s) &\Rightarrow s' = (a-s)(1-p^n) \\ &\Rightarrow a - s = s'(1-p^n)^{-1} \\ &\Rightarrow a = s + s'(1-p^n)^{-1} \in \mathbb{Q}. \end{aligned}$$

Portanto, $a \in \mathbb{Q}$. ■

Nos exemplos que seguem, discutimos a resolução das equações $x^2 - 7 = 0$ e $x^2 - 5 = 0$ em $\widehat{\mathbb{Q}}_3$ e das equações $x^2 - 6 = 0$ e $x^2 - 7 = 0$ em $\widehat{\mathbb{Q}}_5$. Para tal discussão será necessária, no entanto, a seguinte definição:

Definição 3.11 *Dados $x, y \in \widehat{\mathbb{Q}}_p$, definimos:*

$$x \equiv y\,(mod\, p^n) \Leftrightarrow |x-y|_p \leq \left(\frac{1}{p}\right)^n \Leftrightarrow \frac{x-y}{p^n} \in \widehat{\mathbb{Z}}_p \Leftrightarrow$$

os coeficientes a_m das séries de x e de y coincidem para todo $m \leq n$.

Exemplo 3.12 *Consideremos $\widehat{\mathbb{Q}}_3$.*

(1) *7 é um quadrado em $\widehat{\mathbb{Q}}_3$.*

De fato, escrevemos $1 + 2 \times 3 = 7 = (a_0 + a_1 3 + a_2 3^2 + \cdots)^2$, com $0 \leq a_i \leq 2$. Comparando coeficientes, obtemos $1 \equiv a_0^2\,(mod\, 3)$. Essa congruência tem soluções $a_0 = 1$ e $a_0 = 2$. Tomamos $a_0 = 1$. Daí,

$$1 + 2 \times 3 = (1 + a_1 3 + a_2 3^2 + \cdots)^2 = 1 + 2a_1 3 + \cdots \equiv 1 + 2a_1 3\,(mod\, 3^2).$$

Logo, $2 \equiv 2a_1\,(mod\, 3)$ e $a_1 \equiv 1\,(mod\, 3)$. Segue que

$$1 + 2 \times 3 = (1 + 3 + a_2 3^2 + \cdots)^2 \equiv (1 + 3 + a_2 3^2)^2\,(mod\, 3^3) 1 + 2 \times 3 + (2a_2 + 1)3^2\,(mod\, 3^3).$$

Portanto, $2a_2 + 1 \equiv 0\,(mod\, 3)$ e $a_2 \equiv 1\,(mod\, 3)$.

Assim,

$$1+2\times 3 = (1+3+3^2+a_3 3^3+\cdots)^2 \equiv (1+3+3^2+a_3 3^3)^2\,(mod\, 3^4) \equiv 1+2\times 3+0\times 3^2+2a_3 3^3\,(mod\, 3^4).$$

Logo, $2a_3 3^3 \equiv 0\,(mod\, 3^4)$. Portanto, $2a_3 \equiv 0\,(mod\, 3)$ e $a_3 \equiv 0\,(mod\, 3)$.

Assim, $1 + 2 \times 3 = (1 + 3 + 3^2 + 0 \times 3^3 + \cdots)$.

Continuando o processo, obtemos a série

$$a = 1 + 1 \times 3 + 1 \times 3^2 + 0 \times 3^3 + a_4 \times 3 + \cdots,$$

onde $a_1, a_2, a_3, \ldots$ estão unicamente determinados a partir de $a_0 = 1$.

É claro que, escolhendo $a_0 = 2$, obtemos

$$-a = 2 + 1 \times 3 + 1 \times 3^2 + 2 \times 3^3 + (2 - a_4) \times 3^4 + \cdots,$$

a outra raiz quadrada de 7 em $\widehat{\mathbb{Q}}_3$.

(2) *5 não é um quadrado em $\widehat{\mathbb{Q}}_3$.*

De fato, suponhamos, por contradição, que $5 = 2 + 3 = (a_0 + a_1 3 + a_2 3^2 + \cdots)^2$, com $0 \leq a_i \leq 2$. Comparando os coeficientes, obtemos $2 \equiv a_0^2\,(mod\, 3)$, contradizendo o fato dessa convergência não ter solução em $\mathbb{Z}$.

Exemplo 3.13 *Consideremos o corpo* $\widehat{\mathbb{Q}}_5$.

(1) 6 *é um quadrado em* $\widehat{\mathbb{Q}}_5$.

De fato, escrevemos $6 = 1 + 5 = (a_0 + a_1 5 + a_2 5^2 + \cdots)^2$, *com* $0 \leq a_i \leq 4$. *Comparando os coeficientes, obtemos* $1 \equiv a_0^2 \, (mod\, 5)$. *Essa congruência tem as soluções* $a_0 = 1$ *e* $a_0 = 4$. *Tomamos* $a_0 = 1$. *Logo,*

$$6 = 1 + 5 = (a_0 + a_1 5 + a_2 5^2 + \cdots)^2 = 1 + 2a_1 5 + \cdots \equiv 1 + 2a_1 5 \, (mod\, 5^2).$$

Portanto, $2a_1 \equiv 1 \, (mod\, 5)$ *e* $a_1 = 3$. *Segue que*

$$6 = 1 + 5 = (1 + 3 \times 5 + a_2 5^2 + \cdots)^2 = 1 + 3 \times 5 + 2a_2 5^2 + \cdots \equiv 1 + 3 \times 5 + 2a_2 5^2 \, (mod\, 5^3).$$

Daí,

$$2a_2 \equiv 0 \, (mod\, 5) \ \textit{e}\ a_2 \equiv 0 \, (mod\, 5).$$

Logo,

$$\begin{aligned} 6 = 1 + 5 &= (1 + 3.5 + 0 \times 5^2 + a_3 5^3 + \cdots)^2 \\ &= 1 + 5 + 0 \times 5^2 + (2a_3 + 2)5^3 + \cdots \\ &\equiv 1 + 5 + (2a_3 + 2)5^3 \, (mod\, 5^4). \end{aligned}$$

Comparando os coeficientes, obtemos $2a_3 + 2 \equiv 0 \, (mod\, 5)$.

Assim, $2a_3 \equiv 3 \, (mod\, 5)$ *e* $a_3 \equiv 4 \, (mod\, 5)$.

Continuando o processo, obtemos

$$a = 1 + 3 \times 5 + 0 \times 5^2 + 4 \times 5^3 + a_4 5^4 + \cdots \in \widehat{\mathbb{Q}}_5.$$

Tomando $a_0 = 4$, *obtemos*

$$-a = 4 + 1 \times 5 + 4 \times 5^2 + 0 \times 5^3 + (4 - a_4)5^4 + \cdots \in \widehat{\mathbb{Q}}_5.$$

(2) 7 *não é um quadrado em* $\widehat{\mathbb{Q}}_5$.

Com efeito, suponhamos, por contradição, que $7 = 2 + 1 \times 5 = (a_0 + a_1 5 + a_2 5^2 + \cdots)^2$, *com* $0 \leq a_i \leq 4$. *Comparando os coeficientes, obtemos* $2 \equiv 7 \equiv a_0^2 \, (mod\, 5)$, *contradizendo o fato de que* $x^2 \equiv 2 \, (mod\, 5)$ *não ter solução.*

O método para resolver a equação $x^2 - 7 = 0$ em $\widehat{\mathbb{Q}}_3$ e a equação $x^2 - 6 = 0$ em $\widehat{\mathbb{Q}}_5$, começando pela resolução, respectivamente, das congruências $a_0^2 \equiv 7 \equiv 1 \, (\mathrm{mod}\, 3)$ e $a_0^2 \equiv 6 \, (\mathrm{mod}\, 5)$ e após, passo a passo, deteminando a_i é geral, conforme será mostrado a seguir.

Teorema 3.14 ***(Lema de Hensel)*** *Seja* $f(x) = c_0 + c_1 x + \cdots + c_m x^m \in \widehat{\mathbb{Z}}_p[x]$ *e seja* $f'(x)$ *a derivada de* $f(x)$, *isto é,* $f'(x) = c_1 + 2c_2 x + \cdots + m c_m x^{m-1}$. *Se* $b_0 \in \widehat{\mathbb{Z}}_p$ *é tal que* $f(b_0) \equiv 0 \, (mod\, p)$ *e* $f'(b_0) \not\equiv 0 \, (mod\, p)$, *então existe um único* $b \in \widehat{\mathbb{Z}}_p$ *tal que* $f(b) = 0$ *e* $b \equiv b_0 \, (mod\, p)$.

Demonstração. Afirmamos que existe uma única sequência de inteiros não-negativos $b_1, b_2, \ldots$ tais que para todo $n \geq 1$:

(1) $f(b_n) \equiv 0 \, (\mathrm{mod}\, p^{n+1})$;

(2) $b_n \equiv b_{n-1} \, (\mathrm{mod}\, p^n)$;

(3) $0 \leq b_n < p^{n+1}$.

Provamos, por indução sobre n, a existência de b_n e a sua unicidade.

Se $n = 1$, seja $\widetilde{b}_0$ o único inteiro em $\{0, 1, \ldots, p-1\}$ tal que $\widetilde{b}_0 \equiv b_0 \, (\mathrm{mod}\, p)$. Qualquer b_1 tendo as propriedades (2) e (3) é da forma $b_1 = \widetilde{b}_0 + d_1 p$ com $0 \leq d_1 \leq p - 1$. Agora,

$$f(b_1) = f(\widetilde{b}_0 + d_1 p) \ = \ \sum_{i=0}^{m} c_i (\widetilde{b}_0 + d_1 p)^i$$

$$
\begin{aligned}
&= \sum_{i=0}^{m}(c_i\widetilde{b}_0^i + ic_i\widetilde{b}_0^{i-1}d_1p + \text{termos divisíveis por}\, p^2)\\
&\equiv \Big(\sum_{i=0}^{m} c_i\widetilde{b}_0^i\Big) + \Big(\sum_{i=0}^{m} ic_i\widetilde{b}_0^{i-1}\Big)d_1p \,(\mathrm{mod}\, p^2)\\
&= f(\widetilde{b}_0) + f'(\widetilde{b}_0)d_1p \,(\mathrm{mod}\, p^2).
\end{aligned}
$$

Por hipótese, $f(b_0) \equiv 0 \,(\mathrm{mod}\, p)$, logo podemos escrever $f(\widetilde{b}_0) \equiv \alpha p \,(\mathrm{mod}\, p^2)$, para algum $\alpha \in \{0, 1, \ldots, p-1\}$. Portanto, para que $f(b_1) \equiv 0 \,(\mathrm{mod} p^2)$ devemos ter

$$\alpha p + f'(\widetilde{b}_0)d_1p \equiv 0 \,(\mathrm{mod}\, p^2), \text{ isto é, } \alpha + f'(\widetilde{b}_0)d_1 \equiv 0 \,(\mathrm{mod}\, p).$$

Como $f'(b_0) \not\equiv 0 \,(\mathrm{mod}\, p)$, então $f'(b_0)$ é invertível em $\widehat{\mathbb{Z}}_p$, assim,

$$\frac{-\alpha}{f'(b_0)} = d_1 + d_2p + \cdots \in \widehat{\mathbb{Z}}_p$$

e existe um único d_1, $0 \leq d_1 \leq p-1$, com esta propriedade. Desse modo, $\alpha + f'(b_0)d_1$ está no ideal maximal de $\widehat{\mathbb{Z}}_p$, isto é, $\alpha + f'(b_0)d_1 \equiv 0 \,(\mathrm{mod} p)$.

Suponhamos já determinados $b_1, b_2, \ldots, b_{n-1}$. Queremos encontrar b_n. Por (2) e (3), precisamos que $b_n = b_{n-1} + d_np^n$ com $d_n \in \{0, 1, \ldots, p-1\}$. Desenvolvemos $f(b_{n-1} + d_np^n)$ como fizemos anteriormente no caso $n = 1$, dessa vez ignoramos os termos divisíveis por p^{n+1}. Isto nos dá:

$$f(b_n) = f(b_{n-1} + d_np^n) \equiv f(b_{n-1}) + f'(b_{n-1})d_np^n \,(\mathrm{mod}\, p^{n+1}).$$

Por hipótese de indução, $f(b_{n-1}) \equiv 0 \,(\mathrm{mod}\, p^n)$ e podemos escrever $f(b_{n-1}) \equiv \alpha' p^n \,(\mathrm{mod}\, p^{n+1})$ e a condição requerida $f(b_n) \equiv 0 \,(\mathrm{mod}\, p^{n+1})$ é $\alpha' p^n + f'(b_{n-1})d_np^n \equiv 0 \,(\mathrm{mod}\, p^{n+1})$, isto é,

$$\alpha' + f'(b_{n-1})d_n \equiv 0 \,(\mathrm{mod}\, p).$$

Agora, como $b_{n-1} \equiv b_0 \,(\mathrm{mod}\, p)$, segue que $f'(b_{n-1}) \equiv f'(b_0) \not\equiv 0 \,(\mathrm{mod}\, p)$ e podemos determinar $d_n \in \{0, 1, \ldots, p-1\}$, exatamente da mesma maneira que d_1 resolvendo

$$d_n \equiv \frac{-\alpha'}{f'(b_{n-1})} \,(\mathrm{mod}\, p).$$

Isso completa a indução e demonstra a afirmação.

O teorema segue da afirmação, tomando $b = \widetilde{b}_0 + d_1p + d_2p^2 + \cdots$. Como para todo n temos $f(b) \equiv f(b_n) \equiv 0 \,(\mathrm{mod}\, p^{n+1})$, segue que $f(b) = 0$. Reciprocamente, qualquer

$$b = \widetilde{b}_0 + d_1p + d_2p^2 + \cdots$$

dá uma sequência $b_n = \widetilde{b}_0 + d_1p + \cdots + d_np^n$ como na afirmação anterior e a unicidade da sequência implica na unicidade de b. ∎

Observamos que a técnica de aproximação de Hensel é essencialmente a mesma do método de Newton para encontrar uma raiz real de uma equação com coeficientes reais, onde

$$b_n = b_{n-1} - \frac{f(b_{n-1})}{f'(b_{n-1})}.$$

O termo de correção no Lema de Hensel é

$$d_np^n \equiv \frac{-\alpha' p^n}{f'(b_{n-1})} \equiv -\frac{f(b_{n-1})}{f'(b_{n-1})} \,(\mathrm{mod}\, p^{n+1}).$$

No caso p-ádico, a sequência converge para uma raiz do polinômio, enquanto que no método de Newton nem sempre converge.

3.2 A representação por séries de potências

Vimos na seção anterior que, fixado um número natural primo p, os elementos do completamento de $\mathbb{Q}$, com relação à valorização p-ádica v_p de $\mathbb{Q}$, podem ser representados por séries de potências. Veremos, agora, que, dado um corpo qualquer com uma valorização discreta, seu completamento admite esta mesma caracterização, isto é, todos seus elementos podem ser representados por séries de potências.

Seja K um corpo com uma valorização discreta v e seja π uma uniformizante de v. Assim, $M_v = (\pi)$ é o ideal maximal do anel de valorização O_v e $K_v = O_v/(\pi)$ é o corpo residual.

Seja $S \subseteq O_v$ um conjunto de representantes de K_v de modo que cada elemento de O_v seja congruente módulo π a exatamente um elemento de S. Por conveniência, assumimos que $0 \in S$. Supondo v normalizada, temos $v(\pi) = 1$.

O próximo teorema caracteriza os elementos de K como séries de potências. Para concluirmos tal resultado necessitaremos da proposição que segue.

Proposição 3.15 *Seja $a \in K$, $a \neq 0$, tal que $v(a) = r$. Então, para qualquer $n \in \mathbb{Z}$, $n \geq r$, existe uma única expressão*

$$a = b_r\pi^r + b_{r+1}\pi^{r+1} + \cdots + b_n\pi^n \,(mod\, \pi^{n+1}), \qquad (1)$$

onde $b_i \in S$ e $b_r \neq 0$.

Demonstração. Seja $a \in K$, $a \neq 0$, tal que $v(a) = r$. Então, $a\pi^{-r}$ é invertível em O_v e, portanto, existe um único elemento $b_r \in S$, $b_r \neq 0$, tal que $a\pi^{-r} \equiv b_r \,(\mathrm{mod}\,\pi)$. Daí,

$$\begin{aligned} a \equiv b_r\pi^r \,(\mathrm{mod}\,\pi^{r+1}) &\Rightarrow a - b_r\pi^r \in (\pi^{r+1}) \\ &\Rightarrow a - b^r\pi^r = \alpha\pi^{r+1}, \text{ para algum } \alpha \in O_v \\ &\Rightarrow v(a - b_r\pi^r) = v(\alpha\pi^{r+1}) \\ &= v(\alpha) + v(\pi^{r+1}) = v(\alpha) + (r+1)v(\pi) \\ &\geq 0 + (r+1) = r+1. \end{aligned}$$

Logo, existe um único elemento $b_{r+1} \in S$ tal que

$$(a - b_r\pi^r)\,\pi^{-r-1} \equiv b_{r+1} \,(\mathrm{mod}\,\pi).$$

Fazendo indução sobre $n \in \mathbb{Z}$, $n \geq r$, obtemos uma única expressão

$$a = b_r\pi^r + b_{r+1}\pi^{r+1} + \cdots + b_n\pi^n \,(\mathrm{mod}\,\pi^{n+1}), \text{ onde } b_i \in S \text{ e } b_r \neq 0.$$

■

Dados $b, b' \in S$, temos que $b + b', bb' \in O_v$ e, daí, $b + b'$ e bb' são congruentes módulo π a elementos de S unicamente determinados, digamos s e t, respectivamente, isto é,

$$b + b' \equiv s \,(\mathrm{mod}\,\pi) \text{ e } bb' \equiv t \,(\mathrm{mod}\,\pi).$$

Assim, para quaisquer $b, b' \in S$, estas congruências definem a adição e a multiplicação de S.

A estrutura de corpo de K, juntamente com a adição e a multiplicação de S, é determinada completamente para seus elementos pela expressão (1). Assim, podemos adicionar e multiplicar quaisquer expressões do tipo (1). Tomando $r = 0$ por conveniência, suponhamos que

$$a = \sum_{i\geq 0} b_i\pi^i \quad \text{e} \quad a' = \sum_{i\geq 0} a'_i\pi^i,$$

então

$$a + a' = \sum_{i \geq 0} s_i \pi^i \quad \text{e} \quad aa' = \sum_{i \geq 0} t_i \pi^i,$$

onde $s_0, s_1, \ldots$ e $t_0, t_1, \ldots$ são os únicos elementos de S determinados, respectivamente, por

$s_0 \equiv b_0 + b'_0 \pmod{\pi}$,
$s_1 \equiv (b_0 + b'_0 - s_0)\pi^{-1} + b_1 + b'_1 \pmod{\pi}, \ldots$, e (2)
$t_0 \equiv b_0 b'_0 \pmod{\pi}$,
$t_1 \equiv (b_0 b'_0 - t_0)\pi^{-1} + b_0 b'_1 + b_1 b'_0 \pmod{\pi}, \ldots$.

Como a expressão (1) é verdadeira para todo $n \in \mathbb{Z}$, $n \geq r$, podemos representar o elemento $a \in K$, $a \neq 0$, por uma série infinita

$$a = \sum_{i=r}^{\infty} b_i \pi^i, \qquad (3)$$

onde a mesma é entendida como a união de todas as congruências (1) para $n = r, r+1, \ldots$.

Afirmamos que a série infinita (3) determina o elemento a univocamente.

Com efeito, suponhamos que a série infinita (3) represente também o elemento $a' \in K$, $a' \neq 0$. Então, tomando a série até π^n, temos que

$$v(a - a') \geq n + 1, \text{ para todo } n \geq r.$$

Daí, $v(a - a') = \infty$. Portanto, $a = a'$.

Assim, temos que todo elemento não-nulo de K é representado univocamente por uma série infinita do tipo (3). No entanto, em geral não é verdade que toda série infinita do tipo (3) representa um elemento de K.

Afirmamos que toda série infinita do tipo (3) representa um elemento de K se, e somente se, K é completo.

Com efeito, qualquer sequência $\{s_n\}$ de elementos da forma

$$s_n = \sum_{i=r}^{n} b_i \pi^i, \text{ onde } n \in \mathbb{Z}, \, n \geq r, \qquad (4)$$

é uma sequência de Cauchy, pois $v(s_m - s_n) \geq \min\{m+1, n+1\}$.

Suponhamos que K é completo. Então, a equação (4) converge para $\sum_{i=r}^{\infty} b_i \pi^i$. Portanto, toda série infinita do tipo (3) representa um elemento de K. Reciprocamente, se toda série infinita do tipo (3) representa um elemento de K, então podemos expandir todos os elementos da sequência $\{s_n\}$ na forma (3). Daí, como $v(s_m - s_n) \to \infty$, o coeficiente de qualquer potência fixada π^h deve ser o mesmo para todo elemento s_n, com $n > n_0(h)$. Supondo que o último valor deste coeficiente é b_h, temos que a sequência $\{s_n\}$ converge para $\sum_h b_h \pi^h$.

Concluímos, portanto, o seguinte resultado:

Teorema 3.16 *Sejam K um corpo com uma valorização discreta normalizada v, π uma uniformizante de v e S um conjunto de representantes do corpo residual $K_v = O_v/(\pi)$, com $0 \in S$. Então, todo elemento $a \in K$, $a \neq 0$, pode ser representado na forma*

$$a = \sum_{i=r}^{\infty} b_i \pi^i, \text{ onde } b_i \in S, \, b_r \neq 0 \text{ e } v(a) = r. \qquad (5)$$

A adição e a multiplicação em K são definidas pela expressão (2) e, além disso, toda expressão (5) representa um elemento de K se, e somente se, K é completo.

Como primeira aplicação deste teorema, temos o caso em que K é o corpo dos números p-ádicos, para algum natural primo p fixado, isto é, $K = \widehat{\mathbb{Q}}_p$. Neste caso, $v = v_p$ é a valorização p-ádica em $\widehat{\mathbb{Q}}_p$, $\pi = p$ é uma uniformizante de v e $S = \{0, 1, \ldots, p-1\}$ é o conjunto de representantes do corpo residual de $\widehat{\mathbb{Q}}_p$. Dado $a \in \widehat{\mathbb{Q}}_p$, $a \neq 0$, temos, então, que

$$a = \sum_{i=r}^{\infty} b_i p^i, \text{ onde } b_i \in S,\ b_r \neq 0 \text{ e } v(a) = r.$$

Como segunda aplicação do teorema anterior, consideremos o corpo de funções racionais $K(x)$. Como vimos no Corolário 2.46, toda valorização não-trivial v de $K(x)|K$ ou é equivalente a uma valorização v_p de $K(x)|K$, para algum polinômio mônico irredutível p sobre K, ou é equivalente à valorização v_∞ de $K(x)|K$. No primeiro caso, uma uniformizante de v_p é o polinômio p, digamos de grau n, e o corpo residual é $K(\alpha) \simeq K[x]/(p)$, onde α é uma raiz do polinômio p. Como conjunto de representantes de $K(\alpha)$, podemos tomar o conjunto S constituído de todos os polinômios em $K[x]$ de grau $< n$. Assim, cada $\phi \in K(x)$, $\phi \neq 0$, tem a forma

$$\phi = \sum_{i=r}^{\infty} b_i p^i, \text{ onde } b_i \in S,\ b_r \neq 0 \text{ e } v_p(\phi) = r.$$

No caso particular quando $n = 1$, o polinômio p é da forma $p(x) = x - \alpha$. Neste caso, o corpo residual é exatamente K e, assim, cada elemento $\phi \in K(x)$, $\phi \neq 0$, tem a forma

$$\phi = \sum_{i=r}^{\infty} b_i (x-\alpha)^i, \text{ onde } b_i \in K,\ b_r \neq 0 \text{ e } v_p(\phi) = r.$$

Resta ainda o caso em que v é equivalente a valorização v_∞ de $K(x)|K$. Agora, x^{-1} é uma uniformizante de v_∞ e, para cada $\phi \in K(x)$, $\phi \neq 0$, obtemos uma expansão como série de potências inversa:

$$\phi = \sum_{i=r}^{\infty} b_i x^{-i}, \text{ onde } b_i \in K,\ b_r \neq 0 \text{ e } v_\infty(\phi) = r.$$

Capítulo 4

Valorizações de Krull

Apresentaremos, neste capítulo, o conceito de valorizações de Krull e mostraremos que as valorizações apresentadas no capítulo 2 são valorizações de Krull de posto 1.

4.1 Anéis de valorização

Nesta seção, caracterizaremos, de um modo geral, os anéis de valorização de um corpo K e estudaremos seus ideais primos. Iniciaremos, apresentando algumas definições e propriedades que serão necessárias para concluirmos nosso objetivo.

Definição 4.1 *Uma relação binária $\leq$ em um conjunto S é dita uma quase-ordem de S se, e somente se, $\leq$ é reflexiva (isto é, $s \leq s$, para todo $s \in S$) e transitiva (isto é, $s_1 \leq s_2$ e $s_2 \leq s_3$ implicam $s_1 \leq s_3$, para quaisquer $s_1, s_2, s_3 \in S$). A mesma é dita uma quase-ordem total de S se, e somente se, $s_1 \not\leq s_2$ implica $s_2 \leq s_1$, para quaisquer $s_1, s_2 \in S$, e é dita uma quase-ordem trivial de S se, e somente se, $s_1 \leq s_2$, para quasiquer $s_1, s_2 \in S$. Em particular, uma quase-ordem trivial de um um conjunto S é uma quase-ordem total de S.*

Definição 4.2 *Uma relação binária $\leq$ em um conjunto S é dita uma ordem de S se, e somente se, $\leq$ é uma quase-ordem tal que $s_1 \leq s_2$ e $s_2 \leq s_1$ implicam $s_1 = s_2$, para quaisquer $s_1, s_2 \in S$.*

Definição 4.3 *Uma quase-ordem não-trivial $\mid$ de K é dita uma divisibilidade de K se, e somente se, $x \mid y$ implica $xz \mid yz$, e $x \mid y$, $x \mid z$ implicam $x \mid (y - z)$, para quaisquer $x, y, z \in K$.*

Observação 4.4 *Se $\mid$ é uma divisibilidade de K, então $x \mid 0$ e $0 \nmid x$, para qualquer $x \in K, x \neq 0$.*

De fato, para todo $x \in K$, $x \neq 0$, $x \mid (x - x) = 0$. Por outro lado, suponhamos, por absurdo, que existe $y \in K$, $y \neq 0$, tal que $0 \mid y$. Como $x \mid 0$, da transitividade, segue que $x \mid y$ e a quase-ordem é trivial, o que é um absurdo.

Proposição 4.5 *Existe uma correspondência bijetora entre as divisibilidades e os subanéis de um corpo K.*

Demonstração. Dado um subanel R de K, para quaisquer $x, y \in K$, $x \neq 0$, definimos a relação binária $\mid$ em K por

$$x \mid y \Leftrightarrow yx^{-1} \in R.$$

Afirmamos que $\mid$ é uma divisibilidade de K.

De fato, dado $x \in K$, $x \neq 0$, temos que $xx^{-1} = 1 \in R$ e, daí, $x \mid x$. Logo, $\mid$ é reflexiva. Por outro lado, dados $x, y, z \in K$, $x \neq 0, y \neq 0$, temos que

$$x \mid y \text{ e } y \mid z \Rightarrow yx^{-1}, zy^{-1} \in R \Rightarrow zx^{-1} = (yx^{-1})(zy^{-1}) \in R \Rightarrow x \mid z.$$

Daí, $\mid$ é transitiva. Assim, temos que $\mid$ é uma quase-ordem de K. Além disso, para quaisquer $x, y, z \in K, x \neq 0, z \neq 0$, temos que, se $x \mid y$, então $yx^{-1} \in R$, ou seja,

$$yx^{-1} = y(zz^{-1})x^{-1} = (yz)(z^{-1}x^{-1}) = (yz)(xz)^{-1} \in R.$$

Daí, $xz \mid yz$. Ainda, se $x \mid y$ e $x \mid z$, então

$$yx^{-1}, zx^{-1} \in R \Rightarrow yx^{-1} - zx^{-1} = (y - z)x^{-1} \in R,$$

para quaisquer $x, y, z \in K$, $x \neq 0$. Logo, $x \mid (y - z)$ e, portanto, $\mid$ é uma divisibilidade de K.

Em particular, $R = \{x \in K;\ 1 \mid x\}$.

Reciprocamente, seja $\mid$ uma divisibilidade de K.

Afirmamos que o conjunto $R = \{x \in K;\ 1 \mid x\}$ é um subanel de K.

De fato, é claro que $0 \in R$ e $1 \in R$. Dado $x \in R$, temos que $1 \mid (0 - x) = -x$ e, daí, $-x \in R$. Por outro lado, dados $x, y \in R$, temos que, como $-y \in R$, $1 \mid (x - (-y)) = x + y$. Daí, $x + y \in R$. Ainda, como $1 \mid x$ e $1 \mid y$, obtemos $1 \mid x$ e $x \mid xy$. Logo, $1 \mid xy$ e, portanto, $xy \in R$. Assim, temos que R é um subanel de K. Além disso, dado $x \in R$, $x \neq 0$, temos que

$$x^{-1} \in R \Leftrightarrow 1 \mid x^{-1} \Leftrightarrow x \mid 1.$$

Daí, $U_R = \{x \in R;\ x \mid 1\}$. Em particular, dados $x, y \in K$, $x \neq 0$, temos que

$$x \mid y \Leftrightarrow 1 \mid yx^{-1} \Leftrightarrow yx^{-1} \in R.$$

■

Como primeira caracterização de um anel de valorização de um corpo K, temos a seguinte proposição.

Proposição 4.6 *Um subanel R de um corpo K é um anel de valorização de K se, e somente se, a divisibilidade de K correspondente a R é uma quase-ordem total.*

Demonstração. Seja $\mid$ a divisibilidade de K correspondente a R.

($\Rightarrow$:) Seja R um anel de valorização de K. Dados $x, y \in K$, $y \neq 0$, suponhamos que $x \nmid y$. Se $x = 0$, então $y \mid 0$. Se $x \neq 0$, então $1 \nmid (yx^{-1})$ e, daí, $yx^{-1} \notin R$. Logo, $xy^{-1} \in R$, ou seja, $1 \mid xy^{-1}$. Segue que $y \mid x$ e, portanto, $\mid$ é total.

($\Leftarrow$:) Suponhamos que $\mid$ é total. Dado $x \in K$, $x \notin R$, temos que $1 \nmid x$ e, daí, $x \mid 1$. Logo, $1 \mid x^{-1}$ e, portanto, $x^{-1} \in R$. Assim, temos que R é um anel de valorização de K. ■

O seguinte teorema nos dá um segunda caracterização dos anéis de valorização de um corpo K. Para uma melhor compreensão do mesmo, no entanto, necessitaremos da definição que segue.

Definição 4.7 *Um subconjunto M de um corpo K é dito <u>R-estável</u> se, e somente se, $RM \subseteq M$, isto é, $ax \in M$, para quaisquer $a \in R$ e $x \in M$.*

Teorema 4.8 *Seja R um anel e seja K corpo de frações de R. Se $\mathcal{L}$ (respect. $\mathcal{J}$) é o conjunto, ordenado pela inclusão, de todos os subconjuntos R-estáveis não-vazios de R (respect. de K), então, as seguintes afirmações são equivalentes:*

(*i*) *R é um anel de valorização de K.*

(*ii*) *$\mathcal{J}$ é totalmente ordenado.*

(*iii*) *$\mathcal{L}$ é totalmente ordenado.*

(*iv*) *O subconjunto de* $\mathfrak{L}$ *consistindo de todos os ideais principais de* R *é totalmente ordenado.*

Neste caso, $\mathfrak{L}$ *é o conjunto de todos os ideais de* R *e* $\mathfrak{J}$ *dos* R*-submódulos de* K*.*

Demonstração. $(i) \Rightarrow (ii)$: Suponhamos que o conjunto $\mathfrak{J}$ não é totalmente ordenado. Sejam, então, $M, N \in \mathfrak{J}$ tais que $M \nsubseteq N$ e $N \nsubseteq M$. Tomemos $x \in M \backslash N$ e $y \in N \backslash M$. Daí, como $(xy^{-1})y = x \notin N$ e $(yx^{-1})x = y \notin M$, obtemos $xy^{-1} \notin R$ e $yx^{-1} = (xy^{-1})^{-1} \notin R$, respectivamente. Portanto, R não é um anel de valorização de K.

$(ii) \Rightarrow (iii)$ e $(iii) \Rightarrow (iv)$ são triviais.

$(iv) \Rightarrow (i)$: Seja $x \in K$, $x \neq 0$, digamos $x = \dfrac{a}{b}$, onde $a, b \in R$, $a \neq 0$, $b \neq 0$. Se $x \notin R$, então $Ra \nsubseteq Rb$. Daí, $Rb \subseteq Ra$. Logo, $x^{-1} = \dfrac{b}{a} \in R$. Portanto, R é um anel de valorização de K.

Para provarmos a última afirmação é suficiente mostrarmos que, dados $M \in \mathfrak{J}$ e $x, y \in M$, com $x \neq 0$ e $y \neq 0$, obtemos $x - y \in M$: se $Rx \subseteq Ry$, então $x - y = (y^{-1}x - 1)y \in Ry \subseteq M$; se $Rx \nsubseteq Ry$, então $Ry \subseteq Rx$ e, daí, $x - y = (1 - x^{-1}y)x \in Rx \subseteq M$. Portanto, M é um R-submódulo. ∎

Corolário 4.9 *Qualquer ideal finitamente gerado de um anel de valorização é um ideal principal.*

Demonstração. Seja I um ideal finitamente gerado do anel de valorização R, digamos

$$I = Ra_1 + \cdots + Ra_n, \text{ onde } a_1, \ldots, a_n \in R.$$

Pelo teorema anterior, o conjunto $\{Ra_1, \ldots, Ra_n\}$ tem um elemento máximo, digamos Ra_1. Então, $Ra_1 \supseteq Ra_i$, para todo $i = 1, \ldots, n$. Daí, $I = \sum_{i=1}^{n} Ra_i \subseteq Ra_1 \subseteq I$. Logo, $I = Ra_1$. Portanto, I é um ideal principal de R. ∎

No próximo teorema, usaremos o fato de que, para qualquer domínio R de K e qualquer ideal primo P_0 de R, os ideais primos Q do anel de frações R_{P_0} (localização de R em P_0) estão em correspondência bijetora com os ideais primos P de R que estão contidos em P_0 por

$$Q = PR_{P_0} \text{ e } P = Q \cap R.$$

Em particular, R_{P_0} é um anel local cujo ideal maximal é $P_0 R_{P_0}$. [Atiyah, Mac.Donald, corolário 3.13, pg. 42]

Teorema 4.10 *Sejam* R *um anel de valorização do corpo* K*,* $\mathcal{P}$ *o conjunto de todos os ideais primos* P *de* R *e* $\mathcal{S}$ *o conjunto de todos os subanéis* S *de* K *que contêm* R*. Então, qualquer* $S \in \mathcal{S}$ *é um anel de valorização de* K*, com ideal maximal* $M_S \subseteq R$ *e existe uma bijeção que inverte a inclusão* $\mathcal{S} \leftrightarrow \mathcal{P}$*, dada por* $P = M_S$ *e* $S = R_P$*. Além disso,* $\mathcal{S}$ *e* $\mathcal{P}$ *são ordenados pela inclusão.*

Demonstração. Seja $S \in \mathcal{S}$. Dado $x \in K$, $x \notin S$, temos que $x \notin R$. Daí, $x^{-1} \in R$. Logo, $x^{-1} \in S$. Portanto, S é um anel de valorização de K. Por outro lado, dado $x \in M_S$, temos que $x \in S$ e $x^{-1} \notin S$. Daí, $x^{-1} \notin R$. Logo, $x \in R$ e, portanto, $M_S \subseteq R$.

Afirmamos que $M_S = M_S \cap R$ é um ideal primo de R.

De fato, dados $x, y \in R$, $x \notin M_S$, $y \notin M_S$, temos que $x^{-1}, y^{-1} \in S$. Daí,

$$y^{-1}x^{-1} = (xy)^{-1} \in S.$$

Logo, $xy \notin M_S$. Portanto, M_S é um ideal primo de R.

É claro que $R_{M_S} \subseteq S$. Por outro lado, dado $x \in S \backslash R$, temos que $x^{-1} \in R \subseteq S$. Daí, $x^{-1} \notin M_S$. Logo, $x = \dfrac{1}{x^{-1}} \in R_{M_S}$. Portanto, $S \subseteq R_{M_S}$. Segue que $S = R_{M_S}$.

Dado $P \in \mathcal{P}$, temos que $R_P \in \mathcal{S}$ e $M_{R_P} = M_{R_P} \cap R = PR_P \cap R = P$. Assim , temos que a correspondência considerada é, de fato, uma bijeção entre $\mathcal{S}$ e $\mathcal{P}$. Resta mostrarmos que a mesma inverte a inclusão. Dados $S_1, S_2 \in \mathcal{S}$, $S_1 \subseteq S_2$, temos que

$$x \in M_{S_2} \Rightarrow x^{-1} \notin S_2 \Rightarrow x^{-1} \notin S_1 \Rightarrow x \in S_1 \Rightarrow x \in M_{S_1}.$$

Daí, $M_{S_2} \subseteq M_{S_1}$. Por outro lado, dados $P_1, P_2 \in \mathcal{P}$, $P_1 \subseteq P_2$, temos que

$$x \in R_{P_2} \Rightarrow x = \frac{a}{b},\ a, b \in R, b \notin P_2 \Rightarrow x = \frac{a}{b},\ a, b \in R,\ b \notin P_1 \Rightarrow x \in R_{P_1}.$$

Logo, $R_{P_2} \subseteq R_{P_1}$. Portanto, a bijeção considerada inverte as inclusões.

Pelo teorema anterior, temos que $\mathcal{P}$ é totalmente ordenado pela inclusão e, daí, $\mathcal{S}$ também o é. ∎

4.2 Valorização de Krull

As valorizações apresentadas no capítulo 2 utilizaram apenas a propriedade de que o grupo de valores era um subgrupo do grupo abeliano ordenado $\mathbb{R}$, conforme Krull observou. No conceito de valorizações de Krull, utilizamos um grupo de valores abeliano e totalmente ordenado Γ. Para as propriedades de Γ, veja o Apêndice.

Sejam Γ um grupo abeliano totalmente ordenado, K um corpo e $K^* = K \backslash \{0\}$.

Definição 4.11 *Uma aplicação $v : K \to \Gamma \cup \{\infty\}$ é dita uma valorização de Krull de K se, e somente se, v tem as propriedades $(V.1), (V.2)$ e $(V.3)$ apresentadas no capítulo 2. Neste caso, estamos supondo que Γ está escrito aditivamente.*

Observamos que se $v : K^* \to \Gamma$ é uma valorização de Krull e $v(x) \neq v(y)$, $x, y \in K$, então

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

Definição 4.12 *De maneira análoga, definimos $\Gamma_v = v(K^*)$ o grupo de valores de v, que é um subgrupo de Γ. Dizemos que as valorizações de Krull de K, $v : K^* \to \Gamma_v$ e $w : K^* \to \Gamma_w$ são equivalentes se, e somente se, existe um isomorfismo de grupos ordenados $\phi : \Gamma_v \to \Gamma_w$, tal que $w = \phi \circ v$.*

Proposição 4.13 *Se v é uma valorização de Krull de K, então temos que o conjunto $O_v = \{x \in K; v(x) \geq 0\}$ é um anel de valorização de K. Mais ainda, se v e w são equivalentes, $O_v = O_w$.*

Demonstração. Se $x \in K \backslash O_v$, então $v(x) < 0$, $v(x^{-1}) > 0$ e $x^{-1} \in O_v$. Se v e w são equivalentes, então para todo $x \in K$ temos $v(x) \geq 0$ se, e somente se, $w(x) \geq 0$ (pois $\phi : \Gamma_v \to \Gamma_w$ e $\phi^{-1} : \Gamma_w \to \Gamma_v$ são isomorfismos de grupos ordenados), logo $O_v = O_w$. ∎

Teorema 4.14 *A função $v \mapsto O_v$ induz uma bijeção do conjunto das classes de equivalência das valorizações de Krull de K no conjunto dos anéis de valorização de K.*

Demonstração. Se v_1 e v_2 são duas valorizações de Krull equivalentes de K, então, pela proposição anterior, $O_{v_1} = O_{v_2}$. Assim, a função considerada está bem definida.

Seja V um anel de valorização de K e seja U o grupo multiplicativo dos elementos invertíveis de V. Da demonstração da proposição 4.5 temos que a seguinte relação binária em K é uma divisibilidade de K: $x \mid y \Leftrightarrow yx^{-1} \in V$.

Seja $\Gamma = K^*/U$, onde $K^* = K\backslash\{0\}$, e seja $v : K^* \to \Gamma$ o homomorfismo natural. Podemos ordenar Γ escrevendo $v(x) \geq v(y)$ se, e somente se, $y \mid x$, para quaisquer $x, y \in K^*$. Assim, Γ é um grupo abeliano totalmente ordenado que será escrito aditivamente e

$$0 = \{x \in K^*;\, x \in U\} = v(1).$$

Definindo $v(0) = \infty$, afirmamos que v é uma valorização de Krull de K com $O_v = V$. Com efeito,

(V.1) $v(x) = \infty \Leftrightarrow x = 0$.

(V.2) Dados $x, y \in K^*$, $x + y \neq 0$, suponhamos que $v(x) \geq v(y)$. Então,

$$\begin{aligned} y \mid x &\Rightarrow xy^{-1} \in V \Rightarrow xy^{-1} + 1 \in V \Rightarrow (x+y)y^{-1} \in V \\ &\Rightarrow y \mid (x+y) \Rightarrow v(x+y) \geq v(y) \\ &\Rightarrow v(x+y) \geq \min\{v(x), v(y)\}. \end{aligned}$$

Para os demais casos, é claro que a desigualdade acima é satisfeita.

(V.3) Dados $x, y \in K$, $xy \neq 0$, temos que $(xy)U = (xU)(yU)$, e $v(xy) = v(x) + v(y)$.
É claro que para o caso $xy = 0$, a igualdade $v(xy) = v(x) + v(y)$ é verdadeira.

Precisamos mostrar que se $w : K^* \to \Gamma_w$ é tal que $O_w = V$, então w é equivalente a v.

De fato, como w é sobrejetora e tem núcleo U, pelo teorema fundamental dos homomorfismos, w induz um isomorfismo $\phi : K^*/U \to \Gamma_w$, é claro que esse isomorfismo preserva a ordem e $w = \phi \circ v$. ∎

Quando $\Gamma_v = \{0\}$ é o grupo trivial dizemos que $v : K^* \to \{0\}$ é a valorização trivial. Nesse caso, $O_v = K$.

Definição 4.15 *Sejam v e v' duas valorizações de Krull de K. Dizemos que v' está subordinada a v se, e somente se, $O_{v'} \supseteq O_v$. Em particular, $U_{v'} \supseteq U_v$ e $M_{v'} \subseteq M_v$.*

Observação 4.16 *Sejam v e v' duas valorizações de Krull de K. Se v' está subordinada a v, então $\Gamma_{v'} = \Gamma_v/\Delta$, onde Δ é um subgrupo convexo de Γ_v (pelo teorema 6.9 do Apêndice, o quociente de um grupo abeliano ordenado é ordenado e os subgrupos que funcionam são os convexos).*

Com efeito, pela demonstração do teorema anterior, temos que $\Gamma_v = K^*/U_v$ e $\Gamma_{v'} = K^*/U_{v'}$. Daí,

$$\Gamma_{v'} = K^*/U_{v'} \cong (K^*/U_v)/(U_{v'}/U_v) = \Gamma_v/\Delta, \text{ onde } \Delta \cong U_{v'}/U_v.$$

Observação 4.17 *Seja v uma valorização de Krull de K. Então, dado $\alpha \in \Gamma_v$, existe $x \in O_v$ tal que $v(x) = |\alpha|$, onde*

$$|\alpha| = \begin{cases} \alpha, & se \quad \alpha \geq 0 \\ -\alpha, & se \quad \alpha < 0 \end{cases}$$

Com efeito, dado $\alpha \in \Gamma_v$, temos que $\alpha = v(x)$, para algum $x \in K^*$. Se $\alpha \geq 0$, então $|\alpha| = \alpha = v(x)$ e, daí, $x \in O_v$. Se $\alpha < 0$, então $|\alpha| = -\alpha = -v(x) = v(x^{-1})$ e, daí, $x^{-1} \in O_v$.

Teorema 4.18 *Seja v uma valorização de Krull de K. Então, existe uma bijeção, que inverte a inclusão, entre os anéis de valorização de K que contêm O_v e os subgrupos convexos de Γ_v.*

Demonstração. Pelo teorema 4.10, temos que existe uma bijeção que inverte a inclusão entre os anéis de valorização de K que contêm O_v e os ideais primos de O_v. Vamos mostrar que existe uma bijeção que inverte a inclusão entre os ideais primos de O_v e os subgrupos convexos de Γ_v e, portanto, nosso teorema estará concluído.

Seja P um ideal primo qualquer de O_v.

Afirmamos que o conjunto $P^* = \{\lambda \in \Gamma_v;\ |\lambda| < v(x),\ \forall\, x \in P\}$ é um subgrupo convexo de Γ_v.

De fato, é claro que P^* é um conjunto convexo de Γ_v. Basta mostrarmos, então, que P^* é um subgrupo de Γ_v.

Dados $\alpha, \beta \in P^*$, sejam $x, y \in O_v$ tais que $v(x) = |\alpha|$ e $v(y) = |\beta|$. Então, $x \notin P$ e $y \notin P$ e, como P é um ideal primo, $xy \notin P$. Daí, para todo $z \in P$, $z \neq 0$, temos que $xyz^{-1} \notin O_v$. Logo, $v(xyz^{-1}) < 0$, isto é, $v(xy) < v(z)$. Como

$$|\alpha + \beta| \leq |\alpha| + |\beta| = v(x) + v(y) = v(xy),$$

segue que $|\alpha + \beta| < v(z)$, para todo $z \in P$. Portanto, $\alpha + \beta \in P^*$. É claro que $0 \in P^*$ e que, se $\alpha \in P^*$, então $-\alpha \in P^*$. Assim, temos que P^* é um subgrupo convexo de Γ_v.

Reciprocamente, dado qualquer subgrupo convexo Δ de Γ_v, definimos o conjunto

$$\Delta^* = \{x \in O_v;\ v(x) > |\lambda|, \forall\, \lambda \in \Delta\}.$$

Afirmamos que Δ^* é um ideal primo de O_v.

De fato, notemos que $\Delta^* = \bigcap_{\lambda \in \Delta} I_\lambda$, onde $I_\lambda = \{x \in O_v;\ v(x) > |\lambda|\}$.

Como, para todo $\lambda \in \Delta$, I_λ é um ideal de O_v, segue que Δ^* é um ideal de O_v. Resta mostrarmos que Δ^* é um ideal primo de O_v.

Sejam $x, y \in O_v$ tais que $x \notin \Delta^*$ e $y \notin \Delta^*$. Então, $v(x), v(y) \in \Delta$. Daí, $v(xy) = v(x) + v(y) \in \Delta$. Logo, $xy \notin \Delta^*$. É claro que $1 \notin \Delta^*$. Portanto, Δ^* é um ideal primo de O_v.

Para concluírmos nossa bijeção, devemos mostrar que $P^{**} = P$ e $\Delta^{**} = \Delta$, onde

$$P^{**} = \{x \in O_v;\ v(x) > |\lambda|,\ \forall\, \lambda \in P^*\} \text{ e } \Delta^{**} = \{\lambda \in \Gamma_v;\ |\lambda| < v(x),\ \forall\, x \in \Delta^*\}.$$

É claro que $P^{**} \supseteq P$ e $\Delta^{**} \supseteq \Delta$. Por outro lado, dado $x \in O_v$, $x \notin P$, temos que $v(x) \in P^*$ e, daí, $x \notin P^{**}$. Logo, $P^{**} = P$. Analogamente, dado $\lambda \in \Gamma_v$, $\lambda \notin \Delta$, temos que λ majora todos os elementos de Δ e $|\lambda| = v(x)$, para algum $x \in O_v$. Assim, $|\mu| < v(x)$, para todo $\mu \in \Delta$. Logo, $x \in \Delta^*$ e, daí, $v(x) \notin \Delta^{**}$, isto é, $\lambda \notin \Delta^{**}$. Portanto, $\Delta^{**} = \Delta$.

É claro que

$$P_1 \subseteq P_2 \Rightarrow P_1^* \supseteq P_2^* \text{ e}$$
$$\Delta_1 \subseteq \Delta_2 \Rightarrow \Delta_1^* \supseteq \Delta_2^*,$$

ou seja, nossa bijeção inverte a inclusão. ∎

Como o conjunto dos subgrupos convexos de um grupo abeliano ordenado é totalmente ordenado pela inclusão, segue a primeira consequência deste teorema.

Corolário 4.19 *O conjunto dos anéis de valorização de K que estão acima do anel de valorização V de K é totalmente ordenado pela inclusão.*

Demonstração. Pelo teorema 4.14, existe uma valorização de Krull v de K tal que $V = O_v$. Como, pelo teorema 6.13 do Apêndice, o conjunto dos subgrupos convexos de Γ_v é totalmente ordenado pela inclusão, segue do teorema anterior que o conjunto dos anéis de valorização de K que contêm O_v é totalmente ordenado pela inclusão. ∎

Os resultados apresentados no capítulo 2 para um valorização de K são particularidades dos resultados válidos para uma valorização de Krull de K de posto 1.

Definição 4.20 *Uma valorização de Krull v de K é dita de posto 1 se, e somente se, Γ_v tem posto 1, isto é, se, e somente se, Γ_v não tem subgrupo convexo próprio não-trivial se, e somente se, existe um homomorfismo $\phi : \Gamma_v \to \mathbb{R}$ que preserva a ordem (teorema 6.17 do Apêndice).*

Definição 4.21 *Dizemos que um anel de valorização O_v de K é de posto 1 se, e somente se, a valorização de Krull de K v correspondente a O_v é de posto 1.*

Em particular, uma valorização de Krull de K v de posto 1 é discreta se, e somente se, Γ_v é um grupo abeliano ordenado isomorfo a $\mathbb{Z}$ (proposição 6.20 do Apêndice).

Daqui por diante, as valorizações de Krull serão chamadas simplesmente de valorizações.

O teorema anterior também nos dá uma descrição das valorizações de K de posto 1, em termos do seu anel de valorização. Isto é o que trata o seguinte corolário.

Corolário 4.22 *Uma valorização v de K é de posto 1 se, e somente se, o seu anel de valorização O_v é maximal entre os anéis de valorização próprios de K.*

Demonstração. Pelo teorema anterior, temos que os subgrupos convexos de Γ_v correspondem aos anéis de valorização de K que contêm O_v, portanto, O_v é maximal precisamente quando Γ_v não tem subgrupo próprio convexo não-trivial, isto é quando Γ_v tem posto 1, ou seja, quando v é de posto 1. ∎

Este último resultado nos permite dar uma outra caracterização dos anéis de valorização de K de posto 1, isto é, dos anéis de valorização de K correspondentes às valorizações de K de posto 1.

Proposição 4.23 *Seja V um subanel de K. Então, as seguintes afirmações são equivalentes:*

(i) *V é um anel de valorização de K de posto 1.*

(ii) *V é um anel de valorização de K que tem um único ideal primo não-nulo.*

(iii) *V não é um corpo e é um subanel próprio maximal de K.*

Demonstração. $(i) \Rightarrow (ii)$: Suponhamos que V tem um ideal primo não-nulo, digamos P, além do seu ideal maximal. Então, $V_P \supset V$.

Sejam v e v' as valorizações de K correspondentes a V e a V_P, respectivamente. Então, pela observação 4.16, $\Gamma_{v'} \cong \Gamma_v/\Delta$, onde Δ é um subgrupo convexo de Γ. Daí,

$$\text{posto}\,\Gamma_v = \text{posto}\,\Delta + \text{posto}\,(\Gamma_v/\Delta) \Rightarrow \text{posto}\,\Gamma_v = \text{posto}\,\Delta + \text{posto}\,\Gamma_{v'} \geq 2.$$

Logo, v não tem posto 1 e, portanto, V não é um anel de valorização de K de posto 1.

$(ii) \Rightarrow (iii)$: Seja V um anel de valorização de K com um único ideal primo não-nulo. É claro que que V não é um corpo. Suponhamos, por contradição, que W é um subanel de K tal que $W \supset V$. Então, pelo teorema 4.10, temos que W é um anel de valorização de K. Sejam M e N os ideais maximais de V e W, respectivamente. Então, novamente pelo teorema 4.10, temos que $N = N \cap V$ é um ideal primo não-nulo de V e $N \subseteq M$.

Afirmamos que $N \subset M$.

Com efeito, dado $u \in W \backslash V$, temos que

$$u \in W \text{ e } u \notin V \Rightarrow u \in W \text{ e } u^{-1} \in V \subset W \Rightarrow u \in M \backslash N.$$

Portanto, N é um ideal primo não-nulo de V distinto do ideal maximal M de V, o que é uma contradição.

$(iii) \Rightarrow (i)$: Seja V um subanel próprio maximal de K que não é um corpo. Seja $c \in V$, $c \neq 0$, tal que $c^{-1} \notin V$. Então, $V[c^{-1}]$ é um subanel de K contendo V propriamente. Daí, $V[c^{-1}] = K$.

Afirmamos que $K = V[c^{-1}]$ não é um V-módulo finitamente gerado.

Com efeito, suponhamos, por contradição, que $K = V[c^{-1}]$ é um V-módulo finitamente gerado, digamos por $1, c^{-1}, \ldots, c^{-m}$. Então, dado $x \in K$, temos que $x = \sum_{i=0}^{m} a_i c^{-i}$, onde $a_i \in V$.

Daí,

$$\begin{aligned} x &= a_0 + a_1 c^{-1} + \cdots + a_m c^{-m} \\ &= a_0 + \frac{a_1}{c} + \cdots + \frac{a_m}{c^m} \\ &= \frac{a_0 c^m + a_1 c^{m-1} + \cdots + a_m}{c^m} \\ &= \frac{a}{c^m}, \end{aligned}$$

onde $a = a_0 c^m + a_1 c^{m-1} + \cdots + a_m \in V$.

Logo, $x = ac^{-m}$, para algum $a \in V$ e para algum m fixado.

Tomando, então, $x = c^{-m-1} = (c^{-1})^{m+1} \in K$, obtemos $c^{-m-1} = ac^{-m}$ e, daí, $c^{-1} = a \in V$, o que é uma contradição.

Afirmamos, agora, que V é um anel de valorização de K.

De fato, suponhamos, por contradição, que existe $u \in K$, $u \neq 0$, tal que $u, u^{-1} \notin V$. Então, $V[u] = V[u^{-1}] = K$. Daí,

$$\begin{aligned} u &= a_0 + \frac{a_1}{u} + \frac{a_2}{u^2} + \cdots + \frac{a_r}{u^r}, \text{ onde } a_i \in V,\ i = 0, 1, \ldots, r \\ &\Rightarrow u^{r+1} = a_0 u^r + a_1 u^{r-1} + \cdots + a_r \\ &\Rightarrow u^{r+1} \in [1, u, \ldots, u^r] \\ &\Rightarrow u^n \in [1, u, \ldots, u^r],\ \forall\, n \geq r+1. \end{aligned}$$

Logo, $K = V[u]$ é um V-módulo finitamente gerado por $1, u, \ldots, u^r$, o que é uma contradição com a afirmação anterior. Portanto, $u \in V$ ou $u^{-1} \in V$, isto é, V é um anel de valorização.

Seja v a valorização de K correspondente ao anel de valorização V de K. Como, por hipótese, V é um subanel próprio maximal de K, segue, do corolário anterior, que v é de posto 1. Portanto, V é um anel de valorização de K de posto 1. ∎

Capítulo 5

Domínios de Dedekind

Neste último capítulo, estudaremos as extensões de uma valorização de corpos completos e incompletos, apresentaremos a definição de uma família de lugares que tem propriedade da aproximação forte e, finalmente, daremos uma nova caracterização aos domínios de Dedekind mostrando a equivalência desta com a definição usual.

5.1 Generalidades de extensões

Nesta seção, apresentaremos, basicamente, a definição de grau residual e de índice de ramificação de uma extensão de corpos valorizados $L|K$ e estabeleceremos uma desigualdade entre o produto destes e a dimensão de L como K-espaço vetorial, que será de grande importância no decorrer deste capítulo.

Proposição 5.1 *Sejam $L|K$ uma extensão de corpos valorizados e w uma valorização de L tal que $w|_K = v$. Então, $M_v = O_v \cap M_w$ e $L_w|K_v$ é uma extensão de corpos.*

Demonstração. É claro que $M_v = O_v \cap M_w$. Consideremos o homomorfismo $\psi : K_v \to L_w$ definido por $\psi(a + M_v) = a + M_w$, para todo $a \in O_v$. Temos que $N(\psi) = O_v \cap M_w$. Logo, $N(\psi) = M_v$. Portanto, ψ é injetor. ∎

Definição 5.2 *Com as notações da proposição anterior, definimos o grau residual em $L|K$ como a dimensão de L_w como K_v-espaço vetorial e o mesmo será denotado por f, isto é,*

$$f = [L_w : K_v];$$

o índice de ramificação em $L|K$ é o índice de Γ_v como subgrupo de Γ_w e será denotado por e, isto é,

$$e = (\Gamma_w : \Gamma_v).$$

A extensão $L|K$ é dita ramificada quando $e > 1$ e não-ramificada quando $e = 1$.

Observação 5.3 *Sejam $M|L$ e $L|K$ extensões de corpos valorizados. Se denotarmos por $f_{M|L}$, $e_{M|L}$ e $[M : L]$, respectivamente, o grau residual em $M|L$, o índice de ramificação em $M|L$ e a dimensão de M como L-espaço vetorial, então $f_{M|L} = f_{M|L} f_{L|K}$, $e_{M|K} = e_{M|L} e_{L|K}$ e $[M : K] = [M : L][L : K]$.*

O seguinte teorema estabelece uma desigualdade básica entre o grau residual, o índice de ramificação em uma extensão de corpos finita $L|K$ e a dimensão de L como K-espaço vetorial.

Teorema 5.4 *Seja $L|K$ uma extensão de corpos valorizados, onde a valorização w de L estende a valorização v de K. Se $L|K$ é finita, então*

$$ef \leq [L:K],$$

e se v é trivial ou discreta, então w também o é. Se v é discreta e K é completo, então

$$ef = [L:K].$$

Demonstração. Afirmamos, inicialmente, que se $u_1, \ldots, u_r \in O_w$ são tais que seus resíduos $\overline{u}_1, \ldots, \overline{u}_r \in L_w$ são linearmente independentes sobre o corpo residual K_v, então, para quaisquer $\alpha_1, \ldots, \alpha_r \in K$,

$$w(\alpha_1 u_1 + \cdots + \alpha_r u_r) = \min\{v(\alpha_1), \ldots, v(\alpha_r)\}. \qquad (*)$$

Em particular, $u_1, \ldots, u_r \in O_w$ são linearmente independentes sobre K e

$$w(\alpha_1 u_1 + \cdots + \alpha_r u_r) \in \Gamma_v, \text{ para quaisquer } \alpha_1, \ldots, \alpha_r \in K.$$

De fato, enumeremos os u_i's de modo que

$$v(\alpha_1) = \min\{v(\alpha_1), \ldots, v(\alpha_r)\}.$$

Como $\overline{u}_i \neq 0$, para todo $i = 1, \ldots, r$, temos que $w(u_i) = 0$, para todo $i = 1, \ldots, r$. Daí,

$$\begin{aligned} w(\alpha_1 u_1 + \cdots + \alpha_r u_r) &\geq \min\{w(\alpha_1 u_1), \ldots, w(\alpha_r u_r)\} \\ &= \min\{w(\alpha_1) + w(u_1), \ldots, w(\alpha_r) + w(u_r)\} \\ &= \min\{w(\alpha_1), \ldots, w(\alpha_r)\} \\ &= v(\alpha_1). \end{aligned}$$

Suponhamos, por contradição, que $w(\alpha_1 u_1 + \cdots + \alpha_r u_r) > v(\alpha_1)$. Então, $\alpha_1 \neq 0$. Daí,

$$w\Big(u_1 + \frac{\alpha_2}{\alpha_1} u_2 + \cdots + \frac{\alpha_r}{\alpha_1} u_r\Big) > 0,$$

com $w\Big(\dfrac{\alpha_j}{\alpha_1}\Big) = w(\alpha_j) - w(\alpha_1) = v(\alpha_j) - v(\alpha_1) \geq 0$, para todo $j = 2, \ldots, r$. Logo,

$$\overline{u}_1 + \Big(\frac{\overline{\alpha_2}}{\alpha_1}\Big) u_2 + \cdots + \Big(\frac{\overline{\alpha_r}}{\alpha_1}\Big) u_r = 0,$$

o que contradiz o fato de que $\overline{u}_1, \ldots, \overline{u}_r$ são linearmente independentes sobre K_v. Portanto,

$$w(\alpha_1 u_1 + \cdots + \alpha_r u_r) = v(\alpha_1) = \min\{v(\alpha_1), \ldots, v(\alpha_r)\}.$$

Sejam $\pi_1, \ldots, \pi_s \in L$ tais que $w(\pi_i) \not\equiv w(\pi_j) \bmod \Gamma_v$, para todo $i, j = 1, \ldots, s$, $i \neq j$.

Afirmamos que os rs elementos $u_i \pi_j$ são linearmente independentes sobre K.

Com efeito, seja $\displaystyle\sum_{i,j} a_{ij} u_i \pi_j = 0$, onde $a_{ij} \in K$. Escrevendo $a_j = \displaystyle\sum_i a_{ij} u_i$, obtemos $\displaystyle\sum_j a_j \pi_j = 0$.

Suponhamos, por contradição, que $a_j \neq 0$ para algum j. Então, pelo princípio da dominação, temos que

$$w(a_h \pi_h) = w(a_k \pi_k), \text{ para algum } h, k,\ h \neq k.$$

Daí,

$$w(a_h) - w(a_k) = w(\pi_h) - w(\pi_k),$$

o que é uma contradição, visto que $w(a_h) - w(a_k) \in \Gamma_v$, pela particularidade que segue de $(*)$, e $w(\pi_h) - w(\pi_k) \notin \Gamma_v$. Logo, $a_j = 0$, para todo $j = 1, \ldots, s$. Novamente pela particularidade que segue de $(*)$, obtemos $a_{ij} = 0$, para todo $i = 1, \ldots, r$ e $j = 1, \ldots, s$. Portanto, os rs elementos $u_i\pi_j$ são linearmente independentes sobre K.

Assim , temos que $rs \leq [L : K]$. Tomando $r = f = [L_w : K_v]$ e $s = e = (\Gamma_w : \Gamma_v)$, obtemos

$$ef \leq [L : K].$$

Se v é trivial, então Γ_w é finito de ordem e. Como o único grupo ordenado finito é o grupo trivial, segue que w é trivial e $e = 1$.

Se v é discreta, então podemos supor v normalizada, isto é, $\Gamma_v = \mathbb{Z}$. Daí, $\Gamma_w = \frac{1}{e}\mathbb{Z} \cong \mathbb{Z}$. Logo, w também é discreta.

Se v é discreta e K é completo, então, como vimos acima, w também é discreta e, pelo lema 1.40, L é completo. Tomando uniformizantes π_v e π_w para v e w, respectivamente, podemos tomar todo elemento $x \in L$, $x \neq 0$, na forma

$$x = \sum_{i=-N}^{\infty} \alpha_i \pi_w^i,$$

onde $w(x) = -N$ e cada $\alpha_i \in O_w$ está em um conjunto de representantes de L_w.

Afirmamos que

$$x = \sum_{i=-N}^{\infty} \sum_{j,k} a_{ijk} u_j \pi_v^i \pi_w^k, \text{ onde } a_{ijk} \in K,\ 1 \leq j \leq f \text{ e } 0 \leq k \leq e-1.$$

Com efeito, sejam $u_1, \ldots, u_f \in O_w$ tais que $u_1, \ldots, u_f$ constituem uma base de L_w como K_v-espaço vetorial. Então, para cada α_i no conjunto de representantes de L_w, temos

$$\overline{\alpha}_i = \sum_{j=1}^{f} \overline{\alpha'}_{ij} \overline{u}_j,$$

onde cada $\alpha'_{ij} \in O_v$ está no conjunto de representantes de K_v. Daí, no lugar de α_i, podemos tomar $\sum_{j=1}^{f} \alpha'_{ij} u_j$. Além disso, cada potência π_w^i pode ser substituída por uma combinação linear das potências $\pi_v^i, \pi_v^i\pi_w, \ldots, \pi_v^i\pi_w^{e-1}$, visto que $w(\pi_v^i) = i \in \Gamma_w$ está em uma única classe de Γ_w módulo Γ_v e

$$\overline{w(\pi_v^i)} = \overline{i}, \overline{w(\pi_v^i\pi_w)} = \overline{i + \tfrac{1}{e}}, \ldots, \overline{w(\pi_v^i\pi_w^{e-1})} = \overline{i + \tfrac{e-1}{e}}$$

são e classes distintas de Γ_w módulo Γ_v. Logo,

$$x = \sum_{i=-N}^{\infty} \Big(\sum_{j=1}^{f} \alpha'_{ij} u_j \Big) \Big(\sum_{k=0}^{e-1} \beta_k \pi_v^i \pi_w^k \Big), \text{ com } \beta_k \in O_v.$$

Portanto,

$$x = \sum_{i=-N}^{\infty} \sum_{j,k} a_{ijk} u_j \pi_v^i \pi_w^k, \text{ onde } a_{ijk} \in K,\ 1 \leq j \leq f \text{ e } 0 \leq k \leq e-1.$$

Assim, temos que $\{u_j\pi_w^k;\ 1 \leq j \leq f,\ 0 \leq k \leq e-1\}$ é um conjunto de geradores de L. Logo $[L : K] \leq ef$ e, portanto, a igualdade segue. ∎

Corolário 5.5 *Se $L|K$ é uma extensão algébrica e K tem uma valorização v com extensão w a L, então Γ_w/Γ_v é um grupo de torção e $L_w|K_v$ é algébrica.*

Demonstração. Basta observarmos que podemos escrever $L|K$ como uma união de extensões finitas e aplicarmos, então, o teorema anterior a estas extensões. ∎

5.2 Extensões de corpos completos

Sejam K um corpo valorizado e L uma extensão de K finitamente gerada. Examinaremos, agora, modos de estender uma valorização de K a L. Por indução, será suficiente considerarmos uma extensão simples $L = K(\alpha)$ e estudaremos, separadamente, os casos em que α é algébrico ou transcendente sobre K. Assim, nossa primeira tarefa é estender uma valorização v de K ao corpo de funções racionais $K(x)$, onde x é transcendente sobre K. Daremos uma construção simples de uma valorização w de $K(x)$ que estende v.

Definimos uma aplicação w sobre o anel de polinômios $K[x]$ da seguinte maneira:

$$w(f(x)) = \min\{v(a_0), v(a_1), \ldots, v(a_n)\},$$

para qualquer $f(x) = a_0 + a_1x + \cdots + a_nx^n \in K[x]$.

É claro que w coincide com v em K.

Afirmamos que w é uma valorização de $K[x]$.

De fato,

(V.1) Seja $f(x) \in K[x]$, com $f(x) = \sum_i a_i x^i$. Então,

$$\begin{aligned} w(f(x)) = \infty &\Leftrightarrow \min_i\{v(a_i)\} = \infty \Leftrightarrow v(a_i) = \infty, \forall\, i \\ &\Leftrightarrow a_i = 0, \forall\, i \Leftrightarrow f(x) = 0. \end{aligned}$$

(V.2) Sejam $f(x), g(x) \in K[x]$, com $f(x) = \sum_i a_i x^i$ e $g(x) = \sum_i b_i x^i$, tais que

$$w(f(x)) = \min_i\{v(a_i)\} = v(a_r) \text{ e } w(g(x)) = \min_i\{v(b_i)\} = v(b_s).$$

Temos que $f(x) + g(x) = \sum_i c_i x^i$, onde $c_i = a_i + b_i$. Daí,

$$\begin{aligned} w(f(x)+g(x)) &= \min_i\{v(c_i)\} = \min_i\{v(a_i+b_i)\} \\ &\geq \min_i\{\min\{v(a_i), v(b_i)\}\} \\ &= \min\{\min_i\{v(a_i)\}, \min_i\{v(b_i)\}\} \\ &= \min\{v(a_r), v(b_s)\} \\ &= \min\{w(f(x)), w(g(x))\}. \end{aligned}$$

(V.3) Sejam $f(x), g(x) \in K[x]$, com $f(x) = \sum_i a_i x^i$ e $g(x) = \sum_i b_i x^i$, e r e s os menores índices tais que

$$\min_i\{v(a_i)\} = v(a_r) \text{ e } \min_i\{v(b_i)\} = v(b_s).$$

Temos que $f(x)g(x) = \sum_i c_i x^i$, onde $c_i = \sum_{\lambda+\mu=i} a_\lambda b_\mu$. Então,

$$\begin{aligned} v(c_i) &= v\Big(\sum_{\lambda+\mu=i} a_\lambda b_\mu\Big) \geq \min_{\lambda+\mu=i}\{v(a_\lambda b_\mu)\} \\ &= \min_{\lambda+\mu=i}\{v(a_\lambda) + v(b_\mu)\} \geq v(a_r) + v(b_s). \end{aligned}$$

Assim, se exibirmos um índice k de modo que $v(c_k) = v(a_r) + v(b_s)$, então

$$\min_i \{v(c_i)\} = v(c_k)$$

e, daí,

$$w(f(x)g(x)) = w(f(x)) + w(g(x)).$$

Afirmamos que $v(c_{r+s}) = v(a_r) + v(b_s)$. Com efeito, temos que

$$c_{r+s} = a_0b_{r+s} + a_1b_{r+s-1} + \cdots + a_rb_s + \cdots + a_{r+s-1}b_1 + a_{r+s}b_0.$$

Escrevendo, então,

$$u = a_0b_{r+s} + \cdots + a_{r-1}b_{s+1} + a_{r+1}b_{s-1} + \cdots + a_{r+s}b_0,$$

obtemos $c_{r+s} = u + a_rb_s$. Pelas escolhas dos índices r e s temos que,

$$0 \leq i \leq r-1 \text{ e } s+1 \leq j \leq r+s \Rightarrow v(a_i) > v(a_r) \text{ e } v(b_j) \geq v(b_s) \text{ e}$$
$$r+1 \leq i \leq r+s \text{ e } 0 \leq j \leq s-1 \Rightarrow v(a_i) \geq v(a_r) \text{ e } v(b_j) > v(b_s).$$

Daí,

$$v(a_ib_j) = v(a_i) + v(b_j) > v(a_r) + v(b_s),$$

para quaisquer i, j, $0 \leq i, j \leq r+s$, $i \neq r$ e $j \neq s$. Logo, $v(u) > v(a_r) + v(b_s)$. Portanto,

$$v(c_{r+s}) = v(u + a_rb_s) = \min\{v(u), v(a_r) + v(b_s)\} = v(a_r) + v(b_s).$$

Podemos estender, de modo único, w a uma valorização de $K(x)$, ainda denotada w, definida por

$$w\Big(\frac{f(x)}{g(x)}\Big) = w(f(x)) - w(g(x)),$$

para quaisquer $f(x), g(x) \in K[x]$, com $g(x) \neq 0$.

A valorização w assim definida é chamada *extensão gaussiana* de v em $K(x)$. Claramente, v e w têm o mesmo grupo de valores, isto é, $\Gamma_v = \Gamma_w$. Além disso, $w(x) = 0$.

Afirmamos que a imagem $\overline{x}$ de x no corpo residual L_w, onde $L = K(x)$, é transcendente sobre K_v.

Com efeito, suponhamos, por contradição, que x satisfaça uma equação polinomial sobre K_v. Então, existe um polinômio

$$p(x) = \alpha_0 + \alpha_1x + \cdots + \alpha_rx^r \in K[x],$$

tal que $v(\alpha_i) \geq 0$, com $v(\alpha_i) = 0$ para pelo menos um índice i, de modo que

$$p(\overline{x}) = \sum_{i=1}^{r} \overline{\alpha}_i\overline{x}^i = 0.$$

Daí, $w(p(x)) > 0$, o que é uma contradição, visto que, por definição, $w(p(x)) = 0$.

Afirmamos, agora, que L_w é o corpo de funções racionais $K_v(\overline{x})$.

De fato, é claro que $K_v(\overline{x}) \subseteq L_w$. Seja, então, $y \in L = K(\overline{x})$, onde $y = \dfrac{f(x)}{g(x)}$, com $f(x) = \sum_i a_ix^i$ e $g(x) = \sum_j b_jx^j$, tal que $y \in O_w$. Então,

$$w(y) \geq 0 \Rightarrow w(f(x)) - w(g(x)) = v(a_{i_0}) - v(b_{j_0}) \geq 0,$$

onde $v(a_{i_0}) = \min_i \{v(a_i)\}$ e $v(b_{j_0}) = \min_j \{v(b_j)\}$.

Podemos escrever y como o quociente de dois polinômios com coeficientes em O_v.

Com efeito, temos que

$$y = \frac{b_{j_0}^{-1} f(x)}{b_{j_0}^{-1} g(x)} = \frac{r(x)}{s(x)},$$

onde $w(r(x)) = v(b_{j_0}^{-1} a_{i_0}) = -v(b_{j_0}) + v(a_{i_0}) \geq 0$ e $w(s(x)) = v(1) = 0$.

Assim, $r(x), s(x) \in O_v[x] \subset O_w$. Logo,

$$\overline{y} = \Big(\overline{\frac{r(x)}{s(x)}}\Big) = \frac{\overline{r(x)}}{\overline{s(x)}} \in K_v(\overline{x}).$$

Portanto, $L_w \subseteq K_v(x)$.

Concluímos, então, o seguinte teorema:

Teorema 5.6 *Sejam K um corpo com uma valorização v e $L = K(x)$ uma extensão puramente transcendente. Então, a extensão gaussiana de v a L é uma valorização de L, com o mesmo grupo de valores de v e com corpo residual $K_v(\overline{x})$, o qual é uma extensão puramente transcendente do corpo residual K_v de K.* ∎

Observamos que existem outras extensões de v a $K(x)$, entretanto não serão necessárias neste contexto.

Consideremos, agora, o caso em que α é algébrico sobre K, isto é, o caso em que $L = K(\alpha)$ é uma extensão algébrica do corpo K. Pelo teorema 1.41 e pela bijeção existente entre os valores absolutos não-arquimedianos e as valorizações de posto 1, temos que, se o corpo K é completo com a valorização de posto 1 v, então existe no máximo uma extensão w de v a L. Vamos mostrar que, de fato, tal extensão existe e, mais ainda, vamos exibí-la. Para tal, precisaremos do conceito de um elemento inteiro sobre um subanel R de K, que recordaremos brevemente.

Seja K um corpo e seja R um subanel de K. Um elemento $c \in K$ é dito *inteiro sobre R* se satisfaz uma equação mônica sobre R, digamos

$$c^n + a_1 c^{n-1} + \cdots + a_n = 0, \text{ onde } a_i \in R.$$

Se todo elemento de K, inteiro sobre R, está em R, então dizemos que R é *integralmente fechado em K*. Se K é o corpo de frações de R, dizemos, simplesmente, que R é *integralmente fechado*.

O conjunto de todos os elementos de K inteiros sobre R é chamado *fecho inteiro de R em K* e este sempre contém R, visto que qualquer elemento $c \in R$ satisfaz a equação $x - c = 0$. Além disso, o fecho inteiro de R é um subanel de K e, para mostrarmos isto, apresentamos o seguinte resultado:

Lema 5.7 *Seja R um subanel de um corpo K. Um elemento $c \in K$ é inteiro sobre R se, e somente se, existe um R-submódulo não-nulo de K finitamente gerado M, tal que $cM \subseteq M$.*

Demonstração. ($\Rightarrow$:) Seja c um inteiro sobre R, digamos

$$c^n + a_1 c^{n-1} + \cdots + a_n = 0, \text{ onde } a_i \in R.$$

Seja M o R-submódulo de K gerado por $1, c, \ldots, c^{n-1}$, isto é, $M = R + Rc + \cdots + Rc^{n-1}$. Temos que $M \subseteq R[c]$. Por outro lado, $c^n = -a_n - \cdots - a_1 c^{n-1}$ e, para todo $k \geq 0$,

$$c^{n+k} = -a_n c^k - \cdots - a_1 c^{n-1+k} \in M,$$

sempre que $\{1, c, \ldots, c^{n-1+k}\} \subseteq M$. Logo, $R[c] \subseteq M$ e, portanto, $M = R[c]$.

($\Leftarrow$:) Seja $\{u_1, \ldots, u_n\}$ um conjunto de geradores de M. Como $cM \subseteq M$, existem $a_{ij} \in R$ tais que

$$cu_i = \sum_j a_{ij} u_j.$$

Este é um sistema de equações linear homogêneo e, como $M \neq 0$, nem todos os u_i's são iguais a zero. Portanto, seu determinante é zero. Escrevendo este sistema na forma

$$\sum (c\delta_{ij} - a_{ij}) u_j = 0,$$

temos que $\det(cI - A) = 0$, onde $A = (a_{ij})$. Expandindo esta expressão, obtemos uma equação mônica de c sobre R e c é inteiro sobre R. ∎

Corolário 5.8 *Para qualquer subanel R de K, o fecho inteiro de R é um subanel de K contendo R.*

Demonstração. Seja S o fecho inteiro de R. É claro que $R \subseteq S$. Sejam $c_1, c_2 \in S$. Então, pelo teorema anterior, $c_i M_i \subseteq M_i$, $i = 1, 2$. Daí, $(c_1 + c_2)M \subseteq M$ e $(c_1 c_2)M \subseteq M$, onde $M = M_1 M_2$. Portanto, $c_1 + c_2, c_1 c_2 \in S$ e S é um subanel de K. ∎

Proposição 5.9 *Sejam K um corpo e V um anel de valorização de K. Então, V é integralmente fechado.*

Demonstração. Seja $c \in K$ inteiro sobre V. Suponhamos, por contradição, que $c \notin V$. Então, $c^{-1} \in M$, onde M é o ideal maximal de V. Como $c \in K$ é um inteiro sobre V, temos que existe um polinômio mônico $p(x) \in V[x]$, digamos $p(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$, tal que $p(c) = 0$, ou seja,

$$c^n + a_1 c^{n-1} + a_2 c^{n-2} + \cdots + a_n = 0.$$

Daí,

$$1 + a_1 c^{-1} + a_2 c^{-2} + \cdots + a_n c^{-n} = 0 \Rightarrow 1 = -(a_1 c^{-1} + a_2 c^{-2} + \cdots + a_n c^{-n}) \in M,$$

o que é uma contrdição. Logo, $c \in V$ e, portanto, V é integralmente fechado. ∎

Retornaremos, agora, para o estudo da existência de extensões de valorizações de posto 1 no caso algébrico, de importância para os nossos objetivos.

Proposição 5.10 *Seja $L|K$ uma extensão finita de corpos. Então, qualquer valorização de K de posto 1 tem uma extensão a L, também de posto 1.*

Demonstração. Seja v uma valorização de K de posto 1. Pelo corolário 4.22, temos que O_v é o subanel próprio de K maximal. Logo, K é o corpo de frações de O_v.

Seja I o fecho inteiro de O_v em L.

Afirmamos que L é o corpo de frações de I.

Com efeito, como $L|K$ é finita, temos que $L|K$ é algébrica. Assim, dado qualquer elemento $\gamma \in L$, temos que γ é algébrico sobre K e, portanto, satisfaz uma equação com coeficientes em K. Como K é o corpo de frações de O_v, multiplicando a equação anterior por um denominador comum, obtemos uma equação com coeficientes em O_v, digamos

$$a_0 x^n + a_1 x^{n-1} + \cdots + a_n = 0,\ a_0 \neq 0.$$

Daí,

$$\begin{aligned} a_0\gamma^n + a_1\gamma^{n-1} + \cdots + a_n = 0 &\Rightarrow a_0^n\gamma^n + a_1a_0^{n-1}\gamma^{n-1} + \cdots + a_na_0^{n-1} = 0 \\ &\Rightarrow (a_0\gamma)^n + a_1(a_0\gamma)^{n-1} + \cdots + a_na_0^{n-1} = 0. \end{aligned}$$

Segue que $a_0\gamma$ satisfaz a equação

$$y^n + a_1y^{n-1} + \cdots + a_na_0^{n-1} = 0,\ a_i \in O_v,\ a_0 \neq 0.$$

Assim, $a_0\gamma$ é inteiro sobre O_v, ou seja, $a_0\gamma \in I$. Logo, $a_0\gamma = a'$, para algum $a' \in I$. Daí,

$$\gamma = \frac{a'}{a_0},\ \text{onde } a', a_0 \in I,\ a_0 \neq 0.$$

Portanto, L é o corpo de frações de I.

Consideremos, agora, a família $\mathcal{F}$ de todos os subanéis R de L tais que

$$I \subseteq R \subset L \quad \text{e} \quad R \cap K = O_v.$$

Afirmamos que $\mathcal{F}$ tem um elemento maximal.

Com efeito, como O_v é integralmente fechado, temos que $I \cap K = O_v$. Daí, $I \in \mathcal{F}$.

Seja (R_α) um subconjunto de $\mathcal{F}$ totalmente ordenado e seja $R = \bigcup_\alpha R_\alpha$.

Temos que R é um subanel de L tal que $R \cap K = O_v$, $I \subseteq R$ e, como $L \cap K = K \neq O_v$, $R \subset L$. Logo, $R \in \mathcal{F}$.

Como $R_\alpha \subseteq R$, para todo α, temos que R é um elemento maximal de (R_α). Pelo lema de Zorn, segue que $\mathcal{F}$ tem um elemento maximal.

Seja, então, W um elemento maximal de $\mathcal{F}$.

Afirmamos que W é um subanel próprio de L maximal.

De fato, primeiramente, W não é corpo, pois o único corpo contendo I é L e $W \neq L$, visto que $L \cap K = K \neq O_v$.

Seja $c \in L$ tal que $c \notin W$. Então, $W[c] \supset W$ e, pela maximalidade de W, $W[c] \cap K \supset O_v$. Segue da maximalidade de O_v em K que $W[c] \cap K = K$. Daí, $K \subseteq W[c]$. Assim, $L \supseteq W[c] \supseteq K$. Como $L|K$ é finita, temos que $W[c]$ é um corpo. Logo, $W[c] = L$, visto que $W[c] \supset I$. Portanto, W é um subanel próprio de L maximal.

Pelo corolário 4.22, temos que a valorização w associada a W é de posto 1. ∎

Quando K é completo, podemos detereminar explicitamente a única extensão de uma valorização de K de posto 1 em uma extensão finita L de K. Este é o resultado do próximo teorema.

Teorema 5.11 *Seja K um corpo completo e seja v uma valorização de K de posto 1. Se $L|K$ é uma extensão finita de corpos, digamos de grau n, então v tem uma única extensão w em L, dada por*

$$w(\alpha) = \frac{1}{n}\, v(N_{L|K}(\alpha)),\ \textit{para todo } \alpha \in L,\ \textit{onde } N_{L|K} \textit{ denota a norma.}$$

Demonstração. Como $L|K$ é finita de grau n, temos que $L|K$ é finitamente gerada, isto é, existem $a_1, \ldots, a_n \in L$ tais que $L = K(a_1, \ldots, a_n)$.

Seja E uma extensão de L, onde E é o corpo de raízes do polinômio $p(x) = p_1(x) \cdots p_n(x)$ sobre K, sendo $p_i(x)$ o polinômio mínimo de a_i sobre K, $i = 1, \ldots, n$. Então, $E|K$ é finita e normal. Segue da proposição anterior, que v tem uma extensão, digamos w, em E e, pelo teorema 1.41, tal extensão é única.

Seja γ um K-automorfismo de $E|K$.

Afirmamos que $w \circ \gamma$ é uma valorização de E que estende v.

Com efeito, como $(w \circ \gamma)(a) = w(\gamma(a)) = w(a) = v(a)$, para todo $a \in K$, temos que $w \circ \gamma$ estende v. Resta mostrarmos, então, que $w \circ \gamma$ é uma valorização de E.

Para quaisquer $x, y \in E$, temos que:

$(V.1)$ $(w \circ \gamma)(x) = \infty \Leftrightarrow w(\gamma(x)) = \infty \Leftrightarrow \gamma(x) = 0 \Leftrightarrow x = 0$;

$(V.2)$ $(w \circ \gamma)(x+y) = w(\gamma(x+y)) \geq \min\{w(\gamma(x)), w(\gamma(y))\} = \min\{(w \circ \gamma)(x), (w \circ \gamma)(y)\}$;

$(V.3)$ $(w \circ \gamma)(xy) = w(\gamma(xy)) = w(\gamma(x)\gamma(y)) = w(\gamma(x)) + w(\gamma(y)) = (w \circ \gamma)(x) + (w \circ \gamma)(y)$.

Portanto, $w \circ \gamma$ é uma valorização de E que estende v.

Segue da unicidade que $w(\alpha) = (w \circ \gamma)(\alpha)$, para todo $\alpha \in E$.

Seja s o grau de separabilidade da extensão $L|K$ e sejam, então, $\sigma_1, \ldots, \sigma_s$ os K-homomorfismos de $L|K$. temos que, para cada $i = 1, \ldots, s$, $\sigma_i = \gamma_i|_L$, onde γ_i é um K-automorfismo de $E|K$. Daí, $\sigma_i(\alpha) \in E$, para cada $i = 1, \ldots, s$ e para todo $\alpha \in L$.

Dado $\alpha \in L$, temos que

$$N_{L|K}(\alpha) = \Big(\prod_{i=1}^{s} \sigma_i(\alpha)\Big)^{[L:K]_i},$$

onde $[L : K]_i$ denota o grau de inseparabilidade de $L|K$. Como $n = s[L : K]_i$, segue que $N_{L|K}(\alpha) = \alpha_1 \cdots \alpha_n$, onde, para cada $j = 1, \ldots, n$, $\alpha_j = \sigma_i(\alpha)$, par algum $i = 1, \ldots, s$. Em particular, $\alpha_j \in E$, para todo $j = 1, \ldots, n$. Logo,

$$v(N_{L|K}(\alpha)) = v(\alpha_1 \cdots \alpha_n) = \sum_{k=1}^{n} w(\alpha_k) = nw(\alpha).$$

Portanto,

$$w(\alpha) = \frac{1}{n}\, v(N_{L|K}(\alpha)), \text{ para todo } \alpha \in L.$$

■

5.3 Extensões de corpos incompletos

Consideraremos, agora, extensões finitas de corpos incompletos com uma valorização de posto 1. Neste caso, pela proposição 5.10, a valorização pode novamente ser estendida, mas não necessariamente será única, como veremos. Para analisarmos este problema, precisaremos do conceito de produto tensorial de álgebras.

Sejam A e B álgebras sobre o corpo K. O produto tensorial $C = B \underset{K}{\otimes} A$ é definido pela propriedade de que funções K-bilineares em $B \times A$ correspondem a funções K-lineares de C. Explicitamente, se B e A têm bases $\{v_j\}$ e $\{u_i\}$ sobre K, respectivamente, então C tem base $\{v_j \underset{K}{\otimes} u_i\}$ sobre K. Dado $x \in C$, temos que

$$x = \sum_{r=1}^{n} b_r \underset{K}{\otimes} a_r, \text{ onde } n \geq 1,\ b_r \in B \text{ e } a_r \in A,\ r = 1, \ldots, n.$$

Daí,

$$x = \sum_{r=1}^{n} \Big[\Big(\sum_{j=1}^{l} \beta_{r_j} v_j\Big) \underset{K}{\otimes} \Big(\sum_{i=1}^{m} \alpha_{r_i} u_i\Big)\Big] = \sum_{r=1}^{n}\sum_{j=1}^{l}\sum_{i=1}^{m} \beta_{r_j}\alpha_{r_i} v_j \underset{K}{\otimes} u_i.$$

Em particular, se $B = E$ é uma extensão do corpo K e $\{u_i\}$ é uma base de A sobre K, então $\{1 \underset{K}{\otimes} u_i\}$ é uma base da E-álgebra $A_E = E \underset{K}{\otimes} A$, onde a operação soma é a soma em $E \underset{K}{\otimes} A$ como K-módulo e, para quaisquer $x, y \in A_E$, com $x = \sum_r b_r \underset{K}{\otimes} a_r$ e $y = \sum_s b'_s \underset{K}{\otimes} a'_s$, e $e \in E$,

$$xy = \sum_{r,s} b_r b'_s \underset{K}{\otimes} a_r a'_s \quad \text{e} \quad ex = \sum_r e\, b_r \underset{K}{\otimes} a_r.$$

Daí, se $\dim_K A = n$, então $\dim_E A_E = n$.

Observação 5.12 *Seja E uma extensão do corpo K e seja $p(x) \in K[x]$. Então, pela propriedade universal dos produtos tensoriais,*

$$E \underset{K}{\otimes} K[x] \cong E[x] \text{ e } E \underset{K}{\otimes} (p(x)) \cong (p(x))_{E[x]},$$

onde $(p(x))$ e $(p(x))_{E[x]}$ denotam, respectivamente, o ideal gerado por $p(x)$ em $K[x]$ e o ideal gerado por $p(x)$ em $E[x]$.

Com efeito, tomamos as aplicações K-bilineares

$$\sigma : E \times K[x] \to E[x] \text{ e } \tau : E \times (p(x)) \to (p(x))_{E[x]}$$

definidos por $\sigma(e, f(x)) = ef(x)$ e $\tau(e, q(x)p(x)) = eq(x)p(x)$, que induzem, respectivamente, os isomorfismos

$$E \underset{K}{\otimes} K[x] \cong E[x] \text{ e } E \underset{K}{\otimes} (p(x)) \cong (p(x))_{E[x]}.$$

A próxima proposição nos permite descrever as extensões de valorizações de um corpo incompleto, antes, porém, recordaremos a definição de um compósito de dois corpos.

Definição 5.13 *Sejam E e F corpos. Um corpo L é dito compósito de E e de F se, e somente se, L contém cópias isomorfas de E e de F e é gerado por essas cópias.*

Proposição 5.14 *Sejam E e F corpos, ambos contendo K como subcorpo, e suponhamos que a extensão $F|K$ é separável de grau n. Então, temos um isomorfismo de E-álgebras*

$$E \underset{K}{\otimes} F \cong \prod_{i=1}^r F_i = F_1 \times \cdots \times F_r,$$

onde os corpos $F_1, \ldots, F_r$ são compósitos de E e de F.

Demonstração. Como a extensão de corpos $F|K$ é separável de grau n, temos que $F|K$ é simples, isto é, existe $\alpha \in F$, tal que $F = K(\alpha)$.

Seja $p(x) \in K[x]$ o polinômio mínimo de α sobre K e denotemos por $(p(x))$ o ideal gerado por $p(x)$ em $K[x]$. Como $F \cong K[x]/(p(x))$, segue que a sequência

$$0 \longrightarrow (p(x)) \xrightarrow{i} K[x] \xrightarrow{\varphi} F \longrightarrow 0,$$

onde i é a inclusão e φ é a avaliação em α, é exata e, portanto, a mesma se fatora. Logo, a seguinte sequência exata

$$0 \longrightarrow E \underset{K}{\otimes} (p(x)) \xrightarrow{I \otimes i} E \underset{K}{\otimes} K[x] \xrightarrow{I \otimes \varphi} E \underset{K}{\otimes} F \longrightarrow 0, \qquad (*)$$

onde, para quaisquer $e_r \in E$, $q_r(x) \in K[x]$,

$$(I \underset{K}{\otimes} i)\Big(\sum_r e_r \underset{K}{\otimes} q_r(x)p(x)\Big) = \sum_r e_r \underset{K}{\otimes} i(q_r(x)p(x)) \text{ e}$$
$$(I \underset{K}{\otimes} \varphi)\Big(\sum_r e_r \underset{K}{\otimes} q_r(x)\Big) = \sum_r e_r \underset{K}{\otimes} \varphi(q_r(x)).$$

Como $E \underset{K}{\otimes} (p(x)) \cong (p(x))_{E[x]}$ e $E \underset{K}{\otimes} K[x] \cong E[x]$, segue que a sequência exata $(*)$ tem a forma

$$0 \longrightarrow (p(x))_{E[x]} \longrightarrow E[x] \longrightarrow E \underset{K}{\otimes} F \longrightarrow 0.$$

Daí,

$$E[x]/(p(x))_{E[x]} \cong E \underset{K}{\otimes} F.$$

Seja $p(x) = q_1(x) \cdots q_r(x)$ a decomposição de $p(x)$ em fatores irredutíveis sobre E. Então, como $p(x)$ é separável, não existe repetição destes fatores. Para cada $i = 1, \ldots, r$, o quociente $F_i = E[x]/(q_i(x))$, onde $(q_i(x))$ denota o ideal gerado por $q_i(x)$ em $E[x]$, é um corpo, visto que $(q_i(x))$ é um ideal maximal de $E[x]$.

Consideremos, agora, o homomorfismo de anéis $\mu : E[x] \to \prod_{i=1}^{r} F_i$ definido por

$$\mu(\phi(x)) = (\phi(x) + (q_1(x)), \ldots, \phi(x) + (q_r(x))), \text{ para todo } \phi(x) \in E[x].$$

Seja $N(\mu)$ o núcleo de ϕ. Afirmamos que $N(\mu) = (p(x))_{E[x]}$ e que μ é sobrejetora.

De fato, o núcleo de μ é constituído de todos os polinômios $\phi(x) \in E[x]$ que são múltiplos de $q_i(x)$, para todo $i = 1, \ldots, r$. Como cada $q_i(x)$ é irredutível sobre E e não existe repetição entre eles, segue que $\phi(x) = \alpha_r(x)(q_1(x) \cdots q_r(x))$, para algum $\alpha_r(x) \in E[x]$. Daí, $\phi(x) \in (p(x))_{E[x]}$. Por outro lado, é claro que, se $\phi(x) \in (p(x))_{E[x]}$, $\phi(x) \in N(\mu)$. Portanto, $N(\mu) = (p(x))_{E[x]}$.

Resta mostrarmos que μ é sobrejetora.

Para cada $i = 1, \ldots, r$, seja α_i uma raiz de $q_i(x)$, então $F_i = E(\alpha_i)$. Daí,

$$[F_i : E] = [E(\alpha_i) : E] = \text{grau}\, q_i(x).$$

Logo,

$$\dim_E \prod_{i=1}^{r} F_i = \sum_{i=1}^{r} [F_i : E] = \sum_{i=1}^{r} \text{grau}\, q_i(x) = \text{grau}\, p(x).$$

Como $N(\mu) = (p(x))_{E[x]}$, temos que $E[x]/(p(x))_{E[x]} \cong Im(\mu)$. Daí, $\dim_E Im(\mu) = \text{grau}\, p(x)$. Assim, como

$$Im(\mu) \subseteq \prod_{i=1}^{r} F_i \quad \text{e} \quad \dim_E \prod_{i=1}^{r} F_i = \text{grau}\, p(x),$$

segue que $Im(\mu) = \prod_{i=1}^{r} F_i$ e, portanto, μ é sobrejetora.

Temos, então, que $E[x]/(p(x))_{E[x]} \cong \prod_{i=1}^{r} F_i$, isto é, $E \underset{K}{\otimes} F = \prod_{i=1}^{r} F_i = F_1 \times \ldots \times F_r$.

Para completarmos nossa demonstração, resta mostrarmos que, para cada $i = 1, \ldots, r$, F_i é um compósito de E e de F. Consideremos, então, o homomorfismo de anéis

$$\mu_i : E[x]/(p(x))_{E[x]} \to F_i$$

definido por $\mu_i(h(x) + (p(x))_{E[x]}) = h(x) + (q_i(x))$, para todo $h(x) \in E[x]$. A restrição de μ_i ao corpo E ou ao corpo $F \cong K[x]/(p(x))$ é um homomorfismo de corpos injetor, visto que seu núcleo é um ideal em E ou em F que não contém 1. Logo, F_i contém cópias isomorfas de E e de F. Ainda, como cada homomorsfismo μ_i é sobrejetor, temos que F_i é gerado por essas cópias. Portanto, F_i é um compósito de E e de F, para cada $i = 1, \ldots, r$. ∎

Corolário 5.15 *Com as notações do teorema anterior, temos que, para qualquer $\alpha \in F$,*

$$N_{F|K}(\alpha) = \prod_{i=1}^{r} N_{F_i|E}(\mu_i(\alpha)) \quad e \quad Tr_{F|K}(\alpha) = \sum_{i=1}^{r} Tr_{F_i|E}(\mu_i(\alpha)).$$

Demonstração. Com as notações do teorema anterior, sejam $\alpha \in F$ e $\psi, \mu_i(\alpha)$, respectivamente, o polinômio característico de α sobre K e a imagem de α em F_i.

Vamos mostrar que $\psi(x) = \psi_1(x) \cdots \psi_r(x)$, onde $\psi_i(x)$ é o polinômio característico de $\mu_i(\alpha)$ sobre E, $i = 1, \ldots, r$ e, daí, segue o corolário.

Seja $T : F \to F$ a aplicação linear definida por $T(x) = \alpha x$, para todo $x \in F$, e seja $\{v_1, \ldots, v_n\}$ uma base de F sobre K. Então, para cada $i = 1, \ldots, n$, temos

$$T(v_i) = \alpha v_i = \sum_{j=1}^{n} a_{ij} v_j, \text{ onde } a_{ij} \in K.$$

Por hipótese, segue que $\psi(x) = \det(xI_n - A)$, onde $A = (a_{ij})$.

Afirmamos que ψ é também o polinômio carcterístico de α sobre E , como um elemento de $E \underset{K}{\otimes} F$.

Com efeito, temos que $\{1 \underset{K}{\otimes} v_i\}$ é uma base de $E \underset{K}{\otimes} F$ sobre E. Definimos, então, a aplicação E-linear $T_\otimes : E \underset{K}{\otimes} F \to E \underset{K}{\otimes} F$ por $T_\otimes(1 \underset{K}{\otimes} v_i) = 1 \underset{K}{\otimes} T(v_i)$, para cada $i = 1, \ldots, n$. Daí,

$$T_\otimes(1 \underset{K}{\otimes} v_i) = 1 \underset{K}{\otimes} \alpha v_i = 1 \underset{K}{\otimes} \sum_{j=1}^{n} a_{ij} v_j = \sum_{j=1}^{n} a_{ij}(1 \underset{K}{\otimes} v_j), \text{ onde } a_{ij} \in K,$$

mostrando a afirmação.

Para cada $i = 1, \ldots, r$, temos que $\dim_E F_i = \text{grau}\, q_i(x)$, digamos n_i. Sejam, então, $\{v_{ij}\}_{1 \le j \le n_i}$ uma base de $F_i|E$ e $T_i : F_i \to F_i$ a aplicação linear dada por $T_i(a) = a\mu_i(\alpha)$, para todo $a \in F_i$. Temos, para cada $j = 1, \ldots, n_i$,

$$T_i(v_{ij}) = v_{ij}\mu_i(\alpha) = \sum_{k=1}^{n_i} \alpha_{ijk} v_{ik}, \text{ onde } \alpha_{ijk} \in E.$$

Daí, $\psi_i(x) = \det(xI_{n_i} - A_i)$, onde $A_i = (\alpha_{ijk})$, com $1 \le j \le n_i$ e $1 \le k \le n_i$, é o polinômio característico de $\mu_i(\alpha)$ sobre E.

Consideremos, agora, a transformação linear $S : \prod_{i=1}^{r} F_i \to \prod_{i=1}^{r} F_i$ definida por

$$S(a_1, \ldots, a_r) = (a_1\mu_1(\alpha), \ldots, a_r\mu_r(\alpha)), \text{ para todo } (a_1, \ldots, a_r) \in \prod_{i=1}^{r} F_i.$$

Temos que $\{w_{ij}\}_{1 \le i \le r, 1 \le j \le n_i}$ é uma base de $\prod_{i=1}^{r} F_i$ como E-espaço vetorial, onde

$$w_{ij} = (0, \ldots, v_{ij}, \ldots, 0), \text{ com } v_{ij} \text{ na } i\text{-ésima coordenada.}$$

Daí,

$$\begin{aligned} S(w_{ij}) &= (0, \ldots, v_{ij}\mu_i(\alpha), \ldots, 0) = (0, \ldots, \sum_{k=1}^{n_i} \alpha_{ijk} v_{ik}, \ldots, 0) \\ &= \sum_{i=1}^{n_i} (0, \ldots, \alpha_{ijk} v_{ik}, \ldots, 0) = \sum_{k=1}^{n_i} \alpha_{ijk}(0, \ldots, v_{ik}, \ldots, 0) \\ &= \sum_{k=1}^{n_i} \alpha_{ijk} w_{ij}, \text{ onde } \alpha_{ijk} \in E. \end{aligned}$$

Assim, como $E \underset{K}{\otimes} F \cong \prod_{i=1}^{r} F_i$, segue da afirmação anterior que $\psi(x) = \det(xI_n - B)$, onde B é a matriz em blocos (A_i), com $1 \leq i \leq r$, semelhante a A, e

$$\det(xI_n - A) = \det(xI_n - B) = \prod_{i=1}^{r} \det(xI_{n_i} - A_i) = \prod_{i=1}^{r} \psi_i(x).$$

Logo, $\psi(x) = \psi_1(x) \cdots \psi_r(x)$. ∎

Agora, temos condições de descrever as extensões de valorizações discretas de corpos incompletos.

Teorema 5.16 *Seja K um corpo com uma valorização discreta v e seja $F|K$ uma extensão finita separável de grau n. Então, existem, no máximo, n extensões de v a F, digamos $w_1, \ldots, w_r$, $r \leq n$. Se f_i denota o grau residual e e_i o índice de ramificação de w_i, então*

$$\sum_i e_i f_i = n.$$

Além disso, se o completamento de K com respeito a v é $\widehat{K}$ e o de F com respeito a w_i é F_i, então

$$\widehat{K} \underset{K}{\otimes} F \cong F_1 \times \cdots \times F_r. \qquad (*)$$

Demonstração. Pela proposição anterior, $\widehat{K} \underset{K}{\otimes} F$ é uma $\widehat{K}$-álgebra isomorfa a $F_1 \times \ldots \times F_r$, onde cada F_i é um corpo contendo cópias isomorfas a $\widehat{K}$ e a F.

Seja $\widehat{v}$ a valorização de $\widehat{K}$ que estende v. Pelo teorema 5.11, $\widehat{v}$ admite uma única extensão w_i a F_i, cuja restrição a F será denotada por w_i. Então, w_i estende v.

Observemos que F é um subcorpo denso no anel $\widehat{K} \underset{K}{\otimes} F$, pois o fecho $\overline{F}$ de F em $\widehat{K} \underset{K}{\otimes} F$ contém cópias isomorfas a $\widehat{K}$ e F, logo contém o corpo gerado por essas cópias, que é F_i. Portanto, F é denso em F_i. Além disso, o completamento de F com respeito a w_i é um corpo contendo cópias isomorfas a F e a $\widehat{K}$, logo o completamento tem que conter o compósito dessas cópias, que é F_i. Portanto, F_i é o completamento de F com respeito a w_i.

Cada r-upla $(\alpha_1, \ldots, \alpha_r)$ de $\widehat{K} \underset{K}{\otimes} F$ pode ser aproximada, em cada coordenada, por elementos de F na topologia definida por w_i, portanto, isto mostra que $w_1, \ldots, w_r$ são valorizações de F distintas e não-equivalentes.

Precisamos mostrar que não existem outras extensões de v.

Seja w uma valorização de F que estende v. Por continuidade, estendemos w a $\widehat{K} \underset{K}{\otimes} F$, que é um $\widehat{K}$-espaço vetorial normado completo.

Seja $\widehat{F}$ o completamento de F com respeito a w. Então, $\widehat{F}$ tem que ser um dos fatores da direita de $(*)$, isto é, $\widehat{F} \cong F_i$, para algum i e, logo, $w = w_i$. Portanto, $w_1, \ldots, w_r$ são as únicas extensões de v a F.

Seja $[F_i : \widehat{K}] = n_i$. Pelo teorema 5.4, temos que $n_i = e_i f_i$ e, por $(*)$,

$$n = [F : K] = [\widehat{K} \underset{K}{\otimes} F : \widehat{K}] = \sum_{i=1}^{r} n_i.$$

Logo, $n = \sum_{i=1}^{r} e_i f_i$. ∎

Para extensões galoisianas, este resultado assume a seguinte forma.

Teorema 5.17 *Sejam K um corpo com uma valorização discreta v, $\widehat{K}$ o completamento de K com relação a v e $F|K$ uma extensão galoisiana finita, digamos de grau n. Se $w_1, \ldots, w_r (r \leq n)$ são todas as extensões de v a F, então $e_i = e$, $f_i = f$ e, portanto, $n = ref$. Além disso, o grupo de Galois de $F|K$ age transitivamente no conjunto $\{w_1, \ldots, w_r\}$.*

Demonstração. Primeiramente, observemos que a existência das extensões $w_1, \ldots, w_r (r \leq n)$ de v a F é garantida pelo teorema anterior.

Seja G o grupo de Galois de $F|K$, isto é, $G = \mathrm{Gal}\,(F|K)$.

Afirmamos que, dada $\sigma \in G$, $w_i \circ \sigma$ é uma valorização de F cuja restrição a K coincide com v, para cada $i = 1, \ldots, r$.

Com efeito, para $i = 1, \ldots, r$, temos que:

$(V.1)$ $(w_i \circ \sigma)(\alpha) = \infty, \alpha \in F \Leftrightarrow w_i(\sigma(\alpha)) = \infty \Leftrightarrow \sigma(\alpha) = 0 \Leftrightarrow \alpha = 0$.

$(V.2)$

$$\begin{aligned}(w_i \circ \sigma)(\alpha + \beta) &= w_i(\sigma(\alpha + \beta)) = w_i(\sigma(\alpha) + \sigma(\beta)) \\ &\geq \min\{w_i(\sigma(\alpha)), w_i(\sigma(\beta))\} \\ &= \min\{(w_i \circ \sigma)(\alpha), (w_i \circ \sigma)(\beta)\}, \forall\, \alpha, \beta \in F.\end{aligned}$$

$(V.3)$

$$\begin{aligned}(w_i \circ \sigma)(\alpha\beta) &= w_i(\sigma(\alpha\beta)) = w_i(\sigma(\alpha)\sigma(\beta)) \\ &= w_i(\sigma(\alpha)) + w_i(\sigma(\beta)) \\ &= (w_i \circ \sigma)(\alpha) + (w_i \circ \sigma)(\beta), \forall\, \alpha, \beta \in F.\end{aligned}$$

Logo, $w_i \circ \sigma$ é uma valorização de F, para cada $i = 1, \ldots, r$. Ainda,

$$(w_i \circ \sigma)(a) = w_i(\sigma(a)) = w_i(a) = v(a), \text{ para todo } a \in K.$$

Portanto, $w_i \circ \sigma$ coincide com v em K.

Mostraremos, agora, que o grupo de Galois G age transitivamente no conjunto $\{w_1, \ldots, w_r\}$.

Suponhamos, por contradição, que as duas famílias de valorizações $\{w_i \circ \sigma\}$ e $\{w_j \circ \tau\}$, onde $i \neq j$, $\sigma, \tau \in G$, são disjuntas. Então, como w_i e w_j são não-equivalentes, segue do teorema da aproximação forte que existe $\alpha \in F$ tal que $(w_i \circ \sigma)(\alpha) > 0$ e $(w_j \circ \sigma)(\alpha - 1) > 0$, para todo $\sigma \in G$. Daí, $(w_j \circ \sigma)(\alpha) = 0$, para todo $\sigma \in G$. Logo,

$$v(N_{F|K}(\alpha)) = \sum_{\sigma} w_i(\sigma(\alpha)) = \sum_{\sigma} (w_i \circ \sigma)(\alpha) > 0 \text{ e, por outro lado,}$$

$$v(N_{F|K}(\alpha)) = \sum_{\sigma} w_j(\sigma(\alpha)) = \sum_{\sigma} (w_j \circ \sigma)(\alpha) = 0, \text{ o que é uma contradição.}$$

Portanto, existem $\sigma, \tau \in G$ tais que $w_i \circ \sigma = w_j \circ \tau$, ou seja, $w_j = w_i \circ \gamma$, onde temos $\gamma = \sigma \circ \tau^{-1} \in G$. Segue que $\Gamma_{w_j} \cong \Gamma_{w_i}$ e, daí, $e_j = e_i$. Ainda, dado $x \in O_{w_j}$, temos que

$$w_i(\gamma(x)) = (w_i \circ \gamma)(x) = w_j(x) \geq 0.$$

Logo, $\gamma(x) \in O_{w_i}$ e, portanto, $\gamma(O_{w_j}) \subseteq O_{w_i}$. Por outro lado, dado $x \in O_{w_i}$, digamos $x = \gamma(y), y \in F$, temos que $0 \leq w_i(x) = w_i(\gamma(y)) = (w_i \circ \gamma)(y) = w_j(y)$ e, daí, $y \in O_{w_j}$. Logo, $O_{w_i} \subseteq \gamma(O_{w_j})$ e, portanto, $\gamma(O_{w_j}) = O_{w_i}$. Segue que $O_{w_j} \cong O_{w_i}$ e $M_{w_j} \cong M_{w_i}$. Daí, $f_j = f_i$.

Como i, j são quaisquer, obtemos $e_i = e$ e $f_i = f$, para todo $i = 1, \ldots, r$. Portanto,

$$n = \sum_{i=1}^{r} e_i f_i = ref.$$

■

Para finalizarmos esta seção, apresentaremos algumas aplicações dos teoremas aqui estudados no caso em que $K = \mathbb{Q}$ e v é a valorização 3-ádica de $\mathbb{Q}$.

Exemplo 5.18 *Seja $F = \mathbb{Q}(\sqrt{5})$ e seja w uma extensão de v_3 a F. Temos que $K_{v_3} = \mathbb{F}_3$ e $L_w = \mathbb{F}_3(\beta)$, com $e = 1$, $f = 2$ e β raiz de $x^2 - 2\,(mod\,3)$. Isto segue porque $x^2 - 5$ é irredutível sobre $\widehat{\mathbb{Q}}_3$ (não podemos nem mesmo resolver a congruência $x^2 \equiv 5\,(mod\,3)$ em $\mathbb{Z}$). Observe que $\widehat{\mathbb{Q}}_3 \underset{K}{\otimes} \mathbb{Q}(\sqrt{5}) \cong \widehat{\mathbb{Q}}_3[x]/(x^2 - 5)$ já é um corpo, mostrando que há uma única extensão w de v_3 a F.*

Exemplo 5.19 *Seja $F = \mathbb{Q}(\sqrt{7})$. O polinômio $x^2 - 7$ é redutível em $\widehat{\mathbb{Q}}_3$ já que 7 é um quadrado em $\widehat{\mathbb{Q}}_3$. Nesse caso, temos que*

$$\widehat{\mathbb{Q}}_3 \underset{\mathbb{Q}}{\otimes} \mathbb{Q}(\sqrt{7}) \cong \widehat{\mathbb{Q}}_3[x]/(x - 7) \cong \widehat{\mathbb{Q}}_3[x]/(x - \sqrt{7}) \times \widehat{\mathbb{Q}}_3[x]/(x + \sqrt{7}).$$

Assim, há duas valorizações estendendo v_3 a F, ambas com $e = f = 1$, pois

$$2 = [\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = \sum_{i=1}^{2} e_i f_i = 2ef.$$

Exemplo 5.20 *Seja $F = \mathbb{Q}(\sqrt{3})$ e seja w uma extensão de v_3 a F. Temos que*

$$v_3(3) = w(3) = w((\sqrt{3})^2) = 2(w(\sqrt{3})).$$

Daí, $e = 2$ e, como $2 = \sum_{i=1}^{r} e_i f_i = ref, r = f = 1$. Logo, há uma única extensão w de v_3 a F.

5.4 Domínios de Dedekind e o teorema da aproximação forte

Nesta última seção caracterizaremos os domínios de Dedekind como a interseção de uma família de valorizações discretas que tem a propriedade da aproximação forte, provaremos que esta caracterização é equivalente à definição usual e concluiremos nosso estudo mostrando que a propriedade de ser um domínio de Dedekind é preservada por extensões algébricas separáveis.

Seja K um corpo e seja $\{v_p\}_{p \in \mathcal{S}}$ uma família de valorizações discretas de K duas a duas não-equivalentes, onde $M_{v_p} = (p)$, para todo $p \in \mathcal{S}$. Então, os elementos $p \in \mathcal{S}$ são chamados *divisores primos* ou, simplesmente, *lugares* e, a cada $p \in \mathcal{S}$, associamos, respectivamente, o anel de valorização de v_p e o seu ideal maximal

$$O_p = \{x \in K;\, v_p(x) \geq 0\} \text{ e } M_p = \{x \in K;\, v_p(x) \geq 1\}.$$

Um elemento $x \in K$ é dito *inteiro em p* se, e somente se, $x \in O_p$, isto é, $v_p(x) \geq 0$. A interseção

$$R = \bigcap_{p \in \mathcal{S}} O_p$$

de todos os anéis de valorização O_p é o subanel de K chamado *anel dos inteiros de K com respeito a $\mathcal{S}$*. Pela proposição 4.5, temos a seguinte relação de divisibilidade em K:

$$x|y \Leftrightarrow yx^{-1} \in R \Leftrightarrow v_p(x) \leq v_p(y),\, \forall\, p \in \mathcal{S}.$$

Exemplo 5.21 *Seja $K = \mathbb{Q}$. Então, tomando $\mathcal{S} = \{p \in \mathbb{N};\, p\, primo\}$, obtemos $O_p = \mathbb{Z}_{p\mathbb{Z}}$, para cada $p \in \mathcal{S}$, e $R = \mathbb{Z}$.*

Exemplo 5.22 *Considerando o corpo $K(x)$ e tomando*

$$\mathcal{S} = \{p(x) \in K(x);\, p(x)\, \text{é mônico e irredutível sobre}\, K\},$$

obtemos $O_{p(x)} = K[x]_{p(x)K[x]}$, *para cada* $p(x) \in \mathcal{S}$, *e* $R = K[x]$. *Por outro lado, tomando*

$$\mathcal{S} = \{p(x) \in K[x];\ p(x) \text{ é mônico e irredutível sobre } K\} \cup \{p(x) = x^{-1}\},$$

obtemos $O_{p(x)} = K[x]_{p(x)K[x]}$, $O_{x^{-1}} = \left\{ \dfrac{f(x)}{g(x)} \in K(x);\ grau\, g(x) \geq grau\, f(x) \right\}$ *e* $R = K$.

Observemos que, no exemplo anterior, alguma condição é necessária para garantir que R não seja muito pequeno se comparado ao corpo K. Isto nos motiva a seguinte definição.

Definição 5.23 *Dizemos que um conjunto* $\mathcal{S}$ *de lugares de* K *tem a propriedade da aproximação forte se, e somente se, as seguintes propriedades são válidas em* $\mathcal{S}$*:*

$(D.1)$ *Para cada* $p \in \mathcal{S}$, v_p *é uma valorização discreta de* K.

$(D.2)$ *Dado* $x \in K$, *temos que* $v_p(x) \geq 0$, *para quase todo* $p \in \mathcal{S}$.

$(D.3)$ *Dados* $p, p' \in \mathcal{S}$, $p \neq p'$,*e* $N > 0$, *existe* $a \in K$ *tal que*

$$v_p(a-1) > N, v_{p'}(a) > N \text{ e } v_q(a) \geq 0,\ \forall\, q \in \mathcal{S},\ q \neq p, p'.$$

Pelo teorema da aproximação forte, temos que, dados $p, p' \in \mathcal{S}$, $p \neq p'$, $N > 0$ e $1, 0 \in K$, existe $a \in K$ tal que $v_p(a-1) > N$ e $v_{p'}(a) > N$. Se o conjunto $\mathcal{S}$ tem a propriedade da aproximação forte, então a propriedade $(D.3)$ garante que podemos tomar $a \in R$ de modo que a mesma seja verdadeira. Para isto, o anel R tem que ser suficientemente grande se comparado ao corpo K, conforme veremos na proposição que segue.

Proposição 5.24 *Se o conjunto* $\mathcal{S}$ *de lugares de* K *tem a propriedade da aproximação forte, então* K *é o corpo de frações de* R.

Demonstração. É claro que o corpo de frações de R está contido no corpo K. Resta mostrarmos, então, a inclusão inversa.

Seja $a \in K$ tal que $a \notin R$. Então, pela propriedade $(D.2)$, existem $p_1, \ldots, p_n \in \mathcal{S}$ tais que $v_{p_i}(a) < 0$, $i = 1, \ldots, n$, e $v_p(a) \geq 0$, para todo $p \in \mathcal{S}$, $p \neq p_1, \ldots, p_n$.

Seja $N = \max_i \{-v_{p_i}(a)\} > 0$ e fixemos $q \in \mathcal{S}$, $q \neq p_1, \ldots, p_n$. Pela propriedade $(D.3)$, para cada $i = 1, \ldots, n$, existe $b_i \in R$ tal que

$$v_q(b_i - 1) > N,\ v_{p_i}(b_i) > N \text{ e } v_{p'}(b_i) \geq 0,$$

para todo $p' \in \mathcal{S}$, $p' \neq p_i, q$. Tomando, então, $b = b_1 \cdots b_n \in R$, segue que

$$v_{p_i}(b) = \sum_{j=1}^{n} v_{p_i}(b_j) \geq v_{p_i}(b_i), \text{ para todo } i = 1, \ldots, n.$$

Afirmamos que $ab \in R$.

Com efeito, para cada $i = 1, \ldots, n$, temos que

$$v_{p_i}(ab) = v_{p_i}(a) + v_{p_i}(b) \geq v_{p_i}(a) + v_{p_i}(b_i) > v_{p_i}(a) - v_{p_i}(a) = 0.$$

É claro que, para cada $p \in S$, $p \neq p_1, \ldots, p_n$, $v_p(ab) \geq 0$. Logo, $ab \in R$.

Seja $c \in R$ tal que $ab = c$. Então, $a = \dfrac{c}{b}$, onde $c, b \in R$, $b \neq 0$. Portanto, K é o corpo de frações de R. ∎

Teorema 5.25 *Sejam K um corpo e $\mathcal{S}$ um conjunto de lugares de K que tem a propriedade da aproximação forte. Então, para quaisquer elementos distintos $p_1, \ldots, p_n \in \mathcal{S}$, para quaisquer elementos $a_1, \ldots, a_n \in K$ e qualquer $N > 0$, existe $a \in K$ tal que*

$$v_{p_i}(a - a_i) > N, \text{ para cada } i = 1, \ldots, n \text{ e}$$
$$v_q(a) \geq 0, \text{ para todo } q \in \mathcal{S},\ q \neq p_1, \ldots, p_n.$$

Demonstração. Quando o conjunto $\mathcal{S}$ é finito, este é essencialmente o teorema da aproximação forte e, portanto, não há nada a ser demonstrado. Suponhamos, então, que o conjunto S é finito. Podemos assumir, sem perda de generalidade, que $n > 1$.

Seja M uma constante positiva qualquer.

Afirmamos que existe $b_1 \in R$ de modo que

$$v_{p_1}(b_1 - 1) > M \text{ e } v_{p_i}(b_1) > M, \text{ para todo } i = 2, \ldots, n.$$

De fato, pela propriedade $(D.3)$, para cada $i = 2, \ldots, n$, existe $c_i \in R$ tal que

$$v_{p_1}(c_i - 1) > M,\ v_{p_i}(c_i) > M \text{ e } v_q(c_i) \geq 0, \text{ para todo } q \in \mathcal{S},\ q \neq p_1, p_i.$$

Tomando, então, $b_1 = c_2 \cdots c_n \in R$, segue que

$$v_{p_i}(b_1) = \sum_{j=2}^{n} v_{p_i}(c_j) \geq v_{p_i}(c_i) > M, \text{ para todo } i = 2, \ldots, n.$$

Além disso, escrevendo

$$\begin{aligned} b_1 - 1 &= c_2 c_3 \cdots c_n - 1 \\ &= c_2 c_3 \cdots c_n - c_3 c_4 \cdots c_n + c_3 c_4 \cdots c_n - 1 \\ &= (c_2 - 1) c_3 \cdots c_n + c_3 c_4 \cdots c_n - c_4 \cdots c_n + c_4 \cdots c_n - 1 \\ &= (c_2 - 1) c_3 \cdots c_n + (c_3 - 1) c_4 \cdots c_n + \cdots + (c_{n-1} - 1) c_n + c_n - 1, \end{aligned}$$

obtemos

$$\begin{aligned} v_{p_1}(b_1 - 1) &\geq \min \left\{ v_{p_1}(c_2 - 1) + \sum_{j=3}^{n} v_{p_1}(c_j), \ldots, v_{p_1}(c_n - 1) \right\} \\ &= \min \{ v_{p_1}(c_2 - 1), \ldots, v_{p_1}(c_n - 1) \} > M. \end{aligned}$$

De maneira análoga, mostramos que existem $b_2, \ldots, b_n \in R$ tais que, para cada $i = 2, \ldots, n$,

$$v_{p_i}(b_i - 1) > M \text{ e } v_{p_j}(b_i) > M,\ \forall\, j \neq i.$$

Seja, então, $a = \sum_{i=1}^{n} a_i b_i \in K$.

Afirmamos que

$$v_{p_i}(a - a_i) > N, \text{ para cada } i = 1, \ldots, n \text{ e}$$
$$v_q(a) \geq 0, \text{ para todo } q \in \mathcal{S},\ q \neq p_1, \ldots, p_n.$$

Com efeito, para cada $i = 1, \ldots, n$, podemos assumir que $v_q(a_i) \geq 0$, para todo $q \in \mathcal{S}$, $q \neq p_1 \ldots, p_n$, visto que $v_p(a_i) < 0$ para um número finito de lugares $p \in \mathcal{S}$, os quais adicionamos, se necessário, ao conjunto $\{p_1, \ldots, p_n\}$ e tomamos os correspondentes a_i's iguais a zero. Daí, $\min\limits_{i,j} \{ v_{p_j}(a_i) \} < 0$.

Tomando, então, $M > N - \min_{i,j}\{v_{p_j}(a_i)\} > 0$, obtemos

$$\begin{aligned} v_{p_1}(a-a_1) &= v_{p_1}\Big(a_1(b_1-1)+\sum_{i=2}^{n} a_i b_i\Big) \\ &\geq \min\{v_{p_1}(a_1)+v_{p_1}(b_1-1), v_{p_1}(a_2)+v_{p_1}(b_2), \ldots, v_{p_1}(a_n)+v_{p_1}(b_n)\} \\ &> \min_i\{v_{p_1}(a_i)+M\} \\ &= \min_i\{v_{p_1}(a_i)\}+M \\ &\geq \min_{i,j}\{v_{p_j}(a_i)\}+M > N. \end{aligned}$$

Analogamente, obtemos

$$v_{p_i}(a-a_i) > N, \text{ para cada } i = 2, \ldots, n.$$

Ainda, para todo $q \in \mathcal{S}$, $q \neq p_1, \ldots, p_n$, temos que

$$v_q(a) = v_q\Big(\sum_{i=1}^{n} a_i b_i\Big) \geq \min_i\{v_q(a_i)+v_q(b_i)\} \geq 0.$$

■

Para aplicarmos este último resultado, precisaremos da noção de um ideal fracionário de um corpo K. Descreveremos, então, rapidamente a situação geral.

Sejam K um corpo, $K^* = K\backslash\{0\}$ e R um subanel de K.

Definição 5.26 *Dizemos que N é um ideal fracionário de K se, e somente se, as seguintes afirmações são verdadeiras:*

(i) N é um R-submódulo de K.

(ii) Existem $u, v \in K^*$ tais que $Ru \subseteq N \subseteq Rv$.

Exemplo 5.27 *Para cada $u \in K^*$, Ru é um ideal fracionário de K.*

Observação 5.28 (1) *Todo ideal não-nulo I de R é um ideal fracionário de K.*

Com efeito, é claro que I é um R-submódulo de K. Tomando $u \in I$, $u \neq 0$, e $1 \in K$, obtemos $Ru \subseteq I \subseteq R1$.

(2) *Se N é um ideal fracionário de K e $N \subseteq R$, então N é um ideal de R.*

Com efeito, como N é um R-submódulo de K, temos que, dados $x, y \in N$ e $a \in R$, $x+y \in N$ e $ax \in N \subseteq R$.

(3) *Se K é o corpo de frações de R, então, dado um ideal fracionário N de K, existe $b \in R$, $b \neq 0$, tal que Nb é um ideal de R.*

Com efeito, como N é um ideal fracionário de K, N é um R-submódulo de K e existe $u \in K^*$, digamos $u = \dfrac{a}{b}$ tal que $N \subseteq Ru$. Daí, $Nb \subseteq Ra \subseteq R$. É claro que Nb é um ideal de R.

A multiplicação usual de ideais pode ser estendida aos ideais fracionários de K: sejam N_1 e N_2 ideais fracionários de K, então definimos

$$N_1 N_2 = \Big\{\sum_v x_v y_v;\ x_v \in N_1, y_v \in N_2\Big\}.$$

Afirmamos que N_1N_2 é um ideal fracionário de K.

Com efeito, é claro que N_1N_2 é um R-submódulo de K. Resta mostrarmos, então, que existem $u, v \in K^*$ tais que $Ru \subseteq N_1N_2 \subseteq R_v$.

Como N_1 e N_2 são ideais fracionários de K, existem $u_1, u_2, v_1, v_2 \in K^*$ tais que

$$Ru_i \subseteq N_i \subseteq Rv_i,\ i = 1, 2.$$

Seja $x \in N_1N_2$, digamos $x = \sum_v x_v y_v$, onde $x_v \in N_1$ e $y_v \in N_2$. Então, $x_v = a_v v_1$ e $y_v = b_v v_2$, onde $a_v, b_v \in R$. Daí,

$$x = \sum_v (a_v v_1)(b_v v_2) = \sum_v (v_1 v_2)(a_v b_v) = v_1 v_2 \sum_v a_v b_v = a(v_1 v_2),$$

onde $a = \sum_v a_v b_v \in R$ e $v_1 v_2 \in K^*$. Logo, $x \in Rv_1 v_2$, onde $v_1 v_2 \in K^*$. Tomando $v = v_1 v_2$, obtemos $N_1N_2 \subseteq R_v$, onde $v \in K^*$. Por outro lado, seja $x \in Ru_1u_2$, digamos $x = a(u_1u_2)$, onde $a \in R$. Então,

$$x = a(u_1u_2) = (au_1)u_2 = (au_1)(1u_2),$$

onde $au_1 \in N_1$ e $1u_2 \in N_2$. Daí, $x \in N_1N_2$. Tomando $u = u_1u_2$, obtemos $Ru \subseteq N_1N_2$, onde $u \in K^*$e, portanto, N_1N_2 é um ideal fracionário de K.

A multiplicação de ideais fracionários é claramente associativa e

$$RN = NR = N, \text{ para todo ideal fracionário } N \text{ de } K,$$

isto é, R é o elemento neutro da multiplicação de ideais fracionários de K. Assim, o conjunto $\mathcal{F}$ de todos os ideais fracionários de K é um monóide. Além disso, dado um ideal fracionário N de K, existe um inverso generalizado de N que é definido por

$$(R : N) = \{x \in K;\ Nx \subseteq R\}.$$

Afirmamos que $(R : N)$ é um ideal fracionário de K.

De fato, dado $a \in R$, temos que

$$x \in (R : N) \Rightarrow Nx \subseteq R \Rightarrow Nxa \subseteq Ra \subseteq R \Rightarrow xa \in (R : N).$$

Além disso, se $y \in (R : N)$, então $Ny \subseteq R$ e $N(x + y) \subseteq Nx + Ny \subseteq R + R \subseteq R$.

Logo, $(R : N)$ é um R-submódulo de K.

Como N é um ideal fracionário de K, existem $u, v \in K^*$ tais que $Ru \subseteq N \subseteq Rv$. Dado $x \in (R : N)$, escrevemos $x = (xu)u^{-1}$. Como $u \in N$, temos que $xu \in R$. Daí, $x \in Ru^{-1}$. Logo, $(R : N) \subseteq Ru^{-1}$. Por outro lado, dado $x \in Rv^{-1}$, digamos $x = av^{-1}$, onde $a \in R$, temos que, para qualquer $n \in N$, existe $b \in R$ tal que $n = bv$ e, daí,

$$nx = n(av^{-1}) = (bv)(av^{-1}) = ba \in R.$$

Portanto, $Rv^{-1} \subseteq (R : N)$.

Segue imediatamente da definição de $(R : N)$ que $(R : N)N \subseteq R$.

Quando $(R : N)N = R$ dizemos que N é um *ideal fracionário invertível de* K.

Observação 5.29 (1) *Todo ideal fracionário principal de K é um ideal fracionário invertível de K.*

De fato, dado $N = Ra$, $a \in K$,, $a \neq 0$, é claro que $Ra^{-1} \subseteq (R : N)$. Por outro lado, dado $x \in K$, tal que $x \in (R : N)$, temos que $xa \in R$. Logo, $x \in Ra^{-1}$. Portanto, $(R : Ra) = Ra^{-1}$.

(2) *Se I é um ideal de R, então é fácil verificar que $(R : I) \supseteq R$. Em particular, $(R : I)I \supseteq I$.*

Retornaremos, agora, para a nossa situação inicial.

Sejam K um corpo, $\mathcal{S}$ um conjunto de lugares de K e R o anel dos inteiros de K com respeito a $\mathcal{S}$. Então, definimos o *grupo $\mathcal{D}$ dos divisores de K* como o grupo abeliano livre gerado pelo conjunto $\mathcal{S}$. Em particular, um elemento $D \in \mathcal{D}$ é chamado *divisor de K* e tem a forma

$$D = \prod p^{\alpha_p}, \text{ onde } \alpha_p \in \mathbb{Z} \text{ e } \alpha_p = 0 \text{ para quase todo } p.$$

Nosso próximo passo será relacionar o grupo $\mathcal{D}$ dos divisores de K com o monóide $\mathcal{F}$ constituído por todos os ideais fracionários de K.

Proposição 5.30 *Sejam K um corpo, $\mathcal{S}$ uma família de lugares de K e R o anel dos inteiros de K com respeito a $\mathcal{S}$. Se $\mathcal{F}$ é o monóide constituído por todos os ideais fracionários de K e $\mathcal{D}$ é o grupo de divisores de K, então a função $\phi : \mathcal{F} \to \mathcal{D}$ definida por*

$$\phi(N) = \prod p^{v_p(N)},$$

para todo ideal fracionário $N \in \mathcal{F}$, onde $v_p(N) = \min\{v_p(x); x \in N\}$, é um homomorfismo.

Demonstração. Primeiramente, mostremos que, dado $N \in \mathcal{F}$, $v_p(N) = 0$, para quase todo $p \in \mathcal{S}$.

Sejam $u, v \in K^*$ tais que $Ru \subseteq N \subseteq Rv$. Então, dado $p \in \mathcal{S}$,

(1) $u = 1u, 1 \in R \Rightarrow u \in N \Rightarrow v_p(N) \leq v_p(u)$;

(2) $x \in N \Rightarrow x = av, a \in R \Rightarrow v_p(x) = v_p(av) = v_p(a) + v_p(v) \geq v_p(v)$.

De (1) e (2), segue que $v_p(u) \geq v_p(N) \geq v_p(v)$, para todo $p \in \mathcal{S}$. Daí, $v_p(N) = 0$, para quase todo $p \in S$.

Mostremos, agora, que ϕ é, de fato, um homomorfismo.

Sejam $N, N' \in \mathcal{F}$. Dado $x \in NN'$, digamos $x = \sum_v x_v y_v$, com $x_v \in N$ e $y_v \in N'$, temos que

$$v_p(x) \geq \min_v \{v_p(x_v) + v_p(y_v)\} \geq v_p(N) + v_p(N').$$

Daí,

$$v_p(NN') \geq v_p(N) + v_p(N').$$

Seja $x_0 \in NN'$, tal que $x_0 = ab$, onde $v_p(a) = v_p(N)$ e $v_p(b) = v_p(N')$. Então,

$$v_p(x_0) = v_p(ab) = v_p(a) + v_p(b) = v_p(N) + v_p(N').$$

Segue que $v_p(NN') = v_p(x_0)$, isto é, $v_p(NN') = v_p(N) + v_p(N')$. Portanto,

$$\phi(NN') = \phi(N)\phi(N').$$

■

Em geral, não há mais nada a dizer sobre a função ϕ. No entanto, supondo que o conjunto S tem a propriedade da aproximação forte, poderemos concluir que ϕ é um isomorfismo e, daí, todo ideal fracionário de K será invertível e, portanto, $\mathcal{F}$ será um grupo. Para tal conclusão, precisaremos dos lemas que seguem.

Lema 5.31 *Sejam K um corpo e $\mathcal{S}$ uma família de lugares que tem a propriedade da aproximação forte. Então, dados qualquer subconjunto finito $\{p_1, \ldots, p_n\} \subseteq \mathcal{S}$ e quaisquer $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$, existe $a \in K$ tal que*

$$v_{p_i}(a) = \alpha_i, \text{ para cada } i = 1, \ldots, n \text{ e}$$
$$v_q(a) \geq 0, \text{ para todo } q \in \mathcal{S},\ q \neq p_1, \ldots, p_n.$$

Demonstração. Como v_{p_i} é uma valorização normalizada, existe, para cada $i = 1, \ldots, n$, $a_i \in K$ tal que $v_{p_i}(a_i) = \alpha_i$.

Seja $N > 0$, $N > \max_i \{\alpha_i\}$. Então, pelo teorema 5.25, existe $a \in K$ tal que

$$v_{p_i}(a - a_i) > N, \text{ para cada } i = 1, \ldots, n \text{ e}$$
$$v_q(a) \geq 0, \text{ para todo } q \in S,\ q \neq p_1, \ldots, p_n.$$

Escrevendo, para cada $i = 1, \ldots, n$, $a = a_i + (a - a_i)$, obtemos

$$v_{p_i}(a) \geq \min\{v_{p_i}(a_i), v_{p_i}(a - a_i)\} = \min\{\alpha_i, v_{p_i}(a - a_i)\}.$$

Como, para cada $i = 1, \ldots, n$, temos $v_{p_i}(a - a_i) > N > \alpha_i = v_{p_i}(a_i)$, segue que

$$v_{p_i}(a) = \min\{\alpha_i, v_{p_i}(a - a_i)\} = \alpha_i.$$

■

Lema 5.32 *Sejam K um corpo, $\mathcal{S}$ uma família de lugares de K que tem a propriedade da aproximação forte e R o anel dos inteiros de K com respeito a $\mathcal{S}$. Se N é um ideal fracionário de K, então, para todo $x \in K$,*

$$x \in N \Leftrightarrow v_p(x) \geq v_p(N),\ \forall\, p \in \mathcal{S},$$

onde $v_p(N) = \min\{v_p(x);\ x \in N\}$.

Demonstração. ($\Rightarrow$:) É imediata.

($\Leftarrow$:) Fixando $x \in N$, $x \neq 0$, e substituíndo N por Nx^{-1}, basta mostrarmos que

$$v_p(N) \leq 0,\ \forall\, p \in \mathcal{S} \Rightarrow 1 \in N.$$

Substituíndo N por $N \cap R$, obtemos $N \subseteq R$, em particular, N é um ideal de R e a hipótese, passa a ser $v_p(N) = 0$. Portanto, devemos mostrar:

$$v_p(N) = 0 \Rightarrow 1 \in N.$$

Seja $c \in N$, $c \neq 0$. Se $c^{-1} \in R$, então $1 = cc^{-1} \in N$ e, portanto, a implicação considerada é verdadeira. Se $c^{-1} \notin R$, então $v_p(c) > 0$ para um número finito de lugares $p \in \mathcal{S}$, digamos $p = p_1, \ldots, p_n$. Como $v_p(N) = 0$, para todo $p \in \mathcal{S}$, existe, para cada $i = 1, \ldots, n$, $a_i \in N$ tal que $v_{p_i}(a_i) = 0$.

Seja $N = \max_i \{v_{p_i}(c)\} > 0$. Fixando j e tomando $c_j = a_j^{-1}$, $c_i = 0$, com $i \neq j$, temos, pelo teorema 5.25, que existe $b_j \in R$ tal que

$$v_{p_j}(c_j - b_j) > N \geq v_{p_j}(c),$$
$$v_{p_i}(b_j) > N \geq v_{p_i}(c),\ i \neq j, \text{ e}$$
$$v_q(b_j) \geq 0 = v_q(c), \text{ para todo } q \in \mathcal{S},\ q \neq p_1, \ldots, p_n,$$

ou seja,

$$v_{p_j}(a_j^{-1} - b_j) > v_{p_j}(c) \text{ e}$$
$$v_q(b_j) \geq v_q(c), \text{ para todo } q \in \mathcal{S},\ q \neq p_j.$$

Tomemos, então, $a = \sum_i a_i b_i$.

Como, para cada $i = 1, \ldots, n$, $a_i \in N$, $b_i \in R$ e N é um R-submódulo de K, temos que $a \in N \subseteq R$. Além disso, para cada $j = 1, \ldots, n$, obtemos

$$v_{p_j}(1-a) = v_{p_j}\Big((1-a_jb_j) - \sum_{i\neq j} a_ib_i\Big) \geq v_{p_j}(c) \quad (*)$$

e, para todo $q \in \mathcal{S}$, $q \neq p_1, \ldots, p_n$, obtemos

$$v_q(1-a) \geq 0 = v_q(c). \quad (**)$$

Das desigualdades $(*)$ e $(**)$, segue que $c^{-1}(1-a) = d \in R$. Portanto, $1 = a + cd \in N$. ∎

Agora, temos condições de mostrar que a função ϕ é um isomorfismo.

Teorema 5.33 *Sejam K um corpo, $\mathcal{S}$ um conjunto de lugares que tem a propriedade da aproximação forte e R o anel dos inteiros de K com respeito a $\mathcal{S}$. Então, o conjunto dos ideais fracionários de K é um grupo abeliano livre, com a multiplicação e a inversão de ideais fracionários, gerado pelos ideais maximais de R. Além disso, este grupo é isomorfo ao grupo dos divisores de K.*

Demonstração. Vamos mostrar que a função $\psi : \mathcal{D} \to \mathcal{F}$, definida por

$$\psi(D) = \{x \in K; v_p(x) \geq \alpha_p, \text{ para todo } p \in \mathcal{S}\},$$

onde $D = \prod_{p\in S} p^{\alpha_p} \in \mathcal{D}$, é a função inversa de ϕ.

Primeiramente, mostremos que $\psi(D)$ é um ideal fracionário de K.

Dado $a \in R$, temos que

$$x \in \psi(D) \Rightarrow v_p(ax) = v_p(a) + v_p(x) \geq 0 + \alpha_p = \alpha_p, \text{ para todo } p \in \mathcal{S}.$$

Além disso,

$$x, y \in \psi(D) \Rightarrow v_p(x+y) \geq \min\{v_p(x), v_p(y)\} \geq \alpha_p, \text{ para todo } p \in \mathcal{S}.$$

Logo, $ax \in \psi(D)$ e $x + y \in \psi(D)$, daí, $\psi(D)$ é um R-submódulo de K. Resta mostrarmos que existem $u', v' \in K^*$ tais que $Ru' \subseteq \psi(D) \subseteq Rv'$.

Sejam $p_1, \ldots, p_n \in \mathcal{S}$ tais que $\alpha_{p_i} \neq 0$, $i = 1, \ldots, n$. Pelo lema 5.31, existem $u, v \in K$ tais que

$$v_{p_i}(u) = \alpha_{p_i},\ v_{p_i}(v) = -\alpha_{p_i}, \text{ para cada } i = 1, \ldots, n, \text{ e}$$
$$v_q(u) \geq 0,\ v_q(v) \geq 0, \text{ para todo } q \in \mathcal{S},\ q \neq p_1, \ldots, p_n.$$

Dado $x \in \psi(D)$, temos que

$$v_{p_i}(x) \geq \alpha_{p_i} = -v_{p_i}(v) \Rightarrow v_{p_i}(x) + v_{p_i}(v) \geq 0 \Rightarrow v_{p_i}(xv) \geq 0, \text{ para todo } i = 1, \ldots, n, \text{ e}$$
$$v_q(xv) = v_q(x) + v_q(v) \geq \alpha_q + 0 = 0, \text{ para todo } q \in \mathcal{S},\ q \neq p_1, \ldots, p_n.$$

Segue que $xv \in R$ e, daí, $x \in Rv^{-1}$. Logo, $\psi(D) \subseteq Rv^{-1}$. Por outro lado, dado $x \in Ru$, temos que $x = au$, para algum $a \in R$. Daí,

$$v_{p_i}(x) = v_{p_i}(au) = v_{p_i}(a) + v_{p_i}(u) \geq v_{p_i} = \alpha_{p_i}, \text{ para todo } i = 1, \ldots, n, \text{ e}$$
$$v_q(x) = v_q(au) = v_q(a) + v_q(u) \geq v_q(u) \geq 0 = \alpha_q, \text{ para todo } q \in \mathcal{S},\ q \neq p_1, \ldots, p_n.$$

Logo, $x \in \psi(D)$ e, portanto, $Ru \subseteq \psi(D)$. Tomando, então $u' = u$ e $v' = v^{-1}$, obtemos $Ru' \subseteq \psi(D) \subseteq Rv'$, onde $u', v' \in K^*$.

Afirmamos que, dado um ideal fracionário N de K, $\psi(\phi(N)) = N$.

Com efeito, temos que

$$\phi(N) = \prod_{p \in \mathcal{S}} p^{\alpha_p}, \text{ onde } \alpha_p = v_p(N) = \min\{v_p(x);\, x \in N\}.$$

Assim, dado $x \in N$, temos que $v_p(x) \geq v_p(N) = \alpha_p$, para todo $p \in \mathcal{S}$, e, daí, $x \in \psi(\phi(N))$. Logo, $N \subseteq \psi(\phi(N))$. Por outro lado, dado $x \in \psi(\phi(N))$, temos que $v_p(x) \geq \alpha_p = v_p(N)$, para todo $p \in \mathcal{S}$, e, daí, pelo lema 5.32, $x \in N$. Portanto, $\psi(\phi(N)) \subseteq N$.

Afirmamos agora que, dado $D \in \mathcal{D}$, $D = \prod_{p \in \mathcal{S}} p^{\alpha_p}$, $\phi(\psi(D)) = D$.

De fato, tomando $N = \psi(D)$, temos, pelo lema 5.31, que, para qualquer $p \in \mathcal{S}$ fixo, existe $x_p \in N$ tal que $v_p(x_p) = \alpha_p$. Daí, $v_p(N) = v_p(x_p)$, para todo $p \in \mathcal{S}$, ou seja, $v_p(N) = \alpha_p$, para todo $p \in \mathcal{S}$. Logo,

$$\phi(N) = \prod_{p \in \mathcal{S}} p^{v_p(N)} = \prod_{p \in \mathcal{S}} p^{\alpha_p} = D.$$

Portanto, $\phi(\psi(D)) = D$.

Assim, concluímos que ϕ é um isomorfismo e, daí, $\mathcal{F}$ é um grupo. ∎

A definição que segue não é a definição usual de um domínio de Dedekind, no entanto, mostraremos a equivalência desta com as condições que nos são familiares.

Definição 5.34 *Seja R um domínio e seja K o seu corpo de frações. Dizemos que R é um domínio de Dedekind se, e somente se, os ideais fracionários de K constituem um grupo com a multiplicação de ideais fracionários.*

Observemos que, pelo teorema anterior, o anel R dos inteiros de K com relação a um conjunto $\mathcal{S}$ de lugares, que tem a propriedade da aproximação forte, é um domínio de Dedekind. O próximo teorema nos garante que a recíproca é verdadeira. Antes, porém, recordaremos a definição de anel noetheriano e algumas de suas propriedades.

Definição 5.35 *Um anel R é dito noetheriano se, e somente se, tem uma das seguintes condições equivalentes:*

(*i*) *Todo ideal de R é finitamente gerado.*

(*ii*) *Todo subconjunto não-vazio de ideais de R tem um elemento maximal (condição maximal).*

(*iii*) *Para toda cadeia $I_0 \subseteq I_1 \subseteq \ldots$ de ideais de R, existe $n_0 \in \mathbb{N}$ tal que $I_{n_0} = I_{n_0+1} = \ldots$, isto é, toda cadeia ascendente de ideais de R é estacionária (condição da cadeia ascendente).*

Proposição 5.36 *Seja R um domínio noetheriano. Então, todo ideal não-nulo de R contém um produto finito de ideais primos não-nulos de R.*

Demonstração. Suponhamos, por contradição, que existe algum ideal não-nulo de R que não contém um produto finiton de ideais primos não-nulos de R. Então, como R é noetheriano, existe um ideal I não-nulo de R que é o elemento maximal dos ideais não-nulos de R que não contêm um produto finito de ideais primos não-nulos de R. Ainda, I não é primo e $I \neq R$. Daí, existem $b_1, b_2 \in R$ tais que $b_1, b_2 \notin I$ e, no entanto, $b_1 b_2 \in I$. Logo, $I + Rb_i \supset I$, $i = 1, 2$. Pela maximalidade de I, existem ideais primos não-nulos $p_1, \ldots, p_r$ de R tais que

$$I + Rb_1 \supseteq p_1 \cdots p_s \text{ e } I + Rb_2 \supseteq p_{s+1} \cdots p_r.$$

Segue que

$$p_1 \cdots p_r \subseteq (I + Rb_1)(I + Rb_2) \subseteq I,$$

o que é uma contradição. ∎

Proposição 5.37 *Seja R um domínio e seja K o seu corpo de frações. Suponhamos que as seguintes afirmações são verdadeiras:*

(*i*) *R é noetheriano.*

(*ii*) *R é integralmente fechado.*

(*iii*) *Todo ideal primo não-nulo de R é maximal.*

Então, todo ideal maximal p de R é invertível e $p^{-1} \supset R$.

Demonstração. Seja p um ideal maximal de R.

Afirmamos que $(R : p) \supset R$.

Já vimos que $(R : p) \supseteq R$. Basta mostrarmos, então que $(R : p) \neq R$.

De fato, dado $a \in p$, $a \neq 0$, temos, pela proposição anterior, que o ideal não-nulo Ra de R contém um produto finito de ideais primos não-nulos de R, digamos

$$Ra \supseteq p_1 \cdots p_r,$$

onde r é tomado como o mínimo tal que esta inclusão seja verdadeira. Então,

$$p \supseteq Ra \supseteq p_1 \cdots p_r.$$

Sendo p um ideal primo, temos que p contém algum p_i, digamos $p \supseteq p_1$. De (*iii*), segue que p_1 é maximal e, daí, $p = p_1$. Como $p_2 \cdots p_r \nsubseteq Ra$, existe $b \in R$ tal que $b \in p_2 \cdots p_r$ e, no entanto, $b \notin Ra$. Ainda,

$$pb \subseteq Ra \Rightarrow pa^{-1}b \subseteq R \Rightarrow a^{-1}b \in (R : p).$$

Assim, temos que $a^{-1}b \in (R : p)$ e, como $b \notin Ra$, $a^{-1}b \notin R$. Portanto, $(R : P) \supset R$.

Agora, temos que $p \subseteq (R : p)p \subseteq R$. Se $p = (R : p)p$, então, como p é finitamente gerado, temos, pelo lema 5.7, que $(R : p)$ é inteiro sobre R. Daí, por (*ii*), obtemos $(R : p) \subseteq R$, o que contradiz a afirmação acima. Logo, $p \subset (R : p)p \subseteq R$ e, como p é maximal, $(R : p)p = R$. Portanto, $(R : p) = p^{-1}$ e p é invertível. Em particular, $p^{-1} \supset R$. ∎

Proposição 5.38 *Seja R um domínio de Dedekind. Então, R é noetheriano.*

Demonstração. Seja I um ideal não-nulo de R e seja I^{-1} o seu inverso. Então, $II^{-1} = R$ e, daí,

$$1 = \sum_{i=1}^{n} a_i b_i, \text{ onde } a_i \in I \text{ e } b_i \in I^{-1}, \text{ para cada } i = 1, \ldots, n.$$

Logo, dado $x \in I$, temos que

$$x = \sum_{i=1}^{n} a_i (b_i x), \text{ onde } b_i x \in R, \text{ para cada } i = 1, \ldots, n.$$

Portanto, I é gerado por $a_1, \ldots, a_n$. ∎

Teorema 5.39 *Seja R um domínio de Dedekind e seja K o corpo de frações de R. Então, R pode ser definido como a interseção dos anéis de valorização de uma família de valorizações discretas de K não-equivalentes que tem a propriedade da aproximação forte.*

Demonstração. Sejam p_i os ideais maximais distintos de R. Então,

$$\prod_i p_i^{\alpha_i} \subseteq R, \text{ para quaisquer } \alpha_i \geq 0, \text{ e } \prod_i p_i^{\alpha_i} = R \text{ se, e somente se, } \alpha_i = 0, \text{ para todo } i.$$

Assim, os ideais maximais distintos p_i de R geram um grupo abeliano livre, digamos F_0.

Afirmamos que todo ideal não-nulo de R pertence a F_0.

De fato, suponhamos, por contradição, que existe algum ideal não-nulo de R que não pertence a F_0. Então, como R é noetheriano, pela proposição anterior, existe um ideal não-nulo I de R que é o elemento maximal dos ideais não-nulos de R que não pertencem a F_0. Como $R \in F_0$, temos que $I \subset R$. Como todo ideal próprio de um anel comutativo com unidade está contido em um ideal maximal deste anel, segue que existe i tal que $I \subseteq p_i \subset R$ e, mais ainda, $I \subset p_i \subset R$, visto que $p_i \in F_0$ e $I \notin F_0$. Tomando, então, os inversos, obtemos $R \subset p_i^{-1} \subset I^{-1}$. Logo, $I = RI \subset Ip_i^{-1} \subset R$. Pela maximalidade de I, temos que $Ip_i^{-1} \in F_0$. Daí, $I = Ip_i^{-1}p_i \in F_0$, o que é uma contradição.

Em particular, todo ideal principal de R pertence a F_0.

Afirmamos, agora, que todo ideal fracionário de K pertence a F_0.

Com efeito, dado $u \in K^*$, $u = ab^{-1}$, podemos escrever

$$Ru = RaRb^{-1} = Ra(Rb)^{-1}.$$

Pela afirmação anterior, temos que $Ra, (Rb)^{-1} \in F_0$. Logo, o ideal fracionário Ru de K pertence a F_0.

Seja N um ideal fracionário qualquer de K. Então, pela observação 5.28 item (3), existe $b \in R$, $b \neq 0$, tal que Nb é um ideal de R, digamos $Nb = I$. Daí, $N = Ib^{-1} = I(Rb)^{-1}$. Pela afirmação anterior, temos que $I, (Rb)^{-1} \in F_0$. Logo, $N \in F_0$. Portanto, F_0 contém todos os ideais fracionários de K.

Segue que o conjunto dos ideais fracionários de K é um grupo abeliano livre, com a multiplicação de ideais, gerado pelos ideais maximais p_i de R. Assim, dado $a \in K^*$, temos que o ideal fracionário Ra de K admite uma representação da forma

$$Ra = \prod p^{\alpha_p(a)}, \qquad (*)$$

onde os $\alpha_p(a)$ são inteiros quase todos nulos.

Para cada ideal maximal p de R, definimos, então, a aplicação $\alpha_p : K^* \to \mathbb{Z}$. Observemos que

$$x \in R \Leftrightarrow Rx = \prod p^{\alpha_p(x)} \subseteq R \Leftrightarrow \alpha_p(x) \geq 0, \, \forall \, p.$$

Como $R(ab) = RaRb$ e $R(a+b) \subseteq Ra+Rb$, para quaisquer $a, b \in K^*$, segue, respectivamente, que

$$\alpha_p(ab) = \alpha_p(a) + \alpha_p(b) \text{ e } \alpha_p(a+b) \geq \min\{\alpha_p(a), \alpha_p(b)\}.$$

Logo, α_p é uma valorização discreta.

Seja $\mathcal{S}$ o conjunto de lugares de K definido pelas valorizações discretas α_p, isto é,

$$O_p = \{x \in K;\, \alpha_p(x) \geq 0\} \text{ e } M_p = \{x \in K;\, \alpha_p(x) \geq 1\}.$$

Então, $x \in R \Leftrightarrow \alpha_p(x) \geq 0$, $\forall \, p \in \mathcal{S}$. Daí, $R = \bigcap_{p \in \mathcal{S}} O_p$ e $p = M_p \cap R$.

É claro que a propriedades $(D.1)$ é verdadeira. A propriedade $(D.2)$ segue do fato de que em $(*)$, $\alpha_p(a) = 0$ para quase todo $p \in \mathcal{S}$, enquanto que para qualquer ideal fracionário N de K, temos $Ru \subseteq N \subseteq Rv$, para $u, v \in K^*$, e $N = \prod p^{\alpha_p(N)}$, seguindo que $\alpha_p(u) \geq \alpha_p(N) \geq \alpha_p(v)$ e $\alpha_p(N) = 0$ para quase todo p.

Para concluírmos nossa demonstração, basta mostrarmos, então, que a propriedade $(D.3)$ é verdadeira.

Sejam p e q dois ideais maximais de R distintos. Então, $p+q=R$ e, daí, $(p+q)^{2N}=R$, para todo $N>0$. Logo,

$$R=(p+q)^{2N}\subseteq p^{2N}+p^{2N-1}q+\cdots+p^Nq^N+\cdots+pq^{2N-1}+q^{2N}\subseteq p^N+q^N.$$

Assim, podemos escrever $1=a+b$, onde $a\in p^N$ e $b\in q^N$. Daí,

$$\alpha_p(a)\geq N \text{ e } \alpha_q(1-a)\geq N.$$

Como $a\in R=\bigcap_{p\in\mathcal{S}} O_p$, segue que a propriedade $(D.3)$ é satisfeita. ∎

Observação 5.40 *Notemos que neste último teorema não assumimos que o grupo de ideais fracionários de K era abeliano libre, isto se dá como consequência.*

Teorema 5.41 ***(E. Noether)*** *Seja R um domínio e seja K o corpo de frações de R. Então, R é um domínio de Dedekind se, e somente se, as seguintes afirmações são verdadeiras:*

(i) *R é noetheriano.*

(ii) *R é integralmente fechado.*

(iii) *Todo ideal primo não-nulo de R é maximal.*

Demonstração. $(\Rightarrow:)$ Suponhamos que R é um domínio de Dedekind. Então, do fato de que todo ideal I de R é invertível, isto é, $II^{-1}=R$, segue que I é finitamente gerado e R é noetheriano. Portanto, a afirmação (i) é verdadeira.

Pela demonstração do teorema anterior, temos que o conjunto dos ideais fracionários de K é um grupo abeliano livre gerado pelos ideais maximais p de R. Assim, dado um ideal não-nulo I de R, podemos escrever $I=\prod p^{\alpha_p}$, onde os α_p's são inteiros quase todos nulos. Daí, I é um ideal primo de R se, e somente se, $\alpha_p\geq 0$ e $\sum_p \alpha_p=1$, ou seja, se, e somente se, $I=p$, para algum ideal maximal p. Portanto, se I é um ideal primo não-nulo de R, então I é um ideal maximal de R. Segue que a afirmação (iii) é verdadeira.

Resta mostrarmos, então, que a afirmação (ii) é verdadeira. Pelo teorema anterior, temos que

$$R=\bigcap_{p\in\mathcal{S}} O_p,$$

onde $\mathcal{S}$ é uma família de lugares de K. Assim, a afirmação (ii) será verdadeira se mostrarmos que todo elemento de K inteiro sobre R pertence a O_p, para todo $p\in\mathcal{S}$.

Dado $p\in\mathcal{S}$, seja π uma uniformizante da valorização discreta α_p definida como na demonstração do exemplo anterior. Então, $\alpha_p(\pi)=1$.

Seja $b\in K$ um inteiro sobre R, digamos

$$b^n+a_1b^{n-1}+\cdots+a_n=0, \text{ onde } a_i\in R,\ i=1,\ldots,n. \qquad (*)$$

Afirmamos que $b\in O_p$.

De fato, temos, pela proposição 2.44, que $b=\pi^r u$, onde $r\in\mathbb{Z}$ e u é um invertível em O_p, isto é, $\alpha_p(u)=0$. Substituindo, então, em $(*)$, obtemos

$$\begin{aligned}(\pi^r u)^n+a_1(\pi^r u)^{n-1}+\cdots+a_n=0 &\Leftrightarrow \pi^{rn}u^n+a_1\pi^{r(n-1)}u^{n-1}+\cdots+a_n=0\\ &\Leftrightarrow u^n+a_1\pi^{-r}u^{n-1}+\cdots+a_n\pi^{-rn}=0\\ &\Leftrightarrow u^n=-(a_1\pi^{-r}u^{n-1}+\cdots+a_n\pi^{-rn})\end{aligned}$$

Daí,

$$\begin{aligned}
\alpha_p(u^n) &= \alpha_p(-(a_1\pi^{-r}u^{n-1} + \cdots + a_n\pi^{-rn})) \\
&= \alpha_p(a_1\pi^{-r}u^{n-1} + \cdots + a_n\pi^{-rn}) \\
&\geq \min\{\alpha_p(a_1\pi^{-r}u^{n-1}), \ldots, \alpha_p(a_n\pi^{-rn})\} \\
&= \min\{\alpha_p(a_1) + \alpha_p(\pi^{-r}), \ldots, \alpha_p(a_n) + \alpha_p(\pi^{-rn})\} \\
&= \min\{\alpha_p(a_1) - r, \ldots, \alpha_p(a_n) - rn\}.
\end{aligned}$$

Assim, se $r < 0$, temos que $\alpha_p(u^n) > 0$, contradizendo o fato de que $\alpha_p(u) = 0$. Logo, $r \geq 0$. Segue que $b \in O_p$ e, como p é qualquer, $b \in \bigcap_{p \in \mathcal{S}} O_p = R$.

($\Leftarrow$:) Suponhamos que as afirmações $(i)a(iii)$ são verdadeiras. Para mostrarmos que R é um domínio de Dedekind, temos que mostrar que o conjunto dos ideais fracionários de K é um grupo com a multiplicação e a inversão de ideais fracionários. Para isto é suficiente mostrarmos que todo ideal de R é invertível. Com efeito, seja N um ideal fracionário de R e seja $b \in R$, $b \neq 0$, tal que Nb é ideal de R; então, por hipótese, existe N' tal que $NbN' = R$. Daí, $N'b = N^{-1}$ e, portanto, N é invertível.

Suponhamos, por contradição, que existe algum ideal não-nulo de R que não é invertível. Então, como R é noetheriano, existe um ideal I não-nulo de R que é o elemento maximal dos ideais não-nulos de R que não são invertíveis. Ainda, $I \subseteq p \subset R$, para algum ideal maximal p de R. Pela proposição 5.37 temos que existe p^{-1} e, ainda, $p^{-1} \supset R$. Segue imediatamente que $I \subset Ip^{-1} \subseteq R$. Pela maximalidade de I, temos que Ip^{-1} tem um inverso, digamos J. Logo, $Ip^{-1}J = R$. Daí, $p^{-1}J = I^{-1}$, o que é uma contradição. ∎

Concluímos observando que todo domínio principal R é um domínio de Dedekind, visto que todo ideal I de R é principal e, daí, too ideal não-nulo é invertível. Assim, $\mathbb{Z}$ e $K[x]$, onde K é um corpo, são domínios de Dedekind. Contudo, a propriedade de ser um domínio de Dedekind é preservada por extensões algébricas, o que não acontece no caso de domínios principais. Por exemplo, sejam $S = \mathbb{Z}[\sqrt{-5}\,] \subset \mathbb{Q}(\sqrt{-5})$ e $R = \mathbb{Z} \subset \mathbb{Q}$. Temos que S é o fecho inteiro de R em $\mathbb{Q}(\sqrt{-5})$ e em $\mathbb{Z}[\sqrt{-5}\,]$ temos: $2.3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, onde $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ são irredutíveis não-associados em $\mathbb{Z}[\sqrt{-5}\,]$, mostrando que $\mathbb{Z}[\sqrt{-5}\,]$ não é um domínio principal.

Para finalizar, mostraremos que a propriedade de ser um domínio de Dedekind é preservada por extensões algébricas separáveis. Antes, porém, apresentaremos, rapidamente, o conceito de divisibilidade entre divisores primos, que será necessário para obtermos o resultado desejado.

Seja $L|K$ uma extensãode corpos. Se v é a valorização de K correspondente ao divisor primo p e w é a extensão de v a L, correspondendo ao divisor primo q de L, escrevemos $q|p$ e dizemos que q *divide* p.

A razão para esta nomenclatura é que, em termos de ideais fracionários (no caso de domínios de Dedekind), $p \subseteq q$.

Observamos que se $L|K$ é uma extensão finita e separável, então, pelo teorema 5.16, existe apenas um número finito de extensões de v a L, portanto, existe apenas um número finito de $q|p$. Por exemplo, sejam $K = \mathbb{Q}$ e $L = \mathbb{Q}(\sqrt{p})$, onde p é um número natural primo. A valorização p-ádica de $\mathbb{Q}$ tem uniformizante p e sua extensão a L tem uniformizante $\pi = \sqrt{p}$, pois $w(\pi^2) = w(p) = v(p) = 1$. Logo, $w(\pi) = \frac{1}{2}$, $\Gamma_w = \frac{1}{2}\mathbb{Z}$, mostrando que $e = 2$ e, forçosamente, $f = 1$, isto é, $L_w = K_{v_p} \cong \mathbb{F}_p$. Nesse caso, $(p) = q^2$, onde $q = (\sqrt{p})$.

Teorema 5.42 *Seja R um domínio de Dedekind com corpo de frações K, seja L uma extensão finita e separável de K e seja S o fecho inteiro de R em L, isto é, $S = \{x \in L;\ x \text{ é inteiro sobre } R\}$. Então, S é um domínio de Dedekind.*

Demonstração. Pelo teorema 5.39, R pode ser definido por um conjunto de lugares S_K de K, com a propriedade da aproximação forte:

$$R = \bigcap_{p \in S_K} O_p.$$

Seja S_L o conjunto de lugares q de L tais que $q|p$, para algum $p \in S_K$. Pelo teorema 5.16, para cada $p \in S_K$, existe apenas uma número finito de $q \in S_L$ tais que $q|p$.

Pelo teorema 5.33, para S ser um domínio de Dedekind, basta mostrarmos que S_L tem as propriedades $(D.1), (D.2)$, $(D.3)$ e

$$S = \bigcap_{q \in S_L} O_q. \qquad (*)$$

Começamos por $(*)$.

Dado $\alpha \in S$, tomemos uma equação mônica com coeficientes em R, digamos

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_{n-1}\alpha + a_n = 0 \qquad (**)$$

Seja $q \in S_L$ e suponhamos, por absurdo, que $\alpha \notin O_q$. Então, $\alpha^{-1} \in O_q$, logo $\alpha^{-r} \in O_q$ para todo $r \geq 1$ e

$$\alpha = -(a_1 + a_2\alpha^{-1} + \cdots + a_n\alpha^{-(n-1)}) \in O_q,$$

o que é um absurdo. Portanto, $\alpha \in O_q$ para todo $q \in S_L$ e $S \subseteq \bigcap_{q \in S_L} O_q$.

Reciprocamente, se $\alpha \in \bigcap_{q \in S_L} O_q$, então $v_q(\alpha) \geq 0$ para todo $q \in S_L$. Tomamos a equação $(**)$ como o polinômio mínimo de α sobre K e afirmamos que $a_i \in R$, $i = 1, \ldots, n$, isto mostrará que $\alpha \in S$.

De fato, se α' é um conjugado de α (no fecho normal de K em L), então $v_q(\alpha') = v'_q(\alpha)$ para algum $q' \in S_L$ pois, pelo teorema 5.17, o grupo de Galois age transitivamente nas valorizações. Como $v_{q'}(\alpha) \geq 0$, então $v_q(\alpha') \geq 0$. Portanto, todos os conjugados de α são inteiros em cada $q \in S_L$. Os coeficientes $a_i \in K$ são funções simétricas das raízes do polinômio, logo, $v_q(a_i) \geq 0$ para todo $q \in S_L$, e daí, $v_p(a_i) \geq 0$ para todo $p \in S_K$. Portanto, $a_i \in \bigcap_{p \in S_K} O_p = R$ e concluímos que $\alpha \in S$. Isto mostra $(*)$.

Resta mostrarmos as propriedades $(D.1), (D.2)$ e $(D.3)$ para S_L.

A propriedade $(D.1)$ é consequência de S_K satisfazer $(D.1)$ e do teorema 5.4.

Para demonstrarmos $(D.2)$, seja $\alpha \in L$ e consideremos o polinômio mínimo de α sobre K. Digamos que $\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0$. Como S_K satisfaz $(D.2)$, para cada i existe um número finito de lugares de S_K tal que $a_i \notin O_p$. Portanto, existem lugares $p_1, \ldots, p_r$ em S_K tais que $v_p(a_i) \geq 0$, para todo $p \neq p_1, \ldots, p_r$. Pelo teorema 5.16, para cada p_j há apenas um número finito de lugares $q \in S_L$ tal que $q|p_j$ e, logo, α é inteiro em todo $q \nmid p_j$, $j = 1, \ldots, r$. Portanto, $v_q(\alpha) \geq 0$ para quase todo $q \in S_L$ e $(D.2)$ é válida.

Para verificar $(D.3)$, temos que mostrar: dados $q', q'' \in S_L$ e $N > 0$, existe $\alpha \in L$ tal que

$$v_{q'}(\alpha - 1) > N, v_{q''}(\alpha) > N \text{ e } v_q(\alpha) \geq 0, \forall\, q \neq q', q''.$$

Para isto, consideremos $u_1, \ldots, u_n$ uma base de $L|K$ e escolhamos $p_1, \ldots, p_r \in S_K$, tais que:

(1) $v_q(u_i) \geq 0$, para todo $q \in S_L$ com $q \nmid p_j$;

(2) podemos supor $q'|p_i$ e $q''|p_j$ para algum i e j com $1 \leq i, j \leq r$.

Pelo teorema da aproximação em L existe $\beta \in L$ tal que

$$v_{q'}(\beta - 1) > N, v_{q''}(\beta) > N \text{ e } v_q(\beta) \geq 0, \text{ para todo } q|p_j \text{ e } q \neq q', q''.$$

Agora, escrevamos $\beta = \sum_{i=1}^{n} y_i u_i$, com $y_i \in K$, e tomemos $M > 0$, o qual será fixado depois. Pelo teorema 5.25 em K, existe $x_i \in K$ tal que

$$v_{p_j}(x_i - y_i) > M, v_p(x_i) \geq 0, \text{ para } p \neq p_1, \ldots, p_r,$$

para todo $i = 1, \ldots, n$ e $j = 1, \ldots, r$. Para isto, aplicamos o teorema n vezes às r-uplas $(y_i, \ldots, y_i)$, onde $i = 1, \ldots, n$, com os lugares $p_1, \ldots, p_r$.

Seja $\alpha = \sum_{i=1}^{n} x_i u_i$. Observemos que se $q|p_j$, para algum $j = 1, \ldots, n$, então

$$v_q(\alpha - \beta) = v_q\Big(\sum_i (x_i - y_i)u_i\Big) \geq \min_i \{\mu + v_q(\mu_i)\}\Big);$$

e se $q \nmid p_j$, para todo j, então

$$v_q(\alpha) \geq \min_i \{v_q(x_i) + v_q(u_i)\} \geq 0$$

.

Agora escolhemos $M > N - v_q(u_i)$ para todo $q|p_j$, $j = 1, \ldots, r$ e $i = 1, \ldots, n$. Então,

$$\begin{gathered} v_{q'}(\alpha - 1) = v_{q'}(\alpha - \beta + \beta - 1) \geq \min\{v_{q'}(\alpha - \beta), v_{q'}(\beta - 1)\} > N, \\ v_{q''}(\alpha) = v_{q''}(\alpha - \beta + \beta) \geq \min\{v_{q''}(\alpha - \beta), v_{q''}(\beta)\} > N \text{ e} \\ v_q(\alpha) \geq 0, \text{ para todo } q \neq q', q''. \end{gathered}$$

Portanto, S_L tem as propriedades $(D.1), (D.2)$ e $(D.3)$ e S é um domínio de Dedekind. ∎

Capítulo 6

Apêndice

Grupos abelianos ordenados

Definição 6.1 *Seja Γ um grupo escrito aditivamente. Dizemos que Γ é um grupo abeliano ordenado se, e somente se, Γ é um grupo abeliano com uma relação de ordem total $\leq$ preservada pela operação do grupo, isto é,*

$$\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma, \text{ para quaisquer } \alpha, \beta, \gamma \in \Gamma.$$

Exemplo 6.2 *$\mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$ são grupos abelianos ordenados com a relação de ordem usual.*

Exemplo 6.3 *$\mathbb{Z} \times \mathbb{Z}, \mathbb{Q} \times \mathbb{Q}$ e $\mathbb{R} \times \mathbb{R}$ são grupos abelianos ordenados com a relação de ordem lexicográfica.*

Definição 6.4 *Seja Γ um grupo abeliano ordenado. Um subconjunto $\sum$ de Γ é chamado convexo se, e somente se, dados $\alpha, \beta \in \sum$ com $\alpha \leq \beta$ e qualquer $\gamma \in \Gamma$ tal que $\alpha \leq \gamma \leq \beta$ temos $\gamma \in \sum$.*

Exemplo 6.5 *Os subgrupos $\{0\}$ e Γ são subgrupos convexos do grupo abeliano ordenado Γ.*

Exemplo 6.6 *Se $\Gamma = \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, então os únicos subgrupos convexos de Γ são Γ e $\{0\}$.*

Exemplo 6.7 *Se $\Gamma = \mathbb{Z}, \mathbb{Q}$ ou $\mathbb{R}$, então os únicos subgrupos convexos de $\Gamma \times \Gamma$ são $\{0\} \times \{0\}$, $\{0\} \times \Gamma$ e $\Gamma \times \Gamma$.*

O próximo teorema nos diz que os subgrupos Δ de um grupo abeliano ordenado Γ, cujo grupo quociente Γ/Δ tem estrutura de grupo ordenado, são os subgrupos convexos de Γ. No entanto, para a apresentação do mesmo, precisaremos da definição que segue.

Definição 6.8 *Sejam Γ e Γ' grupos abelianos ordenados. Dizemos que a função $f : \Gamma \to \Gamma'$ é um homomorfismo que preserva a ordem se, e somente se, f é um homomorfismo de grupos tal que, para quaisquer $\alpha, \beta \in \Gamma$,*

$$\alpha \leq \beta \Rightarrow f(\alpha) \leq f(\beta).$$

Teorema 6.9 *Sejam Γ, Γ' grupos abelianos ordenados. Se $f : \Gamma \to \Gamma'$ é um homomorfismo que preserva a ordem, então o núcleo $N(f)$ é um subgrupo convexo de Γ. Reciprocamente, se Δ é um subgrupo convexo de Γ, então o grupo Γ/Δ tem uma única estrutura de grupo abeliano ordenado, tal que o homomorfismo canônico de grupos $\Gamma \to \Gamma/\Delta$ preserva a ordem.*

Demonstração. Sejam $\alpha, \beta \in N(f)$, com $\alpha \leq \beta$, e seja $\gamma \in \Gamma$ tal que $\alpha \leq \gamma \leq \beta$. Então, $0 = f(\alpha) \leq f(\gamma) \leq f(\beta) = 0$. Daí, $f(\gamma) = 0$. Logo, $\gamma \in N(f)$. Portanto, o núcleo $N(f)$ é um subgrupo convexo de Γ.

Reciprocamente, seja Δ um subgrupo convexo de Γ e seja $\alpha \in \Gamma$.

Afirmamos que $\alpha + \Delta$ é um subconjunto convexo de Γ.

Com efeito, dados $x, y \in \Delta$, com $\alpha + x \leq \alpha + y$, seja $\gamma \in \Gamma$ tal que $\alpha + x \leq \gamma \leq \alpha + y$. Então, $x \leq \gamma - \alpha \leq y$, onde $x, y \in \Delta$ e $\gamma - \alpha \in \Gamma$. Pela convexidade de Δ, temos que $\gamma - \alpha \in \Delta$. Logo, $\gamma \in \alpha + \Delta$. Portanto, $\alpha + \Delta$ é um subconjunto convexo de Γ.

É claro que Γ/Δ é um grupo abeliano. Então, se $\alpha \mapsto \overline{\alpha}$ é o homomorfismo canônico, definimos, para quaisquer $\alpha, \beta \in \Gamma$,

$$\overline{\alpha} \leq \overline{\beta} \Leftrightarrow \alpha \leq \beta.$$

É fácil ver que a relação de ordem acima definida no conjunto Γ/Δ é total. Resta mostrarmos que a mesma é preservada pela operação do grupo. De fato, para quaisquer $\overline{\alpha}, \overline{\beta} \in \Gamma/\Delta$ com $\overline{\alpha} \leq \overline{\beta}$ e para qualquer $\gamma \in \Gamma$ temos

$$\alpha \leq \beta \Rightarrow \alpha + \gamma \leq \beta + \gamma \Rightarrow \overline{\alpha + \gamma} \leq \overline{\beta + \gamma} \Rightarrow \overline{\alpha} + \overline{\gamma} \leq \overline{\beta} + \overline{\gamma}.$$

Segue que o homomorfismo natural preserva a ordem definida acima e esta é a única ordem preservada pelo mesmo. Portanto, o grupo Γ/Δ tem uma única estrutura de grupo abeliano ordenado tal que o homomorfismo canônico $\Gamma \to \Gamma/\Delta$ preserva a ordem. ∎

Definição 6.10 *Seja Γ um grupo abeliano ordenado. Para qualquer $\alpha \in \Gamma$, definimos*

$$|\alpha| = \begin{cases} \alpha, & se \quad \alpha \geq 0 \\ -\alpha, & se \quad \alpha < 0 \end{cases}$$

Em particular, $|\alpha| \geq 0$ para qualquer $\alpha \in \Gamma$.

Definição 6.11 *Seja Γ um grupo abeliano ordenado. Dados $\alpha, \beta \in \Gamma$, dizemos que α majora β ou que β é majorado por α se, e somente se, $|\alpha| \geq |\beta|$.*

Observação 6.12 *Seja Γ um grupo abeliano ordenado. É claro que, dados $\alpha, \beta \in \Gamma$, temos que ou α majora β ou β majora α. Além disso, os subgrupos convexos de Γ contêm todos os elementos majorados por algum de seus membros.*

De fato, sejam Δ um subgrupo convexo de Γ, $\alpha \in \Delta$, $\beta \in \Gamma$ majorado por α, isto é, $|\alpha| \geq |\beta|$. Como $|\alpha|$ e $-|\alpha|$ estão em Δ, temos que $-|\alpha| \leq |\beta| \leq |\alpha|$. Logo, $|\beta| \in \Delta$ e, portanto, $\beta \in \Delta$.

Teorema 6.13 *Em qualquer grupo abeliano ordenado o conjunto dos subgrupos convexos é totalmente ordenado pela inclusão.*

Demonstração. Sejam Δ_1 e Δ_2 subgrupos convexos de um grupo abeliano ordenado Γ. Suponhamos que $\Delta_1 \nsubseteq \Delta_2$, digamos $\alpha \in \Delta_1$ e $\alpha \notin \Delta_2$. Então, nenhum elemento de Δ_2 pode majorar α. Logo, α majora todos os elementos de Δ_2. Portanto, $\Delta_2 \subseteq \Delta_1$. ∎

Definição 6.14 *Seja Γ um grupo abeliano ordenado. O número de subgrupos convexos próprios de Γ é chamado posto de Γ.*

Exemplo 6.15 *$\mathbb{Z}, \mathbb{Q}$ e $\mathbb{R}$ são grupos abelianos ordenados de posto 1, enquanto que $\mathbb{Z} \times \mathbb{Z}, \mathbb{Q} \times \mathbb{Q}$ e $\mathbb{R} \times \mathbb{R}$ têm posto 2.*

O próximo teorema caracteriza os grupos abelianos ordenados de posto 1, os quais são de nosso interesse principal. Porém, para melhor compreender a demonstração de tal teorema, necessitaremos da seguinte definição.

Definição 6.16 *Seja S um conjunto totalmente ordenado. Um subconjunto $L \subseteq S$, $L \neq \varnothing$, é chamado segmento inferior de S se, e somente se, dados $\alpha \in L$ e $\beta \in S$, com $\beta \leq \alpha$, temos $\beta \in L$; o segmento superior de S é definido como o complementar do segmento inferior.*

Teorema 6.17 *Seja Γ um grupo abeliano ordenado. Então, Γ tem posto positivo se, e somente se, Γ é não-trivial. Além disso, as seguintes afirmações são equivalentes:*

(i) *Γ tem no máximo posto 1.*

(ii) *Γ é arquimediano, isto é, dados $\alpha, \beta \in \Gamma$, com $\alpha > 0$, existe $n \in \mathbb{N}$ tal que $n\alpha > \beta$.*

(iii) *Existe um homomorfismo injetor $\phi : \Gamma \to \mathbb{R}$ que preserva a ordem.*

Demonstração. É claro que Γ tem posto 0 se, e somente se, $\Gamma = \{0\}$. Consideraremos, então, que Γ tem posto positivo.

$(i) \Rightarrow (ii)$: Suponhamos que Γ tem posto 1. Seja $\alpha \in \Gamma$, $\alpha > 0$. Consideremos o subgrupo convexo $\Delta(\alpha)$ de Γ gerado por α. Então, $\Delta(\alpha)$ é o conjunto constituído de todos os elementos $\lambda \in \Gamma$ tais que $-n\alpha \leq \lambda \leq n\alpha$, $n \in \mathbb{N}$, isto é,

$$\Delta(\alpha) = \bigcup_{n \geq 0} I_n, \text{ onde } I_n = \{\lambda \in \Gamma;\ -n\alpha \leq \lambda \leq n\alpha\}.$$

Em particular, $\alpha \in \Delta(\alpha)$. Logo, $\Delta(\alpha) \neq \varnothing$. Assim, como Γ tem posto 1, segue que $\Gamma = \Delta(\alpha)$. Portanto, dado $\beta \in \Gamma$ existe $n \in \mathbb{N}$ tal que $\beta < n\alpha$, ou seja, Γ é arquimediano.

$(ii) \Rightarrow (iii)$: Fixemos $\lambda \in \Gamma$, $\lambda > 0$. Para qualquer $\alpha \in \Gamma$, definimos

$$L(\alpha) = \left\{\frac{m}{n} \in \mathbb{Q}\,;\, m\lambda \leq n\alpha\right\} \quad \text{e} \quad U(\alpha) = \mathbb{Q} \backslash L(\alpha).$$

De (ii), temos que $L(\alpha) \neq \varnothing$ e $U(\alpha) \neq \varnothing$.

Afirmamos que $L(\alpha)$ é um segmento inferior de $\mathbb{Q}$.

Com efeito, sejam $\dfrac{m'}{n'} \in \mathbb{Q}$ e $\dfrac{m}{n} \in L(\alpha)$ tais que $\dfrac{m'}{n'} \leq \dfrac{m}{n}$. Supondo $n, n' > 0$, temos que $m'n \leq mn'$. Como $m\lambda \leq n\alpha$, segue que $mn'\lambda \leq nn'\alpha$. Daí,

$$m'n\lambda \leq mn'\lambda \leq nn'\alpha \Rightarrow m'n\lambda \leq nn'\alpha.$$

Logo, $\dfrac{m'n}{n'n} = \dfrac{m'}{n'} \in L(\alpha)$. Portanto, $L(\alpha)$ é um segmento inferior de $\mathbb{Q}$.

Como $U(\alpha)$ é o complementar de $L(\alpha)$ em $\mathbb{Q}$, segue que $U(\alpha)$ é um segmento superior de $\mathbb{Q}$. Assim, temos um "corte de Dedekind". Dado $\alpha \in \Gamma$, definimos, então, $\phi(\alpha)$ como o número real correspondente. Desta maneira, $L(\alpha)$ consiste de todos os números racionais $\leq \phi(\alpha)$ e $U(\alpha)$ consiste de todos os números racionais $> \phi(\alpha)$. Observemos que $\phi(\lambda) = 1$.

Afirmamos que ϕ é um homomorfismo injetor de Γ em $\mathbb{R}$ que preserva a ordem.

Com efeito, sejam $\alpha, \alpha' \in \Gamma$ e $\dfrac{m}{n}, \dfrac{m'}{n'} \in \mathbb{Q}$, com $\dfrac{m}{n} \in L(\alpha)$ e $\dfrac{m'}{n'} \in L(\alpha')$; então

$$m\lambda \leq n\alpha \text{ e } m'\lambda \leq n'\alpha'.$$

Daí, supondo $n, n' > 0$, temos $mn'\lambda \leq nn'\alpha$ e $m'n\lambda \leq n'n\alpha'$. Logo,

$$(mn' + m'n)\lambda \leq nn'(\alpha + \alpha').$$

Portanto, $\dfrac{m}{n} + \dfrac{m'}{n'} \in L(\alpha + \alpha')$.

Consideremos, agora, as sequências $\left\{\dfrac{m_r}{n_r}\right\}$ e $\left\{\dfrac{m'_r}{n'_r}\right\}$ em $L(\alpha)$ e $L(\alpha')$ que convergem para $\phi(\alpha)$ e $\phi(\alpha')$, respectivamente. Então, a sequência $\left\{\dfrac{m_r}{n_r} + \dfrac{m'_r}{n'_r}\right\}$ em $L(\alpha + \alpha')$ converge para

$\phi(\alpha)+\phi(\alpha')$. Daí, $\phi(\alpha)+\phi(\alpha') \leq \phi(\alpha+\alpha')$. Por outro lado, consideremos a sequência $\left\{\frac{m''_r}{n''_r}\right\}$ em $L(\alpha+\alpha')$ que converge para $\phi(\alpha+\alpha')$. Para cada r, sejam $m_{r_0}, m'_{r_0} \in \mathbb{Z}$ tais que

$$m_{r_0}\lambda \leq n''_r\alpha < (m_{r_0}+1)\lambda, \;\; m'_{r_0}\lambda \leq n''_r\alpha' < (m'_{r_0}+1)\lambda,$$

de modo que m_{r_0}, m'_{r_0} são os maiores inteiros que satisfazem estas desigualdades. Assim, para cada r, podemos escolher $m_r, m'_r \in \mathbb{Z}$ tais que $m''_r = m_r + m'_r$, com $m_r\lambda \leq n''_r\alpha$ e $m'_r\lambda \leq n''_r\alpha'$. Para cada r, temos, então, que

$$\frac{m''_r}{n''_r} = \frac{m_r}{n''_r} + \frac{m'_r}{n''_r}, \text{ onde } \frac{m_r}{n''_r} \in L(\alpha) \text{ e } \frac{m'_r}{n''_r} \in L(\alpha').$$

Daí, $\frac{m''_r}{n''_r} \leq \phi(\alpha)+\phi(\alpha')$, para cada r. Logo, $\phi(\alpha+\alpha') \leq \phi(\alpha)+\phi(\alpha')$. Segue que

$$\phi(\alpha+\alpha') = \phi(\alpha)+\phi(\alpha')$$

e, portanto, ϕ é um homomorfismo. É claro que ϕ preserva a ordem. Resta mostrarmos, então, que ϕ é injetor. De fato, dado $\alpha \in \Gamma$, $\alpha \neq 0$, digamos $\alpha > 0$, temos que $n\alpha > \lambda$, para algum $n \in \mathbb{N}$. Como $\phi(\lambda) = 1$, obtemos

$$\phi(n\alpha) > \phi(\lambda) \Rightarrow \phi(\underbrace{\alpha+\cdots+\alpha}_{n \text{ parcelas}}) > 1 \Rightarrow \underbrace{\phi(\alpha)+\cdots+\phi(\alpha)}_{n \text{ parcelas}} > 1 \Rightarrow n\phi(\alpha) > 1.$$

Logo, $\phi(\alpha) > \frac{1}{n}$. Portanto, $\phi(\alpha) \neq 0$ e ϕ é injetor.

$(iii) \Rightarrow (i)$: Como já foi observado, $\mathbb{R}$ tem posto 1 e o subgrupo convexo de $\mathbb{R}$ gerado por qualquer elemento positivo de $\mathbb{R}$ é o próprio $\mathbb{R}$. A mesma afirmação é válida para qualquer subgrupo não-trivial de $\mathbb{R}$. ■

Corolário 6.18 *Qualquer endomorfismo f de $\mathbb{R}$ que preserva a ordem tem a forma $\alpha \mapsto \alpha\lambda$, para algum $\lambda \geq 0$ fixado. Em particular, f é um automorfismo ou f é nulo.*

Demonstração. Seja f um endomorfismo qualquer de $\mathbb{R}$ que preserva a ordem. Então, tomando $f(1) = \lambda$, temos que λ determina f completamente. Por outro lado, a função $g : \alpha \mapsto \alpha\lambda$ é um endomorfismo de $\mathbb{R}$ que preserva a ordem. Logo, f coincide com g. Se $f \neq 0$, então $\lambda = f(1) > f(0) = 0$. Segue que f é um homomorfismo bijetor e, portanto, f é um automorfismo. ■

Definição 6.19 *Um grupo abeliano ordenado Γ é dito discreto se, e somente se, o conjunto de todos os seus subgrupos convexos é bem ordenado e em cada imagem homomórfica de Γ, por um homomorfismo não-trivial que preserva a ordem, cada elemento tem um sucessor.*

Proposição 6.20 *Seja Γ um grupo abeliano ordenado discreto de posto 1. Então, Γ é isomorfo a $\mathbb{Z}$ e o único automorfismo de $\mathbb{Z}$ que preserva a ordem é a identidade.*

Demonstração. Seja λ o menor elemento positivo de Γ. Então, dado $\alpha \in \Gamma$, existe $n \in \mathbb{N}$ tal que $(n+1)\lambda > \alpha$. Se $\alpha > 0$, tomamos o menor elemento $n \in \mathbb{N}$ tal que $n\lambda \leq \alpha$. Daí, $0 \leq \alpha - n\lambda < \lambda$. Pela escolha de λ, temos que $\alpha - n\lambda = 0$, ou seja, $\alpha = n\lambda$. Analogamente, se $\alpha < 0$, obtemos $\alpha = -n\lambda$, para algum $n \in \mathbb{N}$. Portanto, $\Gamma \cong \mathbb{Z}$. A última afirmação segue do fato de que qualquer automorfismo ordenado de $\mathbb{Z}$ leva o gerador positivo nele próprio. ■

Seja Γ um grupo abeliano ordenado discreto de posto n. Consideremos a seguinte cadeia de subgrupos convexos de Γ:

$$\Gamma = \Gamma_0 \supset \Gamma_1 \supset \cdots \supset \Gamma_n = \{0\}.$$

Temos que cada quociente Γ_{i-1}/Γ_i tem posto 1. Assim, obtemos a seguinte fórmula

$$\text{posto}(\Gamma) = \text{posto}(\Gamma_i) + \text{posto}(\Gamma/\Gamma_i), \text{ para todo } i.$$

Algumas vezes, precisaremos encontrar o posto de um subgrupo não-convexo. O resultado que segue é o único necessário neste contexto.

Proposição 6.21 *Seja Γ um grupo abeliano ordenado e seja Γ' um subgrupo de Γ tal que Γ/Γ' é um grupo de torção. Então, Γ e Γ' têm o mesmo posto.*

Demonstração. Afirmamos que a correspondência $\Delta \mapsto \Delta \cap \Gamma'$ é uma bijeção entre os subgrupos convexos de Γ e os de Γ'.

De fato, dado um subgrupo convexo Δ' de Γ', temos que o conjunto

$$\Delta = \{\lambda \in \Gamma;\ |\lambda| \leq |\alpha|, \text{ para algum } \alpha \in \Delta'\}$$

é um subgrupo convexo de Γ e $\Delta \cap \Gamma' = \Delta'$. Segue que a correspondência considerada é sobrejetora. Por outro lado, sejam Δ_1 e Δ_2 subgrupos convexos de Γ tais que $\Delta_1 \cap \Gamma' = \Delta_2 \cap \Gamma'$ e seja $\alpha \in \Delta_1$. Então, como Γ/Γ' é um grupo de torção, existe $m > 0$ tal que

$$m\alpha \in \Delta_1 \cap \Gamma' = \Delta_2 \cap \Gamma'.$$

Como $|m\alpha| \geq |\alpha|$, segue que $\alpha \in \Delta_2$. Logo, $\Delta_1 \subseteq \Delta_2$. Analogamente, obtemos $\Delta_2 \subseteq \Delta_1$. Assim, $\Delta_1 = \Delta_2$ e, daí, a correspondência considerada é injetora. Segue que a mesma é bijetora e, portanto, $\text{posto}(\Gamma) = \text{posto}(\Gamma')$. ∎

Referências Bibliográficas

[1] Atyah, MacDonald, Introduction to Commutative Algebra, Addison-Wesley Publishing Company,1969.

[2] Cohn, P.H.. Algebraic Numbers and Algebraic Function, Chapman Hall Mathematics, 1991.

[3] Endler, Otto. Valuation Theory, Springer-Verlang, 1972.

[4] Endler, Otto. Teoria dos Números Algébricos, Projeto Euclides, 1986.

[5] Koblitz, Neal. p-adic Numbers, p-adic Analysis and Zeta-functions, Springer Verlang, 1977.

[6]

Livros Grátis

(http://www.livrosgratis.com.br)

Milhares de Livros para Download:

Baixar livros de Literatura
Baixar livros de Literatura de Cordel
Baixar livros de Literatura Infantil
Baixar livros de Matemática
Baixar livros de Medicina
Baixar livros de Medicina Veterinária
Baixar livros de Meio Ambiente
Baixar livros de Meteorologia
Baixar Monografias e TCC
Baixar livros Multidisciplinar
Baixar livros de Música
Baixar livros de Psicologia
Baixar livros de Química
Baixar livros de Saúde Coletiva
Baixar livros de Serviço Social
Baixar livros de Sociologia
Baixar livros de Teologia
Baixar livros de Trabalho
Baixar livros de Turismo